Fabric Vision: Getting Started With MAPS

Consoli Solutions

Disclaimers & Notices

- All sample scripts described herein are licensed under the Apache License, Version 2.0. See module headers for details.
- Sample scripts and libraries are provided as examples. Consoli-Solutions is not responsible for errors.
- Sample scripts and libraries are available for free when used by single customers for their own internal use. Use of these scripts and libraries in the manufacturing process, configuration of equipment for other customers, or providing services requires additional licensing.
- Consoli Solutions is an LLC

The legal disclaimer is here for you to read.

Contact

Jack Consoli

jack_consoli@yahoo.com
Begin the subject with "FOS API"

https://github.com/jconsoli

Consoli-Solutions began as a hobby business after I retired from Broadcom. I had too many hobbies so I dropped this in favor of spending more time with music. This is why I dropped the previous business email address of jack@consoli-solutions.com, but I'll still take questions. Put "FOS API" in the subject line so that I don't automatically delete it.

As of the date this video was created, the LLC was still valid and I intend to keep it up to date. The email domain and insurance were still valid as well; however, I do intend to drop those.

Other YouTube Videos In This Series

Simplified Brocade FOS API: Getting Started
https://www.youtube.com/watch?v=BWz7L0QOtYQ

Simplified Brocade FOS API: Capture Data and Reports
https://youtu.be/n9-Eni_AFCg

Simplified Brocade FOS API: Configuring Switches
https://www.youtube.com/watch?v=WGxXZrvhG2E

Simplified Brocade FOS API: Zoning
https://youtu.be/x1OvuRZRdA8

Scripts & Documentation: https://github.com/jconsoli

This video is primarily focused on Fabric Vision MAPS configuration considerations. I cover using some of the scripts described in other YouTube videos as a tool to facilitate determining MAPS rules and planning prior to enabling the feature. Much of the content herein is applicable regardless of the tools you use. If you do plan on using these tools, you will need to install Python and use the FOS API. I recommend the "Getting Started" and "Capture Data and Reports" videos. "Getting Started" begins with installing Python which most admins skip. There are some specific Python library requirements, FOS requirements, and environment considerations covered in that video as well. Rather than skip the video altogether, just fast forward past the sections you don't need.

Follow the github link at the bottom of the page for a copy of this presentation and the scripts described herein. The last section of the Getting Started video discusses common features and inputs for the sample scripts.

Additional Notes

Simplified Brocade FOS API: Getting Started
Discusses how to download Python, what libraries are needed, how to install

libraries, some tips for Python newbies, a few FOS settings you need to be aware of, an overview of the libraries I created to simplify scripting tasks, and an introduction to the sample scripts.

**Simplified Brocade FOS API: Configuring Switches**
Discusses a few nuances of configuring logical switches, Examples include: how to use sample scripts to configure logical switches from a workbook, and how to use an existing switch as a template for creating and configuring logical switches.

Simplified Brocade FOS API: Capture Data and Reports (This video)
Includes examples on how to collect data from switches, generate a general report, a comparison report, a MAPS report, and an extensive nodefind utility.

