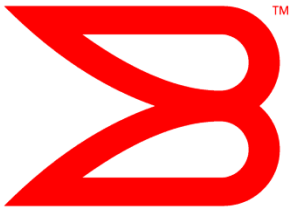


System z

FOS 7.2.0d and Network Advisor 12.1.3 Launch Highlights

BROCADE

CONTENTS

FABRIC VISION: NEW FEATURE SUMMARY

Fabric Vision technology was developed as part of a continuing effort to improve overall application availablility and reduce complexity and costs. It is a suite of monitoring, diagnostic, and traffic generation tools built into the Fabric Operating System (FOS) that runs on the Fibre Channel switches and directors. Some Fabric Vision features are automatically included in the base platform, while other Fabric Vision features are available as an optional license. Network Advisor provides users with an easy-to-use interface to display and manage the Fabric Vision features. Many Fabric Vision features can be displayed in the Network Advisor dashboard.

FOS v7.2 introduces two new capabilities in the Fabric Vision suite: MAPS and Flow Vision, available through the optional Fabric Vision license.

MAPS (Monitoring and Alerting Policy Suite)

MAPS replaces Fabric Watch with many improvements. It tracks a variety of SAN fabric metrics and events providing customers with the following advantages:

- Early fault detection
- Better fault isolation
- Proactively detect deteriorating SFPs
    - Avoid down time and replace in a scheduled maintenance window.
- Apply hundreds of predefined thresholds to monitor with a single mouse click

Flow Vision

Flow Vision is a set of tools primarily designed to help customers troubleshoot fabric wide issues. These tools go beyond just the fabric components. Flow Vision tools help avoid or minimize down time.

- Validate Inter-Switch Links (ISLs) at full line rate before putting them into service.
- Quickly detect unintended device contention
- Monitor performance on a channel path basis, not just a specific port (link address)

FEATURE DETAIL

Licensing

Customers with Fabric Watch (FW) and Advanced Performance Monitoring (APM) will automatically get the Fabric Vision licensed capabilities at no additional charge when upgrading to v7.2.0d. For IBM customers, the bladed chassis (SAN768B-2, SAN384B-2, SAN768B, and SAN384B) ship with the Enterprise Class Bundle which includes the FW and APM licenses so there is no need to purchase additional licenses. For IBM customers who purchased fixed port switches, SAN06B-R, SAN48B-5, and SAN80B-4, FW was included in the base product but APM is an optional feature.

Similarly, bladed chassis shipped new from IBM with FOS v7.2.0d will include the Enterprise Bundle which includes the Fabric Vision license. The Enterprise Bundle2, FC7416, will need to be purchased separately to get Fabric Vision technology.

Since the FW license already exists on fixed port switches, it will be more cost effective to add the APM license rather than add the Fabric Vision license. The APM license can be added either before or after upgrading the code.

Details of the licensing from IBM can be found in "IBM United States Hardware Announcement 113-214"

MAPS (Monitoring and Alerting Policy Suite)

MAPS is available for all Gen 4 (8 Gbps) and Gen 5 (16 Gbps) products. Although it replaces Fabric Watch, Fabric Watch will continue to run after upgrading FOS until MAPS is enabled.

With Fabric Watch, only the port fencing capabilities are configurable through Network Advisor. Since most System z customers only configure features that can be managed with Network Advisor, only the port fencing capabilities of Fabric Watch are used. All MAPS features can easily be managed with Network Advisor so in addition to the new monitoring capabilities in MAPS, unused features in Fabric Watch are effectively new to System z customers as well.

MAPS is enabled on a chassis; however, it is activated on individual logical switches and can be activated with different policies . It is recommended that all System z customers enable MAPS after upgrading to FOS v7.2.0d using the default aggressive policy, "dflt_aggressive_policy".

MAPS operates on a set of defined policies. Policies include what is being monitored and the action to take. Flexibility in policy definition allows users to define different actions and behaviors as the severity of certain monitored metrics increases. Actions can be any combination of RAS log alerting, email notification, SNMP trap, , and where applicable, ports can be disabled.

The ability to apply different rules based on the SFP type and port type allows for more granular actions. Alerting guidelines for SFP power consumption level, Tx/Rx optical power, and temperature are dependent on the SFP type. The acceptable Rx power range, for example, is very different for a 16 Gbps 25Km LW optic than for an 8 Gbps 150m SW optic. All supported SFP types have a predefined class. Specific rules appropriate for the SFP type and port login type (E-Port or F-Port) can be defined.

MAPS Policies

A MAPS policy contains a set of rules. Policies can be copied and edited. There are three default policies: conservative, moderate and aggressive. For Fabric Watch users three additional policies that are the MAPS equivalent of the Fabric Watch policies are automatically created:

- fw_active_policy (the active policy at the time MAPS was enabled)
- fw_custom_policy (the user defined policy)
- fw_default_policy (the default policy)

For System z customers, the default aggressive policy is recommended. Based on experience, a few of the previously recommended port fencing parameters have been changed so there are some differences as outlined in the table below.

Parameter	Previous Recommended Fabric Watch Thresholds (per minute)	MAPS Aggressive Default Policy (per minute)
C3 Discard Frames	2	2 Channels & control units 5 E-Ports (ISLs)
ITW	25	20
CRC	3	2
Link Reset	2	4
Protocol Error	2	2
State Change	7	5

For customers who wish to keep the existing fencing parameters rather than use the fw_active_policy, the recommendation is to copy the default aggressive policy and make the desired changes. MAPS monitors for other metrics besides the aforementioned port fencing parameters so editing a copy of the default aggressive policy allows users to take full advantage of MAPS while maintaining the same port fencing values.

