Brocade® SANnav™ Management Portal Flow Management User Guide, 2.3.x

User Guide
April 28, 2023

Table of Contents

Introduction

Manage and monitor flows using SANnav™ Management Portal.

Supported Hardware and Software

SANnav Flow Management and Fabric OS™ Flow Vision features are supported on Gen 6 and Gen 7 platforms.

Fabric OS v9.0.0 or later is required to manage Gen 6 IT flows.

Fabric OS v9.1.1 or later is required to manage Gen 7 VITL/VITN Flows in SANnav. SANnav Management Portal v2.2.1x or later is required to view the new VM Entity ID information provided in Fabric OS v9.1.1 or later versions for Gen 7 flows.

Brocade® Gen 7 (64G) Fixed-Port Switches

- Brocade G720 Switch
- Brocade G730 Switch

Brocade Gen 7 (64G) Directors

- Brocade X7-4 Director
- Brocade X7-8 Director

Brocade Gen 6 (32G) Fixed-Port Switches

- Brocade G620 Switch
- Brocade G630 Switch

Brocade Gen 6 (32G) Directors

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

Contacting Technical Support for Your Brocade® Product

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

- OEM and 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 or 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 or solution provider.

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

Online	Telephone
For nonurgent issues, the preferred method is to log on to the Support portal at support.broadcom.com. (You must initially register to gain access to the Support portal.) Once registered, log on and then select **Brocade Products**. You can now navigate to the following sites: • **Case Management** • **Software Downloads** • **Licensing** • **SAN Reports** • **Brocade Support Link** • **Training & Education**	For Severity 1 (critical) issues, call Brocade Fibre Channel Networking Global Support at one of the phone numbers listed at www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

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.

Flow Management – Overview

The Flow Management feature provides flow monitoring and management capabilities that help a SAN administrator gather the necessary information to actively manage workloads in the SAN fabrics.

Flow Management learns about various flow metrics for flows traversing in SAN fabrics from the switches connecting to end device ports. These learned flows along with their various statistics give enhanced visibility into the I/O traffic and end device behaviors that can be useful for troubleshooting anomalies in the application performance in the fabric.

The following sections provide basic information about a flow and its components:

- Elements of a Flow
- Storage Protocols

For more information on how to manage flows using SANnav, see Flow Management in SANnav.

Elements of a Flow

The following basic entities are involved in a flow:

- Virtual machine (VM)
- Initiator
- Target
- LUN/Namespace

Virtual Machine

A VM is a virtual computer system with its own CPU, memory, network interface, and storage, created on a physical server.

Customer applications are hosted on VMs in the data center. The physical server can have Host Bus Adaptors (HBAs) that provide one or more physical ports to connect to the Fibre Channel (FC) network and access the SAN storage devices. VMs use this device port to communicate to the storage device. When a VM sends the IOs, it sends the Virtual Machine Identification (VMID) as part of the request header. The VMID is learned by the switch and distinguishes the flows. This helps you to monitor the flows at the VM level (VM-Initiator-Target-LUN/Namespace).

FC HBAs share the VMID with the fabric whenever a VM initiates the storage traffic. The VMID is displayed in the non-human readable format if the vCenter server is not discovered in SANnav. For example, 52 70 04 2a ce d6 13 38-0c de 7a m4 89 42 58 b2. The vCenter server must be discovered in SANnav for the SANnav Management Portal to display the VM name instead of the VMID of VITL/VITN flows. For more information on discovering vCenter, refer to the vCenter Discovery section of the *Brocade SANnav Management Portal User Guide*.

NOTE
End Device port is a general term referring to either *Server Port (Initiator)* or *Storage Port (Target)*.

Initiator

Customer applications are hosted on servers in the data center. These servers have FC HBAs that provide one or more physical ports to connect to the FC network and access the storage devices. Each of these HBA ports (physical and NPIV ports) is referred to as an *Initiator*. This port is represented by a unique 8-byte ID called the port World Wide Name (WWN) and the node WWN. The WWN is used for zoning the storage in the fabric.

Target

Storage arrays and devices serve storage space for all the data persistence needs. The storage spaces are configured and selectively presented to the servers. The storage device port connecting to the FC Network is called a *Target*. These storage ports are represented by the unique 8-byte port WWN and node WWN and assigned a unique 24-bit ID by the switch when connected to a SAN fabric. This 24-bit ID is used as a device address while communicating to the servers for responding to storage commands. Both server and storage device ports must be zoned in the FC network to access the storage space. In this document, Target or Target Port refers to the same entity.

LUN/Namespace

Storage spaces are configured on the storage devices that support the Small Computer System Interface (SCSI) or nonvolatile memory express (NVMe) transport protocols. This storage space is referred to as a *logical unit number (LUN)* in the SCSI protocol and Namespace Identifier (NSID) in the NVMe protocol. One or more LUNs or Namespaces are configured and presented to multiple hosts in the fabric. The operating system of the host discovers the block-level storage when the server boots up and discovers these LUNs or Namespaces presented by the storage devices zoned to them. Servers format filesystems or use as a raw device to persist data from the end-user applications.

Workload

As enterprise applications running on the servers grow, the demand for storage requirements grows exponentially for persisting data as primary or secondary storage. To meet the surge in storage, the storage space is provisioned from any of the following entities:

- Local hard disk
- External storage devices
- Tapes
- Network
- Cloud

External storage devices are typically storage arrays connected to the FC fabric or network-attached storage (NAS) on a Transmission Control Protocol (TCP) network (file servers).

Server and storage ports are zoned for accessing the storage device ports in the FC fabric. Zoning enables the servers to discover the storage (LUN or Namespace) presented to them for persisting the application data.

The following types of workloads are involved in the I/O processing to the storage devices where the data is persisted:

- File access
- Object storage
- Backup IO (tape devices)
- Network drives
- Online Transaction Processing (OLTP) transactions

Each of the workloads mentioned above can result in multiple Read or Write requests to the storage devices. These Read or Write requests are referred to as I/O requests.

In this document, we discuss only monitoring I/O requests from the server to LUNs or Namespaces presented by the storage arrays in the FC fabric.

Storage Protocols

The following storage protocols are the widely used on the FC transport for accessing the high-speed storage systems:

- SCSI
- NVMe

SCSI

SCSI is a transport protocol used between the Host/Initiator and Target to access the storage namespace. The SCSI standards define commands, protocols, electrical, optical, and logical interfaces. For example, the Read request is one of the commands in the SCSI command set similar to the Write command. There are multiple other commands used by the host to discover storage devices, checking device readiness, and reserving/releasing storage.

NVMe

NVMe is a storage access and transport protocol for flash and next-generation solid-state drives (SSDs) that delivers the high throughput and faster response times for all types of workloads. The NVMe protocol supports multiple deep queues, which is an advancement over traditional SCSI protocols for parallel I/O requests. SANnav monitors the flow metrics for the SCSI and NVMe protocols between the server and storage (NVMe over Fabric).

Flow – Overview

A flow is a logical entity that represents an end-to-end communication through a SAN fabric between a VM or physical host port (typically, an HBA port that plays the role of an *Initiator*) and storage port (typically, a storage port that plays the role of a *Target*). A flow is a set of FC frames or application Read/Write requests that share similar traits such as a VMID, source port ID, destination port ID, LUN/Namespace, or any other data that can be used to differentiate one set of related frames from another. These application Read or Write requests are translated into SCSI or NVMe protocol Read/Write commands from the server to the LUN/Namespace on the particular storage device. There can be multiple flows from the same server to different LUNs/Namespaces on the same or different zoned storage devices.

A flow is identified with the following parameters:

- VMID – UUID of the VM
- Source port ID (Initiator) – Originator or host port FC address
- Destination port ID (Target) – Destination or Target port FC address
- LUN/Namespace - LUN of the storage

- **Initiator-Target (IT) Flow** – Represents an IT flow, where **I** represents the device ports playing the role of *Initiator* and **T** represents another device port playing the role of a *Target*. An IT flow involves the FC frames of all SCSI/NVMe Read, SCSI/NVMe Write, and Other (non Read/Write) commands between an Initiator (Server Port) and a Target (Storage Port). The IT flow involves the following addresses:
  – Source port ID – Originator or host port FC address
  – Destination port ID – Destination or Target port FC address

  IT statistics represent the consolidated I/O stats (SCSI/NVMe Read and/or SCSI/NVMe Write) between the Initiator (Server Port) and all visible LUNs/Namespaces of the Target (Storage Port).

  A flow is identified through the zone alias of each device port, typically the zone alias of the host port (Initiator) and the zone alias of the storage port (Target). If a zone alias is not defined for the device ports, then SANnav identifies the I and the T by their FC address (3 bytes) which is not human-readable. Therefore, ensure that unique zone aliases are created for each of your device ports to make the identification of these flows more human-readable.
- **Initiator-Target-LUN (ITL) Flow** – Represents the FC frames of all SCSI/NVMe Read, SCSI/NVMe Write, and Other (non Read/Write) commands between an Initiator (Server Port) and a particular LUN on the Target (Storage Port).

  IO requests from VMs are tagged with a virtual machine ID (VMID). The VMID is a unique 128-bit universal identifier and is used to represent the VM. Switches learn VMIDs from the IO requests and tag them in flow definitions. These flows are classified as VITL/VITN flows.
- **Initiator-Target-Namespace (ITN) Flow** – Represents the FC frames of all NVMe Read, NVMe Write, and Other (non Read/Write) commands between an Initiator (Server Port) and a particular NSID on the Target (Storage Port). NSID is used by a controller to provide access to a namespace presented by the NVMe storage devices.
- **VM-Initiator-Target-LUN (VITL) Flow** – Represents the FC frames of all SCSI Read, SCSI Write, and Other (non Read/Write) commands between a VM and a particular LUN on the Target (Storage Port).

IO requests from a VM are tagged with a VMID. The VMID is a unique 128-bit universal identifier and is used to represent the VM. The VMID is displayed in the non-human readable format if the vCenter server is not discovered in SANnav. For example, 52 70 04 2a ce d6 13 38-0c de 7a m4 89 42 58 b2. The vCenter server must be discovered in SANnav for the SANnav Management Portal to display the VM name instead of VMID of VITL/VITN flows. For more information on discovering vCenter, refer to the vCenter Discovery section of the *Brocade SANnav Management Portal User Guide*.

- **VM-Initiator-Target-Namespace (VITN) Flow** – Represents the FC frames of all NVMe Read, NVMe Write, and Other (non Read/Write) commands between a VM and a particular NSID on the Target (Storage Port). NSID is used by a controller to provide access to a namespace presented by the NVMe storage devices.

  IT statistics represent the consolidated I/O stats (Read/Write) between the Initiator (Server Port) and all visible LUNs/ Namespaces of the Target (Storage Port).

  A flow is identified through the zone alias of each device port, typically the zone alias of the host port (Initiator) and the zone alias of the storage port (Target). If a zone alias is not defined for the device ports, then SANnav identifies the I and the T by their FC address (3 bytes) which is not human-readable. Therefore, ensure that unique zone aliases are created for each of your device ports to make the identification of these flows more human-readable.

These flows are monitored by Brocade switches at F_Port (where the end device port is connected, either to a server or storage port) in the FC fabric and reported to SANnav.

Flow Metrics

The following are the types of flow metrics:

- Latency
- Performance
- Other (non-Read/Write) Commands
- IO Exceptions

Latency

Latency is the time that it takes for an I/O operation to complete between an Initiator and a Target:

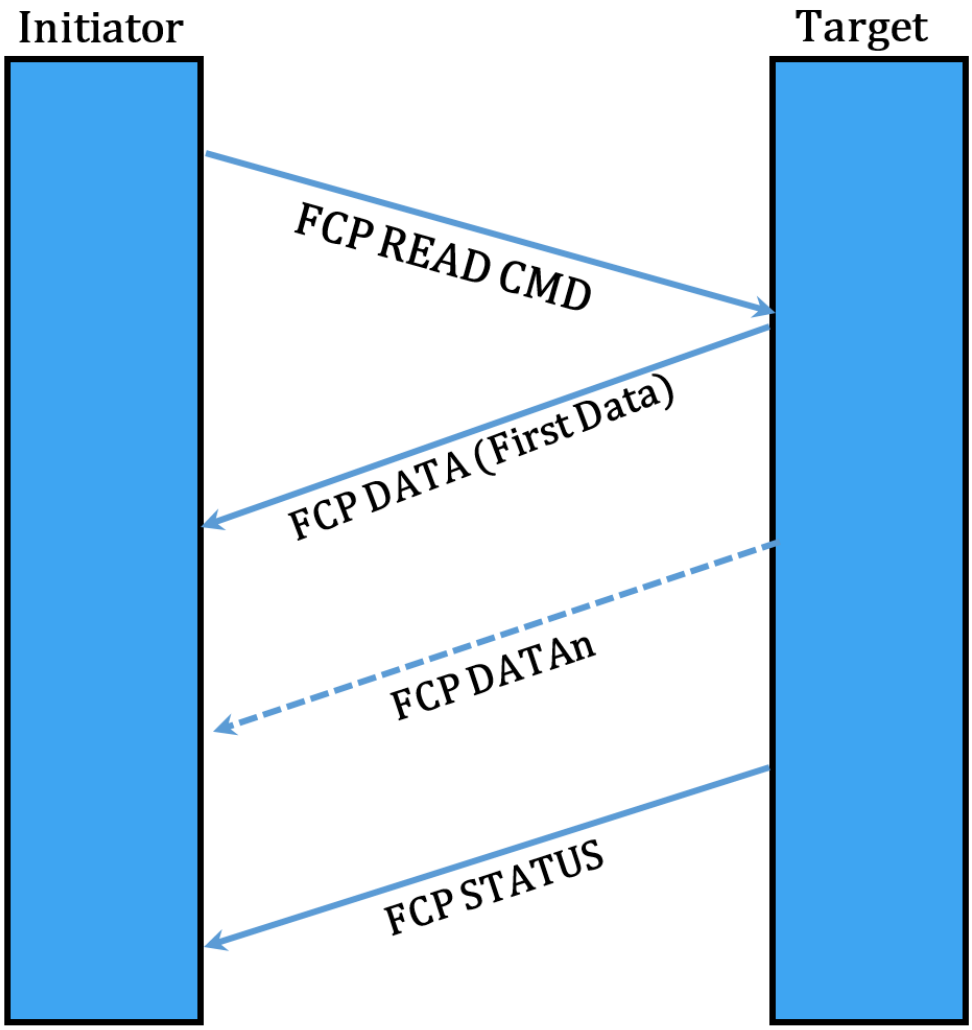
SCSI/NVMe Read

The following sequence describes the SCSI/NVMe Read IO operation protocol transaction between an Initiator and a Target in the FC fabric:

- Every SCSI/NVMe command and response is represented by *Exchange*, an FC terminology.
- The SCSI/NVMe Read command is encapsulated in the FC frame as an FCP Read command.
- The SCSI/NVMe Read data is encapsulated in the FC frame as FCP data. Each FCP data carries 2 KB of data based on the SCSI/NVMe Read data size and the Target sends multiple FCP data frames until the Read data size is fulfilled.
- The SCSI/NVMe Read command status is encapsulated in an FC frame as FCP Status. This FCP Status indicates the completion of the Read command.

The following figure describes the SCSI/NVMe READ transactions between an Initiator and a Target:

Figure 1: SCSI/NVMe READ Transactions



The following list describes supported latency metrics for a SCSI/NVMe Read IO operation:

- **Read First Response Time (RD FRT)** - The time difference between when the FCP Read command frame is transmitted and when the first data frame is returned to the host.
- **Read Exchange Completion Time (RD ECT)** - The time difference between when the FCP Read command frame is transmitted and when the status frame is returned to the host.
- **Pending IO** - The number of I/O (Read/Write) requests waiting to be serviced by the Target. These pending IOs are classified as RD Pending IOs and WR Pending IOs based on the request type.

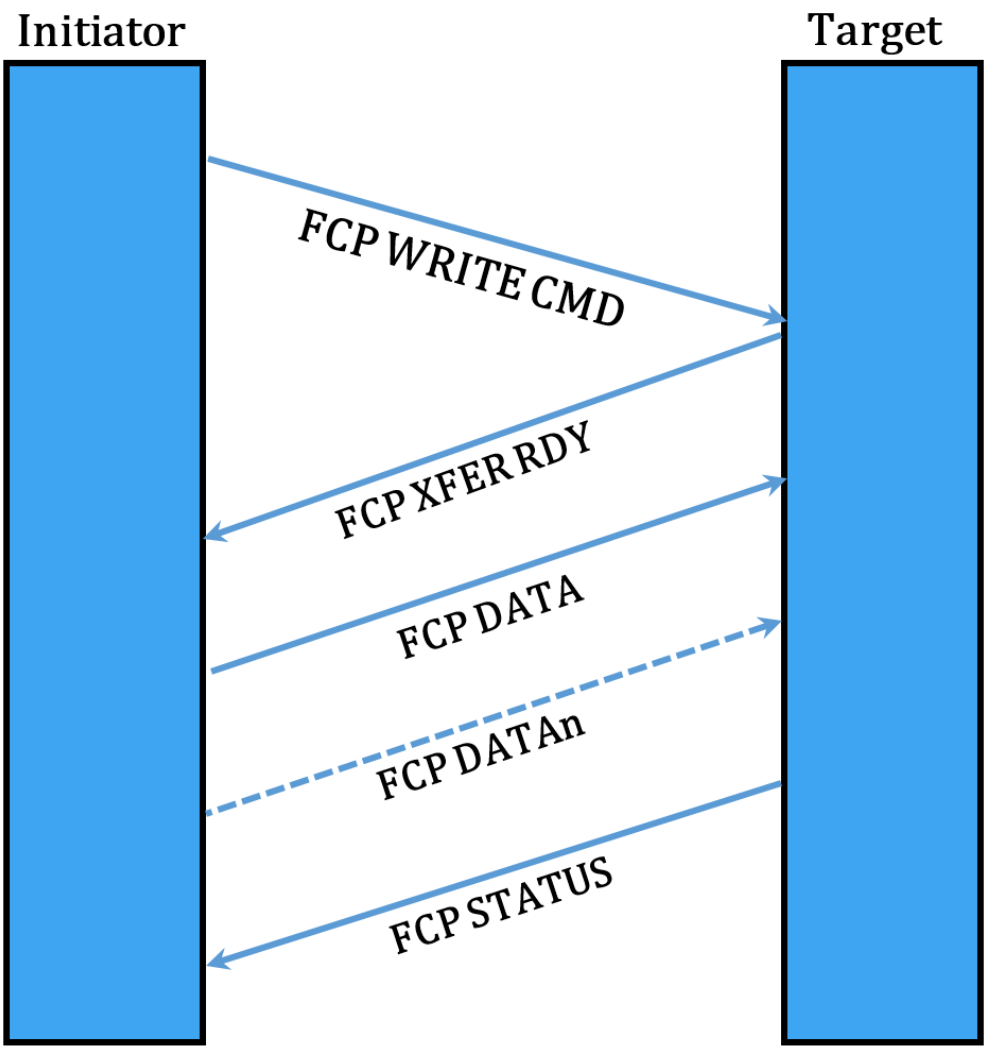
SCSI/NVMe Write

The following sequence describes the SCSI/NVMe Write IO operation protocol transaction between an Initiator and a Target in the FC fabric:

- The SCSI/NVMe Write command and response is represented by *Exchange*, an FC terminology.
- The Transfer Ready semantic from the Target instructs the server to only send the specified size of data. This is depending on Target capacity to hold the data from the servers. There can be multiple transfers ready semantic if the Write Data size is large from the server.
- The SCSI/NVMe Write command is encapsulated in the FC frame as an FCP Write Command.
- The SCSI/NVMe XFER RDY command is encapsulated in the FC frame as FCP XFER RDY. This FC frame instructs the server to send only the specified size of the Write data.
- The SCSI/NVMe Write data is encapsulated in the FC frame as FCP data and each FCP data carries 2 KB of data. The number of FCP data is based on the size that is specified in FCP XFER RDY by Target and the server sends the same number of FC frames with FCP data.

The SCSI/NVMe Write command status is encapsulated in the FC frame as FCP Status. This indicates that the completion of the Write command is a success or failure as described in the following figure:

Figure 2: SCSI/NVMe Write Transactions



The following list describes supported latency metrics for the SCSI/NVMe Write IO operation:

- **Write First Response Time (WR FRT)**: The time difference between when the FCP Write command frame is transmitted and when the XFER RDY frame is returned to the host.
- **Write Exchange Completion Time (WR ECT)**: The time difference between when the FCP Write command frame is transmitted and when the status frame is returned to the host.

Performance

The following performance flow metrics are streamed by Brocade switches and monitored by SANnav:

- The number of I/Os (Read IOPS and Write IOPS commands) completed per second
- The amount of data that is read or written per second (Read Data Rate and Write Data Rate) on an IT or ITL, ITN, VITL, and VITN flow
- The size of data that is read or written (Read Data Size and Write Data Size) on an IT or ITL, ITN, VITL, and VITN flow

Other (non Read/Write) Commands

The *Other* commands are non Read/Write commands to the storage device or LUN/Namespace. These commands are used for discovery and device management. Brocade switches stream the count of the following Other commands:

- SCSI/NVMe Total
- SCSI/NVMe Reserve
- SCSI/NVMe Release
- SCSI Inquiry
- SCSI Request Sense
- SCSI Test Unit Ready
- SCSI Read Capacity
- NVMe Flush
- NVMe Flush Basic Link Service
- NVMe Red Basic Link Service
- NVMe Identify
- NVMe Sequence Recovery

IO Exceptions

The SCSI/NVMe command execution failures are tracked as part of the IO exception metrics.

Brocade switches stream the metrics of the following IO Exceptions commands:

- **SCSI/NVMe:**
  - Total
  - Abort
  - Timeouts
  - Reservation Conflicts
- **SCSI:**
  - Check Conditions
  - Busy
  - Task Set
  - Task Abort
  - ACA
- **NVMe:**

- Namespace Error
- LBA Out of Range
- Format in Progress

Flow Management in SANnav

The Brocade SANnav Flow Management feature provides flow monitoring and management capabilities for Brocade Gen 6 and Gen 7 platforms. These capabilities enable a SAN administrator to gather the necessary information to actively manage flows in the SAN fabrics.

Fabric congestion can occur because of the scale of workloads, slow-drain devices, physical layer errors, and fabric design limitations. This congestion can impact the normal flow of the I/O traffic and result in a degradation of application performance. SANnav Flow Management provides the capability to inspect metrics for latency, performance, and IO exceptions for related flows of an application. This capability helps in troubleshooting the application performance because of fabric congestions.

SANnav Flow Management learns through Fabric OS interfaces about the various flow metrics for flows traversing in SAN fabrics from the switches connecting to end device ports. These learned flows along with various statistics provide enhanced visibility into the I/O traffic and end-device behaviors.The learned flows are useful for troubleshooting anomalies in the application performance in the fabric.

The Flow Management feature provides the following capabilities:

- Provides the IO Health & Latency Dashboard widget to view degraded device ports based on MAPS violations in the flow IO Health and Latency categories. The IO Health and Latency MAPS violations are displayed in the **Investigation Mode** page for flows.
- Provides the inventory of flows (IT and ITL, ITN, VITL, and VITN) along with their related details in the SANnav Flow Inventory. These flows are not created in SANnav, and they are automatically learned by Fabric OS and streamed to SANnav through a streaming interface.

  NOTE
  The vCenter server must be discovered in SANnav for the SANnav Management Portal to display the VM name instead of the VMID of the VITL/VITN flows. For more information on discovering vCenter, refer to the vCenter Discovery section of the *Brocade SANnav Management Portal User Guide*.
- Provides the ability to investigate flows through a user interface to display the historical and real-time performance metrics that are associated with the flow. These metrics vary by protocol (SCSI or NVMe). For more information, see SANnav Flow Metrics.
- Provides custom report widgets using the flow widgets to track the flow-related historical statistics.

  NOTE
  The flow widgets are **deprecated** in SANnav 2.3.0. The flow widgets will be removed from a future version of SANnav.

  For more information, see Report Widgets for Flows.

SANnav Management Portal supports up to 150,000 flows. The following table shows the support metrics for flows.

Supported Metrics	IT	ITL	VITL
Gen 6 Flow Stats Streaming	Yes (>= FOS v9.0.x and >= SANnav v2.1.x)	No	No
Gen 6 Flow Violation Statistics Streaming	No	No	No
Gen 7	Yes (>= FOS v9.0.1 and >= SANnav v2.1.1)	Yes (>= FOS v9.0.1 and >= SANnav v2.1.1)	Yes (>= FOS v9.1.1 and >= SANnav v2.2.1)

Supported Metrics	IT	ITL	VITL
Gen 7 Flow Violation Statistics Streaming	Yes (>= FOS v9.2.x and >= SANnav v2.3.x)	Yes (>= FOS v9.2.x and >= SANnav v2.3.x)	Yes (>= FOS v9.2.x and >= SANnav v2.3.x)

To understand the fabric flow control mechanisms, how congestions occur in the fabric, and the port metrics that help to detect the congestion, refer to the *Brocade Fabric Congestion Troubleshooting Guide*.

Northbound streaming provides support to securely stream port and flow metrics from the switch to a northbound server. Streaming gives you access to a large set of data from one or more managed fabrics that can be used to build customized reports or applications. For more information on configuring the streaming interface using the REST API, see the *Brocade SANnav Management Portal REST API and Northbound Streaming Reference Manual*.

Flow Management – Prerequisites

Before you can manage flows, make sure that you meet all of the following prerequisites:

- SANnav must be installed on a large server with 96GB of memory, 24 cores, and 1.2TB of available storage.
- You have the Flow Management & Dashboard privilege with read-write permission to monitor and manage flows.
- You have the Discovery privilege with read-write permission to manage telemetry registration.
- The latency between the switch and the Brocade SANnav is less than or equal to 100 milliseconds.
- All fabric IDs (FIDs) on a given chassis are discovered in a single (or the same) Brocade SANnav server, and all FIDs are authenticated and managed. For more information about Fabric discovery, refer to the *Brocade SANnav Management Portal User Guide*
- You have access to all discovered fabrics and all fabrics are in your area of responsibility (AOR).
- The switch and SANnav server clocks are synchronized. Clock synchronization is mandatory for all switches and the SANnav application server. If the clocks are not synchronized, you might lose flows and their statistics. An application event message alerts you when the SANnav server and the switch are not synchronized. For more information, refer to the *Brocade SANnav Management Portal Installation and Migration Guide*. You can use NTP or equivalent protocol for clock synchronization.
- Complete the telemetry registration on a chassis for flow monitoring. For more information, see Flow Telemetry Registration Management.
- The vCenter server is discovered in SANnav for the SANnav Management Portal to display the VM name instead of VMID of VITL/VITN flows. For more information on discovering vCenter, refer to the vCenter Discovery section of the *Brocade SANnav Management Portal User Guide*.

SANnav Version Upgrade and Migration Impact

After you upgrade and migrate to SANnav 2.3.x, the registration for flow streaming displays as *Unregistered*, by default for all chassis managed by SANnav. You must register the desired chassis to view flows (up to 150,000 flows maximum for the entire SANnav server).

Flow Monitoring Intervals

Flow metrics can be streamed by chassis at various frequencies. The following table details the streaming intervals that are supported by Fabric OS:

	IT Flows (Gen 6 and Gen 7)	ITL/VITL/ITN/VITN Flows (Gen 7)	Real-Time Flows (Gen 6 and Gen 7)
Flow Metrics Fabric OS 9.0.x and later	5 minutes	6 hours	10 seconds
Flow Violation Metrics Fabric OS 9.2.x and later	5 minutes	5 minutes	10 seconds

A maximum of up to 25 flows per chassis may be investigated in SANnav in real-time mode at a 10 second interval.

SANnav Flow Metrics

The following types of flow metrics are streamed by Brocade switches and monitored by SANnav:

- Latency
- Performance
- Other (non-Read/Write) Commands
- IO Exceptions
- IO Health Violations
- IO Latency Violations

SANnav flow metrics can be used to identify potential sources of traffic delays at the device (both Host and Target) and fabric level.

The following table shows the Flow Latency metrics that are collected by SANnav.

Table 1: Flow Latency Metrics

Metric	Description	Comments
Read Exchange Completion Time (Max)	The time difference between the time when a Read command frame is initiated by the Initiator and when the corresponding status frame is returned by the Target.	A high Read Exchange Completion Time (Max) value indicates that any of the following conditions might exist: • High application load is causing the Read requests of smaller Read size and high load on the storage device • Large Read size requests are increasing the load in the fabric because of many FCP data frames for servicing the large-size Read request, or the server cannot process the amount of Read data • Large pending IO on the Target because of many I/O requests from all servers • ISL/Device port oversubscription • Credit-stall condition on the server-side F_Port • Credit loss on the server-side F_Port The maximum (Max) value indicates a spike in the time taken to complete the Read request during the monitoring interval.
Read Exchange Completion Time (Avg)	The average time taken for all Read I/O exchange completion during the monitoring interval.	A high Read Exchange Completion Time (Avg) value indicates that any of the following conditions might exist: • High application load is causing the Read requests of a smaller Read size and a high load on the storage device • Large Read size requests are increasing the load in the fabric because of many FCP data frames for servicing the large-size Read request, or the server cannot process the amount of Read data • Large pending IO on the Target because of many I/O requests from all servers • ISL/Device port oversubscription • Credit-stall condition on the server-side F_Port • Credit loss on the server-side F_Port

Metric	Description	Comments
Write Exchange Completion Time (Max)	The maximum Exchange Completion Time (command completion time) for any Write I/O in the monitoring interval.	A high Write Exchange Completion Time (Max) value indicates that any of the following conditions might exist: • High application load is causing burst Write requests of a smaller write size, and the requests are causing a high load on the storage device. • Large Write size requests are increasing the load in the fabric because of the large number of FCP data frames for servicing the large size Write request, or the storage cannot process the amount of Read data. • Large pending IO on the Target side because of the large number of I/O requests from all the servers. • ISL or device port oversubscription • Credit-stall condition on the storage F_Port • Credit loss on the storage F_Port The maximum (Max) value indicates a spike in the time taken to complete the Write request during monitoring interval.
Write Exchange Completion Time (Avg)	The average time taken for all Write I/O exchange completion during the monitoring interval.	A high Write Exchange Completion Time (Avg) value indicates that any of the following conditions might exist: • High application load is causing burst Write requests of a smaller write size, and the requests are causing a high load on the storage device. • Large Write size requests are increasing the load in the fabric because of the large number of FCP data frames for servicing the large size Write request, or the storage cannot process so much of Read data. • Large pending IO on the Target side because of the large number of I/O requests from all the servers. • ISL or device port oversubscription • Credit-stall condition on the storage F_Port • Credit loss on the storage F_Port
Read First Response Time (Max)	For Read I/O, the First Response Time is taken when the first data frame is transmitted by the Target after receiving the command frame.	A high Read First Response Time (Max) value indicates that any of the following conditions might exist: • Large pending IO on the storage side (storage device utilization is high or overutilized) is causing an intermittent delay in request processing • Congestion in fabric This value indicates a spike in the time taken to get the first response from the Target for the Read request during the monitoring interval.

