



Brocade SANnav Management Portal and Global View User Guide, 2.0.0

**User Guide
26 September 2019**

Copyright © 2019 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Brocade, and the stylized B logo are among the trademarks of Broadcom in the United States, the EU, and/or other countries. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

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

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, to view the licensing terms applicable to the open source software, and to obtain a copy of the programming source code, please download the open source disclosure documents in the Broadcom Customer Support Portal (CSP). If you do not have a CSP account or are unable to log in, please contact your support provider for this information.

Table of Contents

Chapter 1: Introduction.....	15
1.1 About This Document.....	15
1.2 What Is New in This Document.....	15
1.3 Supported Hardware and Software.....	17
1.4 Contacting Technical Support for Your Brocade® Product.....	18
1.5 Document Feedback.....	19
Chapter 2: Installation and Migration.....	20
2.1 Installation Overview.....	20
2.2 Migration Overview.....	20
2.3 SANnav Management Portal Deployment.....	21
2.3.1 System and Server Requirements for SANnav Management Portal.....	22
2.3.2 Installation Prerequisites for SANnav Management Portal.....	23
2.3.3 Installing the Application for Single-Node Deployment.....	25
2.3.4 Installing the Application for Multi-Node Deployment.....	27
2.3.5 Firewall Requirements for SANnav Management Portal.....	28
2.4 SANnav Global View Deployment.....	30
2.4.1 System and Server Requirements for SANnav Global View.....	30
2.4.2 Installation Prerequisites for SANnav Global View.....	31
2.4.3 Installing the SANnav Global View Application.....	32
2.4.4 Firewall Requirements for SANnav Global View.....	34
2.5 Uninstalling the SANnav Application.....	36
2.6 Additional Scripts.....	36
2.7 Configuring a Firewall for SANnav.....	38
2.8 Example of Provisioning a VM for SANnav Installation.....	38
Chapter 3: Getting Started with SANnav Management Portal.....	46
3.1 SANnav Overview.....	46
3.2 Browser Requirements.....	46
3.3 Launching SANnav Management Portal.....	47
3.4 Overview of the User Interface.....	47
3.4.1 Customizing Table Columns.....	50
3.4.2 Searching for Objects.....	50
3.4.3 Tags.....	52
3.4.4 Tagging Objects.....	52
3.4.5 Filters.....	55
3.4.5.1 Wildcards in Filters.....	56
3.4.5.2 Rules for AND and OR Filters.....	57

3.4.5.3	Creating Filters.....	58
3.4.5.4	Managing Filters.....	60
3.4.5.5	Deleting Filters.....	61
3.4.6	Creating a Network Scope.....	61
3.4.7	Setting the Date Range for Dashboards, Reports, and Events.....	63
3.5	Changing Your Password.....	64
3.6	Initial Setup and Configuration.....	65
Chapter 4:	Licensing.....	69
4.1	SANnav Licensing Overview.....	69
4.1.1	SANnav Licensing Terminology.....	69
4.1.2	SANnav License Types.....	69
4.1.3	Managed Port Count.....	70
4.2	How SANnav Licensing Works.....	70
4.3	Obtaining the Server UID.....	72
4.4	Generating a License.....	73
4.5	Adding a License to SANnav.....	75
4.6	Managing the Port Count	77
4.7	Renewing a License.....	78
4.8	Moving a License to a Different Server: Planned Migration.....	79
4.9	Moving a License to a Different Server: Unplanned Migration.....	80
4.10	Deleting a License.....	80
Chapter 5:	Security.....	81
5.1	User Management.....	81
5.1.1	Configuring Password, Lockout, and Session Policies.....	83
5.1.2	Creating Custom Roles.....	84
5.1.3	Creating Custom AORs.....	85
5.1.4	Creating a User Account.....	86
5.2	Unlocking a User Account.....	87
5.3	SANnav Management Portal User Account Privileges.....	88
5.4	Configuring SANnav to Use an External Server for Authentication.....	90
5.5	LDAP Server Configuration.....	92
5.5.1	Adding LDAP Servers to the Docker Container.....	93
5.5.2	Creating Role and AOR Custom Attributes in the LDAP Active Directory.....	93
5.5.3	Assigning Roles and AORs to Users on the LDAP Server.....	94
5.5.4	Assigning Roles and AORs to LDAP Groups in SANnav.....	95
5.6	RADIUS Server Configuration.....	96
5.6.1	Configuring SANnav Credentials on the RADIUS Server.....	97
5.6.2	Assigning Roles and AORs to Users on the RADIUS Server.....	98
5.6.3	Configuring Role and AOR Attributes on the RADIUS Server.....	99

5.7 TACACS+ Server Configuration	100
5.7.1 Assigning Roles and AORs to Users on the TACACS+ Server.....	101
5.8 Managing Signed Certificates	101
Chapter 6: Monitoring	103
6.1 Discovery	103
6.1.1 Discovering a Fabric.....	104
6.1.2 Stopping Switch Monitoring.....	106
6.1.3 Stopping Fabric Monitoring.....	107
6.1.4 Resuming Switch Monitoring.....	108
6.1.5 Resuming Fabric Monitoring.....	109
6.1.6 Rediscovering a Switch.....	110
6.1.7 Rediscovering a Fabric.....	111
6.1.8 Changing the Seed Switch.....	112
6.1.9 Deleting a Fabric.....	113
6.1.10 Configuring Fabric Tracking.....	114
6.1.11 Updating Fabric Members.....	115
6.2 Dashboards	116
6.2.1 Changing the Favorite Dashboard.....	117
6.2.2 Creating a Dashboard Quickly.....	117
6.2.3 Creating a Dashboard with a Customized Layout.....	120
6.2.4 Viewing Dashboards.....	122
6.2.5 Exporting Dashboard Templates.....	124
6.2.6 Importing Dashboard Templates.....	125
6.2.7 Sharing Dashboards and Reports with Other Users.....	126
6.2.8 Health Summary Dashboard.....	127
6.2.8.1 Customizing the Health Score for Managed Entities.....	129
6.2.8.2 Monitoring SAN Health and Status Daily.....	131
6.2.8.3 Factors Contributing to the Overall Health Score.....	133
6.2.9 Network Port Traffic Conditions Dashboard.....	135
6.2.9.1 Troubleshooting Mode for Network Port Traffic Conditions Dashboard.....	136
6.2.9.2 Congestion Severity States.....	139
6.3 Reports	140
6.3.1 Creating a Report Template.....	140
6.3.2 Editing a Report Template.....	143
6.3.3 Scheduling a Report.....	145
6.3.4 Generating and Exporting Reports.....	146
6.3.5 Exporting Report Templates.....	147
6.3.6 Importing Report Templates.....	148
6.4 Widgets for Dashboards and Reports	149
6.4.1 Performance Widgets.....	152

6.4.2 Status Widgets: Dashboard.....	156
6.4.3 Status Widgets: Reports.....	157
6.5 Performance Monitoring.....	157
6.5.1 Launching Investigation Mode.....	158
6.5.2 Collecting Items in the Sidebar for Investigation Mode.....	160
6.5.3 Using Investigation Mode.....	162
6.5.4 Scheduling High-Granularity Data Collection.....	168
6.5.5 Enabling and Disabling Historic Data Collection.....	170
6.6 Inventory Management.....	171
6.6.1 Adding Custom Fields to a Managed Object.....	172
6.6.2 Identifying Switches to Plan for an Upgrade.....	175
6.6.3 Putting a Switch in Maintenance Mode.....	177
6.6.4 Disabling and Enabling a Switch.....	178
6.6.5 Disabling and Enabling a Switch Port.....	179
6.6.6 Decommissioning E_Ports.....	180
6.6.7 Decommissioning F_Ports.....	181
6.6.8 Registering a CIMOM Server for F_Port Decommissioning.....	183
6.6.9 Viewing Physical Switch Properties.....	184
6.6.10 Renaming Switch Ports, Switches, and Fabrics.....	185
6.6.11 Creating Host and Storage Enclosures.....	187
6.6.12 Mapping Host and Storage Ports.....	188
6.6.13 Converting Initiator and Target Device Types.....	190
6.6.14 Launching Web Tools.....	191
6.6.15 Managing Trunk Inventory.....	192
6.6.16 Exporting Inventory Names and Mapping.....	192
6.6.17 Importing Inventory Names and Mapping.....	193
6.7 Topology Visualization.....	195
6.7.1 Viewing the Fabric Topology.....	196
6.7.2 Showing All Devices in a Fabric.....	201
6.7.3 Viewing Connectivity between Hosts and Storage.....	203
6.7.4 Viewing Link Utilization.....	205
6.7.5 Viewing a Zone Topology.....	208
6.8 Flow Management.....	209
6.8.1 Flow Management Setup.....	209
6.8.2 Configuring vTap for AMP Flow Monitoring.....	210
6.8.3 I/O Violation Summary.....	212
6.8.4 Inventory and IT Reservation.....	213
6.8.4.1 Determining Whether the Switch Is Sending Telemetry Data to the SANnav Server.....	213
6.8.4.2 Viewing the Number of Flows Monitored by the AMP Switch.....	214
6.8.4.3 Reserving a Number of IT Flows to Be Monitored by AMP.....	215

6.8.5 Operating the Flows Window.....	215
6.8.6 Accessing and Exploring Flow Investigation Mode.....	221
6.8.7 Operating in Flow Investigation Mode.....	224
6.8.8 Investigating Flows from Switch Ports.....	231
6.8.9 Creating a Flow Collection.....	236
6.8.9.1 Creating a Flow Filter.....	241
6.8.9.2 Importing and Exporting a Collection.....	243
6.8.10 Creating a Custom Rule Set.....	244
6.8.10.1 Managing a Custom Rule Set.....	245
6.8.10.2 Importing and Exporting a Custom Rule Set.....	247
6.8.11 Investigating an Aggregated Collection View.....	247
6.8.12 Report Widgets for AMP.....	252
6.8.12.1 Generating a Time Series Report of Collection Aggregation.....	253
6.8.12.2 Generating a Time Series Report for Flow Violations.....	257
6.8.12.3 Generating a Top N Report for Collection Aggregation.....	261
6.8.12.4 Generating a Top N Report for SCSI Errors.....	266
6.8.12.5 Generating a Top N Report for Host Ports.....	270
6.8.12.6 Generating a Top N Report for Storage Ports.....	275
Chapter 7: Configuration.....	280
7.1 Policy-Based Configuration.....	280
7.1.1 Creating a Configuration Policy.....	280
7.1.2 Configuring a New Switch Before Adding It to the Fabric.....	284
7.1.3 Configuring a New Switch After Adding It to the Fabric.....	286
7.1.4 Monitoring Configuration Drifts.....	288
7.1.5 Resolving Configuration Drifts.....	289
7.1.6 Configuration Blocks.....	290
7.2 Switch Configuration Backup and Restore.....	298
7.2.1 Backing Up Switch and Logical Fabric Configurations.....	298
7.2.2 Restoring Switch or Logical Fabric Configurations.....	300
7.2.3 Managing Switch Configuration Backups.....	303
7.3 Call Home and ESRS.....	304
7.3.1 Supporting the SANnav License for Call Centers	305
7.3.2 Call Home Events.....	305
7.3.3 Configuring Call Home Notifications.....	306
7.3.4 Configuring the Dell EMC Call Home Support Center.....	308
7.3.5 Enabling and Disabling a Call Home Center.....	310
7.3.6 Call Home Email Notifications.....	311
7.4 Zoning	311
7.4.1 Zone Database Size.....	311
7.4.2 Naming Conventions.....	311

7.4.3	Creating Zone Aliases.....	312
7.4.3.1	Creating a Single Zone Alias with Multiple Members.....	312
7.4.3.2	Creating Multiple Zone Aliases.....	313
7.4.3.3	Importing Zone Aliases.....	315
7.4.3.4	Exporting Zone Aliases.....	316
7.4.4	Configuring Zones in a Fabric.....	316
7.4.4.1	Creating Standard Zones.....	317
7.4.4.2	Creating Peer Zones.....	318
7.4.4.3	Creating LSAN Zones.....	320
7.4.4.4	Creating LSAN Peer Zones.....	322
7.4.4.5	Selecting and Adding Multiple Zone Aliases to a Zone.....	324
7.4.5	Creating Zone Configurations.....	328
7.4.5.1	Selecting and Adding Multiple Zones to a Zone Configuration.....	332
7.4.5.2	Saving the Inactive Zone DB to the Offline Zone DB.....	334
7.4.6	Identifying the Zones without Any Zone Configuration.....	334
7.4.7	Offline Zoning.....	335
7.4.7.1	Creating Offline Zone Configurations.....	335
7.4.7.2	Importing an Offline Zone Configuration.....	337
7.4.7.3	Exporting an Offline Zone Configuration.....	338
7.4.7.4	Saving the Offline Zone Database to the Switch.....	338
7.4.7.5	Creating Offline Zones.....	339
7.4.8	Creating Peer Zones with a Simplified Workflow.....	340
7.4.9	Configuring the Zoning Policy.....	343
7.4.10	Modifying a Zone Configuration.....	343
7.4.11	Comparing Effective and Defined (Modified) Zone Configurations.....	345
7.4.12	Viewing Zone and Zone Configuration Details.....	347
7.4.12.1	Viewing Online or Offline Zone Details.....	347
7.4.12.2	Viewing Online or Offline Zone Configuration Details.....	349
7.5	Virtual Fabrics.....	352
7.5.1	Supported Platforms for Virtual Fabrics.....	353
7.5.2	Creating a Logical Fabric.....	353
7.5.3	Adding Logical Switches to a Logical Fabric.....	356
7.5.4	Activating a Logical Fabric.....	359
7.5.5	Editing Logical Fabrics and Switches.....	361
7.5.5.1	Editing a Logical Fabric.....	361
7.5.5.2	Editing a Logical Switch.....	362
7.5.6	Deleting Logical Fabrics and Switches.....	364
7.5.6.1	Deleting a Logical Fabric.....	364
7.5.6.2	Deleting a Logical Switch.....	365
7.5.7	Fabric Properties for Logical Fabrics.....	366

7.5.8 Logical Fabric Events.....	366
7.6 Monitoring and Alerting Policy Suite.....	367
7.6.1 MAPS Structural Elements.....	368
7.6.2 MAPS Actions.....	368
7.6.3 MAPS Categories.....	370
7.6.4 MAPS Groups.....	371
7.6.5 MAPS Violations.....	372
7.6.5.1 Viewing MAPS Violations.....	373
7.6.6 MAPS Rules.....	373
7.6.7 MAPS Conditions.....	373
7.6.8 MAPS Policies.....	374
7.6.9 MAPS Measures.....	374
7.6.9.1 Port Health.....	375
7.6.9.2 Switch Policy Status.....	376
7.6.9.3 Fabric State Changes.....	377
7.6.9.4 FRU Health.....	378
7.6.9.5 Security Health.....	379
7.6.9.6 Switch Resources.....	380
7.6.9.7 Extension Tunnel.....	380
7.6.9.8 Traffic/Flows Performance.....	381
7.6.9.9 FPI.....	382
7.6.9.10 GigE Port.....	382
7.6.9.11 Backend Port Monitoring.....	383
7.6.10 MAPS Configuration.....	383
7.6.10.1 Configuring a MAPS Policy and Applying It to Multiple Switches.....	384
7.6.10.2 Managing MAPS Configure Actions on a Switch.....	386
7.6.10.3 Enabling or Disabling Policy Actions on a Switch.....	395
7.6.10.4 Configuring an Email Notification for MAPS.....	395
7.7 Fibre Channel Routing.....	396
7.7.1 License Requirements for Fibre Channel Routing.....	396
7.7.2 Supported Platforms for Fibre Channel Routing.....	397
7.7.3 Limitations of Fibre Channel Routing.....	397
7.7.3.1 Backbone Fabric ID Conditions.....	398
7.7.4 Configuring a Backbone Fabric.....	398
7.7.5 Editing a Backbone Fabric.....	401
7.7.6 Viewing the FCR Topology.....	402
7.8 vCenter Discovery.....	405
7.8.1 Adding the vCenter.....	405
7.8.2 Monitoring or Unmonitoring ESXi Hosts.....	405
7.8.3 Rediscovering ESXi Hosts.....	405

7.8.4 Viewing ESXi Host Properties.....	406
7.8.5 Investigating Virtual Machines.....	406
7.8.6 Viewing Virtual Machine Properties.....	407
7.8.7 Viewing ESXi Hosts in Topology.....	408
7.8.8 Creating a VM Alarms Dashboard.....	410
7.9 FICON.....	410
7.9.1 Viewing FICON Fabrics.....	412
7.9.2 Configuring the FICON Display.....	414
7.9.3 FICON Planning.....	415
7.9.3.1 Planning the Configuration.....	415
7.9.4 FICON Fabric Configuration.....	416
7.9.4.1 Configuring a Cascaded FICON Fabric.....	417
7.9.4.2 Adding FICON Logical Switches to a Cascaded FICON Fabric.....	420
7.9.4.3 Adding Ports to a FICON Logical Switch.....	422
7.9.4.4 Port Address Binding.....	423
7.9.5 Cascaded FICON Fabric Merge.....	423
7.9.5.1 Merging Two Cascaded FICON Fabrics.....	424
7.9.5.2 Resolving Merge Conflicts.....	426
7.9.5.3 Resolving Domain ID Conflicts.....	426
7.9.6 Activating a FICON Fabric.....	427
7.9.6.1 Deployment Behavior.....	428
7.9.6.2 Post Deployment Behavior.....	430
7.9.7 Deleting FICON Fabrics and FICON Logical Switches.....	430
7.9.7.1 Deleting a FICON Fabric.....	430
7.9.7.2 Deleting a FICON Logical Switch.....	431
7.9.8 Connecting Cascaded FICON Fabrics over FCIP.....	431
7.9.8.1 Planning the Cascaded FICON Fabrics over FCIP Configuration.....	431
7.9.8.2 Configuring IP Links and Merging the Fabrics.....	432
7.9.8.3 Configuring DWDM Links to Use R_RDYs.....	434
7.9.8.4 Extending RDR Applications over FCIP.....	434
Chapter 8: Event Management.....	437
8.1 Event Management Overview.....	437
8.1.1 Functions of Event Management.....	437
8.1.2 Types of Registration.....	437
8.1.3 Registering for SNMP Traps.....	437
8.1.4 Registering for Syslog.....	438
8.1.4.1 Importing the Server Syslog Certificate Using a CLI Script.....	439
8.1.5 Enabling or Disabling SNMP Informs.....	440
8.1.6 Enabling Event Notifications.....	441
8.1.7 Setting the Frequency to Receive Email Event Notifications.....	442

8.1.8	Configuring an Email Setup.....	443
8.1.9	Defining the Trap Configuration.....	444
8.1.10	Forwarding.....	445
8.1.10.1	Filtering Traps and Messages.....	445
8.1.10.2	Adding a Forwarding Destination.....	447
8.1.10.3	Adding Trap Forwarding Credentials.....	449
8.1.11	Managing Event Actions.....	450
8.1.11.1	Configuring Identification and Action.....	451
8.1.11.2	Creating Events and Policy.....	453
8.1.11.3	Creating Sources.....	455
8.1.11.4	Creating an Event Action for Critical Events.....	457
8.1.11.5	Using Event Action to Suppress Selected Events.....	460
8.1.11.6	Auto Acknowledging Events Based on Event Description.....	463
8.1.12	Filtering Events.....	467
8.1.13	Searching Events.....	470
8.1.14	Viewing Violations.....	471
8.1.15	Acknowledging or Unacknowledging Events.....	473
8.1.15.1	Acknowledging or Unacknowledging a Single Event.....	473
8.1.16	Setting Event Management Reports and Dashboard Widgets.....	474
8.1.16.1	Exporting Event Management Reports.....	477
Chapter 9: Extension Tunnels and Circuits.....		480
9.1	Overview of Extension Tunnels.....	480
9.2	Applying the Extension Dashboard.....	480
9.3	Configuring IPsec Policies.....	488
9.3.1	Creating an IPsec Policy.....	488
9.3.2	Editing an IPsec Policy.....	491
9.3.3	Deleting an IPsec Policy.....	493
9.4	Configuring an Extension Tunnel.....	494
9.5	Editing an Extension Tunnel.....	504
9.6	Deleting a Tunnel.....	507
Chapter 10: Switch Maintenance and Support.....		508
10.1	Firmware Management.....	508
10.1.1	Importing Firmware Files to the Repository.....	508
10.1.2	Managing the Repository.....	510
10.1.3	Updating a Selected Switch from an Internal or External Location	510
10.1.4	Updating the Firmware for One or More Switches from an Internal or External Location.....	512
10.2	Switch SupportSave.....	515
10.2.1	Requirements.....	516
10.2.2	Generating SupportSave for One or More Switches.....	516

10.2.3 Scheduling SupportSave for One or More Switches.....	518
10.2.4 Configuring Trace Dump.....	521
10.2.5 Managing the Switch SupportSave Files.....	521
Chapter 11: SANnav Management Portal Maintenance and Support.....	523
11.1 SANnav Backup and Restore.....	523
11.1.1 Configuring a Scheduled Backup.....	524
11.1.2 On-demand Backup.....	526
11.1.3 Restoring Backup Files.....	526
11.2 Management Portal Server Support Data Collection	527
11.2.1 Generating the Support Data Collection File.....	527
11.2.2 Splitting and Merging SANnav Support Data Files.....	529
11.2.2.1 Splitting SANnav Support Data Files.....	529
11.2.2.2 Merging SANnav Support Data Files.....	530
11.2.3 Downloading the Support Data Collection Files	530
11.2.4 Sending Support Data Collection Files to an FTP Server.....	530
11.2.5 Deleting the Support Data Collection Files.....	531
Chapter 12: Troubleshooting and Diagnostics.....	532
12.1 Master Node Failure.....	532
12.2 Worker Node Failure.....	532
12.3 No Login Page.....	532
12.4 Dashboard Shows No Data for Switches.....	533
12.5 High-Granularity Data Collection Schedule Option Is Unavailable.....	534
12.6 Network Port Traffic Conditions Dashboard Is Blank.....	534
12.7 Repository Tab Not Available for Firmware Management or Switch SupportSave.....	535
12.8 Firmware Download or Switch SupportSave Fails.....	535
12.9 Updating the OS with SANnav Installed.....	535
12.10 Switch Busy Message.....	536
12.11 D_Port Testing.....	536
12.11.1 Starting D_Port Testing.....	536
12.11.2 Scheduling D_Port Testing.....	538
12.11.3 Viewing D_Port Test Results.....	539
12.11.4 Deleting a Scheduled D_Port Test.....	541
Chapter 13: SANnav Global View.....	542
13.1 Overview of SANnav Global View.....	542
13.2 Browser Requirements for SANnav Global View.....	542
13.3 SANnav Global View Compatibility Matrix.....	542
13.4 Logging In to SANnav Global View.....	543
13.5 Quick Tour of SANnav Global View.....	543
13.6 Global View Licensing.....	545

13.7 Creating a New User Account	545
13.7.1 Global View Authentication and Authorization.....	547
13.8 Adding a SANnav Management Portal Instance	547
13.9 Global Dashboard Overview	548
13.9.1 Monitoring Fabric Health.....	549
13.9.2 Monitoring Switch Health across Management Portal Instances.....	551
13.9.3 Displaying Port Usage Details.....	552
13.9.4 Viewing Alerts.....	553
13.10 Creating a Global Report Template	555
13.11 Global View Inventory Management	558
13.11.1 Viewing Inventory Using Filters.....	558
13.11.2 Viewing Performance Measures in the Switch Port Inventory.....	560
13.11.3 Investigating Switch Ports in SANnav Global View.....	562
13.11.4 Exporting Inventory Views.....	563
13.12 Viewing Global View Events	564
13.13 Global View Password and Lockout Policy	565
13.14 Global View Support Data Collection	566
13.15 Global View Backup	567
13.16 Global View Email Setup	567
Chapter 14: Exporting Select Configurations from Brocade Network Advisor to SANnav Management Portal	569
14.1 Overview of Exporting Select Configurations.....	569
14.2 Exporting End Device Names.....	569
14.3 Importing End Device Names as Zone Aliases.....	569
14.4 Exporting Host or Storage Port Mapping.....	570
14.5 Importing Host or Storage Port Mapping.....	570
14.6 Exporting a MAPS Policy.....	571
14.7 Importing MAPS Policies.....	571
Chapter 15: SANnav REST API Overview	572
15.1 Overall Strategy for the SANnav Management Portal REST API.....	572
15.2 Using the SANnav Management Portal REST API.....	572
15.3 SANnav Management Portal Examples.....	573
15.3.1 Logging In and Out.....	573
15.3.2 Discovery Module.....	574
15.3.3 FCR Module.....	576
15.3.4 Fault Module.....	578
15.3.5 Inventory Search Module.....	583
Chapter 16: Revision History	590

Introduction

1.1 About This Document

This guide describes how to monitor and manage your storage area network (SAN) using Brocade SANnav Management Portal and Brocade SANnav Global View. This guide also includes installation procedures.

Within this document, information that pertains to both SANnav Management Portal and SANnav Global View products is referred to simply as "SANnav"; whereas information that pertains to only one or the other refers to the specific product.

1.2 What Is New in This Document

This document includes new and modified information for the SANnav 2.0.0 release.

- Updated screen captures and instructions throughout to reflect the user interface design and navigation changes:
 - The main navigation bar moves from the left side to the top of the page. Navigation links are changed from icons to text.
 - The search box is changed to a magnifying glass icon that expands when you click it. Search now includes the "page content" category to allow searches on the current page content.
 - A new sidebar replaces the collection bucket for selecting items to investigate.
 - The **Configurations and Settings** page layout is different. This page is accessed by clicking **SANnav** in the navigation bar.
 - On the **Dashboard & Reports** page, the **Content** tab has been replaced with **Templates**.
 - On the **Inventory** page, the **Connections** tab has been changed to a drop-down list that includes **ISL Trunks** and **Extension Tunnels**.
 - The **Preferences** page has been moved from the navigation bar to a profile icon in the upper-right side of the page.
 - The **Logout** link has been moved from the lower-left side of the page to the profile icon in the upper-right side of the page.
 - In inventory and events tables, you can rearrange the order in which the columns are displayed.
- Automatic license renewal is supported. SANnav can automatically retrieve and activate renewed licenses.
- The "Installation" chapter has the following changes:
 - Added information about migrating from SANnav 1.1.1x to SANnav 2.0.0. The title of this chapter is changed to "Installation and Migration."
 - Port 22 can now be customized during installation.
 - Automatic license renewal is a new installation option.
 - RHEL and CentOS versions 7.6 and 7.7 are now supported.
- The "Security" chapter includes the following changes:
 - The user name is restricted to a maximum of 63 characters.
 - When assigning roles and AORs to LDAP groups, you can select one or more groups for SANnav to fetch, instead of SANnav automatically fetching all groups in the LDAP server.
- The "Monitoring" chapter includes the following changes:
 - Added behavior of SANnav if you try to discover switches that have reached end of support (EOS).
 - A new default dashboard is added: **Extension Dashboard**.
 - You can now export and import dashboard and report templates.
 - The score for factors that contribute to the overall health score for fabrics, switches, hosts, and storage can now be customized.
 - The following widgets have been added for reports:

- Chassis
- Time Series - Flow Collection (aggregated)
- Time Series - Flow Violations
- Top Collection Aggregation
- Top Flow Violations
- Top Host Port Pending IOs
- Top Host Port Read Oversubscription
- Top SCSI Errors
- Top Storage Port First Response Time
- Top Storage Port IOPS
- Top Storage Port Pending IOs
- The following status widgets have been added for dashboards:
 - Host Port Out Of Range Violations
 - ISL Port Out Of Range Violations
 - Storage Port Out Of Range Violations
- Performance monitoring can now be done on multiple measures and multiple nodes.
- The **Inventory** page includes an option to view the physical chassis. When you put a switch in maintenance mode, you now set this from the chassis details page instead of the switch details page.
- Decommissioning is now supported for F_Ports in addition to E_Ports.
- The **Topology** page provides visual indication of when a link is over 50% utilization and over 80% utilization.
- Flow Management is supported for the Analytics Monitoring Platform.
- The "Configuration" chapter includes the following changes:
 - The DNS configuration block is added to the basic configuration. The SNMPv3 configuration block is enhanced for firmware version 8.2.1b and later.
 - The logical fabric configuration type is added to the switch configuration and restore section.
 - The "Call Home and ESRS" section is updated to reflect password-related changes. You can modify the Call Home configuration without entering the password if you do not modify the email setting for a Call Home center.
 - The "Configuring the Dell EMC Call Home Support Center" section has been updated to reflect the changes regarding device registration in the ESRS. The switches must be registered in ESRS before they are added to the Dell EMC call center.
 - The "Zoning" section is updated to include the following changes:
 - Added the section "Creating Multiple Zone Aliases."
 - Added the section "Selecting and Adding Multiple Zone Aliases to a Zone."
 - Added the section "Selecting and Adding Multiple Zones to a Zone Configuration."
 - Added the section "Viewing Zone and Zone Configuration Details."
 - The "Comparing Effective and Defined (Modified) Zone Configuration" section is updated with the modified zone status.
 - The "Virtual Fabrics" section is updated to include the following changes:
 - Non-VF and AMP support is added for logical fabrics.
 - The LISL option is removed from the XISL template.
 - The FICON template is removed from logical fabrics.
 - Support for FICON fabrics is added.
- The "Event Management" chapter is updated to reflect password-related changes. If you try to modify any of the email settings, you must re-enter the password in the **SMTP Password** field. You must enter the password to send a test email.
- The "Switch Maintenance and Support" chapter is updated to include the following changes:

- Added information on custom port support for SCP/SFTP switch SupportSave and firmware management.
- The password-protected ZIP file behavior is updated in switch SupportSave.
- Added SANnav support for AMP version 3.0.0 or later.
- The "Troubleshooting" chapter has been changed to "Troubleshooting and Diagnostics" and includes support for Brocade ClearLink Diagnostic Port (D_Port) mode.
- SANnav Global View now includes support for the following:
 - A maximum of 20 SANnav Management Portal instances. The total port count must not exceed 120,000 ports.
 - The ability to create and save filters.
 - FICON fabrics.
 - The chassis item in the **Inventory** page.
 - Performance measures in the switch port inventory.
 - The ability to export inventory views.

1.3 Supported Hardware and Software

SANnav 2.0.0 supports the following Fabric OS software versions and hardware platforms.

Fabric OS Software Support

The following Fabric OS software versions are supported by this release of SANnav.

- Fabric OS 8.x or later
- Fabric OS 7.4 or later

Brocade Gen 6 (32Gb/s) Fixed-Port Switches

- Brocade G610 Switch
- Brocade G620 Switch
- Brocade G630 Switch
- Brocade 7810 Extension Switch

Brocade Gen 6 (32Gb/s) Directors

- Brocade X6-4 Director
- Brocade X6-8 Director

Brocade Gen 5 (16Gb/s) Fixed-Port Switches

- Brocade 6505 Switch
- Brocade 6510 Switch
- Brocade 6520 Switch
- Brocade M6505 Blade Server SAN I/O Module
- Brocade 6542 Blade Server SAN I/O Module
- Brocade 6543 Blade Server SAN I/O Module
- Brocade 6545 Blade Server SAN I/O Module
- Brocade 6546 Blade Server SAN I/O Module
- Brocade 6547 Blade Server SAN I/O Module
- Brocade 6548 Blade Server SAN I/O Module
- Brocade 6558 Blade Server SAN I/O Module
- Brocade 7840 Extension Switch

Brocade Gen 5 (16Gb/s) Directors

- Brocade DCX 8510-4 Director
- Brocade DCX 8510-8 Director

Brocade Gen 4 (8Gb/s) Fixed-Port Switches

- Brocade 300 Switch
- Brocade 5410 Blade Server SAN I/O Module
- Brocade 5424 Blade Server SAN I/O Module
- Brocade 5430 Blade Server SAN I/O Module
- Brocade 5431 Blade Server SAN I/O Module
- Brocade 5432 Blade Server SAN I/O Module
- Brocade 5450 Blade Server SAN I/O Module
- Brocade 5460 Blade Server SAN I/O Module
- Brocade 5470 Blade Server SAN I/O Module
- Brocade 5480 Blade Server SAN I/O Module
- Brocade NC-5480 Blade Server SAN I/O Module
- Brocade 7800 Extension Switch
- Brocade Encryption Switch

Brocade Gen 4 (8Gb/s) Directors

- Brocade DCX
- Brocade DCX-4S

Analytics Monitoring Platform

The Analytics Monitoring Platform (AMP) is supported with the following AMP OS software versions:

- AMP OS 3.0.0 or later (includes Flow Management support)
- AMP OS 2.0.x (switch monitoring only)

1.4 Contacting Technical Support for Your Brocade® Product

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

Online	Telephone
<p>For nonurgent issues, the preferred method is to log in to myBroadcom at https://www.broadcom.com/mybroadcom. (You must initially register to gain access to the Customer Support Portal.) Once there, select Customer Support Portal > Support Portal. You will now be able to navigate to the following sites:</p> <ul style="list-style-type: none"> ■ Knowledge Search: Clicking the top-right magnifying glass brings up a search bar. ■ Case Management: The legacy MyBrocade case management tool (MyCases) has been replaced with the Fibre Channel Networking case management tool. ■ DocSafe: You can download software and documentation. ■ Other Resources: Licensing Portal (top), SAN Health (top and bottom), Communities (top), Education (top). 	<p>Required for Severity 1 (critical) issues: Please call Fibre Channel Networking Global Support at one of the numbers listed at https://www.broadcom.com/support/fibre-channel-networking/.</p>

If you purchased Brocade product support from a Broadcom OEM/solution provider, contact your OEM/solution provider for all your product support needs.

- OEM/solution providers are trained and certified by Broadcom to support Brocade products.
- Broadcom provides backline support for issues that cannot be resolved by the OEM/solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information on this option, contact Broadcom or your OEM.
- For questions regarding service levels and response times, contact your OEM/solution provider.

1.5 Document Feedback

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

Installation and Migration

2.1 Installation Overview

The SANnav application uses a script-based installation. You must run the scripts that are provided in the `<install_home>` directory to install the application. All the scripts for the SANnav application must be executed in the bash shell.

The following installations are supported:

- **SANnav Management Portal**
 - Single-node installation
 - Multi-node installation
- **SANnav Global View**
 - Single-node installation

NOTE

SANnav Management Portal and SANnav Global View are two different software products. You cannot install both software products on the same physical host or virtual machine.

NOTE

For switches that are running Fabric OS versions lower than 8.2.2, port 22 is required for SANnav Management Portal to use the internal firmware repository and SCP and SFTP servers. See [Installation Prerequisites for SANnav Management Portal](#) for additional details.

If there is a firewall between the client and server or between the server and the SAN, you must open a set of ports for SANnav to function properly. The list of ports is provided in sections [Firewall Requirements for SANnav Management Portal](#) and [Firewall Requirements for SANnav Global View](#).

If the installation script detects that an earlier version of SANnav is running, you are prompted whether to migrate your data to the new version.

2.2 Migration Overview

If you are upgrading SANnav Management Portal or SANnav Global View from a previous version, the installation script provides the option of migrating your data. Migrating allows you to keep all user-configured data, customized data, and historic data (such as port performance metrics and events) when you upgrade to the latest SANnav version.

When you migrate the data, the following occurs:

- Installation settings (such as port customizations and the database password) from the previous installation are preserved. The installation does not prompt you for these settings.
- The license is carried forward to the new installation. After migration, you do not need to apply a new license. If the license is a trial license, after migration the license is valid for the remaining days of the trial period.
- The discovered fabrics are rediscovered. For SANnav Global View, the discovered portals are rediscovered.
- User-configured data, customized data, and historic data (such as port performance metrics and events) are migrated.

Note that the following data is *not* migrated:

- Support data collection files
- SupportSave files

Migration Prerequisites

Before you migrate to the new SANnav version, back up the server. Use the `backup` script in the `<install_home>/bin/backuprestore` folder.

Ensure that the seed switches for discovered fabrics have not reached end of support (EOS). If a seed switch has reached end of support, after migration the fabric is unmonitored permanently with the discovery status "Unmonitored: Seed switch is no longer supported." In this case, you must delete the fabric and rediscover it with a different seed switch. To avoid this scenario, change the seed switch to a supported switch before migration.

OS Upgrade Options

SANnav 2.0.0 and higher do not support RHEL 7.4. If you are running RHEL 7.4 and want to migrate to SANnav 2.0.0, you must first upgrade the OS to 7.5 or higher. You cannot migrate SANnav and the OS simultaneously. See [Updating the OS with SANnav Installed](#)

Migration Paths

The following table lists the software versions and whether migration is supported.

Table 1: Supported Migration Paths

Current Version	Migration Version	Supported?
SANnav 1.1.0x	SANnav 1.1.1x	No
SANnav 1.1.0x	SANnav 2.0.0	No
SANnav 1.1.1x	SANnav 2.0.0	Yes
SANnav build x	SANnav 2.0.0 build y	No

The following table lists various system configurations and whether migration is supported.

Table 2: Supported System Configuration Paths

Current Deployment	Migration Deployment	Supported?
Single-node	Single-node (same host)	Yes
Multi-node	Multi-node (master node, same host)	Yes
Single-node	Multi-node	No
Multi-node	Single-node	No

2.3 SANnav Management Portal Deployment

SANnav Management Portal provides single-node and multi-node installation. During the installation, you are prompted several times to accept default values or provide customized values for various settings.

For a multi-node installation, you can install SANnav on a cluster of three physical servers or on a cluster of three virtual machines. You assign one node as a master node. The remaining two nodes are assigned as worker nodes.

The multi-node installation includes additional steps that must be performed on the master node and both of the worker nodes.

Installation Customizations

The following customizations are supported in the installation phase. Note that if you are migrating from an earlier version of SANnav, you are not prompted for these customizations, and the settings from the previous installation remain in effect.

- Docker installation directory — The default home directory for installing Docker is `/var/lib/docker`, but you can change this to another directory.
- Setting server-to-switch communication protocol preference. The following is the list of available protocol options:
 - 0 for HTTP (Insecure communication)
 - 1 for HTTPS (Secure communication. Requires that you have an IT-provided SSL certificate (or self-signed certificate) and that your switches are configured for HTTPS.)
 - 2 for HTTPS then HTTP (First HTTPS is tried, and if that fails, HTTP is used.)
- Port customization — You can customize ports when installing SANnav Management Portal. To use a default port, that port must be unused and available. The following is the list of default values:
 - SSH server port is 22
 - Client to Server HTTPS Port: Default HTTPS port is 443
 - SNMP Trap: Default SNMP trap port is 162
 - Syslog Port: Default syslog port is 514
 - Secure Syslog Port: Default Secure syslog port is 6514
 - Database Port: 5432
- Database password — You can change the default SANnav Management Portal database password. You are given an option to proceed installation with the default password or choose a new password for the SANnav database. The default password is **passw0rd** (where 0 is a zero).
- SCP/SFTP password — You can change the default SCP/SFTP password. You are given an option to proceed installation with the default password or choose a new password for the internal SCP/SFTP server. The default password is **passw0rd** (where 0 is a zero).
- License auto-renewal — By default, SANnav is configured to automatically retrieve and activate a renewal license when the license expires. You can deactivate automatic license renewal, in which case you must manually apply the license yourself.

2.3.1 System and Server Requirements for SANnav Management Portal

It is mandatory to meet all the system and server requirements before you start SANnav Management Portal installation.

NOTE

For a multi-node installation, the maximum number of managed ports is the sum of the ports managed by the master node and each worker node, and it cannot exceed 15,000.

The following table lists the system and server requirements for single-node and multi-node deployment for SANnav Management Portal.

NOTE

The disk space requirement listed in the table is for SANnav only. Be sure to account for additional space required by the operating system and for saving files.

The disk space can be from a direct-attached disk or through a network-mounted disk.

NOTE

The default home directory for installing Docker is `/var/lib/docker`, but you can choose another location during installation. Docker must be installed on a local disk.

Table 3: System and Server Requirements for Single-Node and Multi-Node Installation

Requirement	Single-Node		Multi-Node	
	3000 Ports	15,000 Ports	Master Node	Each Worker Node
Operating system	<ul style="list-style-type: none"> ■ Red Hat Enterprise Linux: 7.5, 7.6, and 7.7 ■ CentOS 7.5, 7.6, and 7.7 	<ul style="list-style-type: none"> ■ Red Hat Enterprise Linux: 7.5, 7.6, and 7.7 ■ CentOS 7.5, 7.6, and 7.7 	<ul style="list-style-type: none"> ■ Red Hat Enterprise Linux: 7.5, 7.6, and 7.7 ■ CentOS 7.5, 7.6, and 7.7 	<ul style="list-style-type: none"> ■ Red Hat Enterprise Linux: 7.5, 7.6, and 7.7 ■ CentOS 7.5, 7.6, and 7.7
Host type	<ul style="list-style-type: none"> ■ Bare metal server ■ VMware ESXi virtual machine 	<ul style="list-style-type: none"> ■ Bare metal server ■ VMware ESXi virtual machine 	<ul style="list-style-type: none"> ■ Bare metal server ■ VMware ESXi virtual machine 	<ul style="list-style-type: none"> ■ Bare metal server ■ VMware ESXi virtual machine
CPU	16 cores	24 cores	16 cores	16 cores on each worker node
CPU sockets (minimum)	2	2	2	2 on each worker node
CPU speed (minimum)	2000 MHz	2000 MHz	2000 MHz	2000 MHz on each worker node
Memory (RAM)	48 GB	96 GB	32 GB	32 GB on each worker node
Hard disk space (minimum)	600 GB, distributed as follows: <ul style="list-style-type: none"> ■ 450 GB - Installation directory ■ 120 GB - Docker installation directory ■ 20 GB - "/" ■ 250 MB - /etc 	1.2 TB, distributed as follows: <ul style="list-style-type: none"> ■ 1050 GB - Installation directory ■ 120 GB - Docker installation directory ■ 20 GB - "/" ■ 250 MB - /etc 	600 GB, distributed as follows: <ul style="list-style-type: none"> ■ 450 GB - Installation directory ■ 120 GB - Docker installation directory ■ 20 GB - "/" ■ 250 MB - /etc 	150 GB on each worker node, distributed as follows: <ul style="list-style-type: none"> ■ 120 GB - Docker installation directory ■ 20 GB - "/" ■ 250 MB - /etc

2.3.2 Installation Prerequisites for SANnav Management Portal

Review all SANnav Management Portal installation prerequisites before you unzip the installation files.

NOTE

Use the latest generation processors for better SANnav performance.

Task	Task Details or Additional Information	Completed
Gather necessary information and components.	Make sure that you have the following: <ul style="list-style-type: none"> ■ Root user credentials. You must log in to the SANnav server as the root user or a user with root privilege. ■ The SANnav Management Portal server IP address. 	
Uninstall other applications.	SANnav Management Portal is expected to be installed and run on a dedicated host; if any other application is installed on the host, uninstall it before starting the SANnav Management Portal installation. If you are migrating SANnav, do not uninstall the current SANnav instance.	
Uninstall Docker, if already installed.	The SANnav installation installs Docker. If you have a Docker installed other than the Docker that SANnav installs, you must remove it before starting the installation.	

Task	Task Details or Additional Information	Completed
Check operating system requirements.	<ul style="list-style-type: none"> ■ Ensure that the entire physical server (boot, log, and data) runs on a single partition. ■ Ensure that the operating system can be loaded through a bootable disk or through a PXE server. ■ Ensure that the <code>lsuf</code> and <code>nslookup</code> packages are installed on the operating system machine. 	
Set umask and ulimit.	<ul style="list-style-type: none"> ■ "umask" for the root user must be set to 0022. Enter the following command to set the umask: <pre>umask 0022</pre> You must set the umask before you unzip the installation files. If you extracted the installation files before you set the umask, you must delete the installation folder, run <code>umask 0022</code>, and then unzip the files again. ■ Ensure that the ulimit is set correctly. To set the ulimit, edit the <code>/etc/security/limits.conf</code> file and add the following limit at the end of the file: <code>elasticsearch - nofile 65536</code> 	
Check port 22 availability.	<p>By default port 22 is used for the internal firmware repository, but you can change this port number during installation. If the port is not available, you must use an external FTP, SCP, or SFTP server for switch supportsave and firmware download functionality.</p> <p>If you change to a port number other than 22, then for switches running Fabric OS versions earlier than 8.2.2, you must use an external FTP, SCP, or SFTP server for switch supportsave and firmware download functionality.</p> <p>To free port 22 for SANnav Management Portal, perform the following steps:</p> <ol style="list-style-type: none"> 1. Edit the <code>/etc/ssh/sshd_config</code> file: <ol style="list-style-type: none"> a. Locate the following line: <pre>#port 22</pre> b. Uncomment the line and change the port number to another, unused port, such as 8022. <pre>port 8022</pre> Note that whatever port you select must be available and allowed in the firewall. 2. Restart the SSHD using the following command: <pre>systemctl restart sshd</pre> The current SSH session remains logged in, but any new sessions must now use port 8022. 	
Check port 80 availability.	<p>Port 80 must be available; otherwise, installation fails. After installation, port 80 must continue to be available all the time; otherwise, you cannot start (or restart) SANnav Management Portal.</p> <p>If your network utilizes a firewall, there may be other ports that must be open. See the "Firewall Requirements" section for details.</p>	

Task	Task Details or Additional Information	Completed
Ensure that IPv4 IP forwarding is enabled.	<p>To check whether IPv4 IP forwarding is enabled, enter the following command:</p> <pre>/sbin/sysctl net.ipv4.ip_forward</pre> <p>If the output is <code>net.ipv4.ip_forward=1</code>, forwarding is enabled, and you do not need to make any changes.</p> <p>If the output is <code>net.ipv4.ip_forward=0</code>, forwarding is disabled, and you must change it as follows:</p> <ol style="list-style-type: none"> 1. Enter the following command to set IP forwarding for this session: <pre>/sbin/sysctl -w net.ipv4.ip_forward=1</pre> 2. Edit the <code>/etc/sysctl.conf</code> file and add the following lines: <pre># IP Forwarding is enabled for Brocade SANnav net.ipv4.ip_forward = 1</pre> 	
Run additional commands.	<ul style="list-style-type: none"> ■ Ensure that the <code>hostname -i</code> command resolves to a valid IP address. ■ The <code>nslookup</code> command must be successful for the host name of the physical host and VM. 	

2.3.3 Installing the Application for Single-Node Deployment

Complete these steps to download and install SANnav Management Portal on the server.

Before unzipping the installation file, be sure to review and comply with the system and server requirements and the installation prerequisites listed in the following sections:

- [System and Server Requirements for SANnav Management Portal](#)
- [Installation Prerequisites for SANnav Management Portal](#)

NOTE

If the scripts fail during the installation or startup, uninstall the application and then reinstall it. Do not try to fix the issue and re-run the `install-single-server.sh` without first uninstalling the application.

Download and copy the SANnav Management Portal software package to the server. The package contains the SANnav Management Portal tarball.

1. Download the SANnav Management Portal tarball (for example, `Portal_2.0.0-distribution.tar.gz`) to the folder where you want to install the application.

NOTE

Do not create the SANnav Management Portal installation folder with a space in the name; otherwise, installation will fail.

2. Untar the `.gz` file to extract the file to the current location.

```
tar -xvzf Portal_2.0.0-distribution.tar.gz
```

The following is sample output.

```
[root@RHEL7-10-100 home]# tar -xvzf Portal_2.0.0-distribution.tar.gz
Portal_2.0.0_rc_bldxx/jre/
Portal_2.0.0_rc_bldxx/jre/lib/
(output truncated)
(output truncated)
Portal_2.0.0_rc_bldxx/conf/EULA/BRCD/license.html
Portal_2.0.0_rc_bldxx/conf/EULA/license.html
[root@RHEL7-10-100 home]#
```

This step creates a directory with a name similar to `Portal_2.0.0_rc_bldxx`. This directory is referred to as the `<install_home>` directory in this document.

3. Go to the `<install_home>/bin` directory.

```
[root@RHEL7-10-100 home]# cd Portal_2.0.0_rc_bldxx/bin
```

4. Run the `install-single-node-server.sh` script to install SANnav Management Portal.

```
[root@RHEL7-10-100 bin]# ./install-single-node-server.sh
```

The installation script checks whether an earlier instance of SANnav Management Portal is installed, and if so, it prompts with the following:

```
Found an instance of SANnav 1.1.1 installed on this VM / Host. If you are planning to migrate SANnav
1.1.1 data, we recommend you to take a backup (<SANnav 1.1.1 Home>/backuprestore/backup) before you
proceed further.
If you choose to take a backup of 1.1.1, exit the script execution (Ctrl + c) at this stage and proceed
with SANnav 2.0.0 installation once you finish the backup.
Enter (Yes / Y) to proceed with migration or (No / N) to proceed the installation without migration: [Yes]
```

5. If you are prompted about migrating SANnav, enter one of the following options.

- To continue the installation without migrating, enter **No**. You are instructed to uninstall the existing SANnav instance first, and then you can restart the installation script.
- To back up the server before proceeding with migration, enter **Ctrl-C**. The script ends. You can back up the server and restart the installation script.
- To proceed with migration, enter **Yes**. You are prompted to enter the location of the existing SANnav installation.

As the installation proceeds, the script runs a pre-install requirements test. If any test fails, the installation exits with error messages. You must fix the reported issues, uninstall the application, and repeat from Step 1. After the diagnostics pass, installation of SANnav Management Portal software continues. On successful installation of the software, the SANnav Management Portal server starts up. The startup may take up to 20 minutes.

The following is a sample result of `./install-single-node-server.sh` command execution.

```
Disk space available in /home/Portal_2.0.0_rc_bldxx: 642 GB
Disk space available in /var/lib/: 642 GB
Disk space available in /: 642 GB
Current memory: 117 GB
UMASK set to: 0022
Number of CPU: 40
Host name to IP resolution: 00.000.00.00
Port 80 is free.
Number of CPU sockets available: 20
Operating System: Red Hat Enterprise Linux Server release 7.5 (Maipo)
NSLOOKUP of 00.000.00.00 resolved successfully
CPU Speed: 2592 MHz
```

```
BROCADE END USER LICENSE AGREEMENT
(output truncated)
(output truncated)
```

Successfully installed server. Press Enter to continue with server startup.

```
IP Address of the Manager is 00.000.00.00
```

```
Total Number of nodes in swarm: 1
Time Zone is America/Los_Angeles
MAC Address of the manager node is: 00:0c:00:00:b0:00
# Reading property from /install_home/Portal_2.0.0_rc_bldxx/conf/version.properties
# Build Label is sannav2.0.0
Installing on 96 GB and above VM
There is only one node in cluster with zero worker nodes..Starting single node SWARM
cluster installation
```

```
Ignoring unsupported options: ulimits
```

```
(output truncated)
```

```
(output truncated)
```

```
The server is successfully installed and started. To check the server status, run
/install_home/Portal_2.0.0_rc_bldxx/bin/diag/check-server-status.sh. Launch the client using http://
00.000.00.00
```

2.3.4 Installing the Application for Multi-Node Deployment

Complete these steps to download and install SANnav Management Portal on the server in a multi-node deployment.

Before unzipping the installation file, be sure to review and comply with the system and server requirements and the installation prerequisites listed in the following sections:

- [System and Server Requirements for SANnav Management Portal](#)
- [Installation Prerequisites for SANnav Management Portal](#)

NOTE

All three nodes (the master node and the two worker nodes) must be up and running for the SANnav server to be up and running.

Perform the following steps to run a setup script on the master node and each worker node, and then install the application.

1. Download the utility scripts tarball (for example, `Portal-utility-scripts-distribution.tar.gz`) to the master node and each worker node.
2. On the master node, perform the following steps.
 - a. Untar the utility scripts file.

```
tar -xvzf Portal-utility-scripts-distribution.tar.gz
```

- b. Go to `Portal-utility-scripts` and run the script `setup-multinode-master.sh`.

```
./setup-multinode-master.sh
```

This script performs the following functions:

- Checks the minimum requirements for the master node.
- Sets up the NFS Server.
- Installs all prerequisites for the master node, including Docker.

3. Perform the following steps on each worker node.

- a. Untar the utility scripts file.

```
tar -xvzf Portal-utility-scripts-distribution.tar.gz
```

- b. Go to `Portal-utility-scripts` and run the script `setup-multinode-worker.sh`.

```
./setup-multinode-worker.sh
```

This script performs the following functions:

- Checks the minimum requirements for the worker node.
- Sets up the NFS Client.
- Installs all pre-requisites for the worker node, including Docker.

4. On the master node, download `Portal_2.0.0-distribution.tar.gz` to the NFS location and untar the file.

NOTE

Do not create the SANnav Management Portal installation folder with a space in the name; otherwise, installation will fail.

```
tar -xvzf Portal_2.0.0-distribution.tar.gz
```

This step creates a directory with a name similar to `Portal_2.0.0_rc_bldxx`. This directory is referred to as the `<install_home>` directory in this document.

5. Go to the `<install_home>/bin` folder.

6. Run the `install-multi-node-server.sh` script to install SANnav Management Portal.

```
./install-multi-node-server.sh
```

The installation script checks whether an earlier instance of SANnav Management Portal is installed, and if so, it prompts with the following:

```
Found an instance of SANnav 1.1.1 installed on this VM / Host. If you are planning to migrate SANnav
1.1.1 data, we recommend you to take a backup (<SANnav 1.1.1 Home>/backuprestore/backup) before you
proceed further.
```

```
If you choose to take a backup of 1.1.1, exit the script execution (Ctrl + c) at this stage and proceed
with SANnav 2.0.0 installation once you finish the backup.
```

```
Enter (Yes / Y) to proceed with migration or (No / N) to proceed the installation without migration: [Yes]
No
```

```
Please uninstall the existing instance of SANnav 1.1.1 to install SANnav 2.0 without migration. Press
Enter to exit the installation.
```

```
[root@RHEL7-73-150 bin]#
```

7. If you are prompted about migrating SANnav, enter one of the following options.

- To continue the installation without migrating, enter **No**. You are instructed to uninstall the existing SANnav instance first, and then you can restart the installation script.
- To back up the server before proceeding with migration, enter **Ctrl-C**. The script ends. You can back up the server and restart the installation script.
- To proceed with migration, enter **Yes**. You are prompted to enter the location of the existing SANnav installation.

At this point, the script performs the following functions:

- Runs system checks to ensure that the NFS location has the minimum space needed (450 GB). If any of the checks fails, the installation will stop.
- Installs the SANnav Management Portal server.
- Starts SANnav Management Portal after successful installation.

2.3.5 Firewall Requirements for SANnav Management Portal

If your network utilizes a firewall between the SANnav Management Portal client and server or between the server and SAN, a set of ports must be open in the firewall to ensure proper communication.

The following table lists the ports that must be open in the firewall.

These ports are added to the IP tables by default when the SANnav server is running, so you do not need to open them in the firewall, if it is enabled and running on the SANnav server.

Table 4: Ports That Must Be Open in the Firewall

Port Number	Transport	Inbound/Outbound	Communication Path	Description
22	TCP	Both	Client --> Server Server <--> Switch	Internal SSH server
80	TCP	Both	Client --> Server Server --> Switch	HTTP port for access from browser to server HTTP port for access from server to switch
161	UDP	Outbound	Server --> Switch	SNMP port
162	UDP	Inbound	Switch --> Server	SNMP trap port
443	TCP	Both	Client --> Server Server --> Switch Server --> vCenter	HTTPS port for secure access from browser to server HTTPS port for secure access from server to switch HTTPS port for secure access from server to vCenter
514	UDP	Inbound	Switch --> Server	Syslog port
6514	UDP	Inbound	Switch --> Server	Secure Syslog port
8081	TCP	Inbound	Switch --> Server	Avro schema registry port
19092	TCP	Inbound	Switch --> Server	Kafka port
19094	TCP	Inbound	Switch --> Server	Secured Kafka
29092	TCP	Inbound	Switch --> Server	Kafka port
29094	TCP	Inbound	Switch --> Server	Secured Kafka
39092	TCP	Inbound	Switch --> Server	Kafka port
39094	TCP	Inbound	Switch --> Server	Secured Kafka

The following table lists additional ports that must be open in the following conditions:

- If your network utilizes an external firewall between the nodes in a multi-node deployment, these ports must be open in the firewall.
- If firewalld is enabled in the server, these ports must be open in the firewalld configuration.

If firewalld is enabled, in addition, you must add the ssh service to the trusted zone in the firewalld for the firmware download feature to work. See [Configuring a Firewall for SANnav](#) for instructions on how to configure firewalld.

Table 5: Additional Ports That Must Be Open in the Firewall

Port Number	Transport	Inbound/Outbound	Communication Path	Description
2377	TCP	Both	Server <--> Server	Cluster management communications
4789	UDP	Both	Server <--> Server	Overlay network traffic
7946	TCP	Both	Server <--> Server	Node-to-node communication
7946	UDP	Both	Server <--> Server	Node-to-node communication

If you configure an external authentication server (LDAP, RADIUS, or TACACS+) or an email server (SMTP), ensure that the SANnav Management Portal server has access to the ports listed in the following table. The default ports are listed in the table, but you can change the default.

Table 6: Ports That the Server Must Be Able to Access

Port Number	Transport	Inbound/ Outbound	Communication Path	Description
25	TCP	Outbound	Server --> SMTP Server	SMTP server port for email communication if you use email notifications without SSL or TLS
49	TCP	Outbound	Server --> TACACS+ Server	TACACS+ server port for authentication if you use TACACS+ for external authentication
389	TCP	Outbound	Server --> LDAP Server	LDAP server port for authentication if you use LDAP for external authentication and SSL is not enabled
465	TCP	Outbound	Server --> SMTP Server	SMTP server port for email communication if you use email notifications with SSL
587	TCP	Outbound	Server --> SMTP Server	SMTP server port for email communication if you use email notifications with TLS
636	TCP	Outbound	Server --> LDAP Server	LDAP server port for authentication if you use LDAP for external authentication and SSL is enabled
1812	UDP	Outbound	Server --> RADIUS Server	RADIUS server port for authentication if you use RADIUS for external authentication

2.4 SANnav Global View Deployment

SANnav Global View installation provides single-node installation only. During the installation, you are prompted several times to accept default values or provide customized values for various settings.

Installation Customizations

The following customizations are supported in the installation phase. Note that if you are migrating from an earlier version of SANnav, you are not prompted for these customizations, and the settings from the previous installation remain in effect.

- Docker installation directory — The default home directory for installing Docker is `/var/lib/docker`, but you can change this to another directory.
- Port customization — You can customize ports when installing SANnav Global View. To use a default port, that port must be unused and available. The following is the list of default values:
 - Client to Server HTTPS Port: Default HTTPS port is 443
 - Database Port: 5432
- Database password — You can change the default SANnav database password. You will be given an option to proceed installation with the default password or choose a new password for the SANnav database. The default password is **passw0rd** (where 0 is a zero).
- License auto-renewal — By default, SANnav is configured to automatically retrieve and activate a renewal license when the license expires. You can deactivate automatic license renewal, in which case you must manually apply the license yourself.

2.4.1 System and Server Requirements for SANnav Global View

It is mandatory to meet all the system and server requirements before you start SANnav Global View installation.

The following table lists the system and server requirements for SANnav Global View.

NOTE

The disk space requirement listed in the table is for SANnav only. Be sure to account for additional space required by the operating system and for saving files.

Table 7: SANnav Global View Single-Node Deployment

Requirement	Value
Maximum number of SANnav Management Portal instances	20 SANnav Global View supports up to 20 Management Portal instances as long as the total port count does not exceed 120,000 ports. The total port count is the sum of ports managed by all Management Portal instances.
Operating system	<ul style="list-style-type: none"> ■ Red Hat Enterprise Linux: 7.5, 7.6, and 7.7 ■ CentOS 7.5, 7.6, and 7.7
Host type	<ul style="list-style-type: none"> ■ Bare metal server ■ VMware ESXi virtual machine
CPU	16 cores
Memory (RAM)	32 GB
Hard disk	450 GB, distributed as follows: <ul style="list-style-type: none"> ■ 300 GB - Installation folder ■ 90 GB - /var/lib ■ 20 GB - "/" ■ 100 MB - /etc The disk space can be from a direct-attached disk or through a network-mounted disk.
Minimum number of CPU sockets	2
Minimum CPU speed	2000 MHz

2.4.2 Installation Prerequisites for SANnav Global View

Review all SANnav Global View installation prerequisites before you unzip the installation files.

NOTE

Use the latest generation processors for better SANnav performance.

Task	Task Details or Additional Information	Completed
Gather necessary information and components.	Make sure that you have the following: <ul style="list-style-type: none"> ■ Root user credentials. You must log in to the SANnav server as the root user, or a user with root privilege. ■ The SANnav Global View server IP address. 	
Uninstall other applications.	SANnav Global View is expected to be installed and run on a dedicated host; if any other application is installed on the host, uninstall it before starting the SANnav Global View installation. If you are migrating SANnav, do not uninstall the current SANnav instance.	
Uninstall Docker, if already installed.	The SANnav installation installs Docker. If you have a Docker installed other than the Docker that SANnav installs, you must remove it before starting the installation.	

Task	Task Details or Additional Information	Completed
Check operating system requirements.	<ul style="list-style-type: none"> ■ Ensure that the entire physical server (boot, log, and data) runs on a single partition. ■ Ensure that the operating system can be loaded through a bootable disk or through a PXE server. ■ Ensure that the <code>lsuf</code> and <code>nslookup</code> packages are installed on the operating system machine. 	
Set umask and ulimit.	<ul style="list-style-type: none"> ■ "umask" for the root user must be set to 0022. Enter the following command to set the umask: <pre>umask 0022</pre> You must set the umask before you unzip the installation files. If you extracted the installation files before you set the umask, you must delete the installation folder, run <code>umask 0022</code>, and then unzip the files again. ■ Ensure that the ulimit is set correctly. To set the ulimit, edit the <code>/etc/security/limits.conf</code> file with appropriate privileges. 	
Check port availability.	<p>Ensure that port 80 is available. Port 80 must be available; otherwise, installation fails. After installation, port 80 must continue to be available all the time; otherwise, you cannot start (or restart) SANnav Global View. If your network utilizes a firewall, there may be other ports that must be open. See the Firewall Requirements section for details.</p>	
Ensure that IPv4 IP forwarding is enabled.	<p>To check whether IPv4 IP forwarding is enabled, enter the following command: <pre>/sbin/sysctl net.ipv4.ip_forward</pre> If the output is <code>net.ipv4.ip_forward=1</code>, forwarding is enabled, and you do not need to make any changes. If the output is <code>net.ipv4.ip_forward=0</code>, forwarding is disabled, and you must change it as follows:</p> <ol style="list-style-type: none"> 1. Enter the following command to set IP forwarding for this session: <pre>/sbin/sysctl -w net.ipv4.ip_forward=1</pre> 2. Edit the <code>/etc/sysctl.conf</code> file and add the following lines: <pre># IP Forwarding is enabled for Broadcom SANnav net.ipv4.ip_forward = 1</pre> 	
Run additional commands.	<ul style="list-style-type: none"> ■ Ensure that the <code>hostname -i</code> command resolves to a valid IPv4 address. ■ The <code>nslookup</code> command must be successful for the host name of the physical host and VM. 	

2.4.3 Installing the SANnav Global View Application

Complete these steps to install SANnav Global View on the server.

Before unzipping the installation file, be sure to review and comply with the system and server requirements and the installation prerequisites listed in the following sections:

- [System and Server Requirements for SANnav Global View](#)
- [Installation Prerequisites for SANnav Global View](#)

Download and copy the SANnav Global View software package to the server. The package contains the SANnav Global View tarball.

1. Download the SANnav Global View tarball (for example, `Global_2.0.0_rc_bldxx-distribution.tar.gz`) to the folder where you want to install the application.

NOTE

Do not create the SANnav Global View installation folder with spaces in the name; otherwise, installation will fail.

2. Untar the `.gz` file to extract the file to the current location.

```
tar -xvzf Global_2.0.0_rc_bldxx-distribution.tar.gz
```

The following is sample output.

```
[root@RHEL74-10-26 home]# tar -xvzf Global_2.0.0_rc_bldxx-distribution.tar.gz
Global_2.0.0_rc_bldxx/jre/
Global_2.0.0_rc_bldxx/jre/lib/
Global_2.0.0_rc_bldxx/jre/lib/management/
(output truncated)
(output truncated)
Global_2.0.0_rc_bldxx/bin/replace-server-cert.sh
Global_2.0.0_rc_bldxx/bin/addLdapServer
[root@RHEL74-10-26 home]#
```

This step creates a directory with a name similar to `Global_2.0.0_rc_bldxx`. This directory is referred to as the `<install_home>` directory in this document.

3. Go to the `<install_home>/bin` directory.
4. Run the `install-single-node-server.sh` script to install SANnav Global View.

```
./install-single-node-server.sh
```

The installation script checks whether an earlier instance of SANnav Global View is installed, and if so, it prompts with the following:

```
Found an instance of SANnav 1.1.1 installed on this VM / Host. If you are planning to migrate SANnav
1.1.1 data, we recommend you to take a backup (/SANnav_home/Global_2.0.0_beta_bld173/backuprestore/
backup) before you proceed further.
If you choose to take a backup of 1.1.1, exit the script execution (Ctrl + C) at this stage and proceed
with SANnav 2.0 installation once you finish the backup.
Enter (Yes / Y) to proceed with migration or (No / N) to proceed the installation without migration: [Yes]
```

5. If you are prompted about migrating SANnav, enter one of the following options.
 - To continue the installation without migrating, enter **No**. You are instructed to uninstall the existing SANnav instance first, and then you can restart the installation script.
 - To back up the server before proceeding with migration, enter **Ctrl-C**. The script ends. You can back up the server and restart the installation script.
 - To proceed with migration, enter **Yes**. You are prompted to enter the location of the existing SANnav installation.

As the installation proceeds, the script runs a pre-install requirements test. If any test fails, the installation exits with error messages. You must fix the reported issues and re-run the install script. After the diagnostics pass, installation of SANnav

Global View software continues. On successful installation of the software, the SANnav Global View server starts up. The startup may take up to 10 minutes.

The following is a sample result of `./install-single-node-server.sh` command execution.

```
[root@RHEL74-10-26 home]# cd Global_2.0.0_rc_bldxx/bin
[root@RHEL74-10-26 bin]# ./install-single-node-server.sh
Disk space available in /home/Global_2.0.0_rc_bldxx: 506 GB
Disk space available in /var/lib/: 506 GB
Disk space available in /: 506 GB
Current memory: 47 GB
UMASK set to: 0022
Number of CPU: 16
Host name to IP resolution: 00.000.00.00
Port 80 is free.
Number of CPU sockets available: 16
Operating System: Red Hat Enterprise Linux Server release 7.5 (Maipo)
CPU speed: 2592 MHz
System requirements are passed. Press Enter to continue

BROCADE END USER LICENSE AGREEMENT

(output truncated)
(output truncated)

Press Enter to continue with default port number (443) for HTTPS.
Or manually enter a new port number (1- 65535)
Press Enter to continue with default port number (5432) for database.
Or manually enter a new port number (1- 65535)

Press Enter to continue with default database password, or enter a new password manually.
New password must be between 8 to 64 characters, alphanumeric. Spaces are not allowed. Allowed special
characters are !#$*()
Generated self-signed server certificate.

Successfully installed server. Press Enter to continue with server startup.

Ignoring unsupported options: ulimits

(output truncated)
(output truncated)
docker swarm deployed...
Successfully installed and started the server. Check server status by running /home/
Global_2.0.0_rc_bldxx/bin/diag/check-server-status.sh. After the server has started, launch the client using
https://00.000.00.00:443
```

2.4.4 Firewall Requirements for SANnav Global View

If your network utilizes a firewall between the SANnav Global View client and server or between the server and other SANnav Management Portal servers, a set of ports must be open in the firewall to ensure proper communication.

The following table lists the ports that must be open in the firewall.

Table 8: Ports That Must Be Open in the Firewall

Port Number	Transport	Inbound/ Outbound	Communication Path	Description
80	TCP	Both	Client --> Server	HTTP port for access from browser to server; for HTTP to HTTPS redirection
443 If port 443 is not utilized, open its replacement port.	TCP	Both	Client --> Server Server --> SANnav Management Portal	HTTPS port for secure access from browser to server HTTPS port for secure access from server to SANnav Management Portal

When firewalld is enabled in the server, the following set of ports must also be open in the firewalld configuration. See [Configuring a Firewall for SANnav](#) for instructions on how to configure firewalld.

Table 9: Additional Ports That Must Be Open in the Firewall

Port Number	Transport	Inbound/ Outbound	Communication Path	Description
2377	TCP	Both	Server <--> Server	Cluster management communications
4789	UDP	Both	Server <--> Server	Overlay network traffic
7946	TCP	Both	Server <--> Server	Node-to-node communication
7946	UDP	Both	Server <--> Server	Node-to-node communication

If you configure an external authentication server (LDAP, RADIUS, or TACACS+) or an email server (SMTP), ensure that the SANnav Global View server has access to the ports listed in the following table. The default ports are listed in the table, but you can change the default.

Table 10: Ports That the Server Must Be Able to Access

Port Number	Transport	Inbound/ Outbound	Communication Path	Description
25	TCP	Outbound	Server --> SMTP Server	SMTP server port for email communication if you use email notifications without SSL or TLS
49	TCP	Outbound	Server --> TACACS+ Server	TACACS+ server port for authentication if you use TACACS+ for external authentication
389	TCP	Outbound	Server --> LDAP Server	LDAP server port for authentication if you use LDAP for external authentication and SSL is not enabled
465	TCP	Outbound	Server --> SMTP Server	SMTP server port for email communication if you use email notifications with SSL
587	TCP	Outbound	Server --> SMTP Server	SMTP server port for email communication if you use email notifications with TLS
636	TCP	Outbound	Server --> LDAP Server	LDAP server port for authentication if you use LDAP for external authentication and SSL is enabled
1812	UDP	Outbound	Server --> RADIUS Server	RADIUS server port for authentication if you use RADIUS for external authentication

2.5 Uninstalling the SANnav Application

You can run a single script to uninstall SANnav Management Portal or SANnav Global View. For a SANnav Management Portal multi-node installation, additional scripts are required.

Perform the following steps to uninstall the SANnav application and bring the system back to the original state.

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

```
./uninstall-server.sh
```

2. **NOTE**

For multi-node installations, the uninstall script uninstalls Docker files and swap files on the master node. You must manually uninstall the NFS setup and Docker on the worker nodes.

For SANnav Management Portal multi-node installations only, after you uninstall the application, perform the following steps to uninstall the NFS setup on the master and worker nodes, and clear dead Docker containers on the worker nodes.

- a. Go to the `dcm-utility-scripts` folder in work node 1 and work node 2, and run the following script to uninstall prerequisites and NFS setup installed on the worker nodes.

```
uninstall_nfs_setup.sh
```

- b. Go to the `dcm-utility-scripts` folder in the master node and run the following script to uninstall the NFS server.

```
uninstall_nfs_setup.sh
```

After the application is uninstalled, there might be dead Docker containers in the worker nodes, which must be cleaned manually.

- c. Go to the `dcm-utility-scripts` folder on worker node 1 and worker node 2, and run the following script to clean up the dead Docker containers.

```
uninstall_docker.sh
```

This script removes Docker entirely in these nodes.

2.6 Additional Scripts

You can re-start, stop, and start the SANnav Management Portal and SANnav Global View servers with additional scripts. You can also run a script to replace self-signed certificates with third-party signed certificates. Run these scripts only if required.

The following scripts apply to both SANnav Management Portal and SANnav Global View and, for SANnav Management Portal, apply to both single-node and multi-node installations.

Restarting the Server

To stop the currently running SANnav server and restart the SANnav application, perform the following:

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

```
./restart-server.sh
```

Stopping the Server

To stop the currently running SANnav server, perform the following:

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

```
./stop-server.sh
```

Starting the Server

To start the stopped SANnav server, perform the following:

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

```
./start-server.sh
```

Checking the Server Health

Once the installation is complete, you can check the health of the SANnav server anytime. If any of the services is down, it will be listed.

To check the health of the server, perform the following:

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

```
./check-server-status.sh
```

NOTE

If any service is found down while checking the server health status, it will be automatically started by system-monitor within 20 minutes.

The following is sample output of a healthy server.

```
-bash-4.2# sh ./check-server-status.sh
SANnav server is healthy. All the services are currently in running state.
```

The following is sample output of an unhealthy server.

```
-bash-4.2# sh ./check-server-status.sh
Following services are currently down or starting
filters-middleware
topology-middleware
```

SANnav Disk Usage Alert monitors the disk space used for every ten minutes. There are three threshold levels: 70%, 80%, and 90%. An event is sent when the threshold levels exceed or drop below the defined level. The following is the list of event severity:

- Warning - 70%
- Error - 80%
- Critical - 90%

Changing the Self-Signed Certificates for Client and Server Communication

You can replace the self-signed certificates with third-party signed certificates by performing the following:

Make sure that the SSL certificate and key files are copied to this host or VM.

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

```
./replace-server-cert.sh
```

When you run this script, SANnav is automatically restarted for the new certificates to take effect. After the server is back up, you must rediscover or unmonitor and then monitor all switches that are registered for telemetry data; otherwise, the new certificates do not take effect.

Changing the Self-Signed Certificates for the Kafka Brokers

By default, when SANnav is installed, self-signed certificates for Kafka are generated; these certificates are valid for two years. You can replace the self-signed certificates with third-party signed certificates by performing the following:

Ensure that the following requirements are met before you run the script:

- The common name (CN) of the certificate must match the fully qualified domain name (FQDN) of the host.
- If you have root and intermediate CA certificates, they must be chained into a single certificate.

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

```
./replace-kafka-certificates.sh
```

When you run this script, SANnav is automatically restarted for the new certificates to take effect. After the server is back up, you must rediscover or unmonitor and then monitor all switches that are registered for telemetry data; otherwise, the new certificates do not take effect.

2.7 Configuring a Firewall for SANnav

Perform the following steps to set up a firewall using `firewalld`. This example uses Red Hat Enterprise Linux (RHEL) 7.4.

1. Start the firewall using the following command.

```
sudo systemctl start firewalld
```

2. Check that the firewall is running.

```
sudo systemctl status firewalld
```

3. Enable the firewall automatically after a system reboot.

```
sudo systemctl enable firewalld
```

4. Add the SSH service to the trusted zone.

```
sudo firewall-cmd --zone=public --permanent --add-service=ssh
```

If any other default ports are customized, add the services for these ports as well. For example, if you are using HTTPS port 443, enter the following command:

```
sudo firewall-cmd --zone=public --permanent --add-service=https
```

5. Add ports using the following commands.

Note that in the following commands, `public` is the default zone. If your default zone is different, then use your default zone for the ports.

```
sudo firewall-cmd --zone=public --add-port=2377/tcp --permanent
```

```
sudo firewall-cmd --zone=public --add-port=7946/tcp --permanent
```

```
sudo firewall-cmd --zone=public --add-port=7946/udp --permanent
```

```
sudo firewall-cmd --zone=public --add-port=4789/udp --permanent
```

6. Associate the interface (if this is not done already) with the default profile.

```
sudo firewall-cmd --permanent --zone=public --change-interface=<interface_name>
```

7. After the ports are added, use the following command to reload the firewall configuration.

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

8. Verify whether the configuration is correct.

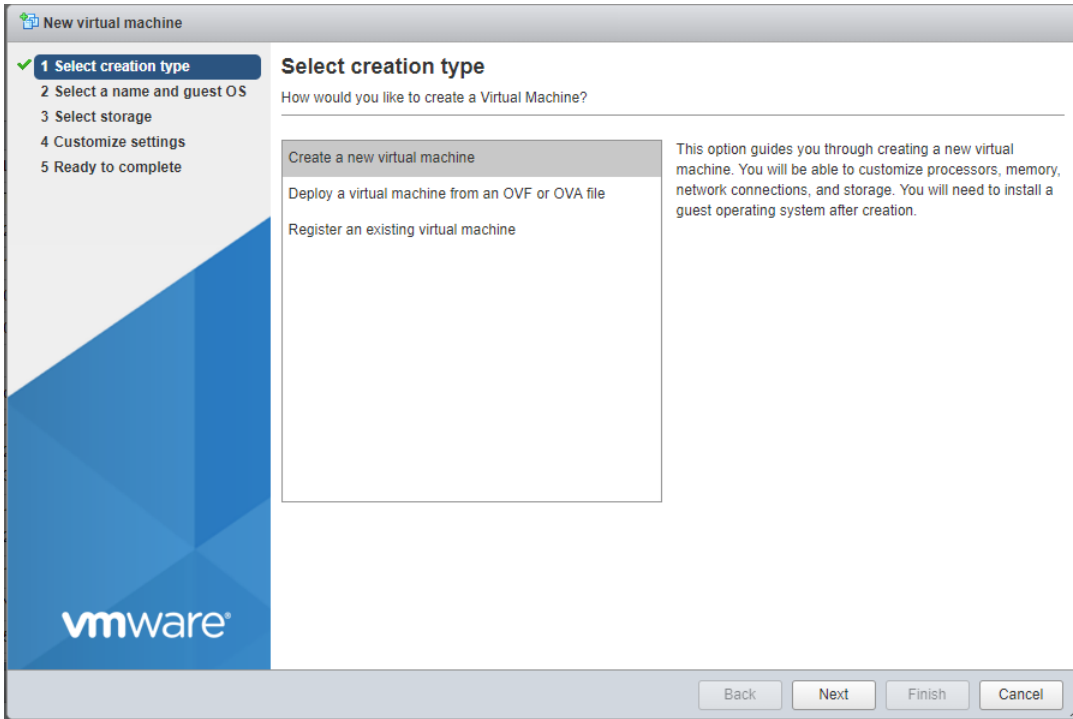
```
sudo firewall-cmd --list-all
```

2.8 Example of Provisioning a VM for SANnav Installation

This sample procedure shows one way to provision a virtual machine (VM) server for SANnav installation. You might use other methods to provision your VM.

1. Launch the VM creation wizard.

2. Select the option **Create a new virtual machine**, and click **Next**.



3. Select the following options to install the operating system, and click **Next**.
This example installs Red Hat Enterprise Linux.
 - Guest OS family: **Linux**
 - Guest OS version: **Red Hat Enterprise Linux 7 (64-bit)**

New virtual machine - SANnav (ESXi 6.7 virtual machine)

- 1 Select creation type
- 2 Select a name and guest OS**
- 3 Select storage
- 4 Customize settings
- 5 Ready to complete

Select a name and guest OS

Specify a unique name and OS

Name

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility:

Guest OS family:

Guest OS version:

Back Next Finish Cancel

4. Select the data store where the VM is to be placed, and then click **Next**.

The entire VM must be placed in a single datastore. The datastore can be from a direct-attached disk or through a network-mounted disk.

New virtual machine - SANnav (ESXi 6.5 virtual machine)

- 1 Select creation type
- 2 Select a name and guest OS
- 3 Select storage**
- 4 Customize settings
- 5 Ready to complete

Select storage

Select the datastore in which to store the configuration and disk files.

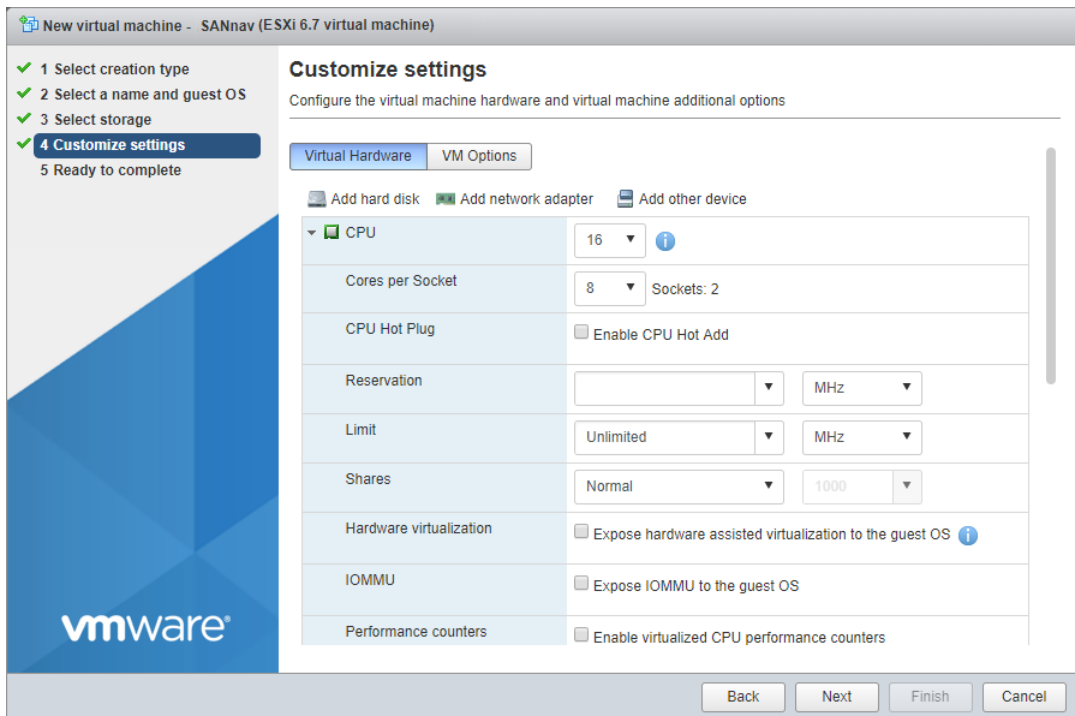
The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	1.63 TB	1.03 TB	VMFS5	Supported	Single
vsanDatastore	0 B	0 B	vsan	Supported	Single

2 items

Back Next Finish Cancel

5. In the **CPU** section, set the required cores, which must be dedicated from two sockets.
 - For managing up to 3,000 ports:
 - **CPU = 16**
 - **Cores per Socket = 8**
 - For managing up to 15,000 ports:
 - **CPU = 24**
 - **Cores per Socket = 12**



6. In the **Memory** section, allocate the RAM capacity:
 - 48 GB for managing up to 3,000 ports
 - 96 GB for managing up to 15,000 ports

New virtual machine - SANnav (ESXi 6.7 virtual machine)

1 Select creation type
 2 Select a name and guest OS
 3 Select storage
 4 **Customize settings**
 5 Ready to complete

Customize settings

Configure the virtual machine hardware and virtual machine additional options

Virtual Hardware | VM Options

CPU	16	
Memory		
RAM	48	GB
Reservation		MB
	<input type="checkbox"/> Reserve all guest memory (All locked)	
Limit	Unlimited	MB
Shares	Normal	1000
Memory Hot Plug	<input type="checkbox"/> Enabled	
Hard disk 1	16	GB

Back Next Finish Cancel

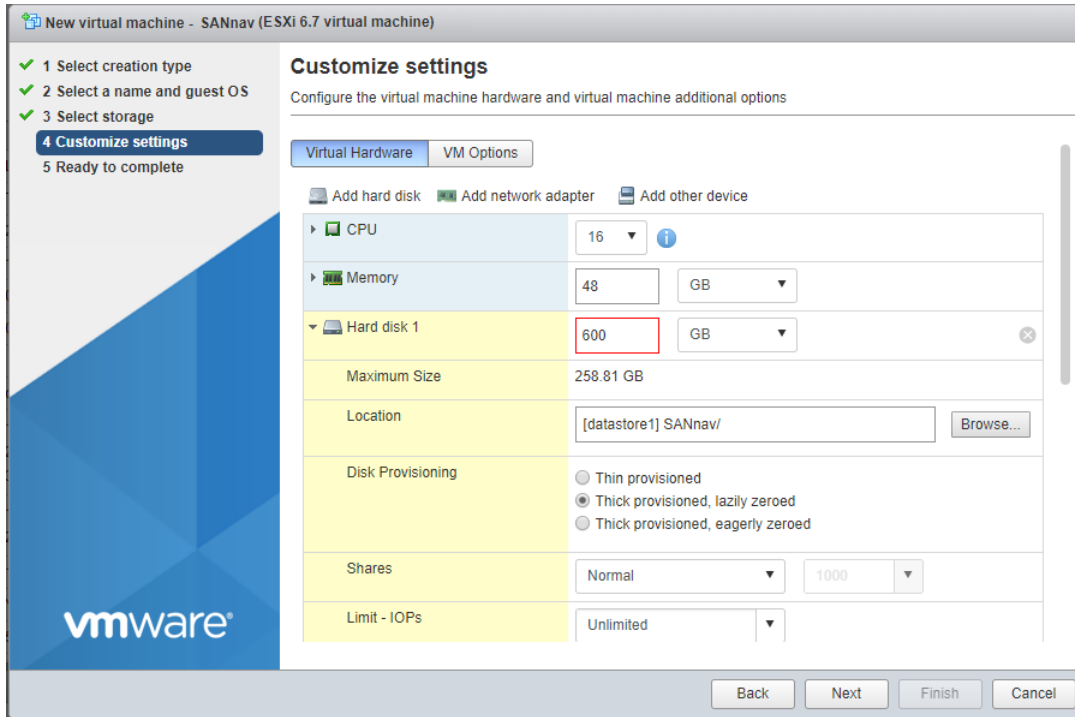
7. In the **Hard Disk** section, allocate the total required disk space:

- 600 GB for managing up to 3,000 ports
- 1.2 TB for managing up to 15,000 ports

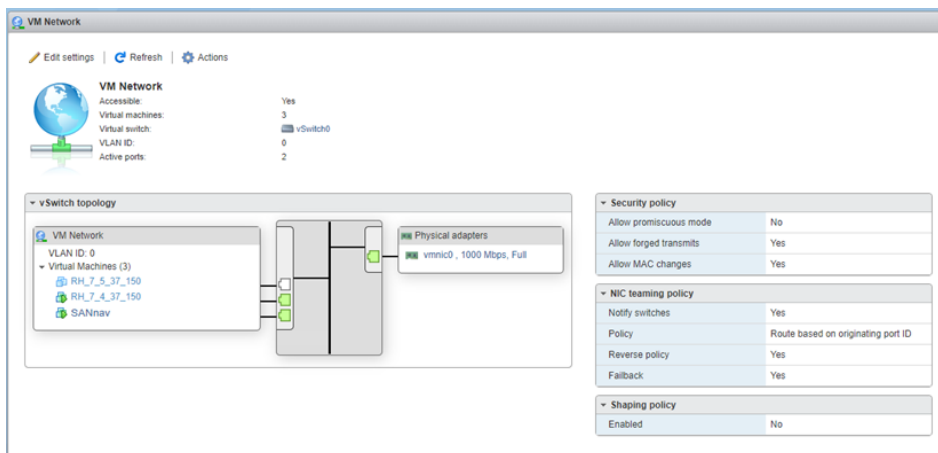
NOTE

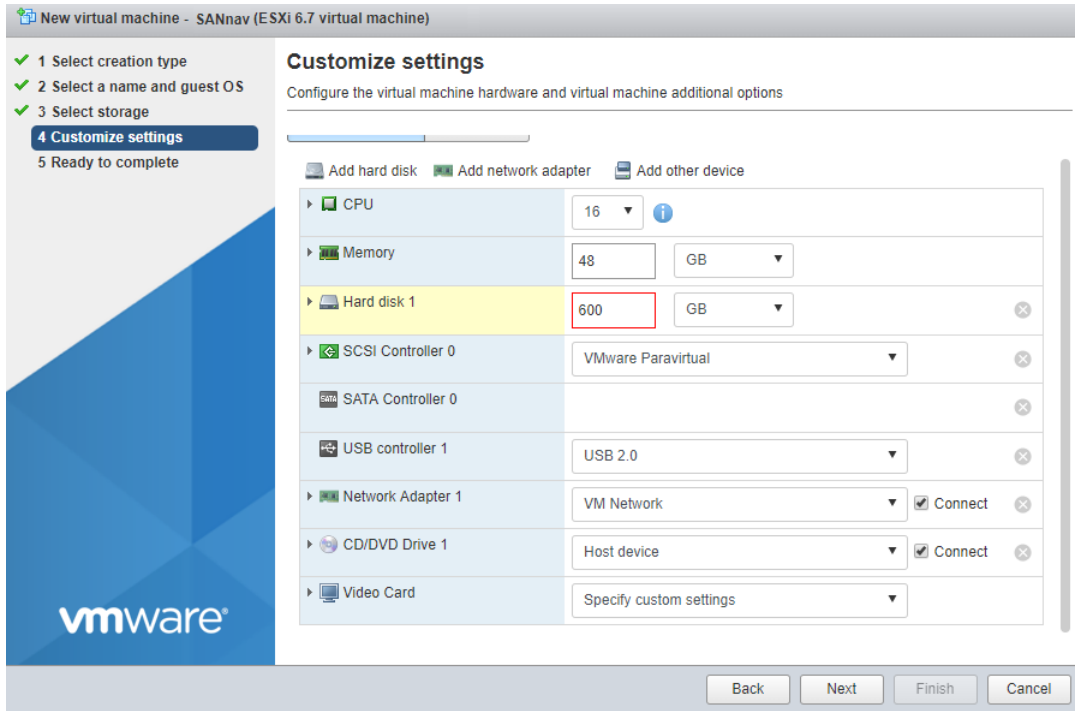
The disk space requirement listed above is for SANnav only. Be sure to account for additional space required by the operating system and for saving files.

Thick-provision the required disk space from a single datastore.



8. Configure the standard virtual switch, and assign the configured switch to the Adapter 1.
By default the virtual switch is **VM Network**.





9. Power on the VM for loading the guest OS.

The partition sizes must be as follows:

- /home: ≥ 450 GB
- /var: ≥ 120 GB
- /: ≥ 20 GB (swap space)
- /boot: \geq minimum required space for running the OS

For this example, the guest OS is Red Hat Enterprise Linux. The Red Hat Enterprise Linux OS can be loaded through a bootable disk or through a PiXe server.

The screenshot shows the 'MANUAL PARTITIONING' screen for 'RED HAT ENTERPRISE LINUX INSTALLATION'. The interface is divided into several sections:

- Left Panel:** A tree view showing the partitioning plan. Under 'New Red Hat Enterprise Linux Installation', there are categories for 'DATA' and 'SYSTEM'.
 - DATA:** /home (rhel-home) with 465.66 GiB.
 - SYSTEM:** /boot (sda1) with 37.25 GiB, / (rhel-root) with 46.57 GiB, and /var (rhel-var) with 139.7 GiB.
 - swap:** rhel-swap with 9536.74 MiB, which is currently selected.
- Bottom Left:** Summary statistics: 'AVAILABLE SPACE' is 1529.97 MiB (in a pink box) and 'TOTAL SPACE' is 700 GiB (in a grey box). A link below reads '1 storage device selected'.
- Right Panel:** Configuration for the selected 'rhel-swap' partition.
 - Mount Point:** An empty text field.
 - Device(s):** 'VMware Virtual disk (sda)'.
 - Desired Capacity:** 9536.74 MiB, with a 'Modify...' button.
 - Device Type:** 'LVM' (dropdown), with an 'Encrypt' checkbox.
 - File System:** 'swap' (dropdown), with a checked 'Reformat' checkbox.
 - Volume Group:** 'rhel (4096 KiB free)' (dropdown), with a 'Modify...' button.
 - Label:** An empty text field.
 - Name:** 'swap' (text field).
- Buttons:** 'Done' (top left), 'Help!' (top right), and 'Reset All' (bottom right).

Next, before installing SANnav, make sure that your system meets the requirements as stated in [SANnav Management Portal Deployment](#) and [SANnav Global View Deployment](#).

Getting Started with SANnav Management Portal

3.1 SANnav Overview

SANnav is the next generation SAN management application suite for Brocade SAN environments.

SANnav enables 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 designed based on real-world use cases and user workflows, providing a highly intuitive user experience. SANnav uses a micro-services-based architecture based on Docker container technology that allows it to scale to meet the management needs of both small and large SAN environments and those that may change over time. This scalable architecture also allows SANnav to support new functionality in the future without causing degradation to the performance of the application.

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

There are two distinct SANnav product offerings:

- SANnav Management Portal
- SANnav Global View

SANnav Management Portal

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.

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. Using filters and tags, you can sort and search your inventory to find exactly the information that you want. A highly flexible reporting infrastructure enables you to generate custom graphical or tabular reports.

SANnav Management Portal does not replace Brocade Web Tools or the Fabric OS command line interface.

SANnav Global View

You can get a comprehensive view of a SAN environment that spans multiple SANnav Management Portal instances through the SANnav Global View product. SANnav Global View enables you to navigate seamlessly across multiple SANnav Management Portal instances and drill down to any individual SANnav Management Portal instance to perform detailed monitoring, investigation, and troubleshooting.

3.2 Browser Requirements

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

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

- Chrome (Google)
- Firefox (Mozilla)

Note that if you access the client from the Remote Desktop, the user interface may have degraded performance.

Launching Brocade Web Tools from a SANnav client is supported only on the following browser:

- Firefox

3.3 Launching SANnav Management Portal

Launch SANnav Management Portal to monitor and manage your fabrics.

1. Open your browser and enter the IP address or fully qualified domain name (FQDN) of the SANnav Management Portal server.

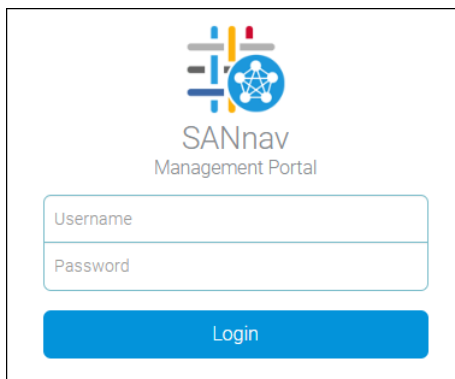
You can use http or https, for example:

```
http://192.0.2.0
```

or

```
https://192.0.2.0
```

The SANnav Management Portal login window appears.



If the login window does not appear, try the following:

- Ping the SANnav server to ensure that it is up.
 - Check if SANnav services are running. See "Checking the Server Health" in [Additional Scripts](#).
 - Check the firewall settings.
2. Enter your SANnav user name and password, and click **Login**.
For the first SANnav login, the default user name is "Administrator" and the default password is "password".
SANnav launches with the default dashboard displayed.

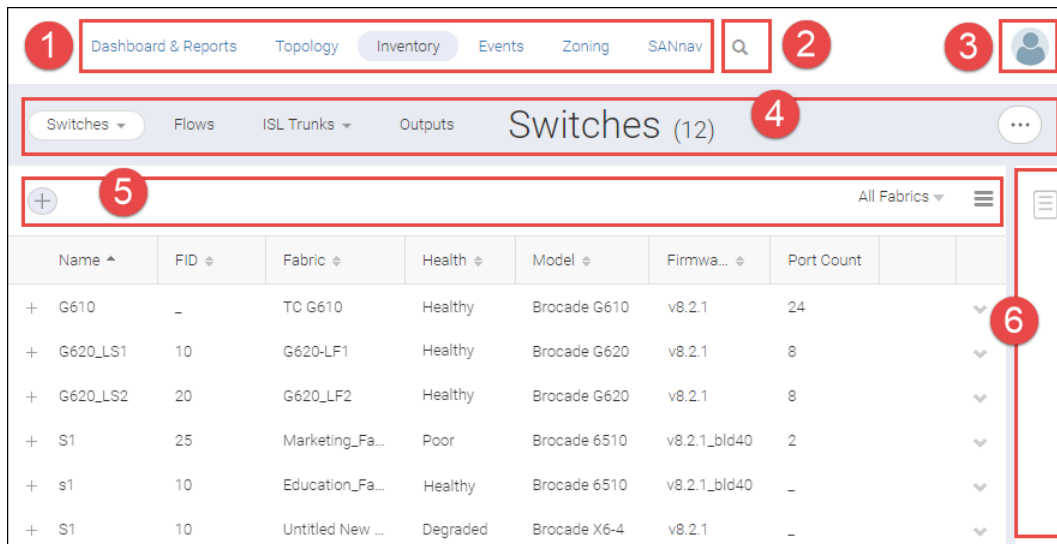
If, instead of launching, SANnav displays the message "Login Failed. Service is not available at this time.", SANnav is in the process of starting up. Wait a few minutes and try to log in again.

The first time you log in, you should change the default password.

3.4 Overview of the User Interface

SANnav Management Portal allows you to manage one or more SAN fabrics in multiple locations. Once familiar with the basic components of SANnav, you can quickly start monitoring and managing your fabrics.

The following screen capture shows the basic layout of the SANnav user interface.

Figure 1: SANnav Management Portal User Interface

1. Navigation bar. Contains links to feature pages. The **SANnav** link displays the **Configurations and Settings** page.
2. Search. Click the icon to display the search box, select a context on which to search from the list, and enter the search term in the field.
3. Profile menu. Click the icon to display additional links for changing user preferences, displaying the SANnav version, and logging out.
4. Subnavigation bar. Provides the page title and optional item count within parentheses. Also includes buttons and menus to take actions within the page. 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, network scope, and customized filters.
6. Expandable sidebar. Provides an area where you can save selected inventory items for investigation later.

Detail Pages

Clicking a fabric name, switch name, or port name in a table opens a detail page for that object. The detail page displays additional information about the object and may contain additional actions that you can perform.

The detail page is different depending on the context. For example, the detail page for a fabric on the **Inventory** page is different from the detail page for the same fabric on the **Discovery** page.

Figure 2: Detail Page for a Switch

Tables

In tables, if an entry is truncated (indicated by an ellipsis at the end of the entry), hover the mouse over the entry to see the full text.

Figure 3: Hovering the Mouse over Truncated Table Text

Source N...	Description	Source Address
RH77_37_2	Successfully authenticated user Adm...	10.155.37.2
RH77_37_2	Failed to register syslog for the switc...	10.155.37.2
RH7	Failed to register syslog for the switch [truncated]. The syslog destination table is full.	[truncated]
RH7	Successfully registered onwip (trap) r...	[truncated]

Many tables have an action menu that you can access by clicking the down arrow in the rightmost column. Click this arrow to display additional actions that you can perform on the associated object.

Figure 4: Using the Down Arrow to Display Additional Actions

Firmware	Port Count	
v8.2.0	8	▼
v8.2.0	8	▼
v8.2.0		View
v8.2.0		Select
v8.2.0		Investigate
v8.2.0		Show in Topology
v8.2.0		Open in WebTools
v8.2.0	29	▼


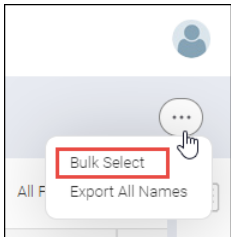
On the right side of the subnavigation bar, the **More** button () often contains a **Bulk Select** option, which allows you to select and perform operations on one or more items at the same time. For example, you can turn monitoring on for multiple fabrics, or you can create a tag and apply it to multiple switches.

Figure 5: Bulk Select





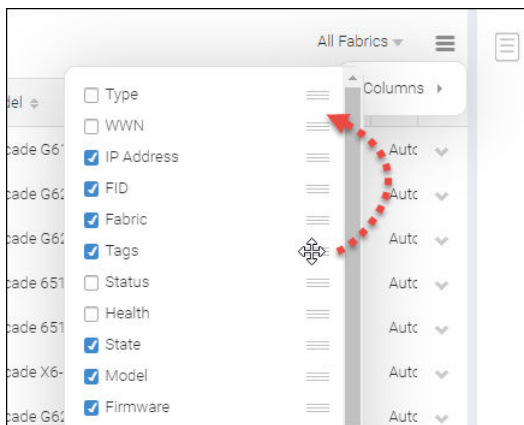
For the **Inventory** and **Events** pages, you can customize which columns are displayed and in what order.

3.4.1 Customizing Table Columns

You can customize table columns in the SANnav **Inventory** and **Events** pages by resizing the columns and adding or deleting columns. You can also rearrange columns on the **Inventory** page.

Column selection and column arrangement persist across page navigation.

1. Click the hamburger icon () on the right side of the filter bar, and select **Columns**.
2. Check the boxes next to the columns that you want to display; uncheck the boxes next to the columns that you want to hide.
3. To rearrange columns, hover over the move icon (), and drag it up or down.



4. Click anywhere outside the column list window to close it.
5. To resize a table column, hover the mouse over the right-side column boundary and drag the boundary.

3.4.2 Searching for Objects

SANnav context search allows you to search for and display specific inventory items and events based on key properties.

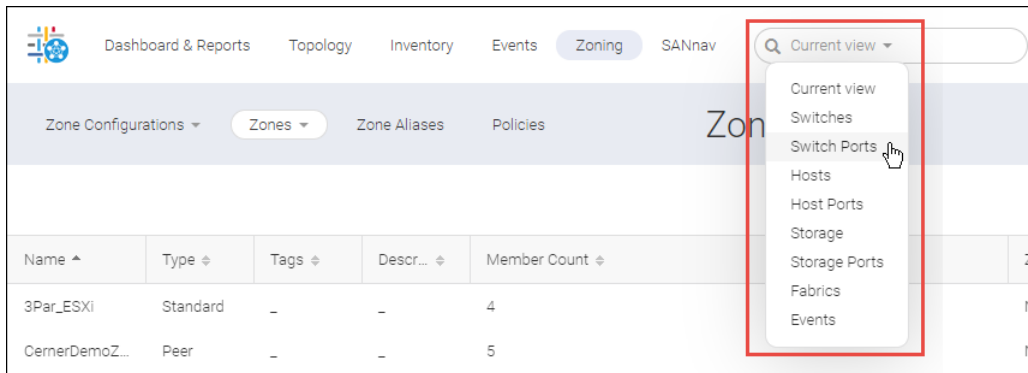
Note that filters and search are independent entities. If you apply a filter and then perform a search, SANnav searches the entire database, not just the filtered items.

1. Click the magnifying glass icon at the top of the page.

- Click the drop-down list, and select the category of objects that you want to search.

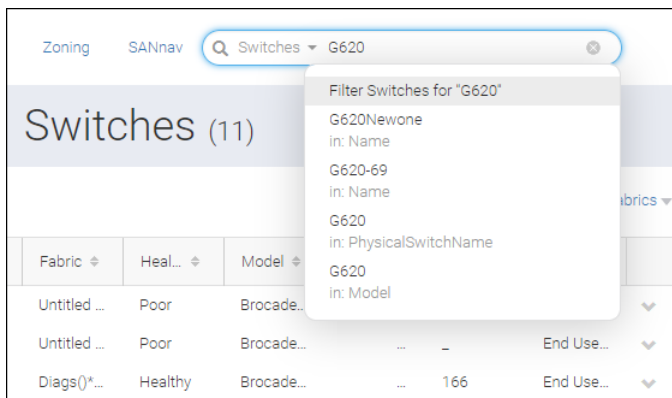
A search finds objects only within the selected category. For example, if you select **Fabrics** and enter **G620**, the search finds fabrics with "G620" in one of the key properties, but it does not find G620 switches.

Selecting the **Current view** category searches the current page. Note that the **Current view** category is not available on every page. The **Current view** category is available for items other than inventory items or events, such as zones, reports, user names, or MAPS policies.



- Type the character string that you want to search for.

If you type three or more characters, up to nine auto-suggestions for key properties are listed. Auto-suggestions are not provided for the **Current view** category.



- Select one of the auto-suggestions, or press **Enter** to display search results matching any property.

SANnav searches the entire page, including hidden columns.

For events, SANnav searches through all stored events, not just those displayed on the page. Note that for events, only the following properties are searched:

- Source Name
- Description
- Source Address
- Fabric
- Severity
- Message ID

The search results are displayed in a list view; however, if you click a **Name** property in the auto-suggestion list, the detail view for that object displays.

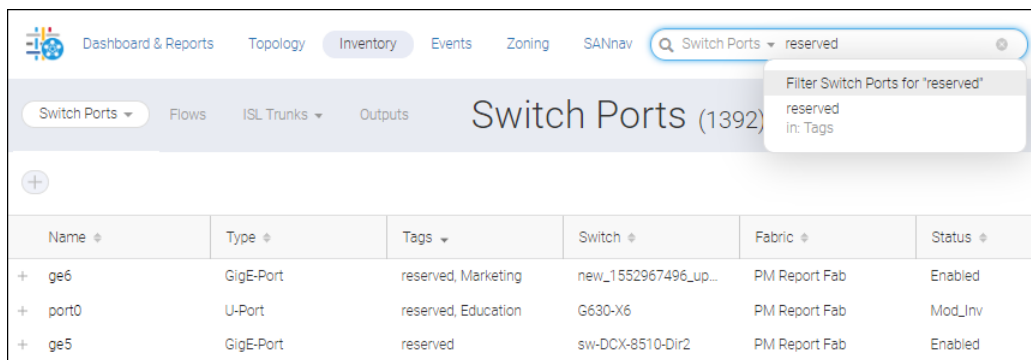
3.4.3 Tags

Tags are short descriptions that you can assign to objects to enable you to quickly retrieve and manage those objects.

For example, you can assign a tag "reserved" to unused switch ports to indicate that they are reserved for future updates. You can assign a tag to switches to indicate in which data center they are located (such as "DC1" or "San Jose DC").

You can assign multiple tags to the same object. For example, for the reserved switch ports, you can assign multiple tags to also indicate for which department they are reserved, such as "reserved, Education" and "reserved, Marketing". For switches, in addition to the data center, you can also indicate the aisle and rack number, such as "DC1, aisle 1, rack 3".

Perform searches using the tags to quickly retrieve information. For example, on the **Inventory** page for switch ports, perform a search on "reserved" to display all switch ports with the "reserved" tag.



Name	Type	Tags	Switch	Fabric	Status
ge6	GigE-Port	reserved, Marketing	new_1552967496_up...	PM Report Fab	Enabled
port0	U-Port	reserved, Education	G630-X6	PM Report Fab	Mod_Inv
ge5	GigE-Port	reserved	sw-DCX-8510-Dir2	PM Report Fab	Enabled

Used with filters, tags provide a powerful way to narrow down and filter data. For example, you can create a switch ports filter to display switch ports with the tag "reserved", operating at "16Gb/s" speed, and currently in the "online" state.

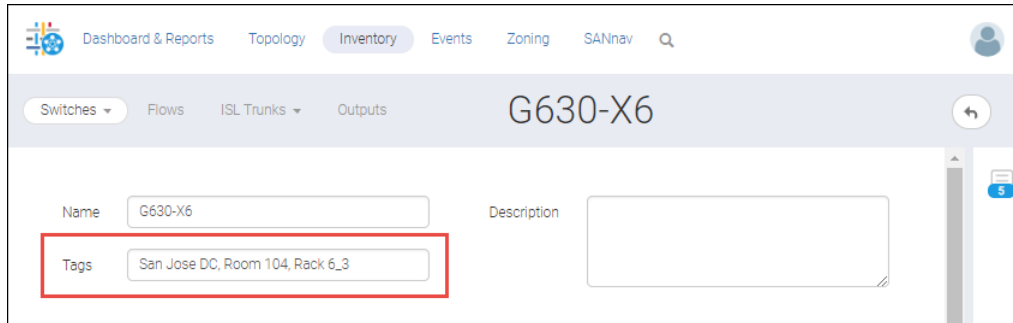
Almost every type of entity supports tagging, including inventory items (such as fabrics, switches, ports), users, roles, areas of responsibility (AORs), dashboards, reports, and extension tunnels.

3.4.4 Tagging Objects

When you tag objects, you can tag them individually or in bulk. Bulk tagging is useful if you want to assign the same tag to several similar objects (such as switches).


Only alphanumeric characters, spaces, and underscores (_) are allowed in tags. Multiple tags are separated by a comma.

Almost every detail page has a **Tags** field, where you can enter and edit the tags for that object. The following switch has three tags, indicating the data center, room number, and rack number of the switch.

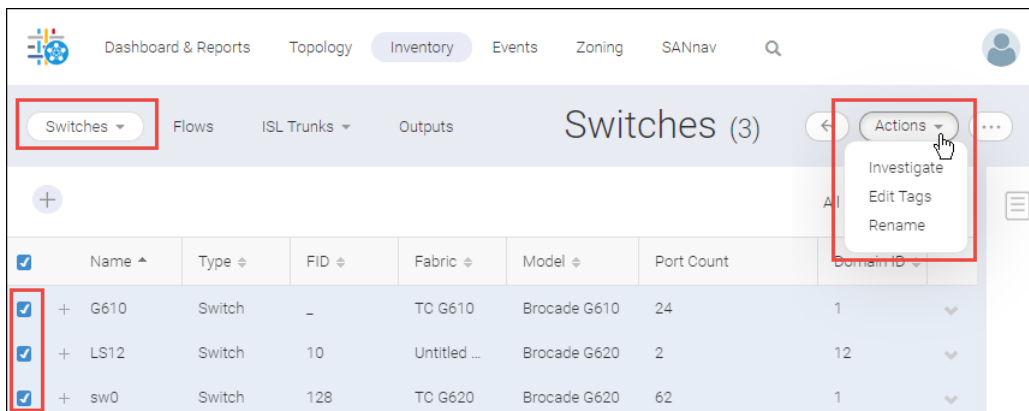


On the **Inventory** page, you can tag multiple objects at the same time, using the bulk select option, as shown in the following procedure.

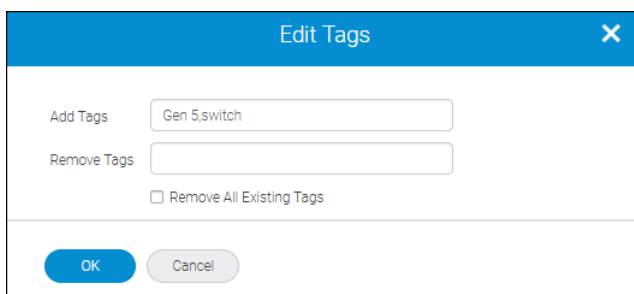
The following example tags all Gen 5 switches as "Gen 5". In addition, the example tags directors and switches as "director" and "switch".

1. Click **Inventory** in the navigation bar, and then select the type of entity that you want to tag.
For this example, select **Switches** from the drop-down list.
2. Click the **More** button () in the top-right corner of the page, and click **Bulk Select**.
A column of checkboxes displays at the left of the table.
3. Select the items that you want to tag, click the **Actions** drop-down, and click **Edit Tags**.

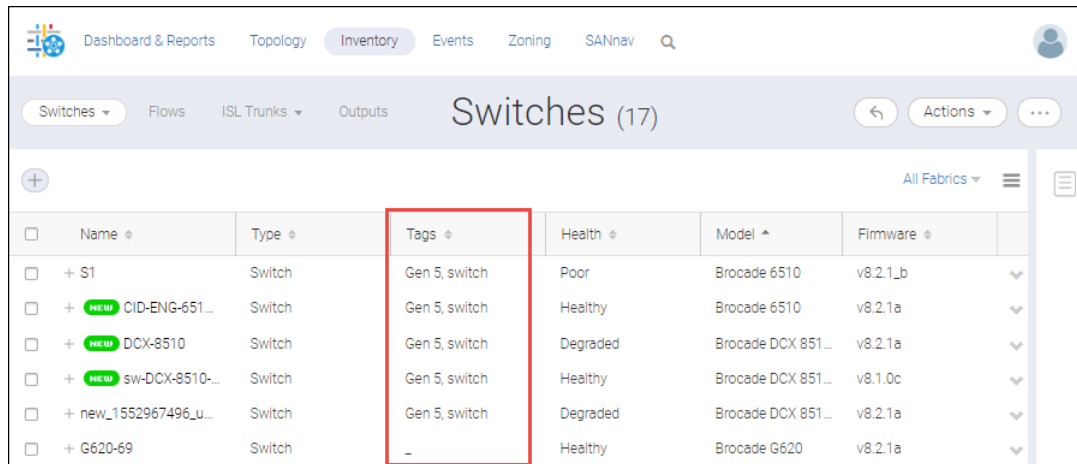
For this example, click the **Model** column to sort the switch inventory list by model, and then select the Gen 5 switches and directors.



4. In the **Edit Tags** dialog, enter the tags in the **Add Tags** field, and click **OK**.
For this example, enter two tags, separated by a comma: **Gen 5,switch**.



The tags are added to the **Tags** column in the **Inventory** page.

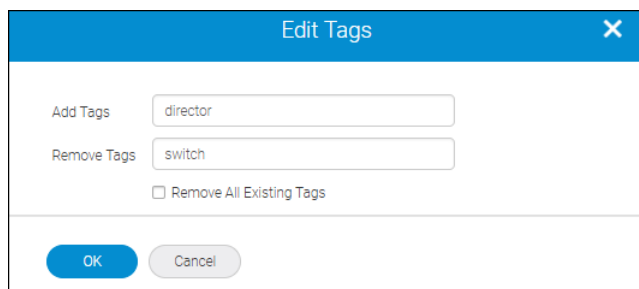


Name	Type	Tags	Health	Model	Firmware
+ S1	Switch	Gen 5, switch	Poor	Brocade 6510	v8.2.1_b
+ NEW CID-ENG-651...	Switch	Gen 5, switch	Healthy	Brocade 6510	v8.2.1a
+ NEW DCX-8510	Switch	Gen 5, switch	Degraded	Brocade DCX 851...	v8.2.1a
+ NEW sw-DCX-8510-...	Switch	Gen 5, switch	Healthy	Brocade DCX 851...	v8.1.0c
+ new_1552967496_u...	Switch	Gen 5, switch	Degraded	Brocade DCX 851...	v8.2.1a
+ G620-69	Switch	-	Healthy	Brocade G620	v8.2.1a

Note that in this example, all switches are tagged with "Gen 5" and "switch"; however, the directors should be tagged with "director" instead of "switch". The following steps show how you can edit and remove tags.

- To edit or remove tags, select the items that you want to edit, click the **Actions** drop-down, and click **Edit Tags**. For this example, select the directors, so that you can remove the "switch" tag and replace it with a "director" tag.
- In the **Edit Tags** dialog, enter the tags that you want to add in the **Add Tags** field, and enter the tags that you want to remove in the **Remove Tags** field.

For this example, add the tag "director" and remove the tag "switch".



Edit Tags
✕

Add Tags

Remove Tags

Remove All Existing Tags

OK
Cancel

Note that when you edit tags in bulk, you cannot modify an existing tag in place. You must add the modified tag and remove the old tag.

To remove all tags from the selected items, select the **Remove All Existing Tags** check box.

- Click **OK**.

The inventory list displays the updated tags.

The screenshot shows the 'Switches (17)' page in the SANnav Management Portal. The table below lists various switches with their details. A red box highlights the 'Tags' column for three specific switches: 'DCX-8510', 'sw-DCX-8510-...', and 'new_1552967496_u...'. All three of these switches have the tag 'Gen 5, director'.

Name	Type	Tags	Health	Model	Firmware
+ S1	Switch	Gen 5, switch	Poor	Brocade 6510	v8.2.1_bld40
+ NEW CID-ENG-651...	Switch	Gen 5, switch	Healthy	Brocade 6510	v8.2.1a
+ NEW DCX-8510	Switch	Gen 5, director	Degraded	Brocade DCX 851...	v8.2.1a
+ NEW sw-DCX-8510-...	Switch	Gen 5, director	Healthy	Brocade DCX 851...	v8.1.0c
+ new_1552967496_u...	Switch	Gen 5, director	Degraded	Brocade DCX 851...	v8.2.1a
+ G620-69	Switch	-	Healthy	Brocade G620	v8.2.1a

3.4.5 Filters

Filters are a set of criteria that limits the data being displayed. You can use filters on the **Events**, **Inventory**, and **Reports** pages.

For example, you can create the following filters:

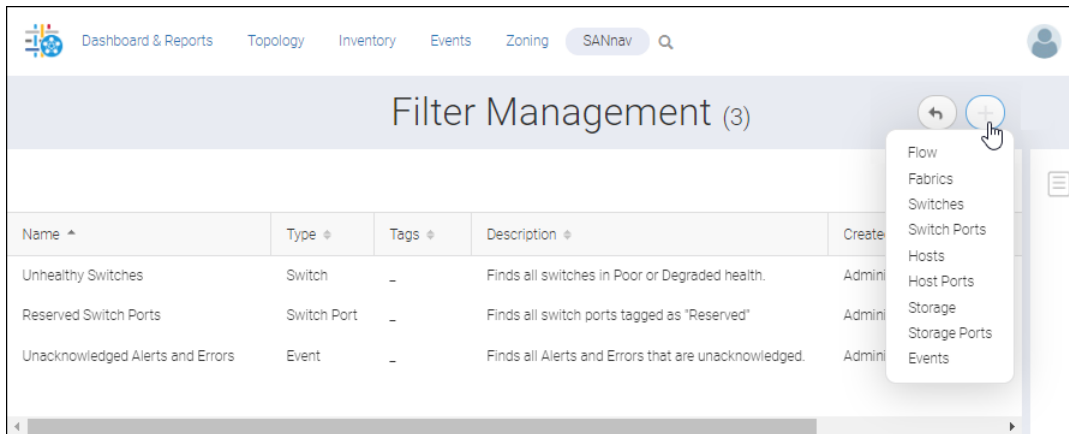
- On the **Inventory** page, you can create filters to display only switches in degraded or poor health.
- On the **Events** page, you can create a filter to display only user action events.
- When generating a report, you can create a filter to gather report data only from switches running a specific Fabric OS version.

Filters can be combined with tags for customized reporting and filtering. For example, you can tag switches based on data center. Then you can create a report filter to gather data only from switches running a specific Fabric OS version in a specific data center.

Filters can be temporary or permanent.

- Temporary filters exist until you close them or log out of the application. You can assign a name to a temporary filter and save it to make it a permanent filter.
- Permanent filters exist until you specifically delete them. Permanent filters are shared with other SANnav users. Only the user who created the permanent filter can update or delete that filter.

You can create, update, and manage filters in the **Filter Management** page. The **Filter Management** page displays all permanent filters, including those created by other users.

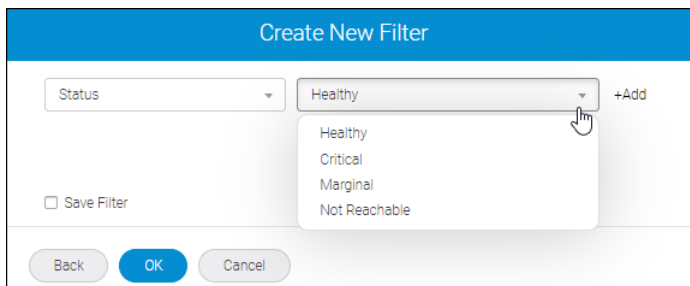
Figure 6: Filter Management Page

You can create filters in the **Filter Management** page and then apply these filters in the **Inventory**, **Events**, and **Reports** pages. Conversely, you can create and save filters in the **Inventory**, **Events**, and **Reports** pages, and you can then view and manage these filters in the **Filter Management** page.

3.4.5.1 Wildcards in Filters

SANnav supports the standard wildcard characters in filters. An asterisk (*) represents zero or more characters, and a question mark (?) represents a single character.

When you create filters, you select properties and values. Some of the properties have fixed values, and you select them from a drop-down list. For example, for a switch filter, the **Status** property has the fixed values **Healthy**, **Critical**, **Marginal**, and **Not Reachable**.



Some of the properties have values that you enter manually. You can enter complete or partial values, and the values are not case-sensitive. For example, you can create a switch filter and specify **65** for the model to display all Brocade 6505, 6510, and 6520 switches in the **Inventory** page. In this case, the wildcard is implicit.

You can also use an explicit wildcard. In the previous example, entering **65** is the same as entering ***65***.

NOTE

Events filters do not support wildcards. For example, if you are filtering based on message ID, you must enter the complete message ID in the filter.

3.4.5.2 Rules for AND and OR Filters

In SANnav, you create AND conditions by adding multiple, dissimilar properties to the same filter. You create OR conditions by creating multiple filters or by adding multiple, similar properties to the same filter.

Adding properties that are different creates an AND condition. For example, if you want to find all Brocade G610, G620, and G630 switches running Fabric OS 8.2.x, you can create a filter with **Model = G6** and **Firmware Version = 8.2**. The following filter finds all switches with "G6" in the model property AND with "8.2" in the firmware version.

Adding properties that are the same creates an OR condition. For example, the following filter finds all fabrics with **Health = Poor OR Health = Degraded**.

Adding a combination of properties creates AND and OR conditions within the same filter. For example, the following filter finds all fabrics with "Fabric" in the **Name** property and with **Health = Poor** or **Health = Degraded**. (The **Name** property is not case-sensitive.)

NOTE

If you use the same property more than once in a filter, wildcards are not accepted, and the values must be an exact match.

For example, if you want to find all Gen 6 switches (switch model is Brocade G610, G620, G630, or 7810), the following filter does not work, because wildcards (even implicit wildcards) are not accepted.

In this case, you must specify the exact model number for each switch, as shown here.

NOTE

You can create an OR condition by creating and applying separate filters.

Using the previous example, you can create one switch filter with **Model = G6** and a second switch filter with **Model = 7810**. Applying both filters produces the same results—all switches are found with the model equal to G610, G620, G630, or 7810. In this case, because each attribute is used only once in a filter, wildcards are accepted.

3.4.5.3 Creating Filters

In SANnav, create filters when you want to view a subset of inventory items or events or when you want to create report content for a subset of objects.

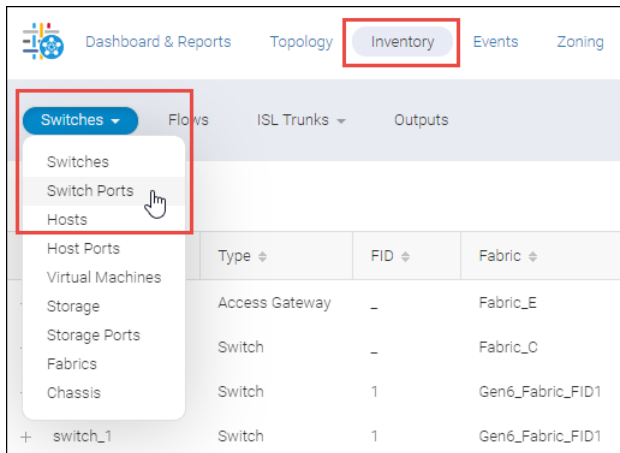
Filters are created on the **Inventory** and **Events** pages and on the **Templates** page when you create or edit report content.

You can create a filter for one-time use, or you can give the filter a name and save it, so you can use it again and make it available for other SANnav users.

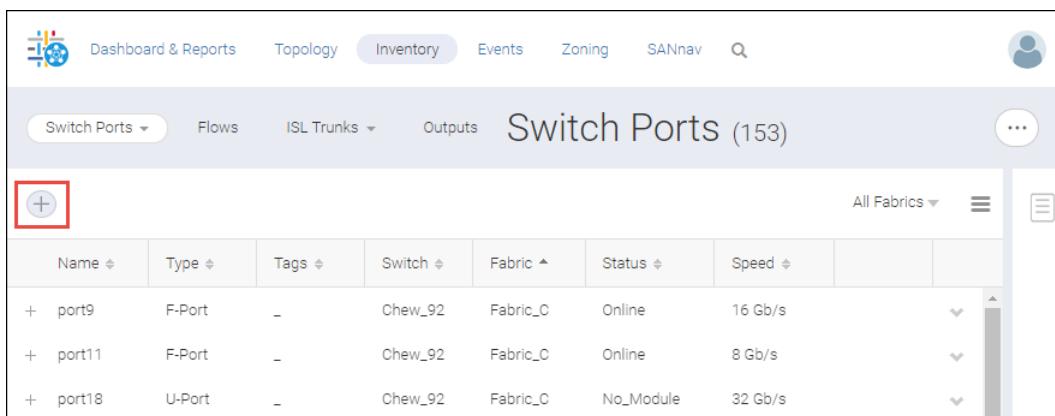
Suppose that you want to locate all available switch ports in Fabric_C and tag them as "reserved" for future expansions. The following example shows how you can create a switch port filter to display all U_Ports in Fabric_C.

1. Navigate to the page where you want to create the filter.
 - Click **Events** in the navigation bar to create an events filter.
 - Click **Inventory** in the navigation bar, and then select the type of inventory from the drop-down list.
 - Click **Dashboard & Reports** in the navigation bar, and then click **Templates**. Either click an existing report in the list or click the **+** button in the upper left corner to create new report content.

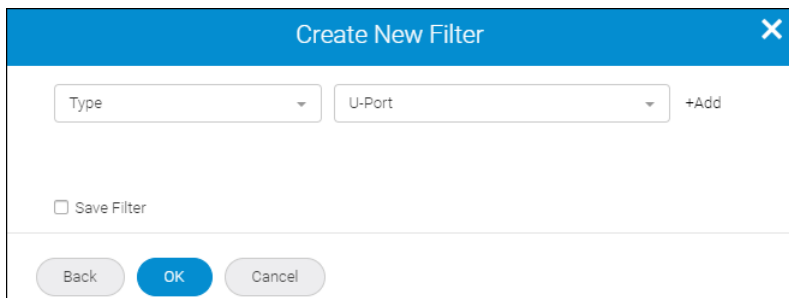
This example assumes that you are viewing the inventory of switch ports. For this example, click **Inventory** in the navigation bar, and then click **Switch Ports** from the drop-down list.



- Click the **Add** button (+) in the filter bar (in the left corner of the page).
If the **Add** button is missing, the page you are on does not support filters.



- In the **Add Filter** dialog, click the **Create New** button.
- In the **Create New Filter** dialog, select any property from the drop-down list, and enter a value on which to filter.
For this example, select **Type** as the property and **U-Port** as the value.



- Click **+Add** to add additional properties to the filter.
For this example, select **Fabric** as the property, and type **Fabric_C** as the value. Notice that as you start typing, SANnav provides auto-suggestions.

6. Save the filter.

- Click **OK** to create a temporary filter on the **Inventory** page. This filter is automatically deleted when you log out of the application.

Or

- Click the **Save Filter** check box, provide **Name**, **Tags**, and **Description** details, and then click **OK**. The filter is available on the **Inventory** page and is also saved as a permanent filter in the **Filter Management** page.

NOTE

Although the **Description** field is optional, provide a good description so you and other users can understand what the filter does.

3.4.5.4 Managing Filters

You can view, modify, create, and delete permanent filters from the SANnav **Filter Management** page.

All permanent filters are managed from the **Filter Management** page. This includes filters that are created from the **Filter Management** page as well as filters created from the **Inventory**, **Events**, and **Templates** (reports) pages.

- Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Filter Management**.

A list of all permanent filters displays.

Name ^	Type ⇅	Tags ⇅	Description ⇅	Created By ⇅	Access Level ⇅	Last Modified ⇅
Available Ports in Fabric	Switch Port	-	Find all available...	Administrator	Read & Write	May 13, 2019 12...
Unhealthy Switches	Switch	-	Show switches...	Administrator	Read & Write	May 13, 2019 12...
User Action Events	Event	-	Show switches with Degraded and Poor health.	Administrator	Read & Write	May 13, 2019 12...

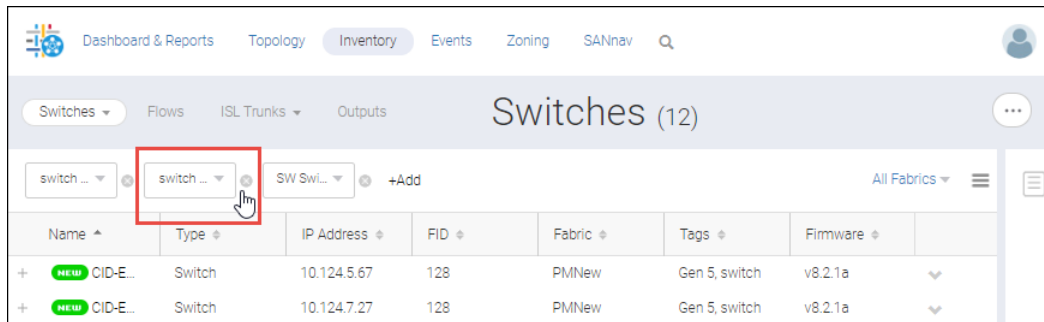
- To modify or delete a filter, click the filter name or click the down arrow in the action menu and select **View**. The filter detail page opens, where you can make changes to the filter, save it as a different filter, or delete it.

- To create a filter, click the add button (+) in the top right corner of the page, and then select the type of filter that you want to create from the drop-down list.

3.4.5.5 Deleting Filters

Only the user who created the filter can delete the filter.

If you want to remove a filter from the filter bar, click the small **X** to the right of the filter.



When you click the **X**, the filter is removed from consideration. If the filter is a temporary filter, it is deleted, and you must recreate it if you want to use it again. If the filter is a permanent filter, it is removed from the filter bar, but it is not deleted. You can select it again when you add a new filter to the page.

To delete permanent filters, perform the following steps.

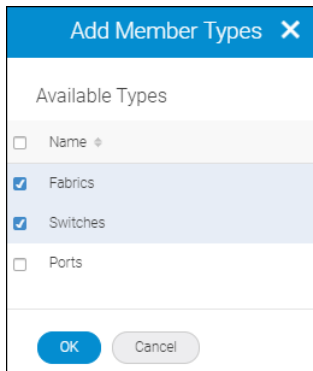
- Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Filter Management**.
The list of permanent filters displays.
- Click the filter name, or click the down arrow to the right of the filter that you want to delete and select **View**.
- Click **Delete** in the filter details page.
- Click **OK** in the confirmation dialog.

3.4.6 Creating a Network Scope

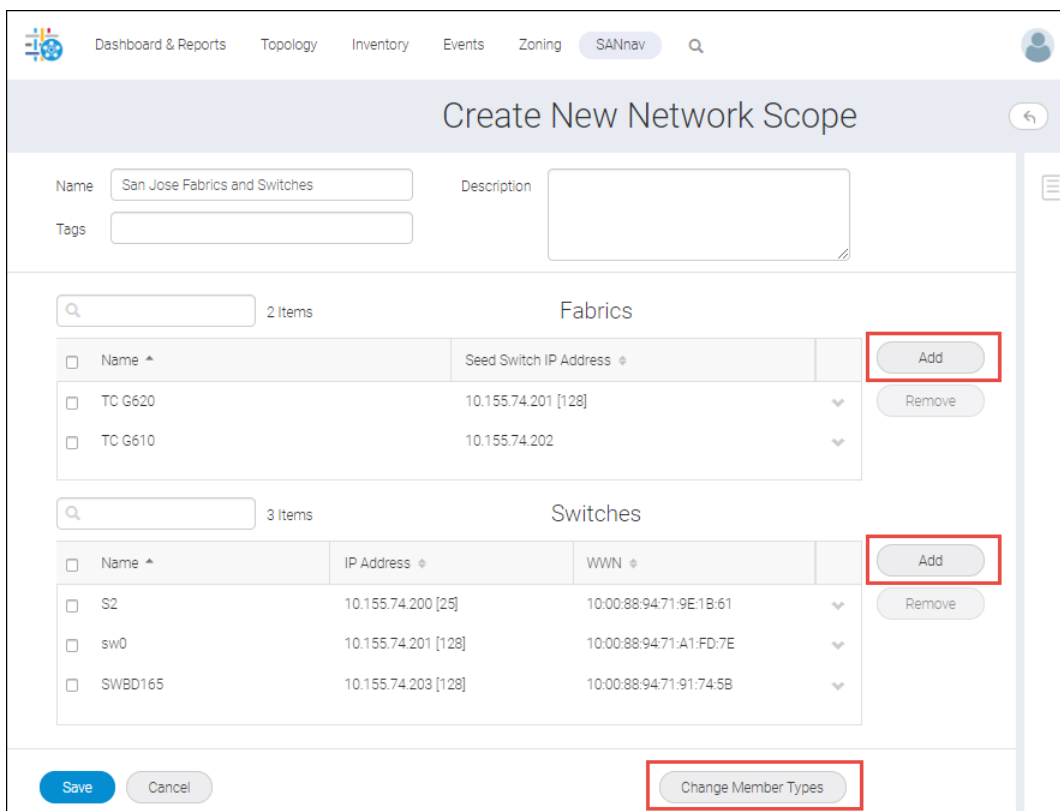
The network scope enables you to view dashboards, reports, and events for a select set of network entities. By default, the network scope is all fabrics. You can create custom network scopes for a subset of fabrics, switches, and switch ports.

- Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Network Scope Management**.
The **Network Scope Management** page appears and lists all of the custom network scopes.
- Click the + icon in the upper right corner of the page to add a network scope.
- Enter a name, tags, and a description for the network scope, and click **Add** to add member types.
- Select the types of members that you want in the network scope, and click **OK**.

A network scope can consist of any combination of fabrics, switches, and switch ports.



- For each member type, click **Add** to add specific members to the scope.
Click **Change Member Types** if you want to add or remove member types.



- Click **Save** when you are finished.
The **Save** button is not activated unless you have specified a scope name and at least one member for each member type.

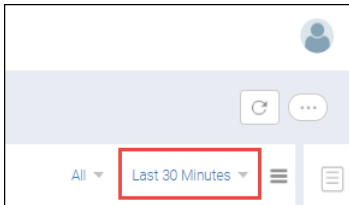
The custom network scope can now be selected from the network scope drop-down for dashboards, reports, and events. Custom network scopes are always listed at the end of the drop-down list.

3.4.7 Setting the Date Range for Dashboards, Reports, and Events

One way to filter the results for dashboards, reports, and events is by specifying a date range for which data is displayed. Although you set date ranges individually on the **Events** page and for each dashboard and report, the process for specifying the date range is the same.

The available date ranges vary, depending on the context (dynamic dashboard, static dashboard, report, or events). Date range customization is not available for the **Health Summary** Dashboard.

1. Click the date range indicator in the top right corner of the **Events** page or a dashboard or report.

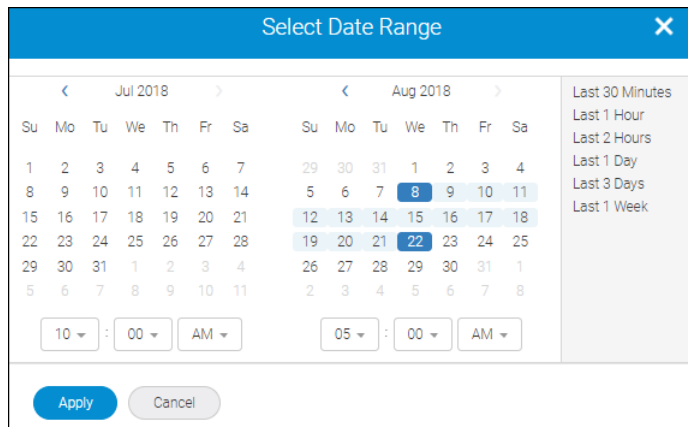


For dynamic dashboards, select the date range from a drop-down list. For static dashboards, reports, and events, the **Select Date Range** dialog displays.

2. Set the time and date range, and click **Apply**.

You can choose from predefined ranges on the right, or you can select start and end dates and times using the calendar. The dialog places no limit on the range selection. Note that the predefined ranges differ, depending on the context of the date range.

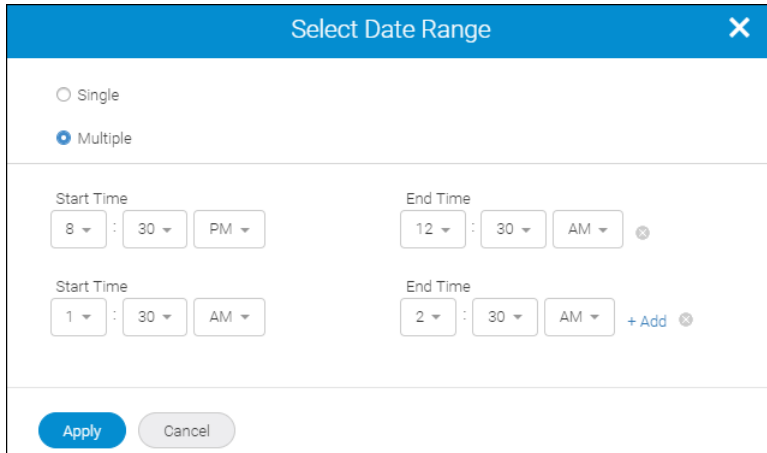
The following example sets the range from Aug 8, 10:00 a.m. to Aug 22, 5:00 a.m.



NOTE

For dashboards, Performance Monitor widgets retain metrics data for only 1 month. If your dashboard contains Performance Monitor widgets, and if you select a date range older than the previous 1 month, the Performance Monitor widgets display data only for the previous month as that is the preservation limit.

3. For reports only, you can specify multiple date ranges by selecting **Multiple** and then specifying up to three start and end times over the previous 24 hours.



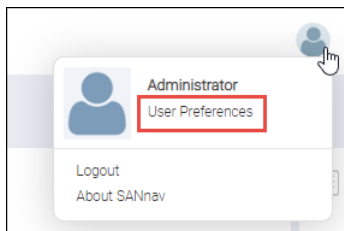
The image shows a 'Select Date Range' dialog box with a blue header and a close button (X) in the top right corner. It contains two radio buttons: 'Single' (unselected) and 'Multiple' (selected). Below the radio buttons are two rows of time selection controls. The first row has a 'Start Time' field with '8', '30', and 'PM' dropdowns, and an 'End Time' field with '12', '30', and 'AM' dropdowns, followed by a small 'x' icon. The second row has a 'Start Time' field with '1', '30', and 'AM' dropdowns, and an 'End Time' field with '2', '30', and 'AM' dropdowns, followed by a '+ Add' button and a small 'x' icon. At the bottom of the dialog are two buttons: 'Apply' (blue) and 'Cancel' (grey).

3.5 Changing Your Password

The first time you log in to SANnav, you should change your password.

After you change your password, you are automatically logged out, and you must log in again using the new password.

1. Click the user icon in the top right corner of the window, and then click **User Preferences**.



2. Click the **Edit** button next to **Logging in**.

Dashboard & Reports Topology Inventory Events Zoning SANnav Q

Preferences

Personal Info

Username Administrator
Phone Number -
Time Zone PDT (America/Los_Angeles)

Logging in

Inactive Logout Time 30 Minutes
Password Last Updated On Mar 29, 2019

Notifications

Email Event Notifications Disable

Tables

FICON Display Disabled
Persist Last Column Selection No

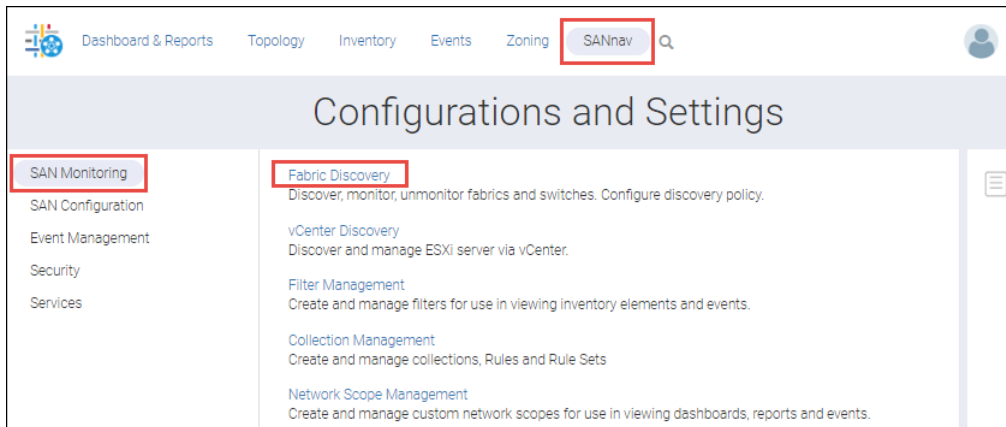
3. Click **Change** on the **Logging in** page.
4. Fill out the **Change Password** fields, and click **OK**.
You are automatically logged out of SANnav.
5. Log in to SANnav again using your new password.

3.6 Initial Setup and Configuration

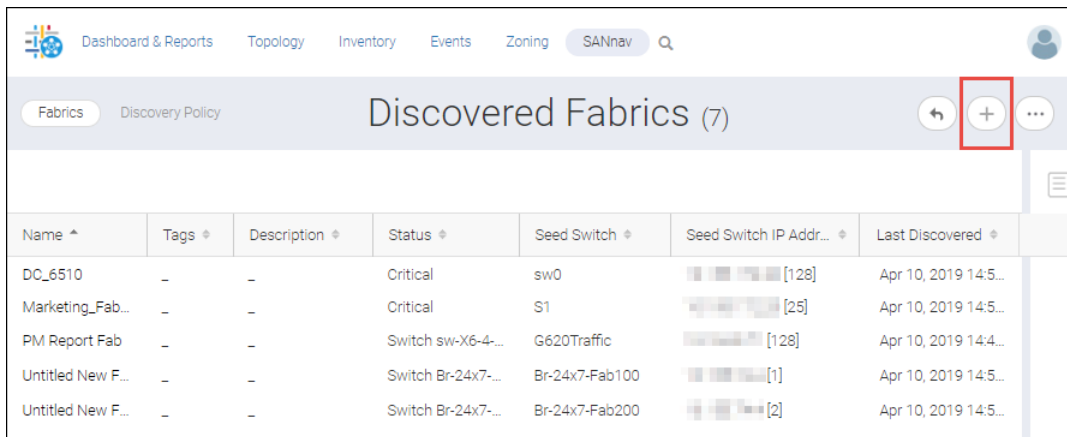
If you are familiar with SAN network management, the brief sections that follow introduce you to several common procedures utilized within SANnav Management Portal. The procedures are described in an introductory manner. Refer to subsequent sections of this guide for detailed information on each.

Discover Fabrics

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



2. Click the **+** button in the top right corner of the page to add a fabric.



For more information on discovery, see [Discovering a Fabric](#).

Configure Service Notifications

To configure service notifications, click **SANnav** in the navigation bar, and then do the following:

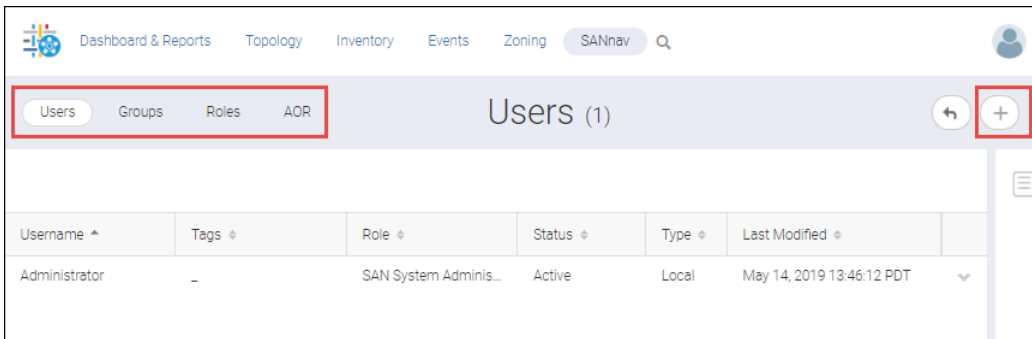
- To configure Call Home, select **Services**, and then click **Call Home Configuration**.
- To configure the SMTP mail server, select **Services**, and then click **SANnav Email Setup**.
- To register the server as a syslog and SNMP trap recipient, select **Event Management**, and then click **Syslog and SNMP Registration**.
- To forward SNMP traps and syslog messages, select **Event Management**, and then click **Event Forwarding**.
 - First click **Credentials** in the subnavigation bar to add trap forwarding credentials.
 - Then click **Destinations** in the subnavigation bar, and click the **+** button in the top right corner of the page to add a forwarding destination.

For more information on service notifications, see [Call Home and ESRS](#) and [Event Management](#).

Set Up User Accounts

To configure user accounts, click **SANnav** in the navigation bar, and then select **Security** > **SANnav User Management**.

To add users, roles, and AORs, click the appropriate link in the subnavigation bar, and then click the + button to add the entities.



The **Groups** link is for assigning roles and AORs to LDAP groups.

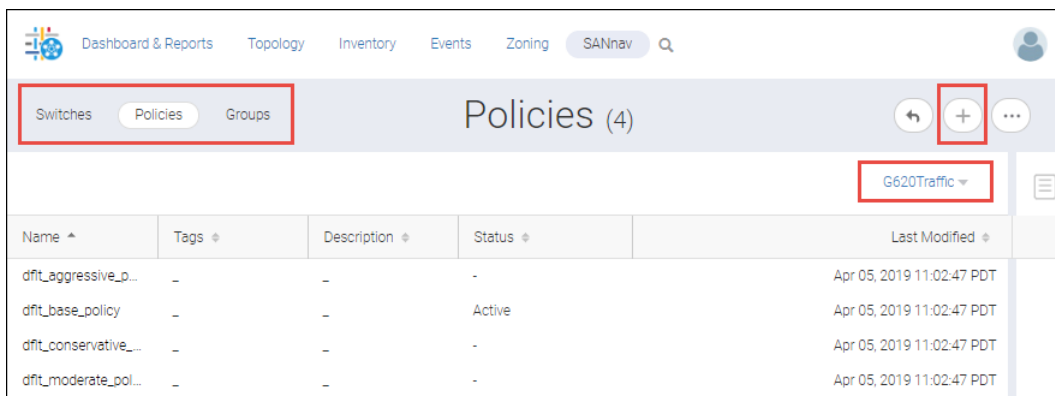
To set up external authentication, click **SANnav** in the navigation bar, and then select **Security > SANnav Authentication and Authorization**.

For more information on setting up user accounts, see [Security](#).

Configure MAPS Policies

To configure Monitoring and Alerting Policy Suite (MAPS) policies, do the following:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > MAPS Policy Management**.
2. Click **Policies** in the subnavigation bar, select a switch from the drop-down list on the right side of the page, and then click the + button.



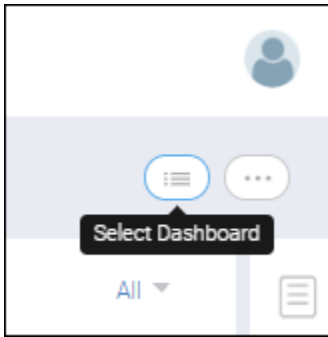
You can create a new policy or you can import policies from a json or xml file. For example, you can import MAPS policies that were exported from Brocade Network Advisor.

For more information on MAPS policies, see [Monitoring and Alerting Policy Suite](#).

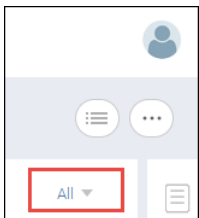
Create Custom Dashboards

Click **Dashboard & Reports** in the navigation bar. The **Health Summary** dashboard with a network scope of **All** is the default dashboard.

To display a different dashboard, click the **Select Dashboard** button in the top right corner of the page.



To change the network scope of the dashboard, click the drop-down arrow on the right side of the filter bar.



To create a custom dashboard, click **Templates** in the subnavigation bar, and then click the **+** button in the top right corner of the page. For more information, see [Dashboards](#).

Licensing

4.1 SANnav Licensing Overview

When you install SANnav Management Portal or SANnav Global View, you have a 90-day trial period, during which you can use SANnav for free, without a license. To use either SANnav product beyond the trial period, you must purchase a software license.

NOTE

The 90-day trial period is activated automatically and starts from the time you install the SANnav product.

SANnav Management Portal and SANnav Global View require separate license keys and are completely 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, together with the transaction key, are used to generate a SANnav license. The license is locked to that server UID and SANnav instance.

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 need to move a license from one SANnav instance to another, such as 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.

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 key. Before your license expires, you should renew the license to ensure uninterrupted service. By default, SANnav is configured to automatically retrieve and activate renewed licenses.

4.1.1 SANnav Licensing Terminology

The following terms are used in this document:

- **License key** – A key that enables you to use a particular SANnav instance. A license key has an expiration date after which you can no longer use SANnav unless you renew the license. The license key 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 virtual machine (VM) to another or when the MAC address of the server changes. The rehost key is generated by SANnav when you release the current license.
- **Server unique ID (UID)** – A unique ID that identifies the physical server and VM on which SANnav is installed. The server UID is used in conjunction 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.
- **Transaction key** – A unique key, along with the server UID, 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.

4.1.2 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.
- The Enterprise license enables management of up to 15,000 ports and can be used to manage fixed-port switches and directors.

During the 90-day trial period, SANnav Management Portal has the same functionality as the Enterprise license except that SANnav server backup and restore is not supported.

SANnav Global View supports only a single license type (Global).

4.1.3 Managed Port Count

SANnav Management Portal audits and verifies the managed port count against the maximum limit for your license. You start receiving warning messages when the managed port count reaches 90% of the supported port count limit.

Table 11: Supported Port Count and Warning Threshold Count Limits

License Type	Supported Port Count	90% Threshold
Base license	600 ports	540 ports
Enterprise license	15,000 ports	13,500 ports

You can find the current managed port count in the **Licensing** page of the SANnav Management Portal user interface.

SANnav Management Portal provides a grace port count limit, which allows you to continue to manage your fabrics with existing licenses, even when the managed port count exceeds the maximum supported limit for your license. The grace port count allows you the opportunity to either reduce the number of ports managed by the SANnav Management Portal instance below the limit or, in the case of the Base license, purchase and install the Enterprise license.

NOTE

The grace port count limit is not the same as the *supported* port count limit.

If the managed port count exceeds the grace port count limit of a given license, SANnav automatically directs you to the **Licensing** page, where you can manage the switches or fabrics to stay within the grace port count limit. You continue to be redirected to the licensing page and are not allowed to access any other feature or function until the managed port count is brought within the grace port count limit.

Following is the list of ports included in the managed port count calculation:

- Licensed switch ports
- Licensed AG ports

The following ports are excluded from the managed port count calculation:

- Unlicensed ports (ports not licensed under a Ports on Demand [POD] license)
- ICL ports
- Logical ports
- Unmonitored ports in fabrics or switches
- Unmanaged or unreachable ports in switches
- Ports on switches that are missing from the fabric

SANnav Global View does not have a managed port count limit.

4.2 How SANnav Licensing Works

Through a combination of the server unique ID (UID) and the transaction key, you can generate a license key to activate the SANnav license.

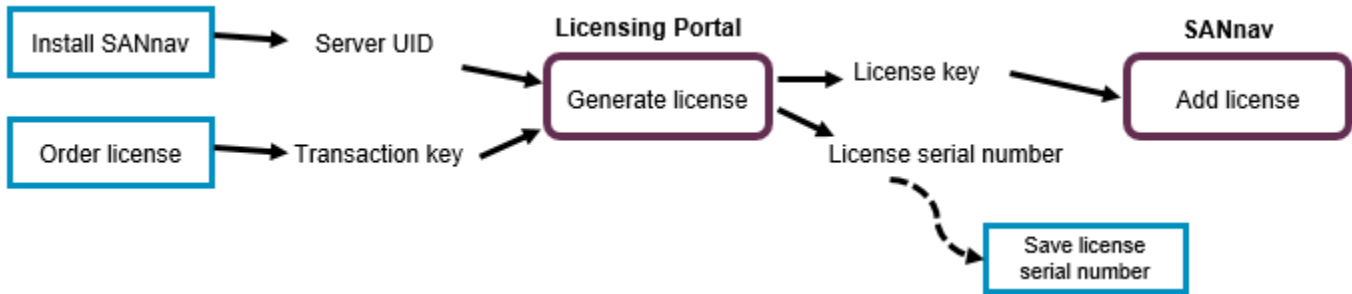
When you install SANnav on a server or virtual machine (VM), a server UID is generated. You can view this server UID and copy it from the **SANnav Licensing** page.

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

After you obtain the license key, add it in SANnav, and activate the license.

This flow is illustrated in the following diagram.

Figure 7: Generating a License



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** page of the SANnav user interface.

Rehosting a License

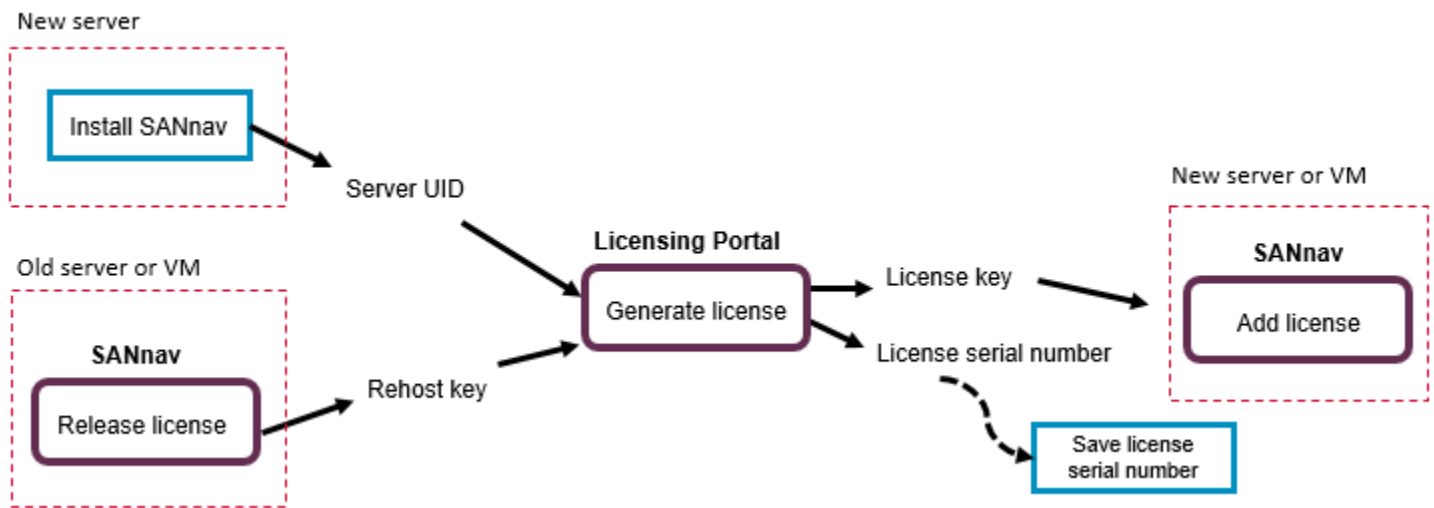
If you want to move SANnav to a different server or VM, you do not need to purchase a new license. But because licenses are locked to the server UID, you do need to obtain a new license key for the new SANnav instance.

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, 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.

You must also use the rehosting process if the MAC address of the server changes for any reason.

The following diagram illustrates the rehosting flow.

Figure 8: Rehosting a License



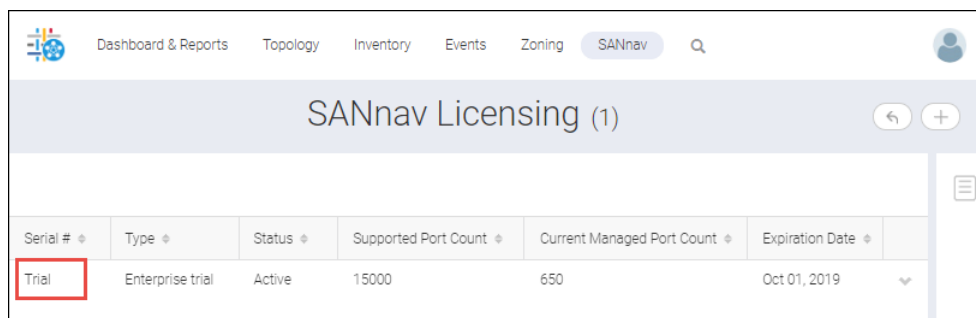
The released license expires on the prior SANnav instance after 30 days from the time of release or on the original expiration date, whichever comes first. This 30-day period allows you to continue using the existing instance while you bring up the SANnav software on a new server or VM and validate whether the new server or VM is working prior to decommissioning the existing SANnav instance.

4.3 Obtaining the Server UID

During installation, SANnav generates a server unique ID (UID), which you need to generate a license. You can obtain the server UID from the **SANnav Licensing** page.

1. Click **SANnav** in the navigation bar, and then select **Services > SANnav Licensing**.
2. Click the license for which you want to obtain the server UID.

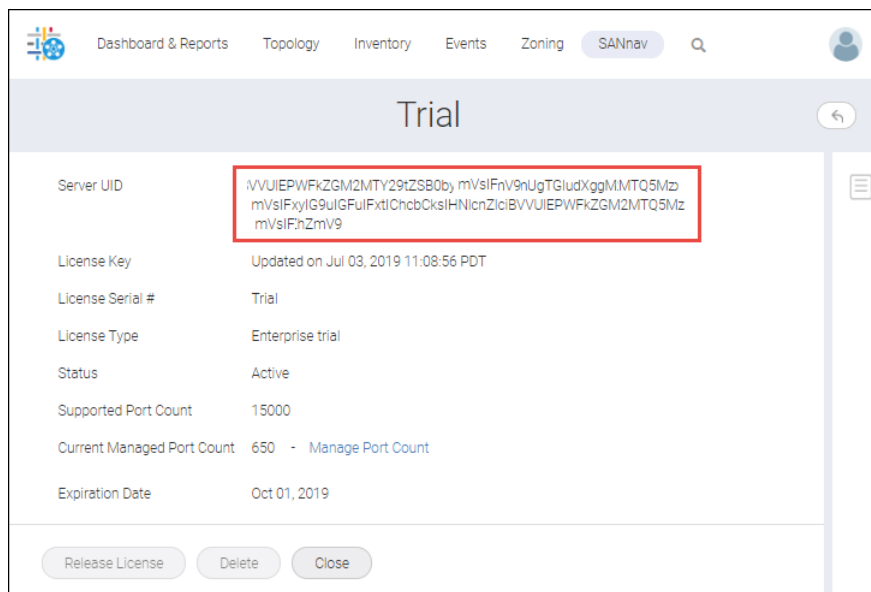
When you first install SANnav, only one license displays, so click **Trial**.



The screenshot shows the SANnav Licensing page with a table of licenses. The 'Trial' license is highlighted with a red box.

Serial #	Type	Status	Supported Port Count	Current Managed Port Count	Expiration Date
Trial	Enterprise trial	Active	15000	650	Oct 01, 2019

3. Copy the server UID so you can paste it later.



The screenshot shows the details of the Trial license. The Server UID is highlighted with a red box.

Server UID	<code>mVUIEPWFkZGM2MTY29tZSB0by mVslFrv9nUgTGludXggMMTQ5Mz mVslFxyIG9uIGFuLFxtlChcbCksIHnIcnZlciBVVUIEPWFkZGM2MTQ5Mz mVslFhZmV9</code>
License Key	Updated on Jul 03, 2019 11:08:56 PDT
License Serial #	Trial
License Type	Enterprise trial
Status	Active
Supported Port Count	15000
Current Managed Port Count	650 - Manage Port Count
Expiration Date	Oct 01, 2019

Buttons: Release License, Delete, Close

The next step is to access the Broadcom licensing portal, where you use the server UID to generate a license key.

4.4 Generating a License

Access the Broadcom licensing portal to generate a SANnav license key.

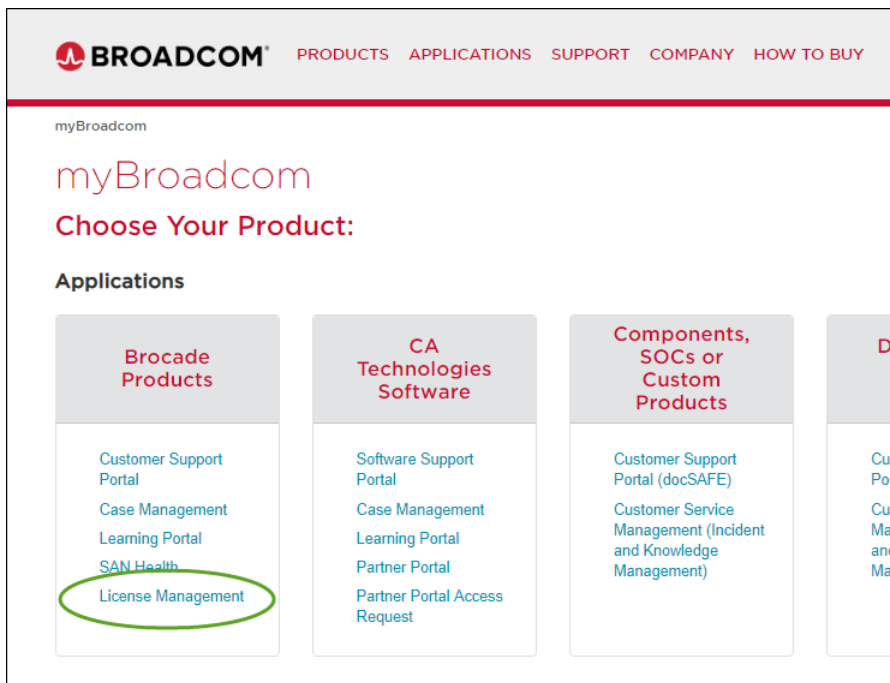
Before you generate the license, make sure that you have a server unique ID (UID). After you install SANnav, you can obtain the server UID from the **SANnav Licensing** page.

Use the following procedure to generate and obtain a SANnav license key.

1. Obtain a transaction key from your SANnav vendor.

You will receive an email with the license transaction key in the form of an electronic transaction key. 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.

2. Log in to the Broadcom licensing portal (<http://portal.broadcom.com>), and complete the software license request. If you do not have a login ID and password, request access by following the online registration instructions.
3. Click **License Management** in the **Brocade Products** section.



4. Enter the licensing transaction key or rehost key in the **License Generation** window and click **Next**.

The screenshot shows the 'License Generation' window with a progress bar at the top containing three steps: 'Identify' (highlighted in blue), 'Information', and 'Results'. Below the progress bar, the text reads 'License Generation' and 'Please proceed for license generation with Transaction Key or Re-Host Key. Read [Input Guidelines](#)'. A text input field contains the placeholder 'Transaction Key or Re-Host Key' and a link 'Add more Transaction Key(s)'. At the bottom right, there are 'Next' and 'Cancel' buttons.

5. Enter the server UID that you obtained from SANnav in the **Product Information** area.

The screenshot shows the 'License Generation' window with the progress bar updated: 'Identify' and 'Results' are greyed out, while 'Information' is highlighted in blue. A license key 'BR-SSMPB1Y-01' with its full alphanumeric string is displayed, along with a 'Remove' button. The 'Customer Information*' section has a text field with 'user@mail.com' and a 'Show More' link. The 'Product Information*' section has a text field for 'Server UID' with a red warning: 'If possible, use copy and paste to enter the Server unique identifier (UID) value to avoid key stroke errors.' At the bottom, there is a checkbox for 'I have read and accept the [Broadcom End User License Agreement](#)', and 'Generate' and 'Cancel' buttons.

6. Read the Broadcom End User License Agreement, and if you agree to the terms, select the **I have read and accept** check box.

7. Click **Generate**.

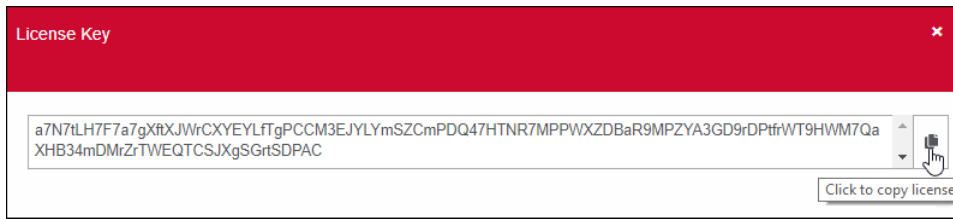
The **Results** window displays an order summary and the results of the license request.

- 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 be taken are displayed on the page.

8. Click the hyperlink in the **License** field to display the license key.

9. Copy the license key to a .txt file and save it.

You will use this license key when you add the license to SANnav.



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

Next, you must add the license to SANnav.

4.5 Adding a License to SANnav

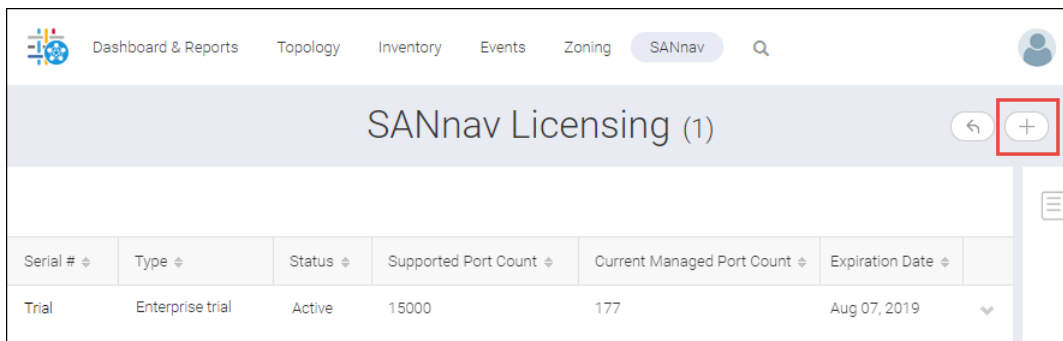
After you obtain a license key from the Broadcom licensing portal, you must add the license key to SANnav to activate the license.

Before you start, make sure that you have copied the license key that was generated from the Broadcom licensing portal. The license key must be the key that was generated for this instance of SANnav (using the server UID of this instance).

NOTE

When you activate a new license, the current license is deactivated, but the expiration date of the current license remains the same. For example, if you install a 1-year Base license and 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).

1. Click **SANnav** in the navigation bar, and then select **Services > SANnav Licensing** to view the license list.
2. Click the **+** button at the top right corner of the **SANnav Licensing** page.



3. Copy and paste the license key that you obtained from the Broadcom licensing portal into the **Add New License** dialog, and click **OK**.

Add New License
✕

Server UID
e09TIE5hbWU9V2VsY29tZS80byBBbHBpbmVsIFxylG9uIGFulFxtlChc
mVsIFxylG9uIGFulFxtlChcbCkslHnlonZlclBVVUEPWFhYzRlNjA4YWEy
e09TIE5hb9

Enter License Key

a7N7lLH7F7a7gXftXJWrCXEYELFTgPCOM3EJYLYmsZCmPDQ47HT
NR7MPWPWXZDBaR9MPZYA3GD9rDPftrWT9HWM7QaXHB34mDMrZr
TWEQTCSJXgSGrtSDPAC

OK
Cancel

The new license is added to the **SANnav Licensing** page.

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

Dashboard & Reports
Topology
Inventory
Events
Zoning
SANnav
Q

👤

SANnav Licensing (1)

↶
+

Serial #	Type	Status	Supported Port Count	Current Managed Port Count	Expiration Date	
LOCAL000001	Base	Inactive	600	411	Aug 28, 2018	
Trial	Enterprise trial	Active	15000	411	Nov 15, 20	<div style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 5px; display: inline-block;"> View </div>

5. Click the **Activate** button to activate the license.

LOCAL000001	
Server UID	e09TIE5hbWU9V2VsY29tZSB0byBBbHBpbmUgTGluXGgMy43S2Vyb mVslFXYlG9uIGFuIFxtlChcbOksIHlNlcnZlciBVVUUEPTlJmJQ5ZTk0NmU3 YzFKYmR9
License Key	Updated on Jul 05, 2018 14:59:55 IST
License Serial #	LOCAL000001
License Type	Base
Status	Inactive - Activate
Supported Port Count	600
Current Managed Port Count	72 - Manage Port Count
Expiration Date	Aug 04, 2018 15:00:12 IST
Release License Delete Close	

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

- Click **Close** to return to the **SANnav Licensing** page.

4.6 Managing the Port Count

If the number of monitored ports gets close to or exceeds the port count limit for your license, you can change which ports are monitored to bring the port count within the licensed limit.

The license details page displays the current managed port count.

NOTE

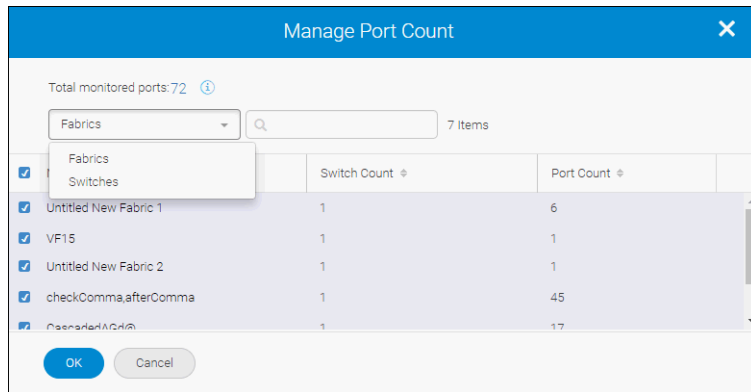
The managed port count does not apply to SANnav Global View.

- Click **SANnav** in the navigation bar, and then select **Services** > **SANnav Licensing** to view the license list.
- Click the down arrow at the right of a license row, and then click **View** to display the license details page.
- Click the **Manage Port Count** link to change the total number of monitored ports.
- Clear the checkbox for the switches and fabrics that you want to unmonitor.

The **Total monitored ports** field displays the number of ports being monitored. This number updates dynamically as you select or unselect switches and fabrics.

NOTE

You cannot unmonitor seed switches individually. The check box next to the seed switch is grayed out. If you unmonitor a fabric, all switches in that fabric, including the seed switch, become unmonitored.



4.7 Renewing a License

Starting 90 days prior to the expiration date, when you log in to SANnav, a popup message alerts you that your license is about to expire and prompts you to renew the license. If configured to do so, SANnav can automatically apply the renewed license.

When you purchase a renewal license, the license key is sent in an email and the Broadcom license portal is updated with the new license key. The serial number of the new license must match the serial number of the existing license.

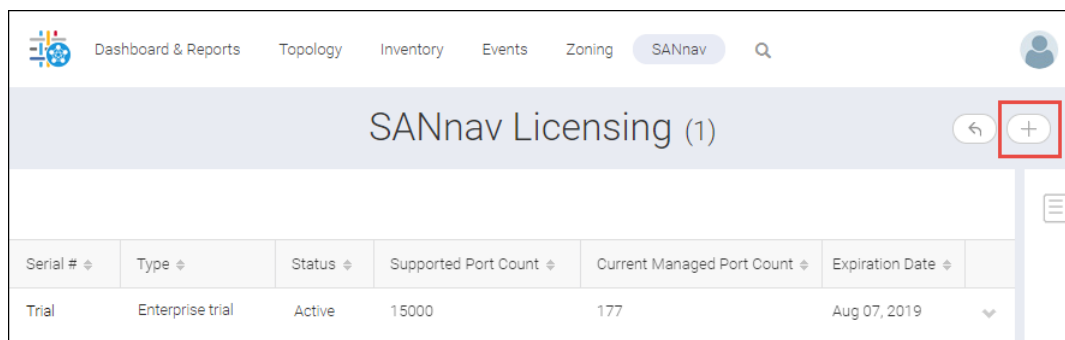
Starting 90 days prior to the license expiration date, in addition to sending alerts, SANnav also starts checking the Broadcom license portal for a new license key. If a new license key is found, SANnav automatically retrieves it from the licensing portal and activates it.

NOTE

When the new license is applied, all logged-in users are automatically logged out and must log in again.

If SANnav is not configured to automatically retrieve and activate renewal licenses, you must manually apply the license using the following steps.

1. Obtain a license key from your SANnav vendor.
You will receive the license key in an email.
2. Log in to SANnav.
3. Click **SANnav** in the navigation bar, and then select **Services > SANnav Licensing** to view the license list.
4. Click the **+** button at the top right corner of the **SANnav Licensing** page.



5. Copy and paste the license key that you received in the email into the **Add New License** dialog, and click **OK**.

The license is automatically activated, and your session is logged out. You must log in again to use the SANnav application.

4.8 Moving a License to a Different Server: Planned Migration

If you want to move SANnav from one server or VM to another, 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.

NOTE

Before you move SANnav, you should take a backup. After the migration, you can restore the backup on the new server or VM.

The license rehosting process is used in the following circumstances:

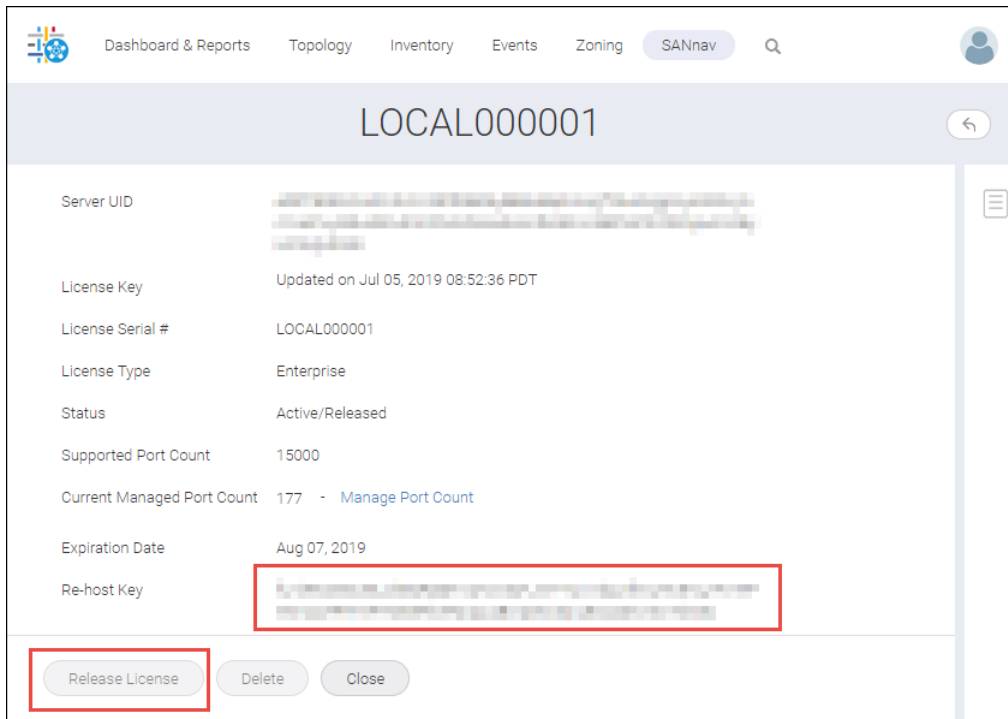
- If you want to migrate SANnav from one server or VM to another
- If the MAC address of the server in which SANnav is installed changes for any reason

To rehost the license, you must release the current license, get a rehost key, and get a new server unique ID (UID).

