
BLOX FEST
Infoblox

Andrew St Jean

Solutions Developer –
Empowered Networks

Topics Covered

- NetMRI Overview
- Compliance Policies and Rules
- Change Scripts and Jobs
- Triggering Jobs using Compliance Rules
- Q&A

NetMRI Overview – Common Pain Points

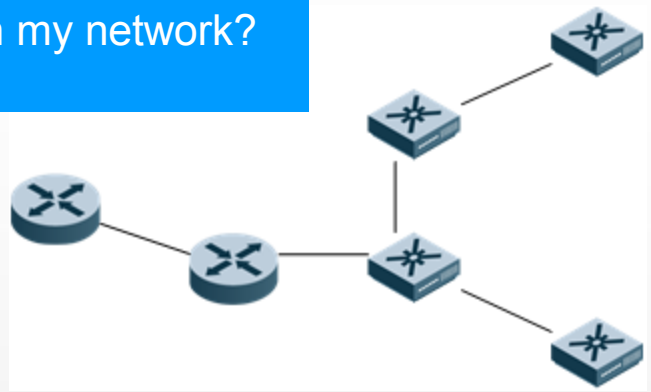
So many changes, so little time.

service timestamps debug uptime ✓
service timestamps log uptime ✓
no service password-encryption ✗

↓

service timestamps debug uptime ✓
service timestamps log uptime ✓
service password-encryption ✓

What's in my network?



Are my devices configured the way they should be?

service timestamps debug uptime ✓
service timestamps log uptime ✓
no service password-encryption ✗