Simplified Brocade FOS API: Zoning
Zone from a workbook, restore zoning from a previous data capture, merge zoning databases from multiple fabrics, and zone from CLI
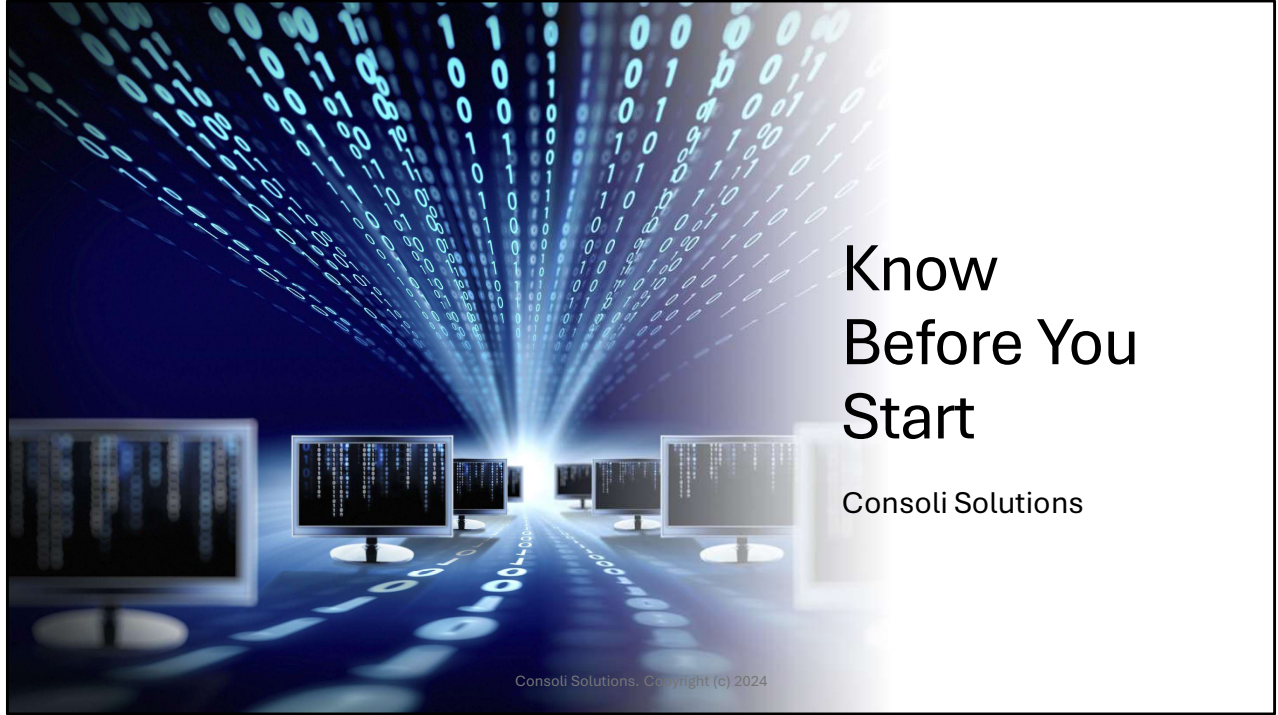
Know Before You Start

Consoli Solutions

Fabric Vision Overview

- SAN fabric diagnostics and real time monitoring
  - Focus of this presentation is the real time monitoring component
  - Use SANnav for diagnostics
- Monitoring and Alerting Policy Suite (MAPS)
  - Consists of groups and rules used to define thresholds and actions which are put in policies managed by FOS.
  - Real time monitoring
  - More than just alerting. It can trigger actionable events.
- Advanced features are licensed
- Search for "Brocade Fabric Vision MAPS"

Fabric Vision is a feature that has two basic components: a diagnostic utility and real time monitoring. This video is only focused on the real time monitoring aspects.

The MAPS policies, rules, and groups define what the real time monitoring component of Fabric Vision looks for. The monitoring is performed at the logical switch level, so you can have different policies for different switches. When the feature was first introduced, it only alerted on events. Hence the name. It now includes the actionable events discussed on the next slide.

The base policy monitors for basic things such as power supply and fan health. The base policy is included with FOS at no additional charge. There is nothing to do to enable it. The more advanced features are licensed.

Brocade was acquired by Broadcom, but the Brocade brand name was kept. There are several good documents and YouTube videos which are easy to search for.

MAPS: Getting Started

- First time enabled: Often floods the log with alerts.
- Evaluate the environment first.
  - Cabling issues
  - Known fabric congestion issues
- Create rules that make sense for your environment.
  - This is the focus of the remainder of this presentation.
- How often do you want to be notified of a potential problem?
  - The "Quiet Time" determines how long to wait before alerting on the same threshold.

Flooding the log with alerts, especially from issues you know are present, can be more harmful than helpful.

Each threshold setting has it's own quiet time.