Metric	Description	Comments
Read First Response Time (Avg)	The average time that is taken for all Read I/O first response completion during the monitoring interval.	A high Read First Response Time (Avg) value indicates that any of the following conditions might exist: • Large pending IO on the storage side (storage device fully loaded) is causing a prolonged delay in request processing • Credit-stall on the storage side F_Ports • Credit loss on the server or the storage F_Ports • ISL or device port oversubscription • Target load (for large pending IO) • Congestion in the fabric This value can also result in a high Read Exchange Completion Time.
Write First Response Time (Max)	For the Write I/O, the First Response Time is taken when the Target sends the Transfer (Xfer) Ready frame after receiving the command frame.	A high Write First Response Time (Max) value indicates that any of the following conditions might exist: • Large pending IO on the storage side (storage device fully loaded) is causing an intermittent delay in request processing • Congestion in the fabric This value indicates a spike in the time taken to get the first response from the Target for the Read request during the monitoring interval.
Write First Response Time (Avg)	The average time that is taken for all Write IO first response completion during the monitoring interval.	A high Write First Response Time (Avg) value indicates that any of the following conditions might exist: • Large pending IOs on the storage side (storage device fully loaded) are causing a prolonged delay in request processing. • Credit-stall on the storage side F_Ports • Credit loss on the server or the storage F_Ports • ISL or device port oversubscription This value can also result in a high Write Exchange Completion Time.
Read Pending IOs (Max)	The maximum number of the Read requests pending for the completion during the monitoring interval.	A high Read Pending IOs (Max) value indicates that any of the following conditions might exist: • High application requests from one or more servers • Storage device is loaded with a high number of outstanding requests • Impaired storage device is not working optimally

Metric	Description	Comments
Read Pending IOs (Avg)	Average number of the Read requests pending for completion during the monitoring interval.	A high Read Pending IOs (Avg) value indicates that any of the following conditions might exist: • High application requests from one or more servers • Storage device is loaded with a high number of outstanding requests • Impaired storage device is not working optimally
Write Pending IOs (Max)	The Max number of Write requests pending at the specified monitoring interval.	A high Write Pending IOs (Max) value indicates that any of the following conditions might exist: • High application requests from one or more servers • Storage device is loaded with a high number of outstanding requests • Impaired storage device is not working optimally
Write Pending IOs (Avg)	The average number of the Write requests pending for completion during the monitoring interval.	A high Write Pending IOs (Avg) value indicates that any of the following conditions might exist: • High application requests from one or more servers • Storage device is loaded with a high number of outstanding requests • Impaired storage device is not working optimally

The following table shows the performance metrics of flows that are collected by Brocade SANnav.

Table 2: Flow Performance Metrics

Metric	Description	Comments
Read Data Size	The total data size measured for all Read I/Os.	The Read Data Size measure shows the cumulative Read Data Size at the specified monitoring interval for the selected flow.
Write Data Size	The total data size measured for all Write I/Os.	The Write Data Size measure shows the cumulative Write Data Size at the specified monitoring interval for the selected flow.

Metric	Description	Comments
Read IOPS	The count of total Read I/O per second at the specified monitoring intervals.	The Read IOPS measure shows the number of Read requests that the host can perform in a second. A low Read IOPS value indicates the following conditions: • Minimal application load. • Large pending IO on the storage side (storage device fully loaded) is causing a delay in the request processing, so Read IOPS is reduced. • ISL oversubscription. • Lower link speeds on the server or storage F_Ports. • Credit-stall on the server side F_Ports. • Credit loss on the server or the storage F_Ports. • Bad SFP/cables in the fabric connectivity. • High Read Exchange Completion Time because of the fabric congestion. • Slow processing of the Read data on the server side.
Write IOPS	The count of total Write IO per second at the specified monitoring interval.	The Write IOPS measure shows the number of Write requests that the host can perform in a second. If the Write IOPS value is lower, this value indicates the following conditions: • Minimal application load. • Large pending IO on the storage side (storage device fully loaded) is causing a delay in the request processing. • ISL oversubscription. • Lower link speeds on the server or storage F_Ports. • Credit-stall on the storage side F_Ports. • Credit loss on the server or the storage F_Ports. • Bad SFP/Cables in the fabric connectivity. • High Write Exchange Completion Time because of the fabric congestion.

Metric	Description	Comments
Read Data Rate	The total Read IO bytes per second at the specified monitoring interval.	The Read Data Rate measure shows that the value of the Read data has moved in the fabric for the selected flow. The lower Read Data Rate indicates the following conditions: • Minimal application load. • Large pending IO on the storage side (storage device fully loaded) is causing a delay in request processing, so the Read Data Rate is reduced. • ISL oversubscription. • Lower link speeds on the server or the storage F_Ports. • Credit-stall on the storage side F_Ports. • Credit loss on the server or the storage F_Ports. • Bad SFP/Cables in the fabric connectivity can result in a high SCSI/NVMe Abort count. • High Read Exchange Completion Time because of the fabric congestion. • Slow processing of Read data on the server side.
Write Data Rate	The total Write IO bytes per second at the specified monitoring interval.	The Write Data Rate measure shows that the amount of Write data has moved in the fabric for the selected flow. The lower Write Data Rate indicates the following conditions: • Minimal application load. • Large pending IO on the storage side (storage device fully loaded) is causing a delay in request processing, so the Write Data Rate is reduced. • ISL oversubscription. • Lower link speeds on the server or the storage F_Ports. • Credit-stall on the storage side F_Ports. • Credit loss on the server or the storage F_Ports. • Bad SFP/cables in the fabric connectivity can result in a high SCSI/NVMe Abort count. • High Write Exchange Completion Time because of the fabric congestion.

The following table shows the Flow Other (non Read/Write) Commands metrics collected by the Brocade SANnav.

Table 3: Flow Other (non-Read/Write) Commands Metrics

Metric	Description	Comments
SCSI/NVMe Total	The Total Other commands received by the flow at the specified monitoring interval.	The SCSI/NVMe Total measure shows the Total metrics (Other non-Read/Write Commands) that occurred between the Initiator and a Target of the selected flow.
SCSI/NVMe Reserve	The total count of Reserve commands received by the flow at the specified monitoring interval.	The SCSI/NVMe Reserve measure shows the total LUN/Namespace Reservation commands between the Initiator and a Target of the selected flow. Reservations of LUN/Namespace are performed in a cluster configuration, where the active server/VM locks the LUN/Namespace for performing I/O in an exclusive or shared basis.
SCSI/NVMe Release	The total count of Release commands received by the flow during the monitoring interval.	The SCSI/NVMe Release measure shows the total LUN/namespace Release commands that occurred between the Initiator and a Target of the selected flow. Reservations release of namespace/LUN is performed in a cluster configuration, where the active server/VM unlocks the LUN/ namespace after performing an I/O (for example, after the application persistency). The LUN or namespace can be reserved by the same or another member in the cluster for an I/O.
SCSI Inquiry	The total count of Inquiry commands received by the flow at the specified monitoring interval.	The SCSI Inquiry measure shows that the total Inquiry admin commands that occurred between an Initiator and a Target of the selected flow. The Inquiry commands are issued by the Initiator/ Hosts during the initial discovery of the storage devices/LUNs at the boot time.
SCSI Request Sense	The total count of Request Sense commands received by the flow at the specified monitoring interval.	The SCSI Request Sense measure shows the total Request Sense commands between the Initiator and a Target of the selected flow. Request Sense commands are issued by the Initiator/Hosts to collect more information about the I/O error when the I/O metrics (Read/write) on the LUNs are errored by the Target/storage devices.
SCSI Test Unit Ready	The total count of Test Unit Ready commands received by the flow at the specified monitoring interval.	The SCSI Test Unit Ready measure shows the total Test Unit Ready commands that occurred between the Initiator and a Target of the selected flow. The Test Unit Ready commands are issued by the Initiator/Hosts to check if the LUN on the storage is ready for performing I/O. This check is done during the discovery of the storage devices/ LUNs by the host at the boot time. This check is also used for the periodic path health check by the host multipath software for managing access paths to the LUN from one or more fabrics.

Metric	Description	Comments
SCSI Read Capacity	The total count of Read Capacity commands received by the flow.	The SCSI Read Capacity measure shows the total Read Capacity commands that occurred between the Initiator and a Target of the selected flow. The Read Capacity commands are issued by the Initiator/Host to check the size of the discovered LUNs on the storage. This information is used by the host for formatting and mounting the LUN for the application data access. This check is done during the discovery of the storage devices/LUNs by the host at the boot time. This check is also used for the periodic path health check by the host multipath software for managing access paths to the LUN from one or more fabrics.
NVMe Flush	The total count of Flush commands received by the flow.	The NVMe Flush measure shows the total Flush commands that occurred between the Initiator and a Target of the selected flow. The NVMe Flush commands might be issued by the Initiator/Hosts at some periodic check points to instruct the NVMe storage to persist all the in-memory volatile data into the disk. This check helps avoid data loss during an abrupt power-down or any unforeseen crash of storage controllers.
NVMe Flush Basic Link Service	The total count of Flush Basic Link Service commands received by the flow.	The NVMe Flush Basic Link Service measure shows the total Flush Basic Link service commands that occurred between Initiator and a Target of the selected flow. This command is used by the NVMe protocol for any link-level I/O recovery purpose.

Metric	Description	Comments
NVMe Identify	The total count of Identify commands received by the flow.	The NVMe Identify measure shows the total NVMe Identify commands that occurred between the Initiator and a Target of the selected flow. This metric is similar to the SCSI Inquiry. The host issues the Identify commands on NVMe storage devices to get controller and namespace attributes during the device discovery process at the boot time or when hosts are notified by the NVMe storage devices for some attribute changes. The following information is retrieved at the storage level: • Supported metrics • Maximum transfer length • Number of I/O queues • Maximum namespaces • Current number of namespaces The following information is retried at the namespace level for the optimal performance and NSID: • Global unique ID • Block size • Recommended I/O size
NVMe Sequence Recovery	The total count of Sequence Recovery commands received by the flow.	The NVMe Sequence Recovery measure indicates the total NVMe Sequence Recovery commands that occurred between the Initiator and a Target of the selected flow. This metric is used by the hosts to recover the NVMe I/O metrics if any intermittent errors are found. The high NVMe Sequence Recovery value shows a bad path in the fabric or some issues in the I/O on the NVMe storage device side.

The following table shows the Flow IO Exceptions metrics collected by SANnav.

Table 4: Flow IO Exceptions Metrics

Metric	Description	Comments
SCSI/NVMe Total	The total non-zero status/exceptions received by the flow at the specified monitoring interval.	The SCSI/NVMe Total measure shows the total I/O exceptions that occurred between the Initiator and a Target of the selected flow. The high SCSI/NVMe Total value indicates a bad path in the fabric or some access issues for an I/O on the LUNs/Namespaces.
SCSI/NVMe Abort	The total count of the Abort commands received by the flow at the specified monitoring interval.	The SCSI/NVMe Abort measure shows the total aborts of I/O requests that occurred between the Initiator and a Target of the selected flow. The SCSI/NVMe Aborts occur because of the timing out of pending IO metrics by host issued to the Target or aborting because of an application exit or crash.

Metric	Description	Comments
SCSI/NVMe Timeout	The total count of the Timeout commands received by the flow at the specified monitoring interval.	The SCSI/NVMe Timeout measure shows the total timeouts of I/O requests that occurred between the Initiator and a Target of the selected flow. These statistics are found when the I/O requests are not completed by the Target in 30 seconds.
SCSI/NVMe Reservation Conflicts	The total count of the Reservation Conflicts received by the flow at the specified monitoring interval.	The SCSI/NVMe Reservation Conflicts measure shows the total reservation conflicts of the I/Os that occurred between the Initiator and a Target of the selected flow. This metric shows that the host is trying to perform I/O on the LUNs/Namespace, which is exclusively reserved by the other host/VM in the cluster.
SCSI Check Conditions	The total count of the Check Condition commands received by the flow at the specified monitoring interval.	The SCSI Check Conditions measure shows the total check condition exceptions for the I/Os (IO exceptions) between the Initiator and a Target of the selected flow. The Check Condition command status indicates the following conditions: • Device not ready • Medium errors • Soft errors • Illegal requests • Any change from storage to host The host issues the Request Sense command to get these sense codes to learn the type of error.
SCSI Busy	The total count of the Busy commands received by the flow at the specified monitoring interval.	The SCSI Busy measure shows the total device busy I/O exceptions received for the I/Os between the Initiator and a Target of the selected flow. The Target/Storage returns Busy if it cannot complete a SCSI command at that time.
SCSI Task Set	Total count of the Task Set commands received by the flow at the specified monitoring interval.	This measure shows the total Task Set full I/O exceptions that are received for the I/Os between Initiator and a Target of the selected flow. The Target/Storage returns the Task Set full status when the logical unit on the Storage/Target lacks the resources to accept a received SCSI task (Abort/terminate or Reset target). This check indicates that the Target already has one outstanding task from that Initiator and a Target, it cannot process the new one until it completes the existing task.
SCSI Task Abort	The total count of the Task Abort commands received by the flow at the specified monitoring interval.	This measure shows the total of Task Aborts I/O exceptions for the I/Os between the Initiator and a Target of the selected flow. The Target/Storage returns the Task Aborted status when the current outstanding task is aborted between this Initiator and a Target.

Metric	Description	Comments
SCSI ACA	The total count of the Auto Contingent Allegiance (ACA) commands received by the flow at the specified monitoring interval.	The SCSI ACA measure shows the total ACA I/O exceptions for the I/Os between the Initiator and a Target of the selected flow. The Target is in the Auto Contingent Allegiance state when the Storage/Target reports errors to the I/O metrics. When the Target returns a Check Condition in response to a command, the Initiator usually issues a SCSI Request Sense command to obtain more information. During the time between the reporting of a Check Condition and the issuing of the Request Sense command, the Target is in this special state. The Target returns this status code if an ACA condition has occurred. The SCSI sense code (error code) is returned along with the status, and there is no need for the server to issue a request sense command for getting the error code.
NVMe Namespace Error	The total count of the Namespace Error commands that is received by the flow at the specified monitoring interval.	The NVMe Namespace Error measure shows the exceptions for any I/Os on the namespace or invalid commands on the namespace.
NVMe LBA Out of Range	The total count of the Logical Block Access Out of Range commands received by the flow at the specified monitoring interval.	The NVMe LBA Out of Range measure shows the exceptions for any I/O requests for the offset beyond the namespace size.
NVMe Format in Progress	The total count of the Format in Progress commands count received by the flow at the specified monitoring interval.	The NVMe Format in Progress measure shows the exceptions for any I/O requests on the namespace when the existing namespace is being formatted as part of some admin operations for repurposing.

You must setup and define the MAPS rules for IO Health Latency and IO Latency Monitoring categories on all flows in a chassis for your environment and business requirements. For additional information, refer to *MAPS Categories* and *MAPS Configuration* in the *Brocade SANnav Management Portal User Guide*.

You must determine if you need to apply aggressive, conservative, or moderate rules for the IO Health Latency and IO Latency Monitoring categories or if you need to customize these rules for your specific needs. These rules are used to detect Flow Violations which impact device ports and drive the IO Health and IO Latency widget. For more information about the IO Health and IO Latency widget, see Monitoring IO Health and Latency.

The following table shows the Flow IO Health Violation metrics collected by SANnav.

Table 5: Flow IO Health Violation Metrics

Metric	Related MAPS Measure	Related MAPS Timebase
RD ECT Violated IO %	Read completion Time (RD_STATUS_TIME)	IO
WR ECT Violated IO %	Write completion Time (WR_STATUS_TIME	IO
RD FRT Violated IO %	First read response (RD_1stDATA_TIME)	IO
WR FRT Violated IO %	First write transfer ready (WR_1stXFER_RDY)	IO
RD Pending Violated IO %	MAX Read Pending IOs (MAX_RD_PENDING_IO)	10 seconds

Metric	Related MAPS Measure	Related MAPS Timebase
WR Pending Violated IO %	MAX Write Pending IOs (MAX_WR_PENDING_IO)	10 seconds

The following table shows the Flow IO Latency Violation metrics collected by SANnav.

Table 6: Flow IO Latency Violation Metrics

Metric	Related MAPS Measure	Related MAPS Timebase
Violated Total %	SCSI or NVMe IO error (IO_TIMEOUT), Timebase: 10 Seconds	10 seconds
Violated Timeouts %	SCSI or NVMe IO timeouttime out error (IO_ERROR), Timebase: 10 Seconds	10 seconds
Violated Reserve %	SCSI or NVMe reserve (RESERVE), Timebase: 10 Seconds	10 seconds
Violated Abort %	SCSI or NVMe IO about error (IO_ABORT), Timebase: 10 Seconds	10 seconds

NOTE
Violation metric statistics streaming is supported only on Gen 7 platforms. SANnav uses the following formula to calculate the percentage:

- When the timebase is IO, the violated percentage equals (violated IOs / total IOs) * 100.
- When the timebase is 10 seconds, violated percentage equals (violated count / 30) * 100.

Flow Telemetry Registration Management

SANnav Management Portal v2.3.0 does not automatically enable flow statistics streaming and flow violation statistics streaming. You must register chassis flow streaming using Flow Telemetry Registration Management. You can also use Flow Telemetry Registration Management to unregister flow streaming or to determine the flow registration status.

You must meet the following requirements for Flow Telemetry Registration Management:

- You must have the Discovery Setup privilege with the read-write permission.
- You must have access to all discovered fabrics and you must have all fabrics in your area of responsibility (AOR).
- SANnav must be installed on a large server with 96GB of memory, 24 cores, and 1.2TB of available storage.

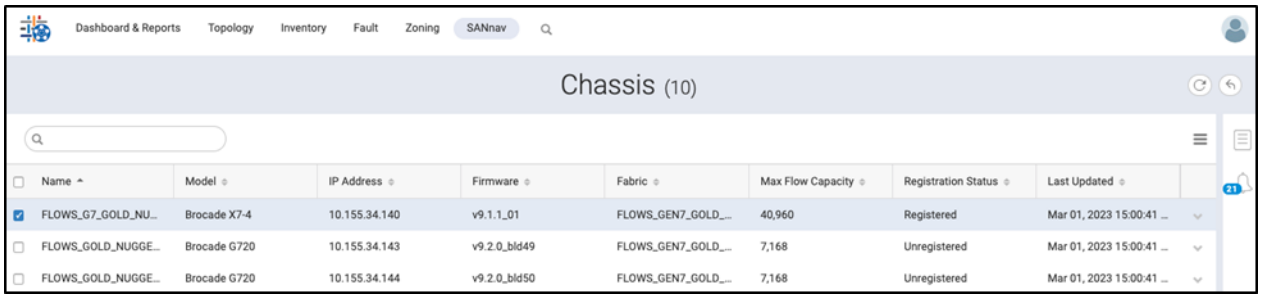
SANnav supports up to 150,000 flows.

Determining the Flow Registration Status on a Chassis

To quickly view the flow registration status on a chassis, complete the following steps:

1. Click **SANnav** in the navigation bar, and then select **SANnav Monitoring** > **Flow Telemetry Registration Management**.

   The **Chassis** page lists all chassis that are flow streaming capable. The **Chassis** page provides the maximum Flow capacity for each chassis.



2. Check the flow registration status.

   The **Registration Status** column displays the status of the streaming registration for the chassis. The following list details the valid values:

   - **Unregistered** – The chassis is not registered for flow streaming to SANnav.
   - **Registered** – The chassis is registered for flow streaming to SANnav.
   - **Registration Failed** <*reason*> – This is a temporary status. When the problem is resolved, SANnav automatically changes the status to Registered. Registration failure can occur for the following reasons:
     - Firmware not supported
     - Chassis is bound to another SANnav server
     - Chassis is not reachable
     - Chassis is not managed or unmonitored
   - **Unregistration Failed** <*reason*> – This is a temporary status. Once the actual problem is resolved then SANnav automatically changes the status to **Unregistered**.
   - **Registration In Progress** – The user-initiated registration action is in progress. This takes a few minutes to complete.
   - **Unregistration In Progress** – The user-initiated Unregistration action is in progress. This takes a few minutes to complete.

SANnav checks the registration status every 15 minutes and updates the **Registration Status** column.

3. Update the Chassis registration view by clicking the refresh icon in the upper-right corner of the page.

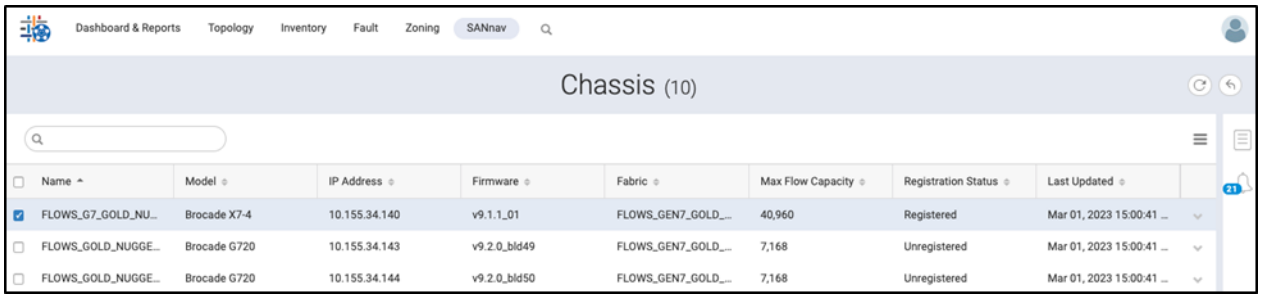
Registering or Unregestering a Chassis for Flow Statistics Streaming

NOTE
If the flow count on a registered chassis exceeds the SANnav flow scale limit (up to 150,000 flows), flow statistics streaming registration is not allowed.

You can use Flow Telemetry Registration Management to register (monitor) or unregister (unmonitor) one or more chassis for flow statistics streaming.

1. Click **SANnav** in the navigation bar, and then select **SANnav Monitoring** > **Flow Telemetry Registration Management**.

   The **Chassis** page lists all chassis that are flow streaming capable. The **Chassis** page provides the maximum Flow capacity for each chassis.



2. Choose one of the following options:

   - Select one or more chassis to register or unregister for flow statistics streaming, click the hamburger icon (☰) on the right side of the filter bar, and click **Register** or **Unregister**.
   - Locate the chassis that you want to register or unregister for flow statistics streaming, and click **Register** or **Unregister** from the action menu.

3. Check the flow registration status.

   The **Registration Status** column displays the status of the streaming registration for the chassis.

   SANnav checks the registration status every 15 minutes and updates the **Registration Status** column.

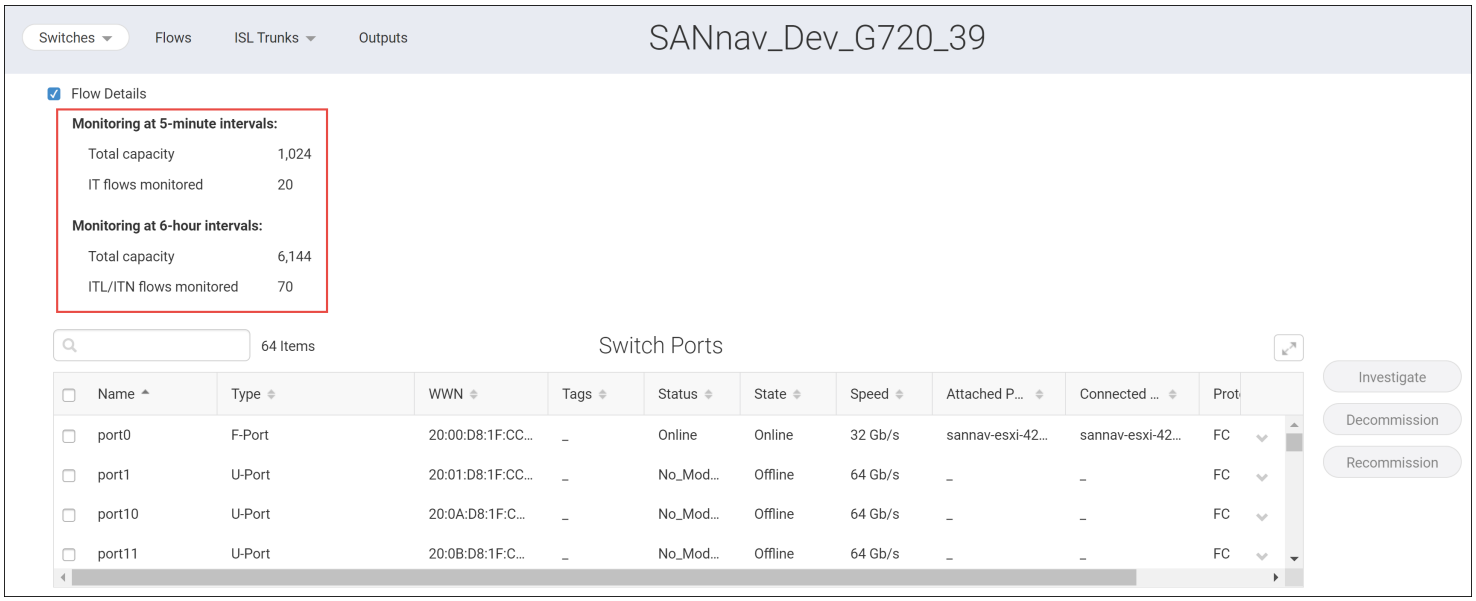
4. Update the Chassis registration view by clicking the refresh icon in the upper-right corner of the page.

Viewing Flow Capacity by Chassis

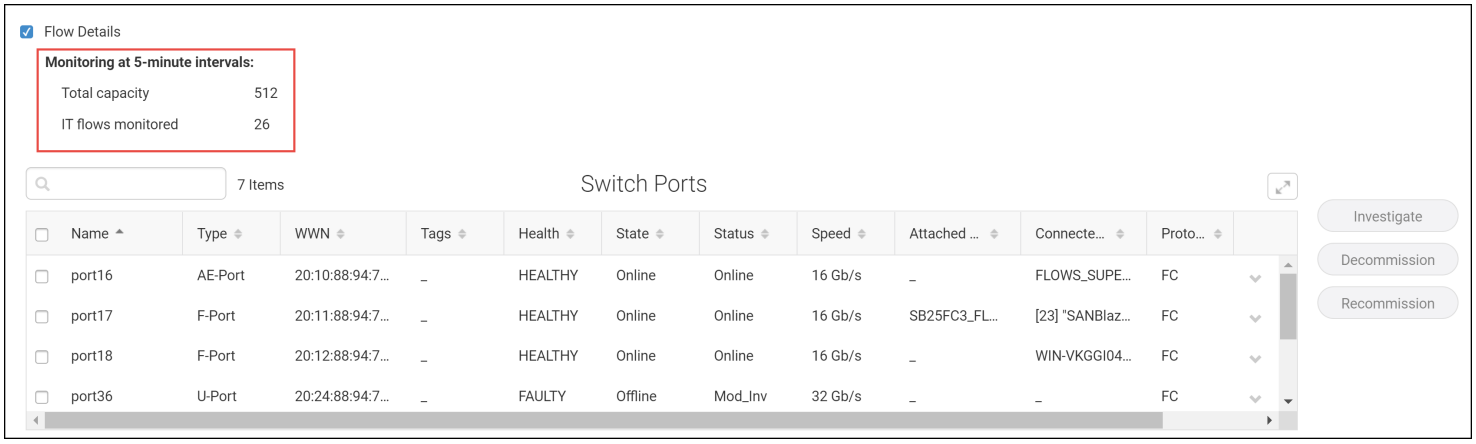
To view the number of flows that a chassis is monitoring, perform the following steps:

1. Click **SANnav** in the navigation bar, and then select **SANnav Monitoring** > **Flow Telemetry Registration Management**.
2. Locate the chassis that you want to unregister from flow statistics streaming, and click **View** from the action menu.
3. Scroll down and select the Flow Details check box.

   For Gen 7 platforms, information on the number of currently monitored flows, and total flow capacity for each 5-minute or 6-hour interval displays as shown the following figure:



For Gen 6 platforms, the Flow Details display information on IT flows at the 5-minute interval as shown in the following figure:



The flow count (IT, ITL, ITN, VITL, and VITN flow counts) is displayed across all logical switches in SANnav.

NOTE
For a list of platforms that support flow streaming, see Supported Hardware and Software.

Flow Dashboard Management

You can create a Flow dashboard using the IO Health & Latency widget. The IO Health & Latency widget is available in the **Status** widget category.

The IO Health & Latency widget in SANnav provides visibility into the IO health of host and storage ports across managed fabrics. The IO Health & Latency widget computes the IO health of host and storage ports and displays the degraded host or storage port based on the MAPS IO Health and IO Latency categories rules.

Based on the configured MAPS policy, a switch sends flow violation data every five minutes. The flow violation data is consumed and processed by SANnav. SANnav determines the IO Health and Latency of the host and storage ports based on the violations of the associated flows, during the selected time period in the dashboard. You can set the time period as the last 30 minutes, 1 hour, or 2 hours. SANnav performs the IO health calculation every five minutes and is only supported for Gen 7 platforms running Fabric OS v 9.2.x or later. For additional information about flow metrics, see SANnav Flow Metrics.

The IO Health & Latency widget classifies the host and storage ports into following three degraded categories:

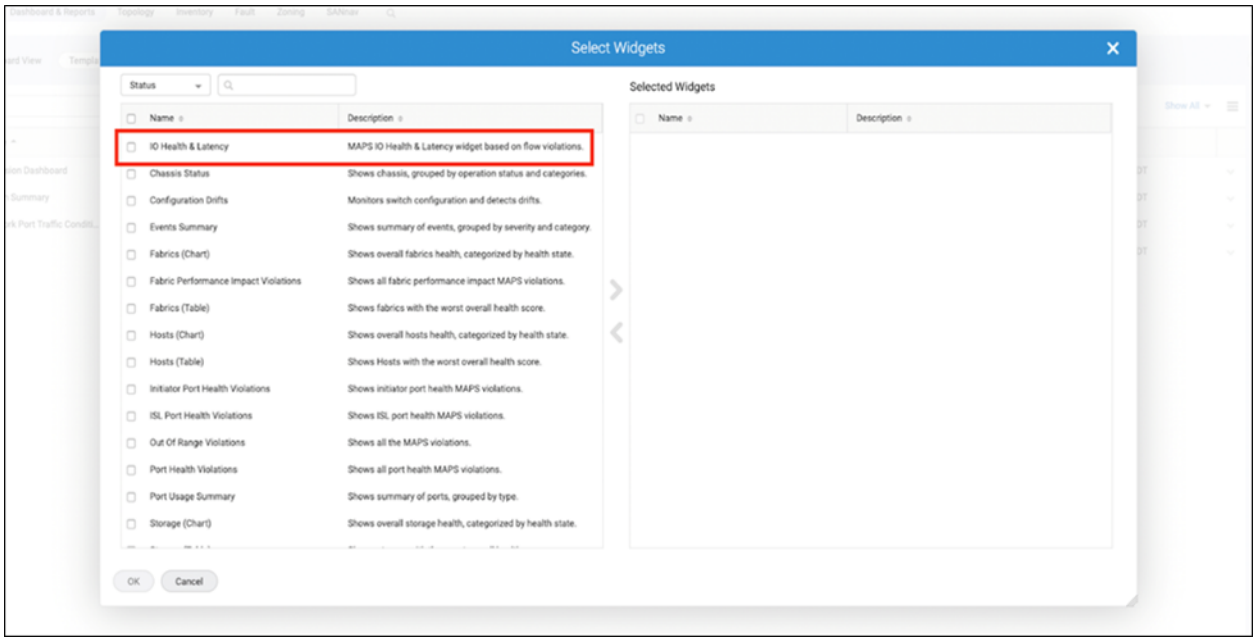
- Severely Degraded
- Degraded
- Marginally Degraded

Creating a Flow Dashboard

You can create a custom flow dashboard using the predefined IO Health & Latency widget. You can save the dashboard and access it at any time to monitor and troubleshoot flow streaming.

You must have the Dashboards and Reports privilege with read/write permission to create a custom dashboard.

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. Select the **IO Health & Latency** widget from the **Status** category, and click the right arrow to move them to the **Selected Widgets** list.
4. Click **OK**. The **Create New Dashboard Template** page displays with the IO Health & Latency widget.
5. Click **Save** > **Save** to preserve this dashboard. Enter a name for the dashboard (such as, Flow - IO Health & Latency Dashboard).
6. Enter tag and a description for the dashboard, if necessary.
7. Select the **Shared** checkbox to make the dashboard available to other SANnav users.
8. Click **Save**.