What MAPS Monitors

- The aforementioned conditions or port fencing
- Chassis FRUs
  - Power supplies, fans, blades, and WWN card
- SFPs
  - Tx & Rx optical power
  - Temperature
  - Voltage
  - Power consumption

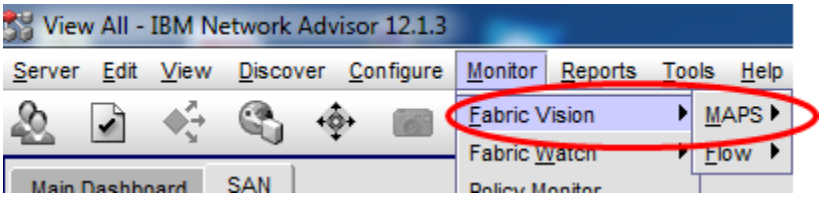
Where MAPS Sends Alerts

- To Network Advisor
  - RAS log
  - Switch properties – also effects icon displayed with switch
- A user defined email address
- A user defined SNMP trap

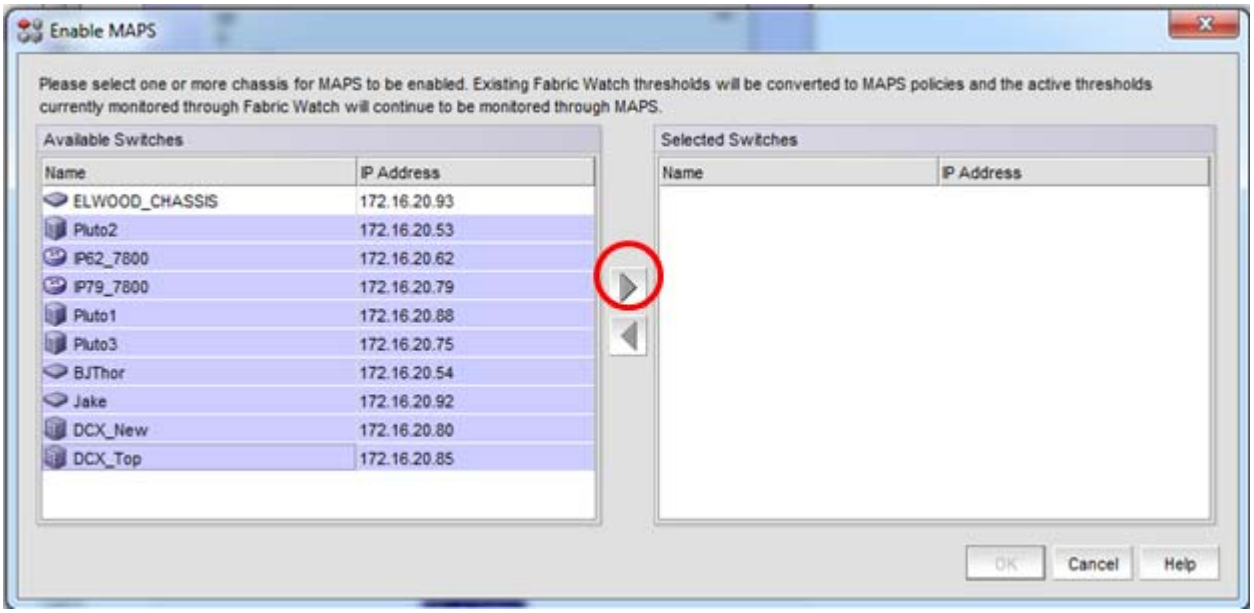
Quick Start Guide

Managing MAPS is easy and intuitive using Network Advisor. This section provides just a few examples to help users get started using MAPS. MAPS configuration videos are coming soon to YouTube.

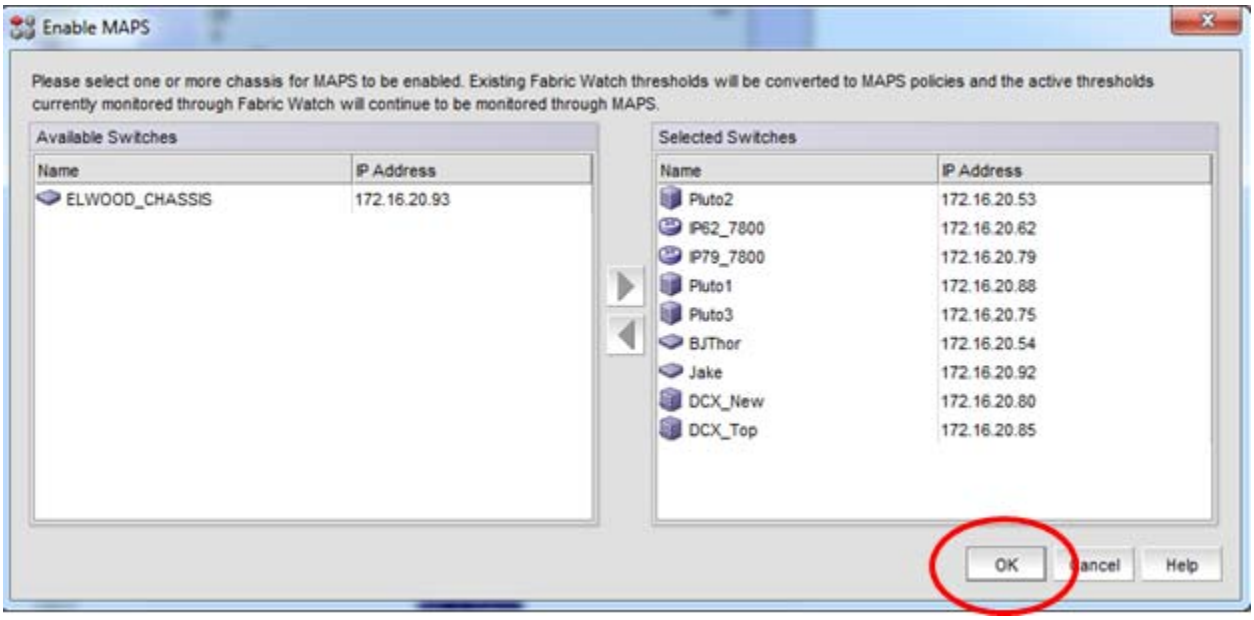
MAPS is not automatically enabled. To enable MAPS:



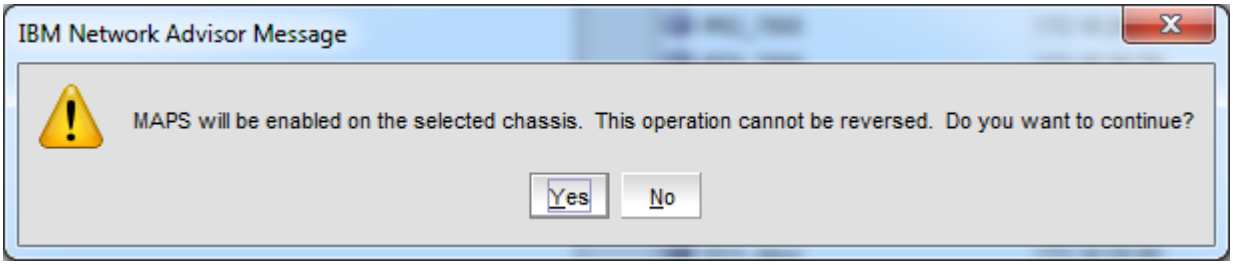
Select the chassis to enable MAPS on from the left column. In this example, MAPS will be enabled on all chassis except the “ELWOOD_CHASSIS”:



After clicking the right arrow button, the selected chassis will be moved to the right hand panel. Click “OK” to enable MAPS.

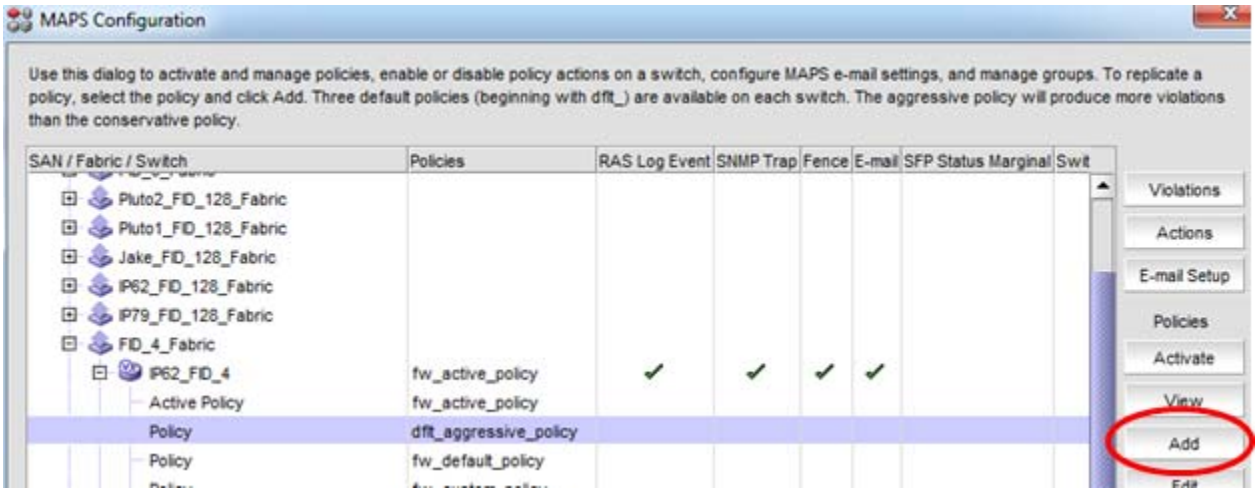


The following warning message is displayed:

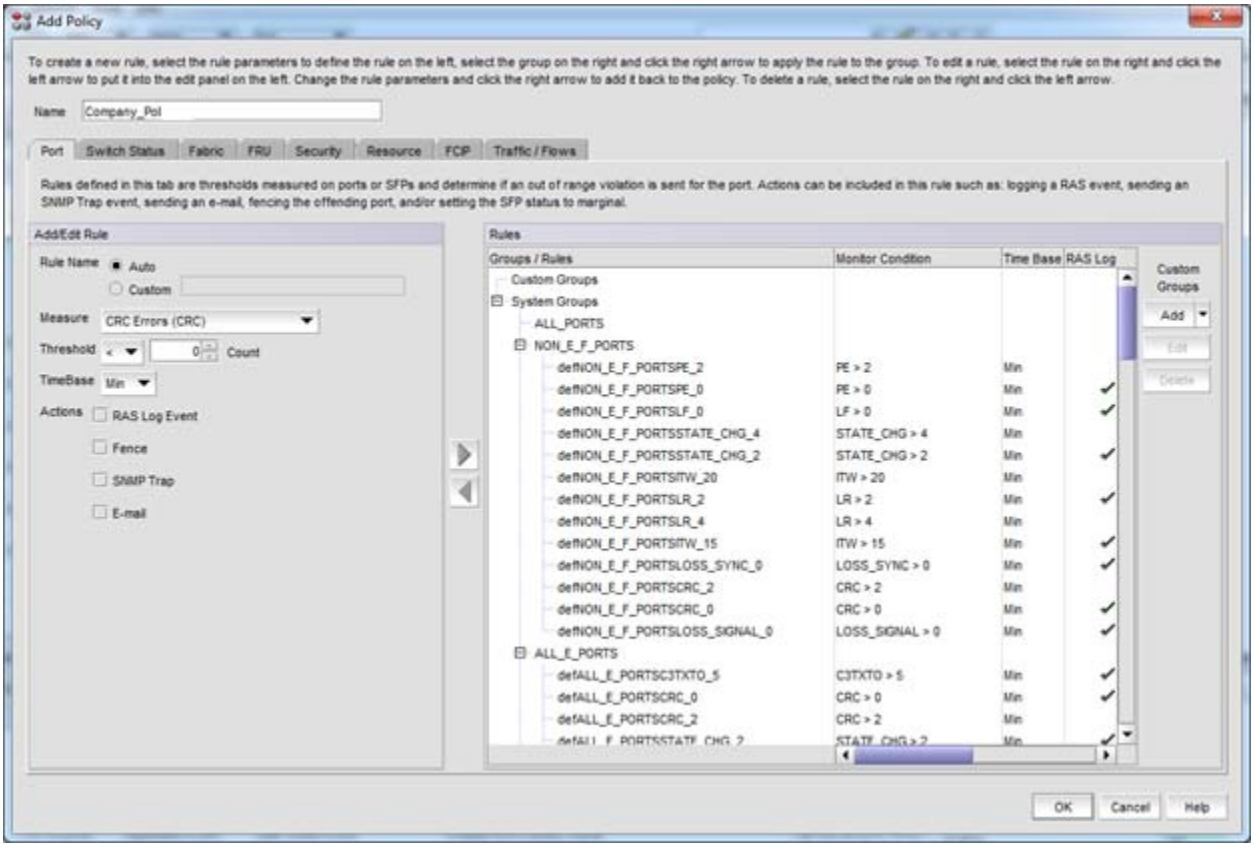


In this example, FOS was upgraded from v7.1.0c to 7.2.0d while Fabric Watch was enabled. When MAPS was enabled, the custom policy fw_active_policy was created and activated. The recommendation is to select the default aggressive policy, dflt_aggressive_policy. To do so, simply highlight dflt_aggressive_policy and then click the "Activate" button in the following figure.

The active policy cannot be copied or edited. None of the default policies can be modified but they can be copied and saved as a new policy. To minimize the risk of missing important settings, the recommended best practice when creating custom policies is to copy a policy closest to what you want and then edit the copy. To copy a policy, highlight the policy you want to copy and then click on the "Add" button.



Enter a name for the policy, in this example "Company_Pol", in the name box then click OK in the lower right.



You can then select this policy for editing and activate it when you are ready. In this example, the policy was only edited for one chassis but in most production environments it's likely that you will want to distribute the policy to all chassis.

Flow Vision

A flow is defined as traffic between two ports or all traffic going or coming from a port. In System z parlance, traffic between two ports is a "path". For example, the path between a CHPID and control unit link address can be monitored and isolated to just that path rather than having to monitor all traffic on either the port where the CHPID is attached or the port where the control unit is attached.

There are three functions within Flow Vision:

Flow Monitor

SAD screens, FICON Director Activity Report, and statistics previously supplied by FOS and reported in Network Advisor are for specific ports. With Flow Monitor, performance analysis can be based on a specific CHPID to link address path. Multiple Flow Monitors can be created. All Flows to a given port can be discovered automatically so performance at a specific port can be analyzed by channel path.

In addition to simplifying configuration, the ability to automatically discover a Flow for all paths to a given port can also be a valuable troubleshooting tool to determine where traffic is coming from. For example, an HCD mistake that results in two CHPIDs from different CECs contending for the same tape port is easily found by setting up a Flow Monitor on the tape port to automatically discover all flows. A single mouse click brings the user right to the port information with the RNID data that articulates the CEC S/N, CHPID, and CSS.

Flow Mirror

With the current implementation, mirrored frames are sent to the chassis processor (CP card on bladed switches). The first 64 bytes of an FC frame can be analyzed unobtrusively. This feature is more valuable with FCP channels than FICON channels. It can be used for:

- SCSI Reserve/Release performance troubleshooting
- Troubleshooting protocol errors
- Troubleshooting slow drain devices

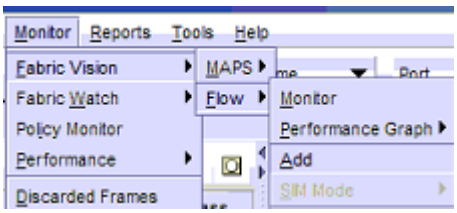
Flow Generator

Generates traffic at line rate. For System z customers, the expected use for this feature is to validate inter-switch links (ISLs), especially through DWDM and over leased lines. Previously, the only feature to generate traffic to validate links was ClearLink but ClearLink was designed to test/validate cables and optics, not to stress links. Flow Generator is a complimentary tool that can stress links at full line rate and validate paths through a switch.