The Default Policies

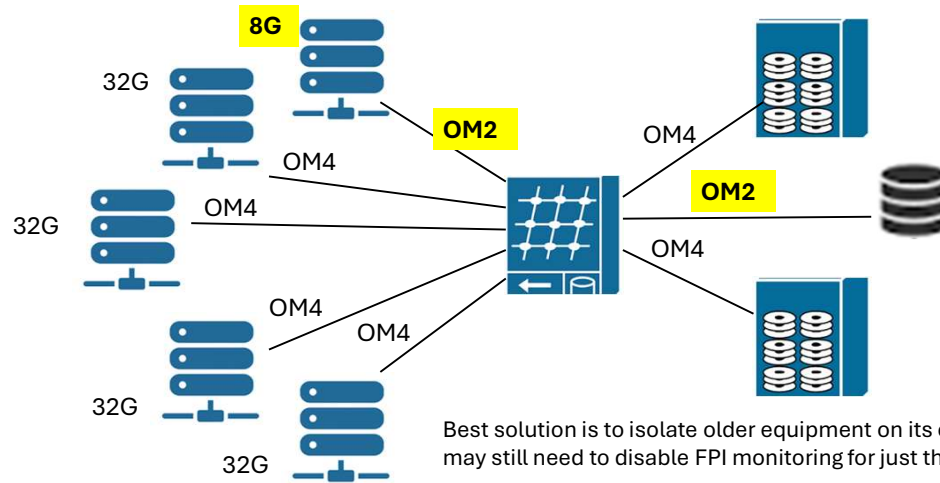| Default Policy	Description
base	Included with basic FOS support. Monitors and alerts on basic chassis parameters such as power supplies, temperature, etc.
aggressive	Licensed. Typically recommended for mainframe environments.
moderate	Licensed. Typically recommended for new open SANs with OM4 or OM5 cabling.
conservative	Licensed. Start here when none of the above applies or your SAN. These more complex SANs to be discussed shortly.

There are default rules, groups that define what the advanced monitoring features look for and the actions to be taken. SAN admins typically copy a default policy to begin with and make it their own. Determining which policy to start with depends on your SAN which is covered on the next slide.