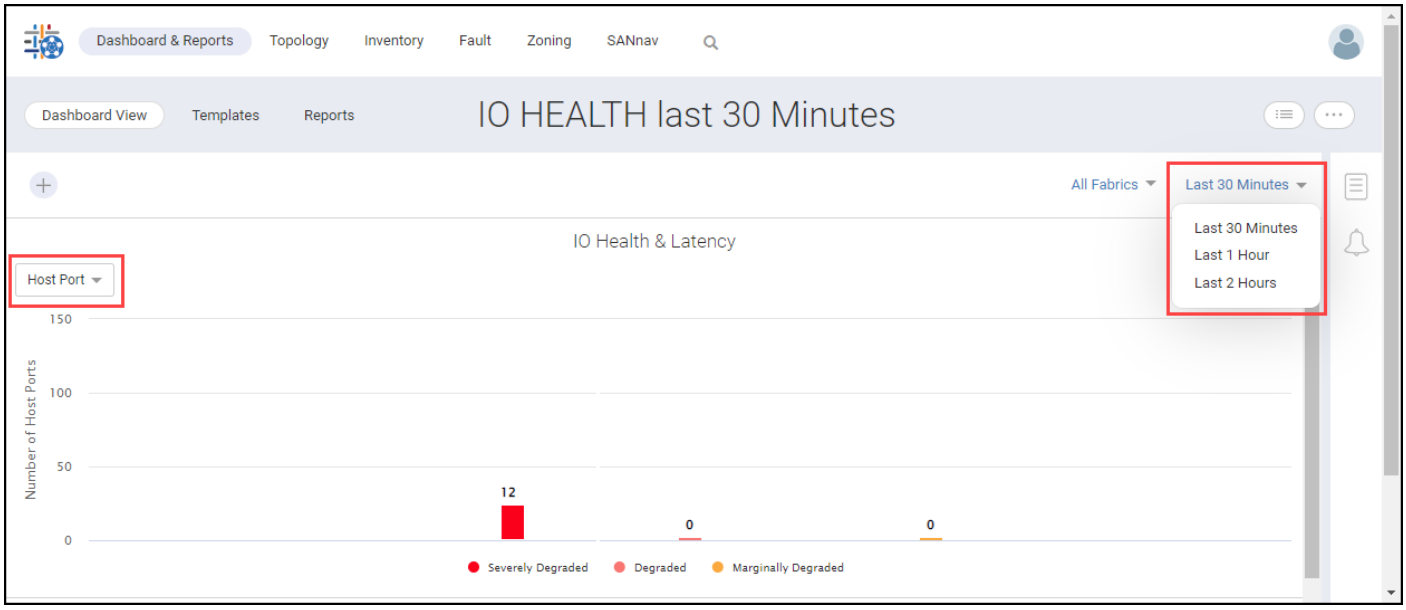
   The dashboard is saved with the provided name. To view the live dashboard, click the more icon (...) and select **View in Dashboard**.

Monitoring IO Health and Latency

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
2. Click the **Select Dashboad** icon on the right side of the subnavigation bar, select the Flow dashboard, and then click **OK**.

   A dynamic view of the Flow dashboard displays. The network scope is all fabrics, and the date range is the last 30 minutes, but you can change these settings.

   The IO Health & Latency widget shows the count of host or storage ports in the severely degraded, degraded, and marginally degraded categories. For each category, one bar displays with the total number of host or storage ports in the category. For example, in the following image, there are 12 host ports which are severely degraded and zero host ports which are degraded and marginally degraded.



NOTE

The IO Health & Latency widget has the following limitations:

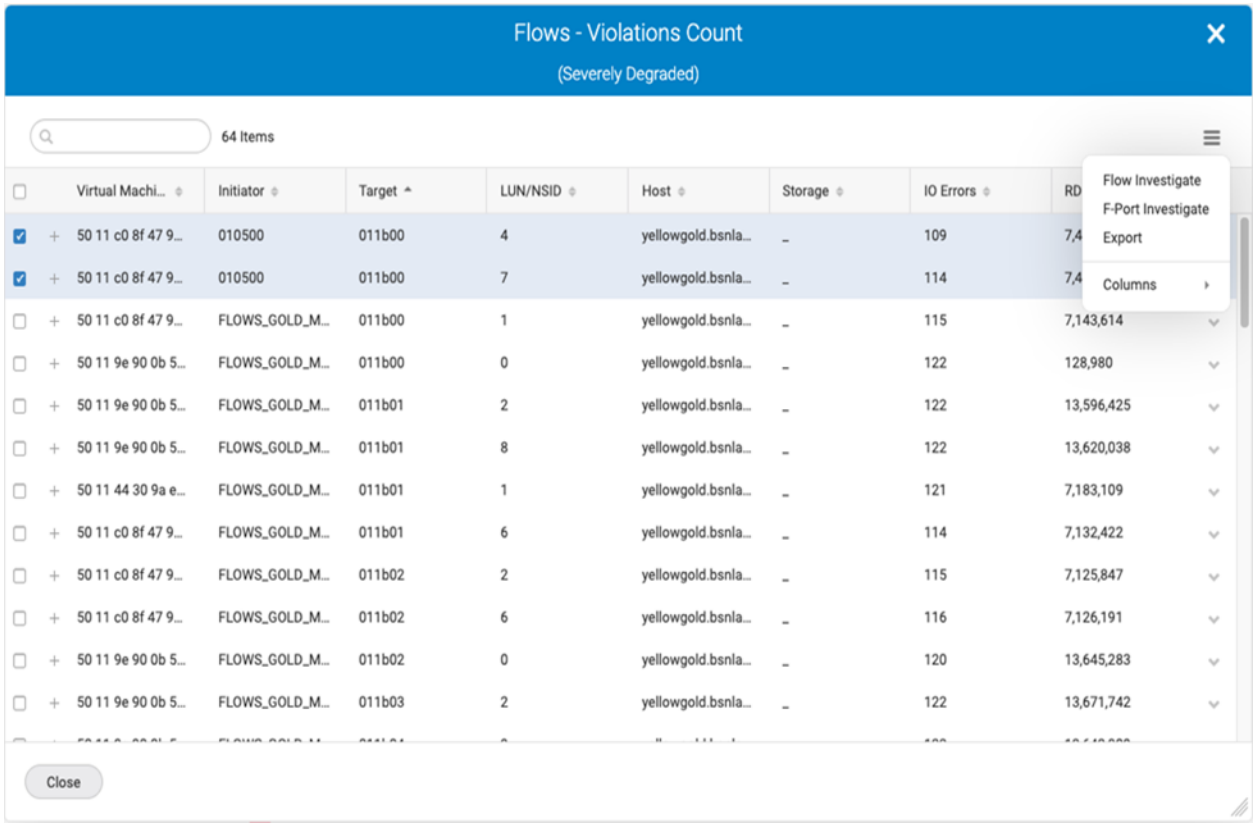
- The fabric scope and filter are not applicable for this widget.
- This widget can be viewed only in live Dashboard.
- If you restart SANnav, the widget data is computed from the time of the restart.

Investigating IO Health and Latency

SANnav supports launching Investigation mode for flows. You can investigate a flow or the associated switch F_Ports for the flow.

1. From the IO Health & Latency widget, click a bar to view the flow violations for the degraded host or storage ports in table format.

   The **Flows – Violations Count** (<*degraded_category*>) details page displays the list of flow violations for the degraded host or storage ports along with the corresponding violation count of each measure during the selected time period.



   By default, the **Flows – Violations Count** (<*degraded_category*>) details page shows the key flow information and a few select violation measures. You can customize columns to see the violation counts for various measures similar to customizing columns in the Inventory view.

   NOTE
   One or more violation measures can be zero when there are no violations for the measure or the MAPS rule is not configured.

2. Select the flows that you want to investigate by choosing one of the following options:

   - Select the checkboxes for the flows that you want to investigate.
   - Click the **+** icon at the left of every row for each flow that you want to investigate.

     As you click the icons, the **+** symbol changes to a **–** symbol, and the sidebar icon increments the count of selected items.

NOTE
No measures are pre-selected in the Investigation Mode page. For ITL/VITL/ITN/VITN flows, the violation metrics data is available at 5-minute intervals; however, the other metric data is only available at 6-hour intervals.

3. Investigate flows by clicking the hamburger icon, and selecting **Flow Investigate**.

   You can use investigation mode to view the historical or real-time statistics. For additional details and instructions, see Flow Investigation.

4. Investigate the connected switch F_Ports for a flow by clicking the hamburger icon, and selecting **F-Port Investigate**.

   You can use the switch port investigation view for the Initiator and Target ports that are associated with the selected flows. For a given flow, there are usually two switches (managed in SANnav), connecting to host and storage ports. If SANnav does not manage one of the switches, the port investigation view is launched with the F-Port of the managed switch only.

   NOTE
   No measures are pre-selected in the switch port Investigation Mode page.

5. Export the flow violations by clicking the hamburger icon in the upper-right corner, and clicking Export.

   The exported file is downloaded to your local machine. The file is in CSV format.

Flow Inventory

The SANnav Inventory page displays flows with the corresponding latest statistics based on an applied flow filter. When you launch the flow Inventory page the first time, the flow Inventory page displays no data. You must apply one or more filters to see flows in the flow inventory list page.

Creating a Flow Filter

Because of the potentially large number of possible flows, the SANnav Flow Inventory does not show any flows by default. You can add an existing flow filter or you can create a flow filter to view flows of interest. Filters allow you to specify criteria for selecting the flows of interest. For example, if you want to see all flows starting at a specific initiator, you can create an ITL filter specifying the Initiator and apply it.

Typically, you do not use the Flow Inventory for exploratory use cases as there could be up to 150,000 flows on the SANnav server at anytime. Therefore, the SANnav Flow Inventory is meant to be used for specific use cases, most notably troubleshooting use cases. The following details two typical use cases that are common for viewing Flow Inventory.

1. From the IO Health & Latency widget which identifies the Initiators and Targets having associated severely or degraded violated flows. In this case, use the Flow Inventory filters to search flows based on the Initiator zone alias name or the Target zone alias name to view all flows going through these ports.
2. From the NPTC Dashboard when a congested or oversubscribed port is identified. In this case, when viewing the information on the F_Port impacted, determine the zone that it belongs to and then search the Flow Inventory to list the flows associated with that zone.

The following flow filters are available in SANnav:

- ITL
- Virtual Machines
- Zone Alias
- Active Zone
- Attached Switch Port

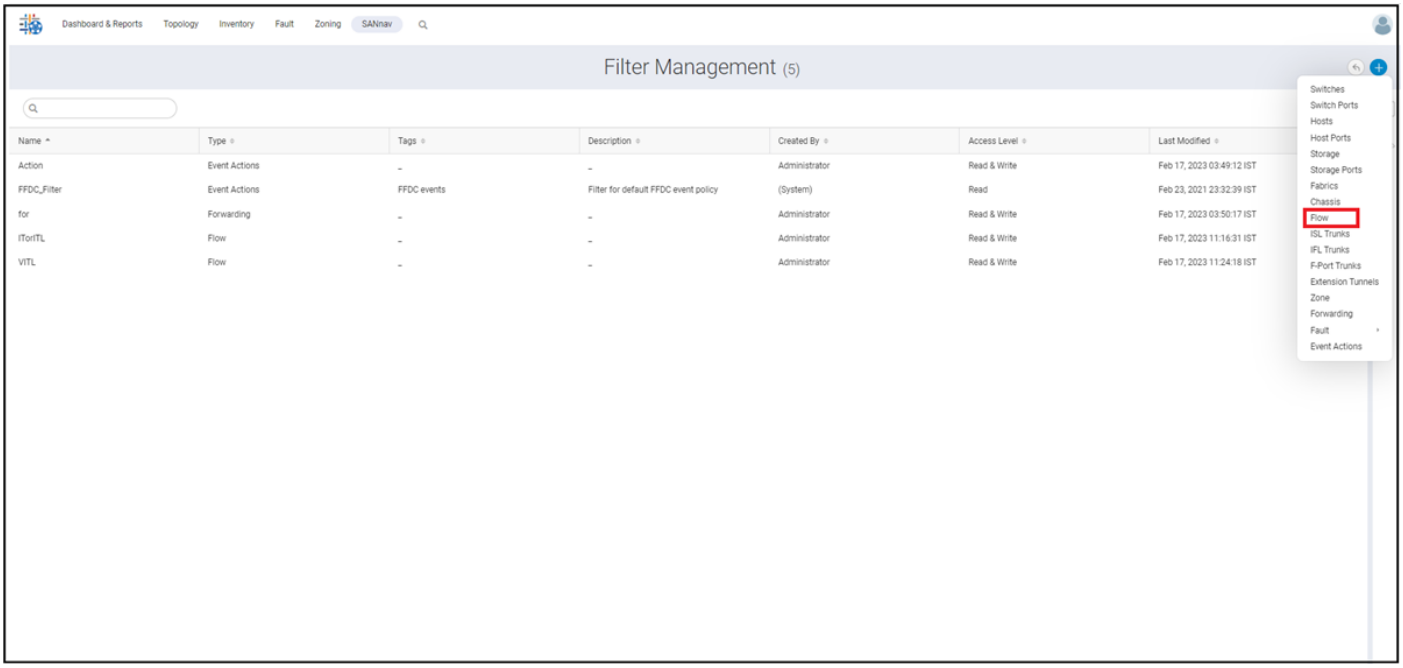
To add a flow filter, complete the following steps:

1. Click **Inventory** in the navigation bar, and then select **Flows**.
   The **Flows** page appears.
2. Select the plus sign (+) from the **Flows** page. The **Add Filter** dialog appears.
3. You can select any of the existing flow filters. To create a flow filter, click **Create New Flow Filter**.
   The **Create New Flow Filter** dialog appears.

   Alternatively, you can create a flow filter using the following steps:
4. Select **SANnav** from the navigation bar, and then select **SAN Monitoring** > **Filter Management**.

   The **Filter Management** page appears, and shows a list of all the current flow filters.

5. Click the plus sign (+) to display a list of filter types. The following figure shows an example list:

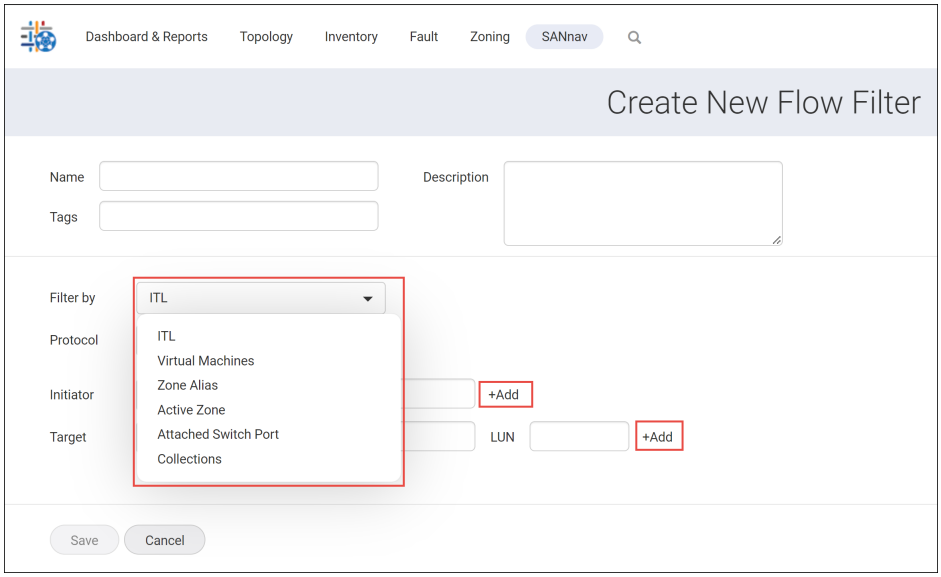


6. Select **Flow** from the **Filter Management** page.

   The **Create New Flow Filter** dialog appears.

   NOTE
   You can add up to 40 Initiators and up to 40 Targets for each filter type such as ITL, Virtual Machines, Zone Alias, Active Zone, and Attached Switch Port.

7. Click **Filter by** from the **Create New Flow Filter** dialog to select a filter category. The following figure shows the list of **Filter by** options:



Each **Filter by** category type (ITL, Virtual Machines, Zone Alias, Active Zone, and Attached Switch Port) has different inputs.

NOTE

- Leave the **LUN** field blank to filter IT flows.
- Use a specific filter value instead of an asterisk (*). When you use an asterisk (*) as a filter parameter, the response can take more than 60 seconds depending on the flow scale.
- SANnav uses the type-ahead functionality; Once you enter three characters, the associated fields appear.

8. Complete the filter field values.
9. Select **Save Filter** to save the flow filter for the future use.

   If you do not save the flow filter, the filter is applied only for the current session.
10. Click **OK**.

    The **Filter Management** page shows the new flow filter.

Flow Filters

The following sections provide additional detail for each type of flow filter as well as usage examples.

ITL Flow Filter

The **ITL** flow filter is an Initiator and Target-based filter. Each parameter can have one or more Initiators or Targets with or without the LUN or NSID. The following table describes the parameters that you use to create an **ITL** flow filter.

Table 7: ITL Flow Filter Parameters

Parameter	Description
Protocol	Describes the supported protocols. You can select any of the following protocols: • SCSI – Filters only SCSI device flows • NVMe – Filters only NVMe device flows • SCSI/NVMe – Filters both SCSI and NVMe device flows
Initiator	Describes the following Initiator port details: • WWN • FC Address
Target	Describes the following Target port details: • WWN • FC Address
LUN/NSID	Describes the following LUN/NSID details: • LUN (for the SCSI storage) • NSID (for the NVMe storage) If you leave this field blank, then only the IT flows are fetched.

For LUN, you can enter any number or range. The following table contains a few examples using the filter and their results.

Table 8: LUN Examples

LUN Usage Example	Comments
23	Using a single LUN – The filter fetches the ITL/VITL flow having LUN 23.
1,2,5	Using multiple LUNs – The filter fetches the ITL/VITL flows having LUN 1 or 2 or 5.

LUN Usage Example	Comments
1-20	Using a LUN range – The filter fetches the ITL/VITL flows having LUNs in the range from 1 to 20.
1-20,40-100	Using multiple LUN ranges – The filter fetches the ITL/VITL flows having multiple LUNs ranging from 1 to 20, and 40 through 100.
1-20,50,70-100	Using a combination of LUN range and specific LUN – The filter fetches the ITL/VITL flows having LUNs ranging from 1 to 20, the specific LUN 50, and ranging from LUNs 70 through 100.
*	Using an asterisk (*) – The filter fetches all the ITL/VITL flows. The filter does not fetch IT flows.
LUN	Empty – The filter fetches only IT flows. The filter does not fetch ITL/VITL flows.

The following tables contain a few examples using the **ITL** flow filter options and their results when you create a flow filter.

Table 9: ITL Flow Filter – Usage Example 1

Parameter	Description
Filter Options	A flow filter is created with two Initiators (Initiator 1 and Initiator 2), two Targets (Target 1 and Target 2), and an empty LUN with the SCSI protocol.
Result	Fetches all the SCSI IT flows with the following filter type combinations: • Initiator 1, Target 1; Initiator 1, Target 2 • Initiator 2, Target 1; Initiator 2, Target 2

Table 10: ITL Flow Filter – Usage Example 2

Parameter	Description
Filter Options	A flow filter is created with two Initiators (Initiator 1 and Initiator 2), two Targets (Target 1 and Target 2), and a LUN as an asterisk (*) with the SCSI protocol.
Result	Fetches all the SCSI ITL flows with the following filter type combinations: • Initiator 1, Target 1, all LUN flows; Initiator 1, Target 2, all LUN flows • Initiator 2, Target 1, all LUN flows; Initiator 2, Target 2, all LUN flows

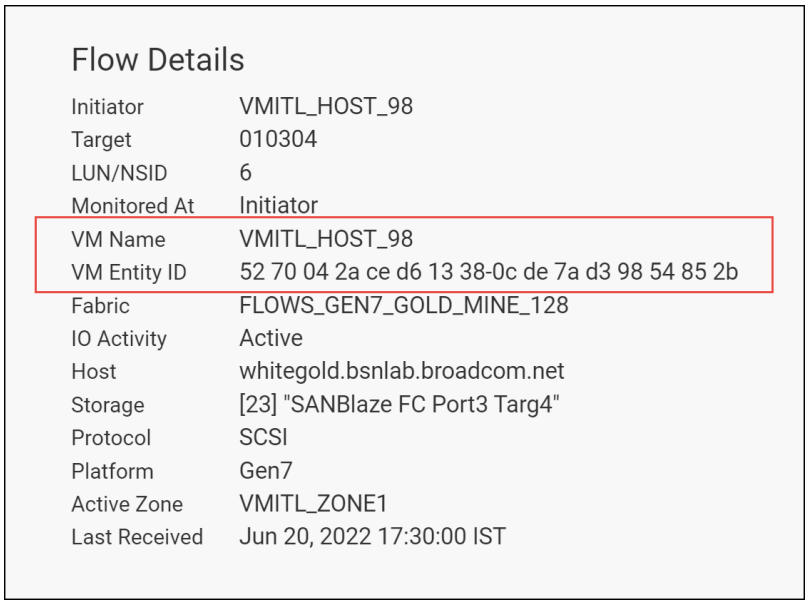
Table 11: ITL Flow Filter – Usage Example 3

Parameter	Description
Filter Options	A flow filter is created with two Initiators (Initiator 1 and Initiator 2), two Targets (Target 1 and Target 2), and a LUN as 3 for both SCSI and NVMe protocols.
Result	Fetches all the SCSI and NVMe ITL/ITN flows with the following filter type combinations: • Initiator 1, Target 1 LUN/NSID 3; Initiator 1, Target 2 LUN/NSID 3 • Initiator 2, Target 1 LUN/NSID 3; Initiator 2, Target 2 LUN/NSID 3

Virtual Machines Flow Filter

The **Virtual Machines** flow filter is a VM-based filter that presents the VITL/VITN flows on a given port. The **Virtual Machines** flow filter can have one or more Initiators or Targets with a LUN or NSID. The following table describes the parameters that you use to create a **Virtual Machines** flow filter.

Table 12: Virtual Machines Flow Filter Parameters

Parameter	Description
Protocol	Describes the supported protocols. You can select any of the following protocols: • SCSI – Filters only SCSI device flows • NVMe – Filters only NVMe device flows • SCSI/NVMe – Filters both SCSI and NVMe device flows
Virtual Machine	Describes the supported parameters that are used to identify a virtual machine. You can select any of the following parameters: • Entity ID – A unique 128-bit universal identifier that is used to represent the VM. The Entity ID is displayed in a non-human readable VM Entity ID format if the vCenter server is not discovered in SANnav. For example, 52 70 04 2a ce d6 13 38-0c de 7a m4 89 42 58 b2. • Name – The name of the virtual machine that is discovered through vCenter and associated with the given Entity ID. If the VM name is determined through the SANnav vCenter discovery, the following SANnav interfaces display a human-readable VM name for the VITL/VITN flows: – Flow Inventory – Flow Reports – Flow Investigation Mode The following figure shows an example with **VM Name** and **VM Entity ID** in the **Flow Details** dialog for a selected flow: 
Initiator	Describes the following Initiator port details: • WWN • FC Address
Target	Describes the following Target port details: • WWN • FC Address

Parameter	Description
LUN/NSID	Describes the following LUN/NSID details: • LUN (for the SCSI storage) • NSID (for the NVMe storage) If you leave this field blank, then all the VITL/VITN flows are fetched where V, I, and T matches the values of Virtual Machine, Initiator, and Target specified in the filter.

The following tables contain a few examples using the **Virtual Machines** flow filter options and their results when you create a flow filter.

Table 13: Virtual Machines Flow Filter – Usage Example 1

Parameter	Description
Filter Options	A flow filter is created with a specific Entity ID, an Initiator, and a Target with an empty value, a LUN with an asterisk (*) value, and the SCSI protocol.
Result	Fetches all the VITL/VITN flows specific to the selected Entity ID.

Table 14: Virtual Machines Flow Filter – Usage Example 2

Parameter	Description
Filter Options	A flow filter is created with two Entity IDs, an Initiator and a Target with an empty value, a LUN with an asterisk (*) value, and the SCSI protocol.
Result	Fetches all the VITL/VITN flows specific to the two selected Entity IDs.

Table 15: Virtual Machines Flow Filter – Usage Example 3

Parameter	Description
Filter Options	A flow filter is created with an Entity ID with an asterisk (*) value, an Initiator, a Target with an empty value, a LUN with an asterisk (*) value, and the SCSI protocol.
Result	Fetches all the VITL/VITN flows.

Table 16: Virtual Machines Flow Filter – Usage Example 4

Parameter	Description
Filter Options	A flow filter is created with an Entity ID with a wildcard value, an Initiator with a Port Identifier (PID), a Target with a PID, a LUN with an asterisk (*) value, and the SCSI protocol.
Result	Fetches all the VITL/VITN flows that are initiated from the specified Initiator PID and destined to the specified Target PID.

Table 17: Virtual Machines Flow Filter – Usage Example 5

Parameter	Description
Filter Options	A flow filter is created with an Entity ID with an asterisk (*) value, an Initiator, a Target with an empty value, a LUN with an asterisk (*) value, and the SCSI protocol. You can add an additional flow filter (for example, an ITL filter) along with the **Virtual Machines** flow filter.
Result	Fetches all the VITL/VITN flows along with the ITL flows specific to the selected ITL flow filter.

Zone Alias Flow Filter

You can use the **Zone Alias** flow filter if you know the zone alias name of the device ports. The following table describes the parameters that you use to create a **Zone Alias** flow filter.

Table 18: Zone Alias Flow Filter Parameters

Parameter	Description
Protocol	Describes the supported protocols. You can select any of the following protocols: • SCSI – Filters only SCSI device flows • NVMe – Filters only NVMe device flows • SCSI/NVMe – Filters both SCSI and NVMe device flows
Zone Alias	Describes the name of the Zone Alias. It can be an Initiator port alias or a Target port alias.
LUN/NSID	Describes the LUN number of the SCSI storage and Namespace ID if the storage is NVMe. If you leave this field blank, then only the IT flows are fetched.

The following tables contain a few examples using the **Zone Alias** flow filter options and their results when you create a flow filter.

Table 19: Zone Alias Flow Filter – Usage Example 1

Parameter	Description
Filter Options	A flow filter is created with two zone aliases and a LUN as empty with the NVMe protocol.
Result	Fetches all the NVMe IT flows based on the Initiator/Target port that is assigned to the given zone alias.

Table 20: Zone Alias Flow Filter – Usage Example 2

Parameter	Description
Filter Options	A flow filter is created with two zone aliases and a LUN as an asterisk (*) with the SCSI protocol.
Result	Fetches all the ITL/VITL flows based on the Initiators and Targets that participate in the given zone alias.

Attached Switch Port Flow Filter

You can use the **Attached Switch Port** flow filter to filter the flows that are passing through the F_Port. This filter fetches both IT and ITL, ITN, VITL, and VITN flows. The following table describes the parameters that you use to create an **Attached Switch Port** flow filter.

Table 21: Attached Switch Port Flow Filter Parameters

Parameter	Description
F_Port	Provides the device port that is connected to a switch port with an FC Address and WWN.

The following table contains an example of the usage of the **Attached Switch Port** flow filter options when you create a flow filter and its result.

Table 22: Attached Switch Port Flow Filter – Usage Example

Parameter	Description
Filter Options	A flow filter is created with two F_Port FC addresses.
Result	Fetches both IT and ITL, ITN, VITL, and VITN flows based on the Initiators or Targets that are connected to the given F_Ports.

Active Zone Flow Filter

You can use the **Active Zone** flow filter to filter the flows that are using a specific zone. The following table describes the parameters that you use to create an **Active Zone** flow filter.

Table 23: Active Zone Flow Filter Parameters

Parameter	Description
Protocol	Describes the supported protocols. You can select any of the following protocols: • SCSI – Filters only SCSI device flows • NVMe – Filters only NVMe device flows • SCSI/NVMe – Filters both SCSI and NVMe device flows
Active Zone	Describes the name of the Active Zone.
LUN/NSID	Describes the LUN number of the SCSI storage and Namespace ID if the storage is NVMe. If you leave this field blank, then only the IT flows are fetched.

The following tables contain a few examples using the **Active Zone** options and their results when you create a flow filter.

Table 24: Active Zone Flow Filter – Usage Example 1

Parameter	Description
Filter Options	A flow filter is created with two active zones and LUN as empty with the SCSI protocol.
Result	Fetches all the IT flows based on the Initiators and Targets that participate in the given two active zones.

Table 25: Active Zone Flow Filter – Usage Example 2

Parameter	Description
Filter Options	A flow filter is created with two active zones and LUN as an asterisk (*) with the SCSI protocol.
Result	Fetches all the ITL/VITL flows based on the Initiators and Targets that participate in the given active zone.

Managing Flow Inventory

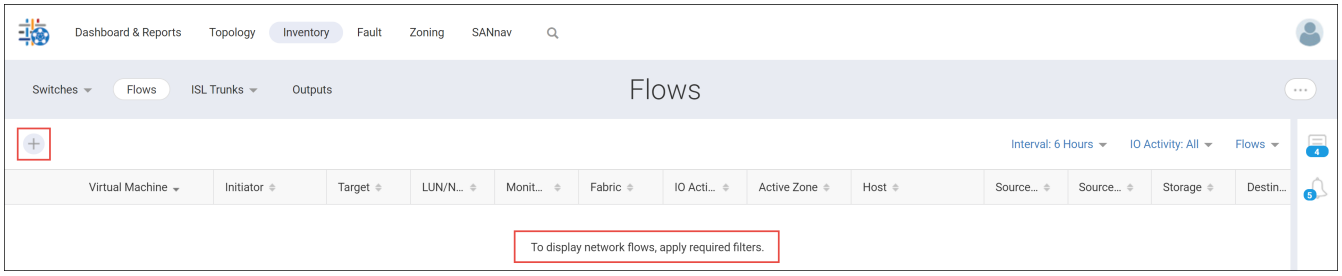
The **Flows** page, which is accessed through the **Inventory** page, displays flows in table format. From the **Flows** page, you can monitor all flows with the latest statistics.

The following high-level actions on the flows are enabled:

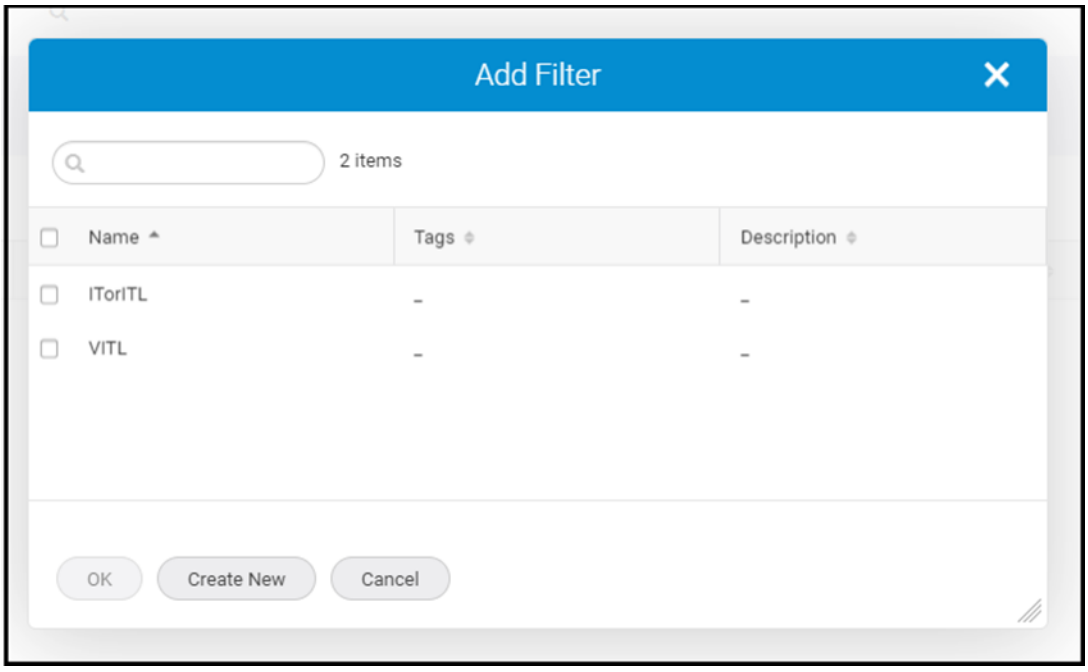
- View detailed statistics and inventory-related information for a given flow.
- View historical or real-time statistics for one or more flows (investigation mode).
- Select one or more flows in the selection sidebar for the later investigation.