Quick Start Guide

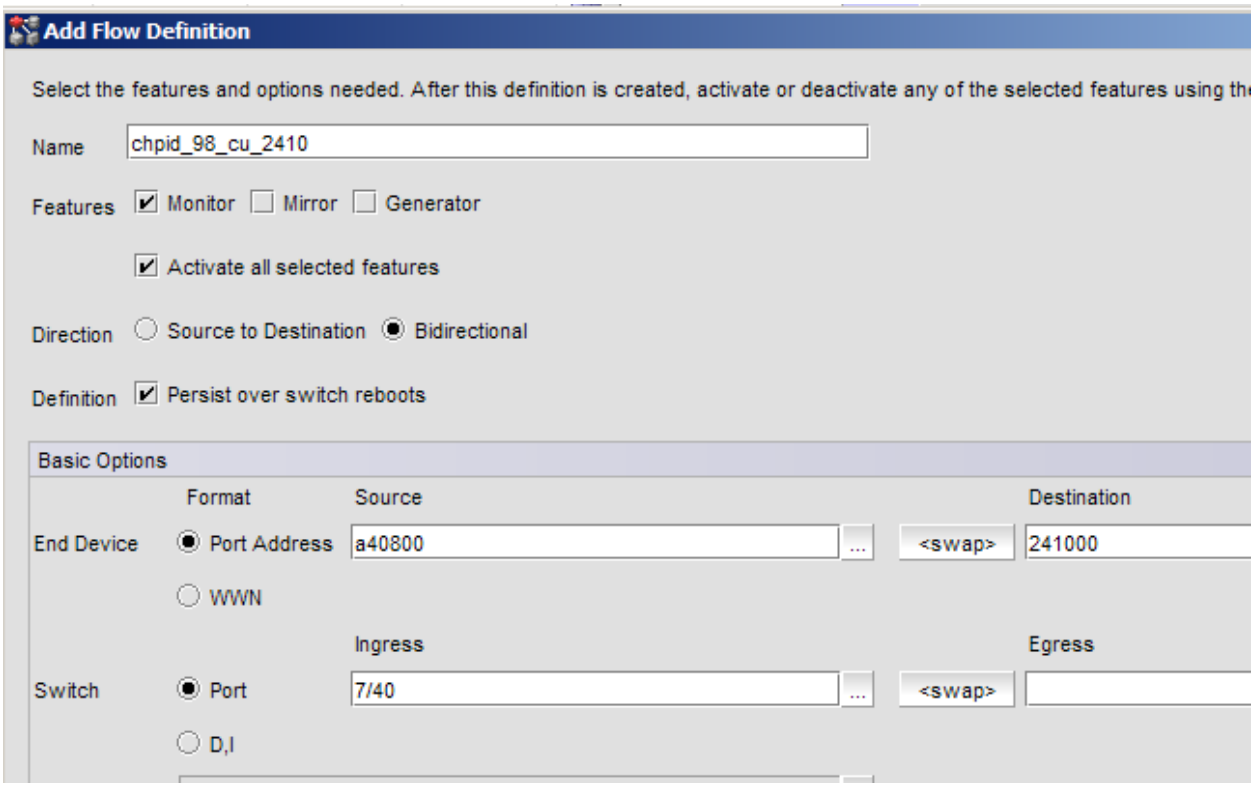
Managing and configuring Flows are easy and intuitive using Network Advisor. This section provides just a few examples to help users get started using Flow Vision. Flow Vision configuration videos are coming soon to YouTube.

The easiest way to create a Flow on an F-Port is to right click on the port in the product tree that you wish to make the source or destination port and select “Flow”.



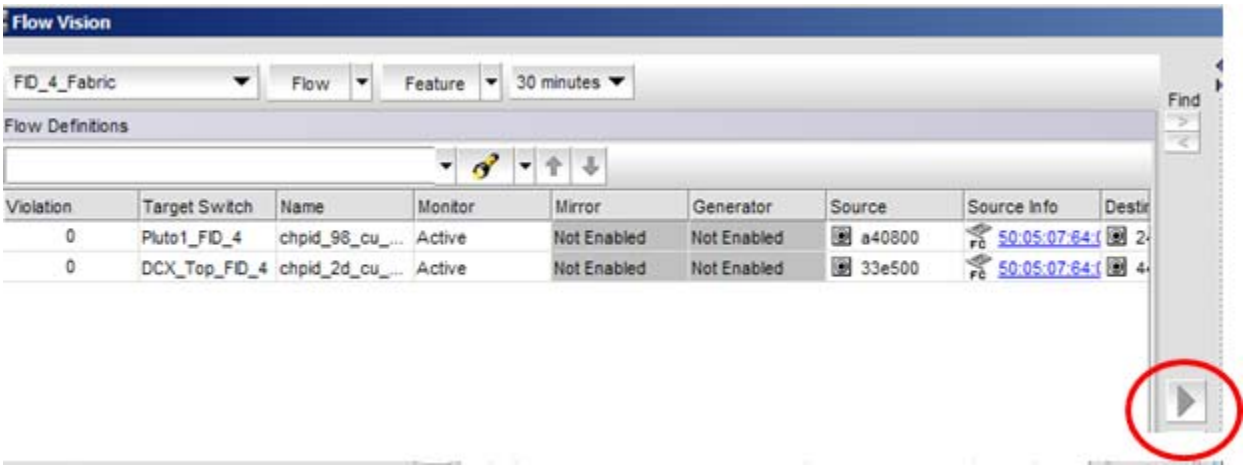
By doing so, all the source port information is automatically populated in the form used to define the flow so all that is needed is the target port information. Note that the full Fibre Channel address must be specified. In this example, link address 2410, which has a full Fibre Channel address of 241000, was chosen.