From a SAN design perspective, mainframe fabrics are typically pristine and use all single mode fibre.
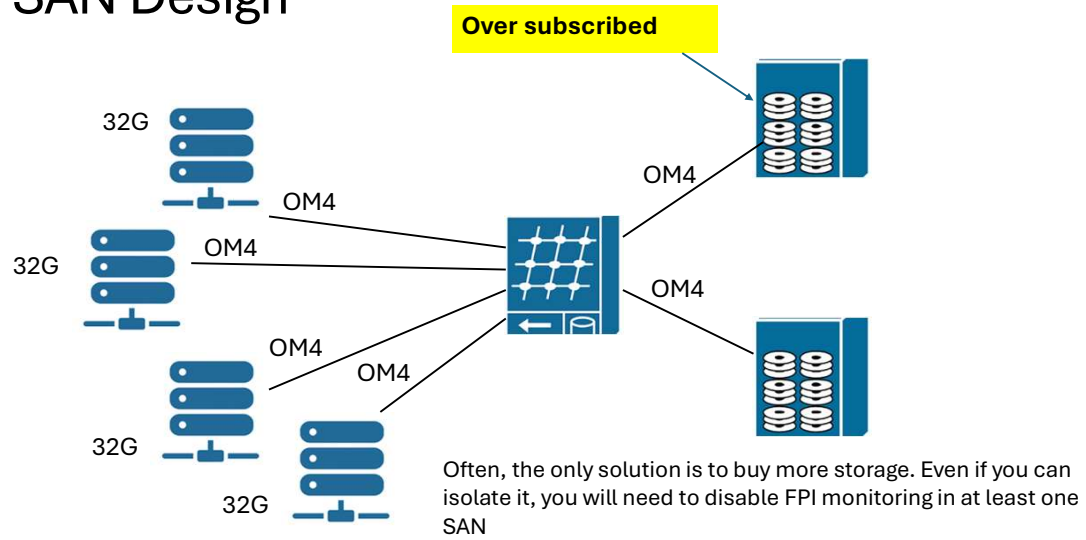
New SANs typically use all OM4 or OM5 cable. SFPs are typically newer 32G or 64G capable. Older SANs often have a mix of older optics and perhaps OM3 cable. There may even be some OM2 in your environment. Bit errors are usually cable infrastructure related, so bit error thresholds are determined by the cable plant.
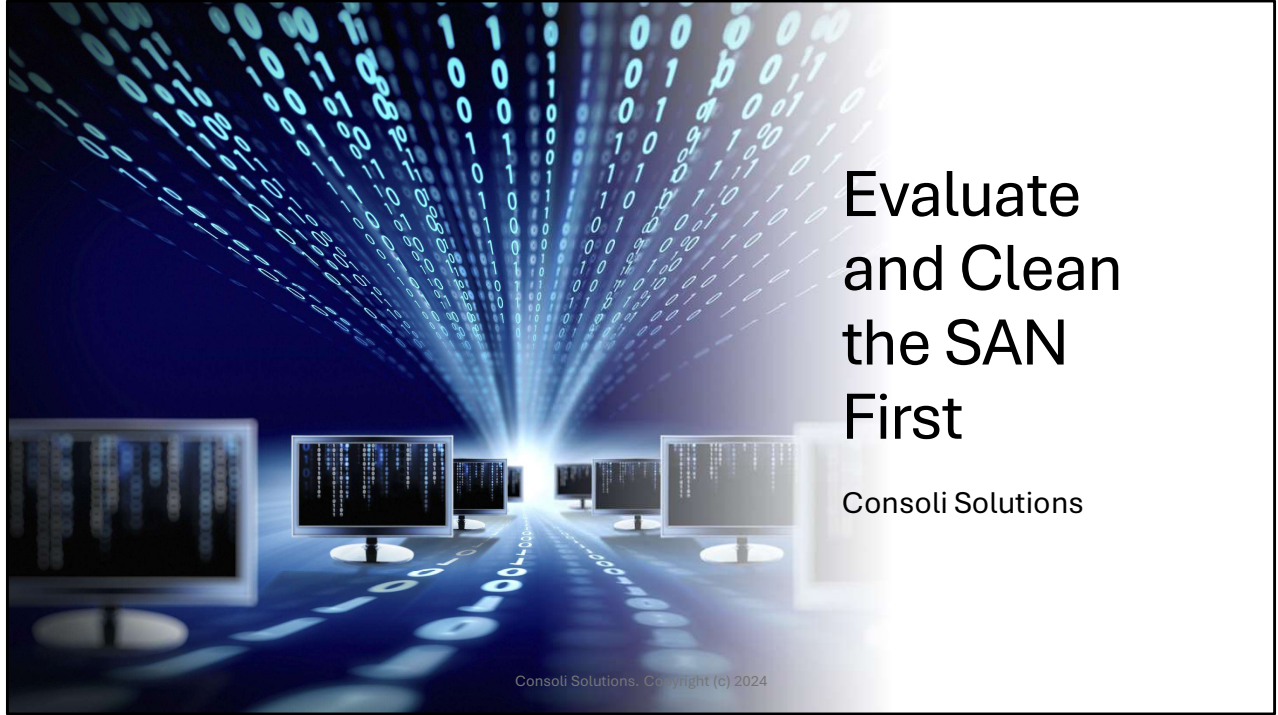
SAN Design

8G

32G

OM2

OM4

OM4

32G

OM4

OM4

OM4

32G

32G

OM4

OM2

OM4

Best solution is to isolate older equipment on its own SAN. You may still need to disable FPI monitoring for just that SAN

SAN Design

32G

OM4

32G OM4

OM4

OM4

32G

32G

Often, the only solution is to buy more storage. Even if you can isolate it, you will need to disable FPI monitoring in at least one SAN

Consoli Solutions. Copyright (c) 2024

10

Evaluate and Clean the SAN First

Consoli Solutions

Run Reports

Simplified Brocade FOS API: Capture Data and Reports:
https://youtu.be/n9-Eni_AFCg

option	Description
-bp	Excel file with best practice definitions.
-sheet	Name of worksheet in the file specified with –bp to use.
-sfp	Excel file with SFP thresholds.
-clr	Clear port stats after polling them.
-group	Name of Excel file that defines zone groups.

```
multi_capture.py -i credentials -bp bp –sheet My_Rules -sfp sfp_rules_test
  -clr –group my_groups –r -log _logs
```

These options are discussed in detail in the referenced YouTube video.

Running the report once clears all port statistics. Subsequent reports are useful monitoring bit errors.

Using SANnav is an easy way to check bit errors and temperature sensors. I prefer this method because it's easy to kick off daily reports, look back at the history, and the best practice settings can be configured to just show specific errors. The resulting best practice violation summary sheet contains just the errors you are looking for. It's also a more convenient way to do some "what if" scenario checking in advance.