To explore the **Flows** list page, perform the following steps:

1. Click **Inventory** in the navigation bar, and then click **Flows** from the subnavigation bar.
   The **Flows** page displays. By default, the **Flows** page shows no flows. You must apply at least one filter to view flows.



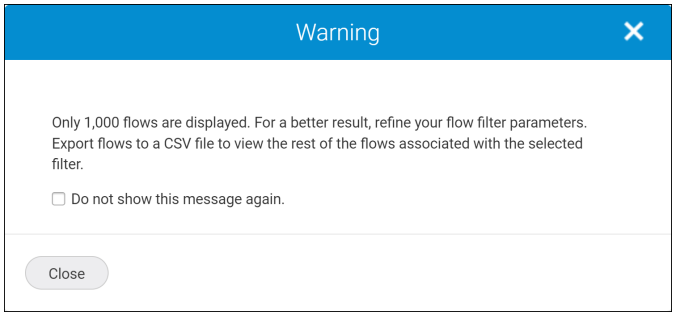
2. Click the plus sign (+) to add a filter.
   The **Add Filter** dialog displays, and you can see a list of previously saved flow filters.
3. Click **Create New** to create a filter.



You can apply more than one filter at a time, although the recommended maximum is three. When you apply more than one filter, the filter displays flows that meet *any* of the filter criteria.

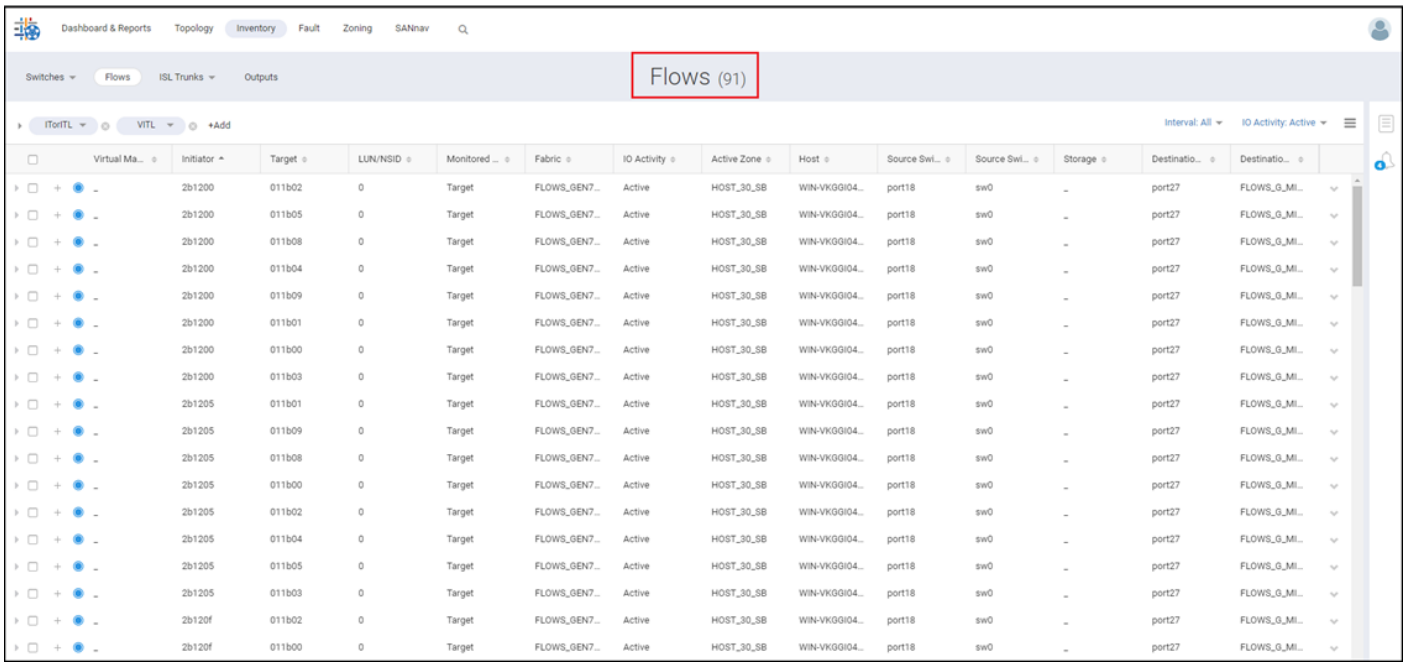
4. Select a filter or create a filter.

   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** option.



5. Click **OK**.

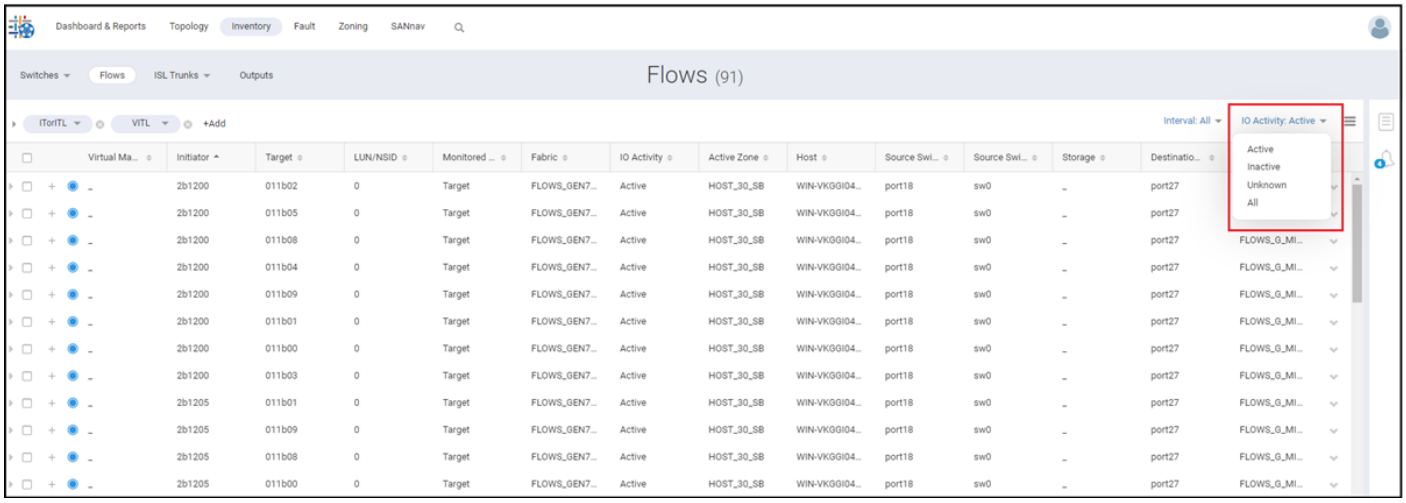
   The **Flows** page displays. The contents reflect the filters that you selected as shown in the following figure:



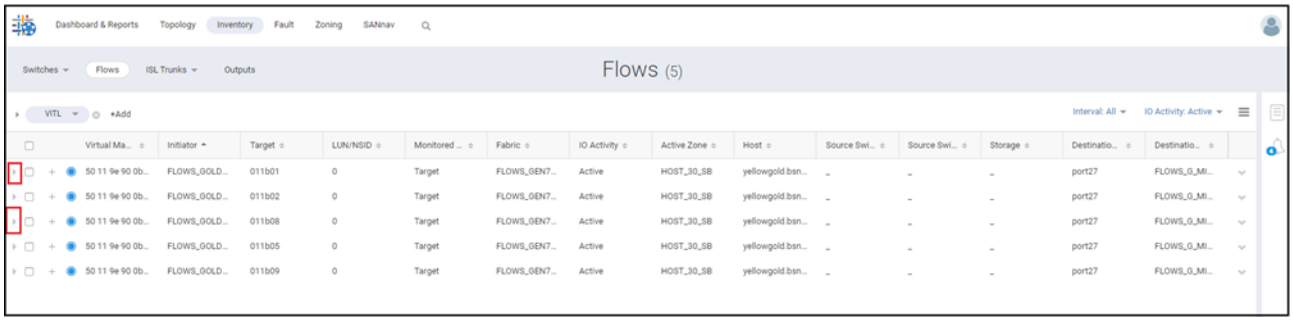
Flow statistics are received from the switch every 5 minutes or 6 hours. Their status (represented by **IO Activity** as shown in the figure) may be either Active, Inactive, or Unknown. The description of each **IO Activity** status is as follows:

- A flow that is tagged as *Active* represents the presence of active traffic on this flow.
- A flow that is tagged as *Inactive* represents the absence of active traffic on this flow. SANnav determines the *Inactive* state based on the number of I/O count in the streamed flow (IT flows for 5 minutes, and ITL, ITN, VITL, and VITN flows for every 6 hours).
- A flow that is tagged *Unknown* represents a flow that is no longer streamed to SANnav, or SANnav is no longer receiving any data for the specific flow from the switch for a period. The period is determined by SANnav based on the number of I/Os in the streamed statistics. If the stream is not received in the past 10 minutes for IT flows or the past 7 hours for ITL, ITN, VITL, and VITN flows, then these flows are marked as *Unknown* in the Fabric OS flow stream.

The following figure shows the options that are listed in the **IO Activity** status:



6. Click the arrow that is associated with the flow to expand the details as shown in the following figure:

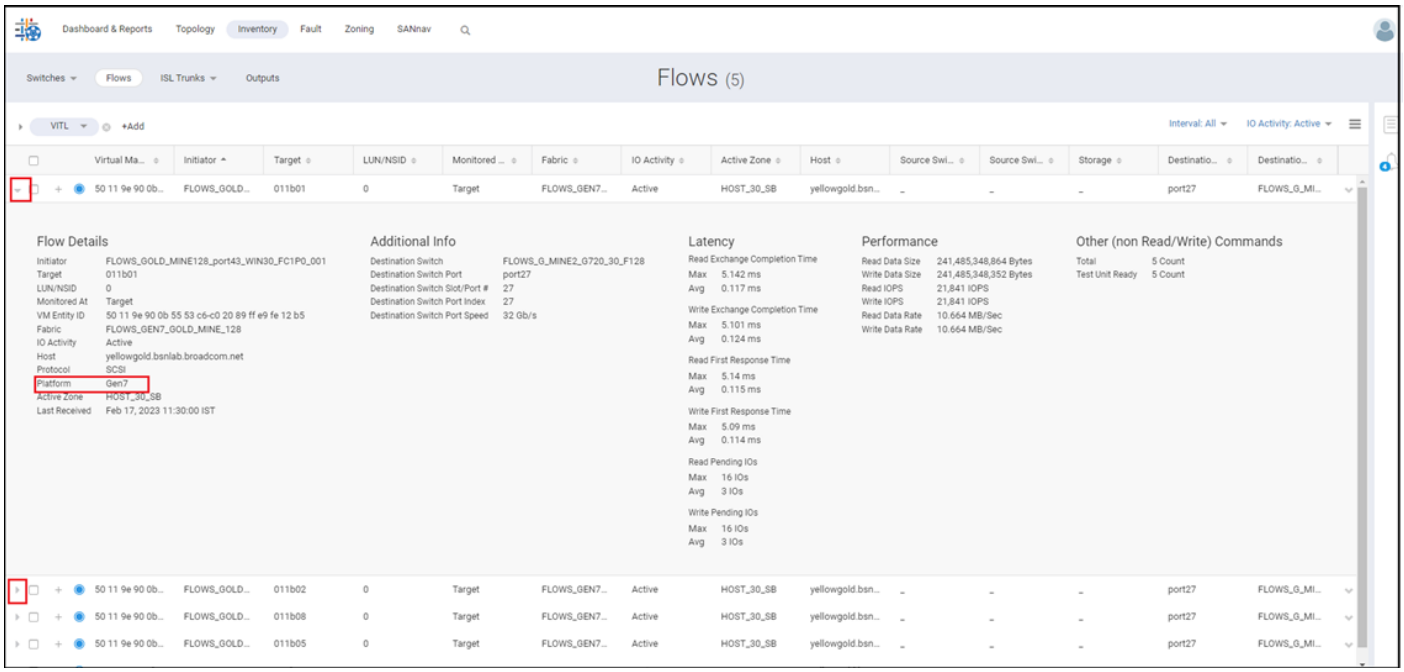


The resulting **Flows** page shows the statistics for the measures of an active or inactive flow that has been based on the selection in the **IO Activity** status at the top of the **Flows** page.

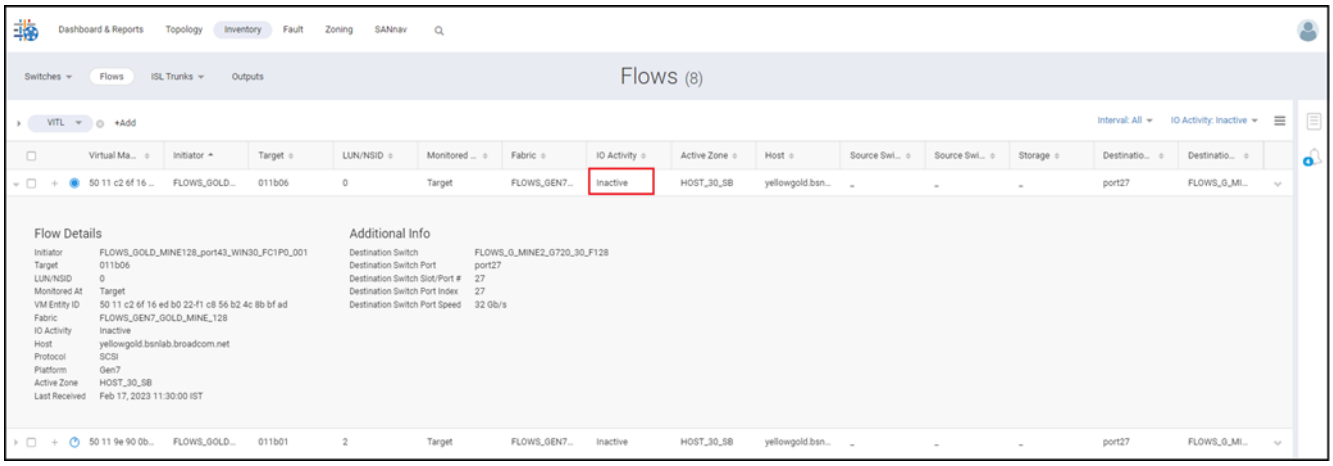
NOTE
Examples of different flows are examined in the following figures.

You can determine the generation of the switch platform (Gen 6 or Gen 7) that monitors the flow by referring to the **Platform** property. The valid values are Gen6 and Gen7. If the flow is monitored at the Gen 6 blade of a Gen 7 chassis, those flows are marked as a Gen 6 platform.

For an active flow, a page similar to the following displays:

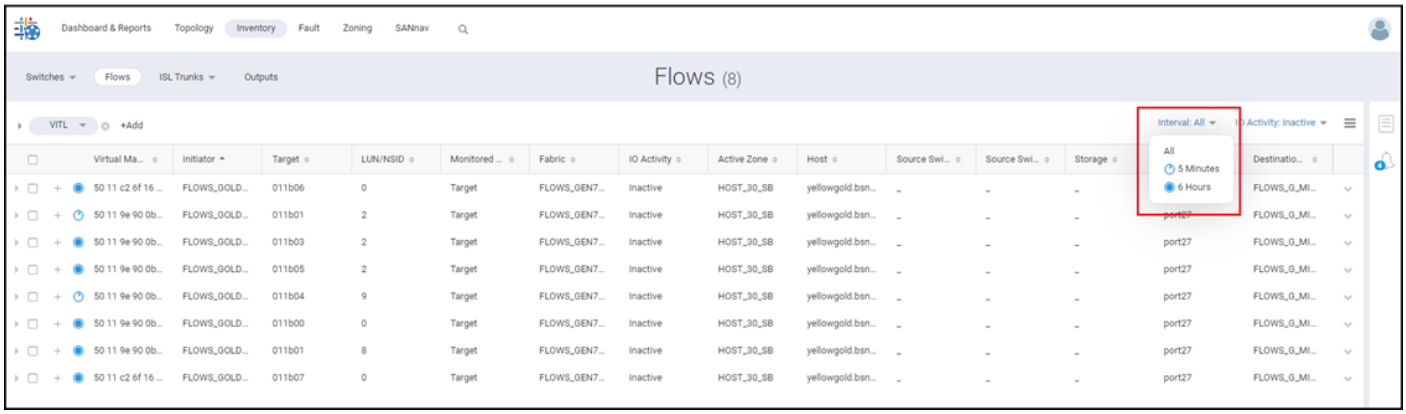


Measures with a value of 0 are excluded from the expanded view. For an inactive flow, a page similar to the following displays:



In the bottom portion of the expanded view, you can see the LUN size, LUN count (only for IT flows), Status, Active Zones, and so on. An active zone reflects the zone in which the Initiator and Target participate. Multiple active zones appear if both the Initiator and the Target participate in multiple active zones.

7. Select **5 Minutes** or **6 Hours** from the **Interval** list to filter the flows for different intervals. The following figure shows the **Interval** options:

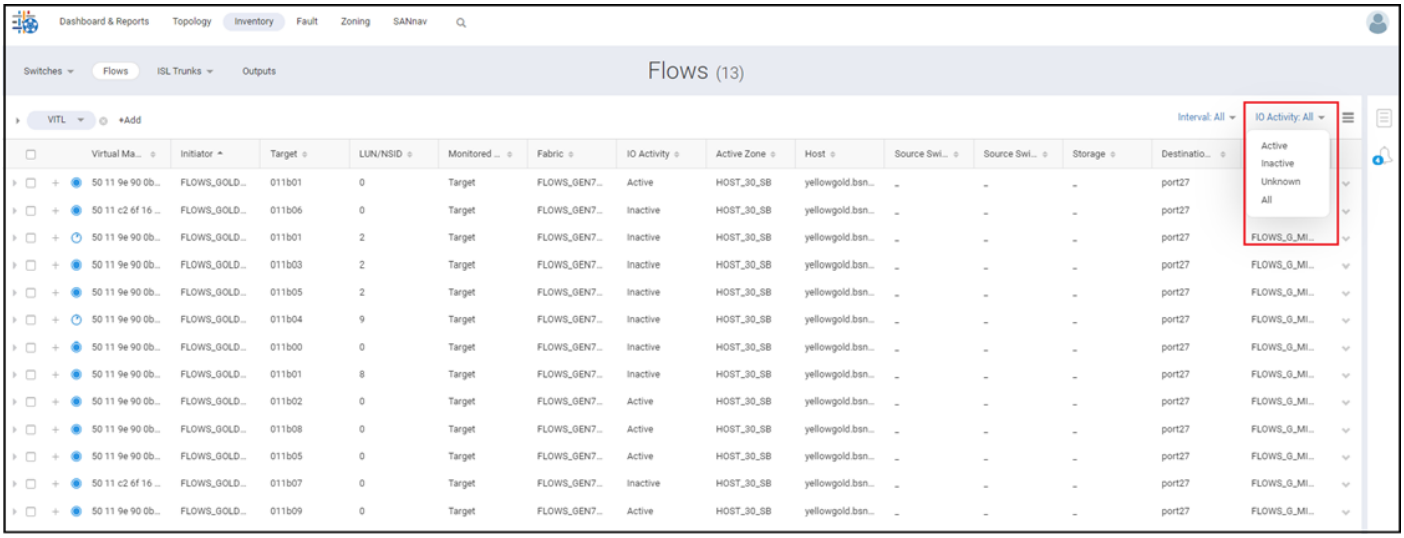


NOTE
For inactive flows, the interval icon displays the last interval that has been received from the switch before it moves to the inactive state.

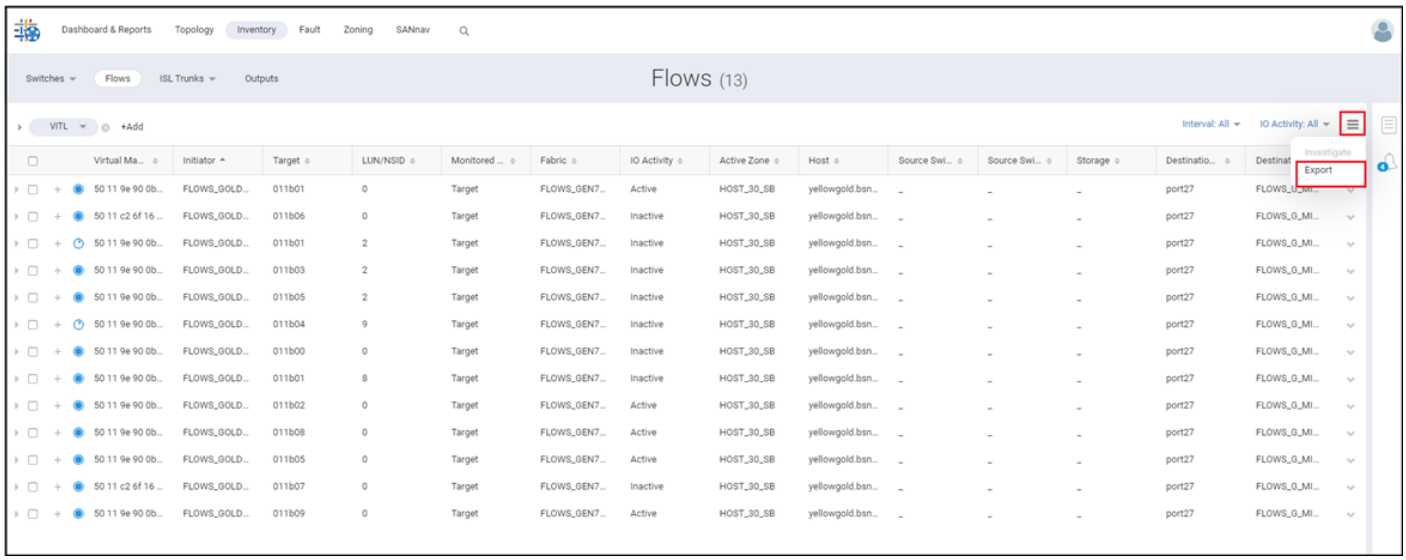
8. Hover over the icons in the list to view information about that icon.

   Select the **All** option (default) to list both 5-minute and 6-hour interval flows. The **All** option lists both active and inactive flows in the **IO Activity** column.

   The following figure shows the example of a mix of Active, Inactive, and Unknown type of flows:



9. Click the hamburger icon, and then click **Export** to export the flows applicable for a specific filter into a CSV file.



NOTE
If no filter is applied or no filter flows are displayed for a given filter, the **Export** selection is disabled.

NOTE
When the CSV files that are exported from SANnav are opened using Microsoft Excel, it may misinterpret and display the *Destination Switch Port* column and the *Source Switch Port* column (and possibly other columns) in the Date/Time format. Verify the exported data before you use it.

The exported file appears in your browser downloads file.

Flow Investigation

The Brocade SANnav **Investigation Mode** page provides the ability to view the historical statistics in a graphical representation. This feature helps you view the collected metrics over the selected duration for troubleshooting.

Performing Flow Investigation

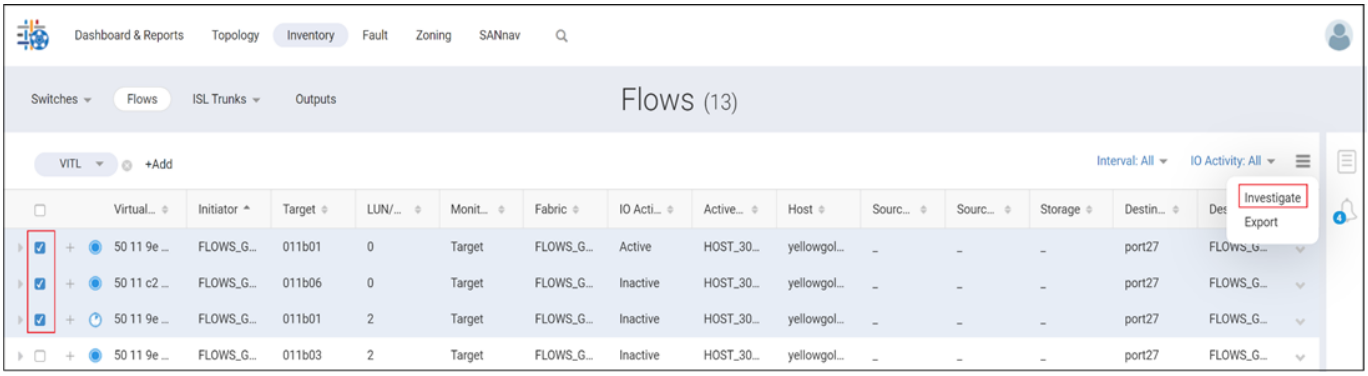
The **Investigation Mode** page is where you can examine one or more flows in real time or in a historical date range and can identify the root cause of issues. To explore **Investigation Mode**, perform the following steps:

> **NOTE**
> The following procedure is written based on the assumption that you have already applied one or more filters to view the relevant flows.

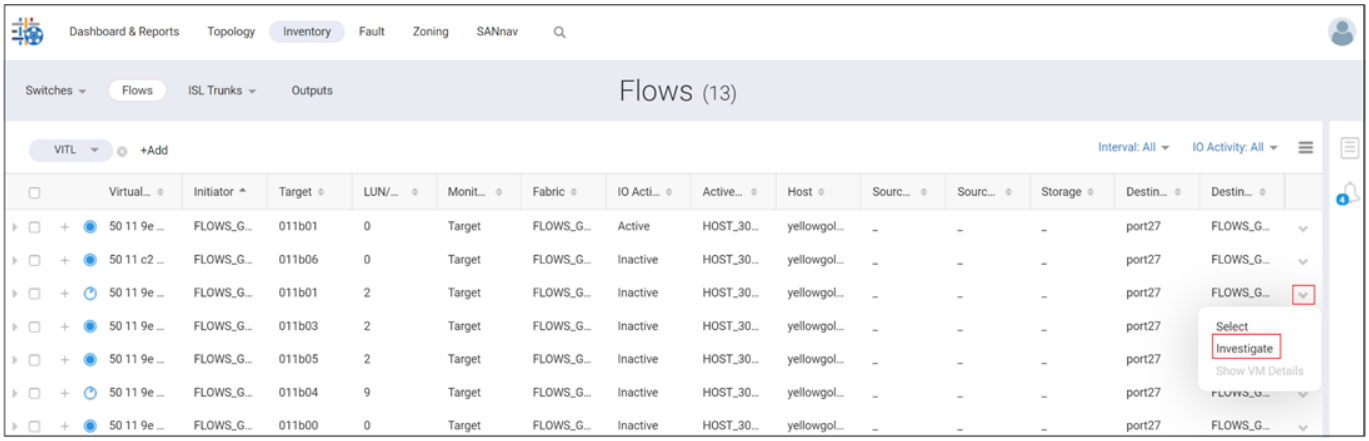
1. Click **Inventory** in the navigation bar, and then click **Flows** in the subnavigation bar.
2. Choose one of the following options:

   The **Investigate** selection is enabled if at least one flow is checked as shown in the following steps:

   - To investigate multiple flows, select two or more flow checkboxes, click the hamburger icon, and select **Investigate**.



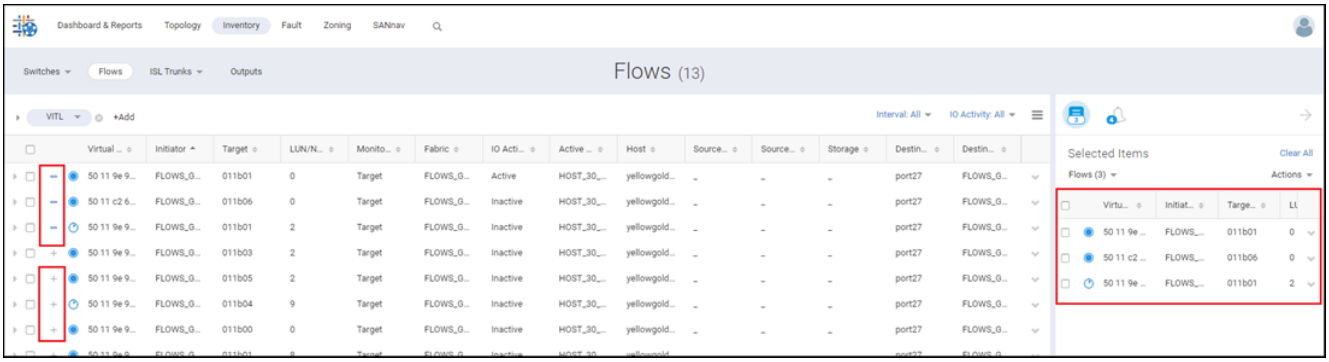
   - To investigate a single flow, click the down arrow in the right-most column for the flow, and select **Investigate** from the action menu.



   - To investigate one or more selected flows from the **Selected Items** sidebar, complete the following steps:

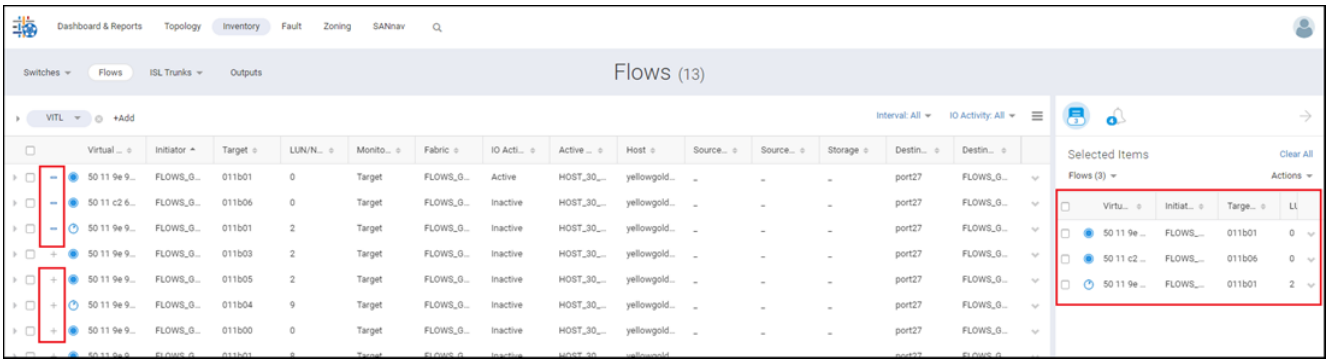
     a. Click the plus sign (+) to the left of a row in the table.

After you select an element, the plus sign (+) changes to a minus sign (-) as shown in the following figure:



The selected flow is added to the **Selected Items** sidebar. You can choose to investigate the flows now or later.

b. Click the **Selected Items** sidebar icon (see the previous figure) to display the elements under **Selected Items**. In this example, the **Selected Items** sidebar displays two flows that were moved to the sidebar.