BLOX FEST

NetMRI Overview

Covers devices from more than 55 manufacturers

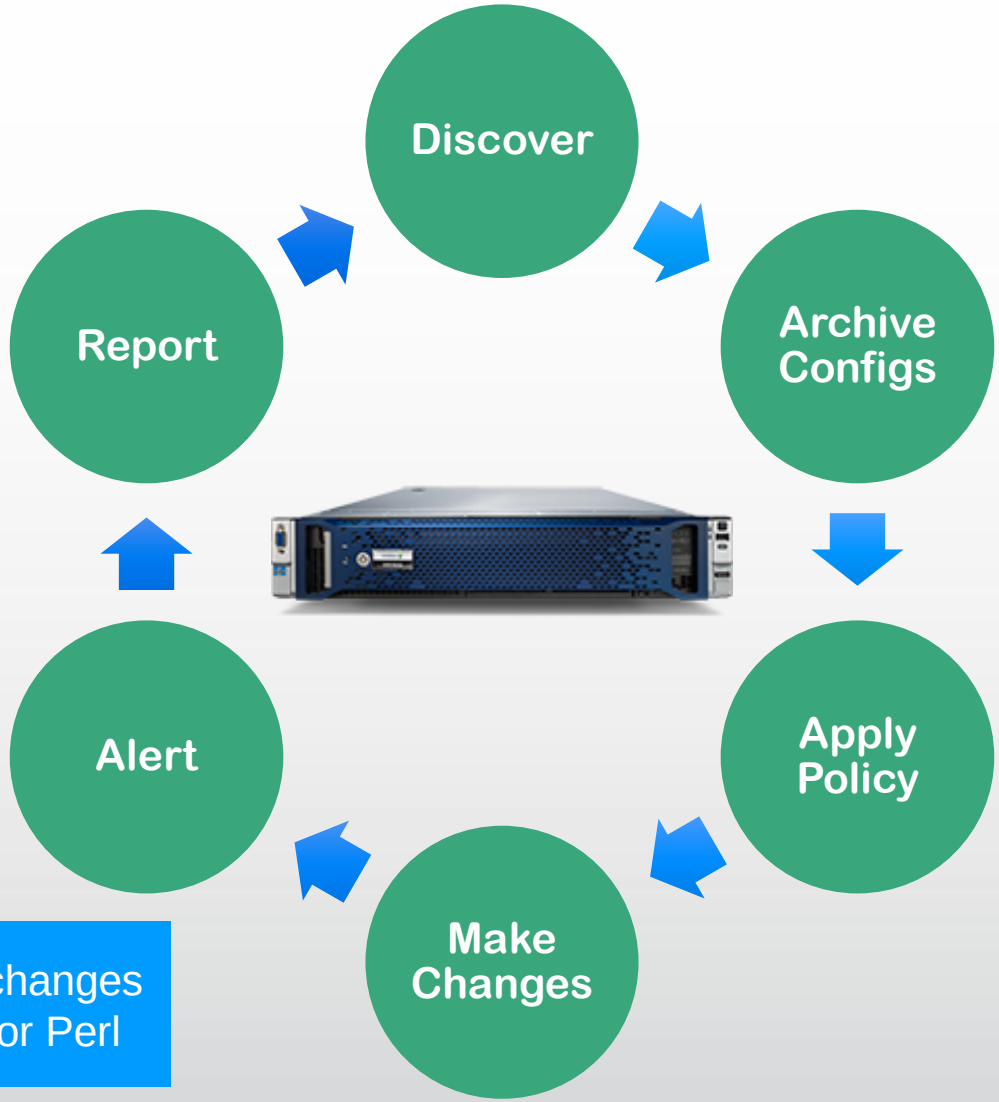
Changes stored effectively indefinitely

PCI, DISA STIG, NSA best practices out of the box

Build a library of changes scripted in CCS or Perl

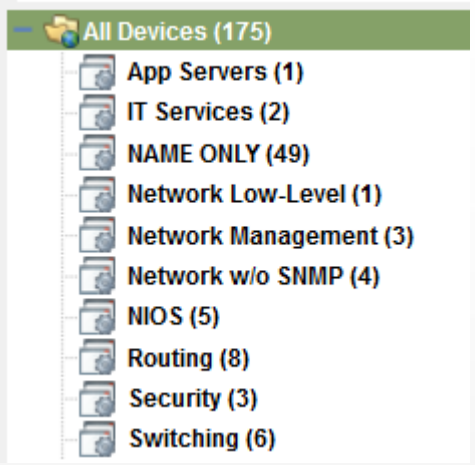
Integration capability with enterprise tools

On demand and scheduled reports (PDF, XLS, DOC, or HTML)



NetMRI Overview – Device Groups

- Used to group and organize managed devices
- Used as targets for compliance policies and change scripts
- Are dynamic

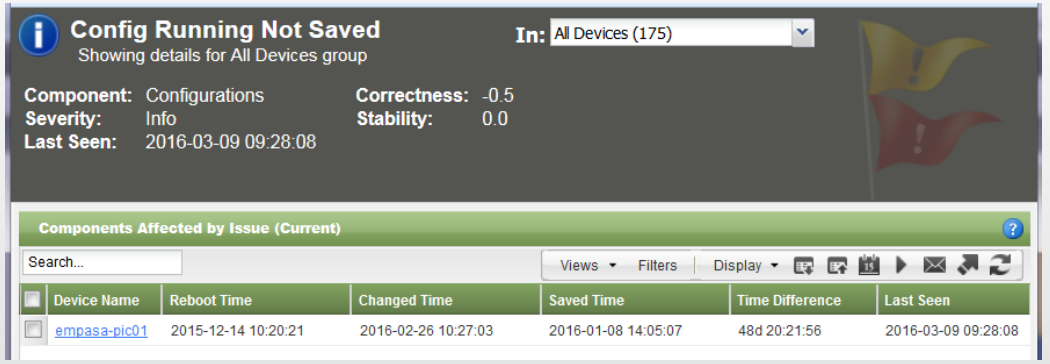



```
$Assurance > 75 and $Type in ["Router","Switch-Router"]
```

NetMRI Overview - Issues

- Tell you when there is a problem with a device
- Compliance policy violations can raise Issues
- Change scripts can raise Issues