When you release the license, you have 30 days before the license expires on the current server or VM. This 30-day period gives you time to install SANnav on the new server or VM and to validate that the new server or VM is working. Note that if the original license expiration date is within 30 days of when you release it, then the license expires on the original expiration date.

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 the license row, and then click **View** to display the license details page.
3. Click the **Release License** button to release the license on the current server or VM.
You can release both active licenses and inactive (licenses not yet active) licenses.

SANnav displays a rehost key.



4. Copy the rehost key for later use when generating the new SANnav license on the Broadcom licensing portal.
5. Install SANnav on the new server or VM and obtain the server UID.
6. Using the rehost key and the server UID from the new server or VM, generate a new license on the Broadcom licensing portal.

4.9 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 cannot get a rehost key. Instead, you must contact Technical Support to get a replacement license key.

1. Locate the license serial number for the original license.
2. Install SANnav on a new server and obtain the server unique ID (UID).
3. Contact Technical Support and provide the license serial number and server UID to request a replacement license key.

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

4.10 Deleting a License

You can delete inactive, expired, and released SANnav licenses.

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 page.
3. Click the **Delete** button to delete the license.

Security

5.1 User Management

Access to SANnav Management Portal is controlled by authentication and authorization of users. *Authentication* is the process of validating user names and passwords. *Authorization* is the process of validating the roles 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 LDAP, RADIUS, or TACACS+).

User management involves the following general steps:

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. This password policy is applicable for SANnav users only when you select primary authentication as the local data base.
2. Creating roles.
You can create custom roles to use, in addition to the preconfigured roles provided by SANnav. If you create custom roles, you should do so before setting up the user accounts, because you assign roles at the same time you create the accounts.
3. Creating AORs.
You can create custom AORs to use, in addition to the preconfigured AOR (**All Fabrics**) provided by SANnav. If you create custom AORs, you should do so before setting up the user accounts, because you assign AORs at the same time you create the accounts.
4. Setting up user accounts.
When you create a user account, you assign specific roles and AORs to that account.

User Accounts

SANnav user accounts contain the identification of the SANnav user, as well as roles and AORs assigned to the user.

SANnav user accounts are completely independent of switch user accounts. SANnav user accounts are used to access SANnav features based on roles and AORs. Switch user accounts are used to log in to individual SAN switches.

User accounts must be assigned at least one role and at least one AOR.

If you are using an external server for authentication and authorization, you might not need to create user accounts on the SANnav server.

NOTE

At least one user account with User Management privilege must always be defined on the SANnav server. You cannot delete this last user account.

NOTE

If a user account does not have at least one role and one AOR, the account becomes inactive. This can happen, for example, if you assign a custom role or AOR to a user account and you later delete that role or AOR.

Roles

A *role* is a group of privileges and access levels that determine the features that a SANnav user can view and modify. Each privilege can have either a Read-Only or Read-Write access level.

You do not assign individual privileges to a user. You assign privileges to a role, and then assign the role to a user. When a user logs into SANnav, the user sees only the options that correspond to the user's privileges.

For example, if you want to create and manage user accounts, you must be assigned a role with the User Management privilege in Read-Write access mode.

SANnav provides several preconfigured roles, as outlined in the following table.

Table 12: Preconfigured Roles

Role Name	Duties	Description
Operator	General switch administration	Routine switch maintenance functions, such as managing configuration policies, scheduling server backup, or configuring Call Home.
SAN System Administrator	All administration	All administrative functions.
Security Administrator	Security administration - switches	Configuration policy and dashboard management.
Security Officer	Security administration - users	Configuration policy and dashboard management, as well as all user management functions.
Zone Administrator	Zone administration	Configuration policy and dashboard management, as well as all zone management functions.

You can create additional custom roles. For example, if you want a user to be able to monitor fabric performance, but not make any changes, you can create a role with read-only access for all privileges.

If you are using an external server for authentication and authorization, you still must create roles in SANnav. The roles are then assigned to users on the external server. This process is described in detail later in this chapter.

You should create custom roles before you create user accounts, because you assign roles at the time you create the accounts. If you delete a role, any logged-in users that are assigned this role are automatically logged out.

Areas of Responsibility

An *area of responsibility* (AOR) is a collection of selected *fabrics* that a SANnav user is allowed to manage. When you create a user account, you assign one or more AORs to that account. The user can view and manage only the fabrics in the assigned AORs.

For example, assume you create an AOR called "HR Fabrics", which includes Fabric1 and Fabric2, and then assign the "HR Fabrics" AOR to UserA. When using SANnav, UserA can create configurations, generate reports, and perform backups only to fabrics in the AOR "HR Fabrics". UserA cannot view or configure Fabric3, because Fabric3 is not in the assigned AOR.

NOTE

The level of granularity for a given AOR is a fabric. Switches within a fabric cannot be assigned individually to an AOR.

The **All Fabrics** AOR is automatically created in SANnav. The **All Fabrics** AOR allows users access to all fabrics that are discovered by SANnav. You must explicitly create additional AORs if you want to limit user access to a subset of the fabrics.

If you are using an external server for authentication and authorization, you still must create AORs in SANnav. The AORs are then assigned to users on the external server. This process is described in detail later in this chapter.

You should create AORs before you create user accounts, because you assign AORs at the time you create the accounts. If you delete an AOR, any logged-in users that are assigned this AOR are automatically logged out.

5.1.1 Configuring Password, Lockout, and Session Policies

Having a strong password policy is a key component for secure access to SANnav. The strength of your password should depend on the security needs of your organization.

To configure the password policy, you must have User Management privilege with read-write permission.

When you set up password policies in SANnav, these policies apply only to the local database. If you are using an external server for authentication, these policies do not apply, and you must set up password policies on the external server. If primary authentication on the external server fails, and you fall back to secondary authentication on the local database, then the password policies defined in SANnav apply.

If you change the password policy so that the passwords of logged-in users are now in violation of the new policy, the users remain logged in, but the next time they try to log in, they get a password violation message and are prompted to change their password.

The following steps provide a guideline for creating a strong password policy. Your policy may vary.

1. Click **SANnav** in the navigation bar, and then select **Security > SANnav Password and Lockout Policy**.
2. Configure the password strength policy, as follows.

Option	Description
Minimum Length	The default minimum length is 8 characters. Longer passwords increase security dramatically. Select a minimum length of 9 or 10 characters for a stronger password policy.
Uppercase Letters, Lowercase Letters, Numbers, and Special Characters	This is the minimum number of upper- and lowercase letters, numbers, and special characters required in the password. The default value for each of these options is 0. For strong passwords, you should set each of these options to at least 1.
Maximum Repeat	Maximum Repeat specifies the maximum number of repeated characters that are allowed. For example, if Maximum Repeat is 2, then "password" is valid, but "passsword" is not. Select a value or use the default value (2).
Maximum Sequence	Maximum Sequence specifies the maximum number of sequential characters that are allowed. The sequence is based on the ASCII value of the characters and also applies to special characters. For example, if Maximum Sequence is 1, then "password1" is valid, but "password12" is not, and "passworda" is valid, but "passworde" is not (sequence "de" violates the policy). Select a value or use the default value (1). Note that if you use the default value, some common two-letter sequences (such as "hi", "st", and "no") will be disallowed in passwords.

3. Configure the password expiration and password history policies.

Option	Description
Password never expires	By default, passwords never expire. If your password policy enforces strong passwords, you might not want the passwords to expire unless security is compromised. Uncheck this box if you want passwords to automatically expire after a specific time period.
Password Age	The amount of time after which a password automatically expires. This value is between 15 days (default) and 12 months. For the most security, choose shorter values. A good value is between 45 days and 6 months.
Warning Period	The number of days prior to password expiration that a user starts getting warning messages. Select a value from 1 (default) to 15 days.

Option	Description
Password History	The number of previous passwords that cannot be reused. For example, if Password History is 5, users cannot reuse their most recent 5 passwords. Select a value between 1 (default) and 5. For the most security, select 5.

- Configure the account lockout and session policy.

Option	Description
Lockout After	By default, a user account is locked after three failed login attempts. You can change this to 4 or 5 failed login attempts. For the most security, keep the default (3).
Lockout Duration	A locked account automatically unlocks after the amount of time specified by Lockout Duration . Lockout duration is between 15 (default) and 60 minutes. Keep in mind that when setting the lockout duration, the higher settings might result in increased support calls, whereas lower settings make SANnav more vulnerable to brute force attacks. For higher levels of security, select the higher settings.
Inactive Duration	By default, you are logged out after 30 minutes of inactivity. You set this value to between 15 minutes and 12 hours. If you select Keep Dashboard active after session expires , then if you are on the dashboard page and the session expires, you are not logged out. You can continue to view the dashboard, which is dynamically updated. If you move off of the dashboard page, however, you are logged out and must log in again.

- Click **Save**.

5.1.2 Creating Custom Roles

You can create custom roles if you want to use roles other than the predefined ones.

To create roles, you must have User Management privilege with read-write permission.

The following task shows how to create a custom role with read-only permission for all privileges.

- Click **SANnav** in the navigation bar, and then select **Security > SANnav User Management**.
- Click **Roles**, then click the **+** button in the subnavigation bar.
- Give the role a name.
For this example, the name is **AllPrivileges_ReadOnly**.
- Optionally add a description to help you identify the role, and one or more tags to help you find the role in a search.
- Select the privileges and corresponding access level you want to assign to the role. Scroll down to see additional privileges.
For this example, check the box next to **Name** to select all privileges. By default, the **Read** access level is selected for all privileges, so for this example, you do not need to change the access levels.

NOTE

The user is granted only the privileges selected, regardless of the access level. If you change the access level to **Read & Write**, but do not select the privilege, the user is not granted the privilege.

The screenshot shows the 'Create New Role' interface in the SANnav management portal. The 'Roles' tab is active. The form fields are as follows:

- Name:** AllPrivileges_ReadOnly
- Description:** Access to all features, but with read-only privileges.
- Tags:** read-only,all-privileges

Below the form is a table of privileges with 33 items. The table has two columns: 'Name' and 'Access Level'. The 'Name' column has a checkbox for each item, and the 'Access Level' column has radio buttons for 'Read' and 'Read & Write'.

Name	Access Level
<input checked="" type="checkbox"/> Call Home	<input checked="" type="radio"/> Read <input type="radio"/> Read & Write
<input checked="" type="checkbox"/> Collection Management	<input checked="" type="radio"/> Read <input type="radio"/> Read & Write
<input checked="" type="checkbox"/> Configuration File Manager	<input checked="" type="radio"/> Read <input type="radio"/> Read & Write
<input checked="" type="checkbox"/> Configuration Policy Manager	<input checked="" type="radio"/> Read <input type="radio"/> Read & Write
<input checked="" type="checkbox"/> Custom Fields – Add/Edit/Delete	<input checked="" type="radio"/> Read <input type="radio"/> Read & Write

At the bottom of the form, there are two buttons: 'Save' and 'Cancel'. The 'Save' button is highlighted with a red box.

6. Click **Save**.

You can now assign this custom role to user accounts.

5.1.3 Creating Custom AORs

You can create custom areas of responsibility (AORs) if you want to use AORs other than the predefined one, which is **All Fabrics**. An AOR defines the fabrics that a user is allowed to manage.

To create AORs, you must have User Management privilege with read-write permission.

The following task shows how to create an AOR of all fabrics located in Europe.

1. Click **SANnav** in the navigation bar, and then select **Security > SANnav User Management**.
2. Click **AOR**, then click the **+** button in the subnavigation bar.
3. Give the AOR a name.
For this example, the name is **Europe Fabrics**.
4. Optionally add a description to help you identify the AOR, and one or more tags to help you find the AOR in a search.
5. Click **Add** to select the fabrics you want to assign to the AOR.

You can assign only fabrics to an AOR. You cannot assign individual switches.

The screenshot shows the 'Create New AOR' interface in the SANnav management portal. The navigation bar at the top includes 'Dashboard & Reports', 'Topology', 'Inventory', 'Events', 'Zoning', and 'SANnav'. The subnavigation bar has 'Users', 'Groups', 'Roles', and 'AOR' (highlighted with a red box). The main form contains:

- Name:** Europe Fabrics (highlighted with a red box)
- Description:** All fabrics located in Europe.
- Tags:** Europe

Below the form is a 'Members' section with a search bar and '3 Items'. The table lists the following members:

Name	Tags	
<input type="checkbox"/> DC_6510	-	▼
<input type="checkbox"/> TC G610	-	▼
<input type="checkbox"/> TC X6-4	-	▼

There are 'Add' and 'Remove' buttons to the right of the table. At the bottom of the form, there are 'Save' and 'Cancel' buttons (both highlighted with red boxes).

6. Click **Save**.

You can now assign this custom AOR to user accounts.

5.1.4 Creating a User Account

This example explains how to set up a user account on the local database. In this example, the user is assigned a custom role with read-only access for all features.

To create a user account, you must have User Management privilege with read-write permission.

If you want to assign custom roles and AORs, they should be created before you create the user account.

1. Click **SANnav** in the navigation bar, and then select **Security > SANnav User Management**.
2. Click **Users**, and then click the **+** button in the subnavigation bar.

3. Fill out the standard user form.

The user name must be from 1 to 63 alphanumeric characters and can contain the following special characters:

. \ _ - ! @ # \$ % ^

4. In the **Roles** section, select one or more roles to assign to the user account.
For this example, select the read-only custom role that you created previously.
5. In the **AORs** section, select the fabrics that you want the user to view and access.
In this example, the default AOR, **All Fabrics**, is selected.

Dashboard & Reports Topology Inventory Events Zoning SANnav

Users Groups Roles AOR Create New User

Username: pam Tags: Trainee

Password: Description: User who can monitor the fabrics but not make any changes.

Confirm Password:

Email: pam@mail.com

Phone Number: 555-1234

6 Items Roles

Name	Tags	Description
<input type="checkbox"/> Zone Administrator	-	Zone Administrator Role
<input type="checkbox"/> Operator	-	Operator Role
<input type="checkbox"/> Security Officer	-	Security Officer Role
<input checked="" type="checkbox"/> AllPrivileges_ReadOnly	read-only,all-privileges	Access to all features, but ...

2 Items AORs

Name	Tags
<input checked="" type="checkbox"/> All Fabrics	-
<input type="checkbox"/> Europe Fabrics	Europe

Activate

Save Cancel

6. Click **Save**.

For this example, the user account is created with the **AllPrivileges_ReadOnly** role and the **All Fabrics** AOR. Note that by default, the account is activated.

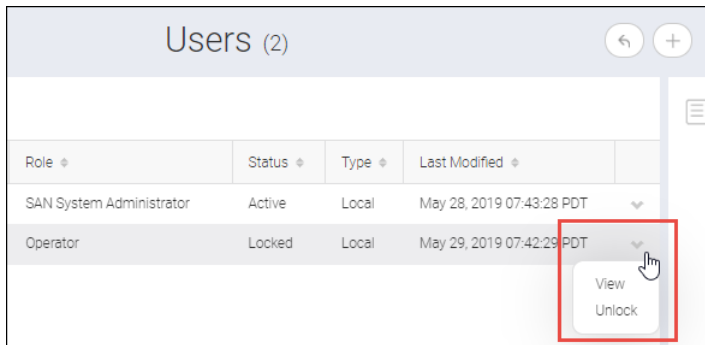
5.2 Unlocking a User Account

If a user account is locked due to excessive failed login attempts, you can manually unlock the account for the user. If the account is not manually unlocked, the user must wait until the lockout duration elapses.

To unlock a user account, you must have User Management privilege with read-write permission.

1. Click **SANnav** in the navigation bar, and then select **Security > SANnav User Management**.

2. Locate the locked user (Status = Locked), click the down arrow at the right of the row, and select **Unlock**.



The status changes to Active and the user can now try to log in again.

5.3 SANnav Management Portal User Account Privileges

The privileges your user account has determine the actions you can perform in SANnav Management Portal. Privileges are assigned to roles, which are assigned to user accounts.

The following table lists all the privileges a role can have, and summarizes what you can do if you have a privilege with read/write access. The table also shows what privileges each of the pre-configured roles has.

In the table, **R** means Read-Only access, and **RW** means Read-Write access.

Privilege	Description for RW Access	Preconfigured Roles				
		Operator	SAN System Admin	Security Admin	Security Officer	Zone Admin
Call Home	Configure Call Home centers.	RW	RW	—	—	—
Collection Management	Manage flow collection and custom rule sets. Must also have Flow Management privilege.	R	RW	—	RW	—
Configuration File Manager	Backup and restore configurations, schedule backups. With Read-only access, you can back up the configuration, but cannot schedule backups.	R	RW	—	—	—
Configuration Policy Manager	Create configuration policies, monitor and resolve configuration drifts.	RW	RW	RW	RW	RW
Custom Fields - Add/Edit/Delete	Create, edit, and delete custom fields for the Inventory page.	R	RW	—	—	—
Dashboard	View and create content for dashboards.	RW	RW	RW	RW	RW
Discover Setup	Discover fabrics, monitor and stop monitoring switches, configure SNMP settings for switches, turn tracking on and off for individual fabrics, delete fabrics.	R	RW	—	—	—
Element Manager - Product Administration	Disable and enable switches, manage switch SupportSaves, import names, schedule high-granularity data collection, open Web Tools to manage a switch, configure backbone fabrics.	—	RW	—	—	—

Privilege	Description for RW Access	Preconfigured Roles				
		Operator	SAN System Admin	Security Admin	Security Officer	Zone Admin
Element Manager - Product Maintenance	Not used.	—	RW	—	—	—
Element Manager - Product Operation	Not used.	RW	RW	—	—	—
Event Management	Define rules with event triggers and actions, SNMP and syslog registration, forwarding, SNMP informs, trap configuration.	R	RW	—	—	—
Extension Tunnel Management	Configure and manage FCIP and IP Extension tunnels, configure IPsec policy.	R	RW	—	—	—
Fabric Configuration	Not used.	R	RW	—	—	—
Fabric Tracking	Configure discovery policy. Must also have Discover Setup permission with either R or RW access.	R	RW	—	—	—
FICON Management	For future use.	R	RW	—	—	—
Firmware Management	Download firmware to selected switches and manage the firmware repository.	R	RW	—	—	—
Flow Management	Monitor and manage flows. Manage flow collection and custom rule sets (must also have Collection Management privilege).	R	RW	—	—	—
Health Score Configuration	Configure rules for computing the health score of fabrics, switches, hosts, and storage.	—	RW	—	—	—
License Update	Update the SANnav license and manage port count.	R	RW	—	—	—
Logical Switch Configuration	Configure and manage logical fabrics and logical switches.	—	RW	—	—	—
MAPS Management	Configure MAPS.	R	RW	—	—	—
Performance	Launch Investigate mode for real-time and historic graphs, modify historic data collector.	R	RW	—	—	—
Port Mapping - Host	Import host mapping, create host enclosures.	R	RW	—	—	—
Port Mapping - Storage	Import storage mapping, create storage enclosures.	R	RW	—	—	—
Reports	Create report content, generate reports.	R	RW	—	—	—
Server Backup	Create and schedule server backups.	RW	RW	—	—	—
Server Software Configuration	Configure email server setup and event notification.	R	RW	—	—	—
Switch Maintenance Mode	Set and schedule maintenance mode on a switch.	R	RW	—	—	—

Privilege	Description for RW Access	Preconfigured Roles				
		Operator	SAN System Admin	Security Admin	Security Officer	Zone Admin
Technical Support Data Collection	Generate SANnav support data collection. With Read-only access, you can view and download the support data collection, but cannot generate it.	R	RW	—	—	—
Troubleshooting	For future use.	R	RW	—	—	—
User Management	Create users, roles, AORs, and LDAP groups. Assign roles and AORs. Unlock user accounts.	R	RW	—	RW	—
Zone Management - Advanced	Perform zoning operations.	R	RW	—	—	RW
Zone Management - Simplified	Perform simplified zoning operations.	R	RW	—	—	RW

5.4 Configuring SANnav to Use an External Server for Authentication

You can configure SANnav to use an external server for authentication of user names and passwords. You can also optionally use this server for user authorization using roles and AORs.

NOTE

If you are configuring an external server for authentication and authorization, this guide assumes that you understand how external authentication works, that the external servers are already set up, and that the user names and passwords are already configured on the external server. This guide explains how to configure SANnav and how to add the specific SANnav role and AOR attributes to the external server for authorization.

SANnav supports the following types of external servers for authentication and authorization:

- LDAP
- RADIUS
- TACACS+

When you select LDAP, RADIUS, or TACACS+ as the primary authentication method, you must provide SANnav with a list of up to three LDAP, RADIUS, or TACACS+ servers. If you provide more than one server, then if the first server is not reachable or if authentication fails, SANnav attempts to access the next server on the list.

If all external servers are unreachable or if authentication fails, you can specify whether to use the local SANnav database as a secondary authentication method.

1. Click **SANnav** in the navigation bar, and then select **Security > SANnav Authentication and Authorization**.
2. Select the type of primary authentication (LDAP, RADIUS, or TACACS+).
3. Optional: Set up secondary authentication, in case the primary authentication method fails.

The default is **None**.

- a. Select **Local Database** in the **Secondary Authentication** drop-down list.

If the primary authentication fails, SANnav uses the local database to try to authenticate the user.

- b. From the **Failover Option** drop-down list, select the condition under which you want to fail over to the local database.

4. Select the authorization preference.

Users are authorized based on their assigned roles and AORs.

Option	Description
Local Database	Users are authorized using the roles and AORs defined in the local database.
Primary Authentication Server	Users are authorized using the roles and AORs defined on the external server. If you select this option, you must ensure that the role and AOR names defined in the local database match the role and AOR names that are assigned to the users on the external server.
Authentication Server Groups	(LDAP only) Select this option to assign roles and AORs to Active Directory (AD) groups and not to individual users. If you are using LDAP for authorization, this is the recommended authorization method.

5. Add the list of external servers to use for authentication.

You must add at least one server, and can add a maximum of three servers. Best practice is to add more than one server.

NOTE

If you have multiple LDAP servers that resolve to a common DNS name, you can use the DNS name instead of adding multiple server entries.

If you add more than one server, make sure that the list is in the correct order. The first server in the list is used first. If that server is not reachable, SANnav tries to reach the next server on the list, and then the next, until either a server is reached or the list is exhausted. Click the arrows in the **Order** column to rearrange the order of the servers.

6. Click **Save** to save the configuration and exit the page.

The screenshot shows the SANnav Authentication and Authorization configuration page. The page has a navigation bar at the top with links for Dashboard & Reports, Topology, Inventory, Events, Zoning, and SANnav. The main content area is titled 'SANnav Authentication and Authorization'. It contains four dropdown menus for configuration: Primary Authentication (set to LDAP Server), Secondary Authentication (set to Local Database), Failover Option (set to LDAP Servers Not Reachable), and Authorization Preference (set to Authentication Server Groups). Below these is a table titled 'LDAP Servers' with 3 items. The table has columns for Order, Hostname/IP, TCP Port, Timeout, and Attempts. The 'Save' button is highlighted with a red box.

Order	Hostname/IP	TCP Port	Timeout	Attempts
↓	192.0.2.0	389	5	3
↕	198.51.100.0	636	10	4
↑	203.0.113.0	389	20	5

The user names and passwords must be configured on the external servers. If you are also using the external servers for authorization, you must assign the roles and AORs to users on the external servers.

5.5 LDAP Server Configuration

If you use an LDAP server for authentication, when users log in to SANnav, they are authenticated using the user name and password list on the LDAP server.

You can use the LDAP server for authentication only or for both authentication and authorization.

- If you are using LDAP for authentication, the user accounts must be created on the LDAP servers.
- If you are also using LDAP for authorization, it is recommended that you use LDAP groups for authorization. Creating LDAP groups allows you to assign the roles and areas of responsibility (AORs) to groups of users instead of individual users.

NOTE

This guide assumes that the LDAP servers are already configured with the list of user accounts. If you are using LDAP groups for authorization, this guide assumes that the LDAP server is already configured with groups, and that users are assigned to the groups.

NOTE

You must add the LDAP server host entry to the Docker container host file to authenticate LDAP server users. For instructions, see [Adding LDAP Servers to the Docker Container](#).

The following table outlines the steps you must perform on SANnav and on the external LDAP servers for various scenarios.

Table 13: Tasks Required for Setting Up Authentication and Authorization on an External LDAP Server

Scenario	Tasks Performed in SANnav	Tasks Performed on the LDAP Servers
Primary authentication = LDAP Server Secondary authentication = None Authorization = Local database	<ol style="list-style-type: none"> 1. Configure SANnav to use an external LDAP server. 2. Create roles and AORs. 3. Create user accounts. 4. Assign roles and AORs to users. 	User accounts must already be created on the LDAP servers. No additional tasks are needed.
Primary authentication = LDAP Server Secondary authentication = None Authorization = External server	<ol style="list-style-type: none"> 1. Configure SANnav to use an external LDAP server. 2. Create roles and AORs. 	User accounts must already be created on the LDAP servers. You must perform the following additional tasks: <ol style="list-style-type: none"> 1. Create role and AOR custom attributes in the LDAP Active Directory. 2. Assign roles and AORs to users.
Primary authentication = LDAP Server Secondary authentication = None Authorization = LDAP groups	<ol style="list-style-type: none"> 1. Configure SANnav to use an external LDAP server. 2. Create roles and AORs. 3. Upload LDAP groups into local database for authorization. 4. Assign roles and AORs to LDAP groups. 	User accounts and groups must already be created on the LDAP servers, and the users must be assigned to groups. No additional tasks are needed.
Primary authentication = LDAP Server Secondary authentication = Local database Authorization = Local database	<ol style="list-style-type: none"> 1. Configure SANnav to use an external LDAP server. 2. Create roles and AORs. 3. Create user accounts. 4. Assign roles and AORs to users. 	User accounts must already be created on the LDAP servers. No additional tasks are needed.

Table 13: Tasks Required for Setting Up Authentication and Authorization on an External LDAP Server (Continued)

Scenario	Tasks Performed in SANnav	Tasks Performed on the LDAP Servers
Primary authentication = LDAP Server Secondary authentication = Local database Authorization = External server	<ol style="list-style-type: none"> 1. Configure SANnav to use an external LDAP server. 2. Create roles and AORs. 3. Create user accounts. 4. Assign roles and AORs to users, in case primary authentication fails. 	<p>User accounts must already be created on the LDAP servers. You must perform the following additional tasks:</p> <ol style="list-style-type: none"> 1. Create role and AOR custom attributes in the LDAP Active Directory. 2. Assign roles and AORs to users.
Primary authentication = LDAP Server Secondary authentication = Local database Authorization = LDAP groups	<ol style="list-style-type: none"> 1. Configure SANnav to use an external LDAP server. 2. Create roles and AORs. 3. Create user accounts, in case primary authentication fails. 4. Upload LDAP groups into local database for authorization. 5. Assign roles and AORs to LDAP groups. 6. Assign roles and AORs to users, in case primary authentication fails. 	<p>User accounts and groups must already be created on the LDAP servers, and the users must be assigned to groups. No additional tasks are needed.</p>

5.5.1 Adding LDAP Servers to the Docker Container

You must add the LDAP server host entry to the Docker container host file to authenticate LDAP server users. A script is provided to add the LDAP server host entry to the Docker container host file.

1. Open a terminal and navigate to the `<install_home>\bin` directory.
2. Type `addLdapServer FQDN.LDAP_Server_IP` (for example: `addLdapServer xxxxx.domain.com:xx.yy.zz.aa`) and press **Enter**.

All existing sessions are logged off.

5.5.2 Creating Role and AOR Custom Attributes in the LDAP Active Directory

If you use the LDAP server for authorization without groups, you must update the Microsoft Active Directory (AD) to add the custom attributes `NmRoles` and `NmAors` for roles and AORs, respectively.

This procedure assumes that you are familiar with Microsoft Management Console (MMC) and Microsoft Active Directory (AD).

Before performing this task, you must obtain two unique object identifiers: one for the roles attribute and one for the AOR attribute.

NOTE

If you have more than just a few users, it is recommended that you perform authorization using LDAP groups. If you use groups, you do not need to perform this task, but you do need to have the groups created on the LDAP server. On SANnav, you must upload the groups and assign roles and AORs to the groups.

Perform the following steps on the LDAP server to add two new custom attributes to the AD: `NmRoles` and `NmAors`.

1. On the LDAP server, install the Active Directory Schema.
 - a. Select **Start > Run**.
 - b. Type `regsvr schmmgmt.dll` and press **Enter**.

2. Open the MMC, and add the Active Directory Schema into the MMC console.
3. Expand the Active Directory Schema tree in the MMC console, right-click the **Attributes** folder, and select **Create Attribute**.
4. Enter values for the Roles attribute in the **Create New Attribute** dialog, and click **OK**.
 - **Common Name** = NmRoles
 - **LDAP Display Name** = NmRoles
 - **Unique X500 Object ID** = The unique OID you obtained previously
 - **Syntax** = Case Insensitive String

Create New Attribute

Create a New Attribute Object

Identification

Common Name: NmRoles

LDAP Display Name: NmRoles

Unique X500 Object ID: 26492.16483.44921.9154894.18300998.2.1

Description:

Syntax and Range

Syntax: Case Insensitive String

Minimum:

Maximum:

Multi-Valued

OK Cancel Help

5. Repeat Step 4 to add the NmAors attribute.
 - **Common Name** = NmAors
 - **LDAP Display Name** = NmAors
 - **Unique X500 Object ID** = The unique OID you obtained previously
 - **Syntax** = Case Insensitive String
6. Add the new attributes to the user class.
 - a. Expand the **Classes** folder, right-click **user**, and select **Properties**.
 - b. Click the **Attributes** tab, and then click **Add**.
 - c. Select the NmRoles attribute, and click **OK**.
 - d. Click **Add** again, select the NmAors attribute, and click **OK**.
 - e. Click **OK** to close the dialog.
7. Close the MMC, and restart the Active Directory service.

5.5.3 Assigning Roles and AORs to Users on the LDAP Server

If you use the LDAP server for authorization without groups, you must assign the roles and AORs to each user on the LDAP server.

The users must already be added to the Active Directory (AD) on the LDAP server.

The NmRoles and NmAors attributes must already be defined in the AD.

NOTE

If you have more than just a few users, it is recommended that you perform authorization using LDAP groups. If you use groups, you do not need to perform this task, but you do need to have the groups created on the LDAP server. On SANnav, you must upload the groups and assign roles and AORs to the groups.

It is recommended that you back up your AD before performing the following steps.

1. On the LDAP server, open ADSI Edit.
 - a. Select **Start > Run**.
 - b. Type `adsiedit.msc` and press **Enter**.
2. Expand the ADSI Edit tree and the **CN=Users** directory.
3. Add the roles and AORs for each user.
 - a. Right-click the `CN=user-name`, and select **Properties**.
 - b. Select **NmRoles** in the **Attributes** list and click **Edit**.
 - c. Enter a comma-separated list of roles in the **Value** field and click **OK**.

NOTE

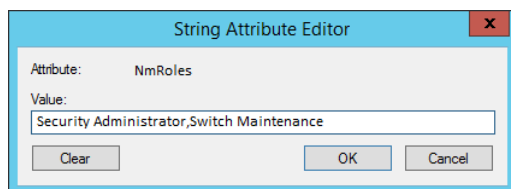
The role names must exactly match the roles defined in the SANnav local database.

- d. Select **NmAors** in the **Attributes** list and click **Edit**.
- e. Enter a comma-separated list of AORs in the **Value** field and click **OK**.

NOTE

The AOR names must exactly match the AORs defined in the SANnav local database.

For example, the following assigns the Security Administrator and Switch Maintenance roles to the selected user. The Switch Maintenance role is a custom role. All roles must be defined in the local SANnav database.



4. Close the **ADSI Edit** dialog.

5.5.4 Assigning Roles and AORs to LDAP Groups in SANnav

If you are using LDAP for authentication and authorization, the recommended method is to use LDAP groups. In SANnav, you must download these groups and then assign roles and AORs to the groups.

1. Click **SANnav** in the navigation bar, and then select **Security > SANnav User Management**.
2. Import the groups from the LDAP server.
 - a. Click **Groups**, and then click the **+** button in the subnavigation bar.
 - b. Enter the LDAP server information in the **Fetch Groups** dialog, and click **OK**.

If you select the **Use group name filter** checkbox and enter a text string, you are presented with a filtered list of groups; otherwise, you are presented with all of the groups in the LDAP server.

- c. Select the groups for which you want to provide authorization, and click **OK**.

NOTE

This process might take several minutes, depending on the number of groups present in the LDAP server.

3. Assign roles and AORs to the groups.

For each group, click the group name to open the detail page, select the roles and AORs to assign to the group, and click **Save**.

Now all users assigned to this group on the LDAP server are granted the assigned roles and AORs.

5.6 RADIUS Server Configuration

If you use a RADIUS server for authentication, when users log in to SANnav, they are authenticated using the user name and password list on the RADIUS server.

If you select RADIUS Server as your primary authentication method, it is assumed that the user names and passwords are already configured on the RADIUS server. You must now configure the following on the RADIUS server:

- Configure SANnav credentials, including the default authentication type.
- If you want authorization to be performed on the RADIUS server, you must perform the following tasks:
 - Assign roles and areas of responsibility (AORs) to users on the RADIUS server.
 - Configure the dictionary file on the RADIUS server to define the symbolic names for the roles and AORs.

Depending on whether secondary authentication is enabled, you must also configure user names and passwords on the local database (the SANnav server). The following table outlines the steps you must perform on SANnav and on the external RADIUS servers for various scenarios.

Table 14: Tasks Required for Setting Up Authentication and Authorization on an External RADIUS Server

Scenario	Tasks Performed in SANnav	Tasks Performed on the RADIUS Servers
Primary authentication = RADIUS server Secondary authentication = None Authorization = Local database	<ol style="list-style-type: none"> 1. Configure SANnav to use an external RADIUS server. 2. Create roles and AORs. 3. Create user accounts. 4. Assign roles and AORs to users. 	User accounts must already be created on the RADIUS servers. You must perform the following additional tasks: <ol style="list-style-type: none"> 1. Configure SANnav credentials.
Primary authentication = RADIUS server Secondary authentication = None Authorization = External server	<ol style="list-style-type: none"> 1. Configure SANnav to use an external RADIUS server. 2. Create roles and AORs. 	User accounts must already be created on the RADIUS servers. You must perform the following additional tasks: <ol style="list-style-type: none"> 1. Configure SANnav credentials. 2. Assign roles and AORs to users. 3. Configure dictionary file to include the role and AOR attributes.
Primary authentication = RADIUS server Secondary authentication = Local database Authorization = Local database	<ol style="list-style-type: none"> 1. Configure SANnav to use an external RADIUS server. 2. Create roles and AORs. 3. Create user accounts. 4. Assign roles and AORs to users. 	User accounts must already be created on the RADIUS servers. You must perform the following additional tasks: <ol style="list-style-type: none"> 1. Configure SANnav credentials.
Primary authentication = RADIUS server Secondary authentication = Local database Authorization = External server	<ol style="list-style-type: none"> 1. Configure SANnav to use an external RADIUS server. 2. Create roles and AORs. 3. Create user accounts. 4. Assign roles and AORs to users, in case primary authentication fails. 	User accounts must already be created on the RADIUS servers. You must perform the following additional tasks: <ol style="list-style-type: none"> 1. Configure SANnav credentials. 2. Assign roles and AORs to users. 3. Configure dictionary file to include the role and AOR attributes.

5.6.1 Configuring SANnav Credentials on the RADIUS Server

Perform this task if you are using a RADIUS server for authentication. You must provide the server with the SANnav configuration information so that the RADIUS server can communicate with the SANnav server.

For this task, you update two files on the RADIUS server:

- Update the `clients.conf` file with the SANnav information.
- Update the `users.conf` file to specify the default authentication type.

Depending on the RADIUS server you install, the configuration files may have different names.

1. On the RADIUS server, open the client configuration file (`clients.conf`) in a text editor (such as Notepad).
The client configuration file contains definitions of the RADIUS clients.
2. Enter the SANnav data.

```
client ip_address
{
  secret      = user-defined_secret
  shortname   = localhost_name
}
```

Where `ip_address` is the address of the SANnav server, `user-defined-secret` is the shared secret that you configured on the SANnav server when you added the RADIUS server for authentication, and `localhost_name` is the host name of the SANnav server.

For example:

```
client 172.26.3.76 {
    secret      = password
    shortname   = GVM1server
}
```

3. Save and close the `clients.conf` file.
4. Open the user configuration file (`users.conf`) in a text editor (such as Notepad).
5. Enter the following line to set the default authentication type.

```
DEFAULT      Auth-Type = authtype
```

Where *authtype* is CHAP or PAP. The default authentication type should match what you configured in SANnav when you added the RADIUS server for authentication.

If you are not sure of the authentication type, in SANnav, click **SANnav** in the navigation bar, and then click **Security > SANnav Authentication and Authorization**.

The screenshot displays the SANnav Authentication and Authorization configuration interface. At the top, there are navigation tabs: Dashboard & Reports, Topology, Inventory, Events, Zoning, and SANnav. The main title is "SANnav Authentication and Authorization". Below the title, there are three dropdown menus: Primary Authentication (set to RADIUS Server), Secondary Authentication (set to None), and Authorization Preference (set to Local Database). Below these are three RADIUS Servers listed in a table. The table has columns for Order, Hostname/IP, TCP Port, Timeout, Attempts, and Authentication Type. The first server has Hostname/IP 192.0.2.0, TCP Port 1812, Timeout 5, and Attempts 3. The Authentication Type for this server is CHAP, which is highlighted with a red box. The second server has Hostname/IP 198.51.100.0, TCP Port 1812, Timeout 10, and Attempts 4, with Authentication Type PAP. The third server has Hostname/IP 203.0.113.0, TCP Port 1812, Timeout 20, and Attempts 5, with Authentication Type CHAP. There are "Add" and "Remove" buttons to the right of the table. At the bottom, there are "Save" and "Close" buttons.

Order	Hostname/IP	TCP Port	Timeout	Attempts	Authentication Type
↓	192.0.2.0	1812	5	3	CHAP
↕	198.51.100.0	1812	10	4	PAP
↑	203.0.113.0	1812	20	5	CHAP

6. Save and close the `users.conf` file.

If you are also using the RADIUS server for authorization, you must assign roles and AORs to users on the RADIUS server.

5.6.2 Assigning Roles and AORs to Users on the RADIUS Server

If you use the RADIUS server for authorization, you must assign the roles and areas of responsibilities (AORs) for each user on the RADIUS server.

The user configuration file on the RADIUS server must already contain the list of user names and passwords.

The user configuration file on the RADIUS server contains the individual user profiles. You must update this file to include the roles and AORs assigned to each user. The roles and AORs must be defined in the local SANnav database. The role and AOR names assigned in the user configuration file on the RADIUS server must exactly match the role and AOR names defined in the local SANnav database.

1. Open the user configuration file (`users.conf`) in a text editor (such as Notepad).

Depending on the RADIUS server you install, the user configuration file might have a different name.

2. Enter the roles and AORs for each user.

```
user_name
User-Password = "password"
NM-Roles-AORs-List = "nmRoles=management_roles; nmAORs=management_AORs"
```

where `management_roles` and `management_AORs` are comma-separated lists of the roles and AORs assigned to the user.

NOTE

These roles and AORs must match exactly the roles and AORs defined in the SANnav local database.

For example, the following assigns the Security Administrator and Switch Maintenance roles and the All Fabrics AOR to the account with username "admin1" and password "PassWord1". The Switch Maintenance role is a custom role. All roles and AORs must be defined in the local RADIUS database.

```
admin1
User-Password = "PassWord1"
NM-Roles-AORs-List = "nmRoles=Security Administrator,Switch Maintenance; nmAORs=All Fabrics"
```

3. Save and close the `users.conf` file.

Next, you must configure the RADIUS dictionary file to include the `NM-Roles-AORs-List` attribute.

5.6.3 Configuring Role and AOR Attributes on the RADIUS Server

If you specify that authorization is to be performed on the RADIUS server, you must create a SANnav dictionary file on the RADIUS server, and modify the RADIUS server dictionary file to reference the SANnav dictionary.

The dictionary file defines the symbolic names for RADIUS attributes and values. This file contains the attribute definition for roles and AORs, which are used for authorization.

Perform the following steps on the RADIUS server. You might need to work with the RADIUS server administrator for assistance in locating and editing the RADIUS server dictionary file.

1. Create a dictionary file and name it **dictionary.NM_AAA_dictionary**.
2. Open the dictionary file and add the following:

```
# -*- text -*-
#
# dictionary.brocade
#

VENDOR          Brocade 1588

BEGIN-VENDOR    Brocade
```

```
ATTRIBUTE      NM-Roles-AORs-List  1  string
```

```
END-VENDOR    Brocade
```

3. Save and copy this SANnav dictionary file to the directory where the RADIUS server dictionary is located.
4. Open the RADIUS server dictionary file in a text editor (such as Notepad).
5. Add the following line to reference the SANnav dictionary file in the RADIUS server dictionary file:

```
$INCLUDE dictionary.NM_AAA_dictionary
```

6. Save and close the RADIUS server dictionary file.

5.7 TACACS+ Server Configuration

If you use a TACACS+ server for authentication, when users log in to SANnav, they are authenticated using the user name and password list on the TACACS+ server.

NOTE

If your TACACS+ server is configured as a RADIUS server, follow the instructions for RADIUS server configuration.

If TACACS+ is your primary authentication method, it is assumed that the user accounts are already configured on the TACACS+ server. If TACACS+ is used for authorization, you must assign roles and AORs to users on the TACACS+ servers.

Depending on whether secondary authentication is enabled, you must also configure user names and passwords on the local database (the SANnav server). The following table outlines the steps you must perform on SANnav and on the external TACACS+ servers for various scenarios.

Table 15: Tasks Required for Setting Up Authentication and Authorization on an External TACACS+ Server

Scenario	Tasks Performed in SANnav	Tasks Performed on the TACACS+ Servers
Primary authentication = TACACS+ Server Secondary authentication = None Authorization = Local database	<ol style="list-style-type: none"> 1. Configure SANnav to use an external TACACS+ server. 2. Create roles and AORs. 3. Create user accounts. 4. Assign roles and AORs to users. 	User accounts must already be created on the TACACS+ servers. No additional tasks are needed.
Primary authentication = TACACS+ Server Secondary authentication = None Authorization = External server	<ol style="list-style-type: none"> 1. Configure SANnav to use an external TACACS+ server. 2. Create roles and AORs. 	User accounts must already be created on the TACACS+ servers. You must perform the following additional tasks: <ol style="list-style-type: none"> 1. Configure SANnav credentials. 2. Assign roles and AORs to users.
Primary authentication = TACACS+ Server Secondary authentication = Local database Authorization = Local database	<ol style="list-style-type: none"> 1. Configure SANnav to use an external TACACS+ server. 2. Create roles and AORs. 3. Create user accounts. 4. Assign roles and AORs to users. 	User accounts must already be created on the TACACS+ servers. No additional tasks are needed.
Primary authentication = TACACS+ Server Secondary authentication = Local database Authorization = External server	<ol style="list-style-type: none"> 1. Configure SANnav to use an external TACACS+ server. 2. Create roles and AORs. 3. Create user accounts. 4. Assign roles and AORs to users, in case primary authentication fails. 	User accounts must already be created on the TACACS+ servers. You must perform the following additional tasks: <ol style="list-style-type: none"> 1. Configure SANnav credentials. 2. Assign roles and AORs to users.

5.7.1 Assigning Roles and AORs to Users on the TACACS+ Server

If you use the TACACS+ server for authorization, you must create the roles and areas of responsibility (AORs) on the SANnav server, and then assign the roles and AORs to each user on the TACACS+ server.

The `tac_plus.cfg` file on the TACACS+ server must already contain the list of user names and passwords.

The `tac_plus.cfg` file on the TACACS+ server contains the individual user profiles. You must update this file to include the roles and AORs assigned to each user. The roles and AORs must also be defined in the local SANnav database. You must ensure that the role and AOR names in the user configuration file on the TACACS+ server exactly match the role and AOR names defined in the local SANnav database.

1. On the TACACS+ server, open the `tac_plus.cfg` file in a text editor (such as Notepad).
2. Enter the roles and AORs for each user.

```
user = username {
    chap = cleartext "chap$password"
    pap = cleartext "pap-password"
    service = exec {
        NM-Roles-AORs-List = "nmRoles=management_roles; nmAORs=management_AORs"
    }
}
```

where `management_roles` and `management_AORs` are comma-separated lists of the roles and AORs assigned to the user.

For example, the following assigns the Security Administrator and Switch Maintenance roles and the All Fabrics AOR to user "admin2". The Switch Maintenance role is a custom role. All roles and AORs must be defined in the local SANnav database.

```
user = admin2 {
    chap = cleartext "my$chap$password"
    pap = cleartext "my-pap-password"
    service = exec {
        NM-Roles-AORs-List = "nmRoles=Security Administrator,Switch Maintenance; nmAORs=All Fabrics"
    }
}
```

3. Save and close the `tac_plus.cfg` file.

5.8 Managing Signed Certificates

It is recommended that you use a trusted certificate authority (CA) signed certificate once the SANnav application is up and running. Using a trusted CA signed certificate assures client users that the server is the correct, approved server.

By default, SANnav uses a self-signed certificate that is created with a unique key at installation time. This self-signed certificate has a 5-year validity period.

After the application is installed and running, it is recommended that you replace the self-signed certificate with a trusted CA signed certificate.

NOTE

SANnav supports TLS 1.1 and higher.

Perform the following steps to replace the SSL certificates in SANnav for client-server communication. In a swarm cluster, perform these steps for the proxy (master) node, as all communication from the client is through the proxy node only. OpenSSL is used in this example.

1. Generate a private key and certificate signing request (CSR) using the following command.

```
openssl req -newkey rsa:2048 -nodes -keyout sannav.key -out sannav.csr
```

Where *sannav.key* is the file where the private key is saved, and *sannav.csr* is the file where the CSR is saved.

Provide all input for the certificate. Ensure that the common name matches the host name of the SANnav server.

2. If you are replacing the certificate with a signed certificate, submit the CSR to your CA with proper credentials to identify you as authorized to create certificates and receive the signed certificate from the CA.

Now you have both the key and the signed certificate.

3. If you are replacing the certificate with a self-signed certificate, generate the self-signed certificate using the key and the following command.

```
openssl req -key sannav.key -new -x509 -days 365 -out sannav.crt
```

Where *sannav.key* is the existing key file, and *sannav.crt* is the file where the certificate is stored.

Provide all required input for the certificate.

Now you have both the key and the self-signed certificate.

4. Copy both the key and the certificate to a location on the SANnav server, for example, `/root/certificates`.
5. If you have CA root and intermediate CA certificates, chain them into one before importing to the switch or replacing the certificates.

Use the following command:

```
cat my_intermediate.crt [intermediate2.crt] ... my_root.crt > ca-cert-chain.pem
```

6. Run the following script to replace the public certificate and private key and restart the services.

```
<install_home>/bin/replace-server-cert.sh
```

Provide the full paths for both the key and the certificate.

After the script starts the services, wait a few more minutes.

NOTE

If you use secure syslog, import the new certificates in the switches registered for secure syslog and run `<install_home>/bin/restart-server.sh` to restart all services.

7. Launch the SANnav client in a browser window, and check if the new certificate information is shown.

Monitoring

6.1 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 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.

When you discover a fabric, monitoring is automatically enabled on the fabric and on all switches in the fabric. When monitoring is enabled, the following occurs:

- Data collection happens periodically at an interval that depends on the size of the SAN.
- SANnav interface displays are updated with the latest fabric and switch information.
- SANnav registers itself as a Simple Network Management Protocol (SNMP) trap recipient and Syslog message recipient.

Considerations for Monitoring Fabric OS 8.2.1 and Later Switches

For optimal performance, you should monitor a fabric in only one instance of SANnav Management Portal, although up to two instances are supported to monitor the same fabric (two instances of SANnav or one instance of SANnav and one instance of Brocade Network Advisor).

If two instances of SANnav Management Portal are monitoring the same switch running Fabric OS 8.2.1 or later, the following features display data in only the first instance:

- **Network Port Traffic Conditions** dashboard
- High-granularity performance data collection
- Zoom and Fetch in performance Investigate view

If one instance of SANnav Management Portal and one instance of Brocade Network Advisor are monitoring the same switch running Fabric OS 8.2.1 or later, you should disable historic data collection in Brocade Network Advisor for that switch.

Seed Switch

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

It is strongly recommended that you 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, on the other hand, is automatically elected when the fabric is formed. The principal switch maintains time and manages domain ID assignment for the fabric.

If a switch that is running in Access Gateway mode is used as the seed switch, the switch is discovered as a standalone 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.

The Brocade Analytics Monitoring Platform cannot be used as a seed switch.

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

Discovery Prerequisites

Before you can discover a fabric, the following prerequisites must be met:

- All switches in the fabric must be running Fabric OS 7.4.0 or higher.
- The seed switch must be reachable from the SANnav server using SNMP and the protocol that was selected for server-to-switch communication during installation.
- If a Fabric Configuration Server (FCS) policy is enabled, the seed switch must be a primary FCS.

If you are using SANnav with a Base license and a director is a member of the fabric, the director is discovered, but its status is "Not manageable."

Note that the supported network latency is 100 ms. The network latency between SANnav Management Portal and the SAN that it is managing should not exceed 100 ms.

Unsupported Switches and Fabric Discovery

If a switch has reached End of Support (EOS), it cannot be used as a seed switch for discovery. Discovery fails if an EOS switch is used as the seed switch. Choose a different, supported switch to be the seed switch.

If you discover a fabric that contains one or more EOS switches, discovery succeeds, but the EOS switches are permanently unmonitored. The only action that you can perform on these EOS switches is to delete them.

If the switch EOS date is reached after the fabric is discovered, you can continue to monitor the switch, but the next time the fabric is rediscovered, the switch becomes permanently unmonitored.

6.1.1 Discovering a Fabric

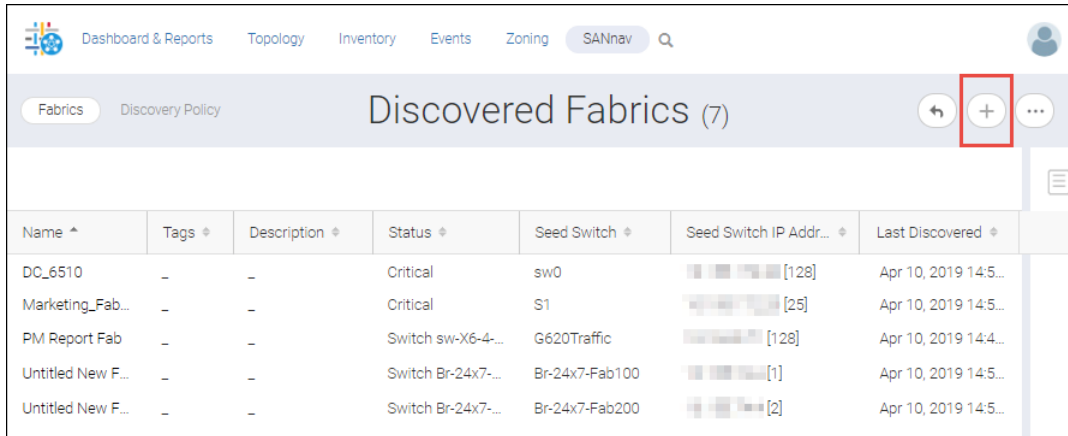
You must discover a fabric before you can monitor and manage it.

Before you can discover a fabric, you must have the following:

- Discover Setup privilege with read/write permission
- IP address and login credentials for the seed switch

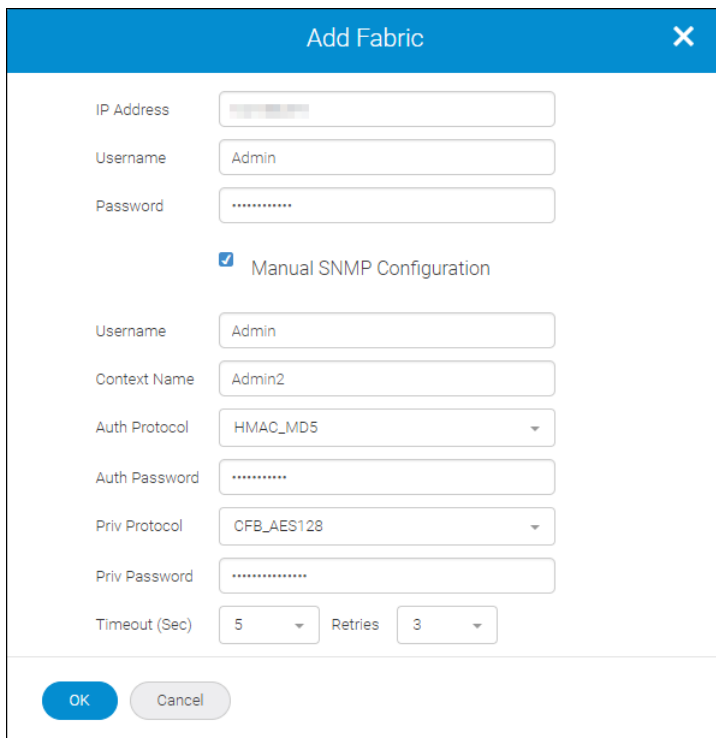
Use the following procedure to discover a fabric.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Fabric Discovery**.
The **Discovered Fabrics** page displays all fabrics that have been discovered.
2. Click the **+** icon in the top-right corner of the page to add a fabric.



Name ^	Tags ^	Description ^	Status ^	Seed Switch ^	Seed Switch IP Addr... ^	Last Discovered ^
DC_6510	-	-	Critical	sw0	[128]	Apr 10, 2019 14:5...
Marketing_Fab...	-	-	Critical	S1	[25]	Apr 10, 2019 14:5...
PM Report Fab	-	-	Switch sw-X6-4...	G620Traffic	[128]	Apr 10, 2019 14:4...
Untitled New F...	-	-	Switch Br-24x7-...	Br-24x7-Fab100	[1]	Apr 10, 2019 14:5...
Untitled New F...	-	-	Switch Br-24x7-...	Br-24x7-Fab200	[2]	Apr 10, 2019 14:5...

3. Enter the IP address and login credentials of the seed switch in the **Add Fabric** dialog. The IP address can be in IPv4 or IPv6 format. If you do not provide login credentials, the default credentials are used.



4. Optional: If you want to manually enter the SNMP configuration parameters, select **Manual SNMP Configuration** and enter the information in the dialog. SANnav supports only SNMPv3. By default, SNMP is automatically configured using predefined SNMPv3 credentials.
5. Click **OK**.

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

The **Add Fabric** dialog displays a list of the logical switches configured on the seed switch. Each logical switch corresponds to a logical fabric, indicated by the fabric ID (FID). The **Name** field displays the logical switch name, not the logical fabric name.

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

<input type="checkbox"/> Name ^	Fabric ID ↕	WWN ↕
<input checked="" type="checkbox"/> LS-1	23	10.00.00:27:f8:37:d2:e4
<input type="checkbox"/> S1	15	10.00.00:27:f8:37:d2:e5
<input type="checkbox"/> s1	10	10.00.00:27:f8:37:d2:e6
<input checked="" type="checkbox"/> sw0	128	10.00.00:27:f8:37:d2:e3

- a. Select one or more logical fabrics to discover.

NOTE

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

- b. Click **OK**.

The **Discovered Fabrics** page displays with the newly discovered fabrics listed.

Click the fabric name to open the detail page, where you can change the fabric name, add tags, and view a list of switches in the fabric. Note that if a switch name is grayed out, the switch is physically disconnected from the fabric. SANnav maintains this information for tracking purposes.

6.1.2 Stopping Switch Monitoring

By default, monitoring is enabled for discovered switches. You should stop monitoring a switch if you want to replace the switch or bring down the monitored port count to within the licensing limit.

Before you can stop monitoring a switch, you must have the following:

- Discover Setup privilege with read/write permission

When you stop monitoring a switch, the following occurs:

- Data collection on the switch stops.
- You no longer receive SNMP traps and Syslog messages.
- You can no longer perform feature-specific operations, such as downloading firmware.
- Any scheduled operations on the switch are stopped.
- The switch is not displayed anywhere in SANnav, except in the Discovery view.

NOTE

You cannot stop monitoring the seed switch.

When you stop monitoring a switch, you do not lose historic data, such as port statistics. So, for example, if you wanted to delete a switch from SANnav, you could stop monitoring the switch, back up necessary data, and then delete the switch.

To stop monitoring a switch, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Fabric Discovery**.
The **Discovered Fabrics** page displays all fabrics that have been discovered.
2. Click the fabric name to open the fabric detail page, which displays the list of switches in the fabric.
3. Select the switches that you want to stop monitoring, and click **Stop Monitoring**.

The screenshot shows the SANnav interface for fabric CID_NPTC. The 'Monitoring' status is set to 'On'. Below the fabric details, there is a table of switches. The 'new_155...' and 'CID-ENG...' switches are selected. The 'Stop Monitoring' button is highlighted with a red box.

Name	WWN	IP Ad...	FID	Com...	Discover...	Firm...
<input type="checkbox"/>	BR-G620-...	10:00:C4:...	10.124.5...	128	http	Discovered: ...
<input checked="" type="checkbox"/>	new_155...	10:00:00:...	10.124.7...	128	http	Discovered: ...
<input checked="" type="checkbox"/>	CID-ENG-...	10:00:00:...	10.124.1...	-	http	Discovered: ...
<input type="checkbox"/>	BR-G630-...	10:00:88:...	10.124.5...	128	http	Discovered

The **Discovery Status** changes to **Unmonitored**.

6.1.3 Stopping Fabric Monitoring

By default, monitoring is enabled for discovered fabrics. You should stop monitoring a fabric if you want to temporarily reduce the monitored port count or as the first step in deleting the fabric.


Required privilege: Discover Setup with read/write permission.

When you stop monitoring a fabric, the following occurs:

- Monitoring stops on all switches in the fabric.
- Data collection on the fabric and all switches in the fabric stops.
- You no longer receive SNMP traps and Syslog messages.
- You can no longer perform feature-specific operations, such as downloading firmware.
- Any scheduled operations on the fabric or switches are stopped.
- The fabric and switches are removed from the SANnav topology and inventory.

When you stop monitoring a fabric, you do not lose historic data, such as port statistics. So, for example, if you wanted to delete a fabric from SANnav, you could stop monitoring the fabric, back up the necessary data, and then delete the fabric.

The following procedure shows how to stop monitoring one or more fabrics. You can also stop monitoring a fabric from the fabric detail page.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Fabric Discovery**.
The **Discovered Fabrics** page displays all fabrics that have been discovered.
2. Click the **More** button () in the upper-right corner of the page, and then click **Bulk Select**.
A column of checkboxes displays to the left of the fabric names.
3. Select one or more fabrics to stop monitoring.
4. Click **Edit** in the upper-right corner of the page, and then select **Stop Monitoring**.



The status column now shows "Unmonitored" for the fabrics.

6.1.4 Resuming Switch Monitoring

If you previously stopped monitoring a switch, you can resume monitoring it to trigger asset collection and receive events and traps from the switch.

Before you resume monitoring the switch, make sure that the previously configured credentials are still accurate and the switch is reachable.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Fabric Discovery**.
The **Discovered Fabrics** page displays all fabrics that have been discovered.
2. Click the fabric name to open the fabric drill-down page, which displays the list of switches in the fabric.
3. Select one or more switches that you want to monitor, and click **Monitor**.

The screenshot shows the SANnav interface for fabric configuration. At the top, there are navigation tabs: Dashboard & Reports, Topology, Inventory, Events, Zoning, and SANnav. The main header displays 'CID_FABRIC_11_D_PORT' with a back arrow and an 'Actions' button. Below the header, there are input fields for Name (CID_FABRIC_11_D_PORT), Description, and Tags. There are also dropdown menus for Tracking (On) and Monitoring (On), along with an 'Update Members' button. A 'Products' table is shown below, with a search bar and '2 Items' indicated. The table has columns: Name, WWN, IP Ad..., FID, Com..., Discover..., and Firm... The first row is selected, and the 'Monitor' button is highlighted. The 'Discovery Status' column shows 'Unmonitored'. Other buttons like 'Rediscover', 'Stop Monitoring', and 'Configure' are also visible. At the bottom, there are 'Save', 'Delete', and 'Cancel' buttons.

The **Discovery Status** column for the switch updates. Events, traps, and asset collection for the switch resume.


6.1.5 Resuming Fabric Monitoring

If you previously stopped monitoring a fabric, you can resume monitoring it to trigger asset collection and receive events and traps from the fabric.

Before you resume monitoring the fabric, make sure that the previously configured credentials are still accurate and the seed switch is reachable.

You must have the Discover Setup privilege with read/write permission.

The following procedure shows how to resume monitoring one or more fabrics. You can also resume monitoring a fabric from the fabric drill-down page.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Fabric Discovery**.
The **Discovered Fabrics** page displays all fabrics that have been discovered.
2. Click the **More** button () in the upper-right corner of the page, and then click **Bulk Select**.
A column of checkboxes displays to the left of the fabric names.
3. Select one or more fabrics to monitor.
4. Click **Edit** in the upper-right corner of the page, and then select **Monitor**.

The screenshot shows the SANnav interface with the 'Discovered Fabrics (12)' page. The table below lists the discovered fabrics and their associated switches. The 'Monitor' option in the context menu is highlighted with a red box.

<input type="checkbox"/>	Name	Tags	Description	Status	Seed S...	Seed Switch IP Add...	FID	Last Discovered
<input checked="" type="checkbox"/>	TC X6-4	-	-	Unmonitored	SWBD165	10.155.74.203	128	Jun 14, 2019 11:28:01
<input checked="" type="checkbox"/>	TC G620	-	-	Unmonitored	sw0	10.155.74.201	-	Jun 14, 2019 11:28:01
<input type="checkbox"/>	DC_6510	-	-	Switch sw0: N...	sw0	10.155.172.20	128	Jun 13, 2019 14:40:01
<input type="checkbox"/>	Marketing...	-	-	Switch S1: No...	S1	10.155.172.20	25	Jun 13, 2019 14:46:31

The status column for the fabric updates. Events, traps, and asset collection for the fabric resume.

6.1.6 Rediscovering a Switch

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

Before you can rediscover a switch, you must have the following:

- Discover Setup privilege with read/write permission

The following procedure shows how to rediscover a switch.

- Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Fabric Discovery**. The **Discovered Fabrics** page displays all fabrics that have been discovered.
- Click the fabric name to open the fabric drill-down page, which displays the list of switches in the fabric.
- Select one or more switches, and click **Rediscover** at the right of the **Products** list. Clicking **Rediscover** at the right of the **Products** list rediscovers the selected switches. Clicking **Rediscover** from the **Actions** menu rediscovers the entire fabric.

The screenshot shows the SANnav management portal interface for a fabric named CID_NPTC. The interface includes a navigation bar with 'SANnav' selected, a breadcrumb trail 'Fabrics > Discovery Policy', and a title 'CID_NPTC'. Below the title are input fields for Name (CID_NPTC), Description, Tags, Tracking (On), and Monitoring (On), along with an 'Update Members' button. A table titled 'Products' shows 6 items with columns for Name, WWN, IP Ad., FID, Com., Discover., and Firm. The first two rows are selected with checkboxes. A 'Rediscover' button is highlighted in a red box on the right side of the table. At the bottom are 'Save', 'Delete', and 'Cancel' buttons.


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

6.1.7 Rediscovering a Fabric

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

Required privilege: Discover Setup with read/write permission.

The following procedure shows how to rediscover one or more fabrics. You can also rediscover a single fabric from the fabric drill-down page.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Fabric Discovery**.
The **Discovered Fabrics** page displays all fabrics that have been discovered.
2. Click the **More** button () in the upper-right corner of the page, and then click **Bulk Select**.
A column of checkboxes displays to the left of the fabric names.
3. Select one or more fabrics to rediscover.
4. Click **Edit** in the upper-right corner of the page, and then click **Rediscover**.

<input type="checkbox"/>	Name ^	Tags	Descr...	Status	Seed S...	Seed Switch IP ...	FID	Last Discovered
<input type="checkbox"/>	OID_FABRIC...	-	-	Switch CID...	OID_D_POR...	10.124.5.71	11	Jun 12, 2019 00:48:15
<input checked="" type="checkbox"/>	OID_NPTC_t...	-	-	Authentica...	BR-G620-21...	10.124.5.71	128	Jun 12, 2019 00:46:08
<input type="checkbox"/>	DC_6510	-	-	Switch sw...	sw0	10.155.172.20	128	Jun 13, 2019 14:40:05
<input checked="" type="checkbox"/>	Education_F...	-	-	Switch s1: ...	s1	10.155.172.20	10	Jun 13, 2019 14:46:30
<input checked="" type="checkbox"/>	FABRIC_10_...	-	-	Authentica...	BR-G620-21...	10.124.5.71	10	Jun 12, 2019 00:48:15
<input type="checkbox"/>	Marketing_F...	-	-	Switch S1: ...	S1	10.155.172.20	25	Jun 13, 2019 14:46:30

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

6.1.8 Changing the Seed Switch

If the status of the current seed switch shows that 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:

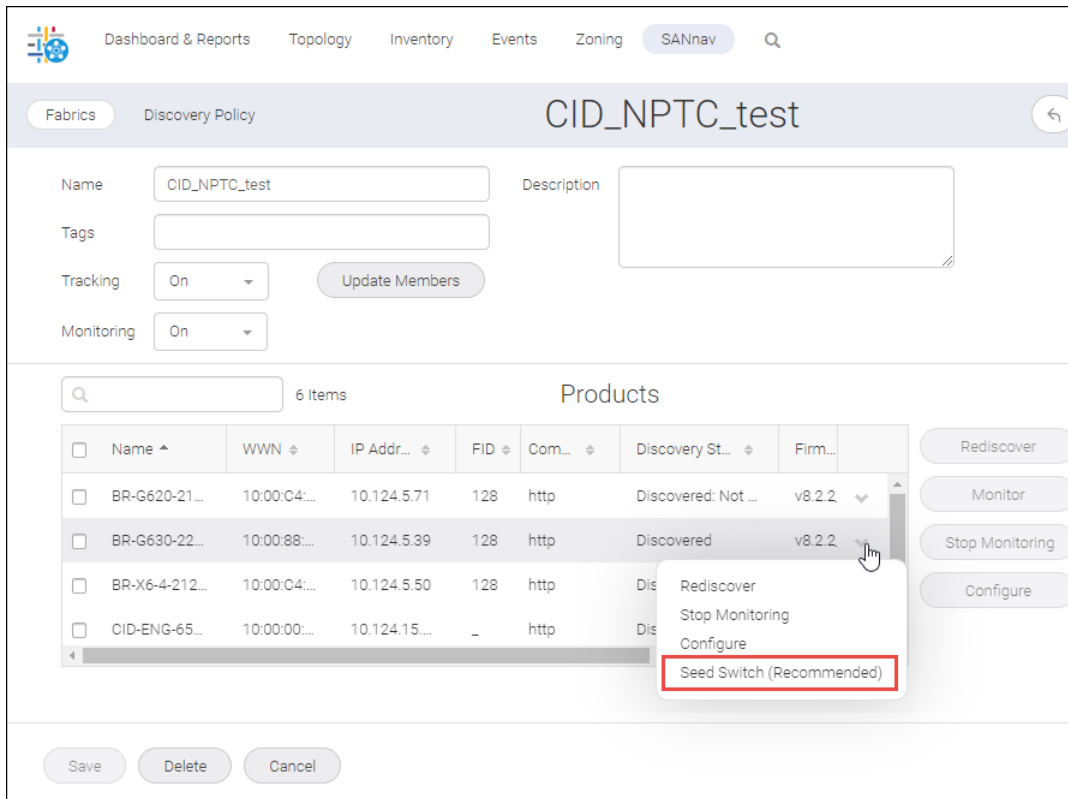
- The seed switch is no longer running the highest Fabric OS version in the fabric, which might happen if newer switches join the fabric or the switch firmware version changes on any switch in the fabric.
- The seed switch needs to be taken down for maintenance or replacement.

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** page displays all fabrics that have been discovered.
2. Click the fabric name to open the fabric details page, 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)**.

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 is capable of acting as a seed switch and the switch is not already the seed switch.



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

6.1.9 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 setting
- 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.

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

The **Discovered Fabrics** page displays all fabrics that have been discovered.

2. Click the fabric name to display the fabric drill-down page.
3. Click **Delete** at the bottom of the page.
4. Confirm the deletion when prompted.

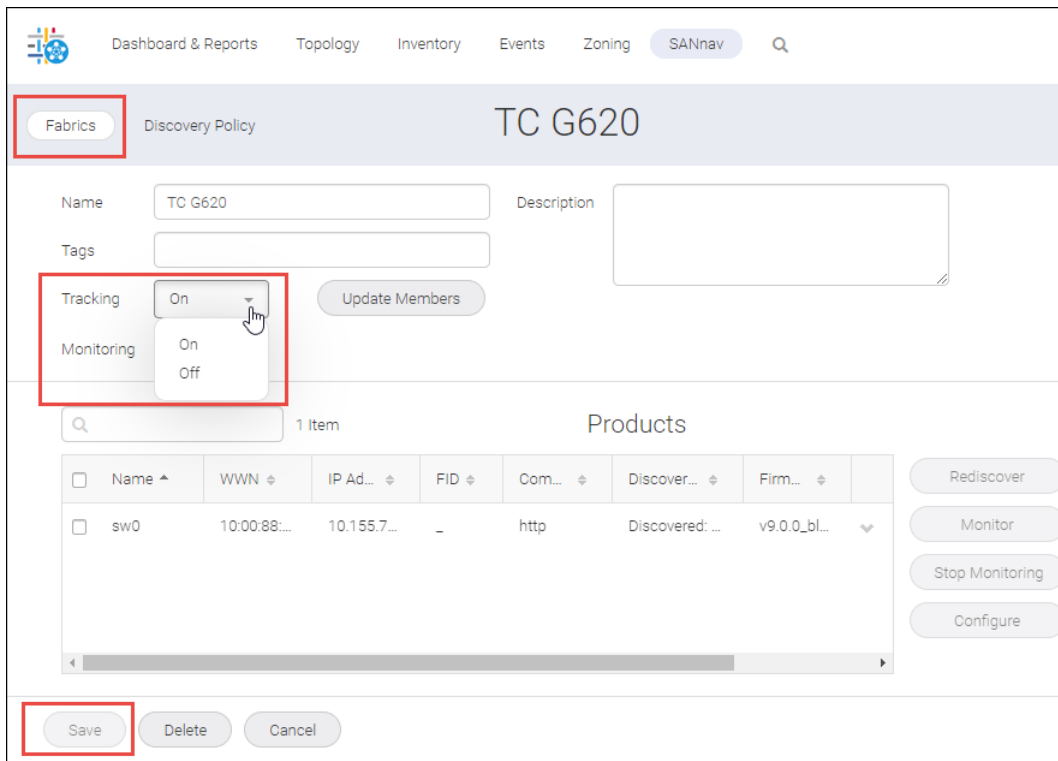
Upon successful removal of the fabric, you are returned to the **Discovered Fabrics** page. The fabric no longer displays in the list of discovered fabrics.

6.1.10 Configuring Fabric Tracking

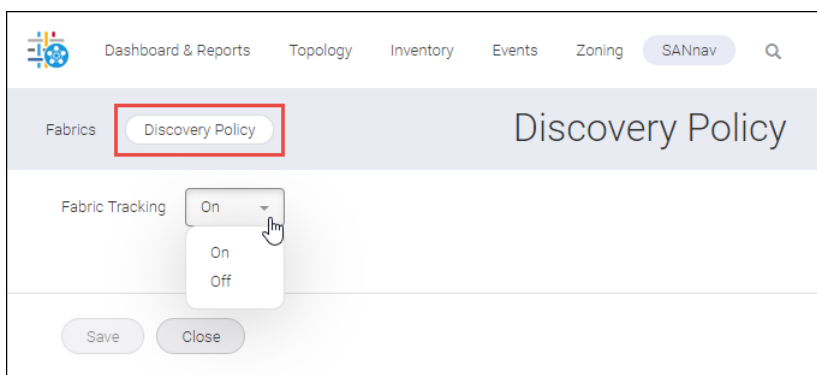
When you discover a new fabric and initial discovery is complete, fabric tracking is automatically enabled. Subsequently, SANnav Management Portal tracks if a switch, end device, or connection is added to or removed from the fabric.

Fabric tracking is configured for all fabrics through a discovery policy. You can also turn fabric tracking on and off for individual fabrics, regardless of the discovery policy.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Fabric Discovery**.
2. To change fabric tracking for individual fabrics, click the fabric name to open the details page, set **Tracking** to **On** or **Off**, and click **Save**.



3. To change the discovery policy for fabric tracking, click the **Discovery Policy** tab, set **Fabric Tracking** to **On** or **Off**, and click **Save**.



The changed policy does not affect fabrics that are already discovered, but applies to newly discovered fabrics.

6.1.11 Updating Fabric Members

When fabric tracking is turned on, and switches, device ports, and connections are added to or removed from the fabric, you must manually update the fabric members.

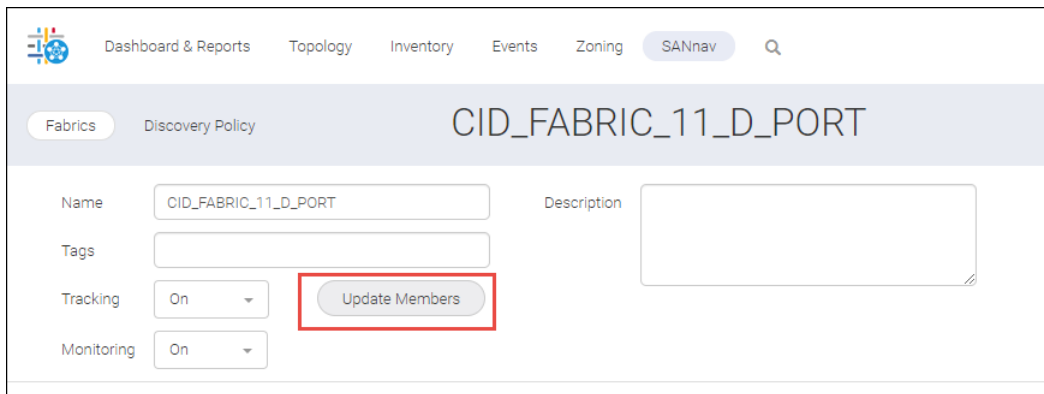
If fabric tracking is turned off, the fabric members are updated automatically.

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

2. Click the fabric name to open the details page.

3. Click **Update Members**.

The **Update Members** button is available only if tracking is turned on.



The screenshot displays the SANnav management portal interface. At the top, there is a navigation bar with tabs for 'Dashboard & Reports', 'Topology', 'Inventory', 'Events', 'Zoning', and 'SANnav'. Below the navigation bar, the main content area shows the 'CID_FABRIC_11_D_PORT' fabric details page. The page includes a 'Name' field with the value 'CID_FABRIC_11_D_PORT', a 'Description' field, a 'Tags' field, and two dropdown menus for 'Tracking' and 'Monitoring', both set to 'On'. A red rectangular box highlights the 'Update Members' button, which is located to the right of the 'Tracking' dropdown menu.

A dialog displays the switches, device ports, and connections that have been added or removed.

Update Members

1 Item Switches

Name ^	IP Address ⇅	Status ⇅	WWN ⇅	Domain ID ⇅
BB1_WEDGE_43	10.38.162.43	Added	10:00:50:EB:1A:F6:55:D0	15

124 Items Device Ports

Switch Name ^	Slot/Port ⇅	Port ⇅	Type ⇅	Status ⇅	Node WWN ⇅	Attached Pr
BB1_WEDGE_42	6	0b0600	Target	Added	20:06:00:11:0D:28	6
BB1_WEDGE_43	8	0f0800	Initiator	Added	20:00:8C:7C:FF:29	8

4 Items Connections

Switch Name(1) ^	Port Name(1) ⇅	Source Slot ⇅	Source Port ⇅	:
BB1_WEDGE_43	port49	-	49	:
BB1_WEDGE_43	port51	-	51	:

4. Click **Accept Changes**.

6.2 Dashboards

SANnav dashboards give you a functional, seamless, and customizable view of your SAN environments so that you can monitor and troubleshoot your SAN environments effectively and efficiently.

Some of the key capabilities of dashboards include the following:

- Live monitoring of network health and performance.
- Out-of-the-box dashboards.
- Ability to build custom dashboard templates for static and dynamic views.
- Out-of-the-box widgets to monitor switch and port status and error and performance statistics.
- Ability to customize content using network scope and date range.

SANnav provides the following "out-of-the-box" system dashboards:

- **Extension Dashboard**
- **Health Summary**
- **Network Port Traffic Conditions**

The **Health Summary** and **Network Port Traffic Conditions** dashboards are described later in this section. The **Extension Dashboard** is described in [Extension Tunnels and Circuits](#).

You can also create your own custom dashboards using system-defined product status and performance widgets that can be shared with all users and can be exported to other SANnav instances.

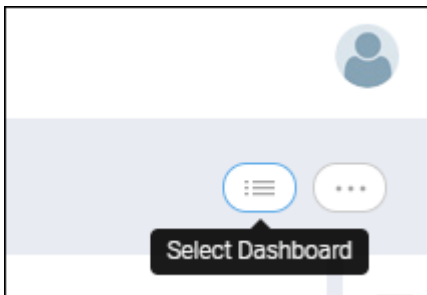
One of the dashboards is designated as the favorite dashboard. The *favorite dashboard* is the default landing view when you log in to SANnav. The **Health Summary** dashboard is the default favorite dashboard after installing SANnav. You can select another out-of-the-box or customized dashboard as the favorite.

6.2.1 Changing the Favorite Dashboard

When you log in to SANnav, the default landing view is the dashboard that is designated as the favorite dashboard. After installation, the **Health Summary** dashboard is the default favorite dashboard, but you can change this selection.

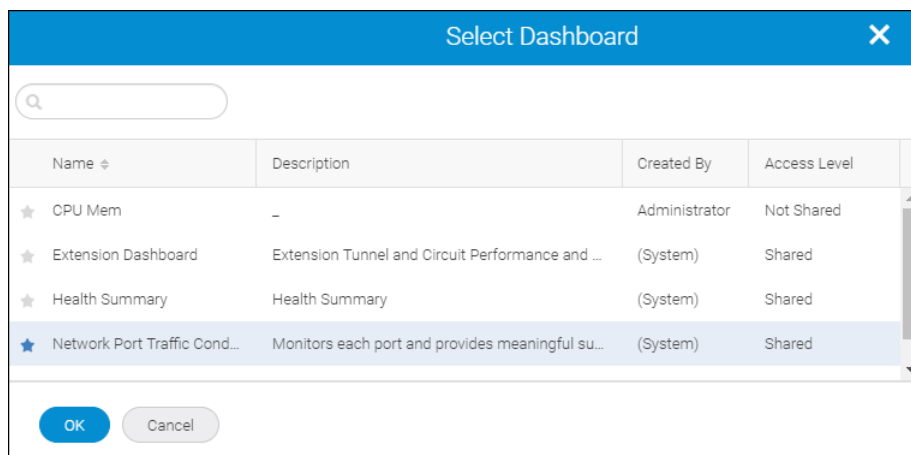
Changing the favorite dashboard can be very helpful when you are working repeatedly with a particular **Dashboard View** and you want it to display as the default view until you change it.

1. Click **Dashboard & Reports** in the navigation bar, and then click the **Select Dashboard** icon at the top right of the page.



The **Select Dashboard** dialog shows all the system-defined and user-defined (custom) dashboards.

2. Click the "star" next to the dashboard that you want to designate as the favorite dashboard, and click **OK**.



The dashboard with a blue-colored star now displays in the dashboard view and serves as the default view the next time you log in.

6.2.2 Creating a Dashboard Quickly

SANnav Management Portal allows you to quickly create custom dashboards using predefined widgets and a default layout. You can save the dashboard and access it at any time to monitor and troubleshoot various network objects such as fabrics, switches, and ports.

You can create a custom dashboard using two options:

- **Select Widgets:** Select from the available widgets using the system default layout and view.

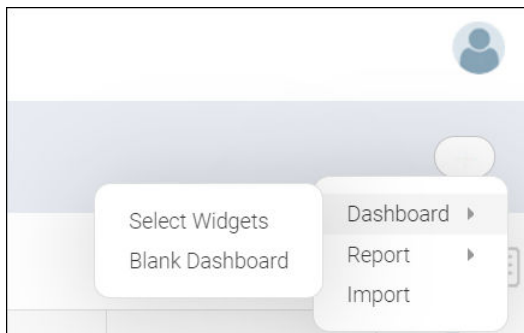
With this option, you can select several widgets at once and add them to the dashboard. The layout is three widgets in each row. Select this option if you do not care about the row arrangement of the widgets or if you want to quickly add many widgets at one time.

- **Blank Dashboard:** Start with a blank template to customize the layout, and then select widgets one at a time for each widget container and row.

With this option, you create an empty dashboard first and then add the widgets in the exact order and layout that you want. This option is preferred if you want to arrange widgets in a specific order. It might be less so if you have many widgets in the dashboard, because you would need to add them one at a time.

Perform the following steps to quickly create a dashboard using the **Select Widgets** option.

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
2. Click the **+** button on the right side of the subnavigation bar, and then select **Dashboard > Select Widgets**.



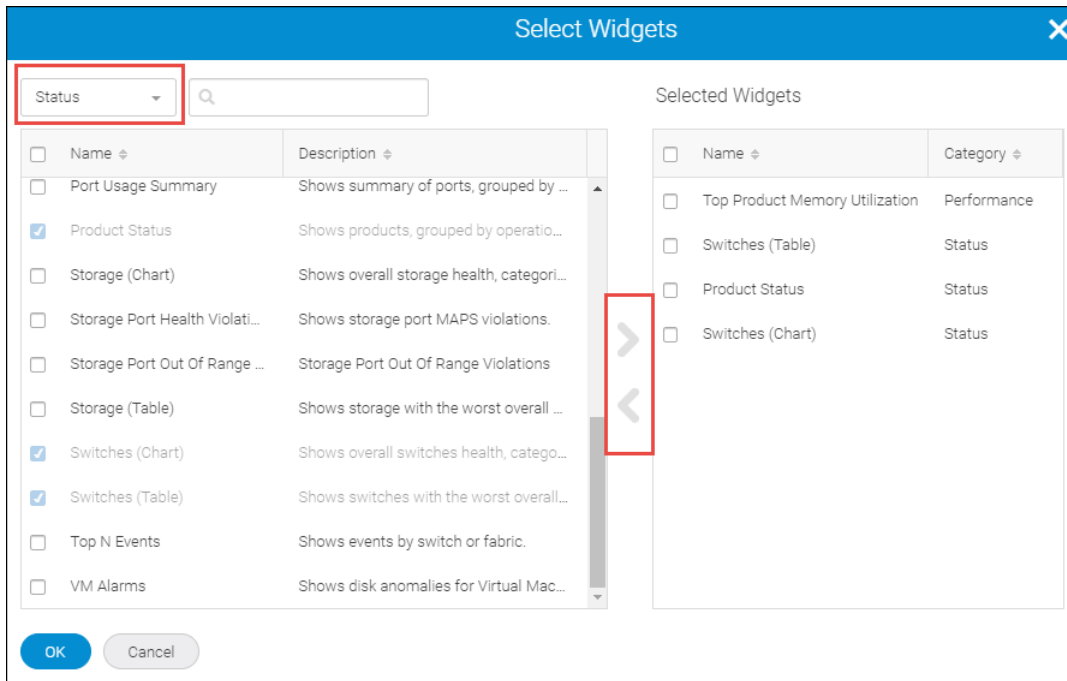
3. Check the widgets that you want in your custom dashboard, and click the right arrow to move them to the **Selected Widgets** list.

You can select from two categories of widgets: **Status** and **Performance**.

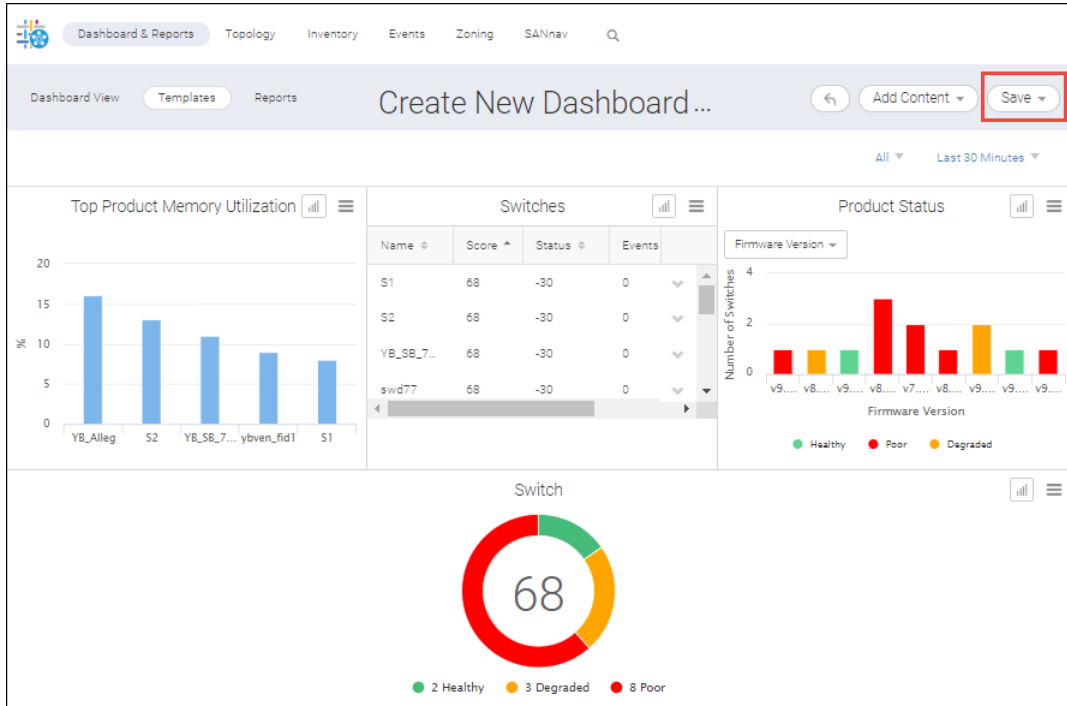
The order of the widgets in the **Selected Widgets** list is the order in which they are displayed in the dashboard, three widgets per row.

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. There is no re-sorting after the move.

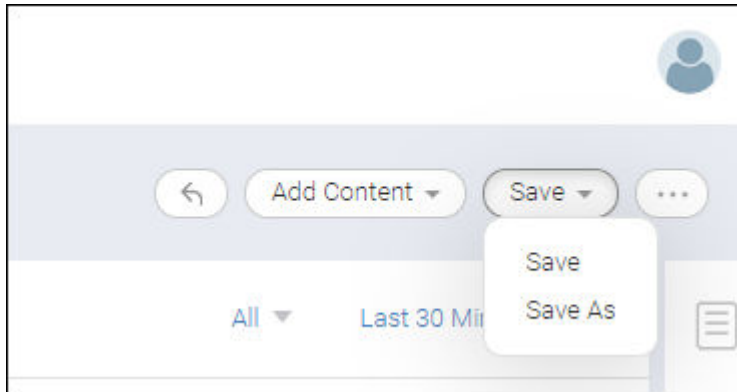
If you want the widgets in a particular order, select each widget separately, and then click the right arrow before selecting the next widget.



4. Click **OK** when you are finished adding widgets.
The **Create New Dashboard Template** page displays with the selected widgets.



5. Click **Save > Save** to preserve this dashboard.



In the **Save** dialog, select the **Shared** checkbox if you want to make the dashboard available to other SANnav users.

6.2.3 Creating a Dashboard with a Customized Layout

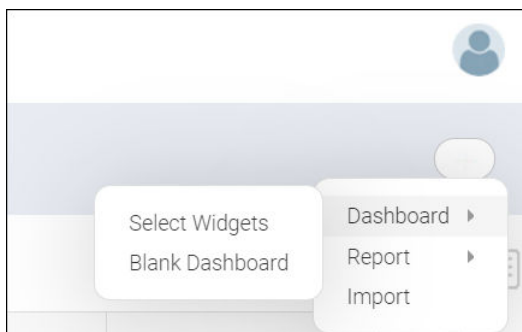
SANnav Management Portal provides the ability to create dashboards using customized layouts for the widgets. For example, you can provide more space for widgets that contain wide graphs or tables.

You can create a custom dashboard using two options:

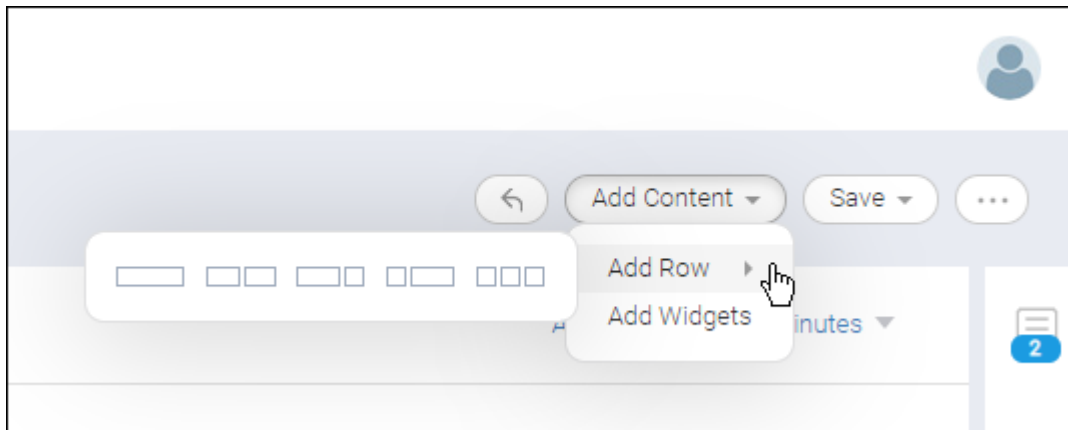
- **Select Widgets:** Select from the available widgets using the system default layout and view. With this option, you can select several widgets at once and add them to the dashboard. The layout is three widgets in each row. Select this option if you do not care about the row arrangement of the widgets or if you want to add many widgets at one time.
- **Blank Dashboard:** Start with a blank template and select widgets to customize the layout and view for each widget container and row. With this option, you can create an empty dashboard first and then add the widgets in the exact order and layout that you want. This option is preferred if you want to arrange widgets in a specific order. It might be less so if you have many widgets in the dashboard, because you would need to add them one at a time.

Perform the following steps to create a dashboard using the **Blank Dashboard** option.

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates**.
2. Click the **+** button in the subnavigation bar, and then select **Dashboard > Blank Dashboard**.



3. To add a row of widgets to the dashboard, select **Add Content > Add Row** and select one of the predefined row formats.

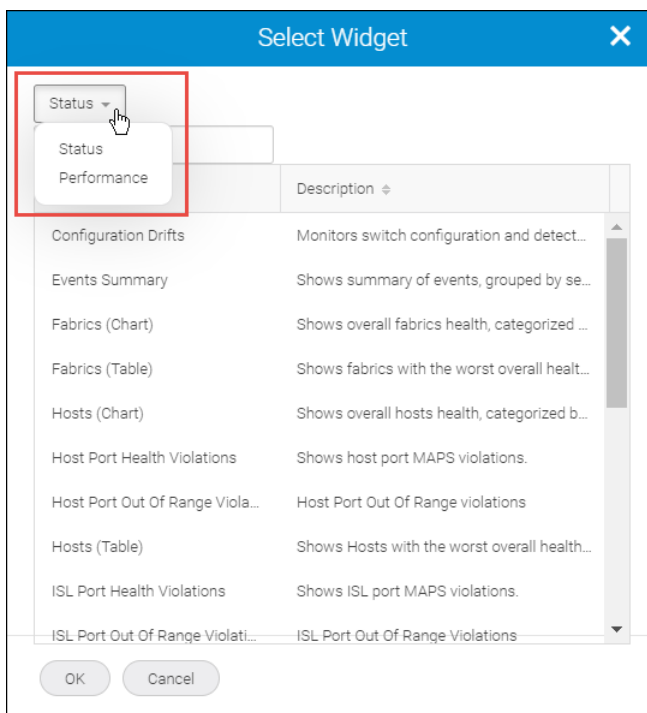


When selecting the row format, consider the type of widgets that you will be using. You might want to select a row format that allows more space for widgets that contain tables or charts.

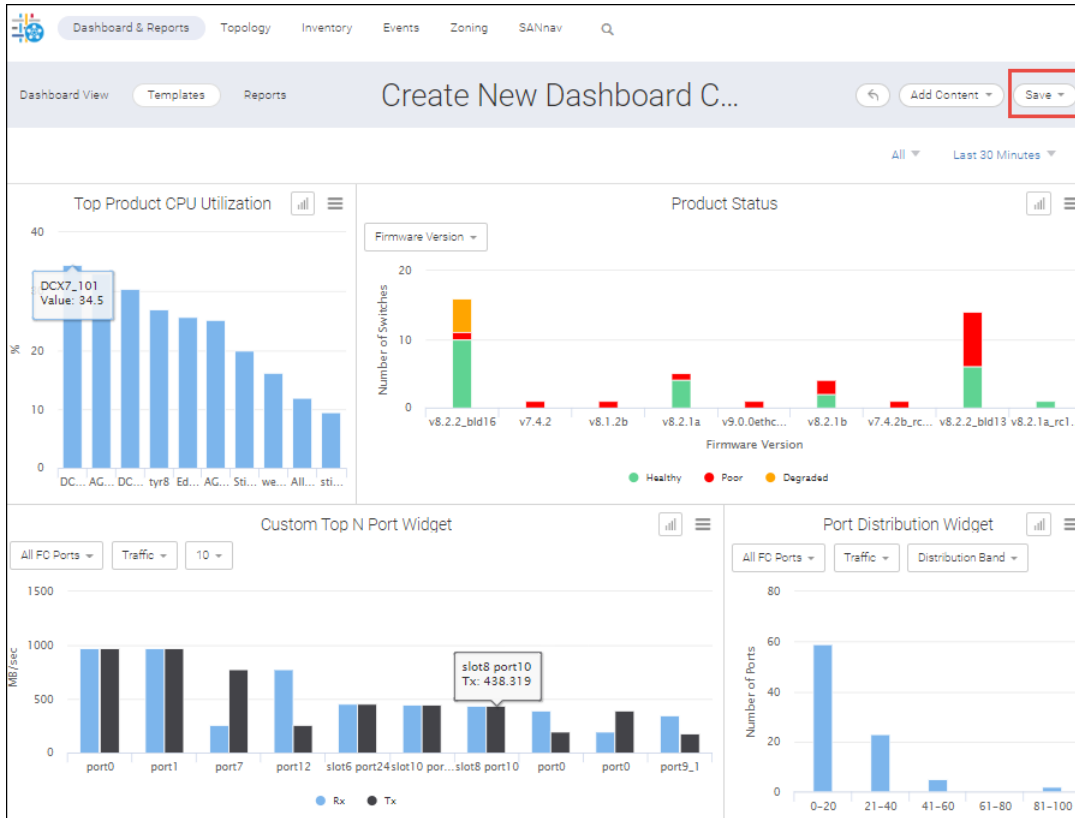
The new row is added with placeholders for the widgets.

4. Click the **+** button on the top-right of each placeholder to populate the placeholder with actual widget content.

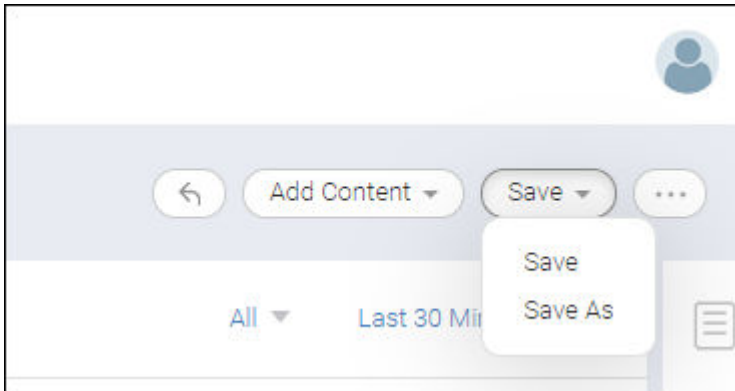
In the **Select Widget** dialog, you can choose from **Status** or **Performance** widgets.



5. Continue adding rows and widgets until you are done.



6. Click **Save** > **Save** to preserve this dashboard.



In the **Save** dialog, select the **Shared** checkbox if you want to make the dashboard available to other SANnav users.

6.2.4 Viewing Dashboards

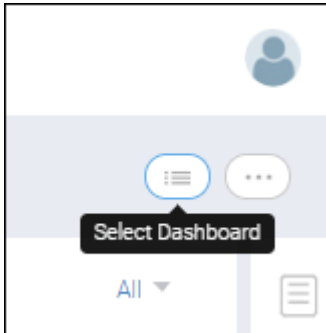
You can view both "static" and "dynamic" versions of an existing dashboard.

A dynamic dashboard provides real-time data for up to the last two hours, and it updates automatically.

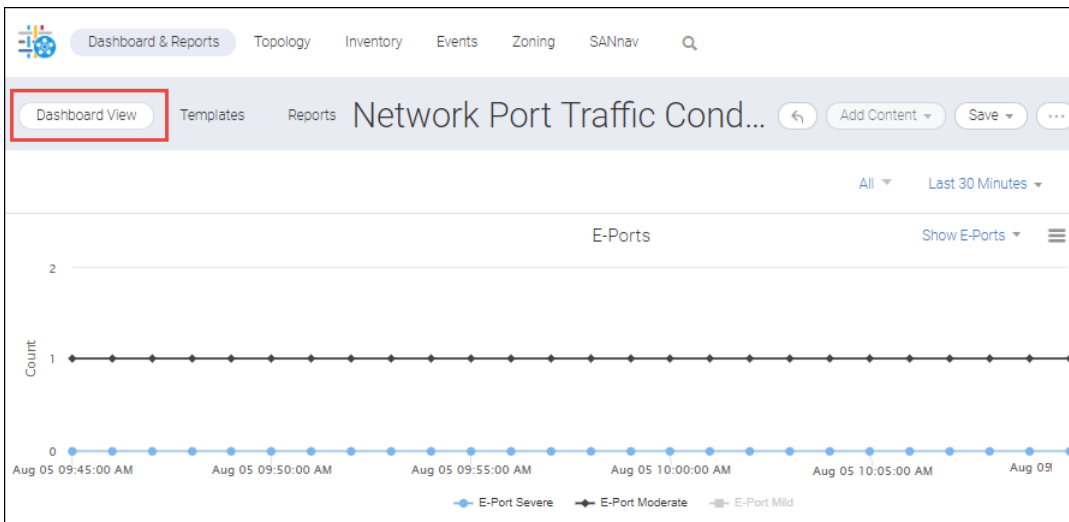
A static dashboard provides historic data for an indefinite period, but it does not automatically update.

An easy way to tell whether you are looking at a dynamic or static dashboard is to check the subnavigation bar. If the dashboard is shown in **Dashboard View**, it is a dynamic dashboard. If it is shown in **Templates**, it is a static dashboard.

1. To view a dynamic dashboard, click **Dashboard & Reports** in the navigation bar, and then click **Dashboard View**.
2. Click the **Select Dashboard** button in the upper right corner of the page, highlight the dashboard that you want to display, and click **OK**.

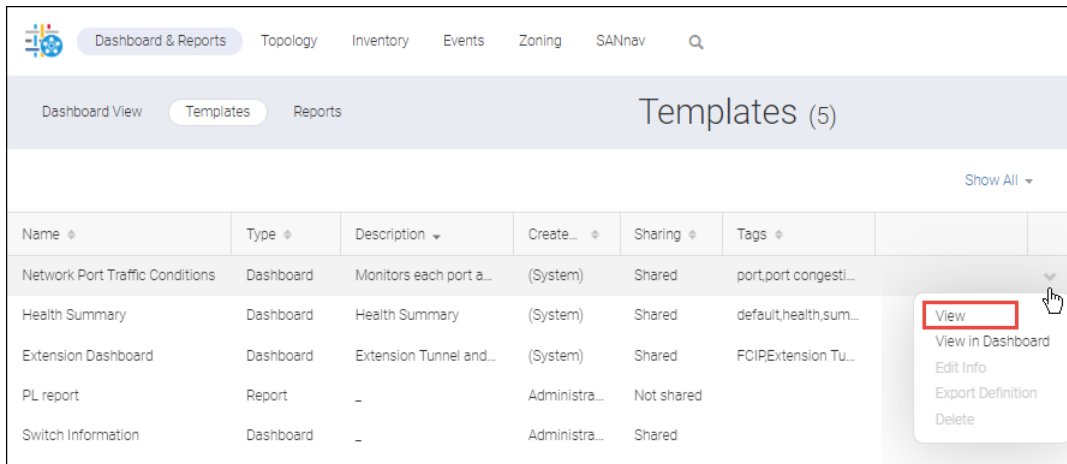


A dynamic view of the dashboard displays. Note that **Dashboard View** is selected in the navigation bar, which indicates that this is a dynamic dashboard.



3. To view a static dashboard, click **Dashboard & Reports** in the navigation bar, and then click **Templates**.

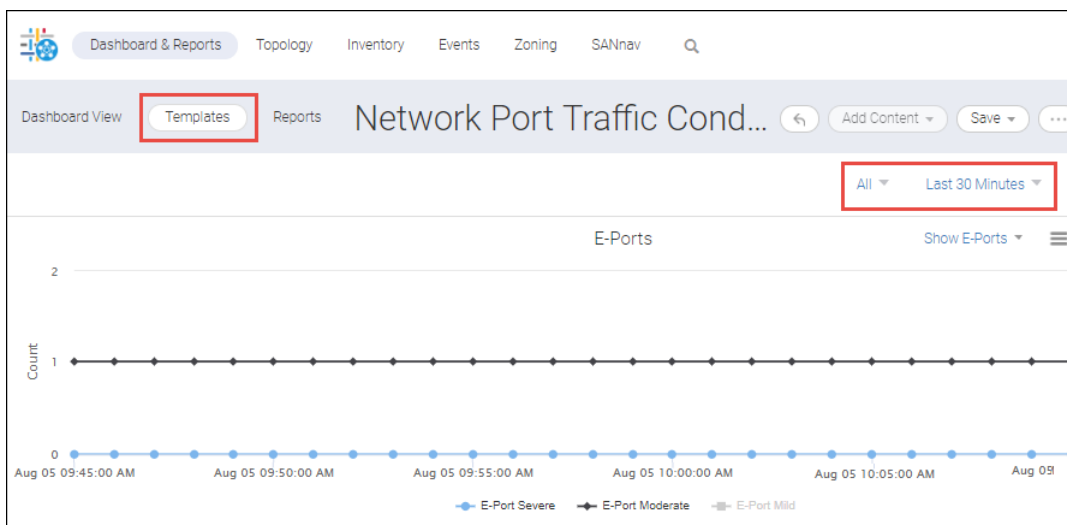
4. Locate the dashboard that you want to display, and click **View** on the action menu.



NOTE

Selecting **View** displays a static dashboard. Selecting **View in Dashboard** displays a dynamic dashboard.

A static view of the dashboard displays. The network scope is all fabrics, and the date range is the last 30 minutes, but you can change these settings. Note that **Templates** is selected in the navigation bar, which indicates that this is a static dashboard.



5. For both static and dynamic dashboards, you can change the network scope and date range. For dynamic dashboards, the maximum date range is two hours.

6.2.5 Exporting Dashboard Templates

You can create a custom dashboard template in one SANnav instance, export the template, and then import the template on another SANnav instance. In this way you can share a dashboard across different instances of SANnav.

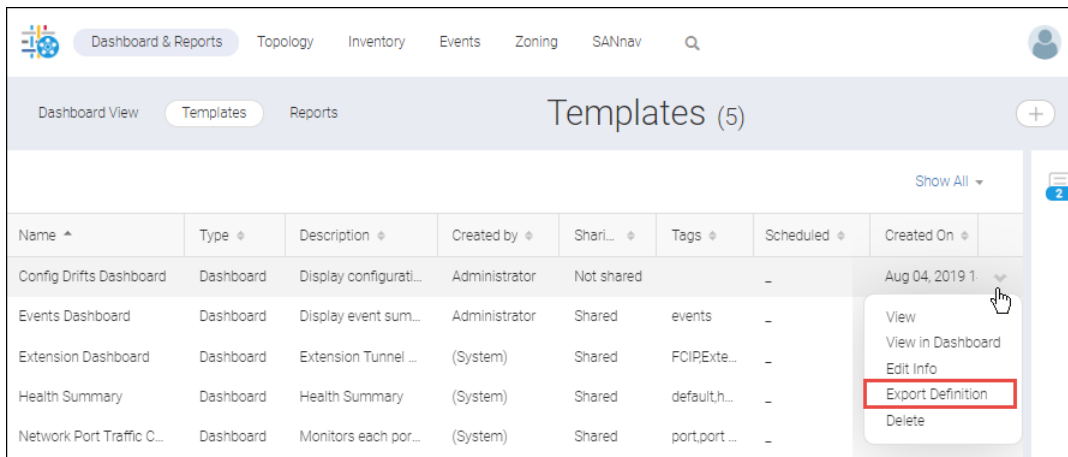
To export dashboards, you must have Dashboard privilege with read/write permission.

Note the following about exporting dashboards:

- You can export only custom dashboards. You cannot export the system default dashboards.
- Only the template definition is exported. The data is not exported.
- Exporting dashboards is not backward compatible. If you export a dashboard, you can import it only on a SANnav instance that is running the same SANnav version or higher.
- Making manual changes to the exported dashboard file and then importing it is not supported.

Perform the following steps to export a custom dashboard template.

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
2. Locate the custom dashboard that you want to export, and select **Export Definition** from the action menu.



The dashboard template definition is downloaded and saved to your local machine as a JSON file. You can now import this template to other SANnav instances.

6.2.6 Importing Dashboard Templates

You can import a SANnav dashboard that was previously exported from another SANnav instance. In this way you can share a dashboard across different instances of SANnav.

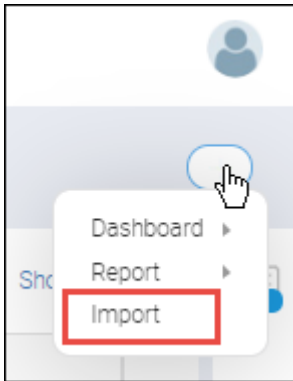
To import dashboards, you must have Dashboard privilege with read/write permission.

Note the following about importing dashboards:

- Importing dashboards is not backward compatible. If you export a dashboard, you can import it only on a SANnav instance that is running the same SANnav version or higher.
- Making manual changes to the exported dashboard file and then importing it is not supported.
- When you import a dashboard, be sure to give it a unique name for this SANnav instance.

Perform the following steps to import a dashboard template.

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
2. Click the **+** button on the right side of the subnavigation bar, and then select **Import**.



3. Browse to the location of the template file, and click **OK**.
The file must be a valid JSON file that was previously exported from SANnav.
4. In the **Import** dialog, optionally change the name of the dashboard and update the tags and description.
The dashboard name must be unique.
Select the **Shared** box if you want other SANnav users to be able to access this dashboard template.

 A screenshot of the 'Import' dialog box. The dialog has a blue header with the title 'Import' and a close button (X). Below the header, there are three input fields: 'Name' with the value 'Config Drifts Dashboard', 'Tags' (empty), and 'Description' with the value 'Display configuration drifts'. Below these fields is a checkbox labeled 'Shared' which is currently unchecked. At the bottom of the dialog, there are two buttons: 'Import' (blue) and 'Cancel' (grey).

5. Click **Import**.
The file is imported and displayed in the **Templates** page.
Note that the imported template defaults to a network scope of **All**, even if the template had a custom network scope when it was exported. You can apply a custom scope after the template is imported.

6.2.7 Sharing Dashboards and Reports with Other Users

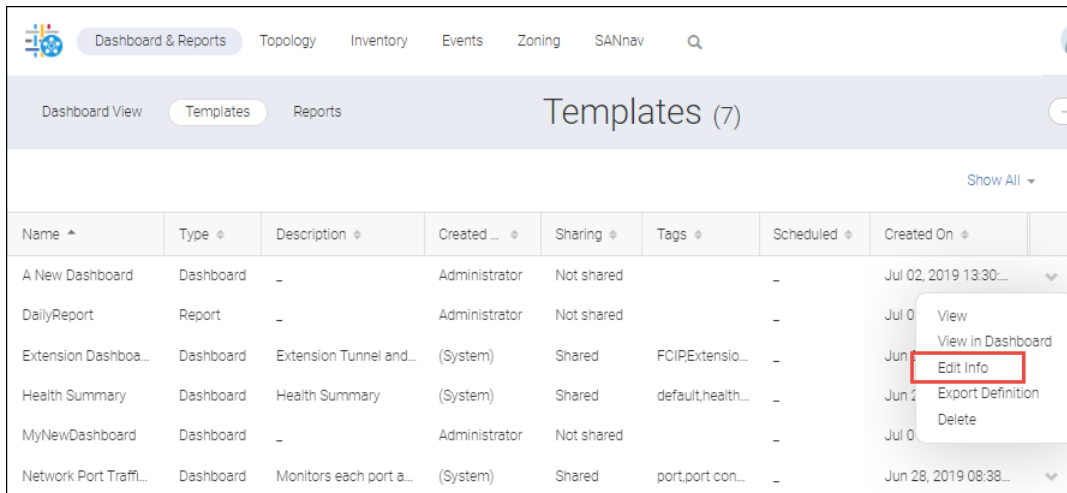
If you create a custom dashboard or a report, you can make it available for other users to access. If you do not share the dashboard or report, only you can see that dashboard or report.

You can share only dashboards and reports that you created. All system templates are shared by default.

To see your shared dashboards or reports, users must have Dashboard or Reports privilege. If users do not have these privileges, they cannot see the shared dashboards and reports.

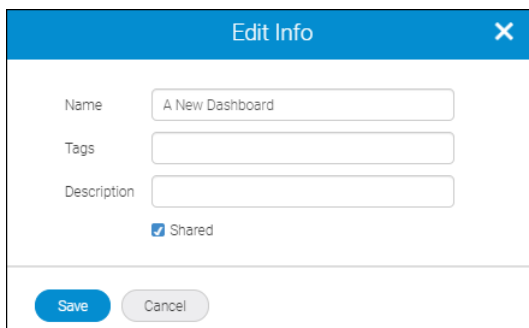
1. Select **Dashboard & Reports** on the navigation bar, and then select **Templates** in the subnavigation bar.

2. Locate the dashboard or report you want to share, and click **Edit Info** on the action menu.



Name ^	Type	Description	Created ...	Sharing	Tags	Scheduled	Created On
A New Dashboard	Dashboard	-	Administrator	Not shared	-	-	Jul 02, 2019 13:30...
DailyReport	Report	-	Administrator	Not shared	-	-	Jul 0...
Extension Dashboa...	Dashboard	Extension Tunnel and...	(System)	Shared	FCIPExtensio...	-	Jun...
Health Summary	Dashboard	Health Summary	(System)	Shared	default,health...	-	Jun...
MyNewDashboard	Dashboard	-	Administrator	Not shared	-	-	Jul 0...
Network Port Traffl...	Dashboard	Monitors each port a...	(System)	Shared	port,port con...	-	Jun 28, 2019 08:38...

3. Select the **Shared** option, and click **Save**.



Edit Info [X]

Name:

Tags:

Description:

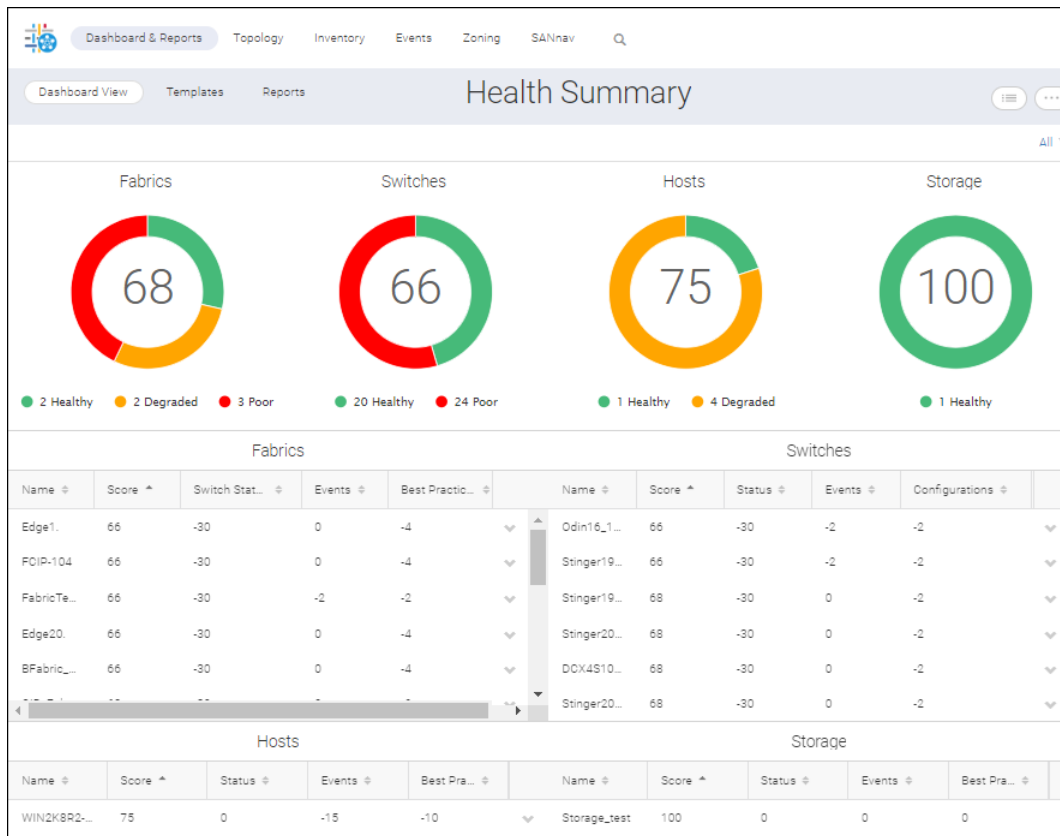
Shared

Now people who are logged in to this instance of SANnav can see the dashboard or report that you created.

6.2.8 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.

The **Health Summary** dashboard is the default "favorite" dashboard when you install SANnav.

Figure 9: Health Summary Dashboard

The **Health Summary** dashboard consists of eight widgets: Fabrics, Switches, Hosts, and Storage.

- 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 displayed in the center of the switch circle. In the above screen capture, the least healthy switch has a score of 66 and the least healthy fabric has a score of 68. The health score is computed based on various factors, such as status, events, and best practice violations.

The overall health is determined by the health score:

- If the health score is greater than 90, then the health is Healthy.
- If the health score is between 71 and 90, then the health is Degraded.
- If the health score is 70 or less, then the health is Poor.

The health score is computed based on various factors, such as status, events, and best-practice violations. You can customize the way in which the health score is computed.

The tabular widgets display details about the health score of each member. Click the down arrow at the right of each table entry to display additional actions that you can take, such as viewing inventory details, displaying properties, or (for switches) opening in Web Tools.

By default, all objects in your area of responsibility (AOR) are displayed. If you want to focus on a particular fabric, you can change the network scope by selecting a fabric from the drop-down list in the upper right corner of 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. You can, however, use these widgets in custom dashboards.

6.2.8.1 Customizing the Health Score for Managed Entities

The SANnav Management Portal **Health Summary** dashboard displays overall health scores for fabrics, switches, hosts, and storage. The ideal health score is 100, although certain factors may cause this score to decrease. You can customize which factors are taken into consideration and the number of points deducted for each violation.

In the Inventory and Dashboard, managed entities (fabrics, switches, hosts, and storage) are assigned an overall health status, which is determined by the health score for that entity.

- If the health score is greater than 90, then the health is Healthy.
- If the health score is between 71 and 90, then the health is Degraded.
- If the health score is 70 or less, then the health is Poor.

The health score is computed based on various factors, such as status, events, and best practice violations. You can customize the way the health score is computed.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Health Score Computation**.
2. Click one of the health factor lists to display detailed information about factors that contribute to reductions in the health score.

For example, the following screen capture shows how the health score for a fabric is computed.

Dashboard & Reports Topology Inventory Events Zoning SANnav

Health Score Computation

The below set of rules are used for computing health score for a managed entity such as Fabric, Switch, Host and Storage. Each rule carries a score that would be deducted from overall score for the entity when they are met. The score for each rule can be changed as long as it does not exceed the total score for the category the rule belongs to.

▼ Fabric Health Factors

- Member Switch Health 30
 - Any switch health Degraded Results 10
 - Any switch health in Poor state results 30
- Important Incidents 50
 - Link down 2
 - FPI violations 2
 - FCIP Tunnel Link - any circuit in offline state 1
 - Congestion state medium for F-Ports 2
- SAN Best Practices 20
 - Any Fabric level Policy check failure 2
 - Missing Redundant Paths(ISLs)
 - FCR Backbone fabrics - Backbone switches are not duplicated
 - EHT settings - Deviation from recommended settings(220ms for edge)
 - Default Zoning - All Access
 - Zone DB size > 90 %

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 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 each included major category 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.

Important Incidents 50
 Link down 10
 FPI violations
 FCIP Tunnel Lin
 Congestion state medium for F-Ports 55

The score for each rule should not exceed the total score for the category the rule belongs to.

Note that for fabric health factors, SAN Best Practices category, most of the rules do not allow you to specify the number of points to be deducted. You can select only whether to include these rules in the health score computation. For these rules, the number of points is fixed at 2.

SAN Best Practices 20
 Any Fabric level Policy check failure 2
 Missing Redundant Paths(ISLs)
 FCR Backbone fabrics - Backbone switches are not duplicated
 EHT settings - Deviation from recommended settings(220ms for edge)
 Default Zoning - All Access
 Zone DB size > 90 %

6. Click **Save** when you are finished making changes.

At any time you can click **Restore Default Settings** to go back to the original settings.

The next time the health score is computed, the **Health Summary** dashboard will reflect the new computations. The health score is computed approximately every 15 minutes.

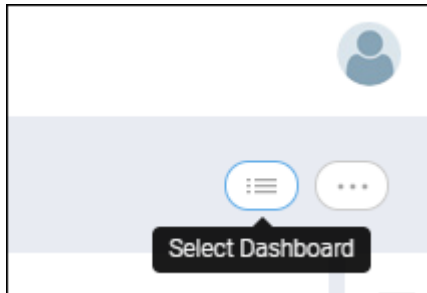
6.2.8.2 Monitoring SAN Health and Status Daily

It is recommended that you periodically check the overall health of the SAN. If you notice problem areas, you can drill down to get additional information.

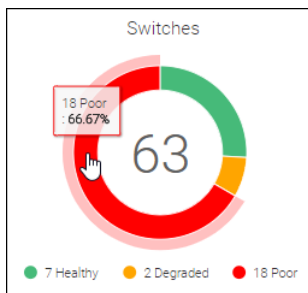
1. Log in to SANnav Management Portal, and click **Dashboard & Reports** in the navigation bar.

The default dashboard (the dashboard designated as the "favorite" dashboard) displays.

If the **Health Summary** dashboard is not the default dashboard, click the **Select Dashboard** icon at the top right of the page, click **Health Summary** in the table, and click **OK**.



2. 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.



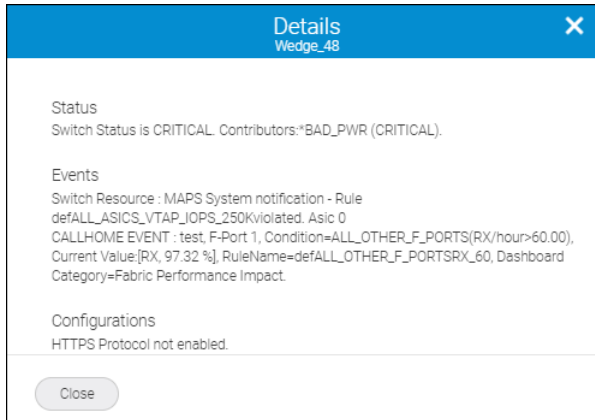
A table displays the objects with the associated score, and shows how many points were deducted for each category. This table displays the same information as the table widgets in the dashboard, except that you see only the entries with the associated score. For example, the following screen capture shows only the switches with Poor health.

Switch Health: 18 Poor					
Name	Score	Status	Events	Configurations	
Wedge_49	63	-30	-7	-2	▼
Wedge_75	68	-30	-	-2	▼
AMP_25_FID_101	68	-30	-	-2	▼
Skyboit_54_FID_100	68	-30	-	-2	▼
Wedge_76_FID_10	68	-30	-	-2	▼

For the first switch in this example, 30 points were deducted for switch status factors, 7 points were deducted for events factors, and 2 points were deducted for configuration factors.

3. 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.

The action menu is available in both the dialog and in the tabular widgets of the **Health Summary** dashboard.



4. Depending on the causes for the health score deductions, select other options from the action menu to drill down for more details.

Switches					
Name	Score	Status	Events	Configurations	
Wedge_75	68	-30	-	-2	
sw0	68	-30	-	-2	Investigate
Wedge_75...	68	-30	-	-2	Show Details
AMP_2	68	-30	-	-2	Show Properties
AMP_25_FI...	68	-30	-	-2	Show in Topology
Skybolt_54...	68	-30	-	-2	View Inventory Details
Wedge_76	68	-30	-	-2	Open in WebTools

For example, select **Investigate** to look into performance issues, or select **View Inventory Details** to look at port optics, set maintenance mode, or disable the switch.

The **Investigate** and **Open in Web Tools** options are available only for switches.

6.2.8.3 Factors Contributing to the Overall Health Score

For the **Health Summary** dashboard, various factors are considered when determining the overall health score for fabrics, switches, hosts, and storage.

Health scores start at 100, and points are deducted for various predefined factors.

The following tables list the factors that go into computing the health score for fabrics, switches, hosts, and storage, and the default number of points deducted from the score. You can customize which factors are taken into consideration and the number of points deducted for each violation.

Table 16: Fabric Health Score Factors and Default Points Deducted

General Category	Factor	Points Deducted
Member Switch Health (Maximum 30 points deducted)	Any switch in the fabric having a status of Degraded.	10
	Any switch in the fabric having a status of Poor.	30

Table 16: Fabric Health Score Factors and Default Points Deducted (Continued)

General Category	Factor	Points Deducted
Important Incidents (Maximum 50 points deducted)	A link went down without coming back up.	2
	Fabric Performance Impact (FPI) violations.	2
	For an FCIP tunnel, any circuit in an offline state.	1
	Congestion state of Medium for F_Ports.	2
SAN Best Practices (Maximum 20 points deducted)	Any fabric-level configuration policy check failure.	2
	Missing redundant ISLs between switches.	2
	For FCR backbone fabrics, no redundant IFL connections from each backbone switch to the edge fabrics.	2
	Edge Hold Time (EHT) > 220 ms for an edge switch. This check is performed only for switches running Fabric OS 8.2.1 and higher.	2
	Default zoning set to All Access.	2
	Zoning database size > 90% of the maximum allowed size.	2

Table 17: Switch Health Score Factors and Default Points Deducted

General Category	Factor	Points Deducted
Switch Status (Maximum 30 points deducted)	Switch status Marginal.	10
	Switch status Down.	30
	Switch status unknown.	10
Important Incidents (Maximum 60 points deducted)	Call Home events originated from the switch.	5
	MAPS violations: <ul style="list-style-type: none"> ■ Port health ■ Fabric state change ■ FRU health ■ Security health ■ Switch resource monitoring measures ■ FCIP Extension tunnel measures ■ Traffic measures ■ Backend port measures 	2 for each category. The score is reduced one time per category, even if multiple violations for that category occur.
	Events, traps, or syslogs that have been marked as "special" in the event policy, and have not been acknowledged.	2
Configuration (Maximum 10 points deducted)	COMPASS configuration drifts.	10
	HTTPS is not enabled.	2

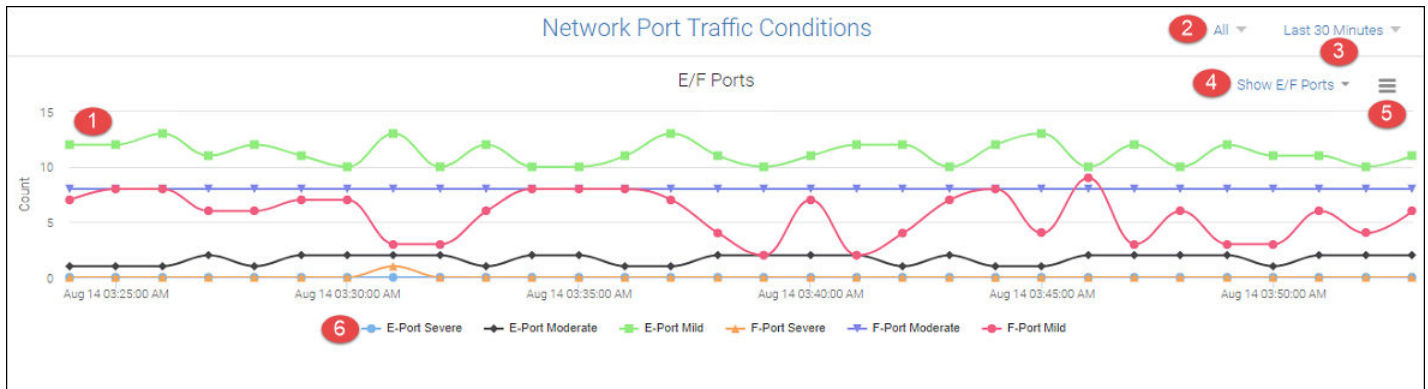
Table 18: Host and Storage Health Score Factors and Default Points Deducted

General Category	Factor	Points Deducted
Device Status (Maximum 30 points deducted)	One or more device ports are offline.	30
Threshold Events (Maximum 60 points deducted)	MAPS violations on F_Ports.	5
	FPI violations or error events on connected F_Ports.	10
	Congestion state of Medium for F_Ports.	2
	Virtual machine (VM) alarms for servers (when vCenter integration is available).	2
Best Practices (Maximum 10 points deducted)	Missing redundant paths between host and zoned storage.	10
	Host not zoned following best practices: <ul style="list-style-type: none"> ■ A zone should have at most one host ■ A peer zone should have the single host as a principle member 	1
	Fan-in ratio to storage exceeds 10:1.	2

6.2.9 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 displays factors that are contributing to the congestion to help you troubleshoot its cause.

As shown in the following illustration, this dashboard provides a graphical display showing the number of E_Ports, EX_Ports, and F_Ports in severe, moderate, and mild congestion severity states over time. The congestion counts are computed once every minute and displayed for the last 30 minutes, 1 hour, or a maximum of 2 hours.

Figure 10: Network Port Traffic Conditions Dashboard

1. Graphs showing port types in various congestion severity states
2. Network scope
3. Date range drop-down
4. Show ports drop-down
5. Hamburger icon for selecting the **Troubleshooting Mode** page
6. Port type and severity state selectors

The **Network Port Traffic Conditions** dashboard is supported on Gen 6 or higher platforms operating with Fabric OS 8.2.1 or greater with MAPS enabled.

Congestion is a network traffic condition that occurs when frames are entering a fabric faster than they are exiting 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).

In the graphical display, each port type (F_Ports, E_Ports, and EX_Ports) and severity state (mild, moderate, and severe) displays as a different colored line graph. Hover your cursor over data points on the graph to display the number of ports detected in a severity state for that time interval. The current time interval configured for monitoring ports is displayed on the **Date Range** drop-down at the top right corner of the page.

To modify the graph display, use the following features:

- Add and remove graphs for different port types and severity levels by clicking a port type and severity state selector below the graph display. Each selector is color-keyed to a line graph.
 - Click a fully-visible selector to deselect it and remove the graph.
 - Click a partially-visible selector to select it and add the graph.

NOTE

Congestion severity for EX_Ports will display using the E-Port Severe, E-Port Moderate, and E-Port Mild selectors.

- Add and remove graphs for the port types only (F_Ports, E_Ports, or E_Ports and F_Ports), by clicking the **Show Ports** drop-down at the top right corner of the **Network Port Traffic Conditions** graph display area.
- Select fabrics for congestion monitoring by clicking the **Network Scope** icon in the top-right corner of the page. Select **All** discovered fabrics or specific discovered fabrics.
- Select a time or date interval for monitoring ports for congestion severity states by clicking the **Date Range** drop-down at the top right corner of the page. Depending on where you are viewing the **Network Port Traffic Conditions** dashboard, selectable time intervals vary as follows:
 - If viewing the dashboard in the **Dashboard View** (dynamic view), selecting the drop-down allows you to select the last 30 minutes, 1-hour, or 2-hour time periods for data display.
 - If viewing the dashboard in the **Templates** tab (static view), selecting the drop-down displays the **Select Date Range** dialog, where you can select the last 30 minutes or hour, day, and more extended time periods.

For more information on metrics used to identify congested ports, troubleshooting congested ports, and identifying the causes and solutions for congestion, see the following:

- For detailed monitoring and display of port metrics used to determine the congestion severity states in the congested ports line graphs, display the **Troubleshooting Mode** page. To display this page, click the hamburger icon at the top right corner of the **Network Port Traffic Conditions** graphical display and select **Troubleshoot**. See [Troubleshooting Mode for Network Port Traffic Conditions Dashboard](#) for details on this page.
- For details on the mild, moderate, and severe states used to identify port congestion severity in this dashboard, see [Congestion Severity States](#).
- For complete information and procedures on troubleshooting port and fabric congestion, refer to the *Brocade Fabric Congestion Troubleshooting Guide*.

6.2.9.1 Troubleshooting Mode for Network Port Traffic Conditions Dashboard

The **Troubleshooting Mode** page provides details on the ports and the metrics that are monitored to determine the port congestion severity states as displayed in the **Network Port Traffic Conditions** dashboard. This detail should help you identify the cause and source of congestion issues.

Click the hamburger icon located on the top right of the **Network Port Traffic Conditions** dashboard graphical display, and select **Troubleshoot** to display the **Troubleshooting Mode** page.

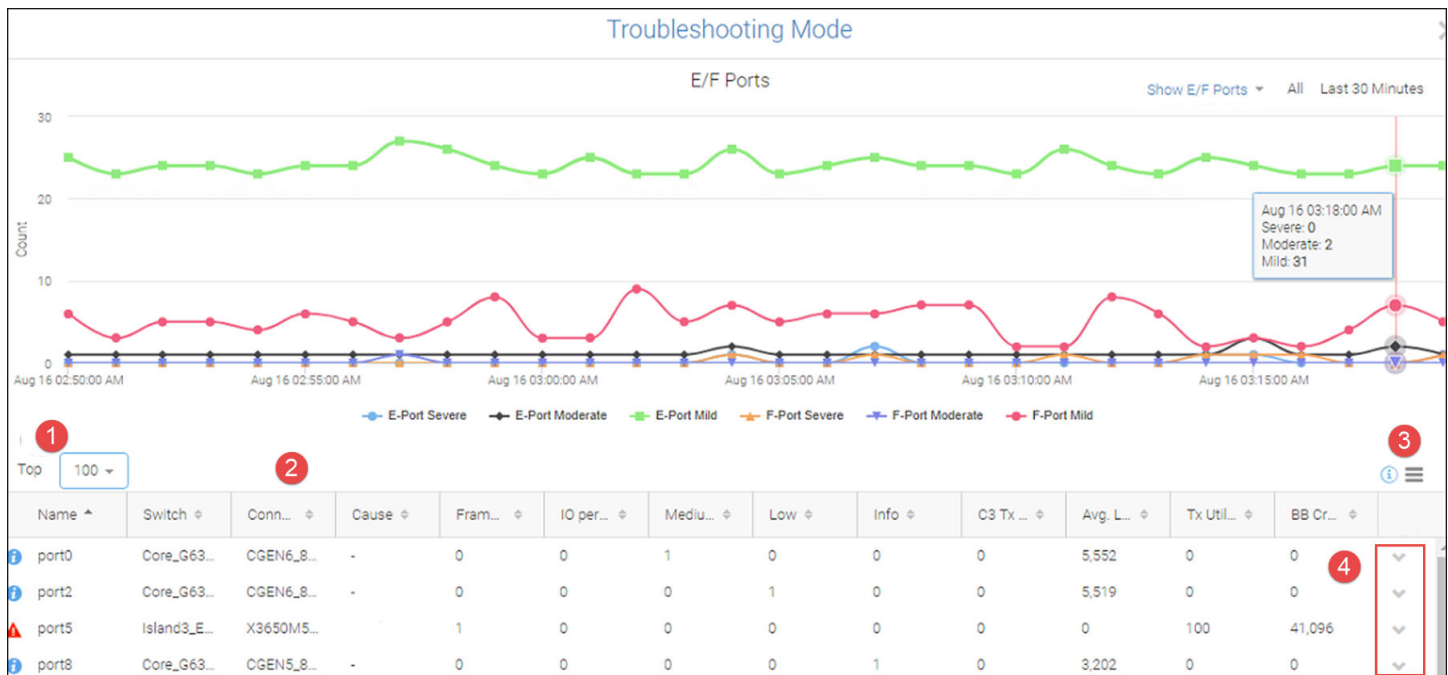
The **Troubleshooting Mode** page displays a table below the **Network Port Traffic Conditions** dashboard with complete information on the congested ports, including the metrics used to determine their congestion states. Clicking on a data point on a line graph in the dashboard refreshes data in the metrics table for that time interval.

The network scope and date range indicators at the top right corner of the page display the values that were specified in the **Network Port Traffic Conditions** dashboard when Troubleshooting Mode was entered.

To modify the display of the table of congestion metrics below the line graphs, use the following features:

- Click any point along a line graph to update data in the table for that data point.
- Click the **Top** drop-down above the table and select 10, 50, or 100 rows to display in the table.
- Select **Columns** from the hamburger icon on the top right side of metrics table to add or remove data columns from the table.

Figure 11: Troubleshooting Mode Page



1. Top drop-down
2. Table of port information and congestion metrics
3. Hamburger icon for adding or removing columns in the metrics table
4. Action menu selector (**Investigate**)

Port Information and Congestion Metrics Table

In the table, icons next to the port name indicate the congestion severity state as follows:

- ▲—severe
- ▲—moderate
- ●—mild

The **Cause** column indicates the probable root cause of congestion, such as a credit-stalled device connected to the port or an unknown issue. The cause is not displayed for E_ports or for ports in the "mild" congestion category.

A credit-stalled device is a misbehaving device that stops returning R_RDY signals (buffer credits) promptly to the switch to facilitate transmitting additional frames to that device. This 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.

The following table describes the port conditions that must occur for a specific cause to display in the congestion metrics.

Table 19: Port Conditions that Determine Congestion Cause

Cause	Port Condition
Credit Stalled Device	Either Frame Loss, IO Perf impact, or both are greater than 0.
Unknown	The port condition for Credit Stalled Device has not been met, but congestion is occurring.

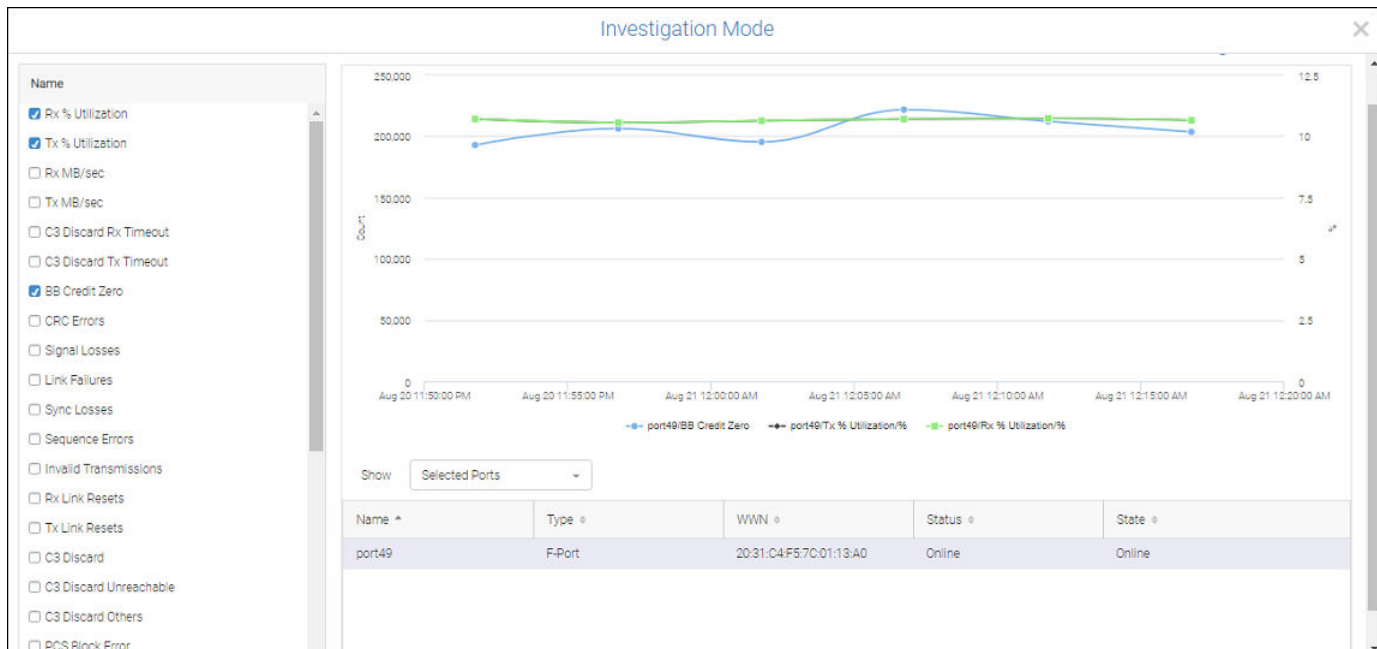
NOTE

If you receive Monitoring and Alerting Policy Suite (MAPS) alerts indicating excessive CRC errors or CRC errors exceeding set threshold limits, suspect a faulty port transceiver or cable. For more details, refer to the *Brocade Fabric OS MAPS User Guide* and the *Brocade Fabric Congestion Troubleshooting Guide*.

The port information table also contains the following congestion metrics.

Metric	Description
Frame Loss IO Perf Impact Medium Low Info	The number of times the port was in the these congested port states. See Congestion Severity States for more information.
C3 Tx Timeout	The number of class 3 (C3) frame transmit timeouts. Transmit (tx) timeouts on an F_Port indicates that the F_Port is the source of congestion and is causing back pressure. Fabric Performance Impact (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 at F_Ports that are connected to credit-stalled devices. Class 3 transmission timeout errors (C3TXTO) on a port will trigger a Frame Loss state for the port.
C3 Rx Timeout	The number of class 3 (C3) frame receive timeouts. C3 receive timeout errors (C3RXTO) on a port will trigger a Frame Loss state for the port. Receive timeouts on an F_Port indicate that frames received on the port are being discarded because of back pressure from upstream ports (ISLs or other devices).
Avg. Latency (ms)	Average time that a frame is in the port transmit queue before being transmitted. Increasing latency at an ISL port is an indication of a downstream congestion caused by oversubscription or a credit-stalled device.
Tx Utilization (%)	The average percentage of link capacity used when transmitting traffic. High bandwidth utilization can indicate a source of oversubscription that can lead to congestion.
Rx Utilization (%)	The average percentage of link capacity used when receiving traffic. High bandwidth utilization can indicate a source of oversubscription that can lead to congestion.
BB Credit Zero (Count)	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 time period and there is a frame waiting in the queue of the port or the 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 a downstream congestion caused by oversubscription or a credit-stalled device.

To perform additional investigation, click the down arrow at the end of a port row to display an action menu, and then select **Investigate** to display the **Investigation Mode** page for the port. Using this page, you can display more detailed data selected port congestion metrics in configurable time ranges of up to 2 hours with 1-minute granularity.

Figure 12: Investigation Mode Page

By default, the **Investigation Mode** page displays graphs showing counts of the following congestion metrics over time:

- BB credit zero
- Tx utilization
- Rx utilization

For more information on using the **Investigation Mode** page, see [Using Investigation Mode](#).

6.2.9.2 Congestion Severity States

The line graphs in the **Network Port Traffic Conditions** dashboard and **Troubleshooting Mode** page 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 used by Fabric Performance Impact (FPI), a Brocade Monitoring and Alerting Policy Suite (MAPS) feature, to monitor congestion. .

The following table compares the severity states identified in the dashboard with congestion states and metrics used to determine these states for the MAPS congestion dashboard and MAPS alerts

Congestion Severity States in Dashboard	MAPS Congestion Severity States	Metrics Used to Determine MAPS Severity States
Severe	Frame Loss	This is the highest congestion severity state. In this state, MAPS FPI has generated a frame loss alert for the port. A Frame Loss state indicates a severe level of latency — frame timeouts either have already occurred or are very likely to occur.
Moderate	I/O Perf Impact	This is the second highest congestion severity state. In this state, MAPS FPI has generated a performance impact alert for the port. This state can occur if the port does not have credit for a substantial period time or if frames are transmitted with delay. A port or device in this state can negatively impact overall network performance.

Congestion Severity States in Dashboard	MAPS Congestion Severity States	Metrics Used to Determine MAPS Severity States
Mild	Medium	A port is in a medium congestion severity state if any or both of the following conditions are met: <ul style="list-style-type: none"> ■ Transmit Queue Latency (TQL) is 5 or more milliseconds, but less than 10 milliseconds. ■ Credit zero statistics indicates 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: <ul style="list-style-type: none"> ■ If the TQL is 3 or more milliseconds but less than 5 milliseconds. ■ If the credit zero statistics indicates 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: <ul style="list-style-type: none"> ■ If the TQL is 1 or more milliseconds but less than 3 milliseconds. ■ If the credit zero statistics indicates a latency of 10 or more milliseconds but less than 50 milliseconds in 1 second.

For more information on how MAPS congested states are determined for a port, refer to the *Brocade Fabric OS MAPS User Guide*.

6.3 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.

To generate reports, first you create report templates, which define the status and performance widgets that comprise the report as well as the network scope, date range, and other filters. 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 ZIP 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.

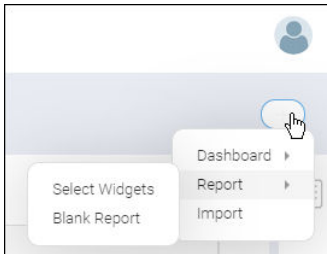
6.3.1 Creating a Report Template

When you want to generate reports, you first create a report template. The report template specifies the widgets to go in the report, as well as the network scope, date range, and specific filters.

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.

The **Templates** page lists all dashboard and reports templates.

- Click the **+** button on the right side of the subnavigation bar, and select **Report > Select Widgets**.



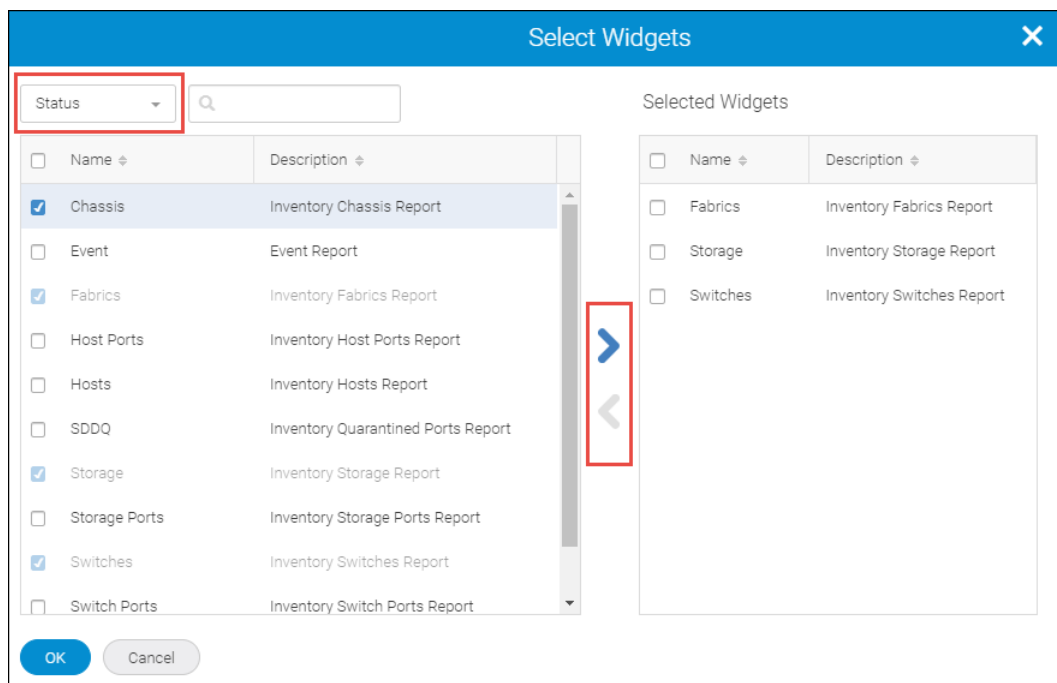
- Select the widgets you want in your report, and click the right arrow to move them to the **Selected Widgets** list.

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 displayed 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. There is no re-sorting 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.



- Click **OK** when you are finished adding widgets.

The template displays with placeholders for each widget.

- Add filters to the report template by clicking the **+** button on the left side of the filter bar.

The filters apply to all widgets in the template. The generated report contains data for only those objects that meet the filter requirements.

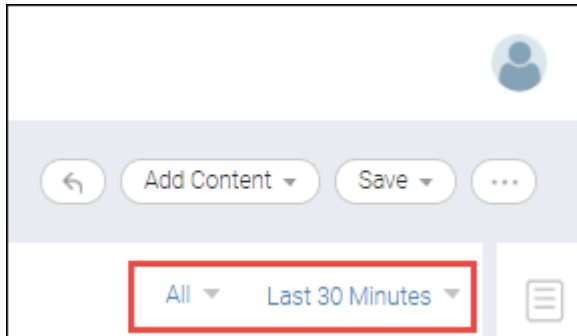
NOTE

Filters are not applicable to circuit or extension widgets.

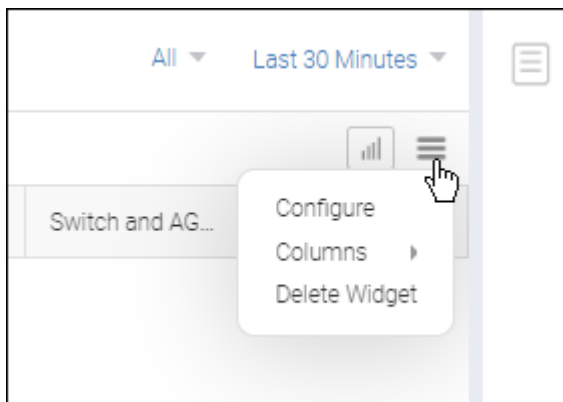
NOTE

Although there is no restriction on the number of filters that can be added or applied as part of the report template, it is recommended that you follow this guideline: two parameter conditions within a filter and two filters within a report.

6. Customize the network scope and date range using the drop-down lists on the right side of the filter bar.



7. Customize the widgets.



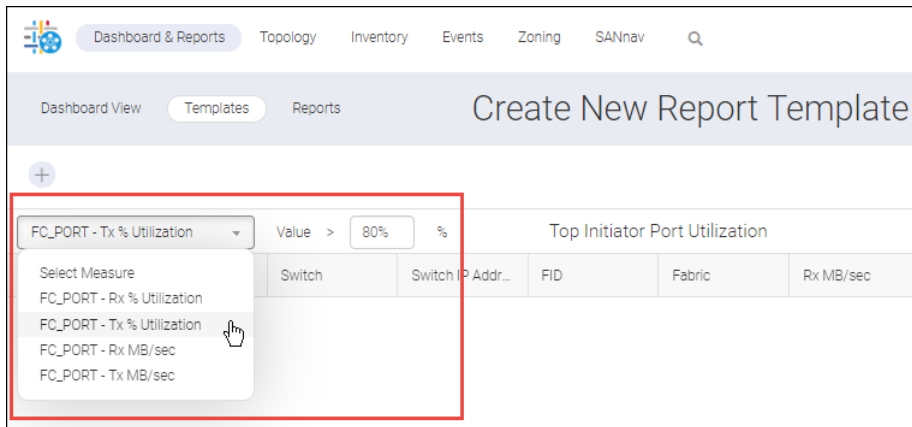
Click the hamburger icon for each widget to do the following:

- Change the name of the widget in the report (**Configure** option).
- Add or delete columns for tabular widgets.
- Delete the widget from the report.

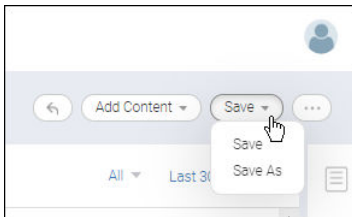
You cannot rearrange the widgets in the report, but you can add widgets to the top and bottom of the report by clicking **Add Content > Add Widgets** in the subnavigation bar.

8. Add measures to utilization widgets.

Some of the widgets require additional customization. For example, some of the top utilization widgets require that you select a measure and a utilization percentage.



9. Click either **Save > Save** or **Save > Save As** to save the report template.



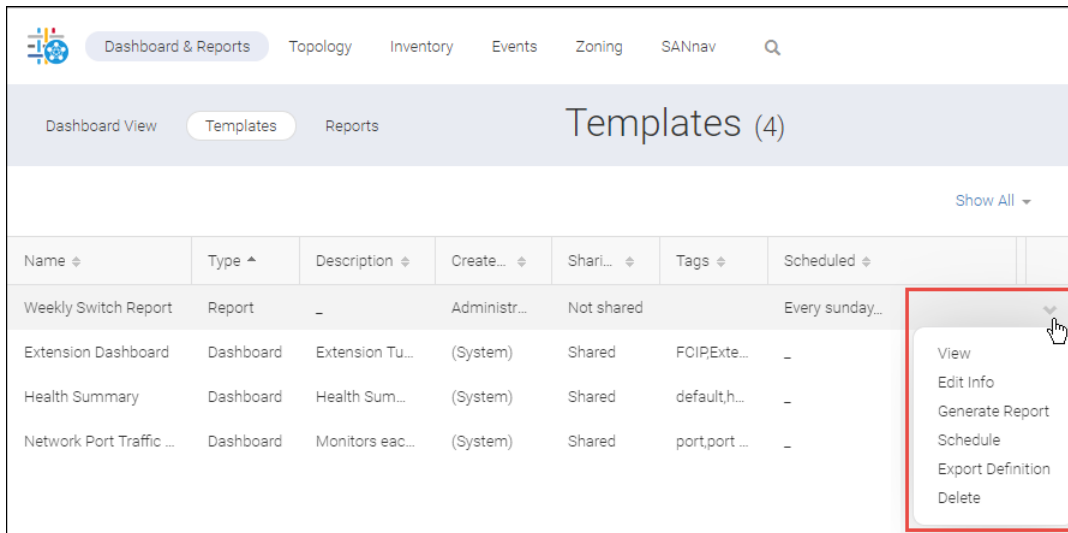
When you save the template, you must supply a name for the template, as well as optional tags and description. The template name can contain alphanumeric and special characters except for the following special characters:

/ \ : * ? % " < > | '

6.3.2 Editing a Report Template

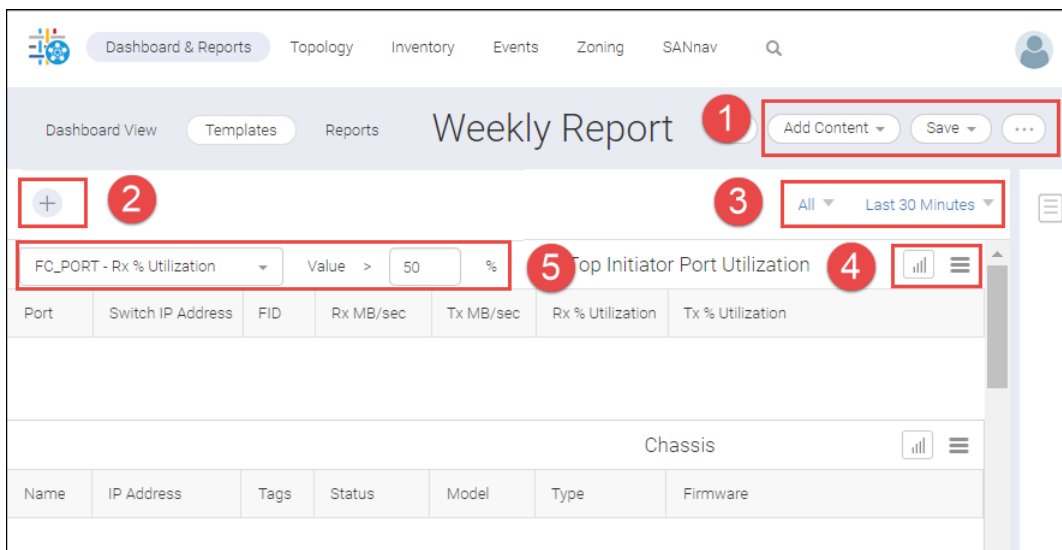
After you create a report in SANnav, you might want to change it or create another, similar report. You can edit the template and replace it or save it as a new copy.

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
The **Templates** page lists all dashboard and reports templates.
2. To edit the template name, tags, description, and sharing, locate the report template you want to modify, and from the action menu on the right side of the table, select **Edit Info**.



The **Edit Info** dialog allows you to change the name of the template, as well as tags and description. From here you can also designate whether the template is to be shared with other SANnav administrators.

- To edit the widgets in the template, from the action menu, click **View** to display the widget layout.



- Add widgets and save the template. The more button (⋮) provides additional options, including updating the schedule and exporting the template definition.
 - Add filters for the report.
 - Update the network scope and date range.
 - Replace or delete the current widget, change the widget name, and customize the displayed columns for the widget.
 - Additional configuration for some widgets.
- Make any changes to the template.
In the above screen capture, items 1, 2, and 3 affect the entire report. Items 4 and 5 affect a specific widget.
 - Click **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.

6.3.3 Scheduling a Report

In SANnav, you can schedule a report to run later. You can create up to four schedules for a single report.

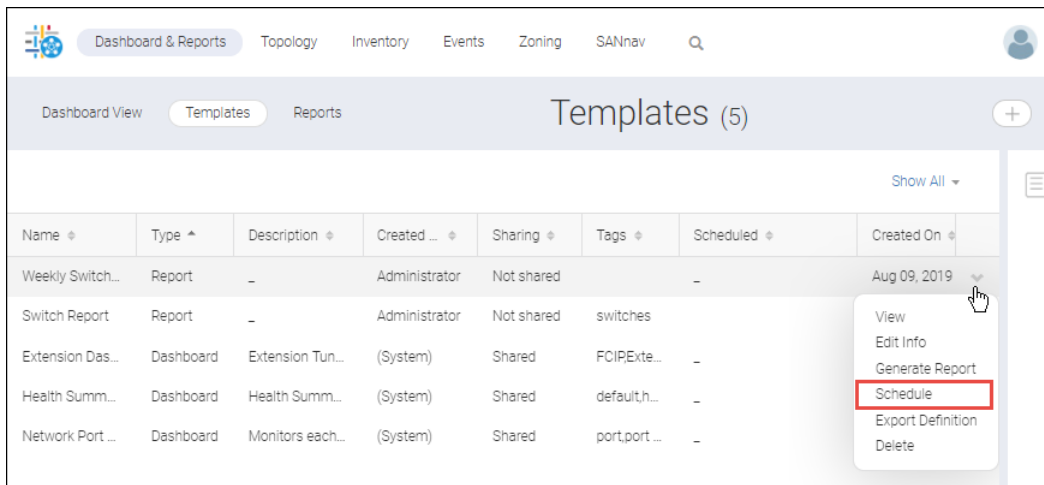
If you want to specify an email address to which the generated report will be sent, the email server must be configured and enabled in SANnav. See [Configuring an Email Setup](#).

NOTE

A maximum of four schedules can be associated with one report template.

To schedule a report, perform the following steps.

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
2. Locate the report template and click **Schedule** on the down arrow to the right of the table entry.



3. Select a time interval and a time to run the report.

For example, the following screen capture schedules a report to run every Sunday at 12:00 a.m.

The 'Schedule Report' dialog box shows the following configuration:

- When to Run:** Weekly (dropdown), Time: 12:00 AM (+Add)
- Day:** Sunday (dropdown)
- Send to:** (empty text field), Format: (dropdown)
- Active:**
- Buttons:** Save, Cancel

4. Specify the email address of the receiver and the formats in which the report will be sent.

You can enter multiple email addresses separated by commas.

If the **Send to** field is disabled, this means that an email server is not configured or is not enabled in SANnav.

If you select multiple formats for the report output, they are zipped into one file.

5. Check **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** page, the **Scheduled** column now shows the schedule for when the report will be run.

6.3.4 Generating and Exporting Reports

In addition to scheduling reports, you can generate and view a report at any time. You also export the generated output to PDF, HTML, and CSV files.

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.

The **Templates** page lists all dashboard and reports templates.

2. Locate the report template 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** page lists all reports that were generated by logged-in users in the past 30 days. Reports older than 30 days are automatically deleted.

4. Locate the report you want to see, and select **View** from the action menu.

Name	Description	Tags	Generated By	Generated On	Action
Weekly Report_2019-08-10-12-...	Run weekly s...	weekly	Administrator	Aug 10, 2019 12:00 AM	View
Inventory Report_2019-08-10-12-...	Run weekly s...	weekly	Administrator	Aug 10, 2019 12:00 AM	View
Weekly Report_2019-08-10-11-...	Run weekly s...	weekly	Administrator	Aug 10, 2019 11:00 AM	View

A report is generated in HTML format. Note that Time series reports generate in CSV format only. This means that to view the data, you must export the report and open the downloaded ZIP file.

On the top left, the context of the reports (applied filters and so on) is displayed.

The generated output data and date range have the time zone of the browser that is used to schedule or generate the report.

Network Scope: All
Date Range: Aug 3, 2019, 12:36 PDT - Aug 10, 2019, 12:36 PDT

Inventory Report

Chassis

3 items

Name	IP Address	Status	Model	Type
BrocadeG610	██████████	Healthy	Brocade G610	Switch
BrocadeG620	██████████	Critical	Brocade G620	Switch
Brocade_X6-4	██████████	Marginal	Brocade X6-4	Switch

Chassis Fan

BrocadeG610

4 items

Slot Number	Speed	Operational Status	Asset Tag
1	6965	On	██████████
2	7187	On	██████████

5. Click the More button (), and then select **Export** to download and export the report.

The report is downloaded as a ZIP file containing HTML, PDF, and CSV files.

6.3.5 Exporting Report Templates

You can create a report template in one SANnav instance, export the template, and then import the template on another SANnav instance. In this way you can share a report template across different instances of SANnav.

To export report templates, you must have Reports privilege with read/write permission.

Note the following about exporting reports:

- Exporting reports is not backward compatible. If you export a report template, you can import it only on a SANnav instance that is running the same SANnav version or higher.
- Report scheduling information is not exported.
- Making manual changes to the exported reports file and then importing it is not supported.

Perform the following steps to export a report template.

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
2. Locate the report template that you want to export, and select **Export Definition** from the action menu.

The screenshot shows the SANnav interface with the 'Templates (5)' page. The navigation bar includes 'Dashboard & Reports', 'Topology', 'Inventory', 'Events', 'Zoning', and 'SANnav'. The subnavigation bar has 'Dashboard View', 'Templates', and 'Reports'. The main content area displays a table of templates. A context menu is open over the 'Weekly Report 2' row, with the 'Export Definition' option highlighted in red.

Name	Type	Description	Created ...	Shari...	Tags	Scheduled
Weekly Report 2	Report	Run weekly swi...	Administrator	Shared	weekly	-
Weekly Report	Report	Run weekly swi...	Administrator	Shared	weekly	Every sunday...
Extension Dash...	Dashboard	Extension Tunn...	(System)	Shared	FCIPEste...	-
Health Summary	Dashboard	Health Summary	(System)	Shared	default,h...	-
Network Port T...	Dashboard	Monitors each ...	(System)	Shared	port,port ...	-

The report template is downloaded and saved to your local machine. You can now import this template to other SANnav instances.

6.3.6 Importing Report Templates

You can import a SANnav report template that was previously exported from another SANnav instance. In this way you can share a report template across different instances of SANnav.

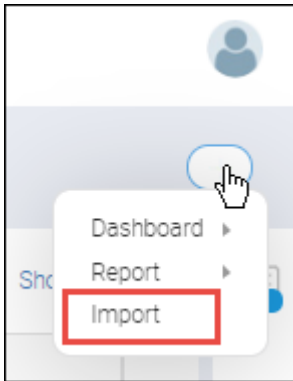
To import report templates, you must have Reports privilege with read/write permission.

Note the following about importing report templates:

- Importing report templates is not backward compatible. If you export a template, you can import it only on a SANnav instance that is running the same SANnav version or higher.
- Report scheduling information is not imported. If you want to schedule the report, you must set up a schedule after it is imported.
- Making manual changes to the exported template file and then importing it is not supported.
- When you import a report, be sure to give it a unique name for this SANnav instance.

Perform the following steps to import a report template.

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
2. Click the **+** button on the right side of the subnavigation bar, and then select **Import**.



3. Browse to the location of the template file, and click **OK**.
The file must be a valid JSON file that was previously exported from SANnav.
4. In the **Import** dialog, optionally change the name of the report template and update the tags and description.
The report template name must be unique.
Select the **Shared** box if you want other SANnav users to be able to access this report template.

 A screenshot of the 'Import' dialog box. The dialog has a blue header with the title 'Import' and a close button (X). Below the header, there are three text input fields: 'Name' with the value 'Weekly Report', 'Tags' with the value 'weekly', and 'Description' with the value 'Run weekly switch report'. Below these fields is a checkbox labeled 'Shared' which is checked. At the bottom of the dialog, there are two buttons: 'Import' (in blue) and 'Cancel' (in grey).

5. Click **Import**.
The file is imported and displayed in the **Templates** page.

6.4 Widgets for Dashboards and Reports

SANnav provides pre-configured widgets, which you can use in tailored dashboards and reports. For example, one of your first tasks might be to tailor a Dashboard view with one or more pre-configured widgets so that you can monitor switch and port status or track error and performance statistics.

When creating a dashboard or report, you can choose from two classes of widgets: Status and Performance. The Performance class comprises Custom and Distribution widgets, which are described as follows:

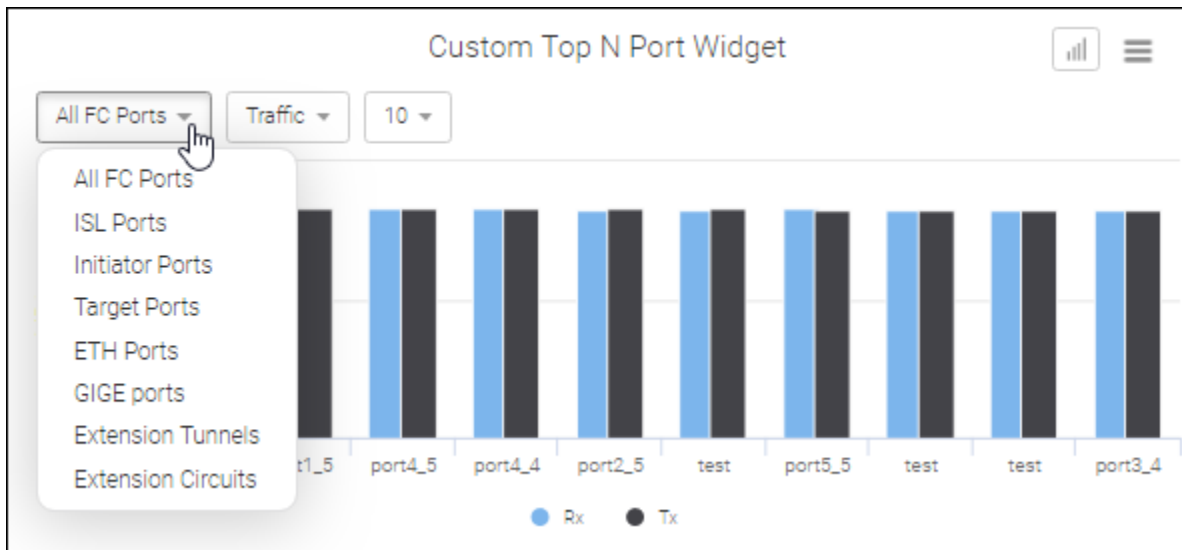
- Custom widget.

You can select the entity type (port type, tunnel, or circuit), performance measure, and the count of Top N items at run time. (For Top N widgets, N represents the text box, where valid values are 10, 15, 20, and 25.) Custom widgets are of two types: product and port/extension tunnel/extension circuit.

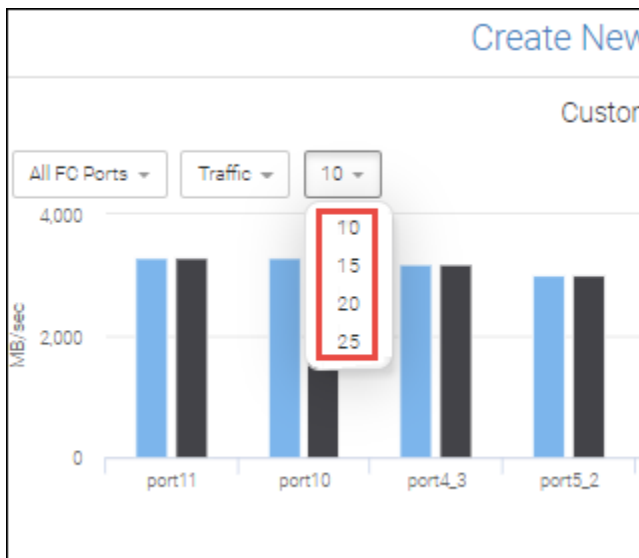
- Distribution widget.

With this widget entities like port and switches are distributed among a maximum of five *percentage* buckets within which selected measures range from 0 to 100%. This widget answers a question like ports utilization over the last hour by showing port count for each percentage bucket.

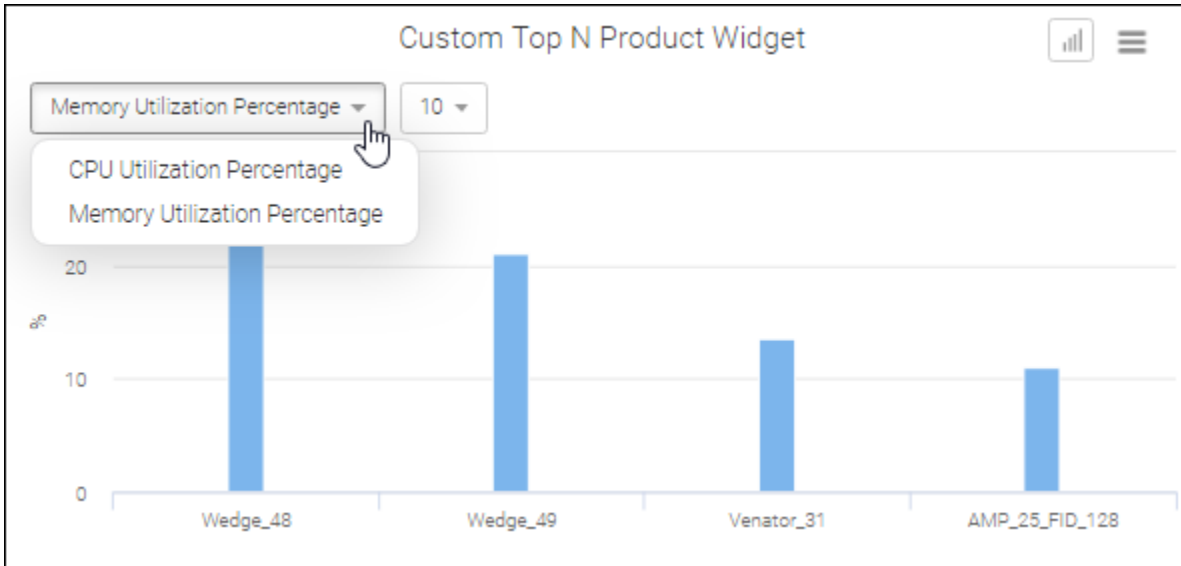
Custom Top N Port allows you to select the performance/error metrics for the selected port type.



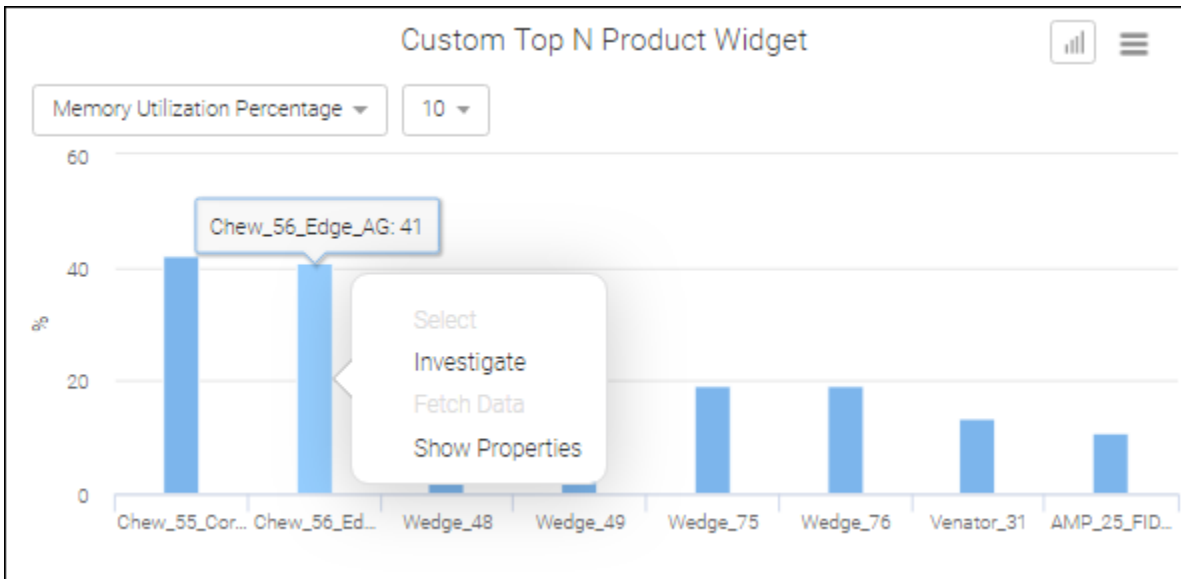
The supported Min and Max values are shown below.



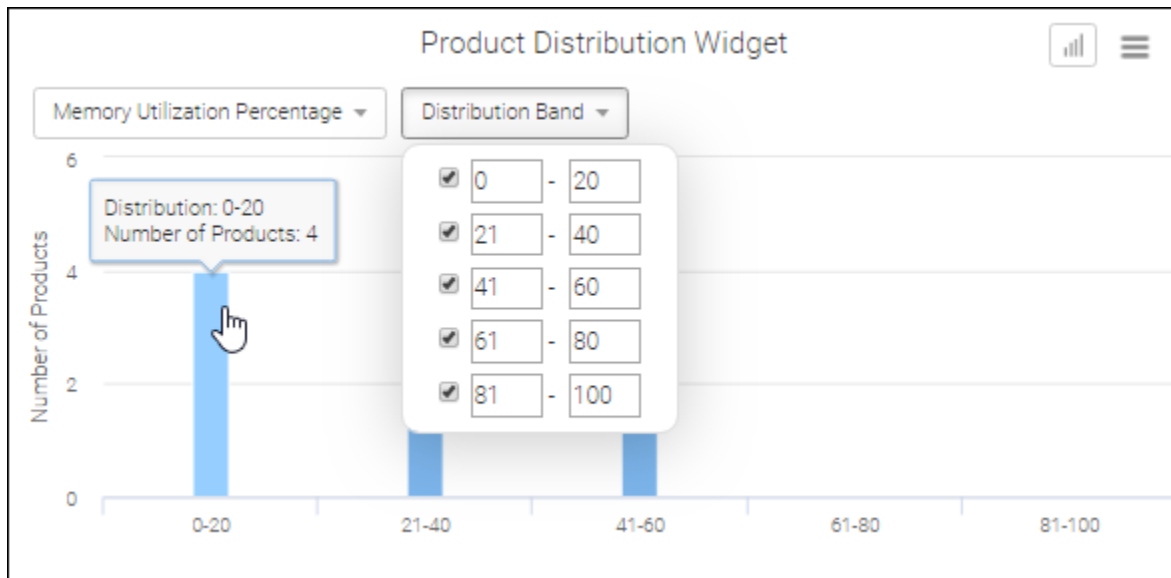
Custom Top N Product allows you to select the performance metric (CPU or memory utilization) for the SAN environment.