Create Groups File (-group)

- Make a copy of groups.xlsx
- Clear examples
- Most customers use a simple alias convention
- Other filters:
    - Zone
    - Switch;port
    - switch;port_name
    - WWN

Group	Filter	Operand	Operator
Storage_Group_1	Alias	Storage_1_*	wild
Storage_Group_2	Alias	Storage_2_*	wild
Storage_Group_3	Alias	Storage_3_*	wild

- Other Operators:
    - regex-m
    - regex-s
    - exact

Modify Best Practices (-bp, -sheet)

	Port
TRUE	sfp_health_check
TRUE	remote_sfp_health_check
TRUE	LOGIN_SPEED_NOT_MAX_W
TRUE	SWITCH_LIMITED_SPEED
TRUE	PORT_F_ZERO_CREDIT
TRUE	PORT_C3_DISCARD
TRUE	PORT_TXC3_DISCARD
TRUE	PORT_RXC3_DISCARD
TRUE	PORT_BIT_ERRORS
TRUE	PORT_FRAME_ERRORS
TRUE	PORT_LOGICAL_ERRORS
TRUE	PORT_ENABLED_NO_LIGHT
FALSE	PORT_TSB_2019_276
TRUE	PORT_FAULT
TRUE	PORT_SEGMENTED
TRUE	PORT_QSFP_BRKOUT_ASN
FALSE	PORT_SFP_HAA_F16_32_P8

active **rules_std** spe

Consoli Solutions. Copyright (c) 2025

- Example: Show bit errors, faulty SFPs, and faulty ports only
  - Copy "rules_std" to another worksheet.
  - In the multi_capture.py example, I named the sheet "My_Rules"
  - Set all of these and all checks in other sections to FLASE
  - Set all others FALSE
- Results in a summary sheet with just the issues that are being investigated.
- For bit errors, just copy and paste that sheet into a work order

14

A Few More Things To Think About

Consoli Solutions

Temperature

- Chassis temperature increases, monitored by the temperature sensors, are the result of diminished air.
- MAPS monitors thresholds
- Default thresholds are to warn against the maximum operating range of the H/W.
- Ambient temperatures vary widely depending on heating and cooling.
- Determine the temperature range for a week.
- Create a threshold that is 5-10^0 C greater than the peak.

20	
21	**Chassis**
22	Test_5_Jun_2025 ←

106	**Sensors**			
107		**Sensor 1**	**Sensor 2**	**Se**
108	Sensor Type	temperature	temperature	temper
109	State	ok	ok	ok
110	Temperature C	30	40	

Rising chassis temperatures are often the result of something changing in the cooling system. I know of a customer who had an asset tag placed over an air vent, but the more common issue is that cabling or new equipment changes effected airflow. Even if you are still within a supported temperature range, most people want to know if this happens.

Heating and cooling can vary from rack to rack, so you'll want to do this for each switch. If your readings are inconsistent, you may need to consider a higher threshold. Rising temperature is a result of increased power consumption, but monitoring power consumption is a little more challenging, so I just look at temperature as a predictor.

To check sensors, run the multi_capture utility. This is discussed in the "Capture Data and Reports" video referenced near the beginning of this presentation.

Did All SFPs Login At Expected Speed?

- A device may negotiate to a lower speed if there are many link errors.
- This may mask cable problems.
- If remote SFP statistics are available, the report will find and flag these as errors.
- Create storage groups
  - Easily identify all login speeds
  - Report flags speed imbalances
  - This will be more useful later when looking for fabric congestion

Looking at Storage Groups

Group	Comments	Switch	Port	Port Name	Zoned To	Speed Gbps
Array_1						
√	Mixed server login speeds zoned to this target.	Switch_1	0/31	Array_1_Int_00	4	32
		Switch_2	0/11	Server_A_0		16
		Switch_2	0/22	Server_B_0		8
		Switch_1	0/10	Server_C_0		16
		Switch_1	0/20	Server_D_0		16
√	Login speed, 16G, is less than maximum speed of group 32G	Switch_1	0/30	Array_1_Int_01	4	16
		Switch_2	0/11	Server_E_0		16
		Switch_2	0/22	Server_F_0		16