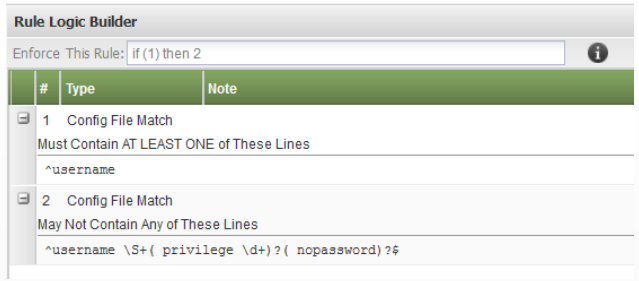
Severity	Last Seen	Title	# Affected	# New	# No Change	# Cleared	# Suppressed
Error	2016-03-08 10:11:36	VLAN Member Priority	1	0	1	0	0
Error	2016-03-08 10:11:26	VLAN Member Minimum Priority	1	0	1	0	0
Error	2016-03-08 10:11:11	Device Issue Limit Exceeded	1	0	1	0	0
Error	2016-03-08 10:10:11	Access Port With PortFast Disabled	14	0	14	0	0
Error	2016-03-08 10:10:11	Trunk Port With PortFast Enabled	1	0	1	0	0
Error	2016-03-08 09:42:28	Policy Violation: ENI ASJ Cust Policy	3	0	3	0	0
Error	2016-03-08 09:42:28	Policy Violation: ENI ASJ Test	3	0	3	0	0
Error	2016-03-08 09:42:27	Policy Violation: ENI JP Cust Policy	3	0	3	0	0
Warning	2016-03-08 10:47:27	Interface Not Stable	3	0	3	0	0
Warning	2016-03-08 10:42:27	Unidirectional Traffic Flow	1	0	1	0	0
Warning	2016-03-08 10:13:45	Device Fan Problem	2	0	2	0	0

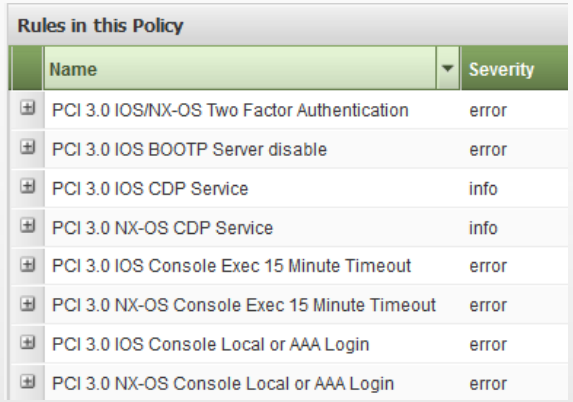


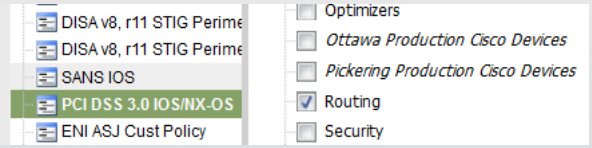
BLOX FEST

Compliance Policies and Rules

- A way to ensure device configurations are what they should be
- Rules check configuration files
- Policies are collections of rules
- Policies are deployed against device groups