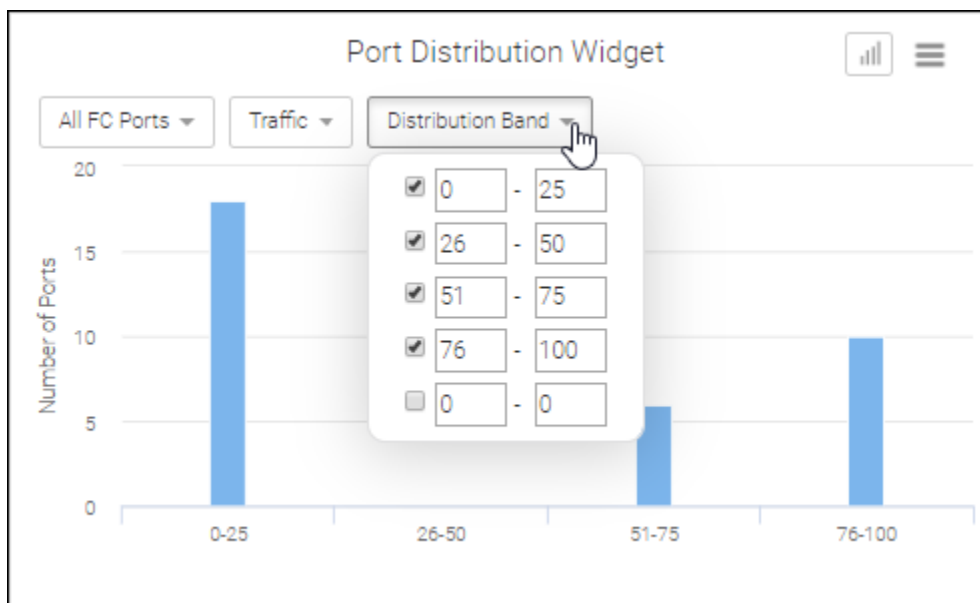
From within a custom widget, you can launch the Investigate option to perform detailed performance monitoring.



Product Distribution allows you to select either CPU or Memory Utilization from one to five distribution buckets to capture the number of products. For each bucket the maximum % distribution is 100%



Port Distribution allows you to select a port and error type from one to five distribution buckets to capture the number of ports. As shown in the following screen capture, this widget has been modified to display only four distribution bands.



NOTE

By default, all widgets limit the number of items displayed to 10. However, custom widgets allow you to select a maximum of 25 items.

Some widgets are exclusive to Extension Tunnels and Circuits. Top Tunnel Utilization and Top Tunnel Dropped Packets comprise the Extension Tunnel widget set, whereas the set of Extension Circuit widgets include Top Circuit Utilization, FC Utilization, IP Extension Utilization, Jitter, and RTT.

6.4.1 Performance Widgets

The following table is a complete list of performance widgets. When used in a dashboard, all performance widgets refresh at 5-minute intervals.

Widget Title	Description	Where Used
Custom Top N Port Widget	Displays the top N ports of a specific port type and based on a specific measure. For example: top 20 ISL ports based on port utilization percentage.	Dashboard
Custom Top N Product Widget	Displays the top N products based on CPU or memory utilization percentage.	Dashboard
Port Distribution Widget	Displays the port count distribution from 0-100 percent based on current counter value. This widget is applicable to traffic as well as error counters.	Dashboard
Product Distribution Widget	Displays the product count distribution from 0-100 percent based on current counter value. This widget is applicable only to CPU and memory utilization.	Dashboard
Time Series - ETH Port Traffic	Displays changes in measures relative to ETH Port Traffic over a specific period of time.	Reports
Time Series - Extension Tunnel Traffic	Displays changes in measures relative to Extension tunnel traffic over a specific period of time.	Reports
Time Series - Flow Collection (aggregated)	Displays aggregated metrics for flow collections.	Reports
Time Series - Flow Violations	Displays violations for selected flows.	Reports
Time Series - GigE Port Traffic	Displays changes in measures relative to GigE port traffic over a specific period of time.	Reports
Time Series - Port Errors	Displays changes in measures relative to port errors over a specific period of time.	Reports
Time Series - Port Traffic	Displays changes in measures relative to port traffic over a specific period of time.	Reports
Time Series - Port Utilization	Displays changes in measures relative to port utilization over a specific period of time.	Reports
Time Series - Product Utilization	Displays changes in measures relative to product utilization over a specific period of time.	Reports
Top Circuit FC Utilization	Displays the top circuit utilization for FC traffic.	Dashboard, Reports
Top Circuit IP Extension Utilization	Displays the top circuit utilization for IP Extension traffic.	Dashboard, Reports
Top Circuit Jitter	Displays the top circuit jitter.	Dashboard, Reports
Top Circuit RTT	Displays the top 10 round-trip times for the circuit.	Dashboard, Reports
Top Circuit Utilization	Displays the top 10 circuits based on traffic utilization.	Dashboard, Reports
Top Collection Aggregation	Consists of a two-widget set that shows the top N collections for selected metrics and occurrences based on the selected threshold value.	Reports
Top Duplicate Acknowledge	Displays the top 10 duplicate acknowledgment packets on a tunnel.	Dashboard, Reports
Top ETH Port Traffic	Displays the top 10 ETH ports based on traffic.	Dashboard
Top ETH Port Utilization	Displays the top 10 ETH ports based on utilization.	Dashboard, Reports
Top Extension Tunnel Dropped Packets	Displays the top 10 extension tunnels based on the number of dropped packets.	Dashboard, Reports
Top Extension Tunnel Utilization	Displays the top 10 extension tunnels based on utilization.	Dashboard, Reports

Widget Title	Description	Where Used
Top Flow Violations	Displays the top flow violations for selected metrics.	Reports
Top GigE Port Traffic	Displays the top 10 GigE ports based on traffic.	Dashboard
Top GigE Port Utilization	Displays the top 10 GigE ports based on utilization.	Dashboard, Reports
Top Host Port Pending IOs	Consists of a three-widget set that shows the top host port pending I/Os, time series, and occurrences, based on the selected threshold value.	Reports
Top Host Port Read Oversubscription	Consists of a three-widget set that shows the top host port read oversubscription, time series, and occurrences, based on the selected threshold value.	Reports
Top Initiator Port Link Failures	Displays the top 10 initiator ports based on the number of link failures.	Dashboard, Reports
Top Initiator Ports BB Credit Zero	Displays the top 10 initiator ports based on the number of transitions in and out of the BB credit zero state.	Reports
Top Initiator Ports C3 Discard RX Timeout	Displays the top 10 initiator ports based on the number of received Class 3 frames discarded due to timeout.	Dashboard, Reports
Top Initiator Ports CRC Errors	Displays the top 10 initiator ports based on the number of cyclic redundancy check (CRC) errors.	Dashboard, Reports
Top Initiator Ports Link Resets	Displays the top 10 initiator ports based on the number of link resets.	Dashboard, Reports
Top Initiator Ports PCS Block Errors	Displays the top 10 initiator ports based on the number of PCS block errors.	Dashboard, Reports
Top Initiator Port Sync Losses	Displays the top 10 initiator ports based on the number of sync losses.	Dashboard, Reports
Top Initiator Port Utilization	Displays the top 10 initiator ports based on utilization.	Dashboard, Reports
Top ISL Port Link Failures	Displays the top 10 ISL ports based on the number of link failures.	Dashboard, Reports
Top ISL Ports BB Credit Zero	Displays the top 10 ISL ports based on the number of transitions in and out of the BB credit zero state.	Reports
Top ISL Ports C3 Discard Rx Timeout	Displays the top 10 ISL ports based on the number of received Class 3 frames discarded due to timeout.	Dashboard, Reports
Top ISL Ports CRC Errors	Displays the top 10 ISL ports based on the number of CRC errors.	Dashboard, Reports
Top ISL Ports Link Resets	Displays the top 10 ISL ports based on the number of link resets.	Dashboard, Reports
Top ISL Ports PCS Block Errors	Displays the top 10 ISL ports based on the number of PCS block errors.	Dashboard, Reports
Top ISL Port Sync Losses	Displays the top 10 ISL ports based on the number of sync losses.	Dashboard, Reports
Top ISL Port Utilization	Displays the top 10 ISL ports based on utilization percentage.	Dashboard, Reports
Top Out of Order	Displays the top 10 circuits based on the number of data packets that were delivered out of order.	Dashboard, Reports
Top Port BB Credit Zero	Displays the top 10 ports based on the number of transitions in and out of the BB credit zero state.	Dashboard, Reports

Widget Title	Description	Where Used
Top Port C3 Discards	Displays the top 10 ports based on the number Class 3 frames discarded.	Dashboard, Reports
Top Port C3 Discard RX Timeout	Displays the top 10 ports based on the number of received Class 3 frames discarded due to timeout.	Dashboard, Reports
Top Port C3 Discard TX Timeout	Displays the top 10 ports based on the number of transmitted Class 3 frames discarded due to timeout.	Dashboard, Reports
Top Port CRC Errors	Displays the top 10 ports based on the number of frames that contain CRC errors.	Dashboard, Reports
Top Port CRC Error with bad EOF	Displays the top 10 ports based on the number of frames that contain CRC errors with bad EOF.	Dashboard
Top Port Encode Error In	Displays the top 10 ports based on the number of encode errors inside of the frame.	Dashboard
Top Port Encode Error Out	Displays the top 10 ports based on the number of encode errors outside of the frame.	Dashboard
Top Port Frame Too Long Errors	Displays the top 10 ports based on the number (error count) of frames longer than the maximum frame size allowed.	Dashboard
Top Port Invalid Transmissions	Displays the top 10 ports based on the number of invalid transmissions.	Dashboard
Top Port Link Failures	Displays the top 10 ports based on the number of link failures.	Dashboard, Reports
Top Port Link Resets	Displays the top 10 ports based on the number of transmit (Tx) or receive (Rx) link resets.	Dashboard, Reports
Top Port PCS Block Errors	Displays the top 10 ports based on the number of Physical Coding Sublayer (PCS) block errors outside of frames.	Dashboard, Reports
Top Port Signal Losses	Displays the top 10 ports based on number of signal failures.	Dashboard, Reports
Top Port Sync Losses	Displays the top 10 ports based on number of synchronization failures.	Dashboard, Reports
Top Port Traffic	Displays the top 10 ports based on transmit (Tx) and receive (Rx) traffic.	Dashboard
Top Port Utilization Percentage	Displays the top 10 ports based on transmit (Tx) and receive (Rx) port utilization percentages.	Dashboard, Reports
Top Port with bad EOF	Displays the top 10 ports based on the number of frames with bad EOF.	Dashboard
Top Product CPU Utilization	Displays the top 10 products based on CPU utilization percentages.	Dashboard, Reports
Top Product Memory Utilization	Displays the top 10 products based on memory utilization percentages.	Dashboard, Reports
Top SCSI Errors	Consists of a two-widget set that shows the top SCSI errors and occurrences based on the selected threshold value.	Reports
Top Slow Start	Displays the top 10 circuits based on the number of slow starts.	Dashboard, Reports
Top Storage Port Data Rate	Consists of a three-widget set that shows the top storage port data rate, time series, and occurrences, based on the selected threshold value.	Reports
Top Storage Port Exchange Completion Time	Consists of a three-widget set that shows the top storage port exchange completion time, time series, and occurrences, based on the selected threshold value.	Reports

Widget Title	Description	Where Used
Top Storage Port First Response Time	Consists of a three-widget set that shows the top storage port first response time, time series, and occurrences, based on the selected threshold value.	Reports
Top Storage Port IOPS	Consists of a three-widget set that shows the top storage port IOPS, time series, and occurrences, based on the selected threshold value.	Reports
Top Storage Port Pending IOs	Consists of a three-widget set that shows the top storage port pending I/Os, time series, and occurrences, based on the selected threshold value.	Reports
Top Target Port Link Failures	Displays the top 10 target ports based on the number of link failures.	Dashboard, Reports
Top Target Ports BB Credit Zero	Displays the top 10 target ports based on the number of transitions in and out of the BB credit zero state.	Reports
Top Target Ports C3 Discard RX Timeout	Displays the top 10 target ports based on number of received Class 3 frames discarded due to timeout.	Dashboard, Reports
Top Target Ports CRC Errors	Displays the top 10 target ports based on the number of CRC errors.	Dashboard, Reports
Top Target Ports Link Resets	Displays the top 10 target ports based on the number of link resets.	Dashboards, Reports
Top Target Ports PCS Block Errors	Displays the top 10 target ports based on the number of PCS block errors.	Dashboard, Reports
Top Target Port Sync Losses	Displays the top 10 target ports based on the number of sync losses.	Dashboard, Reports
Top Target Port Utilization	Displays the top 10 target ports based on utilization.	Dashboard, Reports

6.4.2 Status Widgets: Dashboard

The following table is a complete list of status dashboard widgets. When used in a dashboard, each widget refreshes at the specified interval.

Widget Name	Description	Refresh Interval	Type
Configuration Drifts	Monitors switch configuration and detects drifts.	10 minutes	Chart
Events Summary	Shows summary of events, grouped by severity and category.	30 seconds	Chart
Fabrics (Chart)	Shows overall fabrics health, categorized by health state.	15 minutes	Donut
Fabrics (Table)	Shows fabrics with the worst overall health score.	15 minutes	Table
Host Port Health Violations	Shows host port MAPS violations.	30 seconds	Table
Host Port Out Of Range Violations	Shows the number of violations for each MAPS category for host ports with MAPS violations.	30 seconds	Table
Hosts (Chart)	Shows overall hosts health, categorized by health state.	15 minutes	Donut
Hosts (Table)	Shows hosts with the worst overall health score.	15 minutes	Table
ISL Port Health Violations	Shows ISL port MAPS violations.	30 seconds	Table
ISL Port Out Of Range Violations	Shows the number of violations for each MAPS category for ISLs with MAPS violations.	30 seconds	Table

Widget Name	Description	Refresh Interval	Type
Out Of Range Violations	Shows number of violations for each MAPS category for SAN devices with MAPS violations.	30 seconds	Table
Port Health Violations	Shows all port MAPS violations.	30 seconds	Table
Port Usage Summary	Shows summary of ports, grouped by type.	5 minutes	Chart
Product Status	Shows products, grouped by operational status and categories .	5 minutes	Chart
Storage (Chart)	Shows overall storage health, categorized by health state.	15 minutes	Chart
Storage Port Health Violations	Shows storage port MAPS violations.	30 seconds	Table
Storage Port Out Of Range	Shows the number of violations for each MAPS category for storage ports with MAPS violations.	30 seconds	Table
Storage (Table)	Shows storage with the worst overall health score.	15 minutes	Table
Switches (Chart)	Shows overall switches health, categorized by health state.	15 minutes	Donut
Switches (Table)	Shows switches with the worst overall health score.	15 minutes	Table
Top N Events	Shows events by switch or fabrics.	30 seconds	Chart
VM Alarms	Shows alarms triggered by the following violations: VM disk aborts, VM disk resets, VM disk usage (Kb/s), and VM total disk latency (ms).	5 minutes	Table

6.4.3 Status Widgets: Reports

The following table is a complete list of status report widgets.

Widget Name	Description	Type
Chassis	Inventory Chassis Report	Tables, including tables for blades, fans, and power supplies
Event	Event Report	Table and summary
Fabrics	Inventory Fabrics Report	Table
Host Ports	Inventory Host Ports Report	Table
Hosts	Inventory Hosts Report	Table
SDDQ	Inventory Quarantined Ports Report	Table
Storage	Inventory Storage Report	Table
Storage Ports	Inventory Storage Ports Report	Table
Switches	Inventory Switches Report	Table
Switch Ports	Inventory Switch Ports Report	Table
Violations	MAPS Violations Report	Table

6.5 Performance Monitoring

Performance monitoring gives you visibility into the performance and the error conditions in your SAN environment. Performance monitoring provides real-time and historic data of performance and error information for Fiber Channel ports, Ethernet ports, GbE ports, and extension tunnels and circuits.

The Performance Monitoring feature collects data for a specific set of fabrics from the managed devices in your SAN. It generates historic performance data for selected ports and also provides real-time performance monitoring so that you can investigate port issues.

Every 5 minutes performance data is collected for switches, ports (FC, ETH, and GbE), E_Port trunk ports, extension tunnels, and extension circuits.

SNMPv3 is used to collect the performance metrics for ports (like traffic and errors) and for switches (like CPU utilization and memory utilization). This means that to collect data, SNMPv3 must be configured in the switch.

Historic and Real-Time Data

Performance data is displayed in graphs. When viewing the graphs, you can select whether to view historic or real-time data.

For historic data, you select the time period for which to review the data. The default range is the last 30 minutes, but you can select date ranges of up to the last 30 days. When you are viewing historic data, the system collects metrics every 5 minutes. The rate at which the data is displayed depends on the date range.

- For date ranges of **Last 30 Minutes**, **Last 1 Hour**, and **Last 2 Hours**, the data displays in 5-minute intervals.
- For date ranges of **Last 1 Day**, **Last 3 Days**, and **Last 1 Week**, the data displays in 1-hour intervals.
- For a date range of **Last 30 Days**, the data displays in 1-day intervals.
- For custom date ranges, the data is displayed once, and the graphs do not update.

For real-time monitoring, select a small number of ports (about 10) and measures, and the system collects and displays metrics at 10-second intervals.

High-Granularity Data Collection

For Gen 6 switches running Fabric OS 8.2.1a or higher, SANnav Management Portal can collect and display performance metrics at 2-second intervals. This is not the default, however, and you must schedule high-granularity data collection if you want SANnav to capture metrics at 2-second intervals.

High-granularity data collection is supported for up to 100 ports at a time on one or multiple Gen 6 switches.

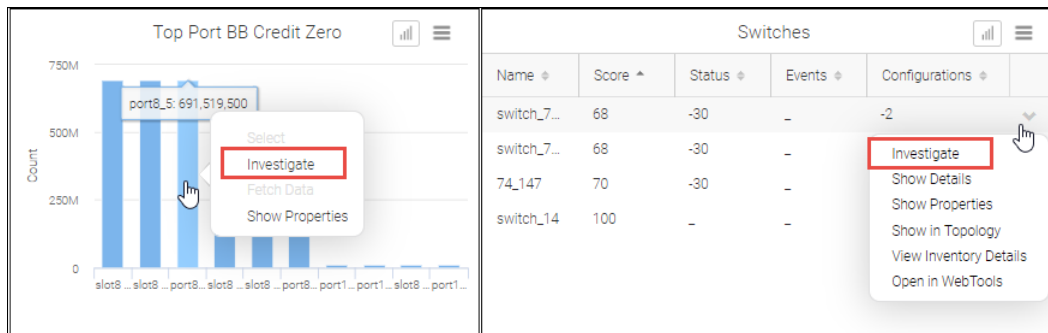
6.5.1 Launching Investigation Mode

The SANnav Investigate function enables you to view performance measures for selected switches, switch ports, extension tunnels, extension circuits, and trunks.

You can launch Investigation mode in several ways, and you can investigate a single element or multiple elements (of the same type). This section describes how to select the elements you want to investigate and launch Investigation mode. The [Using Investigation Mode](#) section describes what happens after you click **Investigate**.

Invoking Investigation Mode from a Dashboard Widget

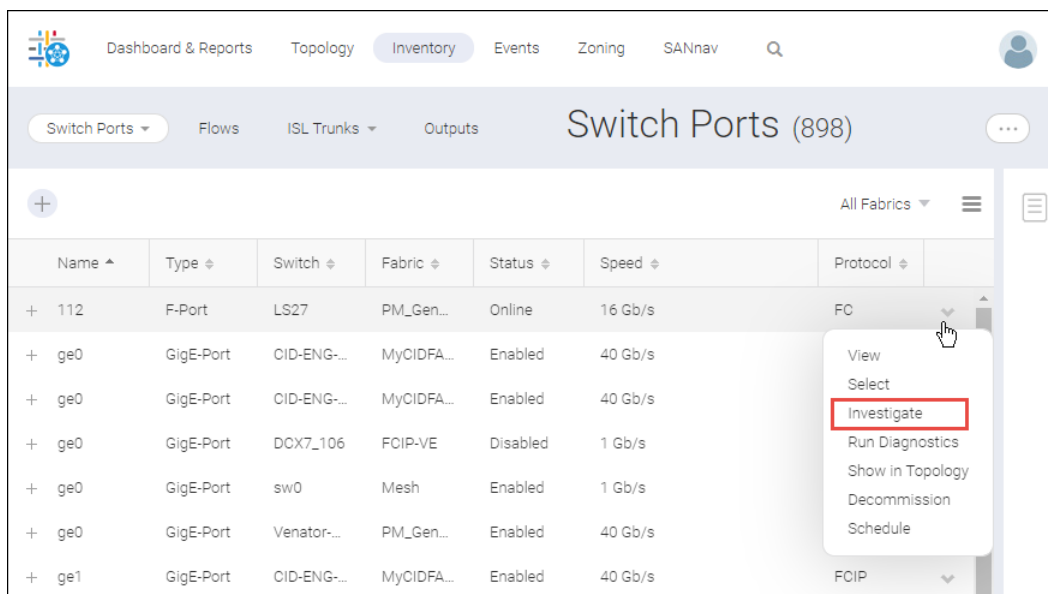
On the **Dashboard View** page, several widgets include the **Investigate** option. For example, you can investigate a switch port by clicking the graph, or you can investigate a switch by clicking the action menu.

Figure 13: Launching Investigation Mode from the Dashboard

Invoking Investigation Mode from an Inventory List

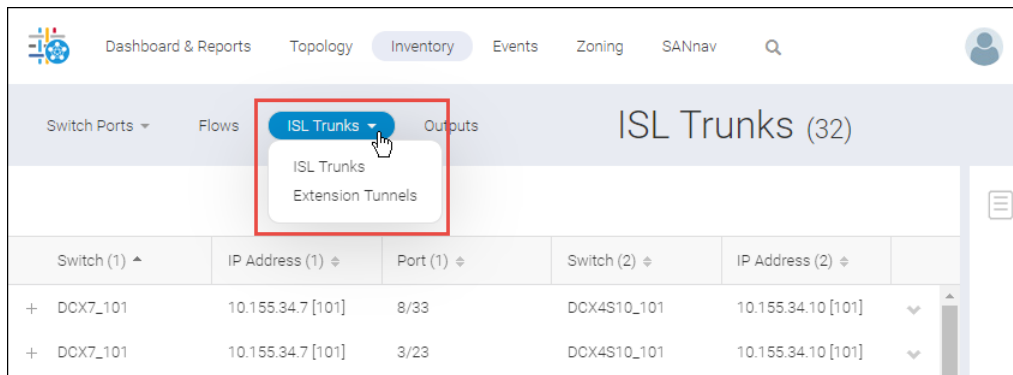
From the **Inventory** page, click **Investigate** from the action menu for switches and switch ports.

The bulk select option is available if you want to investigate multiple items.

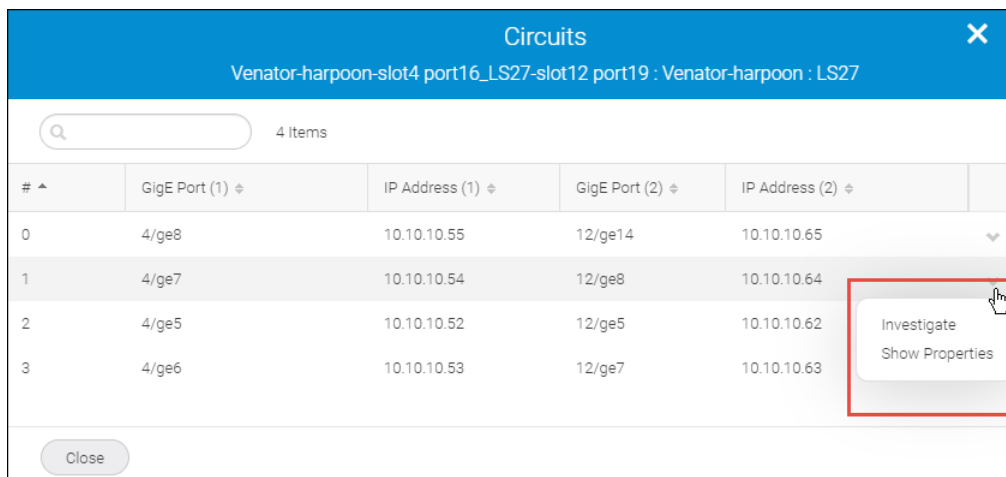
Figure 14: Launching Investigation Mode from the Inventory Page

Note that for switch ports, you can also launch investigation mode from the switch details page.

For extension tunnels and trunks, select either **Extension Tunnels** or **ISL Trunks** from the drop-down in the sub-navigation bar. Then select **Investigate** from the action menu for the selected tunnel or trunk.

Figure 15: Launching Investigation Mode for Extension Tunnels or Trunks

For extension circuits, select **Show Circuits** from the action menu for a tunnel, and then click **Investigate** from the action menu of the **Circuits** popup.

Figure 16: Launching Investigation Mode for Circuits

Invoking Investigation Mode from the Sidebar

From the **Inventory** pages, 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 re-investigate them later, without having to locate them again from the **Inventory** pages.

Invoking Investigation Mode for High-Granularity Data

If a port is scheduled for high-granularity (2-second) data collection, you can launch investigation mode from the **Outputs** page in **Inventory**. Select **Port Data Collection** and click **Investigate** from the action menu for the port you want to investigate.

6.5.2 Collecting Items in the Sidebar for Investigation Mode

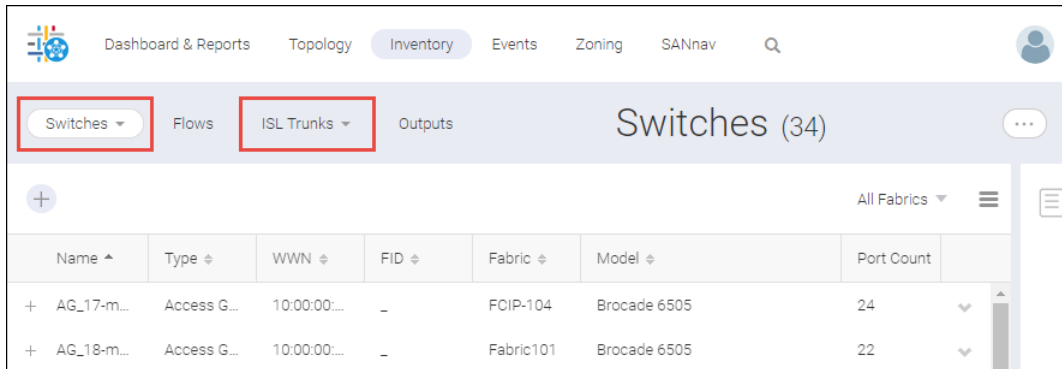
For items that you frequently investigate, you can select them and put them in the SANnav sidebar. The sidebar allows you to easily re-investigate items without having to locate and reselect them from the **Inventory** page.

1. Click **Inventory** in the navigation bar.

2. Locate the type of items that you want to investigate.

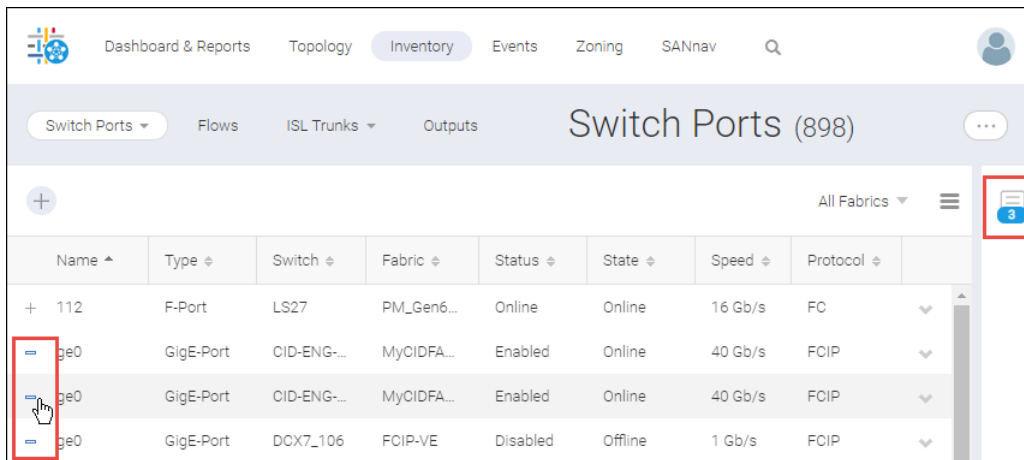
- Select **Switches** or **Switch Ports** from the left-most drop-down list in the subnavigation bar.
- Select **ISL Trunks** or **Extension Tunnels** from the next drop-down list.

You cannot add circuits to the sidebar.



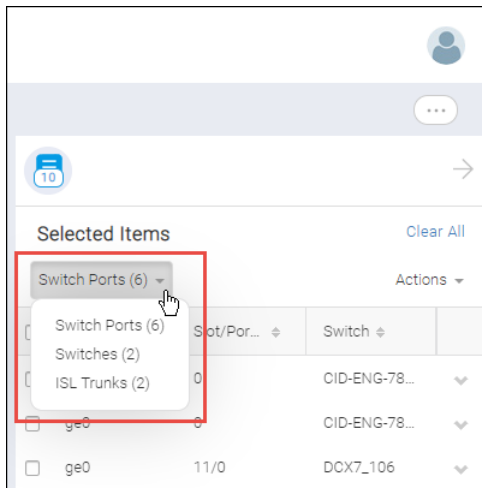
3. Click the + icon at the left of every row for each item that you want to add to the sidebar.

As you click the icons, the + changes to a - symbol, and the sidebar icon increments the count of selected items.



4. Click the sidebar icon to expand the sidebar.

5. In the sidebar, select the type of item that you want to investigate from the drop-down.

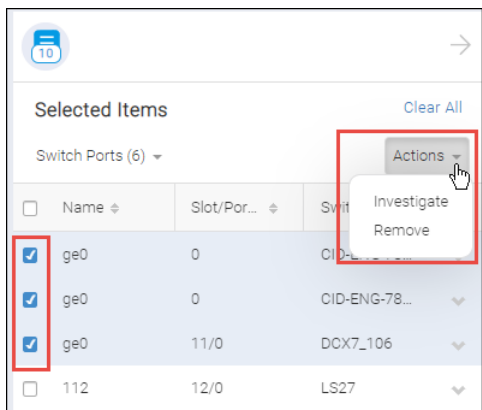


6. Select the items that you want to investigate, and click **Actions > Investigate**.

If you select multiple ports, they must all be of the same type.

NOTE

Clicking **Clear All** deletes all items from the sidebar. If you want to unselect items, you must clear each checkbox individually.



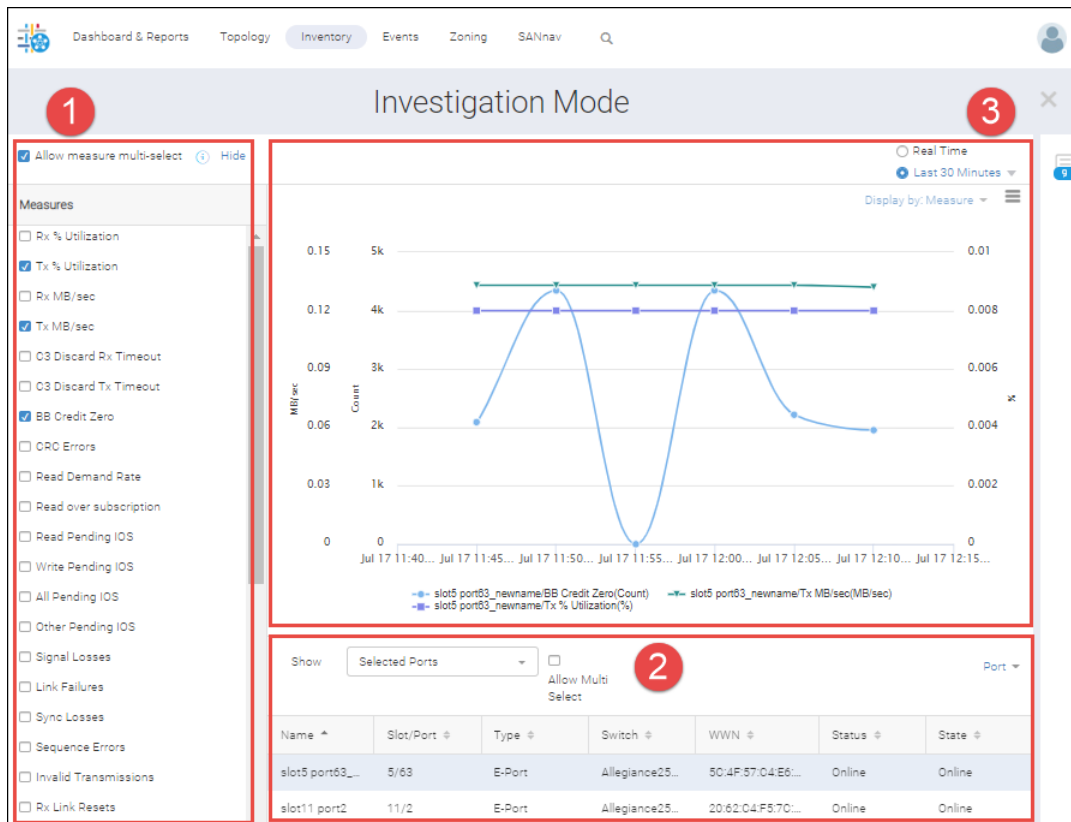
The **Investigation Mode** page displays.

6.5.3 Using Investigation Mode

SANnav Investigation mode displays 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** page, from dashboard widgets, or from the sidebar.

The **Investigation Mode** page consists of three parts: a **Measures** panel, a details table for the selected entities (ports, switches, trunks, tunnels, or circuits), and a graph area. Select measures and entities to investigate, and the resultant graph displays in the graph area.

Figure 17: Investigation Mode Page Overview

1. Measures panel. Contains a list of measures available for the selected entities.
2. Details table. Displays the entities selected for investigation.
3. Graph area. Displays a different colored line for each selected measure-entity pair.

Measures Panel

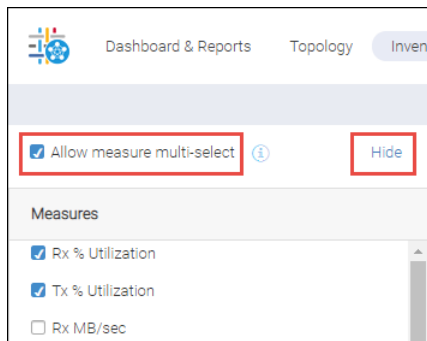
The list of available measures depends on the type of entity selected. For example, switches have different measures than ports, and GigE ports have different measures than F_Ports and E_Ports.

Select the measure that you want to monitor. If you want to display more than one measure in the graph, select the **Allow measure multi-select** checkbox. For ease of viewing in the graph, select no more than four measures, although you can select more. The recommended maximum number of selected measures is eight.

NOTE

If **Allow measure multi-select** is disabled, this means that more than four entities are selected in the details table. If you want to view multiple measures and multiple entities, only up to four entities are supported. If you want to select more measures, unselect entities in the details table until four or less are selected.

After you select the measures, you can click **Hide** to hide the **Measures** panel and allow more space for the graph.

Figure 18: Measures Panel Options**Details Table**

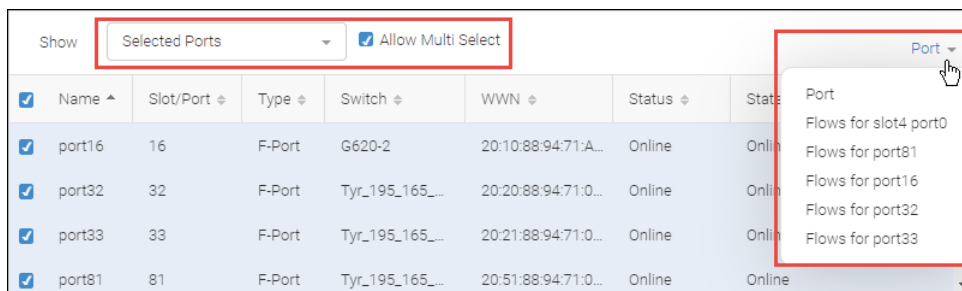
The details table displays the items that are selected for investigation.

If the table includes more than one item, the **Allow Multi Select** checkbox is available for selecting multiple items to investigate. For ease of viewing in the graph, select no more than four items, although you can select more. The recommended maximum number of selected items is eight.

You can display additional items in the table by choosing **Selected** or **All** from the drop-down list.

- For switches, selecting the **All** option displays all switches.
- For ports, tunnels, and circuits, selecting the **All** option displays all ports, tunnels, or circuits in the switch. If you originally selected items from different switches, then all ports, tunnels, or circuits from each of the switches are displayed.

For ports, you can also select flows to investigate, if any are configured. See [Operating in Flow Investigation Mode](#) for information about investigating flows.

Figure 19: Details Table Options**Graph Area**

The graph plot depends on the measures selected. The graph area displays one line for each entity/measure pair.

NOTE

If the graph area is empty, either measures are not selected or there might not be data to display for this combination of measure and port.

Historic vs. Real-Time Data

By default, the graphs display historic data from the last 30 minutes. You can change this value by selecting the date range drop-down in the upper-right corner of the graph area.

The graphs update periodically depending on the granularity of the selected date range. Note that if you select a custom date range (by specifying a start and end date and time), 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. The **Real Time** option is not available if you are investigating switches.

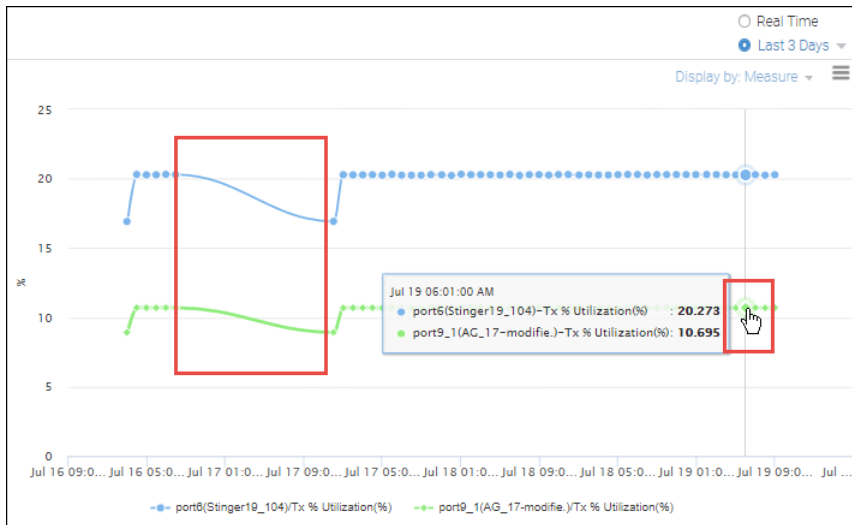
Data Points

Hover the mouse over a data point in the graph to see additional details in a tool-tip box.

Some data points might be missing, which could be due to an SNMP timeout or to performance data collection being disabled.

The following graph plots TX% utilization on two ports. Hovering over a data point in one line gives details for all data points for that same time period. Note the missing data points that occurred earlier in the date range.

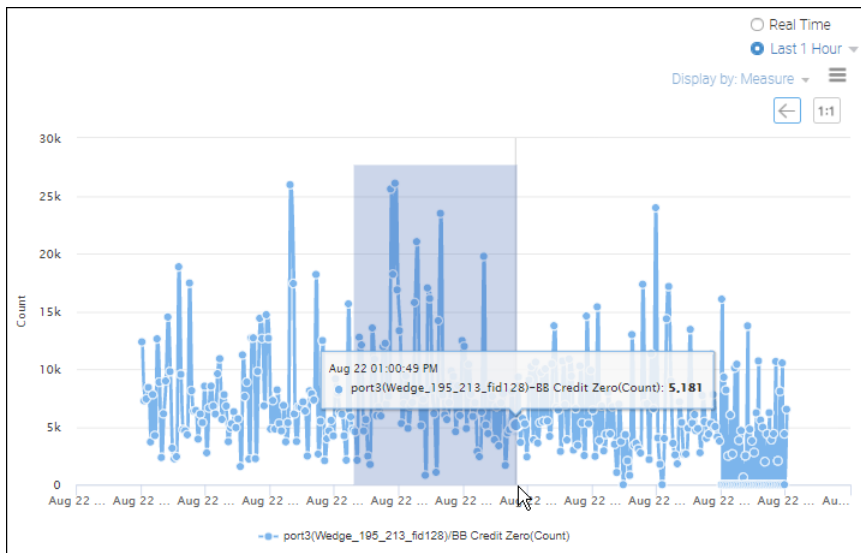
Figure 20: Performance Graph Data Points and Missing Data Points



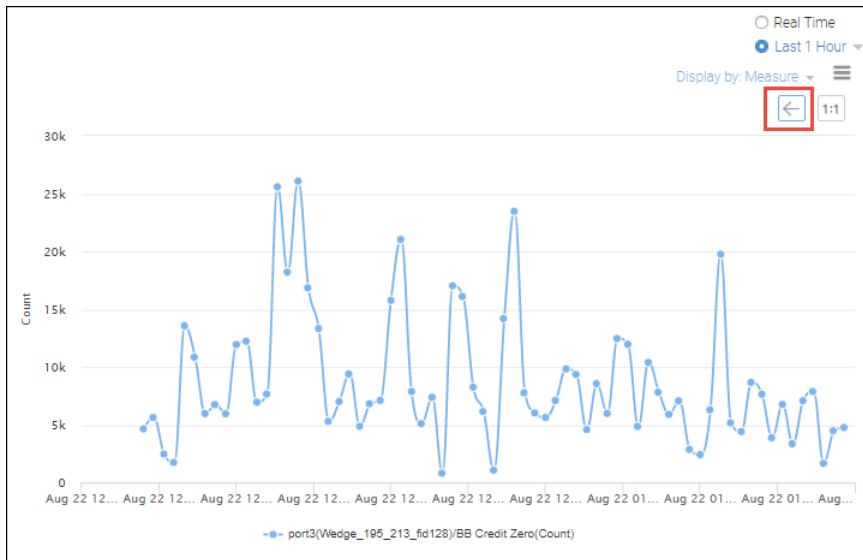
Zooming In on Data

To zoom in on an area of the graph, drag out a rectangular area in the graph with your mouse pointer.

Figure 21: Highlighting Part of a Graph to Zoom In

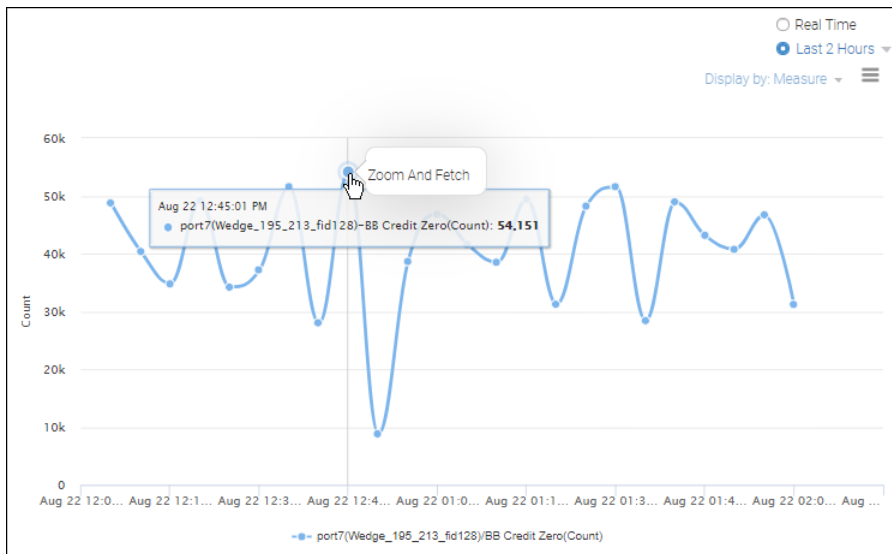


The graph is redrawn with the selected area magnified. Click the back button in the upper-right corner to return to the previous view.



Zoom and Fetch for Higher Granularity

You can obtain ("fetch") a higher level of granularity for a particular data point with **Zoom and Fetch**. Click a data point in the graph, and then click **Zoom and Fetch**.



The graph displays at a higher granularity. Each successive application of **Zoom and Fetch** displays a greater level of granularity. For example, **Zoom and Fetch** applied to 1-day granularity displays data at 1-hour granularity. Applying **Zoom and Fetch** to 1-hour granularity displays data at 5-minute granularity.

For Gen 6 platforms that are running Fabric OS 8.2.1 or later, if you click a 5-minute granularity data point and select **Zoom and Fetch**, the graph displays 1-minute granularity data points. If high-granularity data collection has been scheduled for this port, the graph displays 2-second granularity data points.

NOTE

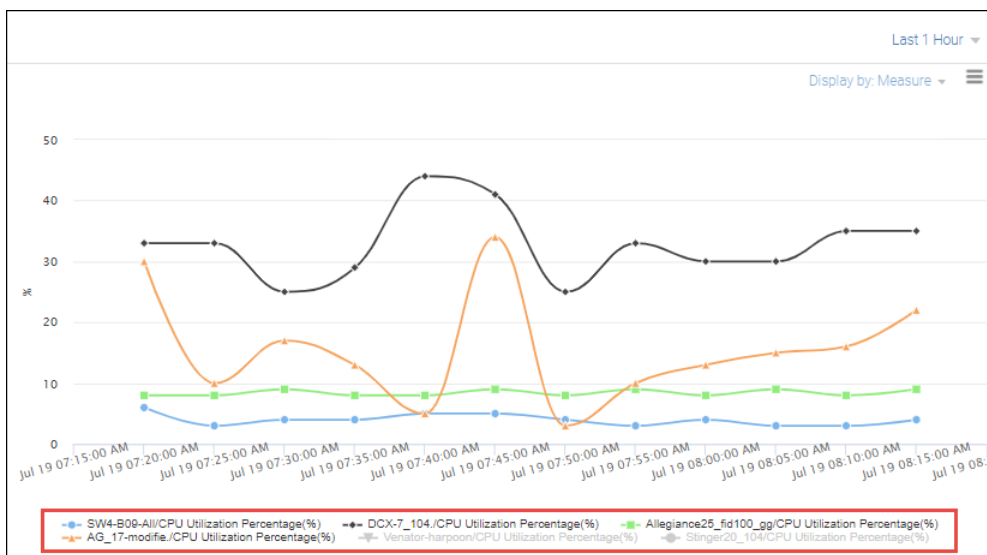
Zoom and Fetch is applicable only to FC switch ports of type E, F, EX, N, and SIM, and only in a graph with one port and one measure. It is not available in real-time mode or if multiple ports or multiple measures are selected.

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 display the corresponding lines in the graph.

The following graph shows CPU utilization percentage for six switches. Note that two of the switches have been de-selected in the legend, so only four lines display in the graph.

Figure 22: Performance Graph Legend



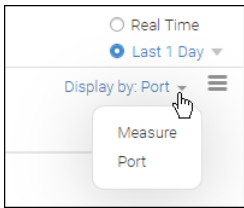
Types of Graphs

The graph area can display different types of graphs:

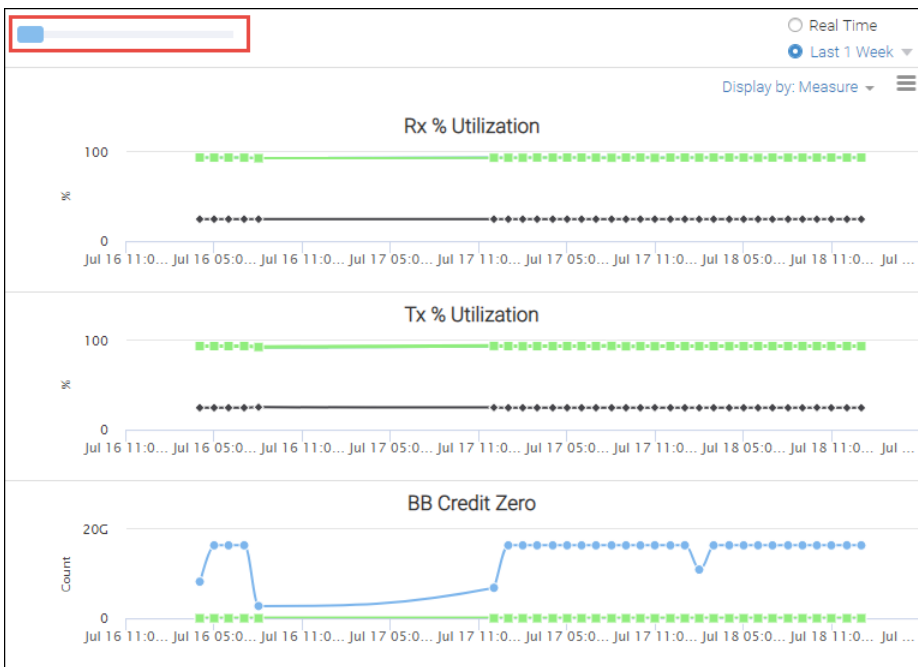
- One entity and multiple measures
- Multiple entities and one measure
- Multiple entities and multiple measures

If you display multiple entities and multiple measures, multiple graphs are generated. SANnav displays up to three graphs, and each graph is limited to four measures or entities. The graphs can be displayed by entity or by measure, depending on the value in the **Display by** drop-down.

- If you display the graphs by entity, you can select at most three entities with four measures each.
- If you display the graphs by measure, you can select up to three measures for four entities.

Figure 23: Displaying Performance Graphs by Measure or by Entity

When multiple graphs are displayed, you can move the slider bar at the top left of the graph area to compress the graphs so that you can view more on a single page. Note that when you compress the graphs, the legend below them disappears.

Figure 24: Multiple Graphs, Compressed

Exporting the Graph

To export a static copy of the graph, click the hamburger icon in the top right of the graph and select **Export**. An HTML file displaying the graph is downloaded to your local machine.

6.5.4 Scheduling High-Granularity Data Collection

By default, Investigate mode provides a view of performance metrics for ports and switches at a granularity of 5 minutes. Additionally, SANnav Management Portal enables you to capture and view performance data for Gen 6 switch ports at a granularity of 2 seconds.

Before you can schedule high-granularity (2-second) data collection, you must have the following:

- Element Manager - Product Administration privilege with read/write permission

To capture high-granularity performance metrics, you must set up a schedule for the data collection. Unlike other scheduling in SANnav, you specify only a start time, and the start time must be for the current day. You cannot set up the schedule to start on a future date. Also, you do not specify an end time. The data collection continues for 3 days and is retained for 14 days, unless you delete it.

The maximum number of ports that can be scheduled for data collection is 100.

High-granularity data collection is supported only on Gen 6 switches and directors that are running Fabric OS 8.2.1a or higher. SANnav collects high-granularity performance data only on FC switch ports.

NOTE

Once you have set high-granularity data collection for a port, you cannot set high-granularity data collection on the same port until the previous collection is completed.

1. Click **Inventory** in the navigation bar, and then select **Switch Ports** from the drop-down list.
2. Select the ports on which you want to collect high-granularity data.

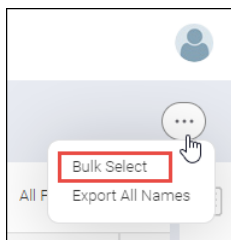
To select a single port, click the down arrow in the rightmost column for the switch port and select **Schedule** from the action menu. Alternatively, to select multiple ports, use the bulk select option.

- a. Click the More button () and click **Bulk Select**.

Using the bulk select option allows you to schedule high-granularity data collection for several ports at the same time.

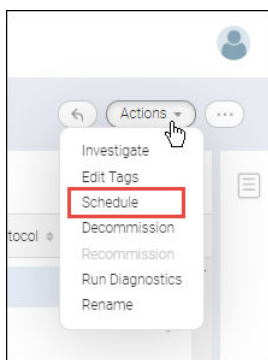
NOTE

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 displays on the leftmost side of the table.

- b. Select the checkboxes for the ports on which you want to collect data, and then click **Actions** > **Schedule** in the upper-right corner of the window.



3. Select the start time for the data collection.

The start time is for today. You cannot schedule a future start date.

4. Click **OK**.

Within 5 minutes of the specified start time, SANnav Management Portal collects metrics of the specified port at high granularity. Collection of high-granularity metrics continues for 3 days, and the collected data is retained by SANnav for 14 days.

5. Click the **Outputs** tab and select **Port Data Collection** to view the scheduled collections.
A separate output collection is generated for each port.

Port No. ^	Port Type ◊	Switch ◊	Scheduling Start Time ◊	Last Collected On ◊	Collection Status ◊	Scheduled to Delete ◊
port19	E-Port	Chew_19...	Aug 12, 2019 11:51:32 PDT	Aug 15, 2019 11:55:00 PDT	Completed	Aug 29, 2019 11:51:32 PI v
port0	F-Port	Chew_19...	Aug 12, 2019 11:51:32 PDT	Aug 15, 2019 11:55:00 PDT	Completed	Aug 29, 2019 11:51:32 PI v
port3	E-Port	Wedge_1...	Aug 22, 2019 11:05:05 PDT	-	Scheduled	Sep 08, 2019 11:05:05 PI v

While high-granularity data collection is in progress, when you investigate the scheduled ports, you can **Zoom and Fetch** down to 2-second granularity.

6.5.5 Enabling and Disabling Historic Data Collection

By default, SANnav collects performance metrics for switches, switch ports, trunk ports, extension tunnels, and circuits. You can disable this data collection on all or specific fabrics, for example, if you want to perform maintenance or diagnostics on the switches.

To enable or disable historic data collection, you must have the following:

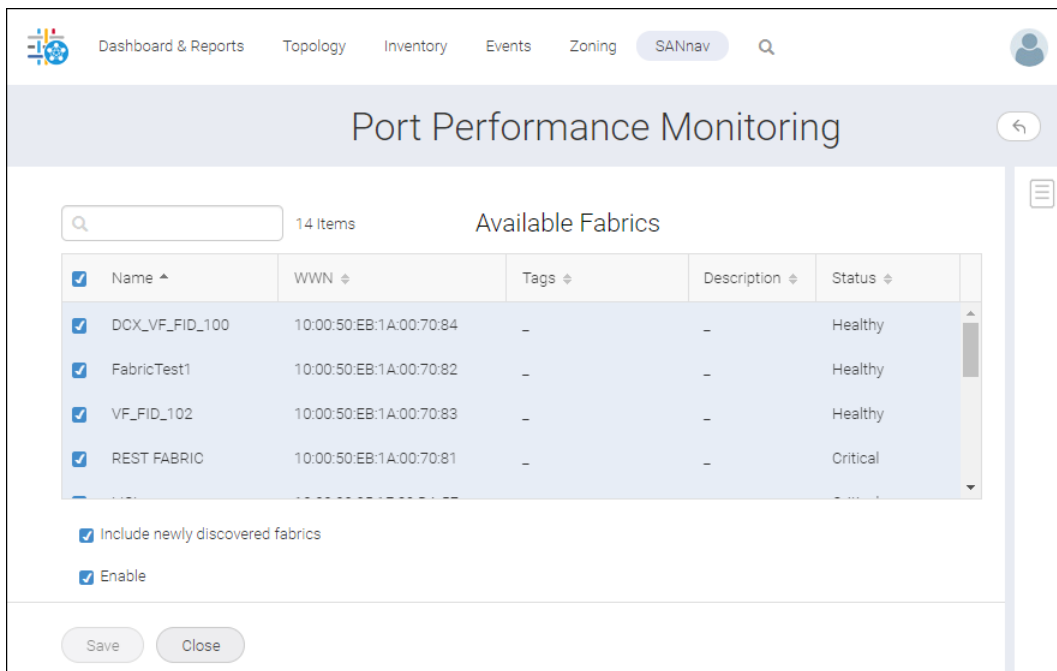
- Performance privilege with read/write permission.

When historic data collection is disabled, you can continue to view historic data, but only up to the point when data collection was disabled.

Enabling and disabling historic data collection is not applicable for high-granularity data collection.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Port Performance Monitoring**.
A list of available fabrics displays.

By default, data collection is enabled for all fabrics, so the first time this page is accessed, all fabrics are selected.



2. Clear the checkboxes for the fabrics on which to disable data collection. Select the checkboxes for the fabrics on which to enable data collection.

If you want to disable data collection on all fabrics, clear the **Enable** checkbox. For example, if you want to temporarily suspend data collection for all fabrics and restart data collection at a later time, unchecking **Enable** lets you avoid first unselecting and then selecting all fabrics each time.

NOTE

Unless **Enable** is also checked, merely selecting a fabric checkbox does not initiate data collection on that fabric. Selecting fabrics simply marks them as candidates for data collection. The fabrics participate in data collection only when **Enable** is also checked.

3. Select the **Include newly discovered fabrics** checkbox if you want to enable data collection on fabrics that are discovered after you configure data collection.
4. Click **Save**.

6.6 Inventory Management

The SANnav Management Portal **Inventory** page is a central location where you can view and manage the inventory of all discovered fabrics, switches, switch ports, hosts, host ports, virtual machines (if vCenter is discovered), physical chassis, storage, storage ports, extension tunnels, and trunks.

Using the **Inventory** page you can select a managed object, such as a switch or a switch port, and drill down to view additional details, launch detailed investigations, initiate various configuration operations, and perform other tasks.

NOTE

If an item is grayed out in the **Inventory** page, this means that the item is missing from the fabric. For example, grayed-out switches are physically disconnected from the fabric. SANnav maintains this information for tracking purposes.

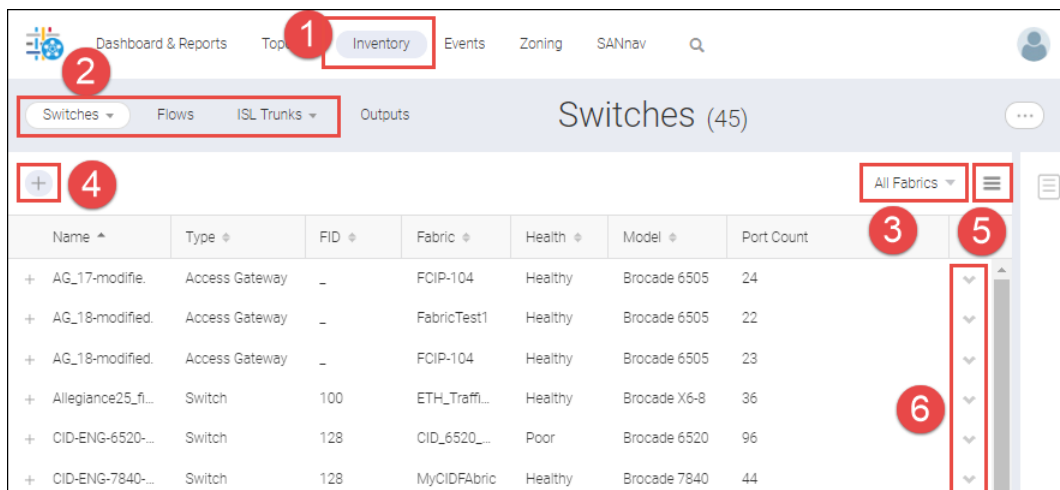
The **Inventory** page displays detailed information about inventory in tabular format. Using tags, filters, and custom fields, you can sort and filter the information to display exactly the data you need. For example, assume you want to upgrade all Gen 5 switches, one data center at a time. You can generate a list of the Gen 5 switches in each data center using the following actions:

- Create a custom field in the **Inventory** page to indicate the data center location.
- Tag switches with the switch family (Gen 5).
- Use filters on the **Inventory** page to display the Gen 5 switches in each data center.

In addition, you can perform the following tasks:

- Perform bulk operations on one or more managed objects. Specific bulk operations vary for the type of the managed object.
- Export names of switches, switch ports, and fabrics.
- Generate inventory reports.

Figure 25: Inventory Page Overview



1. Click **Inventory** in the navigation bar to access the **Inventory** page.
2. Select the type of inventory to view. Click the **ISL Trunks** drop-down if you want to view extension tunnels or trunks.
3. Filter results based on fabric.
4. Click the add filter (+) icon to narrow the results.
5. Customize which columns are displayed in the table and in which order.
6. Click the down arrow to display the action menu with additional actions you can perform.

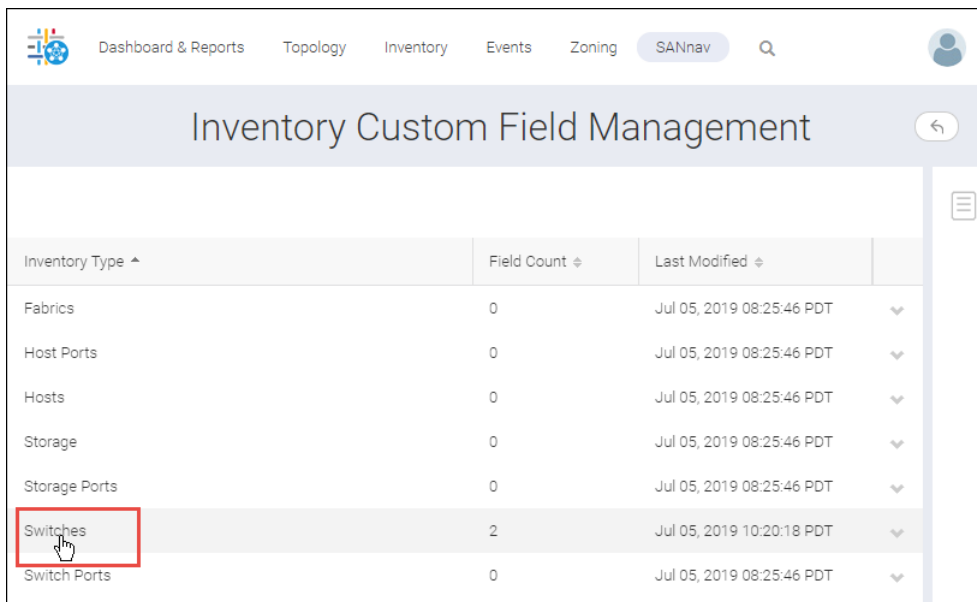
Note that selecting **Switches** in the inventory drop-down list displays information about logical switches. Selecting **Chassis** displays information about the physical chassis, including FRUs and logical switch membership.

6.6.1 Adding Custom Fields to a Managed Object

You can add additional columns to the tables displayed in the SANnav **Inventory** page, and populate the columns with customized values. You can then filter the information based on these values.

For example, suppose you want to be able to identify switches by the location of their data center. The following procedure describes how to add and populate a new column, **Data Center**, for switches.

1. Click **SANnav** in the navigation bar, and then select **Services > Inventory Custom Fields Management**.
2. In the table, select the type of inventory for which you want to add custom fields.
For this example, select **Switches**.

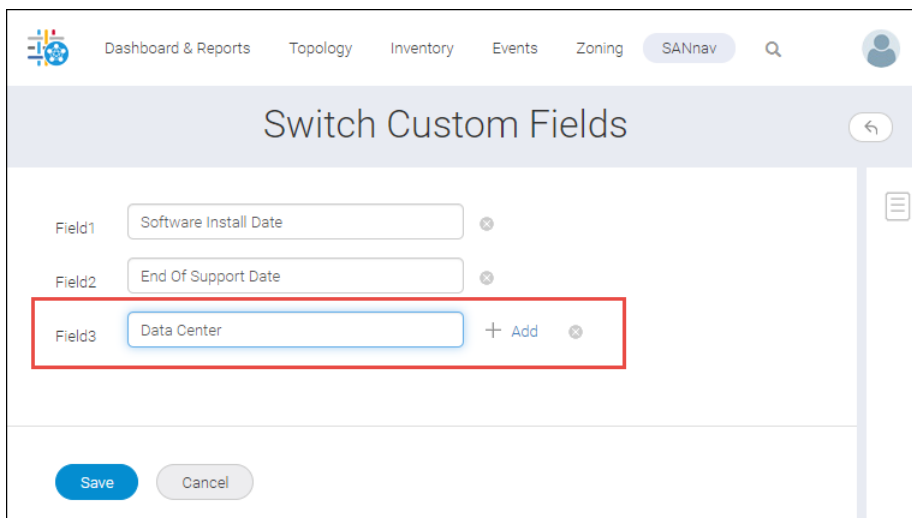


Inventory Type ^	Field Count ↕	Last Modified ↕	
Fabrics	0	Jul 05, 2019 08:25:46 PDT	▼
Host Ports	0	Jul 05, 2019 08:25:46 PDT	▼
Hosts	0	Jul 05, 2019 08:25:46 PDT	▼
Storage	0	Jul 05, 2019 08:25:46 PDT	▼
Storage Ports	0	Jul 05, 2019 08:25:46 PDT	▼
Switches	2	Jul 05, 2019 10:20:18 PDT	▼
Switch Ports	0	Jul 05, 2019 08:25:46 PDT	▼

3. Type the name of the new column in the empty field.

If the field is already populated, click **Add** to add a new field. You can add up to 10 custom fields.

Note that in this example, two custom fields, **Software Install Date** and **End Of Support Date**, are already defined for switches.



Field1: Software Install Date

Field2: End Of Support Date

Field3: Data Center + Add

Save Cancel

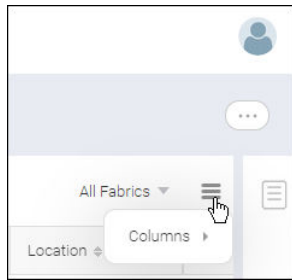
If you want to delete a custom field, click the **X** next to the field. Be aware, however, that when you delete a custom field, any values that were in this field are also deleted.

4. Click **Save**.

5. Display the custom inventory columns.

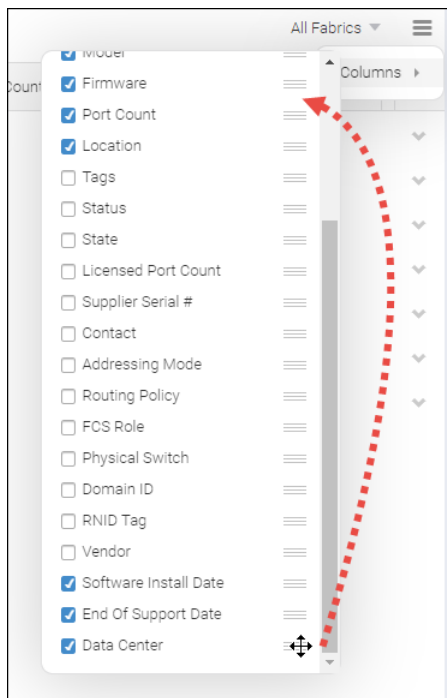
a. Click **Inventory** in the navigation bar, and then select **Switches** from the drop-down list.

- b. Click the hamburger icon (☰) on the right side of the window, and select **Columns**.

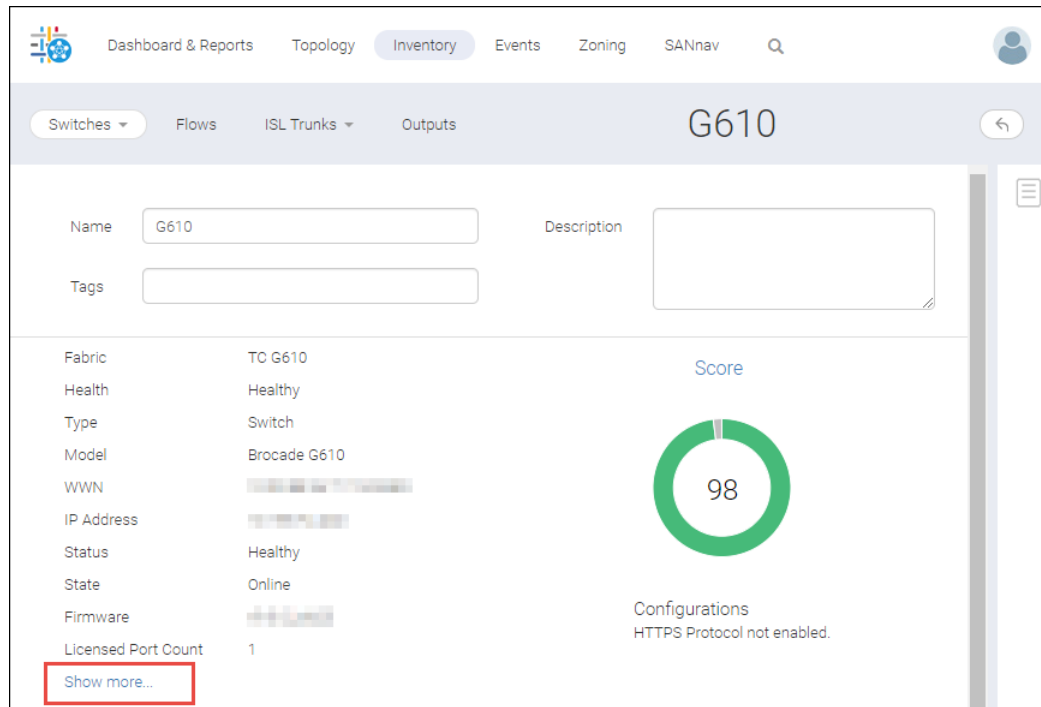


A list of all possible columns displays. User-defined columns are listed at the end.

- c. Scroll down the list and select the columns that you want to display. If you want to rearrange the columns, click the move icon (☰) and drag the column up or down. Click anywhere outside the list window to close it.



6. Populate the custom inventory fields.
- On the **Inventory** page, click the name of the item that you want to modify.
For this example, click the name of the switch that you want to modify.
The details page displays.
 - Click **Show more** to display additional details, including the custom fields.



c. Enter values for the custom fields.

Custom fields are added at the end, so you might need to scroll down to see them.

d. Scroll to the bottom of the window, and click **Save**.

NOTE

If you leave the window without clicking **Save**, there is no warning, and your changes are not saved.

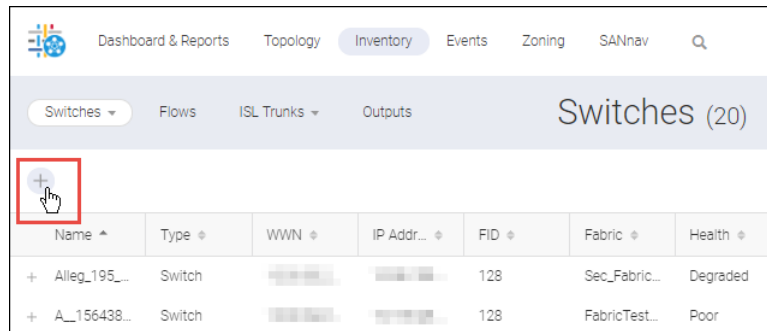
The **Inventory** page displays the custom columns and populated values. You can now use these values in searches and filters of the inventory.

6.6.2 Identifying Switches to Plan for an Upgrade

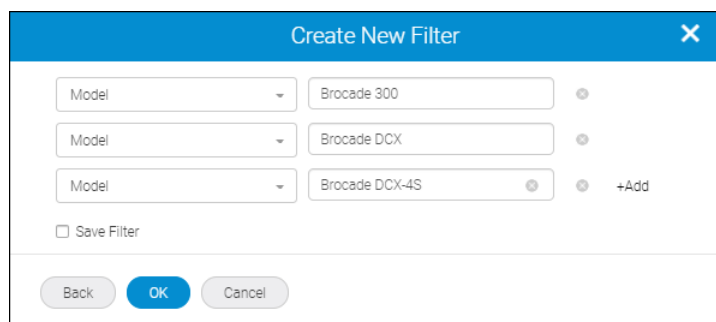
Assume that you want to upgrade all Gen 4 switches in the SAN. You can use tags and filters to identify the Gen 4 switches.

This task shows how you can use tags to tag switches according to product family. Then you can filter the inventory view to display only the Gen 4 switches.

1. Click **Inventory** in the navigation bar, and then select **Switches** from the drop-down list.
2. Filter the switch inventory to display only Gen 4 switch models.
For example, the Brocade 300, Brocade DCX, and Brocade DCX-4S are Gen 4 switches, so filter the switches with model "300" or "DCX".
 - a. Click the **+** icon in the upper left of the window to add a filter.



- b. Click **Create New** in the **Add Filter** dialog.
- c. Select **Model** from the drop-down list, and enter the model name ("Brocade 300").



- d. Click **+Add** to create a second filter for the switch model "Brocade DCX" and again for switch model "Brocade DCX-4S".

You must spell out the switch model names entirely (use "Brocade DCX" and not "DCX") because when the same attribute is used more than once in a filter, wildcards are not accepted and the values must be an exact match.

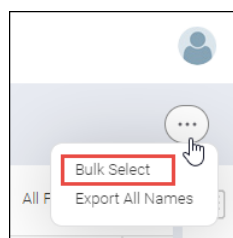
- e. Click **OK** to close the dialog.

The inventory page displays those switches with model Brocade 300, Brocade DCX, or Brocade DCX-4S.

3. Tag each switch according to product family.

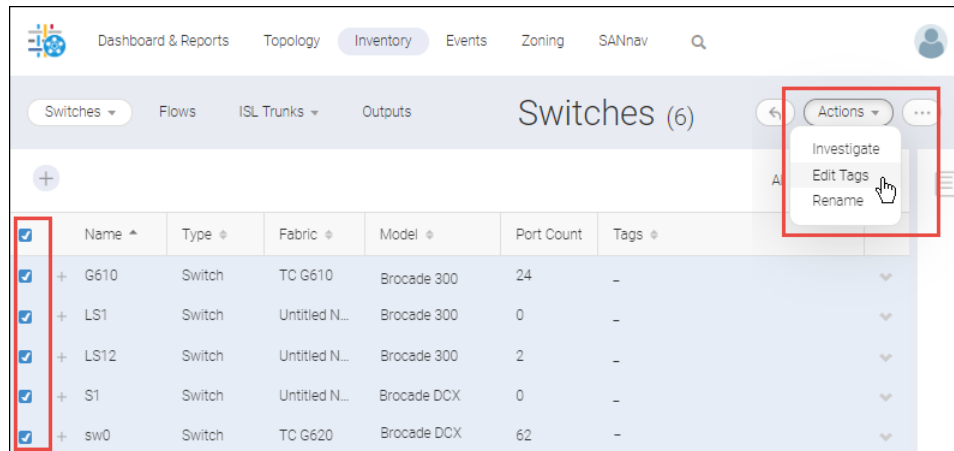
You can use bulk tagging to assign tags to a group of switches at one time.

- a. Click the More button (), and select **Bulk Select**.



- b. Select the checkboxes for the switches that you want to tag, and then click **Actions > Edit Tags** in the upper-right corner of the window.

For this example, select the switches that are model Brocade 300 and Brocade DCX.



- c. Enter the new tag ("Gen 4") and click **OK**.

NOTE

If you do not see the tags in the **Inventory** page, click the hamburger icon (☰), click **Columns**, and make sure that the **Tags** column is selected.

Now that the Gen 4 switches are tagged, whenever you want to see the list of Gen 4 switches, you can create a filter for Tags = "Gen 4". You can perform similar steps to tag the Gen 5 and Gen 6 switches.

6.6.3 Putting a Switch in Maintenance Mode

In SANnav Management Portal, when you want to perform maintenance on a switch, such as upgrading firmware or gathering SupportSave data, you can put the switch in maintenance mode to stop monitoring performance and receiving alerts.

Putting a switch in maintenance mode is done at the chassis level.

- Open the details page for the chassis.
 - Click **Inventory** in the navigation bar, and then select **Chassis** from the drop-down list.
 - Locate the chassis in the table, click the down arrow in the rightmost column, and select **View** from the action menu.

The chassis details page displays.

- Scroll down to the bottom of the details page, and select one of the maintenance mode options:
 - Select **Set Maintenance Mode** to put the chassis in maintenance mode immediately.
 - Select **Schedule Maintenance Mode** to set a time in the future for maintenance mode to start.

You can optionally set an end date and time when maintenance mode ends.

The screenshot shows the SANnav management portal interface. At the top, there are navigation tabs: Dashboard & Reports, Topology, Inventory (selected), Events, Zoning, and SANnav. Below the navigation, there is a header for the chassis 'swd77' with a 'Chassis' dropdown menu highlighted by a red box. Underneath, there are tabs for 'Flows', 'ISL Trunks', and 'Outputs'. A search bar shows '3 Items' and the title 'Fans'. A table lists three fans with columns for Unit, Part Number, Speed (RPM), Tags, and Status. Below the table, there is a form with three checkboxes: 'Set Maintenance Mode' (checked and highlighted with a red box), 'End Date', and 'Schedule Maintenance Mode'. At the bottom, there are 'Save' and 'Cancel' buttons.

Unit	Part Number	Speed (RPM)	Tags	Status
1	-	11635	1158676480	On
2	-	11357	1159725056	On
3	-	11635	1160773632	On

3. Click **Save**.

If you did not set an end date, when the firmware upgrade or other maintenance operations are complete, go back to the chassis details page, uncheck **Set Maintenance Mode**, and click **Save** to put the chassis back in normal mode.

6.6.4 Disabling and Enabling a Switch

To disable or enable a switch, you must have the following:

- Element Manager - Product Administration privilege with read/write permission

To disable or enable a switch, follow the instructions below.

1. Open the details page for the switch.
 - a. Click **Inventory** in the navigation bar, and then select **Switches** from the drop-down list.
 - b. Locate the switch, click the down arrow to the right of the switch, and select **View** from the action menu. The switch details page displays.
2. Scroll down to the bottom of the details page and select **Disable Switch**.

The screenshot shows the SANnav Management Portal interface. At the top, there is a navigation bar with tabs for Dashboard & Reports, Topology, Inventory (selected), Events, Zoning, and SANnav. Below the navigation bar, there are sub-tabs for Switches (selected), Flows, ISL Trunks, and Outputs. The main header displays the switch ID 'swdb148'. A search bar shows '61 Items' and the title 'Switch Ports'. A table lists the following ports:

Name	Type	WWN	Tags	Status	State	Speed	Action
ge9	GigE-Port	-	-	Enabled	Offline	10 Gb/s	Investigate, Decommission, Recommission
ge7	GigE-Port	-	-	Enabled	Offline	10 Gb/s	Investigate, Decommission, Recommission
port24	U-Port	20:18:88:...	-	UNKNO...	Offline	-	Investigate, Decommission, Recommission
ge8	GigE-Port	-	-	Enabled	Offline	10 Gb/s	Investigate, Decommission, Recommission

Below the table, there are checkboxes for 'Port Optics' and 'Disable Switch' (highlighted with a red box). At the bottom, there are 'Save', 'Cancel', and 'View in WebTools' buttons.

3. Click **Save**.

4. Click **OK** in the confirmation dialog.

When you disable a switch, the switch state changes to Offline.

When you want to enable the switch, go back to the switch details page, uncheck **Disable Switch**, and click **Save**.

6.6.5 Disabling and Enabling a Switch Port

1. Open the details page for the switch.

a. Click **Inventory** in the navigation bar, and then select **Switch Ports** from the drop-down list.

b. Locate the switch port, click the down arrow in the rightmost column, and select **View** from the action menu.

The switch port details page displays.

2. Scroll down to the bottom of the details page and select **Disable**.

Select the **Persist** option if you want the ports to remain disabled across power cycles, switch reboots, and switch enables.

The screenshot shows the SANnav Management Portal interface. At the top, there is a navigation bar with tabs for Dashboard & Reports, Topology, Inventory (selected), Events, Zoning, and SANnav. Below the navigation bar, there is a sub-navigation bar with a dropdown menu labeled 'Switch Ports' (highlighted with a red box), and other options: Flows, ISL Trunks, and Outputs. The main content area displays the configuration for 'slot8 port18'. It includes a form with fields for Name (slot8 port18), Description, and Tags. Below the form is a table of port details:

Type	F-Port
WWN	20:D2:C4:F5:7C:66:9F:50
State	Online
Status	Online
Slot/Port #	8/18
Fabric	Fabric_A
Switch	Brocade_X6_31
Protocol	FC
Attached Port	10:00:8C:7C:FF:B0:80:01
Connected Device	WINDOWS-42SRTG2

Below the table, there is a 'Show more...' link. At the bottom of the configuration area, there are two checkboxes: 'Disable' (checked, highlighted with a red box) and 'Persistent' (unchecked). At the very bottom, there are several buttons: Save (highlighted in blue), Cancel, Schedule, CreateZone, Investigate, and Decommission.

3. Click **Save**.

4. Click **OK** in the confirmation dialog.
The port status changes to Disabled.

When you want to enable the switch, go back to the switch port details page, uncheck **Disable**, and click **Save**.
Click **OK** in the confirmation dialog.

6.6.6 Decommissioning E_Ports

Port decommissioning provides a mechanism to remove an E_Port from use (decommission) without frame loss and to put it back in use (recommission).

You must have Element Manager - Product Administration privilege with read-write access.

You can decommission only E_Ports and F_Ports. The following are not supported:

- Mixed-type port (E_Port and F_Port) decommissioning
- QSFP-level decommissioning

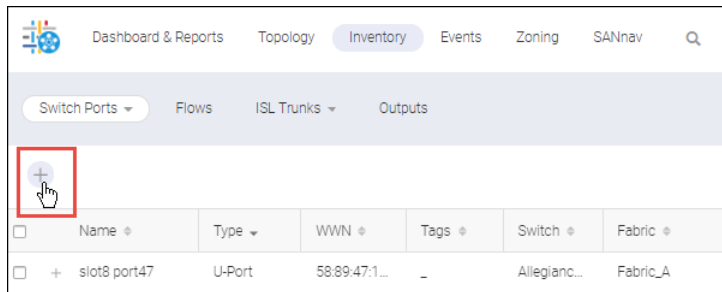
The following steps show how you can decommission a single E_Port. You can also use the bulk select feature to decommission several E_Ports at one time.

1. Click **Inventory** in the navigation bar, and then select **Switch Ports** from the drop-down list.

2. Create a filter to display only E_Ports.

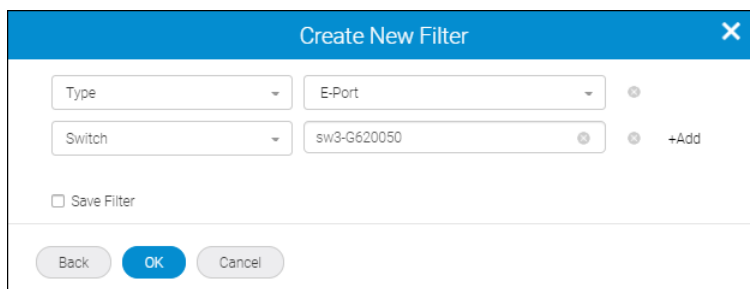
It is not necessary to create a filter, but filtering the inventory is an easy way to see only E_Ports.

- a. Click the **+** icon in the upper left of the window to add a filter.



- b. Click **Create New** in the **Add Filter** dialog.
- c. Select **Type** from the first drop-down list, and select **E-Port** from the next drop-down list.

You can also click **+Add** to add additional filters. The following filter displays all E_Ports for a particular switch.



- d. Click **OK** to return to the **Inventory** page.

3. Locate the port that you want to decommission, click the down arrow in the rightmost column, and select **Decommission**.

4. Click **OK** in the confirmation dialog.

The port status changes to Decommissioning. It takes some time for the port to decommission.

When you want to recommission the port, select **Recommission** from the rightmost column.

6.6.7 Decommissioning F_Ports

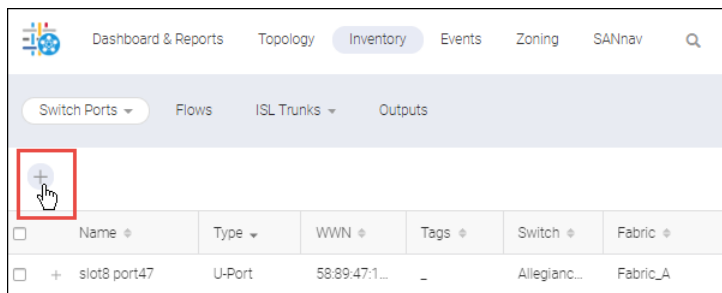
Port decommissioning provides a mechanism to remove an F_Port from use (decommission) without frame loss and to put it back in use (recommission).

Prerequisites for decommissioning F_Ports:

- You must have Element Manager - Product Administration privilege with read-write access.
- The CIMOM servers corresponding to the F_Ports must be registered with SANnav.
- The F_Ports must be connected to trusted devices.
- All Fabric OS switches in the fabric must be running v7.4.0 or higher.

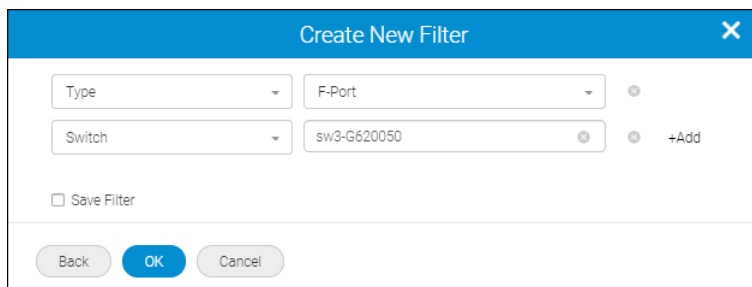
The following steps show how you can decommission a single F_Port. You can also use the bulk select feature to decommission several F_Ports at one time.

1. Click **Inventory** in the navigation bar, and then select **Switch Ports** from the drop-down list.
2. Create a filter to display only F_Ports.
 - a. Click the **+** icon in the upper left of the window to add a filter.



- b. Click **Create New** in the **Add Filter** dialog.
- c. Select **Type** from the first drop-down list, and select **F-Port** from the next drop-down list.

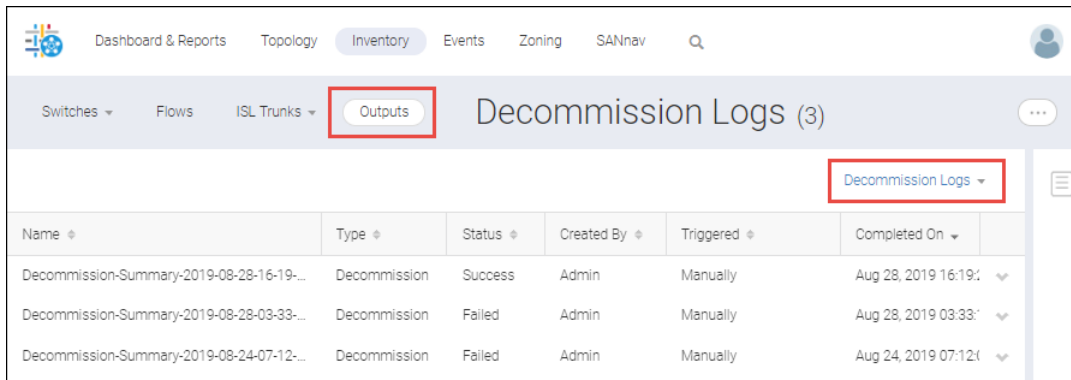
You can also click **+Add** to add additional filters. The following filter displays all F_Ports for a particular switch.



- d. Click **OK** to return to the **Inventory** page.
3. Locate the port that you want to decommission, click the down arrow in the rightmost column, and select **Decommission**.

A confirmation dialog displays, with additional options. By default, both the F_Port (switch port) and N_Port (device port) are decommissioned, unless the N_Port is the last enabled N_Port, in which case it is not decommissioned.
4. Optionally change the default settings in the **Decommission Ports** dialog.
 - Select **Force Decommission N-port** if you want to decommission the N_Port even if it is the last enabled N_Port.
 - Select **Keep switch port enabled** if you want to decommission only the N_Port and not the F_Port.
5. Click **OK** in the confirmation dialog.

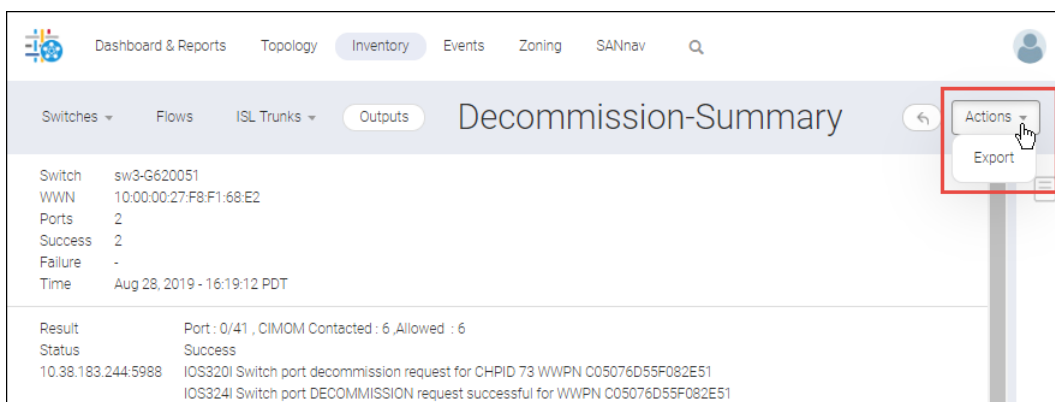
The port status changes to **Decommissioning**. It takes some time for the port to decommission.
6. To view the decommissioning results, click **Outputs** in the subnavigation bar, and then select **Decommission Logs** from the drop-down on the right.



Name	Type	Status	Created By	Triggered	Completed On
Decommission-Summary-2019-08-28-16-19-...	Decommission	Success	Admin	Manually	Aug 28, 2019 16:19:12
Decommission-Summary-2019-08-28-03-33-...	Decommission	Failed	Admin	Manually	Aug 28, 2019 03:33:12
Decommission-Summary-2019-08-24-07-12-...	Decommission	Failed	Admin	Manually	Aug 24, 2019 07:12:12

7. Click the log that you want to view.

In the log details page, you can export the log as an HTML file.



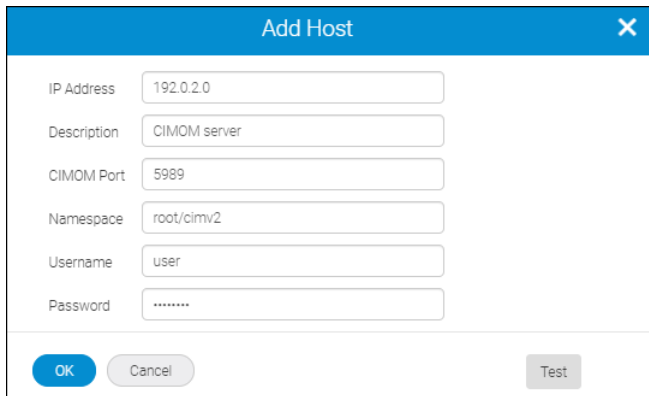
Switch	sw3-G620051
WWN	10:00:00:27:F8:F1:68:E2
Ports	2
Success	2
Failure	-
Time	Aug 28, 2019 - 16:19:12 PDT
Result	Port : 0/41 , CIMOM Contacted : 6 , Allowed : 6
Status	Success
10.38.183.244:5988	IOS320I Switch port decommission request for CHPID 73 WWPN C05076D55F082E51 IOS324I Switch port DECOMMISSION request successful for WWPN C05076D55F082E51

When you want to recommission the port, select **Recommission** from the rightmost column in the switch port inventory page.

6.6.8 Registering a CIMOM Server for F_Port Decommissioning

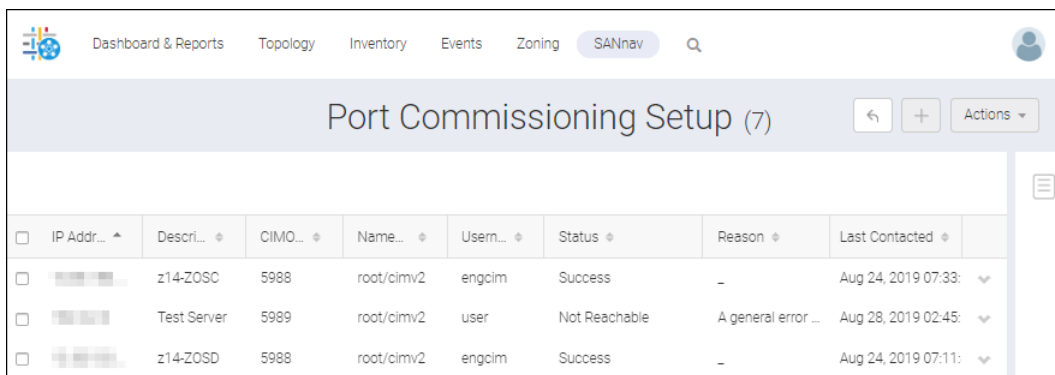
Before you can decommission F_Ports, you must register the CIMOM servers corresponding to those F_Ports. It is then up to the CIMOM servers to honor the decommission requests.

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Port Commissioning Setup**.
2. Click the **+** icon in the upper right corner of the page, and then click **Add**.
You can alternatively click **Import** to import CIMOM server details from a CSV file.
3. Enter the IP address and login credentials for the CIMOM server.
The IP address can be in either IPv4 or IPv6 format. Click the **Test** button to test the connection to the server.



4. Click **OK**.

The CIMOM server displays in the list. If the connection test failed, the reason for the failure is listed in the **Reason** column.



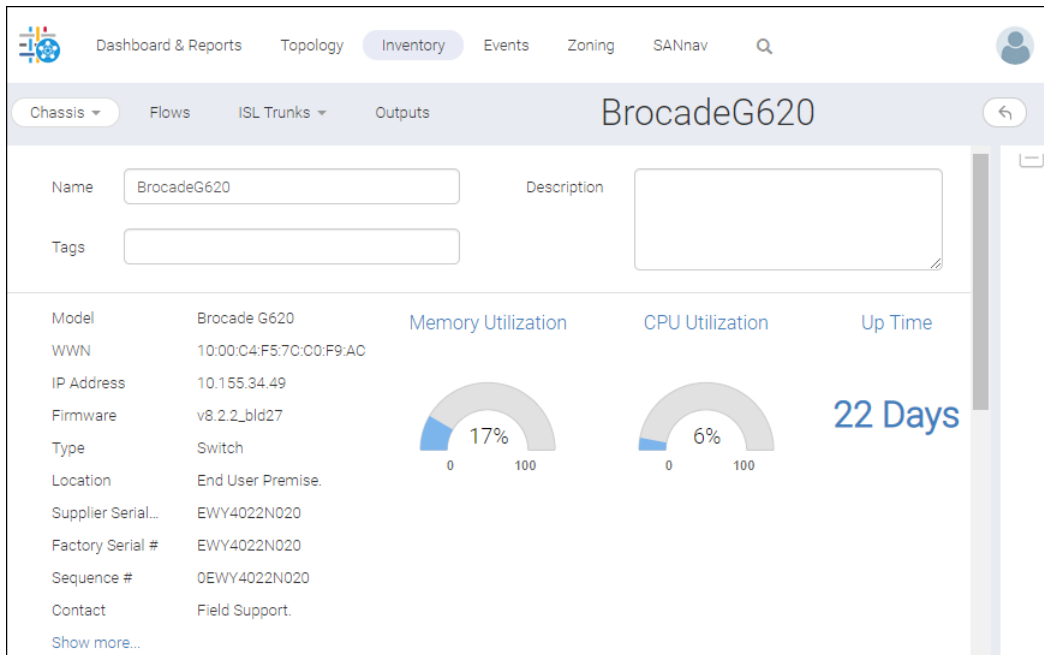
<input type="checkbox"/>	IP Addr... ^	Descri... ♦	CIMO... ♦	Name... ♦	Usen... ♦	Status ♦	Reason ♦	Last Contacted ♦
<input type="checkbox"/>	z14-ZOSC	z14-ZOSC	5988	root/cimv2	engcim	Success	-	Aug 24, 2019 07:33: ▾
<input type="checkbox"/>	Test Server	Test Server	5989	root/cimv2	user	Not Reachable	A general error ...	Aug 28, 2019 02:45: ▾
<input type="checkbox"/>	z14-ZOSD	z14-ZOSD	5988	root/cimv2	engcim	Success	-	Aug 24, 2019 07:11: ▾

6.6.9 Viewing Physical Switch Properties

The chassis details page includes information about switch performance as well as blade, power supply, and fan details.

1. Click **Inventory** in the navigation bar, and then click **Chassis** from the drop-down list.
2. Click the name of the chassis you want to view.

The chassis details page displays. In addition to showing chassis properties on the left side of the page, the page includes widgets showing memory utilization, CPU utilization, and the chassis up time.




3. Scroll down the page to view details about logical switches, blades, power supplies, and fans.

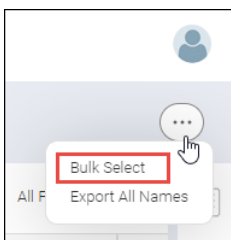
6.6.10 Renaming Switch Ports, Switches, and Fabrics

You can rename switch ports, switches, and fabrics individually or in bulk. For switch ports, you can create a naming convention and automatically rename switch ports, based on their port attributes.

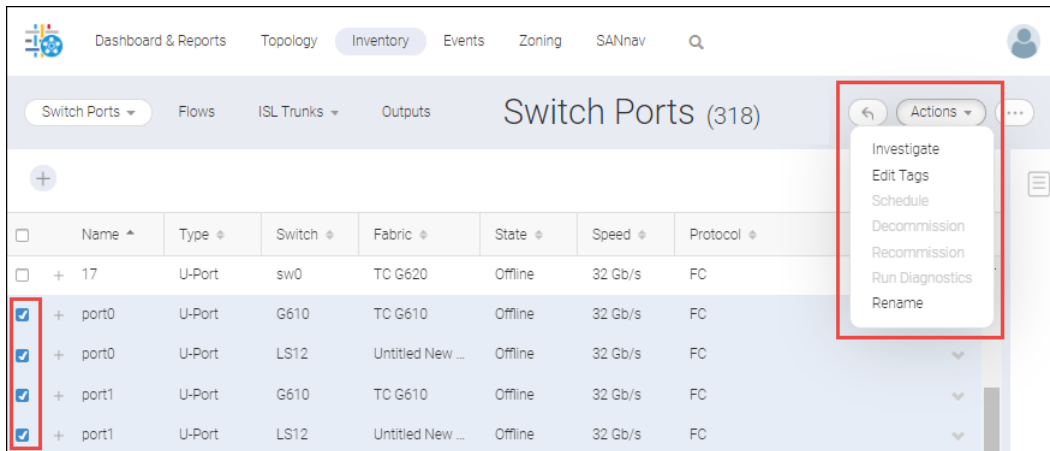
To rename objects individually, go to the details view for the object and enter a new name in the **Name** field. This is the only way you can rename a chassis. Chassis objects cannot be renamed in bulk.

You can rename objects in bulk from the inventory page. The following steps describe how to automatically rename switch ports. The procedure is similar for renaming switches and fabrics, except that you cannot use the automatic function.

1. Click **Inventory** in the navigation bar, and then select **Switch Ports** from the drop-down list.
2. Click the More button (), and select **Bulk Select**.



3. Select the ports you want to rename, and click **Edit > Rename**.
You cannot rename GigE ports. If you have selected any GigE ports, the **Rename** option is not available.



4. Enter the naming values in the **Rename** dialog.

You can select **Rename manually** to enter names individually. For switch ports, an easier way to generate names is to select **Rename automatically**, and then select the components that compose the name.

The following example shows how switch port names will be generated using a concatenation of switch name, slot number, and port number, separated by underscores. Note that the slot number applies only to directors. If the port is not on a director, then the slot number component is ignored.

Rename [X]

Rename automatically
 Rename manually

New Name: +Add

Separator:

Example: Switch_Slot Number_Port Number

You must ensure that the resulting name follows the rules for Fabric OS switch port names. For example, if you select a custom column as one of the components, and the value in the custom column contains a special character that is not allowed in a switch port name, the name is invalid.

For fabrics and switches, only the manual rename option is available.

5. Click **OK**.

In this example, the ports are on fixed-port switches and not directors, so the slot number is ignored, and the format is SwitchName_PortNumber.

	Name	Type	Switch	Fabric	State	Speed	Protocol
<input type="checkbox"/>	G610_1	U-Port	G610	TC G610	Offline	32 Gb/s	FC
<input type="checkbox"/>	G610_0	U-Port	G610	TC G610	Offline	32 Gb/s	FC
<input type="checkbox"/>	LS12_0	U-Port	LS12	Untitled Ne...	Offline	32 Gb/s	FC
<input type="checkbox"/>	LS12_1	U-Port	LS12	Untitled Ne...	Offline	32 Gb/s	FC
<input type="checkbox"/>	slot4 port0	U-Port	SWBD165	TC X6-4	Offline	32 Gb/s	FC
<input type="checkbox"/>	slot4 port1	U-Port	SWBD165	TC X6-4	Offline	32 Gb/s	FC

6.6.11 Creating Host and Storage Enclosures

In SANnav Management Portal you can create logical host and storage enclosures so that you can view the hosts and storage in the topology.

SANnav Management Portal discovers host ports and storage ports, but does not always discover hosts and storage.

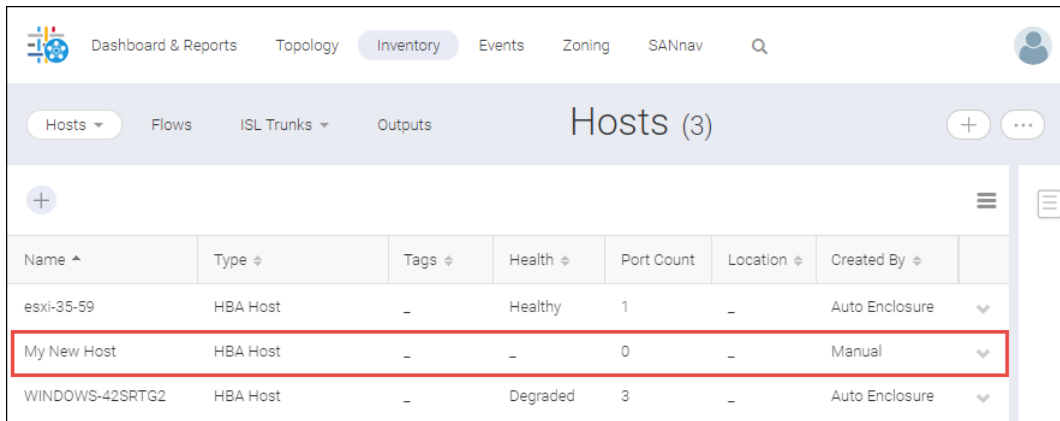
The **Inventory** page displays a list of hosts that SANnav knows about. Some hosts (ESXi hosts) are automatically discovered through vCenter discovery. Some hosts (FDMI hostname-based) are enclosures that are created automatically during discovery. All other hosts must be manually created.

SANnav does not discover any storage devices. You must manually create logical storage enclosures.

The following procedure shows how to create a host enclosure. The steps for creating a storage enclosure are similar.

1. Click **Inventory** in the navigation bar, and then select **Hosts** from the drop-down list.
If you are creating a storage enclosure, select **Storage** from the drop-down list.
2. Click the **+** button in the upper right corner of the window to add a storage or host.
3. Enter a name for the enclosure and additional information, and click **Save**.
Host and storage names must be unique.

The host displays in the **Inventory** page. Notice that the **Created By** column display "Manual", which means you manually created this enclosure.



Name	Type	Tags	Health	Port Count	Location	Created By
esxi-35-59	HBA Host	-	Healthy	1	-	Auto Enclosure
My New Host	HBA Host	-	-	0	-	Manual
WINDOWS-42SRTG2	HBA Host	-	Degraded	3	-	Auto Enclosure


You can view this new host in the **Topology** page, but at this point, no ports are mapped to the enclosure. The next step is to map ports to the host or storage enclosure.

6.6.12 Mapping Host and Storage Ports

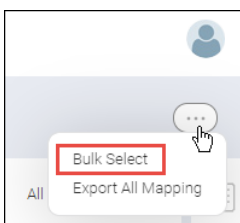
SANnav Management Portal does not automatically map host and storage ports to host and storage enclosures. You should map these ports to host and storage enclosures so you can group and view these ports in the Topology view.

It is recommended that you create zone aliases for your host and storage ports, so you can see which ports to map to which enclosure.

The following procedure shows how to map host ports to a host enclosure, and then view the host in the Topology. The steps for mapping storage ports are similar.

1. Click **Inventory** in the navigation bar, and then select **Host Ports** from the drop-down list.
If you are mapping storage ports, select **Storage Ports** from the drop-down list.
2. Click the More button (), and click **Bulk Select**.

Using the **Bulk Select** option allows you to map several ports at the same time.



A column of checkboxes displays on the leftmost side of the table.

3. Select the checkboxes for the ports that you want to map, and then click **Actions** > **Map** in the upper right corner of the window.

Notice that the **Host** (or **Storage**) column indicates whether the port has already been mapped to an enclosure.

The screenshot shows the 'Inventory' page with a table titled 'Host Ports (36)'. The table has columns for Zone Alias, WWN, Host, Fabric, Connected Product P..., and Connected Product. The 'Host' column contains values like 'MS_Exchange' and 'demo_alias'. A red box highlights the 'Map' option in the 'Actions' dropdown menu.

Zone Alias	WWN	Host	Fabric	Connected Product P...	Connected Product	
<input checked="" type="checkbox"/>	MS_Exchange	10:00:00:1...	-	Fabric_A	port35_3	Wedge_49
<input checked="" type="checkbox"/>	MS_Exchange	10:00:00:9...	-	Fabric_A	port34_3	Wedge_49
<input checked="" type="checkbox"/>	MS_Exchange	10:00:00:1...	-	Fabric_A	port33_3	Wedge_49
<input type="checkbox"/>	MS_Exchange	10:00:00:1...	-	Fabric_A	port32_3	Wedge_49
<input checked="" type="checkbox"/>	MS_Exchange	10:00:00:1...	-	Fabric_A	port32_4	Wedge_48
<input checked="" type="checkbox"/>	MS_Exchange	10:00:00:1...	-	Fabric_A	port33_4	Wedge_48
<input type="checkbox"/>	demo_alias	10:00:00:1...	-	Fabric_A	port44_3	Wedge_49
<input type="checkbox"/>	demo_3	20:03:C4:...	-	Fabric_A	port3_4	Wedge_49

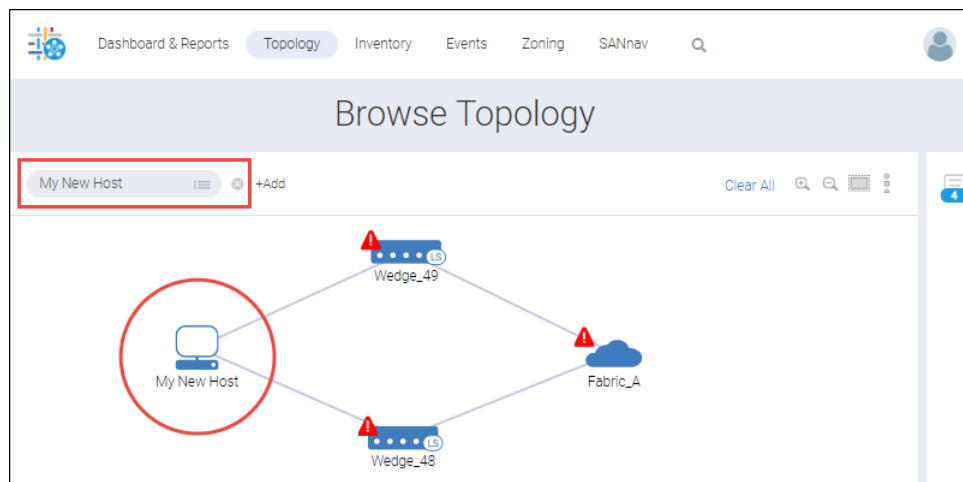
4. In the dialog, select the device to which you want to map the ports, and click **OK**.

If you have not yet created a host or storage enclosure, you can do so now, by clicking the **Create New** button.

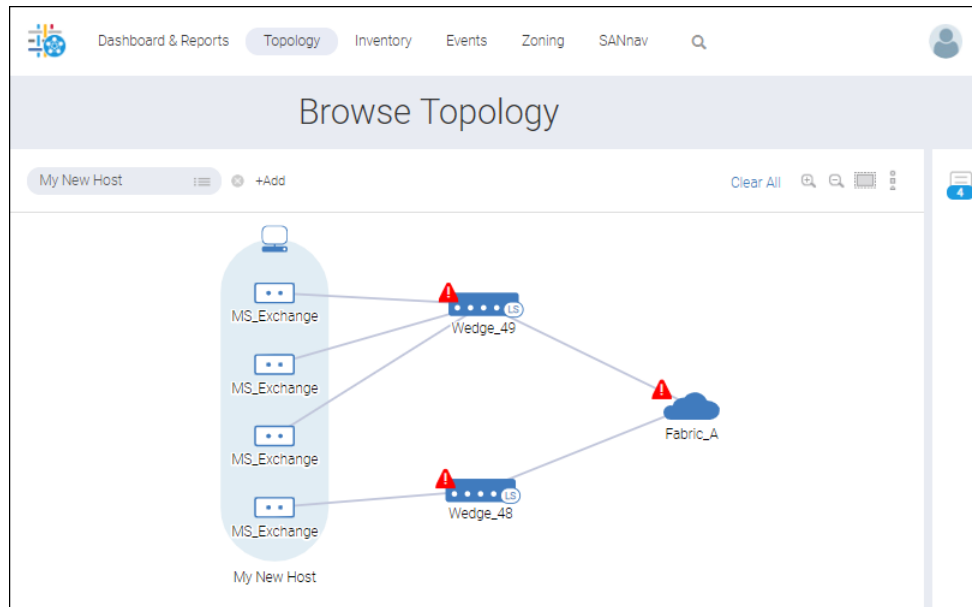
In the **Inventory** page, the **Host** column now shows the host enclosure to which the ports are mapped. You might need to re-sort the columns to see the ports. Now when you view the device in the **Topology** page, you can see the ports that are mapped to it.

5. Perform the following steps to view the host topology.
- Select **Hosts** from the drop-down list.
 - Click the down arrow in the rightmost column of the host that you want to display, and select **View in Topology**.

Notice that the topology is shown in the context of the host.




- Hover over the host and click the **+** icon to display the mapped ports.



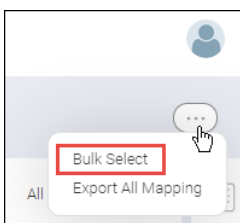
6.6.13 Converting Initiator and Target Device Types

You can change the device type of host and storage ports. For example, you can change a host port to be a target port, and you can change a storage port to be an initiator port.

The following procedure shows how to convert several ports at one time. You can also convert a single port from the port details page.

1. Click **Inventory** in the navigation bar, and then select **Host Ports** or **Storage Ports** from the drop-down list, depending on device type of the object you want to change.
2. Click the More button (), and select **Bulk Select**.

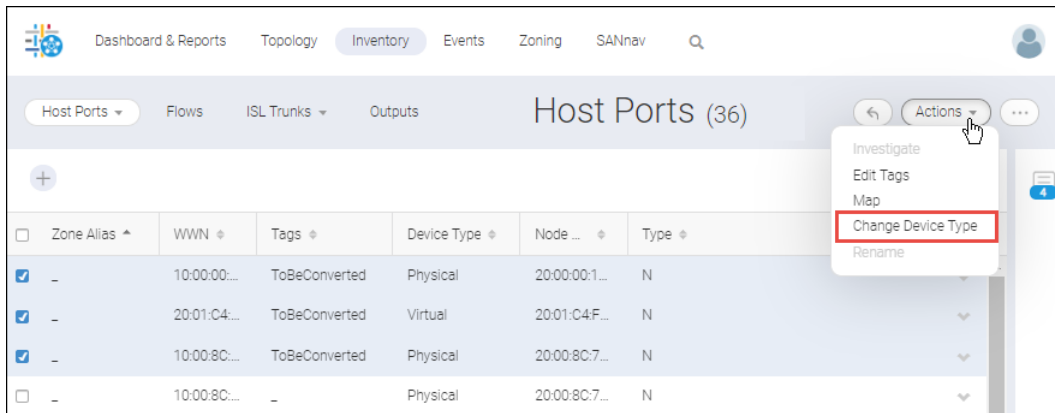
Using the bulk select option allows you to convert several ports at the same time.



A column of checkboxes displays on the leftmost side of the table.

3. Select the checkboxes for the ports that you want to convert, and then click **Actions > Change Device Type** in the upper right corner of the window.

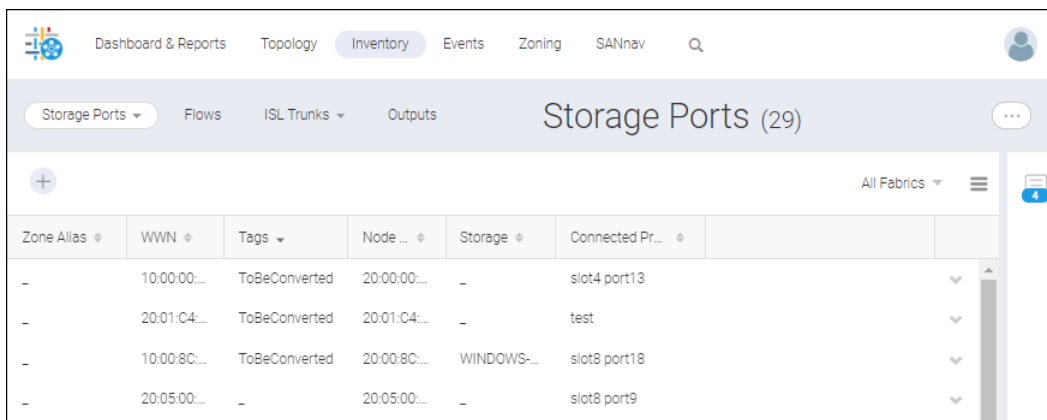
Notice that for this example, the affected ports were previously tagged with **ToBeConverted** tags, and then the Host Port inventory was sorted on tags.



The ports no longer display in the inventory.

4. Select the new Inventory context from the drop-down list to verify the change.

For this example, the host ports were converted to targets and now display in the **Storage Ports** inventory context.



6.6.14 Launching Web Tools

Launch Web Tools to perform more detailed configuration management for a switch.

You must know the login credentials for the switch to log in to Web Tools.

1. Click **Inventory** in the navigation bar, and then select **Switches** from the drop-down list.
2. Locate the switch, click the down arrow to the right of the switch, and select **View in WebTools** from the action menu.
3. Provide the switch login credentials when prompted.

6.6.15 Managing Trunk Inventory

Information about trunks is displayed in the **ISL Trunks** tab of the **Inventory** page. From this page, you can view properties of the trunks and show details about the trunk links. You can also select one or more trunks and launch Investigate mode to view performance information.

The following steps show how to view information about the trunk members.

1. Click **Inventory** in the navigation bar, and then select **ISL Trunks > ISL Trunks** in the subnavigation bar.



The **ISL Trunks** page displays the list of trunks in tabular format.

2. Click the down arrow in the rightmost column of a trunk and select **Show Links**.

A pop-up window displays information about the trunk, including the trunk master and the switch and ports at each end of the trunk.

Port (1) ^	Port (1) Type *	Trunk (1) Info *	Port (2) *	Port (2) Type *	Trunk (2) Info *	Status *
0/34	E-Port	Master Port 0/35	0/34	E-Port	Master Port 0/39	Active
0/35	E-Port	Master	0/39	E-Port	Master	Active
0/38	E-Port	Master Port 0/35	0/38	E-Port	Master Port 0/39	Active
0/39	E-Port	Master Port 0/35	0/35	E-Port	Master Port 0/39	Active

3. Click **Close** to return to the **ISL Trunks** page.

6.6.16 Exporting Inventory Names and Mapping

In SANnav Management Portal, you can export a list of names of all fabrics, switches, Access Gateway switches, and switch ports. You can also export a list of host-storage mappings.

The exported file is downloaded to your local machine. The file is in CSV format. The names file looks like this:

WWN	NAME	TYPE	FCADDRESS
10:00:00:27:F8:37:29:8D	Edge-4	Fabric	
10:00:00:05:1E:75:5C:00	DCX-16	Fabric	
20:11:00:27:F8:37:29:8D	port17	Switch Port	191100


The mapping file looks like this:

Host/Storage Port WWN	FC Address	Host/Storage Name	Port Type
2D:B5:00:05:1E:0C:1C:1A	021c02	WIN2K8R2-35-43	Initiator
25:39:00:05:1E:0C:1C:1A	021c04	WIN2K8R2-35-43	Initiator
10:00:8C:7C:FF:B0:80:01	1fd200	WINDOWS-42SRTG2	Target

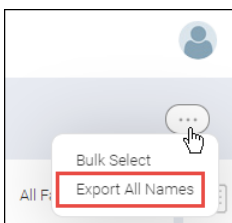
1. Click **Inventory** in the navigation bar.
2. Select an item from the inventory context drop-down list, depending on whether you want to export names or host-storage mapping.
 - If you want to export names, select **Switches**, **Switch Ports**, **Fabrics**, or **Chassis**.
 - If you want to export host-storage mapping, select **Hosts**, **Host Ports**, **Storage**, or **Storage Ports**.

It does not matter which specific item you select. The same list of names is exported whether you select **Switches** or **Fabrics**, and the same mapping is exported whether you select **Hosts** or **Storage Ports**.

Also, the selected network scope does not affect the list of exported names or mapping.

3. Click the **More** button () in the upper right corner of the page, and then select **Export All Names** or **Export All Mapping**.

The available option depends on the inventory context.



The names or mapping file is generated and downloaded.

6.6.17 Importing Inventory Names and Mapping

In SANnav Management Portal, you can import a list of names of all fabrics, switches, Access Gateway switches, and switch ports. You can also import a list of host-storage mappings, from a comma-separated values (CSV) file.

To import host and storage mappings, you must have the following:

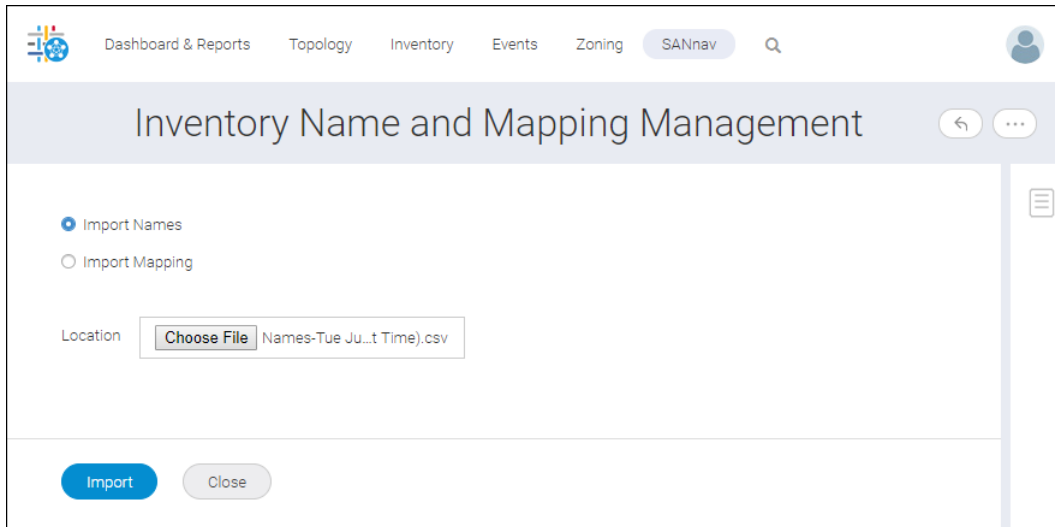
- Port Mapping — Host privilege with read/write permission
- Port Mapping — Storage privilege with read/write permission

To import names, you must have the following:

- Element Manager - Product Administration privilege with read/write permission

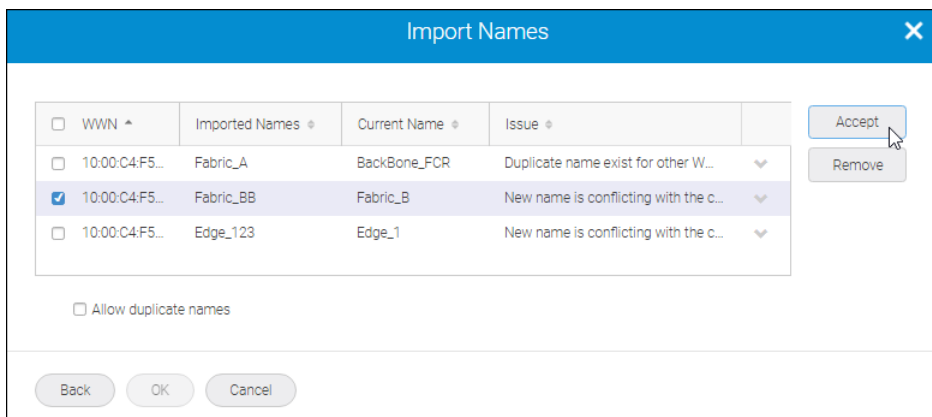
To import names and mapping, follow the instructions below.

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Inventory Name and Mapping Management**.
2. Select whether to import names or host-storage mapping, and click **Choose File** to browse to the file location.



3. Click **Import**.
4. Resolve any naming conflicts.

During the import, if conflicts arise, you are given a choice to accept all changes, reject all changes, or resolve changes one-by-one.



- Select the changes that you want to keep, and click **Accept**.
- Select the changes that you want to reject, and click **Remove**.

When all changes are resolved, click **OK**.

6.7 Topology Visualization

Using the 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 enables you to focus on the information in the topology view instead of a complex network of devices and connections.

The **Topology** page displays 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.

The following are the contexts for which you can display a topology:

- Fabric context: Displays all switches in the fabric and other directly connected fabrics.
- Switch context: Displays all fabrics, switches, and devices directly connected to the selected switch.
- Switch port context: Displays all entities connected to the selected switch port.
- Host or storage context: Displays the connectivity to edge switches, fabrics, and other devices that are zoned with the selected device.
- Host port or storage port context: Displays edge switches, fabrics, and other device ports that are zoned with the selected device port.
- Zone context: Displays all zone members, including involved fabrics.

Topology views are a snapshot in time, and they are not automatically updated.

The topology shows information related to discovered fabrics only. For this reason, it is recommended that, for FC Routing, you discover all fabrics (backbone and edge fabrics) in the same instance of SANnav Management Portal.

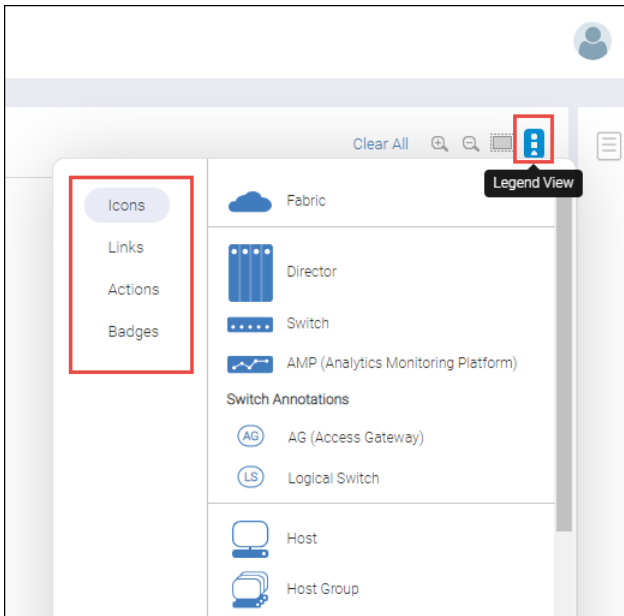
If the topology includes an Access Gateway, and that Access Gateway is present in more than one fabric, only one logical representation of the Access Gateway is shown when viewing topology from the host or storage context.

NOTE

The topology feature is available on SANnav Management Portal only. It is not available on SANnav Global View.

Understanding Topology Icons

Click the **Legend View** icon in the upper-right corner of the **Topology** window to display explanations of the graphics used in the topology.

Figure 26: Topology Legend View

In the legend dialog, click the links on the left to display icons, links, actions, and badges.

NOTE

If an icon on the topology page is grayed out, it means that the associated object is unavailable.

NOTE

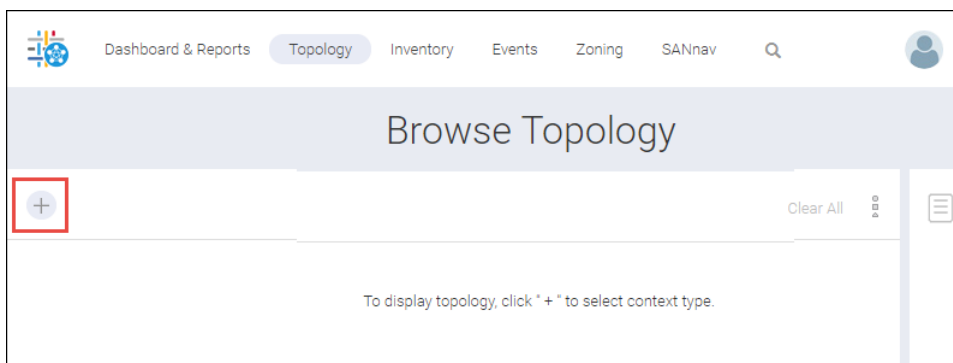
SANnav does not show IFL trunks in the topology.

6.7.1 Viewing the Fabric Topology

After you discover a fabric, you might want to view a pictorial representation of the fabric, including the switches, ports, and connected devices.

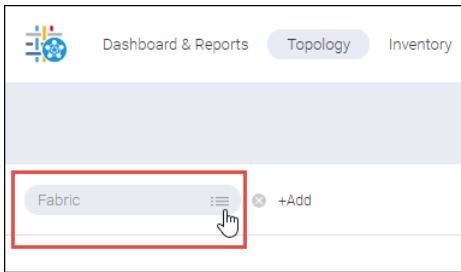
You can launch a topology view in several ways, including from the action menu on the **Inventory** page and **Health Summary** dashboard. The following procedure shows how to launch the topology view from the **Topology** page, by adding a context.

1. Click **Topology** in the navigation bar, and then click the **+** button to add a context.



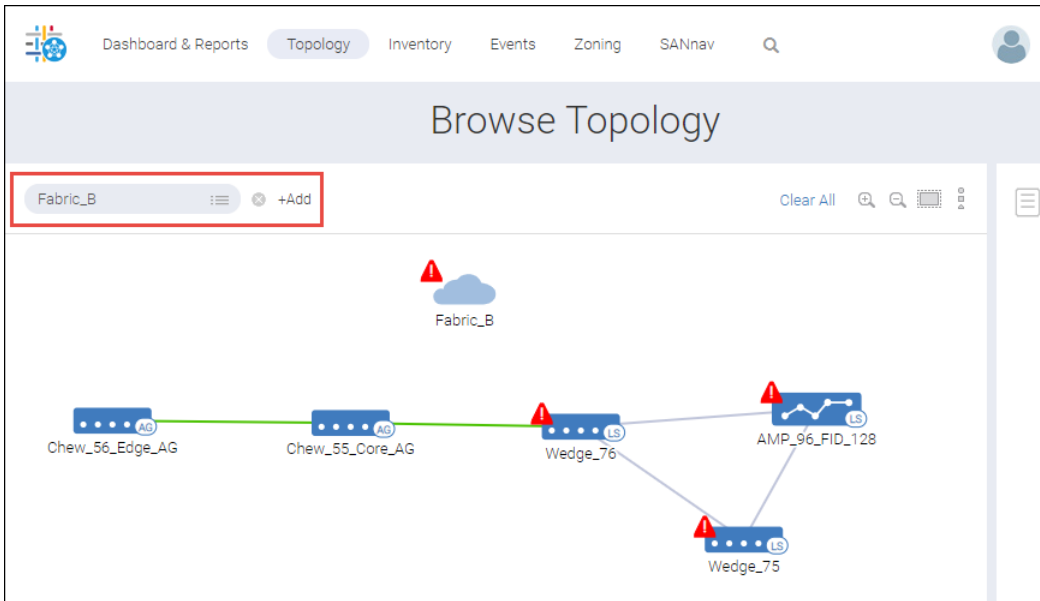
2. In the **Add Context Type** dialog, select the **Fabric** context, and click **OK**.

- 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.

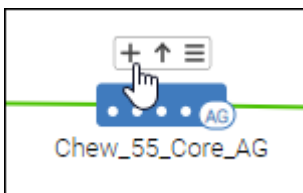


The **Browse Topology** page displays a pictorial view of the fabric. This is the fabric context, so the topology displays all switches in the fabric.

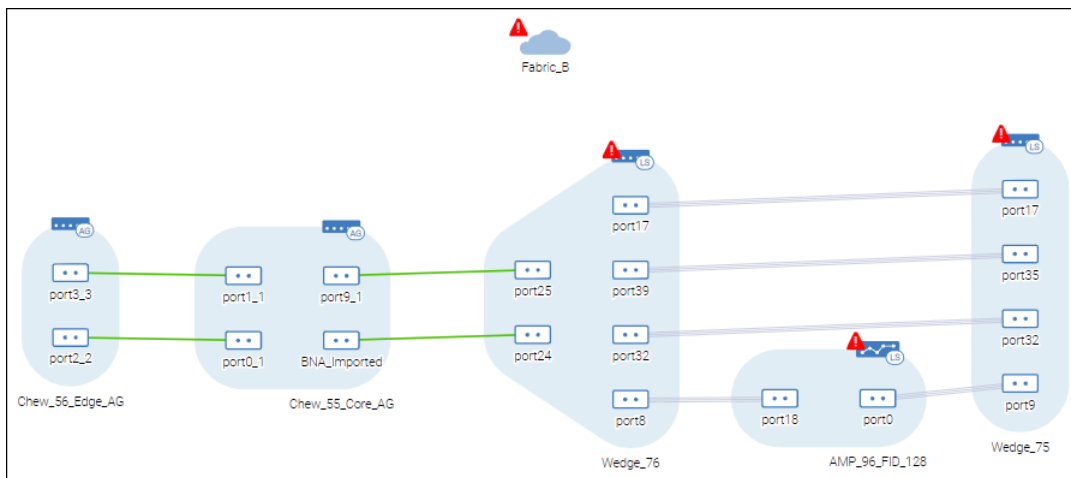
Note the fabric shown in the context navigation panel. This fabric has five switches. One of the switches is a Brocade Analytics Monitoring Platform (AMP).



- Hover the mouse over each switch and click the + icon to display the online ports.

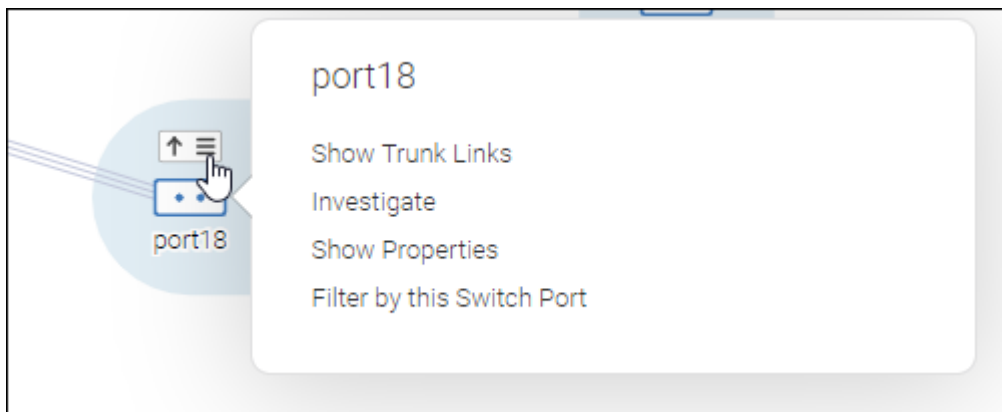


The topology now shows the online ports and the connections between them. (Virtual ports are not shown.) Notice that some the switches are connected with trunk links.

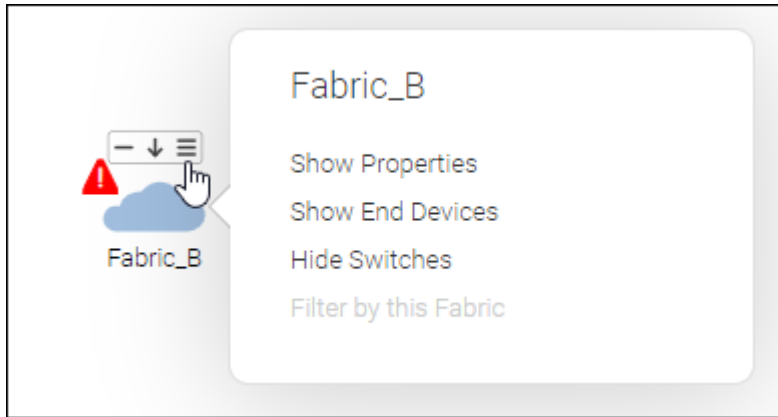
**NOTE**

If the number of connected ports is greater than 15, SANnav displays the ports in a tabular view.

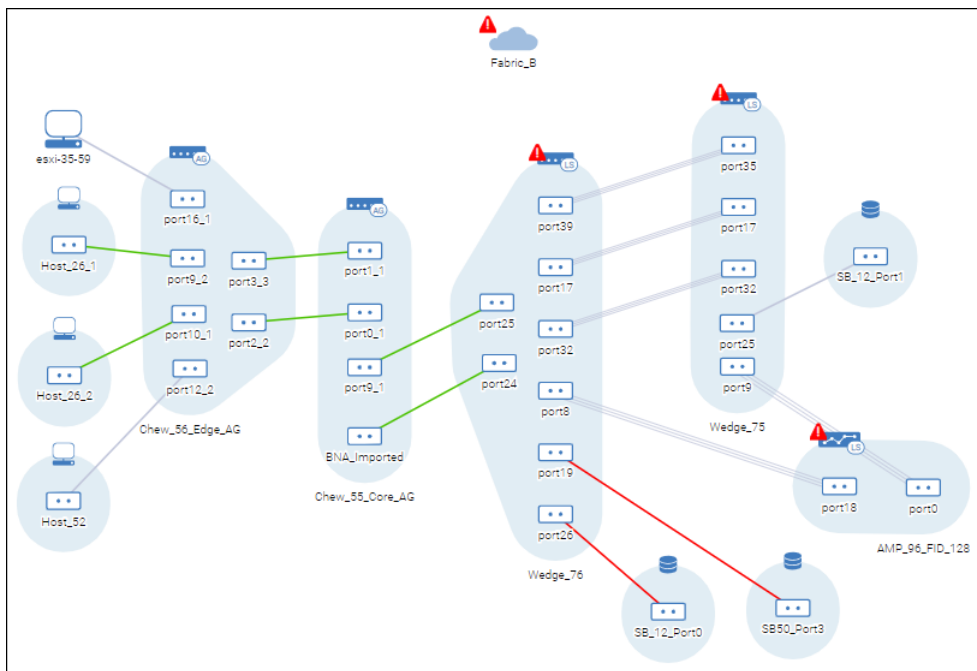
5. Hover over a port icon, click the hamburger icon (☰), and select any of the menu items. For example, if you select **Show Trunk Links**, a popup window displays the master trunk links. Selecting **Investigate** opens Investigate mode for the port.



6. Hover the mouse over the fabric icon or a switch icon, click the hamburger icon, and select any of the attributes. For example, select **Show End Devices**.



The topology now shows the end devices connected to the switches.

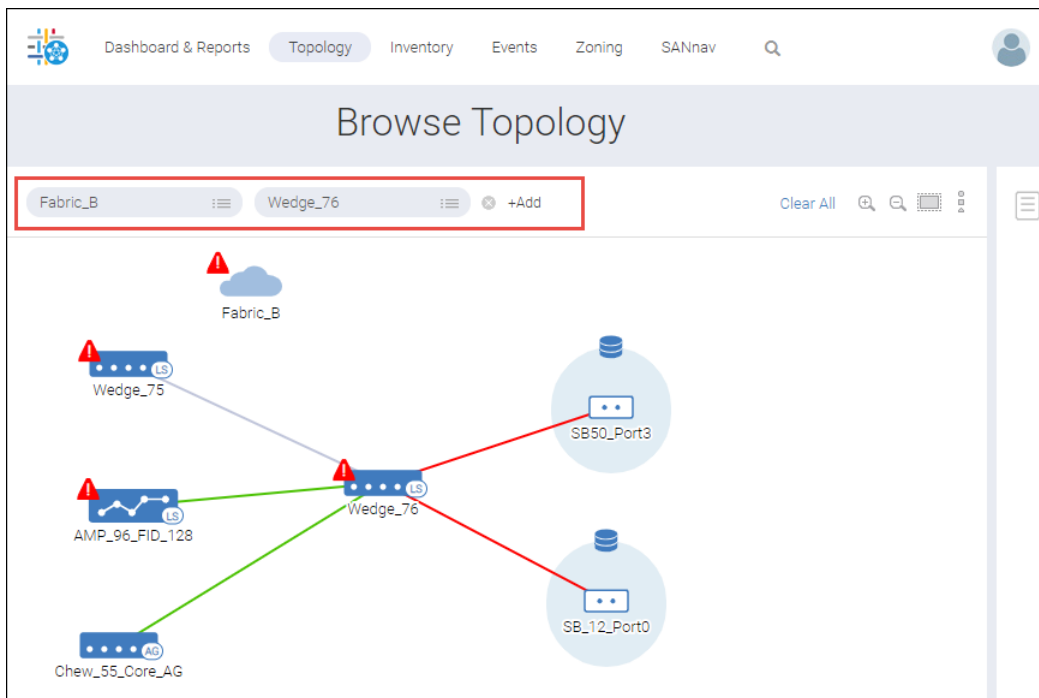


7. Hover over one of the switches, and click the up arrow to change to the switch context.

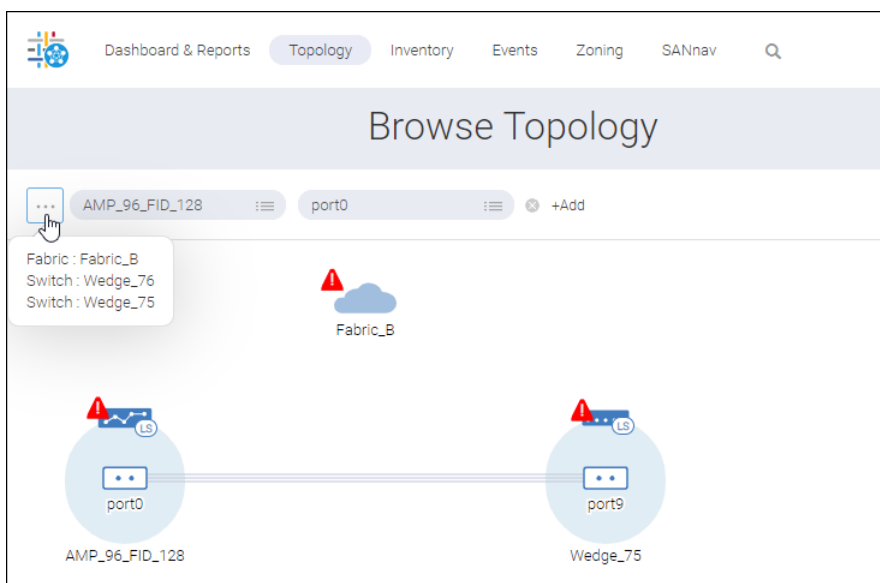


Clicking the up arrow adds a context to the context navigation panel, which is "up" or at the top of the topology window.

Now the topology is in the switch context and displays all switches and devices directly connected to the selected switch. Notice that the context navigation panel now contains two contexts.



You can keep adding contexts by hovering over an object and clicking the up arrow or by clicking **+Add** in the context navigation panel to add a context type relevant to the current contexts. Hover over the more button (. . .) to see the older contexts. Up to eight contexts are retained. If you add more than eight contexts, the older contexts are deleted.



NOTE

If the browser is refreshed, only the latest chosen context is displayed, and the other contexts are deleted.

To go back to the previous context, click the **X** in the context navigation panel, or hover over the selected object and click the down arrow.

8. If necessary, adjust the appearance of the topology.
 - Click any of the device icons (fabric, switch, port) and drag it to a new location.
 - Click the background and drag the entire topology to reposition it in the window.
 - Use the scroll button on the mouse or the zoom buttons in the upper right corner of the window to resize the topology view.
 - Click the Fit Screen button in the top left corner to recenter and resize the topology to fit in the view.

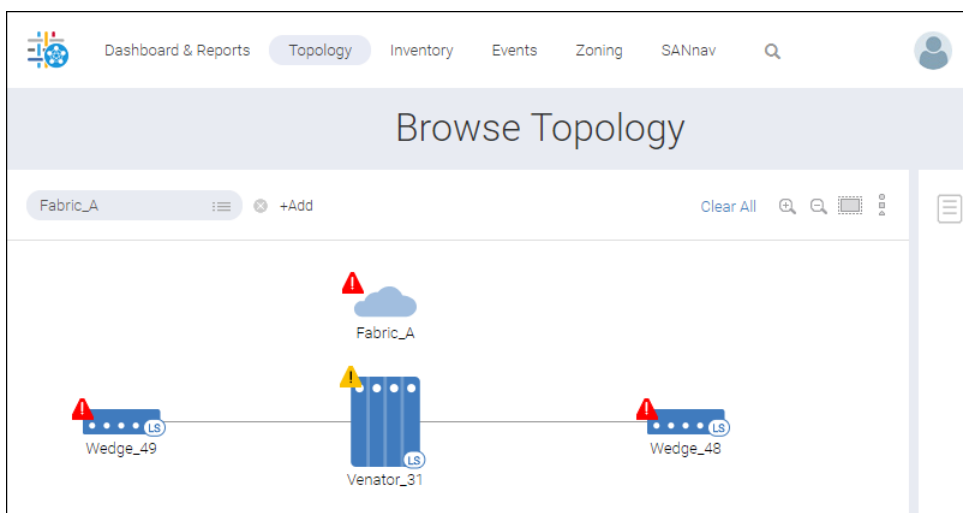


- Click **Clear All** to remove all of the contexts and start over.

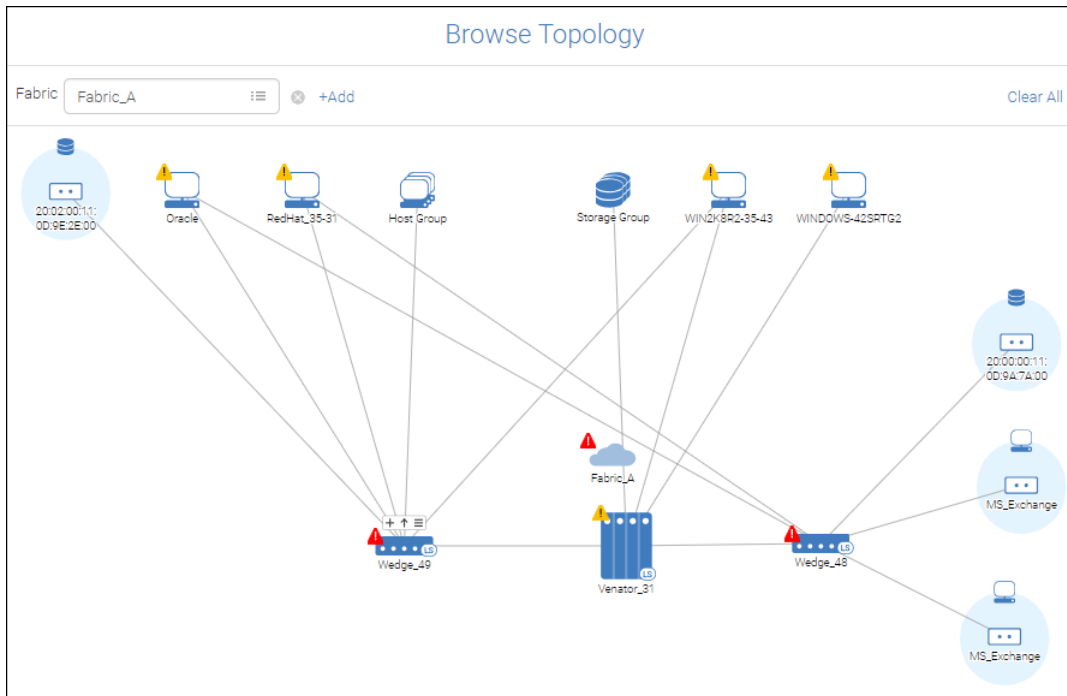
6.7.2 Showing All Devices in a Fabric

The SANnav Management Portal Topology feature allows you to quickly see a graphical representation of all end devices attached to your fabric.

1. Click **Topology** in the navigation bar.
2. Click the **+** button, 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.



4. Hover over the fabric icon, click the hamburger button (☰), and select **Show End Devices**.

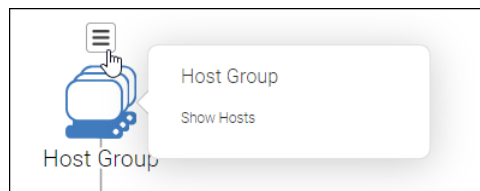


Notice that some of the end devices are shown as groups.



If a switch has more than five end devices of the same type that are connected to that switch, the devices are shown in the topology as a group.

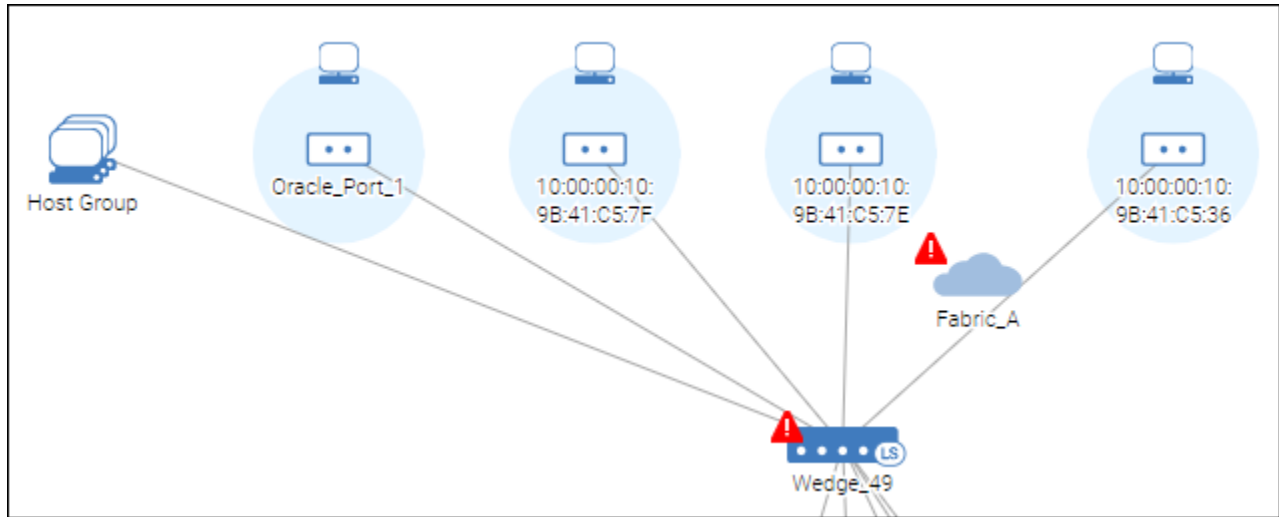
5. To show the objects in a host or storage group individually in the topology, perform the following steps.
 - a. Hover over the group icon, click the hamburger icon, and then select **Show Hosts** (or **Show Storage**).



A list of the devices in that group displays.

- 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 shown individually in the topology.



Note that 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.

6.7.3 Viewing Connectivity between Hosts and Storage

Using the SANnav Management Portal Topology feature, you can view hosts and storage, and all paths between them.

This example shows how to access the topology through the dashboard, starting from a host. 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** page or the **Topology** page, this step shows how to start from the **Health Summary** dashboard and select the item you want to view.

Hosts					
Name ▾	Score ▲	Status ▾	Events ▾	Best Pr... ▾	
Host_a	90	-	-	-10	▾
RedHat_35...	90	-	-		
WIN2K8R2...	90	-	-		

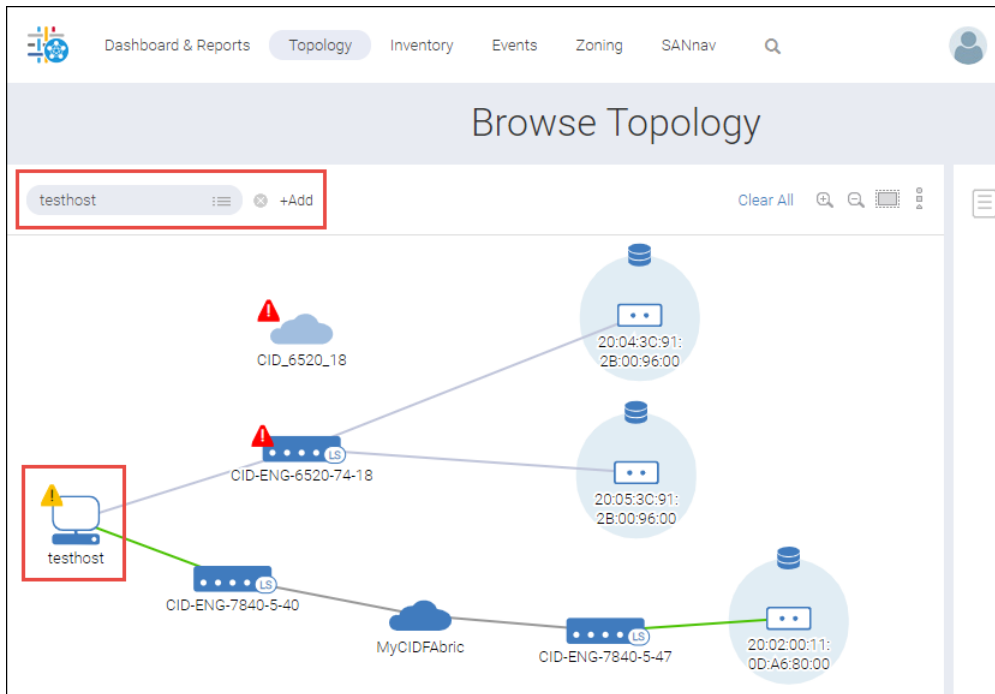
Show Details

Show Properties

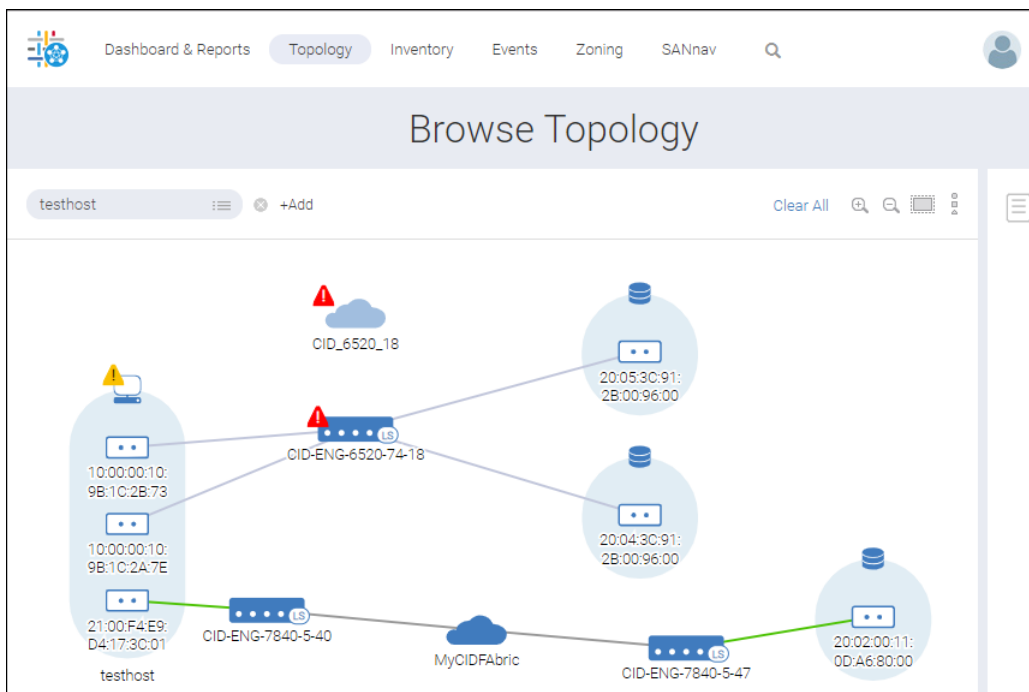
Show in Topology

View Inventory Details

The **Browse Topology** page displays a pictorial view of the fabric from the context of the chosen host. The host name is shown in the context navigation panel. You can see the host, along with all paths to the storage devices that the host connects to.



- To see the host ports, hover over the host icon, and click the + icon.



You can drill-down even further and display the virtual ports associated with the host or storage ports. Hover over a host or storage port icon, click the hamburger icon (☰), and select **Show Virtual Ports** to display the associated virtual ports in tabular format.

Notice that some of the icons have yellow or red warning symbols, indicating degraded or poor health, respectively. You can get additional details about these warnings from the **Health Summary** dashboard.

6.7.4 Viewing Link Utilization

The **Topology** page 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 to 50% utilization
- Yellow = >50 to 80% utilization
- Red = More than 80% utilization
- Gray = The link is not used or not monitored for utilization (default color)

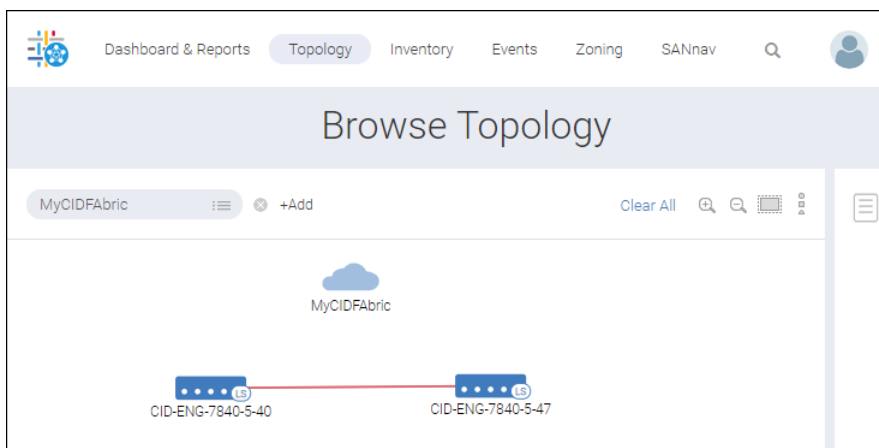
The utilization of a port link is determined by the higher of the transmitted (Tx) and received (Rx) frames. For example, if Tx utilization is 60% and Rx utilization is 40%, the link color is yellow, to reflect the higher utilization.

The utilization of a switch link is determined by the highest of all of 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.

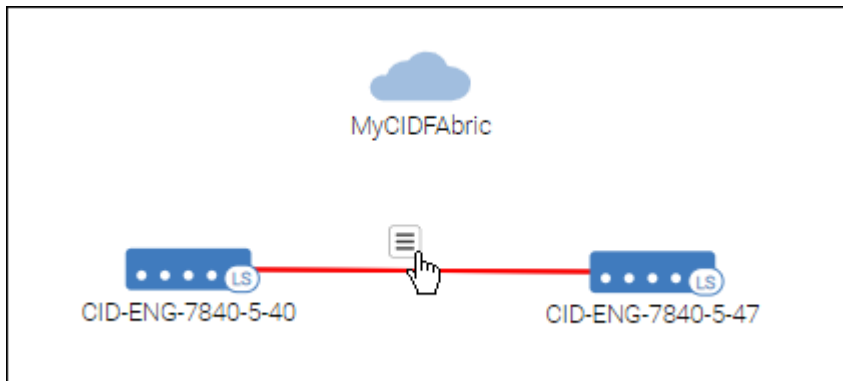
1. Click **Topology** in the navigation bar, and then click the **+** button to add a context.
2. In the **Add Context Type** dialog, select a context, and click **OK**.
For this example, select the **Fabric** context.
3. In the **Fabric** context field, click the menu icon to select a fabric, or type the fabric name directly into the context field.

The **Browse Topology** page displays 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%.



4. Hover the mouse over the link, click the menu icon, and then select **Show Details** to display information about each of the ports in the link.



Notice the Rx and Tx utilization. For two ports, the utilization is high (over 80%).

Details						✕
Source: CID-ENG-7840-5-40 Connected to: CID-ENG-7840-5-47						
Port ^	Port Type ⇅	Attached Port ⇅	Speed ⇅	Rx Utilization(%) ⇅	Tx Utilization(%) ⇅	
port25	VE-Port	port25	0	82.94	83.07	▼
port26	VE-Port	port26	0	82.78	82.68	▼
ge0	GigE-Port	ge0	40	1.04	1.04	▼
ge1	GigE-Port	ge1	40	1.04	1.04	▼

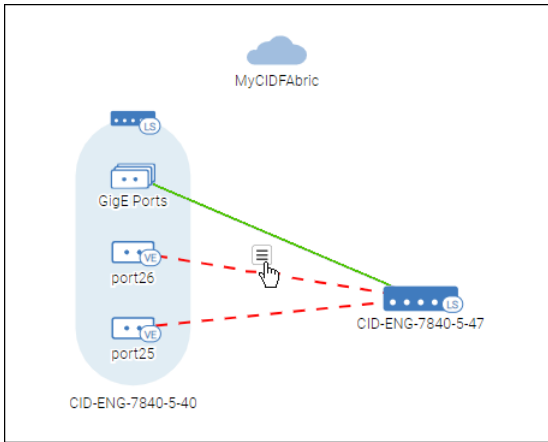
Close

5. Hover over a switch icon, and click the + button to expand the switch and show the ports that make up the link.

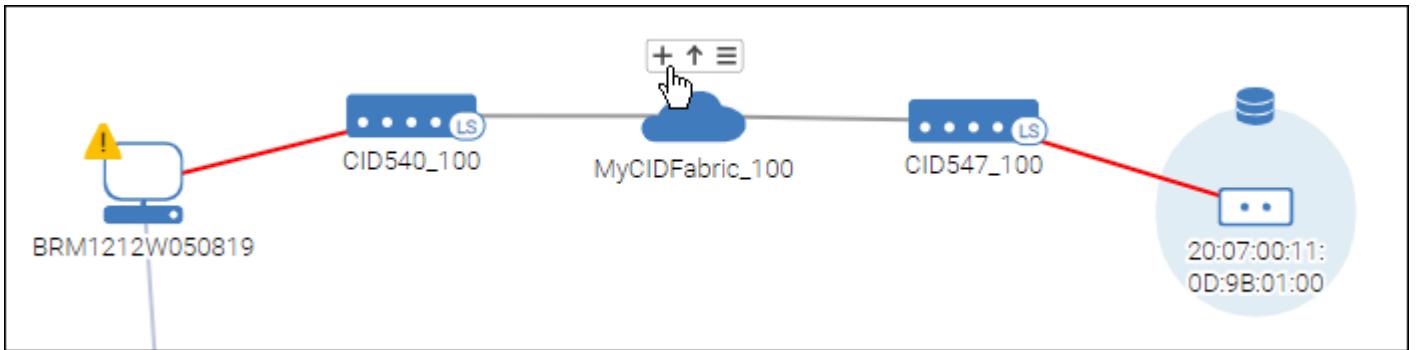
If the switch has more than 15 online ports, expanding the switch displays information in a tabular view.

This switch has three port links, two of which are at over 80% utilization. Even though one of the links is below 50% utilization, the overall utilization state of the switch link is the same as the highest utilization of all of the port links.

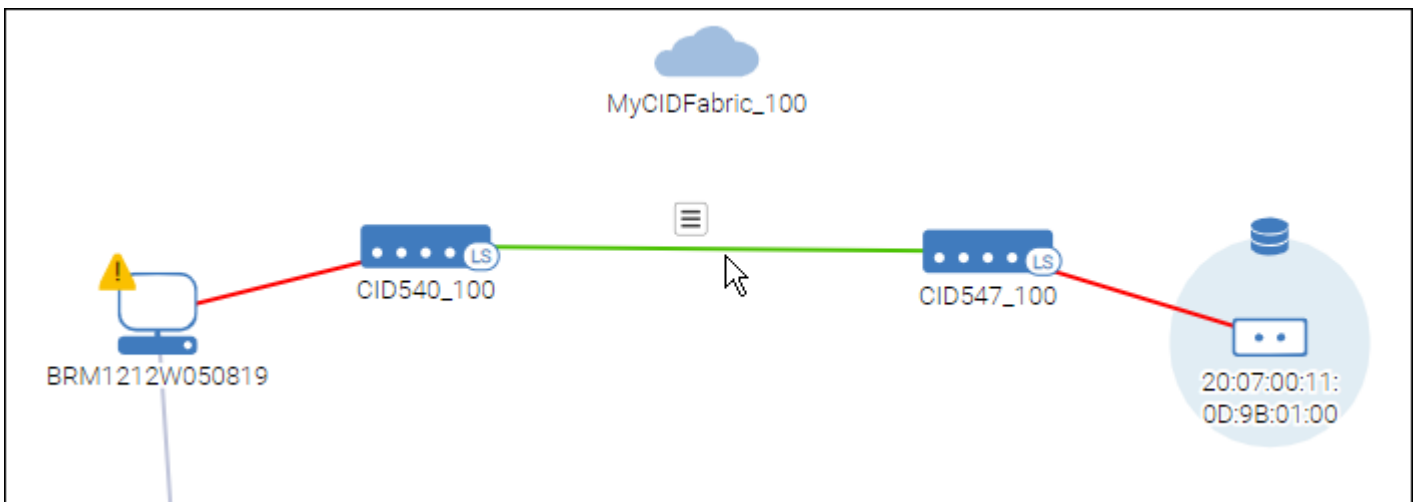
Hover the mouse over one of the port links, click the menu icon, and then select **Show Properties** to display information about that specific port link. The **Show Properties** option is not available for GigE group port links.



Note that link utilization is not shown between a switch icon and a fabric icon. If you want to see the link utilization, you must expand the fabric.



When the fabric is expanded, the link utilization color and details icon are available.



If you find links with high utilization, you can hover the mouse over the switch port, click the hamburger icon, and then select **Investigate** to open Investigate mode where you can look at the usage pattern over time.

For links with consistently high utilization, you might consider adding additional links, creating trunks, or configuring your network to provide alternative paths for the traffic.

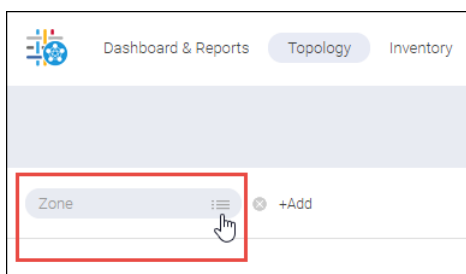
6.7.5 Viewing a Zone Topology

Viewing a zone topology displays all ports that are members of the zone.

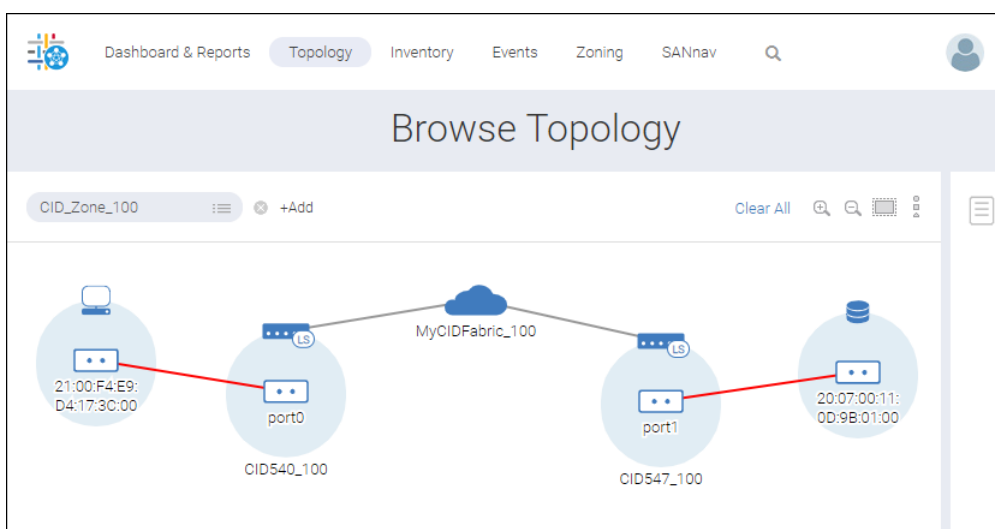
You can view the topology for zones in the active zone configuration only.

The following procedure shows how view zone topology starting from the **Topology** window. You can also launch the **Topology** window from the effective zone configuration details page, by selecting **Show in Topology** from the zone action menu.

1. Click **Topology** in the navigation bar.
2. Click the **+** button, select **Zone** for the context type, and click **OK**.
3. Click the menu icon to select a zone, or type the zone name directly into the context field.



The **Browse Topology** page displays a pictorial view of the zone, showing connectivity between all zone members.



6.8 Flow Management

The Analytics Monitoring Platform (AMP) provides flow monitoring and management capabilities. These capabilities enable a SAN administrator to gather the necessary information to actively manage SAN fabrics. The management process is enhanced with visibility into the behaviors and metrics necessary to resolve problems and, often, to avoid them.

NOTE

The Flow Management feature is supported only on an AMP running AMP OS 3.0.0 or higher.

Refer to the *Brocade Analytics Monitoring Platform User Guide, 3.0.0*, for details on AMP.

Flow Management allows you to monitor and manage flows, enabling you to do the following:

- Reserve initiator-target (IT) flows and display their utilization details.
- Track flows and investigate in both historical and real time.
- View flow and port measures simultaneously on one Investigation mode window.
- Apply measures specifically added to switch investigation for F_Ports that function the same as other port measures.
- Navigate from port to flow investigation for F_Ports.
- List all violated events that are triggered by an aggregated collection.
- Manage collections (aggregated and nonaggregated) with custom rule sets.
- Generate Time Series and Top N Reports like Time Series - Flow Collection for aggregates and Top SCSI Errors (including threshold).
- Include flow statistics in the backup process.
- Clean up existing flow historical data and start fresh through a restore function.

6.8.1 Flow Management Setup

Before you can manage a flow, you need to ensure that the following prerequisites are met. If they are not met, an event is displayed on the **Events** window.

- If the AMP is running a firmware version lower than AMP OS 3.0.0, you must upgrade the AMP to 3.0.0 or higher. After you upgrade the AMP, stop monitoring and then start monitoring the AMP in SANnav.
 - a. Upgrade the AMP firmware to AMP OS 3.0.0.
 - b. In SANnav, select **SANnav** in the navigation bar, and then select **SAN Monitoring > Fabric Discovery**.
 - c. On the **Discovered Fabrics** page, select the fabric where the AMP resides.
 - d. Select the AMP in the **Products** table, and click **Stop Monitoring**.
 - e. Select the AMP again, and click **Monitor**.
- Clock synchronization for the SANnav server and all switches is mandatory. If the clocks are not synchronized, you might lose flows and their statistics.

NOTE

Network Time Protocol (NTP) must to be configured before SANnav installation.

You can synchronize the clocks in three ways:

- Create a configuration policy in SANnav and push it to the switches.

To synchronize the switch time to the NTP server using the SANnav Configuration Management feature, enter the following code on the **Create New Configuration** dialog:

```
{
  "BasicConfiguration":{
    "NTP_TimeServer":[
      {
        ipAddress: "10.156.5.80"
      }
    ]
  }
}
```

```

    ]
  }
}

```

- Synchronize the switch time to the NTP server on the SANnav installed on the host machine.
 - For Red Hat Linux, issue the command `ntpdate NTPserver` on the SANnav server, where `NTPserver` is the hostname or IP address of the NTP server.
 - For CentOS, open the `/etc/ntp.conf` file, ensure that the following line exists, and then restart the server.


```
ntp.server.com:NTPserver
```

 where `NTPserver` is the hostname or IP address of the NTP server.
- Issue the `tscclockserver "<IPV4>;<IPV6>;<DNS name>"` command on the principal switch. This distributes the details to all switches in a fabric.
- The latency between the switch and SANnav must be less than or equal to 100 ms. The recommendation is to place both the switch and SANnav in the same data center.
- All AMP fabric IDs (FIDs) should be discovered in a single (or the same) server, and all FIDs should be authenticated and managed.

SANnav supports 600K total flows (60K 5-minute flows and 540K 6-hour flows). AMP supports a maximum of 200K flows.

6.8.2 Configuring vTap for AMP Flow Monitoring

NOTE

The user with read/write privileges must have vTap configuration access.

A predefined analytics vTap flow (`sys_analytics_vtap`) runs on the monitored switch that is running the specific version of Fabric OS. It mirrors the SCSI I/O command and error frames over the Analytic Switch Link (ASL) to the Analytics Monitoring Platform so that the frame data can be analyzed. All frames and flow statistics are collected and maintained at the flow level of granularity.

You can select or modify a set of ingress ports for monitoring by AMP and SANnav. The port selection can include the following:

- A specific F_Port
- All F_Ports
- MAPS groups

To modify the vTap configuration, do the following:

1. Select **SANnav** on the navigation bar, and then select **SAN Configuration > Analytics Monitoring Platform Connectivity**.

This displays a list of switches that are connected to AMP. If a port is already configured, its port name and configured AMP display. Else, you see “-”.

Name	Connected AMP	AF Port	Status
SW-6510-4	-	-	-
test234	Spectre_Dev_AMP_37	port6	Active

- Click either the switch name or **View** from the action list.

The following dialog displays. Here you can view, change, or enhance the vTap configuration.

SW-6510-4

Ports

Name	Type	AMP	AF Port	
No data to display.				

Add

Save Cancel

- To add a port, click **Add**.

The **Add Ports** dialog displays.

- Select a mirroring option.

Your options include:

- **All F-ports** to mirror all F-ports in the switch (default).
- **Select port manually** to specify the F-Ports to mirror.
- **MAPS Group** to mirror the ports present in the MAPS group.
Recall that MAPS uses the sys_mon_analytics flow to monitor all the metrics associated with flows monitored by AMP.

- Click **Next**.

The **vTap Flow Definition** dialog displays with the **Ports** table populated.

- Click **Change**.

The **Change Ports** dialog displays.

Change Ports

All F-ports
 Select port manually
 MAPS Group

Search

Name	Port Number	Slot Number
port9	9	0

Next Cancel

7. Highlight the port and click **Next**.
8. Click **OK** in the information screen.
9. Click **Save** to deploy the configuration to the switch.

A progress dialog displays.

- If the analytics vTap flow is already active, the **Save** operation deactivates the flow, modifies the flow based on your configuration, and reactivates the flow.
- If the analytics vTap flow is currently de-activated, the **Save** operation modifies the flow based on your configuration and reactivates the flow.

6.8.3 I/O Violation Summary

AMP supports configuration and monitoring of thresholds at the individual I/O level to help you identify the specific I/Os that are misbehaving.

AMP OS 3.0.0 handles I/O violation as follows: For each initiator-target/initiator-target-LUN (IT/ITL) under 200K, AMP maintains I/O violation results as counters and streams all I/O violations to SANnav every 5 minutes for 5-minute and 6-hour flows. AMP monitors I/O violations at the ITL level (for 5-minute and 6-hour flows) and consolidates violation counts across all ITLs into the IT level.

NOTE

If an I/O rule is applied to an ITL flow that is monitoring at 6-hour granularity, then that rule is applied to all ITLs that belong to that IT flow.

NOTE

Occasionally, the total I/O violation count exceeds the total I/Os.

The supported metrics are:

- Read and Write Exchange Completion Time
- Read and Write First Response Time
- Read and Write Pending I/Os
- Other Pending I/Os
- Other Command Frame Latency Time
- Fabric Command Latency Time
- Fabric Status Latency Time

For each one of the above metrics, the AMP streams the following counters:

- Violated Count
- Violated I/O MAX
- Violated I/O Average
- Total I/O Average
- Total I/O Count
- Total Violated I/O Size

In SANnav, a new counter is introduced to calculate the violation I/O percentage, which indicates the severity of the violation. This counter can be displayed historically on the SANnav **Investigation mode** window and can be used to generate top N and time series reports. Through reports, you can view flow-specific summaries of metrics for misbehaving I/Os.

These I/O violations are not displayed in MAPS, and no action is taken.

6.8.4 Inventory and IT Reservation

Inventory is where you obtain a list of switches that are managed by the SANnav server. It is also where you can configure the number of initiator-target (IT) flows that can be monitored by AMP.