18
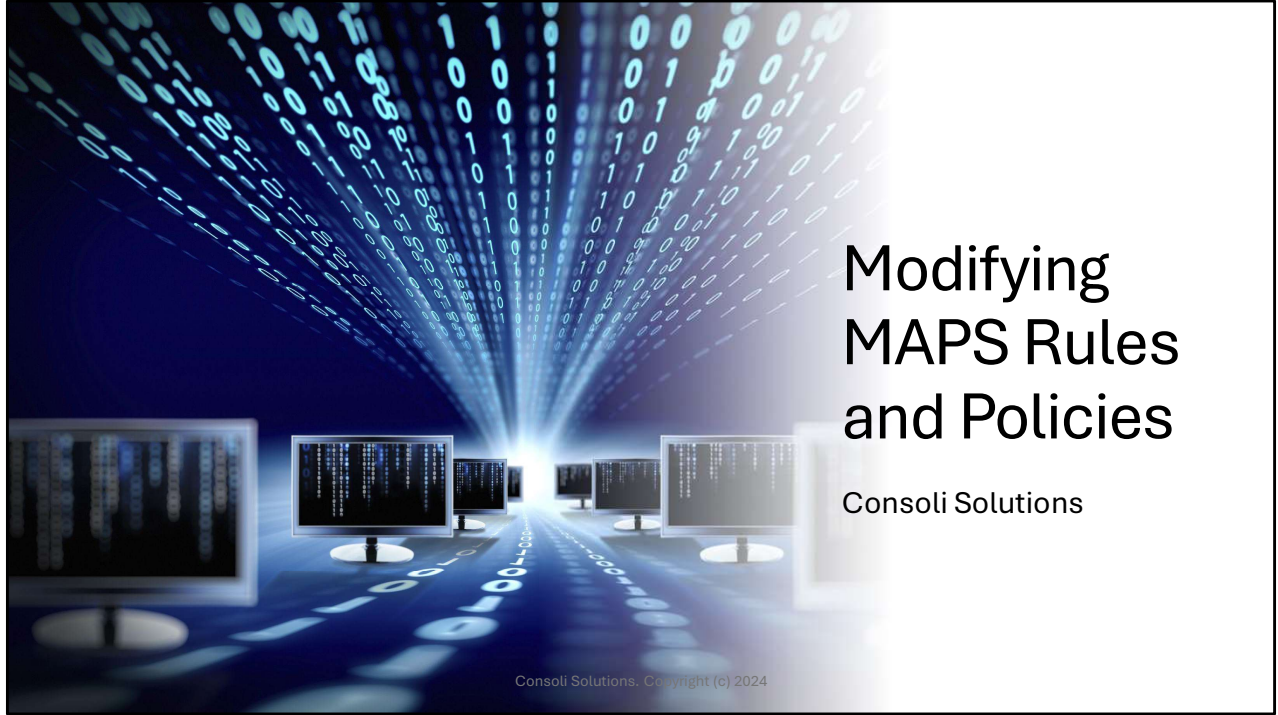
Modifying MAPS Rules and Policies

Consoli Solutions

Notes

- Rules
  - Quiet time ←———————
  - Maximum custom rules: 500
  - "def" in lower case anywhere in a rule is a default rule
- Policy
  - Add/Remove Rules
  - "dflt_" in lower case anywhere in a policy is a default policy
- Groups
  - Not covered in this presentation
- Change With SANnav or CLI

Example

- Disable all performance impact
  - defALL_PORTS_IO_PERF_IMPACT
    - Not: defALL_PORTS_IO_PERF_IMPACT_UNQUAR
  - defALL_PORTS_OVERSUBSCRIBED
    - Not: defALL_PORTS_OVERSUBSCRIPTION_CLEAR
- Set the quiet time for to 86400 (day).
  - 32G SFP Rules
    - ALL_32GSWL_SFP

Check for cable work activity before spending time doing a scientific evaluation of servers or storage.

Frequent loss of signal followed by a successful login is typically a connected device issue.

Modify The Rules

Copy the MAPS report

Find the logical switch to work with

Do not change the header. The FID number is determined by the header. The same is true for groups and policies.