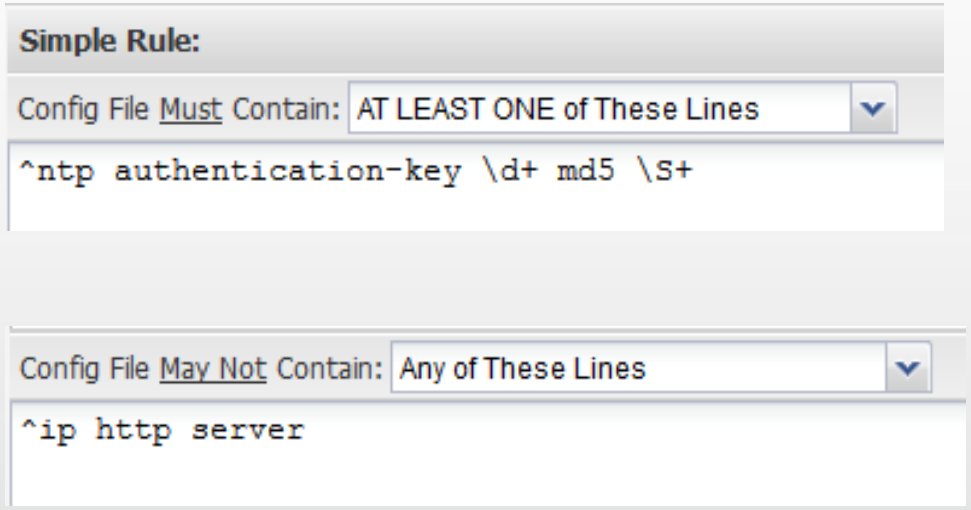




Compliance Policies and Rules

Rule types – Simple rules

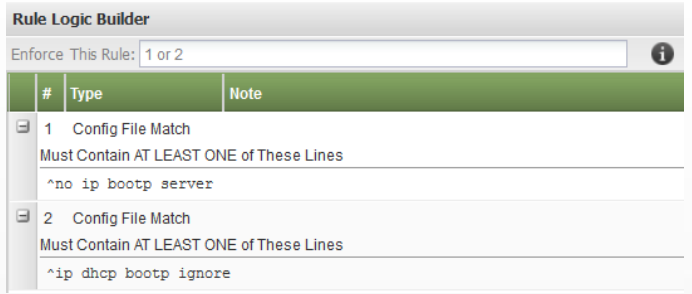
- Most straightforward to write
- Use regular expression matching to ensure certain commands are present in a configuration file
- Can also ensure certain commands are absent

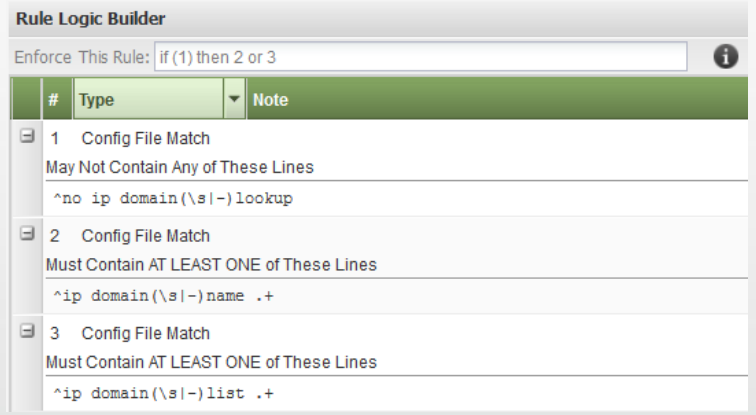


Compliance Policies and Rules

Rule types – Rule logic builder rules

- More complex but more versatile
- Combines multiple simple rules
- Can use conditional logic





Compliance Policies and Rules

Rule Types – Raw XML Rules

- Most complex but can do things other rule types can’t
- Can access List objects
- Can control message output in raised Issues

List Name: Logging Servers **Description:** Syslog servers

Network View	Syslog Server
PIC	192.168.151.33
PIC	192.168.151.34
PIC	192.168.151.254
OTT	192.168.200.90
OTT	192.168.200.92

Message:

```
Extra NTP servers: 10.47.128.10    Missing NTP servers:
```

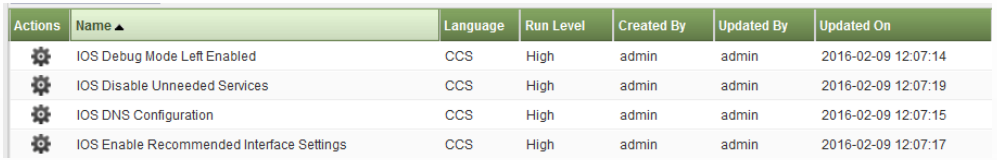
Compliance Policies and Rules

Customer use case

The Customer	Power company subject to NERC Critical Infrastructure Protection
The Requirement	Needed a way to demonstrate compliance with CIP requirements
The Solution	Wrote custom compliance rules using existing out of the box rules as starting point
The Result	Built-in compliance reports used to demonstrate compliance with configuration policies