NOTE

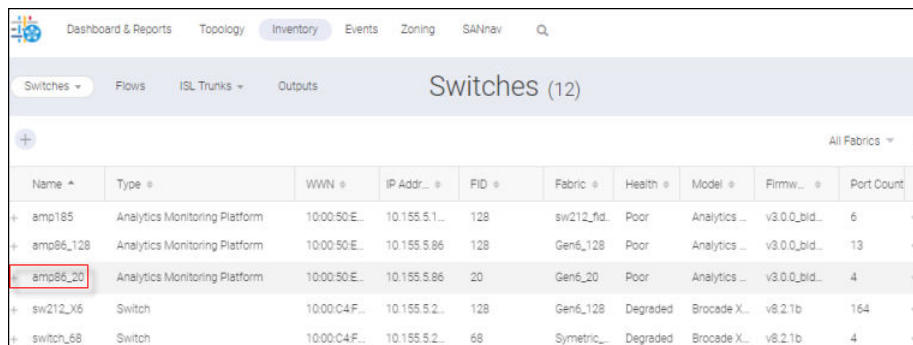
The user with read/write privileges must have IT reservation access.

6.8.4.1 Determining Whether the Switch Is Sending Telemetry Data to the SANnav Server

To determine whether a switch is forwarding telemetry data to the SANnav server, do the following.

1. Select **Inventory** from the navigation bar, and then select **Switches** from the action list.

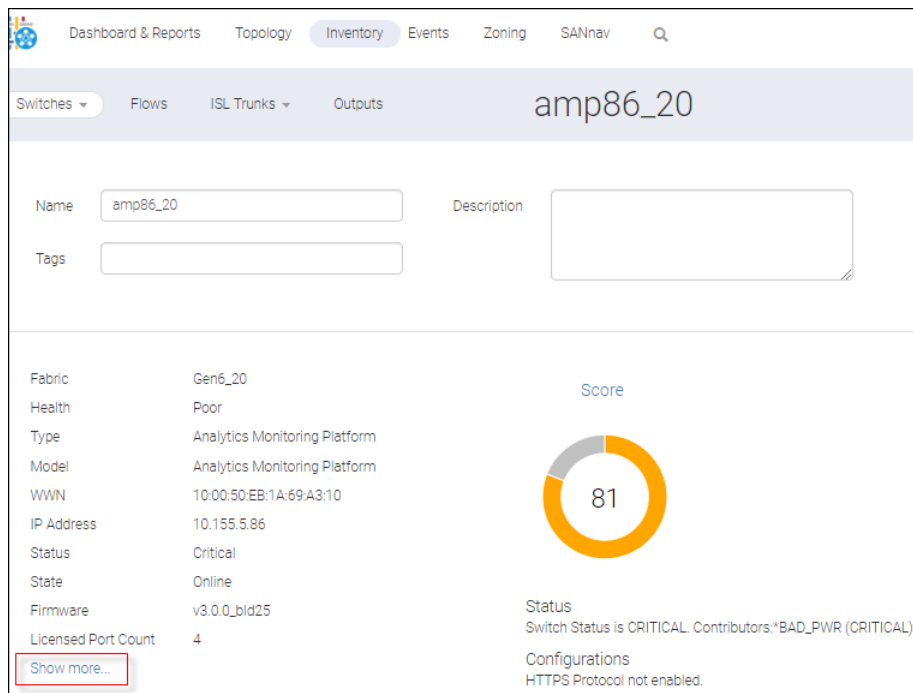
This displays the switches managed by the SANnav server.



Name	Type	WWN	IP Addr.	FID	Fabric	Health	Model	Firmw.	Port Count
amp185	Analytics Monitoring Platform	10:00:50:E...	10.155.5.1...	128	sw212_fd.	Poor	Analytics ...	v3.0.0_bld...	6
amp86_128	Analytics Monitoring Platform	10:00:50:E...	10.155.5.86	128	Gen6_128	Poor	Analytics ...	v3.0.0_bld...	13
amp86_20	Analytics Monitoring Platform	10:00:50:E...	10.155.5.86	20	Gen6_20	Poor	Analytics ...	v3.0.0_bld...	4
sw212_X6	Switch	10:00:C4F...	10.155.5.2...	128	Gen6_128	Degraded	Brocade X...	v8.2.1b	164
switch_68	Switch	10:00:C4F...	10.155.5.2...	68	Symmetric...	Degraded	Brocade X...	v8.2.1b	4

2. Click a switch of type Analytics Monitoring Platform.

This displays detail categories like **Fabric** and **Health** that are common across all switches.



amp86_20

Name: amp86_20

Description: [Empty]

Tags: [Empty]

Fabric	Gen6_20
Health	Poor
Type	Analytics Monitoring Platform
Model	Analytics Monitoring Platform
WWN	10:00:50:EB:1A:69:A3:10
IP Address	10.155.5.86
Status	Critical
State	Online
Firmware	v3.0.0_bld25
Licensed Port Count	4

[Show more...](#)

Score: 81

Status: Switch Status is CRITICAL. Contributors: "BAD_PWR (CRITICAL)"

Configurations: HTTPS Protocol not enabled.

- Click **Show more** to see the value of **Bound to Server**, which indicates the SANnav server to which the AMP is bound.

If amp86_20 is bound to this SANnav server, then the **Bound to Server** value and the SANnav server IP address match. (See the following image.) In this example, a match exists. So, you have verified that amp86_20 is bound to this SANnav server for managing collections.

HIF Mode	Enabled
VF Enabled	Enabled
RNID Tag	96ff
Last Discovery	Fri Jul 26 2019 12:16:52 GMT-0700 (Pacific Da...
Bound to Server	10.155.5.195
Physical Switch	Brocade7840
Chassis Serial #	CWA2506L003
Show less	

If **Bound to Server** indicates that the IP address is "not for the current server," this means that the AMP switch is not bound to this SANnav server.

6.8.4.2 Viewing the Number of Flows Monitored by the AMP Switch

To view the number of flows that the switch is monitoring, do the following.

- Select **Inventory** from the navigation bar, and then select **Switches** from the action list.

This displays the switches managed by the SANnav server.

- Click a switch of type Analytics Monitoring Platform.

This displays the detail window for that switch.

- Scroll down the details window, and then select the **Flow Details** option. Here you can find information about flow consumption and about flow capacity per level of granularity (5 minutes or 6 hours).

Flow Details

Flows at 5 Minutes interval capacity	20000
Flows at 6 Hours interval capacity	200000
IT Reserved	2000
IT flows consumed at 5 Minutes interval	24
ITL flows consumed at 5 Minutes interval	464
ITL flows consumed at 6 Hours interval	46

4 Items

Switch Ports

Name	Type	WWN	Tags	Status	State	Speed	Att	
port13	AF-Port	20:0D:50:...	-	Online	Online	16 Gb/s	-	Investigate
port16	U-Port	20:10:50:...	-	No_Mod...	Offline	16 Gb/s	-	Decommission
port14	AE-Port	20:0E:50:...	-	Online	Online	16 Gb/s	slo	Recommission
port15	U-Port	20:0F:50:...	-	No_Mod...	Offline	16 Gb/s	-	

Port Optics

Disable Switch

Save Cancel View in WebTools Configure Reservation

6.8.4.3 Reserving a Number of IT Flows to Be Monitored by AMP

To reserve a specific number of IT flows to monitor, do the following.

1. Select **Inventory** from the navigation bar, and then select **Switches** from the action list.

This lists the switches managed by the SANnav server.

2. Click a switch of type Analytics Monitoring Platform.

This displays the detail window for that switch.

3. Click **Configure Reservation** at the bottom of the window. (**Configure Reservation** is enabled provided that the switch is registered with **Bound to Server**. Otherwise, it is disabled.)

The **Configure Reservation** dialog displays.

It shows the current value as well as the permitted range of values.

Here you can configure the number of IT flows to be monitored at 5-minute granularity.

By default the value is 2000. In this example, 10,000 is specified.

4. Enter the number of IT flows to monitor at the 5-minute granularity, and click **OK**.

A confirmation dialog displays warning you that changing **IT Reservation** causes a flow reset in the AMP switch.

6.8.5 Operating the Flows Window

NOTE

To perform the following steps, you require Flow Management privilege with read/write permission to monitor and manage flows.

The **Flows** window, accessed through the **Inventory** tab, displays flows in table format. From here, you can monitor all flows with the latest statistics.

All monitor flows with statistics (last received from the switch, without aggregation) are shown. For flows to appear on the window, they must have been streamed from AMP at least once.

Streaming is based on the configured interval, and each interval has a buffer time for processing data. After receiving and processing the flow, SANnav displays the data to you within a time interval that depends on the number of flows.

- For 6-hour data, the time interval is 30 minutes to 1 hour.
- For 30-minute data, the time interval is 15 to 30 minutes.
- For 5-minute data, the time interval is 1 to 2 minutes.

The **Flows** list window displays the flows 5-minute and 6-hour data. The waiting time for the data is based on the interval.

- 5-minute flows are learned after 5 minutes or less once discovery completes.
- 6-hour flows are learned after 6 hours or less once discovery completes, and they are streamed 4 times a day.

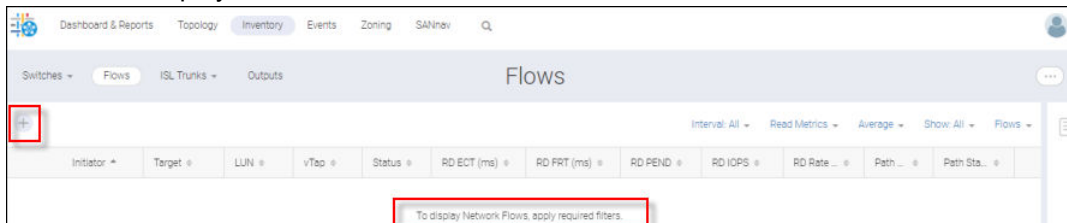
The following high-level actions on the flows are enabled:

- View detailed stats and inventory related information for a given flow.
- View historical or real-time stats for one or more flows (investigation mode).
- Select one or more flows in the selection sidebar for later investigation.

To explore the **Flows** list window, do the following:

1. Select **Inventory > Flows** from the navigation bars.

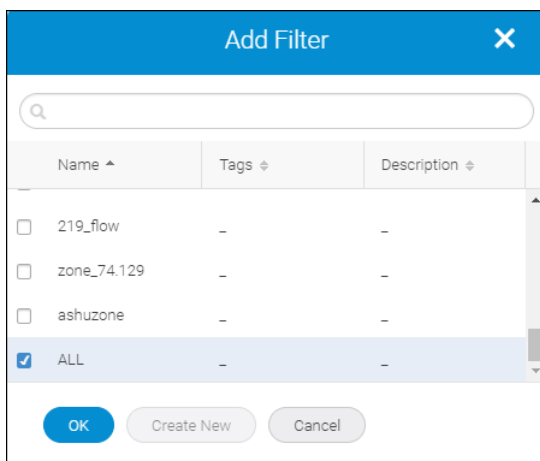
This displays the **Flows** window. By default, no flows are displayed. As the message indicates, you must apply at least one filter to display flows.



2. Click “+” to add a filter.

This displays the **Add Filter** dialog where you see a list of saved flow filters.

If you want to create a new filter, click **Create New**.



NOTE

Only flow filters are listed here.

You can apply more than one filter at a time, although the recommended maximum is three. When more than one filter is applied, flows that meet any of the filter criteria are displayed.

3. Select a filter or create a new one.

If over 1000 flows result from the filtering, a message appears stating that only 1000 flows can be shown. However, you can view all flows in a CSV file using the **Export Definition** option.

4. Click **OK**.

The **Flows** window displays. The contents reflect the filters that you selected.

The screenshot shows the 'Flows (1000)' window in the SANnav interface. The table displays the following data:

Initiat..	Target	LUN	vTap	RD E..	RD F..	RD P..	RD IO..	RD R..
010101	170031	0	170031	-	-	-	-	-
010101	170017	0	170017	-	-	-	-	-
010101	170010	0	170010	-	-	-	-	-

If multiple aliases exist for the same device port, any one of the zone alias names might display.

When sorting the LUN column in the flow list and the table contains both IT and ITL flows, the IT flows will always be at the bottom. They are identified by “-” in the LUN column.

- Click the arrow associated with the flow to expand the details.

The close-up shows three rows of flow data. The second row is highlighted, and a red box highlights the expand arrow (a right-pointing triangle) to its left.

▶ +	010101	17011c	1
▶ +	010101	17011c	2
▶ +	010101	17011c	3

The resultant **Flows** window shows the statistics of the analytics measures for an active flow.

Measures fall under three categories: Latency, Performance, and I/O Exceptions.

Latency measures display maximum and average values, whereas Performance measures display only average values.

The screenshot shows the 'Flows (1000)' window in the SANnav management portal. The window title is 'Flows (1000)'. Below the title bar, there are tabs for 'Switches', 'Flows', 'ISL Trunks', and 'Outputs'. A '+Add' button is highlighted with a red box. The main content area displays a table of flow statistics and a detailed performance section.

Initiat...	Target	LUN	vTap	RD E...	RD F...	RD P...	RD IO...	RD R...
+ 010101	17011c	0	010101	0.031	0.022	1.000	-	0.000
+ 010101	17011c	1	010101	0.031	0.021	1.000	-	0.000
+ 010101	17011c	2	010101	0.031	0.021	1.000	-	0.000

Latency

- Read Exchange Completion Time (Avg/Max, ms): 0.031/0.046
- Write Exchange Completion Time (Avg/Max, ms): 0.037/0.077
- Read First Response Time (Avg/Max, ms): 0.021/0.036
- Write First Response Time (Avg/Max, ms): 0.020/0.058
- Read IO Size (Avg/Max, Bytes):
 - <8K: 512.000/512.000
 - All: 512.000/512.000
- Write IO Size (Avg/Max, Bytes):
 - <8K: 512.000/512.000
 - All: 512.000/512.000
- Read Pending IOs (Avg/Max, IOs): 1/1
- Write Pending IOs (Avg/Max, IOs): 1/1

Performance

- Read Data Rate (Avg, MB/s): 0.000
- Write Data Rate (Avg, MB/s): 0.000

IO Exception

- SCSI Read Command (Count): Total I/O 380
- SCSI Write Command (Count): Total I/O 391

Path Characteristics

- Host port Speed (Gbps): 16
- Storage port Speed (Gbps): 16

For an inactive flow, the **Flows** window shows the following statistics.

The screenshot shows the 'Flows' window in the SANnav management portal. The window title is 'Flows'. Below the title bar, there are tabs for 'Switches', 'Flows', 'ISL Trunks', and 'Outputs'. A '600' dropdown menu and a '+Add' button are visible. The main content area displays a table of flow statistics and a detailed performance section.

Initiator	Target	LUN	vTap
+ 200600	02080e	7	02080e
+ 2d0600	02080e	8	02080e
+ 2d0600	02080e	9	02080e
- 2d0600	02080e	23	02080e

Path Characteristics

- Host port Speed (Gbps): 8
- Storage port Speed (Gbps): 8

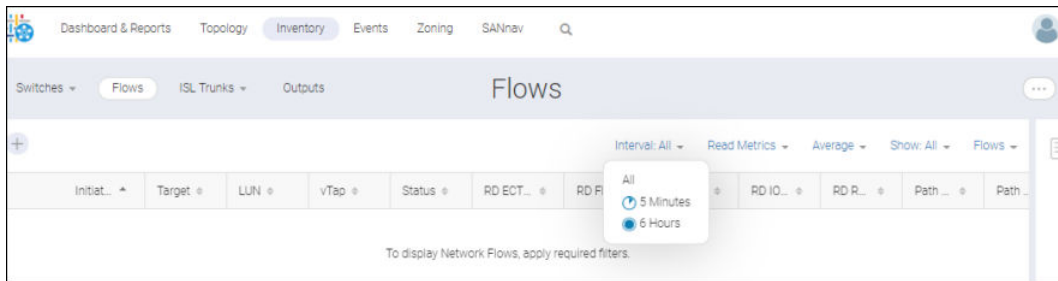
Additional Info

- Status: Inactive since Aug 27, 2019 11:05:00 PDT
- Active Zone: FID1_ALL_IT_Zone
- Fabric: ST_EDGE1_AG

Measures with a "0" value are excluded from the expanded view.

In the bottom portion of the expanded view, you see LUN size, LUN count (only for IT flows), Status, Active Zones, and so on. An active zone reflects the zone where the initiator and target participated. Multiple active zones appear provided that both initiator and target comprise multiple active zones.

6. To filter the flows for a different interval (5 minutes, 6 hours, or All), select from the **Interval** list.



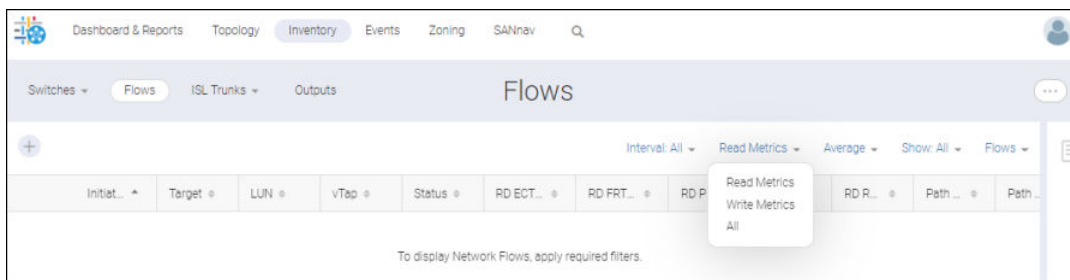
NOTE

For inactive flows, the granularity icon displays the last granularity received from the switch before it moves to the inactive state.

Hovering over the icons in the list displays information for that icon.

The **All** option (the default) lists both 5-minute and 6-hour interval flows.

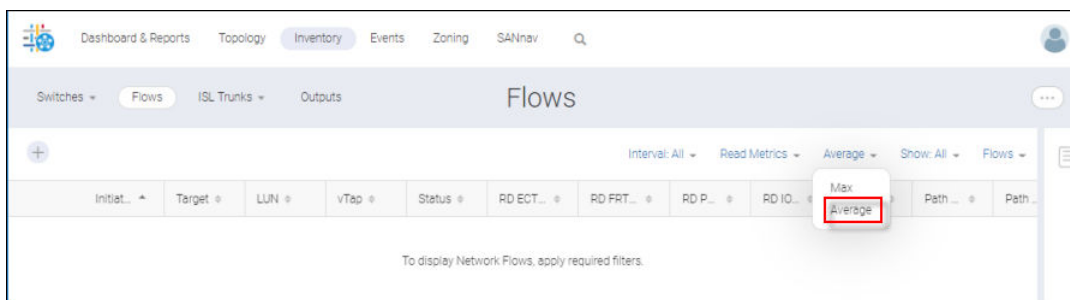
7. Select from the **Metrics** list. From here you can select which measures to view.



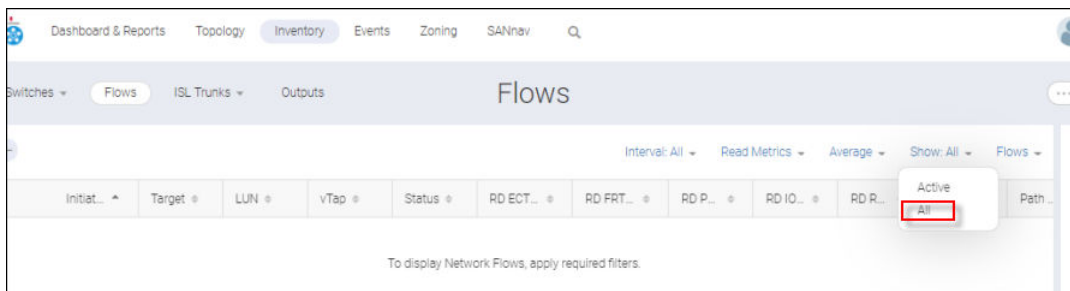
8. Select **Max** or **Average**. For this example, **Average** is selected.

NOTE

Max applies only to Latency metrics, whereas **Average** applies to all three categories.



9. Select **All** from the **Show** list.



This option lists both active and inactive flows and generates a new column (**Status**) to indicate the type. In the following example, you can see a mix of active and inactive flows.

Initiat...	Target	LUN	vTap	Status	RD ECT...	RD FRT...	RD P...	RD IO...	RD R...	Path...
esx87_be...	storage7...	0	storage7...	Active	0.12	0.11	2.00	1844.00	28.82	55.00
esx87_be...	storage7...	1	storage7...	Active	0.12	0.11	2.00	1852.00	28.95	56.00
esx87_be...	storage7...	2	storage7...	Active	0.12	0.11	2.00	1897.00	29.64	57.00
esx87_be...	storage7...	3	storage7...	Active	0.11	0.10	2.00	1953.00	30.52	59.00
esx87_be...	storage7...	11	esx87_be...	Inactive	-	-	-	-	-	-
esx87_be...	storage7...	12	esx87_be...	Inactive	-	-	-	-	-	-
esx87_be...	storage7...	13	esx87_be...	Inactive	-	-	-	-	-	-

Flow statistics are received from the switch every 5 minutes or 6 hours and their status can be either Active or Inactive.

- A flow tagged Active represents active traffic.
- A flow is tagged Inactive if any of the following apply:
 - The flow is available in a previous statistics collection but is unavailable in the current collection.
 - The flow has no associated SCSI operations.
 - The flow is no longer streamed to SANnav (that is, the flow is no longer streamed to SANnav).

If a flow from the 6-hour granularity moves to the 5-minute granularity, and then returns to the 6-hour granularity before the 6-hour collection cycle completes, the AMP CLI shows the flow to be "Active" in the 6-hour category, but SANnav shows it as "Inactive" in the 5-minute category until the next 6-hour collection cycle. This is due to the limitation in SANnav to process data streamed for 6-hour flows only at 6-hour intervals.

After SANnav fails to receive flows them for 24 hours and daily purging has already occurred at 3:00 a.m, flows are greyed out and labeled "Deleted Flow from AMP."

10. Click ... > **Export Definition**.

This action exports the flows applicable for a given filter into a CSV file.

Initiat...	Target	LUN	vTap	Status	RD ECT...	RD FRT...	RD P...	RD IO...	RD R...	Path...
esx103_3...	storage1...	1	esx103_3...	Active	0.432	0.103	2	1636	204.537	50
esx103_3...	storage1...	0	esx103_3...	Active	0.439	0.104	2	1626	203.271	50
esx103_3...	storage1...	2	esx103_3...	Active	0.433	0.103	2	1634	204.299	50.001
esx130_6...	Storage8...	10	esx130_6...	Active	0.0	0.0	0.0	0.0	0.0	0.0
esx130_6...	Storage8...	11	esx130_6...	Active	0.0	0.0	0.0	0.0	0.0	0.0

NOTE

If either no filter is applied or no filter flows are displayed for a given filter, the **Export Definition** selection is disabled.

The exported file appears at the bottom of the **Flows** window.

6.8.6 Accessing and Exploring Flow Investigation Mode

NOTE

Performance privilege is required to investigate device port metrics.

Investigation mode is where you can examine one or more flows in real time or in an historical date range.

To explore Investigation mode, do the following. Assume that you have already applied numerous filters to generate the flows list.

1. Click “+” at the left of a row in the table on the **Flows** window.

After selecting an element, the “+” sign to the far left has changed to a “-” sign.

Initiat...	Target	LUN	vTap	Status	RD ECT...	RD FRT...	RD P...	RD IO...	RD R...	Path...
+ esx103_3...	storage1...	1	esx103_3...	Active	0.088	0.074	1	3025	47.271	49.992
- esx103_3...	storage1...	0	esx103_3...	Active	0.087	0.073	2	3007	46.996	49.995
+ esx103_3...	storage1...	2	esx103_3...	Active	0.088	0.074	2	3026	47.297	49.993
+ esx130_6...	Storage8...	12	esx130_6...	Active	0.0	0.0	0.0	0.0	0.0	0.0

Once selected, the flow is added to the **Selected Items** sidebar where you can choose to investigate flows now or later.

2. Select two more rows.
3. Click the **Select Items** sidebar icon (boxed above) to display the elements under **Selected Items**.

In this example, the **Selected items** sidebar displays the three flows that were moved to the sidebar. You need to select from this set of flows and proceed to investigation.

Initiat...	Target	LUN	vTap	Status	RD E...	RD F...	RD P...
+ esx103_3...	storage1...	1	esx103_3...	Active	0.088	0.074	1
+ esx103_3...	storage1...	0	esx103_3...	Active	0.087	0.073	2
+ esx103_3...	storage1...	2	esx103_3...	Active	0.088	0.074	2
+ esx103_3...	storage1...	3	esx103_3...	Active	0.088	0.074	1
+ esx103_3...	storage1...	0	esx103_3...	Active	0.087	0.078	1
+ esx103_3...	storage1...	1	esx103_3...	Active	0.09	0.08	2
+ esx130_6...	Storage8...	12	esx130_6...	Active	0.0	0.0	0.0

Selected Items				Clear All
Flows (3)				Actions
<input type="checkbox"/>	Initiat...	Target	vTap	LUN
<input checked="" type="checkbox"/>	esx103_3...	storage1...	010000	0
<input checked="" type="checkbox"/>	esx103_3...	storage1...	010000	3
<input checked="" type="checkbox"/>	esx103_3...	storage1...	010000	0

Although the selected items are available for investigation throughout the session, they do not persist at the user level (that is, when you log out or the session expires, the **Selected Items** sidebar resets).

Both flows and collections are supported in the sidebar.

NOTE

Clicking the arrow within the sidebar closes the dialog.

Clicking on the “-” sign on the far left of the row in the table removes the element from the **Selected Items** sidebar and converts the symbol to “+”.

- Select the flows in the **Selected Items** sidebar that you want to investigate by clicking **Investigate** from the **Actions** list.

The screenshot shows the SANnav interface with the 'Flows (506)' table and the 'Selected Items' sidebar. The sidebar contains three selected flow items, and the 'Investigate' action is highlighted in the Actions menu for the selected items.

Initiat...	Target	LUN	vTap	Status	RD E...	RD F...	RD P...
esx103_3_...	storage1...	1	esx103_3_...	Active	0.088	0.074	1
esx103_3_...	storage1...	0	esx103_3_...	Active	0.087	0.073	2
esx103_3_...	storage1...	2	esx103_3_...	Active	0.088	0.074	2
esx103_3_...	storage1...	3	esx103_3_...	Active	0.088	0.074	1
esx103_3_...	storage1...	0	esx103_3_...	Active	0.087	0.078	1
esx103_3_...	storage1...	1	esx103_3_...	Active	0.09	0.08	2
esx130_6_...	Storage8...	12	esx130_6_...	Active	0.0	0.0	0.0

You can select multiple items within the sidebar to investigate.

The **Investigate** selection is disabled unless at least one item is checked.

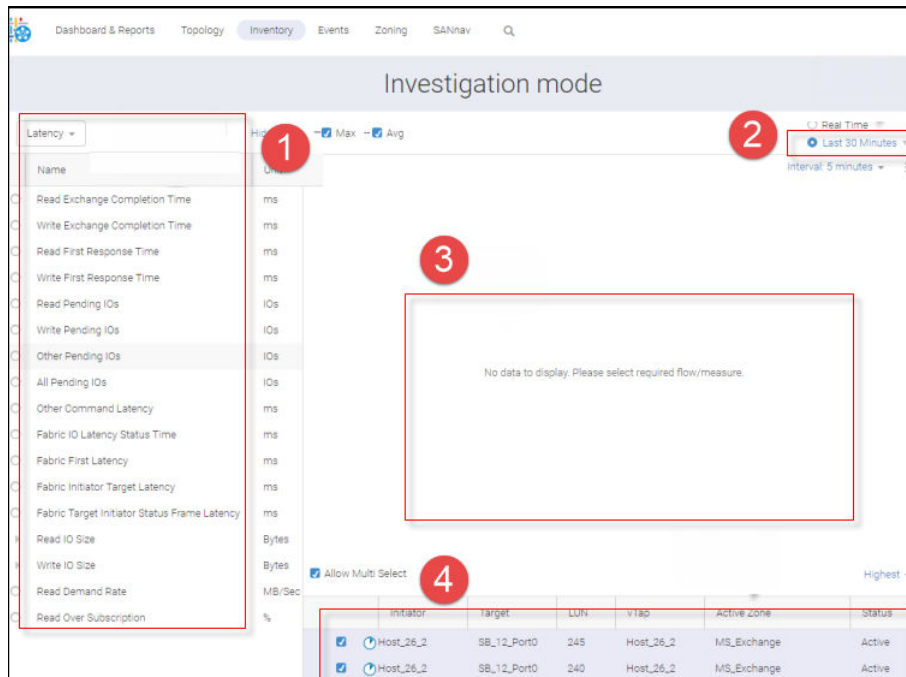
Alternatively, you can launch the **Flow Investigate** page from the action list for a specific item by clicking **Investigate**.

The screenshot shows the SANnav interface with the 'Flows (460)' table. The 'Investigate' action is highlighted in the Actions menu for a specific flow item.

Initiat...	Target	LUN	vTap	Status	RD ECT...	RD FRT...	RD P...	RD IO...	RD R...	Path...
ESX130_...	Storage2...	-	Storage2...	Active	1.639	0.182	45	15210	946.823	-
ESX130_...	Storage2...	-	ESX130_...	Active	2.815	1.307	45	15210	946.82	-
ESX130_...	Storage2...	-	Storage2...	Active	0.518	0.118	36	17571	592.988	-
ESX130_...	Storage2...	-	ESX130_...	Active	1.721	1.274	36	17571	592.987	-
esx130_6_...	Storage8...	1	esx130_6_...	Active	0.122	0.083	1	450	26.424	25
esx130_6_...	Storage8...	10	esx130_6_...	Active	0.0	0.0	0.0	0.0	0.0	0.0
esx130_6_...	Storage8...	11	esx130_6_...	Active	0.0	0.0	0.0	0.0	0.0	0.0

Whether you launch investigation through the **Selected Items** sidebar or individually through a specific flow action list, an **Investigation mode** window displays.

When you pass from the **Flows** window to the **Investigation mode** window, the chart is empty because no measures are selected by default.



1. Measure list – Displays only supported AMP measures (including violation).
2. Date range – Provides real-time, historical-time and custom-time range options.
The date range of the graph is Last 30 Minutes by default.
For a custom date range, end points are always inclusive. For example, a date range of 13:00 to 14:00 with a one-hour interval fetches two data points as well as points at 13:00 and 14:00.
3. Time series graph – Based on selected measures, flows, and date range, shows statistics in graphical format.
The Y axis is in units of the selected measures. The X axis represents time (termed "Interval"). The legend displays the names of a single flow with multiple measures (measure name with MAX and Avg) or multiple flows with a single measure (initiator, target, LUN, and vTap).
For each selected measure, the MAX value will be plotted in solid lines and the Avg values will appear as dotted. Performance and I/O Exception measures are plotted when selecting Avg.
4. Flow table – Lists all selected flows from the flows page. (These flows can be of mixed intervals.)
After applying a filter, the table resets accordingly and the corresponding name appears at the top of the table. The table lists all IT flows with an expander option, which lists all ITLs belonging to the selected IT. When the expander closes, the ITL flows are removed from the list, leaving only the IT flows viewable with the expander option. None of the flows is selected by default. Upon selecting a flow, the chart resets and a flow action menu displays specifics for that flow.
The table lists flows in order of highest priority by default (that is, the last selected measure is listed first).
Supported filter actions for each flow:
 - Show Metrics – Based on launch time, all stats are displayed in a popup dialog. Assuming investigation was launched at 1:00, when you click **Show Metrics**, all the stats for that investigation launched at that time are displayed in the popup.
 - Show All ITLs – Only applicable for ITL flows.
 - Filter by Initiator – Filtering based on the selected flow initiator.
 - Filter by Target – Filtering based on the selected flow target.
 - Filter by Active Zone – Filtering based on the selected flow active zone.
 - Filter by Logical Unit WWN – Filtering based on the selected flow LUN WWID.
5. To remove an item from the **Selected Items** sidebar, click **Remove** on the action list.

6. To empty all items from the sidebar, click **Clear All**.

6.8.7 Operating in Flow Investigation Mode

Whether Investigation Mode is launched from the action list for an individual flow or from the **Selected Items** sidebar for one or more flows, the **Investigation Mode** window displays. You can either investigate multiple flows and one measure, or one flow and multiple measures.

From Investigation mode, you can do the following:

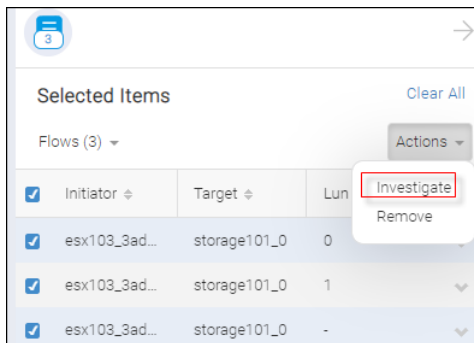
- Filter by target (or initiator, active zone, and logical unit WWN)
- Set the date range
- Inspect multiple flows simultaneously
- Set the time interval (the "granularity")
- Analyze flows in realtime

To understand how to work in Investigation Mode, perform the following steps:

For this example, IT and ITL filters are applied to the flows list and two ITL flows and one IT flow have been selected (the IT flow is identified by the "-" in the **LUN** column). Selection moves the flows to the **Select Items** sidebar.

1. From the sidebar, select the flows you want to investigate and click **Investigate** from the action list.

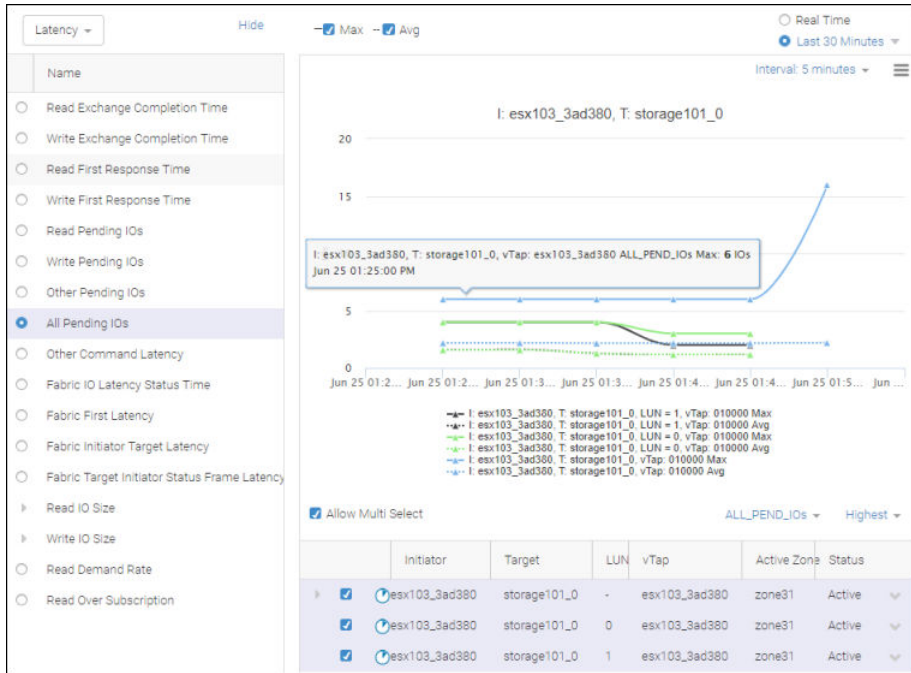
For this example, selections were made from the flows list after IT and ITL filters were applied.



Investigate mode displays and selected flows appear in the table at the bottom of the window.

From here you can examine both IT and ITL flows against the same measure.

- Select the flows and the measure. For this example, all three flows are selected and the measure **All pending IOs** is chosen.



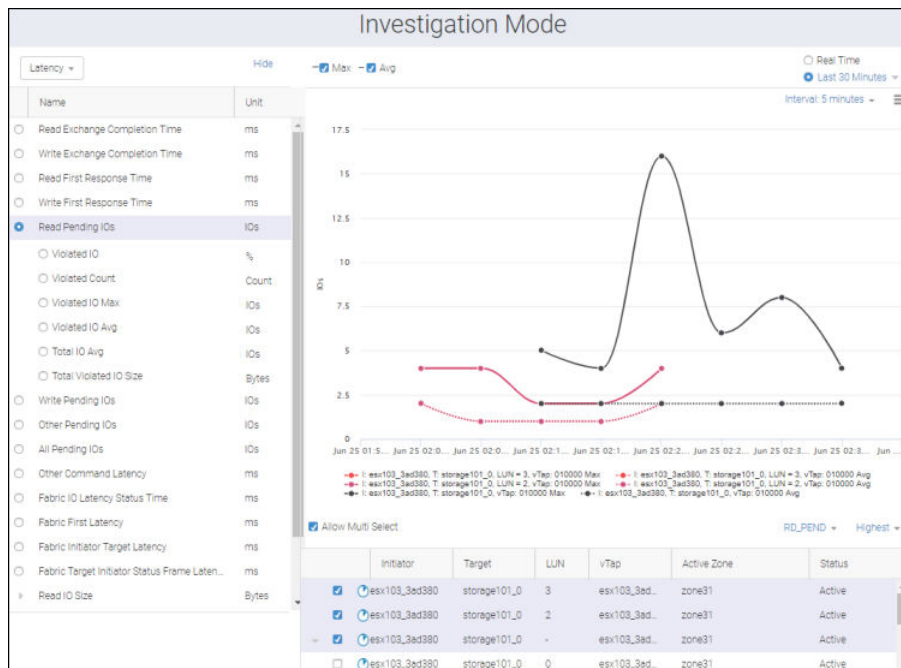
You can discern the Average and Max graphs for each flow by the solid vs dotted lines. You can also notice the flow information like I, T, and LUN details in the chart title and tool tip.

- To view the IT and an associated ITL against the same measure, click the expander option in the left-most column of the IT flow. The IT flow is indicated by the "-" in the **LUN** column.

ITL flows with LUN values 2 and 3 are added to the table. The expanded IT flow is boxed. Notice the "-" mark under **LUN**. This tells you that this is an IT flow.

	Initiator	Target	LUN	vTap	Active Zone	Status
<input checked="" type="checkbox"/>	esx103_3ad380	storage101_0	3	esx103_3ad380	zone31	Active
<input checked="" type="checkbox"/>	esx103_3ad380	storage101_0	2	esx103_3ad380	zone31	Active
<input checked="" type="checkbox"/>	esx103_3ad380	storage101_0	-	esx103_3ad380	zone31	Active
<input type="checkbox"/>	esx103_3ad380	storage101_0	0	esx103_3ad380	zone31	Active

- Select another measure. In this example, **Read Pending IOS** is selected. The graph shows the original IT flow and its two ITL components against this measure.



5. To display the ITLs associated with an IT flow, expand the IT flow from the flow list on the **Investigate mode** window.
 - a. Click the **+** icon to move an IT flow to the **Selected Items** sidebar.

The Flows (28) window displays a table of IT flows. The columns are: Initiator, Target, LUN, vTap, Status, RD ECT (ms), and RD FRT (ms). The flow with Initiator ESX130_6f0801 and Target Storage246_09 is highlighted with a red box, indicating it is selected.

Initiator	Target	LUN	vTap	Status	RD ECT (ms)	RD FRT (ms)
<input checked="" type="checkbox"/> esx103_3ad380	storage101_0	-	esx103_3a...	Active	0.40	0.36
<input checked="" type="checkbox"/> esx103_3ad381	storage101_2	-	esx103_3a...	Active	0.22	0.14
<input checked="" type="checkbox"/> ESX130_6f0801	Storage246_09	-	Storage24...	Active	1.34	0.17
<input checked="" type="checkbox"/> ESX130_6f0801	Storage246_09	-	ESX130_6f...	Active	2.47	1.25
<input checked="" type="checkbox"/> ESX130_6f0801	Storage246_08	-	Storage24...	Active	0.68	0.15

- This action moves the flow to the **Selected Items** sidebar.
 - b. Select the flow from the sidebar and chose **Investigate** from the action list.
- The **Investigate mode** window displays with the selected IT flow in the list at the bottom of the window.
- c. Expand the IT flow by clicking the left-most arrow to view some of its associated ITLs.

The Selected Items sidebar displays a table of ITLs for the selected flow. The columns are: Initiator, Target, LUN, vTap, Active Zone, and Status. The flow with Initiator esx103_3ad380 and Target storage101_0 is selected.

Initiator	Target	LUN	vTap	Active Zone	Status
<input checked="" type="checkbox"/> esx103_3ad380	storage101_0	-	esx103_3ad380	zone31	Active
<input type="checkbox"/> esx103_3ad380	storage101_0	0	esx103_3ad380	zone31	Active
<input type="checkbox"/> esx103_3ad380	storage101_0	3	esx103_3ad380	zone31	Active
<input type="checkbox"/> esx103_3ad380	storage101_0	1	esx103_3ad380	zone31	Active
<input type="checkbox"/> esx103_3ad380	storage101_0	2	esx103_3ad380	zone31	Active

Another way to display the ITLs associated with an IT flow is through the selection of **Show All ITLs** from the action list.

Select **Show All ITLs** from the action list for one of the ITL flows. The "1" under **LUN** identifies the flow as an ITL. The **Show All ITLs** option is available only for ITL flows.

	Initiator	Target	LUN	vTap	Active Zone	Status
<input checked="" type="checkbox"/>	esx103_3ad380	storage101_0	-	esx103_3ad380	zone31	Active
<input checked="" type="checkbox"/>	esx103_3ad380	storage101_0	1	esx103_3ad380	zone31	Active
<input checked="" type="checkbox"/>	esx103_3ad380	storage101_0	0	esx103_3ad380	zone31	Active

The flow list would now include all the ITLs associated with the IT flow in the table.

	Initiator	Target	LUN	vTap	Active Zone	Status
<input type="checkbox"/>	esx103_3ad380	storage101_0	-	esx103_3ad380	zone31	Active
<input checked="" type="checkbox"/>	esx103_3ad380	storage101_0	0	esx103_3ad380	zone31	Active
<input type="checkbox"/>	esx103_3ad380	storage101_0	3	esx103_3ad380	zone31	Active
<input checked="" type="checkbox"/>	esx103_3ad380	storage101_0	1	esx103_3ad380	zone31	Active
<input type="checkbox"/>	esx103_3ad380	storage101_0	2	esx103_3ad380	zone31	Active

After the table refreshes, the arrow icon associated with the IT flow points downward. This indicates that the ITL flows that comprise the IT flow are now listed below it.

6. By default, the flows are listed, highest first (that is, last selected measure first). You can reset this flow order by selecting **Lowest** from the frequency list.

	Initiator	Target	LUN	vTap	Active Zone	Status
<input checked="" type="checkbox"/>	esx103_3ad380	storage101_0	-	esx103_3ad380	zone31	Active
<input checked="" type="checkbox"/>	esx103_3ad380	storage101_0	1	esx103_3ad380	zone31	Active
<input checked="" type="checkbox"/>	esx103_3ad380	storage101_0	0	esx103_3ad380	zone31	Active

7. Change the date range by clicking on the range list.

The **Select Data Range** dialog displays.

Select Date Range
✕

< Apr 2019 >

< May 2019 >

Last 30 Minutes
 Last 1 Hour
 Last 2 Hours
 Last 1 Day
 Last 3 Days
 Last 1 Week
Last 6 Weeks

Su	Mo	Tu	We	Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa
31	1	2	3	4	5	6	28	29	30	1	2	3	4
7	8	9	10	11	12	13	5	6	7	8	9	10	11
14	15	16	17	18	19	20	12	13	14	15	16	17	18
21	22	23	24	25	26	27	19	20	21	22	23	24	25
28	29	30	1	2	3	4	26	27	28	29	30	31	1
5	6	7	8	9	10	11	2	3	4	5	6	7	8

12

:

00

AM

12

:

00

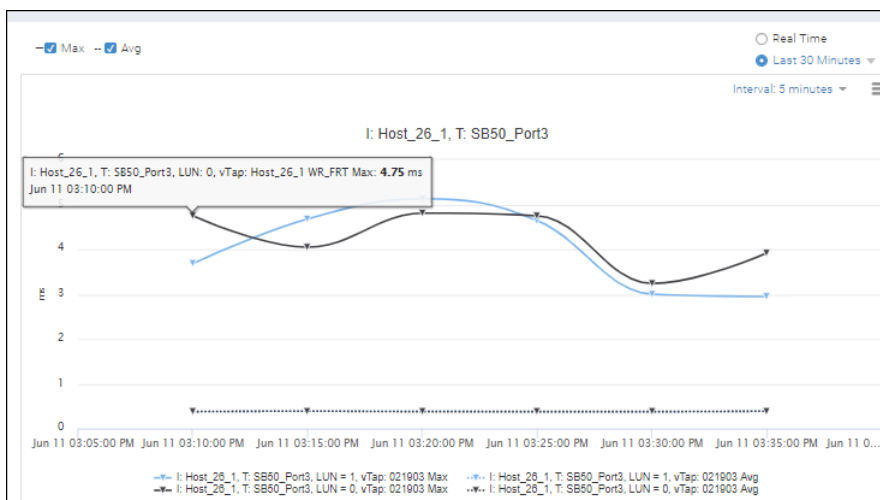
PM

Apply
Cancel

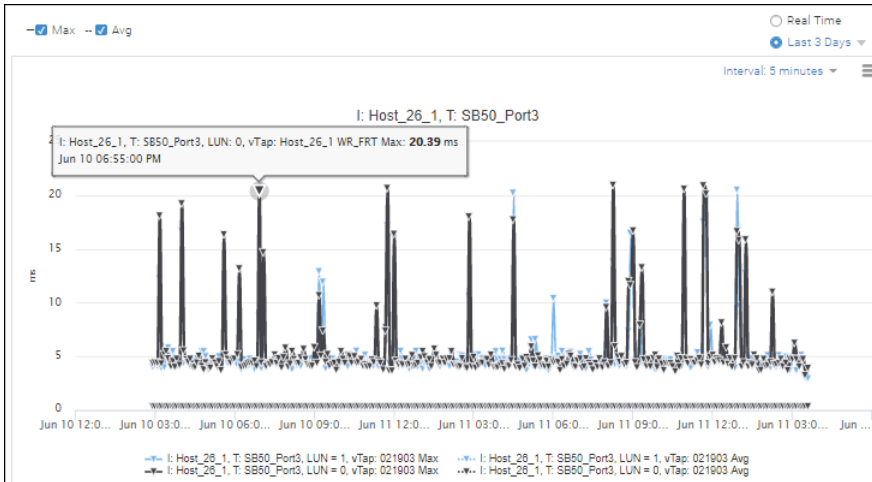
From here you can either use a predefined date range or customize one.

In the previous example, **Last 6 weeks** is selected from the range list.

In the following example, the date range is set to **Last 30 Minutes** (the default).



When you change the time interval, the plotting changes accordingly. In the following example, the interval has changed from **Last 30 Minutes** to **Last 3 Days**.



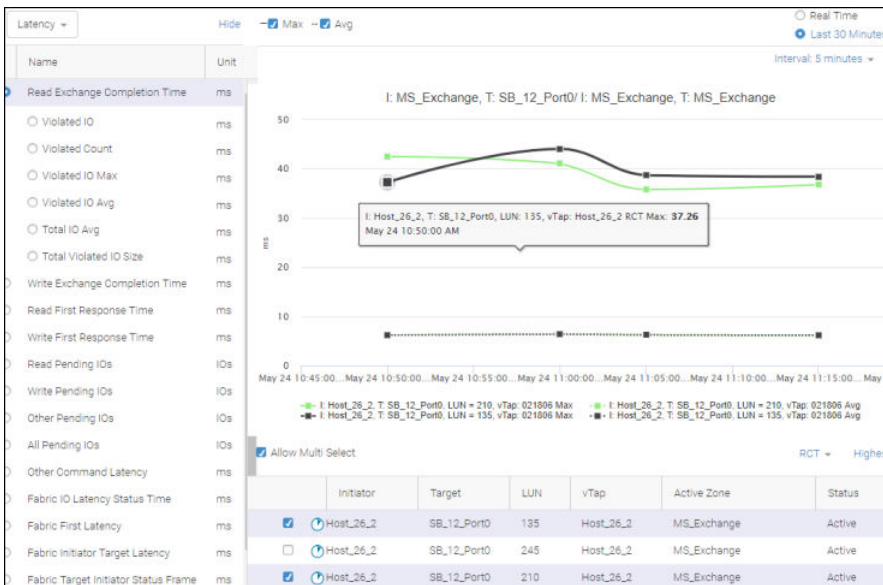
NOTE

You can hide the plotting by selecting or unselecting the legends.

8. Uncheck the **Allow Multi Select** option. This enables you to select multiple measures against one flow.

NOTE

If you launch Investigation for multiple flows through the **Selected Items** sidebar, this option is checked by default.

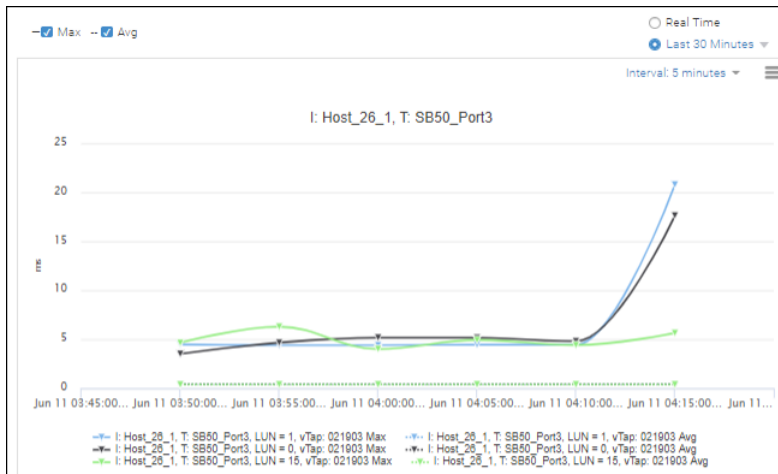


If you launch **Investigate** for single flow, **Allow Multi Select** is unchecked and you can investigate multiple measures.

If you select multiple measures and then check the **Allow Multi Select** option, only the last selected measure is retained.

9. Reset the time interval (termed the "granularity").

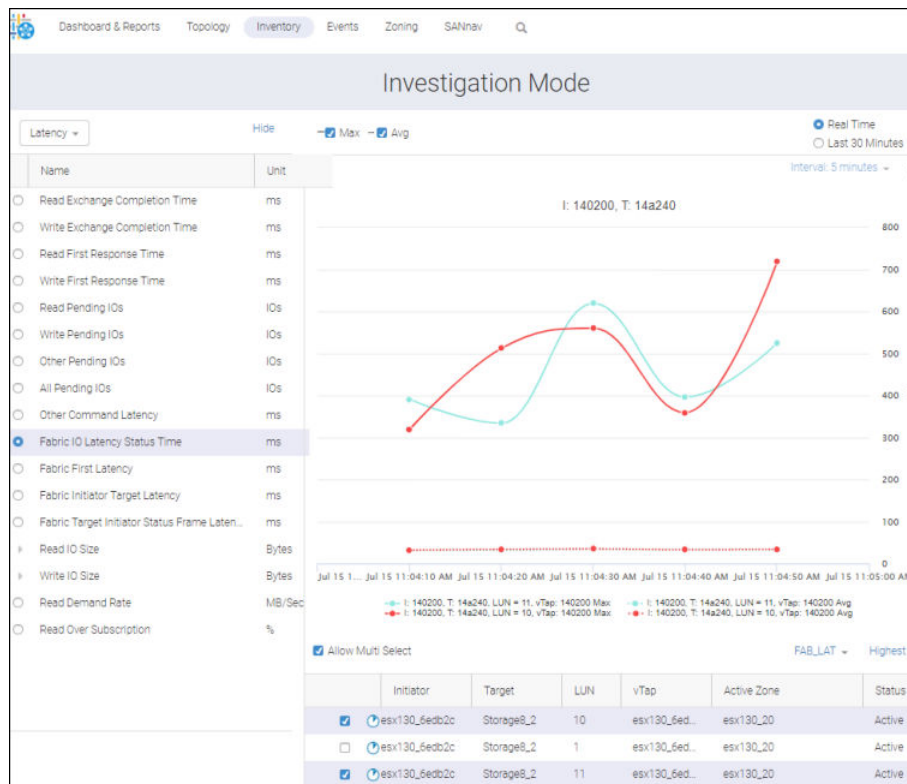
In the following example, three flows have been selected and the default time interval (5 minutes) has been accepted.



If you change the interval to 1 hour, flow statistics populate the chart based on this new interval.

"No data to display" might display either when the graph does not have any data for the selected time range or when no statistics are available for a violation measure. "No data to display" also appears if I/O flows move from the 5-minute to the 6-hour granularity because the 5-minute statistics have not been received. If 6-hour flows now fall into a 5-minute granularity, the graph plots the 5-minute interval for the selected range.

10. Select the **Real Time** option to view the real time data for the selected flows received from the switch. For example, consider another scenario.
 - a. Select 3 flows and check them in the **Selected Items** sidebar.
 - b. Click **Investigate**, check the **Fabric IO Latency Status Time** measure option, and then check the I/O flows with LUN 10 and 11.

c. Click the **Real Time** option.

Notes

- Per AMP, real-time mode supports a maximum of 25 flows to monitor. (No data is plotted for inactive flows.)
- The frequency of data collection is 10 seconds. Data points beyond 1 hour (approximately 360 points) are purged from the graph.
- Switching between an historical and a real-time graph incurs a delay of 20 to 25 seconds before the first point is plotted. The chart resets, and the granularity option is disabled.
- If statistics are unavailable for a particular interval or you selected inactive flows for real-time investigation where the application does not have any historical data, the message "No data to display" appears.

6.8.8 Investigating Flows from Switch Ports

When investigating F_Ports, you can navigate from port to flow investigation, where you can compare port and flow statistics for all flows passing through that F_Port.

1. Select **Inventory** from the navigation bar, and then select **Switch Ports** from the platform list.

The **Switch Ports** list displays.

- Select the ports that you want to investigate. In this example, to illustrate how the capabilities are specific to F_Ports, three different port types are selected.

The screenshot shows the 'Switch Ports (262)' interface. A table lists various ports with columns for Name, Type, WWN, Tags, Switch, Fabric, Status, and State. Three ports are highlighted with red boxes: port8 (U-Port), port9 (AE-Port), and slot12 port11 (F-Port). On the right, the 'Selected Items' sidebar shows these three ports, and the 'Investigate' button is highlighted in the 'Actions' menu.

Name	Type	WWN	Tags	Switch	Fabric	Status	State
port8	U-Port	20:08:50...	-	switch_2	Symetric...	No_Mod...	Offline
port9	AE-Port	20:09:50...	-	amp86_10	Gen6_10	Online	Online
slot12 port11	F-Port	20:7B:C4...	-	sw212_X6	Gen6_128	No_Light	Offline

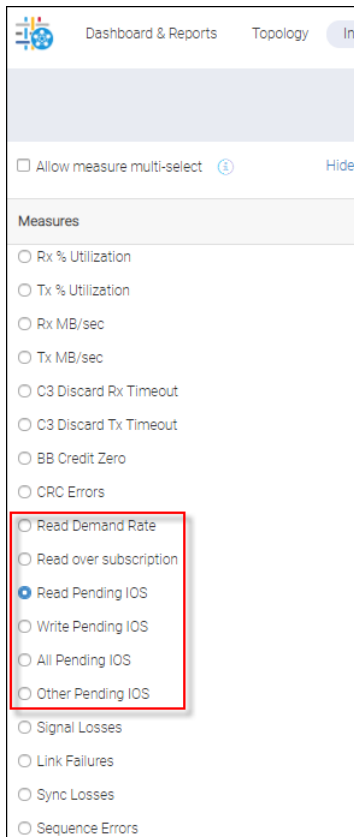
Notice that they have moved to the **Selected Items** sidebar.

- In the sidebar, highlight the ports, and then select **Investigate** from the action list. The **Investigation Mode** window displays for the selected switch ports.

The screenshot shows the 'Investigation Mode' interface. On the left, there is a 'Measures' sidebar with various metrics. The main area displays a table of selected ports. The 'Show' dropdown is set to 'Selected Ports' and 'Allow Multi Select' is checked.

Name	Slot/Port	Type	Switch	WWN	Status	State
port8	8	U-Port	switch_2	20:08:50:EB:1A:8...	No_Module	Offline
port9	9	AE-Port	amp86_10	20:09:50:EB:1A:6...	Online	Online
slot12 port11	12/11	F-Port	sw212_X6	20:7B:C4:F5:70:2...	Online	Online

4. Select from the set of F_Port specific measures (boxed) available on the switch ports **Investigation Mode** window. For this example, **Read Pending IOS** is selected.



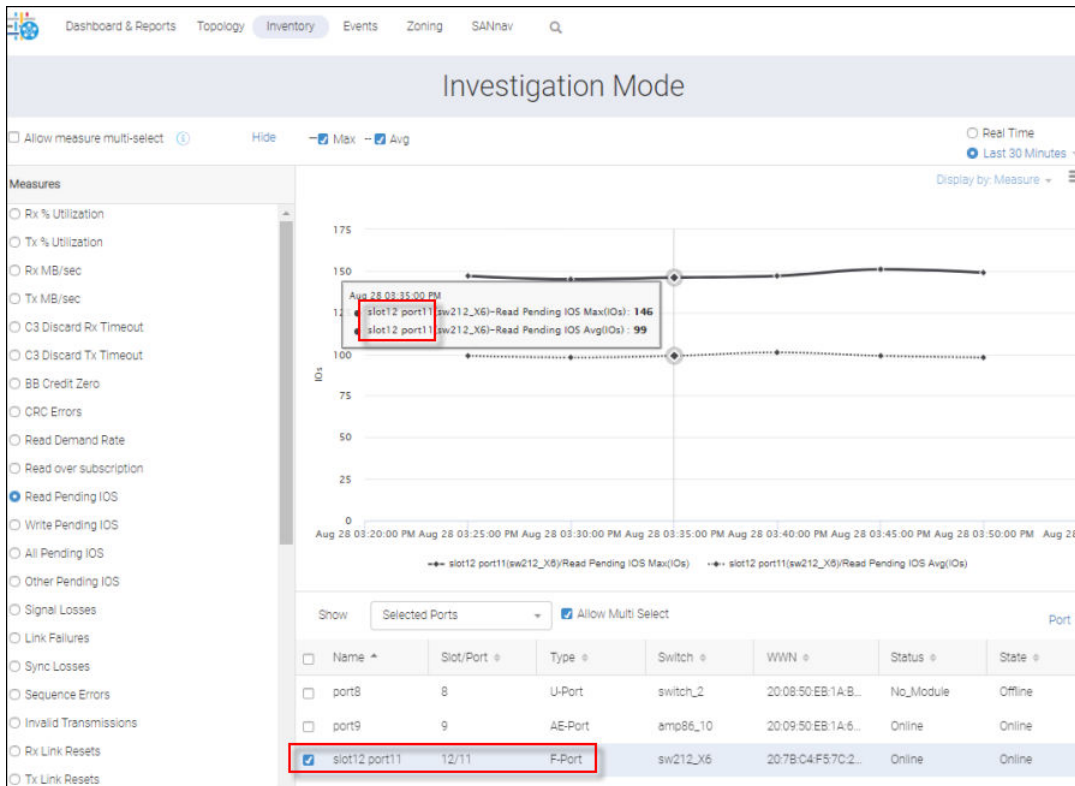
5. Select an F_Port from the ports list at the bottom of the **Investigation Mode** window.

Statistics for these measures are viewable only if an F_port has been selected and there is an applicable AMP connected source switch. Else, the graph displays "No data to display." However, when the value is zero, only "zero" is displayed.

- If an F_port is connected with an initiator, AMP provides a value for Read Demand Rate and Read over subscription. For all other measures, zero statistics are received from the switch.
- If an F_port is connected with a target, AMP provides a value for Pending IOS-related measures. For all others, zero statistics are received from the switch.

Each of these measures have max and average values. The **MAX** measure line is solid and the **AVG** measure line is dotted, but both display in the same color.

In the following example, a tool tip provides information on data points for the **Max** and **Avg** graphs.



Note that if you select ports of different types, only the F_Port data displays. This is because Read Pending IOS is exclusive for F_Ports.

- From the ports table at the bottom of the **Investigation Mode** window, click **Flows for F-Port name** on the port list to launch flow investigation mode for a single F_Port. In this example **F-Port name** is port9.

NOTE

This navigation option is available only for F_Ports, and only one F_Port can transition to the flow **Investigation Mode** window.

NOTE

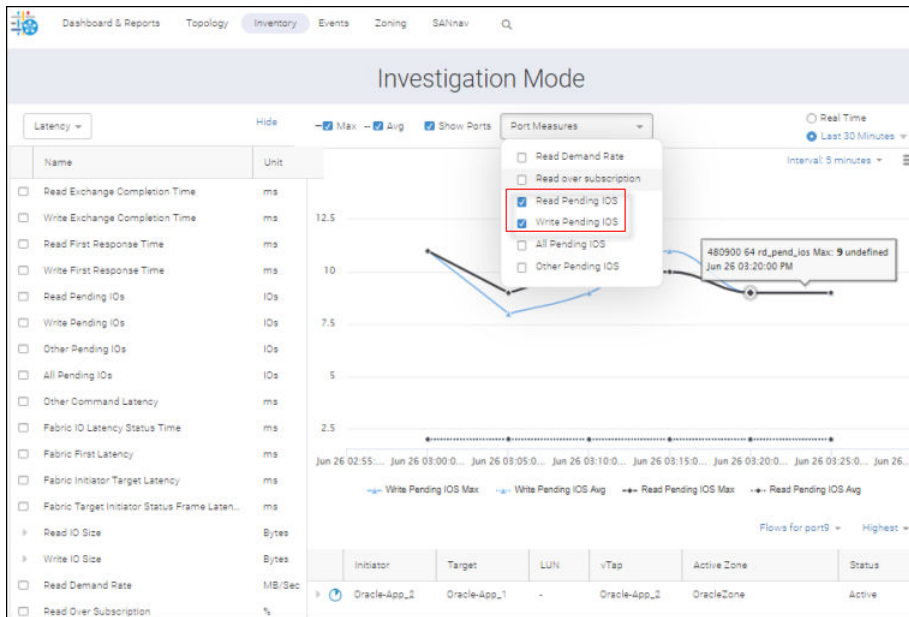
The **Flows for F-Port name** selection is unavailable if the table contains no F_Ports. All F_Ports in the table have the option to launch flow investigation, even if they are not selected in the table view.

Name	Slot/Port	Type	Switch	WWN	Status	Port
port9	9	F-Port	SW-6510-4	20:09:50:EB:1A:...	Online	Online
port16	16	E-Port	SW-6510-4	20:10:50:EB:1A:...	Online	Online
port2	2	AE-Port	SW-6510-4	20:02:50:EB:1A:...	Online	Online

Clicking **Flows for F-Port name** displays all flows passing through the **F-Port name** F-Port.

On the resulting **Investigation mode** window, the **Port Measures** list provides all the port measures specific to F_ports. They have been added to the flow **Investigation mode** view so that you can compare port and flow stats for the same port.

In the following example, you have selected a second port measure from this list, **Read Pending IOS**.



Notice that port list now reads **Flows for Port9**, indicating that you are in Flows Investigation mode, while the tool tip reminds you that the graphs reflect port statistics.

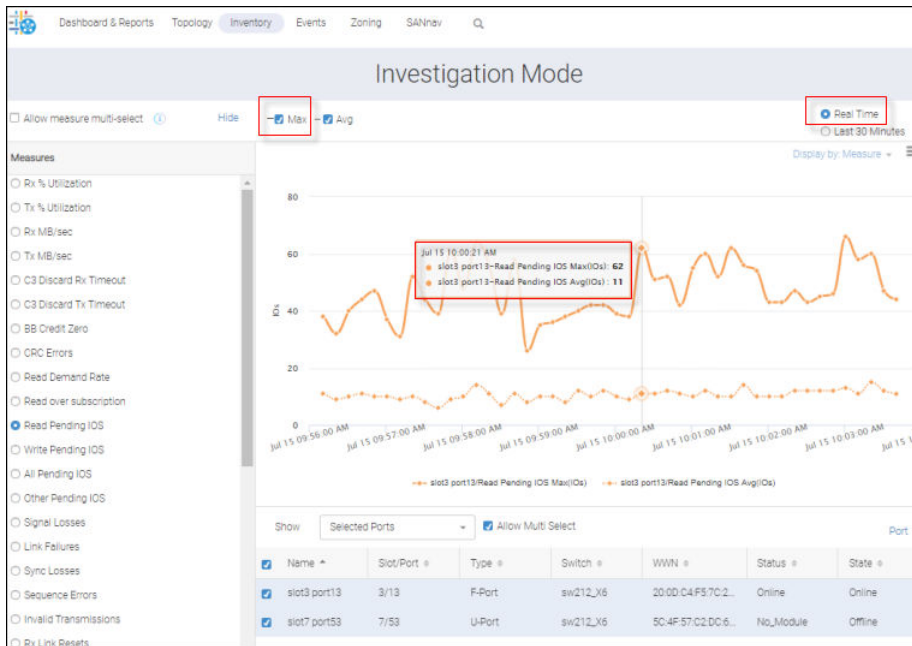
With the **Port** selection on the **Flows for** list, you can return to Port Investigation mode.



7. Select a time interval for the flow investigation.

The time interval applies only to flows. When you return to port investigation mode, the time interval is disabled.

8. Select **Real Time** to see the live performance data.



The time ranges available for port investigation differ slightly from those for flows.

For ports, you can select a date range up to the past 30 days, and for flows you can select a date range up to 6 weeks.

NOTE

Port measures statistics are not visible when NPIV is enabled.

The calculation of granularity is based on the difference between start and end time.

- If the time difference is ≤ 2 hours, it takes a 5-minute data point.
- If the time difference is > 2 hours and ≤ 1 week, it takes a one-hour data point.
- If the time difference is $>$ than 1 week, it takes a 6-hour data point.

6.8.9 Creating a Flow Collection

NOTE

Both Flow and Collection Management privilege are required to manage collections.

Flow Collection, which comprises a set of flows from AMP, enables you to apply advanced capabilities when monitoring a flow. Based on predefined measures, you can create and apply rules to a flow collection. This might enable you to receive early notifications of issues before they deteriorate.

To create a collection, you add flows, add rules, and optionally add aggregated collection rule sets.

1. Select **SANnav** from the navigation bar, and then click **SAN Monitoring > Collection Management**.

This displays the **Collection Management** view where you see both Aggregated and Non aggregated flow collections.

Name	Tags	Description	Member...	Created...	Last Modified
OracleApp	-	-	2	Administrator	Jun 04, 2019 10:21:18...
BankingApp	ITFlows	All IT flows for bank application.	2	Administrator	Jun 04, 2019 10:23:5...

2. To create a flow collection, click **+ > Flow** in the far upper-right corner.

The following dialog appears.

The following guidelines apply to the entry fields (each case insensitive):

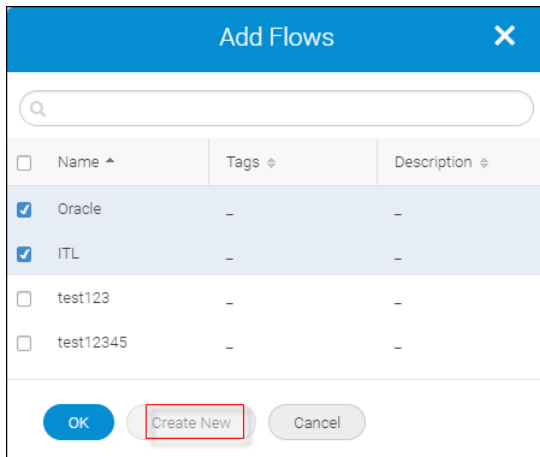
- Collection Name – Alphanumerics with '_' special character (max of 32 chars).
- Tags – Alphanumerics with '_' and comma special character (max of 512 chars).
- Description – All characters accepted (max of 512 chars).

3. To add one or more flows into the new collection view, click **ADD** on the right side of **Flows** in the top half of the **Create New Flow Collection** window.

This displays a list of saved flow filters and you can incorporate their respective flows into your collection.

You can select from the saved filters, or click **Create New** to create a new filter.

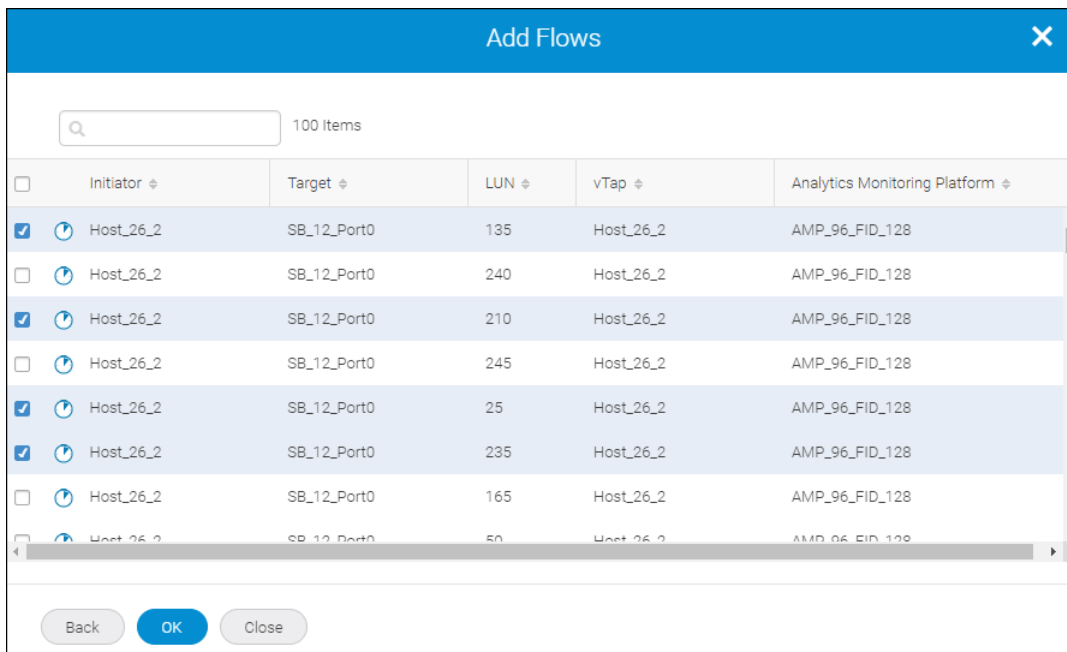
In this example, two filters are selected.



For details on how to create a flow filter, see [Creating a Flow Filter](#).

4. Click **OK**.

You see a list of flows pertaining to the selected filters.



5. Select the flows for the filter, and then click **OK**.

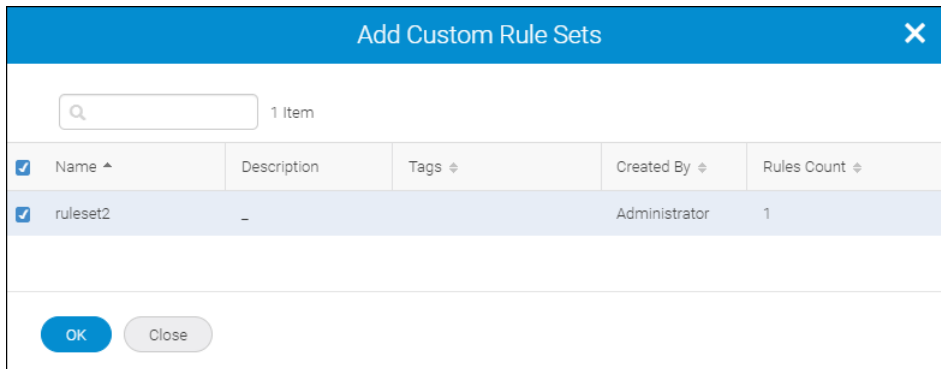
The flows are added to the collection.

NOTE

You can deploy flows to the applicable switches (AMP partitions using FIDs) even if the switch/AMPs that generate the flows differ or AMP is unreachable during the collection deployment.

6. To add to the **Custom Rule Sets** list, click **Add** on the right side of **Custom Rule Sets** in the lower half of the **Create New Flow Collection** window.

The following dialog displays. In this example, ruleset2 has been defined previously.

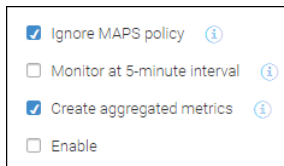


7. Select the rule sets you want to add, and click **OK**.

After clicking **OK**, **ruleset2** has been added to the rule set list.

Your selections are assigned to a collection and the corresponding rules are deployed to the switch and activated along with existing rules.

8. Enable additional options.



Ignore MAPS policy: By default, this option is checked. If unchecked, the rules in the active MAPS policy on the AMP units are enforced against the flows that are defined in this collection.

Monitor at 5-minute interval: This option enables you to either move flows from 6-hour to 5-minute granularity or retain 5-minute flows as is.

You can select a flow (IT or ITL) from the 5-minute or 6-hour category. When select this option, flows from the 6-hour category are moved to the 5-minute category once a collection is deployed to a switch.

Create aggregated metric: This option creates collection-level metrics by aggregating metrics from all the flows that are defined in the collection. An aggregated collection adheres to the aggregated rule sets and notifies you when a threshold met.

If both **Create aggregated metric** and **Monitor at 5-minute interval** are selected, aggregation collection happens every 5 minutes. Else, it happens every 6 hours.

Enable: If checked, the collection aggregation process begins, the collection is saved in SANnav, and it is deployed in the AMP switch. If unchecked, the collection is saved in SANnav but collections are not pushed to AMP and aggregation does not happen.

When AMP fabrics are un-monitored, and then monitoring is reestablished, you can re-edit the collection for a successful redeployment.

NOTE

When you disable the monitoring of a fabric or AMP, all collections are cleared from AMP switch. When monitoring is restored, you must first disable the collection by unchecking the **Enable** checkbox, then save the collection, enable the collection by checking the **Enable** checkbox, and finally save the collection. This redeploys the collection to AMP switch.

NOTE

When you restore the backup in the restore server, you must first disable the collection by unchecking the **Enable** checkbox, then save the collection, enable the collection by checking the **Enable** checkbox, and finally save the collection to redeploy the collection to the AMP switch.

9. Build the aggregated collection rule set. Select the **Create aggregated metric** option on the **Create New Flow Collection** window.

The **Create New Flow Collection** window expands to display an empty **Aggregated Collection Metrics Rule Set** list.

0 Items

Name	Description	Tags	Created By	Rules Count	
No data to display.					

Buttons: Save, Delete, Cancel, Add

- a. To build this list, click **Add**.

The **Add Custom Rule Sets** dialog displays.

In this example, two custom rule sets are already defined.

Name	Description	Tags	Created By	Rules Count
test	-		Administrator	1
testrule	-		Administrator	1

Buttons: OK, Close

- b. Select the rule set that you want to add to the list, and then click **OK**. (In this example, the rule set **test** is selected.)

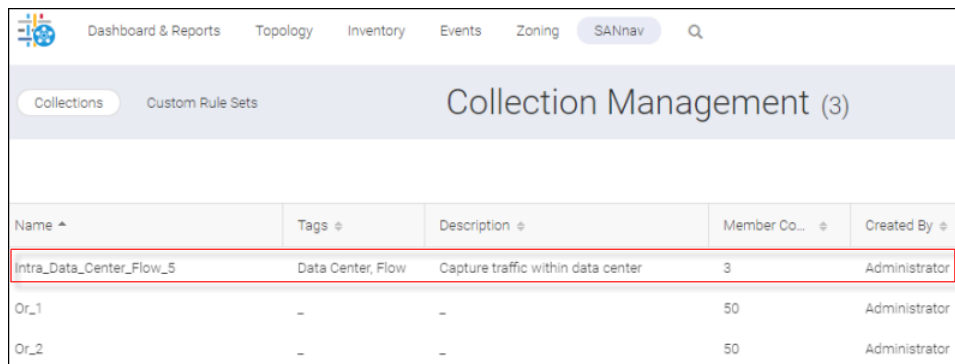
The **Aggregated Collection Metric Rule Set** displays with the added rule set.

Name	Description	Tags	Created By	Rules Count	
test	-		Administrator	1	Change

You can click **Change**, which redisplay the **Add Custom Rule Sets** dialog, and then replace the rule set if necessary.

10. Click **Save** at the bottom of the **Create New Flow Collection** window.

The new Collection appears on the **Collection Management** window.



Name	Tags	Description	Member Co...	Created By
Intra_Data_Center_Flow_5	Data Center, Flow	Capture traffic within data center	3	Administrator
Or_1	-	-	50	Administrator
Or_2	-	-	50	Administrator

SANnav attempts to validate your collection when you click **Save**. This process could fail for the following reasons:

- The collection name is not unique.
- The number of monitoring flows at 5 minute interval exceeds the maximum capacity (For example, ITL capacity could be 5K and the currently consumed maximum is 4700).
- The switch is unmonitored or unreachable.
- A selected flow is also part of real time investigation.
- AMP is not bounded to SANnav. Bounding is necessary to push a collection to a switch.
- The number of flows in a non aggregated collection exceeds the limit for the switch:
 - Max supported flows per collection: 10K
 - Max supported flows across all collections: 40K

You can also delete a collection from the **Collection Management** window.

6.8.9.1 Creating a Flow Filter

The flow Filter Management feature enables you to create filters that narrow your search in general. In SANnav 2.0, Filter Management supports flow filters.

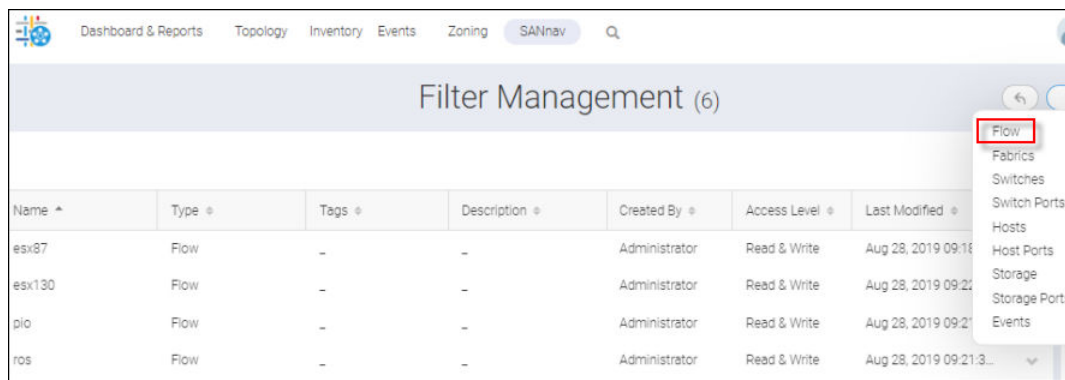
In the following discussion, it is assumed that you have Flow Management privilege. Else, the Flow Option (Step 3) is unavailable.

To apply flow Filter Management, perform the following:

1. Select **SANnav** from the navigation bar, and then click **SAN Monitoring > Filter Management**.

This display the **Filter Management** window where all the current filters are listed.

2. Click "+" to display a list of filter types.



Name	Type	Tags	Description	Created By	Access Level	Last Modified
esx87	Flow	-	-	Administrator	Read & Write	Aug 28, 2019 09:16
esx130	Flow	-	-	Administrator	Read & Write	Aug 28, 2019 09:21
plc	Flow	-	-	Administrator	Read & Write	Aug 28, 2019 09:21
fos	Flow	-	-	Administrator	Read & Write	Aug 28, 2019 09:21:3...

3. Select **Flow**.

NOTE

The **Flow** option is not listed if you do not have Flow Management privilege.

This displays the **Create New Flow Filter** dialog.

You can add up to 40 initiators and/or up to 40 targets for each filter. In this example, the plan is to add 2 initiators and 3 targets on the new filter.

4. Click **Filter by** to show the different filter categories.

Each category type (ITL, Zone Alias, and so on) has different inputs.

For example, if you select **Active Zone** in the **Filter by** list, the inputs would be Active Zone and LUN.

NOTE

If you specify **Filter by ITL** and you want to filter IT flows, leave the **LUN** field blank.

The **Filter by** functionality determines the function of the generated filter and the required input.

For example, consider the **Create New Filter** dialog that appears when you select **Zone Alias** from the **Filter by** list.

If you specify a **Zone Alias** and set **LUN** to *, you pick up all flows based on the initiators and targets participating in either Zone Alias One or Two.

- Referring to the previous example, supply a name, and * for the **Initiator**, **Target**, and **LUN** fields.

For LUN, any number or range can be entered. Valid examples include the following

- 23
- 1,2,3
- 1–20
- 1–20,40–100
- 1–20,50,70–100
- "*"

NOTE

Applying Type Ahead functionality, once you enter 3 characters, the associated fields are displayed.

- Click **OK**.

The **Filter Management** window displays, listing your new filter.

6.8.9.2 Importing and Exporting a Collection

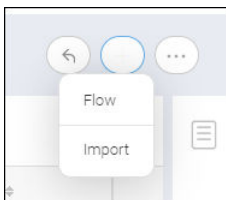
You can import and export a collection by performing the following steps.

- Select **SANnav** from the navigation bar, and then select **SAN Monitoring > Collection Management**.

You see a list of all the collections that are accessible to you.

- Click **+** on top right corner of the **Collection Management** window and click on support.

The action list now displays **Import**.

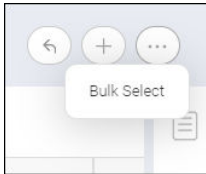


- Click **Import**.

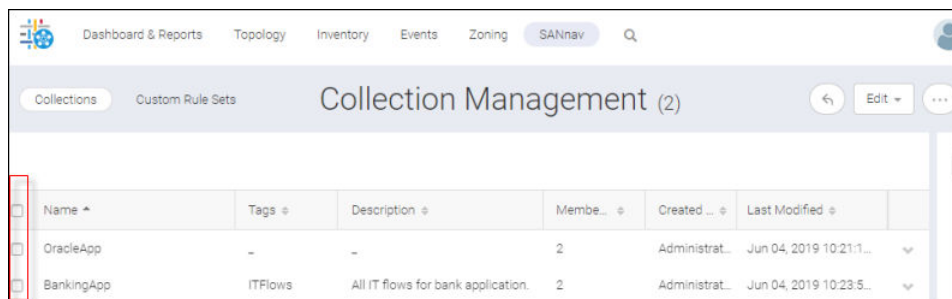
- In the **Browse** file window, browse to the location of the collection JSON file that you want to import.

Once collection is imported it is deployed to AMP depending on the collection definition in the imported JSON file and it is viewable on the **Collection Management** window among the other created collections.

- To export a collection from the **Collection Management** window, click ... in the upper right corner and then select **Bulk Select**.

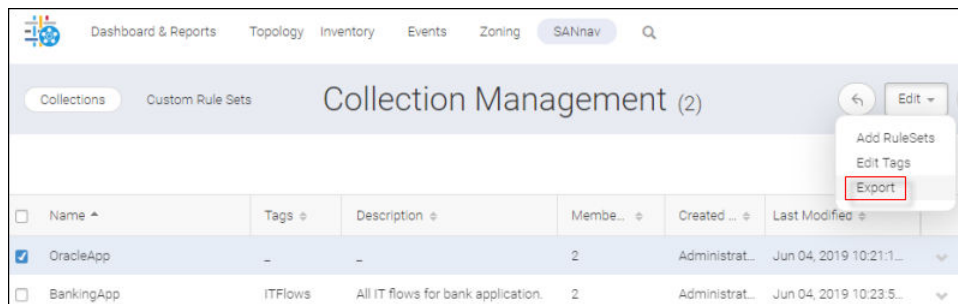


The collections now appear with a checkbox on the far left.



- Click the checkboxes of the collections that you want to export, and then click **Export** from the **Edit** list.

The collection is exported to your local machine as a JSON file.



6.8.10 Creating a Custom Rule Set

NOTE

Both Flow and Collection Management privileges are required to manage custom rule sets.

A rule is a combination of a category type, a measure, a data size, and a threshold value. A rule set is a set of rules grouped together. Customizing a rule set and applying it to collections simplifies the managing process.

Custom collection rule sets are of two types:

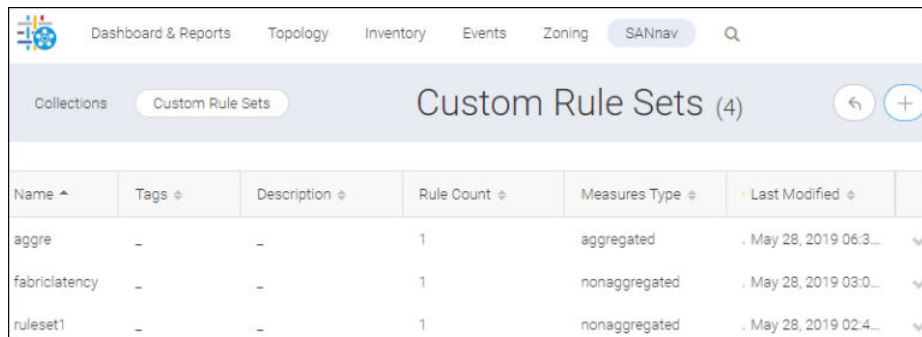
- **Non Aggregated** – This rule set is deployed onto the AMP switch and persists in the database. It is applied to flows after addition to a collection.
- **Aggregated** – This rule set persists in the database but is not deployed onto the AMP switch. It can be added only to aggregate-enabled collections.

6.8.10.1 Managing a Custom Rule Set

To manage custom rule sets, do the following:

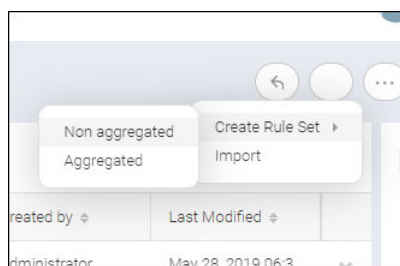
1. Select **SANnav** from the navigation bar, and then select **SAN Monitoring > Collection Management**.
2. Click **Custom Rules Sets** in the subnavigation bar.

You see a list of all the rule sets accessible to you. If you have not created any rule sets, this page is empty.

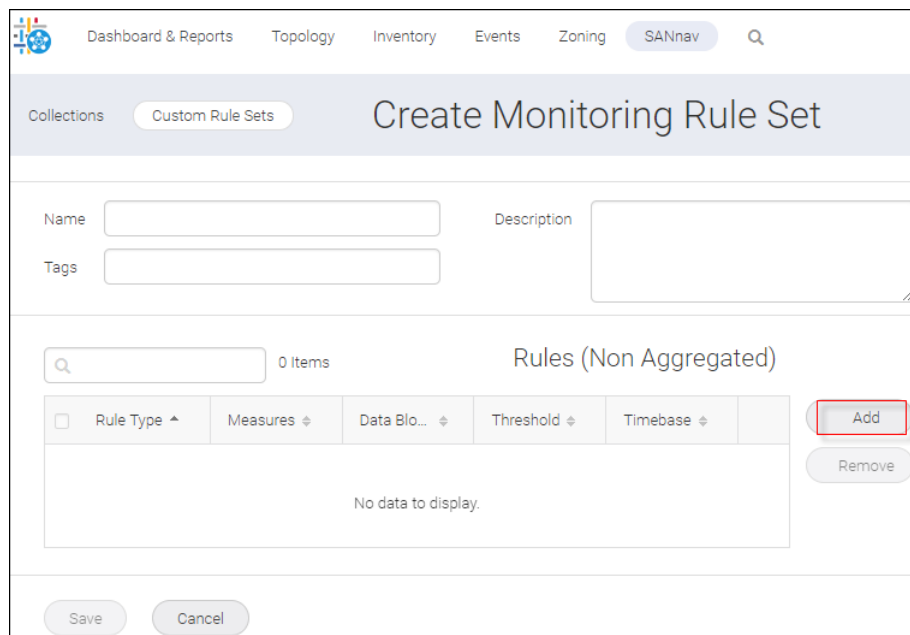


Name	Tags	Description	Rule Count	Measures Type	Last Modified
aggre	-	-	1	aggregated	. May 28, 2019 06:3...
fabriclatency	-	-	1	nonaggregated	. May 28, 2019 03:0...
ruleset1	-	-	1	nonaggregated	. May 28, 2019 02:4...

3. Click **+** on the upper right, and then select **Create Rule Set** and either **Non aggregated** or **Aggregated**.



The **Create Monitoring Rule Set** dialog displays.



Create Monitoring Rule Set

Name: Description:

Tags:

Rules (Non Aggregated)

Rule Type	Measures	Data Blo...	Threshold	Timebase
No data to display.				

Buttons: Add, Remove, Save, Cancel

The case-insensitive fields on this dialog have the following restrictions:

- Custom Rule Set Name text Field - Accepts only alphanumeric and the ‘_’ special char (max of 32 chars for Custom Rule Sets Name [with no empty spaces]).
 - Tags Text Field - Accepts only alphanumeric and the ‘_’ and comma special char (max of 512 chars [with no empty spaces]).
 - Description Text Area - Accepts all characters (max of 512 chars).
4. Click **Add** to add rules to the new rule set.

Select the **Rule Type**, a **Measure**, and a **Data Block Size**. In this example, **IO Performance**, **READ IOPS**, and **<8K** are selected.

The screenshot shows the 'Add Rules' dialog box. On the left, under 'Create Rule', the following settings are visible: Rule Type is 'IO Performance', Measures is 'Read IOPS', Data Block Size is '< 8K', Threshold is '>', IOPS is selected, Timebase is 'SEC', and three action checkboxes (RAS Log Event, SNMP Trap, Email) are all unchecked. On the right, under 'Selected Rules', there is a table with columns 'Type', 'Measures', and 'Data Block Size'. The table is currently empty, displaying 'No data to display.' Below the dialog are 'Ok' and 'Cancel' buttons.

A custom rule set must contain at least one rule.

Because actions are not supported for I/O-based rules, only SEC time base rules can have actions configured.

Notice that for an aggregated rule set, you have a **Severity** option in lieu of **Timebase**, **Actions**, and **Data Size**.

The screenshot shows the 'Add Rules' dialog box. On the left, under 'Create Rule', the following settings are visible: Rule Type is 'IO Latency', Measures is 'Write Exchange Completion Time', Threshold is '>' with a value of '20' and unit 'ms', and Severity is 'Warning'. A dropdown menu for Severity is open, showing options: Warning, Critical, Error, and Info. On the right, under 'Selected Rules', there is a table with columns 'Type', 'Measures', and 'Data Block Size'. The table is currently empty, displaying 'No data to display.' Below the dialog are 'Ok' and 'Cancel' buttons.

NOTE

In the same rule set, you cannot set rules with the same measure and data size but different thresholds.

5. Click **OK** to add the custom rule to the rule set list.

6.8.10.2 Importing and Exporting a Custom Rule Set

You can import and export a custom rule set by performing the following steps.

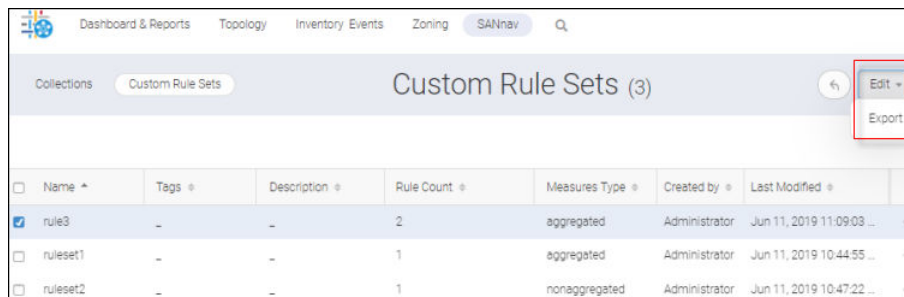
1. Select **SANnav** from the navigation bar, and then select **SANnav > Collection Management**.
2. Click **Custom Rule Sets**.

You see a list of all the rule sets accessible to you.

3. Click ... on the upper right of the rule set list, and then select **Bulk Select**.

The rule sets now appear with a checkbox on the far left.

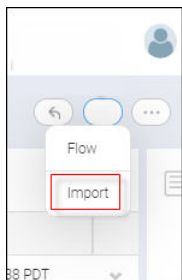
Click the checkboxes for the rule sets you want to export. If you intend to export a single rule set, just click **Export** from the action list.



<input type="checkbox"/>	Name	Tags	Description	Rule Count	Measures Type	Created by	Last Modified	
<input checked="" type="checkbox"/>	rule3	-	-	2	aggregated	Administrator	Jun 11, 2019 11:09:03
<input type="checkbox"/>	ruleset1	-	-	1	aggregated	Administrator	Jun 11, 2019 10:44:55
<input type="checkbox"/>	ruleset2	-	-	1	nonaggregated	Administrator	Jun 11, 2019 10:47:22

The rule set is exported to your local machine as a JSON file.

4. To import a custom rule set, click + > **Import** on the **Collection Management** window.



5. In the browse window, select the rule set JSON file that you want to import.
6. Once **Import** completes, the rule set that you imported is displayed on the **Custom Rule Sets** window.

6.8.11 Investigating an Aggregated Collection View

During the collection process you can aggregate flows to provide an historical perspectives. This might help you understand certain behaviors and their associated issues.

Aggregate collection involves only the latest flow members. Therefore, if the flow members change, they might not be reflected in the completed aggregations.

Flows are aggregated in either 5-minute or 6-hour intervals based on the selections made on creation. For any collection to be aggregated, the **Enable** and **Create aggregated metrics** options must be selected on the **Create New Flow Collection** window. If the **Monitor at 5-minute interval** option is also selected, the collection aggregates at 5-minute. A 5-minute snapshot serves as the source table for the aggregation. Similarly, 6-hour statistics tables are the source for 6-hour collection aggregation.

All flows are considered for aggregation independent of their status (Active or Inactive).

SANnav supports the following:

- A maximum of 500 collections per logical AMP with a maximum of 10k flows in each collection
- A maximum of 40k flow definitions per logical AMP (across 500 collections) and 20k active flows per AMP chassis

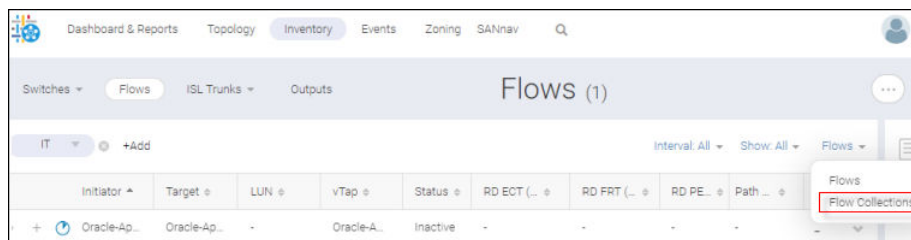
SANnav applies the collection flows only to applicable AMP partitions that are using the flow FIDs.

Starting with AMP OS 3.0.0, you can associate new attributes (like flows time granularity and real-time) with collection. You can also create collections that monitor flows exclusively in 5-minute granularity and that do not age out.

To investigate an aggregate collection, do the following:

1. Select **Inventory** > **Flows** from the navigation bars.

The **Flows** window displays.



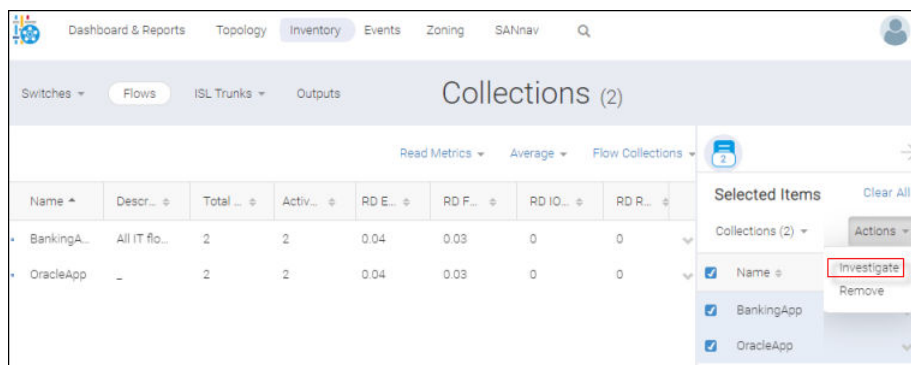
2. For a selected flow, select **Flow Collections** on the **Flows** action list.

The aggregated **Collections** window displays.

Name	Description	Total Flows	Active Flows	RD ECT (ms)	RD FRT (ms)	RD IOPS	RD Rate (M...)
BankingApp	All IT flows for ...	2	2	0.04	0.03	0	0
OracleApp	-	2	2	0.04	0.03	0	0

3. If you want to launch investigation mode immediately, select a collection from the list and click **Investigate** from the action list for that collection.

Alternatively, you can move selected collections to the **Selected Items** sidebar and click **Investigate** from the action list. This method of selection and launch enables you to study the collections at a time of your choosing.



Either way, the aggregate collection **Investigation mode** window displays with the selected collections displayed in the table.

The graph is blank until you select a measure. In the example below, a chart is rendered for the selected measure **Write First Response Time**.

From here, you can view and investigate flows for a particular collection.



All the flow aggregated metrics are available to investigate.

By default, both **Avg** and **Max** are selected. Notice the dotted (Avg) and solid (Max) lines for the selected measure.

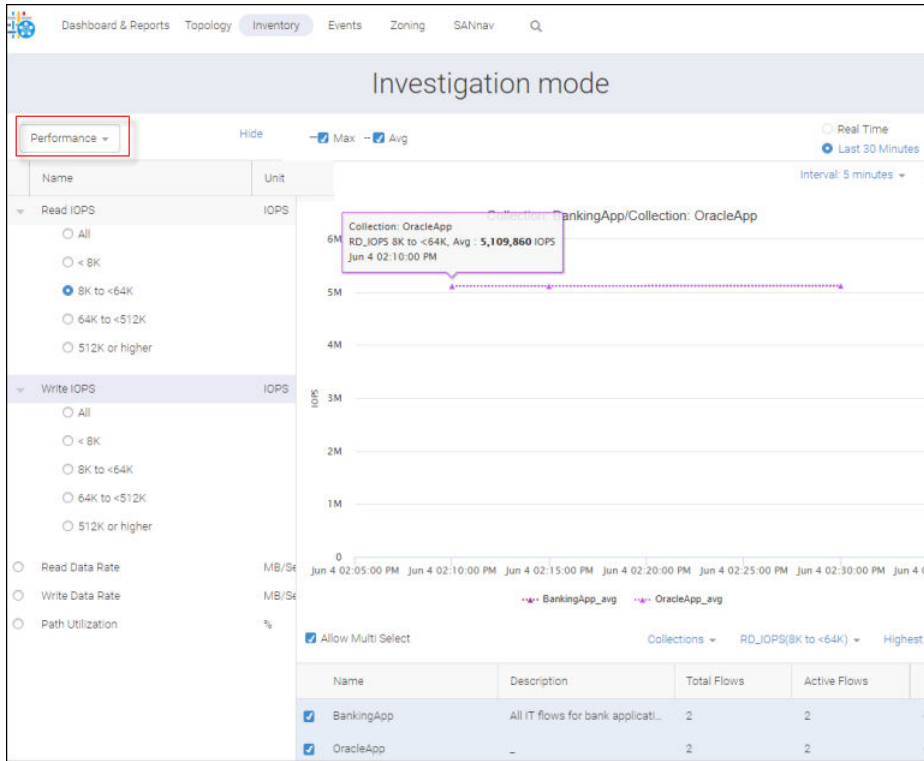
NOTE

The **Real time** option is disabled for collection investigation view.

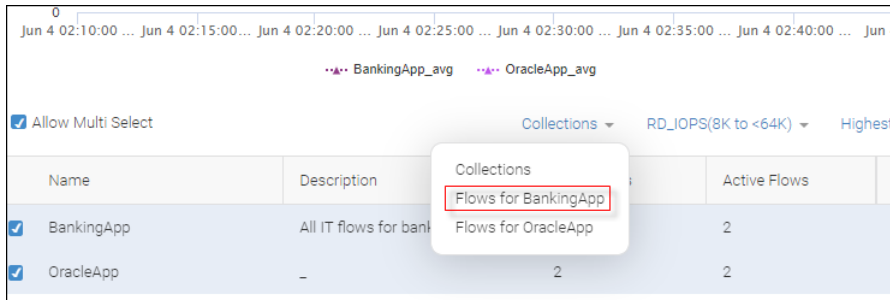
The **Interval** list operates here as it does in flows investigation.

4. Select a category and measure from the measure list.

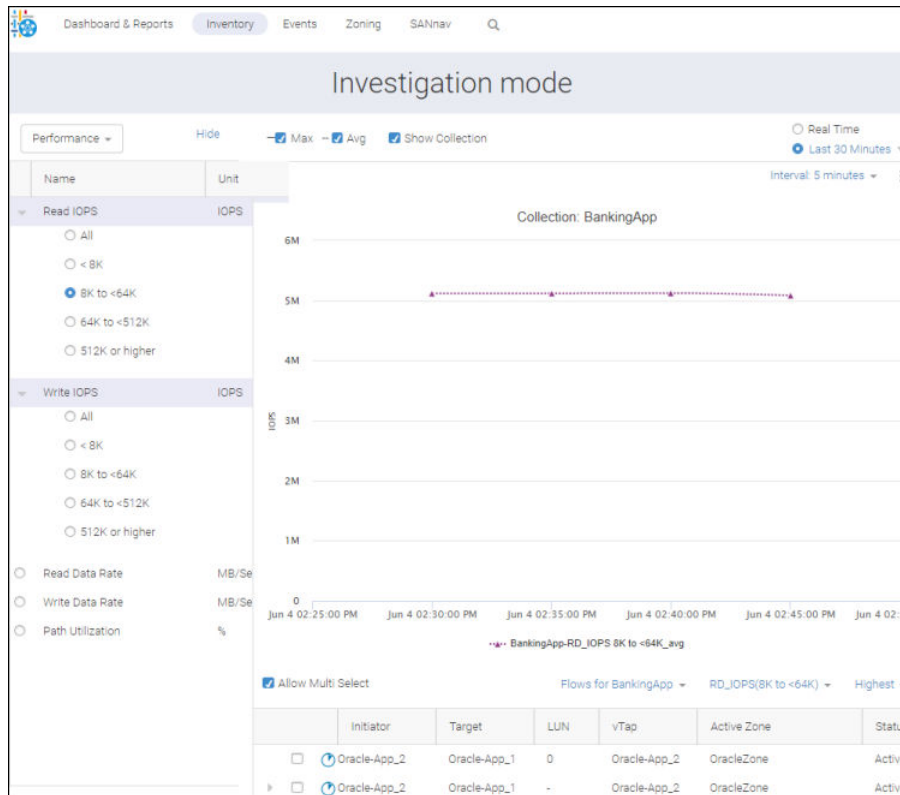
For example, if you first select the category **Performance**, then the measure **Read IOPS** and specify a size **8K to <64K**, your image might appear as follows.



5. To view the flows for a particular collection, click **Flows for <Collection Name>** on the **Collection** list in the bottom right of the **Collection** table.



The **Investigation mode** window displays. Only the collection plotting is represented in the chart.

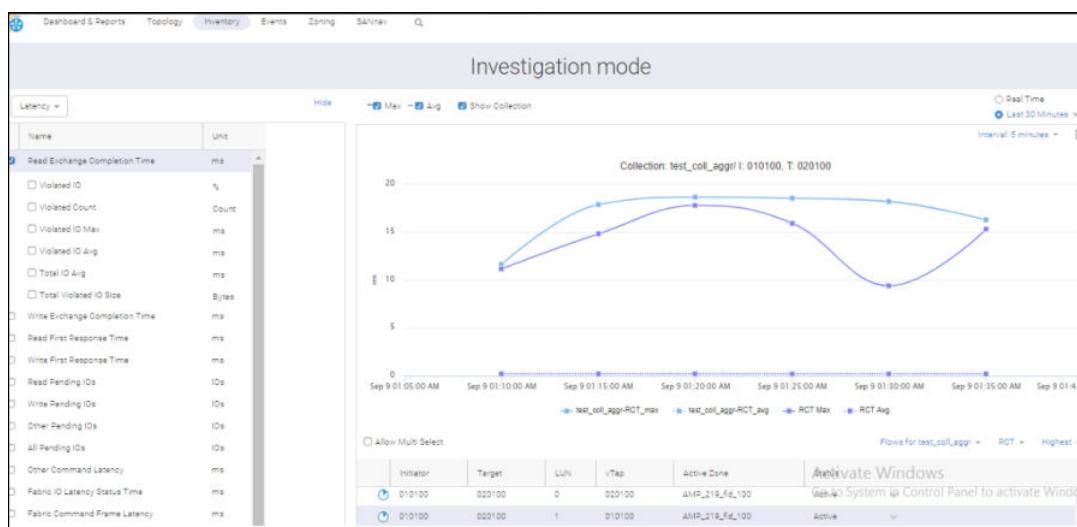


6. Uncheck **Show Collection** to restrict your chart to the selected flows.

By default **Show Collection** is checked, which means that you can view the chart data for the selected collection along with the chart data for the selected flow.

To illustrate this functionality, select one of the flows as well as the measure **Read Pending IOs**. You can see the line for the collection as well as the solid and dotted lines for the flow.

Only the chart data for the selected flow (when the **Show Collection** checkbox is unchecked) displays.



When you switch back to aggregate collection Investigate mode, the initially selected collections are displayed as selected. Moreover, **Measure**, **Avg**, **Max**, and **Date Range** are also retained. Table data alone is modified based on the current view, whether it is a collection or flow.

6.8.12 Report Widgets for AMP

Report procedures like editing and exporting reports are the same for Flow Management as they are for standard reports.

In this section, you see the flow widgets that are unique to AMP and how to create reports incorporating those widgets.

Widgets can be largely categorized under Top N and Time Series. Top N captures the top performers. Time Series captures the performance over time.

In the following table, you see the flows, storage/host ports and collections as well as the widgets associated with Time Series. You also see the top (labeled Top) and bottom (labeled Threshold) portions of Top N. Widgets are also categorized by location on the Top N window as well as whether they relate to Flows, Storage port, Host Port, and Collection.

Category	Flows	Storage Port	Host Port	Collection
Top	Top SCSI Errors Top Flow Violations	Top Storage Port Exchange Completion Time Top Storage Port First Response Time Top Storage Port Data Rate Top Storage Port IOPS Top Storage Port Pending IOS	Top Host Port Pending IOs Top Host Port Read Over Subscription	Top Collection Aggregation
Threshold	Top SCSI Errors (Occurrences) Max of 500 SCSI flows Top Flow Violation (Occurrences)	Top Storage Port Exchange Completion Time (Occurrences) Top Storage Port First Response Time (Occurrences) Top Storage Port Data Rate (Occurrences) Top Storage Port IOPS (Occurrences) Top Storage Port Pending IOS (Occurrences) Max of 100 ports	To Host Port Pending IOs (Occurrences) Top Host Port Read Over Subscription (Occurrences) Max of 100 device ports	Top Collection Aggregation (Occurrences)
Time Series	Time Series – Flow Violations Time Series – Flow Max of 10K flows	Top Storage Port Exchange Completion Time (Time Series) Top Storage Port First Response Time (Time Series) Top Storage Port Data Rate (Time Series) Top Storage Port IOPS (Time Series) Top Storage Port Pending IOS (Time Series)	To Host Port Pending IOs (Time Series) Top ROS (Time Series)	Time Series – Flow Collection (aggregated)

Considerations:

- For most Top N and Time Series reports, a filter is optional (like for storage ports). For others, like for the Top N Collection Aggregation widget, the filter is mandatory.

The following table shows which filter is appropriate to which widget

Report Widget	Applicable Filters	Notes
Top Storage Port Exchange Completion	Storage port	Filter is optional.
Top Storage Port First Response Time Latency	Storage port	Filter is optional.
Top Storage Port Data Rate	Storage port	Filter is optional.
Top Storage Port IOPS	Storage port	Filter is optional.
Top Storage Port Pending IOs	Storage port	Filter is optional.
Top Host Port Pending IOs	Host port	Filter is optional.
Top Host Port Over Subscription	Host Port	Filter is optional.
Top N SCSI Errors	None	Report is generated based on all IT flows.
Top N Collection Aggregation	Collection	Filter is required. You can select multiple collections by collection name.
Top Flow Violation	None	Report is generated based on all IT flows.
Collection Aggregated Time Series	Collection	Filter is required. You can select multiple collections by collection name.
Flow Violation Time Series	Flow	Filter is required.
Flow Time Series	Flow	Filter is required.

- For the Top portions of a report, the format is HTML. For Time Series and Threshold, the format is CSV, which is viewable only upon export.
Top SCSI, Violation, and Collection reports include Top and Threshold portions, while Top Host and Storage reports include Top, Threshold, and Time Series portions.
- The columns available for the Top, Threshold, and Time Series segments depend on the customization in the template view.
- Threshold differs from Top N, in that the former lists the entities that have met the threshold. Consequently, it might not match the Top N result. In fact, it might exceed the Top N.
- For widgets where filter is mandatory, an empty report is generated if the supported filter is not applied.
- Time Series presents a maximum limit of 10K.

Report Data Limitations

Flow widgets. If a filter is applied to more than 10k flows, only data for 10k flows is returned.

6.8.12.1 Generating a Time Series Report of Collection Aggregation

You can create a Time Series report for collection aggregation and flow violations. This section outlines the procedure for creating a template for collection aggregation time series. The procedure is identical for the three time series report types supported by SANnav, except for the widget selection.

Perform the following steps.

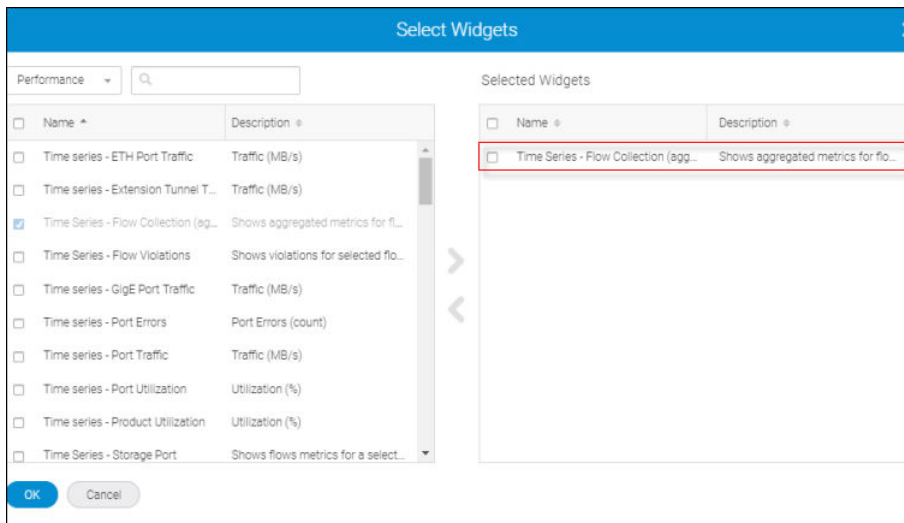
1. Click **Dashboard & Reports** and then **Templates** on the navigation bar.

This displays the **Templates** window.

2. Click **+ > Report > Select Widgets**.

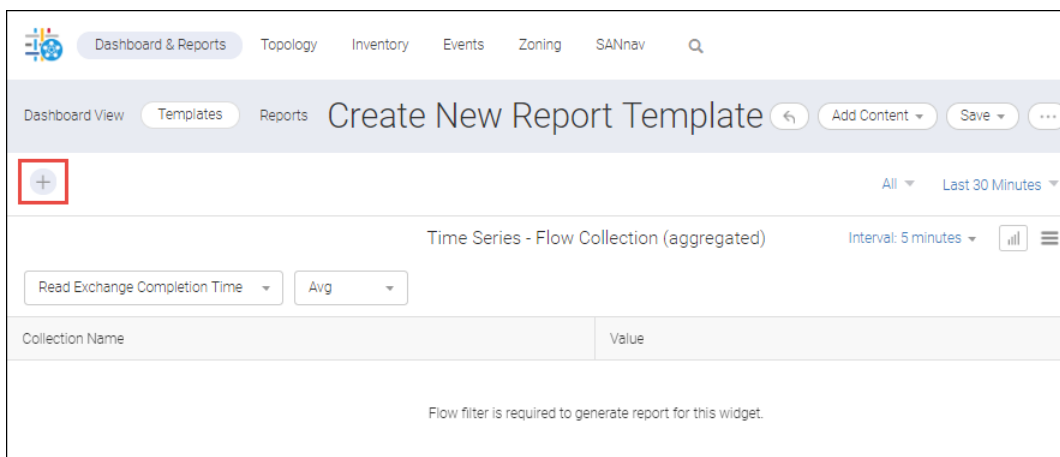
This displays the **Select Widgets** dialog.

3. Select the widget category and a widget within that category, and then click the move icon (>) to position the widget under **Selected Widgets**. In this example, **Performance** and **Time Series - Flow Collection (aggregated)** are selected.



4. Click **OK**.

This displays the **Create New Report Template** dialog.



As the message indicates, to generate a report, a flow **Type Filter** with a collection **Filter By** must be applied to this widget.

5. Create a filter for the report.
 - a. Click **+** on the upper left of the window to add a filter.
 - b. Click **Create New** in the **Add Filter** dialog.
 - c. In the **Create New Filter** dialog, set the following:
 - Filter Type = Flow
 - Filter By = Collections

- d. Click **Add** to add collections to the filter.
- e. Click **OK**. Optionally, you can check the **Save Filter** option, provide values for Name and Tags, and then click **OK**.

The **Create New Port Template** window displays.

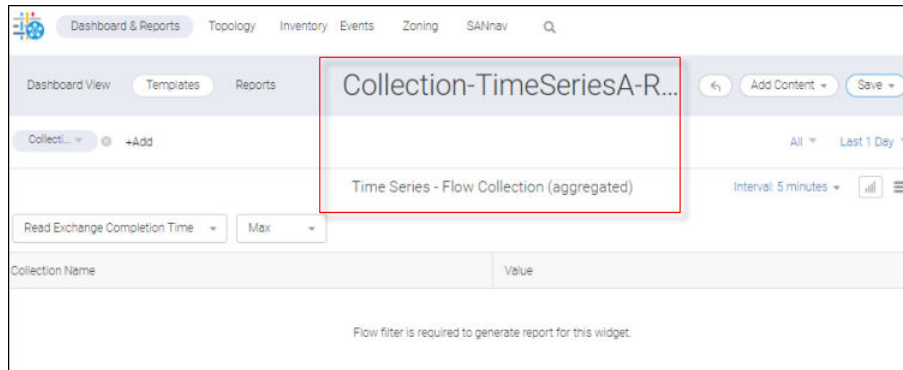
The name you provided appears on the upper left in the filter list. In this example, the name **Collection-TimeSeriesA-Filter** is used.

6. Set the date range and choose **Avg**, **Max**, or both. In this example, **Last 1 Day** and **Max** are selected. You can also change the **Interval** but for this example, the value **5 minutes** is used.

7. Click **Save**.
8. Enter values for the name and tags, and then click **Save**.

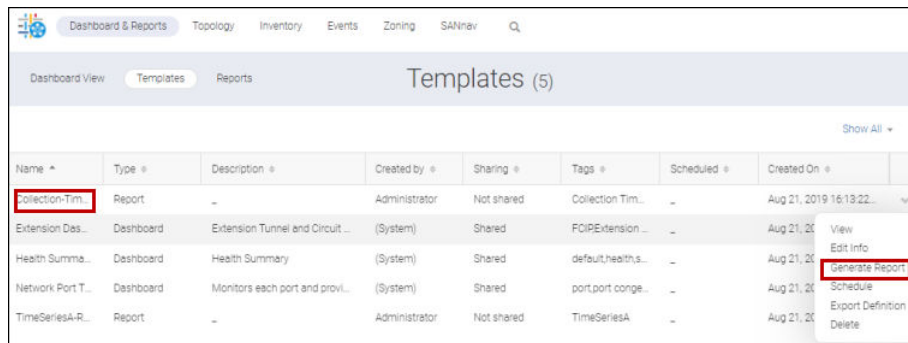
In this example, **Collection-TimeSeriesA-Report** and **Collection TimeSeriesA** are specified.

The new template displays with the name at the top and the widget identifier immediately below.



9. Click the **Templates** tab.

This displays the **Templates** window where you will see the template that you just created.

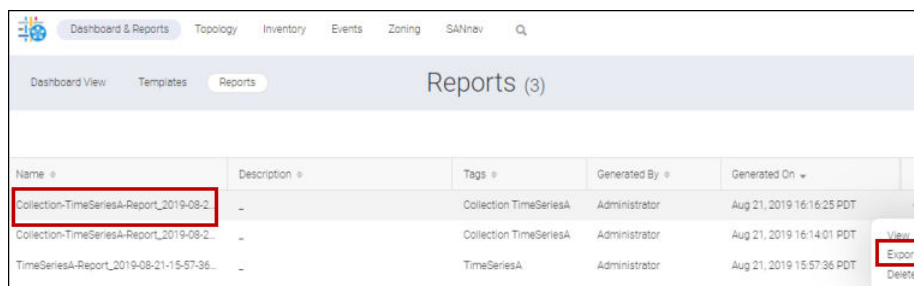


10. Click **Generate Report** from the action list for that template, and then click the **Reports** tab.

NOTE

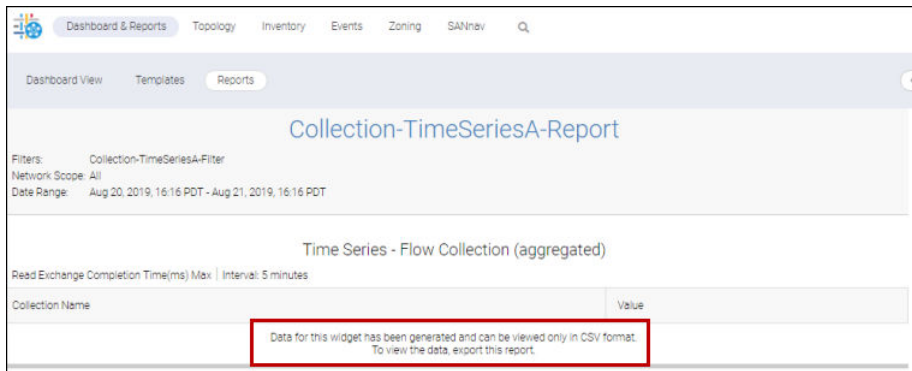
The **Generate Report** option is also available inside the template view.

Notice that your report name now appears in the list appended with a timestamp.



11. Click the report.

As the window indicates, data generated for this widget can only be viewed in CSV format.



12. On the **Reports** window, click **Export** from the action list (boxed).

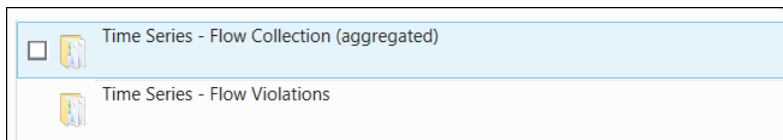
NOTE

The **Export** option is also available in template view.

The report is downloaded as a ZIP file to your local machine and appears on the **Reports** window.

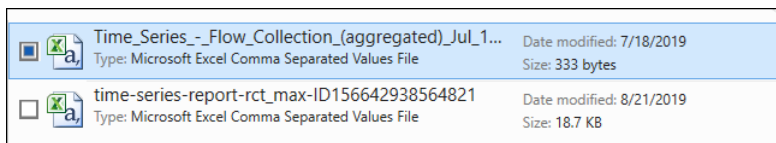
13. Open the ZIP file and double-click the **CSV** folder.

This displays folders of previously generated reports.



14. Double-click the **Time Series - Flow Collection (aggregated)** subfolder.

This displays all the reports created within this category.



15. Double-click the report to display its contents.

6.8.12.2 Generating a Time Series Report for Flow Violations

This section outlines the procedure for flow violations.

Perform the following steps.

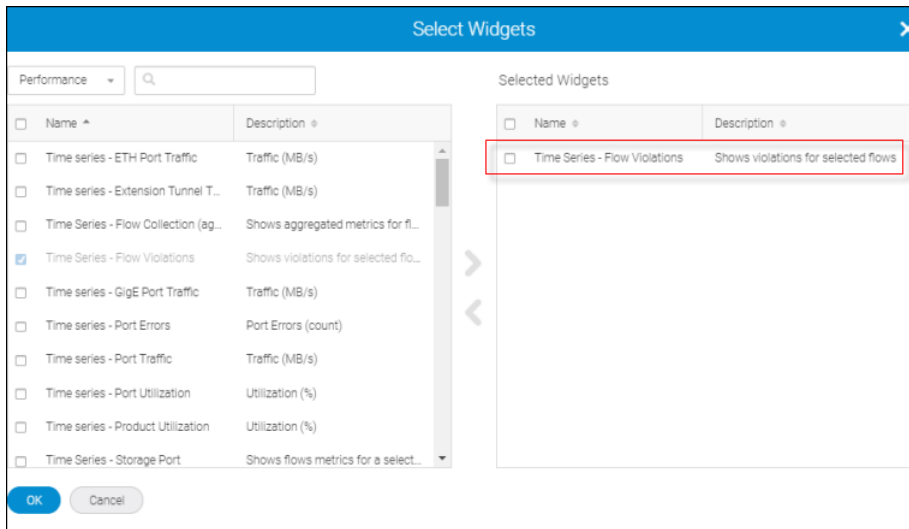
1. Click **Dashboard & Reports** and then **Templates** on the navigation bar.

This displays the **Templates** window.

2. From the **Templates** window, click **+ > Report > Select Widgets**.

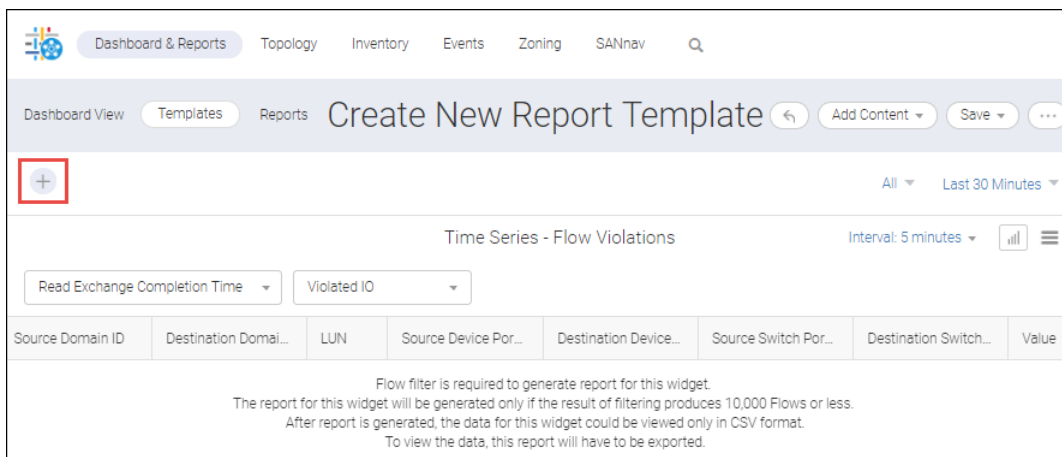
This displays the **Select Widgets** dialog.

3. Select the widget category and a widget within that category, and then click the move icon (>) to position the widget under **Selected Widgets**. In this example, **Performance** and **Time Series - Flow Violations** are selected.



4. Click **OK**.

This displays the **Create New Report Template** dialog.



As the message indicates, you must provide a flow filter to generate a report for this widget and that a report is generated provided the flow number is less than 10K.

5. Create a filter for the report.
- Click **+** on the upper left of the window to add a filter.
 - Click **Create New** in the **Add Filter** dialog.
 - In the **Create New Filter** dialog, set the following to retrieve all ITL flows.
 - Filter Type = Flow
 - Filter By = ITL
 - Initiator = FC Address, Value = *
 - Target = FC Address, Value = *
 - LUN = *

For this example, **FC Address** is accepted for Initiator and Target, and "*" is entered in all entry fields.

However, you could also choose WWN as the input type and the value can be * or any fixed value.

6. Check the **Save Filter** option and specify a name and a set of tags, and then click **OK**. In this example, **FlowViolation-TimeSeriesA-Filter** and **Flow Violation TimeSeriesA** are entered.

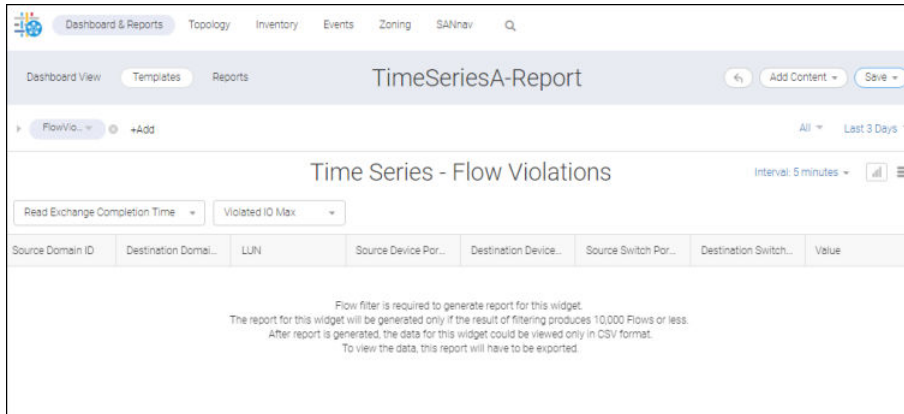
The **Create New Report Template** window displays.

The name that you provided appears on the upper left in the filter list.

7. Set the date range and select from the violation type list. For this example, **Last 3 Day** and **Violated IO Max** are selected. You could also change the interval setting. For this example, the original value of **5 minutes** is unchanged.

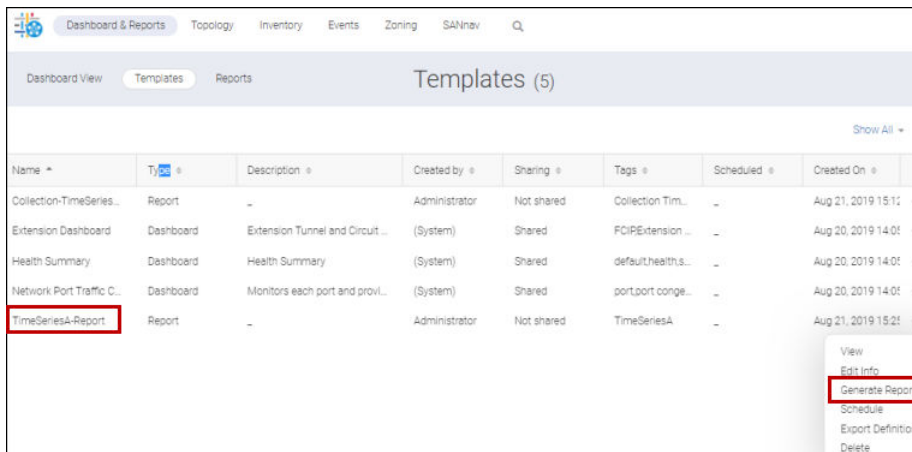
8. Click **Save** to save the new template.
9. Enter a name, define the tags, and then click **Save**. For this example, **TimeSeriesA-Report** and **TimeSeriesA** are entered.

The new template displays with the name at the top and the widget immediately below.



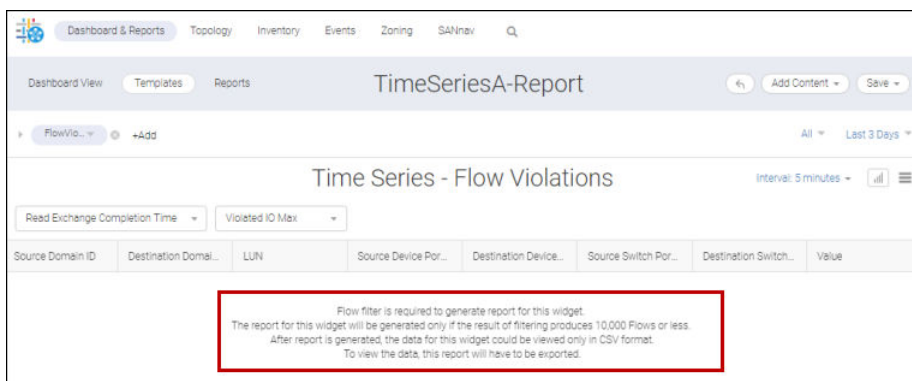
10. Click **Templates**.

This displays the **Templates** window where you will see the template that you just created (boxed).



11. Click a report to display it.

As the boxed text indicates and is typical for a time series reports, generated data is viewable only in CSV format.

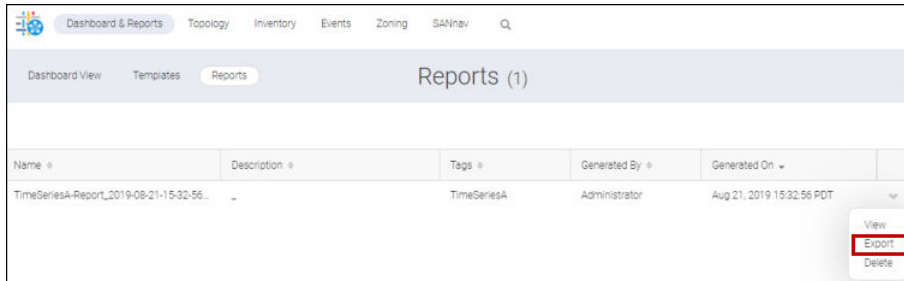


12. Click **Generate Report** from the action list for that template, and then click **Reports**.

NOTE

The **Generate Report** option is also available inside the template view.

Your report name appears in the list appended with a timestamp.



13. On the **Reports** window, click **Export** from the action list (boxed).

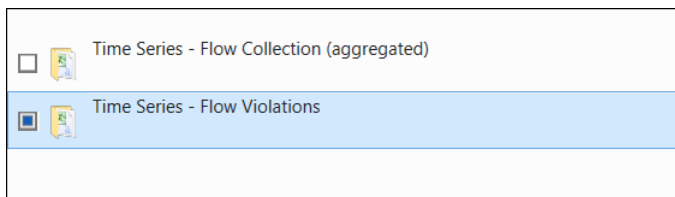
NOTE

The **Generate Report** option is also available inside the template view.

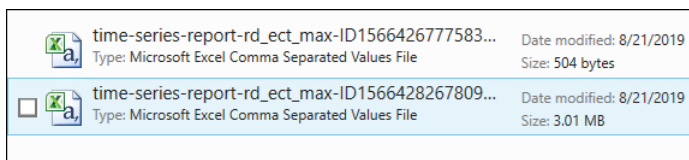
The report is downloaded as a ZIP file to your local machine and it appears on the **Reports** window.

14. Open the ZIP file and double-click the **CSV** folder.

This displays folders of previously generated reports.



15. Double-click the **Time Series - Flow Collection** subfolder.



16. Double-click the report to display its contents.

6.8.12.3 Generating a Top N Report for Collection Aggregation

You can create Top N reports for collection aggregation by doing the following.

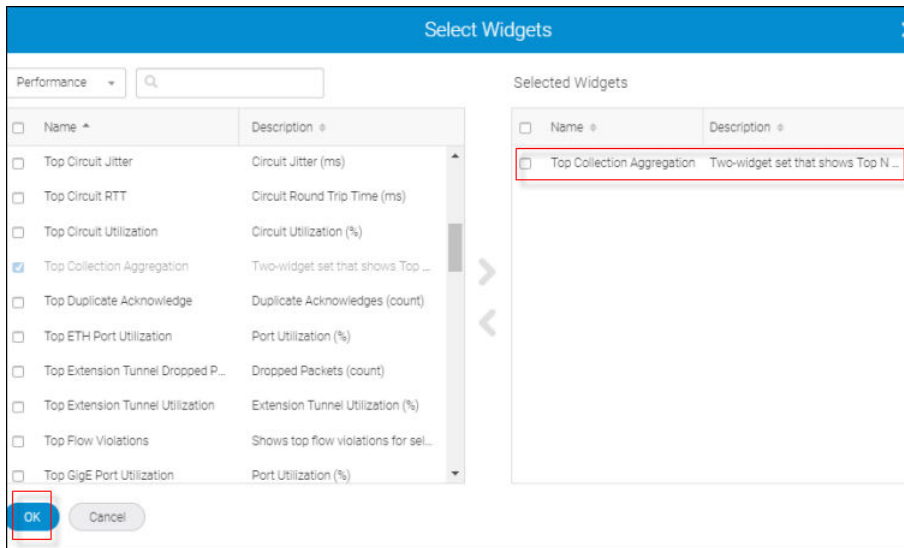
1. Click **Dashboard & Reports** and then **Templates** on the navigation bar.

This displays the **Templates** window.

2. From **Templates** window, click **+ > Report > Select Widgets**.

This displays the **Select Widgets** dialog.

3. Select the widget category and a widget within that category, and then click the move icon (>) to position the widget under **Selected Widgets**. In this example, **Performance** and **Top Collection Aggregation** are selected.

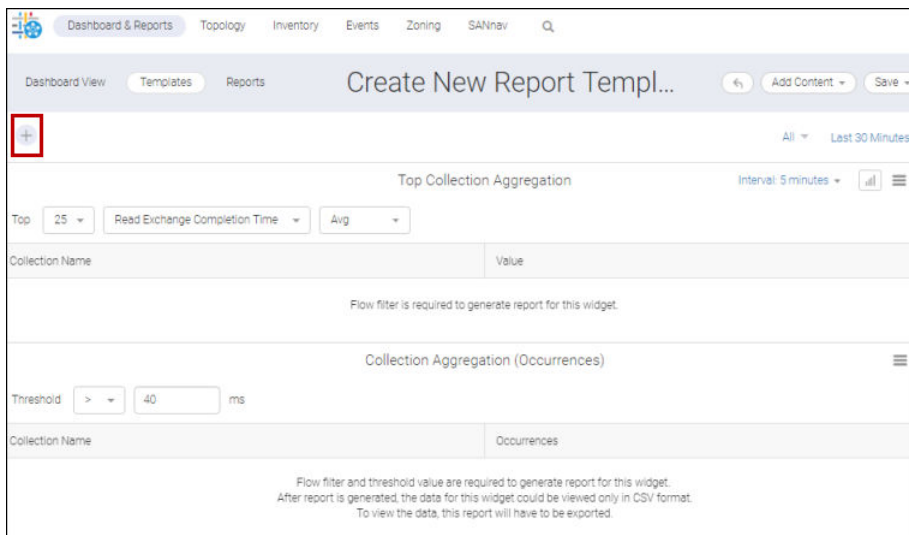


4. Click **OK**.

This displays the **Create New Report Template** dialog.

For Top N reports, you will see two parts: Top N and Occurrences.

As the message indicates, you must provide a flow filter to generate a report for this widget.



As the message indicates, you must provide a flow filter with a collection type filter to generate a report for this widget.

5. Create a filter for the report.
 - a. Click **+** on the upper left of the window to add a filter.
 - b. Click **Create New** in the **Add Filter** dialog.
 - c. In the **Create New Filter** dialog, set the following:
 - Filter Type = Flow
 - Filter By = Collections

Create New Filter

Filter Type: **Flow**

Filter by: **Collections**

Collections: **Add** **Remove**

Save Filter

Back **OK** **Cancel**

- d. Click **Add** to add collections to the filter.
- e. Check the **Save Filter** option, provide a name for the new filter (in this example **MyAllCollection**), and then click **OK**.

The **Create New Port Template** window displays.

The name you provided, **MyAllCollection**, appears on the upper left in the filter list.

Dashboard & Reports | Topology | Inventory | Events | Zoning | SANnav | Q

Dashboard View | Templates | Reports | **Create New Report Template** | Add Content | Save

MyAllC. | +Add | All | Last 30 Minutes

Top: 25 | Read Exchange Completion Time | Avg

Collection Name | Value

Flow filter is required to generate report for this widget.

Collection Aggregation (Occurrences)

Threshold: > 40 ms

Collection Name | Occurrences

Flow filter and threshold value are required to generate report for this widget. After report is generated, the data for this widget could be viewed only in CSV format. To view the data, this report will have to be exported.

6. Select a date range, chose between **Max** or **Average**. In this example, **Last 1 Week** and **Max** are selected. You could also change the Top N value, the measure option, and the interval setting. For this example, the values of **25**, **Read Exchange Completion Time**, and **5 minutes** are selected.

The screenshot shows the 'Create New Report Template' page. At the top right, the date range is set to 'Last 1 Week'. Below that, the 'Top' value is 25, the measure is 'Read Exchange Completion Time', and the aggregation is 'Max'. The 'Interval' is set to 5 minutes. The 'Threshold' is set to 1.5 ms. The interface shows a table structure for 'Collection Name' and 'Value'.

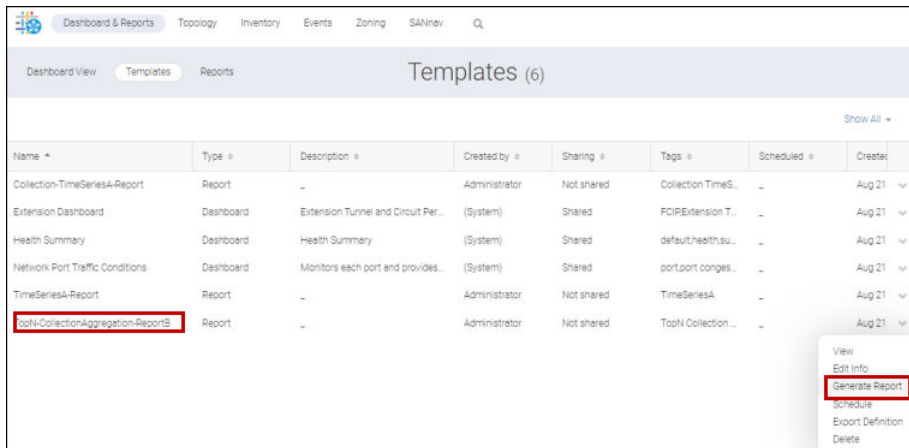
7. For this example, reset the threshold to **> 1.5 ms**.
 8. Click **Save**.
 9. Enter a name and specify tags, and then click **Save**.

For this example, **TopN-CollectionAggrgation-ReportB** and **TopN Collection Aggregation** are specified.
 The new template displays with the specified name at the top.

The screenshot shows the 'Create New Report Template' page with the template name 'TopN-CollectionAggregation-ReportB' highlighted in a red box. The 'Top' value is set to 10, the measure is 'Read Exchange Completion Time', and the aggregation is 'Max'.

10. Click the **Templates** tab.

This displays the **Templates** window where you will find the template that you just created.

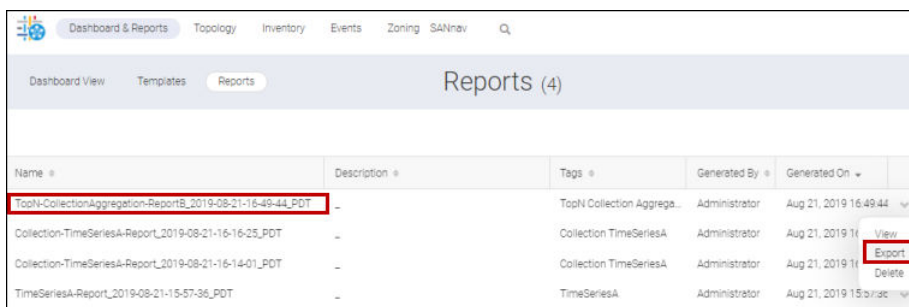


11. Click **Generate Report** from the action list for that template and then click the **Reports** tab.

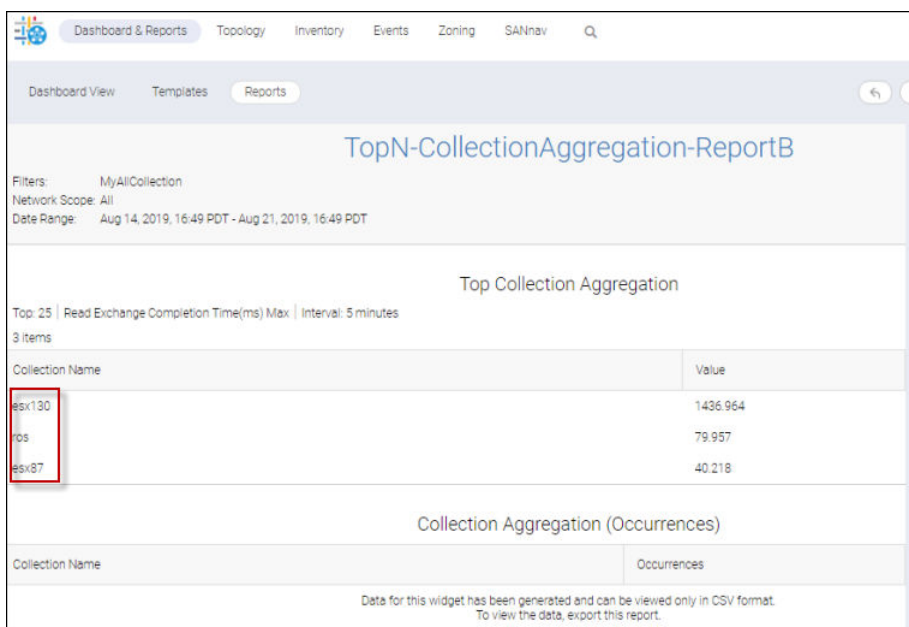
NOTE

The **Generate Report** option is also available inside the template view.

Notice that your report name has now been appended with a timestamp.



12. Click the report.



The TopN collectors are boxed.

As the message indicates, data generated for the Occurrence portion of the report can be viewed only in CSV format.

- On the **Reports** window, select **Export** from the action list.

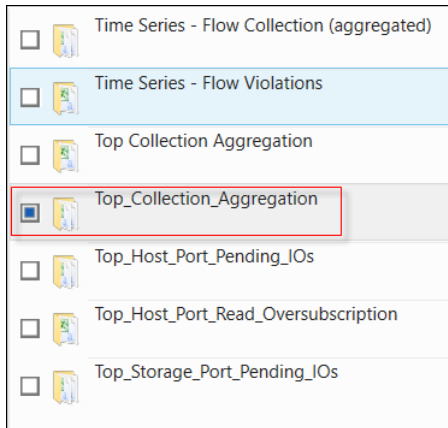
NOTE

The **Export** option is also available in template view.

The report is downloaded as a ZIP file to your local machine and appears on the **Reports** window.

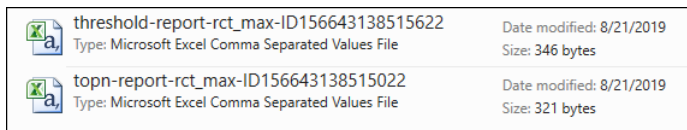
- Open the ZIP file and double-click the **CSV** folder.

- Double-click the **Top Collection Aggregation** folder.



This displays the reports associated with the Top Collection Aggregation report.

- Double-click the report to display its contents.



6.8.12.4 Generating a Top N Report for SCSI Errors

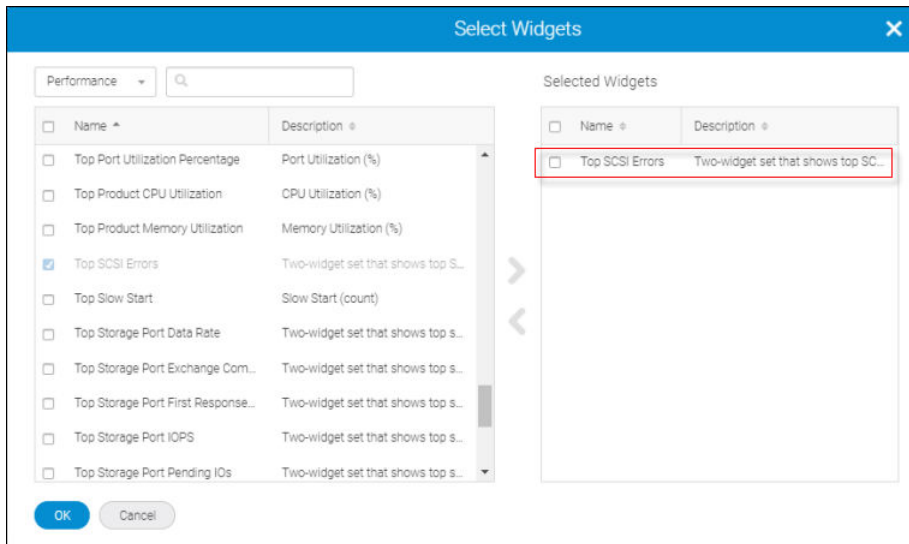
The following procedure shows how to create a Top N SCSI report. The procedure for a Top N Violations report is identical except for the widget used.

- Click **Dashboard & Reports** and then **Templates** on the navigation bar.

This displays the **Templates** window.

- From **Templates** window, click **+ > Report > Select Widgets**.

This displays the **Select Widgets** dialog.

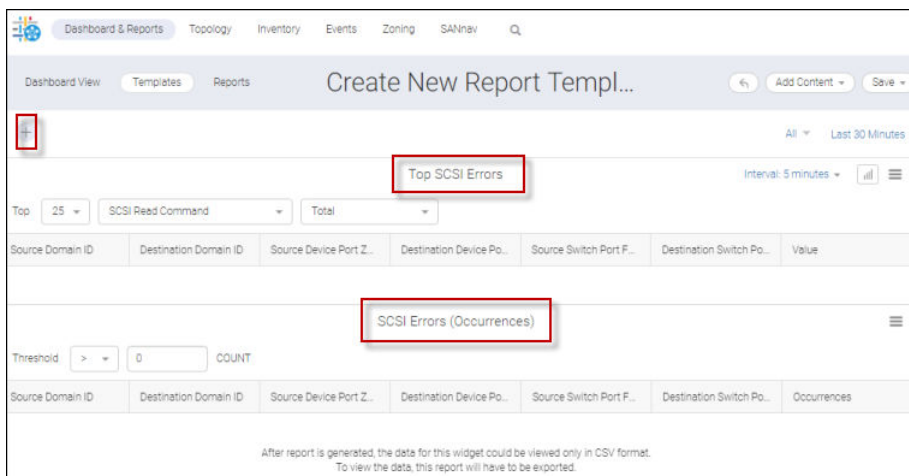


The description in the **Select Widgets** dialog indicates that this is a two-widget set, so you should expect two portions on your template: widget and occurrences.

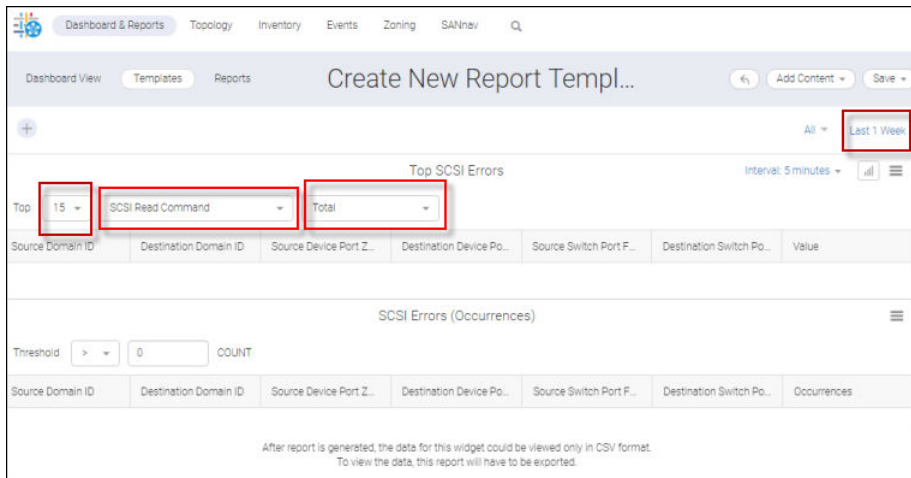
3. Select the widget category and a widget within that category, and then click the move icon (>) to position the widget under **Selected Widgets**. In this example, **Performance** and **Top SCSI Errors** are selected.
4. Click **OK**.

This displays the **Create New Report Template** dialog.

For Top N reports, you will see two parts: Top N and Occurrences.



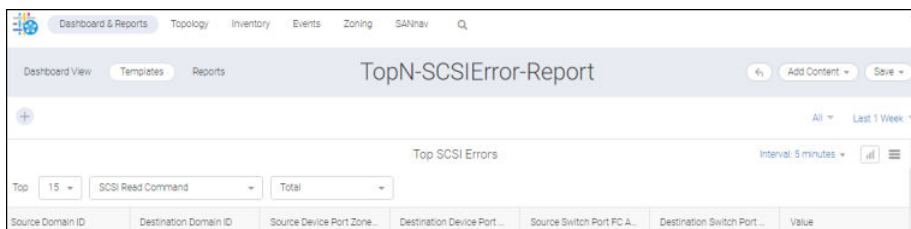
5. Supply a date range and select an "n" from the Top list. For this example, **Last 1 Week** and **15** are selected. You can also select a Top N value, a SCSI measure, and time interval. In this example, **15**, **SCSI Read Command**, and **5 minutes** are selected.



6. Click **Save**.

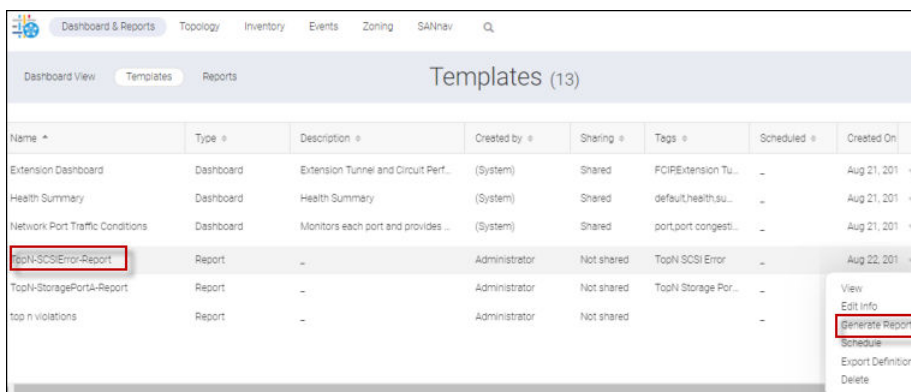
7. Enter a name, specify the tags, and then click **Save**. For this example, **TopN-SCSIError-Report** and **TopN SCSI Error** are selected for tags.

The new template displays with the name at the top.



8. Click **Templates**.

This displays a list of existing templates. Notice the template that you just created.



9. Click **Generate Report** from the action list for that template.

NOTE

The **Generate Report** option is also available inside the template view.

10. Click **Reports**.

Your report appears in the list appended with a timestamp.

Name	Description	Tags	Generated By	Generated On
topN-SCSIError-Report_2019-08-22-11-06-12_P...	-	TopN SCSI Error	Administrator	Aug 22, 2019 11:06:12 PDT
maps_report_2019-08-22-10-59-48_IDT	-		Administrator	Aug 22, 2019 00:59:48 PDT
storage_report_2019-08-22-00-44-44_PDT	-		Administrator	Aug 22, 2019 00:44:44 PDT
top n violations_2019-08-22-10-15-54_IDT	-		Administrator	Aug 22, 2019 00:15:54 PDT

11. Click the report.

You see the top portion of the report populated with the top 15 SCSI errors.

TopN-SCSIError-Report

Network Scope: All
Date Range: Aug 15, 2019, 11:06 PDT - Aug 22, 2019, 11:06 PDT

Top SCSI Errors

Top: 15 | SCSI Read Command(COUNT) | Total | Interval: 5 minutes
15 items

Source Domain ID	Destination Domain ID	Source Device Port Zone Alias	Destination Device Port Zone Alias	Source Switch Port FC Address	Destination Switch Port FC Address	Value
10	10	esx87_oe5900	storage7_02	0e0200	0e0500	5992072
10	10	esx87_oe5900	storage7_02	0a0200	0e0500	5992065
20	20	esx87_oe7800	storage7_01	140100	140600	5989152
20	20	esx87_oe7800	storage7_01	140100	140600	5989111

SCSI Errors (Occurrences)

Source Domain ID	Destination Domain ID	Source Device Port Zone Alias	Destination Device Port Zone Alias	Source Switch Port FC Address	Destination Switch Port FC Address	Occurrences
------------------	-----------------------	-------------------------------	------------------------------------	-------------------------------	------------------------------------	-------------

Data for this widget has been generated and can be viewed only in CSV format.
To view the data, export this report.

The bottom portion of the report, the number of occurrences, must be exported and viewed in CSV format.

12. On the **Reports** window, click **Export** from the action list for that report.

NOTE

The **Export** option is also available in template view.



The report is downloaded as a ZIP file to your local machine.

13. Open the ZIP file and double-click the **CSV** folder.

This displays folders for previously generated reports.

<input type="checkbox"/>	Time Series - Flow Collection (aggregated)
<input type="checkbox"/>	Time Series - Flow Violations
<input type="checkbox"/>	Top Collection Aggregation
<input checked="" type="checkbox"/>	Top SCSI Errors

14. Double-click the **Top_SCSI_Errors** subfolder, and then double-click each report to display its contents.

	threshold-report-scsi_rd_cmd_total-ID156649717... Type: Microsoft Excel Comma Separated Values File	Date modified: 8/22/2019 Size: 1.96 KB
	topn-report-scsi_rd_cmd_total-ID1566497173127... Type: Microsoft Excel Comma Separated Values File	Date modified: 8/22/2019 Size: 1.19 KB

6.8.12.5 Generating a Top N Report for Host Ports

You can create Top N reports for host ports based on Pending IOs or Read Oversubscription. The procedure is identical for both.

This section outlines how to perform the former.

1. Click **Dashboard & Reports** and then **Templates** on the navigation bar.

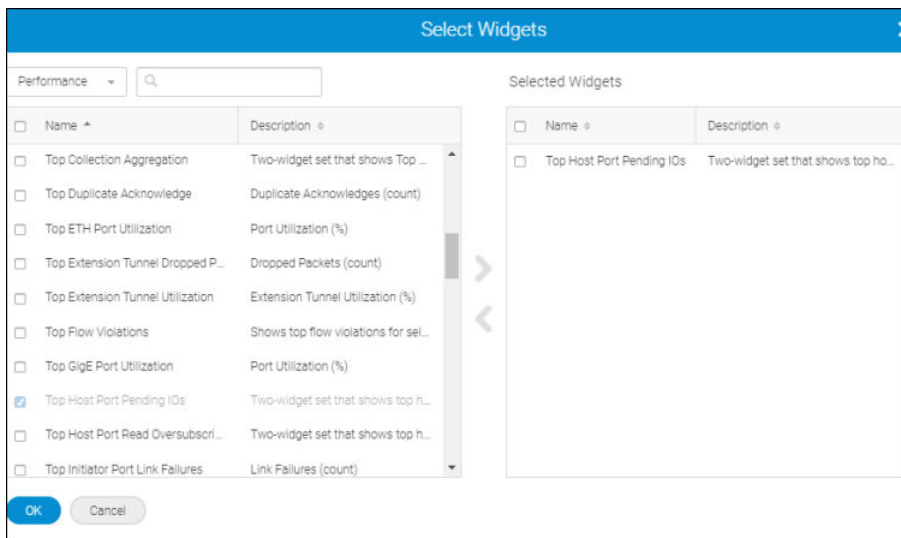
This displays the **Templates** window.

2. From **Templates** window, click **+ > Report > Select Widgets**.

This displays the **Select Widgets** dialog.

3. Select the widget category and a widget within that category, and then click the move icon (**>**) to position the widget under **Selected Widgets**.

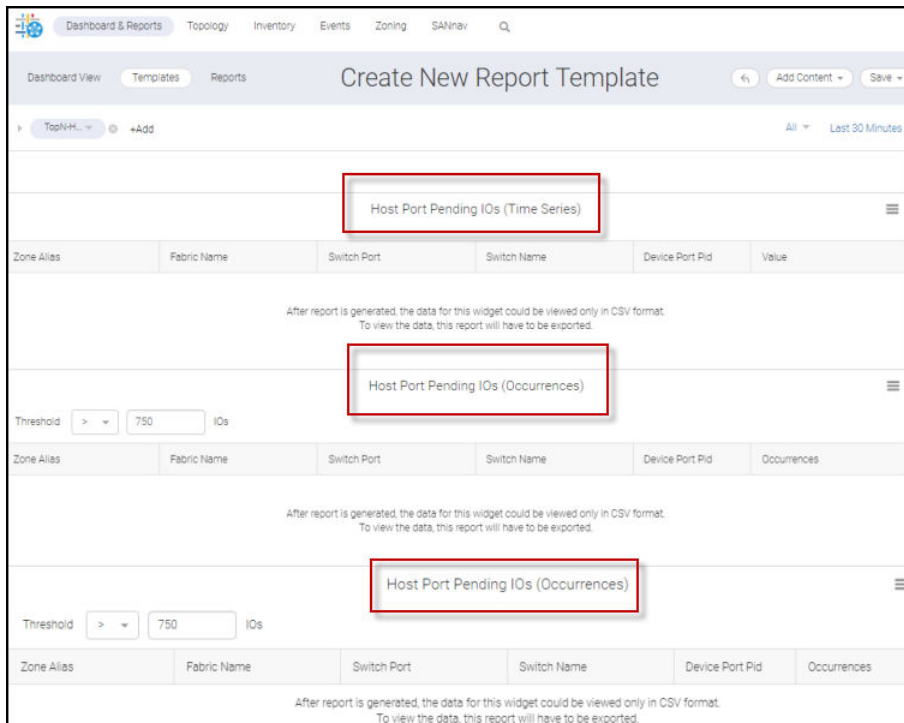
In this example, **Performance** and **Top Host Port Pending IOs** are selected.



4. Click **OK**.

This displays the **Create New Report Template** dialog.

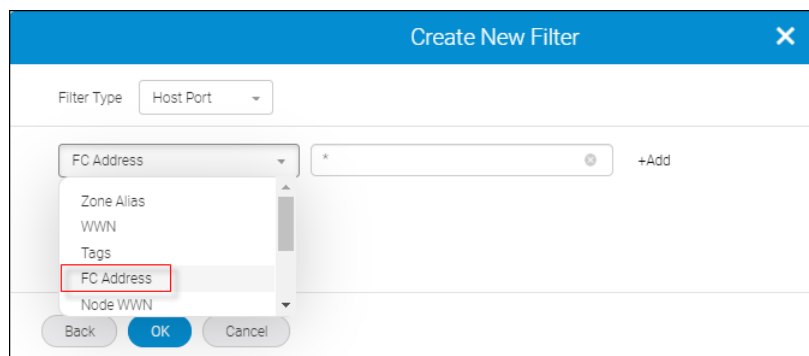
Notice the three components of a Top N host port report: Top N results, Time Series, and Occurrences.



You can provide a flow filter to generate a report for this widget and that report is generated provided the flow number is less than 10K.

5. (Optional) Create a flow filter for the report.
 - a. Click **+** on the upper left of the window to add a filter.
 - b. Click **Create New** in the **Add Filter** dialog.
 - c. In the **Create New Filter** dialog, set the following:
 - Filter Type = Host Port
 - Identifier = FC Address, Value = *

This extracts all host ports.

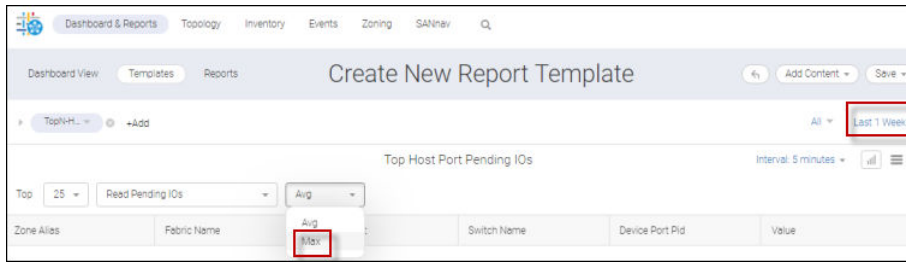


- d. Check the **Save Filter** option and supply a **Name** and optionally **Tags**, and then click **OK**.

The **Create New Report Template** window displays.

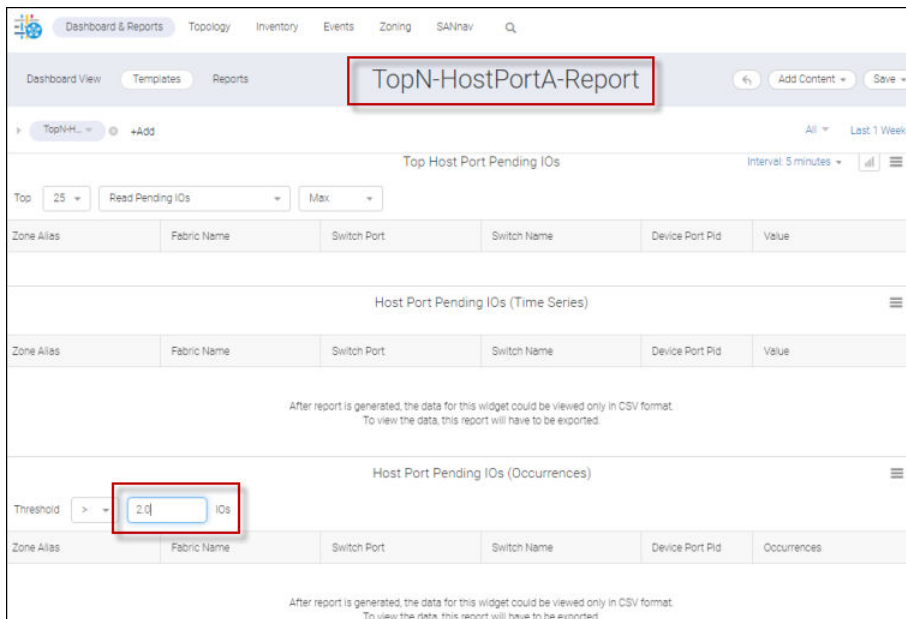
The filter name you supplied appears on the upper left in the filter list.

6. Specify a date range and choose between **Max** or **Avg**. For this example, **Last 1 Week** and **Max** are selected. Although you could change the interval setting, Top N value, and measure option, for this example, the values of **5 minutes**, **25**, and **Read Pending IOs** are selected.



7. Click **Save**.
8. Specify the name and the tag values, and then click **Save**. For this example, **TopN-HostPortA-Report** and **TopN Host PortA** are specified.

The new template displays with the name at the top and the widget identifier immediately below.



9. Reset the threshold and click **Save**. For this example, the threshold is set to **> 2.0 IOs**.
10. Click the **Templates** tab.

There you will see the template that you just created.

Name	Type	Description	Created by	Sharing	Tags	Scheduled	Created On
Extension Dashboard	Dashboard	Extension Tunnel and Circuit Perform...	(System)	Shared	FCIPExtension Tun...	-	Aug 21, 2019 07:10:35 F
Health Summary	Dashboard	Health Summary	(System)	Shared	default.health.sum...	-	Aug 21, 2019 07:10:35 F
Network Port Traffic Conditio...	Dashboard	Monitors each port and provides mea...	(System)	Shared	port.port congestio...	-	Aug 21, 2019 07:10:35 F
TopN-HostPortA-Report	Report	-	Administrator	Not shared	TopN Host PortA	-	Aug 22, 2019 12:34:56 F
TopN-SCSIError-Report	Report	-	Administrator	Not shared	TopN SCSI Error	-	Aug 22
TopN-StoragePortA-Report	Report	-	Administrator	Not shared	TopN Storage PortA	-	Aug 22
top n violations	Report	-	Administrator	Not shared	-	-	Aug 22

11. Click **Generate Report** from the action list for that template, and then click the **Reports** tab.

NOTE

The **Generate Report** option is also available inside the template view.

Notice that your report now appears in the list appended with a timestamp.

Name	Description	Tags	Generated By	Generated On
TopN-HostPortA-Report_2019-08-22-13:00:49_PDT	-	TopN Host PortA	Administrator	Aug 22, 2019 13:00:49 PDT
test1_2019-08-22-12:45:00_IDT	-	-	Administrator	Aug 22, 2019 12:45:00 PDT
SlivaTest_2019-08-22-12:44:31_PDT	-	-	Administrator	Aug 22, 2019 12:44:31 PDT
test lops1_2019-08-22-12:42:09_IDT	-	-	Administrator	Aug 22, 2019 12:42:09 PDT

12. Click the report.

The top portion of the report is populated with the top 10 Host Port Pending IOs.

Dashboard & Reports | Topology | Inventory | Events | Zoning | SANnav | Q

Dashboard View | Templates | Reports

TopN-HostPortA-Report

Filters: TopN-HostPortA-Filter
 Network Scope: All
 Date Range: Aug 15, 2019, 13:00 PDT - Aug 22, 2019, 13:00 PDT

Top Host Port Pending IOs

Top: 25 | Read Pending IOs(I/Os) Max | Interval: 5 minutes
 15 items

Zone Alias	Fabric Name	Switch Port	Switch Name	Device Port Pid	Value
ESX130_6f0901	Gen6_128	slot12 port19	sw212_X6	01f340	110
Host_Lucs_3_2	Gen6_128	slot3 port5	sw212_X6	010541	67
Host_Lucs_4_1	Gen6_128	slot3 port4	sw212_X6	010442	67

Host Port Pending IOs (Time Series)

Zone Alias	Fabric Name	Switch Port	Switch Name	Device Port Pid	Value
Data for this widget has been generated and can be viewed only in CSV format. To view the data, export this report.					

Host Port Pending IOs (Occurrences)

Zone Alias	Fabric Name	Switch Port	Switch Name	Device Port Pid	Occurrences
Data for this widget has been generated and can be viewed only in CSV format. To view the data, export this report.					

The bottom portion of the report, Time Series and Occurrences, must be exported and viewed in CSV format.

- Click the "return" icon to display the **Reports** window, and then click **Export** on the action list for that report.

NOTE

The **Export** option is also available in template view.

The report is downloaded as a ZIP file to your local machine and appears on the **Reports** window.

- Open the ZIP file and double-click the **CSV** folder.

This displays folders for previously generated reports.

<input type="checkbox"/>	Time Series - Flow Collection (aggregated)
<input type="checkbox"/>	Time Series - Flow Violations
<input type="checkbox"/>	Top Collection Aggregation
<input checked="" type="checkbox"/>	Top Host Port Pending IOs
<input type="checkbox"/>	Top SCSI Errors

- Double-click the **Top_Host_Port_Pending_IOs** subfolder, and then double-click each report to display its contents.

	threshold-report-rd_pend_ios_max-ID156650404...	Date modified: 8/22/2019 Size: 1.12 KB
	time-series-report-rd_pend_ios_max-ID156650404...	Date modified: 8/22/2019 Size: 467 KB
	topn-report-rd_pend_ios_max-ID156650404945844	Date modified: 8/22/2019 Size: 1.08 KB

6.8.12.6 Generating a Top N Report for Storage Ports

You can create Top N reports for storage ports based on Data Rate, IOPS, ECT, FRT, and Pending IOs. The procedure is identical for all five statistical categories.

The following procedure outlines how to create a Top N report based on Pending IOs.

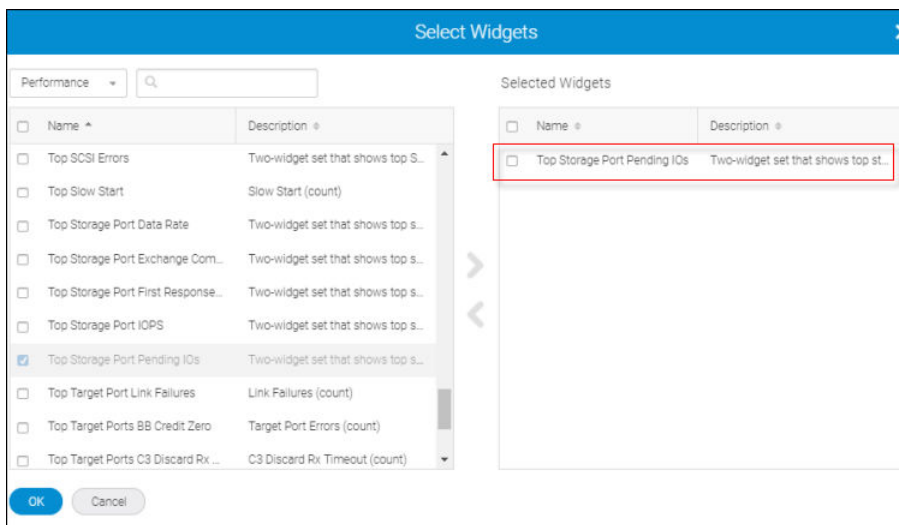
1. Click **Dashboard & Reports** and then **Templates** on the navigation bar.

This displays the **Templates** window.

2. From **Templates** window, click **+ > Report > Select Widgets**.

This displays the **Select Widgets** dialog.

3. Select the widget category and a widget within that category, and then click the move icon (>) to position the widget under **Selected Widgets**. In this example, **Performance** and **Top Storage Port Pending IOs** are selected.



4. Click **OK**.

This displays the **Create New Report Template** dialog.

Notice the three components of a template for a Top N storage port report: Top N results, Time Series, and Occurrences.

You can provide a filter to narrow the search.

5. (Optional) Create a flow filter for the report.
 - a. Click **+** on the upper left of the window to add a filter.
 - b. Click **Create New** in the **Add Filter** dialog.
 - c. In the **Create New Filter** dialog, set the following:
 - Filter Type = Storage Port
 - Identifier = FC Address, Value = *

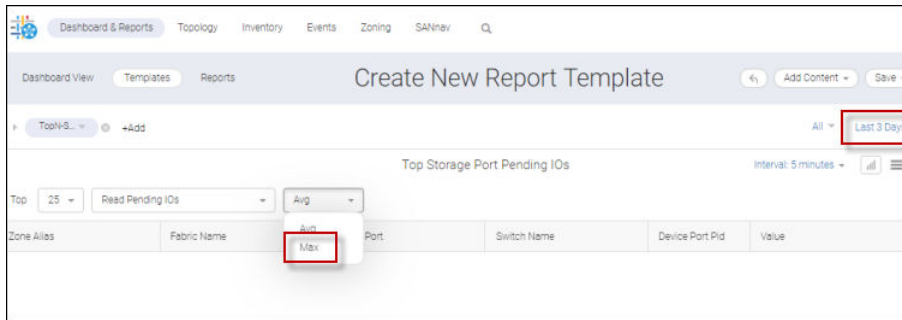
This extracts all storage ports.

- d. Check the **Save Filter** option and supply a **Name** and optionally **Tags**, and then click **OK**

The **Create New Report Template** window displays.

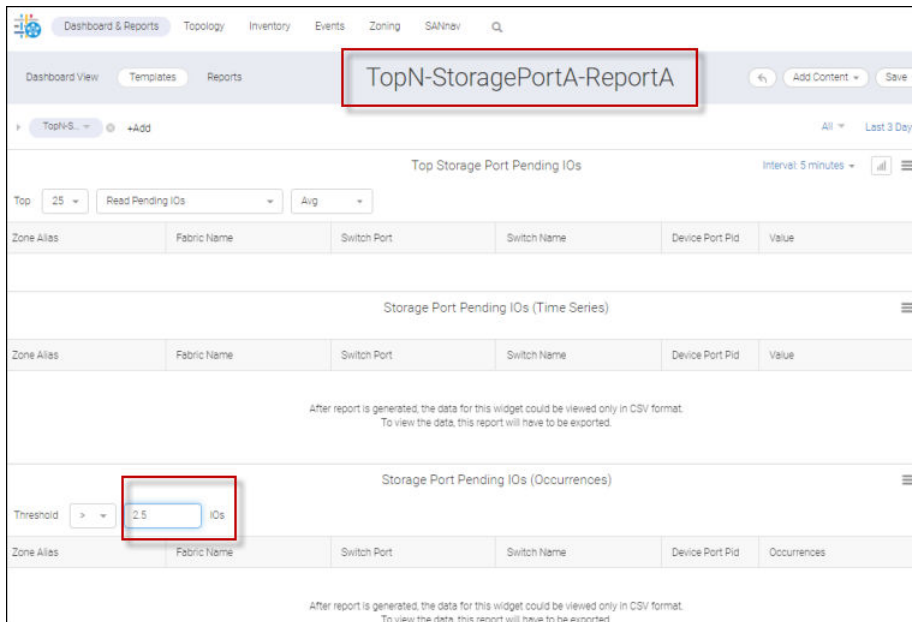
The filter name you supplied appears on the upper left in the filter list.

6. Specify the date range and choose between **Max** and **Average**. For this example, **Last 3 Days** and **Max** are selected. You could also change the interval setting, Top N value, and measure option. For this example, the values of **5 minutes**, **25**, and **Read Pending IOs** are selected.



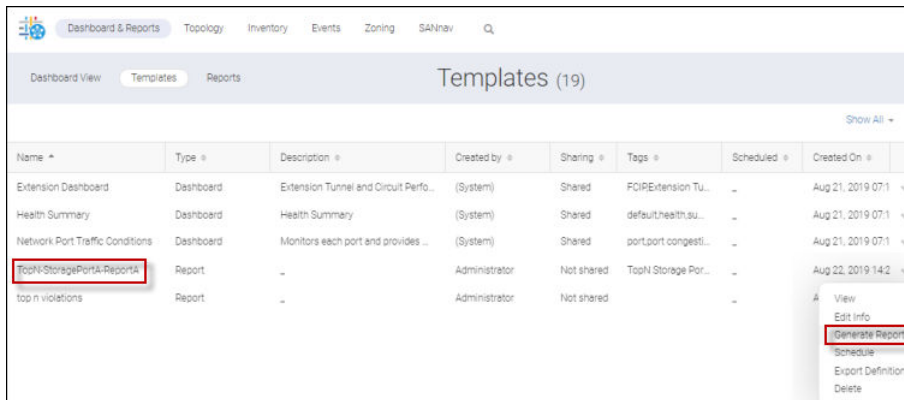
7. Click **Save**.
8. Assign a name and specify tags, and then click **OK**. For this example, **TopN-StoragePortA-ReportA** and **TopN Storage PortA** are specified.