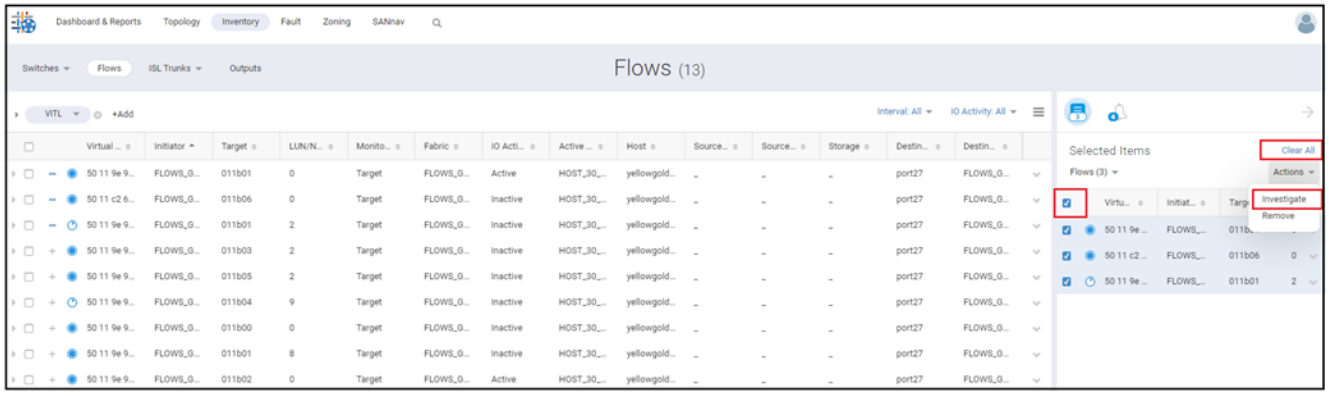
The selected items are available for investigation throughout the session. When you log out or the session expires, the **Selected Items** sidebar resets. Select from this set of flows and proceed to investigation.

NOTE

Clicking the arrow in the top right within the sidebar closes the **Selected Items** sidebar.

Click the minus sign (-) on the far left of the row in the table to remove the element from the **Selected Items** sidebar and converts the symbol to the plus sign (+). Alternatively, you can remove the element by selecting flows from the **Selected Items** sidebar and clicking **Remove** from the down arrow in **Selected Items**.

c. Select the flows in the **Selected Items** sidebar that you want to investigate and click **Investigate** from the **Actions** list.



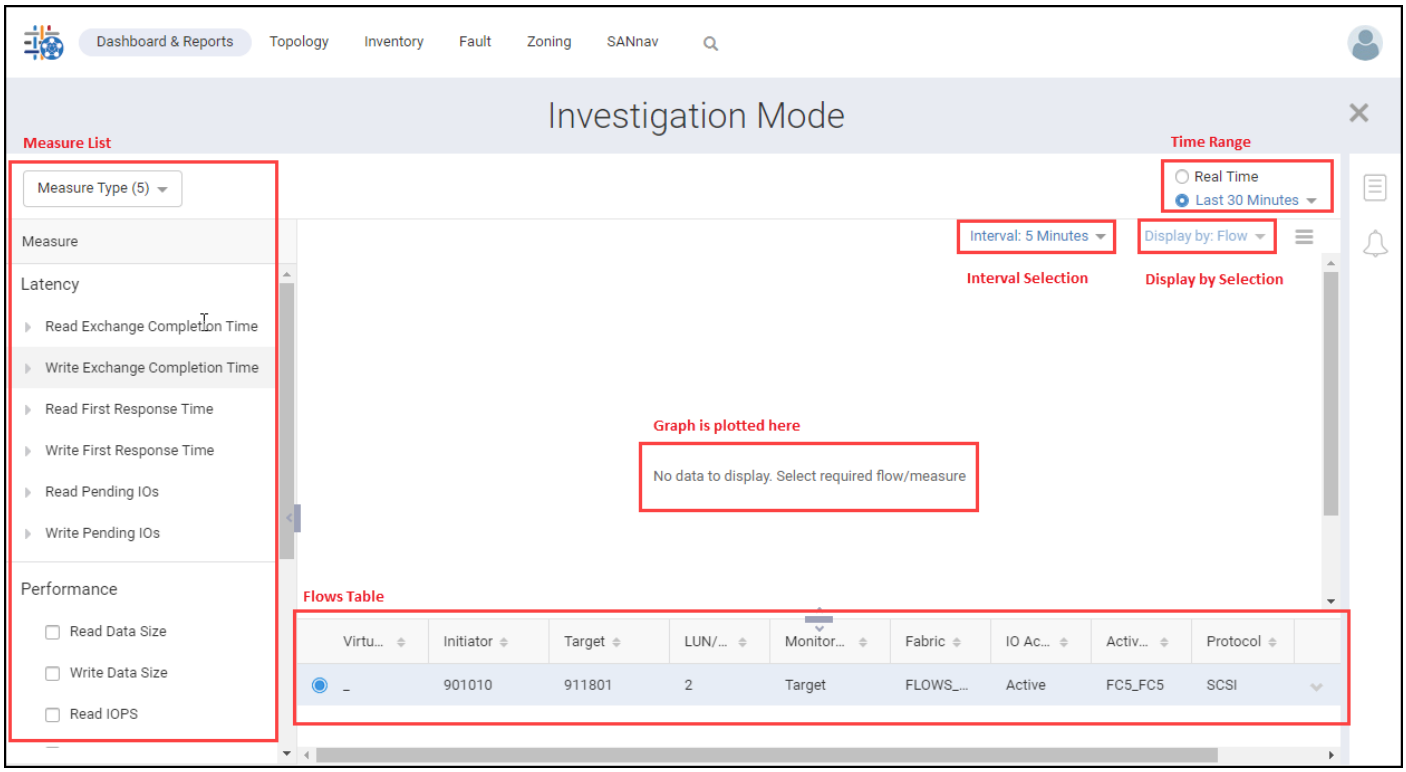
You can select multiple items within the sidebar to investigate. You can also investigate an individual flow by selecting **Investigate** from a specific action menu.

NOTE
If any of the selected flows become stale (fabric was deleted or unmonitored), SANnav deletes the stale entries from the Selected Items sidebar and the Investigate View page is launches with the remaining flows.

The **Investigate** selection is enabled if at least one flow is checked as shown in the following steps:

Whether you launch an investigation through the **Flows** list view, the **Selected Items** sidebar, or individually through the action list for a specific flow, the **Investigation Mode** page displays.

The chart appears empty as shown in the following figure because no measures are selected by default.

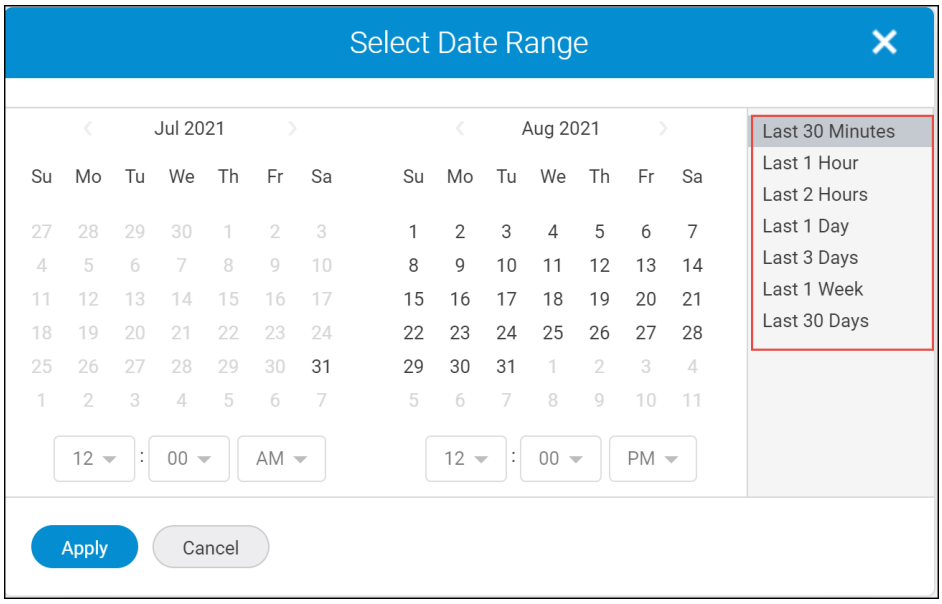


3. Select one or more measures and set the time range to proceed to the investigation:

- **Measure List** – Displays both Gen 6 or Gen 7 platform measures.

  NOTE
  Gen 7 platforms support all the listed metrics. Gen 6 platforms support only **Latency** and **Performance** categories. Gen 6 platforms do not support **IO Exceptions** and **Other** commands.

- **Time Range** – Provides Real Time, Historical Time, and Custom-Time Range (Historical) options as shown in the following figure.



NOTE

On the **Investigate Mode** page, when you select **Real Time** as the time scope, the number of data points is limited to 180. Real-time data is updated in 10-second intervals. During updates, SANnav purges the oldest data points and adds the newest data points.

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 **Last 1 Hour**, starting at 13:00, with a five-minute interval fetches 12 data points and points at 13:00 and 14:00.

- **Time Series Graph** – Based on selected measures, flows, and date range, shows statistics in a graphical format. The X-axis represents time and the Y-axis represents the units of the selected measures.

  NOTE

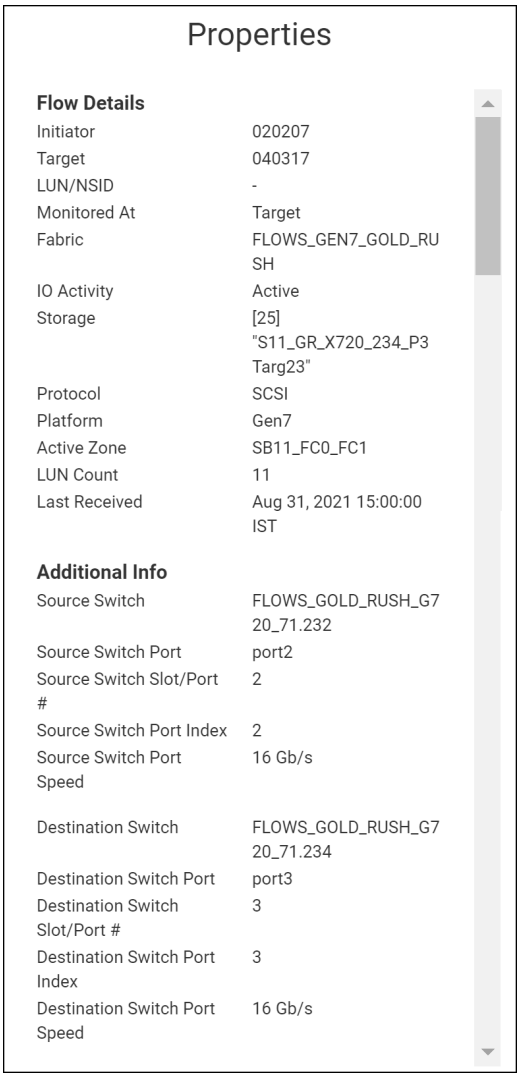
  For measures that are not supported, zero values are shown in the **Investigation** view.

- **Flow Table** – Lists all selected flows from the **Flows** page or **Violations List** view.

  SANnav supports the following actions for each flow:

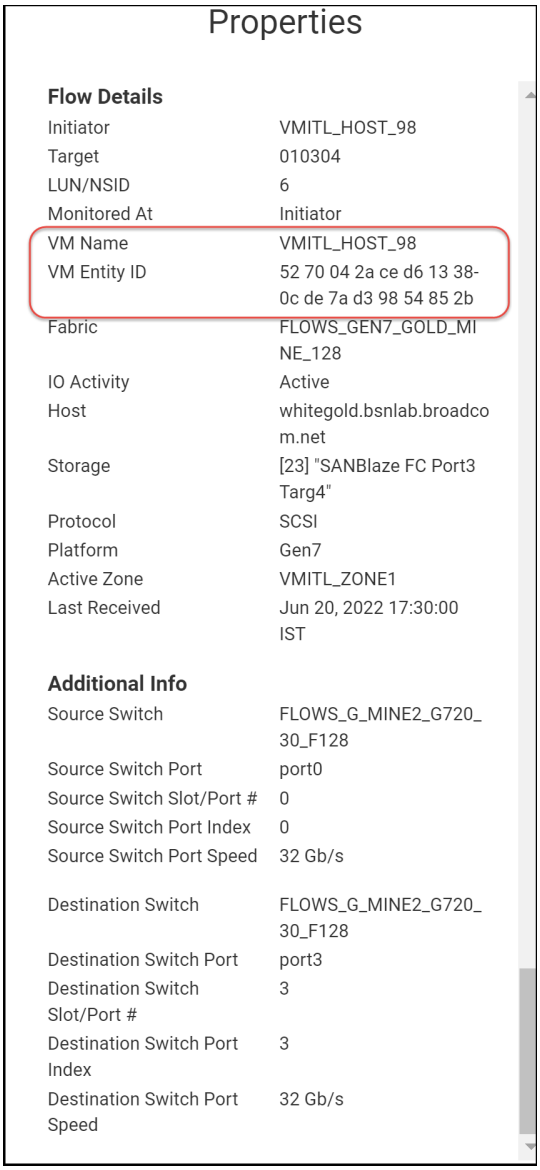
  – **Show Metrics** – The latest values of all measures are displayed in a popup. You can select any flow from the **Flow** table, click the **arrow** icon in the flow that points downward to view the metrics in the popup.

  – **Show Properties** – Displays **Flow Details** and **Additional Info** applicable only for the selected flow as shown in the following figure:



The vCenter server must be discovered in SANnav for the SANnav Management Portal to display the VM name instead of the VMID of the VITL/VITN flows. For more information on discovering vCenter, refer to the vCenter Discovery section of the *Brocade SANnav Management Portal User Guide*.

If the vCenter server for SANnav is discovered, the **Show Properties** option displays additional VM information such as **VM Name** and **VM Entity ID** as shown in the following figure:

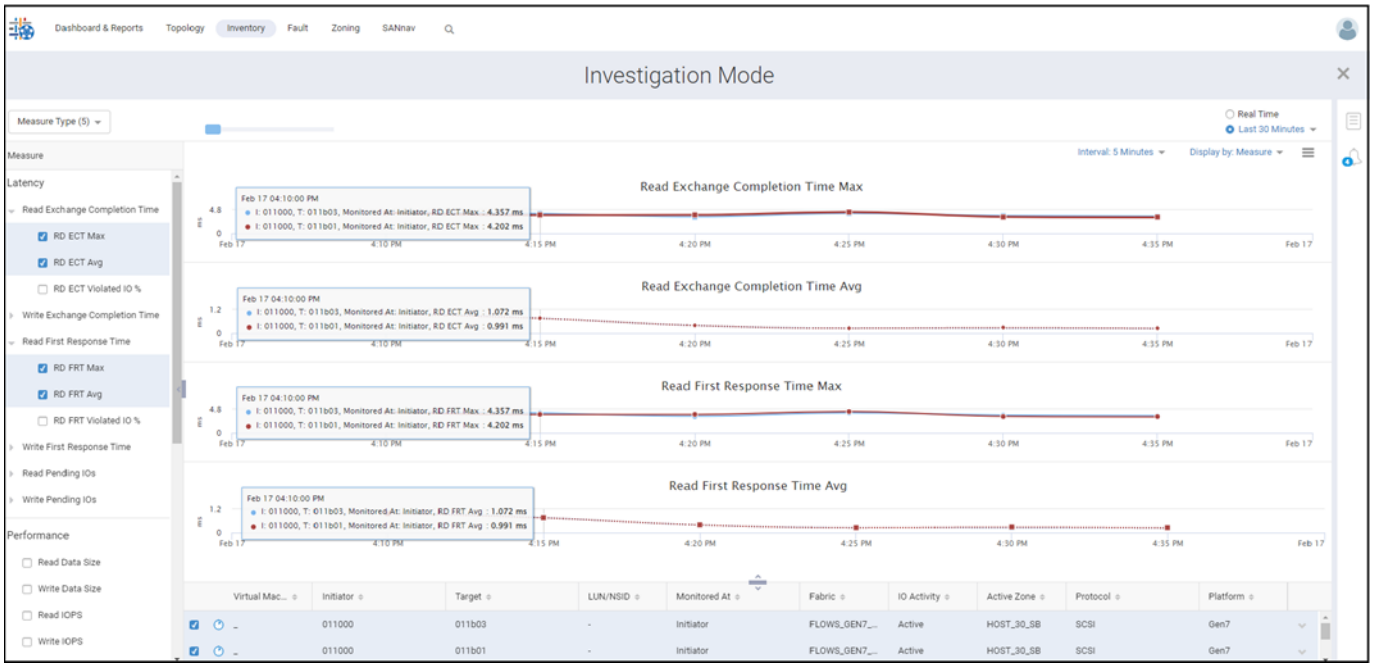


Operating in Flow Investigation Mode

To investigate the flows in the **Investigate Mode** page, perform the following steps:

1. Select flows and click **Investigate**.
2. Select up to four measures.

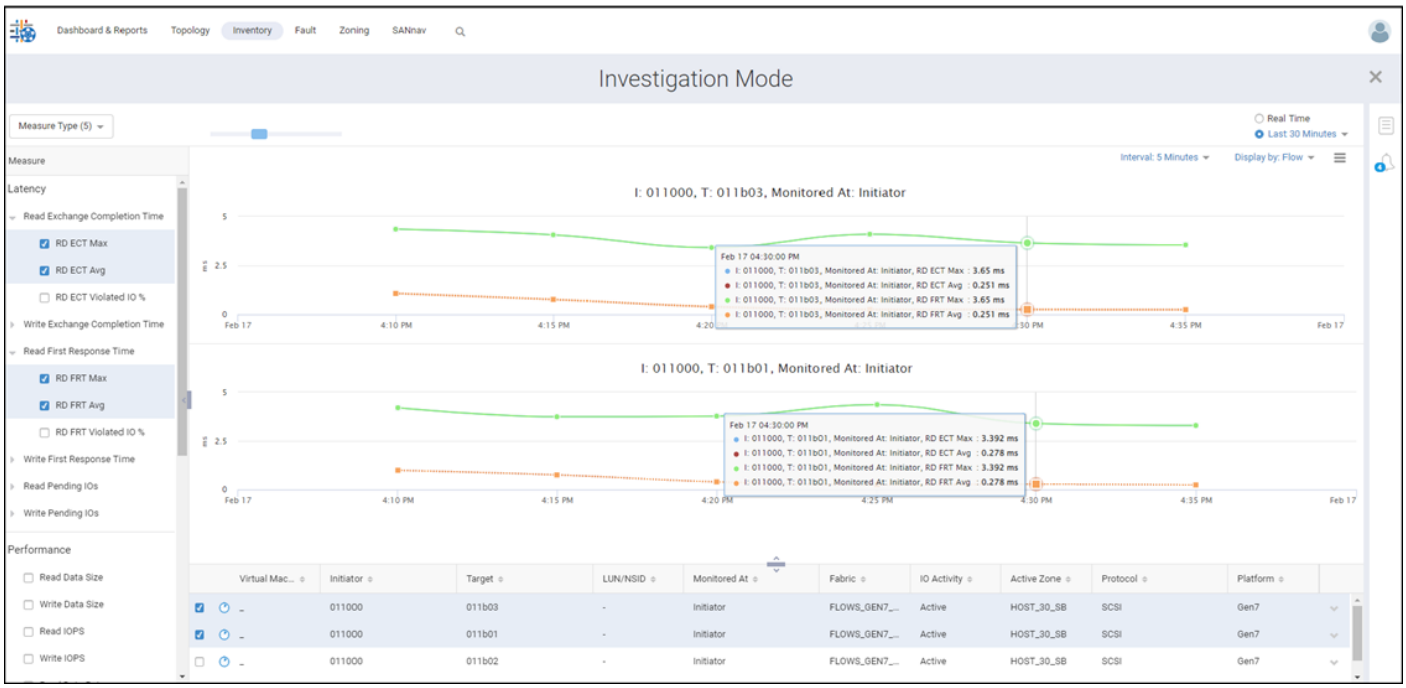
   In this example, you select the **Read Exchange Completion Time (Max and Avg)** and **Read First Response Time (Max and Avg)** values. A page similar to the following graph appears.



This example shows the **Display by Measure** view with four graphs. Each graph represents one measure for two selected flows.

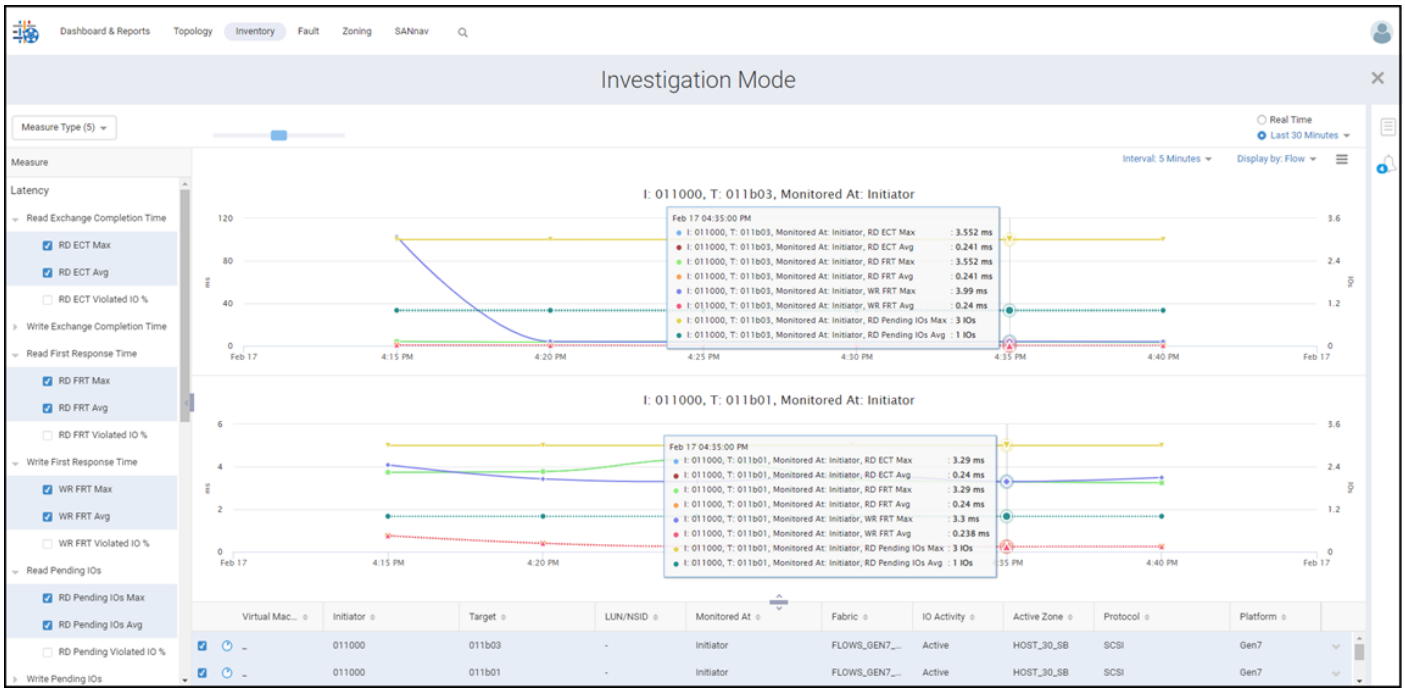
3. Select **Display by Flow** from the action menu in the far right.

   SANnav plots the graphs for each flow as shown in the following figure:



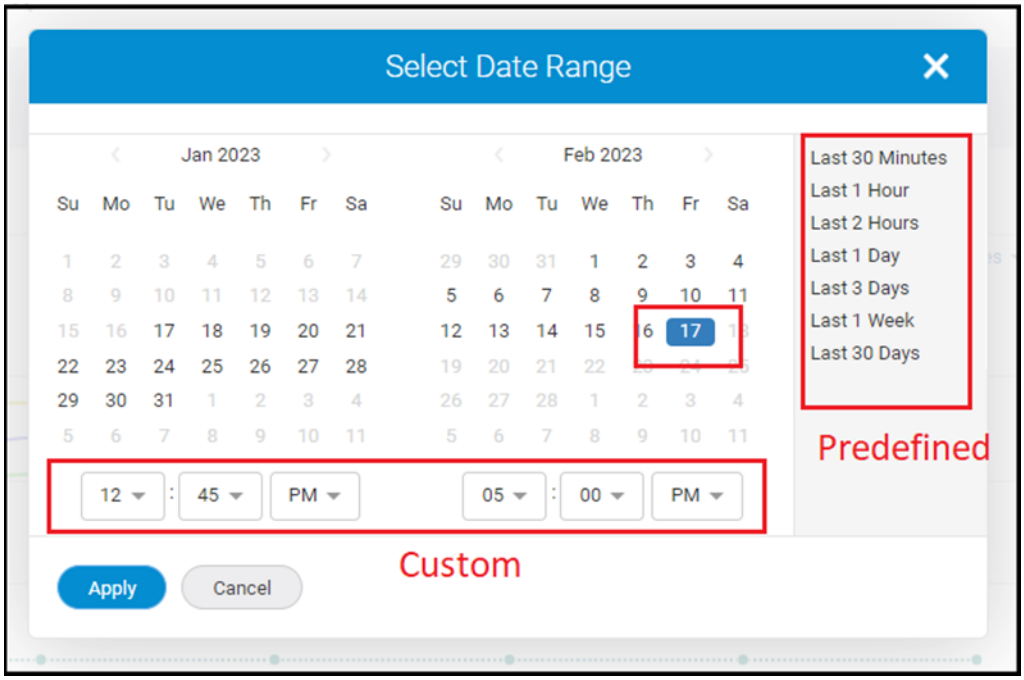
Each of these measures has maximum and average values. The maximum measure displays as a solid line and the average measure displays as a dotted line. Because you selected two measures and selected both maximum and average values for the measures, you see two lines for each flow.

Select two more measures (in this example, **Write First Response Time** and **Read Pending IOs**), a figure similar to the following appears:



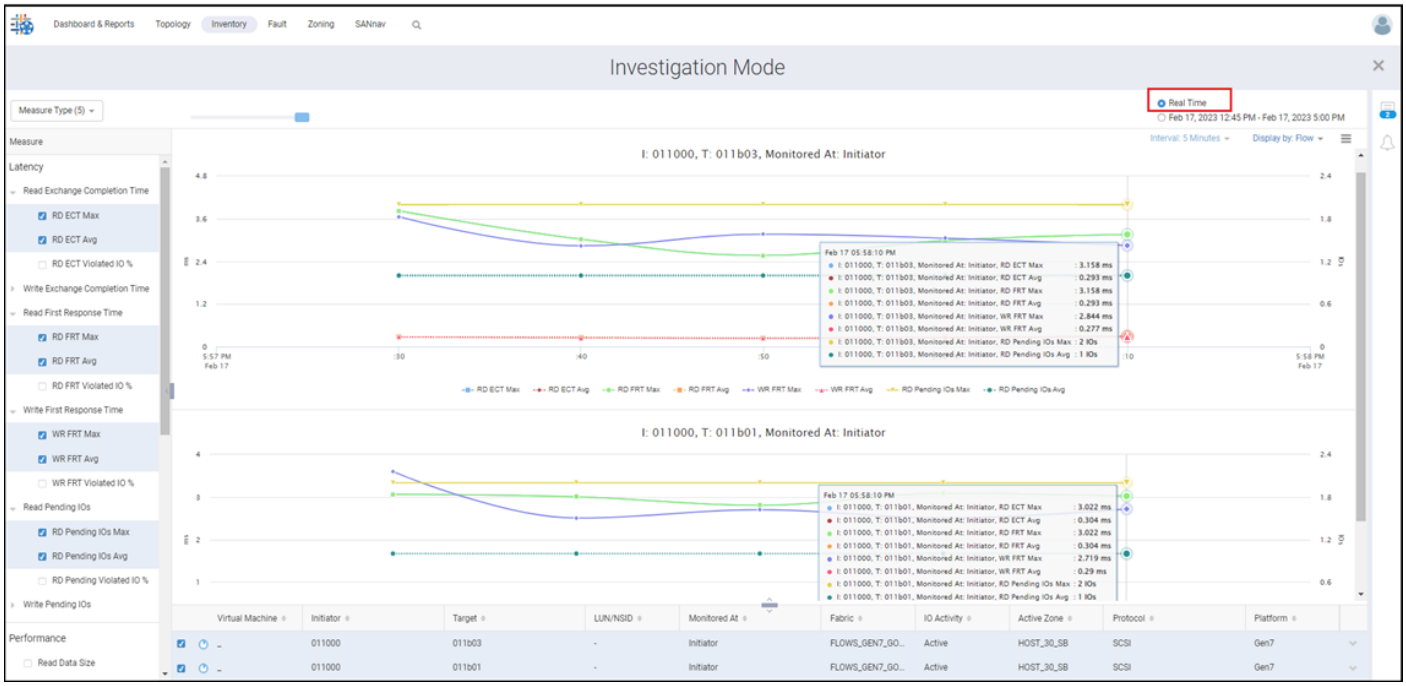
4. Change the date range by clicking the range list.

   The **Select Date Range** dialog appears.



From here, you can either use a predefined date range or customize one. When you change the time interval, the plotting changes accordingly. The following figure shows an example where the time scope was changed to a custom time range.

5. Select the **Real Time** option to investigate the selected flows in real time.



Note the following points when you investigate the flows using Investigation Mode:

- The example above demonstrates IT flows. To investigate ITL flows, select the **6 Hours** interval to view the chart for historical data.
- You can select a maximum of eight measures and four flows or you can select a maximum of eight flows and four measures at a time.
- Real Time mode supports a maximum of 25 flows to monitor per switch. SANnav does not plot data for inactive flows.
- The frequency of real-time data collection is 10 seconds. Data points beyond 30 minutes are purged from the graph.
- Switching between a 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 interval 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 data, the message *No data to display* appears.

Displaying SNMP Flow Violations

The non-I/O violations are reported through SNMP traps and are called SNMP violations. These are SNMP traps that are sent by FOS for IO Health and Latency MAPS rules being violated and Port violations on the associated F_Port (the ingress and egress F_Ports for the flow).

When you launch the **Investigation Mode** page for SNMP flow violations from the **Violations** page, SANnav preselects measures based on the violation category. The default interval is 5 minutes. The default time scope is based on the value of **Last Occurrence Host Time** in the violation record.