To automatically learn flows to specific destinations use an asterisk, '*'. Keep in mind that the concept of source and destination ports is from the perspective of the port of interest and the direction of the traffic flow. If you wanted to learn Flows for all channels with a path to a certain tape port, the tape port would be the source port and ingress port while the destination port would be '*'.

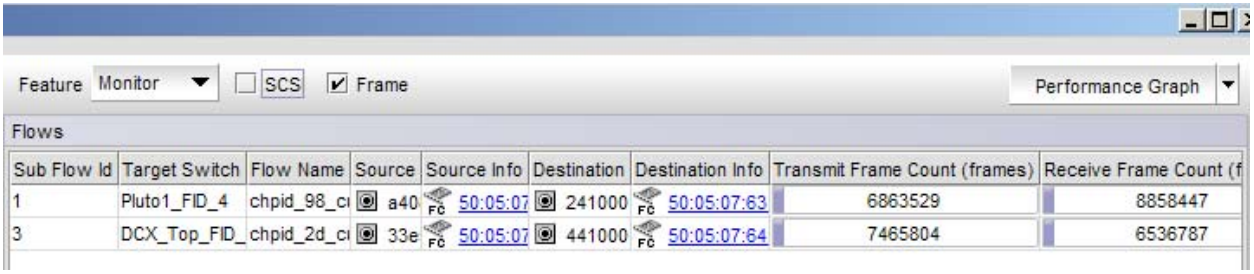


After clicking OK, you can define what you want to monitor. In this example, another Flow was added.

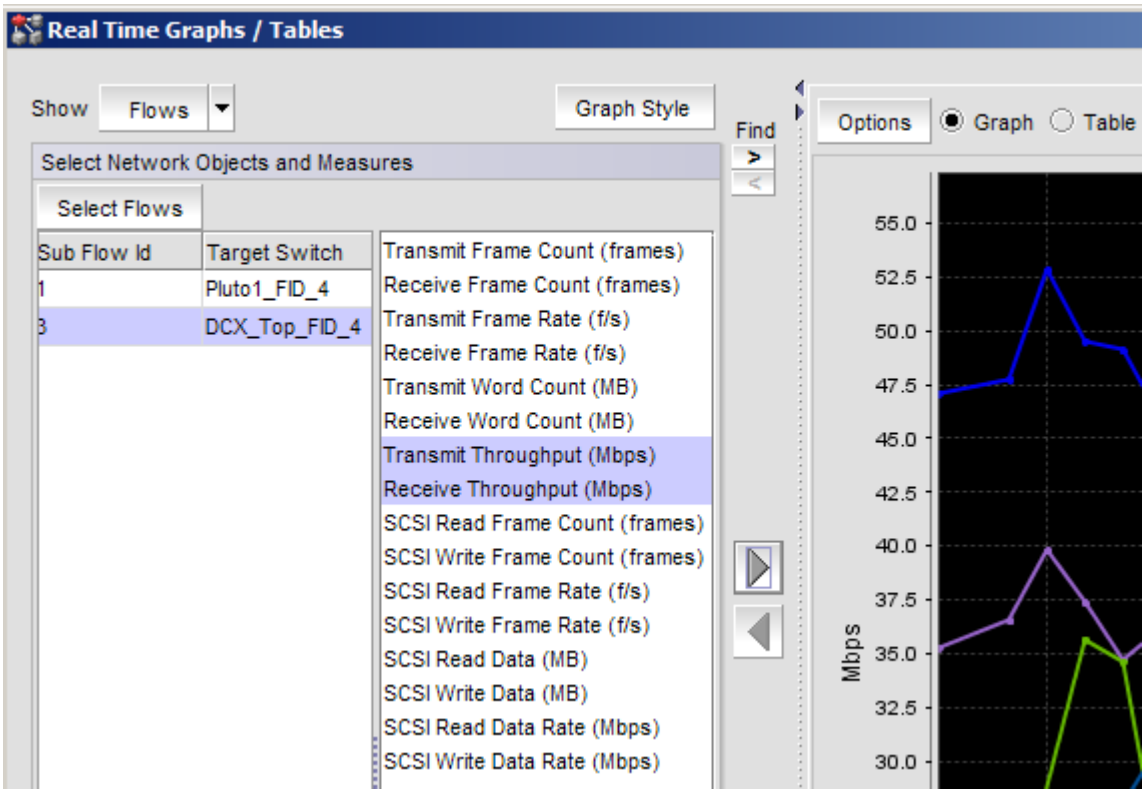
The left panel is:



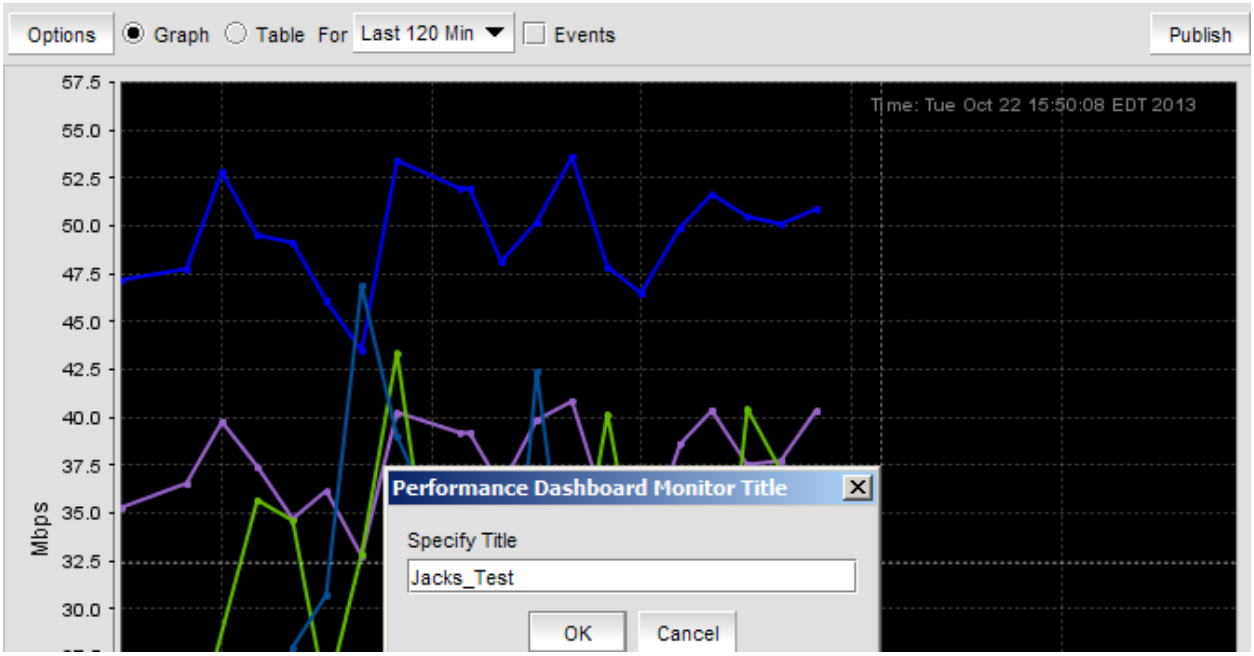
After clicking the right arrow button, the flow is moved to the right panel. Note that for FICON, SCSI is unchecked and only frames should be checked. SCSI protocol can be selected for FCP channels on System z. In this example a Flow monitor to display performance is defined for these two flows.



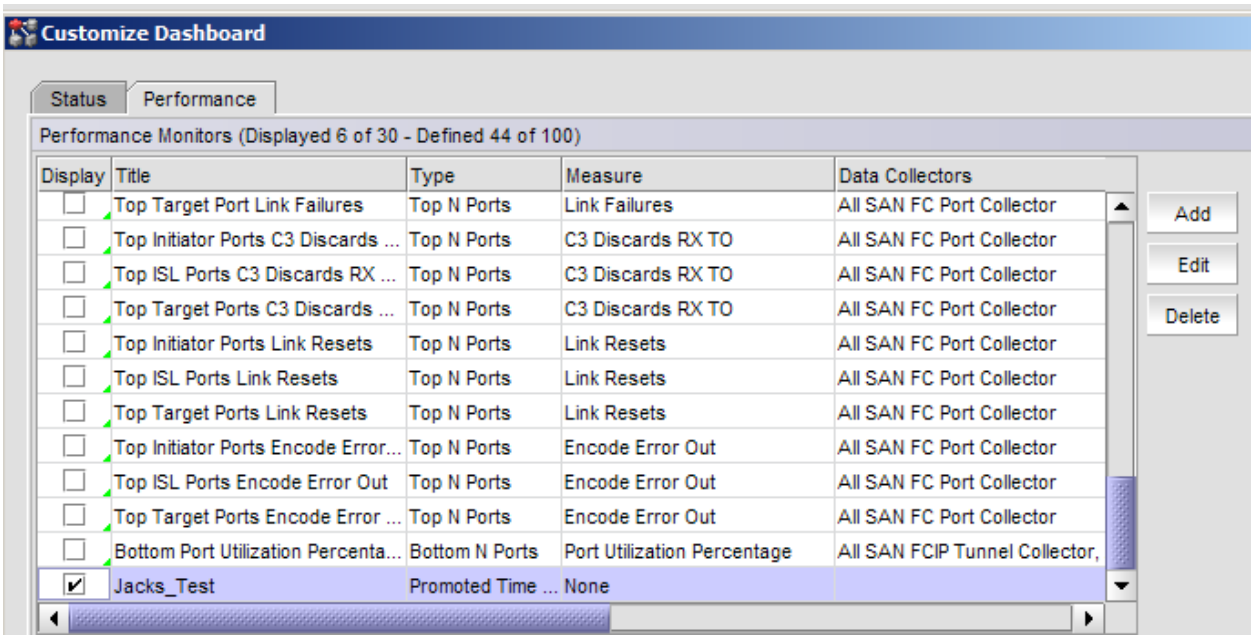
Details of what to graph are then defined by selecting the measurement objects and using the arrows to move those objects to the graph.



Once the graph is complete, clicking on the “Publish” button in the upper right corner of this dialog box makes the Flow Monitor available to be added to the Network Advisor dashboard.



Moving over to the dashboard, “Jacks_Test” can now be added.



CODE

FOS:	7.2.0d
Network Advisor:	12.1.3 (build 4)
JRE:	1.7 build 25 (for Network Advisor)

Code Upgrade/Downgrade Notes

The Fabric Watch configuration at the time of the code upgrade is preserved so that customers requiring a code upgrade backout plan can down level without any change to the existing configuration. Since there is no equivelent function to Flows in v7.1.0c, if any Flows are defined they only need to be disabled before down grading code.