The new template displays with the name at the top and the widget identifier immediately below.



9. Assign a **Threshold** value and click **Save**. For this example set the **Threshold** to **> 2.5 IOs**.
10. Click the **Templates** tab.

There you will see the template that you just created.



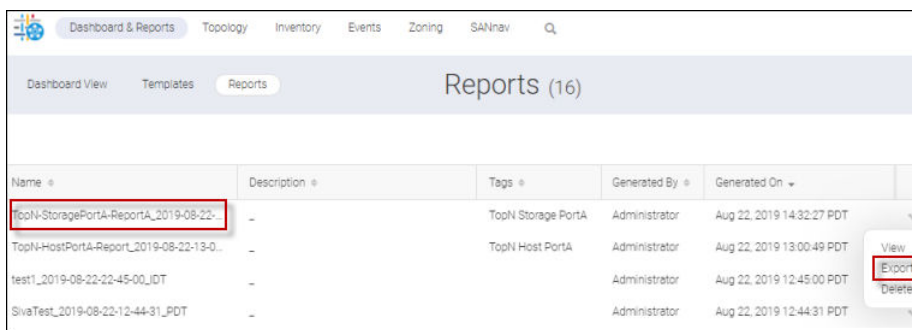
11. Click **Generate Report** from the action list for that template.

NOTE

The **Generate Report** option is also available inside the template view.

12. Click the **Reports** tab.

Notice that your report name now appears in the list appended with a timestamp.



13. Click the report.

The top portion of the report is populated with the top 10 Storage Port Pending IOs.

The bottom portion of the report, Time Series and Occurrences, must be exported and viewed in CSV format.

Dashboard & Reports | Topology | Inventory | Events | Zoning | SANnav

Dashboard View | Templates | Reports

TopN-StoragePortA-ReportA

Filters: TopN-StoragePort-Filter
 Network Scope: All
 Date Range: Aug 19, 2019, 14:32 PDT - Aug 22, 2019, 14:32 PDT

Top Storage Port Pending IOs

Top: 25 | Read Pending IOs(I/Os) Avg | Interval: 5 minutes
 8 Items

Zone Alias	Fabric Name	Switch Port	Switch Name	Device Port Pid	Value
Storage_246_10	Gen6_128	slot12.port11	sw212_X6	017b40	97.538
Storage246_09	Gen6_128	slot3.port13	sw212_X6	010d40	49.621
Storage101_03	Gen6_128	slot3.port9	sw212_X6	010940	0.013

Storage Port Pending IOs (Time Series)

Zone Alias	Fabric Name	Switch Port	Switch Name	Device Port Pid	Value
Data for this widget has been generated and can be viewed only in CSV format. To view the data, export this report.					

Storage Port Pending IOs (Occurrences)

Zone Alias	Fabric Name	Switch Port	Switch Name	Device Port Pid	Occurrences
Data for this widget has been generated and can be viewed only in CSV format. To view the data, export this report.					

14. Click ... > **Export**.

NOTE

The **Export** option is also available in template view.

The report is downloaded as a ZIP file to your local machine and appears on the **Reports** window.

15. Open the ZIP file and double-click the **CSV** folder.

This displays folders for previously generated reports.

- Time Series - Flow Collection (aggregated)
- Time Series - Flow Violations
- Top Collection Aggregation
- Top Host Port Pending IOs
- Top SCSI Errors
- Top Storage Port Pending IOs

16. Double-click the **Top_Storage_Port_Pending_IOs** subfolder, and then double-click each report to display its contents.

- threshold-report-rd_pend_ios_avg-ID1566509547... Date modified: 8/22/2019
Type: Microsoft Excel Comma Separated Values File
Size: 711 bytes
- time-series-report-rd_pend_ios_avg-ID156650954... Date modified: 8/22/2019
Type: Microsoft Excel Comma Separated Values File
Size: 262 KB
- topn-report-rd_pend_ios_avg-ID156650954795249 Date modified: 8/22/2019
Type: Microsoft Excel Comma Separated Values File
Size: 752 bytes

Configuration

7.1 Policy-Based Configuration

It is important to 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, display the configuration drifts, and allow you to synchronize the switches to the policy.

- 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 areas that you are interested in monitoring for drifts. SANnav monitors for configuration drift every 15 minutes; configuration drift can be monitored through the **Config Drifts** widget and through application events.

Configurations are defined using the JavaScript Object Notation (JSON) schema format.

7.1.1 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 and fabrics.

To create a configuration policy, you must have the Configuration Policy Manager privilege with read-write permission.

If you are going to import a configuration policy from a switch running Fabric OS 8.2.1 or higher, you must first increase the sampling request count for REST operations. The default is to allow 30 requests in 30 seconds. If VF is enabled, change the setting to allow $60 * (\text{number of logical switches})$ requests in 30 seconds by using the command line interface. Setting the request count to this value, allows SANnav to gather data quickly and avoid retry requests. For example, if you have three logical switches, the configuration must be modified to $60 * 3 = 180$ requests in 30 seconds.

```
switch:admin> mgmtapp --config -samplerequest 60  
Configuration succeeded.
```

Before you create a configuration policy, you should determine how it will be used.

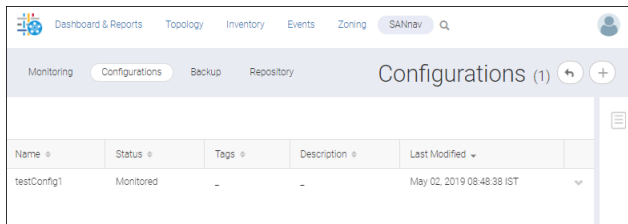
- If you are going to use the configuration policy to monitor for drifts, you might want to create a policy with just a subset of the full configuration, to monitor only the configuration blocks that you are interested in.
- If you are going to create a configuration policy for one switch and then apply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

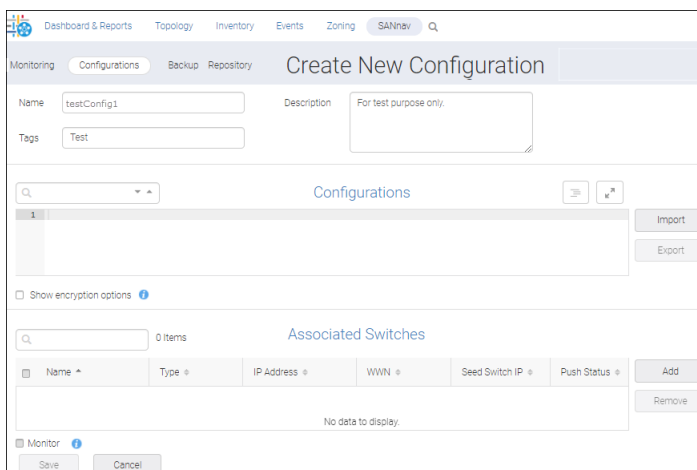
1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Configuration and Operations Monitoring Policy**.

The **Monitoring** window displays.

- Click **Configurations**, and then click the **+** button to add a policy.



- Type a name for the policy.
The name can contain up to 32 alphanumeric characters.



- Create the policy by either importing it or entering it manually.
 - Click **Import** to import the configuration policy from a file or a switch.
 - Select **Import file** to import the policy from a JSON file.
 - Select **Import from switch** to import the policy from a switch.
 - Paste text or start typing in the first line of the **Configurations** panel if you want to enter the policy manually.

NOTE

If you are entering the policy manually, it might be easier to first import an existing policy from a switch or file, and then modify the policy rather than typing the entire policy. You can also copy and paste from a template file. SANnav Management Portal provides a template file that you can use for creating policies from scratch: `BasicConfigurationsTemplate.txt`. This template file is located in the following location: `<install_home>/conf/cfgmgmt/BasicConfigurationsTemplate.txt`.

- You can enter the password into the policy by encrypting the password.
 - Select **Show encryption options**, type the password in the **Enter Text** field, and click **Encrypt**.
The encrypted text displays in the **Encrypted Text** field.
 - Copy the encrypted text and paste it into the policy.

Dashboard & Reports Topology Inventory Events Zoning SANnav

Monitoring Configurations Backup Repository testConfig1

Name testConfig1 Description

Tags

Configurations

```

5      "minOffset": 0
6    },
7    "Chassis": {
8      "vfEnabled": true
9    },
10   "FTP": {
11     "password": "O4hwF196Lm7YQwRgACEj+g==",
12     "protocol": "FTP",
13     "remoteDirectory": "",
14     "serverConnectivityCheckIntervalInHours": 1,
15     "host": "None",
16     "username": ""
17   },
18   "AAAConfig": {

```

Import Export

Show encryption options

Enter Text Encrypt

Encrypted Text O4hwF196Lm7YQwRgACEj+g==

Associated Switches 0 Items

Name	Type	IP Address	WWN	Seed Switch IP	Push Status
0 Items					

Monitor

Save Delete Cancel

6. Edit the policy to make any changes or to fix any errors.

If you encounter errors, hover over the line number with the error to see a description of the error.

1 error found

```

4      "hourOffset": 0,
5      "minOffset": 0
6    },
7    "FTP": {
8      "password": "iCS1AD3shxJ52nxo116NXA==",
9      "protocol": "FTP",
10     "remoteDirectory": "",
11     "serverConnectivityCheckIntervalInHours": 1,
12     "host": "None",
13     "username": ""
14   },
15   "AAAConfig": {
16     "authSpec": {
17       "authMode": "local",

```

requires property "host"

You cannot save the policy until all errors are fixed.

In this case, the error was fixed.

```

4      "hourOffset": 0,
5      "minOffset": 0
6    },
7    "FTP": {
8      "password": "ics1A03shx352nxo116NXA==",
9      "protocol": "FTP",
10     "remoteDirectory": "",
11     "serverConnectivityCheckIntervalInHours": 1,
12     "host": "None",
13     "username": ""
14   },
15   "AAAConfig": {
16     "authSpec": {
17       "authMode": "local",

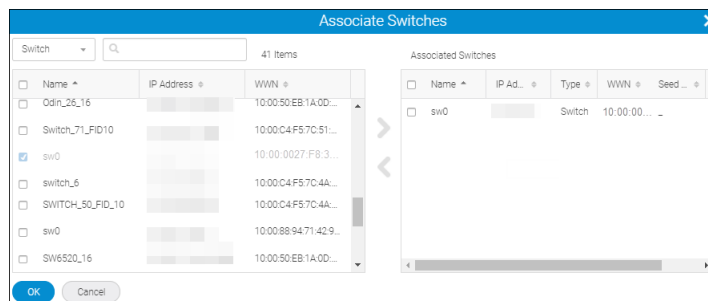
```

7. Apply the policy to switches and fabrics.

- a. Click **Associate Switches**.
- b. Select the switches and fabrics to which the policy is to be applied, and click the arrow to move the selected items to the right panel.

You can select fabrics, switches, or both fabrics and switches.

If you apply the policy to a fabric, the policy is applied to all the switches in the fabric. In addition, the policy is automatically applied to any switches that are added to the fabric later.



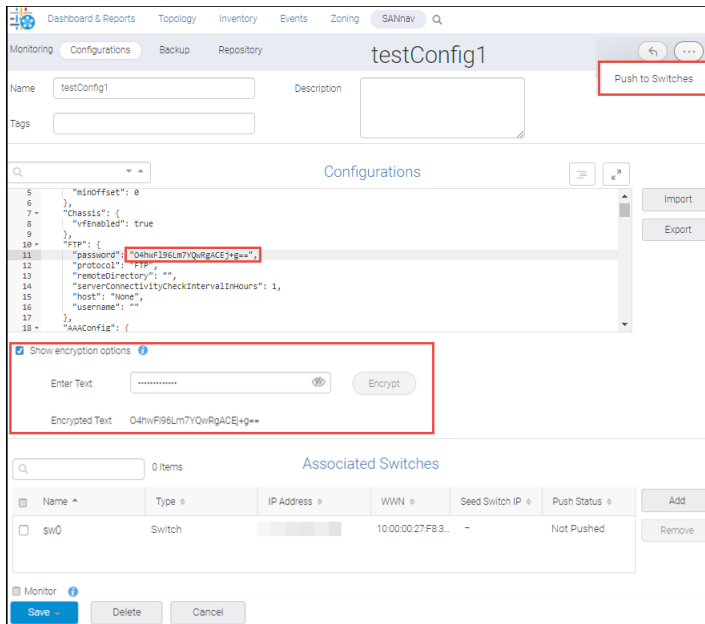
- c. Click **OK**.

8. In the **Configuration** page, click the down arrow next to the configuration policy and select **Monitor** to start monitoring the switches for configuration drifts.

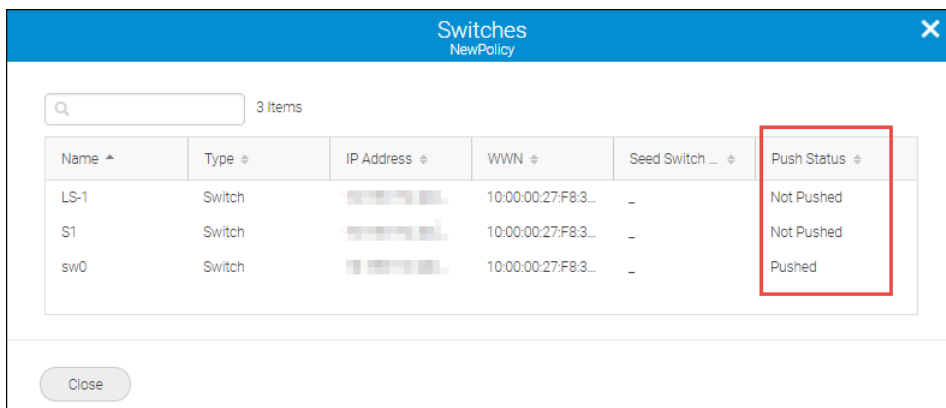
The **Monitor** checkbox is disabled if no switches are associated with the configuration.

9. Click **Save** to save your changes and return to the **Configurations** page.

Click **Push to Switches** to save your changes and to apply the configuration to the associated switches and fabrics.



10. On the **Configurations** page, click the down arrow next to the configuration and select **View Switches** to see the list of switches associated with the configuration and whether the configuration has been pushed to the switches.



7.1.2 Configuring a New Switch Before Adding It to the Fabric

Before adding a new switch to a fabric, you can provision the switch according to existing configuration policies.

This task assumes that Basic Configuration policies are already created and imported into SANnav Management Portal.

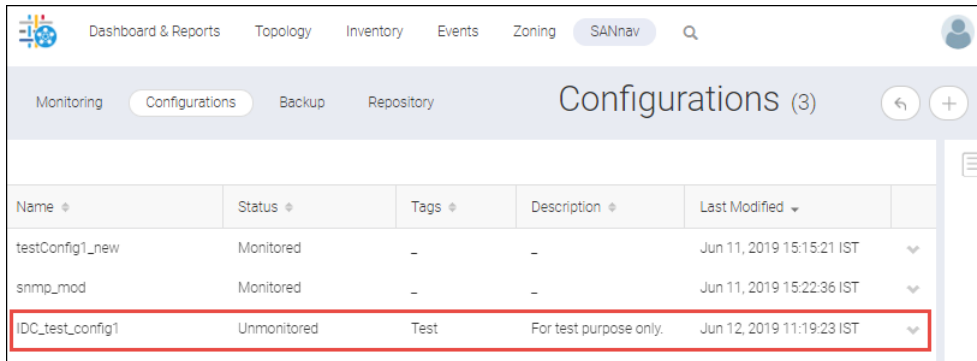
You must have the Configuration Policy Manager privilege with read-write permission.

If you assign a policy to a fabric instead of a switch, any new switches added to the fabric are automatically configured with that policy. Use the following procedure if the fabric has not been assigned a policy.

1. Discover the switch.

To discover the new switch, click **SANnav** in the navigation bar, and then select **SAN Monitoring > Fabric Discovery**. For complete details, see [Discovering a Fabric](#).

2. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Configuration and Operations Monitoring Policy**.
3. Click the **Configurations** tab, and then select the policy that you want to apply to the new switch.



The screenshot shows the SANnav interface with the 'Configurations' tab selected. The table below lists the configurations:

Name	Status	Tags	Description	Last Modified
testConfig1_new	Monitored	-	-	Jun 11, 2019 15:15:21 IST
snmp_mod	Monitored	-	-	Jun 11, 2019 15:22:36 IST
IDC_test_config1	Unmonitored	Test	For test purpose only.	Jun 12, 2019 11:19:23 IST

4. Apply the configurations to the switch.
 - a. In the **Associated Switches** table, click **Add** to select the new switch and click the right arrow to move it to the right side of the window, and click **OK**.
 - b. Click **Push to Switches**.

NOTE

The **Push to Switches** option is visible only when the switch is added to the configured policy.

The screenshot displays the SANnav Management Portal interface for configuring a switch. The main configuration area shows a JSON configuration for 'IDC_test_config1'. The configuration includes basic settings like 'Chassis', 'NTP_TimeZone', and 'FTP'. Below the JSON editor, there are 'Import' and 'Export' buttons. The 'Associated Switches' section shows a table with one switch, 'Switch74', which has a 'Push Status' of 'Not Pushed'. A red box highlights the 'Push to Switches' button in the top right corner of the configuration area.

5. Make other configurations, if applicable.
6. Connect the switch to the fabric.
The switch now has the correct configurations.

7.1.3 Configuring a New Switch After Adding It to the Fabric

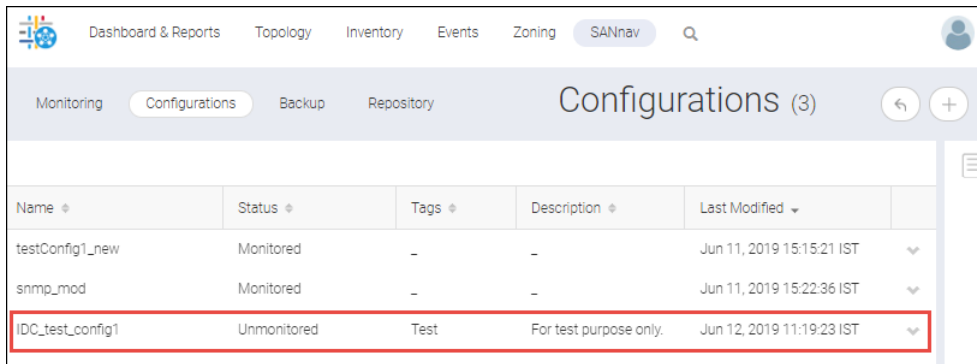
After adding a new switch to a fabric, you can provision the switch according to configuration policies.

This task assumes that Basic Configuration policies are already created and imported into SANnav.

You must have the Configuration Policy Manager privilege with read-write permission.

After you add a switch to a fabric, the switch is automatically discovered. If you assigned a policy to the fabric, the new switch is automatically configured with this policy. Use the following procedure if the fabric has not been assigned a policy.

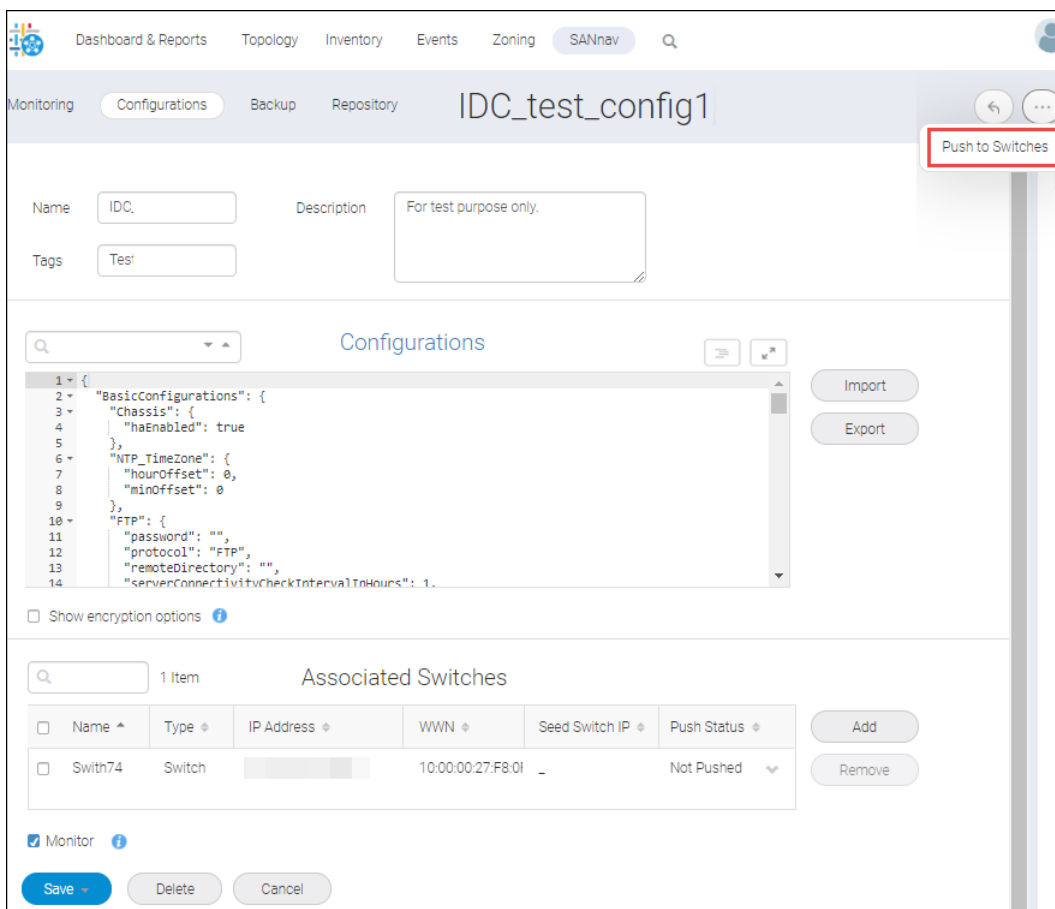
1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Configuration and Operations Monitoring Policy**.
2. Click the **Configurations** tab, and then click the policy that you want to apply to the new switch.



Name	Status	Tags	Description	Last Modified
testConfig1_new	Monitored	-	-	Jun 11, 2019 15:15:21 IST
snmp_mod	Monitored	-	-	Jun 11, 2019 15:22:36 IST
IDC_test_config1	Unmonitored	Test	For test purpose only.	Jun 12, 2019 11:19:23 IST

3. Apply the configurations to the switch.

- a. In the **Associated Switches**, click **Add** to select the new switch and click the right arrow to move it to the right side of the window, and click **OK**.
- b. Click **Push to Switches**.



Push to Switches

Name: IDC. Description: For test purpose only. Tags: Test

```

1 {
2   "BasicConfigurations": {
3     "Chassis": {
4       "haEnabled": true
5     },
6     "NTP_TimeZone": {
7       "hourOffset": 0,
8       "minOffset": 0
9     },
10    "FTP": {
11      "password": "",
12      "protocol": "FTP",
13      "remoteDirectory": "",
14      "serverConnectivityCheckIntervalInHours": 1.

```

Associated Switches

Name	Type	IP Address	WWN	Seed Switch IP	Push Status
Switch74	Switch		10:00:00:27:F8:01		Not Pushed

Monitor Save Delete Cancel

The switch is now provisioned with the selected policy.

7.1.4 Monitoring Configuration Drifts

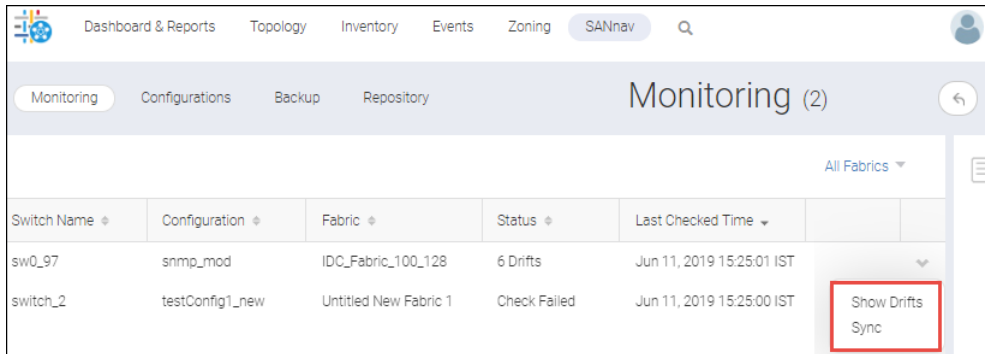
As part of your daily operations, you should check the switches for drifts between the switch configuration and the configuration policy.

This task assumes that configuration policies have been created and are currently being monitored.

To monitor the configuration for drifts, you must have the Configuration Policy Manager privilege with read permission.

A configuration drift generally means an uncontrolled change or an exception happened on the switch. SANnav monitors the switches for configuration drifts every 15 minutes.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Configuration and Operations Monitoring Policy**.
2. Click **Monitoring** to see a list of switches that are being monitored for configuration drifts.
The **Status** column indicates how many drifts have occurred. If the status is **In Sync**, no drifts have seen. If the status is **Check Failed**, SANnav is unable to contact the switch.
3. For switches with drifts, click the down arrow in the right-most column and select **Show Drifts**.



Switch Name	Configuration	Fabric	Status	Last Checked Time	
sw0_97	snmp_mod	IDC_Fabric_100_128	6 Drifts	Jun 11, 2019 15:25:01 IST	
switch_2	testConfig1_new	Untitled New Fabric 1	Check Failed	Jun 11, 2019 15:25:00 IST	Show Drifts Sync

4. Select the **Show Drifts Only** option to display the drifts side-by-side or inline. You can also select the **Side By Side** or **Inline** options to view the drifts with the entire configuration.

NOTE

The inline view does not display modified drifts. Drifts that appear as modified in the side-by-side view are shown as a combination of deleted and inserted drifts in the inline view.

Configuration Drifts
sw0_97

Show Drifts Only
 Side By Side
 Inline

Configuration on SANnav	Configuration on Switch
6 7 8 26 28 29 216 224 232	23 25 26 27 28 215 223 231 239 240 241 242 243 244 245
}, "Chassis":{ "haEnabled": true "Banner": "\n", "domainName": "", "ipAddresses": [] "usmIndex": 6 "usmIndex": 6 "usmIndex": 6	"Banner": "", "domainName": "test6.bsmlab.broadcom.net", "ipAddresses": ["2620:100:4:e200::180"] "usmIndex": 1 "usmIndex": 2 "usmIndex": 3 "usmIndex": 4 }, { "notifyType": "trap", "port": 162, "trapLevel": "4-Info", "host": "10.157.15.118"

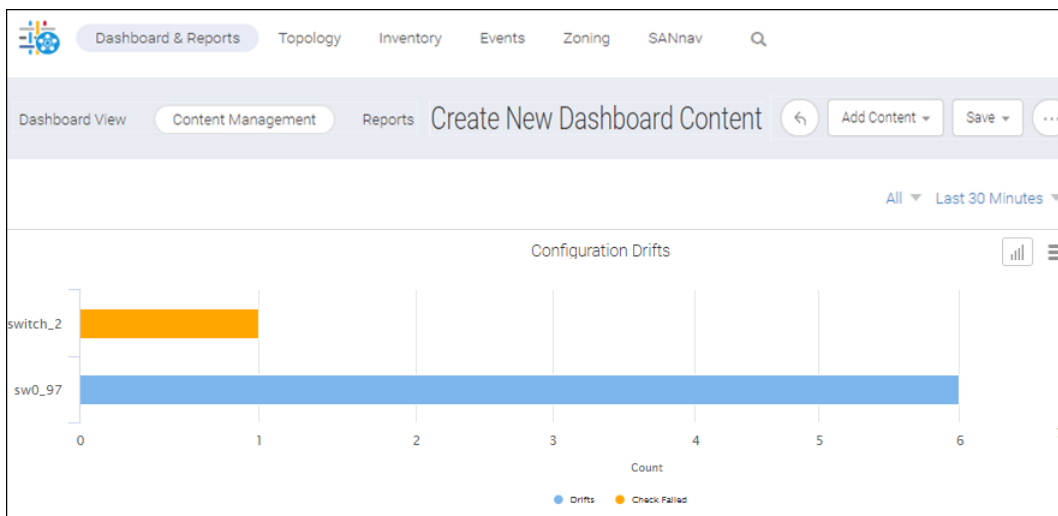
Deleted (red) Inserted (green) Modified (yellow) Empty (grey)

Sync Close

5. You can also check the dashboard to quickly see switches with configuration drifts.

The **Configuration Drifts** widget displays the switches with configuration drifts. You can quickly look at this widget, or you can create a saved dashboard with the widget.

Click the bars in the widget to view the drift counts for switches belonging to a specific fabric. Click the **All** drop-down to see the switches for a specific fabric.



7.1.5 Resolving Configuration Drifts

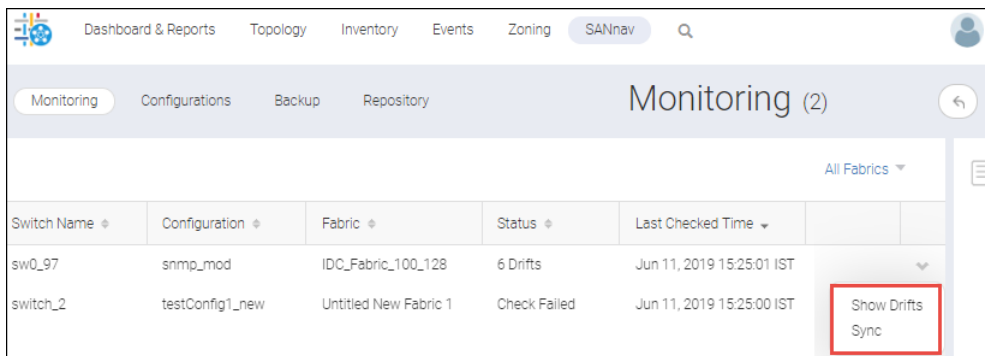
If configuration drifts occur between the switch configuration and the configuration policy, you can resolve the drifts immediately.

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

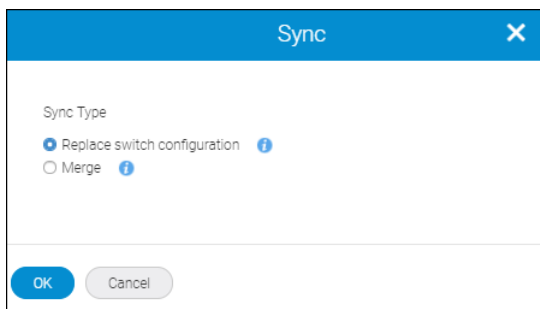
When you resolve a configuration drift, you can either replace the configuration on the switch with the defined configuration policy or you can update the configuration policy with the configuration found on the switch.

For example, if all switches in Fabric A are forwarding syslogs to Server X, but one switch in the fabric is forwarding syslogs to Server Y, you need to know this and act accordingly. You can change the switch configuration to forward syslogs to Server X, or you can change the configuration policy to forward syslogs to Server Y.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Configuration and Operations Monitoring Policy**.
2. Click **Monitoring** to see a list of switches that are being monitored for configuration drifts.
3. Click the down arrow in the rightmost column of a switch and select **Sync** to resolve drifts immediately.



4. Select the sync type.
 - If you want to replace the configuration on the switch with the configuration that is defined in the policy, select **Replace switch configuration**.
 - If you want to leave the switch settings unchanged, but add the switch settings to the configuration policy, select **Merge**.



5. Click **OK**.

7.1.6 Configuration Blocks

A configuration policy is defined in JSON schema format. This file is made up of one or more configuration blocks. A configuration block is a group of configuration settings.

SANnav Management Portal compares the configuration settings on a switch with the configuration settings in the configuration policy to determine if drifts have occurred.

When checking for drifts, you might want to monitor certain settings only, and not the entire configuration. In this case, you can create a configuration file with only the configuration blocks that you want to monitor.

The following table lists the configuration blocks that are supported and provides examples for each. You can find a complete template in the following location: <install_home>/conf/cfgmgmt/BasicConfigurationsTemplate.txt.

Configuration Block	Property	Supported Fabric OS Versions	Notes and Examples
AAAConfig:authSpec	authMode	8.2.1+	The <code>activateNoLogout</code> property cannot be imported from the switch and is not included in drift detection. Example: <pre>"AAAConfig": { "authSpec": { "authMode": "ldap;local", "backup": false, "activateNoLogout": false, "primaryLogMessages": true } },</pre>
	backup	8.2.1+	
	activateNoLogout	8.2.1+	
	primaryLogMessages	8.2.1+	
AAAConfig:LDAP	port	All	Example: <pre>"AAAConfig": { "LDAP": [{ "port": 389, "domain": "ldapsecurity.example.com", "ipAddress": "10.40.60.12", "timeout": 3 }] },</pre>
	domain	All	
	ipAddress	All	
	timeout	All	
AAAConfig:RADIUS	ipAddress	All	The <code>secret</code> property cannot be imported from the switch and is not included in drift detection. The secret must be encrypted in the JSON text when saved in the configuration policy. Example: <pre>"AAAConfig": { "RADIUS": [{ "ipAddress": "10.40.80.12", "port": 1812, "timeout": 3, "secret": "thZi3XgrAbH+h5gyJu+I7g==", "encryptionLevel": "NONE", "authentication": "CHAP" }] },</pre>
	port	All	
	timeout	All	
	secret	All	
	encryptionLevel	All	
	authentication	All	

Configuration Block	Property	Supported Fabric OS Versions	Notes and Examples
AAACfg:TACACS+	ipAddress	All	<p>The <code>secret</code> property cannot be imported from the switch and is not included in drift detection. The secret must be encrypted in the JSON text when saved in the configuration policy.</p> <p>Example:</p> <pre>"AAACfg": { "TACACS+": [{ "ipAddress": "10.40.70.12", "port": 49, "timeout": 3, "secret": "thZi3XgrAbH+h5gyJu+I7g==", "encryptionLevel": "NONE", "authentication": "CHAP" }] },</pre>
	port	All	
	timeout	All	
	secret	All	
	encryptionLevel	All	
	authentication	All	
ACL	ipAddress	All	<p>Example:</p> <pre>"ACL": [{ "ipAddress": "10.50.1.12", "control": "read-write" }, { "ipAddress": "10.50.1.13", "control": "read-write" }],</pre>
	control	All	
AuditCfg	severity	8.2.1+	<p>Example:</p> <pre>"AuditCfg": { "severity": "INFO", "enable": true, "class": ["zone", "security", "configuration", "firmware", "fabric", "ls", "cli", "maps"] },</pre>
	enable	8.2.1+	
	class	8.2.1+	
Banner	Banner	8.2.1+	<p>Example:</p> <pre>"Banner": "This is a test banner",</pre>

Configuration Block	Property	Supported Fabric OS Versions	Notes and Examples
Chassis	haEnabled	8.2.1+	<p>The Chassis configuration block is for director-class switches only.</p> <p>The <code>haEnabled</code> property is a read-only property. Changes made in the JSON text of the policy will not be reflected on the switch.</p> <p>Example:</p> <pre>"Chassis": { "haEnabled": true },</pre>
DNS	domainName	8.2.1+	<p>Example:</p> <pre>"DNS": { "domainName": "test6.bsmlab.broadcom.net.", "ipAddresses": ["2620:100:4:e200::180"] },</pre>
	ipAddresses	8.2.1+	
FTP	password	All	<p>The password must be encrypted in the JSON text when saved in the configuration policy. You cannot import the <code>password</code> property from the switch. The <code>password</code> property is not included in drift detection.</p> <p>Example:</p> <pre>"FTP": { "password": "jP6gyHn8DTty9oyf93Rujw==", "protocol": "FTP", "remoteDirectory": "/home/support/uploads", "serverConnectivityCheckIntervalInHours": 1, "host": "supportFtpServer", "username": "admin" },</pre>
	protocol	All	
	remoteDirectory	All	
	serverConnectivityCheckIntervalInHours	All	
	host	All	
	username	All	

Configuration Block	Property	Supported Fabric OS Versions	Notes and Examples
IPFilter	ipVersion	8.2.1+	Example: <pre>"IPFilter": [{ "ipVersion": "ipv4", "name": "default_ipv4", "active": true, "rules": [{ "destinationIp": "any", "destinationEndPort": "22", "protocol": "tcp", "sourceIp": "any", "destinationStartPort": "22", "index": 1, "action": "permit", "trafficType": "input" }] }],</pre>
	name	8.2.1+	
	active	8.2.1+	
	rules	8.2.1+	
LDAPRoleMap	ldapRole	8.2.1+	Example: <pre>"LDAPRoleMap": [{ "ldapRole": "FabricAdmin", "switchRole": "fabricAdmin=1-128", "homeVirtualFabric": 128, "chassisAccessRole": "admin" }, { "ldapRole": "", "switchRole": "", "homeVirtualFabric": 128, "chassisAccessRole": "" }],</pre>
	switchRole	8.2.1+	
	homeVirtualFabric	8.2.1+	
	chassisAccessRole	8.2.1+	
NTP_TimeServer	ipAddress	All	Example: <pre>"NTP_TimeServer": [{ "ipAddress": "10.40.10.10" }, { "ipAddress": "10.40.10.11" }],</pre>

Configuration Block	Property	Supported Fabric OS Versions	Notes and Examples
NTP_TimeZone	timeZoneName	All	Example: <pre>"NTP_TimeZone": { "timeZoneName": "America/Los_Angeles", "hourOffset": 0, "minOffset": 0 },</pre>
	hourOffset	All	
	minOffset	8.2.1+	
PasswordCfg	minimumLength	8.2.1+	The resetPasswordCfgToDefault and enforceExpire properties cannot be imported from the switch, and are not included in drift detection. Example: <pre>"PasswordCfg": { "minimumLength": 8, "characterSet": 0, "userNameAllowed": true, "reverseUserNameAllowed": false, "minLowercaseChar": 0, "minUppercaseChar": 0, "minNumericChar": 0, "minSpecialChar": 0, "pastPasswordHistory": 1, "minPasswordAge": 0, "maxPasswordAge": 0, "warnOnExpire": 0, "lockoutThreshold": 0, "lockoutDuration": 30, "enableAdminLockout": false, "repeatCharLimit": 1, "sequenceCharLimit": 1, "hashType": "sha512", "manualHashEnabled": false, "minimumDifference": 0, "enforceExpire": false, "resetPasswordCfgToDefault": false },</pre>
	characterSet	8.2.1+	
	userNameAllowed	8.2.1+	
	reverseUserNameAllowed	8.2.1+	
	minLowercaseChar	8.2.1+	
	minUppercaseChar	8.2.1+	
	minNumericChar	8.2.1+	
	minSpecialChar	8.2.1+	
	pastPasswordHistory	8.2.1+	
	minPasswordAge	8.2.1+	
	maxPasswordAge	8.2.1+	
	warnOnExpire	8.2.1+	
	lockoutThreshold	8.2.1+	
	lockoutDuration	8.2.1+	
	enableAdminLockout	8.2.1+	
	repeatCharLimit	8.2.1+	
	sequenceCharLimit	8.2.1+	
	hashType	8.2.1+	
manualHashEnabled	8.2.1+		
minimumDifference	8.2.1+		
enforceExpire	8.2.1+		
resetPasswordCfgToDefault	8.2.1+		
PortConfiguration	portnameMode	8.2.1+	Example: <pre>"PortConfiguration": { "portnameMode": "default", "dynamicDPortEnabled": true, "onDemandDPortEnabled": false, "dynamicPortnameFormat": "S.T.I.A" },</pre>
	dynamicDPortEnabled	8.2.1+	
	onDemandDPortEnabled	8.2.1+	
	dynamicPortnameFormat	8.2.1+	

Configuration Block	Property	Supported Fabric OS Versions	Notes and Examples
SNMPv3	encryptionEnabled	8.2.1b+	Example: <pre> "SNMPv3": { "encryptionEnabled": false, "recipients": [{ "notifyType": "trap", "port": 162, "trapLevel": "4-Info", "host": "10.155.37.157", "index": 1, "usmIndex": 2 }, { "notifyType": "trap", "port": 162, "trapLevel": "4-Info", "host": "10.155.41.116", "index": 2, "usmIndex": 2 }], "auditInterval": 60, "secSetLevel": "3-No access", "enableInforms": false, "secGetLevel": "0-No security", "usmAccounts": [{ "privProtocol": "No Priv", "index": 1, "userName": "snmpadmin1", "userGroup": "read-write", "authProtocol": "No Auth", "managerEngineId": "00:00:00:00:00:00:00:00:00" }, { "privProtocol": "No Priv", "index": 2, "userName": "snmpadmin2", "userGroup": "read-write", "authProtocol": "No Auth", "managerEngineId": "00:00:00:00:00:00:00:00:00" }] } </pre>
	recipients.notifyType	All	
	recipients.port	All	
	recipients.trapLevel	All	
	recipients.host	All	
	recipients.index	All	
	recipients.usmIndex	8.2.1b+	
	auditInterval	8.2.1b+	
	secSetLevel	8.2.1b+	
	enableInforms	All	
	secGetLevel	8.2.1b+	
	usmAccounts.privProtocol	8.2.1b+	
	usmAccounts.privPassword	8.2.1b+	
	usmAccounts.index	8.2.1b+	
	usmAccounts.userName	8.2.1b+	
	usmAccounts.userGroup	8.2.1b+	
	usmAccounts.authProtocol	8.2.1b+	
usmAccounts.authPassword	8.2.1b+		
usmAccounts.managerEngineId	8.2.1b+		

Configuration Block	Property	Supported Fabric OS Versions	Notes and Examples
SwitchConfiguration	edgeHoldTime	8.2.1+	Example: <pre>"SwitchConfiguration": { "edgeHoldTime": 220, "wnnPortIdMode": false },</pre>
	wnnPortIdMode	8.2.1+	
Syslog	ipAddresses.port	All	Example: <pre>"SYSLOG": { "ipAddresses": [{ "port": 514, "ipAddress": "10.50.1.12", "secureMode": false }, { "port": 514, "ipAddress": "10.50.1.17", "secureMode": false }], "facility": "LOG_LOCAL7" },</pre>
	ipAddresses.ipAddress	8.2.1+	
	ipAddresses.secureMode	8.2.1+	
	facility	8.2.1+	
Users	username	All	<p>The password must be encrypted in the JSON text when saved in the configuration policy.</p> <p>The password property is used from JSON only when adding a new user. It cannot be used to modify the password of an existing user account.</p> Example: <pre>"Users": [{ "username": "root", "password": "", "role": "SAN System Administrator", "accountDescription": "root", "accountEnabled": true, "passwordChangeEnforced": false, "accountLocked": false, "accessStartTime": "", "accessEndTime": "", "homeVirtualFabric": 128, "chassisAccessRole": "root", "virtualFabricRoleList": [{ "role": "root", "fabricIds": "1-128" }] }],</pre>
	password	8.2.1+	
	role	8.2.1+	
	accountDescription	8.2.1+	
	accountEnabled	8.2.1+	
	passwordChangeEnforced	8.2.1+	
	accountLocked	8.2.1+	
	accessStartTime	8.2.1+	
	accessEndTime	8.2.1+	
	homeVirtualFabric	8.2.1+	
	chassisAccessRole	8.2.1+	
	virtualFabricRoleList	8.2.1+	

7.2 Switch 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 additional 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 on reception of audit events in the master log. Note that SANnav must be registered as an SNMP trap recipient for event-triggered backup to occur.
- **Manual**
You can back up a switch configuration on-demand.
- **Scheduled**
You can set up a daily or weekly schedule when backups are to occur automatically.

Configuration backups are stored in a repository in the SANnav database. There is no limit to the number of backups that are stored.

Configuration backups can be kept in the repository for 30 days, 90 days, or indefinitely. By default, configuration backups are kept for 30 days. If you schedule a configuration backup, you have the option to change the default retention period to 90 days.

One configuration backup 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. You cannot delete the baseline configuration from the repository.

In addition to storing the configurations in the repository, you can also export a configuration to a file as an additional safety measure.

7.2.1 Backing Up Switch and Logical Fabric Configurations

You can back up switch and logical fabric configurations on-demand. You can also set up a schedule for backing up switch and logical fabric configurations on a regular basis. In addition to the basic daily, weekly, monthly, or on-demand backup, you can enable or disable backups created when specific events occur in the switches.

You must have the Configuration File Manager privilege with read permission to back up a configuration on-demand and with read-write permission to schedule a backup.

The three types of backup configurations are as follows:

- Switch
- Chassis
- Logical fabric

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

- When a new switch is discovered.
- When on-demand (Backup Now)
- When a backup is scheduled.
- When the following RASLOG events are received:

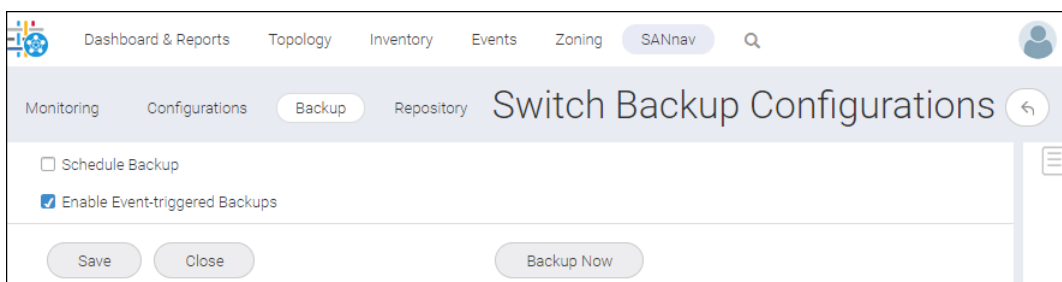
- Creating logical switch
- Deleting logical switch
- Moving ports between the logical switch
- Changing base switch
- Enabling FICON on logical switch

NOTE

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

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Configuration and Operations Monitoring Policy**.
2. Click **Backup**.

The **Switch Backup Configurations** window displays.



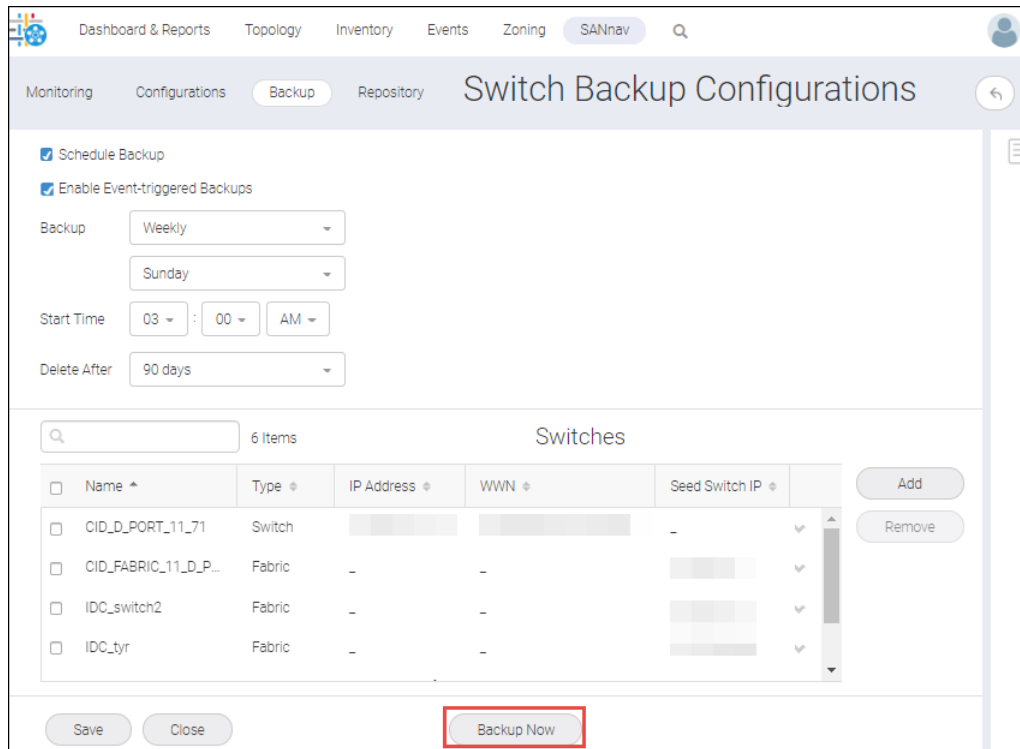
NOTE

By default, the **Enable Event-triggered Backups** option is enabled.

3. Set up a schedule for future backups, immediate backups, or create a backup when specific events occur.
 - If you want to set up a regular schedule for backups, select **Schedule Backup** and fill out the backup schedule.
 - If you want to back up a configuration immediately, click **Backup Now**.
 - If you want to create backups when specific events occur in the switches, select the **Enable Event-triggered Backups** check box and click **Save**. Event-triggered backups are generated for both the **Schedule Backup** and **Backup Now** options.

When configuring the backup, you can choose to back up individual switches or fabrics, or both. If you select fabrics, then all switches in the selected fabrics are backed up automatically.

The following example shows a scheduled backup that runs every Sunday at 3:00 a.m. The configuration files for one switch and three fabrics are backed up. For the fabric, all switches in the fabric are backed up in separate files. These configuration files are kept in the repository for 90 days unless manually deleted before then.



7.2.2 Restoring Switch or Logical Fabric Configurations

You can restore a switch configuration to a saved backup based on the need.

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 read-write permission.

You can restore the switches and logical fabric configurations as follows:

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

NOTE

Restoring a configuration is a disruptive operation.

Perform the following steps to restore the switch or logical fabric configuration.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Configuration and Operations Monitoring Policy**.

2. Click **Repository** to display a list of the configuration backups.

The **Backup Configurations** window displays.

NOTE

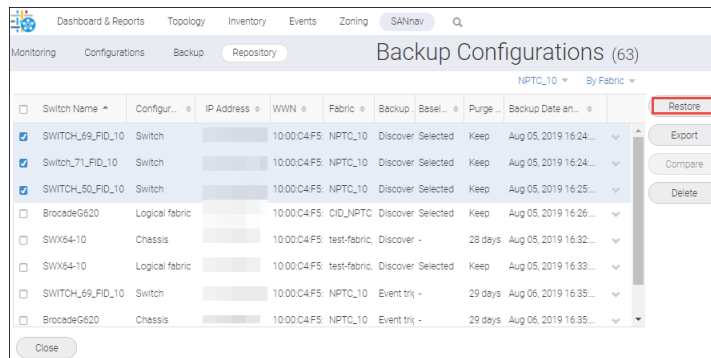
The displayed list is for monitored switches only. If you want to view configuration backups for unmonitored switches, select **Other** from the **By Fabric** drop-down list.

You can restore either the switch configuration or the logical fabric configurations.

3. To restore the switch configurations, follow the steps below:
 - a. Select the switch configuration that you want to restore, and click **Restore**. If VF is enabled, ensure logical fabric configuration is restored before attempting switch or chassis configuration restore.

NOTE

A switch can have more than one backup configuration types, so be sure to select the correct configuration type. You can search on the switch name to display only the configurations for that switch. If you select a logical fabric configuration type along with a switch or a chassis for the same switch, the **Restore** button is inactivated. You can select multiple switches to restore at the same time. For example, you can select a specific fabric and restore all switches in that fabric.

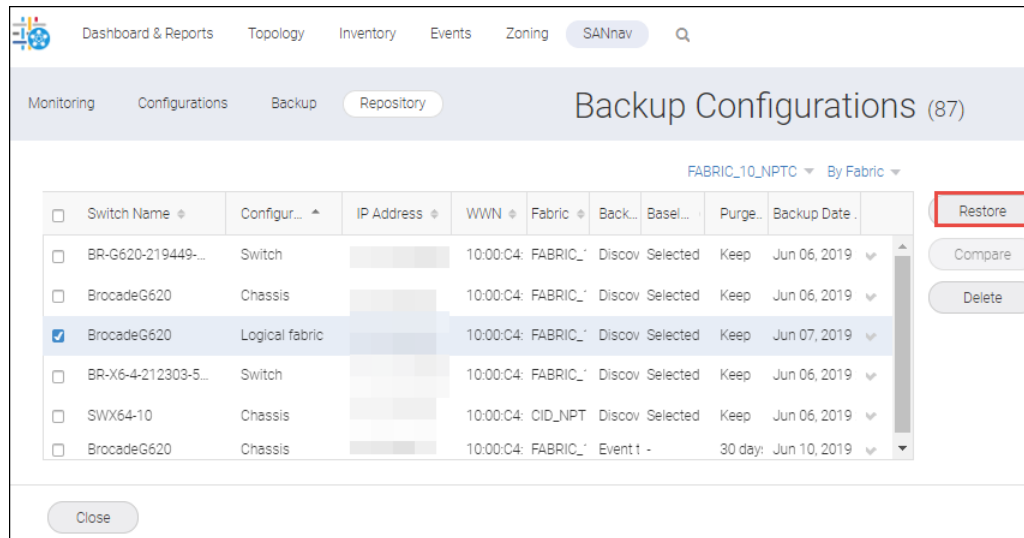


The **Restore Switch Configurations** window displays.

- b. Click **OK** in the confirmation window , and then click **Done**.
4. To restore the logical fabric configurations to the same switch, follow the steps below:
 - a. Select the logical fabric configuration that you want to restore, and click **Restore**.

NOTE

A logical fabric can have more than one backup configuration, so be sure to select the correct configuration. You can search on the logical fabric name to display only the configurations for that logical fabric. You can restore only one configuration for a logical fabric. If you select more than one configuration for the same logical fabric, the **Restore** button is inactivated. You can select multiple logical fabrics to restore at the same time. For example, you can select a specific fabric and restore all logical fabrics in that fabric.



The **Restore Logical Fabric Configurations** window displays.

- b. Click **OK** in the confirmation window, and then click **Done**.

The logical fabric configurations are restored.

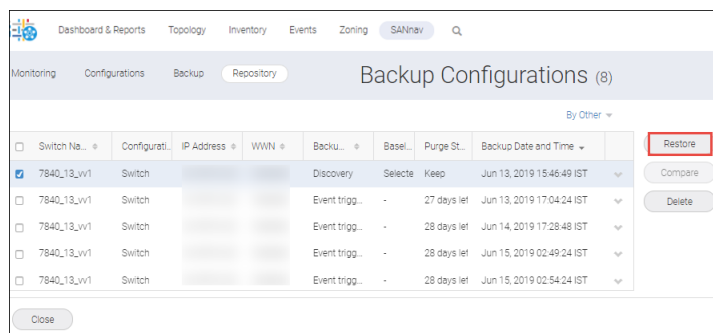
NOTE

When you restore the logical fabric configuration to the same switch, the switch reboots and creates the logical switches based on the logical fabric configuration.

5. To restore the switch or chassis or logical fabric configuration of a missing switch to multiple applicable switches, follow the steps below:
 - a. Select **Other** from the **By Fabric** drop-down list.

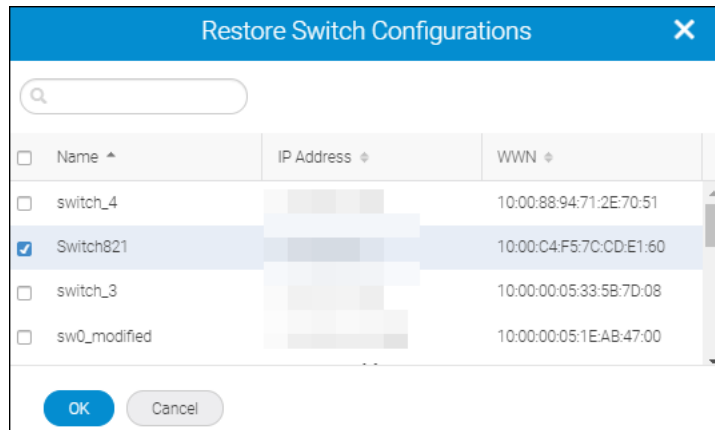
The backup entries for all missing switches are displayed.

- b. Select the switch configuration that you want to restore, and click **Restore**.



The **Restore Switch Configurations** window displays. This window displays the list of switches whose configuration you can restore. This window displays all applicable switches based on the type of backup entry, the switch model, and the version.

- c. Select the switch and select **OK**.



This operation replaces the current configuration on the switch and disables and then enables the switch.

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

NOTE

SANnav checks the status of the Virtual Fabric configuration restore operation 5 minutes after the operation is triggered, and the application event is raised with the success or failure status details of the operation.

7.2.3 Managing Switch Configuration Backups

You can back up configurations on one or more switches or entire fabrics on a daily or weekly basis or on-demand. You can view, delete, and export these backups, change the retention period, designate a backup as a baseline, and compare two configurations. Configuration backups are stored in the SANnav Management Portal repository; however, you can save backups to an offline location and restore them to switches based on need. SANnav Management Portal allows you to take configuration backups of one or more switches or entire fabrics. Switch configuration backups can be scheduled on a daily or weekly basis, or can be created on-demand. You can save backups to an offline location or restore them to the switches based on need.

To manage configuration backups, you must have the Configuration File Manager privilege with 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.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Configuration and Operations Monitoring Policy**.

The **Backup Configurations** window displays.

2. Click **Repository** to display a list of the configuration backups.

Switch	Configura.	IP Ad...	WWN	Fabric	Backu...	Basel...	Purge...	Backu...
BrocadeGf	Logical fat		10:00:C4	FABRIC...	Event trig...	-	30 days l...	Jun 10, 2...
BrocadeGf	Chassis		10:00:C4	FABRIC...	Event trig...	-	30 days l...	Jun 10, 2...
CID_D_POI	Switch		10:00:C4	CID_FAB...	Discovery	Selected	Keep	Jun 10, 2...
BR-G620-2	Switch		10:00:C4	FABRIC...	Event trig...	-	30 days l...	Jun 10, 2...
BR-G620-2	Switch		10:00:C4	CID_NPT...	Event trig...	-	30 days l...	Jun 10, 2...
switch_10	Switch		10:00:00	IDC_swit...	Event trig...	-	30 days l...	Jun 10, 2...
SWX64-10	Logical fat		10:00:C4	CID_NPT...	Discovery	Selected	Keep	Jun 10, 2...
SWX64-10	Chassis		10:00:C4	CID_NPT...	Event trig...	-	30 days l...	Jun 10, 2...
BrocadeGf	Logical fat		10:00:C4	FABRIC...	Discovery	Selected	Keep	Jun 10, 2...
BrocadeGf	Chassis		10:00:C4	FABRIC...	Event trig...	-	30 days l...	Jun 10, 2...

In the table, note the following:

- The **Configuration Type** column indicates Chassis, Switch, or Logical fabric.
 - The **IP address** column indicates the IP address for a switch, a chassis, or a logical fabric. The logical switch displays the fabric ID in brackets after the address.
 - The **Backup Type** column indicates how the backup was triggered.
3. To designate a configuration as a baseline, click the down arrow next to the configuration and select **Select Baseline**. Baseline configurations are kept indefinitely. A switch can have only one baseline configuration.
 4. To change the retention period for a configuration backup, click the down arrow next to the configuration and select one of the following options:
 - To retain a backup indefinitely, select **Keep**.
 - To delete a backup after the configured retention period (30 days or 90 days), select **Do Not Keep**.
 - 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 click **Compare**. You can compare backups only from the same switch and from the same type. You cannot compare backups from different switches.

7.3 Call Home and ESRS

Use the Call Home feature to send an email alert to one or more support centers to report problems based on events configured on Fabric OS devices.

When a 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 a Call Home event. When the event occurs, the location where the SupportSave data is stored is sent by email. In addition, some MAPS and application events are identified as Call Home events.

ESRS is an application used to collect product information and share it with the EMC server. The SANnav application sends the Call Home events, inventory, and SupportSave data (if enabled) to the ESRS application, which is managed by the EMC call center.

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

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

NOTE

If email configuration details of any of the call centers (Brocade Email, DELL EMC, IBM Email, and NetApp Email) are changed, you must enter the password.

7.3.1 Supporting the SANnav License for Call Centers

In SANnav, if you have installed the EMC license, the EMC Call Home center is enabled, and the other Call Home centers are disabled by default. However, you can enable and use the other Call Home centers also. For all other licenses, all of the Call Home centers are enabled by default.

7.3.2 Call Home Events

Call Home and ESRS are supported only on SANnav Management Portal. These features are not supported on SANnav Global View.

The table below lists the events that trigger Call Home:

FRU Code	Description
EM-1034	Faulty FRU.
Ethernet	Switch is not reachable.
MAPS-1003	Faulty SFPs.
MAPS-1021	Faulty or absent power supplies.
MAPS-1021	Faulty ports.
MAPS-1021	Marginal ports.
MAPS-1021	Missing SFPs.
MAPS-1021	Error ports.
MAPS-1021	Faulty WWN cards.
MAPS-1021	HA monitoring.
MAPS-1021	Core blade down.
MAPS-1021	Faulty or absent blades.
MAPS-1021	Faulty or absent fans.
MAPS-1021	Faulty temperature sensors.
MAPS-1021	Flash usage is out of range.
MAPS-2180	Faulty SFPs.
MAPS-2181	Faulty SFPs.

FRU Code	Description
MAPS-2182	Faulty SFPs.
MS-1009	Error in registered link incident record (RLIR).
SW-Missing	Switch is missing from the fabric.

7.3.3 Configuring Call Home Notifications

To configure Call Home notifications, you must have Call Home privilege with read-write permission.


You can view all Call Home operations in the **Events** tab.

When a critical event occurs in the switch (for example, a faulty FRU), a notification is sent to the Brocade Call Home along with the SupportSave data location.

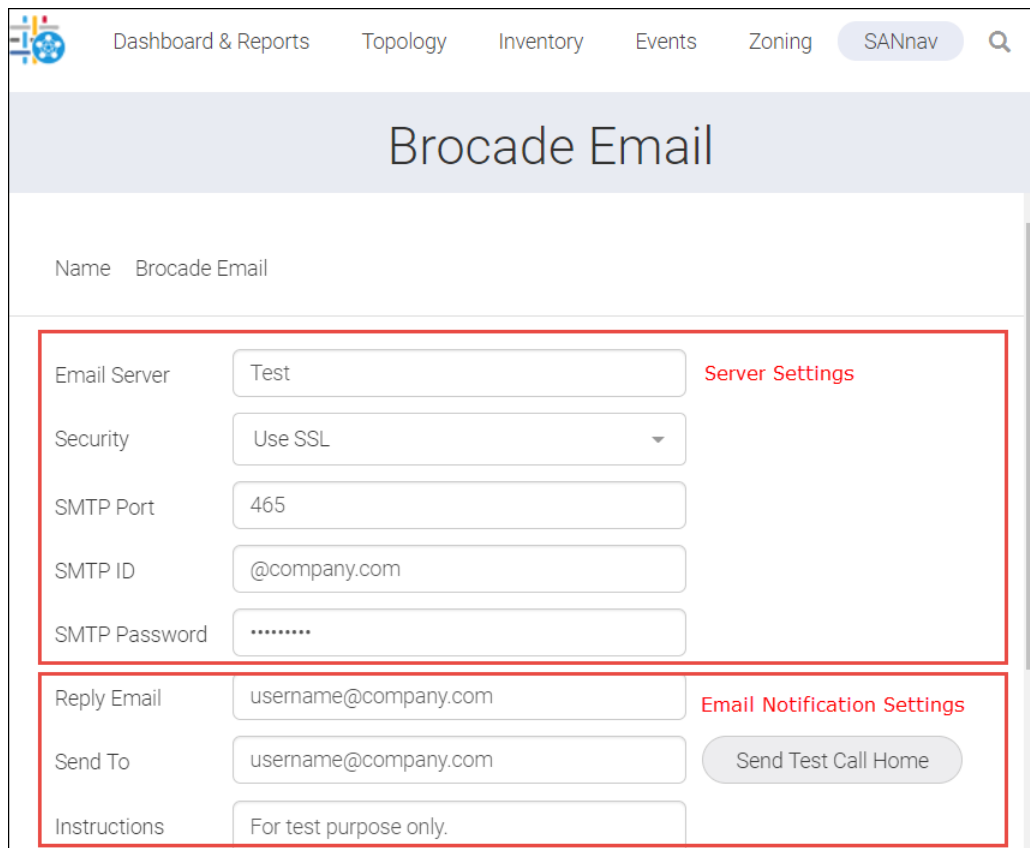
To configure the Call Home support center, follow the instructions below:

NOTE

The following steps do not support the Dell EMC support center. See [Configuring the Dell EMC Call Home Support Center](#).

1. Click **SANnav** in the navigation bar, and then select **Services > Call Home Configuration**.
2. Click the down arrow icon () on any Call Home support center (except for the Dell EMC Call Home center) and select **View** to display the details page.

The following screen capture shows the **Brocade Email** details page.



Dashboard & Reports Topology Inventory Events Zoning SANnav

Brocade Email

Name Brocade Email

Email Server Test **Server Settings**

Security Use SSL

SMTP Port 465

SMTP ID @company.com

SMTP Password

Reply Email username@company.com **Email Notification Settings**

Send To username@company.com **Send Test Call Home**

Instructions For test purpose only.

3. Enter the server and email notification settings. If you select security as none, the **SMTP ID** and **SMTP Password** fields are not available.

NOTE

If you modify the email settings for a call center, the **Save** button is not enabled until you enter the password. If you do not modify the email settings for a call center and want to add or remove a device, the **Save** button is enabled and you can modify the Call Home configuration without entering the password.

4. Click **Send Test Call Home** to check whether the server setting is valid.

In this case, a fake events report is sent to the Brocade Call Home center. You can verify with the Brocade Call Home center if the format of the email is correct. See [Call Home Email Notifications](#).

NOTE

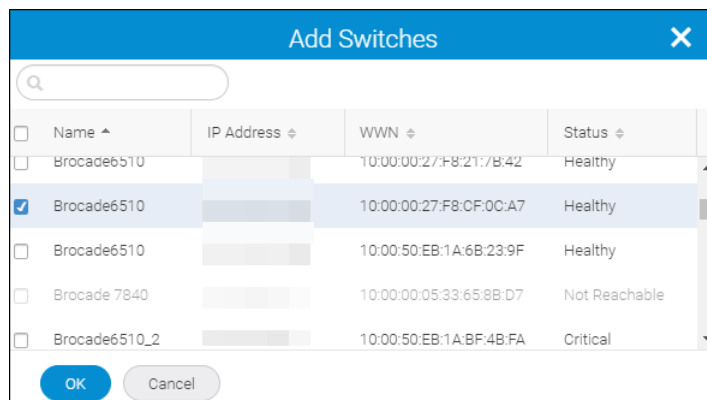
You must enter the password for sending a test call.

5. Assign switches to the Call Home.

- a. In the **Switches** section, click **Add**. The **Add Switches** window appears.
- b. Select the switches and click **OK**.

NOTE

- A switch can be assigned to one Call Home only.
- If the switch status is **Not Reachable**, you cannot add devices to any of the call centers.

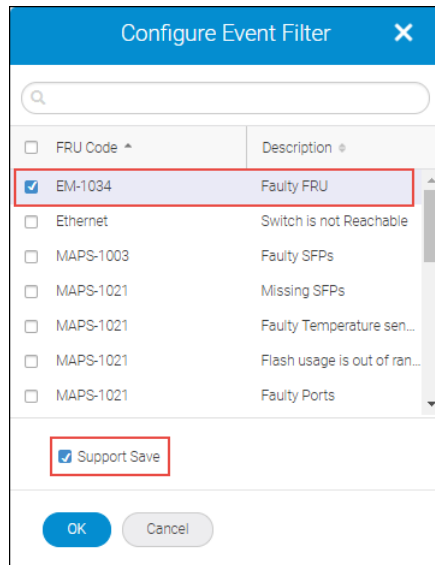


6. Configure Call Home events for the switches.

- a. Select one or more switches from the **Switches** section, and click **Configure**.
- b. Select the events for which you want to trigger Call Home, enable the **Support Save** option, and then click **OK**.

NOTE

When you select a single switch to configure events for the Brocade Call Home, no events are applied to the switch unless you select them. For the other Call Homes, all events are applied to the switch by default. When you select multiple switches to configure an event, you must select the events manually.



7. Click the **Enable** option before you save to activate the Call Home email notification.
8. Click **Save** to save the configuration.

In this case, the switch sends an event to the application via SNMP. The SANnav server checks whether the received event is a Call Home event. If SupportSave is enabled, the SupportSave operation is triggered for the affected switch, and the SupportSave storage location is shared through email to the respective call center. The last 30 events are collected for the affected switch for all centers. The Call Home module sends the Call Home events through email to the respective call center.

7.3.4 Configuring the Dell EMC Call Home Support Center

To configure Call Home notification, you must have Call Home privilege with read-write permission.

You can view all the Call Home operations in the **Events** tab.


NOTE

You cannot add switches successfully to DELL EMC call center if they are not registered in ESRS.

NOTE

When you apply an EMC license, all other call home centers are disabled except the Dell EMC Call Home center.

To configure the Dell EMC Call Home support center, follow the instructions below.

1. Click **SANnav** in the navigation bar, and then select **Services > Call Home Configuration**.
2. Click the down-arrow icon () on the **DELL EMC** Call Home, and select **View** to display the details page.
3. Enter the report interval to send the Dell EMC Call Home SYR to the ESRS application.

- Enter the SRS Gateway IP Address, SRS Port number, and user credentials.

- Click **Send Test Call Home** to check the whether the ESRS is valid.
- Assign switches to the Dell EMC Call Home.
 - In the **Switches** section, click **Add**.
 - Select the switches and click **OK**.

NOTE

You cannot use the same switch for the other Call Homes.

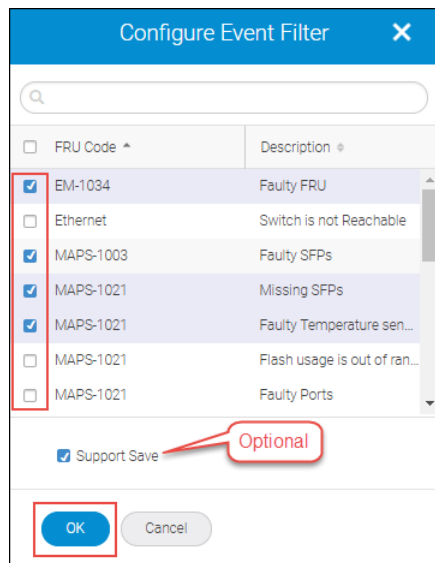
- Configure Call Home events for the switches.
 - Select one or more switches from the **Switches** section, and click **Configure**.

NOTE

If you try to add four switches and out of these four switches three are added to the ESRS, the failed switch is displayed in a pop-up window with the IP address and failure reason.

Name	WWN	IP Address	Support S...	serial #
<input checked="" type="checkbox"/> BrocadeG610			Enabled	EZL1907Q0L8
<input type="checkbox"/> TestAutoSWNa...			Enabled	BRW2549K039
<input type="checkbox"/> TestSetup_74_1...			Enabled	CGM0329H001


- Select the events that you want to trigger Call Home, and click **OK**.
By default, all events will be applied to the switch. If you deselect all the events and save the call home, you will not receive any notification for the switch.
- Select the **SupportSave** checkbox (optional), and click **OK**.
If **SupportSave** is checked, the generated SupportSave will be transferred to the ESRS appliance.

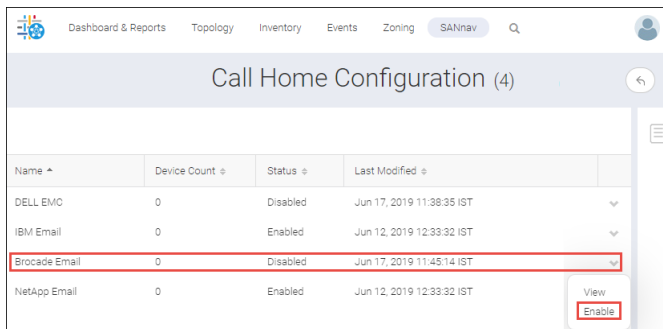


- Click **Download** to download the firmware files for the switches assigned to Dell EMC Call Home. The downloaded firmware files are imported to the FOS Version Management repository.
- Click the **Enable** check box before you save to activate the Call Home email notification.
- Click **Save** to save the changes.

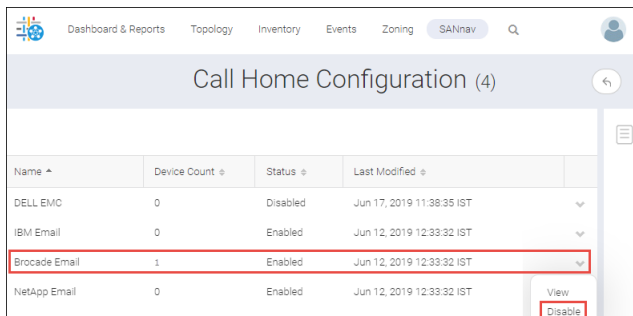
7.3.5 Enabling and Disabling a Call Home Center

To enable or disable a Call Home Center, follow the below instructions.

- Click **SANnav** in the navigation bar, and then select **Services > Call Home Configuration**.
- Click the down arrow icon () on any Call Home Support and select **Enable** from Call Home Management window.



- Click the down arrow icon () on any Call Home Support and select **Disable** from Call Home Management window.



7.3.6 Call Home Email Notifications

The email contains details about the call home event, the application server, the switch, and the last 30 events prior to the call home event. Each email contains an HTML attachment with details about the events.

The last 30 events prior to the event that triggered the call home are displayed at the end of the email.

Each email contains an HTML attachment with details about the events. One of the purpose of the HTML attachment is to save the attachment to your local machine for future references.

You can view all the Call Home operations in the Events tab.

7.4 Zoning

An administrator can partition the network into logical groups of devices through zoning. This partition allows the devices to interconnect and prevent access from the other devices outside the group, thereby providing increased network security and stability. Zoning also relieves the network from registered state change notification (RSCN) storms created due to multiple device interactions.

When a device is not included in the zone that device is not available to members of that zone. When zoning is enabled, devices that are not included in any zone configuration are inaccessible to all other devices in the fabric.

Using the **Zoning** tab in the SANnav Management Portal navigation bar, you can perform the following tasks:

- Create zone aliases.
- Create standard zones, peer zones, logical SAN (LSAN) zones, and LSAN peer zones.
- Create zone configurations.
- Create offline zones.
- Configure zones from the **Inventory** page.

In addition, SANnav Management Portal implements a highly simplified workflow called “simplified zoning” to create peer zones. The simplified zoning workflow allows you to easily create and activate peer zones in SANs. You can initiate zone creation from the inventory view of hosts, host ports, or storage ports. Created peer zones are automatically activated in the fabrics based on the devices selected. For example, if you choose a host that has ports in the A and B fabrics and you select target ports from those fabrics, LSAN peer zones are created and activated in both the A and B fabrics.

7.4.1 Zone Database Size

The database size for Zoning differs based on the fabric used and can be summarized as follows:

- For a fabric with a minimum of one fixed port switch, the supported maximum zone database size is 1 MB.
- For a fabric containing only directors, the supported maximum zone database size is 2 MB.
- If Virtual Fabrics is enabled, the sum of the zone database sizes on all logical fabrics should not exceed the maximum size as follows:
 - The maximum size allowed for the chassis is 2 MB.
 - The maximum size allowed for the fixed-port switch is 1 MB.

7.4.2 Naming Conventions

Zoning includes the zone names, zone aliases, zone configurations, and zonedb names. The naming rules for these vary with the type of fabric used. The following naming conventions apply:

- Names are case-sensitive.
- Names cannot begin with a special character.
- The maximum limit is 64 characters.
- A zone name cannot contain both of the following: the "BFA_" prefix and the "_BLUN" suffix as these names are used in Boot LUN zoning and do not support boot LUN zoning.
- Names consist of alphanumeric characters and one or more special characters.
 - For switches running Fabric OS 8.1.0 or later, names must begin with an alphanumeric character and can contain the following special characters: underscore (_), hyphen (-), dollar sign (\$), and caret (^).
 - For switches running Fabric OS 8.0.x and earlier, names must begin with a letter and can contain only the special character underscore (_).
- Names cannot begin with "bfa_", "lsan_red_", or "d__efault__".
- Zone configuration names cannot begin with any of the following reserved prefixes:
 - lsan_red_0917
 - lsan_red_1109
 - msfr_cfg_
 - m_u_l_t_i_r_e_d_i_r__cfg
 - msfr_zn_
 - red_0917
 - red_1109
 - red_____base
 - r_e_d_i_r_c_fg
 - t_r_a_f_f_i_c_i_s_o_c_fg
 - t_r_a_f_f_i_c_i_s_o_prop_zn
- Duplicate names are not allowed between zones, zone aliases, and zone configurations within a zone database.

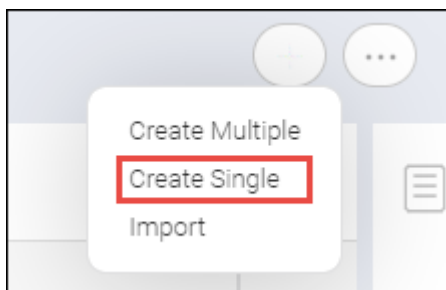
7.4.3 Creating Zone Aliases

A zone alias is a logical group of domain, port index numbers or WWNs. Zone aliases facilitate zone configuration by using the alias instead of selecting individual WWNs or domain, port index numbers.

7.4.3.1 Creating a Single Zone Alias with Multiple Members

To create a single zone alias, follow the instructions below:

1. Click **Zoning** in the navigation bar, and then select the **Zone Aliases** tab.
The **Zone Aliases** window displays.
2. Select the fabric from the **Select Fabric** drop-down list to add multiple members to the zone alias, and then click **OK**.
3. Click the **+** icon on the top-right corner of the window, and then select **Create Single** option from the available options.



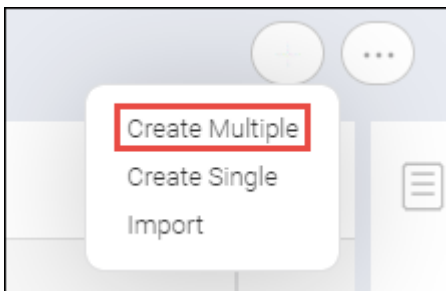
The **Create New Zone Alias** window displays.

4. Enter the zone alias name in the **Name** field.
As a best practice, use a unique alias name for a member.
5. Add members to the zone alias.
 - a. Click the **Add** button.
 - b. Select either **Select discovered Devices/Port** to choose the members from a list or **Enter manually** to type them in yourself.
 - c. Select the type of the zone member (**WWN** or **Domain, Port Index**) from the drop-down list.
 - d. Select the discovered members or type the name of the offline members, and then click the **>** to move them to the **Selected Members** list.
6. Click **OK** to add the members to the zone alias.
7. Click **Save** to save the zone alias.

7.4.3.2 Creating Multiple Zone Aliases

Multiple aliases can be created in a single workflow by using the **Create Multiple** option. This process creates zone aliases consisting of one member each. It is a fast way to assign zone alias names to ports. You can select all of the ports in a switch, and configure auto-generated alias names for each one. To create multiple aliases in a single workflow, follow the instructions below:

1. Click **Zoning** in the navigation bar, and then select the **Zone Aliases** tab.
The **Zone Aliases** window displays.
2. Select the fabric from the **Select Fabric** drop-down list to add the members to the zone alias, and then click **OK**.
3. Click the **+** icon on the top-right corner of the window, and then select the **Create Multiple** option from the available options.



The **Create Zone Alias** window displays.

4. Add members to the zone alias.
 - a. Click the **Add** button.
 - b. Select either **Select discovered devices/port** to choose the members from a list or **Enter manually** to type them in yourself.
 - c. Select the type of the zone member (**WWN** or **Domain, Port Index**) from the drop-down list.
 - d. Select the discovered members or type the name of the offline members, and then click **>** to move them to the **Selected Members** list.
5. Click **Next** to choose the method of naming the aliases.

6. Create zone aliases. You can create zone aliases either automatically or manually.
 - a. To automatically create the zone alias, follow the instructions below:
 1. Select the **Create aliases automatically** option.
 2. Enter the zone alias name in the **Zone Alias** field.
 3. Select the required option from the **Include** drop-down list. Zone alias names are uniquely created based on the include option that is either by appending numbers or by appending a letter to the zone alias name.

Examples:

 - Sequence letter option: aliasname_a, aliasname_A, and so on.
 - Sequence number option:
 - One-digit option: aliasname_1, aliasname_2, and so on.
 - Two-digit option: aliasname_01, aliasname_34, aliasname_67, and so on.
 - Three-digit option: aliasname_001, aliasname_023, aliasname_453, aliasname_239, and so on.
 4. Select the required option from the **Separator** drop-down list. Zone alias names are uniquely created based on the separator option, either by appending an underscore or by appending a hyphen.

Create Zone Alias [X]

Create aliases automatically
 Enter aliases manually

Zone Alias:

Include:

Separator:

Example: Zone Alias_02

- b. To create the zone alias manually, follow the instructions below:
 1. Select the **Enter aliases manually** option.
 2. Enter the zone alias name in the **New Zone Alias** field.

Create Zone Alias [X]

Create aliases automatically
 Enter aliases manually

Domain, ...	Port Name	FC Address	Switch	Connecte...	Connecte...	New Zone Alias
12,5	slot3 port5	0cfe80	switch_fid10...	_	20:05:04:F5:7...	<input type="text" value="Zone1"/>
11,1	port1_FOR_D...	0b0000	switch_fid10...	switch_fid10...	slot3 port3	<input type="text" value="Zone2"/>

NOTE

Based on the name entered for the first alias, auto-suggestable type must be there for the remaining alias names.

- Click **OK**.

The zone aliases are created and displayed under the **Zone Aliases** window.

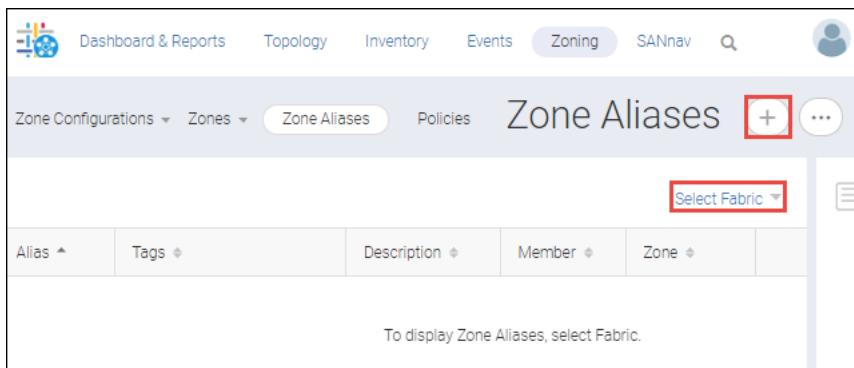
7.4.3.3 Importing Zone Aliases

You can import zone aliases from your local machine. To import zone aliases from your local machine, follow the instructions below:

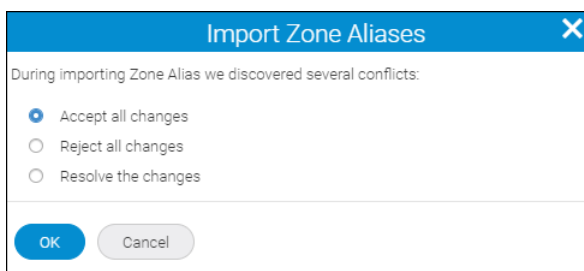
NOTE

Only `.csv` files are supported. You can also import files exported from the Brocade Network Advisor application.

- Click **Zoning** in the navigation bar, and then select the **Zone Aliases** tab.
- Select the fabric from the **Select Fabric** drop-down list into which to import the zone aliases, and then click **OK**.



- Click the **+** icon on the top-right corner of the window and select **Import**.
- Browse through the folders to select the file that contains the zone aliases.
- Click **Open** to import the zone aliases.
The **Import Zone Aliases** window displays.
- Select the desired action for when a conflict error message displays.
 - **Accept all changes** applies to all conflicts.
 - **Reject all changes** rejects 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.
 - **Resolve the changes** allows you to select from the conflicts.




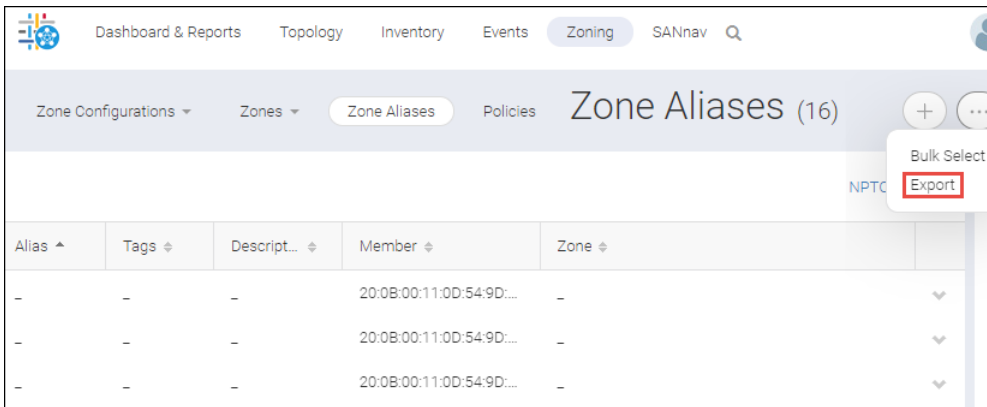
- Click **OK** to confirm the selected action.

7.4.3.4 Exporting Zone Aliases

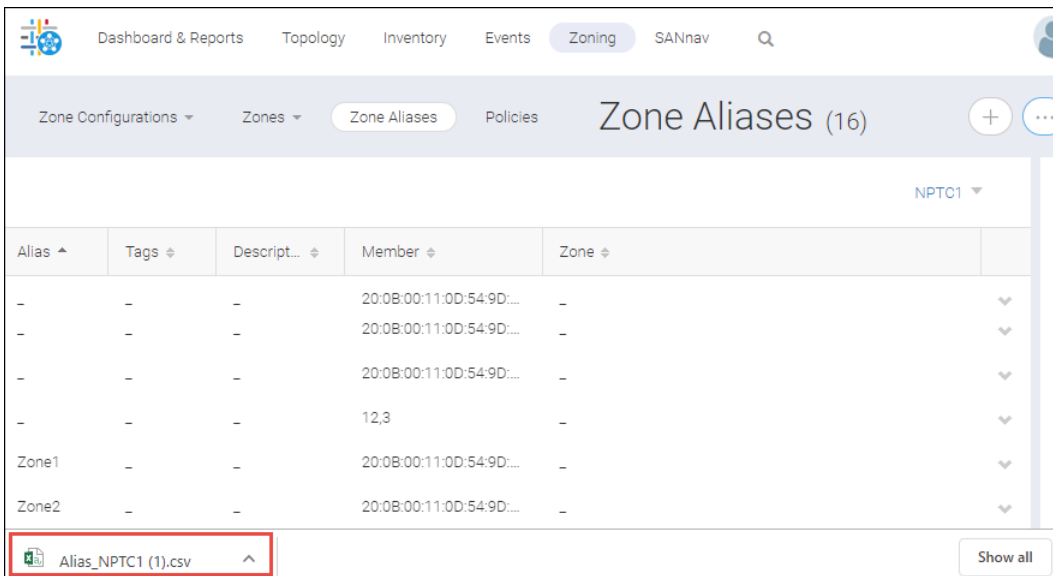
You can export zone aliases. For example, if a device is relocated to another fabric, you can use this alias in the other fabric. You can use this zone alias as a backup in case all zone databases are lost.

To export a zone alias, follow the instructions below:

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 the more icon (), on the top-right corner of the window, and then select **Export**.



The zone aliases of the selected fabric are downloaded as a `.csv` file to your local machine.



7.4.4 Configuring Zones in a Fabric

You can create new 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 peer zones
- LSAN zones
- Peer zones
- Standard zones

NOTE

SANnav does not support zoning with WWN, "Domain, Port Index", and alias together. If the zone members containing WWN, "Domain, Port Index", and alias together are created using another interface like the command line interface (CLI), Brocade Network Advisor, or Brocade Web Tools, they are listed as read only. However, you can create a new zone configuration using these mixed zone members and then activate the zone configuration.

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 were created using other interfaces, like the CLI, Brocade Network Advisor, or Brocade Web Tools, you can view these zones in SANnav but cannot modify them. If boot LUN or target driven zones are in a zone configuration, you can view the configuration but cannot modify or activate the configuration.

The created zone will not be activated unless you add the zones to a fabric and select the **Activate** checkbox in the zone configuration.

7.4.4.1 Creating Standard Zones

Standard zones allow communication between all members in the zone.


To create a standard zone, follow the instructions below:

1. Click **Zoning** in the navigation bar, and then select **Zones** from the **Zones** drop-down.
2. Select a fabric to which to create a zone, and then click **OK**.
3. Click the **+** icon on the top-right corner of the window to create a standard zone.
4. Enter a name for the zone, along with any tags and description.

5. Select **Standard Zone** from the **Zone Type** drop-down.

6. Add members to the standard 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**.

- c. Select discovered members to include the discovered members in the zone, and click () to move them to the **Selected Members** list.
- d. You can also select **Enter manually**, and type the name of offline members.

7. Click **OK** and then click **Save**.

7.4.4.2 Creating Peer Zones

A peer zone can be created with one or more devices 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 a fewer number of zones.

To create a peer zone, follow the instructions below:

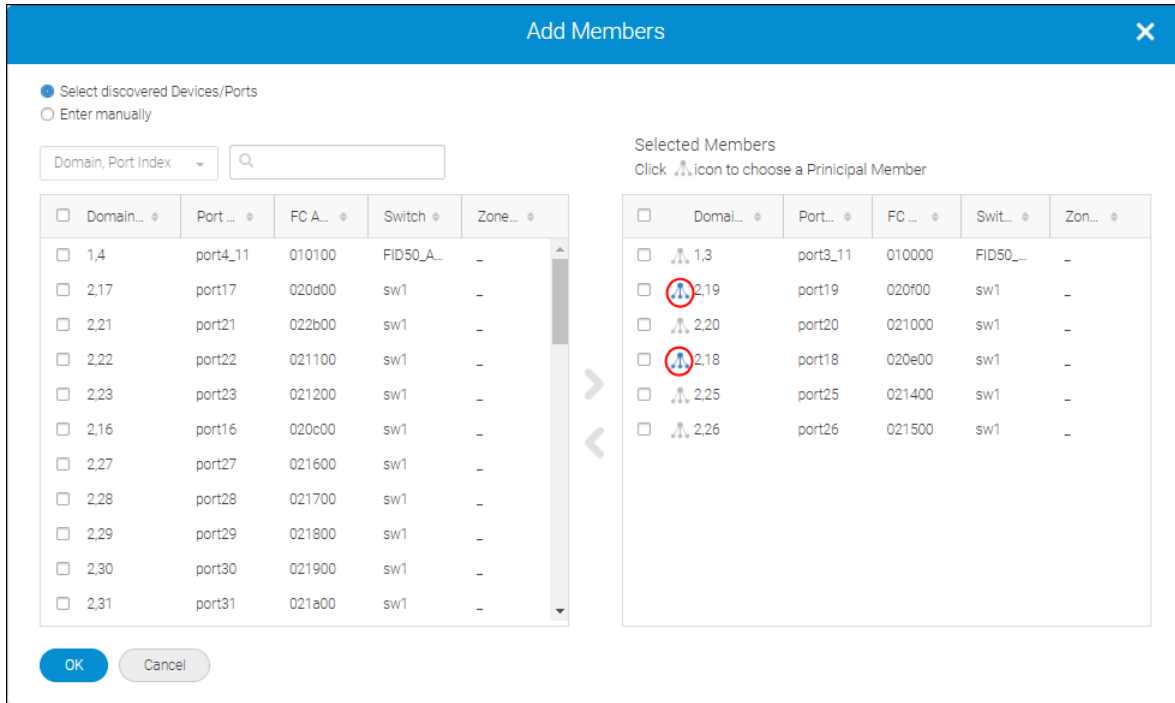
1. Click **Zoning** in the navigation bar, and then select **Zones** from the **Zones** drop-down.
2. Select a fabric in which to create a zone, and click **OK**.
3. Click the **+** icon on the top-right corner of the window to create a peer zone.
4. Enter a name for the zone, along with any tags and description.
5. Select **Peer Zone** from the **Zone Type** drop-down.

The screenshot shows the 'Create New Zone' interface. The 'Zone Type' dropdown menu is open, and 'Peer Zone' is selected. The form fields are as follows:

- Name: Test
- Tags: Testing
- Description: (empty text area)
- Zone Type: Standard Zone (dropdown menu open, showing options: Standard Zone, Peer Zone, LSAN Zone, LSAN Peer Zone)
- Fabric: (empty dropdown)

Below the form is a 'Members' table with columns for Zone Alias, Member Count, and Type. There are 'Add' and 'Remove' buttons to the right of the table. At the bottom of the form are 'Save' and 'Cancel' buttons.

6. Add principal members and peer members to the peer 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**.
 - c. Select discovered members to include in the zone, and click (**>**) to move them to the **Selected Members** list.
 - d. You can also select **Enter manually** and type the names of offline members.
 - e. Click (**⚙**) to add a selected member as a principal member in the zone.
The nonselected members will be present as peer members of the principal members in the zone.



7. Click **OK**, and then click **Save**.

7.4.4.3 Creating LSAN Zones

You can create an LSAN zone to allow the devices to communicate with the other devices 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.

NOTE

When you configure an LSAN zone, SANnav does not support aliases of the same name with the same member already present in another edge fabric.

To create an LSAN zone, follow the instructions below:

1. Click **Zoning** in the navigation bar, and then select **Zones** from the **Zones** drop-down.
2. Select a fabric to which to create a zone, and click **OK**.
3. Click the **+** icon on the top-right corner of the window to create an LSAN zone.

The screenshot shows the 'Create New Zone' page in the SANnav management portal. The navigation bar includes 'Dashboard & Reports', 'Topology', 'Inventory', 'Events', 'Zoning', and 'SANnav'. The main header shows 'Zone Configurations' with a dropdown menu set to 'Zones', and 'Zone Aliases' and 'Policies' links. The title is 'Create New Zone'. The form contains the following fields:


- Name:** Text input with 'Test' entered.
- Tags:** Text input with 'Testing' entered.
- Description:** Text area.
- Zone Type:** Dropdown menu with 'Standard Zone' selected. The dropdown is open, showing options: 'Standard Zone', 'Peer Zone', 'LSAN Zone' (highlighted with a red box), and 'LSAN Peer Zone'.
- Fabric:** Text input.

Below the form is a 'Members' section with a search icon and a table:

<input type="checkbox"/>	Zone Alias	Member Count	Type	
<input type="checkbox"/>				<input type="button" value="Add"/>
<input type="checkbox"/>				<input type="button" value="Remove"/>

At the bottom of the form are 'Save' and 'Cancel' buttons.

4. Enter a name for the zone, along with any tags and description.
5. Select **LSAN Zone** from the **Zone Type** drop-down.
6. Add members to the LSAN zone.
 - a. Click **Add** in the **Create New Zone** window.
 - b. Select the type of zone member from the drop-down list: **WWN** or **Alias**. Only aliases configured with WWN members are listed.

- c. Select discovered members to include in the zone, and click () to move them to the **Selected Members** list.

Add Members
✕

Select discovered Devices/Ports
 Enter manually

<input type="checkbox"/>	WWN	Type	Fabric	Host...	Zone...
<input type="checkbox"/>	30:15:00:0...	Initiator	Fabric101	-	-
<input type="checkbox"/>	30:0E:00:0...	Initiator	Fabric101	-	-
<input type="checkbox"/>	30:16:00:0...	Initiator	Fabric101	-	-
<input checked="" type="checkbox"/>	30:13:00:0...	Initiator	Fabric101	-	-
<input checked="" type="checkbox"/>	30:0B:00:0...	Initiator	Fabric101	-	-
<input type="checkbox"/>	20:01:00:0...	Target	Fabric101	AG-FDMI	-
<input type="checkbox"/>	30:10:00:0...	Initiator	Fabric101	-	-
<input type="checkbox"/>	20:00:00:1...	Target	Fabric101	-	Storage...
<input type="checkbox"/>	30:12:00:0...	Initiator	Fabric101	-	-
<input type="checkbox"/>	20:00:00:1...	Target	Fabric101	-	Storage...
<input type="checkbox"/>	30:11:00:0...	Initiator	Fabric101	-	-

➤

Selected Members

<input type="checkbox"/>	WWN	Type	Fabric	Host...	Zone...
<input type="checkbox"/>	30:14:00:0...	Initiator	Fabric101	-	-
<input type="checkbox"/>	30:17:00:0...	Initiator	Fabric101	-	-
<input type="checkbox"/>	20:00:00:1...	Target	Fabric101	-	Storage...

OK
Cancel

- d. You can also select **Enter manually** and type the names of the offline members.

7. Click **OK** and then click **Save**.

7.4.4.4 Creating 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.

NOTE

When configuring an LSAN zone, SANnav does not support aliases of the same name with the same member already present in the other edge fabric.

Newly created peer zones are automatically activated in the fabrics based on the devices selected. For example, if a host that has ports in fabrics A and B is chosen and target ports from fabrics A and B are selected, LSAN peer zones are created and activated in both fabrics A and B.

To create an LSAN peer zone, follow the instructions below:

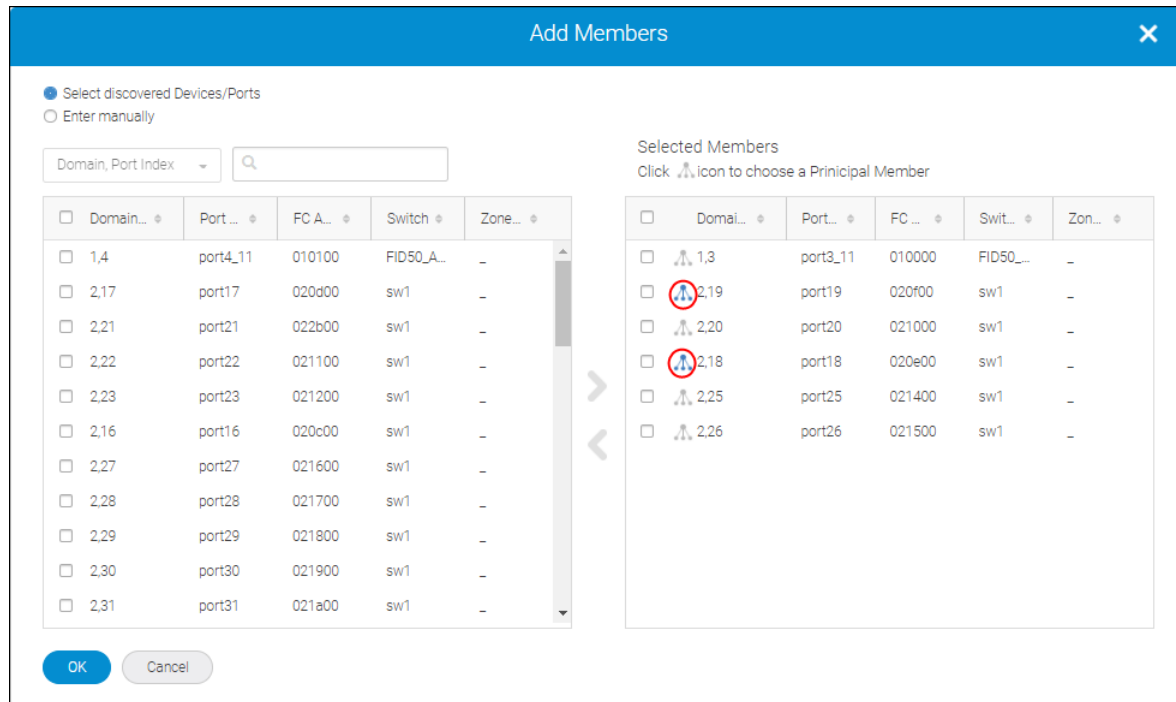
1. Click **Zoning** in the navigation bar, and then select the **Zones** from **Zones** drop-down.
2. Select a fabric in which to create a zone, and click **OK**.
3. Click the **+** icon on the top-right corner of the window to create an LSAN peer zone.

The screenshot shows the 'Create New Zone' page in the SANnav management portal. The navigation bar includes 'Dashboard & Reports', 'Topology', 'Inventory', 'Events', 'Zoning', and 'SANnav'. The main header shows 'Zone Configurations' with a dropdown menu set to 'Zones', and 'Zone Aliases' and 'Policies' links. The title is 'Create New Zone'. The form contains the following fields:

- Name:** Text input with 'Test' entered.
- Tags:** Text input with 'Testing' entered.
- Description:** Text area.
- Zone Type:** Dropdown menu with 'Standard Zone' selected. The dropdown list is open, showing 'Standard Zone', 'Peer Zone', 'LSAN Zone', and 'LSAN Peer Zone'. 'LSAN Peer Zone' is highlighted with a red box.
- Fabric:** Text input.

Below the form is a 'Members' section with a search icon and a table with columns: 'Zone Alias', 'Member Count', and 'Type'. There are 'Add' and 'Remove' buttons to the right of the table. At the bottom of the page are 'Save' and 'Cancel' buttons.

4. Enter a name for the zone, along with any tags and description.
5. Select **LSAN Peer Zone** from the **Zone Type** drop-down.
6. Add principal members and peer members to the LSAN peer zone.
 - a. Click **Add** in the **Create New Zone** window.
 - b. Select the type of zone member from the drop-down list: **WWN** or **Alias**. Only aliases configured with WWN members will be listed.
 - c. **Select discovered Devices/Ports** to include in the zone, and click (➤) to move them to the **Selected Members** list.
 - d. You can also select **Enter manually**, and type the name of the offline members.
 - e. Click (⤴) to add the selected member as a principal member in the zone.
The nonselected members are present as the peer members of the principal members in the zone.



7. Click **OK**, and then click **Save**.

7.4.4.5 Selecting and Adding Multiple Zone Aliases to a Zone

The bulk select feature allows you to select multiple zone aliases and create zones with these aliases. You can add multiple zone aliases to a zone in the following ways:

- Adding the selected zone aliases to an existing zone.

NOTE

The zone can be a part of the active or inactive zone configuration.

- Adding the selected zone aliases to a newly created zone.


NOTE

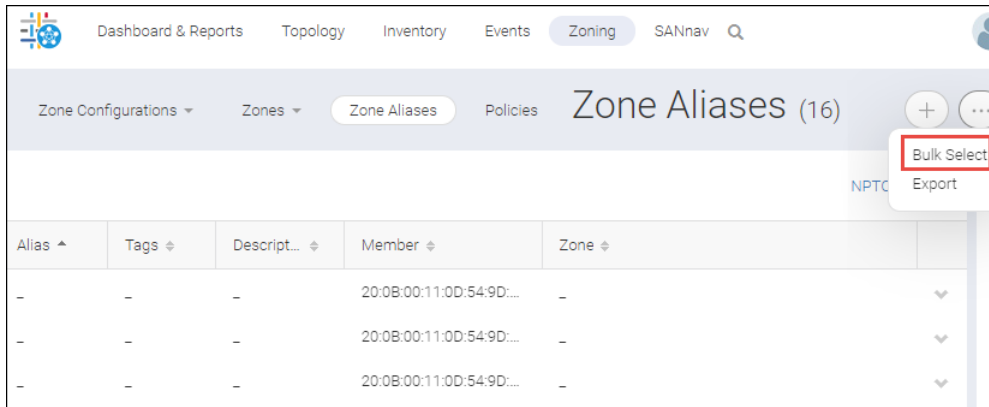
- After selecting the zone aliases, the **Add to Zone** and **Create New** options are available to create a new zone.
- After creating the zone, the **Add to Zone Config** option is available.

To add multiple zone aliases to a zone in bulk, follow the instructions below:

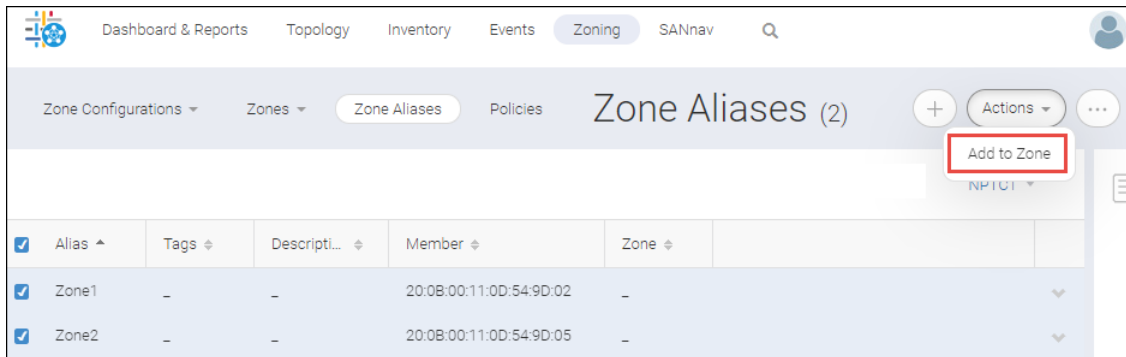
1. Click **Zoning** in the navigation bar, and then select the **Zone Aliases** tab.

The **Zone Aliases** window displays.

2. Click the more icon (), on the top-right corner of the window, and then select **Bulk Select**.



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.



The **Add to Zone** window displays.

4. Add aliases to an existing zone.
 - a. Select the zone to which to add the zone aliases, and then click **Next**.
The **Add to Zone** window displays a message either to add the zone aliases to the selected zone or to view and activate the zone configuration.

Fabric: NPTC1

Zone Name ▲	Type ◆	Status ◆
ZoneA	Standard	Inactive

Next Cancel Create New

- b. You can either view and activate the zone configuration or add the selected zone aliases to the selected zone.

Zone aliases have been successfully added to the active zone(s) listed below.
Click Next to view and activate the zone configuration or Close to finish.

Modified zones: ZoneA

Next Close

- Click **Close** to add the zone aliases to the selected zone and push the changes to the switch.
 - Click **Next** to view and activate the zone configuration.
5. Add aliases to a newly created zone.
- a. Click **Create New** from the **Add to Zone** window.

Fabric: NPTC1

<input type="checkbox"/> Zone Name ▲	Type ⇅	Status ⇅
<input type="checkbox"/> ZoneA	Standard	Inactive

Next Cancel **Create New**

The **Create New Zone** window displays. You can create only a standard or peer zone while creating a new zone to which to add the multiple zone aliases.

- b. Enter the zone name, the zone type, and the description of the zone.

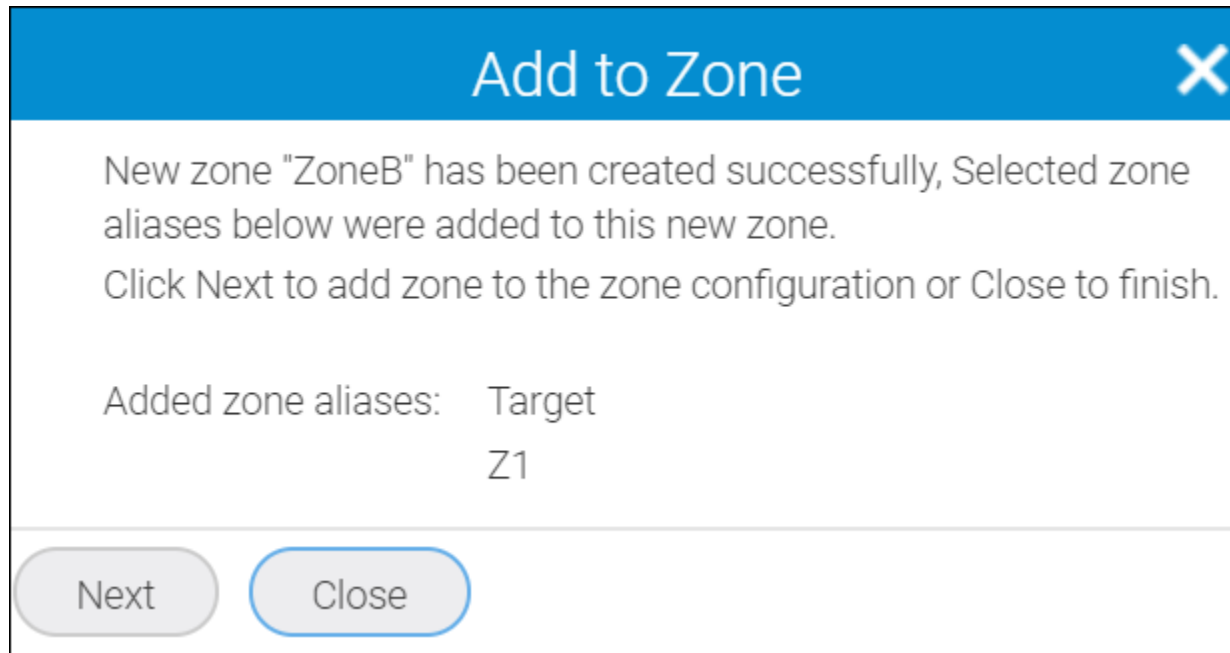
Zone Name: ZoneB

Zone Type: Standard Zone

Description: Test

Back OK Cancel

- c. Click **OK**. The **Add to Zone** window displays a message either to add the zone aliases to the selected zone or to view and activate the zone configuration.
- d. You can either view and activate the zone configuration or add the selected zone aliases to the newly created zone.



- Click **Close** to add the zone aliases to the selected zones and push the changes to the switch. Alternatively, you can click **Next** to view and activate the zone configuration.

For detailed information on activating the zone configuration, see section [Selecting and Adding Multiple Zones to a Zone Configuration](#).

7.4.5 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 reside on a switch at once, and you can quickly alternate among them. For example, you might want to have one configuration enabled during business hours and another 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.

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 configuration.

The **Zones** tab also lists the Target Driven Zones (TDZs). A TDZ is automatically created by SANnav Management Portal and you can only view the TDZ details. The TDZ concept allows a storage port to create an FC zone automatically. Using a storage array management interface, an initiator can be added to all the targets that are required to communicate. The target will then automatically setup the appropriate zones to allow each initiator to access it.

SANnav does not support zoning with WWN, "Domain, Port Index", and Alias together. In case the zone members containing WWN, "Domain, Port Index", and Alias together are created using other interfaces like command line interface (CLI), Brocade Network Advisor, or Brocade Web Tools, they are listed as read only. However, you can create a new zone configuration using these mixed zone members and then activate the Zone Configuration.

NOTE

Only one active Zone Configuration per fabric is allowed.

NOTE

Empty zone configurations and zones cannot be created from SANnav. If empty zone configurations and zones are created using the CLI, you can view and delete the empty zone configuration and zones in SANnav. You cannot add empty zones to zone configuration, and edit them in SANnav.

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 were created using other interfaces, like the CLI, Brocade Network Advisor, or Brocade Web Tools, you can view these zones in SANnav but cannot modify them. If boot LUN or target driven zones are in a zone configuration, you can view the configuration but cannot modify or activate the configuration.

To create a new zone configuration, follow the instructions below:

1. Click **Zoning** in the navigation bar, and then select the fabric and click **OK** to create a zone configuration in the fabric. By default, the **Zone Configurations** window displays.
2. Click the **+** icon on the top-right corner of the **Zone Configuration** window. The **Create New Zone Configurations** window displays.
3. Enter a name for the zone configuration, along with any tags and description.
4. Click **Add** to select from the list of zones, or select **Create New** to create new zones.
 - a. Enter a zone name, along with any tags and description in the **Create New Zone** window.
 - b. Select the zone type from the **Zone Type** drop-down list. When you select **Standard Zone** or **Peer Zone** as the zone type, you can select **Alias**, **WWN**, or **Domain, Port Index**. When you select **LSAN Zone** or **LSAN Peer Zone** as the zone type, you can select **Alias** or **WWN** as members.

- C. **Select discovered Devices/Ports** to include the discovered members in the zone, and click () to move them to the **Selected Members** list. You can also select **Enter manually**, and type the names of the offline members.

Create New Zone
✕

Zone Name

Tags

Zone Type

Description

Select discovered Devices/Ports


Enter manually

Domain, Port Index

<input type="checkbox"/>	Domain, Po...	Port Name	FC Adresse...	Switch
<input type="checkbox"/>	1,64	slot2 port0	014000	DCX-8510-4-...
<input checked="" type="checkbox"/>	1,149	slot7 port21	019500	DCX-8510-4-...
<input type="checkbox"/>	1,151	slot7 port23	019700	DCX-8510-4-...
<input checked="" type="checkbox"/>	1,152	slot7 port24	019800	DCX-8510-4-...
<input type="checkbox"/>	1,146	slot7 port18	019200	DCX-8510-4-...
<input checked="" type="checkbox"/>	1,154	slot7 port26	019a00	DCX-8510-4-...
<input type="checkbox"/>	1,155	slot7 port27	019b00	DCX-8510-4-...
<input type="checkbox"/>	1,156	slot7 port28	019c00	DCX-8510-4-...
<input type="checkbox"/>	1,157	slot7 port29	019d00	DCX-8510-4-...
<input type="checkbox"/>	1,158	slot7 port30	019e00	DCX-8510-4-...
<input type="checkbox"/>	1,145	slot7 port17	019100	DCX-8510-4-...

Selected Members

<input type="checkbox"/>	Domain, Po...	Port Name	FC Adresse...	Switch
<input type="checkbox"/>	1,147	slot7 port19	019300	DCX-8510-4-...
<input type="checkbox"/>	1,148	slot7 port20	019400	DCX-8510-4-...
<input type="checkbox"/>	1,150	slot7 port22	019600	DCX-8510-4-...

5. If you are creating a peer zone or an LSAN peer zone, click () to add the selected member as a principal member of the zone. The nonselected members are present as the peer members of the principal members in the zone.

Create New Zone
✕

Zone Name


Tags

Zone Type

Description

Select discovered Devices/Ports
 Enter manually

<input type="checkbox"/>	Domain, Po...	Port Name	FC Addr...	Switch
<input checked="" type="checkbox"/>	1,64	slot2 port0	014000	DCX-8510-4...
<input type="checkbox"/>	1,145	slot7 port17	019100	DCX-8510-4...
<input checked="" type="checkbox"/>	1,149	slot7 port21	019500	DCX-8510-4...
<input type="checkbox"/>	1,151	slot7 port23	019700	DCX-8510-4...
<input checked="" type="checkbox"/>	1,153	slot7 port25	019900	DCX-8510-4...
<input type="checkbox"/>	1,144	slot7 port16	019000	DCX-8510-4...
<input type="checkbox"/>	1,156	slot7 port28	019c00	DCX-8510-4...
<input type="checkbox"/>	1,157	slot7 port29	019d00	DCX-8510-4...
<input type="checkbox"/>	1,158	slot7 port30	019e00	DCX-8510-4...
<input type="checkbox"/>	1,159	slot7 port31	019f00	DCX-8510-4...
<input type="checkbox"/>	1,160	slot7 port32	01a000	DCX-8510-4...

Selected Members
Click  icon to choose a Principal Member

<input type="checkbox"/>	Domain, P...	Port Na...	FC Addr...	Switch
<input checked="" type="checkbox"/>	1,146	slot7 port18	019200	DCX-8510-...
<input type="checkbox"/>	1,152	slot7 port24	019800	DCX-8510-...
<input checked="" type="checkbox"/>	1,154	slot7 port26	019a00	DCX-8510-...

6. To add one or more zones to zone configurations, follow the steps below:
- Click **Add**. The **Add Zones** window displays.
 - Select the existing zones to add to the zone configuration.

Add Zones
✕

<input type="checkbox"/>	Name ▲	Type	Tags
<input type="checkbox"/>	ESXi49_A_SVC	Standard	-
<input checked="" type="checkbox"/>	ESXi49a_VMAX4E1	Standard	-
<input checked="" type="checkbox"/>	ESXi51_A_SVC	Standard	-
<input checked="" type="checkbox"/>	ESXi51a_VMAX4E1	Standard	-

OK

Create New

Cancel

7. Click **OK** to add the new zones to the zone configurations.
8. Click **Activate** to activate the zone configuration, and click **Save**.
Click **OK** in the confirmation dialog.


The following are the behavioral changes of the LSAN zone configuration when it is activated:

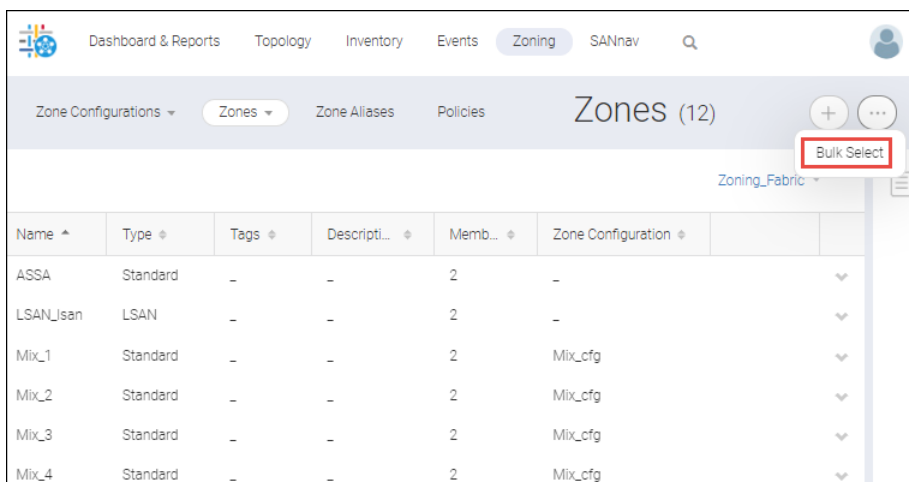
- Traffic is disrupted in the edge fabric.
- A zone configuration is automatically created when there is no active zone configuration in the fabric.
- The new LSAN zone overwrites the existing zone if the new LSAN zone name is similar to the existing LSAN zone name.
- For the LSAN zones that contain both offline and online devices but are not assigned to any other fabrics, the zones are pushed automatically to the fabrics that contain the online devices.
- The inactive zone configuration with changes in the fabric will be automatically activated when any LSAN zone changes are sent to the fabric.

7.4.5.1 Selecting and Adding Multiple Zones to a Zone Configuration

Multiple zones can be selected and added to a zone configuration.

To select and add multiple zones to a zone configuration, follow the instructions below:

1. Click **Zoning** in the navigation bar, and then select **Zones** from the **Zones** drop-down.
The **Zones** window displays.
2. Select the fabric from the **Select Fabric** drop-down, and then click **OK**.
The **Zones** window displays with the list of zones of the selected fabric.
3. Click the more icon () on the top-right corner of the window, and then select **Bulk Select**.



Name	Type	Tags	Descripti...	Memb...	Zone Configuration
ASSA	Standard	-	-	2	-
LSAN_Isan	LSAN	-	-	2	-
Mix_1	Standard	-	-	2	Mix_cfg
Mix_2	Standard	-	-	2	Mix_cfg
Mix_3	Standard	-	-	2	Mix_cfg
Mix_4	Standard	-	-	2	Mix_cfg

The select options for the zones are displayed.

4. Select the zones to add them to the existing zone configuration, and then select **Add to Zone Config** from the **Actions** drop-down.

Dashboard & Reports Topology Inventory Events Zoning SANnav

Zone Configurations Zones Zone Aliases Policies Zones (12)

Actions Add to Zone Config zoning_fabric

<input type="checkbox"/>	Name ^	Type	Tags	Description	Member Count	Zone Configuration
<input type="checkbox"/>	LSAN_1san	LSAN	-	-	2	-
<input checked="" type="checkbox"/>	Mix_1	Standard	-	-	2	Mix_cfg
<input checked="" type="checkbox"/>	Mix_2	Standard	-	-	2	Mix_cfg
<input checked="" type="checkbox"/>	Mix_3	Standard	-	-	2	Mix_cfg
<input checked="" type="checkbox"/>	Mix_4	Standard	-	-	2	Mix_cfg
<input type="checkbox"/>	P1	Peer	-	-	3	-
<input type="checkbox"/>	alzone1	Standard	-	-	2	alifcg
<input checked="" type="checkbox"/>	nnw	Standard	-	-	2	alifcg
<input type="checkbox"/>	peer_1	Peer	-	-	2	peer_cfg

To add a single zone to the zone configuration, click symbol next to a zone, and then select **Add to Zone Config** option.

The **Add to Zone Config** window displays.

- Select the zone configuration to which to add the zones. After selecting the zone configuration, you can add the zones to the zone configuration and activate it by selecting the **Activate selected configuration**. If you do not select **Activate selected configuration**, the zones are added to the zone configuration without activating it.

Add to Zone Config Selected Zones (4)

Fabric: Zoning_Fabric

Zone Config Name ^ Status

Mix_cfg	Defined
alifcg	Defined (Modified)
peer_cfg	Defined

Activate selected configuration

OK Cancel Compare

NOTE

While adding changes to a zone configuration, the **Compare** button is available to view the changes between the effective zone configuration and the defined modified copy of that zone configuration. You can directly compare the effective zone configuration and defined modified copy of that zone configuration without submitting the changes to the database. For detailed information on comparing the zone configurations, see section [Comparing Effective and Defined \(Modified\) Zone Configurations](#).

6. Click **OK**.

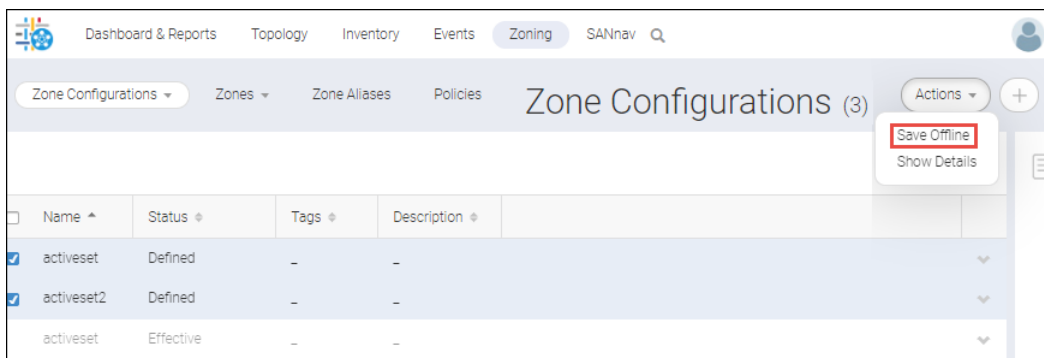
The zones are added to the selected zone configuration.

7.4.5.2 Saving the Inactive Zone DB to the Offline Zone DB

You can copy a zone configuration by selecting the required defined zone configurations and assigning them to an offline zone database. The benefits include editing the zone database currently and applying the changes later, and multiple zone databases (one or more for backup and one for normal operation) to edit and switch between them.

To duplicate a zone configuration to the offline zone DB, follow the instructions below:

1. Click **Zoning** in the navigation bar, and then select a fabric from the **Select Fabric** drop-down, and click **OK**.
By default, the **Zone Configurations** window displays.
2. Select only the defined zones, and click **Save Offline** from the **Actions** drop-down list to save them as offline zone DB.



The **Save Offline** window displays.

3. Enter the offline zone DB name in the **Name** field and click **OK** to save the selected defined zone configuration to the offline zoneDB. The zone name must be a maximum of 64 characters.
The current zoneDB is saved as offline copy.
4. Click **Close** to close the confirmation window.

7.4.6 Identifying the Zones without Any Zone Configuration

You can view the list of zones that do not have any configured zone configuration.

To identify the zones that are not part of any zone configuration, follow the steps below:

1. Click **Zoning** in the navigation bar, and then select **Zones** from the **Zones** drop-down.
The **Zones** window displays.
2. Check the **Zone Configuration** column. The zones that are not part of any zone configuration contain hyphen (-) value for zone configuration column against each zone.

The screenshot shows the SANnav Zoning interface. At the top, there is a navigation bar with tabs for Dashboard & Reports, Topology, Inventory, Events, Zoning (selected), and SANnav. Below the navigation bar, there are sub-tabs for Zone Configurations, Zones (selected), Zone Aliases, and Policies. The main content area displays a table of zone configurations for the selected fabric, FABRIC_10_NPTC. The table has columns for Name, Type, Tags, Description, Member Count, and Zone Configuration. The 'Zone Configuration' column header and the configuration for the 'SANBLAZE1' zone are highlighted with red boxes.

Name	Type	Tags	Description	Member Cou...	Zone Configuration
SANBLAZE1	Peer	-	-	2	SZAutoCfgSANBLAZE1
ZoneB	Standard	-	-	2	-

7.4.7 Offline Zoning

Offline zoning allows you to copy a fabric zone database and edit it offline. The benefits of using offline zoning include the following:

- Add changes to the zone database but apply them later.
- Save multiple copies of the zone database and switch between them.
- Analyze the impact of changes to storage access before applying the changes.

7.4.7.1 Creating Offline Zone Configurations

To create a new zone DB, follow the instructions below:

1. Click **Zoning** in the navigation bar, and then select **Offline Configurations** from the **Zone Configurations** dropdown.
2. Click **Select Zone DB** to create an offline configuration, and click **OK**.
3. Click the **+** icon on the top-right corner of the window, and select **Create New Offline Zone Configuration**.
The **Create New Offline Zone Configuration** window displays.
4. Enter a name for the offline zone configuration, along with any tags and description.

Dashboard & Reports Topology Inventory Events Zoning SANnav

Offline Configurations Zones Zone Aliases Policies Create New Offline Zone Configuration

Name OfflineZoneConfig1 Description For test purpose only.

Tags Test

Fabric Zoning_Fabric

0 Items Zones

Name ^	Type ^	Member Count ^

Add Remove

Save Cancel

5. Click **Add** to select from the list of zones, or select **Create New** to create new zones.

To add an offline zone member in the **Create New Zone** window, follow the steps below:

- a. Select zone type from the **Zone Type** drop-down. When you select the **Standard Zone** or **Peer Zone** as the zone type, you can select **WWN** or **Domain, Port Index**. When you select the **LSAN Zone** or **LSAN Peer Zone** as the zone type, you can select only **WWN** as members.
 - b. **Select discovered Devices/Ports** to include the discovered members in the zone, and click (➤) to move them to the **Selected Members list**.
You can also select **Enter manually**, and type the names of the offline members.
6. In case of offline peer zone or LSAN peer zone, click (⚙) to add the selected member as principal members in the zone.

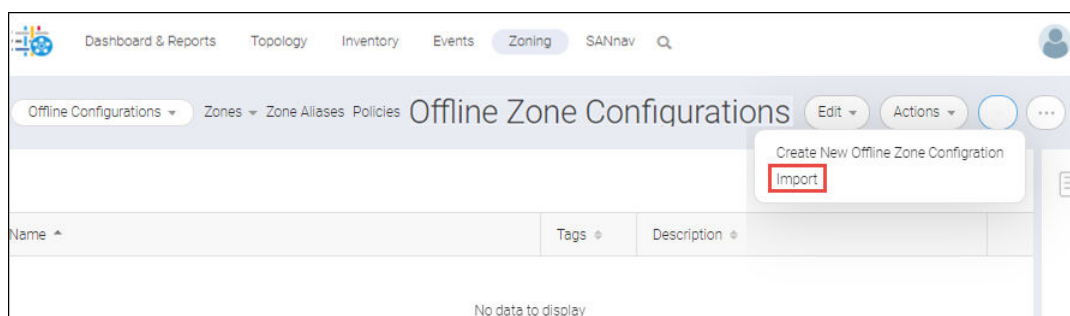
The nonselected members are present as the peer members of the principal members in the zone.

7. Click **OK** and then click **Save**.

7.4.7.2 Importing an Offline Zone Configuration

You can import a zone configuration from your local machine. To import a zone configuration from your local machine, follow the instructions below:

1. Click **Zoning** in the navigation bar, and then select **Offline Configurations** from the **Zone Configurations** dropdown.
2. Click **Select Zone DB** to select the fabric, and click **OK** to import the zone configurations and zones in the selected fabric.
3. Click the **+** icon on the top-right corner of the window, and select **Import**.



4. Browse through the folders to select the files that contain the zone and click **Open** to import the selected file to the offline zone configuration.

7.4.7.3 Exporting an Offline Zone Configuration

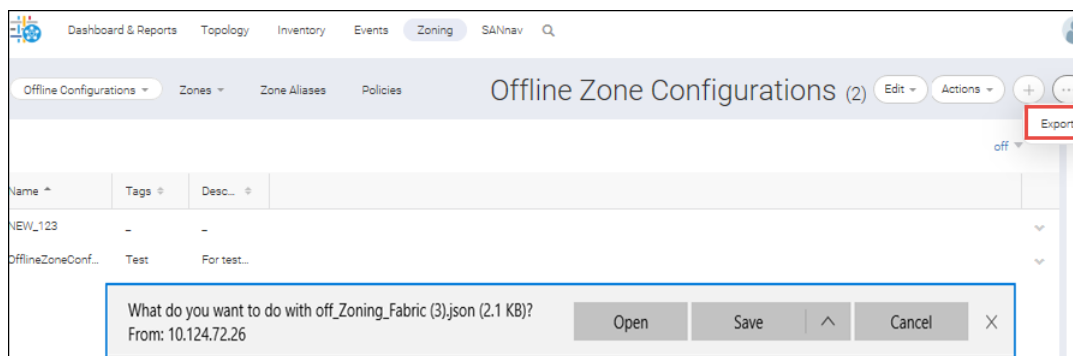
You can export a zone configuration to your local machine. To export a zone configuration to your local machine, follow the instructions below:

1. Click **Zoning** in the navigation bar, and then select **Offline Configurations** from the **Zone Configurations** dropdown.
2. Click **Select Zone DB** to select the fabric to export, and click **OK**.
3. Click the more icon (⋮), on the top-right corner of the window, and then select **Export**.

The selected zone DB is downloaded as a `.json` file to your local machine.

NOTE

The `.json` export file also contains the zone alias present in the selected fabric.



7.4.7.4 Saving the Offline Zone Database to the Switch

The Offline Zone DB helps you configure zones without affecting the active or online configurations. You can also use this data as a backup configuration. After configuring the zones offline, you can move the configured zone DB to online.

For example:

- Online configuration CFG1 (Z1) and CFG2 (Z2).
- Offline configuration CFG3 (Z3) and CFG4 (Z4).

By saving the offline configuration to online, SANnav merges both the offline and online configurations together.

- Online configuration CFG1 (Z1), CFG2 (Z2), CFG3 (Z3), and CFG4 (Z4).

If both the online and offline DB have the same configuration, SANnav replaces the online configuration with the offline DB.

To save offline configurations to the switch, follow the instructions below:

1. Click **Zoning** in the navigation bar, and then select **Offline Configurations** from the **Zone Configurations** dropdown.
2. Click **Select Zone DB** to select an offline zone DB, and click **OK**.
3. Click **Save To Switch**, and click **OK**.
4. Select the **Keep current Zone DB in offline configuration folder** checkbox if you want to retain the offline zone DB, and click **OK**.

NOTE

Offline zones cannot be deployed directly to switch. It must be associated to any zone configuration for deployment.

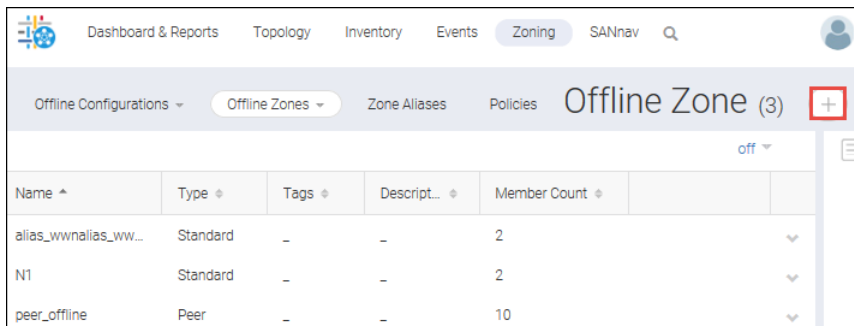
7.4.7.5 Creating Offline Zones

You can create an offline zone and work on it later without disturbing the active zones.

NOTE

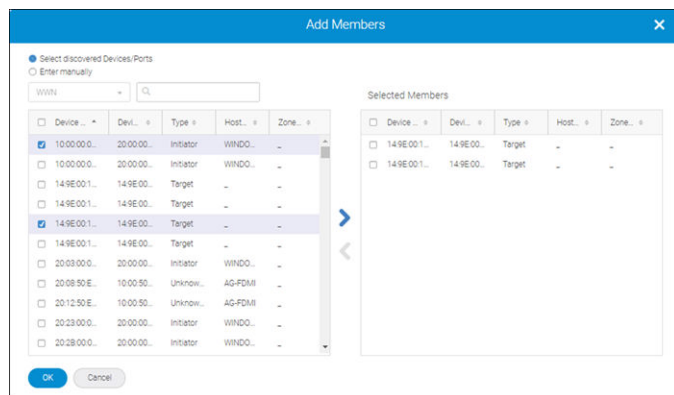
To create an offline zone or an offline zone configuration, the offline zone DB must be configured.


1. Click **Zoning** in the navigation bar, and then select **Offline Zones** from the **Zones** drop-down.
2. Select an offline zone DB, and click **OK** to create a new offline zone configuration.
3. Click the **+** icon on the top-right corner of the **Offline Zone** window.




The **Create New Zone** window displays.

4. Enter a name for the zone along with any tags and description.
5. To add an offline zone member, perform the following steps:
 - a. Select the zone type from the **Zone Type** drop-down. When you select the **Standard Zone** or **Peer Zone** as the zone type, you can select **WWN** or **Domain, Port Index**. When you select the **LSAN Zone** or **LSAN Peer Zone** as the zone type, you can add only **WWN** as members.
 - b. Click **Add** in the **Create New Zone** window.



- c. **Select discovered Devices/Ports** to include the discovered members in the zone, and click () to move them to the **Selected Members** list.


You can also select **Enter manually**, and type the names of offline members.







6. If you are adding a peer zone or an LSAN peer zone, click () to add the selected members as a principal members of the zone. The nonselected members will be present as the peer members of the principal members in the zone.

Add Members
✕

Select discovered Devices/Ports
 Enter manually

<input type="checkbox"/>	Domain...	Port...	FC A...	Switch	Zone...
<input type="checkbox"/>	1,4	port4_11	010100	FID50_A...	-
<input type="checkbox"/>	2,17	port17	020d00	sw1	-
<input type="checkbox"/>	2,21	port21	022b00	sw1	-
<input type="checkbox"/>	2,22	port22	021100	sw1	-
<input type="checkbox"/>	2,23	port23	021200	sw1	-
<input type="checkbox"/>	2,16	port16	020c00	sw1	-
<input type="checkbox"/>	2,27	port27	021600	sw1	-
<input type="checkbox"/>	2,28	port28	021700	sw1	-
<input type="checkbox"/>	2,29	port29	021800	sw1	-
<input type="checkbox"/>	2,30	port30	021900	sw1	-
<input type="checkbox"/>	2,31	port31	021a00	sw1	-

Selected Members
Click  icon to choose a Principal Member

<input type="checkbox"/>	Doma...	Port...	FC ...	Swit...	Zon...
<input type="checkbox"/>	 1,3	port3_11	010000	FID50_...	-
<input type="checkbox"/>	 2,19	port19	020f00	sw1	-
<input type="checkbox"/>	 2,20	port20	021000	sw1	-
<input type="checkbox"/>	 2,18	port18	020e00	sw1	-
<input type="checkbox"/>	 2,25	port25	021400	sw1	-
<input type="checkbox"/>	 2,26	port26	021500	sw1	-

OK
Cancel

7. Click **OK**, and then click **Save**.

7.4.8 Creating Peer Zones with a Simplified Workflow

SANnav Management Portal provides a simplified way to create peer zones by selecting hosts, host ports, and storage ports from the **Inventory** page as the principal member and then adding host ports as the peer members.

Peer zoning allows a principal device to communicate with the rest of the devices in the zone. Other nonprincipal devices (peers) in the zone can communicate with the principal device only; they cannot communicate with each other.

Typically a peer zone consists of a storage port as the principal member and multiple host ports as the peer members. When you create a peer zone using the following procedure, start by selecting the storage port. The storage port automatically becomes the principal member, and the host ports are assigned as peer members.

NOTE

Only switches with Fabric OS 8.2.0 and later allow you to create zones using this simplified workflow.

The following procedure shows how to create a typical peer zone, which consists of a single principal member (storage port) and several peer members (host ports).

1. Click **Inventory** in the navigation bar, and select **Storage Ports** from the drop-down.
2. Locate the port that you want to be the principal member of the peer zone, click the down arrow in the right-most column, and select **Create Zone** from the action menu.

Zone Ali...	WWN	FC Address	Node WWN	Connected Pt...	Connected Prod	Fabric	Concte
Alias	20:02:00:11:0D:1...	7e0e00	20:02:00:11:0D:1D:0...	port2	71.169_FID2	PM_strea	2
PM_Flow_zo...	20:02:00:11:0D:1...	7e0e0a	20:02:00:11:0D:1D:0...	port2	71.169_FID2	PM_strea	2
PM_Flow_zo...	20:03:00:11:0D:3...	7e0303	20:03:00:11:0D:3C:5...	port44	71.169_FID2	PM_strea	44
PM_Flow_zo...	20:02:00:11:0D:1...	7e0e07	20:02:00:11:0D:1D:0...	port2	71.169_FID2	PM_strea	
PM_Flow_zo...	20:02:00:11:0D:1...	7e0e0e	20:02:00:11:0D:1D:0...	port2	71.169_FID2	PM_strea	
PM_Flow_zo...	20:03:00:11:0D:3...	7e030b	20:03:00:11:0D:3C:5...	port44	71.169_FID2	PM_strea	

The **Create Zone** dialog displays a list of host ports that you can select to be peer members of the zone.

3. Select the peer members that you want to add to the zone and click the right arrow (**>**) to move them to the **Selected Members** list.

Create Zone ✕

Selected StoragePorts: 20:05:00:11:0D:C5:E4:00

Fabric_A

<input type="checkbox"/>	Name ^	Host	Fabric
<input type="checkbox"/>	10:00:00:10:9B:22:EB...	-	Fabric_A
<input type="checkbox"/>	10:00:00:10:9B:41:C5...	-	Fabric_A
<input checked="" type="checkbox"/>	10:00:00:10:9B:41:C6...	-	Fabric_A
<input checked="" type="checkbox"/>	10:00:00:10:9B:41:C6...	-	Fabric_A
<input type="checkbox"/>	10:00:00:10:9B:41:C7...	-	Fabric_A
<input type="checkbox"/>	20:01:00:10:9B:41:C5...	-	Fabric_A

Selected Members

<input type="checkbox"/>	Name ^	Host	Fabric
<input type="checkbox"/>	10:00:00:10:9B:41:C5...	-	Fabric_A
<input type="checkbox"/>	10:00:00:10:9B:41:C5...	-	Fabric_A
<input type="checkbox"/>	10:00:00:10:9B:22:EB...	-	Fabric_A

Zone Name

Save
Cancel

4. Type a name in the **Zone Name** field, and click **Save**.
Click **OK** in the confirmation dialog.


NOTE

On clicking **OK** button, SANnav creates a new zone, and add it to the current active configuration, and activate it immediately. If there is no active configuration, it creates a new zone configuration and activate it.

You can verify that the new zone is active from the **Zone Configurations** page.

The screenshot shows the SANnav Zoning configuration page for 'ALL_IT_Zone_fid2_zone_config'. The page includes a navigation bar with 'Dashboard & Reports', 'Topology', 'Inventory', 'Events', 'Zoning', and 'SANnav'. Below the navigation bar, there are tabs for 'Zone Configurations', 'Zones', 'Zone Aliases', and 'Policies'. The main content area shows the configuration details for the selected zone, including 'Name' (ALL_IT_Zone_fid2_zone_config), 'Description', 'Tags', and 'Fabric' (PM_streaming_1). Below this, there is a table titled 'Zones' with 4 items. The table has columns for 'Name', 'Type', and 'Member Count'. The 'PeerZone_1' row is highlighted, indicating it is the selected zone member. The table also includes 'Add' and 'Remove' buttons. At the bottom, there are 'Save' and 'Cancel' buttons.

Name	Type	Member Count
ALL_IT_Zone_fid2_zone	Standard	1
PeerZone_1	Peer	2
test_34	Standard	1

The zone details page shows the zone members. The target member (the storage port) is the principal member, as indicated by the colored icon (). The initiator members (host ports) are the peer members.

The screenshot shows the SANnav Zoning configuration page for 'PeerZone_1'. The page includes a navigation bar with 'Dashboard & Reports', 'Topology', 'Inventory', 'Events', 'Zoning', and 'SANnav'. Below the navigation bar, there are tabs for 'Zone Configurations', 'Zones', 'Zone Aliases', and 'Policies'. The main content area shows the configuration details for the selected zone, including 'Name' (PeerZone_1), 'Description', 'Tags', 'Zone Type' (Peer), and 'Fabric' (PM_streaming_1). Below this, there is a table titled 'Members' with 2 items. The table has columns for 'Zone Alias', 'Member Count', 'Type', 'WWN', 'Zone Alias', 'Type', 'FC A...', and 'Host/Stor'. The 'Target' row is highlighted, indicating it is the principal member. The table also includes 'Add' and 'Remove' buttons. At the bottom, there are 'Save', 'Del', and 'Cancel' buttons.

Zone Alias	Member Count	Type	WWN	Zone Alias	Type	FC A...	Host/Stor
-	-	-	20:03:00:11:0D:...	-	Target	7d0704	-
-	-	-	10:00:00:05:1E:...	ALL_IT_Zone_fi...	Initiator	7d0500	BRM105C

NOTE

You can edit the existing zone configuration by using the **Save As** option from the **Save** drop-down..

7.4.9 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 switch model. The default setting is All Access.

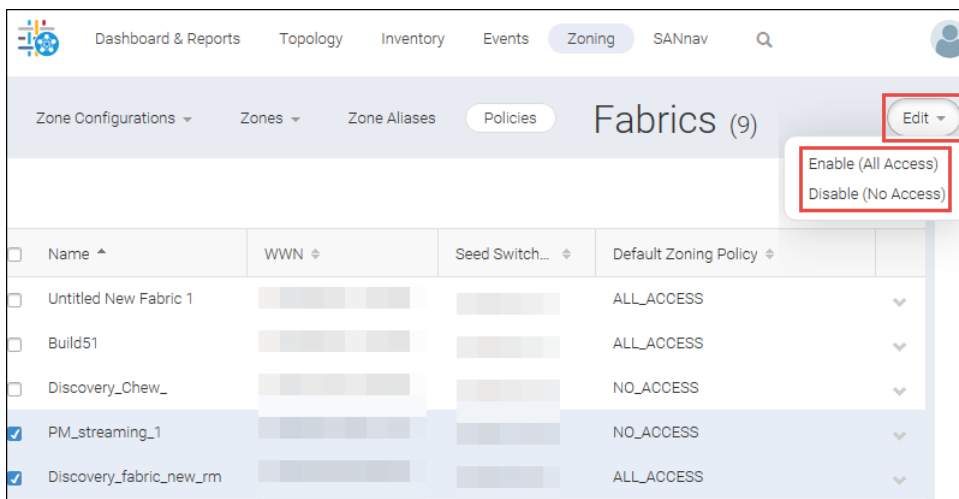
Typically, when you disable the zoning configuration in a large fabric with thousands of devices, the name server indicates to all hosts that they can communicate with each other. Each host can receive an enormous list of PIDs and ultimately cause other hosts to run out of memory or crash. To ensure 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 should be set to No Access. You cannot deactivate the active configuration if the default zone policy is All Access and you have more than 120 devices in the fabric.

To modify the fabric policies, follow the instructions below:

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 **Edit** drop-down, and select **Enable** or **Disable**.

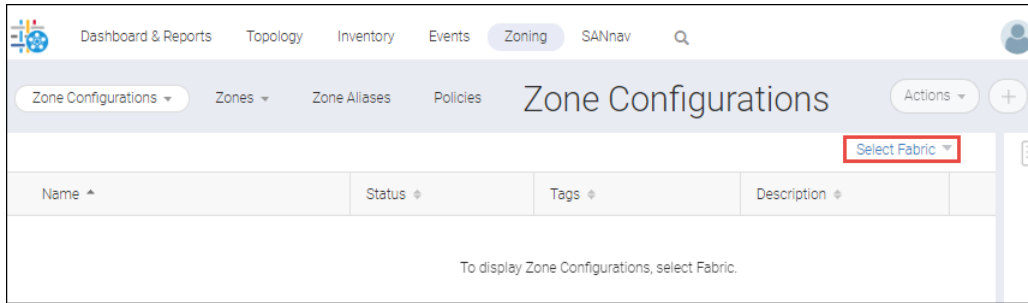


Alternatively, you can change the policy for a single fabric by selecting NO_ACCESS or ALL_ACCESS from the action menu for that fabric.

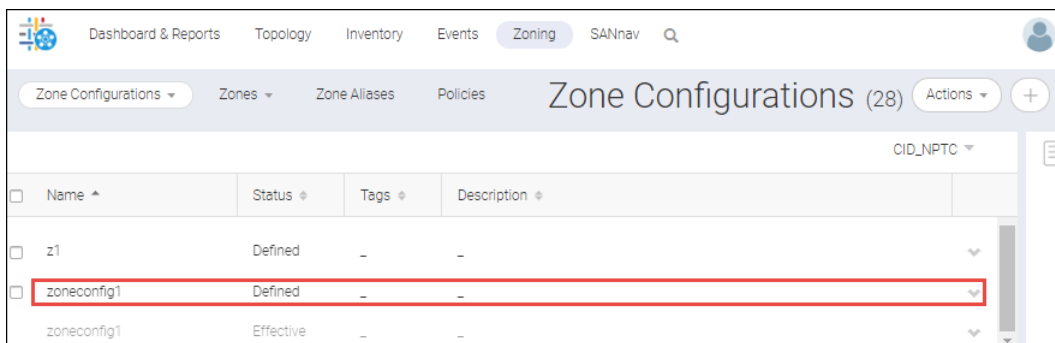
7.4.10 Modifying a Zone Configuration

To modify a zone configuration, perform the following steps:

1. Click **Zoning** in the navigation bar. The **Zone Configurations** window displays.

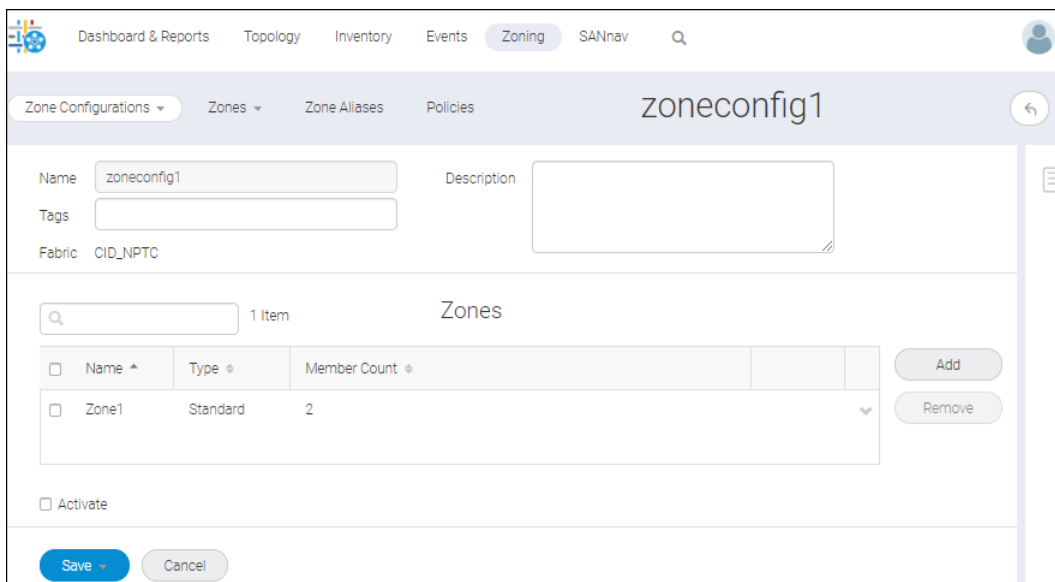


2. Select the fabric from the **Select Fabric** drop-down, and then click **OK**.
The zone configurations display in the **Zone Configurations** window.



3. To modify a zone configuration, select the desired zone configuration with the **Defined** status. You cannot modify the zone configuration with the **Effective** status.

The selected zone displays. Modify (add, remove, or both) as required.



- To add a zone, click the **Add** button, select the desired 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.
4. Click the **Save** button, and then click either **Save** or **Save As** if you want to save the configuration with a different name
 5. Click **OK** in the confirmation dialog to save the changes.

The modified zone configuration can be viewed under the **Zone Configurations** window with the **Defined (Modified)** status.

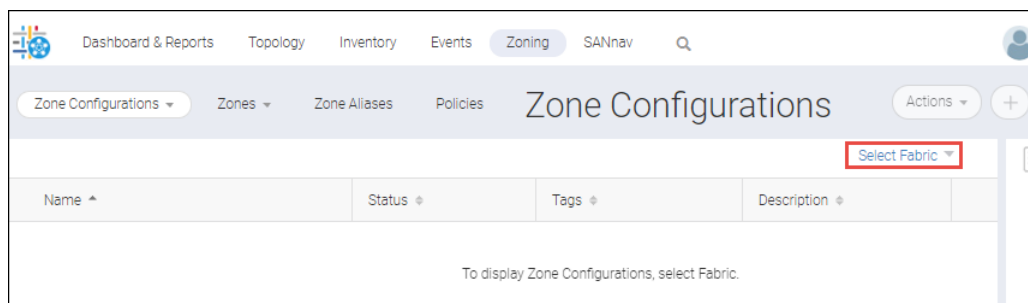
Name	Status	Tags	Description
FAB_A	Defined	-	-
Test_Config1	Defined	-	-
z1	Defined	-	-
zoneconfig1	Defined (Modified)	-	-
zoneconfig1	Effective	-	-

7.4.11 Comparing Effective and Defined (Modified) Zone Configurations

The compare zone configurations feature supports comparing the configuration between the effective and the defined (modified) zones.

To compare the configuration between the effective and the defined (modified) zones, perform the following steps:

1. Click **Zoning** in the navigation bar. The **Zone Configurations** window displays.



2. Select the fabric that you want to import from the **Select Fabric** drop-down, and then click **OK**.
The modified zone configurations appear in the **Zone Configurations** window with the **Defined (Modified)** status.
3. Select the **Compare** option for the modified zone. The **Compare** option is visible only when there is a modification in the effective zone configuration and the defined copy of the effective zone configuration.

Name	Status	Tags	Description
Test_Config1	Defined	-	-
z1	Defined	-	-
zoneconfig1	Defined (Modified)	-	-
zoneconfig1	Effective	-	-

The **Compare** window appears. The left panel of the **Compare** window displays the configuration of the effective zone. The right panel of the **Compare** window displays the configuration of the defined (modified) zone.

The differences between two configurations can be viewed in the form of **Deleted**, **Inserted**, **Modified**, and **Empty**. You can use either of the following options to view the configuration differences:

- **Side By Side**
- **Inline**

NOTE

The **Show Differences Only** option is used only to view the differences between the effective and defined (modified) zone configurations.

- Select the **Side By Side** option to compare the zones side by side. By default, the **Side By Side** option is selected.

Compare ✕

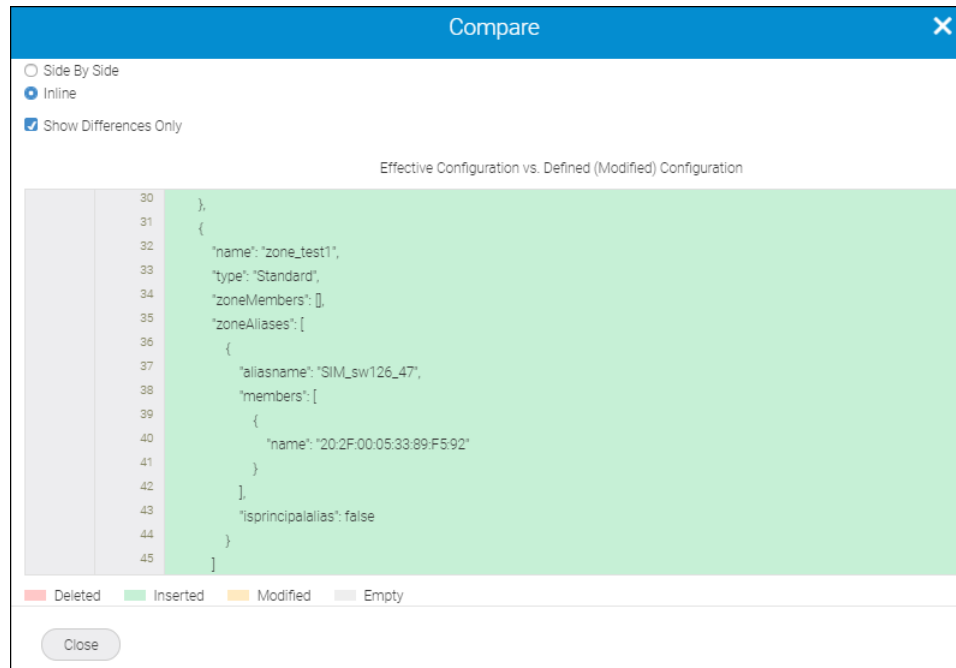
Side By Side
 Inline
 Show Differences Only

Effective Configuration	Defined (Modified) Configuration
<pre> 30 }, 31 { 32 "name": "zone_test1", 33 "type": "Standard", 34 "zoneMembers": [], 35 "zoneAliases": [36 { 37 "aliasname": "SIM_sw126_47", 38 "members": [39 { 40 "name": "20:2F:00:05:33:89:F592" 41 } 42], 43 "isprincipalalias": false 44 } 45] </pre>	<pre> 30 }, 31 { 32 "name": "zone_test1", 33 "type": "Standard", 34 "zoneMembers": [], 35 "zoneAliases": [36 { 37 "aliasname": "SIM_sw126_47", 38 "members": [39 { 40 "name": "20:2F:00:05:33:89:F592" 41 } 42], 43 "isprincipalalias": false 44 } 45] </pre>

■ Deleted ■ Inserted ■ Modified ■ Empty

Close

- Select the **Inline** option to view the changes inline.



7.4.12 Viewing Zone and Zone Configuration Details

7.4.12.1 Viewing Online or Offline Zone Details

You can view the following details on the same page:

- 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, follow steps below:

1. Click **Zoning** in the navigation bar, and then select **Zones** from the **Zones** drop-down. The **Zones** window displays.
2. Select a fabric from the **Select Fabric** option, and then click **OK**.
A list of zones for the selected fabric displays.
3. Select the **Show Details** option for an individual zone from the action drop-down.

Dashboard & Reports Topology Inventory Events Zoning SANnav

Zone Configurations Zones Zone Aliases Policies Zones (87)

Zoning_Fabric

Name	Type	Tags	Description	Member Co...	Zone Configuration
2_wnn_zone	Standard	-	-	3	CFG_ALL,CFG_Physical;
aa_zone_direct_member	Standard	-	-	2	CFG_AI
add_to_zone_peer	Peer	-	add_to_zone_peer	1	CFG_1;
add_to_zone_standard	Standard	-	add_to_zone_standard	2	CFG_12,CFG_ALL
aftr_mig	Peer	-	-	127	CFG_ALL,migration_test

The **Zone Details** window displays and shows the list of zones present in the fabric.

- To view the list of zone aliases present in a particular zone, select a zone from the **Zones** list.

Zone Details

Zones		Members		
Zone Name	Type	Zone Alias	WWN	Dom...
2_wnn_zone	Standard	123tear_1	-	-
aa_zone_direct_mem...	Standard	123tear_2	-	-
add_to_zone_peer	Peer	w	-	-
add_to_zone_standard	Standard			
aftr_mig	Peer			
Alias_last_member	Standard			

Close


The list of configured zone aliases within the zone displays in the **Members** list.

- To view any alias members present in the zone alias, select the zone alias name from the **Members** list.

Zone Details					
Zones		Members			
Zone Name ^	Type ^	Zone Alias ^	WWN ^	Domain, P... ^	Alias Member
2_wwn_zone	Standard	123tear_1	-	-	23:91:8C:7C:FF:32:0B:80
aa_zone_direct_member	Standard	123tear_2	-	-	21:11:8C:7C:FF:32:0B:80
add_to_zone_peer	Peer	w	-	-	20:EC:8C:7C:FF:32:0B:80
add_to_zone_standard	Standard				
aftr_mig	Peer				

The list of alias members displays in the **Members** list.

NOTE

The principal members in a peer zone are highlighted with the () symbol.

- You can also view the details about the zones that are present in the online and offline zone configurations. You can view the details about a zone that is present in a zone configuration by selecting the zone configuration, and then selecting the **Show Details** option from the action drop-down for that zone.

NOTE

The zone details can be viewed both for effective and defined zone configurations.

- If you want to view details about the offline zones, select **Offline Zones** from the **Zones** drop-down, and then select the zone DB from the **Select Zone DB** drop-down.

The **Offline Zone** window displays. You can view the details for all offline zones by selecting the **Show Details** option from the action drop-down for that offline zone.

7.4.12.2 Viewing Online or Offline Zone Configuration Details

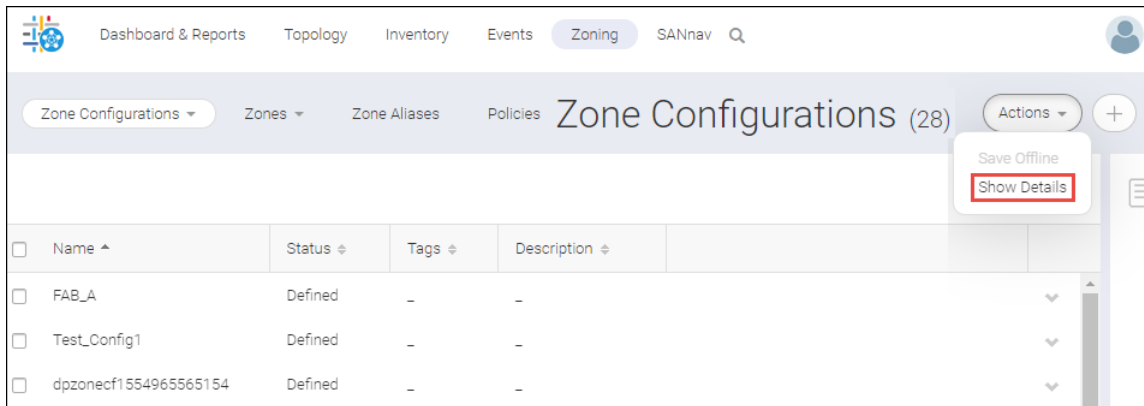
You can view the following details on the same page:

- 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.

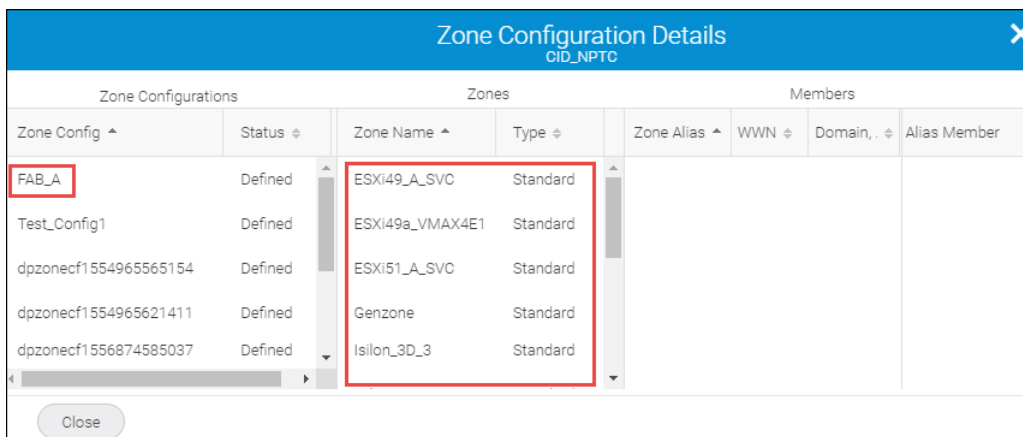
To view the details about zone configurations, follow the steps below:

- Click **Zoning** in the navigation bar. The **Zone Configurations** window displays.
- Select a fabric from the **Select Fabric** option, and then click **OK**.
A list of zone configurations for the selected fabric displays.
- Select the **Show Details** option from the **Actions** drop-down.



The **Zone Configuration Details** window displays and shows the list of configured zones present in the fabric.

- To view the list of zones present in a particular zone configuration, select a zone configuration from the **Zone Configurations** list.



The list of configured zones within the zone configuration displays in the **Zones** list.

- To view the zone aliases present in a zone, select a zone from the **Zones** list.

Zone Configuration Details CID_NPTC							
Zone Configurations		Zones		Members			
Zone Config	Status	Zone Name	Type	Zone Ali...	WWN	Domai...	Alias Member
FAB_A	Defined	ESXi49_A_SVC	Standard	-	50:05:07:68:...	-	
Test_Config1	Defined	ESXi49a_VMA...	Standard	-	50:05:07:68:...	-	
dpzonecf1554...	Defined	ESXi51_A_SVC	Standard	-	50:05:07:68:...	-	
dpzonecf1554...	Defined	Genzone	Standard	-	50:05:07:68:...	-	
dpzonecf1554...	Defined	HUR_1	Standard	-	50:05:07:68:...	-	
dpzonecf1555...	Defined	Isilon_3D_1	Standard	-	50:05:07:68:...	-	
dpzonecf1555...	Defined	Isilon_3D_2	Standard	-	50:05:07:68:...	-	
dpzonecf1556...	Defined	Isilon_3D_3	Standard	-	50:05:07:68:...	-	
				ESXi49_A	-	-	


The list of zone aliases within the zone displays in the **Members** list.

- To view any alias members present in the zone alias, select the zone alias name from the **Members** list.

Zone Configuration Details CID_NPTC							
Zone Configurations		Zones		Members			
Zone C...	Status	Zone Na...	Type	Zone ...	WWN	Dom...	Alias Member
FAB_A	Defined	ESXi49_A_S...	Standard	-	50:05:07:6...	-	10:00:8C:7C:FF:3A:BF:80
Test_Confi...	Defined	ESXi49a_VM...	Standard	-	50:05:07:6...	-	
dpzonecf1...	Defined	ESXi51_A_S...	Standard	-	50:05:07:6...	-	
dpzonecf1...	Defined	Genzone	Standard	-	50:05:07:6...	-	
dpzonecf1...	Defined	HUR_1	Standard	-	50:05:07:6...	-	
dpzonecf1...	Defined	Isilon_3D_1	Standard	-	50:05:07:6...	-	
dpzonecf1...	Defined	Isilon_3D_2	Standard	-	50:05:07:6...	-	
dpzonecf1...	Defined	Isilon_3D_3	Standard	-	50:05:07:6...	-	
				ESXi49_A	-	-	

The list of alias members displays in the **Members** list.

NOTE

The principal members in a peer zone are highlighted with the () symbol.

You can also view details for a single zone configuration by selecting **Show Details** from the action menu for that configuration.

7. If you want to view details about the offline zone configurations, select **Offline Configurations** from the **Zone Configurations** drop-down, and then select the zone DB from the **Select Zone DB** drop-down.

The **Offline Zone Configurations** window displays. You can view the details for all offline zone configurations by selecting the **Show Details** option from the **Actions** drop-down. You can also view details for a single offline zone configuration by selecting **Show Details** from the action menu for that configuration.

7.5 Virtual Fabrics

Virtual Fabrics is an architecture to virtualize hardware boundaries.

Traditionally, the designing and managing of a SAN are performed at the granularity of a physical switch. With the Virtual Fabrics architecture, the designing and managing of a SAN are performed at the granularity of a port. Virtual Fabrics consists of the following two features, which can be customized based on your requirements.

- Logical switch
- Logical fabric

For more information on Virtual Fabrics, refer to the *Brocade Fabric OS Administration Guide*.

Logical Switch

Traditionally, each switch and all ports in the switch act as a single Fibre Channel (FC) switch that participates in a single fabric. The logical switch feature allows you to divide a physical chassis into multiple fabric elements. Each of these fabric elements is referred to as a logical switch. Each logical switch functions as an independent, self-contained FC switch.

Logical switches consist of one or more ports that act as a single FC switch. The logical switches can connect to physical switches or to other logical switches in a different chassis.

The Virtual Fabrics mode on the switch is enabled by default, which creates a single logical switch in the physical chassis. This logical switch is called the default logical switch.

NOTE

When the Virtual Fabrics feature is enabled, you can create up to 16 logical switches depending on the switch model.

Logical Fabric

A logical fabric is a fabric that contains at least one logical switch. Using logical fabrics, you can divide one physical chassis into multiple logical switches, which can be managed by separate administrators.

The following are the benefits of using logical fabrics:

- Enables viewing your entire SAN (both physical and virtual) at a glance.
- Enables managing a logical switch in the same way that you manage a physical switch, so that fewer physical chassis are required for deployment.
- Enables the using of a logical switch for discovery and eliminates the requirement of one physical chassis for each fabric.
- Enables managing multiple logical-fabric-capable physical chassis from the same interface.
- Provides logical isolation of data, control, and management paths at the port level.
- Enables better use of switches for different ports in different switches to be consolidated.
- Enables scalability benefits of dividing the physical network into isolated fabrics where any error condition within a fabric is limited to the boundary of the fabric only.
- Enables the departmental mode of managing fabrics, in which the physical network can be managed by one department and the fabrics can be managed by other departments.

The **Logical Fabrics** tab displays only fabrics in which VF is enabled and HIF is disabled.

NOTE

In case of any update to the switch, the update occurs to SANnav in the next data collection and the fabric is displayed accordingly.

7.5.1 Supported Platforms for Virtual Fabrics

NOTE

SANnav supports switches and directors with Fabric OS version 7.4.0 and later.

The following table lists the platforms that support Virtual Fabrics.

Table 20: Platforms That Support Virtual Fabrics

Platforms	Directors (16Gb/s)	Switches (16Gb/s)	Directors (32Gb/s)	Switches (32Gb/s)
Gen 6	N/A	N/A	Brocade X6-4 Brocade X6-8	Brocade G620 Brocade G630
Gen 5	Brocade DCX 8510-4 Brocade DCX 8510-8	Brocade 6510 Brocade 6520 Brocade 7840 Extension	N/A	N/A

The Virtual Fabrics feature is not supported by the following platforms:

- Gen 5 (16Gb/s) Switches
 - Brocade 6505
- Gen 6 (32Gb/s) Switches
 - Brocade G610
 - Brocade 7810 Extension

The following table lists the maximum number of logical fabrics supported by the various platforms.

Table 21: Number of Logical Fabrics Supported by the Various Platforms

Platforms	Directors (Fabric OS 8.1.0 and Later)	Switches (Fabric OS 8.1.0 and Later)	Directors (Prior to Fabric OS 8.1.0)	Switches (Prior to Fabric OS 8.1.0)
Gen 6	16	4	8	4
Gen 5	8	4	8	4

7.5.2 Creating a Logical Fabric

This procedure creates an empty logical fabric. You can add logical switches to the fabric now or later. A fabric must be created with at least one VF-enabled switch.

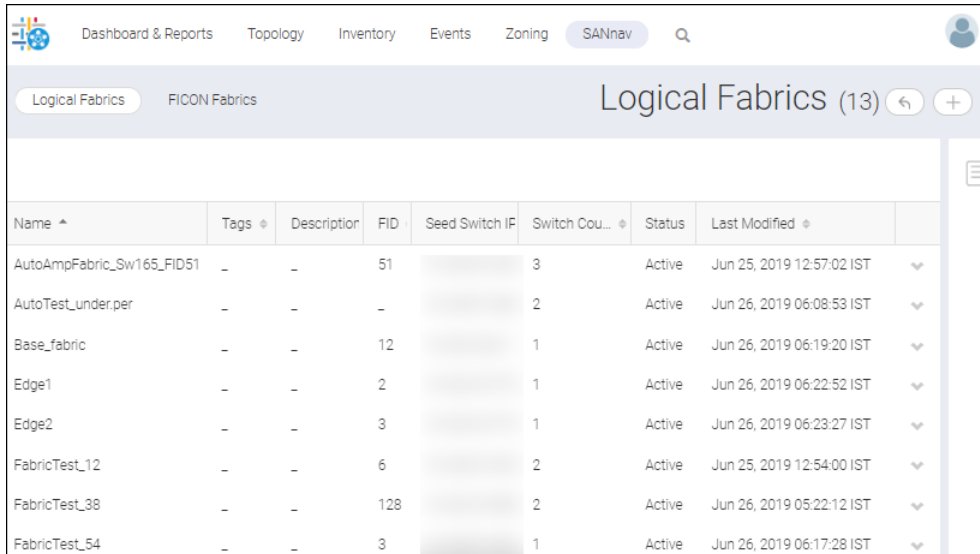
To create a logical fabric, you must have Logical Switch Configuration privilege with read-write permission.

NOTE

- A fabric can be created with a VF-disabled switch, but it becomes VF-enabled switch during the create operation. Only fabric properties and the domain ID can be edited.
- A fabric cannot be created with an AMP. Only fabric properties can be edited. An FID change on the fabric does not reflect on an AMP.
- A fabric cannot be created with a default switch. You can edit fabric properties, the domain ID, and ports to the fabric. However, port removal from the default FID is not supported.

To create a logical fabric, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**.
The **Logical Fabrics** window is displayed.
2. Click the (+) icon on the top-right corner of the window to create a new logical fabric.



Name ^	Tags	Description	FID	Seed Switch IP	Switch Cou...	Status	Last Modified
AutoAmpFabric_Sw165_FID51	-	-	51		3	Active	Jun 25, 2019 12:57:02 IST
AutoTest_under.per	-	-	-		2	Active	Jun 26, 2019 06:08:53 IST
Base_fabric	-	-	12		1	Active	Jun 26, 2019 06:19:20 IST
Edge1	-	-	2		1	Active	Jun 26, 2019 06:22:52 IST
Edge2	-	-	3		1	Active	Jun 26, 2019 06:23:27 IST
FabricTest_12	-	-	6		2	Active	Jun 25, 2019 12:54:00 IST
FabricTest_38	-	-	128		2	Active	Jun 26, 2019 05:22:12 IST
FabricTest_54	-	-	3		1	Active	Jun 26, 2019 06:17:28 IST

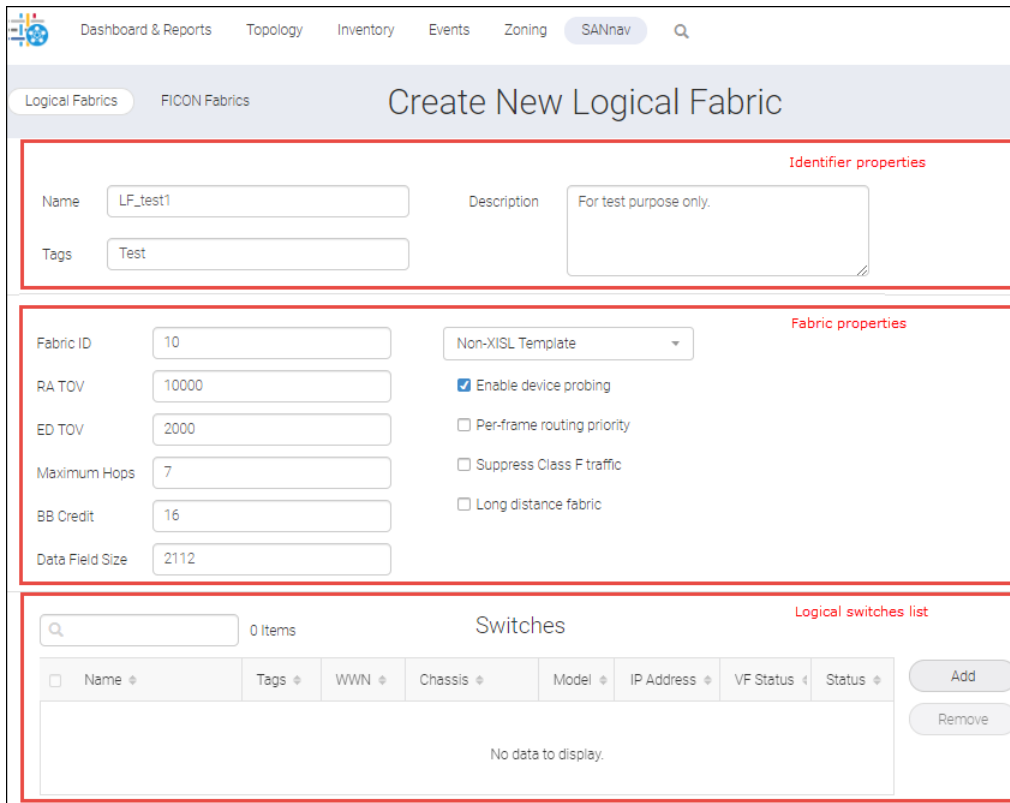
The **Create New Logical Fabric** window is displayed. The **Create New Logical Fabric** window is used to create a logical switch template. This logical switch template can be deployed across multiple physical chassis if those chassis are capable of supporting it. When the logical switch is created, the switch is discovered automatically.