Table 26: Last Occurrence Host Time and Default Time Scope

Last Occurrence Host Time	Default Time Scope
Within 30 minutes	Last 1 hour
Exceeds 30 minutes	Start time is 30 minutes before **Last Occurrence Host Time** and end time is 30 minutes after **Last Occurrence Host Time**

The supported SNMP flow violations categories include the following metrics:

- **Port:**
  - Port Congestion
  - Port Utilization
  - Port Health

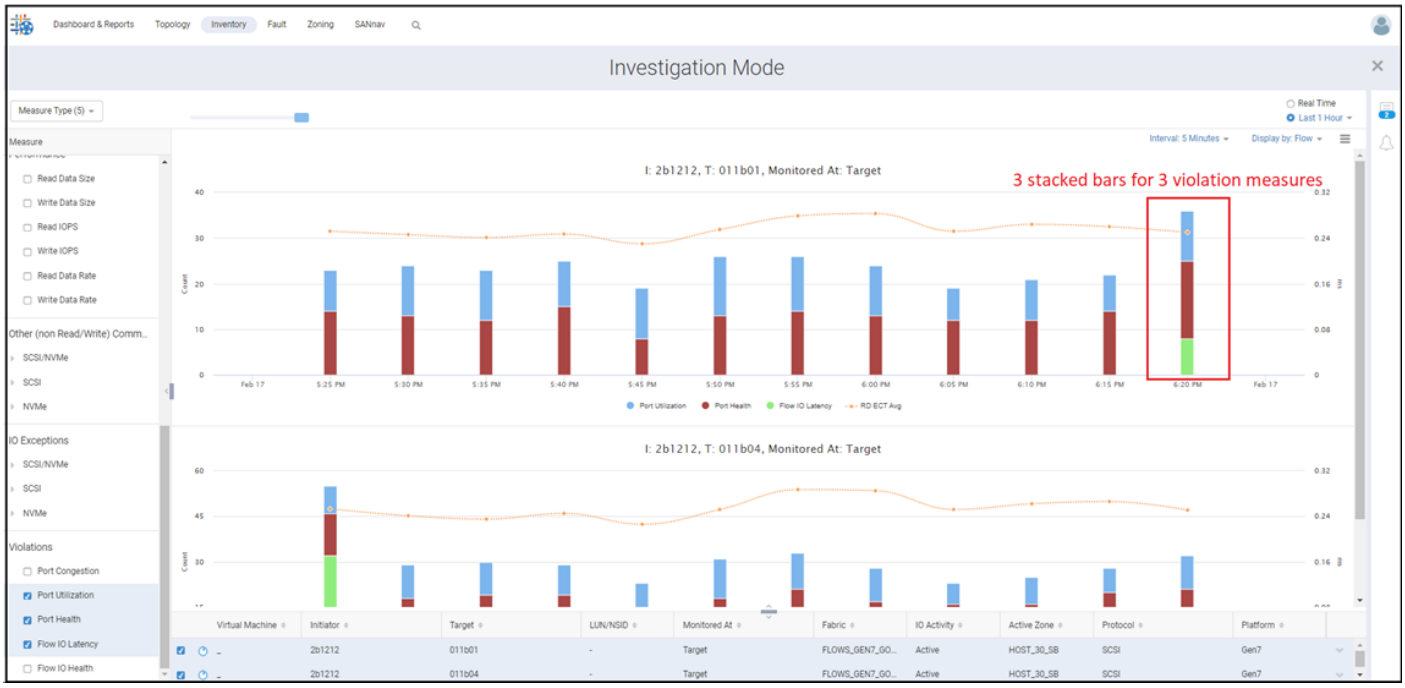
  The port is referred to as an F_Port where the Initiator and the Target are connected and the flow is being transported on. The port violations occur on F_Ports for the flow and the sum of violations occur at the Initiator F_Port and the Target F_Port.
- **Flow:**
  - Flow IO Latency
  - Flow IO Health

Once you select a violation category, it is plotted in the chart.

To view the Flow SNMP violations, perform the following steps:

1. Select violation measures.

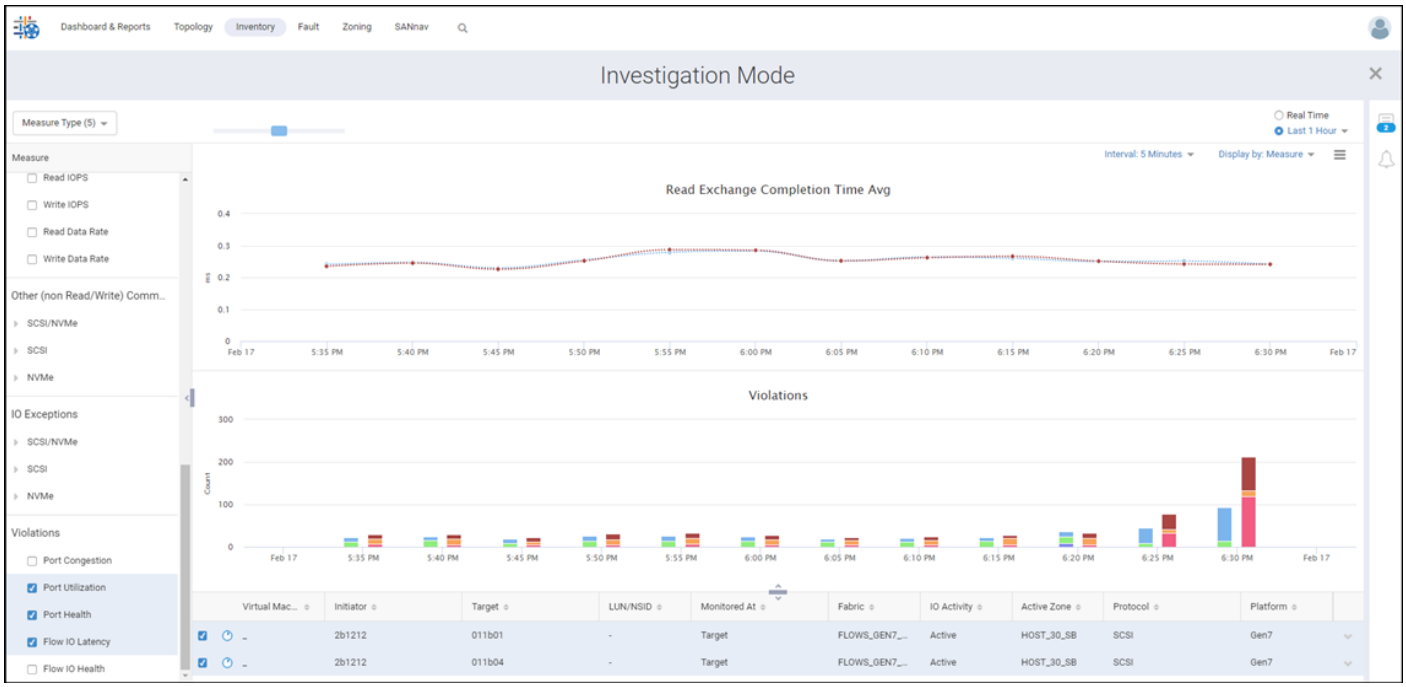
   In this example, three violation measures are selected. The following figure shows the charts of the **Display by Flow** category:



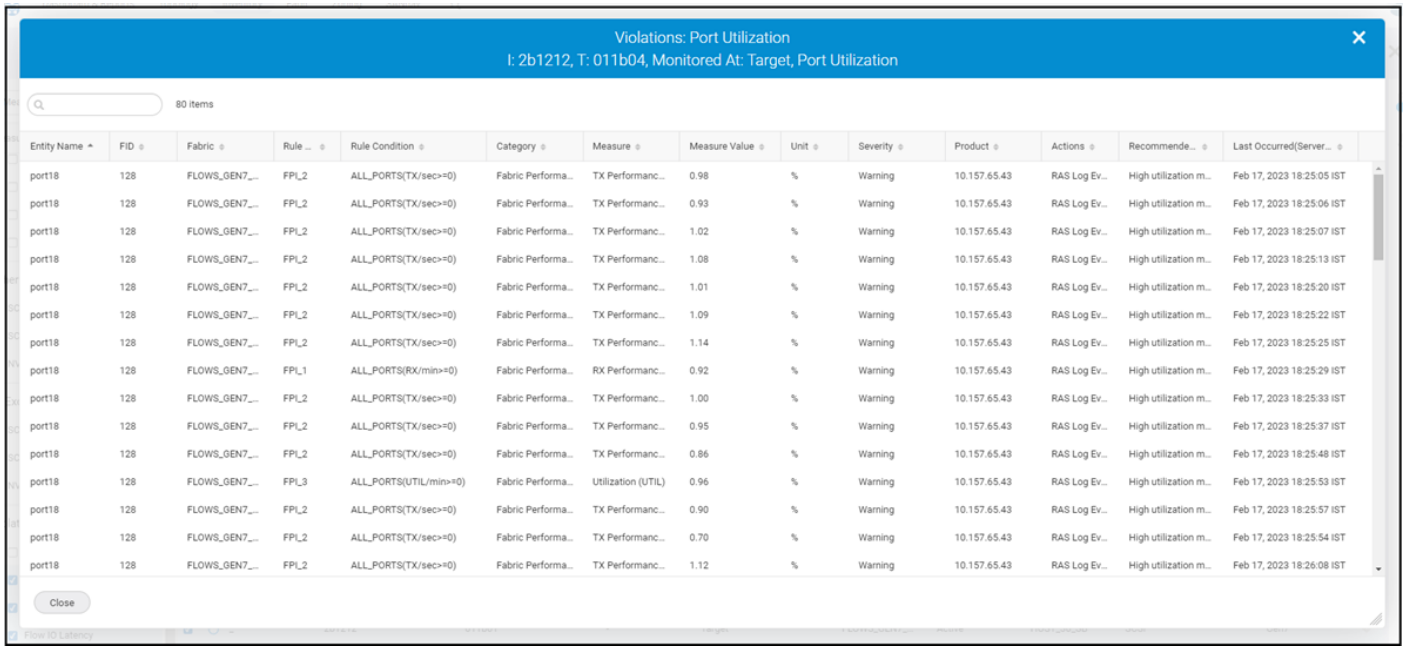
In this chart, the violations are displayed in bar charts. For two flows and two violations, you see two stacked bars with two colors. Multiple violations that are represented within the same bar are distinguished in different colors. The plotted measures appear on the same chart.

2. Select **Display by Measure** from the **Action** menu in the upper right to display by measure.

   For this example, two measures and three violation categories are selected. The following figure shows the charts of the **Display by Measure** category:



3. Click a section of the bar in the chart to view a **Violations** dialog, similar to the following figure:



Based on where you click in a chart, the entries in this dialog change. For example, if you click the bar in a port-related violation area, the dialog lists all violations in the section that occurred at that Initiator or Target port (depending on which side is being monitored) at that particular time. Similarly, if you click the bar in the flow-related violation area, the dialog lists all the violations that occurred for that flow at that particular time.

Flow Investigation – Miscellaneous Information

The following table provides information on flow intervals and the recommended time scope for each flow interval:

Table 27: Recommendation of Flow Intervals and Historical Statistics Interval Duration

Interval	Recommended Time Scope
5 Minutes	1 day
1 Hour	1 week
6 Hours	30 days

SANnav retains the **5 Minutes** interval flow metrics for the last eight days. SANnav retains the **1 Hour** and **6 Hours** interval flow metrics for the last 30 days.

NOTE
You can investigate a maximum of eight flows with a single measure or eight measures with a single flow.

Flow SNMP Violations – Important Notes

You can view the SNMP violations in a bar chart along with other selected measures. Based on the selected interval, measures, and aggregated violations count are plotted at the same data point with the following limitations:

- SNMP violations are not applicable for real-time data in an investigation view. The violation measures are disabled for real-time cases.
- One stacked bar is displayed for each selected flow.
- SNMP violations are supported for up to 24 hours. When the time scope exceeds 24 hours, you are prompted with a dialog showing appropriate messages.

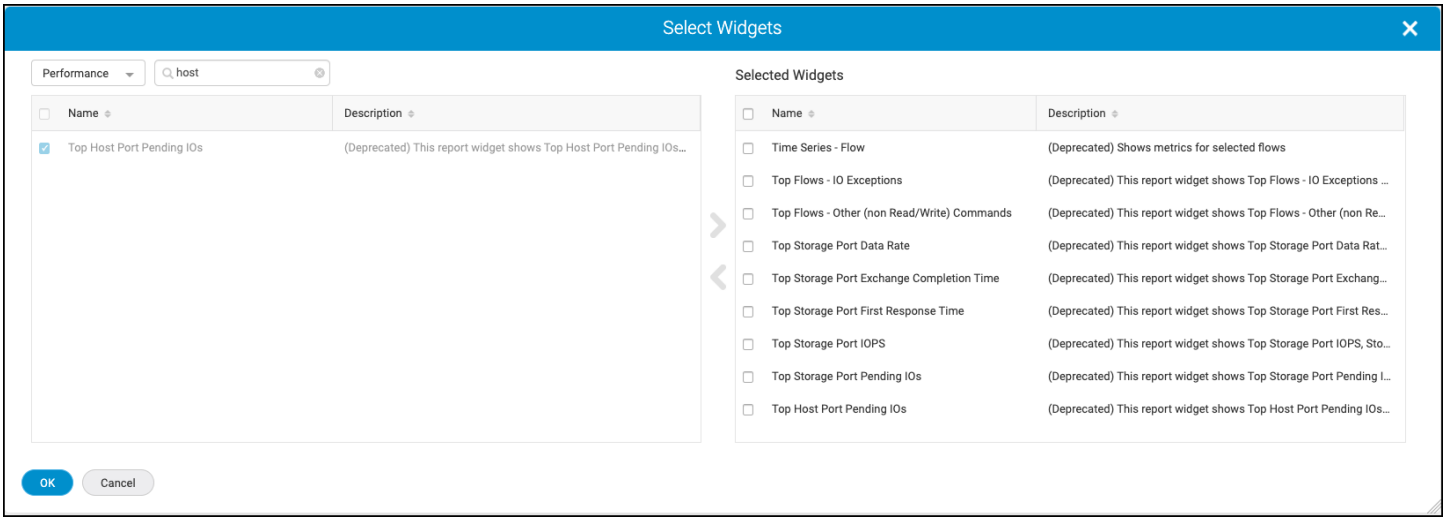
Flow Reports

The Flow Reports feature allows you to generate the custom designed reports with summaries of flow inventory and performance that can be scheduled and viewed in various formats such CSV, PDF, and HTML.

NOTE
The following flow widgets are **deprecated** in SANnav 2.3.0. These flow widgets will be removed from a future version of SANnav.

- Time Series - Flow
- Top Flows - IO Exceptions
- Top Flows - Other Commands
- Top Host Port Pending IOs
- Top Storage Port Data Rate
- Top Storage Port Exchange Completion Time
- Top Storage Port First Response Time
- Top Storage Port IOPS
- Top Storage Port Pending IOs

The description of the deprecated flow widgets include (Deprecated) in the description.



Report Widgets for Flows

Procedures such as editing and exporting reports for Flow Management, are similar to other SANnav standard report procedures.

This section describes how to create reports incorporating the flow widgets.

NOTE
For measures that are not supported, zero values are shown.

Widgets are categorized under Top N and Time Series. Top N widgets capture the top contributors based on metrics. Time Series widgets capture the historical statistics.

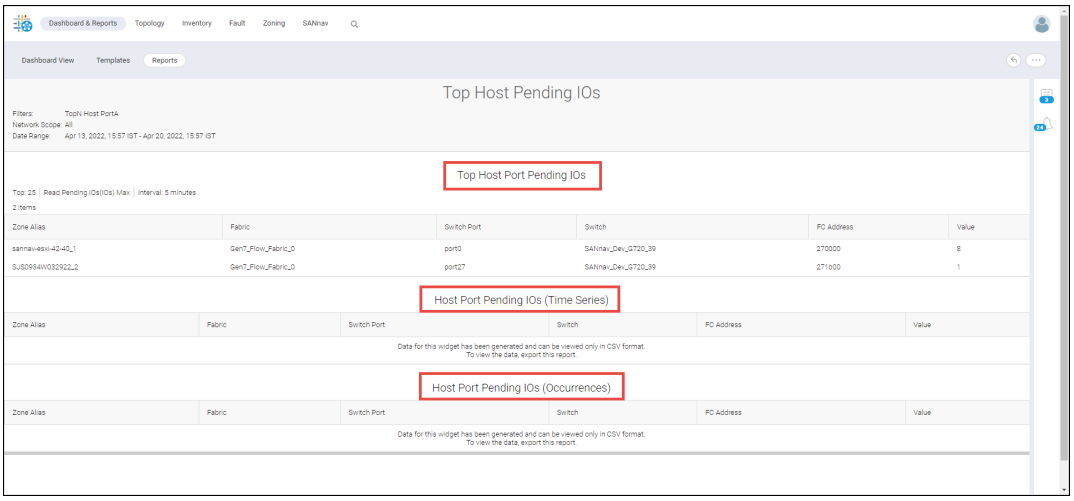
The following table lists the available widgets specific to flows, storage, and host ports.

Flow Widgets	Storage Port Widgets	Host Port Widgets
• Top Flows - IO Exceptions (deprecated) • Top Flows - Other (non Read/Write) Commands (deprecated)	• Top Storage Port Exchange Completion Time (deprecated) • Top Storage Port First Response Time (deprecated) • Top Storage Port Data Rate (deprecated) • Top Storage Port IOPS (deprecated) • Top Storage Port Pending IOS (deprecated)	• Top Host Port Pending IOs (deprecated)
• Time Series - Flow (deprecated) Supports a maximum of 10,000 flows only.	• Storage Port Exchange Completion Time (Time Series) (deprecated) • Storage Port Pending IOs (Time Series) (deprecated) • Storage Port First Response Time (Time Series) (deprecated) • Storage Port IOPS (Time Series) (deprecated) • Storage Port Data Rate (Time Series)	• Host Port Pending IOs (Time Series)

The **Occurrences** is a sub-widget of Top N flows-related widgets (for example, Top Storage Port Pending IOs and Top Storage Port Data Rate). This widget takes the threshold value as an input. The threshold value is applied against the results of the applied filter and lists all the top 100 records irrespective of the Top N value selection. After a report is generated, the data for this widget can be viewed only in the CSV format in the exported report. This sub-widget is optional. If you want to remove the sub-widgets, then click the hamburger ☰ menu in the top-right corner of the sub-widget and click **Delete**.

The following screen shows an example of a widget with its sub-widgets:

- Top Host Port Pending IOs (Top N)
- Host Port Pending IOs (Time Series)
- Host Port Pending IOs (Occurrences)



The vCenter server must be discovered in SANnav for the SANnav Management Portal to display the VM name instead of VMID of VITL/VITN flows. If the VM name is determined through the SANnav vCenter discovery, the **Flows** page

displays the human-readable VM name for VITL/VITN flows. The VMID is displayed in the non-human readable format if the vCenter server is not discovered in SANnav. For example, 52 70 04 2a ce d6 13 38-0c de 7a m4 89 42 58 b2.

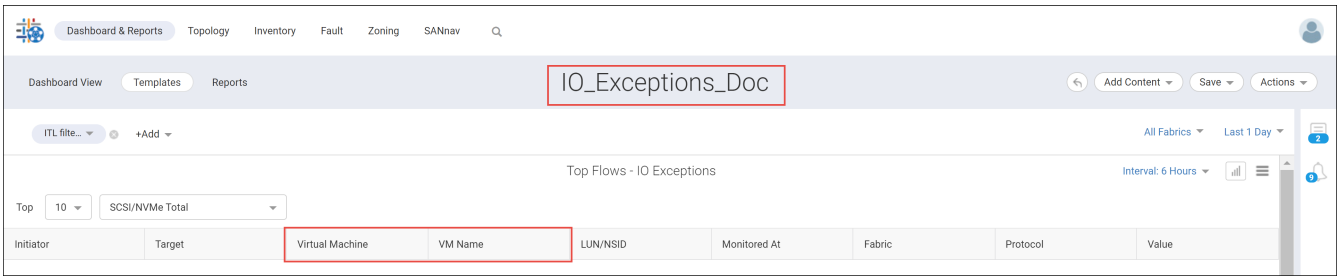
The following flow report widgets show the **VM Name** and **VM Entity ID** columns:

- Time Series - Flow
- Top Flows - IO Exceptions
- Top Flows - Other (non Read/Write) Commands

You can select the **VM Name** and **VM Entity ID** columns in the ☰ > **Columns** navigation path on the top right of the **Templates** page.

NOTE
You must create the **Virtual Machines** filter to generate reports for the VITL/VITN flows.

The following figure shows an example of the report with the VITL/VITN flows:



NOTE
The report widget templates created with SANnav release versions older than v2.2.1x do not display the **VM Name** and **VM Entity ID** columns by default. You must manually add those columns to the widget templates.

Note the following points when you work with report widgets:

- For Top N reports, the HTML and CSV formats are supported. For Time Series reports, only the CSV format is supported, which is viewable only upon export.
- The columns available for the Top, Occurrences (Threshold), and Time Series segments depend on the customization in the template view.
- The Occurrences (Threshold) rows differ from Top N, in that the Occurrences (Threshold) rows list the entities that have met the threshold. Therefore, the Occurrences (Threshold) rows might not match the Top N result.
- For widgets where a filter is mandatory, an empty report is generated if the supported filter is not applied.

The following table shows which filter is appropriate for a widget and whether the filter is required or optional.

Table 28: Widgets and Corresponding Filters

Report Widget	Applicable Filters	Notes
Time Series - Flow	Flow	Filter is required.
Top Flows - IO Exceptions	Flow	Filter is required.
Top Flows - Other (non Read/Write) Commands	Flow	Filter is required.
Top Storage Port Pending I/Os	Storage port	Filter is optional.
Top Host Port Pending I/Os	Host port	Filter is optional.

Generating a Top N Report for Host Ports

Use the following steps to generate the Top N Report for host ports:

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.

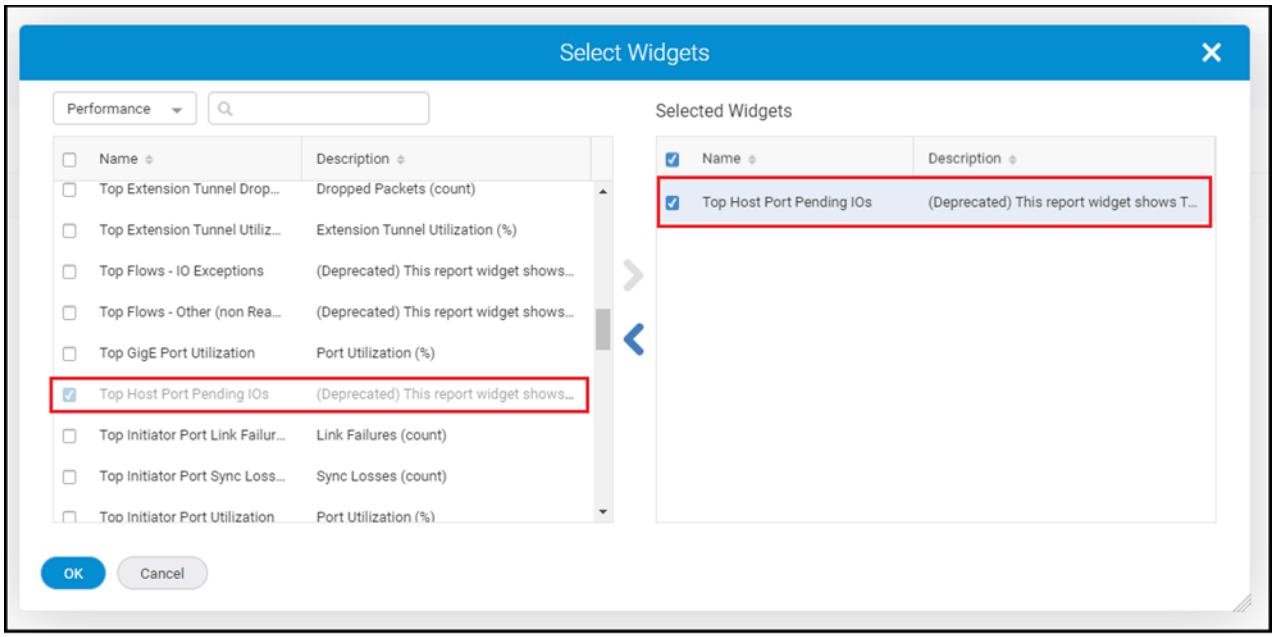
   The **Templates** page displays.

2. Click the **+** button on the right side of the subnavigation bar, and then select **Report** > **Select Widgets**.

   The **Select Widgets** dialog displays.

3. Select the **Performance** category and a *Top N* widget within that category, and then click the right arrow to move the widget to the **Selected Widgets** list.

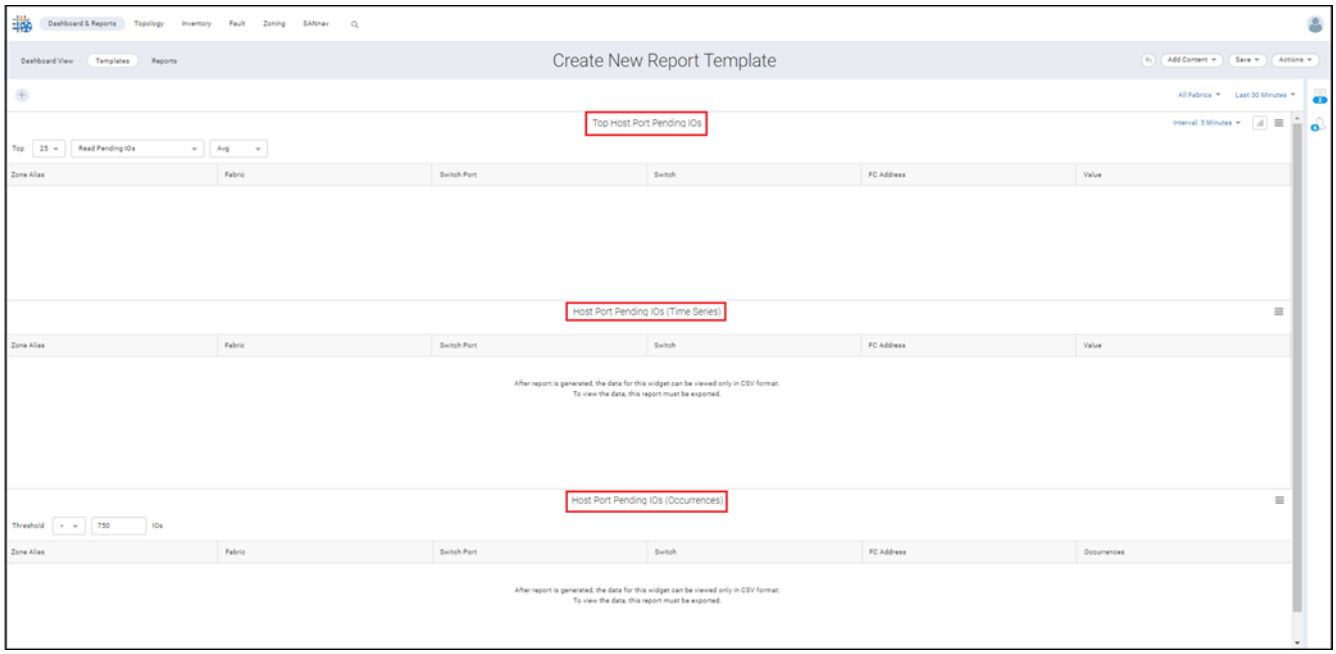
   In this example, the **Top Host Port Pending IOs** is selected.



4. Click **OK**.

   The **Create New Report Template** dialog appears.

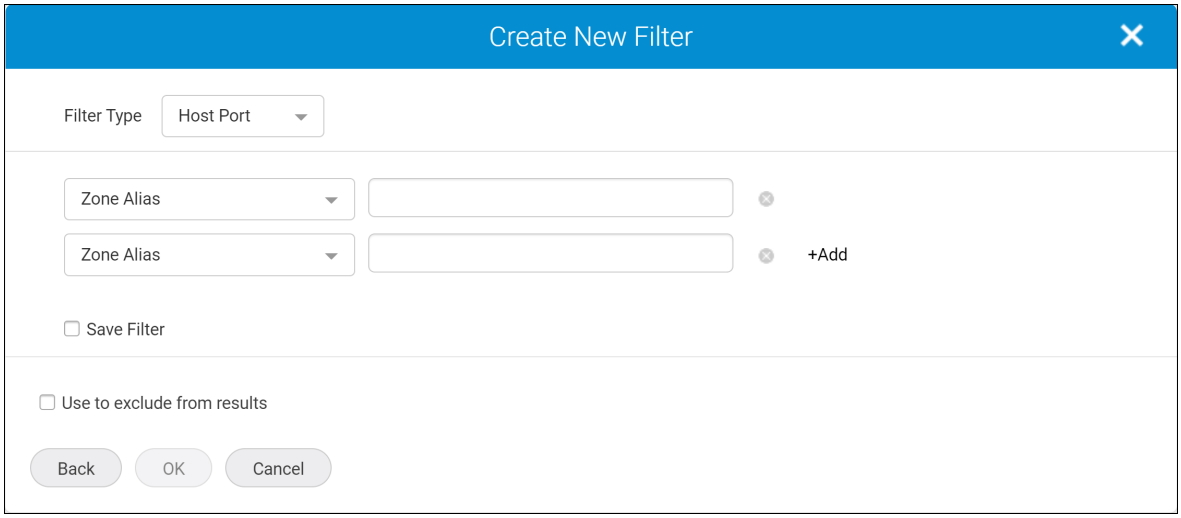
   Notice the three components of a Top N host port report: Top N results, Time Series, and Occurrences.



5. Add and save a flow filter for the report by clicking the plus icon (+) on the left side of the filter bar.

   In the **Create New Filter** dialog, set the following values:

   - Filter Type = Host Port
   - Identifier = Zone Alias, Value = Zone Alias

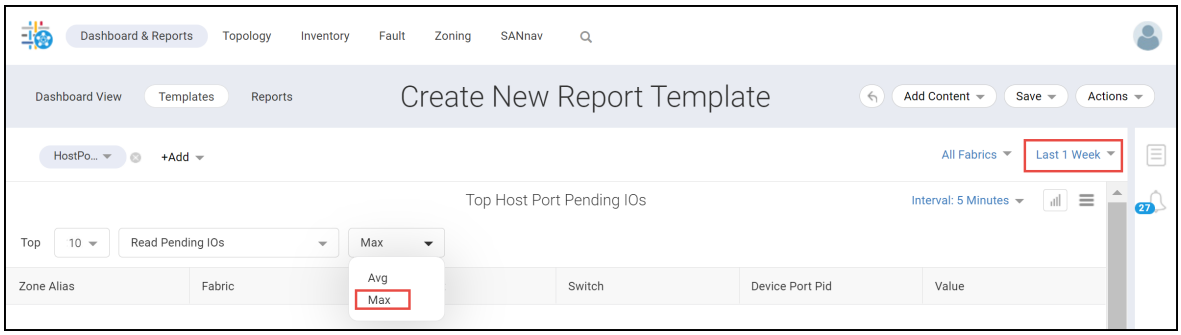


   The filter name that you enter appears on the upper left in the filter list.

6. Customize the date range and widget contents.

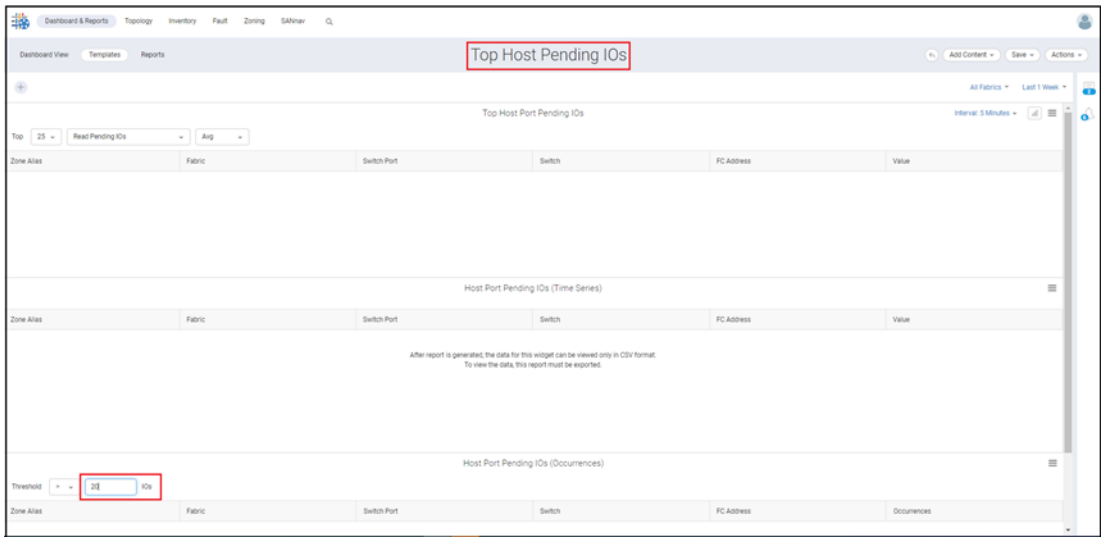
   For this example, set the following values:

- Date range = Last 1 Week
- Interval = 5 Minutes
- Top N = 25
- Measure = Read Pending IOs
- Avg/Max = Max



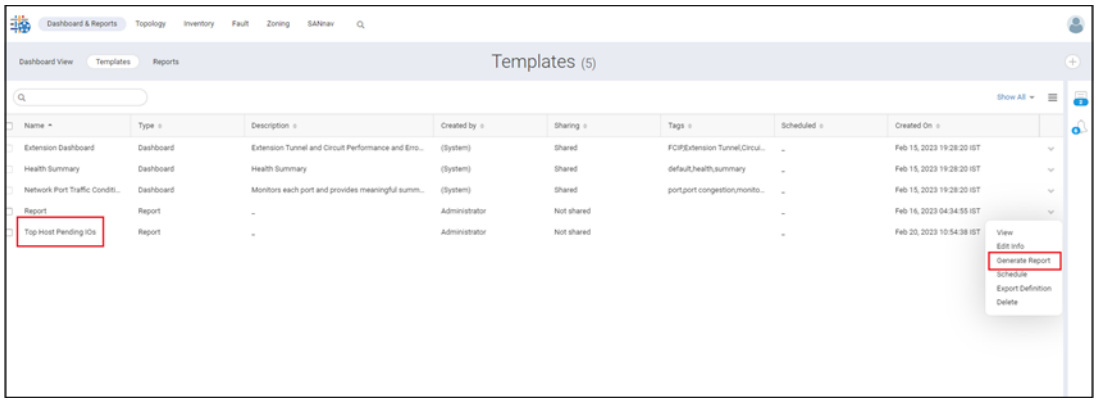
7. Click **Save**.
8. Specify a name for the report and any tag values, and then click **Save**.