Contents

Select the worksheet of the switch rules you want to modify.
Tip: Make a copy of this worksheet.

MAPS Rules for: Switch_1 (FID: 1) 10:00:c4:f5:7c:16:8b:3d)

Rule Name	Group Name	Predefined
defALL_100M_16GSWL_QSFPCURRENT_1	ALL_100M_16GSWL_QSFP	√

Consoli Solutions. Copyright (c) 2024

22

MAPS Rules for: Switch 1 FID: 1 (10:00:c4:f5:7c:16:8b:3d)

Rule Name	Group Name	Predefined	Quiet Time	Actions
defALL_32GSWL_SFPCURRENT_1	ALL_32GSWL_SFP	√	3600	raslog, snmp-trap, e-mail, sfp-marginal
defALL_32GSWL_SFPCURRENT_13	ALL_32GSWL_SFP	√	3600	raslog, snmp-trap, e-mail, sfp-marginal
defALL_32GSWL_SFPRXP_2187	ALL_32GSWL_SFP	√	3600	raslog, snmp-trap, e-mail

Add The Modified Rules To The Worksheet

- Copy the custom rules and insert them after the last row of rules on the worksheet you copied.
- Delete the worksheet you used for as a scratch worksheet
- Do not change any other columns
  - Most are read only.
  - Assigning the rule to a policy is not done here.

Modify The Policy

Tip: Run the maps_config.py utility before creating the policy.

Contents

default_switch FID: 128 DID: 1
   policy
   group
   rule
Switch_1 FID: 1 DID: 1
   policy
   group
   rule
Switch_2 FID: 2 DID: 2

Select the worksheet of the policy you want to modify.

MAPS Policies for: Switch 1 FID: 1 (10:00:c4:f5:7c:1...

Policy Name	Predefined	Active	Members
dflt_moderate_policy	√		defALL_100M_16GSWL_QSFPCU defALL_100M_16GSWL_QSFPRX defALL_100M_16GSWL_QSFPVC defALL_10GLWL_SFPCURRENT_...

MAPS Policies for: Switch 1 FID: 1 (10:00:c4:f...

Policy Name	Predefined	Active	Members
ABC_Policy			defALL_100M_16GSWL defALL_100M_16GSWL_ defALL_100M_16GSWL_ defALL_10GLWL_SFPCU

1. Copy members to a scratch file.
2. Delete:
   - defALL_PORTS_IO_PERF_IMPACT
   - defALL_PORTS_OVERSUBSCRIPTION
3. Replace all modified default rules with the custom rules. **Use log output to determine which custom rules where created**. Example:
   - defALL_32GSWL_SFPCURRENT_1
   - ABC_ALL_32GSWL_SFPCURRENT_1
4. After the last row on the policies worksheet:
   - Create a new policy
   - Add the modified membership list from the scratch file.

Update MAPS with maps_config.py

```
py maps_config.py -ip 10.144.72.15 -id admin -pw AdminPassw0rd!
  -i test/maps_test -log _logs
```

```
_add_maps fid: 1, Type: rule
  ABC_ALL_32GSWL_SFPCURRENT_1
  ABC_ALL_32GSWL_SFPCURRENT_13
  ABC_ALL_32GSWL_SFPRXP_2187
  ABC_ALL_32GSWL_SFPRXP_63
  ABC_ALL_32GSWL_SFPSFP_TEMP_85
Success
_add_maps fid: 1, Type: maps-policy
  ABC_Policy
Success
Logging out

Processing Complete. Exit code: 0
```

Update Remaining FIDs

```
py maps_config.py -ip 10.144.72.15 -id admin -pw AdminPassw0rd!
  -i test/maps_test -log _logs -fm 1,2-127
```

-fm 1,2-127 instructs the script to set the MAPS rules, groups, and policies defined for FID 1 in "test/maps_test.xlsx" for any FID in the chassis matching FIDs 2-127

Concluding Remarks

- maps_config.py does not activate any policy. It just edits the rules, groups, and policies.
  - Use SANnav or "`mapspolicy --enable ABC_Policy`" command to enable a policy
- You can also distribute MAPS policies using restore.py. restore.py will activate whatever policy, if any, was active.