NOTE

All logical switches are discovered if they are connected with each other. If they are not interconnected, only one logical switch is discovered.

The **Create New Logical Fabric** window consists of following three components.

- Identifier properties
- Fabric properties
- Logical switch list



Dashboard & Reports Topology Inventory Events Zoning SANnav

Logical Fabrics FICON Fabrics

Create New Logical Fabric

Identifier properties

Name: LF_test1
 Tags: Test
 Description: For test purpose only.

Fabric properties

Fabric ID: 10
 RA TOV: 10000
 ED TOV: 2000
 Maximum Hops: 7
 BB Credit: 16
 Data Field Size: 2112

Non-XISL Template
 Enable device probing
 Per-frame routing priority
 Suppress Class F traffic
 Long distance fabric

Logical switches list

0 Items

Name	Tags	WWN	Chassis	Model	IP Address	VF Status	Status
No data to display.							

Add
Remove

3. Enter a name for the logical fabric along with tags and a description in the identifier properties section.
4. To define fabric properties, perform the following steps:
 - a. Enter the unique identification for the fabric in the **Fabric ID** field.
 - b. Select any of the following templates from the drop-down.
 - Base Switch Template
 - XISL Template
 - Non-XISL Template

NOTE

Based on the selected template, the properties to be configured are displayed.

For more information on template configuration, see [Fabric Properties for Logical Fabrics](#).

NOTE

Do not change the default values of the **RA TOV**, **ED TOV**, **Maximum Hops**, **BB Credit**, and **Data Field Size** fields unless it is directed by your switch service provider.

5. Click **Save**. The newly created logical fabric can be viewed under the **Logical Fabrics** tab.

Name ^	Tags ^	Descr...	FID ^	Seed Switch IP Addr... ^	Switch Co...	Status ^	Last Modified ^
FabricTest_12	-	-	6	10.124.72.165	2	Active	Jun 25, 2019 12:54:00 IST
FabricTest_38	-	-	128	10.102.18.188	2	Active	Jun 26, 2019 05:22:12 IST
FabricTest_54	-	-	3	10.124.72.165	1	Active	Jun 26, 2019 06:17:28 IST
LF_test1	Test	For test	10	-	0	Inactive	Jun 26, 2019 09:34:36 IST

7.5.3 Adding Logical Switches to a Logical Fabric

To add a logical fabric, you must have Logical Switch Configuration privilege with read-write permission.

To add a logical switch to a logical fabric, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**. The **Logical Fabrics** window is displayed.
2. Click the logical fabric where you want to add the logical switch.

Name ^	Tags ^	Descr...	FID ^	Seed Switch IP Addr... ^	Switch Co...	Status ^	Last Modified ^
FabricTest_12	-	-	6		2	Active	Jun 25, 2019 12:54:00 IST
FabricTest_38	-	-	128		2	Active	Jun 26, 2019 05:22:12 IST
FabricTest_54	-	-	3		1	Active	Jun 26, 2019 06:17:28 IST
LF_test1	Test	For test	10	-	0	Inactive	Jun 26, 2019 09:34:36 IST

The selected logical fabric appears.

3. Click the **Add** button from the **Switches** table.

0 Items

Switches

<input type="checkbox"/>	Name ^	Tags ^	WWN ^	Chassis ^	Model ^	IP Address ^	VF Status ^	Status ^
No data to display.								

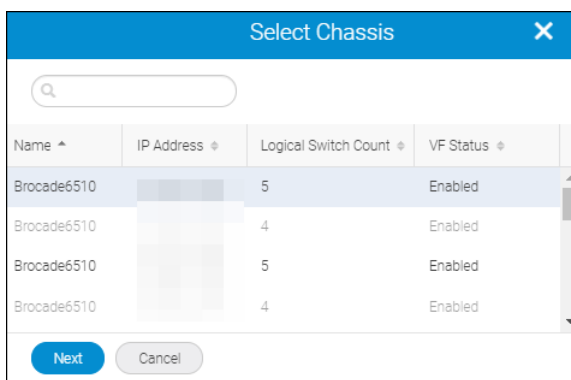
Activate

The **Select Chassis** window is displayed. The **Select Chassis** window displays all Virtual Fabrics-capable switches. You can select one switch at a time to select the required ports to create the logical switch. If the selected switch is not Virtual Fabrics-enabled, you can see the confirmation message upon enabling the virtual fabric after clicking the **Save** button. The **Logical Switch Count** column in the **Select Chassis** window displays the switch count per chassis.

4. Select the chassis to which the logical switch is added.

NOTE

- The chassis is greyed out when it reaches the maximum logical switch count.
- The chassis does not appear under the following conditions:
 - When the selected fabric ID is already present on the discovered logical fabric.
 - When the base switch template is selected and you are trying to select a chassis where the base switch is already configured.



5. Click **Next**. The **Add Logical Switch** window appears.
6. Enter the logical switch name and the domain ID, and select at least one port to create the logical switch.

7. Select the **Insistent** checkbox to enable the insistent domain ID.
8. Select the required area limit from the **Area Limit** drop-down.

The options are as follows:

- **Disable 256 limit (00 – FFC0)**
This option enables 10-bit addressing. This addressing scheme supports a large number of F_Ports.
- **Zero Based Assignment**
Unique area assignments begin at zero regardless of where the port is physically located. When a port is assigned to a logical switch, the next free port identifier (PID) starting from 0x00 is assigned.
- **Port Based Assignment**

- Unique area assignments are based on the port index. This mode is compatible with domain-index zoning.
- This option is not supported on the default logical switch.

For detailed information on the area limit, refer to the *Brocade Fabric OS Administration Guide*.

9. Select the ports that you want to add from the **Available Ports** list and then click (>) to move the ports to the **Selected Ports** list.

NOTE

- Initially, all ports belong to the default logical switch. When you create additional logical switches, they are empty and you must assign ports to those logical switches.
- A given port can be used in only one logical switch. The ports that are not assigned to the newly created logical switch remain in the default switch.

10. Click **Next**.

The **Add Logical Switch** window is displayed with different operations.

For detailed information on the different operations, refer to the *Fabric OS Command Reference Manual*.

The following table lists the address binding properties and the switch types.

Table 22: Address Binding Properties

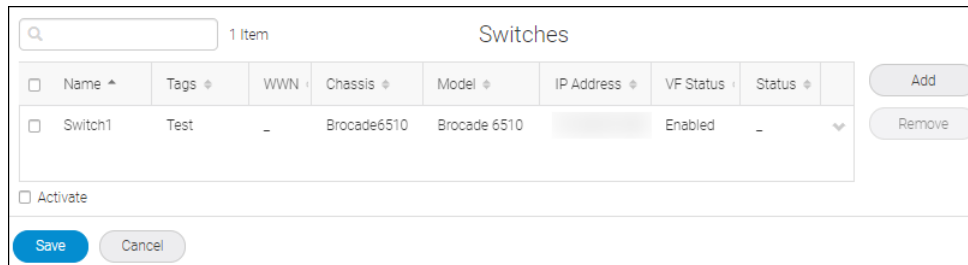
Chassis Type	Template	256 Disable Limit		Zero Based		Port Based	
		Auto Bind	Manual Bind (Starting Area)	Auto Bind	Manual Bind (Starting Area)	Auto Bind	Manual Bind (Starting Area)
Switches	Base Switch Template	Yes	—	—	—	—	—
	XISL Template	Yes	—	—	—	—	—
	Non-XISL Template	Yes	—	—	—	—	—

Table 22: Address Binding Properties (Continued)

Directors	Base Switch Template	Yes	7000-FFC0	Yes	00-FF	Yes	—
	XISL Template	Yes	7000-FFC0	Yes	00-FF	Yes	—
	Non-XISL Template	Yes	7000-FFC0	Yes	00-FF	Yes	—

11. Click **OK**.

The logical switch is created and can be viewed under **Switches** option.



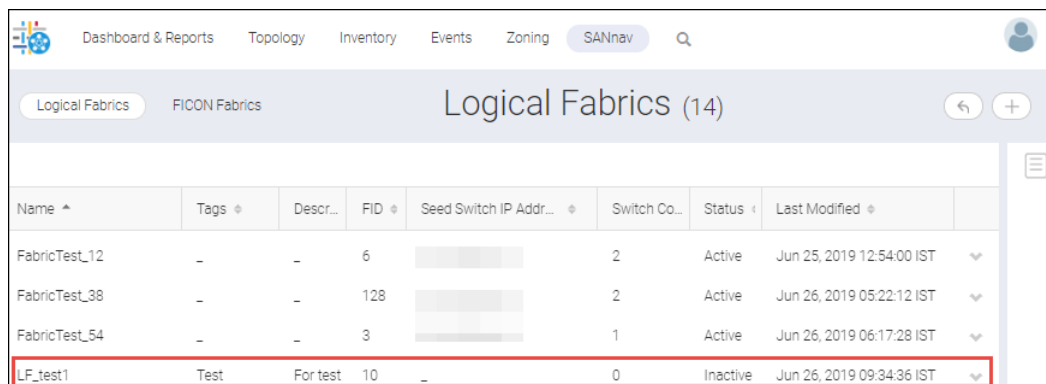
12. Click **Save** to add the logical switch to the logical fabric.

7.5.4 Activating a Logical Fabric

To activate a logical fabric, you must have Logical Switch Configuration privilege with read-write permission.

To activate the logical fabric, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**. The **Logical Fabrics** window is displayed.
2. Click the logical fabric that you want to activate.



The selected logical fabric appears.

3. Select the switch from the **Switches** table and select the **Activate** checkbox.

Name	Tags	WWN	Chassis	Model	IP Address	VF Status	Status
Switch1	Test	-	Brocade6510	Brocade 6510	[redacted]	Enabled	-

- Click **Save** to deploy the configuration, and then click **OK** in the confirmation dialog. On successful configuration of the logical fabric, the confirmation message appears in the **Save** window.
- Click **Done**.
The logical fabric is activated with the **Active** status.

Name	Tags	Description	FID	Seed Switch IP Ad	Switch C	Status	Last Modified
bulkports,test	-	-	25	[redacted]	1	Active	Jun 26, 2019 11:07:09 IST
Fab81 *	-	-	128	[redacted]	4	Active	Jun 27, 2019 14:46:07 IST
LF_test1	-	-	10	[redacted]	1	Active	Jun 27, 2019 15:16:41 IST

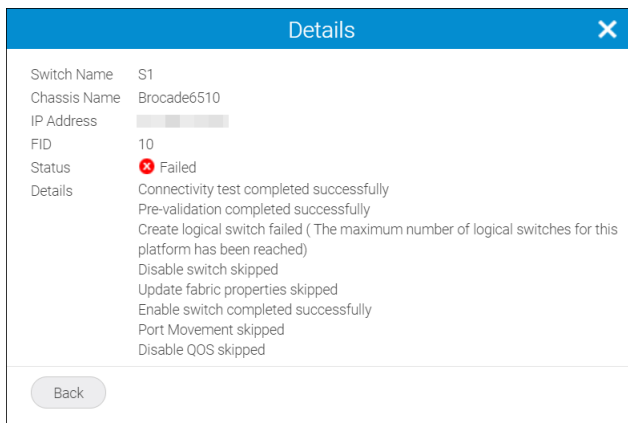
In case of failure, the **Save** popup appears automatically after the deployment process is completed.

Save

Failed to save logical fabric. Failed to Create logical switch on the switch [redacted]

Close Show Details

Click **Show Details** option to view the details of the logical fabric. The **Details** message displays the error messages while deploying the logical switches.



7.5.5 Editing Logical Fabrics and Switches

To edit a logical fabric, you must have Logical Switch Configuration privilege with read-write permission.

NOTE

- The fabric name, description, and tags cannot be edited for an active logical fabric. If you want to change these properties, you can do so from the **Inventory** page.
- In case of fabric ID (FID) update, the new switch with the new FID is not discovered automatically. You must delete the logical fabric and add it back to reflect the updated data.
- The edit fabric operation is not allowed in the following conditions:
 - All fabric properties are not collected.
 - The fabric is not manageable.

7.5.5.1 Editing a Logical Fabric

To edit a logical fabric, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**.
The **Logical Fabrics** window is displayed.
2. Click the name of the logical fabric that you want to edit.

Name ^	Tags *	Descr...	FID *	Seed Switch IP Addr... *	Switch Co...	Status †	Last Modified *
FabricTest_12	-	-	6	10.124.72.165	2	Active	Jun 25, 2019 12:54:00 IST
FabricTest_38	-	-	128	10.102.18.188	2	Active	Jun 26, 2019 05:22:12 IST
FabricTest_54	-	-	3	10.124.72.165	1	Active	Jun 26, 2019 06:17:28 IST
LF_test1	Test	For test	10	-	0	Inactive	Jun 26, 2019 09:34:36 IST

The selected logical fabric appears.

3. Modify the values to edit the logical fabric.

NOTE

Do not change the default values of **RA TOV**, **ED TOV**, **Maximum Hops**, **BB Credit**, and **Data Field Size** unless it is directed by your switch service provider.

The screenshot displays the SANnav interface for editing a logical fabric. The top navigation bar includes 'SANnav' and a search icon. The main header shows 'Logical Fabrics' and 'FICON Fabrics' tabs, with the current fabric named 'LF_test_1'. The configuration form includes:

- Name:** LF_test_2
- Description:** (empty text area)
- Tags:** (empty text area)
- Fabric ID:** 25
- RA TOV:** 10000
- ED TOV:** 2000
- Maximum Hops:** 7
- BB Credit:** 16
- Data Field Size:** 2112
- Template:** Non-XISL Template
- Options:**
 - Enable device probing
 - Per-frame routing priority
 - Suppress Class F traffic
 - Long distance fabric

Below the configuration is a 'Switches' table with 0 items. The table has columns: Name, Tags, WWN, Chassis, Model, IP Address, VF Status, and Status. There are 'Add' and 'Remove' buttons for the table. At the bottom, there are 'Save', 'Delete', and 'Cancel' buttons.

4. Click **Save**.

The modified logical fabric is displayed under **Logical Fabrics** tab.

7.5.5.2 Editing a Logical Switch

NOTE

- The **Activate** checkbox is selected and greyed out. During the edit operation, you cannot save the configuration only to the database. The configurations are saved to the database and pushed to the switch.
- The **Configure** option is disabled for the un-monitor, maintenance mode, unreachable, or authentication failure switches.

To edit a logical switch, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**. The **Logical Fabrics** window is displayed.
2. Click the name of the logical fabric containing the switch that you want to edit.

Name ^	Tags ^	Descr...	FID ^	Seed Switch IP Addr... ^	Switch Co...	Status ^	Last Modified ^
FabricTest_12	-	-	6	10.124.72.165	2	Active	Jun 25, 2019 12:54:00 IST
FabricTest_38	-	-	128	10.102.18.188	2	Active	Jun 26, 2019 05:22:12 IST
FabricTest_54	-	-	3	10.124.72.165	1	Active	Jun 26, 2019 06:17:28 IST
LF_test1	Test	For test	10	-	0	Inactive	Jun 26, 2019 09:34:36 IST

The selected logical fabric appears.

3. Select the **Configure** option from the action menu in the **Switches** list.

NOTE

The **Configure** option is available only for VF switches. The **Configure Domain ID** option is available for non-VF switches. With this option you can configure the domain ID of non-VF switches.

Logical Fabrics FICON Fabrics

LF_test_1

Name: LF_test_1 Description:

Tags:

Fabric ID: 25 Non-VFSL Template:

RA TOV: 10000 Enable device probing

ED TOV: 2000 Per-frame routing priority

Maximum Hops: 7 Suppress Class F traffic

BB Credit: 16 Long distance fabric

Data Field Size: 2112

Switches

Name ^	Tags ^	WWN	Chassis ^	Model ^	IP Address ^	VF Stat... ^	Status ^
S1	test	-	Brocade6510_2	Brocade 6510	10.124.71.130	Enabled	-

Activate

Save Delete Cancel

The **Configure Logical Switch** window is displayed.

4. Modify the fields based on your requirements, and then click **Next**.

The screenshot shows the 'Configure Logical Switch' window. It includes the following fields and options:

- Name: S1
- Description: (empty text area)
- Tags: test
- Chassis: Brocade6510_2
- Domain ID: 10 (Decimal)
- Area Limit: Disable 256 limit(00-FFC0)
- Available Ports table:

Name	Port N.	Fabric ID	Type	State
port10	10	128	U-Port	Offline
- Selected Ports table:

Name	Port Number	Type
port9	9	U-Port
- Buttons: Next (highlighted), Cancel

The **Add Logical Switch** window is displayed.

- Click **OK**. The logical switch is modified.

7.5.6 Deleting Logical Fabrics and Switches

7.5.6.1 Deleting a Logical Fabric

To delete a logical fabric, you must have Logical Switch Configuration privilege with read-write permission.

To delete a logical fabric, perform the following steps:

- Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**. The **Logical Fabrics** window is displayed.
- Select the logical fabric that you want to delete from the **Logical Fabrics** list.

The screenshot shows the 'Logical Fabrics' management page with the following table:

Name	Tags	Description	FID	Seed Switch IP	Switc.	Status	Last Mo
Fault Management	-	-	128		7	Active	Jul 03, 2
LFabric	-	-	125		1	Active	Jul 03, 2
F_test_1	-	-	25		1	Active	Jul 03, 2
new	-	-	12		1	Active	Jul 03, 2

The selected logical fabric appears.

- Click **Delete**.

Logical Fabrics FICON Fabric LF_test_1

Name: LF_test_1 Description: [Text Area]

Tags: [Text Area]

Fabric ID: 25 Non-VISL Template: [Dropdown]

RA TOV: 10000 Enable device probing

ED TOV: 2000 Per-frame routing priority

Maximum Hops: 7 Suppress Class F traffic

BB Credit: 16 Long distance fabric

Data Field Size: 2112

Switches (2 items)

Name	Tags	WWN	Chassis	Model	IP Address	VF Stat.	Status
S1	test	10:00:50:EB:1A	Brocade6510, Brocade 6510			Enabled	Discovered/Seed
S2	test	-	dB510_2_1_Di	Brocade DCK		Disabled	-

Activate

Save Delete Cancel

The logical fabric is removed from the **Logical Fabrics** page.

7.5.6.2 Deleting a Logical Switch

To delete a logical switch, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**. The **Logical Fabrics** window is displayed.
2. Click the name of the logical fabric containing the switch that you want to delete.

Logical Fabrics (9)

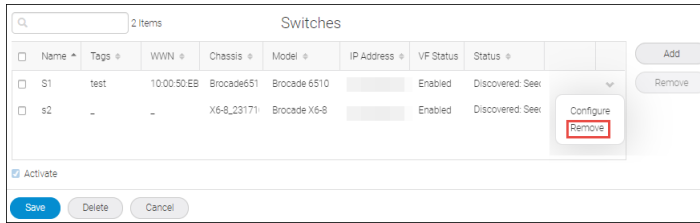
Name	Tags	Description	FID	Seed Switch IP	Switch	Status	Last Mo
Fault Management	-	-	128		7	Active	Jul 03, 2
LFabric	-	-	125		1	Active	Jul 03, 2
LF_test_1	-	-	25		1	Active	Jul 08, 2
new	-	-	12		1	Active	Jul 03, 2

The selected logical fabric appears.

3. Select the **Remove** option from the action menu of the switch that you want to remove. The **Remove** option is greyed out if a single switch is present in the **Switches** list. The **Remove** option is disabled for the un-monitor, maintenance mode, unreachable, or authentication failure switches.

NOTE

The VF-disabled switch, AMP, and the default switch cannot be deleted from a fabric.



The logical switch is removed from the **Switches** list.

7.5.7 Fabric Properties for Logical Fabrics

Fabric properties vary based on the template selection. Only applicable properties of the selected template are displayed for configuration.

Base Switch Template

The Base Switch template is used for creating a logical fabric with base switches.

XISL Template

The XISL template is used for creating a logical switch as XISL.

Non-XISL Template

The Non-XISL template is used for creating a logical fabric without a base Switch or XISL. By default, this template is selected.

The following table describes the properties of these templates.

Template Properties	Description
Enable device probing	When this checkbox is selected, the private devices are not registered to be entered in the Name Server and receive complete fabric access.
Per-frame routing priority	When this checkbox is selected, the frame header is used with the virtual channel ID to determine the frame routing priority.
Suppress Class F traffic	When this checkbox is selected, Class F traffic is converted to Class 2 traffic before being transmitted.
Long-distance fabric	When this checkbox is selected, ISLs in the fabric can be up to 100 km long.

For detailed information on the fabric properties, refer to the *Fabric OS Command Reference Manual*.

7.5.8 Logical Fabric Events

The following events are generated for each action while creating a logical fabric.

Message ID	Severity	Description	Association
SSMP-LF-1001	INFO	Successfully created logical fabric {fabric name} with logical switch {switch name}.	—
SSMP-LF-1002	INFO	Successfully created logical fabric {fabric name} with {logical switch count} logical switches.	—

Message ID	Severity	Description	Association
SSMP-LF-1003	ERROR	Failed to create logical fabric {fabric name}.{reason}.	—
SSMP-LF-1004	INFO	Successfully updated logical fabric {fabric name}.	Fabric
SSMP-LF-1005	ERROR	Failed to update logical fabric {fabric name}.{reason}.	Fabric
SSMP-LF-1006	INFO	Successfully deleted logical fabric {fabric name}.	—
SSMP-LF-1007	ERROR	Failed to update logical fabric {fabric name}.{reason}.	—
SSMP-LF-1008	INFO	Successfully created logical switch {logical switch name} in the chassis {ipAddress} for the fabric {fabric name}.	—
SSMP-LF-1009	ERROR	Failed to create logical switch {logical switch name} in the chassis {ipAddress} for the fabric {fabric name}. {reason}.	—
SSMP-LF-1010	INFO	Successfully updated logical switch {logical switch name} in the fabric {fabric name}.	Logical switch
SSMP-LF-1011	ERROR	Failed to update logical switch {logical switch name} in the fabric {fabric name}. {reason}.	Logical switch
SSMP-LF-1012	INFO	Successfully deleted logical switch {logical switch name} from the chassis {ipAddress} and the fabric {fabric name}.	—
SSMP-LF-1013	ERROR	Failed to delete logical switch {logical switch name} in the chassis {ipAddress} for the fabric {fabric name}. {reason}.	—
SSMP-LF-1014	INFO	Enabled VF on the chassis {chassis name}.	Chassis
SSMP-LF-1015	ERROR	Failed to enable VF on the chassis {chassis name}.	Chassis
SSMP-LF-1016	INFO	Successfully created logical fabric {fabric name} (inactive).	—
SSMP-LF-1017	INFO	Successfully updated logical fabric {fabric name} (inactive).	—
SSMP-LF-1018	INFO	Successfully deleted logical fabric {fabric name} (inactive).	—
SSMP-LF-1019	INFO	Successfully updated switch {switch name} in the fabric {fabric name}.	—
SSMP-LF-1020	INFO	Successfully updated Analytical Monitoring Platform {amp name} in the fabric {fabric name}	—
SSMP-LF-1021	ERROR	Failed to update switch {switch name} in the fabric {fabric name}. {reason}.	—
SSMP-LF-1022	ERROR	Failed to update Analytical Monitoring Platform {amp name} in the fabric {fabric name}. {reason}.	—

7.6 Monitoring and Alerting Policy Suite

The SANnav Monitoring and Alerting Policy Suite (MAPS) feature allows you to configure and monitor policies on discovered switches in a fabric. MAPS is an optional storage area network (SAN) health monitor that allows you to enable each switch to constantly monitor its SAN fabric for potential faults and automatically alert you to problems long before they become costly failures.

MAPS tracks a variety of SAN fabric measures and events. Monitoring fabric-wide events, ports, and environmental parameters enables early fault detection and isolation as well as performance measurement. You can configure fabric measures and alert thresholds on an individual port and group basis.

For Fabric OS devices, MAPS provides customizable monitoring thresholds. You can configure MAPS to provide notifications before problems arise, such as reporting when network traffic through a port is approaching the bandwidth limit. This information enables you to perform preemptive network maintenance, such as trunking or zoning, and avoid potential network failures.

MAPS enables you to define how often to check each switch and fabric measure and to specify notification thresholds. Whenever fabric measures exceed these thresholds, MAPS automatically provides notification using several methods, including email messages, SNMP traps, and log entries.

NOTE

An active and valid Fabric Vision license is required to configure and view MAPS policies.

MAPS must already be enabled on the switch. The MAPS enable function is not supported in SANnav.

MAPS is supported on switches that run Fabric OS 7.4.0 and later. It is enabled by default on switches running Fabric OS 8.x and later.

MAPS configuration requires read and write permissions to the MAPS Management privilege.

7.6.1 MAPS Structural Elements

MAPS has the following structural elements: actions, categories, conditions, measures, objects, groups, rules, and policies.

The following table provides a brief description of MAPS structural elements.

Element	Description
Action	What MAPS will do if a condition defined in a rule evaluates to true.
Category	A grouping of similar elements that can be monitored (for example, Security Violations).
Condition	A condition includes a time base and a threshold. If the condition is evaluated as true, the rule is triggered. The condition depends on the element that is to be monitored.
Measure	A value that can be monitored. This includes switch conditions, data traffic levels, error messages, and many other values.
Object	An object that can be monitored. This includes FC ports, SFP transceivers, a local switch, a flow, and other values.
Group	A collection of similar objects that you can monitor as a single entity. For example, you can create a group of E_Ports to be monitored by the same policies.
Rule	A rule associates a condition with one or more actions to be performed when the specified condition is triggered.
Policy	A set of rules defining thresholds for triggering the actions that MAPS takes when a threshold is triggered. When a policy is activated, all rules in the policy are in effect.

7.6.2 MAPS Actions

MAPS provides actions (event notifications) in several different formats to ensure that event details are accessible from all platforms and operating systems. In response to an event, MAPS can record event data as any (or all) of the following alarm options.

RAS Log Event

Following an event, MAPS adds an entry to the internal event log for an individual switch. The RAS log stores event information but does not actively send alerts.

SNMP Trap

In environments in which you have a high number of messages coming from a variety of switches, you may want to receive them in a single location and view them using a graphical user interface (GUI). In this type of scenario, the Simple Network Management Protocol (SNMP) notifications may be the most efficient notification method. You can avoid logging in to each switch individually as you would have to do for error log notifications.

SNMP performs an operation called a *trap*. A trap notifies a management station using SNMP when events occur. Log entries can also trigger SNMP traps if an SNMP agent is configured. When an SNMP agent is configured to a specific error message level, error messages at that level trigger SNMP traps.

The SNMP trap action is checked by default when you add a new rule.

Email

An email alert sends information about a switch event to a specified email address. An email alert can send information about any error from any element, area, and class (only one email recipient can be configured per class). The email alert specifies the threshold and describes the event, much like an error message.

The email action is checked by default when you add a new rule. The From address field is supported by Fabric OS 8.2.0 and later.

Port Decommission

Port decommission automatically takes ports offline when the configured thresholds in a rule are exceeded. Port fencing is auto-enabled if port decommission is enabled for a MAPS rule or action.

Fence

Port fencing takes ports offline if the user-defined thresholds are exceeded. Fence the port if port fencing is enabled.

SFP Status Marginal

The SFP Status Marginal action is used to set the SFP status to marginal. From Fabric OS 8.0.0, SFP Status Marginal is enabled by default.

FICON Management Service

FICON Management Service (FMS) is used to notify the FICON Host management service of a MAPS violation. Rules with the FICON notification action will be a part of all three default policies (`dflt_aggressive_policy`, `dflt_moderate_policy`, and `dflt_conservative_policy`). In an active policy, if FICON notification is configured for any triggered events, MAPS sends the notification to FMS with event information.

Slow Drain Device Quarantine (SDDQ)

Slow Drain Device Quarantine is used to isolate the traffic targeted to slow-drain devices and reduce the impact of traffic targeted on other devices. Due to this automatic isolation from the regular flows, the effects of the slow-drain flows on the fabric are reduced. If the quarantined ports go offline or are disabled, the ports remain in the Slow Drain Quarantined state. Once the ports come online, the flows destined to the port are quarantined.

Un-Quarantine

Un-Quarantine is used to automatically quarantine a port when Slow Drain Quarantine does not take place for a given timeout period. You can set the timeout period for days, hours, minutes, or seconds. Un-Quarantine is supported by Fabric OS 8.1.0 and later.

Toggle

Use Toggle to recover ports from bottleneck conditions caused by the target device. The MAPS toggle action helps to recover from the bottleneck or forces the Fibre Channel traffic to switch over on the redundant path. The MAPS toggle action can be configured for a shorter or longer duration. The minimum timeout duration is 2 seconds, and the maximum is 3600 seconds (24 hours).

Switch Status Marginal

The Switch Status Marginal action sets the switch status to marginal. From Fabric OS 8.0.0, the Switch Status Marginal action is enabled by default.

Switch Status Critical

The Switch Status Critical action sets the switch status to critical. From Fabric OS 8.0.0, the Switch Status Critical action is enabled by default.

RE Balance

The RE Balance action is used to bring the port group state back into a balanced state in three or more seconds. The RE Balance action is inactive by default and must be enabled.

7.6.3 MAPS Categories

MAPS enables you to monitor the independent components that are listed in this section by creating policies. When you create a rule, MAPS provides the following rule categories.

Port Monitoring Category

The Port category monitors port statistics and takes action based on the configured thresholds and actions. You can configure thresholds per port type and apply the configuration to all ports of the specified type. Configurable ports include physical ports, E_Ports, optical F_Ports (FOP_Ports), copper F_Ports (FCU_Ports), and Virtual E_Ports (VE_Ports).

The Port category also monitors the physical aspects of an SFP transceiver, such as voltage, current, RXP, TXP, and state changes in physical ports, E_Ports, FOP_Ports, and FCU_Ports.

Switch Status Monitoring Category

The Switch Status category enables you to monitor the health of the switch by defining the number of types of errors that transition the overall switch state into a state that is not healthy. For example, you can specify a switch policy so that if a switch has two port failures, it is considered to be in a marginal state; and if it has four failures, it is in a down state.

Fabric Monitoring Category

The Fabric category groups areas of potential problems arising between devices, such as zone changes, fabric segmentation, downed E_Ports, fabric reconfiguration, domain ID changes, and fabric logins.

FRU Monitoring Category

The FRU category enables you to define rules for field-replaceable units (FRUs), including ports, power supplies, and flash memory.

Security Monitoring Category

The Security category monitors different security violations on the switch and takes action based on the configured thresholds.

Resource Monitoring Category

The Resource category monitors the system RAM, flash, CPU, and memory. The Resource category uses monitors to perform the following tasks:

- Configure thresholds for MAPS event monitoring and reporting for the environment and resource classes. Environment thresholds enable temperature monitoring, and resource thresholds enable monitoring of flash memory.
- Configure memory or CPU usage parameters on the switch or display memory or CPU usage. Configuration options include setting usage thresholds that if exceeded, trigger a set of specified MAPS alerts. You can set up the system monitor to poll at certain intervals, and you can specify the number of retries required before MAPS takes action.

Fabric Performance Impact (FPI) Monitoring Category

The FPI category groups areas that measure the thresholds on the performance of the fabric.

Extension Tunnel Category

The Extension Tunnel category enables you to define rules for Fibre Channel over IP (FCIP) health, including circuit state changes and utilization as well as packet loss.

Extension GE Port Health Monitoring Category

The Extension GE Port Health category groups areas that measures thresholds to monitor the Extension GE port health.

Backend Port Monitoring Category

The Backend Port monitoring category groups areas that measure thresholds to monitor the back-end port health.

7.6.4 MAPS Groups

A MAPS group is a collection of similar objects that you can monitor as a single entity.

You can create a group of objects and then use that group in rules, thus simplifying rule configuration and management. For example, you can create a group of UNIX ports, and then create specific rules for monitoring this group. MAPS provides several preconfigured groups.

The following table list the preconfigured groups.

Preconfigured Group Name	Element Type	Description
ALL_PORTS	FC Port	All FC ports physically present in the logical switch.
ALL_F_PORTS	FC Port	All F_Ports present in the logical switch, including all ports in F_Port trunks.
ALL_E_PORTS	FC Port	All E_Ports and EX_Ports present in the logical switch, including all ports in E_Port and EX_Port trunks.
ALL_D_PORTS	FC Port	All D_Ports (Diagnostic ports) present in the logical switch.
ALL_TARGET_PORTS	FC Port	All logical switch ports connected to targets. MAPS automatically detects if a device connected on a port is a target port and adds it to this set.
ALL_HOST_PORTS	FC Port	All ports in the logical switch connected to hosts. MAPS automatically detects if a device connected on a port is a host port and adds it to this set.
ALL_SFP	FC Port	All gigabit interface converters (GBICs) and SFP transceivers present in the logical switch.
ALL_QSFP	FC Port	All QSFP transceivers present in the logical switch.
ALL_32GSWL_SFP	FC Port	All 32Gb/s Short Wavelength (SWL) SFP transceivers present in the logical switch.
ALL_25Km_16GLWL_SFP	FC Port	All 25-Km 16Gb/s Long Wavelength (LWL) SFP transceivers present in the logical switch.
ALL_16GLWL_SFP	FC Port	All 16Gb/s LWL SFP transceivers present in the logical switch.
ALL_16GSWL_SFP	FC Port	All 16Gb/s SWL SFP transceivers in the logical switch.
ALL_10GLWL_SFP	FC Port	All 10Gb/s LWL SFP transceivers on FC ports in the logical switch.
ALL_10GSWL_SFP	FC Port	All 10Gb/s SWL SFP transceivers on FC ports in the logical switch.
ALL_QUARANTINED_PORTS	FC Port	All ports in the logical switch that have been quarantined for slow-drain performance.
ALL_EXT_GE_PORTS	GigE Port	All GigE ports physically present in the logical switch.
ALL_SLOTS	Slot	All slots present in the chassis.
ALL_SW_BLADES	Blade	All port and application blades in the chassis.
ALL_CORE_BLADES	Blade	All core blades in the chassis.
ALL_PS	Power Supply	All power supplies present in the chassis.

Preconfigured Group Name	Element Type	Description
ALL_TS	Temperature Sensor	All temperature sensors present in the chassis.
ALL_FAN	Fan	All fans present in the chassis.
ALL_TUNNELS	Tunnel	All Extension tunnels present in the logical switch.
ALL_TUNNEL_HIGH_QOS	Tunnel	Monitors 50% of the available bandwidth.
ALL_TUNNEL_MED_QOS	Tunnel	Monitors 30% of the available bandwidth.
ALL_TUNNEL_LOW_QOS	Tunnel	Monitors 20% of the available bandwidth.
ALL_TUNNEL_F_QOS	Tunnel	Monitors bandwidth at the expense of the lowest priority.
ALL_TUNNEL_IP_HIGH_QOS	Tunnel	Monitors 50% of the available bandwidth.
ALL_TUNNEL_IP_MED_QOS	Tunnel	Monitors 30% of the available bandwidth.
ALL_TUNNEL_IP_LOW_QOS	Tunnel	Monitors 20% of the available bandwidth.
SWITCH	Switch	Default group used to define rules on global parameters for the entire switch; for example, security violations or fabric health.
CHASSIS	Chassis	Default group used to define rules on global parameters for the entire chassis; for example, CPU and flash.
ALL_FLASH	Flash	All monitored flash.
ALL_WWN	WWN	All monitored WWN cards.
ALL_2K_QSFP	SFP	All 2K QSFP transceivers present in the logical switch.
ALL_100M_16GSWL_QSFP	SFP	All 100m 16Gb/s SWL QSFP transceivers in the logical switch.
ALL_CIRCUITS	Circuit	All Extension tunnel circuits present in the logical switch.
ALL_CIRCUIT_F_QOS	Circuit	Monitors bandwidth at the expense of the lowest priority.
ALL_CIRCUIT_HIGH_QOS	Circuit	Monitors 50% of the available bandwidth.
ALL_CIRCUIT_MED_QOS	Circuit	Monitors 30% of the available bandwidth.
ALL_CIRCUIT_LOW_QOS	Circuit	Monitors 20% of the available bandwidth.
ALL_CIRCUIT_IP_HIGH_QOS	Circuit	Monitors 50% of the available bandwidth.
ALL_CIRCUIT_IP_MED_QOS	Circuit	Monitors 30% of the available bandwidth.
ALL_CIRCUIT_IP_LOW_QOS	Circuit	Monitors 20% of the available bandwidth.
ALL_BE_PORTS	Ports	All back-end ports in the physical switch.
ALL_LOCAL_PIDS	Ports	All local PIDs in the physical switch.
ALL_ASICS	Asic	All ASIC chips in the physical switch.
ALL_CERTS	Security	All security certificates

7.6.5 MAPS Violations

A violation is an alert sent by MAPS if the triggering condition persists every time a rule is checked.

The following 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.

7.6.5.1 Viewing MAPS Violations

You can view MAPS violations in the **Events** page. Violations are filtered based on severity, network Scope, and date range. Available violation severities are All, Critical, Error, Warning, and Info.

Perform the following steps to view the MAPS violations:

1. Click **Events** in the navigation bar, and then select the **MAPS Violations** tab. The **Violations** window is displayed with a list of MAPS violations.
2. Click the (▶) button next to a rule to view the violation details.

Rule Name	Categ...	Rule C...	Meas...	Product	Object Name	Last Occurred(Server ...)
fabric_zone_chg	Fabric He...	SWITCH(...)	0	10.38.151.57	sw6543e057	Jul 18, 2019 11:08:35 IST
defALL_OTHER...	Fabric Per...	ALL_OTH...	96.11	10.124.72.1...	port7	Jul 18, 2019 11:08:33 IST
defALL_OTHER...	Fabric Per...	ALL_OTH...	96.02	10.124.72.1...	port2	Jul 18, 2019 11:08:33 IST

Event Action Name	defALL_OTHER_F_PORTSTX_95	Port Type	SIM-Port
Rule Condition	ALL_OTHER_F_PORTS(TX/min>95.00)	Product Address	10.124.72.179 [128]
Severity	Warning	Unit	%
Measure Value	96.02	Fabric	FabricTest_10
Actions	RasLog,Snmp,Email	Recommended Action	High utilization may indicate a need bandwidth or redistributing traffic (load balancing).

7.6.5.1.1 Troubleshooting MAPS Violations

You can troubleshoot the MAPS event violations by taking recommended actions. See [Managing Event Actions](#) for information on recommended actions.

7.6.6 MAPS Rules

A MAPS rule associates a condition with actions that will be triggered when the specified condition is evaluated to be true. The combination of actions, conditions, and measures allows you to create a rule for almost any scenario required for your environment.

Each rule specifies the following items:

- A group of objects to be evaluated.
- The measure to be monitored.
- The severity to be monitored.
- The condition. Each rule specifies a single condition. A condition includes a time base and a threshold.
- The actions to take if the condition is evaluated to be true.

7.6.7 MAPS Conditions

A condition includes a time base and a threshold. If the condition is evaluated as true, the rule is triggered. The condition depends on the element that is to be monitored.

Consider the following rule:

For all F_Ports, if the change in the CRC counter in the last minute is greater than 10, then fence the port and issue a RASLog message.

In this rule, the condition is whether the change in the CRC counter in the last minute is greater than 10.

Thresholds

Thresholds are the values at which potential problems might occur. For example, in configuring a port threshold, you can select a specific value at which an action is triggered because of too many threshold violations.

Time Base

Time bases specify the time interval between two samples to be compared. You can set the time base to Day (samples are compared once a day), Hour (samples are compared once an hour), or Minute (samples are compared every minute). The time base affects the comparison of sensor-based data with user-defined threshold values. For measures where the time base is not applicable, the time base is automatically set to None.

Severity

MAPS allows you to configure the severity when a policy rule is created. The default severity value is Default. You can import and distribute the severity only for switches running Fabric OS 8.1.0 and later.

Quiet Time

The quiet time is used as a rule parameter to avoid sending alerts for the set quiet time duration (Days, Hours, Minutes, Second) set, after alerting the user for the first time. You can configure the quiet time for all rules, but it is applicable only for RAS Log, E-mail, and SNMP Trap actions.

7.6.8 MAPS Policies

A MAPS policy is a set of rules that define thresholds for measures and the action to take when a threshold is triggered. When you enable a policy, all rules in the policy are in effect. MAPS provides four preconfigured default policies. One policy must be active on the switch.

- `dflt_aggressive_policy` – Contains rules with very strict thresholds.
- `dflt_conservative_policy` – Contains rules with more lenient thresholds that allow a buffer and do not immediately trigger actions. Use this policy in environments where the elements are resilient and can accommodate errors.
- `dflt_moderate_policy` – Contains rules with threshold values between the aggressive and conservative policies.
- `dflt_base_policy` – Provides limited monitoring support. When MAPS is unlicensed (without the Fabric Vision license), `dflt_base_policy` will be the default policy activated.

You cannot modify or delete the default policies, but you can create a user-defined policy based on default policies. The following lists the user-defined limitations for MAPS-enabled Fabric OS switches:

- The maximum number of user-defined rules per logical switch is 500.
- The maximum number of rules in a user-defined policy per logical switch is 350.
- The maximum number of user-defined policies per logical switch is 20.
- The maximum number of RoR rules per logical switch is 50.
- The maximum number of groups per logical switch is 64.

7.6.9 MAPS Measures

The following tables detail the Fabric OS object types for each category, the threshold measures for each object type, and the actions that you can configure when a threshold is crossed.

7.6.9.1 Port Health

Objects	Measures	Measure Descriptions	Possible Actions
FC Port	CRC — CRC errors	The number of times an invalid cyclic redundancy check error occurs on a port or a frame that computes to an invalid CRC. Invalid CRCs can represent noise on the network. Such frames are recoverable by retransmission. Invalid CRCs can indicate a potential hardware problem.	<ul style="list-style-type: none"> ■ RAS Log Event ■ Port Decommission ■ Fence ■ SNMP Trap ■ E-mail ■ FICON Management Service
	ITW — Invalid transmit words	The number of times an invalid transmission word error occurs on a port. A word did not transmit successfully, resulting in encoding errors. Invalid word messages usually indicate a hardware problem.	
	LOSS_SYNC — Loss of synchronization	The number of times a synchronization error occurs on the port. Two devices failed to communicate at the same speed. Synchronization errors are always accompanied by a link failure. Loss of synchronization errors frequently occur due to a faulty SFP transceiver or cable.	
	LF — Link failures	The number of times a link failure occurs on a port or the port sends or receives a Not Operational Sequence (NOS) state. Both physical and hardware problems can cause link failures. Link failures also frequently occur due to a loss of synchronization or a loss of signal.	
	LOSS_SIGNAL — Signal loss	The number of times that a signal loss occurs in a port. Signal loss indicates that no data is moving through the port. A loss of signal usually indicates a hardware problem.	
	PE — Protocol errors	The number of times a protocol error occurs on a port. The error occurs for an invalid state due to a link reset response (LRR) sequence on an online link. Occasionally these errors occur due to software glitches. Persistent errors occur due to hardware problems.	
	LR — Link resets	The ports on which the number of link resets exceed the specified threshold value.	
	C3TXTO — Class 3 timeouts	The number of class 3 frames discarded due to timeouts.	
	STATE_CHG — State changes	The state of the port has changed for one of the following reasons: <ul style="list-style-type: none"> ■ The port has gone offline. ■ The port has come online. ■ The port is faulty. 	
	DEV_NPIV_LOGINS — Device NPIV logins	The number of logins on F_Ports in a switch.	

Objects	Measures	Measure Descriptions	Possible Actions
SFP	CURRENT — SFP transceiver current	The amount of supplied current to the SFP transceiver. Current area events indicate hardware failures.	<ul style="list-style-type: none"> ■ RAS Log Event ■ Port Decommission ■ Fence ■ SNMP Trap ■ E-mail ■ FICON Management Service
	RXP — SFP transceiver receive power	The amount of incoming laser power, in microwatts (μW). This is used to help determine if the SFP transceiver is in good working condition. If the counter often exceeds the threshold, the SFP transceiver is deteriorating.	
	TXP — SFP transceiver transmit power	The amount of outgoing laser power, in microwatts (μW). This is used to help determine if the SFP transceiver is in good working condition. If the counter often exceeds the threshold, the SFP transceiver is deteriorating.	
	VOLTAGE — SFP transceiver voltage	The amount of voltage supplied to the SFP transceiver. If this value exceeds the threshold, the SFP transceiver is deteriorating.	
	SFP_TEMP — SFP transceiver temperature	The physical temperature of the SFP transceiver, in degrees Celsius. A high temperature indicates that the SFP transceiver might be in danger of damage.	
	PWR_HRS1 — SFP transceiver power-on hours	The number of hours that the 16Gb/s SFP transceiver is powered on.	

7.6.9.2 Switch Policy Status

Objects	Measures	Measure Description	Possible Actions
Chassis	BAD_PWR — Absent or faulty power supply	Power supply thresholds detect absent or failed power supplies and power supplies that are not in the correct slot for redundancy.	<ul style="list-style-type: none"> ■ Status Critical ■ Status Marginal ■ FICON Management Service
	BAD_TEMP — Temperature sensors outside range	Temperature thresholds, faulty temperature sensors.	
	BAD_FAN — Absent or faulty fans	Fan thresholds, faulty fans.	
	FLASH_USAGE2 — Flash usage	Flash thresholds.	
	WWN_DOWN — WWN faulty or down	Faulty WWN card (applies to modular switches).	
	DOWN_Core — Core blade monitoring	Faulty core blades.	
	FAULTY_BLADE — Faulty blades	Faulty blades (applies to modular switches).	
	HA_SYNC — HA monitoring	The high availability (HA) state of the active CP is out of synchronization with the HA state of the standby CP.	

Objects	Measures	Measure Description	Possible Actions
Local Switch	MARG_PORTS — Percentage of marginal ports	Physical port, E_Port, FOP_port (optical), and FCU_Port (copper) thresholds. Whenever these thresholds are persistently high, the port is marginal.	<ul style="list-style-type: none"> ■ Status Critical ■ Status Marginal ■ FICON Management Service
	FAULTY_PORTS — Percentage of faulty ports	Hardware-related port faults.	
	MISSING_SFP — Percentage of missing SFP transceivers	Ports that are missing an SFP transceiver.	
	ERR_PORTS — Percentage of error ports	Ports with errors.	

7.6.9.3 Fabric State Changes

Objects	Measures	Measure Description	Possible Actions
Local Switch	DID_CHG — Domain ID change	Monitors forced domain ID changes. Forced domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch must assign another domain ID to a switch.	<ul style="list-style-type: none"> ■ RAS Log Event ■ SNMP Trap ■ E-mail ■ FICON Management Service
	FLOGI — Fabric login	Activates when ports and devices initialize with the fabric.	
	FAB_CFG — Fabric reconfigurations	Tracks the number of reconfigurations of the fabric. Fabric reconfiguration occurs when: <ul style="list-style-type: none"> ■ Two fabrics with the same domain ID are connected. ■ Two fabrics are joined. ■ An E_Port or VE_Port goes offline. ■ A principal link segments from the fabric. 	
	EPORT_DOWN — E_Ports down	Tracks the number of times that an E_Port or VE_Port goes down. E_Ports and VE_Ports go down each time you remove a cable or an SFP transceiver (where there are SFP transceiver failures or transient errors).	
	FAB_SEG — Fabric segmentation	Tracks the cumulative number of segmentation changes. Segmentation changes occur because of one of the following: <ul style="list-style-type: none"> ■ Zone conflicts. ■ Incompatible link parameters. During E_Port and VE_Port initialization, ports exchange link parameters, and incompatible parameters result in segmentation. This is a rare event. ■ Domain conflicts. ■ Segmentation of the principal link between two switches. 	
	ZONE_CHG — Zone changes	Tracks the number of zone changes. Because zoning is a security provision, frequent zone changes might indicate a security breach or weakness. Zone change messages occur whenever there is a change in zone configurations.	

Objects	Measures	Measure Description	Possible Actions
	L2_DEVCNT_PER — Layer 2 device count	Tracks the number of device connections in Layer 2 fabrics. The maximum supported limits in Layer 2 fabrics are the following: <ul style="list-style-type: none"> ■ 4096 for all platforms supported by Fabric OS v7.4.x ■ 6000 for all other fabrics. 	
	LSAN_DEVCNT_PER — LSAN device count	Tracks the maximum number of imported LSAN devices per the total number of devices imported from all the edge fabrics. The maximum supported limits are the following: <ul style="list-style-type: none"> ■ 1000 with the following devices: <ul style="list-style-type: none"> – 8Gb/s 4-slot backbone chassis – 8Gb/s 8-slot backbone chassis – 16Gb/s 4-slot backbone chassis – 16Gb/s 8-slot backbone chassis ■ 5000 with the following devices: <ul style="list-style-type: none"> – 24-port, 8Gb/s FC switch – 40-port, 8Gb/s FC switch – 80-port, 8Gb/s FC switch – 8Gb/s Extension switch – 48-port, 16Gb/s switch – 96-port, 16Gb/s switch 	
	ZONE_CFGSZ_PER — Zone configuration size	Tracks the zone configuration size limit per switch.	
	BB_FCR_CNT — FCR count	Tracks the number of Fibre Channel routers present on the backbone fabric.	

7.6.9.4 FRU Health

Objects	Measures	Measure Description	Possible Actions
Power Supply	PS_STATE — Power supply state	The state of a power supply has changed.	<ul style="list-style-type: none"> ■ RAS Log Event ■ SNMP Trap ■ E-mail ■ FICON Management Service
Fan	FAN_STATE — Fan state	The state of a fan has changed.	
Blade	BLADE_STATE — Blade state	The state of a blade has changed.	
SFP Transceiver	SFP_STATE — SFP transceiver state	The state of an SFP has changed.	
WWN	WWN — World Wide Name state	The state of a World Wide Name (WWN) card has changed.	

7.6.9.5 Security Health

Objects	Measures	Measure Description	Possible Actions
Local Switch	SEC_DCC — Device connection control violations	An unauthorized device attempts to log in to a secure fabric.	<ul style="list-style-type: none"> ■ RAS Log Event ■ SNMP Trap ■ Email ■ FICON Management Service
	SEC_HTTP — HTTP violations	A browser access request reaches a secure switch from an unauthorized IP address.	
	SEC_CMD — Illegal command	Commands permitted only to the primary Fabric Configuration Server (FCS) are executed on another switch.	
	SEC_IDB — Incompatible security DB	Secure switches with different version stamps have been detected.	
	SEC_LV — Login violations	Login violations occur when a secure fabric detects a login failure.	
	SEC_CERT — Invalid certifications	There is a missing or invalid certificate file.	
	SEC_FCS — No Fabric Configuration Server (FCS) switch	The switch has lost contact with the primary FCS.	
	SEC_SCC — Switch Connection Control violations	SCC violations occur when an unauthorized switch tries to join a secure fabric. The WWN of the unauthorized switch appears in the ERRLOG.	
	SEC_AUTH_FAIL — Authentication failures	Authentication failures occur when packets try to pass from a nonsecure switch to a secure fabric.	
	SEC_TELNET — Telnet violations	Telnet violations occur when a Telnet connection request reaches a secure switch from an unauthorized IP address.	
	SEC_TS — Time server out of synchronization	Time Server (TS) violations occur when an out-of-synchronization error has been detected.	
	DAYS_TO_EXPIRE — Number of days before certificate expiry	Number of days before which a certificate expires because it is less than the threshold specified in the rule.	
EXPIRED_CERTS — Number of expired certificates greater than the threshold	Monitors if the number of expired certificates is greater than the configured threshold.		

7.6.9.6 Switch Resources

Objects	Measures	Measure Description	Possible Actions
Temperature Sensor	TEMP — Temperature	Refers to the ambient temperature inside the switch, in degrees Celsius. Temperature sensors monitor the switch in case the temperature rises to levels at which damage to the switch might occur.	<ul style="list-style-type: none"> ■ RAS Log Event ■ SNMP Trap ■ E-mail ■ FICON Management Service
Local Chassis	FLASH_USAGE — Flash usage	Monitors the available compact flash space by calculating the percentage of flash space consumed and comparing it with the configured high-threshold value.	<ul style="list-style-type: none"> ■ RAS Log Event ■ SNMP Trap ■ E-mail ■ FICON Management Service
	CPU — CPU usage	Monitors the available CPU utilization by calculating the percentage of CPU utilization consumed and comparing it with the configured threshold value.	
	MEMORY_USAGE — Memory usage	Monitors the available memory by calculating the percentage of memory consumed and comparing it with the configured threshold value.	
Fan	FAN_AIRFLOW_MISMATCH — Fan airflow direction mismatch.	Monitors the fan airflow direction.	<ul style="list-style-type: none"> ■ RAS Log Event ■ SNMP Trap ■ E-mail ■ FICON Management Service ■ SW_MARGINAL ■ SW_CRITICAL

7.6.9.7 Extension Tunnel

Objects	Measures	Measure Description	Possible Actions
Circuit	CIR_STATE — Extension tunnel circuit state changes	The state of the circuit has changed for one of the following reasons: <ul style="list-style-type: none"> ■ The circuit has gone offline. ■ The circuit has come online. ■ The circuit is faulty. 	<ul style="list-style-type: none"> ■ RAS Log Event ■ Fence CIR_STATE ■ SNMP Trap ■ E-mail ■ FICON Management Service
	CIR_UTIL — Extension tunnel circuit utilization	The percentage of utilization for the circuit at the time of the last poll.	
	CIR_PKTLOSS — Extension tunnel circuit packet loss	The number of packets routed through a port exceeds the port bandwidth.	
	PKTLOSS — Extension tunnel packet loss	Monitors the number of retransmitted packets in the tunnel.	
	RTT — Round-trip time of the circuit	Monitors the round-trip time of the circuit.	
	Jitter — The variance in the round-trip time of the circuit	Monitors the variance in the round-trip time of the circuit.	
	TUNNEL_UTIL — Tunnel utilization	Monitors throughput in the channel.	
	TUNNEL_STATE — Extension tunnel status	Monitors the tunnel state.	

7.6.9.8 Traffic/Flows Performance

Objects	Measures	Measure Description	Possible Actions
Flow	TX_FCNT — Tx Frame Count	The number of transmitted frames for the flow that exceeds the configured thresholds.	<ul style="list-style-type: none"> ■ RAS Log Event ■ SNMP Trap ■ E-mail ■ FICON Management Service
	RX_FCNT — Rx Frame Count	The number of received frames for the flow that exceed the configured thresholds.	
	TX_THPUT — Tx Throughput	The number of transmitted words for the flow that exceed the configured thresholds.	
	RX_THPUT — Rx Throughput	The number of received words for the flow that exceed the configured thresholds.	
	IO_RD — IO Read Command Count	The number of SCSI read commands for the flow that exceed the configured thresholds.	
	IO_WR — IO Write Command Count	The number of SCSI write commands for the flow that exceed the configured thresholds.	
	IO_RD_BYTES — IO Read Data	The SCSI read data rate (Mb/s) for the flow that exceed the configured thresholds.	
	IO_WR_BYTES — IO Write Data	The SCSI write data rate (Mb/s) for the flow that exceed the configured thresholds.	
	RD_PENDING_IO — IO Pending Read Data	The number of pending read I/O requests.	
	WR_PENDING_IO — IO Pending Write Data	The number of pending write I/O requests.	
	RD_STATUS_TIME — Read Completion Time	The total read request completion time.	
	WR_STATUS_TIME — Write Completion Time	The total write request completion time.	
	RD_1stDATA_TIME — First Read Response Time	How quickly the target responds to read the command.	
	WR_1stXFER_RDY — First Write Response Time	Hhow quick the target responds to write the command.	

7.6.9.9 FPI

Object	Measures	Measure Descriptions	Possible Actions
FC Port	DEV_LATENCY_IMPACT — Device latency impact	The latency impact of the device.	<ul style="list-style-type: none"> ■ RAS Log Event ■ SNMP Trap ■ E-mail ■ FICON Management Service ■ SDDQ ■ Un-Quarantine ■ Toggle
	RX — Receive bandwidth usage percentage	The Rx bandwidth of the device.	<ul style="list-style-type: none"> ■ RAS Log Event ■ SNMP Trap ■ E-mail ■ FICON Management Service
	TX — Transmit bandwidth usage percentage	The Tx bandwidth of the device.	
	UTIL — Trunk utilization	The Tx bandwidth of the device.	
	ALL_LOCAL_PIDS – Initiator to target ratio	Initiator to target ratio.	<ul style="list-style-type: none"> ■ RAS Log Event ■ SNMP Trap ■ E-mail ■ FICON Management Service
	IT_FLOWS - IT flow ratio	Initiator to target flow ratio.	<ul style="list-style-type: none"> ■ RAS Log Event ■ SNMP Trap ■ E-mail

7.6.9.10 GigE Port

Objects	Measures	Measure Description	Possible Actions
GigE Port	GE_CRC — Frames received with a CRC error.	The number of times an invalid cyclic redundancy check error occurs on a GigE port or a frame that computes to an invalid CRC.	<ul style="list-style-type: none"> ■ RAS Log Event ■ SNMP Trap ■ E-mail
	GE_LOS_OF_SIG — Frames aborted because of a carrier sense error, no carrier, or loss of a carrier.	The number of frames received with an invalid length.	
	GE_INV_LEN — Frames received with a length error when the Length_Type field does not match the frame size.	The number of frames aborted.	

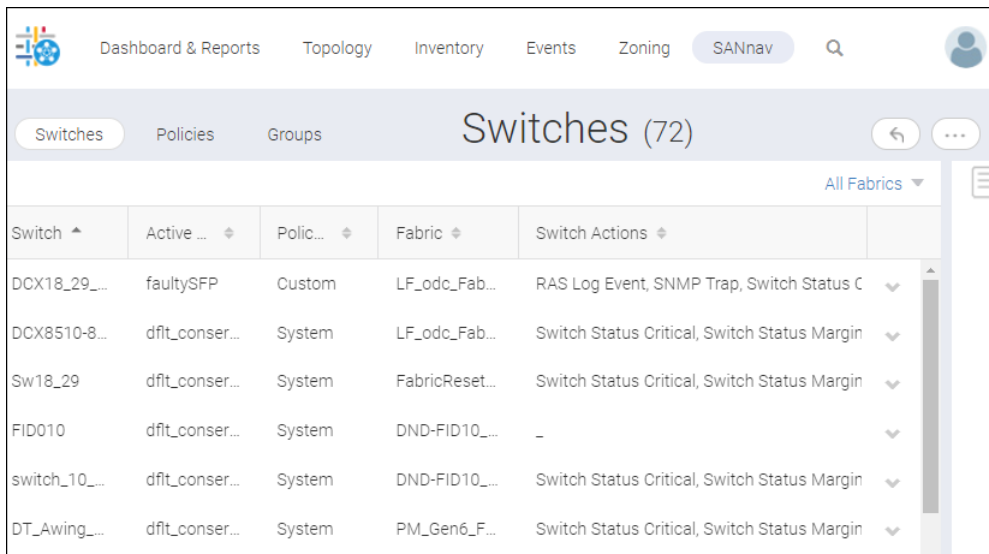
7.6.9.11 Backend Port Monitoring

Objects	Measures	Measure Description	Possible Actions
Backend Port	LR — Link resets	The ports on which the number of link resets exceed the specified threshold.	<ul style="list-style-type: none"> ■ RAS Log Event ■ SNMP Trap ■ E-mail
	BAD_OS — Invalid ordered sets	The number of invalid ordered sets (platform and port-specific).	
	CRC — CRC errors	The number of times an invalid cyclic redundancy check error occurs on a port or a frame that computes to an invalid CRC.	
	ITW — Invalid transmit words	The number of times an invalid transmission word error occurs on a port.	
	FRM_TRUNC — Frames shorter than the minimum	Frames shorter than the minimum.	
	FRM_LONG — Frames longer than the maximum	Frames longer than the minimum.	

7.6.10 MAPS Configuration

SANnav MAPS policy management allows you to create new MAPS policies, rules, and custom groups; and apply and activate MAPS policies across one or more switches. You can import and modify existing MAPS policies. You can also view MAPS-enabled switches, policies and rules, fabrics and groups to which the switches belong, and switch configuration actions.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > MAPS Policy Management**. The **Switches** window is displayed.



Switch	Active Policy	Policy Type	Fabric	Switch Actions
DCX18_29...	faultySFP	Custom	LF_odc_Fab...	RAS Log Event, SNMP Trap, Switch Status C
DCX8510-8...	dft_conser...	System	LF_odc_Fab...	Switch Status Critical, Switch Status Margin
Sw18_29	dft_conser...	System	FabricReset...	Switch Status Critical, Switch Status Margin
FID010	dft_conser...	System	DND-FID10...	-
switch_10...	dft_conser...	System	DND-FID10...	Switch Status Critical, Switch Status Margin
DT_Awing...	dft_conser...	System	PM_Gen6_F...	Switch Status Critical, Switch Status Margin





2. Click the **Switches** tab to view the list of MAPS-enabled switches with an active policy name, policy type, and the fabric to which they belong, and switch configuration actions.
3. Click the **Policies** tab to view the policies applied to the switch. See [MAPS Policies](#) for information on default policies and custom policies.

- Click the **Groups** tab to view the preconfigured groups available on the switch. You can create user-defined custom groups only for ports, SFPs, and circuits. See [MAPS Groups](#) for information on predefined and custom MAPS groups.

7.6.10.1 Configuring a MAPS Policy and Applying It to Multiple Switches

You can create a new MAPS policy or custom policy on the switch.

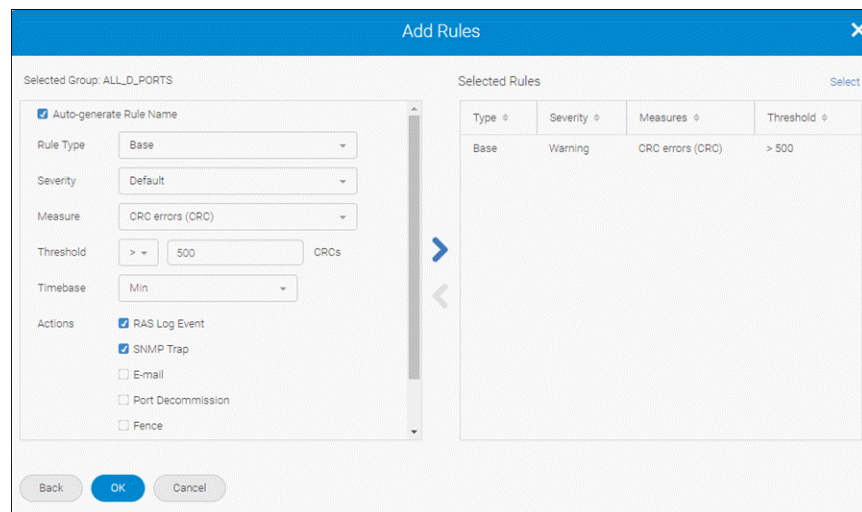
Following is an example of creating a custom policy and applying it to all switches in the fabric. In this example, the policy is to generate a RASlog event and SNMP trap whenever the number of CRC errors on any D_Port exceeds 500. The quiet time is one day, which means that the RASlog and SNMP trap are generated no more than once per day, regardless of how often the rule is triggered.

- Click **SANnav** in the navigation bar, and then select **SAN Monitoring > MAPS Policy Management**.
- In the **Switches** tab, click the down-arrow () next to the switch for which you want to create the policy, and select **View Policies**.
- Click the add button (+) in the top-right corner of the page, and click **Create New**.
- Enter the name, tags, and description of the new policy, and click the expand button () for the rules category. For this example, expand the **Port** rules category.
(Optional) You can click the expand button () for **Switch Status, Fabric, FRU, Security, Resource, Traffic/Flows,** and **FPI** to add rules.
- Add rules to the policy.
 - Click the **Add** button under **Rules**, select the group to which the rule applies, and click **Next**. For this example, select the ALL_D_Ports group.
 - Select or enter the required values, and click the right arrow () to move them to the **Selected Rules** column.

The right arrow is not activated unless all required fields are entered.

For this example, enter the following:

- **Measure:** CRC errors
- **Threshold:** > 500 CRCs
- **Actions:** RAS Log Event and SNMP Trap
- **Quiet Time:** 1 day (Scroll down to select the **Quiet Time** checkbox.)



The screenshot shows the 'Add Rules' dialog box with the following configuration:

- Selected Group: ALL_D_PORTS
- Auto-generate Rule Name
- Rule Type: Base
- Severity: Default
- Measure: CRC errors (CRC)
- Threshold: > 500 CRCs
- Timebase: Min
- Actions:
 - RAS Log Event
 - SNMP Trap
 - E-mail
 - Port Decommission
 - Fence

The 'Selected Rules' table is as follows:

Type	Severity	Measures	Threshold
Base	Warning	CRC errors (CRC)	> 500

NOTE

If you want to create a rule that monitors how often another rule is executed, select **Rule on Rule** for the **Rule Type**.

6. Add any additional rules for the selected group, and click **OK** to add the rules to the policies.

Dashboard & Reports Topology Inventory Events Zoning SANnav

Switches Policies Groups **Create New Policy**

Name: Custom_policy Description: Create custom policy for switch wedge 202.

Tags: ports

Port

1 Item

Rules

<input type="checkbox"/>	Name	Group	Sever...	Measure	Thres...	Time...	Actio...	
<input type="checkbox"/>	ADP_CRC_G50.	ALL_D_P...	Warning	CRC errors	> 500	-	RAS Log ...	Remove

Switsh Status

7. Add more rules to the policy, either for the same category or for different categories.
8. After adding rules to the policy, click the **Active** checkbox to activate this policy on the switch, and then click **Save**. The new policy is added to the switch policy and is the active policy on the switch.

Dashboard & Reports Topology Inventory Events Zoning SANnav

Switches Policies Groups **Policies (4)**

Wedge-202

Name	Tags	Description	Status	Last Modified
dflt_aggressive_policy	-	-		Jul 17, 2019 14:24:40 IST
dflt_moderate_policy	-	-		Jul 17, 2019 14:24:40 IST
dflt_conservative_policy	-	-	Active	Jul 17, 2019 14:24:40 IST
dflt_base_policy	-	-		Jul 17, 2019 14:24:40 IST

9. Apply the policy to multiple switches. For this example, apply the policy to all switches in the fabric.
- Click the down arrow next to the new policy, and select **Distribute**.
 - In the **Distribute** dialog, select the switches to which you want to apply the policy, and click **OK**.

For this example, sort the switch list based on the **Fabric** column, and then select all switches in the targeted fabric.

7.6.10.2 Managing MAPS Configure Actions on a Switch

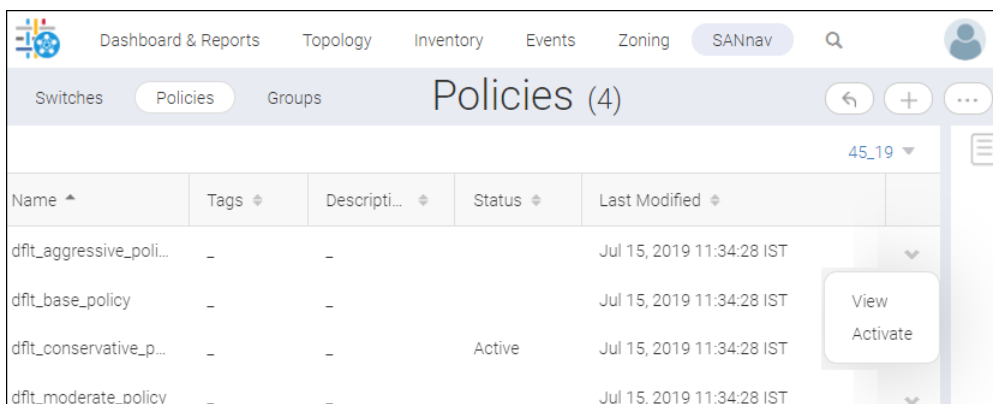
In the **Switches** tab, you can view the policies on the switch, configure actions, and configure emails to send alerts. Select a switch in the **Switches** tab and perform available actions.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > MAPS Policy Management**.
2. In the **Switches** tab, click the down-arrow (\vee) next to a switch, and then select **View Policies**.



3. Select a default type of policy, and click the action drop-down (\vee), and perform the following actions.

Figure 27: Default Policy Type Switch Actions



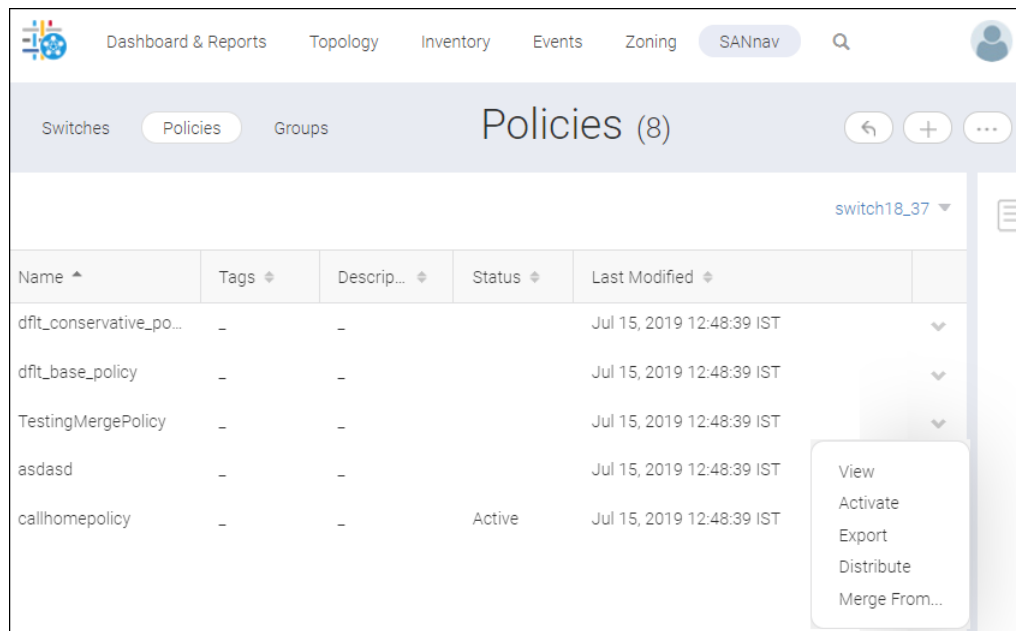
- a) Click **View** to view the policy details page.
- b) Click **Activate** to activate the policy on the selected switch. The policy activated in the earlier switch is deactivated.


NOTE

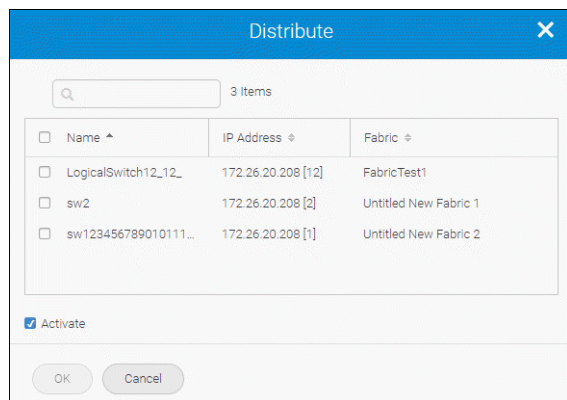
For default type policies, only **View** and **Activate** actions are supported.

4. Select a custom type policy, click the action drop-down (), and perform the following actions.

Figure 28: Custom Policy Type Switch Actions



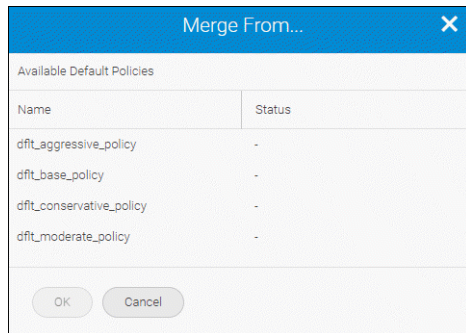
- a) Click **View** to view the policy details page.
- b) Click **Activate** to activate the policy on the selected switch. The **Activate** option is listed only if the policy is not activated on the switch.
- c) Click **Export** to save and export a policy as a file with all policy details. To export multiple policies, click the more () button, and then select **Bulk Select**. Select multiple policies, and then select **Export** from the **Edit** drop-down. Browse to the location where you want to save the policy, and click **Save**. You can export a policy to a JSON file format. The exported policies contain default group names to which their rules are applicable. If the exported policies contain rules applicable to custom groups, the name of the custom groups along with their members will also be exported.
- d) Click **Distribute** to distribute policies to different switches. In the **Distribute**, select the switches to which the policies need to be distributed. Click the **Activate** checkbox to immediately activate the policy on the selected switch. Only the rules applicable to the switches are copied based on the switch type and firmware version.



- e) Click **Merge From** to merge all default rules from the available default policies to the custom policy selected. The **Merge From** option will display only for custom policies.

The **Merge From** function is used in the following conditions:


- When you want to copy the existing default policy rules to a custom policy and customize the policy.
- When a custom policy is created based on default policy.
- When a switch in which a policy is created was migrated to a new firmware version.
- When extra measures are supported in the new firmware version.



7.6.10.2.1 Importing MAPS Policies



You can import a policy to a switch. The policy file must be in JSON file format or XML file format.

You can import a policy with the same name. When you import a policy with the same name, a warning message displays to accept all changes or reject all changes and continue with the import function.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > MAPS Policy Management**.
2. In the **Switches** tab, click the down-arrow () for the switch to which you want to import the policy, and select **View Policies**.
3. Click the add button (+) at the top-right corner of the **Policies** page, and select **Import**.
4. Browse to the location of the policy that you want to import, and click **Open**.
You cannot import policies at the SAN or fabric level.

7.6.10.2.2 Cloning MAPS Policies


You can clone a default policy or custom policy.

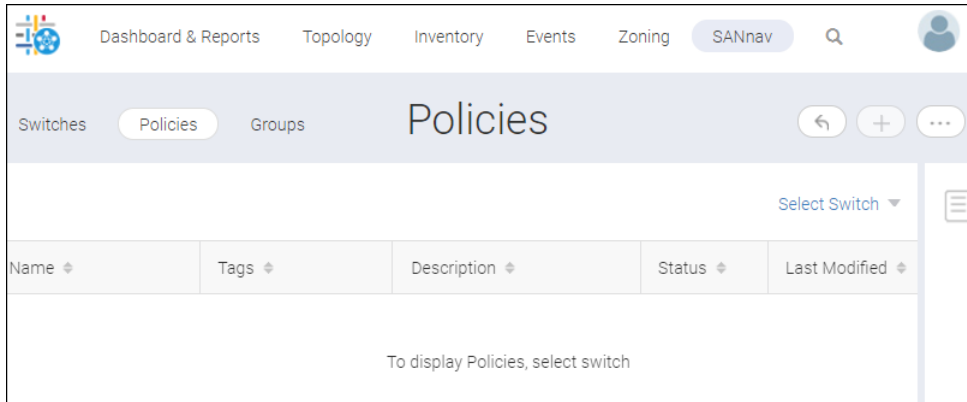
1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > MAPS Policy Management**.
2. In the **Switches** tab, click the down-arrow () for the switch in which you want to clone the policy, and select **View Policies**.
3. Select a policy in the **Policies** page, click (), and select **View**.
4. In the policy details page, click the **Save As** button.
5. In the **Save As** page, enter a new name for the policy in the **Name** field, and then click the **Save** button.
The policy will be cloned and saved with a new name in the **Policies** page.

7.6.10.2.3 Cloning MAPS Default Rules

You can clone a default rule into a custom rule and modify it as per your requirement.

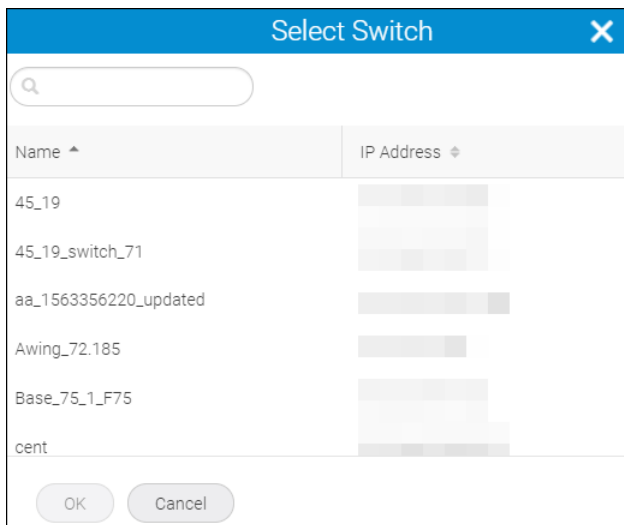
To clone a default rule, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > MAPS Policy Management**. The **Switches** window appears.
2. Select the **Policies** tab, and then select the switch from the **Select Switch** down-arrow ().




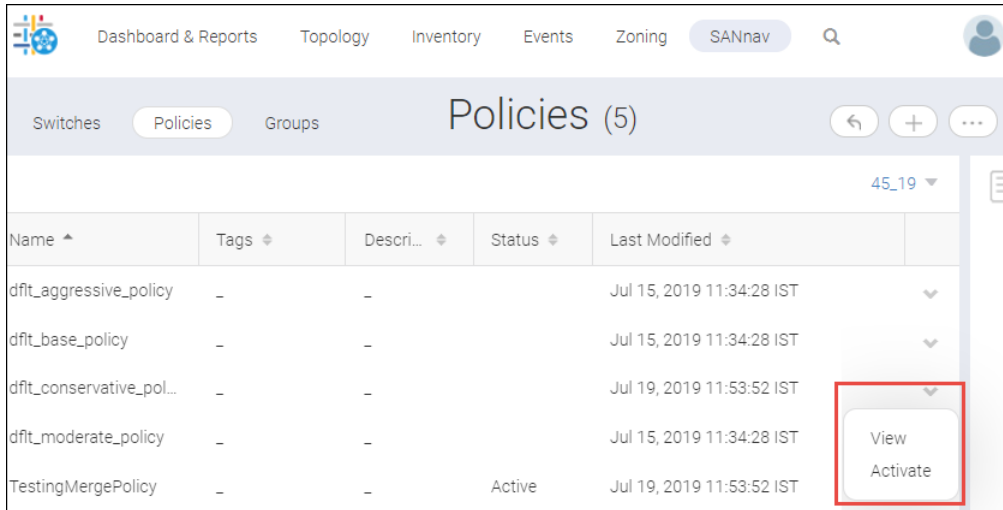
The **Select Switch** window is displayed.

3. Select the switch where you want to clone the default rule, and then click **OK**.



The **Policies** window appears.

4. Select a policy in the **Policies** page, click (), and select **View**.



The screenshot shows the SANnav interface with the 'Policies' tab selected. The page title is 'Policies (5)'. Below the title is a table with columns: Name, Tags, Description, Status, and Last Modified. The table contains five rows of policy data. The 'TestingMergePolicy' row is highlighted, and a red box highlights the 'View' and 'Activate' buttons in the right-hand column of that row.

Name ^	Tags	Descri...	Status	Last Modified	
dft_aggressive_policy	-	-		Jul 15, 2019 11:34:28 IST	▼
dft_base_policy	-	-		Jul 15, 2019 11:34:28 IST	▼
dft_conservative_pol...	-	-		Jul 19, 2019 11:53:52 IST	▼
dft_moderate_policy	-	-		Jul 15, 2019 11:34:28 IST	▼
TestingMergePolicy	-	-	Active	Jul 19, 2019 11:53:52 IST	View Activate

The selected policy appears. You cannot modify a default policy rule and must create a clone to modify a rule.

5. Click **Save As** from the **Save** drop-down.

The screenshot shows the SANnav Management Portal interface. The top navigation bar includes 'Dashboard & Reports', 'Topology', 'Inventory', 'Events', 'Zoning', and 'SANnav'. The main header shows 'Switches', 'Policies', and 'Groups' tabs, with the current page title 'dflt_conservative_policy'. The form contains the following elements:

- Name:** dflt_conservative_policy
- Description:** A text area for entering a description.
- Tags:** A text input field.
- Expandable sections:** A list of sections with expandable arrows: Port, Switch Status, Fabric, FRU, Security, Resource, Traffic/Flows, FPI, Extension, and Extension GE Port.
- Active:** A checkbox labeled 'Active'.
- Buttons:** A blue 'Save' button, a grey 'Cancel' button, and a 'Save As' button highlighted with a red box.

The **Save As** window appears.

6. In the **Save As** window, enter a new name for the policy in the **Name** field, and then click the **Save** button.

Dashboard & Reports Topology Inventory Events Zoning SANnav Q

Switches Policies Groups Save As...

Name Clone_dft_conservative_policy Description

Tags

- Port
- Switch Status
- Fabric
- FRU
- Security
- Resource
- Traffic/Flows
- FPI
- Extension
- Extension GE Port

Active

Save Cancel

The policy is cloned and saved with a new name in the **Policies** window.

Dashboard & Reports Topology Inventory Events Zoning SANnav Q


Switches Policies Groups Policies (6)

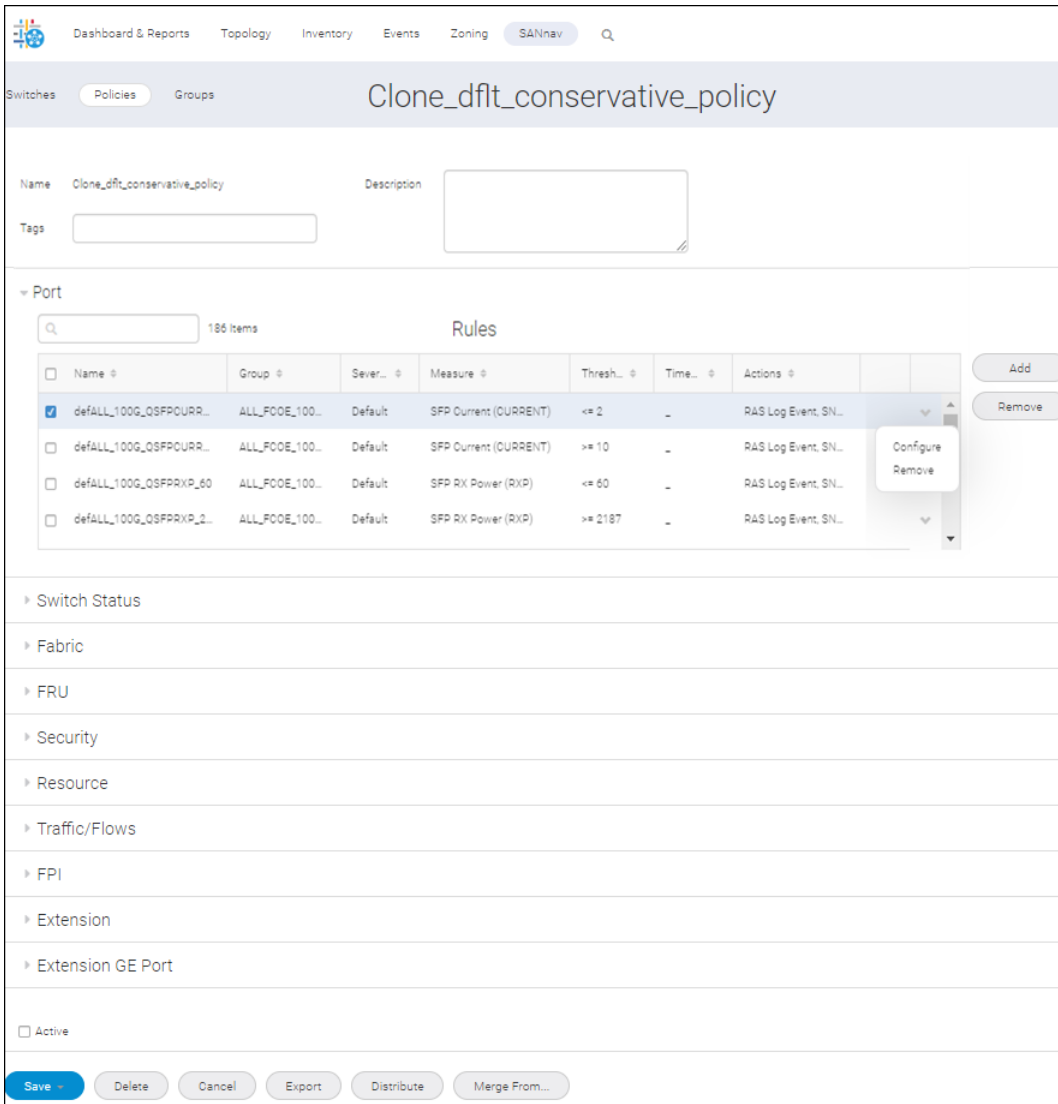
45_19

Name ^	Tags ◊	Description ◊	Status ◊	Last Modified ◊	
dft_aggressive_policy	-	-		Jul 15, 2019 11:34:28 IST	▼
dft_moderate_policy	-	-		Jul 15, 2019 11:34:28 IST	▼
dft_conservative_policy	-	-		Jul 19, 2019 11:53:52 IST	▼
dft_base_policy	-	-		Jul 15, 2019 11:34:28 IST	▼
TestingMergePolicy	-	-	Active	Jul 19, 2019 11:53:52 IST	▼
Clone_dft_conservative_policy	-	-		Jul 19, 2019 14:55:49 IST	▼

7. Select the cloned policy.

The cloned policy window appears.

8. Select the options (Port, Switch Status, Fabric, FRU, Security, Resource, Traffic/Flows, and FPI), and then select a rule to clone.
9. Click the down-arrow () of the selected rule, select the **Configure** option, and then click **Save**.



The screenshot shows the SANnav management portal interface. The main heading is "Clone_dflt_conservative_policy". Below this, there are fields for "Name" (Clone_dflt_conservative_policy) and "Description". There is also a "Tags" input field. The "Port" section is expanded, showing a search bar and "186 Items". A table of rules is displayed with columns: Name, Group, Sever., Measure, Thresh., Time., and Actions. The first rule is selected, and a context menu is open over it, showing "Configure" and "Remove" options. The "Configure" option is highlighted. Below the table, there are several expandable sections: Switch Status, Fabric, FRU, Security, Resource, Traffic/Flows, FPI, Extension, and Extension GE Port. At the bottom, there is an "Active" checkbox and a row of buttons: Save, Delete, Cancel, Export, Distribute, and Merge From...

Name	Group	Sever.	Measure	Thresh.	Time.	Actions
<input checked="" type="checkbox"/> defALL_100G_QSFPDURR...	ALL_FCOE_100...	Default	SFP Current (CURRENT)	<= 2	-	RAS Log Event, SN...
<input type="checkbox"/> defALL_100G_QSFPDURR...	ALL_FCOE_100...	Default	SFP Current (CURRENT)	>= 10	-	RAS Log Event, SN...
<input type="checkbox"/> defALL_100G_QSFP2RX_P60	ALL_FCOE_100...	Default	SFP RX Power (RXP)	<= 60	-	RAS Log Event, SN...
<input type="checkbox"/> defALL_100G_QSFP2RX_P2...	ALL_FCOE_100...	Default	SFP RX Power (RXP)	>= 2187	-	RAS Log Event, SN...

The **Configure Rule** window appears.

10. Modify the rule name and the other properties per your requirement, click **Save As**, and then click **Save**.

Configure Rule
✕

Auto-generate Rule Name

Rule Name:

Auto-Append (_number) if rule name exists

Rule Type:

Severity:

Measure:

Threshold: mAmps

Actions:

- RAS Log Event
- SNMP Trap
- E-mail
- SFP Status Marginal
- FICON Management Service

Save
Cancel

The modified rule can be viewed under the **Rules** table.

Dashboard & Reports
Topology
Inventory
Events
Zoning
SANnav
Q

Switches
Policies
Groups
Clone_dflt_conservative_policy

Name:

Tags:

Description:

Port

186 Items

Name	Group	Sever...	Measure	Thresh...	Time	Actions
<input type="checkbox"/> clone_defALL_100G_QSFPCURRENT...	ALL_F00E_100...	Warning	SFP Current (CU	>= 10	-	RAS Log Ev
<input type="checkbox"/> defALL_100G_QSFPCURRENT_10	ALL_F00E_100...	Default	SFP Current (CU	>= 10	-	RAS Log Ev
<input type="checkbox"/> defALL_100G_QSFPRXP_60	ALL_F00E_100...	Default	SFP RX Power (F	<= 60	-	RAS Log Ev
<input type="checkbox"/> defALL_100G_QSFPRXP_2187	ALL_F00E_100...	Default	SFP RX Power (F	>= 2187	-	RAS Log Ev


Add

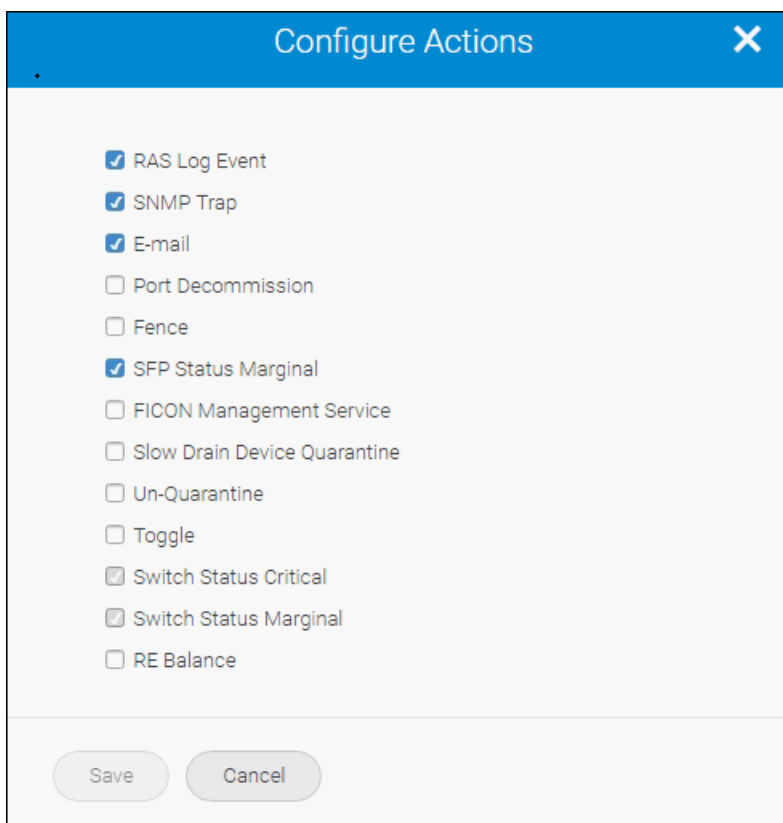
Remove

7.6.10.3 Enabling or Disabling Policy Actions on a Switch

MAPS provides actions (event notifications) in several different formats to ensure that event details are accessible from all platforms and operating systems. In response to an event, MAPS can record event data for any (or all) of the alarm options.

For example, if you define a rule in SANnav with an SNMP action and a violation of that rule occurs, the switch with the violation sends the SNMP trap only if you configured SNMP on that switch.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > MAPS Policy Management**.
2. In the **Switches** tab, click the down-arrow () for the switch on which you want to create the policy, and select **Configure Actions**.
3. Select the list of actions in the **Configure Actions** dialog that need to be configured on the switch.
The available actions vary depending on the switch selected. See [MAPS Actions](#) for information on configuring actions.




Configure Actions [X]

- RAS Log Event
- SNMP Trap
- E-mail
- Port Decommission
- Fence
- SFP Status Marginal
- FICON Management Service
- Slow Drain Device Quarantine
- Un-Quarantine
- Toggle
- Switch Status Critical
- Switch Status Marginal
- RE Balance

Save Cancel

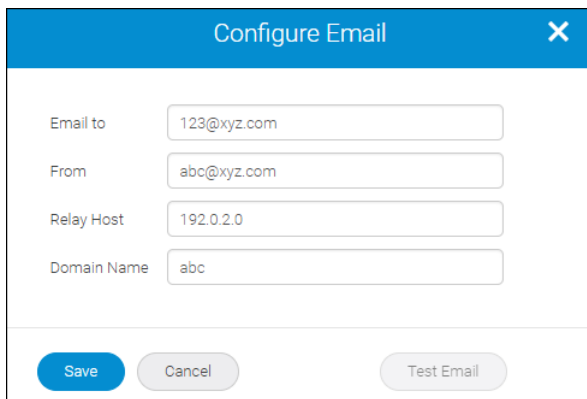
7.6.10.4 Configuring an Email Notification for MAPS

In environments where it is critical that you are notified about errors quickly, you can use email notifications to send alerts. You can add up to five comma-separated email addresses.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > MAPS Policy Management**.
2. In the **Switches** tab, click the down-arrow () for the switch on which you want to configure email notifications, and select **Configure Email**.
3. Enter the details in the **Configure Email** dialog.

Relay Host and **Domain Name** are physical chassis settings. These settings affect all logical switches in the physical chassis. The **From** address field is supported by Fabric OS 8.2.0 and later.

4. Click **Save** to configure the email settings in the switch and send email alerts about switch events to the specified email address.
5. (Optional) Click the **Test Email** button to send a test email to all the email addresses in the **Email to** field.



7.7 Fibre Channel Routing

Fibre Channel Routing (FCR) connects two or more fabrics without merging the fabrics.

The FC router connects two or more fabrics through EX_Ports or VEX_Ports. The fabric that contains the FC router is known as the backbone fabric.

An edge fabric is a standard Fibre Channel fabric with targets and initiators that are connected through an FC router to another Fibre Channel fabric.

The link between an E_Port and an EX_Port or between a VE_Port and a VEX_Port is called the inter-fabric link (IFL). LSAN is a logical SAN that spans fabrics. An LSAN is defined by zones in two or more edge or backbone fabrics that contain the same devices. LSANs enable Fibre Channel zones to cross physical SAN boundaries without merging the fabrics while maintaining the access controls of zones.

An EX_Port is a type of E_Port that connects a Fibre Channel router in a backbone fabric to an edge fabric without merging the fabrics. The EX_Ports presents proxy devices representing devices in remote fabrics. An EX_Port in the FC router connects to an E_Port in the edge fabric.

A VEX_Port is a type of VE_Port that connects a Fibre Channel router in a backbone fabric to an edge fabric over an FCIP tunnel without merging the fabrics. A VEX_Port in the FC router connects to a VE_Port in the edge fabric.

For Virtual Fabric (VF) enabled fabrics, only the base switch can be configured as the FC router. For example, EX_Ports can be configured only on a base switch for a VF-enabled switch.

In SANnav Management Portal, you can manage Fibre Channel Routing Management by clicking **SANnav** in the navigation bar, and then selecting **SAN Configuration > Fibre Channel Routing Management**. You can view all the discovered backbone fabrics and connected edge fabrics, the newly created backbone fabrics, and the configured Ex_Ports in the **Fibre Channel Routing Management** window.

7.7.1 License Requirements for Fibre Channel Routing

An Integrated Routing license is required for FC-FC routing between Fabric OS fabrics. To install an Integrated Routing license on the discovered switches to configure the EX_Ports, the below-mentioned criteria should be fulfilled:

- The Integrated Routing license must be installed for 8Gb/s and 16Gb/s FC ports on Brocade Gen 5 and Gen 6 switches to configure EX or VEX ports.
- The Integrated Routing POD license must be installed on Brocade G620 switches to configure EX_Ports.

7.7.2 Supported Platforms for Fibre Channel Routing

The supported hardware platforms are listed in the table below.

NOTE

In SANnav Management Portal irrespective of platform type, you cannot configure EX_Ports without an Integrated Routing license.

NOTE

For inter-chassis link (ICL) ports on the core blades, if all the four ports of the quad-port are not available on the same logical switch, the ports are not available for selection. You must select all the four ports in a quad for EX_Port configuration.

NOTE

In the Brocade FC32-64 port blade, you select only from port 48 to 63 to configure EX_Ports in a non virtual fabric.

Table 23: Supported Platforms and Conditions

Supported Platforms	Hardware Type	Conditions
Gen 5 (16Gb/s)	Brocade 6510 Switch	—
	Brocade 6520 Switch	—
	Brocade 7840 Extension Switch	VEX_Ports are not supported. EX_Ports are supported only in the base switch.
	Brocade DCX 8510 Backbones 16Gb/s port blades (FC16-32, FC16-48, FC16-64) FX8-24 extension blade ICL ports on the core blades	An EX_Port on an ICL is supported only in DCX 8510-8 and DCX 8510-4 when all port blades in the chassis belong to one of these blade types: FC16-32, FC16-48, FC16-64.
Gen 6 (32Gb/s)	Brocade G610	—
	Brocade G620	—
	Brocade G630	—
Brocade X6 Directors	FC32-48 port blade FC32-64 port blade SX6 extension blade	VEX_Ports are not supported on the extension blade.

7.7.3 Limitations of Fibre Channel Routing

Interop mode 5 (Brocade NOS interop mode) is not available from Fabric OS 8.2.0 and above.

In SANnav Management Portal, only Brocade native IM0 is supported irrespective of any Fabric OS version. You cannot configure IM5 on Fabric OS 7.4.x.

The backbone fabric connected to NOS edges can be discovered but the EX_Ports connected to the NOS edge are greyed out and cannot be configured or removed.

7.7.3.1 Backbone Fabric ID Conditions

- If an active router is present in the fabric and you want to add a new router in the same fabric, SANnav will change the backbone ID to the existing backbone ID.
- If multiple routers are present in the same fabric, the first created backbone ID is applied by SANnav when you create a new backbone fabric.
- When multiple active routers are present in the same fabric with different backbone fabric IDs, SANnav will list the lowest backbone fabric ID among them.
- If EX_Ports are configured using CLI scripts, but FCR is disabled and when you want to configure ports in SANnav, perform the following:
 - Delete all the configured ports.
 - Rediscover the switches and then add the ports.
- By default the backbone fabric ID is 1 when you select a non-VF to configure a new backbone (when FCR is disabled or no EX_Ports are configured), you can modify the default backbone fabric ID. In case of VF, SANnav does not allow you to modify the default backbone ID.

7.7.4 Configuring a Backbone Fabric

To create a new backbone fabric, follow the instructions below.

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Fibre Channel Routing Management**.
2. Click the **+** icon on the top-right corner of the window, and select a fabric to be added as a backbone.

NOTE

You can select only one fabric at a time. Fabrics that have at least one platform with an Integrated Routing license will be listed.

3. Click **OK** to configure the selected fabric as the backbone.
4. Enter the backbone fabric ID.

NOTE

For Virtual Fabrics, the base fabric ID is reflected as a backbone fabric ID and cannot be modified.

For non Virtual Fabrics, if the switches do not contain a fabric ID, you should enter the backbone fabric ID. In case of switches with a fabric ID, you can select any fabric ID from the drop-down.

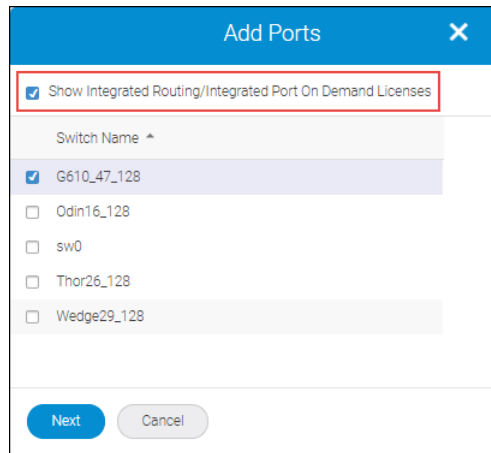
The backbone fabric ID ranges from a 1 to 128 characters.

The screenshot shows the SANnav interface for configuring a backbone fabric. The breadcrumb navigation is 'Dashboard & Reports > Topology > Inventory > Events > Zoning > SANnav'. The main heading is 'DND-FID10_BB'. Below the heading, there is a 'Backbone Fabric ID' input field with the value '10'. A search bar shows '1 Item'. The 'Ports' table has the following data:

Name	Switch	Edge Fabric ID	Status	
slot11 port30_1	switch_10_new	13	No_Light	<input type="checkbox"/> Add <input type="button" value="Configure"/> <input type="button" value="Remove"/>

At the bottom of the form are 'Save', 'Delete', and 'Cancel' buttons.

5. Add ports to the backbone fabric. The **Add Ports** dialog appears.
 - a. Click **Add** to select the switches in the fabric.
 - b. Checking **Show Integrated Routing/Integrated Port On Demand Licenses**, displays only the switches for which you can configure EX_Ports.


NOTE

If you uncheck **Show Integrated Routing/Integrated Port On Demand Licenses** the switches that do not have Integrated Routing licenses are also displayed.

- c. Select the switches and click **Next** to list all the ports.

NOTE

For Fabric OS 8.1.0 or later versions, you can select a maximum of 16 switches.

For versions earlier than Fabric OS 8.1.0, you can select a maximum of 12 switches.

- d. Select the ports and click **Next** to configure the ports as EX_Ports.

NOTE

SANnav does not support ports with the FCIP or Ethernet protocol to configure VEX_Ports.

NOTE

The ports already configured as EX_Ports are not listed.

When configuring EX_Ports, ensure that the edge fabric ID is consistent for all EX_Ports that connect to the same edge fabric.

Ensure that the ports to be configured as EX_Ports are not connected.

- e. Enter the edge ID in the **Edge Fabric ID** field in the **Add Ports** window.
- f. Enter the virtual switch ID for the edge fabric in the **Front Domain ID** field.

Fill in the port properties.

- g. Select the **Enable** check box to access the specified port.

NOTE

If the **Enable** check box is not selected, the EX_Port will be configured, but it will be in a disabled state.

- h. Click **OK** to list the ports in the fabric window.
6. Click **Save** to configure the backbone fabric.

Click **OK** in the confirmation dialog.

SANnav performs the following operations:


- In case of non-VF, the backbone fabric ID is configured on all switches in the fabric (for the switches with and without a routing license).
- The FC Routing service is enabled on all switches selected for EX_Port configuration (if FCR is not enabled already).
- Assigns edge fabric ID and EX_Port configuration.

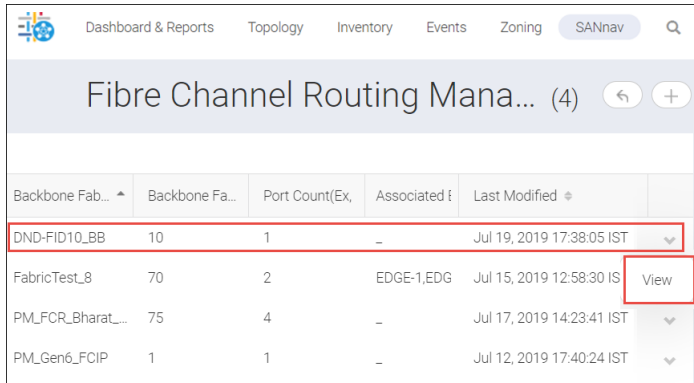
The new backbone fabric will take some time to reflect in the **Fibre Channel Routing Management** window.





You can view the progress in the **Events** tab.

7.7.5 Editing a Backbone Fabric

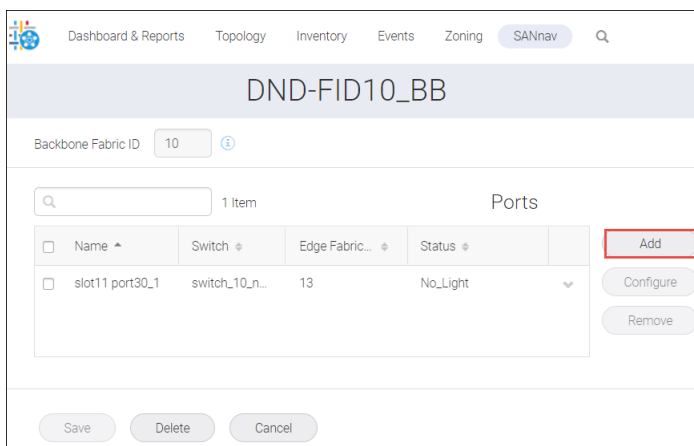
To edit a configured backbone fabric from the Fibre Channel Routing Management window, follow the instructions below:


1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Fibre Channel Routing Management**.
2. Click the down arrow icon () on an existing backbone, and then select **View**.




Backbone Fab...	Backbone Fa...	Port Count(Ex,	Associated f	Last Modified	
DND-FID10_BB	10	1	-	Jul 19, 2019 17:38:05 IST	
FabricTest_8	70	2	EDGE-1,EDG	Jul 15, 2019 12:58:30 IS	 View
PM_FCR_Bharat...	75	4	-	Jul 17, 2019 14:23:41 IST	
PM_Gen6_FCIP	1	1	-	Jul 12, 2019 17:40:24 IST	

3. Click **Add** to add a new port.



Name	Switch	Edge Fabric...	Status	
slot11 port30_1	switch_10_n...	13	No_Light	

4. For configuring and removing ports from the backbone fabric, perform the following steps:
 - a. Click the down arrow icon () on a port, and select **Configure** or **Remove**.

You can select multiple ports and click **Configure** to edit the port properties or **Remove** to reset the specific EX-Ports.

You can also enable or disable the ports in the **Configure** window.

- b. Click **OK** to confirm the changes.
5. Click **Save** to overwrite the changes.
 - Click **Cancel** to discard the changes.
 - Click **Delete** to delete the configured backbone fabric.

When you click **Delete** SANnav disables the EX_Ports and changes the EX_Ports to normal ports. Also, SANnav disables the Fibre Channel Routing service but retains the configured backbone fabric ID.

NOTE

There is no provision to configure the Translate domain.

It will take some time to reflect the changes in the **Fibre Channel Routing Management** window.

You can view the progress in the **Events** tab.

7.7.6 Viewing the FCR Topology

You can view the FCR in the **Inventory** tab. The topology view shows a hierarchical graphical presentation of the configured FCR.

To view the FCR in the **Inventory** tab, follow the instructions below:

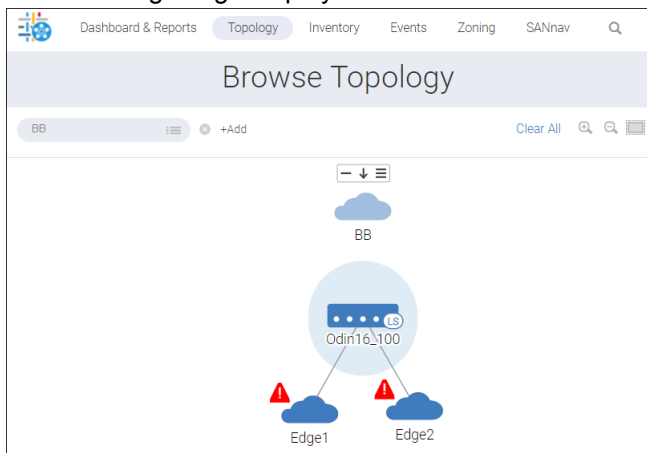
1. Select **Inventory** in the navigation bar, and then click the **Switches** drop-down to select **Fabrics**.
By default, the switches inventory list is displayed.

Type	WWN	IP Ad.	FID	Fabric	Health	Model	Firm...	Port C	Location
Switch	10:00:50...	10.124.7...	128	Zoning_F	Healthy	Brocade ...	v8.2.2_bi	47	End User Pre
Switch	10:00:C4...	10.155.4...	67	delete_m	Healthy	Brocade ...	v8.2.1b_	2	End User Pre
Switch	10:00:C4...	10.155.4...	71	Fabric_71	Degraded	Brocade ...	v8.2.1b_	2	End User Pre

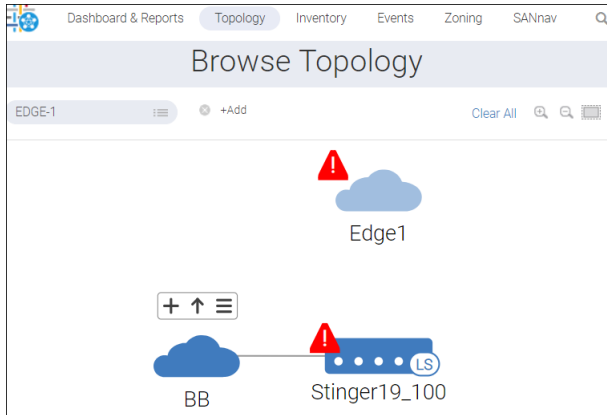
- Click () on a selected fabric, and select **Show in Topology** to view the selected fabric in context in the **Browse Topology** window.


Name	Tags	Health	Active...	Seed ...	Seed S...	Principal ...	FID	Switch	Last Discovery
century	-	Poor	-	cent	10.155.45...	10.155.45.18	100	1	Jul 23, 2019 15:37:
delete	-	Healthy	-	delete	10.124.74...	10.124.74.123	12	1	Jul 23, 2019 15:37:
BB	-	Healthy	-	45_19	10.155.45...	10.155.45.19	67	1	Jul 23, 2019 15:37:
dffd	-	Poor	-	test123	10.102.18...	10.102.18.12	58	1	Jul :
DiscoveryF...	-	Poor	-	switch15...	10.124.74...	10.124.74.154	14	2	Jul :
DND-FID 5...	-	Poor	-	nancfg	switch_18	10.155.45...	5	2	Jul 23, 2019 15:37:

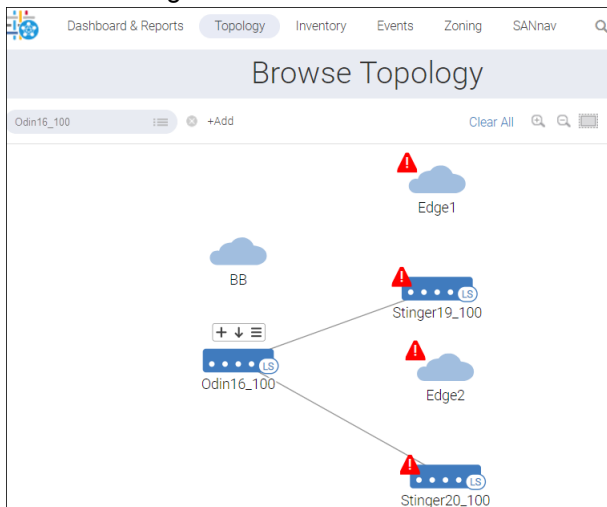
The following image displays the backbone fabric in context along with its edge fabrics.



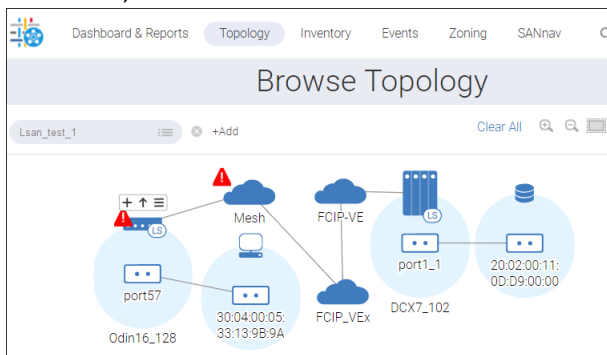
Click the up-arrow icon () to view the edge fabric in context with the backbone fabric and the switch associated with it.






Click the up-arrow icon () on a backbone switch to represent the backbone switch in context with the connected edge fabric switches.



The LSan zones are viewed in context with its immediate end devices connected to switches and fabrics (edge and backbone).



- Hover the mouse over the fabric icon, switch icon, or port icon, and click the up-arrow icon () to view the selected icons in context.
- Hover the mouse over each switch, and click the + icon () to display the physical ports.
- Hover the mouse over the fabric icon, switch icon, or port icon, click the hamburger icon (), and select any of the attributes.

7.8 vCenter Discovery

The VMware vCenter allows you to create virtual machines through the ESXi operating system. The vCenter feature enables you to discover the ESXi host and the virtual machines present inside the discovered vCenter server. By discovering the vCenter, you can perform the following actions:

- View ESXi hosts
- View virtual machines created in the hosts
- Monitor or unmonitor ESXi hosts
- Monitor virtual machine alarms in the SANnav Management Portal **Events** tab

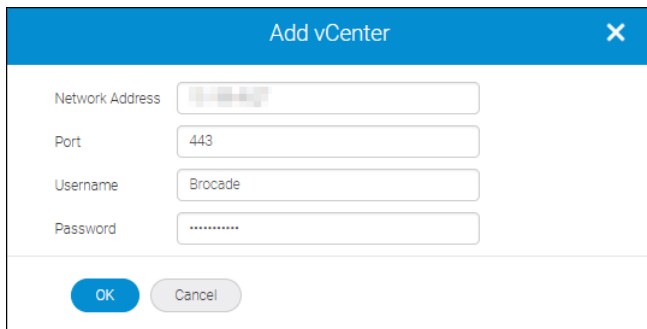
7.8.1 Adding the vCenter

To add the VMware vCenter, follow the instructions below:

NOTE

SANnav Management Portal supports VMware vCenter server versions 6.0 and later.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > vCenter Discovery**.
2. Click the **+** icon on the top-right corner of the window in the **Discovered vCenters** window. The **Add vCenter** dialog appears.



3. Enter the vCenter IP address and login credentials.
4. Click **OK** to discover the vCenter.

7.8.2 Monitoring or Unmonitoring ESXi Hosts

To monitor or unmonitor the hosts in a VMware vCenter, follow the instructions below:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > vCenter Discovery**.
2. Click (▼) on a discovered VMware vCenter, and select **View**.
3. Select one or more hosts, and click **Monitor** or **Unmonitor**.
4. Click **Save** to update the tags and description.

7.8.3 Rediscovering ESXi Hosts

You can rediscover an already discovered vCenter to list the updated information about the vCenter server.

To rediscover the latest ESXi hosts, follow the instructions below:

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > vCenter Discovery**.
2. Click (▼) on a discovered VMware vCenter, and select **View**.
3. Click **Rediscover**.

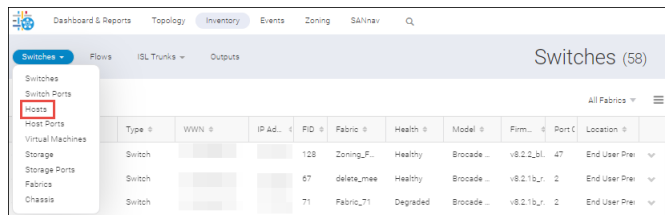
7.8.4 Viewing ESXi Host Properties

In the **Inventory** window, you can view the list of ESXi hosts discovered in the vCenter. Based on FDMI information, manual and auto-discovered hosts are listed along with the ESXi hosts.

To view the ESXi host properties, follow the instructions below:

1. Select the **Inventory** tab in the navigation bar, and then click the **Switches** drop-down and select **Hosts**.

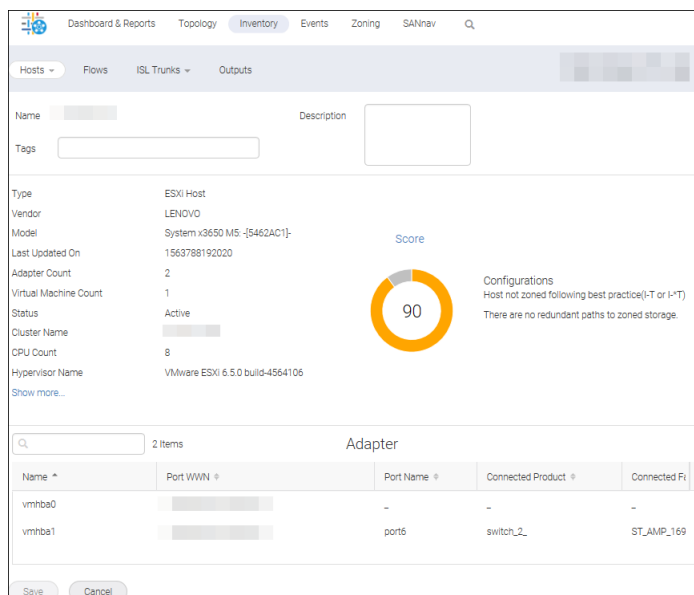
By default, the switches inventory list is displayed.



2. Click () on a selected ESXi host, and select **View**.

The selected ESXi host properties window is displayed.

The ESXi host window displays the ESXi properties and the adapter details.



3. Click () on an adapter, and select **Show Properties** to view the adapter properties.

4. Click **Save** to save the tags and description.

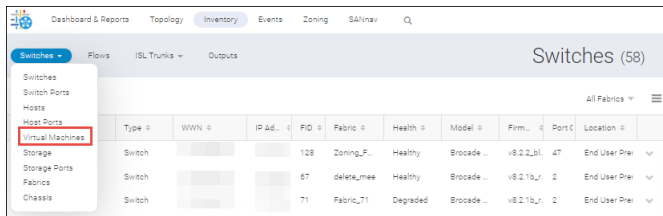
7.8.5 Investigating Virtual Machines


To investigate the CPU, memory, network, and disk utilization, perform the following steps:

1. Select the **Inventory** tab in the navigation bar, and then click the **Switches** drop-down and select **Virtual Machines**.

By default, the switches inventory list is displayed.

- Click the **Switches** drop-down, and select **Virtual Machines**.



- Click () on a selected virtual machine, and select **Investigate**.

Name ^	Tags ⇅	UUID ⇅	Host ⇅	vCenter Name ⇅	IP Address ⇅	Network A	Status ⇅
AShutosh_Win12_75_2...	-	564d4b3c-9d...		VMware vCenter Se...		Win2k12_A	Running
VCENTER_VM	-	564ddccc-2b7...		VMware vCenter Se...	-	-	View Investigate
WIN12R2_74_231	-	42051630-82...		VMware vCenter Se...	-	-	
Windows-2016	-	564d403e-dfa...		VMware vCenter Se...	-	-	Stopped

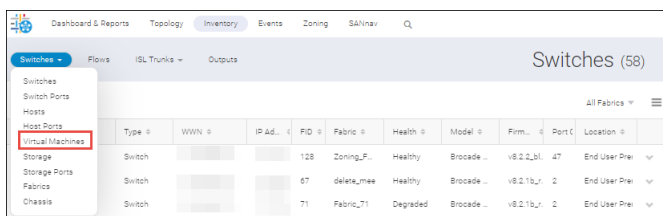
The **Investigation Mode** window appears. The **Investigation Mode** window displays the CPU, network, memory, and disk utilization statistics.

7.8.6 Viewing Virtual Machine Properties

You can view the list of virtual machines in the vCenter.

To view the virtual machine, follow the instructions below:

- Select the **Inventory** tab in the navigation bar, and then click the **Switches** drop-down and select **Virtual Machines**. By default, the switches inventory list is displayed.



- Click () on a selected virtual machine, and select **View**.

The **Virtual Machine** window displays the VM properties, VM path information, and VM datastore information.

Dashboard & Reports Topology **Inventory** Events Zoning SANnav Q

Virtual Machines Flows ISL Trunks Outputs AShutosh_Win12_75.241

Name AShutosh_Win12_75.241 Description

Tags

UUID 564d4b3c-9d1e-359fb0ab-a372c3b0dec1

Network Address Win2k12_Ashu.Broadcom.net

Hypervisor VMware ESXi 6.5.0 build-8294253

Operating System Microsoft Windows Server 2012 (64-bit)

Status Running

CPU Resource 0 MHz reserved, no maximum limit

Memory Size 16384 MB

Instance UUID 526027e2-b2d7-dade-15a9-69dc51952e9b

Used Storage 796.11 GB

Connection State CONNECTED

Show more...

0 Items VM Path Information

Name	Initiator	Target	Status	Device Name	Model	Storage	Storage Status
No data to display.							

1 Item VM Datastore Information

Name	Location	Status	Type	Total Capacity	Free Space	Last Updated On
datastore1	ds://vmfs/vme/5...	normal	VMFS	1.63 TB	148.38 GB	Jun 18, 2019 11:19:5...

Save Cancel Investigate

NOTE

You can investigate the CPU, memory, network, and disk utilization by clicking the **Investigate** button. For more information, see [Investigating Virtual Machines](#) section.

- Click () an entry in the **VM Path Information** area or **VM Datastore Information** area, and select **Show Properties** to view the properties.
- Click **Save** to save the tags and description.

7.8.7 Viewing ESXi Hosts in Topology

The **Topology** tab presents a graphical presentation of the VMware vCenter server. You can access this view from the **Inventory** tab or the **Topology** tab.

- Select **Inventory** tab in the navigation bar, and then click the **Switches** drop-down and select **Hosts**.

Dashboard & Reports Topology **Inventory** Events Zoning SANnav Q

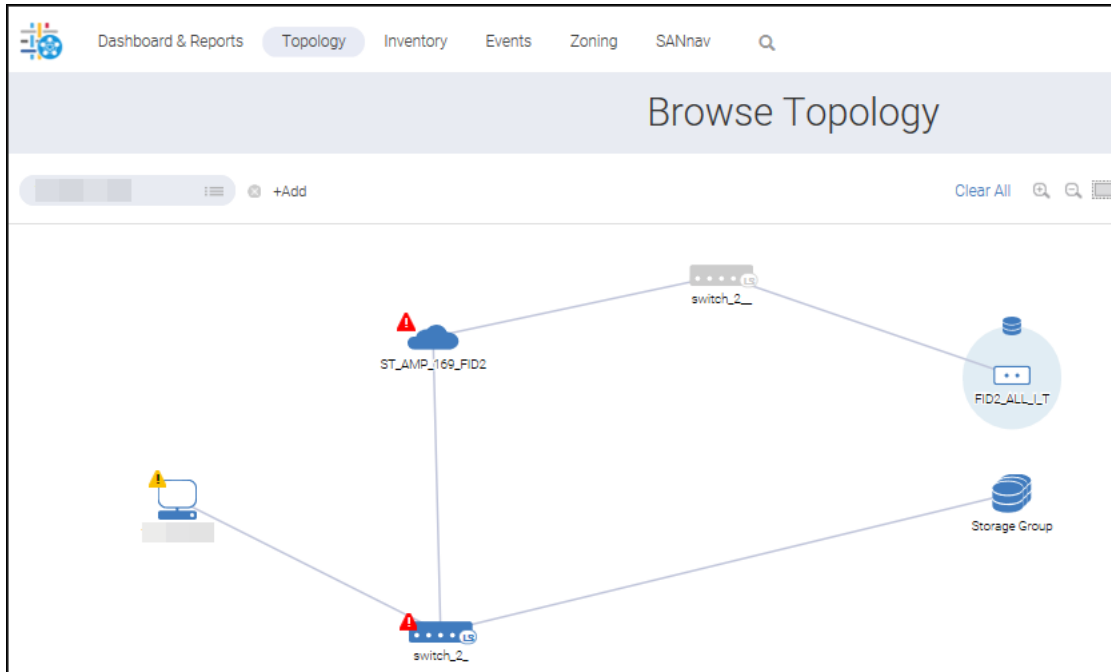
Switches (58)

Switches Switch Ports **Hosts** Host Ports Virtual Machines Storage Storage Ports Fabrics Chassis

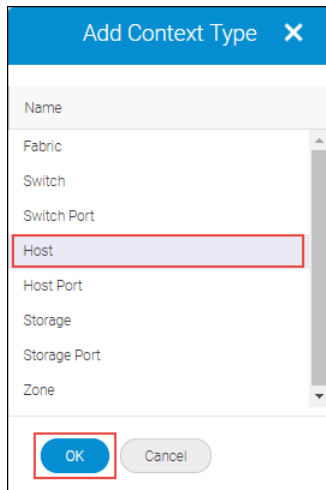
Type	WWN	IP Ad.	FID	Fabric	Health	Model	Firm.	Port C	Location
Switch			128	Zoning_F...	Healthy	Brocade ...	v8.2.1b...	27	End User Pri...
Switch			67	delera_mee...	Healthy	Brocade ...	v8.2.1b...	2	End User Pri...
Switch			71	Fabric_T1	Degraded	Brocade ...	v8.2.1b...	2	End User Pri...

By default, the switches inventory list is displayed.

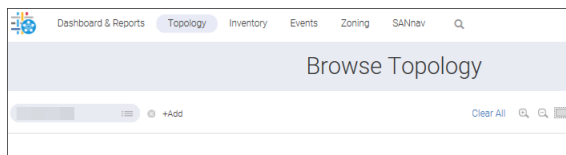
- Click () on a selected ESXi host, and select **Show in Topology**. The **Browse Topology** window is displayed.



3. Alternatively, you can view the topology directly from the **Topology** tab.
 - a. Select the **Topology** tab in the navigation bar.
The **Browse Topology** window is displayed.
 - b. Click **+** on the **Browse Topology** window, select **Host**, and click **OK**.



- c. Enter the host IP address, and press **Enter**.




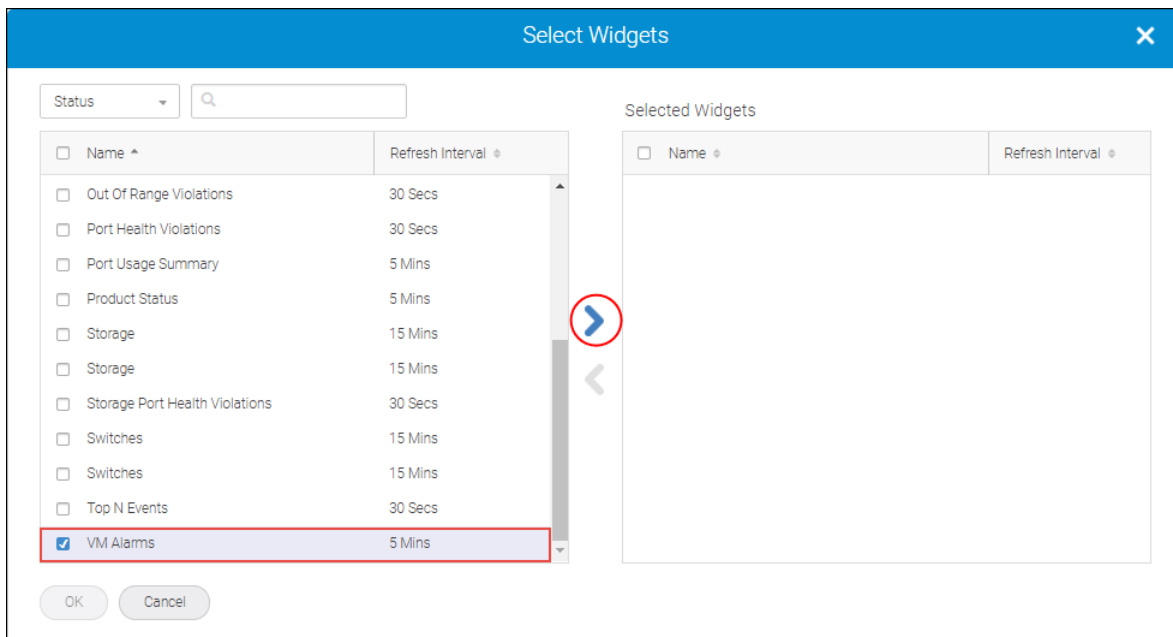
- d. Click **+Add** to add other contexts.

7.8.8 Creating a VM Alarms Dashboard

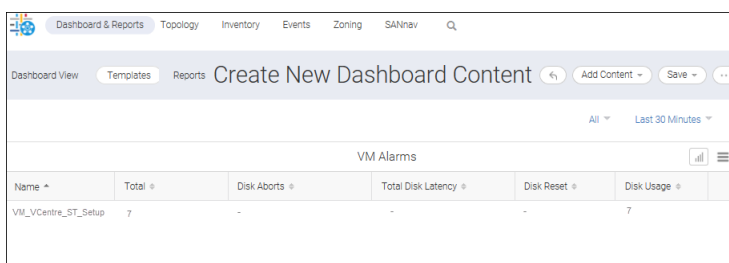
You can monitor the vCenter in the SANnav Management Portal dashboard with the help of the VM Alarms widget.

To add the VM Alarms widgets to your dashboard view, follow the instructions below:

1. Select the **Dashboard & Reports** tab in the navigation bar, and then click the **Templates** tab.
2. Click **+** on the top-right corner of the **Templates** page, and then click **Dashboard > Select Widgets**.
3. Select **VM Alarms** and click () to move the widget to the **Selected Widgets** column.



4. Click **OK** to add the widget to the dashboard.



5. Click **Save** to save the content.

As a best practice, first discover the fabrics and then vCenter to view the VM alarms immediately. If vCenter is discovered and then the fabric is discovered, SANnav Management Portal will take some time to generate VM alarms. The events are created after the creation of the VM and dashboard alarms, vCenter discovery, and ESXi discovery.

7.9 FICON

IBM Fibre Connection (FICON) is a protocol used between IBM (and compatible) mainframes and storage.

FICON fabrics require a FICON logical switch. Note that the default switch cannot be used as a FICON logical switch, so Virtual Fabrics must be enabled and used.

NOTE

To configure FICON fabrics, you must have the FICON Management privilege with read-write permission. To access the FICON fabric feature, you must have the FICON Management privilege with read permission.

For more information on FICON, refer to the *Brocade Fabric OS FICON Administration Guide*.

Supported Platforms for FICON Fabrics

The following table lists the platforms that support FICON fabrics.

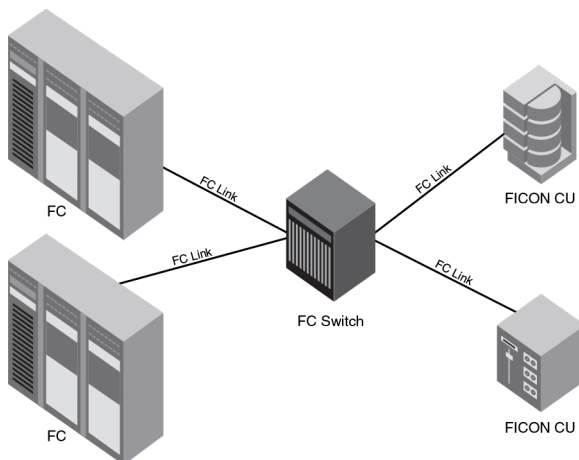
Table 24: Platforms That Support FICON Logical Fabrics

Platforms	Directors (16Gb/s)	Switches (16Gb/s)	Directors (32Gb/s)	Switches (32Gb/s)
Gen 6	N/A	N/A	<ul style="list-style-type: none"> ■ Brocade X6-4 ■ Brocade X6-8 	<ul style="list-style-type: none"> ■ Brocade G620 ■ Brocade G630
Gen 5	<ul style="list-style-type: none"> ■ Brocade DCX 8510-4 ■ Brocade DCX 8510-8 	<ul style="list-style-type: none"> ■ Brocade 6510 	N/A	N/A

FICON Configurations

FICON configurations can be categorized into three types, based on complexity:

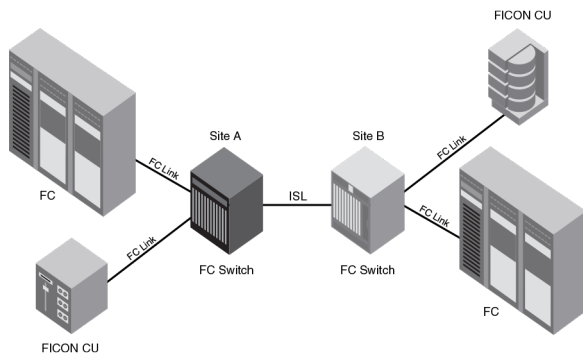
- Point-to-point configurations that do not use a switch.
- Switched point-to-point configurations, also called single switch configurations, connect a host channel to a storage control unit using a single switch. In this type of configuration, the channel is configured to use single-byte addressing.

Figure 29: Switched Point-to-Point FICON

- Cascaded FICON refers to an implementation of FICON that uses one or more FICON channel paths in which the domain ID of the entry switch is different than the domain ID of the switch where the control unit (CU) is attached. Therefore, cascading requires a 2-byte link address. Anytime a 2-byte link address is defined on a channel, all link addresses associated with that channel must be 2-byte link addresses.

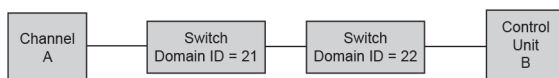
Switches may be interconnected using the following links:

- Traditional inter-switch links (ISLs)
- Inter-chassis links (ICLs)
- Fibre Channel over Internet Protocol (FCIP)
- Base fabric (LISLs/XISLs)

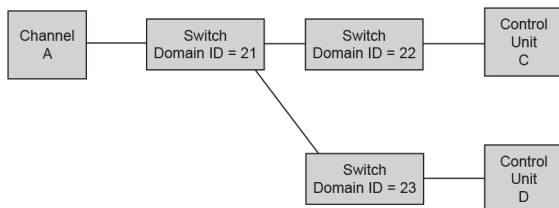
Figure 30: Cascaded FICON

Cascaded configurations, also called high-integrity fabrics, connect host channels and storage control units that reside in different domains. Cascaded FICON fabrics must be configured as high-integrity fabrics. In this type of configuration, the channel is configured to use two-byte link addressing.

The following figures show two cascaded configurations. These configurations require Channel A to be configured for 2-byte addressing. It is recommended that there be only two domains in a path from a FICON channel interface to a FICON control unit interface.

Figure 31: Cascaded Configuration: Two Switches

The following figure illustrates multiple switches cascaded off switch 21. As of Fabric OS 8.1.0b, up to three hops are supported from the channel to the control unit.

Figure 32: Cascaded Configuration: Core-Edge Architecture

7.9.1 Viewing FICON Fabrics

To view FICON fabrics, you must have the FICON Management privilege with read only permission.

NOTE

For FICON fabrics, SANnav requires at least one switch running Fabric OS 8.1 or later that has HIF mode enabled or is a FICON logical switch.

This procedure enables you to view all configured FICON fabrics. The FICON display configures any table that contains FICON descriptions to include the following columns: Attached Port#, FC Address, Serial #, Tag, Product Type, Model, Vendor, Port Type, and WWN. To set the FICON display, see [Configuring the FICON Display](#).

To view a FICON fabric, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**.
The **Logical Fabrics** window displays.
2. Click **FICON Fabrics**.
The **FICON Fabrics** window displays.

Logical Fabrics								FICON Fabrics(6)		Actions	
Name	Tags	Description	Fabric ID	Seed Switch IP Address	Principal Switch WWN	Status	Last Modified				
<input type="checkbox"/> 53_FICON Logical Fabric	-	-	53	10.38.46.82	10.00.00.27.F8.F3.3D.B4	Active	Aug 13, 2019 16:29:39 MDT				
<input type="checkbox"/> FICON_66	-	-	66	10.38.46.82	10.00.00.27.F8.F3.3D.B3	Active	Aug 13, 2019 16:30:32 MDT				
<input type="checkbox"/> Ficon_Fabric_Learning	-	-	44	10.38.46.82	10.00.00.27.F8.F3.3D.B2	Active	Aug 13, 2019 16:28:29 MDT				
<input type="checkbox"/> IBM_87	-	-	87	10.38.46.82	10.00.00.27.F8.F3.3D.B6	Active	Aug 13, 2019 16:32:37 MDT				
<input type="checkbox"/> JPMC_Columbus_22	-	-	22	10.38.46.82	10.00.00.27.F8.F3.3D.B7	Active	Aug 13, 2019 16:27:14 MDT				
<input type="checkbox"/> Wedge_2_FICON	-	-	2	10.38.46.39	10.00.04.F5.7C.4D.68.79	Active	Aug 13, 2019 16:40:27 MDT				

- Click the name of the FICON fabric for which you want to view additional data. The detail page for the selected FICON fabric displays.

Fabric properties

Name: Description:

Tags:

Fabric ID:

Switches list

2 Items

Name	WWN	IP Address	Domain ID	Model	VF St.	Status	RNID Tag	
<input type="checkbox"/> 53_AllegianceBottom	10.00.00.27.F8.F3.88.80	10.38.46.82 [53]	0x79	Brocade X6-8	Enabled	Discovered: Seed Switch	79ff	<input type="button" value="Add"/> <input type="button" value="Remove"/>
<input type="checkbox"/> 53_AllegianceTop	10.00.00.27.F8.F3.3D.B4	10.38.46.228 [53]	0x7A	Brocade X6-8	Enabled	Discovered	7aff	

Fabric parameters

RA TOV: Allow XL use

ED TOV: Enable vice probing

Maximum Hops: Per-fran routing priority

BB Credit: SuppresClass F traffic

Data Field Size: Long dance fabric

Routing Policy:

Activate

4. Click the right arrow to expand the FICON fabric parameters.
 - **RA TOV**. Default is 10000. The Resource Allocation TimeOut Value (RA TOV). Do not change unless directed by your switch service provider.
 - **ED TOV**. Default is 2000. The Error Detect TimeOut Value (ED TOV). Do not change unless directed by your switch service provider.
 - **Maximum Hops**. Default is 7. Do not change unless directed by your switch service provider.
 - **BB Credit**. Default is 16. Do not change unless directed by your switch service provider.
 - **Data Field Size**. Default is 2112. Do not change unless directed by your switch service provider.
 - **Routing Policy**. Default is Device Based. Select the routing policy (**Device Based** or **Exchange Based**).
 - **Allow XISL use** check box. Default is not selected. When selected, ICL ports do not display in the available ports list. However, if you previously added ICL ports to the FICON fabric, this check box is not available.
 - **Per-frame routing priority** check box. Do not select this check box.
 - **Enable device probing** check box. Selected by default. The recommended best practice is to disable device probing. When not selected, third-party software, except for CUP, is prohibited from managing the switch. Do not select this check box unless otherwise advised by your switch service provider.
 - **Suppress Class F traffic** check box. Do not select this check box.
 - **Long distance fabric** check box. The recommended best practice is to configure individual ports for long distance when cascading at extended distances. This parameter sets E_Ports to LD mode (increases BB credits for long-distance performance). Select this check box only when ISLs between the switch and a connected device exceed 10 km. Dense wavelength division multiplexing (DWDM) equipment usually provides BB credits, so there is typically no reason for additional BB credits unless there are direct ISLs between switches or coarse wavelength division multiplexing (CWDM) is being used. A long-distance fabric requires a license.
 - **Activate** check box. Select to activate the FICON fabric. For more information about activating a FICON fabric and the associated automatic FICON configurations that occur on the FICON devices, see [Activating a FICON Fabric](#).
5. Click **Cancel** to close the detail page for the selected FICON fabric.

7.9.2 Configuring the FICON Display

To set the FICON display, you must have the FICON Management privilege with read-write permission.

The FICON display setup configures any table that contains FICON descriptions for switches and switch ports to include the following columns: Attached Port#, FC Address, Serial #, Tag, Product Type, Model, Vendor, Port Type, and WWN. To set the FICON display, complete the following steps.

1. Click the user icon in the top right corner of the window, and then click **User Preferences**.
The **Preferences** window displays.
2. Click **Edit** next to **Tables**.
The **Tables** window displays.
3. Click the **FICON Display** check box.
4. Select **Yes** from the **Persist Last Column Selection** menu.
5. Click **Save**.

FICON Display now shows as **Enabled** under **Tables**. You can verify this change by checking one of the changed tables. For example, click **Inventory** in the navigation bar to verify the changes in the **Switches** table of the **Inventory** page.

7.9.3 FICON Planning

This section provides a basic guide for configuring a switch for FICON operation. Procedures assume that the switch is installed and IP addresses are assigned to the switch for discovery and access by SANnav. These procedures may refer to additional sections in this chapter or chapters in this manual for more detailed information.

7.9.3.1 Planning the Configuration

Perform the following tasks to plan your configuration:

1. Obtain a high-level drawing of the intended fabric configuration.
2. Obtain all required license keys for the switch features and the SANnav application.

Licenses must be converted from transaction codes that are delivered with the switch. Access to a public Internet connection is required.

It is highly recommended that you obtain license keys before the scheduled configuration.

3. Obtain all versions of firmware for switches that will be managed by SANnav so that you can add them to the SANnav firmware repository in [Importing Firmware Files to the Repository](#).

NOTE

For FICON fabrics, SANnav requires at least one switch running Fabric OS 8.1 or later that has HIF mode enabled or is a FICON logical switch.

Although switches are loaded with the latest firmware at the time of manufacture, firmware may be out of date due to switch storage and transit times. If adding a switch to an existing fabric, you may need to upgrade the existing fabric, downgrade the new switch, or use a mixture of firmware in the fabric. Note that using firmware versions for switches in the same fabric that vary by one release is not recommended.

Observe the following best practices:

- Always check the version of firmware on a switch.
 - Unless otherwise advised by a certified Fabric OS support professional, always load the most recently qualified firmware.
 - Before upgrading or downgrading firmware, read the upgrade and downgrade considerations in the firmware release notes.
4. If incorporating more than one switch into a fabric, see the planning steps in [Cascaded FICON Fabric](#).
 5. Make a record of the following information for the switch:
 - Fabric name.
 - Switch name.
 - Domain ID (DID).

Domain IDs are entered in hexadecimal. Use a domain ID that is the hexadecimal equivalent of the switch ID in the Input/Output Configuration Program (IOCP). For example, for switch ID 1F, set the domain ID to 1F in hexadecimal. The recommended best practice is the make the hexadecimal equivalent of the domain ID match the switch ID in the hardware configuration definition (HCD) or IOCP.

Also, use a unique domain ID for every switch, although this is obviously not possible in very large data centers.
 - Fabric ID (FID).

Configure a FID for the FICON fabric. A FID can be any number from 1 through 128, and all switches in the same FICON fabric must have the same FID. Note that FICON Management Server (FMS) cannot be enabled in the default switch. Therefore, the recommended best practice is leave the default switch FID at 128 and create a new

FICON logical switch for all FICON ports. A simple FID numbering scheme starting from 1 is recommended. There is no correlation between the FID and the DID.

- SANnav IP address.

- Administrator password.

SANnav is configured to manage the switch as an admin user. The default admin password is “password.” You do not need to change the password during installation; however, if the password is changed, the password for device discovery must be changed also. Although launched from SANnav, the Element Manager (Web Tools) passwords do not propagate in SANnav.

The recommended best practice is to create identical passwords for all switches in the same fabric. This not only simplifies discovery, but in most cases since users are given access to a fabric, not an individual switch, there are fewer passwords to remember and maintain.

- Call home number.

This may not apply. If using a call home service, you will need the phone number for the service and an understanding of what is being covered in the service agreement.

- Required firmware for the switch (see Step 3).

- Port addressing.

The port address is important because it is implemented in HCD or IOCP. The easiest port addressing scheme is to start from 0x00 at the bottom left of the port card, increment on ports going up the card, and then continue starting numbering from the bottom right of the next column of ports.

6. If you are considering creating a cascaded switch configuration, consider connecting all ISLs between switches first. This will help simplify cascaded configuration. If this is not possible, you can merge cascaded fabrics later using steps in [Cascaded FICON Fabric Merge](#).
7. If you are considering connecting cascaded switches over IP networks, see the planning considerations in [Connecting Cascaded FICON Fabrics Over FCIP](#).

7.9.4 FICON Fabric Configuration

This section provides a basic guide for configuring a switch for FICON operation. Procedures assume that the switch is physically installed in your SAN and IP addresses are assigned to the switch for discovery and access by SANnav. These procedures may refer to additional sections in this chapter or chapters in this manual for more detailed information.

Cascaded FICON Fabric

SANnav enables you to easily configure a fabric for cascaded FICON. You must have FICON Management privileges to configure a fabric for cascaded FICON.

NOTE

Configuring a fabric for cascaded FICON may be disruptive to current I/O operations in the fabric, as this involves disabling and enabling the switches in the fabric.

NOTE

If HIF mode is not enabled and the FMS mode is deployed, then the FICON fabric sets the HIF key during the FICON fabric deployment.

FICON configuration performs the following operations on the selected fabric:

- Turns on the insistent domain ID flag (IDID) on all switches.
- Sets High Integrity Fabric Configuration (HIFC) on the seed switch.

- The Fabric-Wide Consistency Policy (FWCP) is configured to include SCC in strict mode.
- The SCC policy is created or modified to limit connectivity to only the switches in the selected fabric.
- Enables device-based routing on all switches.
- Enables In-Order Delivery (IOD) on all switches.
- Enables Dynamic Load Sharing (DLS) based on user selection and the firmware level.

7.9.4.1 Configuring a Cascaded FICON Fabric

To configure cascaded FICON fabrics, you must have the FICON Management privilege with read-write permission.

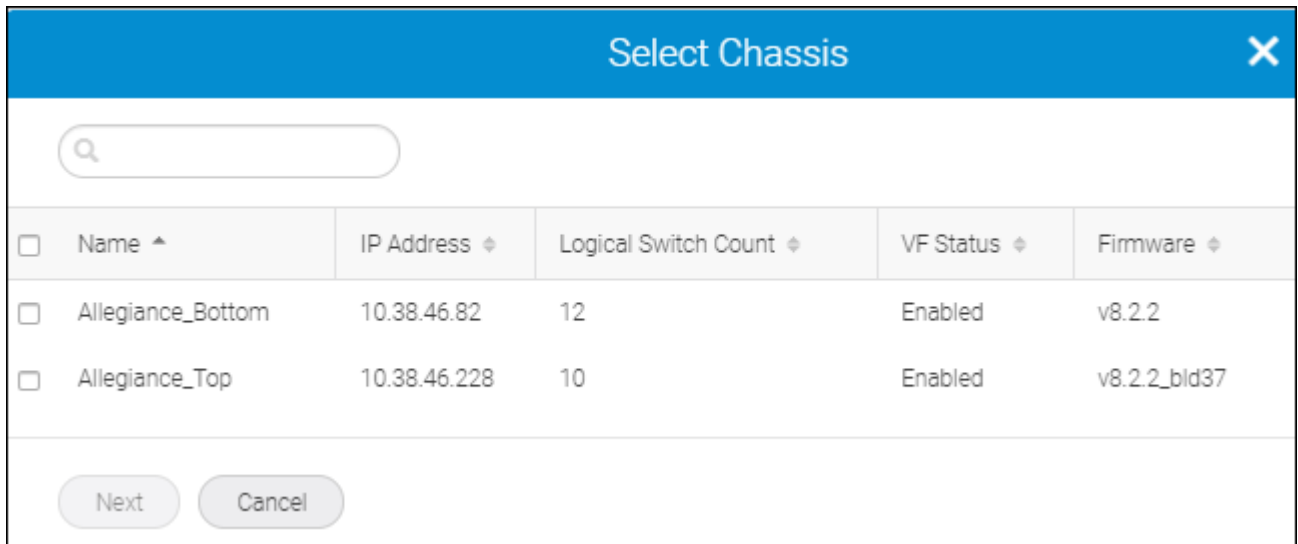
To configure a cascaded FICON fabric, complete the following steps.

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**.
The **Logical Fabrics** window displays.
2. Click **FICON Fabrics**.
The **FICON Fabrics** window displays.
3. Click the (+) icon on the top-right corner of the window to create a new cascaded FICON fabric.
The **Create New Fabric** window displays.

The screenshot shows the 'Create New Fabric' window. At the top, there are tabs for 'Logical Fabrics' and 'FICON Fabrics'. The main title is 'Create New Fabric'. Below this, there are input fields for 'Name', 'Description', 'Tags', and 'Fabric ID'. The 'Description' field is a larger text area. Below the input fields is a section for 'Switches' with a search bar and '0 Items' indicator. A table with columns for Name, WWN, IP Address, Domain, Model, VF St., Status, and RNID T. is shown, but it is empty with the message 'No data to display.' and 'Add' and 'Remove' buttons. At the bottom, there is a 'Fabric Parameters' section with an 'Activate' checkbox and 'Save' and 'Cancel' buttons.

4. Enter a name for the cascaded FICON fabric along with tags and a description in the identifier properties section.
The **Tags** and **Description** fields are optional.
5. Enter the unique identification for the fabric in the **Fabric ID** field.
6. Click the **Add** button from the **Switches** table.
The **Add** button is enabled after you provide the fabric ID.

The **Select Chassis** window displays. The **Select Chassis** window displays all Virtual Fabrics-capable devices running Fabric OS 8.1 or later.

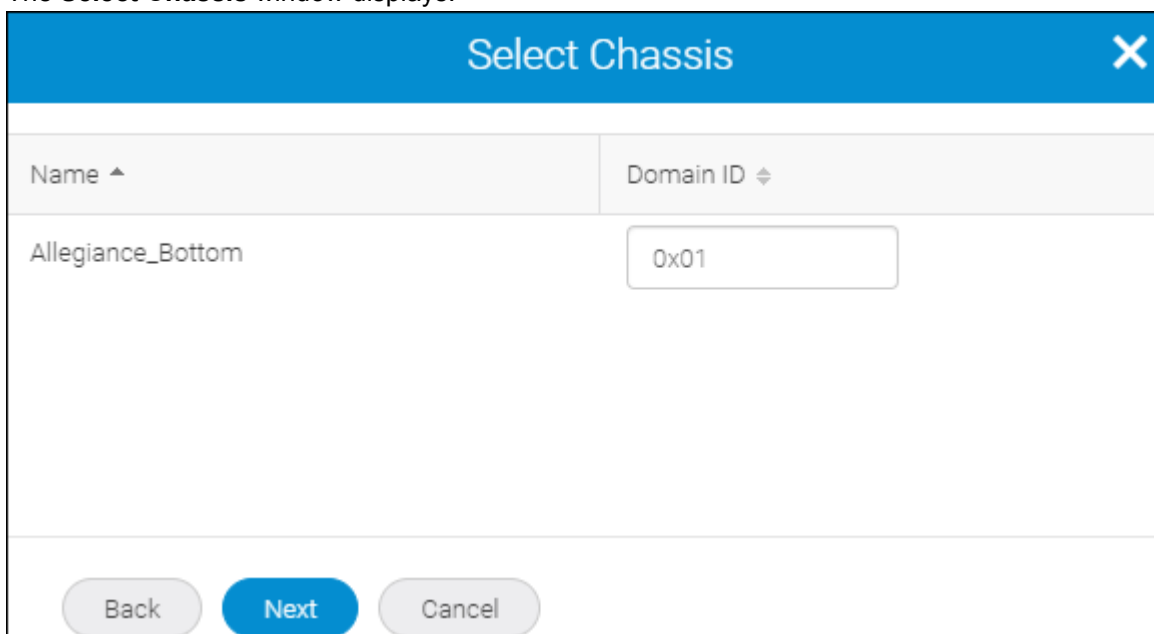


The screenshot shows the 'Select Chassis' window with a search bar and a table of devices. The table has columns for Name, IP Address, Logical Switch Count, VF Status, and Firmware. Two devices are listed: Allegiance_Bottom and Allegiance_Top.

<input type="checkbox"/>	Name ^	IP Address ↕	Logical Switch Count ↕	VF Status ↕	Firmware ↕
<input type="checkbox"/>	Allegiance_Bottom	10.38.46.82	12	Enabled	v8.2.2
<input type="checkbox"/>	Allegiance_Top	10.38.46.228	10	Enabled	v8.2.2_bld37

Buttons: Next, Cancel

7. Select two or more Virtual Fabrics-enabled devices to add to the cascaded FICON fabric and click **Next**. The **Select Chassis** window displays.

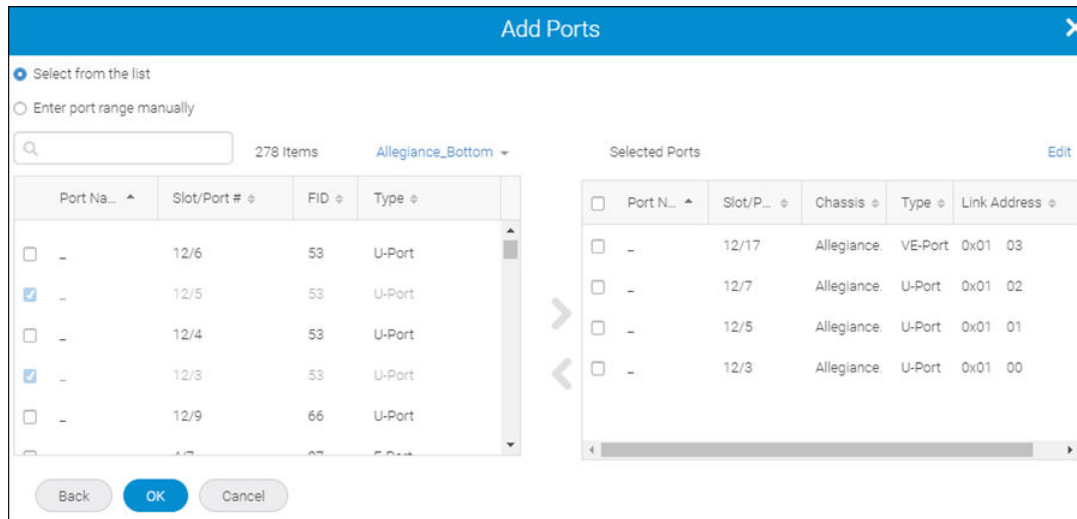


The screenshot shows the 'Select Chassis' window with a detailed view of a device. The 'Name' field is 'Allegiance_Bottom' and the 'Domain ID' field is '0x01'. Buttons: Back, Next, Cancel.

Name ^	Domain ID ↕
Allegiance_Bottom	0x01

Buttons: Back, Next, Cancel

8. Enter the domain ID for each device, if necessary, and click **Next**. The **Domain ID** field is auto-populated with the first unused domain ID from the possible domain ID range (for example from 01 to EF). The **Add Ports** window displays.



9. Select one or more ports to add to the FICON logical switch.

You must select at least one port to create the FICON logical switch.

You can enter a range of ports by clicking the **Enter port range manually** option and entering the range (for example, 1/1-1/10, 1/12, 1/14) in the **Port Range** field.

10. Click the right arrow to move the ports to the **Selected Ports** table.

The **Add Ports** windows displays the ports for one device at a time. To add ports to another device, select the device from the device drop-down list and repeat Steps 9 and 10 for each device.

NOTE

- Initially, all ports belong to the default logical switch. When you create additional logical switches, they are empty and you must assign ports to those logical switches.
- A given port can be used in only one logical switch. The ports that are not assigned to the newly created logical switch remain in the default switch.

When you move a port to the **Selected Ports** table, the application automatically assigns (binds) a link address to the port by selecting the first unused link address from the possible address range (for example from 00 to FD). To manually edit a link address for a port, complete the following steps.

- a. Click **Edit**.
- b. Enter a link address in the **Link Address** field.

When you start to enter a link address, a list of available link addresses displays in a drop-down list. SANnav does not allow you to enter a link address already in use.

Repeat this step for each link address you want to edit.

The upper bound area address range is based on the maximum number of physical ports available in the chassis or 253 whichever is less. SANnav identifies the physical ports using the following criteria: the port protocol is FC or the port protocol is FCIP and the port type is not Gig-E.

- c. Click **Save**.

11. Click **OK**.

The newly created cascaded FICON fabric window displays.

12. Click the arrow to expand the **Fabric Parameters** option.

Make changes to the fabric parameters, if necessary.

- **RA TOV.** Default is 10000. The Resource Allocation TimeOut Value (RA TOV). Do not change unless directed by your switch service provider.
- **ED TOV.** Default is 2000. The Error Detect TimeOut Value (ED TOV). Do not change unless directed by your switch service provider.
- **Maximum Hops.** Default is 7. Do not change unless directed by your switch service provider.
- **BB Credit.** Default is 16. Do not change unless directed by your switch service provider.
- **Data Field Size.** Default is 2112. Do not change unless directed by your switch service provider.
- **Routing Policy.** Select the routing policy (**Device Based** or **Exchange Based**).
- **Allow XISL use** check box. Default is not selected. When selected, ICL ports do not display in the available ports list. However, if you previously added ICL ports to the FICON fabric, this check box is not available.
- **Per-frame routing priority** check box. Do not select this check box.
- **Enable device probing** check box. Selected by default. The recommended best practice is to disable device probing. When not selected, third-party software, except for CUP, is prohibited from managing the switch. Do not select this check box unless otherwise advised by your switch service provider.
- **Suppress Class F traffic** check box. Do not select this check box.
- **Long distance fabric** check box. The recommended best practice is to configure individual ports for long distance when cascading at extended distances. This parameter sets E_Ports to LD mode (increases BB credits for long-distance performance). Select this check box only when ISLs between the switch and a connected device exceed 10 km. Dense wavelength division multiplexing (DWDM) equipment usually provides BB credits, so there is typically no reason for additional BB credits unless there are direct ISLs between switches or coarse wavelength division multiplexing (CWDM) is being used. A long-distance fabric requires a license.

13. Activate the cascaded FICON fabric by selecting the **Activate** check box.

For more information about activating a FICON fabric and the associated automatic FICON configurations that occur on the FICON devices, see [Activating a FICON Fabric](#).

14. Click **Save** to deploy the configuration.

15. Click **OK** on the message.

7.9.4.2 Adding FICON Logical Switches to a Cascaded FICON Fabric

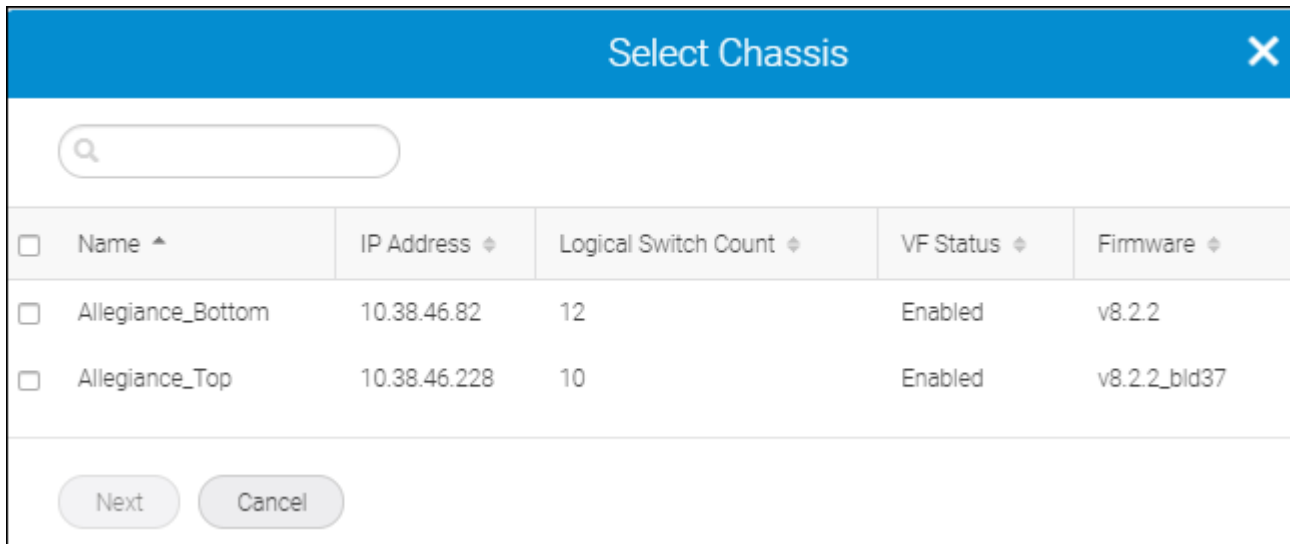
To add FICON logical switches to a FICON fabric, you must have the FICON Management privilege with read-write permission.

NOTE

If you add a Virtual Fabrics-capable switch with Virtual Fabrics disabled, you will not be able to enable Virtual Fabrics on the switch after the FICON fabric is saved.

To add FICON logical switches to a FICON fabric, complete the following steps.

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**.
The **Logical Fabrics** window displays.
2. Click **FICON Fabrics**.
The **FICON Fabrics** window displays.
3. Click the name of the cascaded FICON fabric where you want to add the FICON logical switch.
The selected FICON fabric displays.
4. Click the **Add** button from the **Switches** table.
The **Select Chassis** window displays.



The **Select Chassis** window displays all Virtual Fabrics-capable devices running Fabric OS 8.1 or later. The **Logical Switch Count** field displays the switch count per chassis.

NOTE

- The chassis is greyed out when it reaches the maximum logical switch count.
- The chassis does not appear under the following conditions:
 - When the selected fabric ID is already present on the discovered logical fabric.
 - When the base switch template is selected and you are trying to select a chassis where the base switch is already configured.

5. Select one or more Virtual Fabrics-enabled devices to add to the cascaded FICON Fabric and click **Next**.

The **Select Chassis** window displays.

6. Enter the domain ID for each device, if necessary, and click **Next**.

The **Domain ID** field is auto-populated with the first unused domain ID from the possible domain ID range (for example from 01 to EF).

The **Add Ports** window displays.

7. Select one or more ports to add to the FICON logical switch.

You must select at least one port to create the FICON logical switch.

You can enter a range of ports by clicking the **Enter port range manually** option and entering the range (for example, 1/1-1/10, 1/12, 1/14) in the **Port Range** field.

8. Click the right arrow to move the ports to the **Selected Ports** table.

The **Add Ports** windows displays the ports for one device at a time. To add ports to another device, select the device from the device drop-down list and repeat Steps 5 and 6.

NOTE

- Initially, all ports belong to the default logical switch. When you create additional logical switches, they are empty and you must assign ports to those logical switches.
- A given port can be used in only one logical switch. The ports that are not assigned to the newly created logical switch remain in the default switch.

When you move a port to the **Selected Ports** table, the application automatically assigns (binds) a link address to the port by selecting the first unused link address from the possible address range (for example from 00 to FD). To manually edit a link address for a port, complete the the following steps.

- a. Click **Edit**.
- b. Enter a link address in the **Link Address** field.

When you start to enter a link address, a list of available link addresses displays in a drop-down list. SANnav does not allow you to enter a link address already in use.

Repeat this step for each link address you want to edit.

The upper bound area address range is based on the maximum number of physical ports available in the chassis or 253 whichever is less. SANnav identifies the physical ports using the following criteria: the port protocol is FC or the port protocol is FCIP and the port type is not Gig-E.

- c. Click **Save**.

9. Click **OK**.

7.9.4.3 Adding Ports to a FICON Logical Switch

To add ports to a FICON logical switch, you must have the FICON Management privilege with read-write permission.

To add ports to a FICON logical switch, complete the following steps.

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**. The **Logical Fabrics** window displays.
2. Click **FICON Fabrics**. The **FICON Fabrics** window displays.
3. Click the name of the FICON fabric containing the FICON logical switch that you want to edit. The selected FICON fabric displays.
4. Select the **Configure** option from the action menu for the FICON logical switch. The **Configure <logical_switch>** window displays.

Configure
Switch:53_AllegianceBottom

Domain ID

Select from the list
 Enter port range manually

150 Items

Port Name	Slot/Port #	FID	Type
<input checked="" type="checkbox"/> -	12/17	53	VE-Port
<input checked="" type="checkbox"/> -	4/7	87	F-Port
<input checked="" type="checkbox"/> -	4/6	87	F-Port
<input checked="" type="checkbox"/> -	4/5	87	F-Port
<input checked="" type="checkbox"/> -	4/4	87	F-Port
<input checked="" type="checkbox"/> -	4/3	87	F-Port

Port Name	Slot/Port #	Type	Link Address
<input type="checkbox"/> ge14	12/14	GigE-Port	0x79 -
<input type="checkbox"/> -	12/17	VE-Port	0x79 <input type="text" value="00"/>
<input type="checkbox"/> -	4/3	F-Port	0x79 <input type="text" value="01"/>
<input type="checkbox"/> -	4/4	F-Port	0x79 <input type="text" value="02"/>
<input type="checkbox"/> -	4/5	F-Port	0x79 <input type="text" value="03"/>

Save | Cancel

OK Cancel

5. Select one or more ports to add to the FICON logical switch.

You must select at least one port to create the FICON logical switch.

You can enter a range of ports by clicking the **Enter port range manually** option and entering the range (for example, 1/1-1/10, 1/12, 1/14) in the **Port Range** field.

6. Click the right arrow to move the ports to the **Selected Ports** table.

The **Add Ports** window displays the ports for one device at a time. To add ports to another device, select the device from the device drop-down list and repeat Steps 5 and 6.

NOTE

- Initially, all ports belong to the default logical switch. When you create additional logical switches, they are empty and you must assign ports to those logical switches.
- A given port can be used in only one logical switch. The ports that are not assigned to the newly created logical switch remain in the default switch.

When you move a port to the **Selected Ports** table, the application automatically assigns (binds) a link address to the port by selecting the first unused link address from the possible address range (for example from 00 to FD). To manually edit a link address for a port, complete the following steps.

- a. Click **Edit**.
- b. Enter a link address in the **Link Address** field.

When you start to enter a link address, a list of available link addresses displays in a drop-down list. SANnav does not allow you to enter a link address already in use.

Repeat this step for each link address you want to edit.

The upper bound address range is based on the maximum number of physical ports available in the chassis or 253 whichever is less. SANnav identifies the physical ports using the following criteria: the port protocol is FC or the port protocol is FCIP and the port type is not Gig-E.

- c. Click **Save**.

7. Click **OK**.

7.9.4.4 Port Address Binding

Each port you add to a FICON logical switch must be bound to a link address. Note that you cannot edit link addresses for GbE and ICL ports. SANnav displays the link address using the domain ID (in hex) and the link address (for example, 0x01 00).

When you add ports to the FICON logical switch during FICON configuration, SANnav automatically populates the link address with the first available link address from the possible address range (from 00 to FD).

The upper bound address range is based on the maximum number of physical ports available in the chassis or 253 whichever is less. For example, if a chassis has 48 ports, the upper bound of the address is 0x2F (47) or if a chassis has 512 ports, the upper bound of the address is 0xFD (253).

SANnav identifies the physical ports using the following criteria:

- the port protocol is FC
- the port protocol is FCIP and the port type is not GbE

7.9.5 Cascaded FICON Fabric Merge

SANnav enables you to easily merge two FICON fabrics for cascaded FICON.

NOTE

Note that merging two cascaded FICON fabrics may be disruptive to current I/O operations in the secondary FICON fabric as this involves disabling and enabling the switches in the secondary FICON fabric. The merge process does not make any disruptive configuration changes on the primary (production) fabric.

NOTE

It is recommended that you run a configuration backup on all switches before performing the fabric merge. This helps you to revert back to the switch configurations later.

The cascaded FICON fabrics merge performs the following operations:

- Checks the primary and secondary fabrics for any merge issues.
- Configures the following High Integrity Fabric Configuration (HIFC) on the seed switch of the primary and secondary fabric.
 - The SCC policy is created or modified to limit connectivity to switches from both fabrics.
 - The Fabric-Wide Consistency Policy (FWCP) is configured on both fabrics.
- Primary fabric switches will not be disturbed for disruptive operations, such as IDID and APT. Instead, all primary fabric switches will be validated for current routing policies, and the same policies will be enabled on all secondary fabric switches.
- Sets the default zoning configuration on the secondary fabric to match the default zoning status of the primary fabric.
- Modifies the ACL policy on the secondary fabric to match the primary fabric parameters, including Accept Distribution and FWCP.
- Sets FWCP in strict mode for SCC for the primary fabric.

7.9.5.1 Merging Two Cascaded FICON Fabrics

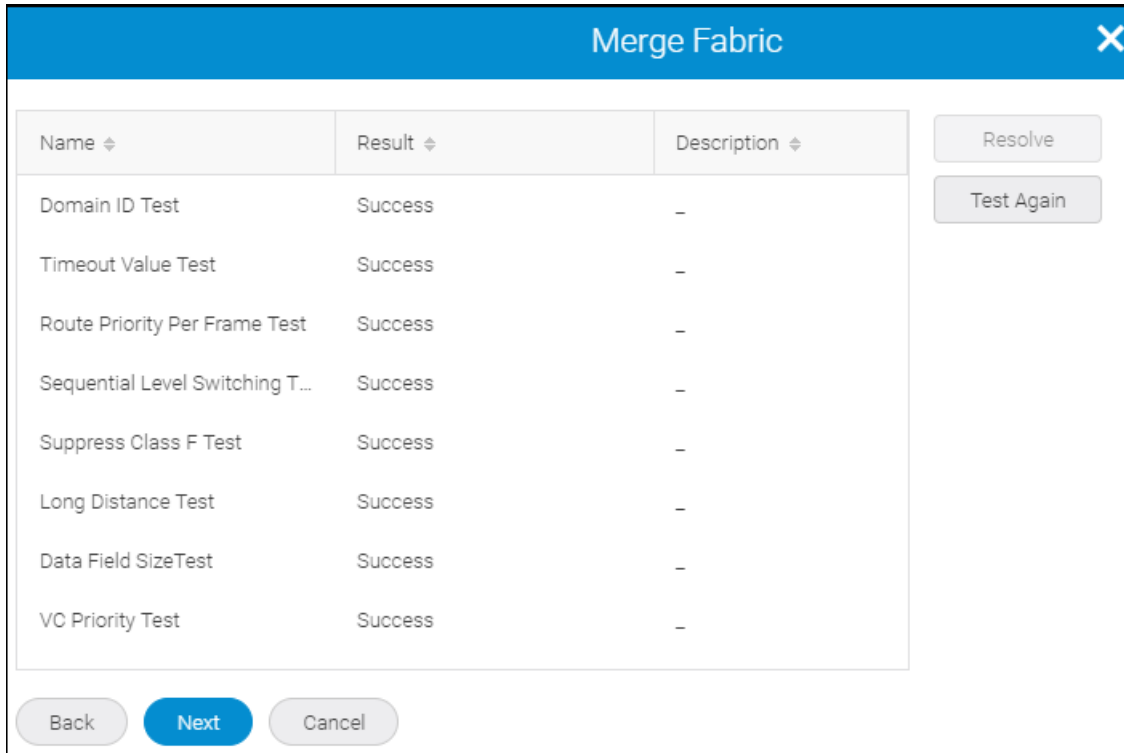
To merge two FICON fabrics, you must have the FICON Management privilege with read-write permission.

To merge two FICON fabrics, complete the following steps. Note that you can merge only two FICON fabrics at a time.

NOTE

To merge two FICON fabrics, both FICON fabrics must have the same fabric ID.

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**.
The **Logical Fabrics** window displays.
2. Click **FICON Fabrics**.
The **FICON Fabrics** window displays.
3. Select the two FICON fabrics that you want to merge.
4. Select **Merge** from the **Actions** list.
The **Merge Fabric** window displays.
5. Select the primary fabric and click **Next**.
The Merge Fabric operation runs the following tests:



6. If all tests are successful, click **Next**.

If a test fails, resolve the merge conflicts (see [Resolving Merge Conflicts](#)).

If the domain ID test fails, the **Resolve Domain ID Conflict** window lists all devices that have the domain ID conflict (see [Resolving Domain ID Conflicts](#)).

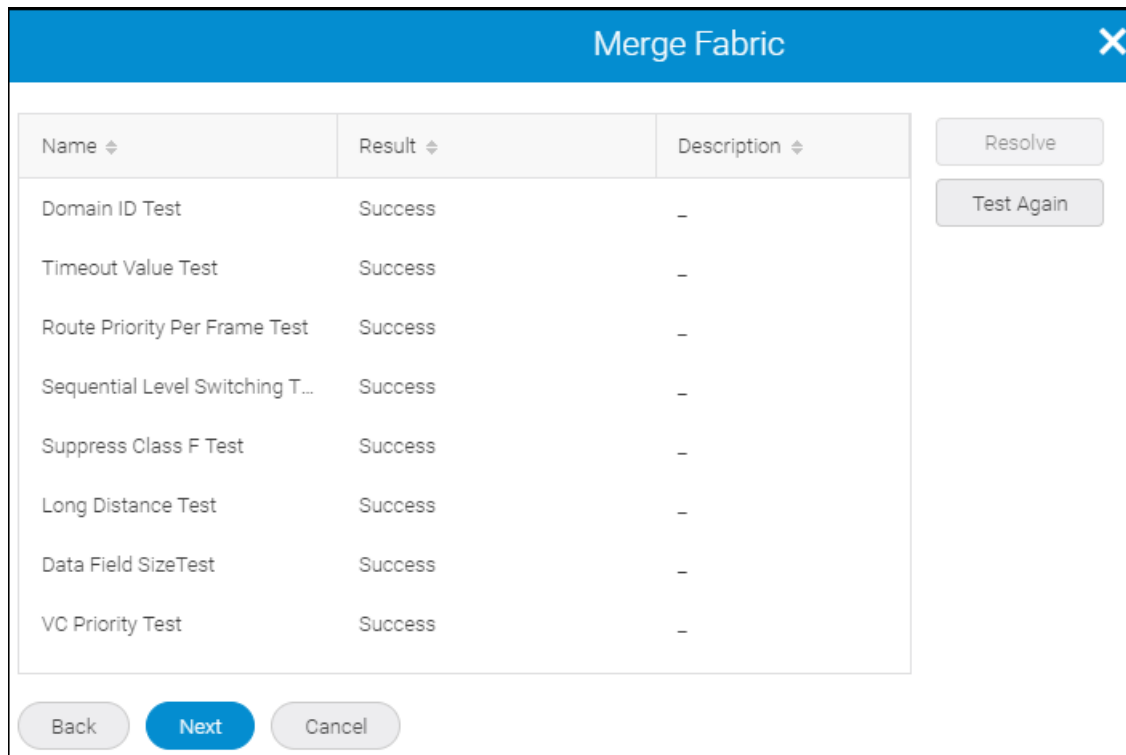
7. Click **Next** on the test complete message (see example below).

Configuration was successfully completed to allow the fabric *<secondary_fabric_name>* to join the fabric *<primary_fabric_name>* for FICON.

If fabrics do not merge automatically, check the **Additional Port Info** column in the **Inventory** page for segmentation issues.

- Review and confirm the merge actions.