   The new template displays with the name at the top and the widget identifier immediately below, as shown in the following figure:



9. Modify the threshold, if necessary.
10. Click the **Templates** tab.

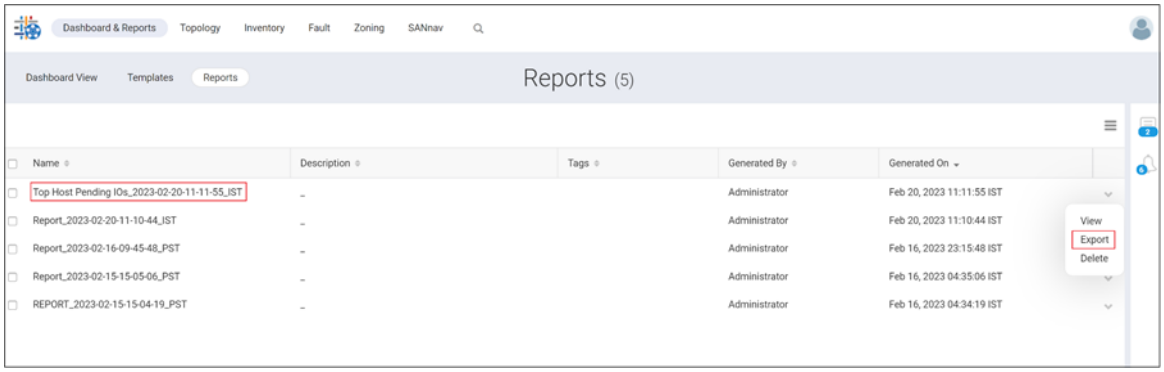
    The template that you created appears as shown in the following figure:



11. Click **Generate Report** from the action menu for the template, and then click the **Reports** tab.

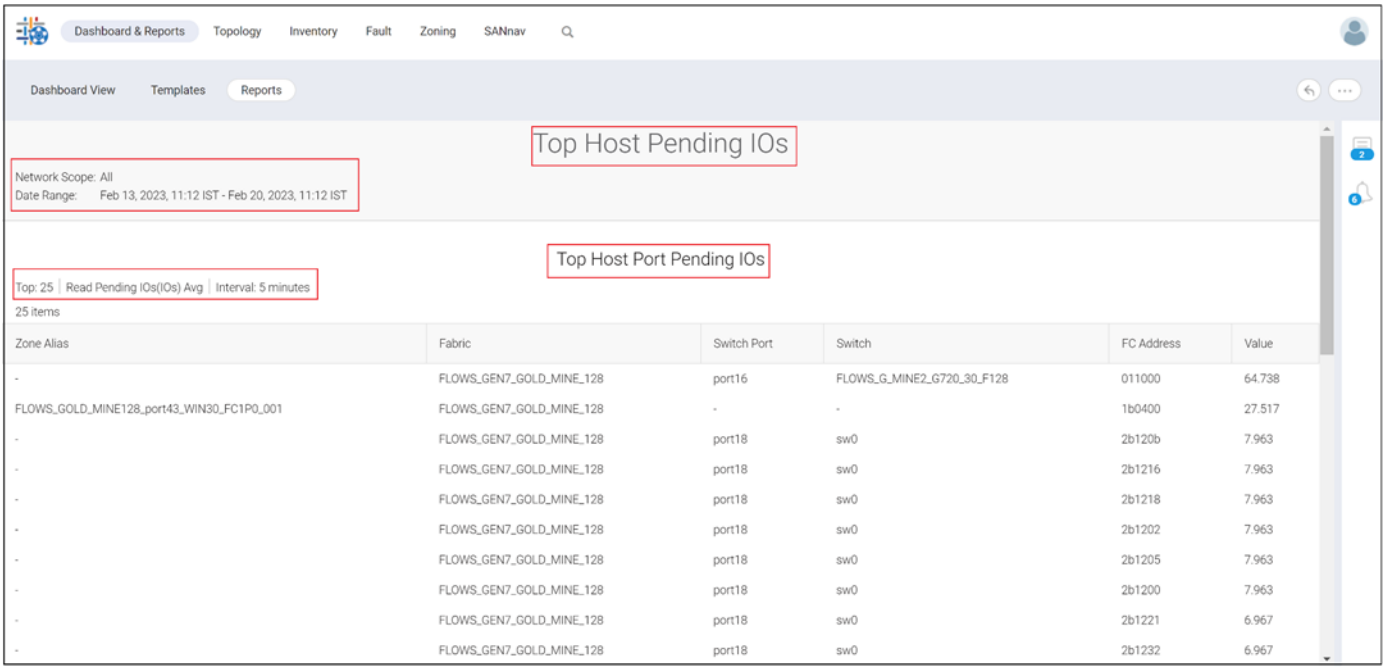
    NOTE
    The **Generate Report** option is also available in the **Actions** list inside the template view.

    Notice that your report now appears in the list appended with a timestamp.



12. Click the report name to display the report.

    The top portion of the report is populated with the top 10 Host Port Pending IOs.



The bottom portion of the report, Time Series and Occurrences, must be exported and viewed in CSV format.

13. Click **Export** from the more icon (...).

    NOTE
    The **Export** option is also available in the **Templates** view.

    The report is downloaded as a ZIP file to your local machine.

14. Unzip the downloaded zip file.
15. Double-click the Top_Host_Port_Pending_IOs subfolder, and then double-click each report to view its contents.

Generating a Top Flow Report for IO Exceptions

Other commands and IO Exception reports are applicable to Gen 7 platforms only. The remaining reports are supported for both Gen 6 and Gen 7 platforms.

You can create Top Flow reports for IO exceptions by performing the following steps:

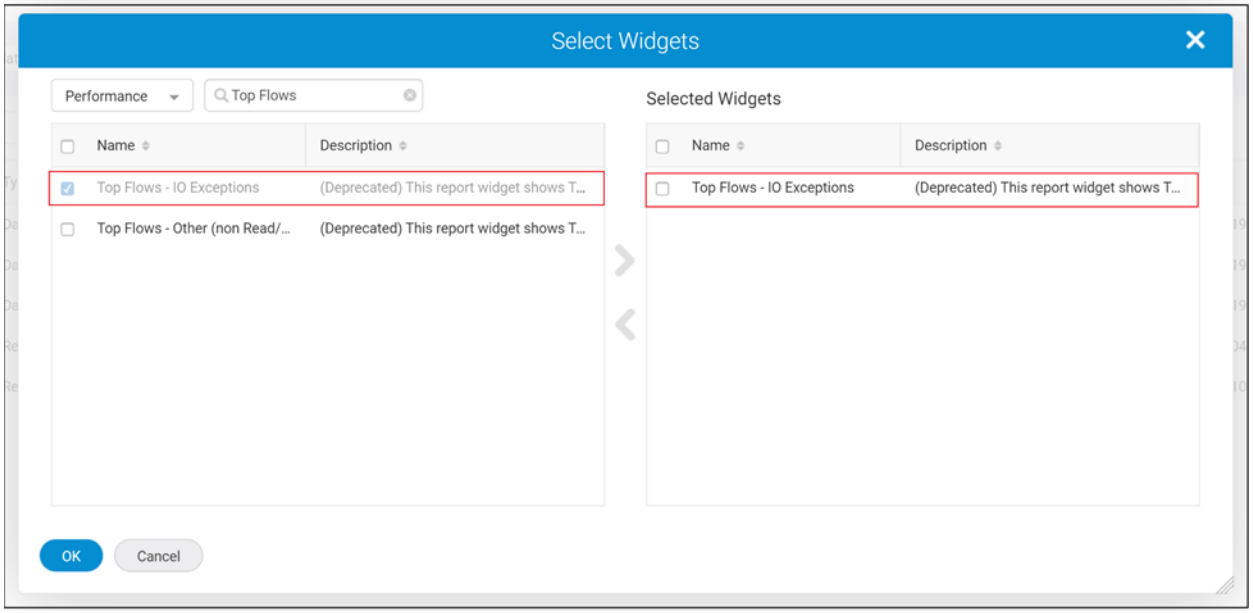
1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.

   The **Templates** page appears.

2. Click the **+** button on the right side of the subnavigation bar, and then select **Report** > **Select Widgets**.

   The **Select Widgets** dialog displays.

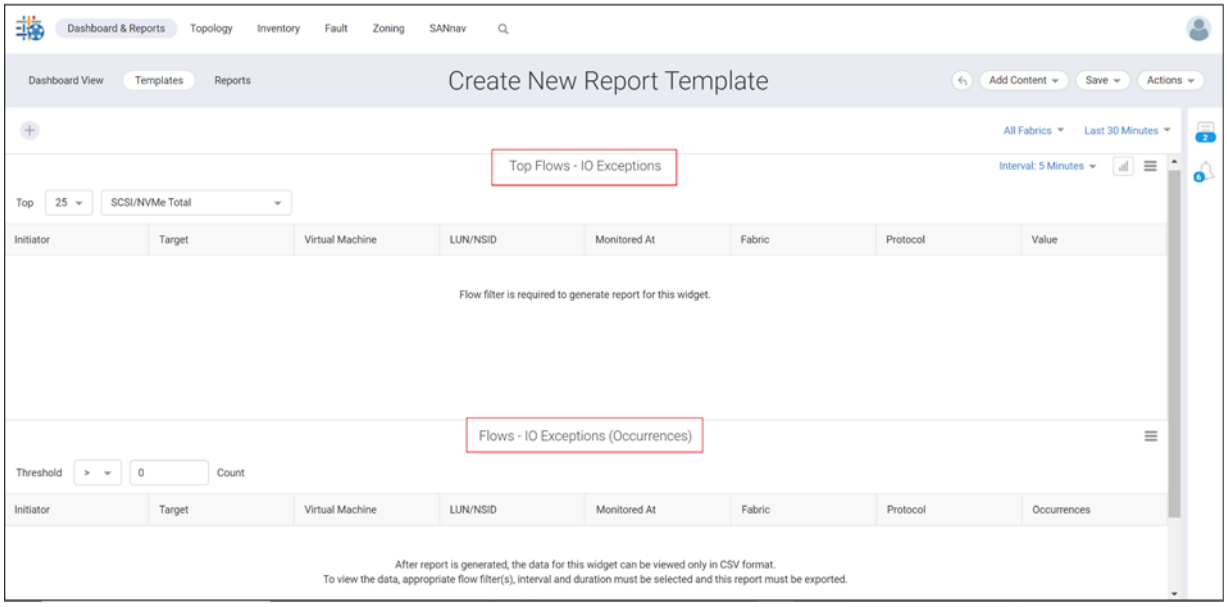
3. In the **Performance** category, select the **Top Flows - IO Exceptions** widget, and then click the right arrow to move the widget to the **Selected Widgets** list.



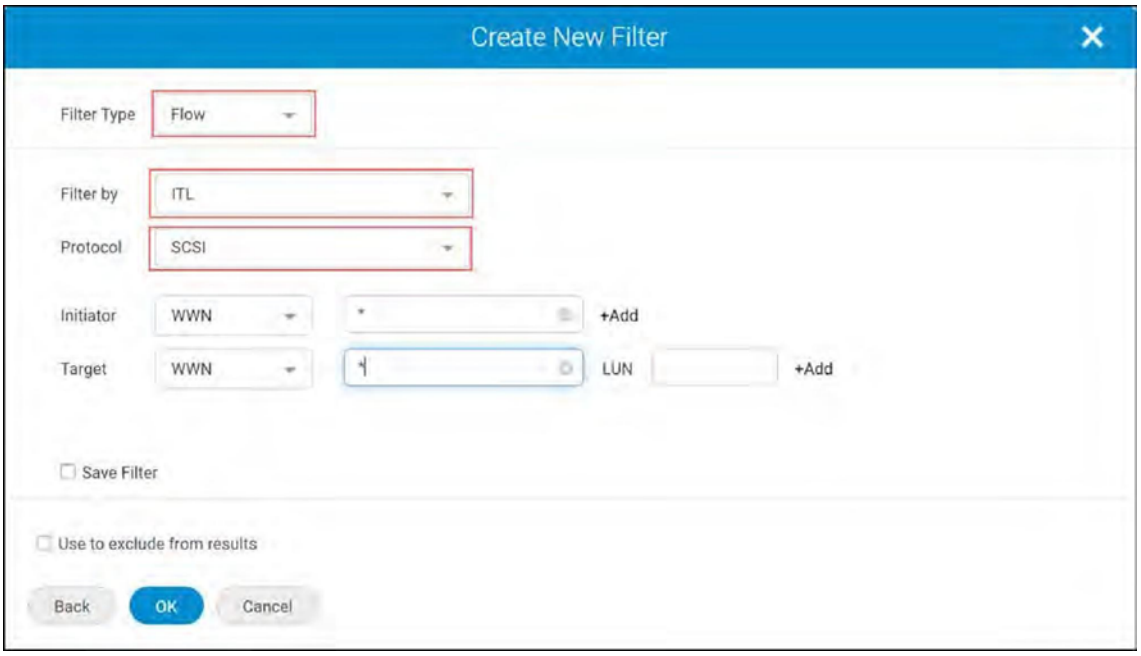
4. Click **OK**.

   The **Create New Report Template** dialog appears.

   For Top Flow reports, you can see two parts: Top Flows and Occurrences.



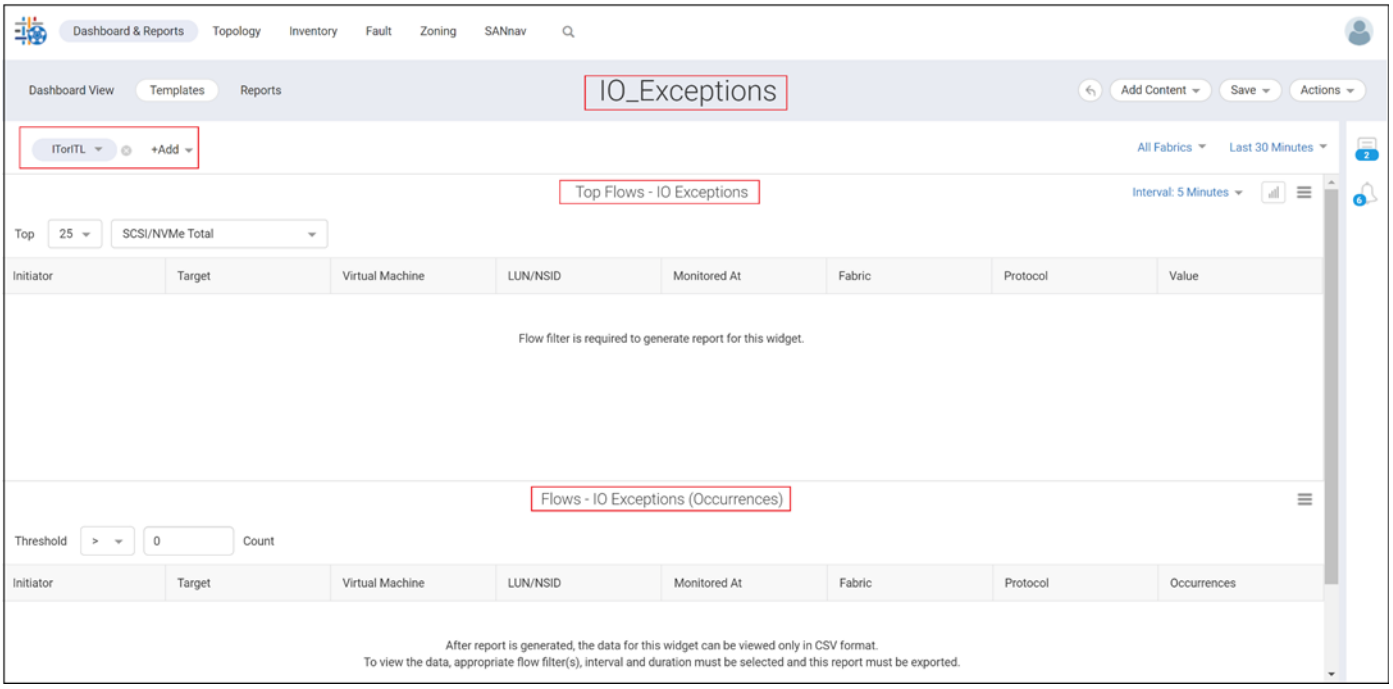
5. To create a flow filter for the report, perform the following steps:
   a) Click the **+** button on the upper left of the page to add a filter.
   b) In the **Add Filter** dialog, click **Create New**.
   c) In the **Create New Filter** dialog, set the following values:
      - Filter Type = Flow
      - Filter By = ITL
      - Protocol = SCSI or NVMe



   d) Click **Add** to create a new flow filter.
   e) Select the **Save Filter** checkbox and enter a **Name** (in this example ITorITL) and any **Tags** (optional), and then click **OK**.

      The **Create New Report Template** dialog displays.

      The filter name (ITorITL) you entered appears on the upper left in the filter list.



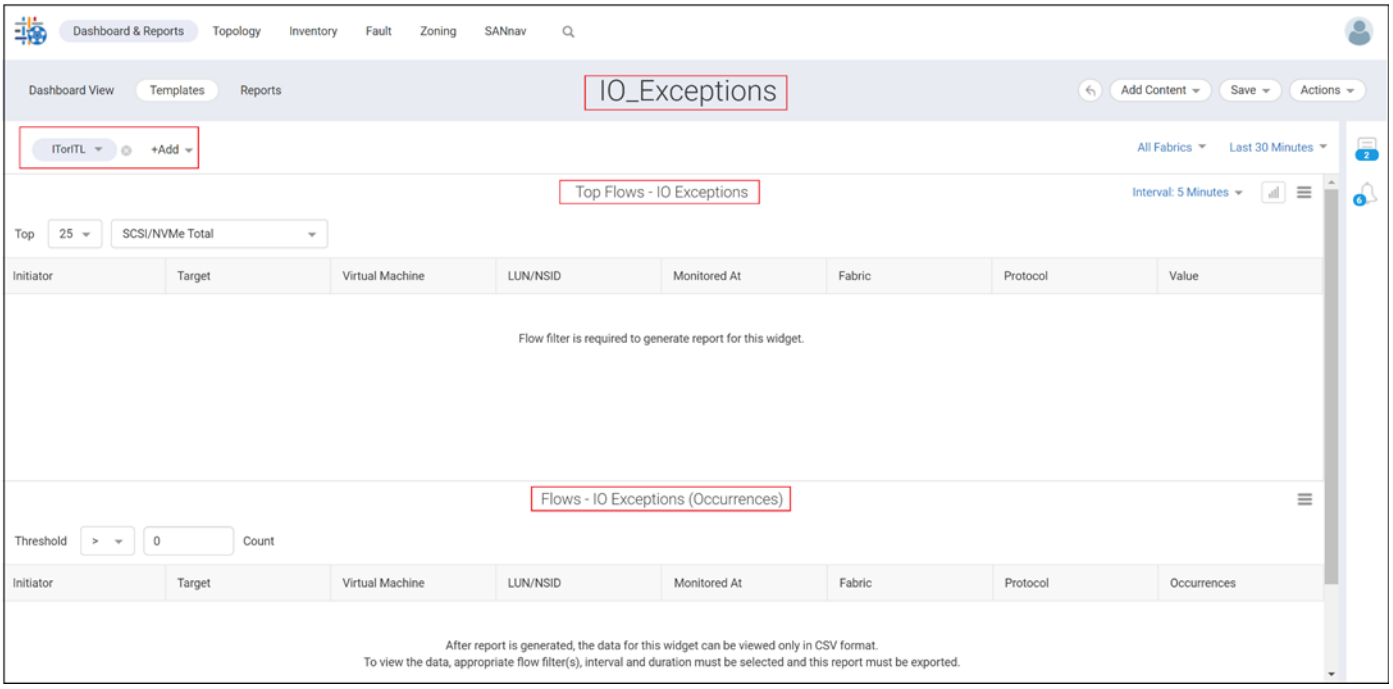
6. Customize the date range and widget contents.

   In this example, set the following values:

   - Date range = Last 30 Minutes
   - Top N = 25
   - Measure = SCSI/NVMe Total
   - Interval = 5 Minutes

7. Modify the threshold for the report.

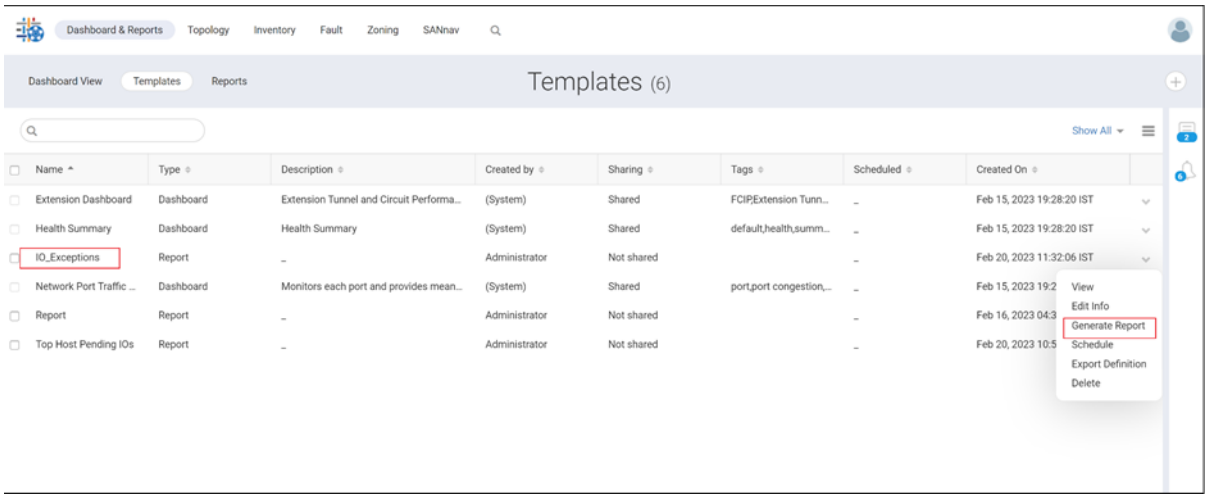
   For example, change the threshold to greater than (>) **10 count**.



8. Click **Save**.
9. Specify a name for the report (IO_Exceptions) and any tag values, and then click **Save**.

   The new template shows with the specified name at the top.
10. Click the **Templates** tab.

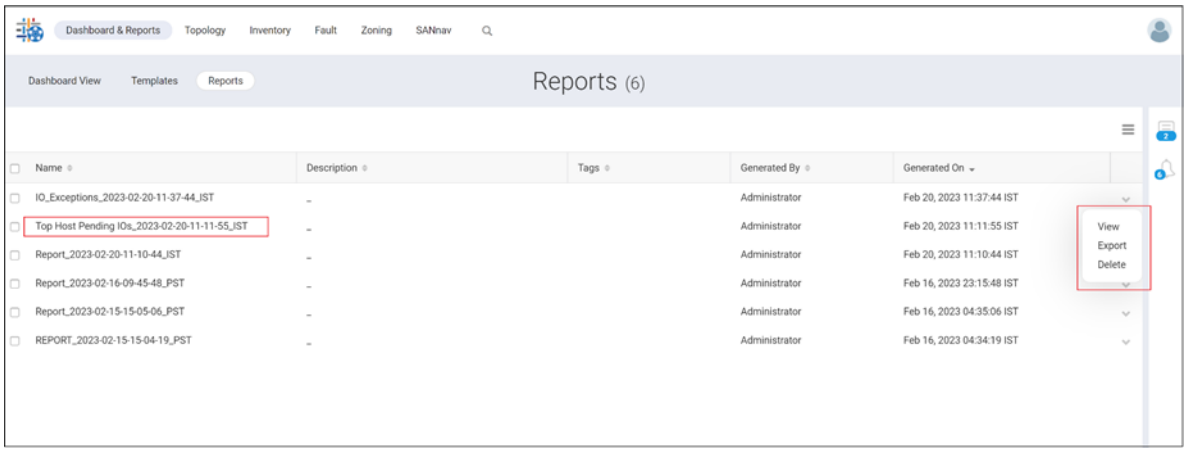
    The **Templates** page shows the template that you created.



11. Click **Generate Report** from the action menu for the template, and then click the **Reports** tab.

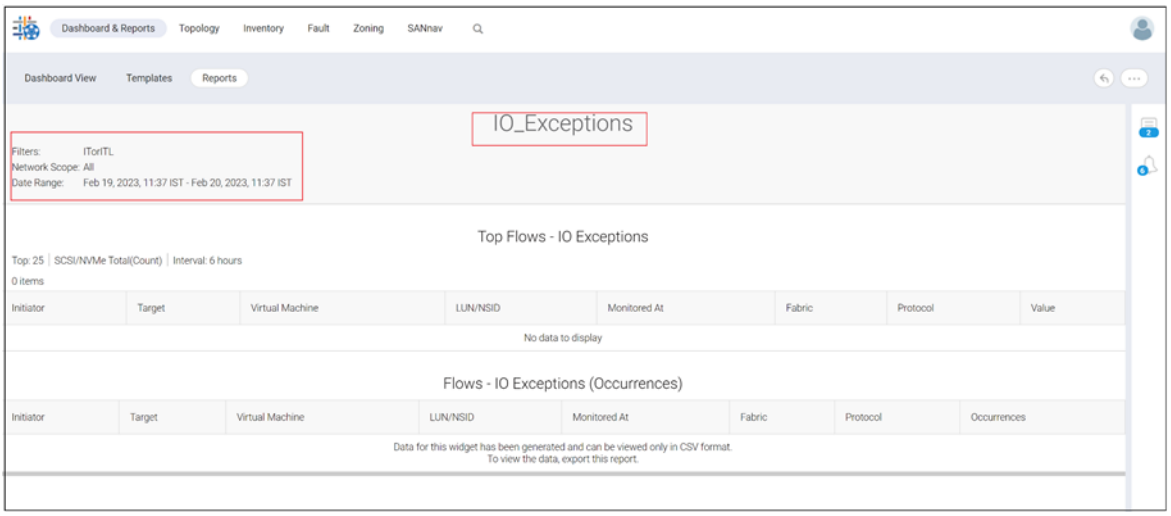
    NOTE
    The **Generate Report** option is also available in the **Actions** list inside the template view.

Notice that your report now appears in the list appended with a timestamp.



12. Click the report name to display the report.

    The **Top Flow IO Exceptions** is boxed. The bottom portion of the report, **Top Flow IO Exceptions (Occurrences)**, must be exported and viewed in CSV format.



13. Click **Export** from the more icon (...).

    NOTE
    The **Export** option is also available in the **Templates** view.

    The report is downloaded as a ZIP file to your local machine.

14. Unzip the downloaded zip file.

15. Double-click the IO Exceptions folder, and then double-click each report to view its contents.

    If the VM name is determined through SANnav vCenter discovery, the **Flow Reports** page displays the human-readable VM name for the VITL/VITN flows. The VMID is displayed in the non-human readable format if the vCenter server is not discovered in SANnav. For example, 52 70 04 2a ce d6 13 38-0c de 7a m4 89 42 58 b2. The vCenter server must be discovered in SANnav for the SANnav Management Portal to display the VM name instead of the VMID of the VITL/VITN flows. For more information on discovering vCenter, refer to the vCenter Discovery section of the *Brocade SANnav Management Portal User Guide*.

NOTE

Apply the **Virtual Machines** flow filter to fetch the VITL/VITN flows.

Troubleshooting Use Cases

This section describes the following troubleshooting scenarios, steps to troubleshoot, and symptoms to identify the issues.