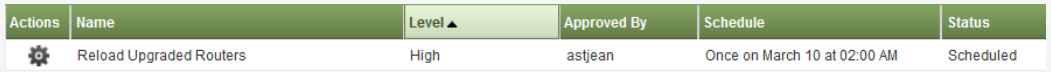
Change Scripts and Jobs

- Change scripts are used to push changes to network devices



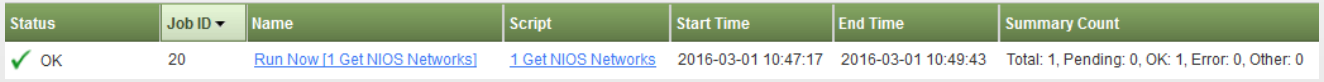
Actions	Name	Language	Run Level	Created By	Updated By	Updated On
	IOS Debug Mode Left Enabled	CCS	High	admin	admin	2016-02-09 12:07:14
	IOS Disable Unneeded Services	CCS	High	admin	admin	2016-02-09 12:07:19
	IOS DNS Configuration	CCS	High	admin	admin	2016-02-09 12:07:15
	IOS Enable Recommended Interface Settings	CCS	High	admin	admin	2016-02-09 12:07:17

- Running or scheduling a change script creates a job



Actions	Name	Level	Approved By	Schedule	Status
	Reload Upgraded Routers	High	astjean	Once on March 10 at 02:00 AM	Scheduled

- Job results are viewable in NetMRI

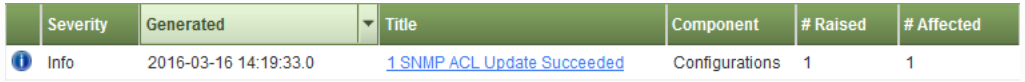


Status	Job ID	Name	Script	Start Time	End Time	Summary Count
✓ OK	20	Run Now [1 Get NIOS Networks]	1 Get NIOS Networks	2016-03-01 10:47:17	2016-03-01 10:49:43	Total: 1, Pending: 0, OK: 1, Error: 0, Other: 0

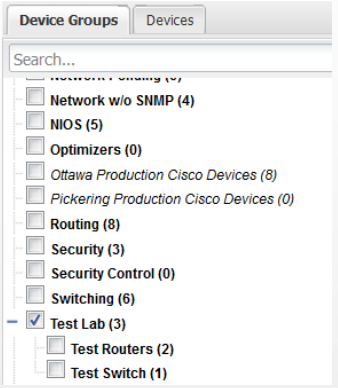
Change Scripts and Jobs

Change Script Capabilities

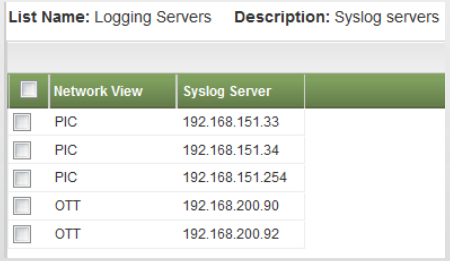
- Can raise Issues



- Can be applied to individual devices and device groups



- Can access List objects



Change Scripts and Jobs

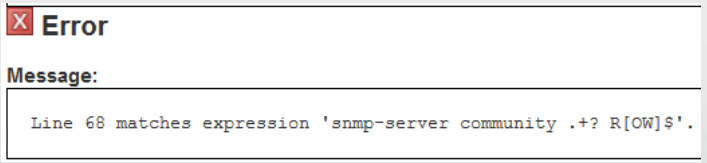
Customer use case

The Customer	Retail company with thousands of stores
The Requirement	After router firmware upgrade, wanted to check each device immediately after reload to ensure it was back on the network
The Solution	Used a change script to reload device and ping until the device responded. Issues raised on success and failure.
The Result	Change script run against sets of devices. Admins notified via email of job results.

Triggering Jobs

- Change scripts usually run immediately or scheduled by a person

- Change scripts can also be run automatically, triggered by policy rules



Triggering Jobs

Why use triggered jobs to push changes?

- Low priority problems that don’t impact device functioning

- Misconfigurations that open security vulnerabilities

Triggering Jobs

Customer use case

The Customer	Oil and gas company subject to PCI audits
The Requirement	Needed to reduce time between the detection of a policy violation and remediation of the violation
The Solution	Use triggered jobs to automatically correct misconfigurations related to PCI standard
The Result	PCI violations are remediated automatically for relevant devices

Questions?