Figure 33: Merge Fabric Window



- Click **Next** to perform the merge.
SANnav runs the Merge Fabric operation.
- Click **Done** on the confirmation message.

7.9.5.2 Resolving Merge Conflicts

To resolve merge conflicts, complete the following steps.

- Select the failed test where the **Result** column contains the text "Failed".
- Click **Resolve**.

If you are resolving a domain ID error, the **Resolve Domain ID Conflict** window lists all devices that have the domain ID conflict (see [Resolving Domain ID Conflicts](#)).

The values of the primary FICON fabric selected in the merge fabric operation are applied to all devices in the second FICON fabric. Once the settings are applied, the test is run again and the merge results are updated.

- Return to Step 7 of [Merging Two Cascaded FICON Fabrics](#).

7.9.5.3 Resolving Domain ID Conflicts

SANnav allows you to edit the domain IDs manually or to automatically populate the **New Domain Id** field the first unused domain ID from the possible domain ID range.

To resolve domain ID conflicts, complete the following steps.

- Select the Domain ID Test and click **Resolve**.
The **Resolve Domain ID Conflict** window displays.

Switch Name ▲	IP Address ◆	Current Domain Id ◆	New Domain Id ◆
Tyr_44	10.38.46.237	0x7A	<input type="text"/>
Venator_44	10.38.46.61	0x7B	<input type="text"/>

OK Cancel

2. Choose one of the following options on the **Resolve Domain ID Conflict** window:
 - Enter a new domain ID in the **New Domain Id** field for each device with a conflict.
 - Automatically resolve the domain ID conflicts by going to Step 2.
3. Click **OK** on the **Resolve Domain ID Conflict** window.

7.9.6 Activating a FICON Fabric

To activate a FICON fabric, you must have the FICON Management privilege with read-write permission.

NOTE

FICON fabric activation is disruptive. It disables then enables the devices in the FICON fabric.

To activate the FICON fabric, complete the following steps.

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**.
The **Logical Fabrics** window displays.
2. Click **FICON Fabrics**.
The **FICON Fabrics** window displays.
3. Click the FICON fabric that you want to activate.
The selected FICON fabric displays.
4. Select the **Activate** checkbox.
5. Click **Save** to deploy the FICON configuration, and then click **OK** in the confirmation dialog.

When you activate a new or existing FICON fabric, SANnav performs the following FICON configurations automatically:

- For Virtual Fabric-enabled devices, the following configurations occur:
 - Creates the FICON logical switch, if necessary.
 - Sets the SCC security policy.
 - Enables Dynamic Load Sharing (DLS).
 - Sets in-order delivery (IOD).
 - Binds a port address to each port you added to the FICON logical switch.
- For non-Virtual Fabric-enabled devices, the following configurations occur:

- Sets the Insistent Domain ID (IDID).
- Sets the SCC security policy and Fabric Wide Consistency Policy.
- Sets the high-integrity fabric mode (HIF).
- Enables Dynamic Load Sharing (DLS).
- Sets in-order delivery (IOD).

When the activation is complete, the FICON fabric displays in the **FICON Fabrics** window with the **Active** status.

7.9.6.1 Deployment Behavior

The deployment process of the FICON fabric configuration is in the asynchronous mode where the deployment occurs on the switches in parallel as a block.

If any of the following operations fails in any switch in the fabric, the remaining operations for all switches move to a suspended state.

■ FICON logical switch preparation

This is a basic check performed before configuration.

The following conditions are verified as part of the FICON logical switch preparation:

- Connectivity test
 - Switch connectivity check using the password available in SANnav.
- Prevalidation
 - Create/edit case—Availability of the new FID in the chassis.

■ Create FICON logical switch

The following steps occur during FICON logical switch creation. If any one of the following steps fail, the operation fails.

- Create FICON logical switch
 - Creates a FICON logical switch using the FID (same as `lscfg --create --lisldisable` in CLI)
- Disable switch
 - Disables the switch to perform the fabric property update.
- Update fabric properties
 - Updates the fabric and switch properties. If any of the changes fail, the step fails and the operation is terminated.
- Enable switch
 - Enables the newly created switch.

■ Fabric-level FICON configurations

The following steps occur during fabric-level FICON configurations. The specific steps that occur are based on whether the device is Virtual Fabrics-enabled or not.

Virtual Fabrics-enabled devices

- Set the accept distribution flag
 - Sets the accept distribution flag on the switch to accept SCC policy updates.
- Set the high integrity fabric (HIF) configuration
 - When creating a FICON fabric, updates the SCC policy with the fabric member WWNs and configures the fabric wide consistency policy to SCC:S (strict mode).
 - When editing a FICON fabric, updates the SCC policy list with the fabric member WWNs and updates the FWCP to that of the seed switch.

Non-Virtual Fabrics-enabled devices

- Disable HIF mode
 - Disables HIF mode on the switch if it is already enabled.
- Enable insistent domain ID (IDID) mode

- Enables IDID on the switch.
- Set the accept distribution flag
Sets the accept distribution flag on the switch to accept SCC policy updates.
- Clear zones
Clears zone configurations on the switch.
- Set the high integrity fabric (HIF) configuration
When creating a FICON fabric, updates the SCC policy with the fabric member WWNs and configures the fabric wide consistency policy to SCC:S (strict mode).
When editing a FICON fabric, updates the SCC policy list with the fabric member WWNs and updates the FWCP to that of the seed switch.
- Set the default zone policy
Sets the default zone policy on the switch. When creating a FICON fabric, the default zone policy is set to All Access.
- Enable HIF mode
Enables HIF mode on the switch.

■ **Switch-level FICON configurations**

The following steps occur during switch-level FICON configurations on both Virtual Fabrics-enabled devices or non-Virtual Fabrics-enabled devices.

- **Disable the switch**
Disables the switch if it is not already disabled.
- **Configure the routing policy**
Configures the routing policy to device-based or exchange-based routing.
- **Enable Dynamic Load Sharing (DLS) with Lossless.**
Enables DLS with Lossless on the switch.
- **Sets in-order delivery (IOD).**
Enables IOD on the switch.
- **Enable the switch**
Enables the switch if it is disabled.
- **Port configuration clearing**
Clears all port configurations and resets the port back to the factory default settings.
- **Fabric property update**
The following steps occur during fabric property update. SANnav performs these steps automatically to verify whether the configuration in the switch and client matches. If the configuration does not match, SANnav initiates the fabric update. If you modify the fabric ID (FID), SANnav does not automatically discover the fabric. You must delete and discover the newly created fabric.
 - **Disable switch**
Disables the switch to perform a fabric property update.
 - **Update fabric properties**
Updates the fabric properties and switch properties. If any of the changes fail, the step fails and the operation is terminated.
- **Port movement**
Port movement is a common operation for the create or delete operation. When you perform a create operation, the port is moved to the destination FID. When you perform a delete operation, the port is moved to the default FID. If you do not select VE for movement and GbE is trying to move, the operation fails. You must delete tunnels in the VE_Ports before proceeding further.
 - Disable ports

- Disable the port in the source switch before moving the port.
- Add ports
 - Move the port to the destination switch.
- Remove ports
 - Move the port to the default FID.
- Enable ports
 - Enable the port in the destination switch.
- **Port binding**
 - Disable ports
 - Disable the port in the destination switch.
 - Bind ports
 - Bind the ports with an address.
 - Enable ports
 - Enable the port in the destination switch.
- **Port unbinding**
 - Unbind the port.
- **Delete FICON logical switch**
 - Delete the FICON logical switch (same as `lscfg --delete fid`).
 - If any of the ports is not moved to the default, the delete operation fails.

When the deployment process is complete, a popup message displays. If deployment is successful, a Success message displays. If deployment fails, a Failure message displays. Click **Show Details** to display a list of the deployment operations for each switch in the fabric and whether the operation succeeded or failed.

7.9.6.2 Post Deployment Behavior

Once FICON fabric configuration is complete, SANnav automatically initiates the discovery of the FICON fabric. If auto-discovery fails or times out, the failure message displays on the **FICON Fabrics** window. You must perform manual discovery in case of failure.

The following error message is displayed when you fail to discover a FICON fabric:

```
Discovery / Re-discovery of the fabric is failed, perform manual discovery
```

7.9.7 Deleting FICON Fabrics and FICON Logical Switches

7.9.7.1 Deleting a FICON Fabric

To delete a logical fabric, you must have FICON Management privilege with read-write permission.

To delete a logical fabric, complete the following steps.

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**.
The **Logical Fabrics** window displays.
2. Click **FICON Fabrics**.
The **FICON Fabrics** window displays.
3. Select the FICON fabric that you want to delete from the **FICON Fabrics** list.
4. Click **Delete**.
The FICON fabric is removed from the **FICON Fabrics** list.

7.9.7.2 Deleting a FICON Logical Switch

To delete a FICON logical switch, you must have the FICON Management privilege with read-write permission.

Note that the **Remove** button is greyed out if the switch meets any of the following criteria:

- It is the only switch present in the **Switches** list.
- It is the last switch in the FICON fabric running Fabric OS 8.1.0 or later.
- It is a non-Virtual Fabrics switch.
- It is the FICON fabric seed switch.

To delete a FICON logical switch, complete the following steps.

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Logical Fabric Management**.
The **Logical Fabrics** window displays.
2. Click **FICON Fabrics**.
The **FICON Fabrics** window displays.
3. Select the FICON fabric containing the FICON logical switch that you want to delete from the **FICON Fabrics** list.
The selected FICON fabric displays.
4. Select the switch that you want to remove and click **Remove**.
The FICON logical switch is removed from the **Switches** list.

When you delete a FICON logical switch, we recommend that you perform fabric rediscovery (see [Rediscovering a Fabric](#)). Otherwise, the FICON logical switch count may not be accurate until after the next data collection.

7.9.8 Connecting Cascaded FICON Fabrics over FCIP

This section provides a basic guide of IP best practices for connecting cascaded FICON fabrics over an IP network through FCIP and merging the fabrics. Included are planning considerations, steps for configuring an IP link between two extension switches and merging them into one fabric, and steps for configuring DWDM links to use R_RDYs.

IP best practice for connecting the fabrics is to perform the following steps in order:

1. Configure all IP tunnels and circuits between the fabrics.
2. Merge the FICON fabrics.

NOTE

Merging two cascaded FICON fabrics may be disruptive to current I/O operations in both fabrics, as the switches in both fabrics need to be disabled and enabled. The merge process will not make any configuration changes on the primary (production) fabric that are disruptive.

3. Configure FICON emulation features, if applicable.

NOTE

Consult with a qualified support specialist before implementing the FICON Acceleration feature.

The following procedures apply to configuring an IP connection between two extension switches or blades, and then merging the fabrics to which they belong.

Procedures in this section may refer to additional sections in this chapter or additional chapters in this manual for more detailed information. This section assumes that the switches in the fabrics to be merged have been configured for FICON operation using procedures under [FICON Fabric Configuration](#).

7.9.8.1 Planning the Cascaded FICON Fabrics over FCIP Configuration

Create a drawing to summarize the following elements of your planned configuration.

- IP network connections.

- Tunnels
- Addresses
- Bandwidth requirements for all circuits
- Labels for all circuits and tunnels

Determine how the IP network will be used by identifying redundant routes and minimum and maximum bandwidth requirements. The FICON Acceleration feature is required for distances greater than 300 km. Before configuring this feature, Fabric OS professional services are highly recommended.

- Network distance.

Make sure that network distance is measured in actual network delay. The FICON Acceleration license is required if distance exceeds 300 meters.

- Buffer-to-buffer credit management for long-distance links.

- Use of dense wavelength division multiplexing (DWDM) or time division multiplexing (TDM) interfaces and buffer-to-buffer credit management for these interfaces.

Typically the long-distance BB credits are supplied if DWDM is used. Some older DWDM interfaces do not supply BB credits (R_RDY), so check with the DWDM vendor. You may need to calculate the correct number of BB credits required if using DWDM that does not provide BB credits. Note that BB credits depend not only on distance, but on average frame size as well. Be sure and contact a Fabric OS support professional for assistance.

Double-check the type of optics required since long-wave optics are commonly ordered for mainframe environments and occasionally DWDM interfaces use short-wave optics. Also find out if a TDM card is being used as you will need to follow procedures under [Configuring DWDM Links to Use R_RDYs](#) .

7.9.8.2 Configuring IP Links and Merging the Fabrics

Use the following procedures to configure an IP connection between two extension switches or blades, and then merge the fabrics to which they belong.

1. FCIP configuration always involves two or more extension switches. The following should occur first before you configure a working FCIP connection from SANnav:
 - The WAN link should be provisioned and tested for integrity.
 - Cabling within the data center should be completed.
 - Equipment should be physically installed and powered on.
 - SANnav must have management port access to the extension switches.
 - SANnav must be able to discover the fabrics that contain the extension switches.
 - The Extension Switches should be physically connected to the IP network that they will be using to pass data, and the connection should be active and working.
 - Identify all devices in the data path between the Extension Switches, including Ethernet switches, Ethernet routers, firewalls, and common carrier equipment. A network diagram is very helpful. Support engineers may ask you to provide a network diagram when troubleshooting problems.
 - Routers and firewalls must be configured to pass ARP, ICMP, and IP layer 3 protocols.
 - Persistently disable the VE_Ports before you configure them. Ports on a new extension switch or extension blade are persistently disabled by default.
2. Configure tunnels circuits between the switches by following the steps under [Configuring a Two-Sided Tunnel](#).

3. Follow these guidelines when configuring tunnels:
 - You can configure either switch as switch 1 or switch 2.
 - Specifications for FCIP circuits per tunnel, number of IP addresses per port, and other trunking capacities for the Brocade 7800 Extension Switch and FX8-24 Extension Blade are detailed in the *Brocade Fabric OS Extension Configuration Guide*.
 - For configuring the port type, VEX connections on the Brocade 7800 Extension Switch and FX8-24 Extension Blade are for Fibre Channel Routing (FCR) and are not supported for FICON. Select VE_Port as this refers to an E_Port connected to an IP instead of a Fibre Channel link.
4. For transmission-related properties (access by clicking **Transmission** on the **Create New Tunnel** page), the best practice is to set the FC compression mode to Deflate.
For more information, see Step 8 of [Configuring a Two-Sided Tunnel](#).
5. For security-related properties (access by clicking **Security** on the **Create New Tunnel** page), follow these guidelines:
 - The recommended best practice is to enable IPsec. IPsec on a Brocade 7800 Extension Switch or FX8-24 Extension Blade is Advanced Encryption Standard (AES) 256 only.
 - The policy must match in the tunnel configurations for both switches.For more information, see Step 8 of [Configuring a Two-Sided Tunnel](#).
6. For FICON emulation-related properties (access by selecting **Emulation** on the **Create New Tunnel** page), follow these guidelines:
 - The recommended best practice is to complete all configuration for the IP connection and merge the fabrics before configuring FICON Emulation. Configure settings in this area after merging the fabrics.
 - FICON Acceleration features require a license. These features include FICON Tape Emulation, FICON XRC Emulation, and FICON Teradata Pipelining.
 - Select **Populate Default Values** unless recommended otherwise by a qualified Fabric OS support professional.
 - Only select the features that you require.
 - Whenever selecting a FICON emulation feature, also select the **FICON** radio button.
 - Set the FICON acceleration features (Tape, XRC, and Teradata Pipelining) per tunnel. The Tape fields are already populated with default values, which you can override.
 - Fast Write is not necessary for FICON. Keep in mind that disk-to-disk mirroring is native FCP even if the front-side ports are FICON. If sharing FICON and FCP on the same tunnel, you can enable Fast Write. Enabling Fast Write depends on the application being extended over FCIP. See [When to Enable Fast Write](#). As with any feature, if it is not needed, the best practice is to disable Fast Write.For more information, see Step 8 of [Configuring a Two-Sided Tunnel](#).
7. Configure circuits for tunnels using the steps under [Configuring a Two-Sided Tunnel](#) (beginning with Step 9).
Follow these guidelines when configuring circuits:
 - Start by configuring circuit 0, and then add additional circuits if desired.
 - Make changes to IP settings by clicking **Transmission on the Add Circuit** on the **Create New Tunnel** page. Make changes to this area only under direction of network administrators.
8. After you complete the tunnel and circuit configuration between the fabrics, merge the fabrics (see [Cascaded FICON Fabric Merge](#)).
Consider the following when merging fabrics:

- When merging fabrics, the primary fabric is the production fabric where disruption should not occur. The merge process will not make any disruptive configuration changes on the primary fabric. The secondary fabric is merged into the primary fabric.
 - Any CHPIDs with local connections in the secondary fabric should be configured offline.
 - The merged fabric will retain zone configurations from the primary fabric, so any zone configurations involving ports on the secondary fabric must be redone after the fabric merge.
 - There are no long-distance parameters to configure for IP links. Except for CWDM, most DWDM equipment provides the required buffer credits. Typically, it is only necessary to set long-distance mode when there are direct fibre runs.
9. After fabrics are successfully merged, configure FICON Emulation features, as required.
10. Rezone the fabric as zoning was removed from the secondary fabric that you merged.

7.9.8.3 Configuring DWDM Links to Use R_RDYs

Time Division Multiplexing (TDM) requires that you configure DWDM links to use R_RDYs and not VC_RDYs.

To configure DWDM links to use R_RDYs, execute the following Fabric OS commands on E_Ports (ISL connections).

1. Enter the following command to disable credit recovery on a port.
`portcfgcreditrecovery --disable slot/port`
2. Enter the following command to set the speed for the link. Only speeds supported by the installed SFP are supported. Use 0 to return to automatic sensing mode.
`portcfgspeed slot/port speed`
3. Enter the following command to disable QoS.
`portcfgqos --disable slot/port`
4. Enter the following command to enable ISL R_RDY mode.
`portcfgislmode slot/port 1`
5. Enter the following command to disable trunking on the port.
`portcfgtrunkport slot/port 0`
6. Enter the following command to display port settings.
`portcfgshow`

7.9.8.4 Extending RDR Applications over FCIP

This section provides considerations for configuring tunnels and circuits when extending remote data replication (RDR) applications over FCIP.

When to Enable Fast Write

Enabling Fast Write depends on the application that you are extending over FCIP. Use the following table to determine if Fast Write should be enabled for a tunnel configuration. Enable Fast Write through the **Create New Tunnel** page by clicking **Transmission** (see [Configuring a Two-Sided Tunnel](#)).

NOTE

The following table details the applications that can benefit from enabling Fast Write. Although there is a No entry in the table for some applications, you can still enable Fast Write when sharing applications over the same tunnel.

Table 25: Using Fast Write for Extended Applications

Manufacturer	RDR Application	Platform	Type	Use Fast Write
IBM	Global Mirror	DS	Async	No
IBM	Metro Mirror	DS	Sync	No
IBM	XIV	XIV	Sync	Yes
IBM	Global Mirror	SVC	Async	No
IBM	Metro Mirror	SVC	Sync	No
EMC	SRDF/A	Symmetrix	Async	Yes
EMC	SRDF/S	Symmetrix	Sync	Yes (SiRT disabled)
EMC	SRDF Adaptive Copy	Symmetrix	Async	Yes
EMC	MirrorView	CLARiiON	Async	Yes
EMC	MirrorView	CLARiiON	Sync	Yes
EMC	SANcopy	CLARiiON	Async	Yes
HDS	Universal Replicator (HUR)	All	Async	No
HDS	TrueCopy	All	Async	No
HP	Continuous Access	EVA	Hybrid	No
*	OSTP	Tape	Tape	Yes (required for OSTP)

Compression Mode

More aggressive compression modes can be used for asynchronous mirroring. For synchronous mirroring, only hardware or standard compression should be used. This is because more aggressive algorithms work by receiving additional frames to find compressible patterns on larger blocks of data. The time it takes to read these additional frames adds latency, which may not be tolerated by synchronous mirroring. For more information about compression mode, refer to the *Brocade Fabric OS Extension User Guide*. Set compression modes in the **Transmission** area of the **Create New Tunnel** page (see [Configuring a Two-Sided Tunnel](#)).

Circuit Keep Alive Time Out Value

The circuit Keep Alive Time Out value, located in the **Transmission** area of the **Add Circuit** page (see [Configuring a Two-Sided Tunnel](#)), should be less than the protocol timeout for the application being extended. This allows circuit failover to be nondisruptive. By default, the circuit keepalive is 6 seconds on the SX6 extension blade and the 7840 and 7810 switches. For older extension products, the circuit keepalive default is 10 seconds (10,000 ms). If FICON emulation is enabled on the extension tunnel when a circuit is created, the keepalive timeout defaults to 1 second (1000 ms). Set this to 6 seconds (6000 ms) for IBM peer-to-peer remote copy (PPRC). All other applications should use the default.

NOTE

It is recommended that if there are 2 or more circuits, then each circuit's keepalive should be set to 3 seconds (as most RDR applications have a 6 second command timeout) to prevent application errors in the event of a single circuit failure.

SRDF Considerations

Use SRDF/S SiRT (Single Roundtrip) or SRDF/A with FCIP-FW, but not both. Using SRDF/A and SRDF/S on the same remote adapter (RA) ports on the array is not recommended. Use different VE_Ports for the tunnels, as if the tunnel destinations were different. If there is only one destination (SRDF/A and SRDF/S are going to the same place), isolate

traffic from the SRDF/A and SRDF/S RA ports using different logical switches to isolate traffic to specific VE ports in a configuration. Note that there may be differences in bandwidth, Fast Write, and compression mode tunnel parameters.

Event Management

8.1 Event Management Overview

Using Event Management features, you can configure traps; register to receive SNMP traps, syslog events, and other information from switches; view, search and filter event logs; and forward SNMP traps and syslog messages to the selected destinations.

Following are some of the actions that you can configure for events:

- Generating email alerts.
- Triggering SupportSave.
- Enabling maintenance mode to suppress a switch events in the event log.

You can also perform powerful event analysis by filtering events using network scope, date range, and custom filters. You can also perform searches within the event log and generate event reports.

In addition, Event Management provides several events managing widgets, such as the **Top N Events**, **Events Summary**, and **Health Violations** widgets, that you can add to dashboards.

8.1.1 Functions of Event Management

The limitations for scalability of Event Management are listed below:

- Receives 100 traps per second.
- Stores 50000 to 10 million events up to a maximum of one year (by default it is 14 days or 50000 events).
- Stores 50000 to 10 million MAPS violations up to a maximum of one year (default is 14 days).
- Sends email notification for the first 5000 event occurrences.

The advantages of Event Management are provided below:

- Minimizes downtime by proactively monitoring the devices.
- Provides reactive troubleshooting functionalities.
- Provides advanced data visualization for logs and events to improve the user experience.
- Supports many out of the box templates and widgets for dashboard and reports.

8.1.2 Types of Registration

Registration for all the switches is mandatory for viewing all the events of all the discovered switches. There are two types of registration. You can register through the following:

- SNMP Trap / Informs registration.
- Syslog registration.

8.1.3 Registering for SNMP Traps

SANnav provides an option to automatically register the SANnav server as SNMP trap recipients for the discovered switches.

SANnav supports two types of SNMP notifications:

- Traps
- Informs

With SNMP traps, the receiver does not send any acknowledgment when it receives a trap; and thus, the sender cannot determine if the trap was received. With informs, the receiver of the inform returns an acknowledgment to the SNMP agent.

To enable automatic SNMP TRAP registration, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **Event Management > Syslog and SNMP Registration**.
2. Select the **SNMP Trap** tab.

By default the **Auto register server as SNMP trap recipient** option is selected to register the new switches automatically.

NOTE

If the **Auto register server as SNMP trap recipient** option is not enabled, the new switches are not registered automatically.

3. Select the **Enable Informs** option to register the server as an SNMP informs recipient.

NOTE

You cannot modify the **SNMP Listening Port (Server)** as it is defined by you at the time of SANnav installation.

The SNMP traps are less reliable than informs as the sender does not know whether the receiver has received the traps or not. When inform is enabled, SANnav acknowledges an inform message with an SNMP response PDU. If the sender did not receive a response for an inform, the inform is sent again.

4. Click **Save** to save the settings.

8.1.4 Registering for Syslog

The Syslog registration automatically registers all the servers as Syslog recipients.

To enable Syslog registration, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **Event Management > Syslog and SNMP Registration**.
2. Select the **Syslog** tab.

By default the **Auto register server as Syslog recipient** option is selected to register the new switches automatically.

NOTE

If **Auto register as Syslog recipient** option is not enabled, the new switches are not registered automatically.

3. Enable the **Secure Syslog** option to register the switch for secure Syslog reception.

NOTE

You must manually import the SANnav server certificate in the switch (see [Importing the Server Syslog Certificate Using a CLI Script](#)).

NOTE

You cannot modify the **Syslog Listening Port (Server)** as it is defined at the time of SANnav installation.

4. Click **Save** to update the Syslog registration settings.

8.1.4.1 Importing the Server Syslog Certificate Using a CLI Script

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 in the switch.

To import the Syslog certificate, perform the following steps:

1. Enter `-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 the **Enter IP address** field.
4. Enter the certificate location in the **Enter remote directory** field.
5. Enter the certificate file name in the **Enter certificate name** field.
6. Enter the login name and password of the certificate location and press **Enter** to import the server cert with the `seccertmgmt import -ca -server syslog` to the switch.

```
CID-TAC-X6-8-84-2_new:admin> seccertmgmt import -ca -server syslog
Select protocol [ftp or scp]: scp
Enter IP address:
Enter remote directory: /root/local/server_new/etc/conf/security
Enter certificate name (must have ".crt" or ".cer" ".pem" or ".psk" suffix):https_cert.pem
Enter Login Name: root
root@'s password:
Success: imported syslog server CA certificate [https_cert.pem].
CID-TAC-X6-8-84-2_new:admin> seccertmgmt show -all

ssh private key:
  Does not Exist

ssh public keys available for users:
  None

Certificate Files:
-----
Protocol  Client CA      Server CA      SW              CSR             PVT Key Passphrase
-----
FCAP      Empty          NA             Empty           Empty           Empty           Empty
RADIUS    Empty          Empty          Empty           Empty           Empty           NA
LDAP      Empty          Empty          Empty           Empty           Empty           NA
SYSLOG    Exist          Exist          Empty           Empty           Empty           NA
HTTPS     NA             Empty          Empty           Empty           Empty           NA
EXTN      NA             NA             Empty           Empty           Empty           NA
CID-TAC-X6-8-84-2_new:admin>
```

- You can also enter `show -all` to verify the Syslog certificate files, as in the following screen capture.

```
CID-TAC-X6-8-84-2_new:admin> seccertmgmt show -all
ssh private key:
  Does not Exist

ssh public keys available for users:
  None

Certificate Files:
-----
Protocol  Client CA      Server CA      SW              CSR    PVT Key Passphrase
-----
FCAP      Empty          NA             Empty           Empty  Empty  Empty
RADIUS    Empty          Empty          Empty           Empty  Empty  NA
LDAP      Empty          Empty          Empty           Empty  Empty  NA
SYSLOG    Empty          Empty          Empty           Empty  Empty  NA
HTTPS     NA            Empty          Empty           Empty  Empty  NA
EXTN      NA            NA             Empty           Empty  Empty  NA
CID-TAC-X6-8-84-2_new:admin>
```

- Enter `delete -ca -server syslog` to delete a current server Syslog certificate (see the image below).

```
Usage:
seccertmgmt delete
  -cert <fcap|commoncert|https|radius|ldap|syslog|extn <certificate name> | -keypair_tag <keypair_tag>|mgmtip <certificate name>|all>
  -ca -client|-server <fcap|commoncert|https|radius|ldap|syslog|extn <certificate name> |all>
  -csr <fcap|commoncert|https|radius|ldap|syslog|extn -keypair_tag <keypair_tag>>
  -all <default|fcap|commoncert|https|radius|ldap|syslog|extn|mgmtip>
  [-f] - no warning

CID-TAC-X6-8-84-2_new:admin> seccertmgmt delete -ca -server syslog
WARNING!!!

About to delete syslog CA certificate file(s)

Continue (yes, y, no, n): [no] y
Syslog is configured in secure mode, so certificate cannot be deleted. Please remove secure mode configuration for Syslog and try again.
CID-TAC-X6-8-84-2_new:admin> syslogadmin --show -ip
syslog.1
syslog.2
syslog.3
syslog.4          secure: port 6514
syslog.5
syslog.6
CID-TAC-X6-8-84-2_new:admin> syslogadmin --remove -ip
Syslog IP address removed
CID-TAC-X6-8-84-2_new:admin> seccertmgmt delete -ca -server syslog
WARNING!!!

About to delete syslog CA certificate file(s)

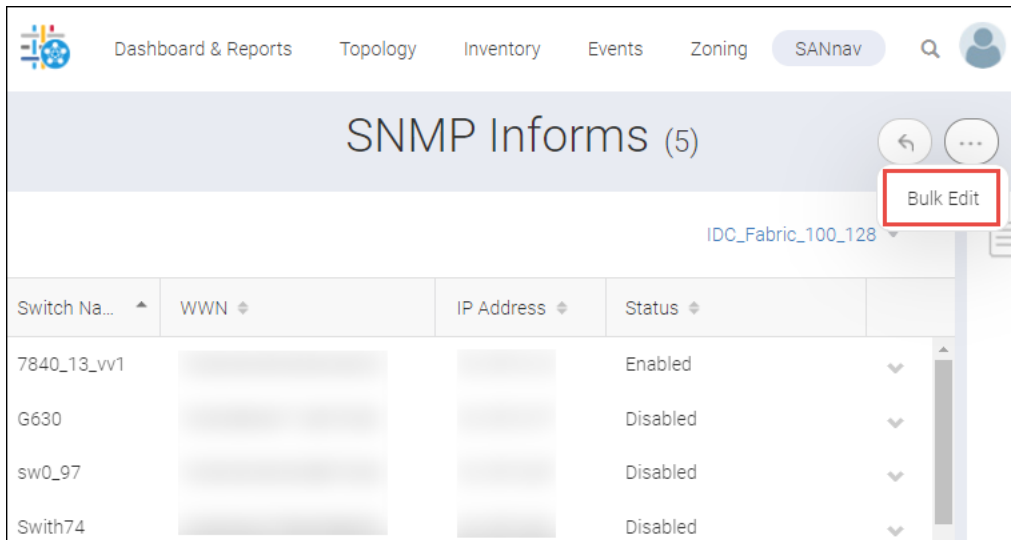
Continue (yes, y, no, n): [no] y
CID-TAC-X6-8-84-2_new:admin>
```

8.1.5 Enabling or Disabling SNMP Informs

Enabling SNMP Informs allows SANnav to acknowledge the trap. It also assists in enabling or disabling informs at switch level on informs-capable products.

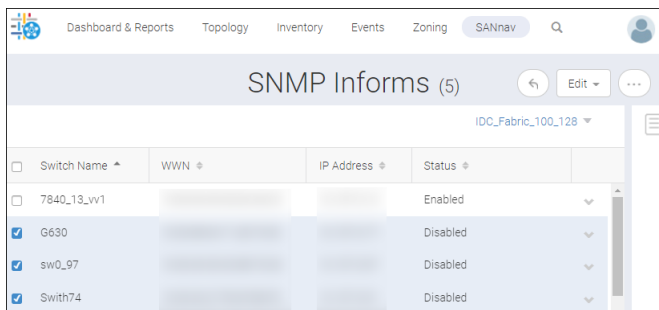
To enable or disable SNMP Informs, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **Event 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 the more icon (⋮), on the top-right corner of the window, and then select **Bulk Edit**.

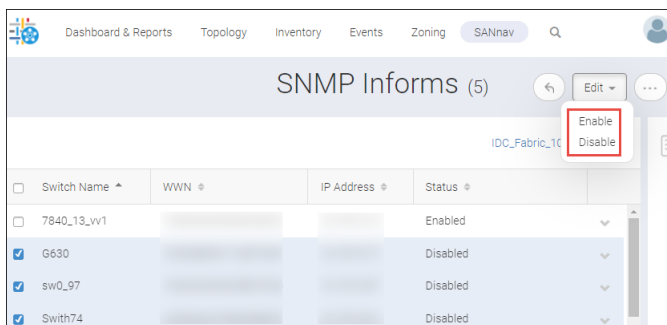


The select options for the switches are displayed.

4. Select one or more switches you want to enable or disable.



5. Click **Edit**, and then select **Enable** or **Disable**.



6. SNMP informs is enabled or disabled at the switch level. To receive actual informs, enable the **SNMP Informs** option in the **SNMP Trap** tab.


8.1.6 Enabling Event Notifications

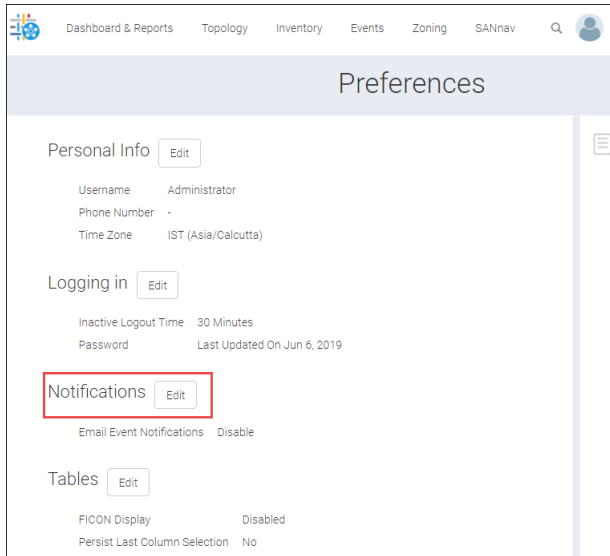
You can enable the email event notification in user preferences. You cannot receive the event notification unless the administrator has enabled the email event notification.

NOTE

You must set the duration to receive the email events and configure email id in the **User** window.

To enable email event notification, perform the following steps:

1. Click **User Preferences** from the () icon.
The **Preferences** window is displayed.
2. Click **Edit** button next to the **Notifications** preference.

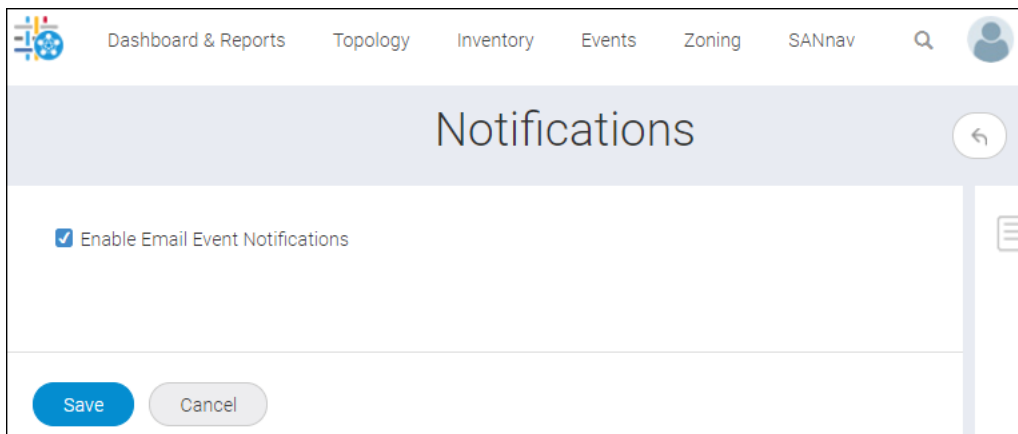


The screenshot shows the 'Preferences' window with the following sections:

- Personal Info** (Edit): Username Administrator, Phone Number -, Time Zone IST (Asia/Calcutta)
- Logging in** (Edit): Inactive Logout Time 30 Minutes, Password Last Updated On Jun 6, 2019
- Notifications** (Edit): Email Event Notifications Disable
- Tables** (Edit): FICON Display Disabled, Persist Last Column Selection No

The **Notifications** window is displayed.

3. Select the **Enable Email Event Notifications** checkbox, and then click **Save**



The screenshot shows the 'Notifications' window with the following elements:

- Header: Notifications
- Checkbox: Enable Email Event Notifications
- Buttons: Save (highlighted in blue), Cancel

8.1.7 Setting the Frequency to Receive Email Event Notifications

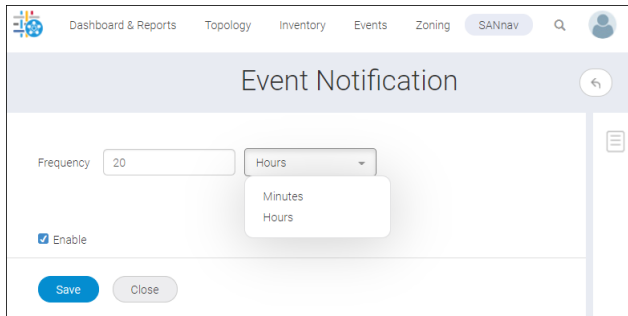
You can set the interval to receive email event notifications for the new events received in SANnav.

NOTE

To receive email event notifications, you must enable event notifications in the **Preferences** window, configure email address in the **User** window, and configure the email server.

To set the frequency for receiving email event notifications, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **Event Management > Event Notification**.
The **Event Notification** window is displayed.
2. Enter the time interval for the notification in the **Frequency** field.
The range for **Minutes** is 1 to 59 and for **Hours** is 1 to 24.
3. Select the time from the drop-down in **Minutes** or **Hours**.



4. Select the **Enable** option to activate the event notification, and then click **Save**.

8.1.8 Configuring an Email Setup

You can configure the email server to send event notifications to users who are enabled to receive them.

NOTE

To receive email event notifications, you must enable event notifications in the user preferences and set the duration to receive the email events (see [Enabling Event Notifications](#) and [Setting the Frequency to Receive Email Event Notifications](#)).

To set up your email account, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **Services > SANnav Email Setup**.
The **SANnav Email Setup** window is displayed.
2. Enter the email server in the **Email Server** field.
3. Select **None**, **Use SSL**, or **Use TLS** from the **Security** drop-down.

NOTE

When you select security as **Use SSL** or **Use TLS**, the **SMTP ID** and **SMTP Password** fields are available.

NOTE

If you try to modify any of the email settings, you must re-enter the password in the **SMTP Password** field. You must enter the password to send a test email.

4. Enter the SMTP port number, ID, and password in the respective 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 either of the following options:
 - **All users enabled for notification** – This option is used to send a test email notification to all the application users who have a valid email ID configured in the **Users** page.

- **This email** – This option is used to specify the list of users who must receive the test email notification. When you select the **This Email** option, a field appears to specify the email ID(s).

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. Click **Send Test Email**.
8. Click the **Enable** checkbox to activate the email configuration.
9. Click **Save** to save the email setup.

8.1.9 Defining the Trap Configuration

Using Trap Configuration, you can select the existing OID and offer recommended actions.

To define the actions for each OID, follow the below instructions:

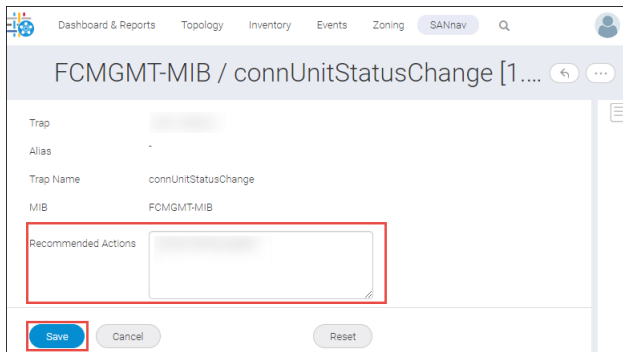
1. Click **SANnav** in the navigation bar, and then select **Event Management > Trap Configuration**.
2. Click the **+** icon on the top-right corner of the **Trap Configuration** window.
3. Enter the trap OID in the **Trap** field, and then click **OK** to view the details of the trap.

NOTE

Only the OIDs present in the `<SANnav installation>/conf/trapConfigurationDefault.xml` file are supported in this configuration.

4. Enter the recommended action to take when the specific event occurs, and then click **Save** to save the trap recommended action.

When SANnav receives the trap with this OID, the user-defined recommended action is executed. You can view this recommended action in the **Events** list view.



8.1.10 Forwarding

You can forward the SNMP trap and Syslog messages to a third-party application or server. You can forward application events as traps. You can customize the configuration of forwarding for both SNMP trap and Syslog messages.

To forward SNMP trap and Syslog messages, define the following three tabs:

- **Filters (optional)** - When forwarding Syslog or SNMP trap, you can filter the parameters prior to being sent.
- **Destinations** - You can define the destination details of the third-party application or the server where the SNMP trap and Syslog are forwarded.
- **Credentials** - You must configure credentials before you configure destinations. You can specify authentication or privacy protocols for the trap messages to forward to the other server.

8.1.10.1 Filtering Traps and Messages

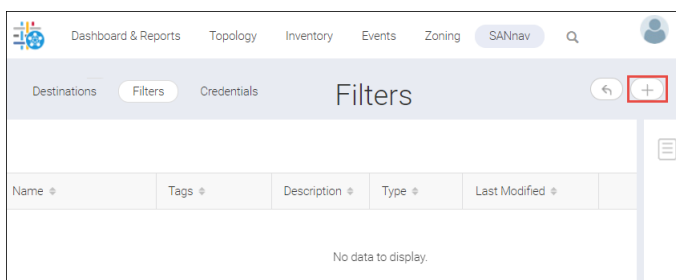
You can set up filters to determine which traps and messages are forwarded.

You can filter traps and Syslog messages based on one or more of the following criteria:

- Message type
- Product
- Regular Expression
- Severity
- Trap type

To create a filter, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **Event Management > Event Forwarding**. The **Forwarding Destinations** window is displayed.
2. Click the **Filters** tab, and then select **+** icon on the top-right corner of the **Filter** window.



3. Select either **Syslog** or **SNMP Trap** option to create filter. The **Add Filter** window is displayed.

4. Enter a unique filter name along with tags and description.

For example, in this case, enter **FILTER cdef**.

The screenshot shows the 'Add Filter' form in the SANnav management portal. The form is titled 'Add Filter' and has tabs for 'Destinations', 'Filters', and 'Credentials'. The 'Filters' tab is active. The form contains the following fields and options:

- Name:** Filter cdef
- Description:** To filter 'cdef' from the trap messages.
- Tags:** cdef
- Type:** SNMP Trap
- Regular Expression:** *cdef*
- Severity:** info
- Forward Application Events
- Forward Correlated Events

Below the form is a 'Products' section with a search bar and a table for selecting products. The table has columns for Name, WWN, and IP Address. The table is currently empty, with the message 'No data to display.' and buttons for 'Add' and 'Remove'.

5. Type the description of an event to forward in the **Regular Expression** (optional) field.

The trap messages matching cdef is forwarded. You can also add an asterisk:

- *cdef* - Matches a message that contains cdef
- *cdef - Matches a message ending with cdef
- cdef* - Matches a message beginning with cdef.

For example, in this case, type *cdef* within asterisk (*).

The maximum length is 512 characters.

6. Select **Severity** level from the drop-down.

For example, in this case, select **Info**. The trap messages containing cdef with the severity level info are forwarded.

7. Select the check boxes to **Forward Application Messages** generated by the application and to **Forward Correlated Events**.

8. To filter the messages containing "cdef" based on the origin of the product, click **Add**, and then select one or more products.

The screenshot shows the 'Products' selection dialog box. The dialog has a search bar and a table with columns for Name, WWN, and IP Address. The table contains the following data:

Name	WWN	IP Address
<input checked="" type="checkbox"/> 7840_13_w1	10:00:00:05:33:65:A8:C3	
<input checked="" type="checkbox"/> BASE_7840_13_rags	10:00:00:05:33:65:A8:C4	
<input checked="" type="checkbox"/> BR-G620-219444-71-10	10:00:C4:F5:7C:51:78:D9	
<input type="checkbox"/> BR-G620-219449-69-10	10:00:C4:F5:7C:4D:67:29	

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

9. Click **OK**.

The messages from the selected products are forwarded. For example, if you do not select any product, then the trap messages containing "cdef" from all the products are forwarded.

The products are listed in the **Products** table of the **Add Filters** window.

10. To filter a specific SNMP trap, enter the name and OID of the trap. Click **+Add** to add additional traps.

NOTE

These fields are available only when **SNMP Trap** is selected as the filter type.

Dashboard & Reports Topology Inventory Events Zoning SANnav

Destinations **Filters** Credentials **Add Filter**

Name Filter cdef Description To filter 'cdef' from the trap messages.

Tags cdef

Type SNMP Trap

Regular Expression *cdef*

Severity Info

Forward Application Events
 Forward Correlated Events

3 items **Products**

<input type="checkbox"/> Name ^	WWN ^	
<input type="checkbox"/> 7840_13_vv1	10:00:00:05:33:65:A8:C3	▼
<input type="checkbox"/> BASE_7840_13_rags	10:00:00:05:33:65:A8:C4	▼
<input type="checkbox"/> BR-G620-219444-71-10	10:00:C4:F5:7C:51:78:D9	▼

Name 1 OID + Add

Save Delete Cancel

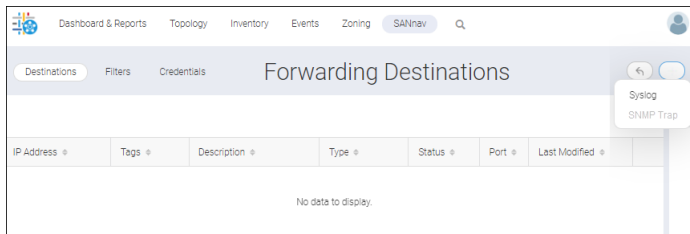
11. Click **Save** to save the new filter.

8.1.10.2 Adding a Forwarding Destination

To add a destination for forwarding, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **Event Management > Event Forwarding**.

- Click **Destinations** tab, and then select the **+** icon on the top-right corner of the **Destinations** window.
You can add trap forwarding destination only when trap forwarding credentials are configured in **Credentials** tab.
When you do not configure the trap forwarding credentials, the **+** icon shows the **Syslog** and **SNMP Trap** is disabled.



- Select either **Syslog** or **SNMP Trap** option to add forwarding destinations.
The **Add Destination** window is displayed.
- Enter the IP address along with the description and tags.

NOTE

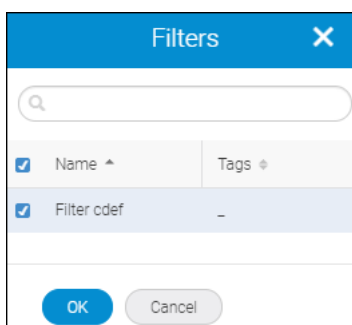
Only IPV4 address is accepted. DNS names are not accepted.

- Enter the **Port** number, which ranges from 1 to 65535 numerical characters.
- Enable **Repeater** option when the filter is not required.

NOTE

By enabling Repeater, all the Syslog or SNMP trap information are sent to the assigned destination.

- Click **Add** in the **Filters** table to add the predefined filters. You can add up to five filters.



NOTE

If you do not add any filter, you must select Syslog or Trap repeater to save the destination.

8. Click **OK**.

The filter is added under the **Filter** table of the **Add Destination** window.

9. Select **Enable** to begin the process of forwarding, and then click **Save** to save the forwarding destination.

The screenshot shows the 'Add Destination' window in the SANnav management portal. The window has a navigation bar at the top with 'SANnav' selected. Below the navigation bar are tabs for 'Destinations', 'Filters', and 'Credentials'. The main content area is titled 'Add Destination' and contains several input fields: 'IP Address', 'Description', 'Tags' (with 'Test' entered), 'Type' (set to 'SNMP Trap'), 'Port' (set to '162'), and a 'Repeater' checkbox. Below these fields is a 'Filters' section with a search bar, a table with one item, and an 'Enable' checkbox. The 'Save' button is highlighted in blue.

Name	Tags	Description	Severity
Filter cdef	-	-	INFO

8.1.10.3 Adding Trap Forwarding Credentials

As part of trap forwarding, you can specify the credentials of the receiver allowed to receive the forwarded traps and messages. Forwarding of traps will not function if credentials are not defined.

To set the credentials, follow the instructions below:

1. Click **SANnav** in the navigation bar, and then select **Event Management > Event Forwarding**.

- Click the **Credentials** tab, and then enter the **Username** and **Context Name**.

- Select an authentication protocol from the **Auth Protocol** drop-down (optional) and enter the **Auth Password**.

NOTE

The **Auth Password** and **Confirm Password** fields are available only when you select an auth protocol from the **Auth Protocol** drop-down.

NOTE

SANnav will not encode the forwarded trap if no protocol is selected.

- Select a privacy protocol from the **Privacy Protocol** drop-down (optional) and enter the **Privacy Password**.

NOTE

The **Privacy Password** and **Confirm Password** fields are available only when you select a privacy protocol from the **Privacy Protocol** drop-down.

NOTE

SANnav will not encode the forwarded trap if no protocol is selected.

- Click **Save** to save the credentials.

8.1.11 Managing Event Actions

The **Events Action Policies** window allows you to configure different actions, when the event is triggered based on the policy configured.

The **Event Actions** window provides control over the following processes:

- Type of events to be monitored
- Products to be monitored
- Monitoring frequency
- Actions required for the monitored events

You can select any of the five actions below to perform as an event action.

- Select **Alert by Email** to be notified by email about a selected event.
- Select **Suppress Event**. The selected event under suppress events will not be notified by the SANnav. For example, events with no impact or informational events do not require notification.
- Set the events that require SANnav to **Auto Acknowledge** when the events are triggered.
- Select **Capture SupportSave** to collect the SupportSave details when the event is triggered.
- Select **Special Event** to mark events for future review. For example, when few least priority switches are discovered, you can be notified regarding the switch events when you select **Specials Events** in the **Events** tab.
- Select **Maintenance Mode** to be informed of the events that are occurring from a maintenance switch. For example, in the case of a faulty switch with many captured events, select maintenance mode. The related switch events will be recorded in the maintenance mode list.

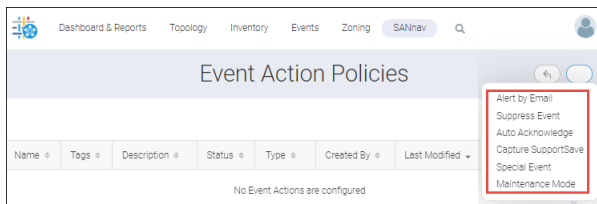
The following three sections need to configure to configure an event action:

- Identification and Action
- Events and Policy
- Sources

8.1.11.1 Configuring Identification and Action

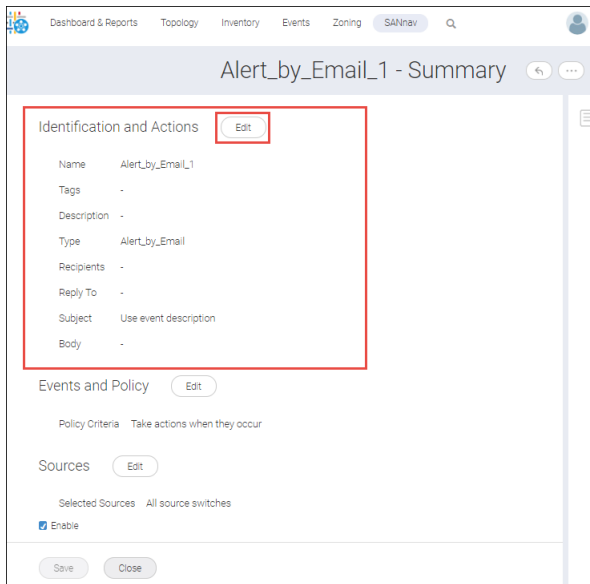
To add an event action, follow the instructions below:

1. Click **SANnav** in the navigation bar, and then select **Event Management > Event Action Policies**. The **Event Action Policies** window is displayed.
2. Click the **+** icon on the top-right corner of the window to configure an event action.

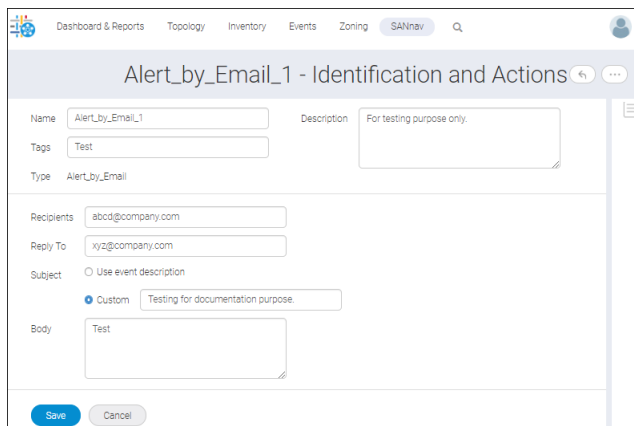


3. Select the action required to perform at an event from the drop-down. For example, in case you want to be notified about an event by email select **Alert by Email**.

4. Click **Edit** to edit Identification and Actions in the respective event actions summary window.



5. Customize the settings for the edit window of Identification and Actions as follows:
- Type the name of the event action in the **Name** field.
Minimum is 1 and maximum up to 64 alphanumerical characters.



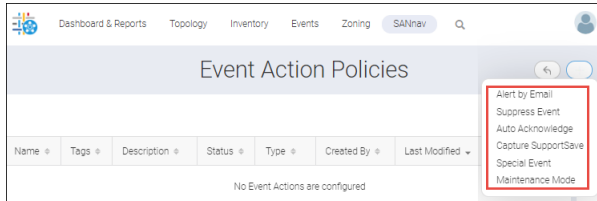
- Type the description of the selected event action in the **Description** field (optional).
 - Type the email ID of the recipient in **Recipients** field to whom the mail must be sent. Type the email ID of the sender in the **Reply To** field.
 - You can perform either of the below-mentioned actions to state in the subject of the email:
 - Select **Use event description** to utilize the existing event description.
 - Select **Custom** to enter a new event description in the subject field.
 - Type the email information in the **Body** field.
6. Click **Save** to save the changes / customization.
- Click **Cancel** to cancel the operation and revert to the event action summary window.

8.1.11.2 Creating Events and Policy

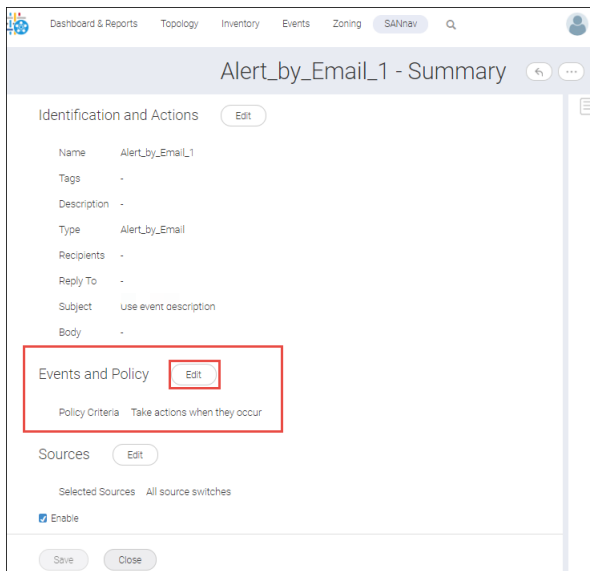
In the Events and Policy window, add the events that require action.

To create Events and Policy in the respective events action summary window, follow the instructions below:

1. Click **SANnav** in the navigation bar, and then select **Event Management > Event Action Policies**. The **Event Actions Policies** window is displayed.
2. Click the **+** icon on the top right corner of the window to configure an event action.

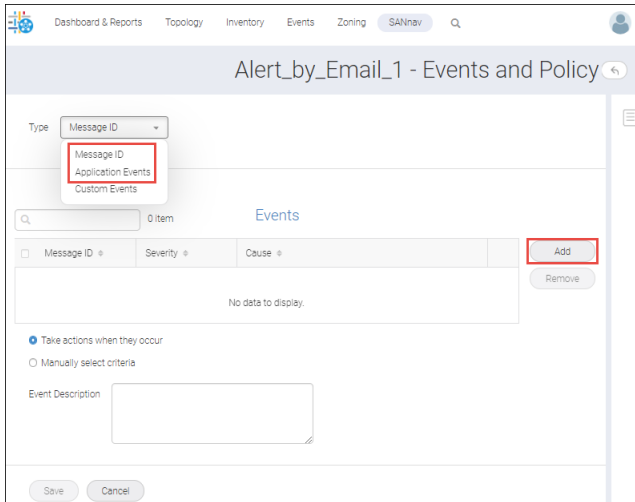


3. Click **Edit** in the Events and Policy section.



4. You can configure events and policies by selecting one of the following options:

- Message ID
 - Application Events
 - Custom Events
- a. To add an event by Message ID or Application:
 - Select **Message ID** or **Application Events** from the **Type** drop-down.

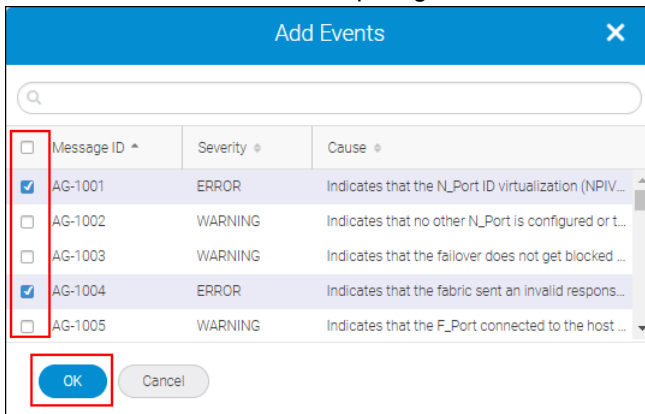


- Click **Add** to add the events for action.

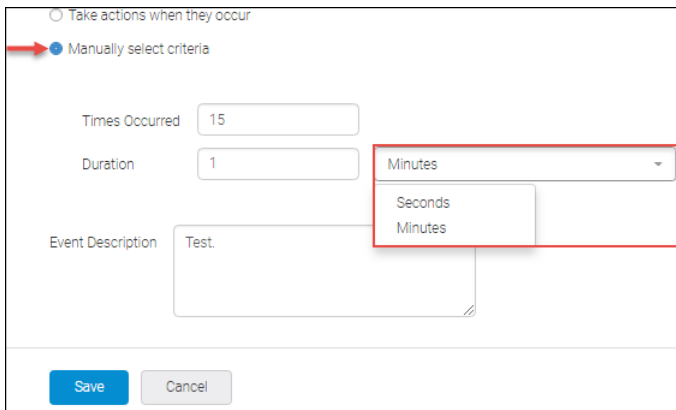
NOTE

You can view the Add Events displayed based on the selected criteria for the type.

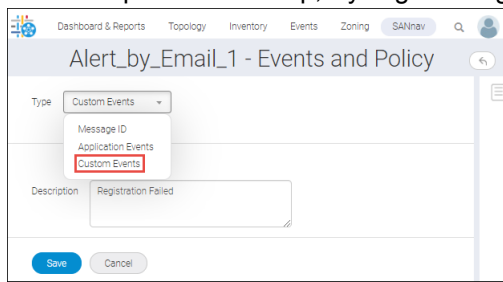
- Message ID
 - Application Events
- Select one or more events requiring the action and click **OK**.



- Select **Manually select criteria** to perform the action on a specific instruction.



- Specify after how many occurrences of the selected event the action should be performed, in **Times Occurred**. Occurrences count must be between 1 and 999.
 - Set Duration in **Seconds** or **Minutes**.
For seconds - occurrences duration must be between 0 and 59940.
For minutes - occurrences duration must be between 1 and 999.
 - Type the required message in the **Events Description** field.
Minimum is 1 and maximum is 256 alphanumerical characters.
 - You can also select **Take actions when they occur** to perform the action when the selected event occurs and enter the required message (optional) in the Events Description field.
- b. To add events by description:
- Select **Custom Event** and type the description of the event in the **Description** field.
Minimum is 1 and maximum up to 1024 alphanumerical characters. Double quotation (") is not allowed in the description field.
For example, when you type "Registration Failed" in the description field, the event action is triggered based on the description in the Trap, Syslog Message (Product Audit Event), or Application event.

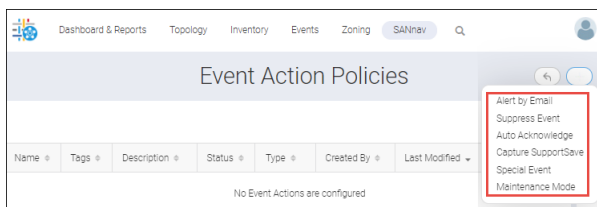


5. Click **Save** to save the changes.

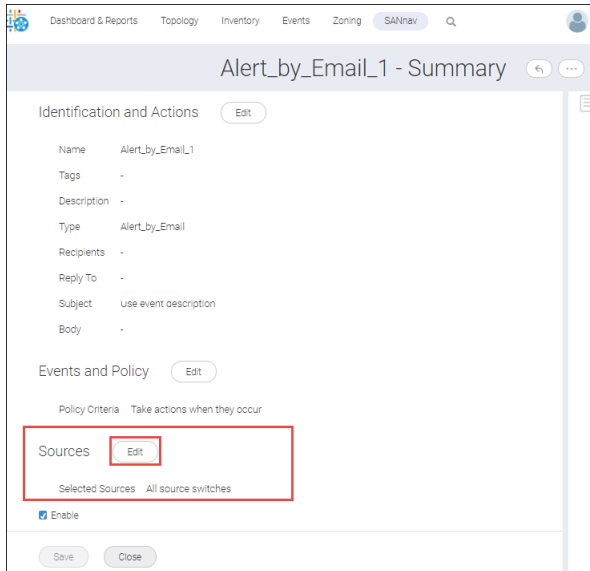
8.1.11.3 Creating Sources

To manage the sources for events, follow the instructions below:

1. Click **SANnav** in the navigation bar, and then select **Event Management > Event Action Policies**.
2. Click the **+** icon on the top right corner of the window to configure an event action.



3. Click **Edit** in the Sources section.



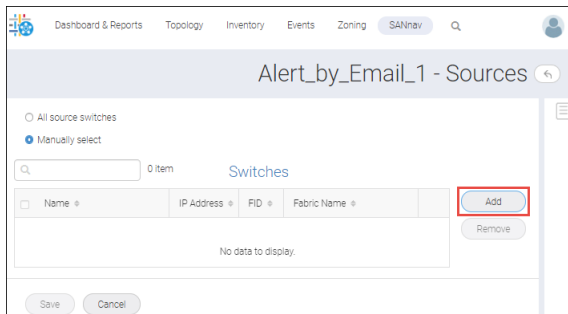
4. To select switches from source, select one of the following option:

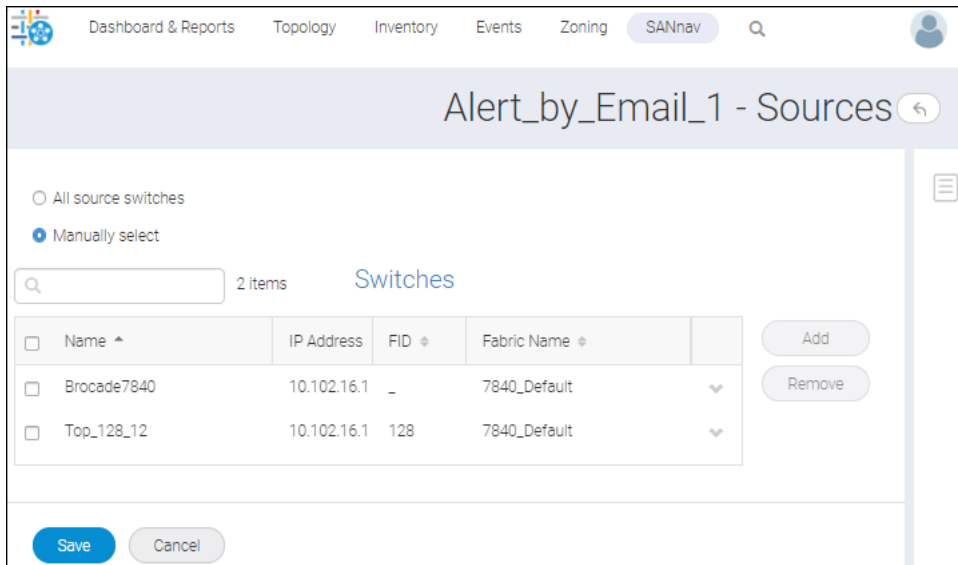
- **All source switches**

The selected event action applies to all the switches discovered in the application when **All source switches** option is enabled. By default, the **All source switches** option is selected.

- **Manually select.**

The **Manually select** option is used to add one or more switches. Click **Add** to add the switches. The **Select Sources** window is displayed, and click **OK** to add the switches.





5. Click **Save** to save the switch as a source for the events.

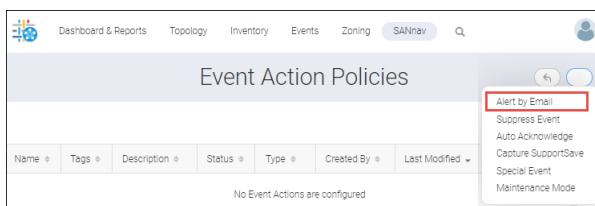
8.1.11.4 Creating an Event Action for Critical Events

Scenario

You will be notified when a critical event occurs on a device, port, or system without a remediation action within a certain time frame. For example, you may want to be notified immediately by email when a certain device interface is down for more than one minute.

User Action

1. Click **SANnav** in the navigation bar, and then select **Event Management > Event Action Policies**.
2. Click the **+** icon on the top-right corner of the window, and select **Alert by Email**.



3. Click **Edit** in the **Identification and Actions** to configure the email setup.
4. Type the event action name in the **Name** field along with tags and a description.
For example, in this case, enter **Critical_Event**.

The minimum is 1 and a maximum of 256 alphanumeric characters are allowed in the **Name** field.

The minimum is 1 and a maximum of 1024 alphanumeric characters are allowed in the **Description** field.

The screenshot shows the 'Critical_Event - Identification and Actions' form. The fields are as follows:

- Name: Critical_Event
- Description: [Empty text area]
- Tags: Critical
- Type: Alert_by_Email
- Recipients: abc@company.com
- Reply To: xyz@company.com
- Subject: Use event description, Custom
- Body: [Empty text area]

Buttons: Save, Cancel

5. Type the email ID of the recipient in the **Recipients** and **Reply To** fields.
6. To create the subject line of the email, select one of the following:
 - Select **Use event description** to utilize the existing event description.
 - Select **Custom** to enter a new event description in the subject field.
7. Type the email information in the **Body** field, and click **Save** to save the configuration and revert to the action summary window.
8. Click **Edit** in the **Events and Policy** section to add the events.
9. Select the type of event from the **Type** drop-down, and click **Add** to add the events for action.

The screenshot shows the 'Critical_Event - Events and Policy' form. The 'Type' dropdown menu is open, showing the following options:

- Message ID
- Application Events
- Custom Events

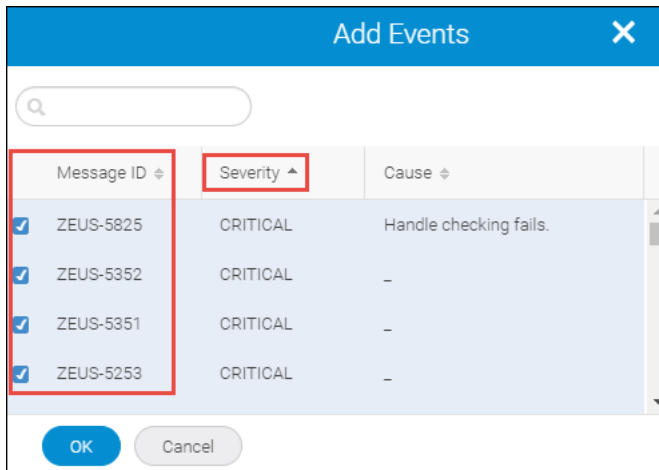
Below the dropdown is a table with the following columns: Message ID, Severity, Cause, and an Add button. The table is currently empty with 'No data to display.'

Below the table are radio buttons for 'Take actions when they occur' (selected) and 'Manually select criteria'.

Event Description: [Empty text area]

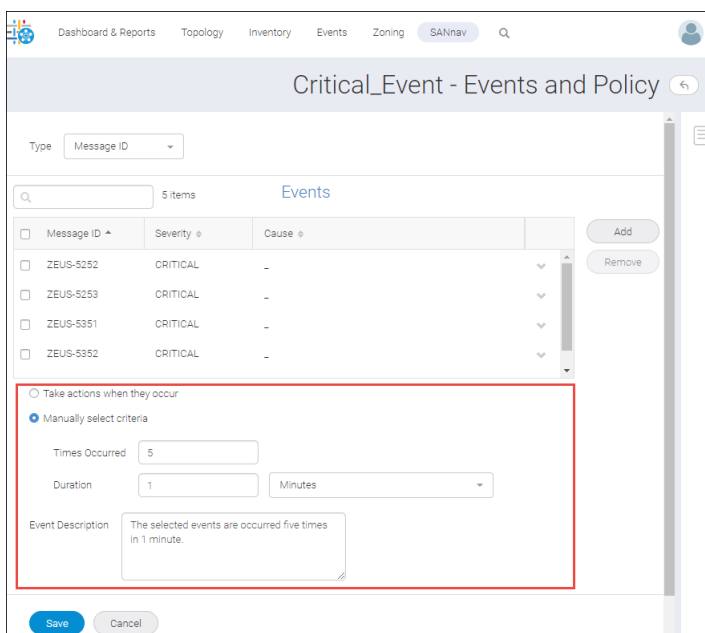
Buttons: Save, Cancel

10. Click **Severity** to sort the severity level, and select one or more critical events that you require to be notified by email. Click **OK** to add the events.



11. When you want to be notified after the event has occurred a few times within the specified time duration, select **Manually select criteria**.

In this case, the events have occurred five times in one minute, and then the email notification is triggered.



12. Click **Save** to save the events and policy.

13. Click **Edit** in **Sources** to add the switches.

Critical_Event - Summary

Identification and Actions Edit

Name Critical_Event
 Tags Critical
 Description -
 Type AlertBy_Email
 Recipients abc@company.com
 Reply To xyz@company.com
 Subject Use event description
 Body

Events and Policy Edit

Details

Policy Criteria Manually select criteria

Sources Edit

Selected Sources All source switches

Enable

Save Close

14. Select **Manually select**, and click **Add**.

Critical_Event - Sources

All source switches
 Manually select

2 items Switches

<input type="checkbox"/>	Name	IP Address	FID	Fabric Name	
<input type="checkbox"/>	Brocade7840		-	7840_Default	Add Remove
<input type="checkbox"/>	Top_128_12		128	7840_Default	

Save Cancel

15. Select one or more switches by selecting the checkboxes, and click **OK**.

16. Click **Save** to save the switches as a source.

17. Select **Enable** to make the Alert by Email action effective.

NOTE

By default, the **Enable** option is selected.

18. Click **Save** to commence the event action.

System Behavior

You will receive the correlated events generated by the event action, not the actual event in the email after the critical events occur within the stipulated time duration.

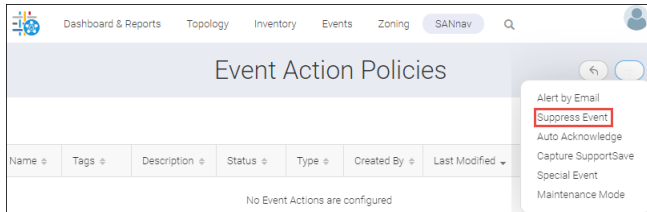
8.1.11.5 Using Event Action to Suppress Selected Events

Scenario

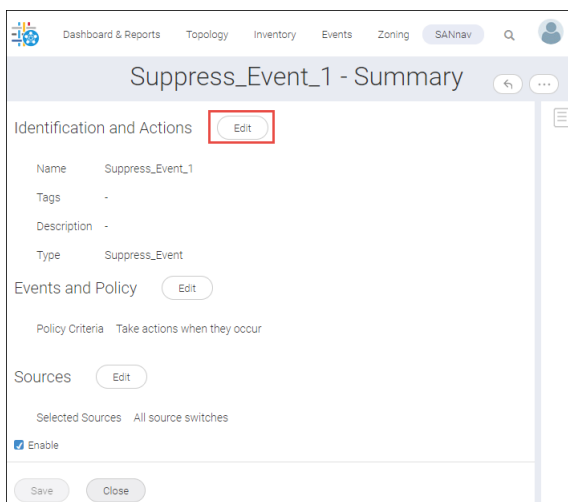
Event action can be set in such a way to suppress events and only log an entry, which shows the summary of the number of events that occurred during a specified time frame when the number of events exceeds a certain threshold.

User Action

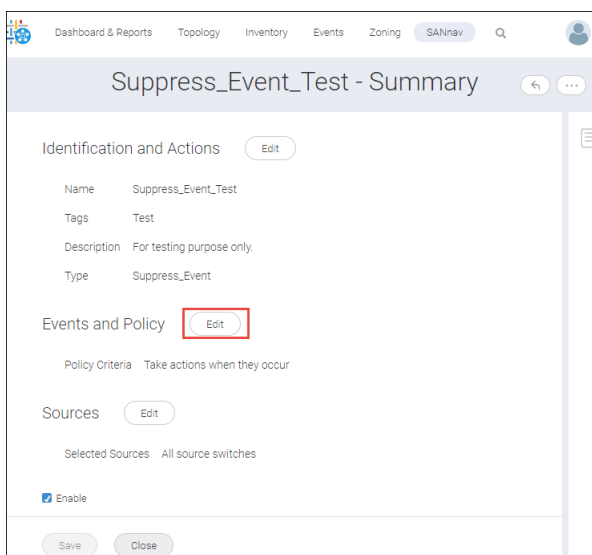
1. Click **SANnav** in the navigation bar, and then select **Event Management > Event Action Policies**.
2. Click the **+** icon on the top-right corner of the window, and select **Suppress Event**.



3. Click **Edit** in the **Identification and Actions** section.



4. Enter the event identification name and description, and click **Save**.
5. Click **Edit** in the **Events and Policy** section.



6. Select the type of event from the **Type** drop-down, and click **Add** to add the events to be suppressed.
7. Select one or more events by selecting the checkboxes and click **OK** to add the events.

<input type="checkbox"/>	Message ID ^	Severity *	Cause *
<input checked="" type="checkbox"/>	AG-1001	ERROR	Indicates that the N_Port ID virtualization (NPV...)
<input type="checkbox"/>	AG-1002	WARNING	Indicates that no other N_Port is configured or t...
<input type="checkbox"/>	AG-1003	WARNING	Indicates that the failover does not get blocked ...
<input checked="" type="checkbox"/>	AG-1004	ERROR	Indicates that the fabric sent an invalid respons...
<input type="checkbox"/>	AG-1005	WARNING	Indicates that the F_Port connected to the host ...

OK Cancel

8. Click **Save** to save the events and policies.
9. Click **Edit** in the **Sources** section.

Dashboard & Reports Topology Inventory Events Zoning SANnav Q

Suppress_Event_Test - Summary

Identification and Actions [Edit](#)

Name Suppress_Event_Test
 Tags Test
 Description For testing purpose only.
 Type Suppress_Event

Events and Policy [Edit](#)

› Details

Policy Criteria Take actions when they occur

Sources [Edit](#)

Selected Sources All source switches

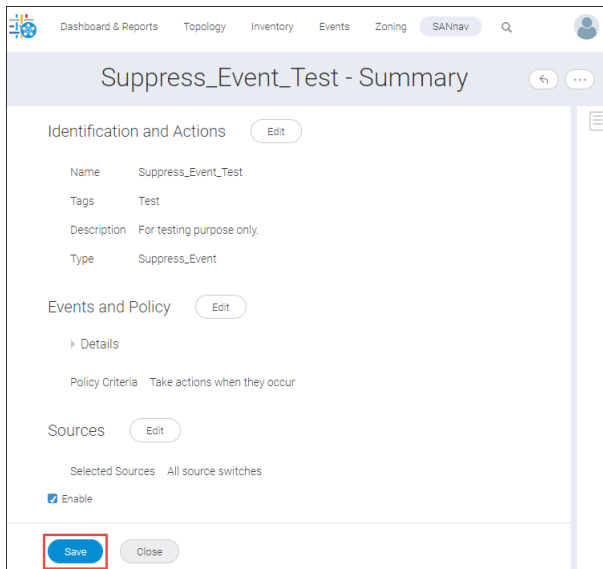
Enable

Save Close

10. Select **All source switches** to suppress the events from all switches that are discovered in SANnav, and click **Save**.
11. Select **Enable** to make the suppress events action effective, and click **Save** to commence the event action.

NOTE

By default, the **Enable** option is selected.



System Behavior

There is no log entry in case of suppress events. Events will not be persisted in the DB, and you will not be able to view these events.

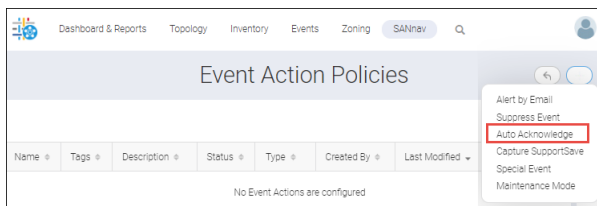
8.1.11.6 Auto Acknowledging Events Based on Event Description

Scenario

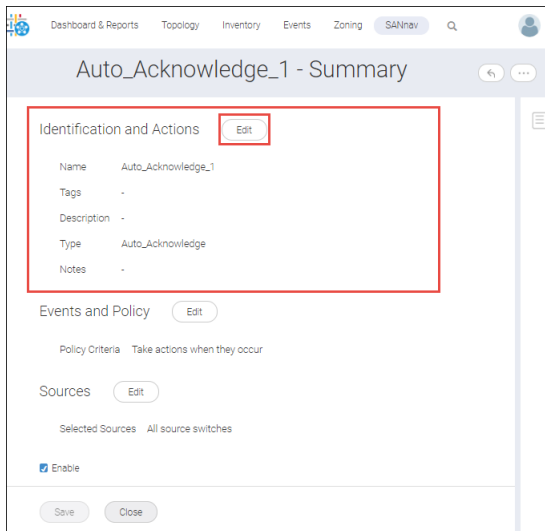
For event actions defined on SNMP traps, you can further utilize the Varbind filter capability. For example, if you want to acknowledge **SWEvent**, enter **SWEvent** and events that match this string will be acknowledged.

User Action

1. Click **SANnav** in the navigation bar, and then select **Event Management > Event Action Policies**.
2. Click the **+** icon on the top right corner of the window and click **Auto Acknowledge**.



3. Click **Edit** in the **Identification and Actions** section.



4. Enter the event identification name and description.

5. Enter the reason for auto acknowledge in the **Notes** field, and click **Save** to save the acknowledgment notes.

The screenshot shows the SANnav management portal interface for editing the 'Auto_Acknowledge_1' configuration. The top navigation bar is the same as in the previous screenshot. The main heading is 'Auto_Acknowledge_1 - Identific...'. The form contains the following fields: 'Name' (Auto_Acknowledge_1), 'Description' (For test purpose only), 'Tags' (Test), 'Type' (Auto_Acknowledge), and 'Notes' (The reason to auto acknowledge). At the bottom, there are 'Save' and 'Cancel' buttons. The 'Save' button is highlighted in blue.

6. Click **Edit** in the **Events and Policy** section.

The screenshot shows the 'Auto_Acknowledge_1 - Summary' page in the SANnav management portal. The page has a navigation bar at the top with 'Dashboard & Reports', 'Topology', 'Inventory', 'Events', 'Zoning', and 'SANnav'. Below the navigation bar, the page title is 'Auto_Acknowledge_1 - Summary'. The main content area is divided into several sections: 'Identification and Actions' with an 'Edit' button, 'Name' (Auto_Acknowledge_1), 'Tags' (Test), 'Description' (For test purpose only.), 'Type' (Auto_Acknowledge), and 'Notes' (The reason to auto acknowledge.). Below this is the 'Events and Policy' section, which is highlighted with a red box. It contains a 'Policy Criteria' field with the value 'Take actions when they occur' and an 'Edit' button, also highlighted with a red box. Below the 'Events and Policy' section is the 'Sources' section with an 'Edit' button, 'Selected Sources' (All source switches), and an 'Enable' checkbox. At the bottom of the page are 'Save' and 'Close' buttons.

7. Customize the settings for the edit window of Events and Policy as follows:

a. Select **Custom Events** from the **Type** drop-down.

The screenshot shows the 'Auto_Acknowledge_1 - Events and Policy' edit window in the SANnav management portal. The page title is 'Auto_Acknowledge_1 - Events and ...'. The 'Type' drop-down menu is open, showing three options: 'Message ID', 'Application Events', and 'Custom Events'. The 'Custom Events' option is highlighted with a red box. Below the drop-down menu is the 'Description' field with the value 'SWEvent'. At the bottom of the window are 'Save' and 'Cancel' buttons.

b. Type the description of the event in the **Description** field.

For example: When you type **SWEvent** in the description field, the application will add all the events with the description of "swEvent".

c. Click **Save** to save the custom event.

8. Click **Edit** in the **Sources** section.

Dashboard & Reports Topology Inventory Events Zoning SANnav Q

Auto_Acknowledge_1 - Summary

Identification and Actions

Name Auto_Acknowledge_1
 Tags Test
 Description For test purpose only.
 Type Auto_Acknowledge
 Notes The reason to auto acknowledge.

Events and Policy

Policy Criteria Take actions when they occur

Sources

Selected Sources All source switches

Enable

9. Select the **Manually Select** option, and click **Add** to add the switches manually.

Dashboard & Reports Topology Inventory Events Zoning SANnav Q

Auto_Acknowledge_1 - Sources

All source switches
 Manually select

Q 0 item Switches

<input type="checkbox"/>	Name	IP Address	FID	Fabric Name	<input type="button" value="Add"/>
No data to display.					

10. Select one or more switches by selecting the checkboxes, and click **OK** to add the switches as a source.

Select Sources X

Q

<input checked="" type="checkbox"/>	Name	IP Address	FID	Fabric Name	WWN	Status
<input checked="" type="checkbox"/>	Brocade7840	10.102.16.13	-	7840_Default	10:00:00:05:1E:65...	Critical
<input checked="" type="checkbox"/>	Top_128_12	10.102.16.12	128	7840_Default	10:00:00:05:1E:65...	Not Reachable

11. Click **Save** to add the switches to the source for the event.

12. Select **Enable** to make the auto acknowledge event action effective.

NOTE

By default, the **Enable** option is selected.

The screenshot shows the SANnav Management Portal interface for configuring an auto-acknowledge event. The page title is "Auto_Acknowledge_1 - Summary". It features several sections: "Identification and Actions" with fields for Name (Auto_Acknowledge_1), Tags (Test), Description (For test purpose only.), Type (Auto_Acknowledge), and Notes (The reason to auto acknowledge.); "Events and Policy" with a "Details" section containing a "Custom Description" field set to "SWEEvents"; and "Sources" with a "Selected Sources" section showing "Manually selected source switches (2)". A checkbox labeled "Enable" is checked and highlighted with a red box. At the bottom, there are "Save" and "Close" buttons, with the "Save" button also highlighted with a red box.

13. Click **Save** to commence the event action.

System Behavior

The action is triggered on the selected events that have an event description that matches the string pattern (in this case, **SWEEvent**), and are is specified in the Events and Policy details.

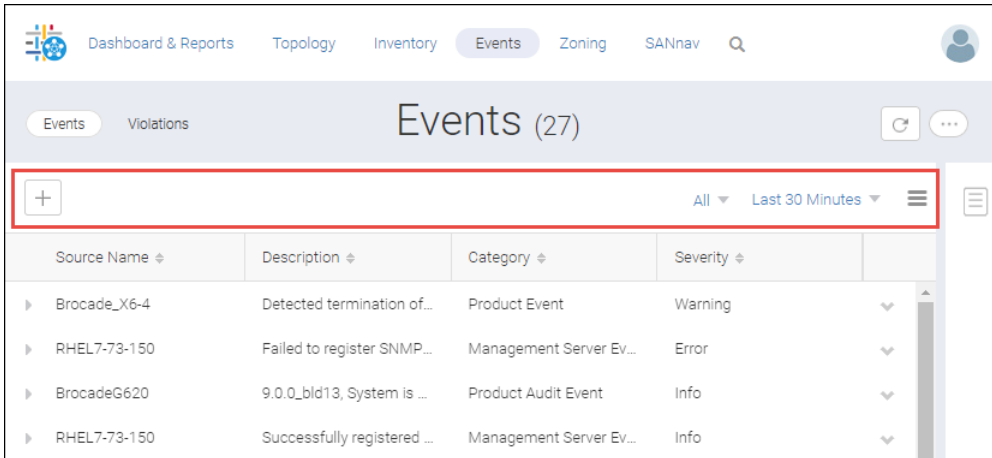
8.1.12 Filtering Events

SANnav Management Portal provides several options for displaying events. You can filter events based on network scope, date range, and customized filters. In addition, you can customize which columns are displayed on the page.

NOTE

When you are viewing events, the filter bar on the **Events** window provides several options for filtering the displayed events.

- Click the **+** button to add existing filters and create new filters.
- Click **All** to select the network scope of the displayed events.
- Click **Last 30 Minutes** to select the date range for displayed events.



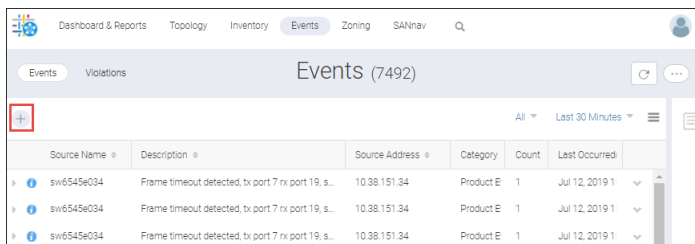
In addition to filtering the events, you can also click the hamburger icon (≡) to hide or display specific columns of data.

The following procedure shows how to create a custom event filter to display.

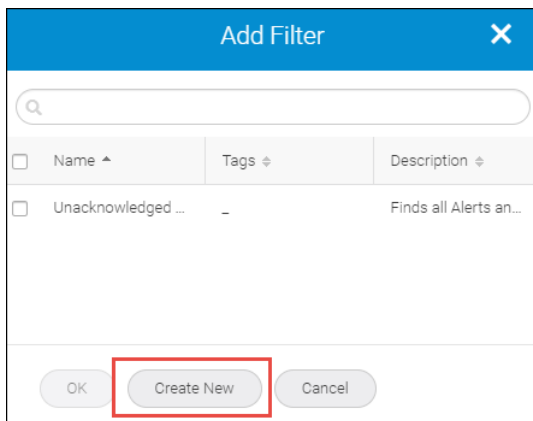
1. Click **Events** in the navigation bar.

The filter bar contains several options for filtering events.

2. Click the **+** button on the left side of the filter bar.



3. Select one or more existing event filters and click **OK**, or click **Create New** to add a new event filter.



The **Create New Filter** window is displayed.

4. Click **Event Categories and Severity** and then select category and corresponding severity.

5. Click **Included Events** or **Excluded Events** (optional) to filter the event further and click **Add**.

6. Select the event from the **Filter Options** and click to move the event as selected events. Click **OK** to add the filters to the new event filter.

7. Click **OK** to apply the filter in the list view.

You can also select **Save Filter** check box to save the event filter by entering the filter name, tags and description.

8.1.13 Searching Events

You can view specific events in the Events tab by searching using a particular keyword.

To search for a particular event in the **Events** tab, follow the instructions below:

1. Click **Events** in the navigation bar. By default, the **Events** tab is selected.
2. Enter three or more characters and SANnav Management Portal will fetch the auto-suggestions. The search results are populated based on the properties listed below:

- Source Name
- Source Address
- Description
- Fabric Name
- Message ID
- Severity

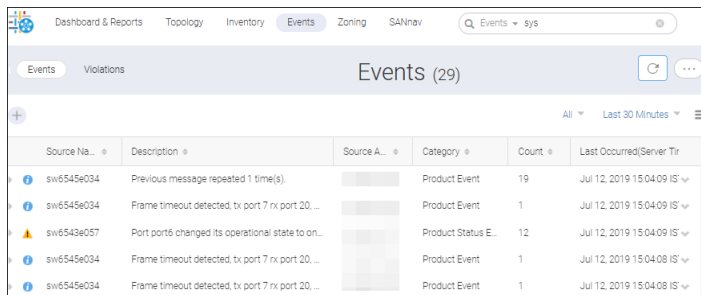
Source	Description	Source A.	Category	Count	Last Occurred(Sever Time)
sw16505...	Port port23 changed its operational st...		Product Status Ev...	14	Jul 12, 2019 14:35:21 IST
sw6545e0...	Frame timeout detected, tx port 7 rx po...		Product Event	1	Jul 12, 2019 14:35:21 IST
RHEL7.6	Failed to register syslog for the switch ...		Management Serv...	1	Jul 12, 2019 14:35:21 IST
sw6545e0...	Previous message repeated 1 time(s).		Product Event	149	Jul 12, 2019 14:35:21 IST
sw6545e0...	Frame timeout detected, tx port 7 rx po...		Product Event	1	Jul 12, 2019 14:35:21 IST
sw6545e0...	Frame timeout detected, tx port 7 rx po...		Product Event	1	Jul 12, 2019 14:35:21 IST
sw5480e0...	The port port7 state has changed to o...		Product Status Ev...	8	Jul 12, 2019 14:35:21 IST

- You can also click **Filter Events for "sys"** to match the entered string in all the six properties.

Click the refresh button on the top-right corner of the window to view the latest events occurred.

NOTE

Refresh button is disabled in case of any custom filter is applied to the events list.



Source No.	Description	Source A.	Category	Count	Last Occurred/Server Tr
swi6545e034	Previous message repeated 1 time(s)		Product Event	19	Jul 12, 2019 15:04:09 IST
swi6545e034	Frame timeout detected, tx port 7 rx port 20...		Product Event	1	Jul 12, 2019 15:04:09 IST
swi6543e057	Port port6 changed its operational state to on...		Product Status E...	12	Jul 12, 2019 15:04:09 IST
swi6545e034	Frame timeout detected, tx port 7 rx port 20...		Product Event	1	Jul 12, 2019 15:04:08 IST
swi6545e034	Frame timeout detected, tx port 7 rx port 20...		Product Event	1	Jul 12, 2019 15:04:08 IST

8.1.14 Viewing Violations

You can view violations in the **Events** tab. The **Violations** tab displays the violations for the switches for which the rule threshold has crossed.

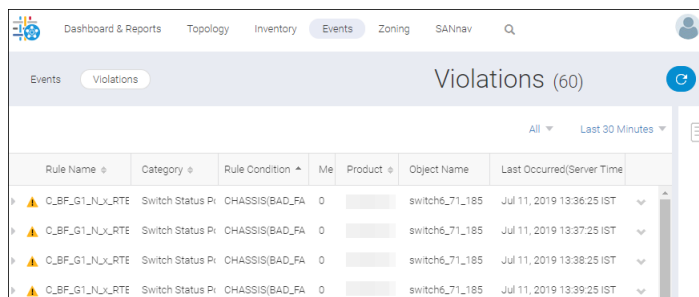
To view the MAPS violations in the **Events** tab, follow the instructions below:

1. Click **Events** in the navigation bar, and then select **Violations** tab to view the violations.

The **Violations** window is displayed. The Violations window lists the MAPS violations based on the selected network scope and date range.

NOTE

SANnav does not support applying filters to the violations view.



Rule Name	Category	Rule Condition	Me	Product	Object Name	Last Occurred/Server Time
C_BF_G1_N_X_RTE	Switch Status Pi	CHASSIS(BAD_FA	0		switch6_71_185	Jul 11, 2019 13:36:25 IST
C_BF_G1_N_X_RTE	Switch Status Pi	CHASSIS(BAD_FA	0		switch6_71_185	Jul 11, 2019 13:37:25 IST
C_BF_G1_N_X_RTE	Switch Status Pi	CHASSIS(BAD_FA	0		switch6_71_185	Jul 11, 2019 13:38:25 IST
C_BF_G1_N_X_RTE	Switch Status Pi	CHASSIS(BAD_FA	0		switch6_71_185	Jul 11, 2019 13:39:25 IST

2. Click the  icon to view the details of a rule.

The screenshot shows the SANnav Events page with the 'Violations' tab selected. The main heading is 'Violations (60)'. Below the heading, there are filters for 'All' and 'Last 30 Minutes'. A table lists violations with columns: Rule Name, Category, Rule Condition, Measure Value, Product, Object Name, and Last Occurred. The first violation is highlighted with a red box, and its details are expanded in a modal window. The details include:

Rule Name	C_FU_G1_N_x_RTExxx	Product Address	
Rule Condition	CHASSIS(FLASH_USAC	Unit	%
Severity	Warning	Fabric	chewbecca_185
Measure Value	46	Recommended Action	Flash increases and decreases slight normal operation of the switch. Excessive permanent increases can lead to failure. Remove some unwanted files to clear flash space. Execute the support scripts to remove files from the kernel space.
Actions	None		

3. You can view the product and fabric details of a rule. To view the details, click icon.

If the event is associated with the product you can view the product details by selecting **View Product**.

If the event is associated with a fabric you can view the fabric details by selecting the **View Fabric** option.

The options to view product and fabric details are displayed.

The screenshot shows the SANnav Events page with the 'Violations' tab selected. The main heading is 'Violations (60)'. Below the heading, there are filters for 'All' and 'Last 30 Minutes'. A table lists violations with columns: Rule Name, Category, Rule Condition, Measure Value, Product, Object Name, and Last Occurred. The first violation is highlighted with a red box, and its details are expanded in a modal window. The details include:

Rule Name	C_FU_G1_	Category	Switch Res	Rule Con...	CHASSIS(F	Meas	46	Product	switch6_71	Object Name	switch6_71	Last Occurred(Server ...	Jul 11, 2019 15:07:25 IST
Rule Name	C_BF_G1_	Category	Switch Stal	Rule Con...	CHASSIS(B	Meas	0	Product	switch6_71	Object Name	switch6_71	Last Occurred(Server ...	Jul 11, 2019 15:07:25 IST
Rule Name	C_FU_G1_	Category	Switch Res	Rule Con...	CHASSIS(F	Meas	46	Product	switch6_71	Object Name	switch6_71	Last Occurred(Server ...	Jul 11, 2019 15:06:25 IST
Rule Name	C_BF_G1_	Category	Switch Stal	Rule Con...	CHASSIS(B	Meas	0	Product	switch6_71	Object Name	switch6_71	Last Occurred(Server ...	Jul 11, 2019 15:06:25 IST


The 'View Product' and 'View Fabric' options are highlighted with a red box.

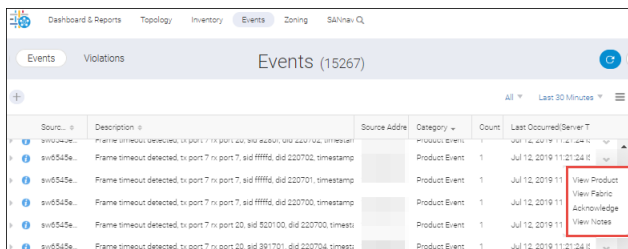
8.1.15 Acknowledging or Unacknowledging Events

You can acknowledge or unacknowledge events in the **Events** List view. You can acknowledge or unacknowledge a single event or multiple events at a time.

8.1.15.1 Acknowledging or Unacknowledging a Single Event

To acknowledge or unacknowledge a single event, follow the instructions below:

1. Click **Events** tab in the navigation bar. By default the **Events** tab is selected. The **Events** list is displayed.
2. Click the  icon next to the event that you want to acknowledge or unacknowledge.
3. Select **Acknowledge** or **Unacknowledge** option based on the requirement



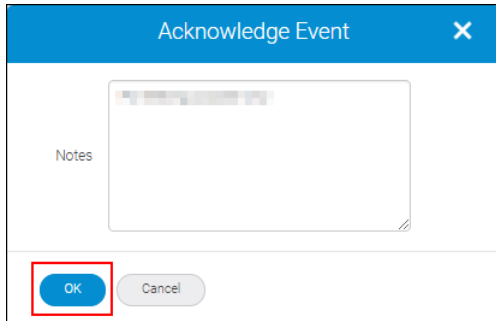
Source	Description	Source Address	Category	Count	Last Occurred	Server T
svd545e...	Frame timeout detected: tx port 7 rx port 7, sid fffff, did 220702, timestamp		Product Event	1	Jul 12, 2019 11:21:24 a	
svd545e...	Frame timeout detected: tx port 7 rx port 7, sid fffff, did 220701, timestamp		Product Event	1	Jul 12, 2019 11:21:24 a	
svd545e...	Frame timeout detected: tx port 7 rx port 7, sid fffff, did 220700, timestamp		Product Event	1	Jul 12, 2019 11:21:24 a	
svd545e...	Frame timeout detected: tx port 7 rx port 20, sid 520100, did 220700, timestamp		Product Event	1	Jul 12, 2019 11:21:24 a	
svd545e...	Frame timeout detected: tx port 7 rx port 20, sid 391701, did 220704, timestamp		Product Event	1	Jul 12, 2019 11:21:24 a	

The **Acknowledge Event** or **Unacknowledge Event** window is displayed.

4. Enter the acknowledge or unacknowledged event notes and click **OK**.

NOTE

SANnav does not add the notes on an already acknowledged or unacknowledged event.



If the event is associated with the product you can view the product details by selecting **View Product** option.

If the event is associated with a fabric you can view the fabric details by selecting the **View Fabric** option.

You can also view notes of the acknowledged or unacknowledged event(s) using the **View Notes** option.


NOTE

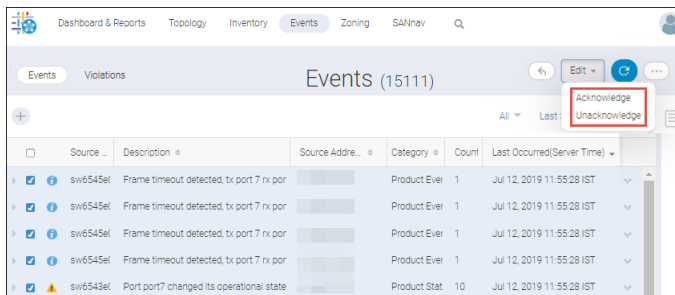
You can view product and fabric details of a single event.

8.1.15.1.1 Acknowledging or Unacknowledging Multiple Events

To acknowledge or unacknowledge multiple events at a time, follow the instructions below:

1. Click **Events** tab in the navigation bar. By default the **Events** tab is selected. The **Events** list is displayed.

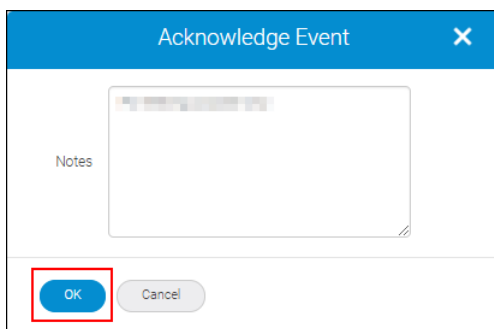
- Click the more icon (), on the top-right corner of the window and then select **Bulk Select**. The options to select multiple events are displayed.
- Select one or more events and click **Acknowledge** or **Unacknowledge** under **Edit**.



- Enter the acknowledge or unacknowledged event notes and click **OK**.

NOTE

SANnav does not add the notes on an already acknowledged or unacknowledged event.



8.1.16 Setting Event Management Reports and Dashboard Widgets

The Event Management dashboard allows you to view all the widgets and reports in the application dashboard window.

To add the Event Management reports and dashboard widgets, follow the instructions below:

- Click **Dashboard & Reports** in the navigation bar, and then select the **Templates** tab to add the Event Management widgets.
- Click the **+** icon on the top-right corner of the window and click **Select Widgets** under **Dashboard** or **Report**.

The Event Management dashboard widgets are of two categories:

Events widgets

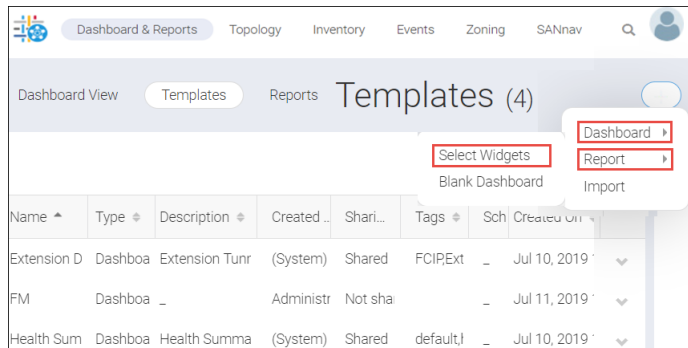
- Events Summary
- Top N Events


MAPS widgets

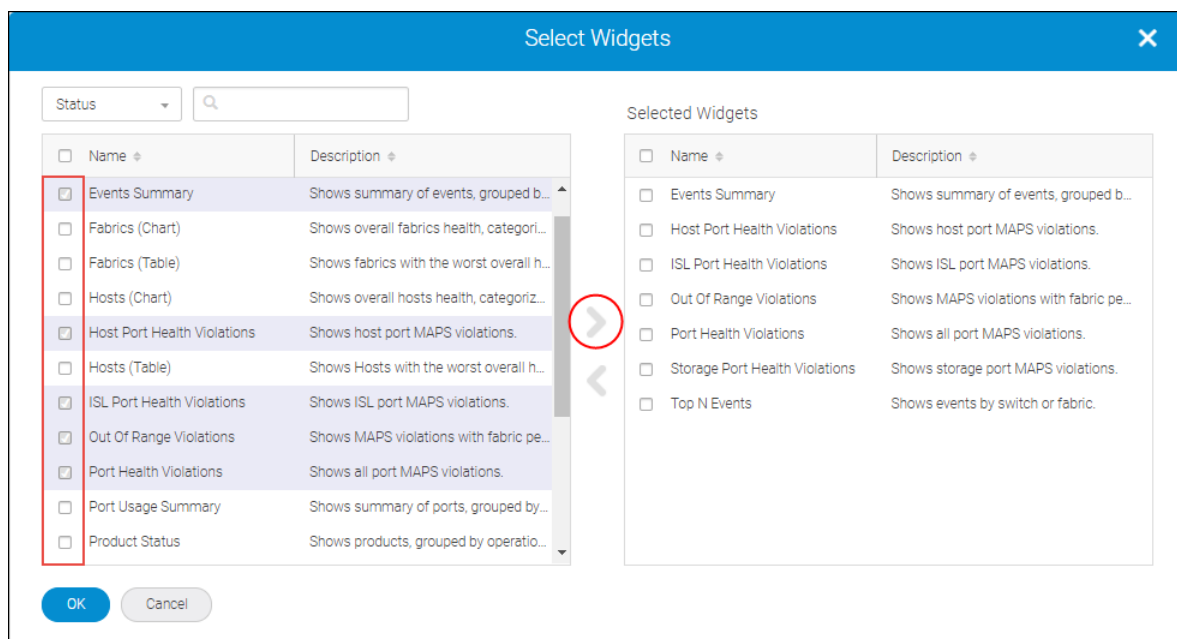
- Host Port Health Violations
- ISL Port Health Violations
- Out of Range Violations
- Port Health Violations
- Storage Port Health Violations.

The Event Management reports is categorized as mentioned below:

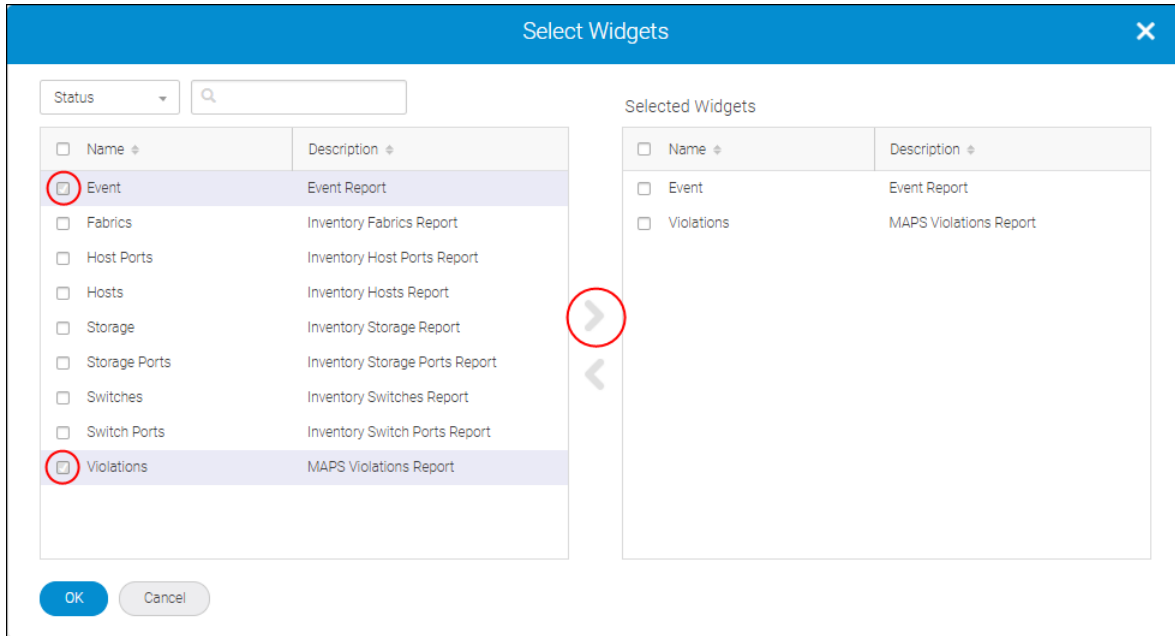
- Event
- Violations.



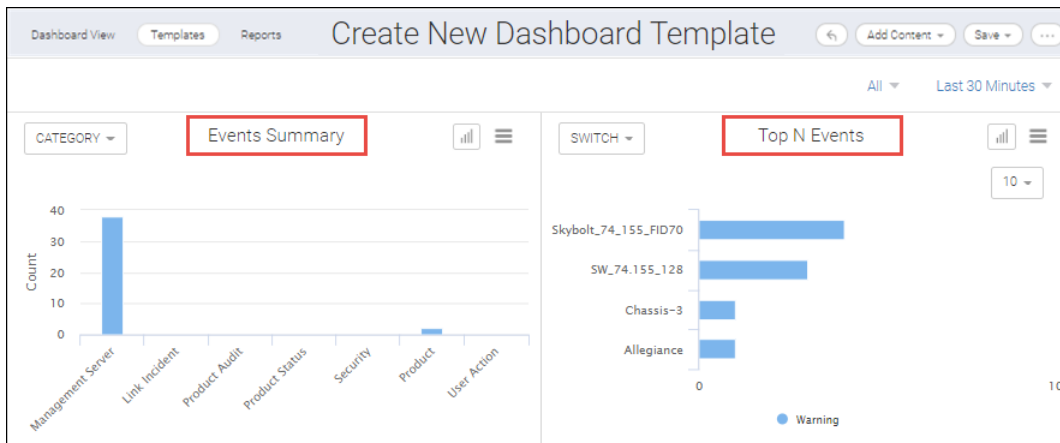
3. Select the **Dashboard** or **Report** widgets.
The **Select Widgets** window is displayed.
4. Click () to move to the **Selected Widgets**.
The following is an example of selecting **Dashboard** widgets.



The following is an example of selecting **Reports** widgets.



5. Click **OK**. The **Create New Dashboard Template** or **Create New Report Template** window is displayed. The selected widgets will fetch the data from the application and are displayed in the content management window. You can also select **Add Row** or **Add Widgets** under **Add Content** to modify the widgets layout. The following is an example of creating dashboard content for events.



The following is an example of creating report content for events.

The screenshot displays the 'Create New Report Content' page. At the top, there are navigation tabs for 'Dashboard View', 'Templates', and 'Reports'. The main title is 'Create New Report Content'. Below the title, there are buttons for 'Add Content', 'Save', and a menu icon. The page is divided into three main sections, each with a table and a 'Save' button:


- Event:** A table with columns: Source Name, Description, Source Address, Category, Count, and Last Occurred(Serv...). A 'Save' button is located to the right of the table.
- Event Severity Summary:** A table with a single column for the summary. A 'Save' button is located to the right of the table.
- Violations:** A table with columns: Sev., Ru..., Cat..., Me..., Unit..., Ru..., Fab..., Pro..., Pro..., Obj..., Port..., and Last... A 'Save' button is located to the right of the table.

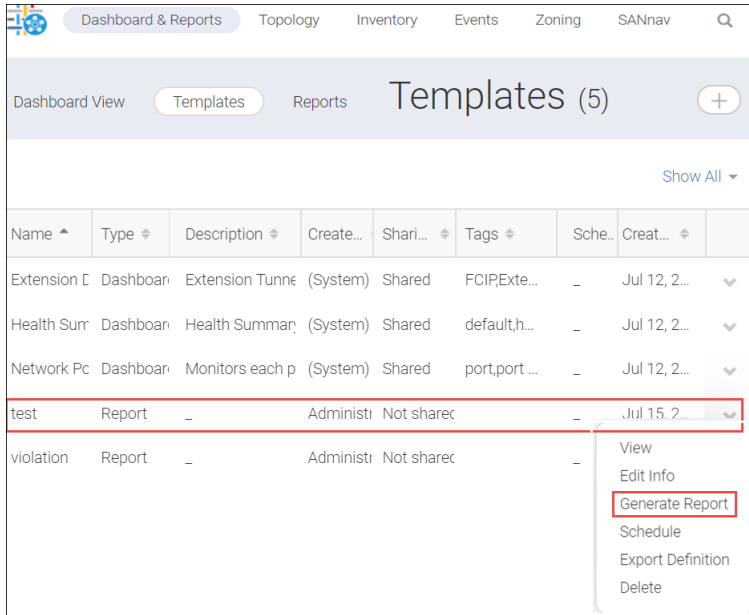
6. Click **Save** and type the name, tags, and description of the Event Management dashboard details.

8.1.16.1 Exporting Event Management Reports

You can save a copy of Event Management reports to your local machine.

To export Event Management reports, follow the instructions below:

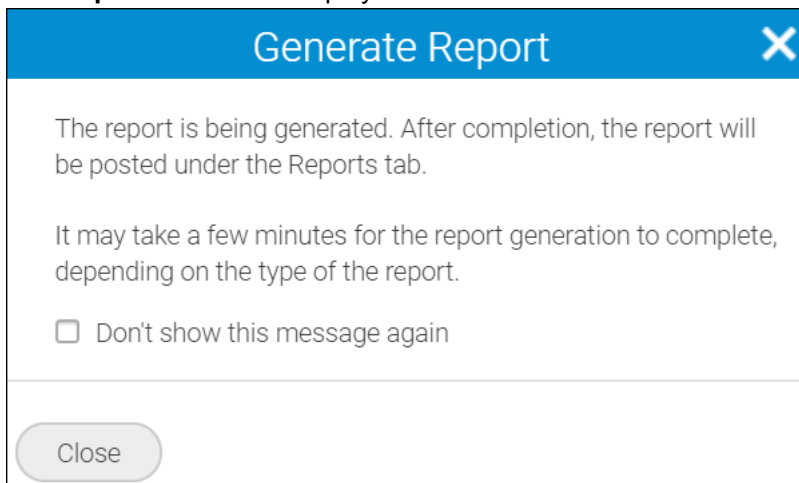
1. Click **Dashboard & Reports** in the navigation bar, and then select **Templates** to view the saved dashboard and report widgets.
2. Click () on a saved report and select **Generate Report**. SANnav collects the reports data and you can view the generated data in the **Reports** tab.



The **Generate Report** window is displayed.

3. Click **Close**. The report is generated under the **Reports** tab.
4. Click **Reports** tab.

The **Reports** window is displayed.



5. Click () on a generated data and select **Export** to download the reports data.

The downloaded reports ZIP file contains **.csv**, **.html**, and **.pdf** files.

Maximum of 50000 reports data is saved in **.csv** file.

Maximum of 5000 reports data is saved in **.pdf** and **html** file.

The screenshot shows the 'Reports (1)' page in the SANnav interface. The page has a navigation bar with 'Dashboard & Reports', 'Topology', 'Inventory', 'Events', 'Zoning', and 'SANnav'. Below the navigation bar, there are tabs for 'Dashboard View', 'Templates', and 'Reports'. The main content area displays a table with the following columns: Name, Description, Tags, Generated By, and Generated On. A single report entry is shown with the name 'test_2019-07-15-12-...', description '-', generated by 'Administrator', and generated on 'Jul 15, 2019 12:56:08 I...'. A context menu is open over the report entry, showing 'View', 'Export', and 'Delete' options. The 'Export' option is highlighted with a red box. Below the table, a file download notification shows 'test_2019-07-15-1....zip' with a red box around it.

Name	Description	Tags	Generated By	Generated On
test_2019-07-15-12-...	-		Administrator	Jul 15, 2019 12:56:08 I...

test_2019-07-15-1....zip

Extension Tunnels and Circuits

9.1 Overview of Extension Tunnels

Brocade extension products support both FC/FICON-based data flows and IP-based storage data flows. Brocade extension solutions maximize replication and backup throughput over distance, using data compression, disk and tape protocol acceleration, and WAN-optimized TCP. Brocade extension supports applications such as remote data replication (RDR), centralized backup, and data migration.

Brocade extension uses the existing IP wide area network (WAN) infrastructure to connect Fibre Channel and IP fabrics between distant endpoints, that are impractical or costly using native Fibre Channel or IP connections. The basis of the connection is the extension tunnel, which is built on a physical connection between two extension switches or blades. Extension tunnels allow Fibre Channel and IP traffic to pass through the IP WAN. The extension tunnel connections ensure lossless transmission and that FC and IP frames are delivered in the correct order. The Fibre Channel fabric and all targets and initiators, whether FC or IP, are unaware of the presence of the IP WAN.

The extension tunnel provides load balancing across separate network paths, optimization for extended links, rate limiting to ensure optimal performance, and lossless link loss (LLL) recovery.

Two major classifications exist based on the type of I/O.

- FCIP (Fibre Channel over IP)
- IP Extension

Using SANnav Management Portal, you can set up both FCIP tunnels and IP Extension tunnels.

FCIP Tunnels

FCIP tunnels are typically established across WANs. Management of the tunnels often involves monitoring the FCIP traffic across the WAN, and monitoring the associated FC traffic and each end of the tunnel—SANnav Management Portal provides ample tools for monitoring both types of traffic.

IP Extension Tunnels

The Brocade 7840 Switch, the Brocade 7810 Switch, and the Brocade SX6 Blade support IP Extension.

Extended IP traffic receives the same benefits as traditional FCIP traffic. IP Extension provides Layer 3 extension for IP storage replication.

The deployment models include:

- Direct connection (IP storage with the Brocade 7840 Switch or the Brocade SX6 Blade)
- LAN ports connected to a Layer 2 switch

SANnav Management Portal supports configuration of hybrid tunnels (FCIP + IP Extension).

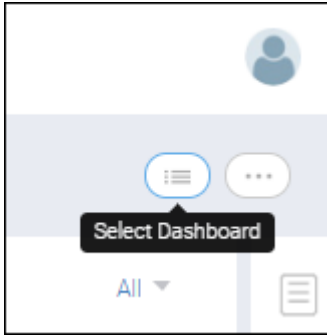
9.2 Applying the Extension Dashboard

SANnav dashboards provide you a customizable view of your SAN environment. SANnav provides four dashboards, one of which is devoted to Extension Tunnel Management.

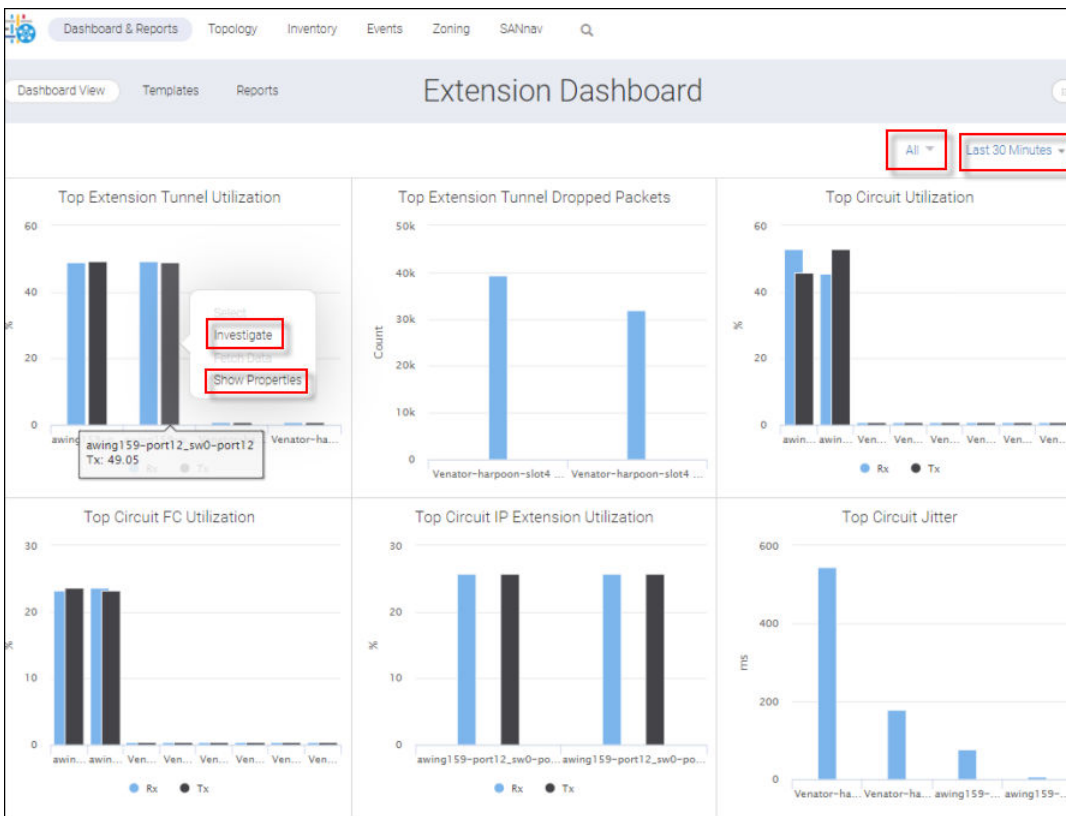
Upon login, you see the **Health Summary** dashboard. From here, do the following to launch and utilize the **Extension Dashboard**.

1. Click **Dashboard & Reports** in the navigation bar, and then click **Dashboard View** in the subnavigation bar.

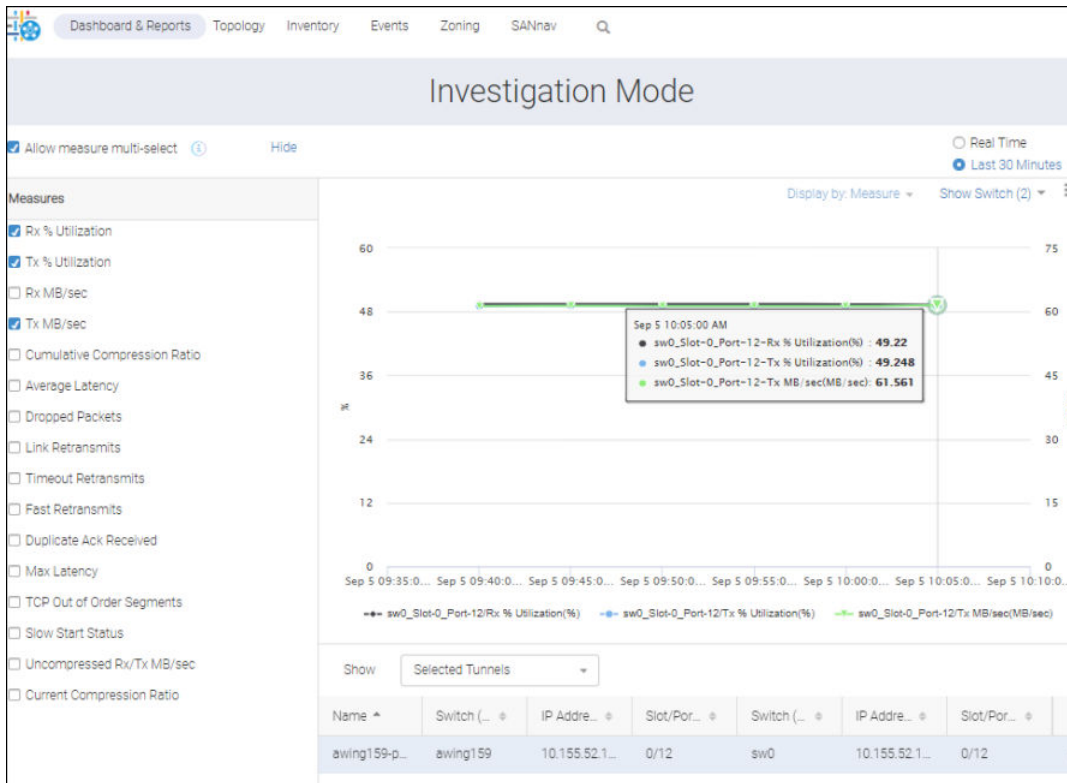
- Click the **Select Dashboard** button in the upper-right corner of the window, highlight the **Extension Dashboard**, and click **OK**.



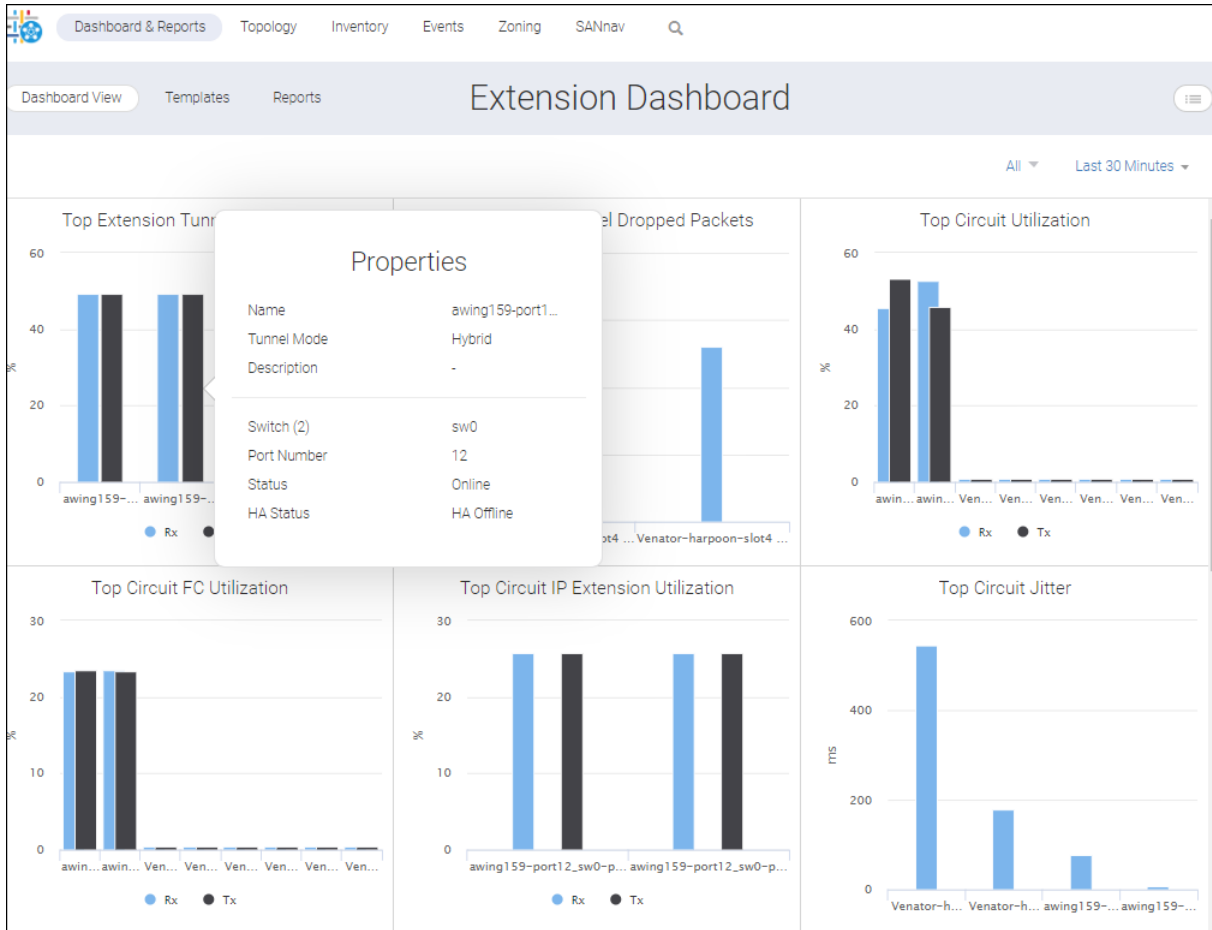
The **Extension Dashboard** displays.



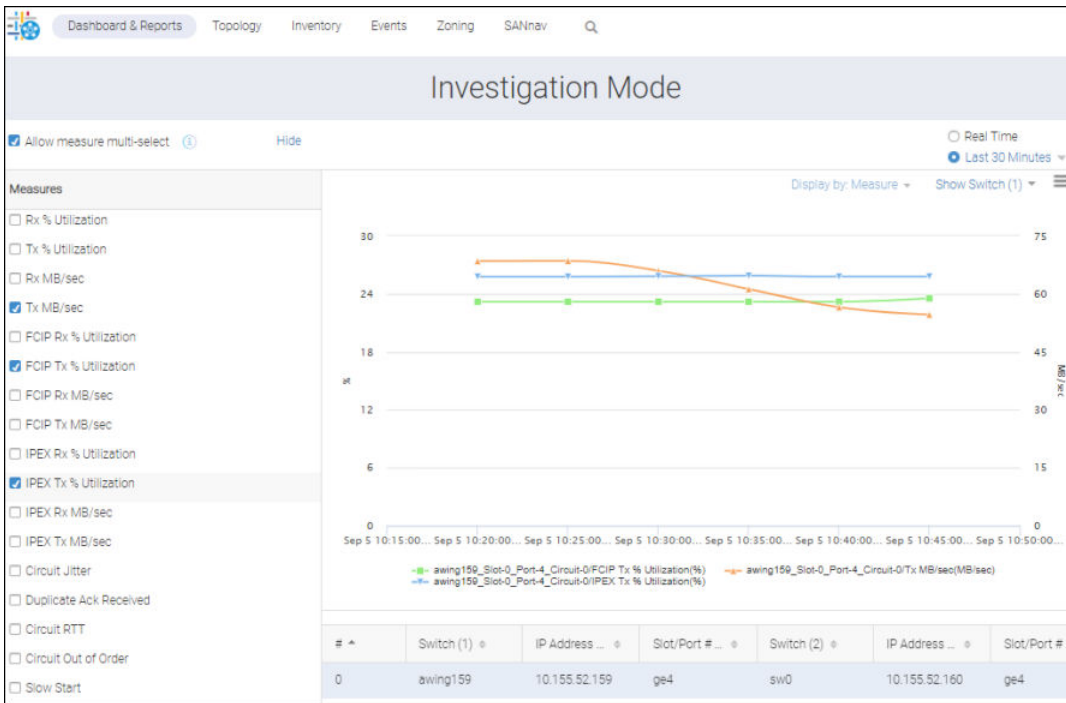
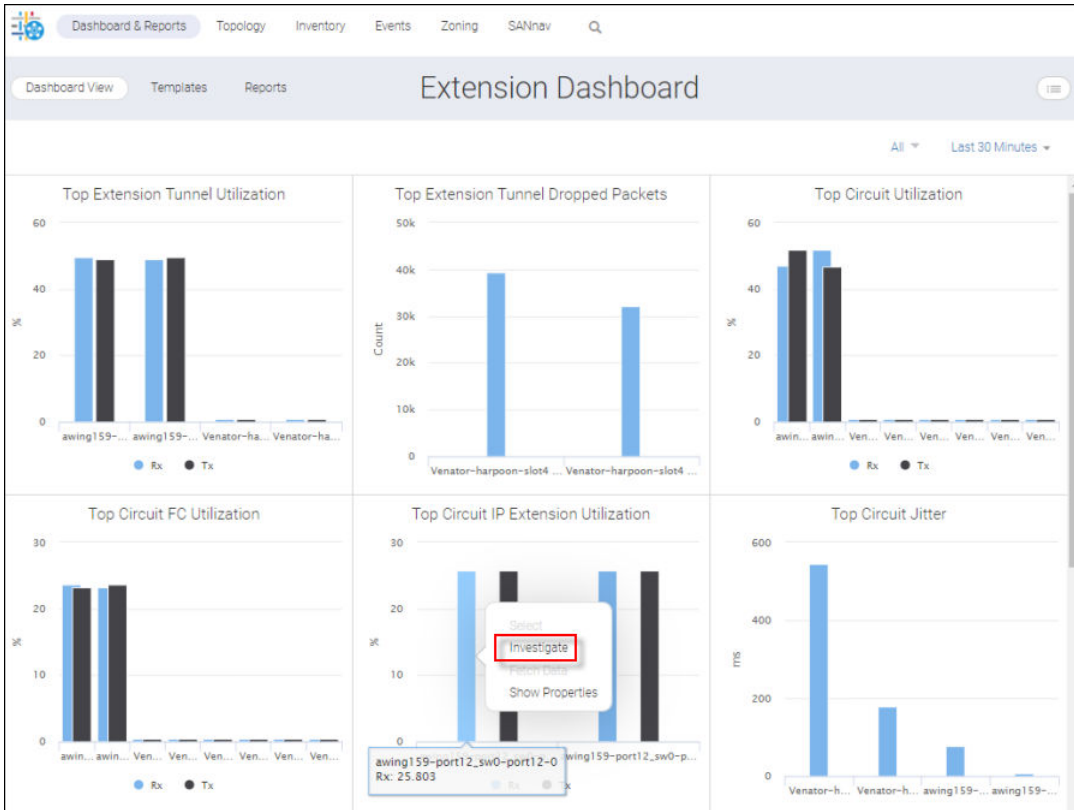
3. If you want to examine Top Extension Tunnel Utilization, click on a bar, and then select **Investigate** from the list. This way you see the trends over time.



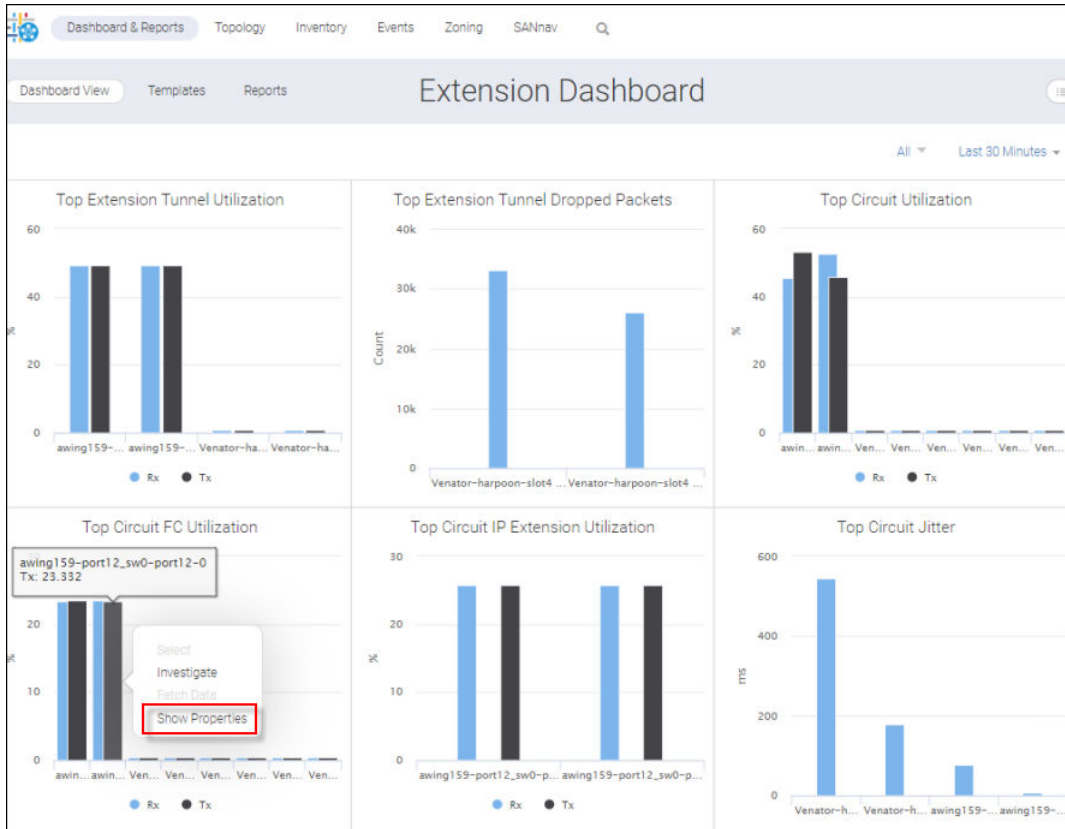
4. If you want to display properties of the tunnel, click on a bar, and then select **Show Properties** from the list. This displays details like tunnel mode and port number.



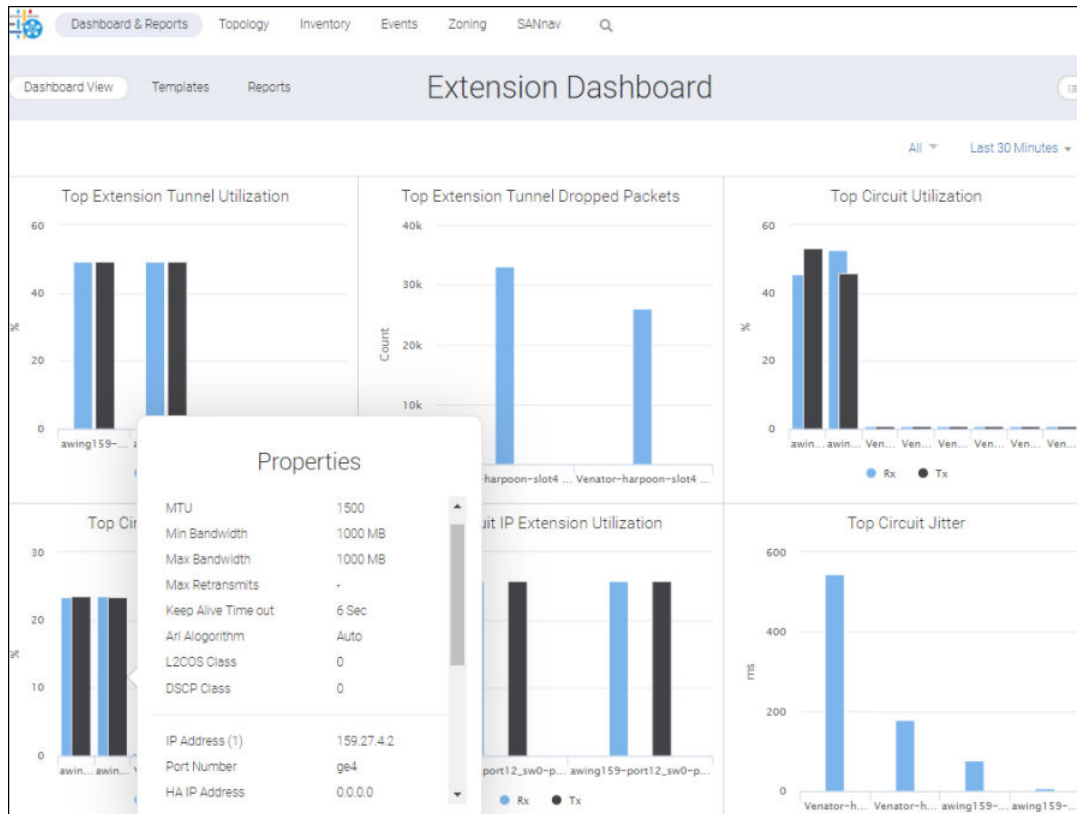
- If you want to examine Top Circuit IP Extension utilization, select a bar on the graph and click **Investigate** from the action list



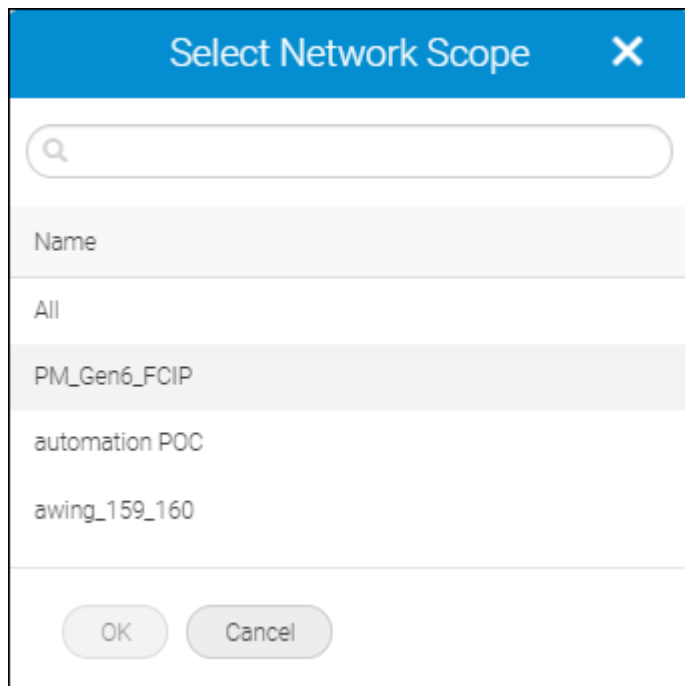
- If you want to display examine a particular switch with respect to Top Circuit FC Utilization, click on a bar, and select **Show Properties** from the list.



This displays Extension Circuits properties.

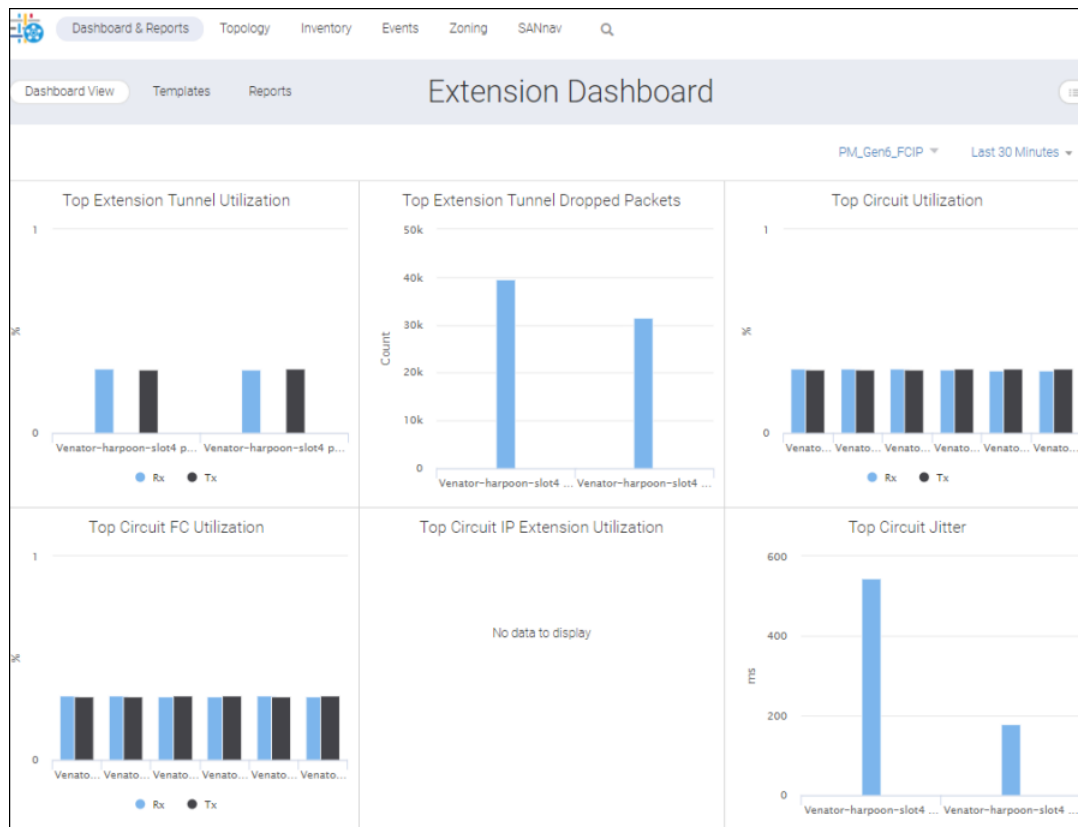


- To change the Network Scope, click **All** in the upper-left of the **Extension Dashboard** window. This displays the **Select Network Scope** dialog.



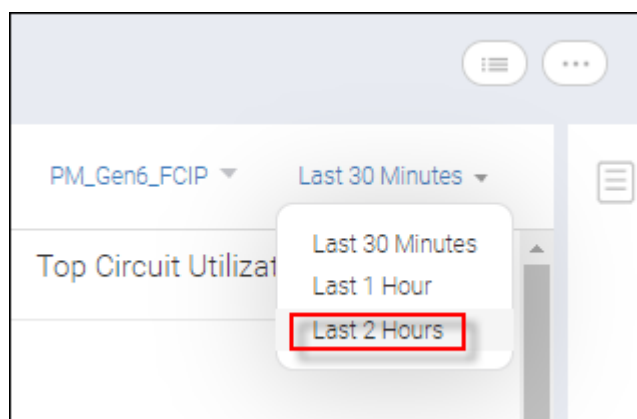
Upon selecting the **PM_Gen6_FCIP**, the **Extension Dashboard** appears under a new fabric and the extension widgets will display the tunnels and circuits that belong to the fabric.

Notice the fabric listed in the upper right of the window.



8. To change the time scope, click **Last 30 Minutes** on the upper right of the **Extension Dashboard**.

This displays a list of supported time scopes.



Upon clicking **Last 2 Hours** (boxed), the dashboard displays all the widgets with this new time scope.

9.3 Configuring IPsec Policies

When configuring tunnels to utilize IPsec, IPsec policies must be created before configuring the tunnel. Once created successfully, an IPsec policy can be selected for use by tunnels during the tunnel creation process.

If IPsec is not utilized by your extension tunnels, you can skip this section and go directly to setting up extension tunnels.

IPsec is enabled on the tunnel, not the circuit level. This means that all circuits in a tunnel use the same IPsec settings, although different tunnels can have different IPsec settings.

IPsec uses Internet Key Exchange (IKE) to set up the security association. The key exchange can be through a pre-shared key (PSK) or through public key infrastructure (PKI).

When you use a pre-shared key (PSK), both ends of the secure tunnel must be configured with the same key string. If not, the IKE session does not come up, and this prevents the extension tunnel from coming up.

SANnav Management Portal enables you to configure policies that utilize PSKs, with the following requirements:

- For the Brocade 7840 Switch, the Brocade 7810 Switch, or the Brocade SX6 Blade, the pre-shared key must be a 16-to-64 character string.
- For the Brocade FX8-24 Blade, the pre-shared key must be a 32-character string.

SANnav Management Portal also enables you to configure policies that utilize Public key infrastructure (PKI) on the Brocade 7840 Switch, the Brocade 7810 Switch, and the Brocade SX6 Blade.

To configure PKI policies on these products, you must utilize the CLI, as follows:

1. Using the switch CLI, create keyPair with the `secCertMgmt` command.
2. Create the IPsec policy applying the new keyPair.
3. Configure the tunnel using IPsec Policy functionality described below.

9.3.1 Creating an IPsec Policy

1. Click **SANnav** in the navigation bar, and then select **SANnav Configuration > Extension Tunnels Management**.
2. Click the **Policies** tab to display all IPsec policies created on all switches.

3. To create a new Preshared policy, click the **+** button on the top right of the policy list, and then enter a policy name and pre-shared key value. The dialog will appear as shown below.

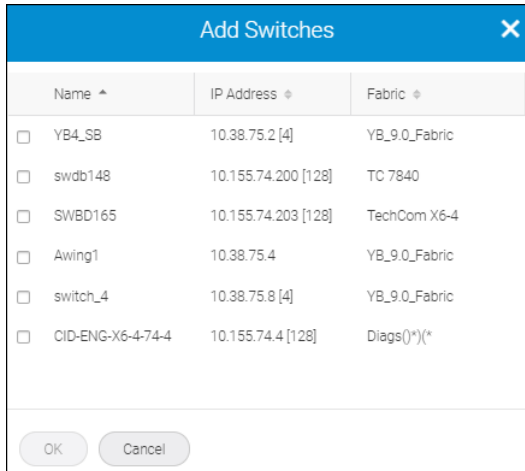
The screenshot shows the 'Create New IP Sec Policy' dialog. The 'Name' field is filled with 'CaliforniatoBurbankPOLICY1' and the 'Key Type' is set to 'Preshared'. Below the 'Switches' section, there is a table with columns for Name, IP Address, and Fabric. An 'Add' button is highlighted with a red box. At the bottom, there is a 'Key' input field and an 'Import' button.

To create a PKI policy, click the **+** button on the top right of the policy list, then enter a policy name, select **PKI** from the **Key Type** list, and then specify a pre-shared key value. Your dialog should like this.

The screenshot shows the 'Create New IP Sec Policy' dialog. The 'Name' field is filled with 'PublicKey248!' and the 'Key Type' is set to 'PKI'. Below the 'Switch' section, there is a table with columns for Name, IP Address, and Fabric. An 'Add' button is highlighted with a red box. At the bottom, there is a 'Key' input field and 'Save' and 'Cancel' buttons.

4. Click **Add** to add switches.

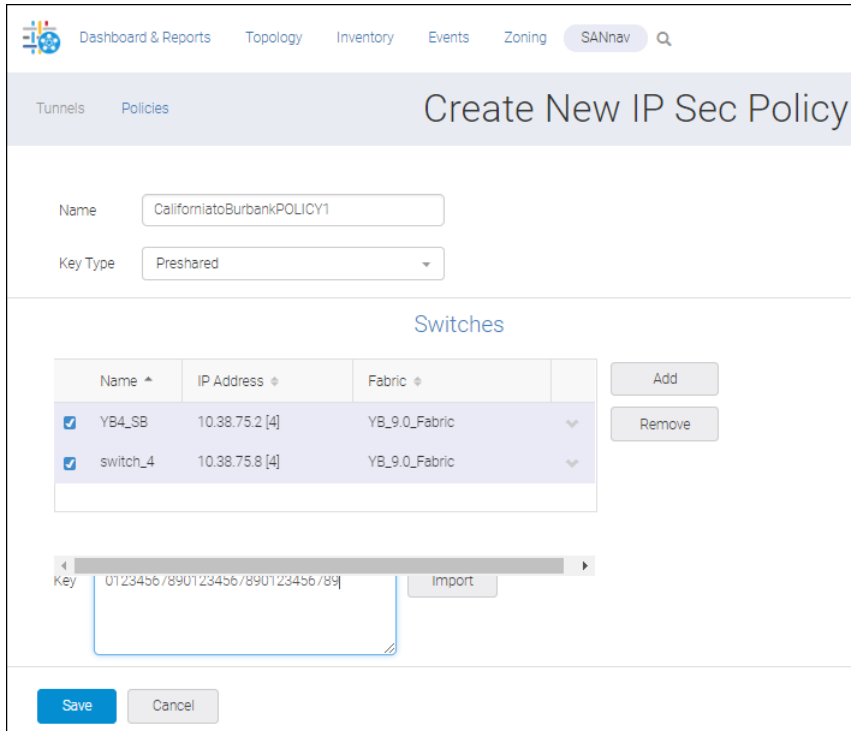
The **Add Switches** dialog appears.



The 'Add Switches' dialog box displays a table with columns for Name, IP Address, and Fabric. It contains six rows of switch information, each with a checkbox in the first column. At the bottom, there are 'OK' and 'Cancel' buttons.

Name	IP Address	Fabric
<input type="checkbox"/> YB4_SB	10.38.75.2 [4]	YB_9_0_Fabric
<input type="checkbox"/> swdb148	10.155.74.200 [128]	TC 7840
<input type="checkbox"/> SWBD165	10.155.74.203 [128]	TechCom X6-4
<input type="checkbox"/> Awing1	10.38.75.4	YB_9_0_Fabric
<input type="checkbox"/> switch_4	10.38.75.8 [4]	YB_9_0_Fabric
<input type="checkbox"/> CID-ENG-X6-4-74-4	10.155.74.4 [128]	Diags(*)(*

5. For a Preshared policy, select a switch for each end of the tunnel and then click **OK**. A dialog similar to the following displays.



The 'Create New IP Sec Policy' dialog box shows the configuration for a preshared policy. The 'Name' field is 'CaliforniatoBurbankPOLICY1' and the 'Key Type' is 'Preshared'. Under the 'Switches' section, two switches are selected: 'YB4_SB' and 'switch_4'. A 'Key' field contains the value '0123456/890123456/890123456/89' and an 'Import' button is visible. At the bottom, there are 'Save' and 'Cancel' buttons.

For a PKI policy, select one switch. Your dialog would look like the following.

Dashboard & Reports Topology Inventory Events Zoning SANnav

Tunnels Policies **Create New IP Sec Policy**

Name

Key Type

Switch

Name	IP Address	Fabric
YB4_SB	10.38.75.2 [4]	YB_9_0_Fabric

Change

Key

Save Cancel

On a **PKI** dialog, the **Add** button disappears after you have added a switch. Only **Change** appears. This is because you are limited to one switch if the key type is **PKI**.

- On the **Preshared** dialog, check both switches.

On the **PKI** dialog, the selection of the single switch is by default.

- On the **Preshared** dialog, either manually enter or import a pre-shared key.

On the **PKI** dialog, manually enter the PKI key pair name assigned when this policy was created through the CLI on the Brocade 7840 Switch or Brocade SX6 Blade

NOTE

Public key policies are created (in the application) only after the key file key pair has been generated through the CLI.

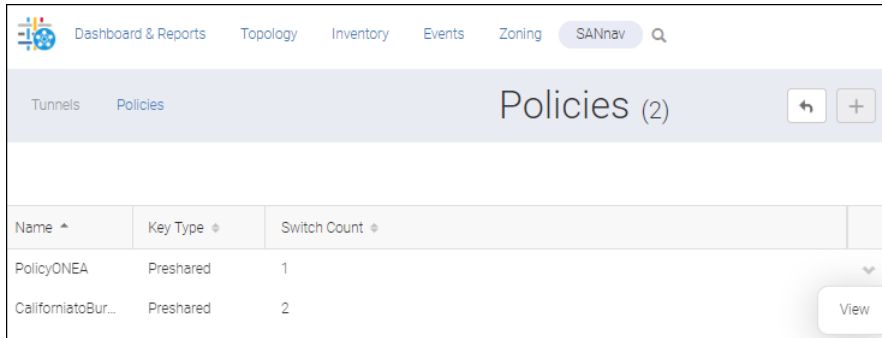
- Click **Save**. This action pushes the IPsec policy configuration to the switch on the **PKI** dialog and the switches on the **Preshared** dialog.

9.3.2 Editing an IPsec Policy

- Click **SANnav** on the navigation bar, and then select **SANnav Configuration > Extension Tunnels Management**.
- Click the **Policies** tab to display all IPsec policies created on all switches.

NOTE

No IPsec policies are displayed if the SANnav Management Portal has failed to discover at least one Brocade 7840 switch or Brocade SX6 blade.



The screenshot shows the SANnav interface with the 'Policies' page selected. The page title is 'Policies (2)'. Below the title is a table with the following data:

Name ^	Key Type ^	Switch Count ^
PolicyONEA	Preshared	1
CaliforniatoBur...	Preshared	2

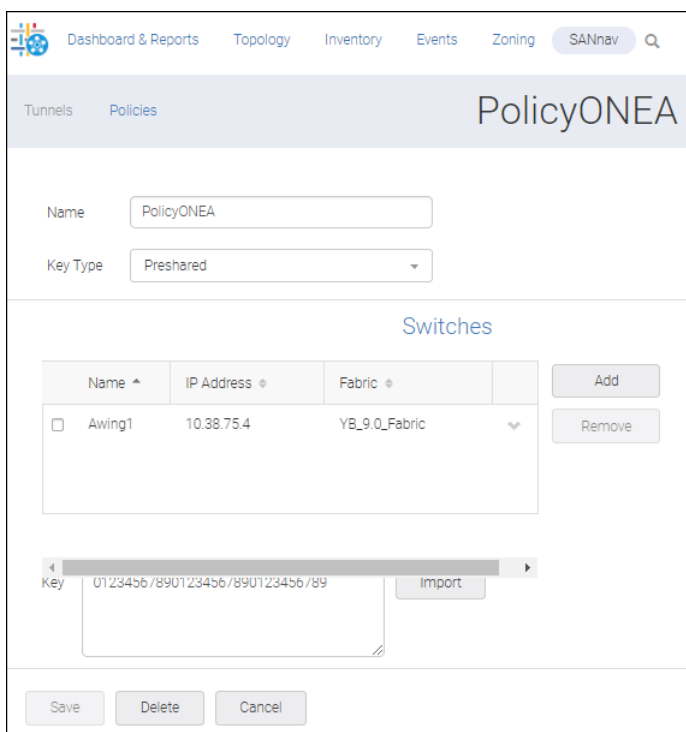
A 'View' button is located to the right of the table.

The **Key Type** indicates the type of policy that was created. **Preshared** indicates that the policy was created using a pre-shared key. **Public** indicates that the policy was created using the PKI.

Switch Count is the number of switches configured to use the indicated policy.

- To edit an IPsec policy, click the policy or click **View**.

You see the following dialog, which lists all the extension products currently configured to use the selected policy.



The screenshot shows the SANnav interface with the 'PolicyONEA' dialog open. The dialog has the following fields and sections:

- Name:** PolicyONEA
- Key Type:** Preshared
- Switches:** A table with columns for Name, IP Address, and Fabric. One switch is listed:

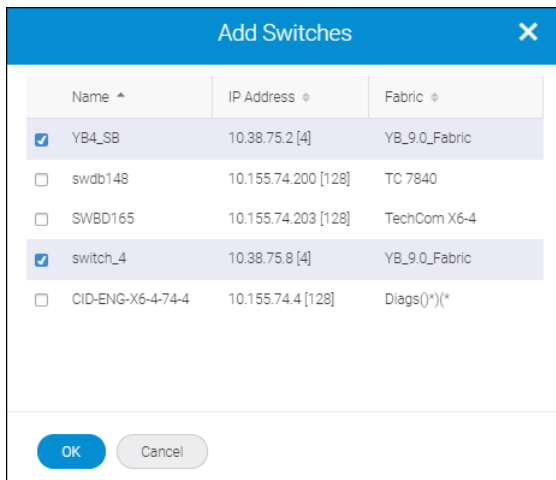
Name ^	IP Address ^	Fabric ^
<input type="checkbox"/> Awing1	10.38.75.4	YB_9_0_Fabric

 There are 'Add' and 'Remove' buttons next to the table.
- Key:** A text input field containing '0123456/890123456/890123456/89' and an 'Import' button.
- Buttons:** 'Save', 'Delete', and 'Cancel' buttons at the bottom.

From here you can change the key type and key, remove the associated switch, and add a switch.

- Click **Add**.

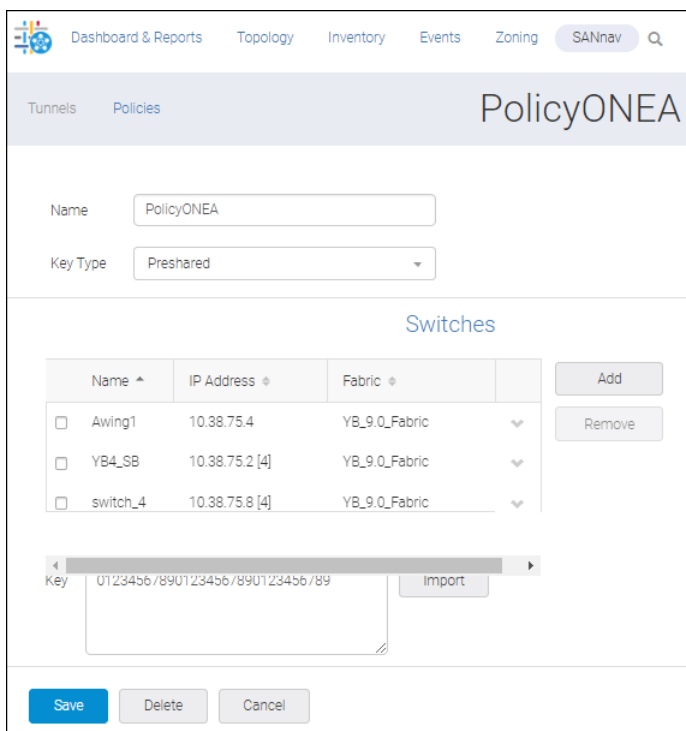
The **Add Switches** dialog appears.



- Select two switches (YB4_SB and switch_4) and then click **OK**. The selected switches are now visible in the Switches area (below). Each switch is now configured to use the selected policy.

NOTE

You can add the same policy on multiple switches.



- Click **Save** to push the configuration to the switches.

9.3.3 Deleting an IPsec Policy

- Select **SANnav** on the navigation bar, and then select **SANnav Configuration > Extension Tunnels Management**.
- Click the **Policies** tab to display all IPsec policies created on all switches.

3. Either click the policy or select **View** on the action list for the policy that you want to delete, and then click the **Delete** button.

The screenshot shows the SANnav management portal interface. At the top, there are navigation tabs: Dashboard & Reports, Topology, Inventory, Events, Zoning, and SANnav. Below these is a search bar. The main content area is titled 'CaliforniatoBurbankPOLICY1'. It contains a form with the following elements:

- Name:** CaliforniatoBurbankPOLICY1
- Key Type:** Preshared
- Switches:** A table with columns for Name, IP Address, and Fabric. It lists two switches: YB4_SB (IP: 10.38.75.2 [4], Fabric: YB_9.0_Fabric) and Awing1 (IP: 10.38.75.4, Fabric: YB_9.0_Fabric). There are 'Add' and 'Remove' buttons next to the table.
- Key:** A text field containing '0123456/890123456/890123456/89' and an 'Import' button.
- Buttons:** 'Save', 'Delete' (highlighted with a red box), and 'Cancel'.

4. Click **OK** in the confirmation message.

9.4 Configuring an Extension Tunnel

If both end switches [Switch (1) and Switch (2)] are reachable from the SANnav management server, you can create a two-sided extension tunnel provided that you have the Extension Tunnel Management privilege with read-write permission. If Switch (2) becomes unreachable after the tunnel becomes double-sided, the tunnel remains double-sided.

When creating a two-sided extension tunnel, you must select the local and remote extension products that are to be used at each end of the tunnel. After selecting an extension switch for one end, you must select a *supported* switch for the other end. The following table indicates which extension products can be used together to form tunnels. For example, if one end of the tunnel is a Brocade FX8-24 Blade, the other end must be another Brocade FX8-24 Blade.

Platform	Brocade 7840 Switch	Brocade SX6 Blade	Brocade FX8-24 Blade
FX8-24	No	No	Yes
7840	Yes	Yes	No
7810	Yes	Yes	No
SX6	Yes	Yes	No

NOTE

For the Brocade 7840 Switch, the WAN Rate Upgrade 2 license must be installed if you want to view and select the 40GbE ports.

The process of configuring tunnels consists of the following steps.

1. Click **SANnav** on the navigation bar, and then select **SANnav Configuration > Extension Tunnels Management**.

2. Click the **Tunnels** tab.

All tunnels that are configured between the discovered extension-tunnel-capable switches are displayed.

Name	Switch (1)	Switch (1) Model	Switch (2)	Switch (2) Model	Circuit Count	Status	Last Modified
sw62181-port12_sw62182...	sw62181	Brocade 7810	sw62182	Brocade 7810	2	Disabled	Aug 07, 2019 11:55:20 MDT
sw62184-port24_sw62183...	sw62184	Brocade 7840	sw62183	Brocade 7840	1	Offline	Aug 07, 2019 11:56:15 MDT
sw062193-port13_sw0621...	sw062193	Brocade 7810	sw062194	Brocade 7810	1	Online	Aug 06, 2019 15:19:35 MDT
sw062193-port15_sw0621...	sw062193	Brocade 7810	sw062119_f50_d1	Brocade X6-4	1	Online	Aug 06, 2019 15:21:18 MDT
sw062194-port12_sw0621...	sw062194	Brocade 7810	sw062196	Brocade 7840	1	Degraded	Aug 06, 2019 15:19:38 MDT
sw7800c150-port16_sw78...	sw7800c150	Brocade 7800	sw7800c149	Brocade 7800	4	Online	Aug 06, 2019 13:44:45 MDT
switch_50-slot7-port18_sw...	switch_50	Brocade X6-4	sw062119_f50_d1	Brocade X6-4	1	Online	Aug 06, 2019 15:21:18 MDT

The configuration status values are defined below.

Configuration Status	Description
Online	Both ends of the tunnel have a status of Online.
Offline (In Progress)	If either end of the tunnel is not Online, then the tunnel status is Offline.
Inactive	The tunnel configuration is not pushed to the switch.
Degraded	One switch is Degraded and the other is either Online or Degraded.
Disabled	If either end of the tunnel is Disabled, then the tunnel status is Disabled.

NOTE

If the list of tunnels is incomplete, the SANnav server has yet to discover all the switches.

The description from Switch (1) displays. If this description is unavailable for Switch (1), then data from Switch (2) is displayed. If the description is available on the server but on neither switch, the server's settings are displayed.

3. Click the + icon in the upper right corner of the **Extension Tunnels** dialog to create a new tunnel.

The screenshot shows the 'Create New Tunnel' dialog in the SANnav management portal. The dialog is titled 'Create New Tunnel' and has tabs for 'Tunnels' and 'Policies'. It contains input fields for 'Name', 'Description', and 'Tags'. Below these is a 'Switches' section with a table for selecting switches and 'Add' and 'Remove' buttons. The 'Ports' section has two columns for 'Switch (1)' and 'Switch (2)', each with 'Port Type' and 'Port ID' dropdown menus.

The screenshot shows the 'Circuits' section in the SANnav management portal. It shows a table with columns for '#', 'GigE Port (1)', 'IP Address (1)', 'Op. Status (1)', 'GigE Port (2)', 'IP Address (2)', and 'Op. Status (2)'. There are 'Add' and 'Remove' buttons. Below the table are checkboxes for 'Activate' and 'Enable', and 'Save' and 'Cancel' buttons.

Once a name has been specified, it can be changed only through tunnel management configuration.

If Switch (1) is FCR supported and both Switch (1) and Switch (2) belong to different FIDs, the default value for Switch (1) and VEX is listed before VE, whereas Switch (2) lists VE before VEX.

The port ID selects the virtual ports configured in the selected switch. If you change the port ID for one or both ports in the existing tunnel configuration, the complete tunnel configuration is recreated.

4. Enter a tunnel name, a description, and, optionally, tags. The description can be at most 512 characters, and valid characters include numbers, letters, and underscores.

5. Click the **Add** button to display the **Add Switches** dialog.

Name	Mgmt. IP Address	Fabric
YB4_SB	10.38.75.2 [4]	YB_9.0_Fabric
swdb148	10.155.74.200 [128]	TC 7840
SWBD165	10.155.74.203 [128]	TechCom X6-4
Awing1	10.38.75.4	YB_9.0_Fabric
switch_4	10.38.75.8 [4]	YB_9.0_Fabric
CID-ENG-X6-4-74-4	10.155.74.4 [128]	Diags()*(*)

6. Select two switches from the listing (switch_4 and YB4_SB), one for each end of the tunnel, and click **OK**. The list under **Switches** would look like this.

Name	Mgmt. IP Address	Fabric
<input type="checkbox"/> switch_4	10.38.75.8 [4]	YB_9.0_Fabric
<input type="checkbox"/> YB4_SB	10.38.75.2 [4]	YB_9.0_Fabric

NOTE

The **Add** button is disabled if two switches already reside in the list.

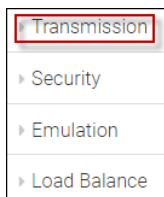
7. Scroll down to the **Ports** area in the second half of the **Create New Tunnel** dialog. The switches selected in the previous step appear here. Now, select the port type and ID for the ports used at each end of the tunnel.

Switch (1)	Switch (2)
switch_4	YB4_SB
Port Type: VE	Port Type: VE
Port ID: 4/18	Port ID: Select

NOTE

For the Brocade 7840 Switch and the Brocade SX6 Blade, only the VE port type is applicable.

8. Scroll down the page to configure additional tunnel properties.



- To assign transmission-related properties, click **Transmission**.

These properties (compression mode, QoS distribution, and IP Extension configurations) are specific to the switch and tunnel type.

This is a sample **Transmission** dialog for an FCIP tunnel on a Brocade 7840 Switch or Brocade SX6 Blade.

 A dialog box titled 'Transmission' with a dropdown arrow. It contains:

- FC Compression Mode: Fast Deflate (dropdown)
- Enable IP Extension Mode
- QoS High: 50 %
- QoS Medium: 30 %
- QoS Low: 20 %

By default, the configured tunnel is enabled to run FCIP mode. However, if you want to enable the configured tunnel in Hybrid mode, thereby running both FC and IP traffic, you must check **Enable IP Extension Mode**, as in the following sample Transmission dialog.

NOTE

To enable IP Extension mode, Hybrid mode must be enabled on the switch.

 A dialog box titled 'Transmission' with a dropdown arrow. It contains:

- FC Compression Mode: Fast Deflate (dropdown)
- Enable IP Extension Mode
- FC: 50 %
- IP: 50 %
- QoS High: 50 %
- QoS High: 50 %
- QoS Medium: 30 %
- QoS Medium: 30 %
- QoS Low: 20 %
- QoS Low: 20 %
- IP Compression Mode: Off (dropdown)

NOTE

IP Extension mode is not supported on the Brocade FX8-24 Blade.

Select the desired IP compression mode. The default is Off.

- To establish WWN-based authentication, click **Security**.

Here you assign a security policy to a tunnel that is already configured within the switch.

▼ Security

Remote WWN Switch (1)

Remote WWN Switch (2)

Enable IPsec

Enter WWNs in the **Remote WWN Switch (1)** and **Remote WWN Switch (2)** fields. This ensures that both switches have known World Wide Names.

Check **Enable IPsec**.

▼ Security

Remote WWN Switch (1)

Remote WWN Switch (2)

Enable IPsec

Policy for switch_4 Use for both switches

Policy for YB4_SB

Notice the policy name appended to the switch names.

If you intend to use the same IPsec policy for both switches, check **Use for both switches**.

For example, if you wanted to use the same IPsec (PSK) policy on both switches, you would do one of the following.

- As you configure a tunnel, set the IPsec policy:
 - a. Enable IPsec.
 - b. Select the configured IPsec policy from the configured switch.
 - c. Check **Use for both switches**.
 - d. Save the configuration.
- Configure a tunnel with an IPsec enabled PKI:
 - a. Configure an IPsec policy on a switch and its peer.
 - b. During tunnel configuration, enable IPsec.
 - c. Choose the configured IPsec policy name for both switches.
 - d. Save the configuration.
- Click **Emulation**.

If the switch is FICON-enabled, you would see the following dialog after selecting the FICON option.

Select Fast Write option to enable this capability.

Select the underlying FICON options to enable them. The Tape fields are already populated with default values, which you can override.

▼ Emulation

Fast Write

FICON

Enable XRC Emulation

Enable Tape Read Emulation

Enable Tape Write Emulation

Enable Teradata Read Pipelining

Enable Teradata Write Pipelining

Enable Tape Read Block ID

Enable Device level Ack Emulation

Tape Read Max Pipe: (1-100)

Tape Write Max Pipe: (1-100)

Tape Read Max Ops: (1-32)

Tape Write Max Ops: (1-32)

Tape Write Time: (100-1500 ms)

Tape Max Write Chain: (500-5000 KB)

Oxid Base: (0x0000-0xD000)

NOTE

Although values within the range 0x0000 to 0xF000 are valid for Oxid Base, to avoid conflicts you should choose a value outside the range used by FICON channels and devices.

If the switch is not FICON-enabled, you would see the following dialog.

If you select **Fast Write**, you can choose to enable **Tape Pipelining**.

▼ Emulation

Fast Write

Enable Tape Pipelining

- To load-balance your circuits in the event of failover or spillover, click **Load Balance**.

▼ Load Balance

Failover

Spillover

NOTE

The **Spillover** option is supported on only the Brocade 7840 Switch, the Brocade 7810 Switch, and that the Brocade SX6 Blade, provided the firmware on both switches is FOS version 8.0.1 or above.

9. To add circuits, scroll down the **Create New Tunnel** dialog, and then click **Add**.

The **Add Circuit** dialog appears.

Although you can choose either the IPv4 or IPv6 address type based on the interface requirements, your selection of address type must match for both switches.

Starting with SANnav 2.0.0, **VLAN ID Settings** is unchecked by default and the **VLAN ID** field is blank. If you check **VLAN ID Settings**, you can assign a value between 1 and 4094.

Starting with SANnav 2.0.0, the **Automatically choose MTU Size** checkbox is unchecked by default and the MTU value is set to 1500 for usability purposes. You can override this default setting within these parameters: 1280 thru 9216 (for 7840 and SX6) and 1260 through 1500 (for FX8-24).

If you check the box, the system will automatically choose the MTU size.

- If you are operating on a Brocade 7840 Switch or a Brocade SX6 Blade and you want to specify the HA (High Availability) setting for a circuit to enable HCL over the tunnel (that is, define the HA IP interface for both ends of the tunnel), check **Add HA Connectivity**.

NOTE

Removing HA is disruptive, but adding HA is not.

Observe the following considerations when setting the IP and remote IP addresses.

Switch1	Switch2	Local HA	Remote HA
Brocade 7840 Switch or SX6 Blade	Brocade 7840 Switch or SX6 Blade	Yes	Yes
Brocade 7810 Switch	Brocade 7810 Switch	HA not supported.	
Brocade 7840 Switch or SX6 Blade	Brocade 7810 Switch	Yes	No
Brocade 7810 Switch	Brocade 7840 Switch or SX6 Blade	No	Yes
Brocade 7840 Switch or SX6 Blade	—	Yes	Optional. Specify the HA IP address if required. If the remote IP address is null, then remote HA is not configured.
Brocade 7810 Switch	—	No	Yes. If you select HA, you must provide the remote IP address.

On the lower half of the **Add Circuit** dialog, you can set circuit values to maximize the effectiveness of the extension tunnels.

11. Click **Transmission**.

The Add Circuit dialog displays some default configuration values for Bandwidth and Keep Alive.

Add Circuit [X]

Transmission

Metric: 0

Failover Group ID: 0

Minimum Bandwidth: 20 (20-10000 MB)

Maximum Bandwidth: 20 (20-10000 MB)

Keep Alive Time Out: 6000 (500-7200000 ms)

Metric identifies the failover circuit. Typically, all circuits within a given tunnel utilize the same metric ID number. If you want some circuits to function solely as failover circuits, configure as metric 1.

If the circuit transmission fails, SANnav attempts to resend the transmission through the same metric ID. If that fails, SANnav retransmits through the next metric ID. For example, only after all circuits with metric ID number 0 fail will circuits with metric ID number 1 be used.

For **Keep Alive Time Out**, the default values are 6000 ms (for the Brocade 7840 Switch and the Brocade SX6 Blade) and 10000 ms (for the Brocade FX8-24 Blade).

L2Cos F-Class: 0

L2Cos Low: 0

L2Cos Medium: 0

L2Cos High: 0

ARL Algorithm: Auto

Enable

DSCP F-Class: (0-63)

DSCP Low: (0-63)

DSCP Medium: (0-63)

DSCP high: (0-63)

Save Cancel

In the bottom section under **Transmission**, you can configure the Circuit QoS settings to match those defined in your network.

12. At the bottom of the **Create New Tunnel** page, you determine the activation and status of the tunnel.

Hovering over each **i** (information) icon displays details for that option.

Remove Activate *i* Enable *i*

Indicates the tunnel status on switches.
If unchecked, the tunnel will be disabled and cannot be used for data transfer.

Save Cancel

The following scenarios describe the interaction between the checkboxes and the **Save** button.

- If you uncheck **Enable**, check **Activate**, and click **Save**, the tunnel is deployed to the switch but is in a disabled state.
- If you uncheck **Enable**, uncheck **Activate**, and click **Save**, the tunnel is saved to the SANnav database but is not deployed to the switch.
- If you check **Enable** (**Activate** is thereby checked automatically) and click **Save**, the tunnel is deployed to the switch in an online state.

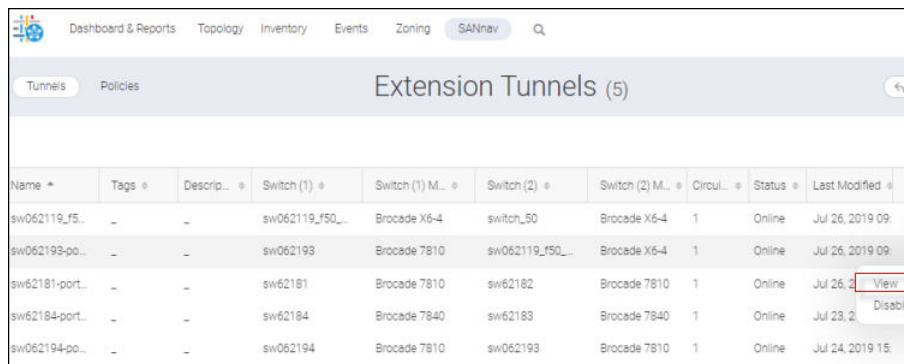
NOTE

This is your most likely choice.