Use this section to identify and troubleshoot the following issues:

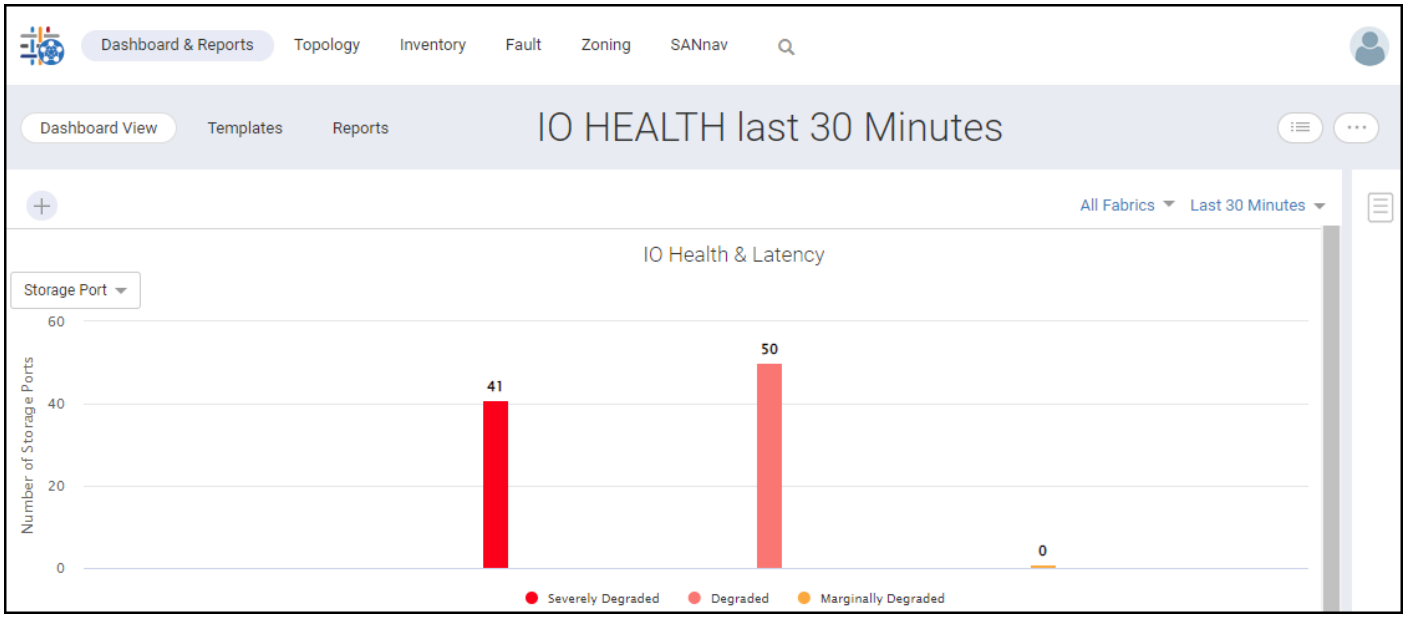
- Degraded host or storage ports in the IO Health & Latency widget
- Congested switch ports in the Network Port Traffic Conditions (NTPC) dashboard
- High-utilization of links in the SANnav Topology page

Troubleshooting a Degraded Host Port or Storage Port using Flow or F_Port Statistics

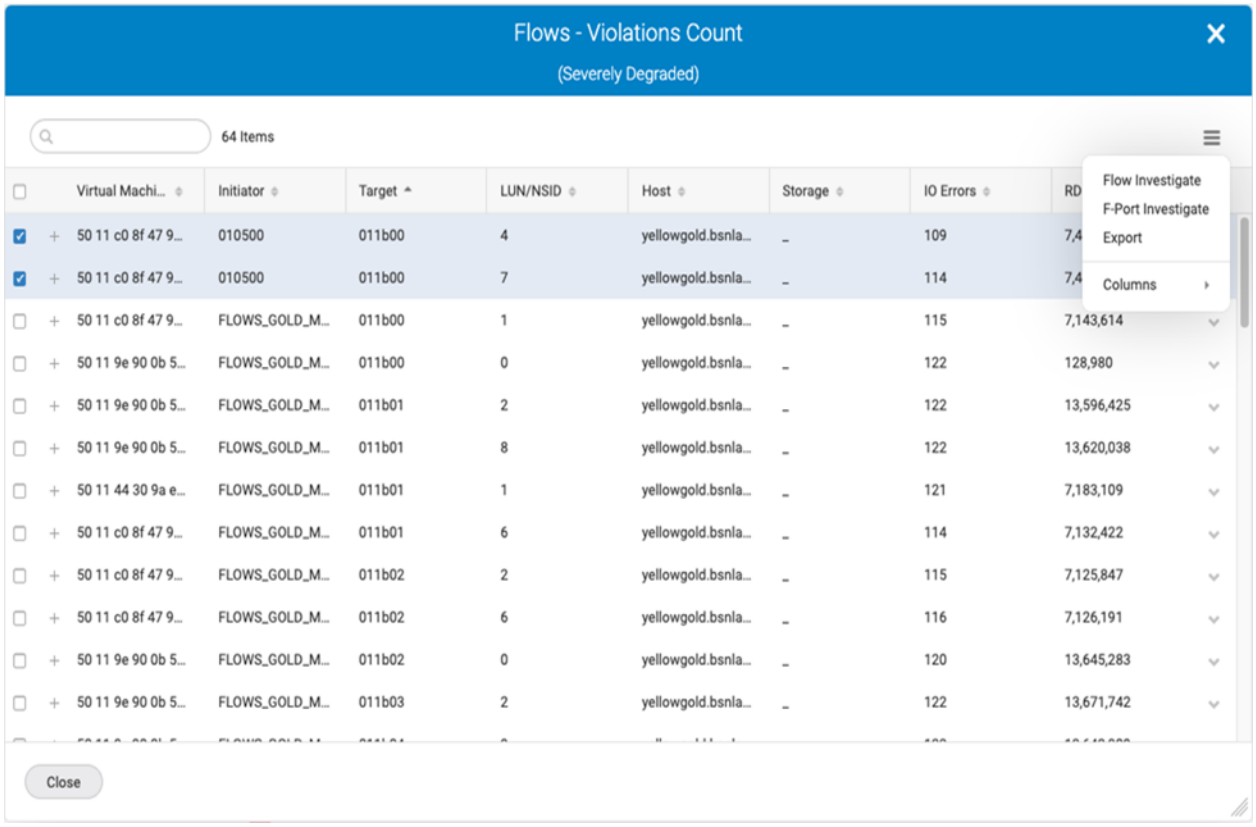
To identify and troubleshoot the degraded Host ports and Storage ports in the IO Health & Latency widget and its associated flows, perform the following steps:

1. Click **Dashboard & Reports** in the navigation bar, and then click **Templates** in the subnavigation bar.
   Create a Flow dashboard with the IO Health & Latency widget. For instructions, see Creating a Flow Dashboard.
2. Click the more icon (...) in the subnavigation bar, and select **View in Dashboard**.
3. Troubleshoot degraded host or storage ports by choosing one of the following options:
   - Select **Host Port** from the drop-down list.
   - Select **Stroage Port** from the drop-down list.

   The IO Health & Latency widget shows the count of host or storage ports in the severely degraded, degraded, and marginally degraded categories. For each category, one bar displays with the total number of host or storage ports in the category. For example, in the following image, there are 41 storage ports severely degraded, 50 storage ports are degraded, and zero moderately degraded storage ports.



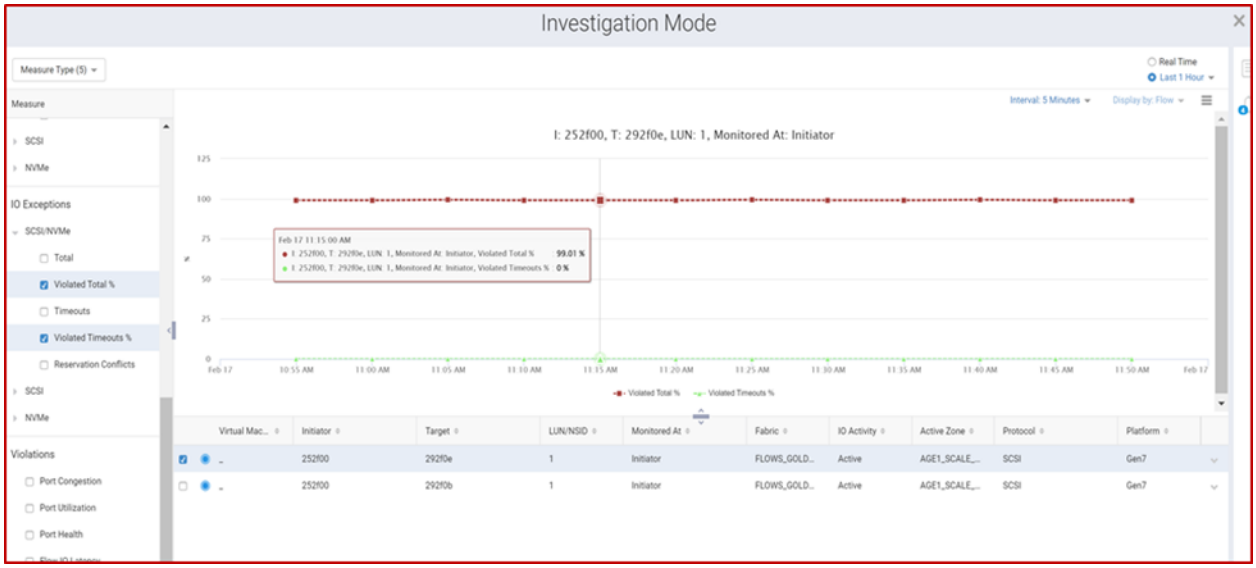
4. Click a bar to view the flow violations for the degraded hosts or storage ports in table format.
   For example, click the severely degraded bar. The Flows - Violations Count (Severely Degraded) page displays.



You can copy the Initiator or Target zone alias (if configured) or the FC address to use in a Flow Inventory filter to view the flows for the selected Initiator or Target. For additional information, see Creating a Flow Filter.

5. Investigate the historical or real-time statistics for the flow by locating the flow, and selecting **Flow Investigate** from the action menu.

   To investigate more than one flow, click the **+** icon at the left of every row for each flow that you want to investigate, and select **Investigate** > **Actions** from the **Selected Items** sidebar.

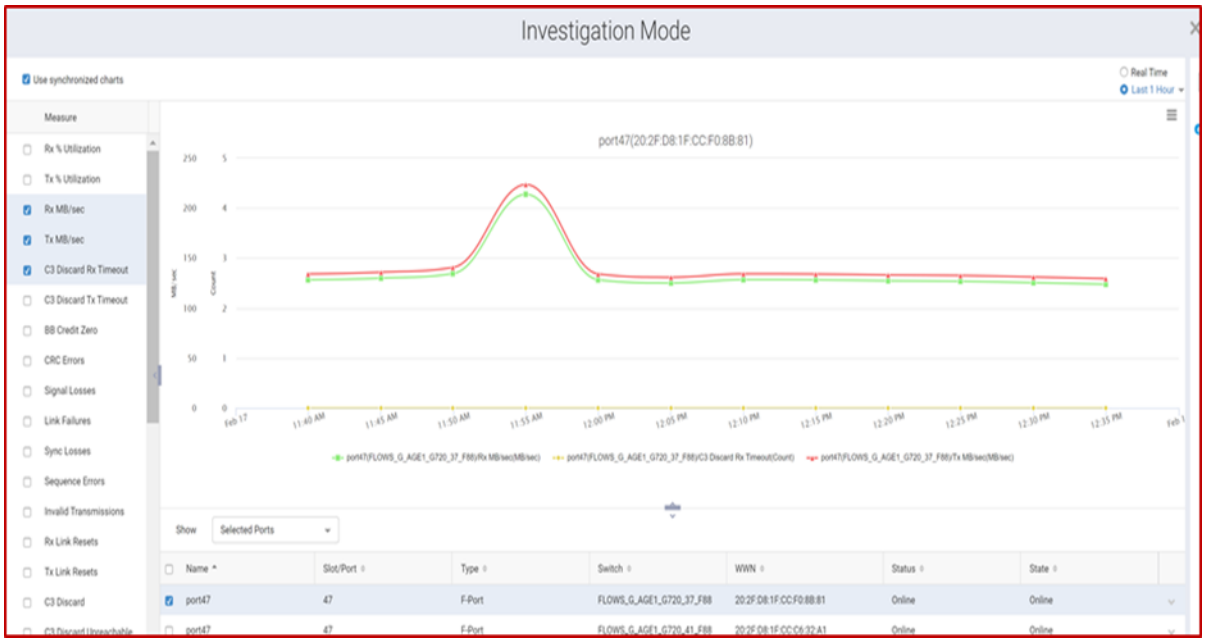


By default, SANnav Investigation mode displays historical statistics based on the dashboard time scope. Select violation measures to view the measures in a graph and compare the values to identify the root cause.

Click the **Real Time** option to check if the violations are still there for the selected flows while troubleshooting the issue.

6. Click the **Real Time** option to check if the violations are still there for the selected flows while troubleshooting the issue.
7. Investigate the historical or real-time statistics for the connected switch port by locating the flow, and selecting **F-Port Investigate** from the action menu.

   To investigate more than one connected switch port, select the checkbox for each flow that you want to investigate, click the hamburger icon, and select **F-Port Investigate**.

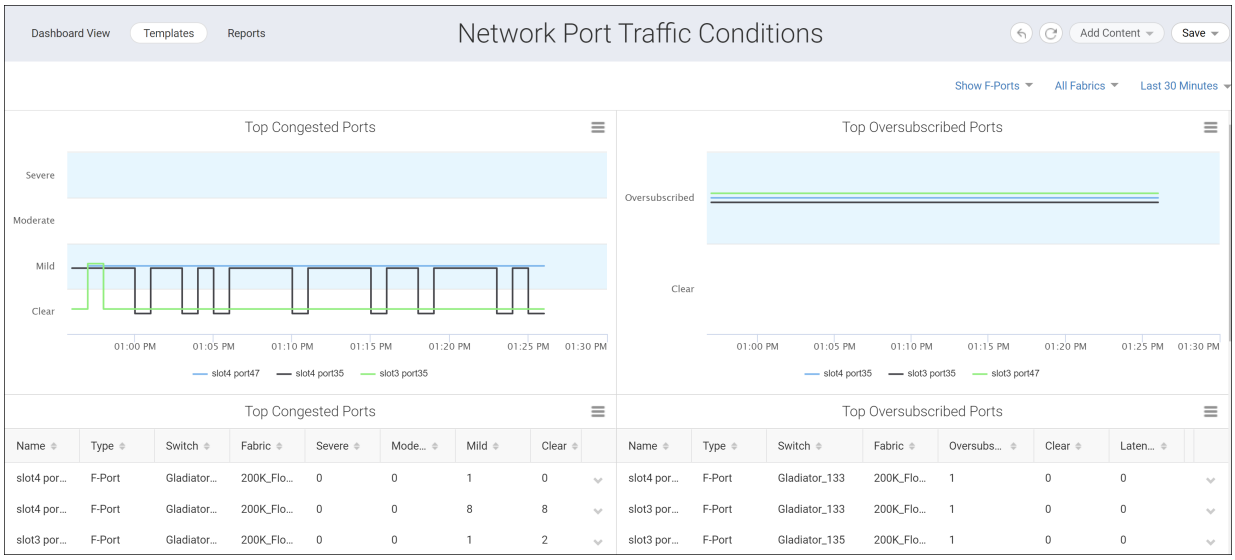


8. Select violation measures to view the measures in a graph and compare the values to identify the root cause.
9. Click the **Real Time** option to check if the violations are still there for the selected flows while troubleshooting the issue.

Troubleshooting Congested Switch Port (F_Port) Using Flows

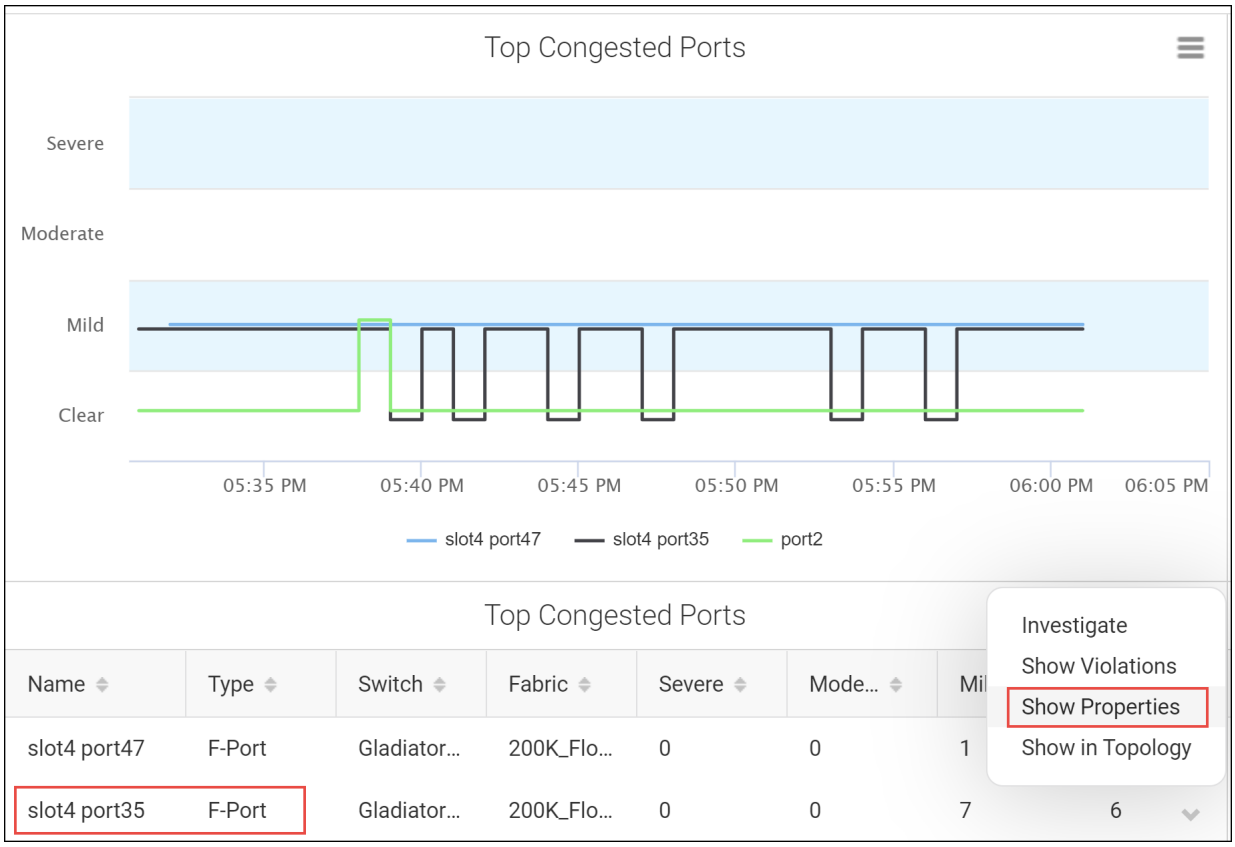
To identify and troubleshoot the congested switch ports in the Network Port Traffic Conditions (NTPC) dashboard and its associated flows, perform the following steps:

1. View an NPTC dashboard. Click **Dashboard & Reports** in the navigation bar, and then click **Templates**.
2. Locate the NPTC dashboard, and click **View** on the **Action** menu. A static view of the dashboard appears. In this example, **All Fabrics** is selected as the network scope and **Last 30 Minutes** is selected as the time interval.

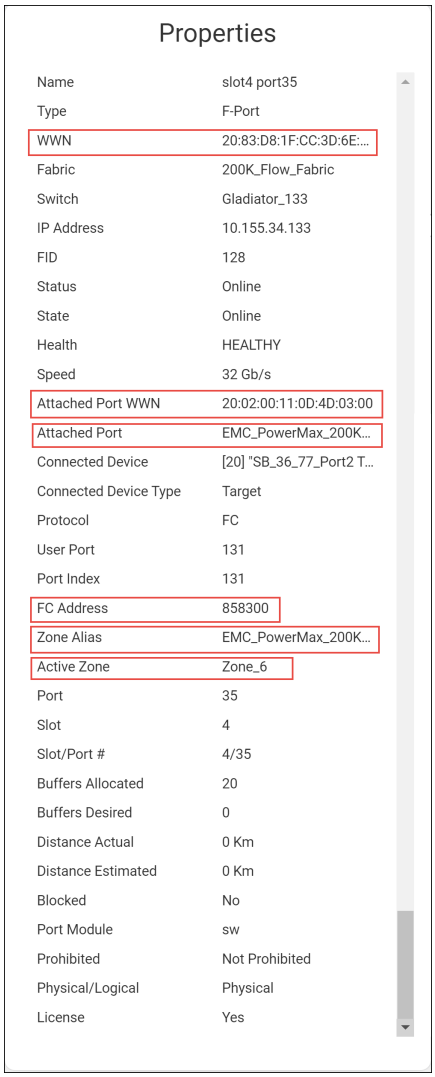


The NPTC dashboard displays information about various traffic conditions on network ports. You can access the **Top Congested Ports** widget on this dashboard to identify the potentially congested F_Ports and E_Ports on discovered switches and troubleshoot the causes of congestion.

3. Investigate the flows on the congested F_Ports. Select the port where you want to view the associated flows from in the **Top Congested Ports** collection table, and then click the down arrow on the right. Click **Show Properties**.



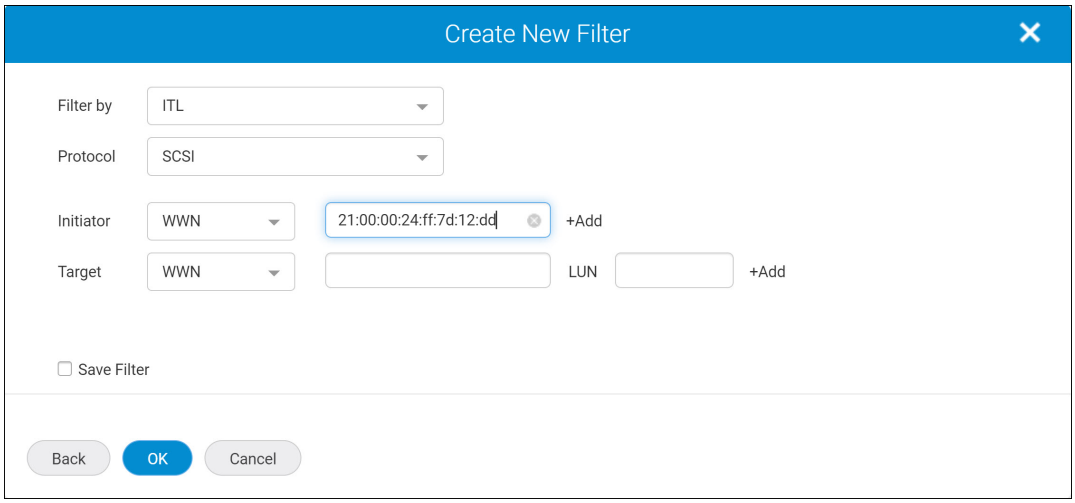
The **Show Properties** dialog box shows details about the selected F_Port.



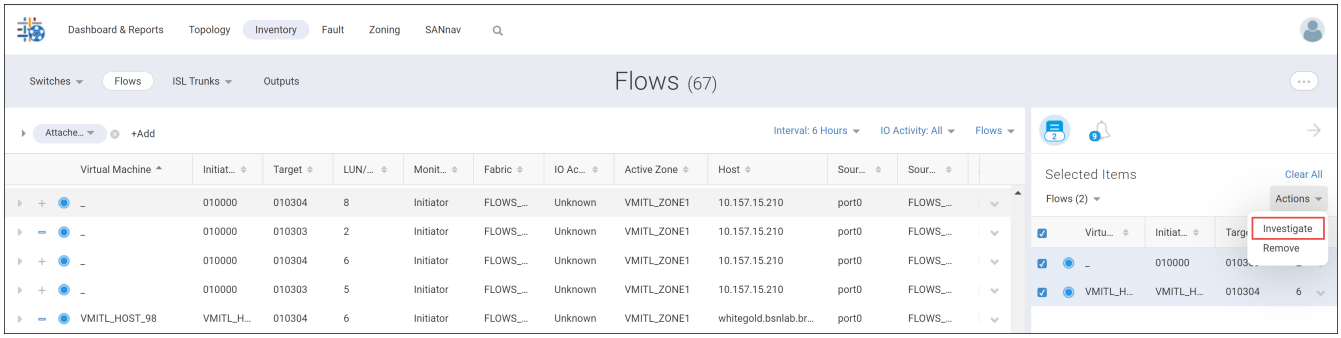
4. Copy the context for your search from the **Show Properties** dialog box.

   For example, you can record the required filter criteria details such as **Attached Port WWN**, **Active Zone**, or **Zone Alias**. For additional information, see Creating a Flow Filter.

5. Select **Inventory** > **Flows** from the top navigation menu. The **Flows** page appears. By default, no flows are displayed.
6. Apply at least one filter to display the flows. Click the plus icon (+) in the upper left of the page to add a filter. The **Add Filter** dialog appears, and you can see a list of saved flow filters.
7. Click **Create New** to view the **Create New Flow Filter** dialog.
8. Enter the **Attached Port WWN** address that you recorded previously from the **Show Properties** dialog box. Use either the **Initiator WWN** field or **Target WWN** field based on the connected device type.

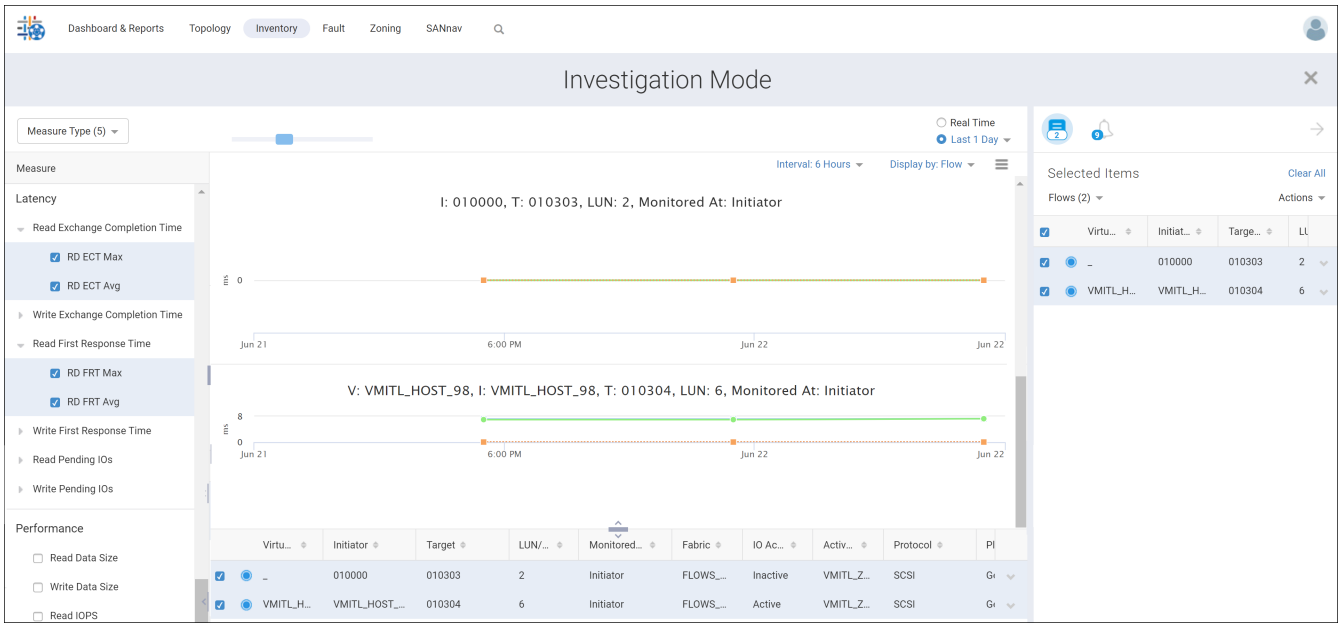


9. Click **OK** to view the flows that are associated with the attached ports on the **Flows** page.



In this example, flows are passing through the port which is congested.

10. Click the **Action** menu and select **Investigate**. If there is more than one flow, click the plus icon (+) on the left to add them to **Selected Items**.
11. Select flows from **Selected Items** and click **Investigate**.



The **Investigation Mode** page appears.

12. Select various measures and compare the values to identify the root cause of the congestion.

High-Utilization Port Flow Investigation

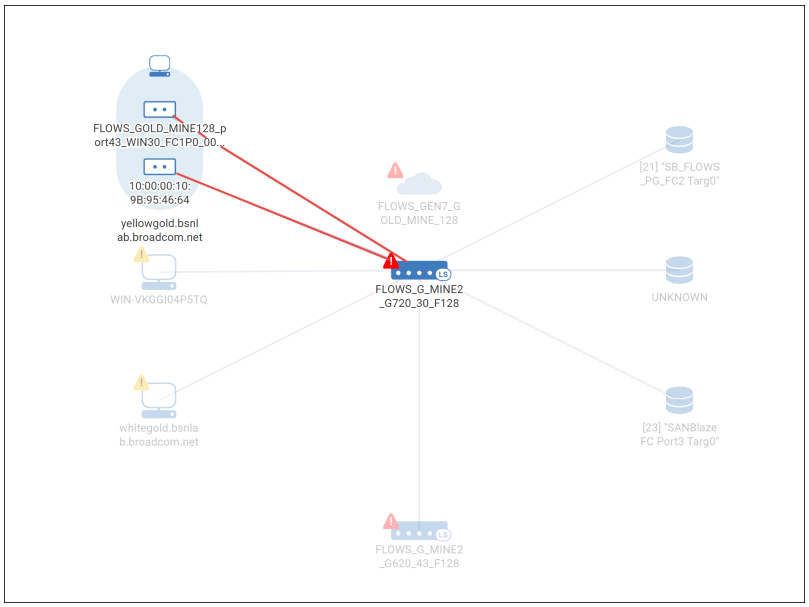
The **Topology** page provides a graphical representation of the fabrics. For example, after you discover a fabric, you might want to view the topology to see the pictorial representation of the connected switches and devices. When a busy link is over 50% utilization or over 80% utilization, you can identify the link by its color. In general, the congested or oversubscribed links are red.

Perform the following steps to view links and link utilization:

1. Click **Topology** in the navigation bar, and then click the **+** button to add a context.
2. Go to the **Add Context Type** dialog, select a context, and then click **OK**. For example, you might select the **Host Port** context.
3. Go to the **Host Port** context field, click the menu icon to select a **Host Port** into the context field.

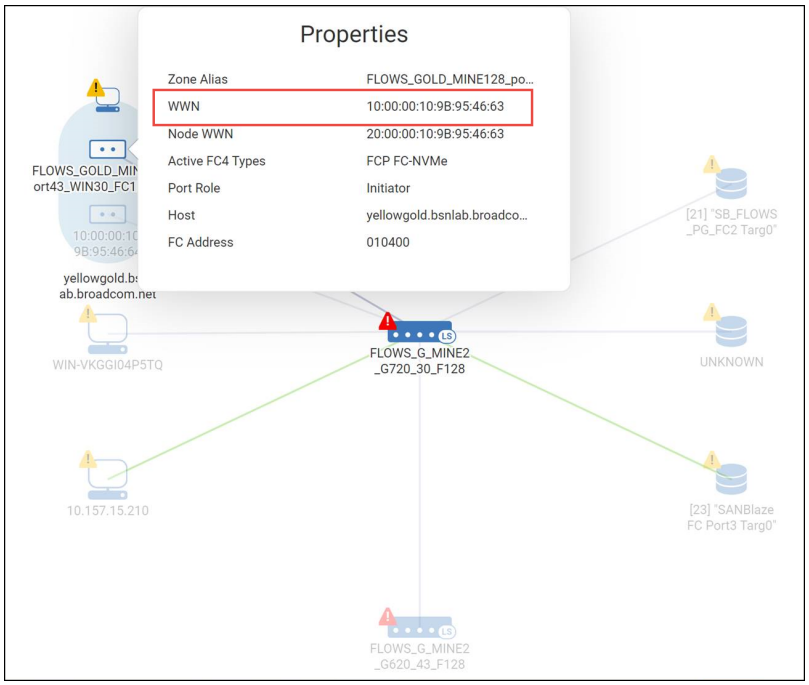
   The **Browse Topology** page displays a pictorial view of topology that is associated with the **Host Port**.

   This fabric has two switches and the link between the **Host Port** and **Switch Port** is red. This color means that the link utilization is over 80%.



4. Hover the mouse over the **Host Port**, click the menu icon, and then select **Show Properties** to display information about the port. Copy the WWN of the **Host Port** and navigate to **Inventory** > **Flows**.

   The following figure shows the WWN details from the **Properties** popup:



5. Select **Inventory** > **Flows** from the top navigation menu. The **Flows** page appears. By default, no flows are displayed.
6. Click the plus icon (+) in the top-left of the page to add a filter.

   The **Add Filter** dialog appears, where you see a list of saved flow filters.

7. Click **Create New** to view the **Create New Flow Filter** dialog. Select **ITL** from the **Filter by** field and **SCSI/NVMe** from the **Protocol** field. Enter the Port WWN copied from **Topology** > **Host Port Properties** in the **Initiator WWN** field.
8. Click **OK** to view the flows that are initiated from this Host Port on the **Flows** page.

   In this example, flows are passing through the port which is congested.
9. Click the **Action** menu and select **Investigate** to investigate a flow. If more than one flow must be investigated, then add them to **Selected Items** by clicking the **+** icon on the left.
10. Go to **Selected Items**, select the flows, and click **Investigate**.

    The **Investigation Mode** page appears. You can select various measures and compare the values to identify the root cause of the high-utilization.

Revision History

Lists the changes in the document since the initial release.

SANnav-23x-FM-UG100; April 28, 2023

Initial document version.

Documentation Legal Notice

This notice provides copyright and trademark information as well as legal disclaimers.

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 or to view the licensing terms applicable to the open source software, please download the open source attribution disclosure document in the Broadcom Support Portal. If you do not have a support account or are unable to log in, please contact your support provider for this information.


BROADCOM®