The supported non-disruptive upgrade path from Brocade is from 7.1.x to 7.2.0d. Although Brocade supports disruptive upgrades from earlier versions of FOS, the majority of testing is done from 7.1.x to 7.2.0d and all upgrade testing performed as part of the IBM qualification process are done from 7.1.0c to 7.2.0d. IBM customers on any version of FOS v7.1 should upgrade directly to 7.2.0d. All other customers should follow the upgrade to v7.1.0c specified in the release notes for 7.1.0c before upgrading to v7.2.0d. Refer to the FOS v7.2.0d release notes for additional upgrade/downgrade considerations.

Similarly, the majority of Network Advisor upgrade testing is performed from 12.0.x to 12.1.3 and all upgrade testing performed as part of the IBM qualification process are done from 12.0.2 to 12.1.3. IBM customers on any version of Network Advisor 12.0.x should upgrade directly to 12.1.3. All other customers should follow the upgrade path to 12.0.2 specified in the release notes for 12.0.2 before upgrading to 12.1.3. See the Network Advisor 12.1.3 release notes for additional upgrade/downgrade considerations.

The Java Runtime Environment (JRE) used in Network Advisor 12.0.2 is 1.7 build 17. The recommended upgrade procedure is to upgrade the server to 12.1.3 first, then load the new JRE from Network Advisor.

RESOURCES

IBM Qual Letter

An IBM login ID is required.

https://www-304.ibm.com/servers/resourcelink/lib03020.nsf/pages/switchesAndDirectorsQualifiedForIbmSystemZRFiconRAndFcpChannels?OpenDocument

Code and Release Notes

You will need an IBM login ID to click though the links displayed at this site. You will be redirected to a Brocade site for code and release notes. Code and release notes are also avail from MyBrocade.com; however, IBM customers are advised to use the IBM link because only IBM qualified code is displayed when using the IBM link.

https://www-304.ibm.com/support/docview.wss?mynp=OCSTMSAD&mync=E&uid=ssg1S1003855&myns=s031

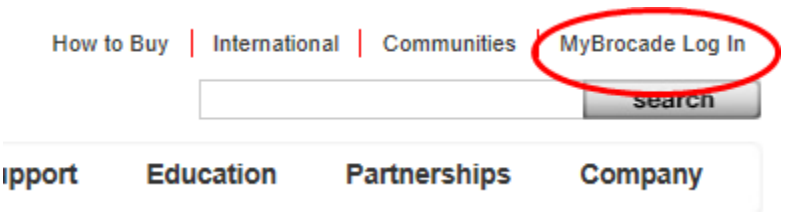
Miscellaneous Documentation (Best practices, configuration guides)

Brocade public website:

www.brocade.com/solutions-technology/technology/san-fabric-technology/mainframe.page

MyBrocade

From www.brocade.com click on “MyBrocade Lode In” in the upper right corner:



Search on “Fabric Vision” or the specific name of the feature to find detailed documentation. For mainframe specific information, Navigate to Communities->Mainframe Solutions

If you don’t already have a user ID, you’ll need to create one. Creating a user profile is easy and free for Brocade customers and business partners.

FEATURE AND HARDWARE REFERENCE TABLES

Virtual Fabric and CUP Support

Product	Highest FOS	Base Switch (XISL)	Maximum Logical Switches	Maximum Instances of CUP	Notes
SAN256B	6.4.2a				
SAN40B-4	7.0.0d	Open Only			Withdrawn from marketing.
SAN80B-4	7.2.0d	Open Only	4	2	
7800	7.2.0d	Prevented by Software	4	2	GE interfaces can be placed in the default switch with tunnels defined in each logical switch to get the same functionality as XISLs
SAN384B	7.2.0d	√	8	4	
SAN768B	7.2.0d	√	8	4	
SAN48B-5	7.2.0d	Open Only	4	2	
SAN384B-2	7.2.0d	√	8	4	
SAN768B-2	7.2.0d	√	8	4	

Blade Support

Any blade not listed in the table below is not supported in a chassis used for System z.

	DCX DCX-4S	DCX8510-8 DCX8510-4
FX8-24	√	√
FX8-24E	√	√

FC8-16	√	
FC8-32	√	
FC8-48[2]	√	
FC8-64[1]	√	√
FC16-32		√
FC16-48[2]		√

Notes

1. The FC8-64 is supported for open systems only. Although the blade may be in the same chassis that will have FICON traffic, all ports of the FC8-64 must be in a logical switch that is not used for FICON connectivity.
2. The FC8-48 and FC16-48 blades are only supported in a logical switch configured for address mode 1, zero-based addressing, on the DCX and DCX8510-8.

Switch Type and Model/Brand Cross Reference Table

IBM Brand Name	IBM Model	Brocade Brand Name	Product Type
SAN256B	2109-M48	48000	4 Gbps
SAN40B-4	2498-B40	5100	8 Gbps
SAN80B-4	2498-B80	5300	8 Gbps
SAN06B-R	2498-R06	7800	8 Gbps
SAN384B	2499-192	DCX-4S	8 Gbps
SAN768B	2499-384	DCX	8 Gbps
SAN48B-5	2498-F48	6510	Gen 5
SAN384B-2	2499-416	DCX8510-4	Gen 5
SAN768B-2	2499-816	DCX8510-8	Gen 5

TRADEMARKS AND NOTICES