9.5 Editing an Extension Tunnel

Perform the following steps.

1. Select **SANnav** from the navigation bar, and then select **SANnav Configuration > Extension Tunnels Management**.
2. For the desired tunnel, select **View** from the action list.



Name	Tags	Descrip.	Switch (1)	Switch (1) M.	Switch (2)	Switch (2) M.	Circul.	Status	Last Modified	
sw062119_f5...	-	-	sw062119_f50...	Brocade X6-4	switch_50	Brocade X6-4	1	Online	Jul 26, 2019 09:...	
sw062193-po...	-	-	sw062193	Brocade 7810	sw062119_f50...	Brocade X6-4	1	Online	Jul 26, 2019 09:...	
sw62181-port...	-	-	sw62181	Brocade 7810	sw62182	Brocade 7810	1	Online	Jul 26, 2019 09:...	View
sw62184-port...	-	-	sw62184	Brocade 7840	sw62183	Brocade 7840	1	Online	Jul 23, 2019 15:...	Disable
sw062194-po...	-	-	sw062194	Brocade 7810	sw062193	Brocade 7810	1	Online	Jul 24, 2019 15:...	

A detail page for that tunnel displays. This is the top half.

Dashboard & Reports Topology Inventory Events Zoning SANnav

Tunnels Policies sw062193-port15_sw062...

Name: sw062193-port15_sw062119_f50_d1-slot4 pr Description: Description field Description field

Tags: Tags field

Switches

<input type="checkbox"/>	Name	Mgmt. IP Address	Fabric	
<input type="checkbox"/>	sw062193	10.38.62.193	EMC_FID50_193	▼
<input type="checkbox"/>	sw062119_f50...	10.38.62.119 [50]	EMC_FID50_193	▼

Add Remove

Ports

Switch (1) sw062193 Port Type VE Port ID 15

Switch (2) sw062119_f50_d1 Port Type VE Port ID 4/20

This is the bottom half.

Transmission

Security

Emulation

Load Balance

1 Item

Circuits

<input checked="" type="checkbox"/>	#	GigE Port (1)	IP Address (1)	Op. Status (1)	GigE Port (2)	IP Address (2)	Op. Status (2)	
<input checked="" type="checkbox"/>	0	ge3	1111:1db8:111...	Online	4/ge17	1111:1db8:111...	Online	▼

Add Remove

Configure Disable Remove

Activate Enable Save Delete Cancel

3. Scroll down to the **Circuits** list on the bottom half of the window.

NOTE

To be operational, at least one circuit must be configured to the extension tunnel.

The circuit number in the left-most column represents the number pushed to the switch. It is automated by SANnav during circuit configuration. Values range from 0 to a maximum that is platform and fabric dependent (see the table below).

Fabric OS Version	FX8-24	7840	7810	SX6
v7.4 to 8.1 (VE)	10	8	N/A	8
v8.1 or above (VE)	10	10	6 (v8.2.1 and later)	10
v7.4 or above (VEX)	10	Not supported	Not supported	Not supported

Provided that the maximum count has not been reached, the lowest unused circuit number is used.

If **Op. Status** is listed as "-", the circuit operational status from that switch is inactive.

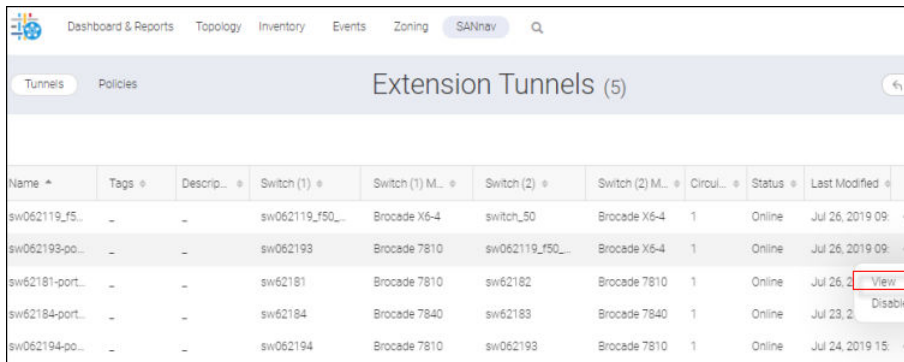
- If you click **Remove** from the action list, you can delete a circuit from the list.
- If you click **Configure** from the action list, the **Edit Circuit** dialog displays.

By default, the **Automatically choose MTU Size** option is unchecked, enabling you to replace the MTU value in the MTU Size field. Check **Automatically choose MTU size** to allow the system to assign the MTU size.

Modify the tunnel and click **Save**.

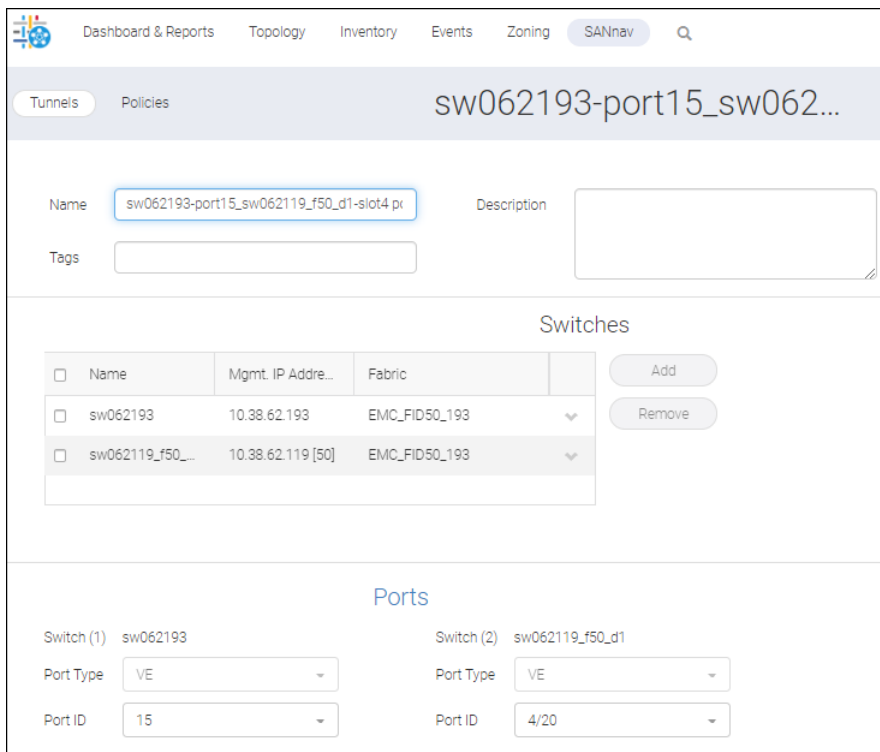
9.6 Deleting a Tunnel

1. Select **SANnav** on the navigation bar, and then select **SANnav Configuration > Extension Tunnels Management**.



Name	Tags	Descrip...	Switch (1)	Switch (1) M...	Switch (2)	Switch (2) M...	Circul...	Status	Last Modified
sw062119_f5...	-	-	sw062119_f50...	Brocade X6-4	switch_50	Brocade X6-4	1	Online	Jul 26, 2019 09:...
sw062193-po...	-	-	sw062193	Brocade 7810	sw062119_f50...	Brocade X6-4	1	Online	Jul 26, 2019 09:...
sw62181-port...	-	-	sw62181	Brocade 7810	sw62182	Brocade 7810	1	Online	Jul 26, 2019 09:...
sw62184-port...	-	-	sw62184	Brocade 7840	sw62183	Brocade 7840	1	Online	Jul 23, 2019 09:...
sw062194-po...	-	-	sw062194	Brocade 7810	sw062193	Brocade 7810	1	Online	Jul 24, 2019 15:...

2. Click on the tunnel you want to delete.



sw062193-port15_sw062...

Name: sw062193-port15_sw062119_f50_d1-slot4 pr

Description: [Empty]

Tags: [Empty]

Switches

<input type="checkbox"/>	Name	Mgmt. IP Adresse...	Fabric
<input type="checkbox"/>	sw062193	10.38.62.193	EMC_FID50_193
<input type="checkbox"/>	sw062119_f50...	10.38.62.119 [50]	EMC_FID50_193

Buttons: Add, Remove

Ports

Switch (1): sw062193 Switch (2): sw062119_f50_d1

Port Type: VE Port Type: VE

Port ID: 15 Port ID: 4/20

3. Click **Delete** at the bottom of the window.

This removes the tunnels and all associated circuits, which disrupts traffic transiting the tunnel and might cause fabric reconfiguration.

For switches running Fabric OS prior to v8.2.0, IP interfaces configured using IPv6 are deleted. and IP routes are not deleted.

Switch Maintenance and Support

10.1 Firmware Management

Firmware management allows you to download firmware to one or more switches in two ways: by importing the firmware images into the SANnav repository and then downloading them to the switch or by downloading them directly from an external FTP or SCP or SFTP server.

Firmware management is provided for switches running Fabric OS v7.4 or later.

In a storage area network (SAN), Fabric OS is the firmware for the Fibre Channel switches. The firmware is made available periodically to enhance the feature set or to address bug fixes. The list of discovered switches is displayed in the **FOS Version Management** window. You can select the discovered switches to upgrade or downgrade the firmware of one or multiple switches from the repository or from the external storage.

You can update to only one firmware version at a time. The firmware update is done either serially or in parallel when you select multiple switches.

When you select multiple switches for firmware update, a parallel firmware download is triggered based on the following scenarios:

- A chassis without a Brocade SX6 Extension Blade.
- A chassis with a Brocade SX6 Extension Blade running with Fabric OS version 8.2.0 or later.
- Fixed-port switches that are not connected in the same fabric, including logical fabrics.
- Brocade 7840 to Brocade 7840 without an HA online tunnel.

When you select multiple switches for firmware update, a serial firmware download is triggered based on the following scenarios:

- Switch port switches that are connected in the same fabric through an inter-switch link (ISL) or between two fabrics through an inter-fabric link (IFL), including the logical fabrics.
- Brocade 7840 to Brocade 7840 with an HA online tunnel.
- A chassis with a Brocade SX6 Extension Blade that has an HA online tunnel running with Fabric OS version 8.2.0 or later.

To update the firmware from an internal location, you must first import the firmware to the SANnav repository.

Refer to the latest Fabric OS Target Path document for the firmware paths.

10.1.1 Importing Firmware Files to the Repository

You must import the firmware files into the SANnav repository to upgrade or downgrade the switch firmware from internal storage.

The firmware package contains the following three files:

- `.gz` or `.tar` (mandatory) - The firmware file.
- `.md5` (optional) - This is a checksum file that validates the firmware file before importing the file into the SANnav server repository. The check is triggered automatically while importing, and an error message displays when the `.gz` file is not valid.
- `.pdf` (optional) - Release note of the firmware.

To import firmware to the repository, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > FOS Version Management**.

2. Select the **Repository** tab.
3. Click **Import**, and then click **+ Select files to import** to select the firmware file from your local machine.

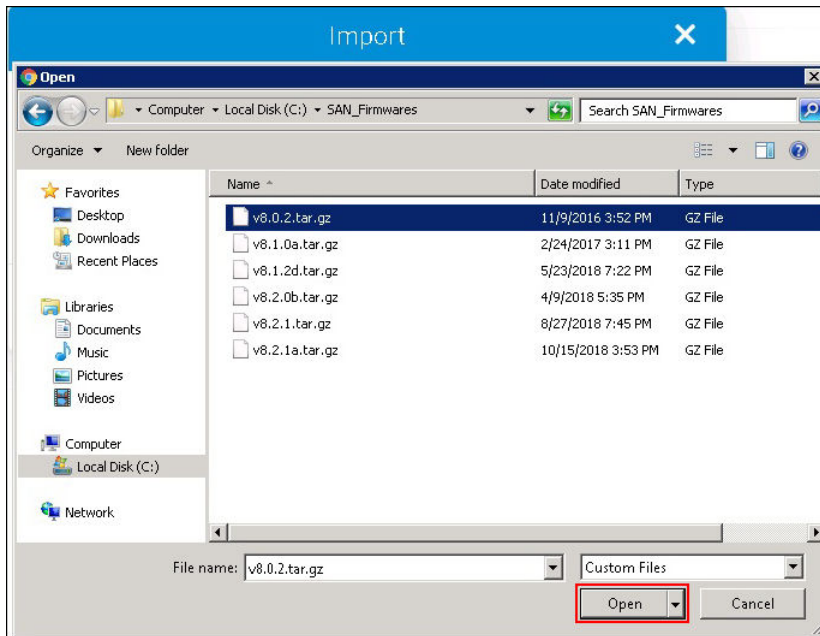
NOTE

SANnav does not support firmware versions earlier than 7.4.0.

4. Browse through the folder to select the firmware file, and click **Open** to import the selected files to the SANnav repository.

NOTE

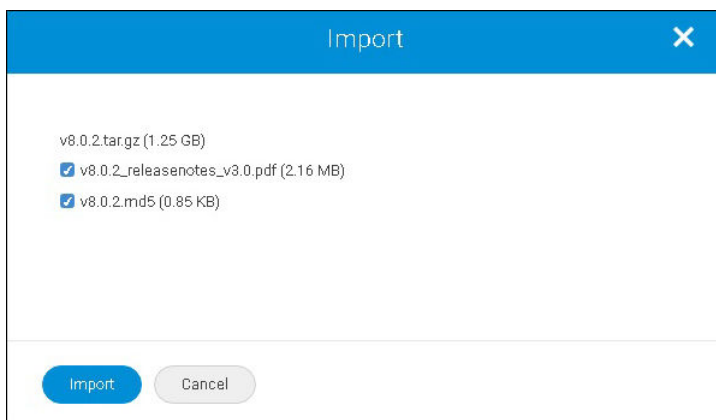
The `.tar.gz` file is a mandatory file to import.



5. Click **+ Add more files** to add the other files (`.md5` or `.pdf`).

NOTE

When `.tar.gz`, `.pdf`, and `.md5` files are selected, the **+ Add more files** option will not be present.




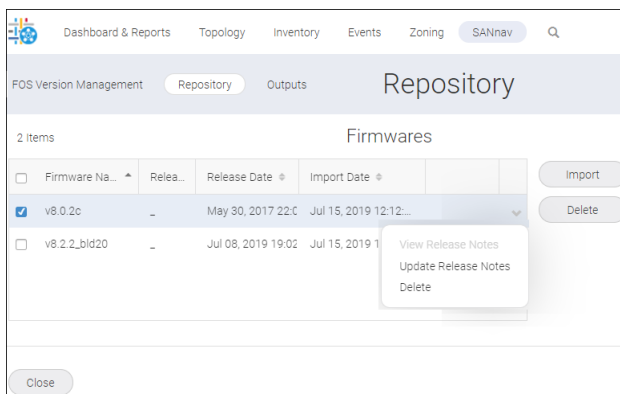
6. Click **Import**. The files are saved in the default SANnav repository (`<install_home>/data/filetransfer/Firmware/Switches`).

10.1.2 Managing the Repository

The **Repository** tab shows the imported files to update the firmware using an internal location.

To manage the firmware, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > FOS Version Management**.
2. Select the **Repository** tab to view the imported files.
3. Click the () down arrow on a firmware file to select any of the following:
 - **View Release Notes** to view the release notes PDF of the firmware. If the release note PDF file is not imported, the **View Release Notes** option is disabled.
 - **Update Release Notes** to add or replace the release notes PDF to the selected firmware.
 - **Delete** to delete the firmware from the SANnav repository.



4. Click **Close** to close the **FOS Version Management** interface.

10.1.3 Updating a Selected Switch from an Internal or External Location

You can update the firmware version of a particular switch from an internal or external location.

For example, if you want to update the Brocade 7840 Switch from firmware version 8.0.x to 8.2.x, perform the following steps:

NOTE

It is recommended to take a backup of 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.

NOTE

To update the switch using internal storage, you must save the firmware files to the SANnav repository (see [Importing Firmware Files to the Repository](#)).

NOTE

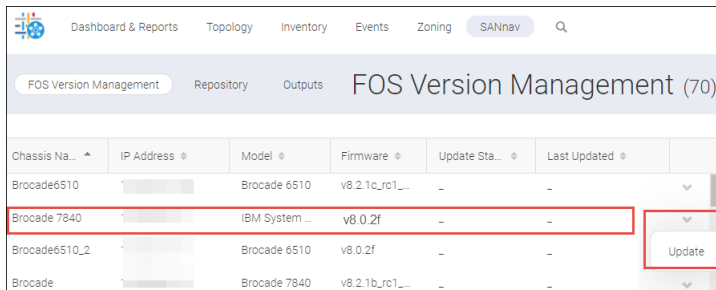
You must have read and write privilege to access FOS Version Management. An administrator has access to FOS Version Management and can grant you access. Refer to the user preference section to establish the Area of Responsibility (AOR) and roles.

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > FOS Version Management**.

- Click the () down-arrow on a particular switch, and then click **Update**.

NOTE

In case of an upgrade from 7.4.x to 8.2.x, you must first update the firmware version from 7.4.x to 8.0, and then SANnav allows you to update to firmware version 8.2.x. An error message displays if you skip the switch firmware path.



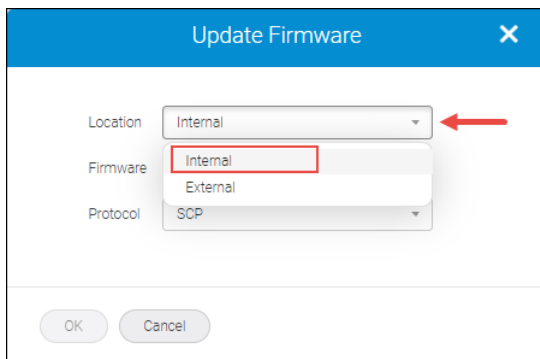
Chassis Na...	IP Address	Model	Firmware	Update Sta...	Last Updated
Brocade6510		Brocade 6510	v8.2.1c_rc1_...	-	-
Brocade 7840		IBM System ...	v8.0.2f	-	-
Brocade6510_2		Brocade 6510	v8.0.2f	-	-
Brocade		Brocade 7840	v8.2.1b_rc1_...	-	-

- Select **Internal** or **External** from the **Location** drop-down to update the selected switch. SANnav supports port 22 or custom port number (other than port 22) to transfer files using SCP and SFTP protocols.

- If you select **Internal** as the location, you must specify the firmware that is imported in the SANnav repository and the protocol (SCP or SFTP).

NOTE

During a firmware update with internal SCP or SFTP server, if the FOS version is 8.2.2 or higher, SANnav sends the internal port details to the switch. If the FOS version is less than 8.2.2 and if you select the custom port (other than port 22) for internal SSH server, you cannot use the internal server for the firmware update.



- If you select **External** as the location, enter the path (.gz or .tar file) where the firmware file is extracted, select the protocol (SCP, SFTP, or FTP), enter the host name or IP address, and enter the login credentials for the external server. You can also click the **Save login information** check box to save your login information for future use. To populate the previously saved login information, select the **Save login information** check box. The user credentials are saved only after the firmware update succeeds.

NOTE

- For a firmware update with external SCP or SFTP server, the port number can be customized only when the FOS version is 8.2.2 or higher.
- SANnav does not support customizing the port for an FTP protocol.

- Click **OK** to begin updating the firmware to the switch.
Click **OK** in the confirmation dialog.

- Select the **Outputs** tab, and then select **View** from the down-arrow for the switch whose firmware update status you want to view. If there are any errors in the update, you will be notified in the **Outputs** tab.

System Behavior

The firmware update begins and the update status changes to In Progress in the **FOS Version Management** window.

To view the final success or error report, select the **Outputs** tab.

Failure Cases

- If you downgrade a switch without following the suggested firmware path, a warning message displays: `Cannot download the requested firmware because the firmware doesn't support this platform. Please enter another firmware path..`
- Downgrading a seed switch impacts the fabric; in this case, a warning message displays: `Downgrading the firmware on the seed switch will have impact on the fabric..`
- If you attempt to upgrade a switch while skipping the supported firmware path, a warning message displays: `Non disruptive firmware download is not supported when firmware download with two versions apart. Please try again from cli with single mode option enabled..`

10.1.4 Updating the Firmware for One or More Switches from an Internal or External Location

You can update the firmware to enhance the feature set and to address bug fixes. You can update the firmware version of a switch from an internal or external location.

For example, if you want to update the firmware of multiple switches from firmware version 8.2.1 to 8.2.2, perform the following steps:

NOTE

Take a backup of 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.

NOTE

To update a switch using internal storage, you must first save the firmware files to the SANnav repository (see [Importing Firmware Files to the Repository](#)).


NOTE

You cannot upgrade or downgrade the firmware for a switch that is running a version earlier than Fabric OS version 7.4.0.

NOTE

You must have read and write privilege to access the FOS Version Management. An administrator has access to FOS Version Management and can grant you the necessary permissions. Refer to the user preference section to set up your Area of Responsibility (AOR) and roles.

To update the firmware for multiple switches, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > FOS Version Management**.
2. Click the more icon  on the top-right corner of the window, and then select **Bulk Select**.
3. Select one or more switches to update the firmware.

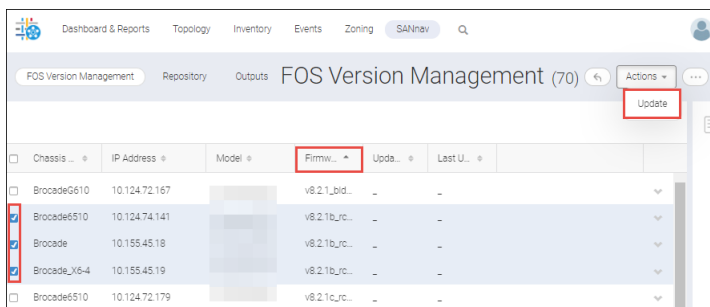
NOTE

If more than one switch is selected, a common firmware version is sought. If it does not exist, the **Firmware** drop-down is empty.

For this example, click the **Firmware** column to sort on the firmware version, and then select all the switches that are running a firmware version earlier than Fabric OS 8.2.2.

NOTE

Ensure that you do not skip the supported firmware path for the selected switch.



Chassis	IP Address	Model	Firmware	Update	Last U.
<input type="checkbox"/>	BrocadeG610	10.124.72.167	v8.2.1_bld...	-	-
<input checked="" type="checkbox"/>	Brocade6510	10.124.74.141	v8.2.1b_rc...	-	-
<input checked="" type="checkbox"/>	Brocade	10.155.45.18	v8.2.1b_rc...	-	-
<input checked="" type="checkbox"/>	Brocade_X6-4	10.155.45.19	v8.2.1b_rc...	-	-
<input type="checkbox"/>	Brocade6510	10.124.72.179	v8.2.1c_rc...	-	-

4. Select **Actions** on the upper-right subnavigation bar, and then click **Update**.
5. Select **Internal** or **External** from the **Location** drop-down to update the selected switches. SANnav supports port 22 or custom port number (other than port 22) for SCP and SFTP protocols for file transfer operation.
 - If you select **Internal** as the location, select the firmware that is imported in the SANnav repository and protocol (SCP or SFTP).

NOTE


During a firmware update with internal SCP or SFTP server, if the FOS version is 8.2.2 or higher, SANnav sends the internal port details to the switch. If the FOS version is less than 8.2.2 and if you select the custom port (other than port 22) for internal SSH server, you cannot use the internal server for the firmware update.

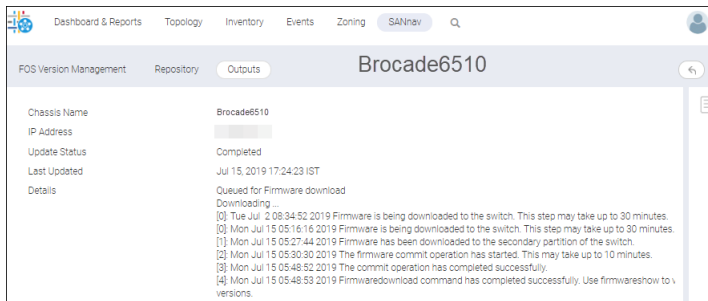
- If you select **External** as the location, enter the path (`.gz` or `.tar` file) where the firmware file is extracted, select the protocol (SCP, SFTP, or FTP), enter the host name or IP address, and enter the login credentials for the external server. You can also click the **Save login information** check box to save your login information for future use. To populate the previously saved login information, select the **Save login information** check box. The user credentials are saved only after the firmware update succeeds.

NOTE

- For a firmware update with external SCP or SFTP server, the port number can be customized only when the FOS version is 8.2.2 or higher.
- SANnav does not support customizing the port for an FTP protocol.

6. Click **OK** to begin updating the firmware to the switches.
Click **OK** in the confirmation dialog.

7. Click the () down arrow and select **View** on any switch in the **Outputs** tab to view the firmware update status. The **Outputs** tab displays both success and failure reports.



System Behavior

When you select multiple switches for a firmware update, parallel firmware download is triggered based on the following scenarios:

- A chassis without a Brocade SX6 Extension Blade.
- A chassis with Brocade SX6 Extension Blade running with Fabric OS version 8.2.0 or later.
- Fixed-port switches that are not connected in the same fabric, including the logical fabrics.
- Brocade 7840 to Brocade 7840 without an HA online tunnel

When you select multiple switches for firmware update, serial firmware download is triggered based on the following scenarios:

- All fixed-port switches that belong to the same fabric or that are connected through an inter-fabric link (IFL).
- Brocade 7840 to Brocade 7840 with an HA online tunnel.
- A chassis with a Brocade SX6 Extension Blade having an HA online tunnel running with Fabric OS version 8.2.0 or later.

Failure Cases

- If you downgrade a switch without following the suggested firmware path, a warning message displays: `Cannot download the requested firmware because the firmware doesn't support this platform. Please enter another firmware path..`
- Downgrading a seed switch impacts the fabric; in this case, a warning message displays: `Downgrading the firmware on the seed switch will have impact on the fabric..`
- If you attempt to upgrade a switch while skipping the supported firmware path, a warning message displays: `Non disruptive firmware download is not supported when firmware download with two versions apart. Please try again from cli with single mode option enabled..`

10.2 Switch SupportSave

Switch SupportSave allows you to collect switch data, such as RASLOG and trace dumps, from one or multiple switches across a fabric to support troubleshooting activities.

You can save SupportSave data to a SANnav server using the SCP or SFTP protocols or to an external server using SCP, FTP, or SFTP protocols. SANnav uses port 21 to transfer files using the FTP protocol and port 22 or custom port number (other than port 22) to transfer files using the SCP and SFTP protocols. You can also generate a SupportSave immediately or schedule it to be run on daily, weekly, or monthly basis. The events and conditions that might lead a switch to fail are collected by trace dump. RASLog messages report significant system events (failure, error, or critical conditions) and are also used to show the status of the high-level user-initiated actions.

NOTE

SupportSaves that are collected with the SANnav server's internal SCP/SFTP service, are displayed only in the web UI (**SANnav > Services > Supportsave Management > Generated Files**).

10.2.1 Requirements

Switches must be in reachable mode or under maintenance mode to collect SupportSave data.

NOTE

It is recommended to take a backup of 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.

10.2.2 Generating SupportSave for One or More Switches

Generating switch SupportSave allows you to generate the SupportSave data immediately by defining the location where you want to save the file (internal or external location). The SupportSave data is saved to a user-defined path only when the location external is selected. If the internal SSH server is not active, you can generate switch SupportSave on an external server location only. Ciphers and MAC algorithms are configured for SANnav inbuilt SSH servers to generate SupportSave in an internal location.


NOTE

- SANnav supports AMP version 3.0.0 or later. If the supported version is less than 3.0.0, SANnav may not generate switch SupportSave files.
- The FTP protocol does not support Brocade 6547 and Brocade 6558 switches.

Table 26: Supported Ciphers and MAC Algorithms for Internal SSH Servers

Mac Algorithms		Ciphers Algorithms	
Default Algorithms	Supported Algorithms	Default Algorithms	Supported Algorithms
HMACSHA1	HMACMD5	AES128_CTR	AES128_CBC
HMAC_SHA2_256	HMACSHA1	AES192_CTR	AES192_CBC
HMAC_SHA2_512	HMACMD596	AES256_CTR	AES256_CBC
	HMACSHA196		AES128_CTR
	HMAC_SHA2_256		AES192_CTR
	HMAC_SHA2_512		AES256_CTR
			ARC4_128
			ARC4_256
			3DES_CBC
			BLOWFISH_CBC

To generate the latest switch SupportSave data, perform the follow steps:

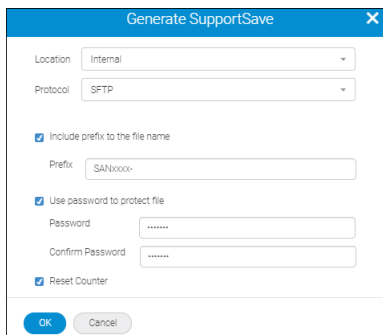
1. Click **SANnav** in the navigation bar, and then select **Services > Supportsave Management**.
2. Click the more icon (), and then select **Bulk Edit**.
3. Select one or more switches for which you want to generate a SupportSave.
4. Click **Edit**, and then select **Generate**.

5. If you select **Internal** as the location, enter the protocol as either SCP or SFTP. You can select the **Include prefix to the file name** option to provide a ticket number to the SupportSave file. The **Prefix** text field appears. If you provide the ticket number, it is prefixed to the file name of the generated switch SupportSave file. Select the **Use password to protect file** option to provide a password for the generated switch SupportSave files. If you want to use internal server with customized port to generate support save files, you must customize the port. SANnav allows you to customize the internal SSH server port during installation. While generating support save files with internal SCP or SFTP server, if the FOS version is 8.2.2 or higher, SANnav sends internal port details to the switch. If the FOS version is less than 8.2.2 and if you want to customize the port for internal SSH server, the internal server cannot generate support save files.

NOTE

The **Prefix** field supports a total of 16 characters.

The default location for internal storage is `<install_home>/data/filetransfer`.



6. If you select the **External** as location, enter the path to which to save the SupportSave files, select the protocol SCP, SFTP, or FTP, enter the host IP address, and enter the login credentials for the external server. You can select the **Include prefix to the file name** option to provide a ticket number to the SupportSave file. The **Prefix** text field appears. If you provide the ticket number, it is prefixed to the file name of the generated switch SupportSave file. You can select the **Save Login information** check box to save the login information for the future.

NOTE

- While generating switch support save files with external SCP or SFTP server, the port number can be customized only when the FOS version is 8.2.2 or higher.
- SANnav does not support customizing the port for an FTP protocol.

7. Select the **Reset Counter** check box if you want to clear the Fibre Channel and GbE counters after collecting the SupportSave.

The Port reset counter will reset all the counters related to port statistics.

For example:

- Link resets
- Invalid CRC
- Loss of sync
- Loss of signal

8. Click **OK** to start generating the Switch SupportSave.

You can view the success or error report in the **Events** tab.

NOTE

The folder where the switch SupportSave files are generated is suffixed with a *yyyy-mm-dd* date format.

10.2.3 Scheduling SupportSave for One or More Switches

For a switch, the SupportSave file can be very large, and it takes some time to generate. To save time and also collect the switch SupportSave data on a regular basis, you can schedule SupportSave for one or more switches.

You can schedule switch SupportSave daily, weekly, or monthly and specify the start time. You can save the SupportSave file to your internal or external location. Ensure that you have enough space on your storage device for scheduled backups.


NOTE

- If the internal SSH server is not active, you can generate switch SupportSave only on an external server location.
- The FTP protocol does not support Brocade 6547 and Brocade 6558 switches.
- View the success or error report of the switch SupportSave in the **Events** tab.

The default SupportSave schedule behavior is supported in the following scenarios:

- If a single switch is selected.
- If two or more switches with the same schedule are supported.
- If two or more switches with different schedules are supported.

To configure a scheduled switch SupportSave, follow the instructions below:

1. Click **SANnav** in the navigation bar, and then select **Services > Supportsave Management**.
2. Click the more icon (), and then select **Bulk Edit**.
3. Select one or more switches for which you want to generate a SupportSave.
4. Click **Edit** and select **Schedule**.
5. Select **Daily**, **Weekly**, or **Monthly** from the **When** drop-down and specify the start time.
If you select **Daily**, specify the time at which you want to generate the SupportSave file.
If you select **Weekly**, specify the day on which you want to generate the SupportSave file.
If you select **Monthly**, specify the date on which you want to generate the SupportSave file.
6. Select **Internal** or **External** from the **Location** drop-down to save the SupportSave file.
 - Select the SCP or SFTP protocol, if you select **Internal** as the location. If you want to use internal server with customized port to generate support save files, you must customize the port. SANnav allows you to customize the internal SSH server port during installation. While scheduling the generation of the support save files with internal SCP or SFTP server, if the FOS version is 8.2.2 or higher, SANnav sends internal port details to the switch. If the FOS version is less than 8.2.2 and if you want to customize the port for internal SSH server, the internal server cannot be scheduled to generate support save files.

NOTE

The default location for internal storage is `<install_home>/data/filetransfer`.

- Select the **Include prefix to the file name** option to provide a ticket number to the SupportSave file. The **Prefix** text field appears. If you provide the ticket number, it is prefixed to the file name of the generated switch SupportSave file.

NOTE

The **Prefix** field supports maximum number of 16 characters.

- Select the **Use password to protect file** option to provide a password for the generated switch SupportSave files. After the switch SupportSave is completed, the password that is provided for zipping the content is used to protect the ZIP file. You need to provide the same password to extract the ZIP file.

NOTE

- The password-protected ZIP file support is available only for the internal file transfer server and is not applicable for the external server. If the external server is chosen, this option is not visible.
- You can use third-party tools (for example 7-Zip or WinRAR) to unzip password-protected ZIP files as Windows does not support extracting password-protected ZIP files.
 - In case of WinRAR, if you enter a wrong password to extract the ZIP file, it creates an empty parent folder and subfolder.
 - In case of 7-Zip, if you enter a wrong password to extract the ZIP file, it creates an empty parent folder, subfolder, and files.

The default location for internal storage is `<install_home>/data/filetransfer`.

- Enter the path to which to save the SupportSave files, select the protocol SCP, SFTP, or FTP, enter the host IP address, and enter the login credentials for the external server if you select **External** as the location. You can select the **Include prefix to the file name** option to provide a ticket number for the support save file. The **Prefix** text field appears. If you provide the ticket number, it is prefixed to the file name of the generated switch support save file. You can click the **Save Login Information** check box to save the login information for the future.

NOTE

- While scheduling the generation of the switch support save files with external SCP or SFTP server, the port number can be customized only when the FOS version is 8.2.2 or higher.
- SANnav does not support customizing the port for an FTP protocol.

7. Select the **Reset Counter** check box if you want to clear the counters after collecting SupportSave. The port reset counter will reset all the counters related to port statistics:

- Link resets
- Invalid CRC
- Loss of sync
- Loss of signal

8. Select the **Enable** check box and click **OK** to schedule the switch SupportSave.


10.2.4 Configuring Trace Dump

Trace dump must be enabled to collect a trace dump report of a switch.

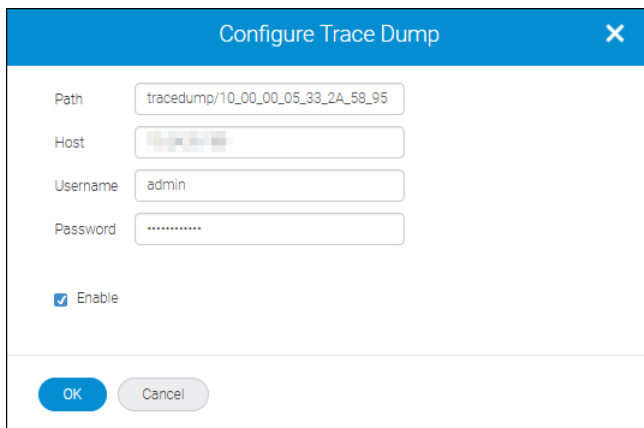
NOTE

- By default, trace dump can be configured to the external location only. FTP is the protocol for an external location.
- You cannot configure trace dump in bulk.

To enable trace dump for any switch, follow the instructions below:

1. Click **SANnav** in the navigation bar, and then select **Services > Supportsave Management**.
2. Click () on any of the discovered switches, and select **Configure Trace Dump**.
3. Enter the path where the failure report should be saved in the **Path** field.

SANnav creates a new folder in the specified path and configures the same in the switch to collect trace dump reports of the switch.



4. Enter the host IP address and server login credentials.
5. Select the **Enable** check box and click **OK** to enable trace dump on the selected switch.

10.2.5 Managing the Switch SupportSave Files

You can view the SupportSave files that are saved in the internal server location. You can perform the following actions:

- Download
- Send
- Delete

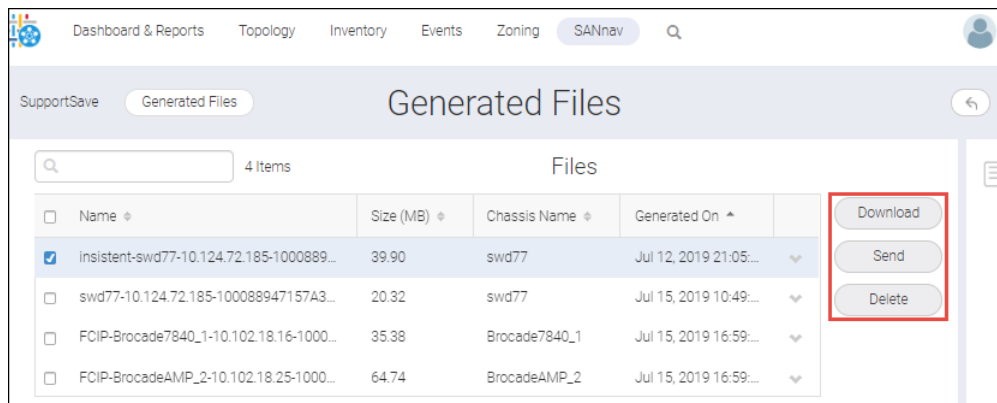
To manage the SupportSave saved files, follow the instructions below:

1. Click **SANnav** in the navigation bar, and then select **Services > Supportsave Management**.
2. Select the **Generated Files** tab to select the generated switch SupportSave files.

3. You can perform any of the following actions on the selected file:

NOTE

Only files that are saved to the internal server location will be displayed.



- Click **Download** to save the file to the local machine.

You can download or send only one SupportSave file at a time. When you select multiple files, you can perform only the delete action.

- Click **Send** to send the file to the external location.

Select **Login Type (Normal or Anonymous)**.

The **Username** and **Password** fields are grayed out when you select **Anonymous** under the **Login Type**. The **Anonymous** option is applicable for FTP protocol only.

Enter the username and password when you select **Normal** under the **Login Type**.

You can save the login credentials by enabling the **Save login information**.

- Click **Delete** to delete the file from the repository.

SANnav Management Portal Maintenance and Support

11.1 SANnav Backup and Restore

SANnav allows you to back up the SANnav server data and restore it as required, such as in scenarios where the data is deleted or corrupted. Also, you can use the backup when you want to bring up a new SANnav server. Creating a backup helps to protect the server's data and configuration in the event of a disaster, such as server failure. You have options to exclude large data sets, which can save restoration time in some situations. You can perform a scheduled daily or weekly backup or an on-demand backup.

NOTE

The backup option is not supported with the trial license.

The following is the list of core and optional backups in SANnav:

Core Backup (Default)

The default backup file includes the core schema in PostgreSQL, Elasticsearch indexes except for the events and configuration files.

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

Optional Backup

Optional backup files include historical statistics, events from Elasticsearch, and reports.

- Fault event data and reports
- Performance data

SANnav does not purge older backups. Make sure that you check the disk space periodically for successful scheduled backups.

Prerequisites

Ensure that the PostgreSQL and Elasticsearch services are working for a successful backup. For Linux OS, the external location should be mounted in the SANnav server to validate the location.

Backup Recommendations

The recommendations for backup are given below:

- Perform a full backup on a weekly or monthly basis since the daily backup may 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 the SANnav Management Portal is installed.
- For scheduled backups, check occasionally if the backup data size is having any abnormal pattern like some files being too large or too small.

11.1.1 Configuring a Scheduled Backup

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

When you schedule a backup, you specify the time for the backup to occur. You can save the backup file on your local machine or on external storage. Make sure that you check the disk space periodically for successful scheduled backups. 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. Enter the Linux location where you want to save the backup file, and click **Validate Location**.
The **Location** field turns yellow if you enter an invalid location.

NOTE

The location should be the path of the server where SANnav is installed.

You can also enter the external storage path of the mounted SANnav server.

3. Select the **New backup** drop-down, and enter the name for the new backup.
4. Select **Daily** from the backup drop-down, and enter the start time for the daily backup.
By default, the backup includes database and configuration files.
For this scenario, do not select any of the optional datasets.
5. Check **Enable** to activate the backup.
6. Click the **+** icon on the top-right corner of the window to add a new backup.

NOTE

You can create a maximum of two scheduled backups. You can create one weekly and one daily scheduled backup, or you can create two weekly scheduled backups. You cannot create two daily scheduled backups.

7. Enter the name for the second backup in the **Name** field.
8. For this example, select the optional backup check boxes.
9. Select **Weekly** from the **Backup** drop-down, and then select the day and start time.

There must be more than three hours difference between the start times of the two backups. For example, if the daily start time is 12:00 AM, the weekly start time must be set to more than three hours before or after the daily start time; for example, 8:45 PM or 3:15 AM.

If you create two weekly backups, in addition to the 3-hour time difference, the weekly backups must start on two different days.

10. Check **Enable** to activate the second scheduled backup, and click **Save**.

NOTE

You must enable each scheduled backup to generate that backup.

System Behavior

SANnav verifies the storage location and starts the backup as per the schedule.

11.1.2 On-demand Backup

You can back up the SANnav Management Portal server data immediately, to save the latest configurations. For example, you can backup the application before you update the firmware. If the firmware did not complete successfully and the data is corrupted or deleted, you can use the backup file to restore your data.

To back up the files on demand, follow the instructions below:

1. Click **SANnav** in the navigation bar, and then select **Services > SANnav Backup**.
2. Click **Backup Now** on the top-right corner of the window.

3. Enter the location where you want to save the backup file in the **Location** field.
4. Click **Validate Location**.
The **Location** field turns yellow if you enter an invalid location.
5. Click **OK**.

NOTE

Select **Optional Backup** check boxes if it is required.

11.1.3 Restoring Backup Files

You can restore the backup files in the SANnav server by using the CLI script. The restore script is accessed from the master node with the administrator privilege.

The restoration process stops all SANnav Management Portal services, restores the data from the backup files, and then restarts the SANnav services. The restore ZIP file contains a checksum file, which ensures that the file is not corrupted and is a valid backup file.

The restoration process time depends on the size of the backup file.

NOTE

Before starting the restore process, all users must log out from SANnav.

If the backup server uses LDAP as the primary authentication method, after restoring the backup you must manually add the LDAP server to the restore server using a provided script.

Restrictions for Restoration

- Both the backup server and the restore server should have the same version and build.
- Both the backup server and the restore server should have the same license.

Supported Restore Combinations

- Back up from a single-node SANnav instance and restore to a single-node instance.
- Back up from a single-node SANnav instance and restore to a multi-node instance.
- Back up from a multi-node SANnav instance and restore to a multi-node instance.

To restore the backup using the CLI script, follow the instructions below:

1. Go to `<install_home>/bin/backuprestore` with the administrator privilege.
2. Issue the `./restore.sh <backup file_path>`.

```
root@CentOS74_41_53:/opt/dcm_1.1_tag_bld1.1/bin/backuprestore
[root@CentOS74_41_53 backuprestore]# ./restore.sh /opt/dcm-ondemand-backup-09-12-2018-13-53-55.zip
```

3. If the backup server uses LDAP as the primary authentication method, manually add the LDAP server to the restore server.

Go to the `<install_home>/bin` location, and run the `addLdapServer` script.

```
./addLdapServer <hostname_with_domain:ipaddress>
```

11.2 Management Portal Server Support Data Collection

You can collect support data from the SANnav Management Portal server for offline analysis. To customize this data collection, you can collect logs only or logs and the database, and you can select the time period for collecting the data.

SANnav Management Portal Server support data collection collects data from the server and stores it in a single ZIP file, which you can send to an FTP server or download for troubleshooting. The collected data can help find the root cause and resolve issues in SANnav.

You must have enough internal and external hard disk space to collect the database and cache information. The collected data is consolidated, and one archived ZIP file is created.

The collected data includes the following:

- Client logs
- Service logs
- Configuration files
- Cache details
- Database (full) and logs
- Switch HTTP capture
- Thread and heap dump usage data
- The date and time of the data collection

11.2.1 Generating the Support Data Collection File

Generate the support data collection file when you encounter any issues with the SANnav modules. You must collect the support data immediately following an issue.

If the SANnav application is down, you can generate the support data from the command line interface (CLI).

```

root@RHEL7_109:/opt/dcm_nfs_mount/Portal_1.1_rc_bld29/bin/supportsave
[root@RHEL7_109 supportsave]# ./supportsave
*****
***** Support Data CLI *****
*****
1) Logs Only
2) Logs and Database
3) Exit
#? █

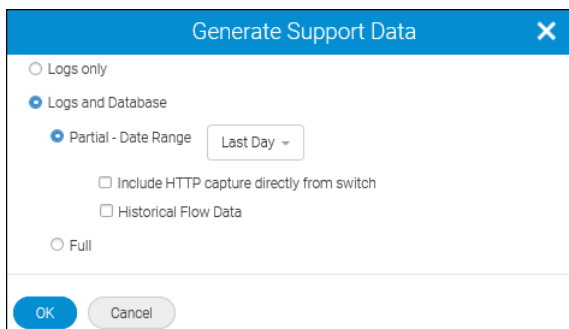
```

You can run the `supportsave` command and generate the following data:

- **Logs Only**
 - Log files
 - Configuration files
- **Logs and Database**
 - Log files
 - Configuration files
 - PostgreSQL and Elasticsearch data folders

To capture support data, complete the following steps:

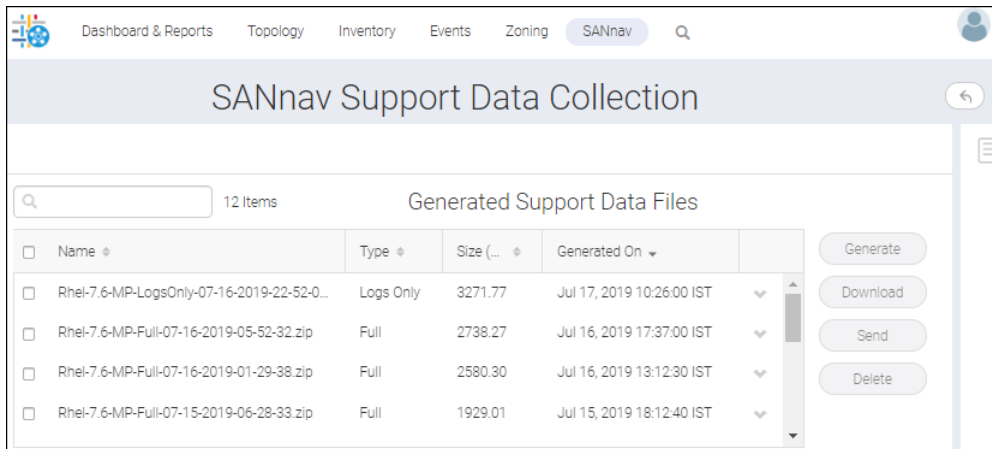
1. Click **SANnav** in the navigation bar, and then select **Services > SANnav Support Data Collection**.
2. Click the **Generate** button.
The **Generate Support Data** dialog displays.
3. Select one of the following radio buttons, and click **OK**.
 - **Logs only** — Collect only the logs, cache information, and configuration files from the SANnav server and create a consolidated ZIP file.
 - **Logs and Database:**
 - **Partial - Date Range** — Collect support data for a specific date range: **Last Day**, **Last Week**, or **Last Month**. You can collect historical statistics and events data.
Select the **Include HTTP capture directly from switch** check box to collect switch data along with partial support data.
Select **Historical Flow Data** check box to collect historical flow data.
 - **Full** — Collect all data from the SANnav server and create a consolidated ZIP file.



Collecting support data takes some time. The files generated are listed under **Generated Support Data Files** in the **SANnav Support Data Collection** page.

NOTE

The **Generate** button is in a disabled state while support data is being collected.



11.2.2 Splitting and Merging SANnav Support Data Files

With the implementation of the file split and merge feature, you can split large support data collection files into smaller chunks and merge them back into a single file for faster transmission over the network. The following two scripts are used to support this functionality:

- `fileSplitter.bat/sh`
- `filesMerger.bat/sh`

NOTE

The file chunks that are generated by `fileSplitter` and merged by `filesMerger` cannot be opened with any editor. These scripts are only for splitting a big file into smaller chunks and assembling them into a single file.

11.2.2.1 Splitting SANnav Support Data Files

To split a large file into smaller chunks, perform the following steps:

1. Copy the `.zip` file to the `SANnav_HOME` directory, and extract it to the same location.
2. Open the command prompt, and navigate to the `SANnav_HOME\bin` directory.
3. Enter the following command:

```
fileSplitter.sh <"full_path_of_original_file_to_be_split"> <chunk_size>
```

For example, `FileSplitter.sh "/root/dcm1.0.0/rhel_44_65-MP-Full-12-27-2018-00-58-45.zip" 500`

Where the `<full_path_of_original_file_to_be_split>` parameter defines the location of the original file to split, and the `<chunk_size>` parameter defines the size of the parts in MB.

NOTE

If the file chunk size is not provided, by default the chunk size is set to 100 MB.

The split files are captured in the same location with the name `<original_file>.<part_number>`.

For example, `rhel_44_65-MP-Full-12-27-2018-00-58-45.zip.001`, `rhel_44_65-MP-Full-12-27-2018-00-58-45.zip.002`, and so on.

11.2.2.2 Merging SANnav Support Data Files

NOTE

The Technical Support team can use the following procedure/script to merge the file. It is not necessary for the user to perform it.

To merge the split files into a single file, perform the following steps:

1. Open the command prompt, and navigate to the `SANnav_HOME\bin` directory.
2. Enter the following command:

```
filesMerger.bat <"one_of_chunk_filename"> <"merged_filename">
```

For example, `filesMerger.bat "C:\AMP\New\DCM-SS-10-15-2018-13-46-53.zip.001" "C:\AMP\New\MergedFile\DCM-SS-10-15-2018-13-46-53.zip"`

Where the `<one_of_chunk_filename>` parameter defines the chunk file name and the `<merged_filename>` parameter defines the location to capture the merged file.

11.2.3 Downloading the Support Data Collection Files

You can download the support data collection files to a local machine, upload them, and manually send them to an external server later.

To download the collected support data, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Services > SANnav Support Data Collection**.
The **SANnav Support Data Collection** page displays with a list of generated support data collection files.
2. Select a support data collection file, and click the **Download** button.
Note that only one support data collection ZIP file can be download at a time. The files are downloaded to the local server. If you select multiple data collection files, the **Download** button is disabled.

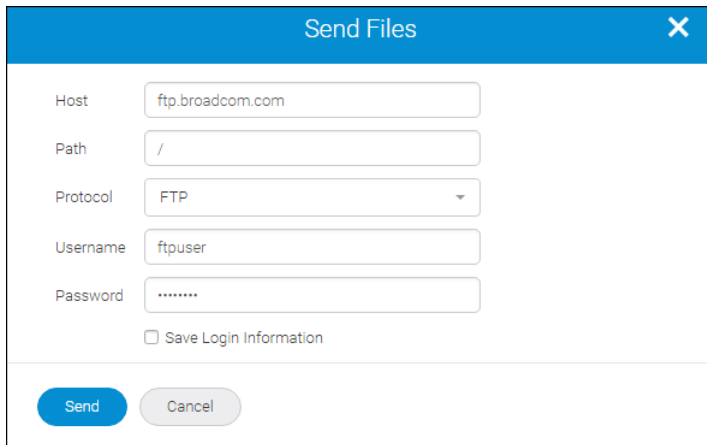
11.2.4 Sending Support Data Collection Files to an FTP Server

Support data collection files are intended for your switch service provider. Send the support data collection files to a remote FTP server for troubleshooting. Only the FTP path and the FTP protocol are supported.

To send the support data collection file to an external server, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Services > SANnav Support Data Collection**.
The **SANnav Support Data Collection** page displays with a list of generated support data collection files.
2. Select a support data collection file, and click the **Send** button.
You can select only one file at a time.

3. Enter the host, server path, username, and password. Select the **Save Login Information** check box if you want to save the login credentials for the future use.



4. Click the **Send** button.
The file is sent or uploaded to the external server location.

11.2.5 Deleting the Support Data Collection Files

You can delete the support data collection files from the server.

To delete the support data collection files, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **Services > SANnav Support Data Collection**.
The **SANnav Support Data Collection** page displays with a list of generated support data collection files.
2. Select one or more support data collection files, and click the **Delete** button.
The support data collection files are removed from the **Generated Support Data Files** list and from the server.

Troubleshooting and Diagnostics

12.1 Master Node Failure

In a multi-node installation, if the master node fails and cannot be recovered, you must get a new host or virtual machine (VM) for the master node and reinstall SANnav Management Portal.

Before installing SANnav on the new host or VM, you must run some scripts on the worker nodes to remove traces of the previous installation.

Perform the following steps on each worker node.

1. Go to `Portal-utility-scripts` and run the script `uninstall_nfs_setup.sh`.
`./uninstall_nfs_setup.sh`
2. In the same `Portal-utility-scripts` directory, run the script `uninstall_docker.sh`.
`./uninstall_docker.sh`

After performing these steps on each worker node, you can now install SANnav Management Portal on the new host or VM as usual.

12.2 Worker Node Failure

In a multi-node SANnav installation, if a worker node fails and cannot be recovered, you can safely replace the failed worker node with a new one.

1. On the master node, remove the failed worker node from the NFS client list and add the new worker as a new NFS client.

Go to the `<install_home>/bin/tools` directory and run the following script:

```
./replace-nfs-client.sh
```

2. On the new worker node, go to `Portal-utility-scripts` and run the following script to set up the new worker.
`./setup-multinode-worker.sh`

3. On the master node, delete the existing stack and deploy the new stack based on the three new nodes. Go to the `<install_home>/bin/tools` directory and run the following script:

```
./replace-worker-and-restart.sh
```

The new worker node is set up and the server is restarted.

You must restart all three VMs after completing this procedure.

12.3 No Login Page

After installation completes, if the SANnav login page does not appear, this might mean that the proxy service is up or the firewall is blocked.

1. Check all services to make sure they are up.
2. Check the firewall to make sure all required ports are available.

3. Ensure that IPv4 IP forwarding is enabled by entering the following command:

```
/sbin/sysctl net.ipv4.ip_forward
```

If the output is `net.ipv4.ip_forward=1`, then forwarding is enabled, and you do not need to make any changes.

If the output is `net.ipv4.ip_forward=0`, this means that forwarding is disabled, and you must change it as follows:

- a. Enter the following command to set IP forwarding for this session:

```
/sbin/sysctl -w net.ipv4.ip_forward=1
```

- b. Edit the `/etc/sysctl.conf` file and add the following lines:

```
# IP Forwarding is enabled for Broadcom SANnav
net.ipv4.ip_forward = 1
```

12.4 Dashboard Shows No Data for Switches

If SANnav Management Portal is not collecting performance statistics, the dashboard is not showing any data for one or more switches, or the performance monitoring graphs are not showing any data points for switch ports, add the SANnav server IP address to the allowed ACL list on the switch.

1. On the switch, check if SNMPv3 access control is set to not allow any new IP addresses to communicate with the switch.

```
switch:admin> snmpconfig --show accesscontrol
```

```
SNMP access list configuration:
```

```
Entry 0: No access host configured yet
Entry 1: No access host configured yet
Entry 2: No access host configured yet
Entry 3: No access host configured yet
Entry 4: No access host configured yet
Entry 5: No access host configured yet
```

2. Add the SANnav server IP address to the allowed ACL list on the switch side.

Enter the `snmpconfig --set accesscontrol` command, specifying an index (1 - 6), the SANnav host IP address, and read-write access.

```
switch:admin> snmpconfig --set accesscontrol -index 2 -host 192.0.2.0 -access rw
Committing configuration.....done.
```

```
switch:admin> snmpconfig --show accesscontrol
```

```
SNMP access list configuration:
```

```
Entry 0: No access host configured yet
Entry 1: Access host subnet area 192.0.2.0 (rw)
Entry 2: No access host configured yet
Entry 3: No access host configured yet
Entry 4: No access host configured yet
Entry 5: No access host configured yet
```

3. On the SANnav server, restart all SANnav services.

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

```
./restart-server.sh
```

12.5 High-Granularity Data Collection Schedule Option Is Unavailable

High-granularity data collection is supported only on Gen 6 or higher switches and directors, running Fabric OS 8.2.1 or higher. Switch ports must be E_Ports or F_Ports.

If the high-granularity scheduling option is not available, perform the following steps:

1. Check whether the switches are Gen 6 or higher switch models, running Fabric OS 8.2.1 or higher.
The Inventory page for switches lists the switch models.
2. Check whether the ports are either E_Ports or F_Ports.
The Inventory page for switch ports lists the switch port type.
3. If the switches and switch ports are supported, the switch might be bound to a different SANnav server. Follow the instructions in [Network Port Traffic Conditions Dashboard Is Blank](#).

12.6 Network Port Traffic Conditions Dashboard Is Blank

If the **Network Port Traffic Conditions** dashboard is blank, this might mean that the switch is bound to a different SANnav server. In this case, you will also not be able to schedule high-granularity data collection.

Perform the following steps to detect if the switch is bound to a different SANnav server, and to bind the switch to the correct server.

1. Go to the **Events** page and look for an event that indicates the switch is already bound to another SANnav server (search events for "bound").

Example event description:

```
Switch 192.0.2.0 already bound to another server: 198.51.100.0
```

2. If event messages indicate that the switch is bound to a different SANnav server, perform the following steps:
 - a. Go to the switch command line interface and enter the following command to clear the binding of the switch to the SANnav server.
`mgmtapp --unbind`
 - b. In , stop monitoring the switch, and then start monitoring the switch.
 - c. Check the events page for the event saying that the switch is bound to the server.

Source Name	Description	Category
RHEL7-73-150	Successfully bound to SANnav server: [IP] with switch: [IP]	Management Server Event
RHEL7-73-150	Successfully bound to SANnav server: [IP] with switch: [IP]	Management Server Event

12.7 Repository Tab Not Available for Firmware Management or Switch SupportSave

If, when you installed SANnav, port 22 was in use, the internal firmware repository is not available. To make the internal repository available, you must free port 22 and reinstall SANnav.

1. Edit the `/etc/ssh/sshd_config` file.

- a. Locate the following line:

```
#port 22
```

- b. Uncomment the line and change the port number to another, unused port, such as 8022.

```
port 8022
```

2. Restart the SSHD.

```
systemctl restart sshd
```

The current SSH session remains logged in, but any new sessions must now use port 8022.

3. Uninstall and then reinstall SANnav.

You must uninstall SANnav completely before you reinstall it.

12.8 Firmware Download or Switch SupportSave Fails

A firmware download or switch supportsave operation initiated from SANnav Management Portal using the SCP or SFTP protocol fails in the following scenario:

1. A firmware download or switch supportsave was performed at least once on the switch using SANnav Management Portal.
2. SANnav Management Portal was uninstalled and then re-installed.
3. A firmware download or switch supportsave for the same switch as in Step 1 was attempted.

To avoid this situation, before uninstalling SANnav Management Portal, take a backup of the file `ssh-keypair.ser` from the following location: `<install_home>/conf/security`. After reinstalling SANnav, restore the previously backed-up file to the same location.

To recover from this situation, log in to the switch on which the firmware download or supportsave was performed, and delete the SANnav Management Portal server IP address from the list of known hosts by using the following command:

```
sshutil delknownhost <SANnav-server-IP>
```

12.9 Updating the OS with SANnav Installed

If you update the OS from one supported version to another using Yellowdog Updater, Modified (YUM) on the same host where SANnav is running, you must first stop the SANnav services, perform the update, and then start SANnav services.

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

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

```
./stop-server.sh
```

2. Perform the YUM update to the new OS version.

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

```
./start-server.sh
```

12.10 Switch Busy Message

The maximum number of sessions for a switch is 50. If this maximum is reached, you might get switch busy messages for certain switch operations. The switch busy message also appears in the Events list.

If you are performing simplified zoning or configuration management operations and you get a message that the switch is busy, this means that the maximum number of HTTP sessions has been reached. It can also mean that the fabric is reconfiguring.

If you get a switch busy message, wait for some time and then try again.

12.11 D_Port Testing

Brocade ClearLink Diagnostic Port (D_Port) mode allows you to convert a Fibre Channel port into a diagnostic port for testing traffic and running electrical loopback and optical loopback tests. The test results can be very useful in diagnosing a variety of port and link problems.

NOTE

This feature uses Brocade ClearLink® proprietary technology.

ClearLink D_Port testing can be used to exercise the hardware before deploying ports into the fabric. For example, you might install new SFPs to link two switches or to link a host/target to a switch, and you want to exercise the hardware before adding them to the fabric. If the test passes, you can go ahead and add the ports to the fabric. If the test fails, you can fix the problem accordingly.

When D_Port testing is in progress, SANnav Management Portal changes the port type for all selected ports and associated attached ports to D-Port for the duration of the test. A port in D_Port mode does not carry any user traffic and is designed to run only specific diagnostics tests for identifying link-level faults or failures. When the test is complete, SANnav changes the port type back to the original port type.

The following tests are performed:

- Electrical loopback test
- Optical loopback test
- Link traffic test
- Link latency and distance measurement

Test results are presented after each test completes.

Refer to the *Brocade Fabric OS Troubleshooting and Diagnostics User Guide* for the supported platforms and license requirements for D_Port testing. In SANnav Management Portal, D_Port testing is not supported on QSFPs.

12.11.1 Starting D_Port Testing

D_Port testing is useful if you want to diagnose port and link problems or if you want to exercise hardware before deploying ports into the fabric.

Requirements:

- You must have Troubleshooting privilege with read-write permission.
- Both the source and destination ports must be managed by SANnav Management Portal.

Once you start a D_Port test, you cannot stop it.

NOTE

When you run a D_Port test, SANnav Management Portal changes the port type for all selected ports and associated attached ports to D_Port for the duration of the test. This may cause the fabric to segment. When the test is complete, SANnav changes the port type back to the original port type.

1. Click **Inventory** in the navigation bar, and then select **Switch Ports** from the drop-down list.

2. Select the ports on which you want to perform the diagnostic tests.

To select a single port, click the down arrow in the rightmost column for the switch port, and select **Run Diagnostics**. Alternatively, to select multiple ports, use the bulk select option.

a. Click the more button (), and select **Bulk Select**.

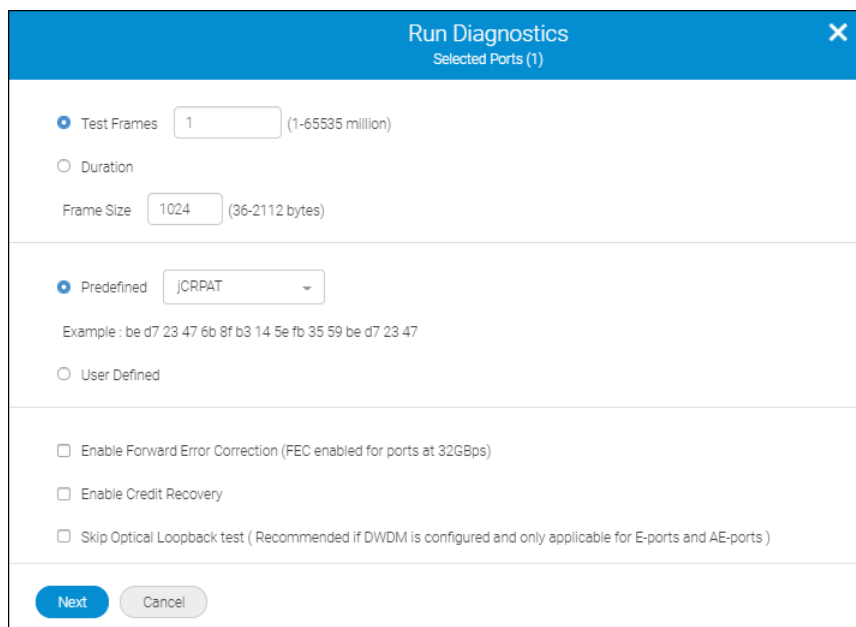
A column of check boxes displays on the leftmost side of the table.

b. Select the check boxes for the ports on which you want to collect data, and then click **Actions > Run Diagnostics** in the upper-right corner of the window.

If **Run Diagnostics** is grayed out, one or more of the selected ports are not supported for running diagnostic tests.

3. Click **OK** in the confirmation dialog.

4. Configure the test parameters, or accept the default values.



Specify either the number of frames to send (in millions) or the time duration for which the frame traffic test will run. The default is to send one million test frames.

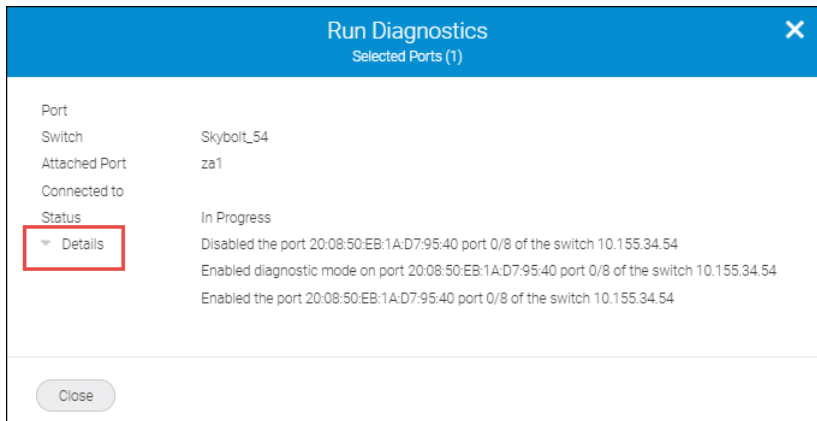
In the **Frame Size** field, enter the size of the test frames that are generated to run the test. The size of the frames can be specified in multiples of four; otherwise, the nearest higher multiple of four value is taken as the frame size. The default value is 1024.

Select a predefined pattern to be used in the payload, or enter a user-defined pattern in decimal. The default is to use the pattern jCRPAT.

You can optionally select the check boxes at the bottom of the dialog. Note that FEC is not supported on D_Ports that are configured with dense wavelength division multiplexing (DWDM). For 32Gbps ports, FEC is automatically enabled and cannot be disabled.

5. Click **Next**.

The diagnostic test starts running. A dialog displays the status of the test.



Testing might take a few minutes to several hours, depending on the selected parameters.

6. Click **Close**.

You can view this status on the **Outputs** page.

7. Click **Done** in the confirmation dialog to return to the **Inventory** page.

Note that the port type for the selected ports has been changed to D-Port.

To view the test results, click **Outputs** in the subnavigation bar, and select **Diagnostics** from the drop-down list.

12.11.2 Scheduling D_Port Testing

You can schedule D_Port testing to run at some time in the future. Since D_Port testing may cause the fabric to segment, you might want to schedule the test at a time when traffic is lighter, such as in the middle of the night.

Requirements:

- You must have Troubleshooting privilege with read-write permission.
- Both the source and destination ports must be managed by SANnav Management Portal.

1. Click **Inventory** in the navigation bar, and then select **Switch Ports** from the drop-down list.

2. Select the ports on which you want to perform the diagnostic tests.

To select a single port, click the down arrow in the rightmost column for the switch port, and select **Schedule**. Alternatively, to select multiple ports, use the bulk select option.

a. Click the more button (), and select **Bulk Select**.

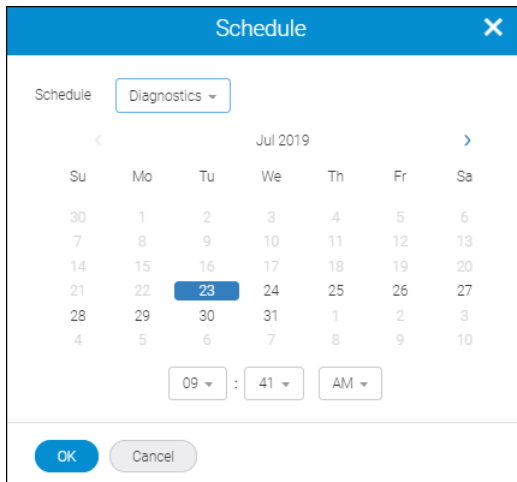
A column of check boxes displays on the leftmost side of the table.

b. Select the check boxes for the ports on which you want to collect data, and then click **Actions > Schedule** in the upper-right corner of the window.

If **Schedule** is grayed out, one or more of the selected ports are not supported for running diagnostic tests.

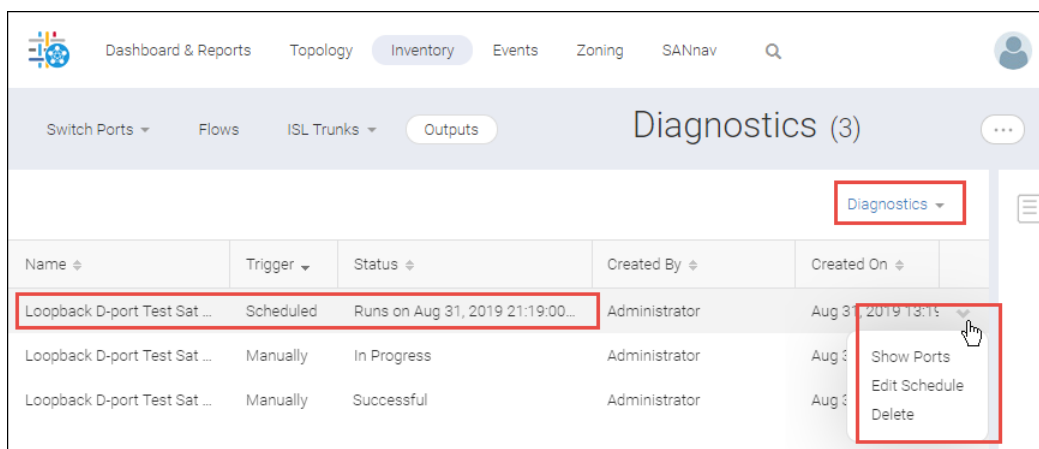
3. Select **Diagnostics** from the drop-down list, select the date and time for the test to start, and click **OK**.

Note that if **Diagnostics** is grayed out, one or more of the selected ports are not supported for running diagnostics tests.



4. Click **OK** in the confirmation dialog.
5. Configure the test parameters or accept the default values, and click **Next**.
6. Click **Done** in the confirmation dialog to return to the **Inventory** page.

You can view the scheduled test by clicking **Outputs** in the subnavigation bar and then selecting **Diagnostics** from the drop-down in the upper-right corner of the page.



From the action menu of the scheduled test, you can display the ports selected for the test, edit the schedule, and delete the test.

12.11.3 Viewing D_Port Test Results

While D_Port tests are running and after the tests are complete, you can view the results from the **Diagnostics** section of the **Outputs** tab.

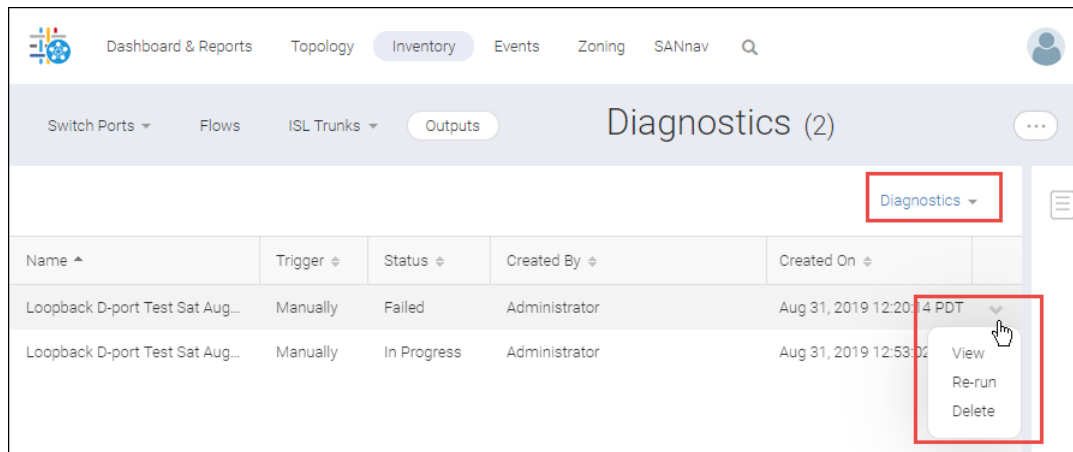
Only the user who ran or scheduled the test can view, delete, or re-run the test.

1. Click **Inventory** in the navigation bar, and then click **Outputs**.

2. Select **Diagnostics** from the drop-down list in the upper-right corner.
3. Locate the test that you want to view, and click **View** from the action menu in the rightmost column.

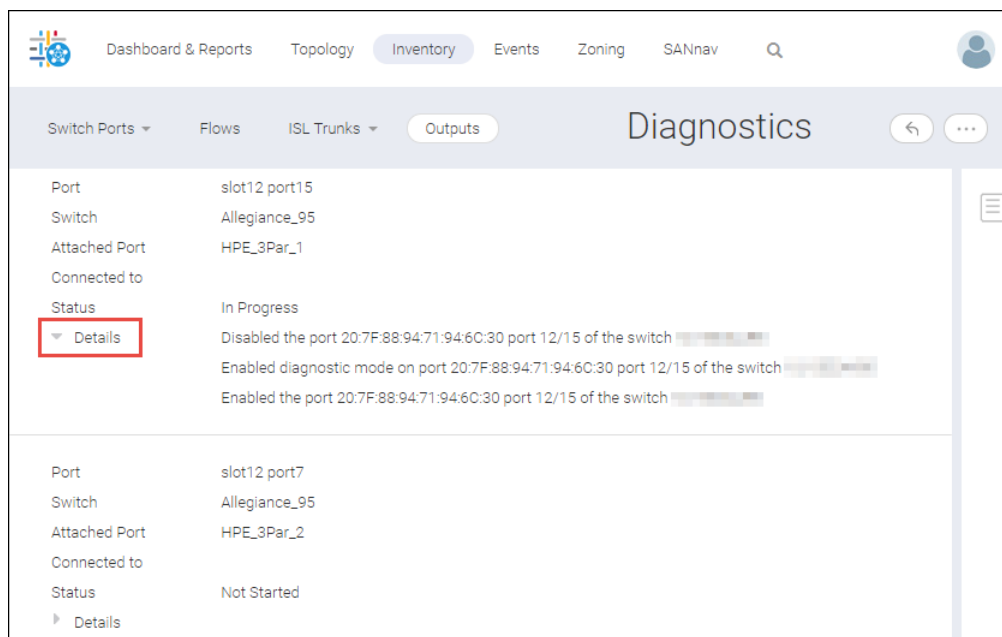
Note that the **View** option is available only for tests that have completed or are in progress. It is not available for scheduled tests.

If you used the **Bulk Select** option to run diagnostics on several ports at the same time, only one entry exists in the **Outputs** page for those tests.



4. Click **Details** to see the detailed results of the test.

The following screen capture shows the test results when the **Bulk Select** option is used to run diagnostics on multiple ports.

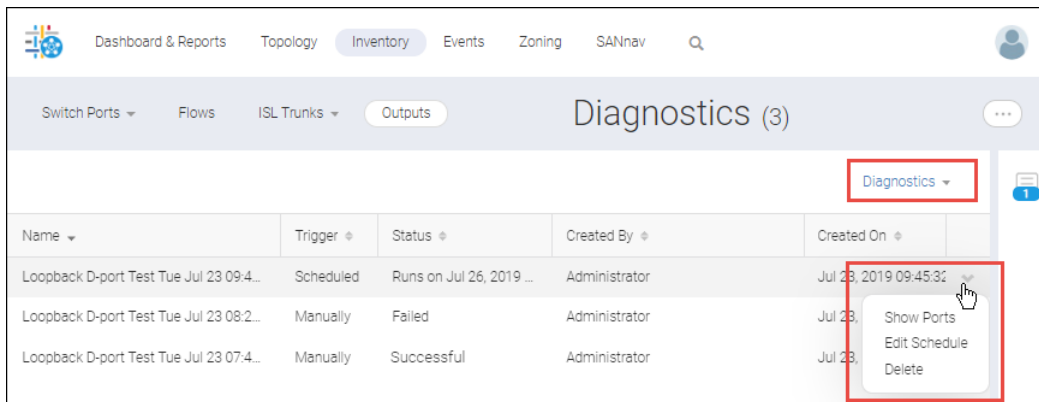


Note that you can re-run a test on the same port by selecting **Re-run** from the action menu for a completed test in the **Outputs** page.

12.11.4 Deleting a Scheduled D_Port Test

When a D_Port test starts running, you cannot stop it. You can, however, delete scheduled D_Port tests that have not started running.

1. Click **Inventory** in the navigation bar, and then click **Outputs**.
2. Select **Diagnostics** from the drop-down list in the upper right corner.
3. Locate the scheduled test that you want to delete, and click **Delete** from the action menu in the rightmost column.



The screenshot shows the SANnav interface with the 'Diagnostics (3)' page open. The 'Outputs' tab is selected. A table lists three tests. The first test is 'Scheduled' and is highlighted. An action menu is open for this test, showing options: 'Show Ports', 'Edit Schedule', and 'Delete'. The 'Delete' option is highlighted by a mouse cursor. Red boxes highlight the 'Diagnostics' dropdown and the action menu.

Name	Trigger	Status	Created By	Created On	
Loopback D-port Test Tue Jul 23 09:4...	Scheduled	Runs on Jul 26, 2019 ...	Administrator	Jul 23, 2019 09:45:32	Show Ports Edit Schedule Delete
Loopback D-port Test Tue Jul 23 08:2...	Manually	Failed	Administrator	Jul 23, 2019 08:21:12	
Loopback D-port Test Tue Jul 23 07:4...	Manually	Successful	Administrator	Jul 23, 2019 07:41:12	

4. Click **OK** in the confirmation dialog.

SANnav Global View

13.1 Overview of SANnav Global View

SANnav Global View is a higher-level "global" management application that provides a comprehensive view of a SAN environment that spans multiple SANnav Management Portal instances.

Using SANnav Global View, you can navigate seamlessly across multiple SANnav Management Portal instances and drill down to any individual instance to perform detailed monitoring, investigation, and troubleshooting.

NOTE

SANnav Global View is a separate product from SANnav Management Portal, and it requires separate installation and licensing.

You log in to the SANnav Global View application and add portals to SANnav Global View, which then uses information in the portals to build a global view of the dashboard and inventory.

13.2 Browser Requirements for SANnav Global View

Any laptop or machine that launches web applications can be used to launch SANnav Global View. For optimal performance, have at least 16GB memory.

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

- Chrome (Google)
- Firefox (Mozilla)

Note that if you access the client from the Remote Desktop, the user interface may have degraded performance.

13.3 SANnav Global View Compatibility Matrix

Before you add SANnav Management Portal instances to SANnav Global View, you must know whether the release version of Management Portal is supported by your version of Global View.

SANnav Global View is compatible with the same major release of SANnav Management Portal, including older minor releases. Global View is not compatible with newer releases of Management Portal and is not backward compatible with older major releases.

You cannot add a Management Portal instance with a version that is not supported by Global View.

Table 27: Supported Releases of SANnav Management Portal

SANnav Global View Versions	SANnav Management Portal Versions		
	1.1.0	1.1.1	2.0.0
Global View 1.1.0	Yes	No	No
Global View 1.1.1	Yes	Yes	No
Global View 2.0.0	No	Yes	Yes

13.4 Logging In to SANnav Global View

To log in to SANnav Global View, perform the following:

1. Open your browser and enter the IP address or fully qualified domain name (FQDN) of the SANnav Global View server.

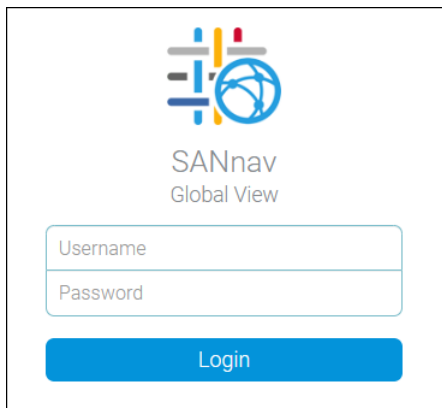
You can use HTTP or HTTPS, for example:

```
http://192.0.2.0
```

or

```
https://192.0.2.0
```

The SANnav Global View login window appears.



If the login window does not appear, try the following:

- Ping the SANnav server to ensure that it is up.
 - Check if SANnav services are running. See "Checking the Server Health" in [Additional Scripts](#).
 - Check the firewall settings.
2. Enter your SANnav user name and password, and click **Login**.

For the first SANnav login, the default user name is "Administrator" and the default password is "password".

SANnav launches with the default dashboard displayed.

If, instead of launching, SANnav displays the message "Login Failed. Service is not available at this time.", SANnav is in the process of starting up. Wait a few minutes and try to log in again.

13.5 Quick Tour of SANnav Global View

Once familiar with the basic components of SANnav Global View, you can quickly start monitoring SANnav Management Portal instances.

When you first log in to SANnav Global View, you see the **Summary** dashboard, the single dashboard provided with Global View. The following screen capture shows the basic layout of the SANnav Global View user interface.



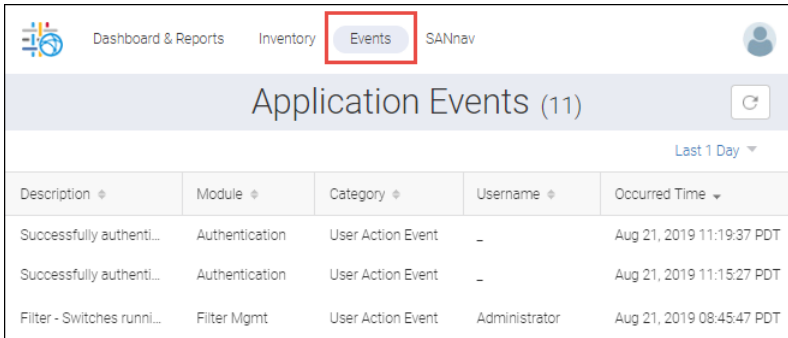
1. Navigation bar. Contains links to feature pages. The **SANnav** link displays the **Configurations and Settings** page.
2. Profile menu. Displays additional links for changing user preferences, displaying the SANnav version, and logging out.
3. Subnavigation bar. Provides the page title and optional item count within parentheses. Also includes buttons and menus to take actions within the page.
4. Filter bar. Allows you to filter the display based on columns, portal scope, and customized filters.

Click **Inventory** to display inventory information about fabrics, switches, switch ports, chassis, host and storage devices, and host and storage ports across all Management Portal instances.

The screenshot shows the 'Inventory' page in the SANnav Management Portal, specifically the 'Switches (78)' view. The page has a navigation bar with 'Dashboard & Reports', 'Inventory', 'Events', and 'SANnav'. A subnavigation bar shows 'Switches' and a filter bar with 'All Swit...' and '+Add'. The main content is a table with the following columns: Name, Type, FID, Fabric, Health, Model, Port Count, and Portal.

Name ^	Type ^	FID ^	Fabric ^	Health ^	Model ^	Port Count ^	Portal ^
A_15643...	Switch	128	FabricTest...	Poor	Brocade X6-8	221	Munich DC
AG_17-mo...	Access Gate...	-	FCIP-104	Healthy	Brocade 6505	24	San Jose DC
AG_17-mo...	Access Gate...	-	Untitled N...	Healthy	Brocade 6505	24	Untitled New Portal

Click **Events** to show all application events that stem from a user or system action. A system action is triggered under certain situations like when a portal is disconnected. You can filter the events list by date range. Events from SANnav Management Portal instances are not listed here.



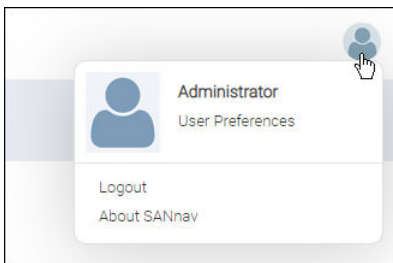
Description	Module	Category	Username	Occurred Time
Successfully authenti...	Authentication	User Action Event	-	Aug 21, 2019 11:19:37 PDT
Successfully authenti...	Authentication	User Action Event	-	Aug 21, 2019 11:15:27 PDT
Filter - Switches runni...	Filter Mgmt	User Action Event	Administrator	Aug 21, 2019 08:45:47 PDT

Click **SANnav** to discover Management Portals, manage filters, and perform various configuration settings across several feature categories.

The profile menu is where you can add your phone number and change your password. It is also where you can enable **Persist Last Column Selection**, wherein the system remembers your column customization, and **FICON Display**.

Column customization is the ability to choose what columns you want to see in a tabular view. For example, by default, only a few of the many available columns in inventory are shown, but you can customize the table by adding or removing columns.

When FICON Display is enabled, certain columns in the switch and switch port inventory pages are rearranged for FICON mode.



13.6 Global View Licensing

SANnav Global View requires a Global license key to function. By default, a 90-day license is included with the product. To obtain complete functionality after the trial period, you must obtain a license key and add it to SANnav Global View.

For detailed information on generating and applying a license, see [Licensing](#).

13.7 Creating a New User Account

Creating user accounts in SANnav Global View is similar to creating user accounts in SANnav Management Portal. All users created in SANnav Global View have all privileges in the product and can do all operations and functions provided by the Global View.

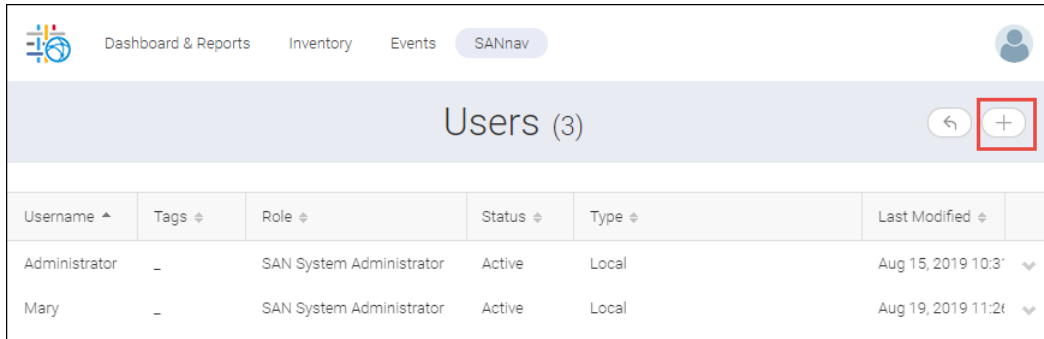
A SANnav Global View user does not have privileges to modify a SANnav Management Portal instance. An attempt to do this triggers a request to log in to the Management Portal. The SANnav Management Portal login credentials determine what a user can perform in that portal.

A SANnav Global View user can see summarized information regarding all fabrics as managed by various portals (though this information is limited to what SANnav Global View presents).

1. Click **SANnav** in the navigation bar, and then select **Security > SANnav User Management**.

A list of users displays.

2. Click the **+** icon in the top-right corner of the page.



3. Fill out the **Create New User** form, and click **Save**.
By default, saving the form activates the account.

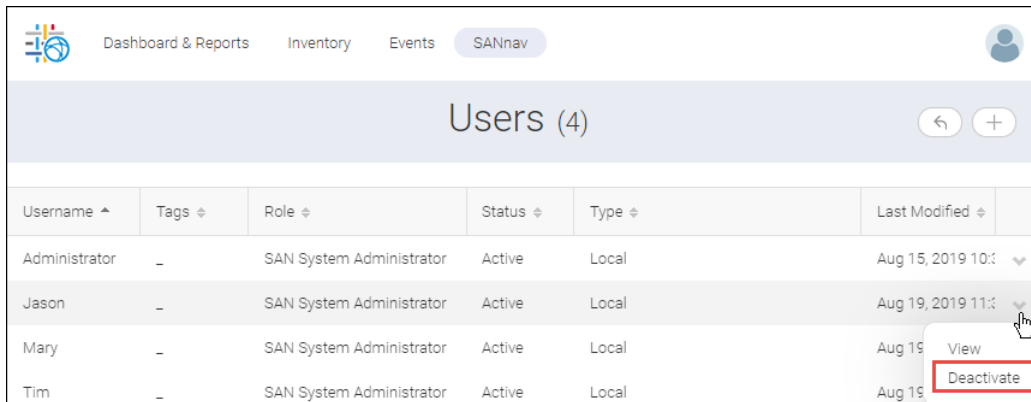
The screenshot shows the 'Create New User' form in the SANnav management portal. The form has the following fields and values:

- Username: Jason
- Password: [masked]
- Confirm Password: [masked]
- Email: user@mail.com
- Phone Number: 123-456-7890
- Tags: [empty]
- Description: New SANnav global administrator.

At the bottom of the form, there is a checkbox labeled 'Activate' which is checked and highlighted with a red box. Below the checkbox are two buttons: 'Save' and 'Cancel'.

The new user is added to the list of Global View users.

- If you want to deactivate a user account, click the down arrow in the rightmost column and select **Deactivate**.



The screenshot shows the SANnav interface with the 'Users (4)' page. A table lists four users: Administrator, Jason, Mary, and Tim. The 'Jason' row is selected, and a dropdown menu is open, showing 'View' and 'Deactivate' options. The 'Deactivate' option is highlighted with a red box.

Username	Tags	Role	Status	Type	Last Modified	
Administrator	-	SAN System Administrator	Active	Local	Aug 15, 2019 10:00	▼
Jason	-	SAN System Administrator	Active	Local	Aug 19, 2019 11:00	▼
Mary	-	SAN System Administrator	Active	Local	Aug 15, 2019 10:00	View
Tim	-	SAN System Administrator	Active	Local	Aug 15, 2019 10:00	Deactivate

13.7.1 Global View Authentication and Authorization

Similar to SANnav Management Portal, SANnav Global View enables you to set up the authentication and authorization policies for local database, LDAP, RADIUS, and TACACS+.

To access authentication and authorization, click **SANnav** in the navigation bar, and then select **Security > SANnav Authentication and Authorization**.

For further details, see [Configuring SANnav to Use an External Server for Authentication](#).

13.8 Adding a SANnav Management Portal Instance

After you add SANnav Management Portal instances to the SANnav Global View, you can monitor them.

When adding the SANnav Management Portal instance to SANnav Global View, you must provide the Management Portal IP address/hostname, port number, username, and password. The login credentials are used for authentication of SANnav Global View when communicating with the Portal instance for retrieving data.

When you add portal instances to SANnav Global View, the Portal credentials must have SAN System Administrator or equivalent privilege and full areas of responsibility (AORs) to all fabrics in the SANnav Management Portal. If not, the addition and discovery of that instance fails.

A maximum of 20 SANnav Management Portal instances can be connected to one SANnav Global View. The total port count must not exceed 120,000 ports. The total port count is the sum of ports that are managed by all Management Portal instances.

- Click **SANnav** in the navigation bar, and then select **SAN Monitoring > Portals**.

The **SANnav Management Portals** list displays.

- Click the **+** icon in the upper-right corner, and specify the IP address and login credentials of the SANnav Management Portal server.

- Click **OK**.

The new portal appears in the list. The default name of the portal is "Untitled New Portal #".

- If you want to change the name of the portal, either click the name or select **View** on its action menu.

Name ^	Status ▾	Connection Detail ▾	IP Address ▾	Port ▾	Username ▾	Last Discovered ▾	
Bangalore DC	Connected	Successfully connected	██████████	443	Administrator	Aug 16, 2019 10:10:07 f	▾
San Jose DC	Connected	Successfully connected	██████████	443	Administrator	Aug 16, 2019 10:08:07 f	▾
Untitled New Portal 1	Connected	Successfully connected	██████████	443	Administrator	Aug 16, 2019 10:18:12 f	▾
Untitled New Portal 2	Connected	Successfully connected	██████████	443	Administrator	Aug 16, 2019 10:22:17 f	▾

Notice that the action menu also has options to reconnect a disconnected portal and delete a portal.

- Edit the name field, and then click **Save**.

The new name appears on the Portals list.

13.9 Global Dashboard Overview

The SANnav Global View dashboard provides comprehensive "global" visibility across multiple SANnav Management Portal instances.

The Global View dashboard is auto-refreshed every 15 minutes.

The Global View dashboard provides the following widgets: Health summary, Switch Health, Port Usage Summary, and Alerts. These widgets indicate the status of the fabric, switch, host, and storage entities managed by the Portals that are currently added in SANnav Global View.

The health summary widgets are categorized by health state: **Healthy**, **Degraded**, or **Poor**. Listed below each widget are the exact number of entities in each health state.

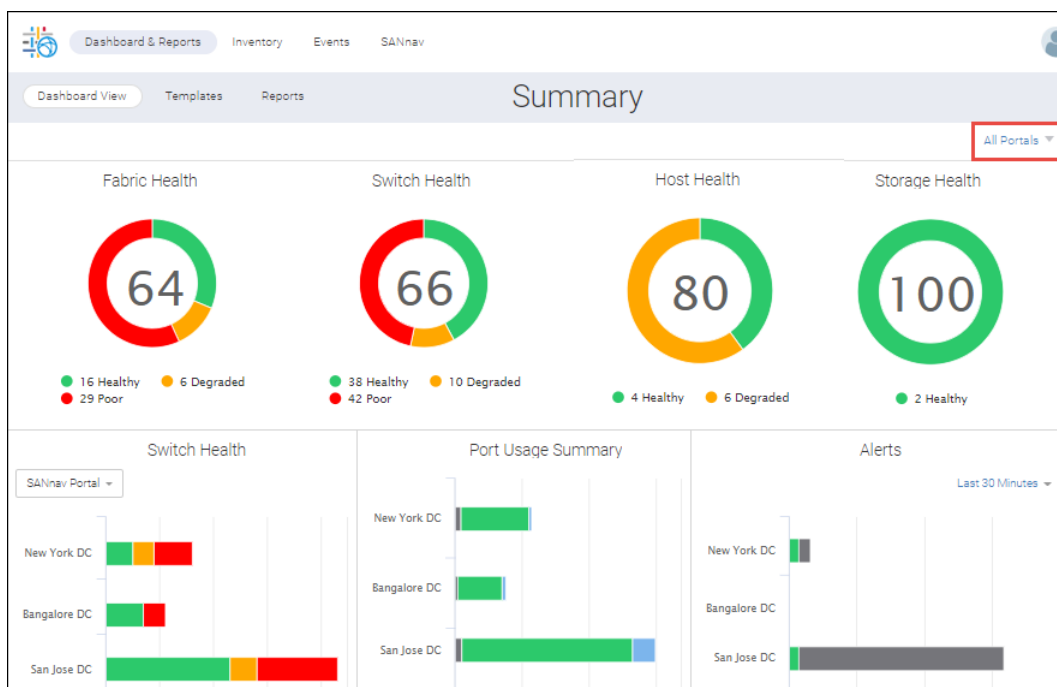
The health state for each type of object is determined by its health score, which is determined by a set of predefined factors. For example, a health score for fabrics is influenced by whether a link is down or redundant paths are missing. For more details on how health score is computed, see [Factors Contributing to the Overall Health Score](#).

Health State	Health Score
Healthy	Greater than 90
Degraded	Between 71 and 90
Poor	70 or less

The health information is retrieved from each of the SANnav Management Portal instances and an aggregate Global View is presented. Health calculations for various entities are done at the SANnav Management Portal level.

SANnav dashboards allow you to gather additional information by drilling down into the dashboard widgets.

By default, the scope of SANnav Global View is set to **All Portals** (that is, all Management Portal instances). You can choose one or more Management Portal instances to change the scope.



13.9.1 Monitoring Fabric Health

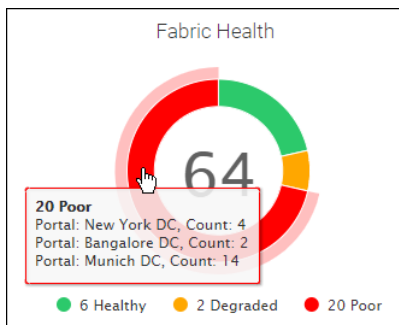
The Fabric Health widget of SANnav Global View shows the number of fabrics in Healthy, Degraded, and Poor state. The least overall score across all objects in this group of fabrics is shown in the center of the circular widget.

The following procedure shows how to use the Global View dashboard to investigate the health state of fabrics across all Management Portals. You can similarly investigate the health state of switches, hosts, and storage using the respective circular widgets.

1. Click **Dashboard & Reports** in the navigation bar.

2. Hover over a colored portion of the **Fabric Health** widget to display details of the fabrics with that state.

For example, hover over the red portion to display a list of portals and the number of fabrics in each portal having a poor state.



3. To view further details on the fabrics, click the colored segment of the widget.

For example, clicking the red segment displays a table showing the health scores for the fabrics in poor health.

4. Click **Show Details** on the action menu of the fabric list to see details associated with that health score.

The **Show Details** option is available only if the score is less than 100.

Name	Score	Switch Status	Events	Configurations	Portal
Fabric_A	64	-30	-2	-4	New York DC
FabricTest_27	70	-30	0	0	M
FcoE	68	-30	0	-2	M
FIDnine	70	-30	0	0	Munich DC

A popup window displays the factors that cause deductions in the health score for this fabric.

5. Click **Back** to return to the list of portals.
6. Select **Show in SANnav Portal** from the action menu to launch the Management Portal instance responsible for the data you are viewing.

You might need to make sure that popups are not blocked in your browser.

If you are not logged in to this portal, credentials (for this portal) are required.

13.9.2 Monitoring Switch Health across Management Portal Instances

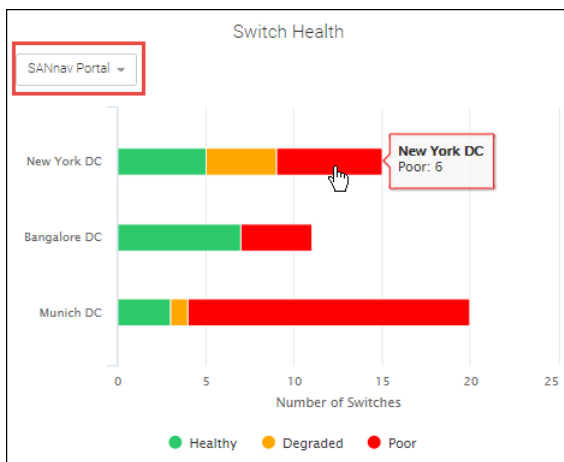
The Switch Health widget displays details of switch health across Management Portal instances. You can get a summarized view as well as details of switches based on firmware version, Management Portal instance, switch model, and product category.

The following procedure shows how to use the Global View dashboard to display switch health across multiple Management Portal instances.

1. Click **Dashboard & Reports** in the navigation bar.

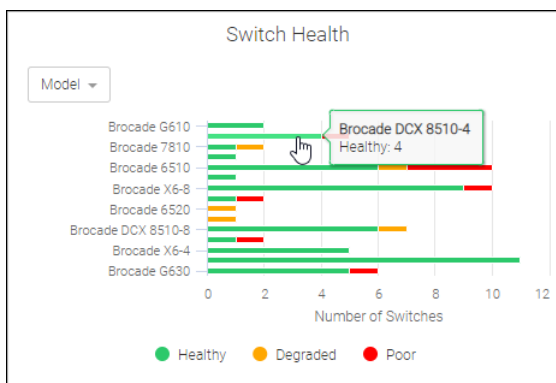
On the bottom row of the dashboard, the **Switch Health** widget displays.

In this screen you see switches grouped by **SANnav Portal** instances. You can select a different grouping from the drop-down list.



2. Hover over the graph to display details.

Note that for the **Firmware Version** and **Model** categories, more bars may be displayed in the graph than are listed in the row names on the left. In this case, hover over an intermediate bar in the graph to display the details.



- To see the details on all switches in a particular category, click the bar chart of the widget, and then select **Show Details**.

Name	IP Ad.	WWN	State	Status	Status Reason	Fabric
A_1564...	10.155.4...	10:00:C4:...	Online	Critical	Switch Status is CRITICAL. Contributors:*B...	FabricTest_27
stinger16	10.155.4...	10:00:50:...	Unknown	Not Reach	Switch Status is CRITICAL. Contributors:*BAD_PWR (CRITICAL), *BAD_FAN (CRITICAL).	st_27
sw2	10.155.4...	10:00:C4:...	Online	Marginal	Switch Status is MARGINAL. Contributors:...	Switched New ...
sw3	10.155.4...	10:00:C4:...	Online	Critical	Switch Status is CRITICAL. Contributors:*B...	FcoE

- Click **Close** to return to the dashboard.
- Select **SANnav Portal** from the drop-down list in the widget, click the bar graph, and select **Show in Portal** to display the switch inventory in the selected SANnav Management Portal instance.

If you are not logged in to this portal, credentials (for this portal) are required.

A separate window opens for the Management Portal instance.

13.9.3 Displaying Port Usage Details

The Port Usage Summary widget displays data for each SANnav Management Portal instance categorized by the number of device ports, unused ports, and ISL/IFL ports.

Note the following:

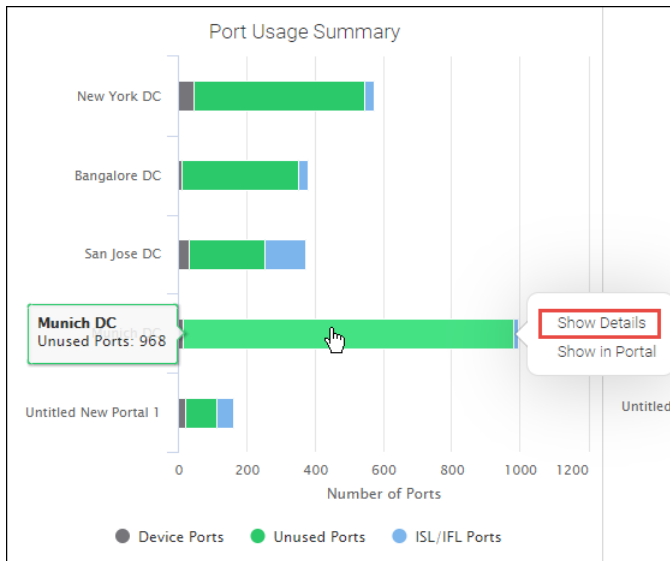
- Device ports include F_, L_, and N_Ports.
- Unused ports include G_ and U_Ports.
- ISL/IFL ports include E_ and EX_Ports.

This widget covers only the FC ports. FCIP and ETH ports are not covered as part of the widget

Tooltips provide the count and Management Portal name. You can see port details related to a particular section of the bar chart as well as navigate to a web page in SANnav Management Portal for ports related to that section.

The following procedure shows how to use the Global View dashboard to display details on port usage across Management Portal instances.

- Click **Dashboard & Reports** in the navigation bar, and then click **Dashboard View** in the subnavigation bar.
On the bottom row of the dashboard, the **Port Usage Summary** widget displays.
- Hover over a segment of the **Port Usage Summary** widget to see details on that segment of the bar graph.



- To view more details on the ports, click on the port usage summary bar graph, and then select **Show Details**. You see a table that details the ports for that segment of the fabric.

Port Usage Summary: ISL/IFL Ports
San Jose DC

120 Items

Name ^	WWN ^	Switch ^	Fabric ^	Attac... ^	Connected Device ^
port2	20:02:C4:...	CID540_100	MyCIDFa...	port2	CID547_100
port2	20:02:C4:...	CID547_100	MyCIDFa...	port2	CID540_100
port3	20:03:C4:...	CID547_100	MyCIDFa...	port3	CID540_100
port3	20:03:C4:...	CID540_100	MyCIDFa...	port3	CID547_100

Close

- Click **Close** to return to the dashboard.
- To see the Management Portal instance responsible for the data you are viewing, click on the port usage summary bar graph, and then select **Show in Portal**.

If you are not logged in to this portal, credentials (for this portal) are required.

13.9.4 Viewing Alerts

For each SANnav Management Portal instance, the **Alerts** widget displays the count of alerts, those switch-generated and those triggered by special events and configuration drifts.

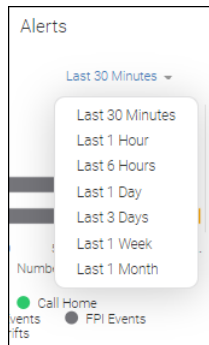
The alerts shown are based on the chosen date range.

The following procedure shows how to use the Global View dashboard to investigate details behind Global View alerts.

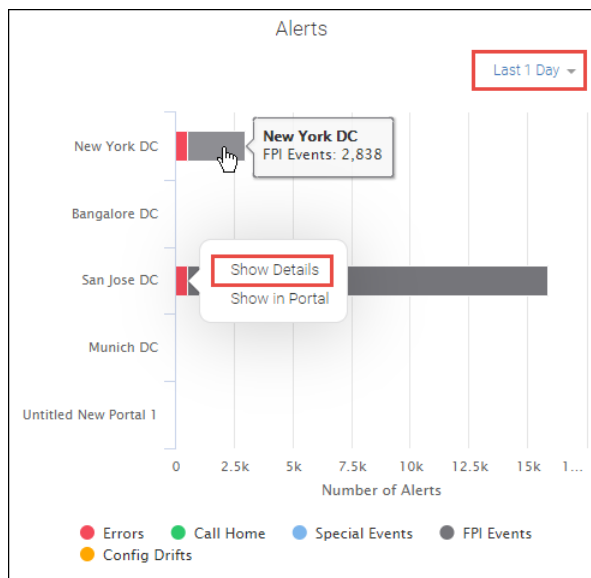
1. Click **Dashboard & Reports** in the navigation bar, and then click **Dashboard View** in the subnavigation bar..

On the bottom row of the dashboard, the **Alerts** widget displays.

The Alerts widget contains a date range, which is set to **Last 30 Minutes** by default. You can select a different date range, up to 1 month.



2. Hover over a segment of a bar to see the number of alerts (associated with a particular Alert category) received for that Management Portal instance.



3. To drill down for more details, click on the alerts bar graph, and then select **Show Details**.

The alerts are listed in a table along with their category, occurrence count, and fabric. The heading indicates the particular SANnav Management Portal instance involved.

Description	Category	Count	Fabric Name
Failed to register syslog for the switch 10...	Management Se...	3	-
FTP Connectivity Test failed due to error.	Product Event	1	FCIP-104
S0,P7(Bp6) user_idx:7 [PID 0x510800] fau...	Product Event	1	FCIP-104
S0,P7(Bp6) user_idx:7 [PID 0x510800] fau...	Product Event	1	Fabric101

Click **Close** to return to the Global View dashboard.

- Click the alerts bar graph and then select **Show in Portal** to see the actual events on the Management Portal responsible for the data you are viewing.

If you are not logged in to this portal, credentials (for this portal) are required.

13.10 Creating a Global Report Template

You can create summary reports from data gathered from all SANnav Management Portal instances.

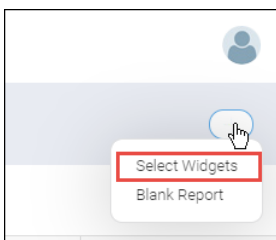
To generate reports, first you create report templates, which define the widgets that comprise the report as well as the Management Portal scope and other filters.

You can create several types of report templates, such as one template for daily reports and another one for weekly reports. Or, you can create separate templates for individual data centers and one template for all the data centers together.

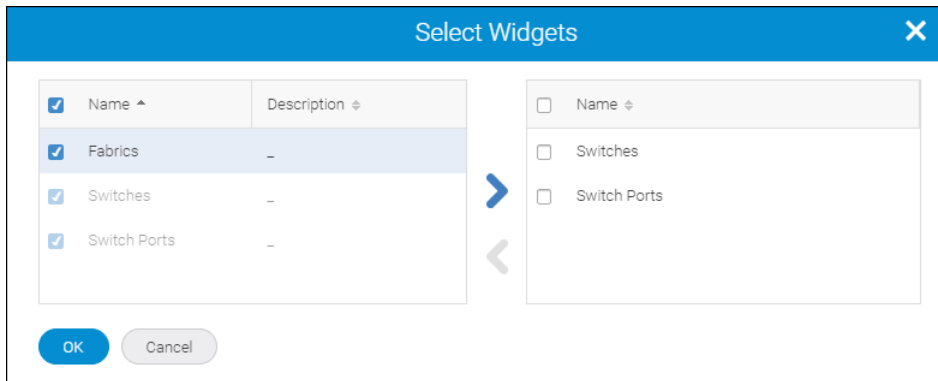
The process for creating report templates is similar to the process for SANnav Management Portal, except that with SANnav Global View, the scope of the reports is based on Management Portal instances. Report scheduling, generation, and exporting are the same as in SANnav Management Portal.

Perform the following procedure to create a report template in SANnav Global View.

- Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
- Click the **+** icon in the upper-right corner, and then select **Select Widgets**.



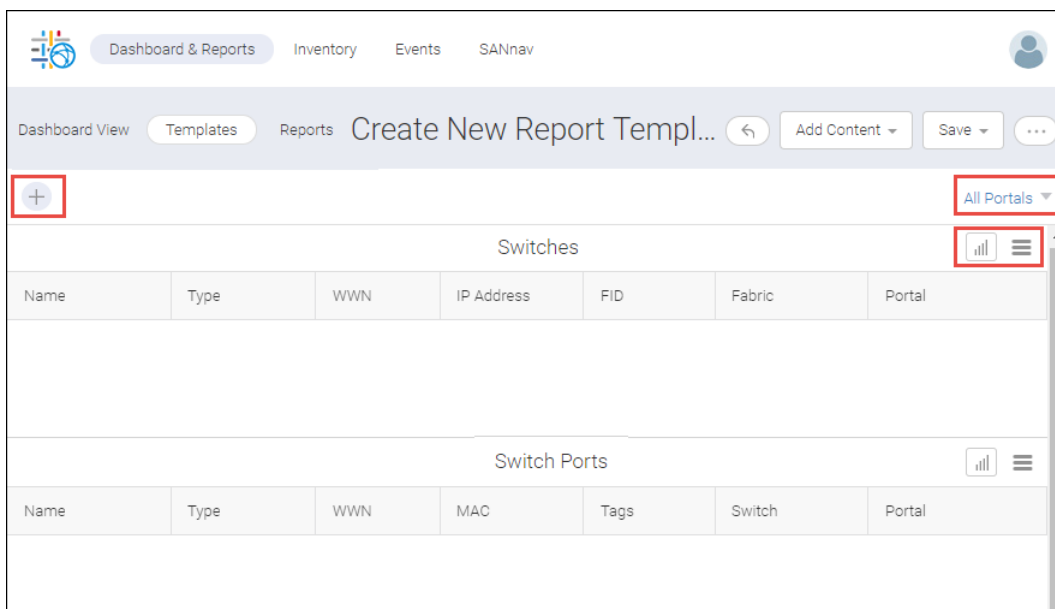
- Select the widgets that you want in your report, and click the right arrow to move them to the right side of the dialog. If you want the widgets in a particular order, select each widget separately and then click the right arrow before selecting the next widget.



4. Click **OK**.

The template displays with placeholders for each widget.

A report layout is created with a default name and default columns, which you can now customize.



5. Add filters to the report template.

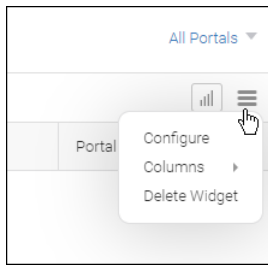
You can customize the report by changing the Management Portal scope using the drop-down list on the right side of the filter bar. Click the + button on the left side of the filter bar to add specific filters for fabrics, flows, switches, and switch ports. The filters apply to all widgets in the template.

The generated report contains data for only those objects that meet the filter requirements.

NOTE

Although there is no restriction on the number of filters that can be added or applied as part of the report template, it is recommended that you follow this guideline: two parameter conditions within a filter and two filters within a report.

6. Customize the widgets.

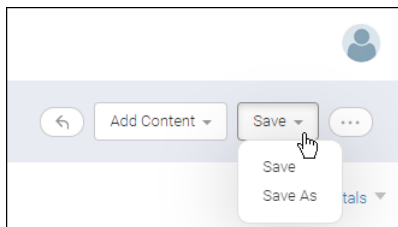


Click the hamburger icon for each widget to do the following:

- Change the name of the widget in the report (**Configure** option).
- Add or delete columns.
- 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 clicking **Add Content > Add Widgets**.

7. Click either **Save > Save** or **Save > Save As** to save the report template.



8. Enter a name for the template, along with optional tags and a description, and select the **Shared** box if you want other SANnav Global View users to view the content.

The template name can contain only alphanumeric characters, as well as the hyphen (-), underscore (_), and period (.).

9. Click **Save**.

To generate your report, go to the **Templates** page and select **Generate** from the action menu. To schedule report generation to run at a future time, select **Schedule**. For detailed instructions, see [Scheduling a Report](#) and [Generating and Exporting Reports](#).

13.11 Global View Inventory Management

The SANnav Global View **Inventory** page is a central location where you can view and manage the inventory of all discovered fabrics, switches, switch ports, hosts, host ports, storage, storage ports, and physical chassis across all SANnav Management Portal instances.

When you first view the **Inventory** page, it is empty. You must add filters to display the data. The exception to this is that when you view chassis objects, all of the chassis display. Other than Portal scope, filters are not supported with chassis objects.

In addition to viewing inventory, you can export the data to a CSV file.

For switch ports, you can launch investigate mode to view performance measures.

13.11.1 Viewing Inventory Using Filters

Inventory can contain thousand of components. In searching for inventory items, use filters to drill down through the inventory and display the items you are interested in from among all SANnav Management Portal instances.

If you want to see all of the inventory for a particular object type, you can enter a wildcard (*) for the filter.

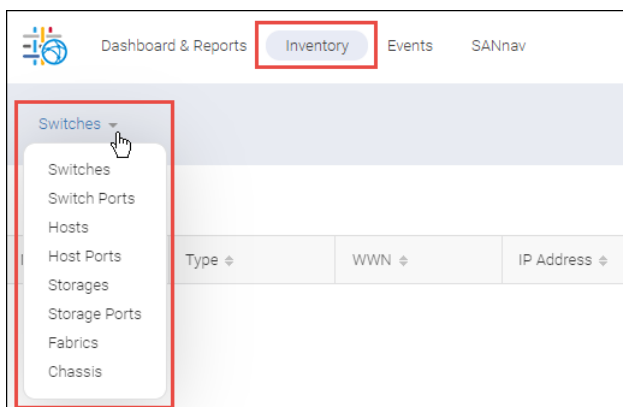
NOTE

When creating filters, type-ahead is not supported in SANnav Global View.

The following procedure shows how to use filters to display a list of switches in degraded or poor health across all Management Portal instances.

1. Click **Inventory** in the navigation bar, and then select the type of inventory object.

For this example, select **Switches**.

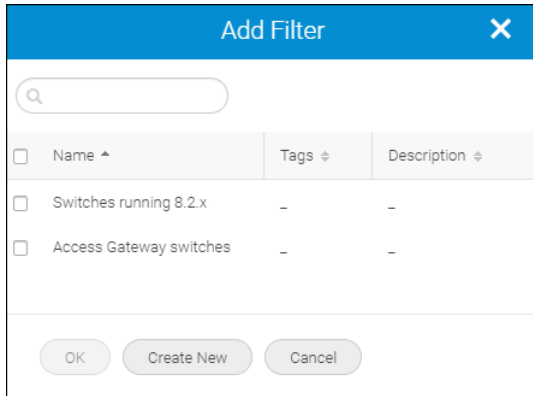


For all inventory objects other than **Chassis**, the inventory page is empty. You must add filters to determine which objects in inventory are displayed.

2. Click the **+** on the upper left to add a filter.

You can select from existing filters, or you can create a new filter.

In the following example, two switch filters have already been created and saved; however, for this example, a new filter is created.

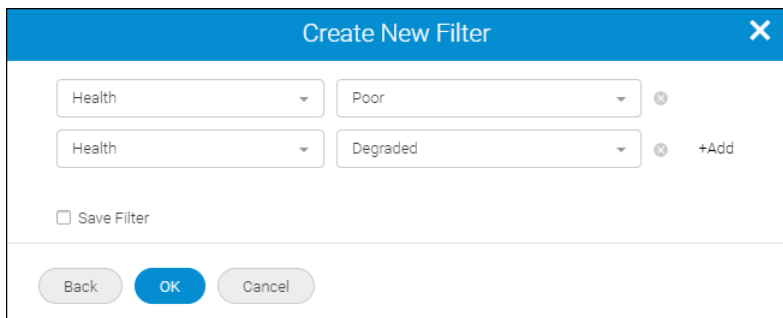


3. Click **Create New**.

4. Select the filter attribute and value.

Click **+Add** if you want to add additional attribute-value pairs.

The following filter displays all switches with poor or degraded health.



For a complete description of filters and filtering rules, see [Filters](#).

5. Select the **Save Filter** box if you want to name this filter and save it to use later.

6. Click **OK**.

The inventory page displays all switches that meet the filter criteria.

You can perform additional filtering by limiting the display to specific Management Portal instances. You can filter the columns that are displayed by clicking the hamburger icon (☰).

Dashboard & Reports Inventory Events SANnav

Switches (42)

Poor an... +Add

Poor and Degraded switches

Name	Type	FID	Fabric	Health	Model	Port Count	Portal
A_15643...	Switch	128	FabricTes...	Poor	Brocade X6-8	221	Munich DC
Alleg_195...	Switch	128	Sec_Fabri...	Degraded	Brocade X6-8	230	Munich DC
Allegianc...	Switch	128	Fabric_A	Degraded	Brocade X6-8	171	New York DC

All Portals

A convenient way to view the inventory items without filtering is to create and save a filter with a wildcard for the name. For example, the following filter displays all switches in the inventory.

Figure 34: Creating a Filter with a Wildcard

Create New Filter

Name * +Add

Save Filter

Name: All Switches Description: Display all switches, with no filtering.

Tags

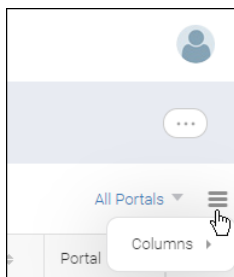
Back OK Cancel

13.11.2 Viewing Performance Measures in the Switch Port Inventory

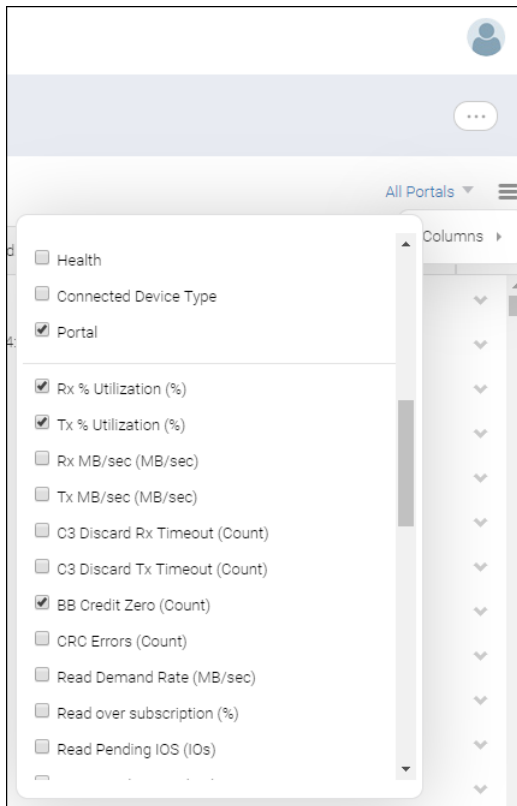
When viewing switch ports in the SANnav Global View inventory page, you can display performance measures for those ports.

The maximum number of inventory items that display at one time is 500; however, if you select any performance measure columns for switch ports, the maximum number of switch ports that displays is 100.

1. Click **Inventory** in the navigation bar, and select **Switch Ports** from the context drop-down.
2. Add a filter to display switch ports.
3. Click the hamburger icon (☰), and then click **Columns**.



4. Scroll down to the performance measures (below the line), and select the performance measures that you want to display.



5. Click anywhere outside the box to close the columns list.

The performance measure columns are added to the left side of the table, after the port name column.

Name	Rx % Utilization	Tx % Utilization	BB Credit Zero	Type	Portal
port14	17.388	7.769	0	F-Port	San Jose DC
port16_4	4.000	7.945	0	F-Port	New York DC
port16_5	3.867	8.165	0	F-Port	New York DC

13.11.3 Investigating Switch Ports in SANnav Global View


Similar to SANnav Management Portal, SANnav Global View investigation enables you to search for and investigate switch ports. The switch ports span all SANnav Management Portal instances that have been added to SANnav Global View.

Investigation mode is available for all FC protocol switch ports; for FCIP, it is available for GigE-Port type switch ports, and for Ethernet, it is available for ETH type switch ports.

Investigation mode differences between SANnav Global View and SANnav Management Portal include the following:

- In Global View, you cannot hide the measures panel.
- Global View monitoring is historical only. Real-time monitoring is unavailable.
- In Global View, you can display the following types of graphs:
 - One entity and multiple measures
 - Multiple entities and one measureYou cannot display multiple entities and multiple measures.
- In Global View, the maximum date range is the last 30 days.

The following procedure shows you how to launch investigation mode for switch ports. For additional information, see [Using Investigation Mode](#).

1. Click **Inventory** in the navigation bar, and select **Switch Ports** from the context drop-down.
2. Add a filter to display switch ports.
3. Select the ports that you want to investigate.
 - To investigate a single port, select **Investigate** from the action menu for that port.
 - To investigate multiple ports, click the More button (), and click **Bulk Select**. Select the switch ports that you want to investigate, and click **Edit > Investigate**.

The **Investigation Mode** page displays.

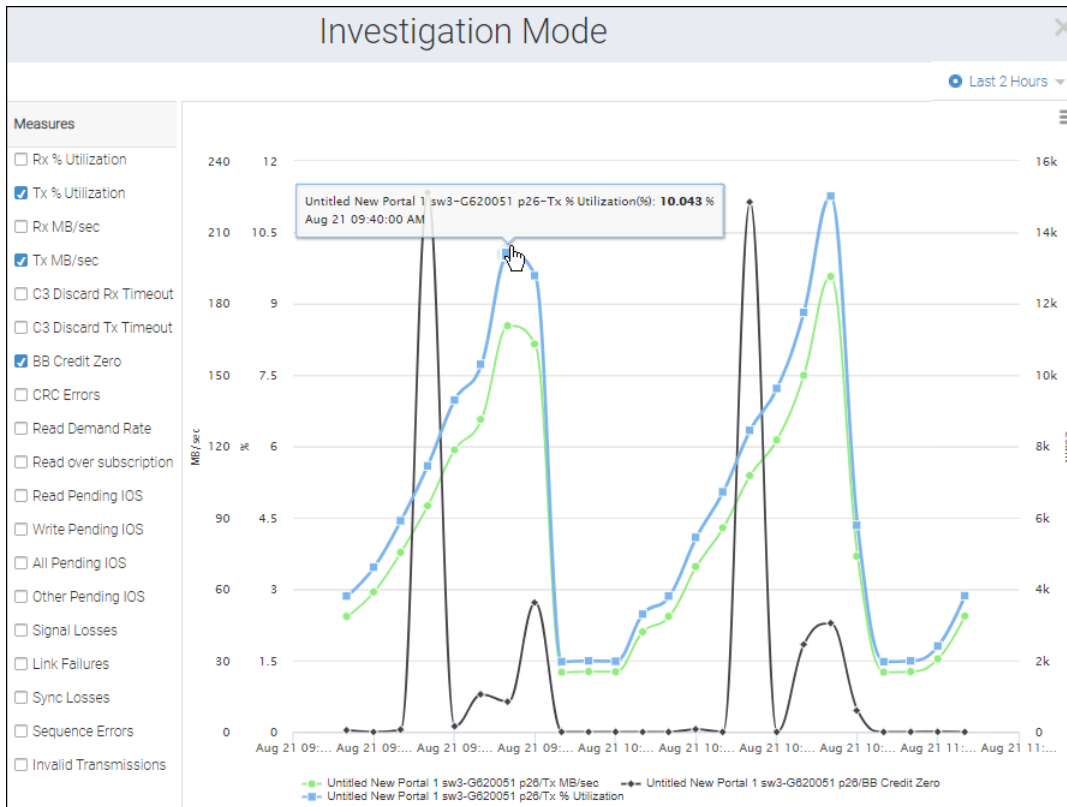
By default, this page is blank. You must select measures to obtain the related details.

4. Select the measures from the panel on the left.

If one port is selected, you can select multiple measures. If more than one port is selected, you can select only one measure.

The list of available measures depends on the selected port type.

A graph displays for the selected measures. If you hover on a point of the graph, you see the details associated with that data point.



The date/time of the graph is shown in the upper-right drop-down. By default, **Last 30 Minutes** is selected.

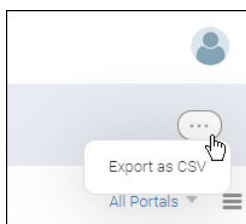
5. To change the scale of the graph, click the drop-down to display the **Select Date Range** dialog.

You can either select a predefined time interval or manually specify a date range, up to the last 30 days.

13.11.4 Exporting Inventory Views

In SANnav Global View, you can export the inventory tables to a CSV file.

1. Click **Inventory** in the navigation bar, and select the type of inventory that you want to view.
2. Add filters to display the inventory.
3. Click the More button in the upper-right corner, and select **Export as CSV**.



A CSV file is downloaded to your local machine. The file name is `export_data.csv`.

13.12 Viewing Global View Events

SANnav Global View displays application events, including those generated by user action. SANnav Global View does not display events from the SANnav Management Portal instances.

The following procedure describes how to view the events and filter them based on date range.

1. Click **Events** in the navigation bar.

By default, events recorded in the **Last 30 Minutes** are displayed, as indicated by the Date Range drop-down in the upper-right corner.

2. Click the date range drop down, and then select the range for which you want to display events.

You can select from fixed ranges on the right side of the dialog, or select custom start and end dates using the calendar.

For example, the following screen capture selects a date range from 8:00 a.m. on August 12 to 5:00 p.m. on August 16.

The screenshot shows a 'Select Date Range' dialog box with a blue header and a close button (X). It features two calendar views for July and August 2019. The date range is set from August 12, 2019, 08:00 AM to August 16, 2019, 05:00 PM. The 'Apply' button is highlighted in blue.

3. Click **Apply**.

Events for the given date range are displayed. For this example, 28 events are displayed, as indicated by the page title.

Note that if you want to see the full event message, you can widen the **Description** column, or you can hover over the truncated message to see the complete description.

The screenshot shows the 'Application Events (28)' page with a date range filter set to 'Aug 12, 2019 8:00 AM - Aug 16, 2019 5:00 PM'. The table below shows several events, with the first three rows highlighted in red.

Description	Module	Category	Username	Occurred Time
Successfully authenti...	Authentication	User Action Event	-	Aug 16, 2019 13:59:20 PDT
Successfully authenti...	Authentication	User Action Event	-	Aug 16, 2019 11:12:29 PDT
Successfully authenticated user Administrator.	Authentication	User Action Event	Administrator	Aug 16, 2019 10:47:05 PDT
New York DC Portal u...	Portals	User Action Event	Administrator	Aug 16, 2019 10:46:56 PDT

13.13 Global View Password and Lockout Policy

Having a strong password policy is a key component for secure access to SANnav. The strength of your password should depend on the security needs of your organization.

When you set up password policies in SANnav Global View, these policies apply only to the local database. If you are using an external server for authentication, these policies do not apply, and you must set up password policies on the external server. If primary authentication on the external server fails, and you fall back to secondary authentication on the local database, then the password policies defined in SANnav apply.

If you change the password policy so that the passwords of logged-in users are now in violation of the new policy, the users remain logged in, but the next time they try to log in, they get a password violation message and are prompted to change their password.

The following steps provide a guideline for creating a strong password policy. Your policy may vary.

1. Click **SANnav** in the navigation bar, and then select **Security > SANnav Password and Lockout Policy**.
2. Configure the password strength policy, as follows.

Option	Description
Minimum Length	The default minimum length is 8 characters. Longer passwords increase security dramatically. Select a minimum length of 9 or 10 characters for a stronger password policy.
Uppercase Letters Lowercase Letters Numbers Special Characters	This is the minimum number of upper- and lowercase letters, numbers, and special characters required in the password. The default value for each of these options is 0. For strong passwords, you should set each of these options to at least 1.
Maximum Repeat	Maximum Repeat specifies the maximum number of repeated characters that are allowed. For example, if Maximum Repeat is 2, then "password" is valid, but "passsword" is not. Select a value or use the default value (2).
Maximum Sequence	Maximum Sequence specifies the maximum number of sequential characters that are allowed. The sequence is based on the ASCII value of the characters and also applies to special characters. For example, if Maximum Sequence is 1, then "password1" is valid, but "password12" is not, and "passworda" is valid, but "passworde" is not (sequence "de" violates the policy). Select a value or use the default value (1). Note that if you use the default value, some common two-letter sequences (such as "hi", "st", and "no") will be disallowed in passwords.

3. Configure the password expiration and password history policies.

Option	Description
Password never expires	By default, passwords never expire. If your password policy enforces strong passwords, you might not want the passwords to expire unless security is compromised. Uncheck this box if you want passwords to automatically expire after a specific time period.
Password Age	The amount of time after which a password automatically expires. This value is between 15 days (default) and 12 months. For the most security, choose shorter values. A good value is between 45 days and 6 months.
Warning Period	The number of days prior to password expiration that a user starts getting warning messages. Select a value from 1 (default) to 15 days.
Password History	The number of previous passwords that cannot be reused. For example, if Password History is 5, users cannot reuse their most recent 5 passwords. Select a value between 1 (default) and 5. For the most security, select 5.

- Configure the account lockout and session policy.

Option	Description
Lockout After	By default, a user account is locked after three failed login attempts. You can change this to 4 or 5 failed login attempts. For the most security, keep the default (3).
Lockout Duration	A locked account automatically unlocks after the amount of time specified by Lockout Duration . Lockout duration is between 15 (default) and 60 minutes. Keep in mind that when setting the lockout duration, the higher settings might result in increased support calls, whereas lower settings might make SANnav more vulnerable to brute force attacks. For higher levels of security, select the higher settings.
Inactive Duration	By default, you are logged out after 30 minutes of inactivity. You set this value to between 15 minutes and 12 hours. If you select Keep Dashboard active after session expires , then if you are on the dashboard page and the session expires, you are not logged out. You can continue to view the dashboard, which is dynamically updated. If you move off of the dashboard page, however, you are logged out and must log in again.

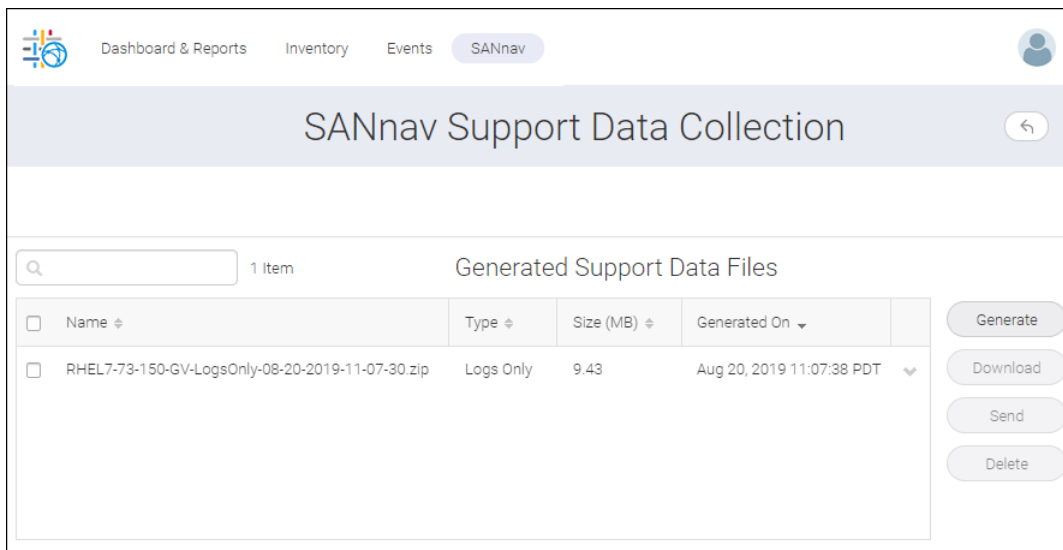
- Click **Save**.

13.14 Global View Support Data Collection

Similar to SANnav Management Portal, SANnav Global View enables you to collect support data (during a chosen time) from the SANnav Global View server for offline analysis. You can collect logs alone or logs and the database.

The following steps show how to perform SANnav Global View data collection.

- Click **SANnav** in the navigation bar, and then select **Services > SANnav Support Data Collection**.



From the **SANnav Support Data Collection** page, you can collect data, download data collection files to an offline storage, and send them to an external FTP server.

- Click **Generate** to generate support data (logs or logs and database).
- Select a data collection file and click **Download** to download the file to offline storage.
- Select a data collection file and click **Send** to forward the file to an external server.

13.15 Global View Backup

Similar to SANnav Management Portal, SANnav Global View provides support for backup. This includes all data on the Global View database, system configuration and (optionally) reports generated in the system. You can perform an on-demand backup with or without reports, as well as schedule periodic backups.

To access backup, click **SANnav** in the navigation bar, and then select **Services > SANnav Backup**.

For further details, see [SANnav Backup and Restore](#).

13.16 Global View Email Setup

Similar to SANnav Management Portal, SANnav Global View enables you to configure the email server, which the system can then use to send an email notification during report generation if you elect to do so.

1. Click **SANnav** in the navigation bar, and then select **Services > SANnav Email Setup**.

The **SANnav Email Setup** dialog displays.

2. Enter the email server in the **Email Server** field.

3. Select an option from the **Security** list.

If you select **Use SSL** or **Use TLS**, you must also provide the SMTP ID and password.

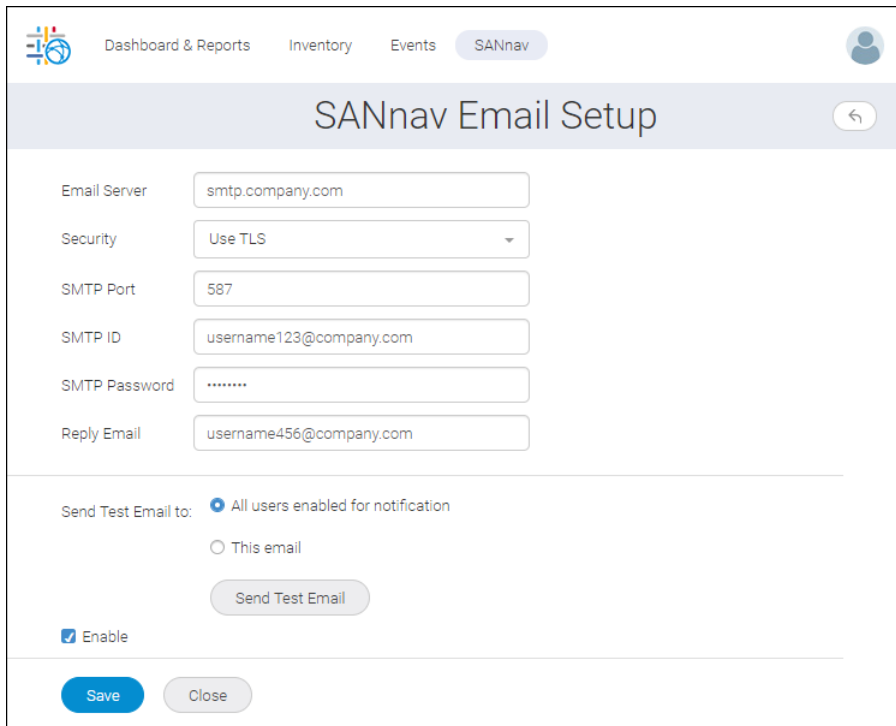
4. Enter the email address in the **Reply Email** field.

The **Reply Email** is the email address to which reply notifications are sent.

5. To send a test email, select either of the following options:

- The **All users enabled for notification** option is used to send a test email notification to all the application users who have a valid email ID configured in the **Users** page.
- The **This email** option is used to specify the list of users who must receive the test email notification. When you select this option, a field appears to specify the email IDs.

If you have more than one email ID to set up, separate the email IDs with a comma (and no space).



The screenshot shows the SANnav Email Setup configuration page. The page has a navigation bar at the top with links for Dashboard & Reports, Inventory, Events, and SANnav. The main heading is "SANnav Email Setup". The configuration fields are as follows:

Email Server	smtp.company.com
Security	Use TLS
SMTP Port	587
SMTP ID	username123@company.com
SMTP Password
Reply Email	username456@company.com

Below the fields, there is a "Send Test Email to:" section with two radio buttons: "All users enabled for notification" (selected) and "This email". A "Send Test Email" button is located below these options. At the bottom left, there is an "Enable" checkbox which is checked. At the very bottom, there are "Save" and "Close" buttons.

6. Click **Send Test Email**.
7. Click the **Enable** checkbox to activate the email configuration.
8. Click **Save** to save the email setup.

Exporting Select Configurations from Brocade Network Advisor to SANnav Management Portal

14.1 Overview of Exporting Select Configurations

This chapter provides instructions for moving select Brocade Network Advisor configurations to SANnav Management Portal. You can import the following select configurations from Network Advisor:

- You can export user-defined device and device port (HBA or storage) names from Brocade Network Advisor to a CSV file. You can then import the names into SANnav Management Portal to use them as Zone Alias Names.
- You can export Host port mapping from Brocade Network Advisor to a CSV file. You can then import the Host port mapping into SANnav Management Portal.
- You can export storage port mapping from Brocade Network Advisor to a CSV file. You can then import the storage port mapping into SANnav Management Portal.
- You can export MAPS policy from Brocade Network Advisor to an xml file format. You can then import the MAPS policy into SANnav Management Portal.

14.2 Exporting End Device Names

Use the `exportdeviceportnames` batch script to extract user-defined device and device port (HBA or storage) names from Brocade Network Advisor to a CSV file. You can then import the names into SANnav Management Portal to use them as Zone Alias Names.

1. Copy the `export_device_port_names` ZIP file in the `Network_Advisor_Home` directory.
Contact your vendor to obtain the batch script file.
2. Extract the export device port names ZIP file in the `Network_Advisor_Home` directory.
 - Make sure that the `exportdeviceportnames.sh` file is present inside `Network_Advisor_Home\bin`.
 - Make sure that the `ExportDevicePortNames.jar` file is present inside `Network_Advisor_Home\lib`.
3. Open a command prompt and navigate to the `Network_Advisor_Home\bin` directory.
4. Type `exportdeviceportnames` and press **Enter**.

The batch script collects the Fabric details for each Fabric present in the Brocade Network Advisor database. For each Fabric that contains user-defined names, the batch script creates two Names files (one listing valid names and the other listing invalid names) and a log file. If a Fabric does not contain user-defined names, the batch script does not create the Names files; however the log file is generated and states there are no user-defined names.

The Names files are created in the `Network_Advisor_Home\temp\ExportDevicePortNames` directory. These files use the following naming format: `FabricName_SeedSwitchWWN_ValidNameList.csv` and `FabricName_SeedSwitchWWN_InvalidNameList.csv`. The Log file is created in the `Network_Advisor_Home/logs/export_device_port_names.log`.

14.3 Importing End Device Names as Zone Aliases

You can import end device names exported from Brocade Network Advisor into SANnav Management Portal to use them as zone alias names.

1. Click **Zoning** in the navigation bar, and then select the **Zone Aliases** tab.
2. Select the fabric from the **Select Fabric** drop-down at the top-right corner.

3. Select the fabric in which you want to import zones and click **OK**.
 4. Click the add button (+) at the top-right corner and select **Import**.
 5. If conflicts arise during the import, choose one of the following options:
 - Select the **Accept all changes** option to accept all changes from the imported file and overwrite the zone alias names in the fabric.
 - Select the **Reject all changes** option to reject only the conflicts from the imported file.
 - Select the **Resolve the changes** option to allow you to fix from the conflicts.
 6. Click **OK**.
 7. Resolve any naming conflicts.
 - Accept the new zone alias name by selecting the changes you want to keep and clicking **Accept**.
 - Reject the new zone alias name by selecting the changes you want to reject and clicking **Remove**.
- When all changes are resolved, click **OK**.

14.4 Exporting Host or Storage Port Mapping

Use the `Export_port_Mapping` script to extract host port and storage port mapping to a CSV file. You can then import this mapping into SANnav Management Portal.

1. Copy the `Export_port_mapping` ZIP file in the `Network_Advisor_Home` directory.
Contact your vendor to obtain the batch script file.
2. Extract the `Export_port_mapping` ZIP file in the `Network_Advisor_Home` directory.
Make sure that the `Export_port_Mapping.sh` file is present inside `Network_Advisor_Home\bin`. If the `Export_port_Mapping.sh` file is not in the `Network_Advisor_Home\bin` directory, then move it there manually after extracting the ZIP file.
3. Open a command prompt and navigate to the `Network_Advisor_Home\bin` directory.
4. Type the following command and press **Enter**.

```
Export_port_Mapping dbusername dbpassword absolutefilepath
```

The `absolutefilepath` denotes the file location in which to export the generated CSV file, and must include a file name with a `.csv` extension. The file path should be an absolute path, not a relative path.
Make sure that you have full read and write permissions to the `absolutefilepath` directory; otherwise, the script cannot export the data to the required file.

The script exports the storage and host port mapping to the designated CSV file, which contains port WWN, port FC address, Host/Storage name, and port type. A log file is created in `Network_Advisor_Home/logs/Export_port_Mapping.log`.

14.5 Importing Host or Storage Port Mapping

In SANnav Management Portal, you can import a list of host or storage port mappings from a comma-separated values (CSV file).

1. Click **SANnav** in the navigation bar, and then select **SAN Configuration > Inventory Name and Mapping Management**.
2. Select the **Import Mapping** option, and click **Browse** to browse to the file location.

3. Click **Import**.

If the mapping already exists, the import fails.

14.6 Exporting a MAPS Policy


Using Brocade Network Advisor you can export a MAPS policy to an xml file format.

1. Right-click a device in the Product List or Connectivity Map and select **Fabric Vision > MAPS > Configure**. The **MAPS Configuration** dialog displays.
2. Select the policy you want to export in the list and click **Export**.
3. Browse to the location you want to save the policy and click **Save**.
4. Repeat step 1 through step 3 for each MAPS policy you want to export.
5. Click **Close** on the **MAPS Configuration** dialog.

14.7 Importing MAPS Policies

You can import a policy to a switch. The policy file must be in JSON file format or XML file format.

You can import a policy with the same name. When you import a policy with the same name, a warning message displays to accept all changes or reject all changes and continue with the import function.

1. Click **SANnav** in the navigation bar, and then select **SAN Monitoring > MAPS Policy Management**.
2. In the **Switches** tab, click the down-arrow () for the switch to which you want to import the policy, and select **View Policies**.
3. Click the add button (+) at the top-right corner of the **Policies** page, and select **Import**.
4. Browse to the location of the policy that you want to import, and click **Open**.
You cannot import policies at the SAN or fabric level.

SANnav REST API Overview

Overview of the SANnav REST API

SANnav Management Portal supports an application programming interface (API) for managing Brocade storage area network (SAN) fabrics.

NOTE

The REST API does not support SANnav Global View.

Note that the content in this section is an overview of the SANnav REST API and does not contain a complete list of the REST API features. This section does not include examples for all REST API features. For a complete list of the SANnav REST API features and descriptions, refer to the *SANnav Management Portal REST API Reference Manual*.

HTTPS Protocol Support

The SANnav REST API supports the HTTPS protocol. The default HTTPS port number is 443.

To use HTTPS protocol, a valid security certificate must be installed on the server before beginning REST operations. SANnav installs with a self-signed certificate. The SANnav certificate files are located in the *Install_Home/conf/nginx* directory on the SANnav server.

15.1 Overall Strategy for the SANnav Management Portal REST API

The SANnav REST API provides functionality that is not available in the Fabric OS REST APIs.

What SANnav Provides

The SANnav REST API includes support for the following SANnav features:

- List fabrics managed by the SANnav server
- List the seed and principal switch data for each fabric
- List switches (members) in the fabric
- Display FCR topology information for routing topologies such as edge-to-edge, backbone-to-edge, and edge-to-backbone
- Event forwarding configuration
- Acknowledge or unacknowledge events
- Display a list of filtered events
- Inventory search

15.2 Using the SANnav Management Portal REST API

Before You Begin

Before you can use the SANnav REST API, you must obtain a user name and password authorized to access the SANnav server through the SANnav REST API.

To use the recommended HTTPS protocol, a valid security certificate must be installed on the server before beginning REST operations. SANnav installs with a self-signed certificate. The SANnav certificate files are located in the *Install_Home/conf/nginx* directory on the SANnav server.

Session Authorization Key

To log in to a SANnav server, you must provide a valid SANnav user name and password through an authorization header in a POST login request. If the authentication is successful, SANnav returns the session ID in the body (for example: "sessionId": "dd903934-f4d7-4eee-b05f-a7d2f48a733c"). Subsequent SANnav REST API operations must include this session ID in the request authorization header. The client applications use this token to obtain further access to the server using the persistent connection.

15.3 SANnav Management Portal Examples

This section provides a few examples for using the SANnav REST API modules.

15.3.1 Logging In and Out

The following items should be kept in mind when logging in and out of the SANnav REST API.

To log in to SANnav, you must provide a valid user name and password through an authorization header in a `POST https://<host>/external-api/v1/login/` request. If the authentication is successful, SANnav returns the session ID in the body (for example: "sessionId": "dd903934-f4d7-4eee-b05f-a7d2f48a733c"). Subsequent SANnav REST API operations must include this session ID in the request authorization header. The client applications use this token to obtain further access to the server using the persistent connection.

Examples

Here is a login statement.

```
POST https://10.10.10.10/external-api/v1/login/
```

URI Headers

You must include the following keys and values in the headers.

- username = guest
- password = guest
- Content-Type = application/json

URI Request

```
POST https://10.10.10.10/external-api/v1/login/
```

Request Body

There is no request body; however, you must provide a valid user name and password (such as, guest / guest) through an authorization header.

Response Data

```
{  
  "sessionId": "dd903934-f4d7-4eee-b05f-a7d2f48a733c"  
}
```

If authentication is successful, a session ID key (for example, "sessionId": "dd903934-f4d7-4eee-b05f-a7d2f48a733c") is returned to the client in the response body. Subsequent SANnav REST API operations must include this session ID in the request authorization header. The client applications use this token to obtain further access to the server using the persistent connection.

To log out from SANnav, close the session using a `POST https://<host>/external-api/v1/logout/` request. You must include the session ID in the request authorization header. The SANnav address can be in the form of either an IPv4 or IPv6 address or a host:port ID.

Examples

Here is a logout statement.

```
POST https://10.10.10.10/external-api/v1/logout/
```

URI Headers

You must include the following keys and values in the header.

- Authorization = Session ID
- Content-Type = application/json

URI Request

```
POST https://10.10.10.10/external-api/v1/logout/
```

Request Body

There is no request body; however, you must include the session ID key in the request authorization header.

Response Data

```
{
  "ResponseCode": "AUTHENTICATION_2012",
  "ResponseId": "authentication.logout.success",
  "ResponseMessage": "User logout success"
}
```

15.3.2 Discovery Module

The Discovery module is used to retrieve information about the fabrics managed by the SANnav server as well as the seed and principal switch data for each fabric. You can also retrieve a list of switches (members) in the fabric.

Version History

This API call was introduced in SANnav Management Portal 1.1.0.

Examples

Retrieving a List of Fabrics in Your AOR

The following example uses a GET request to retrieve a list of fabrics in your Area Of Responsibility (AOR).

Request Headers

- Authorization = Session ID (authorization key from the login API response data)
- Accept = application/json
- Content-Type = application/json

URI Structure

```
GET https://<host>/external-api/v1/discovery/fabrics/
```

Request URI

```
GET https://10.10.10.10/external-api/v1/discovery/fabrics/
```

Request Body

There is no request body.

Response Data

When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```
{
  "Fabrics": [
    {
      "name": "DevDontDisturb",
      "description": "",
      "seedSwitchName": "Sw00abcdvs123311122rr1SS",
      "seedSwitchIPAddress": "10.102.16.23",
      "seedSwitchWwn": "10:00:50:EB:1A:FD:A5:BD",
      "principalSwitchIPAddress": "10.102.16.23",
      "principalSwitchWwn": "10:00:50:EB:1A:FD:A5:BD"
    }
  ]
}
```

Retrieving a List of Members in the Fabric

The following example uses a GET request to retrieve a list of switches (members) in the fabric.

Request Headers

- Authorization = Session ID (authorization key from the login API response data)
- Accept = application/json
- Content-Type = application/json

URI Structure

GET https://<host>/external-api/v1/discovery/fabric-members/?principalSwitchWWN={principal switch wwn}

Request URI

```
GET https://10.10.10.10/external-api/v1/discovery/fabric-members/?principalSwitchWWN=10:00:00:05:1E:75:AF:00
```

Request Body

There is no request body.

Response Data

When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```
{
  "Switches": [
    {
      "name": "sw0sw0sw0sw022334",
      "ipAddress": "10.102.16.24",
      "physicalSwitchWwn": "10:00:50:EB:1A:FE:00:DF",
      "firmwareVersion": "v8.2.1_bld44",
      "virtualSwitchWwn": "10:00:50:EB:1A:FE:00:C0",
      "model": "2",
      "modelName": "Brocade X6-8",
    }
  ]
}
```

```

    "switchMode": "2",
    "role": "Unknown",
    "state": "Online",
    "status": "3"
  },
  {
    "name": "Sw00abcdvs123311122rr1SS",
    "ipAddress": "10.102.16.23",
    "physicalSwitchWwn": "10:00:50:EB:1A:FD:A5:DC",
    "firmwareVersion": "v8.2.1_bld44",
    "virtualSwitchWwn": "10:00:50:EB:1A:FD:A5:BD",
    "reachable": "0",
    "model": "2",
    "modelName": "Brocade X6-8",
    "switchMode": "0",
    "role": "Primary",
    "state": "Online",
    "status": "0"
  },
  {
    "name": "Sw00Sw00224",
    "ipAddress": "10.102.16.25",
    "physicalSwitchWwn": "10:00:50:EB:1A:FD:D7:BD",
    "firmwareVersion": "v8.2.1_bld29",
    "virtualSwitchWwn": "10:00:50:EB:1A:FD:D7:BD",
    "model": "2",
    "modelName": "Brocade X6-8",
    "switchMode": "2",
    "role": "Unknown",
    "state": "Online",
    "status": "3"
  }
]
}

```

15.3.3 FCR Module

The FCR module is used to retrieve FCR topology information for routing topologies (edge-to-edge, backbone-to-edge, and edge-to-backbone) and the relationship to front domain and translate domain.

Version History

This API call was introduced in SANnav Management Portal 1.1.0

Examples

Retrieving the FCR Topology

The following example uses a GET request to retrieve the FCR topology.

Request Headers

- Authorization = Session ID (authorization key from the login API response data)
- Accept = application/json
- Content-Type = application/json

URI Structure

GET https://<host>/external-api/v1/fcr/topology/

Request URI

```
GET https://10.10.10.10/external-api/v1/fcr/topology/
```

Request Body

There is no request body.

Response Data

When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```
{
  "topology": [
    {
      "backboneFabricID": 70,
      "backboneSwitch": [
        {
          "backboneIPAddress": "10.102.18.11",
          "backboneSwitchWwn": "10:00:88:94:71:16:36:01",
          "EdgeFabric": [
            {
              "exPortWwn": "20:2F:88:94:71:16:36:01",
              "edgeFCRFabricID": 27,
              "edgeIPAddress": "10.102.18.148",
              "edgeSwitchWwn": "10:00:C4:F5:7C:16:50:E5",
              "edgePortWwn": "20:04:C4:F5:7C:16:50:E5",
              "frontDomainId": 160,
              "translateDomainId": [
                200
              ],
            },
            {
              "exPortWwn": "20:29:88:94:71:16:36:01",
              "edgeFCRFabricID": 15,
              "edgeIPAddress": "10.102.18.147",
              "edgeSwitchWwn": "10:00:C4:F5:7C:16:51:A5",
              "edgePortWwn": "20:29:C4:F5:7C:16:51:A5",
              "frontDomainId": 160,
              "translateDomainId": [
                200,
                201,
                202,
                203,
                204,
              ],
            }
          ]
        }
      ]
    }
  ]
}
```


When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```
{
  "code": 200,
  "message": "Event details updated successfully."
}
```

Unacknowledging an Event

The following example uses a POST request to unacknowledge an event.

Request Headers

- Authorization = Session ID (authorization key from the login API response data)
- Accept = application/json
- Content-Type = application/json

URI Structure

POST https://<host>/external-api/v1/fault/events/unacknowledge

Request URI

POST https://10.10.10.10/external-api/v1/fault/events/unacknowledge

Request Body

```
{
  "eventIdentifiers": [
    "c0f695a7-066d-4c55-b695-a7066dec5554"
  ],
  "eventNotes": "Need to update the Administrator and take appropriate action."
}
```

Response Data

When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```
{
  "code": 200,
  "message": "Event details updated successfully."
}
```

Subscribing to SAN Events

The following example uses a POST request to create a SANnav Management Portal event recipient.

Request Headers

- Authorization = Session ID (authorization key from the login API response data)
- Accept = application/json
- Content-Type = application/json

URI Structure

POST https://<host>/external-api/v1/fault/events/forwarding/subscribe

Request URI

POST `https://10.10.10.10/external-api/v1/fault/events/forwarding/subscribe`

Request Body

```
{
  "forwardApplicationEvents": true,
  "forwardCorrelatedEvents": true,
  "includeSourceAddress": true,
  "port": 162,
  "products": [],
  "recipientAddress": "10.155.41.52",
  "recipientType": "SNMP",
  "severityLevel": "Info",
  "trapOid": []
}
```

Response Data

When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```
{
  "code": 200,
  "message": "Forwarding Target added Successfully"
}
```

Unsubscribing to SAN Events

The following example uses a POST request to unsubscribe a SANnav Management Portal event recipient.

Request Headers

- Authorization = Session ID (authorization key from the login API response data)
- Accept = application/json
- Content-Type = application/json

URI Structure

POST `https://<host>/external-api/v1/fault/events/forwarding/unsubscribe`

Request URI

POST `https://10.10.10.10/external-api/v1/fault/events/forwarding/unsubscribe`

Request Body

```
{
  "port": 162,
  "recipientAddress": "10.155.41.52",
  "recipientType": "SNMP"
}
```

Response Data

When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```
{
  "code": 200,
  "message": "Deleted the Target Successfully"
}
```

Retrieving a Filtered List of Events

The following example uses a POST request to retrieve a list of events based on filter criteria.

Request Headers

- Authorization = Session ID (authorization key from the login API response data)
- Accept = application/json
- Content-Type = application/json

URI Structure

POST <https://<host>/external-api/v1/fault/events/>

Request URI

POST <https://10.10.10.10/external-api/v1/fault/events/>

Request Body

```
{
  "endTime": 1537269900000,
  "eventProductDetails": [],
  "filters": {
    "filter": [
      {
        "categories": {
          "correlationEvent": [],
          "linkIncidentEvent": [],
          "managementServerEvent": [
            "Emergency", "Alert", "Error", "Info"
          ],
          "productAuditEvent": [
            "Emergency", "Alert", "Error", "Info"
          ],
          "productEvent": [
            "Emergency", "Alert", "Error", "Info"
          ],
          "productStatusEvent": [
            "Info"
          ],
          "securityEvent": [
            "Emergency", "Alert", "Error"
          ],
          "userActionEvent": [
            "Emergency", "Alert", "Error", "Info"
          ]
        }
      ]
    ]
  },
}
```

```

        "excludedEvents": [],
        "includedEvents": [
            {
                "category": "ALL",
                "eventColumn": "ACKNOWLEDGED",
                "value": "No"
            }
        ]
    }
}
],
"pageSize": 100,
"startIndex": 0,
"startTime": 1537266600000
}

```

Response Data

When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```

{
  "events": [
    {
      "eventID": "9521d239-78ac-4a78-a1d2-3978ac8a7811",
      "severity": "Error",
      "sourceName": "rhel74_34186",
      "sourceAddress": "10.124.72.36",
      "lastOccurrenceHostTime": 1538130213556,
      "firstOccurrenceHostTime": 1538130213556,
      "origin": "Application Event",
      "eventCategory": "Management Server Event",
      "description": "Failed to register SNMP(trap) for the switch 10.155.34.16. The Trap Recipient table is
full.",
      "correlatedEventIDs": "",
      "recommendedActions": "",
      "probableCause": "",
      "messageId": "SSMP-EVNT-2002",
      "ruleName": "",
      "rulePolicy": "",
      "ackNotes": "",
      "ackBy": "",
      "sourceType": "OTHERS"
    }
  ],
  "eventSeverityGroupSummaryList": [
    {
      "severityGroup": "ERROR",
      "counter": 59
    },
    {
      "severityGroup": "INFO",
      "counter": 2
    }
  ],
}

```

```

{
  "severityGroup": "ALERT"
}
],
"startIndex": 0,
"pageSize": 100,
"totalRecords": 61,
"nextPageIndex": "3a42ff68-c588-417f-82ff-68c588617fa3,1538126737459"
}

```

15.3.5 Inventory Search Module

The Inventory Search module is used to search the SANnav inventory database with flexible query parameters. The Inventory Search module supports wildcard characters in the search.

The Inventory Search module uses the following URI structure and input parameters to search the SANnav inventory database.

URI Structure

GET https://<hostname>/external-api/v1/inventory/search/?
objecttype=<object_type>&searchparam=<parameter_name>&value=<any_string>&parentid=<switch_WWN>

The objecttype parameter accepts the following values:

- Switch
- SwitchPort (Note that SwitchPort requires an additional parameter (parentId) to return the correct value. The parentId parameter is the switch WWN. The parentId parameter is optional.)
- Device
- DevicePort
- ZoneAlias

The searchparam parameter accepts the following values based on the specified objecttype parameter:

- Switch. Valid values include: switchWWN (switch WWN) or serialnumber (Brocade and OEM serial numbers)
- SwitchPort. Valid values include: switchportWWN (switch port WWN), switchportname (switch port name), portfcid (fc address), and macaddress.
- Device. Valid values include: deviceNodeWWN (device node WWN)
- DevicePort. Valid values include: deviceportWWN (device port WWN)
- ZoneAlias. Valid values include: deviceNodeWWN (device node WWN), deviceportWWN (device port WWN)

Version History

This API call was introduced in SANnav Management Portal 2.0.0

Examples

Searching for a Switch by Switch WWN

The following example uses a GET request to search for a switch using the switch WWN.

Request Headers

- Authorization = Session ID (authorization key from the login API response data)

URI Structure

GET https://<hostname>/external-api/v1/inventory/search/?
objecttype=Switch&searchparam=switchWWN&value=<switch_WWN>

Request URI

```
GET https://10.10.10.10/external-api/v1/inventory/search/?  
objecttype=Switch&searchparam=switchWWN&value=10:00:00:10:F1:F2:11:01
```

Request Body

There is no request body.

Response Data

When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```
{  
  "searchQuery": "10:00:00:27:F8:F4:13:01",  
  "inventory": [  
    {  
      "switch": "BASE_FID3_148",  
      "searchResult": "10:00:00:27:F8:F4:13:01",  
      "principleSwitchWwn": "10:00:00:05:1E:B7:85:01",  
      "switchIPAddress": "10.124.71.148",  
      "switchWwn": "10:00:00:27:F8:F4:13:01",  
      "seedSwitchWwn": "10:00:C4:F5:7C:B9:48:2E",  
      "vfId": "3",  
      "fabric": "ST_BASE"  
    }  
  ]  
}
```

Searching for a Switch by Serial Number

The following example uses a GET request to search for a switch using the serial number

Request Headers

- Authorization = Session ID (authorization key from the login API response data)

URI Structure

https://<hostname>/external-api/v1/inventory/search/?
objecttype=Switch&searchparam=serialnumber&value=<serial_number>

Request URI

```
GET https://10.102.16.202/external-api/v1/inventory/search/?  
objecttype=Switch&searchparam=serialnumber&value=ANN0609F01K
```

Request Body

There is no request body.

Response Data

When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```
{
  "searchQuery": "ANN0609F01K",
  "inventory": [
    {
      "switch": "BASE_FID3_155",
      "searchResult": "ANN0609F01K",
      "principleSwitchWwn": "10:00:00:05:1E:B7:85:01",
      "switchIPAddress": "10.124.71.155",
      "switchWwn": "10:00:00:05:1E:E3:24:01",
      "seedSwitchWwn": "10:00:C4:F5:7C:B9:48:2E",
      "vfId": "3",
      "fabric": "ST_BASE"
    }
  ]
}
```

Searching for a Switch Port by the WWN of the Switch Port

The following example uses a GET request to search for a switch using the WWN of the switch port.

Request Headers

- Authorization = Session ID (authorization key from the login API response data)

URI Structure

```
https://<hostname>/external-api/v1/inventory/search/?
objecttype=Switch&searchparam=SwitchPortWWN&value=<switch_port_WWN>
```

Request URI

```
GET https://10.10.10.10/external-api/v1/inventory/search/?
objecttype=SwitchPort&searchparam=SwitchPortWWN&value=20:15:50:EB:1A:D0:50:00
```

Request Body

There is no request body.

Response Data

When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```
{
  "searchQuery": "20:15:50:EB:1A:D0:50:00",
  "inventory": [
    {
      "switch": "Allegiance_128",
      "searchResult": "20:15:50:EB:1A:D0:50:00",
      "principleSwitchWwn": "",
      "switchIPAddress": "",
      "switchWwn": "10:00:50:EB:1A:D0:50:FF",
      "seedSwitchWwn": "",
      "vfId": "128",
    }
  ]
}
```

```

        "fabric": "new"
    }
]
}

```

Searching for a Switch Port by Switch Port Name

The following example uses a GET request to search for a switch using the name of the switch port.

Request Headers

- Authorization = Session ID (authorization key from the login API response data)

URI Structure

```

https://<hostname>/external-api/v1/inventory/search/?
objecttype=Switch&searchparam=SwitchPortWWN&value=<switch_port_name>

```

Request URI

```

GET https://10.10.10.10/external-api/v1/inventory/search/?
objecttype=SwitchPort&searchparam=SwitchPortName&value=slot4 port5

```

Request Body

There is no request body.

Response Data

When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```

{
  "searchQuery": "slot4 port5",
  "inventory": [
    { "switch": "Allegiance_128",
      "searchResult": "slot4 port5",
      "principleSwitchWwn": "",
      "switchIPAddress": "",
      "switchWwn": "10:00:50:EB:1A:D0:50:FF",
      "seedSwitchWwn": "",
      "vfId": "128",
      "fabric": "new"
    }
  ]
}

```

Searching for a Switch by Device Node WWN

The following example uses a GET request to search for a switch using the device node WWN.

Request Headers

- Authorization = Session ID (authorization key from the login API response data)

URI Structure

```

GET https://<hostname>/external-api/v1/inventory/search/?
objecttype=Switch&searchparam=DeviceNODEWWN&value=<device_node_WWN>

```

Request URI

```
GET https://10.10.10.10/external-api/v1/inventory/search/?
objecttype=Device&searchparam=DeviceNodeWWN&value=20:05:00:11:0D:5B:01:00
```

Request Body

There is no request body.

Response Data

When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```
{
  "searchQuery": "20:05:00:11:0D:5B:01:00",
  "inventory": [
    {
      "switch": "Allegiance_128",
      "searchResult": "20:05:00:11:0D:5B:01:00",
      "principleSwitchWwn": "10:00:50:EB:1A:D0:50:00",
      "switchIPAddress": "11.11.11.11",
      "switchWwn": "10:00:50:EB:1A:D0:50:00",
      "seedSwitchWwn": "10:00:50:EB:1A:D0:50:00",
      "vfId": "128",
      "fabric": "new"
    }
  ]
}
```

Searching for a Switch by Device Port WWN

The following example uses a GET request to search for a switch using the device port WWN.

Request Headers

- Authorization = Session ID (authorization key from the login API response data)

URI Structure

```
GET https://<hostname>/external-api/v1/inventory/search/?
objecttype=Switch&searchparam=DevicePortWWN&value=<device_port_WWN>
```

Request URI

```
GET https://10.10.10.10/external-api/v1/inventory/search/?
objecttype=DevicePort&searchparam=DevicePortWWN&value=20:05:00:11:0D:5B:01:08
```

Request Body

There is no request body.

Response Data

When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```
{
  "searchQuery": "20:05:00:11:0D:5B:01:08",
  "inventory": [
```

```

    {
      "switch": "Allegiance_128",
      "searchResult": "20:05:00:11:0D:5B:01:08",
      "principleSwitchWwn": "10:00:50:EB:1A:D0:50:00",
      "switchIPAddress": "11.11.11.11",
      "switchWwn": "10:00:50:EB:1A:D0:50:00",
      "seedSwitchWwn": "10:00:50:EB:1A:D0:50:00",
      "vfId": "128",
      "fabric": "new"
    }
  ]
}

```

Searching for a Zone Alias by Device Node WWN

The following example uses a GET request to search for a zone alias using a device node WWN in the zone alias.

Request Headers

- Authorization = Session ID (authorization key from the login API response data)

URI Structure

```
GET https://<hostname>/external-api/v1/inventory/search/?
objecttype=ZoneAlias&searchparam=DeviceNODEWWN&value=<device_node_WWN>
```

Request URI

```
GET https://10.10.10.10/external-api/v1/inventory/search/?
objecttype=ZoneAlias&searchparam=DeviceNodeWWN&value=20:03:00:11:0D:BC:5F:00
```

Request Body

There is no request body.

Response Data

When the operation is successful, the response has a message body similar to the following, and a "200 OK" status in the headers.

```

{
  "searchQuery": "20:03:00:11:0D:BC:5F:00",
  "inventory": [
    {
      "switch": "SW6510",
      "searchResult": "test_target",
      "principleSwitchWwn": "10:00:00:05:33:8C:0D:DC",
      "switchIPAddress": "11.11.11.11",
      "switchWwn": "10:00:50:EB:1A:36:F0:07",
      "seedSwitchWwn": "10:00:00:05:33:8C:0D:DC",
      "vfId": "128",
      "fabric": "Fab81*"
    }
  ]
}

```

Searching for a Zone Alias by Device Port WWN

The following example uses a GET request to search for a zone alias using a device port WWN in the zone alias.

Request Headers

- Authorization = Session ID (authorization key from the login API response data)

URI Structure

GET https://<hostname>/external-api/v1/inventory/search/?
objecttype=ZoneAlias&searchparam=DevicePortWWN&value=<device_port_WWN>

Request URI

```
GET https://10.10.10.10/external-api/v1/inventory/search/?  
objecttype=ZoneAlias&searchparam=DevicePortWWN&value=20:03:00:11:0D:BC:5F:00
```

Request Body

There is no request body.

Response Data

When the operation is successful, the response has a message body similar to the following, and a “200 OK” status in the headers.

```
{  
  "searchQuery": "20:03:00:11:0D:BC:5F:00",  
  "inventory": [  
    {  
      "switch": "SW6510",  
      "searchResult": "test_target",  
      "principleSwitchWwn": "10:00:00:05:33:8C:0D:DC",  
      "switchIPAddress": "11.11.11.11",  
      "switchWwn": "10:00:50:EB:1A:36:F0:07",  
      "seedSwitchWwn": "10:00:00:05:33:8C:0D:DC",  
      "vfId": "128",  
      "fabric": "Fab81*"  
    }  
  ]  
}
```

Revision History

SANnav-200-UG100; 26 September 2019

- Updated screen captures and instructions throughout to reflect the user interface design and navigation changes:
 - The main navigation bar moves from the left side to the top of the page. Navigation links are changed from icons to text.
 - The search box is changed to a magnifying glass icon that expands when you click it. Search now includes the "page content" category to allow searches on the current page content.
 - A new sidebar replaces the collection bucket for selecting items to investigate.
 - The **Configurations and Settings** page layout is different. This page is accessed by clicking **SANnav** in the navigation bar.
 - On the **Dashboard & Reports** page, the **Content** tab has been replaced with **Templates**.
 - On the **Inventory** page, the **Connections** tab has been changed to a drop-down list that includes **ISL Trunks** and **Extension Tunnels**.
 - The **Preferences** page has been moved from the navigation bar to a profile icon in the upper-right side of the page.
 - The **Logout** link has been moved from the lower-left side of the page to the profile icon in the upper-right side of the page.
 - In inventory and events tables, you can rearrange the order in which the columns are displayed.
- Automatic license renewal is supported. SANnav can automatically retrieve and activate renewed licenses.
- The "Installation" chapter has the following changes:
 - Added information about migrating from SANnav 1.1.1x to SANnav 2.0.0. The title of this chapter is changed to "Installation and Migration."
 - Port 22 can now be customized during installation.
 - Automatic license renewal is a new installation option.
 - RHEL and CentOS versions 7.6 and 7.7 are now supported.
- The "Security" chapter includes the following changes:
 - The user name is restricted to a maximum of 63 characters.
 - When assigning roles and AORs to LDAP groups, you can select one or more groups for SANnav to fetch, instead of SANnav automatically fetching all groups in the LDAP server.
- The "Monitoring" chapter includes the following changes:
 - Added behavior of SANnav if you try to discover switches that have reached end of support (EOS).
 - A new default dashboard is added: **Extension Dashboard**.
 - You can now export and import dashboard and report templates.
 - The score for factors that contribute to the overall health score for fabrics, switches, hosts, and storage can now be customized.
 - The following widgets have been added for reports:

- Chassis
- Time Series - Flow Collection (aggregated)
- Time Series - Flow Violations
- Top Collection Aggregation
- Top Flow Violations
- Top Host Port Pending IOs
- Top Host Port Read Oversubscription
- Top SCSI Errors
- Top Storage Port First Response Time
- Top Storage Port IOPS
- Top Storage Port Pending IOs
- The following status widgets have been added for dashboards:
 - Host Port Out Of Range Violations
 - ISL Port Out Of Range Violations
 - Storage Port Out Of Range Violations
- Performance monitoring can now be done on multiple measures and multiple nodes.
- The **Inventory** page includes an option to view the physical chassis. When you put a switch in maintenance mode, you now set this from the chassis details page instead of the switch details page.
- Decommissioning is now supported for F_Ports in addition to E_Ports.
- The **Topology** page provides visual indication of when a link is over 50% utilization and over 80% utilization.
- Flow Management is supported for the Analytics Monitoring Platform.
- The "Configuration" chapter includes the following changes:
 - The DNS configuration block is added to the basic configuration. The SNMPv3 configuration block is enhanced for firmware version 8.2.1b and later.
 - The logical fabric configuration type is added to the switch configuration and restore section.
 - The "Call Home and ESRS" section is updated to reflect password-related changes. You can modify the Call Home configuration without entering the password if you do not modify the email setting for a Call Home center.
 - The "Configuring the Dell EMC Call Home Support Center" section has been updated to reflect the changes regarding device registration in the ESRS. The switches must be registered in ESRS before they are added to the Dell EMC call center.
 - The "Zoning" section is updated to include the following changes:
 - Added the section "Creating Multiple Zone Aliases."
 - Added the section "Selecting and Adding Multiple Zone Aliases to a Zone."
 - Added the section "Selecting and Adding Multiple Zones to a Zone Configuration."
 - Added the section "Viewing Zone and Zone Configuration Details."
 - The "Comparing Effective and Defined (Modified) Zone Configuration" section is updated with the modified zone status.
 - The "Virtual Fabrics" section is updated to include the following changes:
 - Non-VF and AMP support is added for logical fabrics.
 - The LISL option is removed from the XISL template.
 - The FICON template is removed from logical fabrics.
 - Support for FICON fabrics is added.
- The "Event Management" chapter is updated to reflect password-related changes. If you try to modify any of the email settings, you must re-enter the password in the **SMTP Password** field. You must enter the password to send a test email.
- The "Switch Maintenance and Support" chapter is updated to include the following changes:

- Added information on custom port support for SCP/SFTP switch SupportSave and firmware management.
- The password-protected ZIP file behavior is updated in switch SupportSave.
- Added SANnav support for AMP version 3.0.0 or later.
- The "Troubleshooting" chapter has been changed to "Troubleshooting and Diagnostics" and includes support for Brocade ClearLink Diagnostic Port (D_Port) mode.
- SANnav Global View now includes support for the following:
 - A maximum of 20 SANnav Management Portal instances. The total port count must not exceed 120,000 ports.
 - The ability to create and save filters.
 - FICON fabrics.
 - The chassis item in the **Inventory** page.
 - Performance measures in the switch port inventory.
 - The ability to export inventory views.

