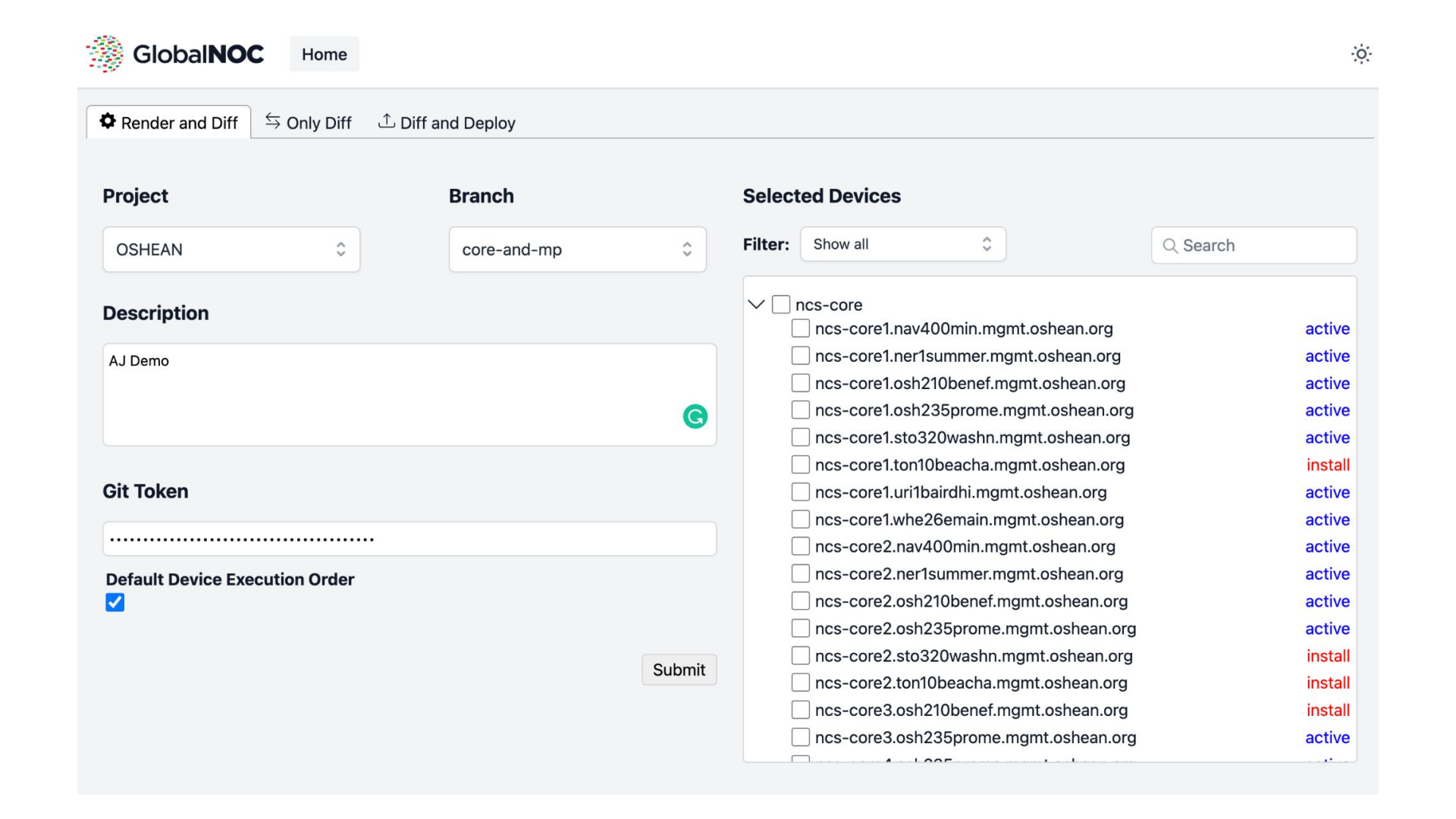
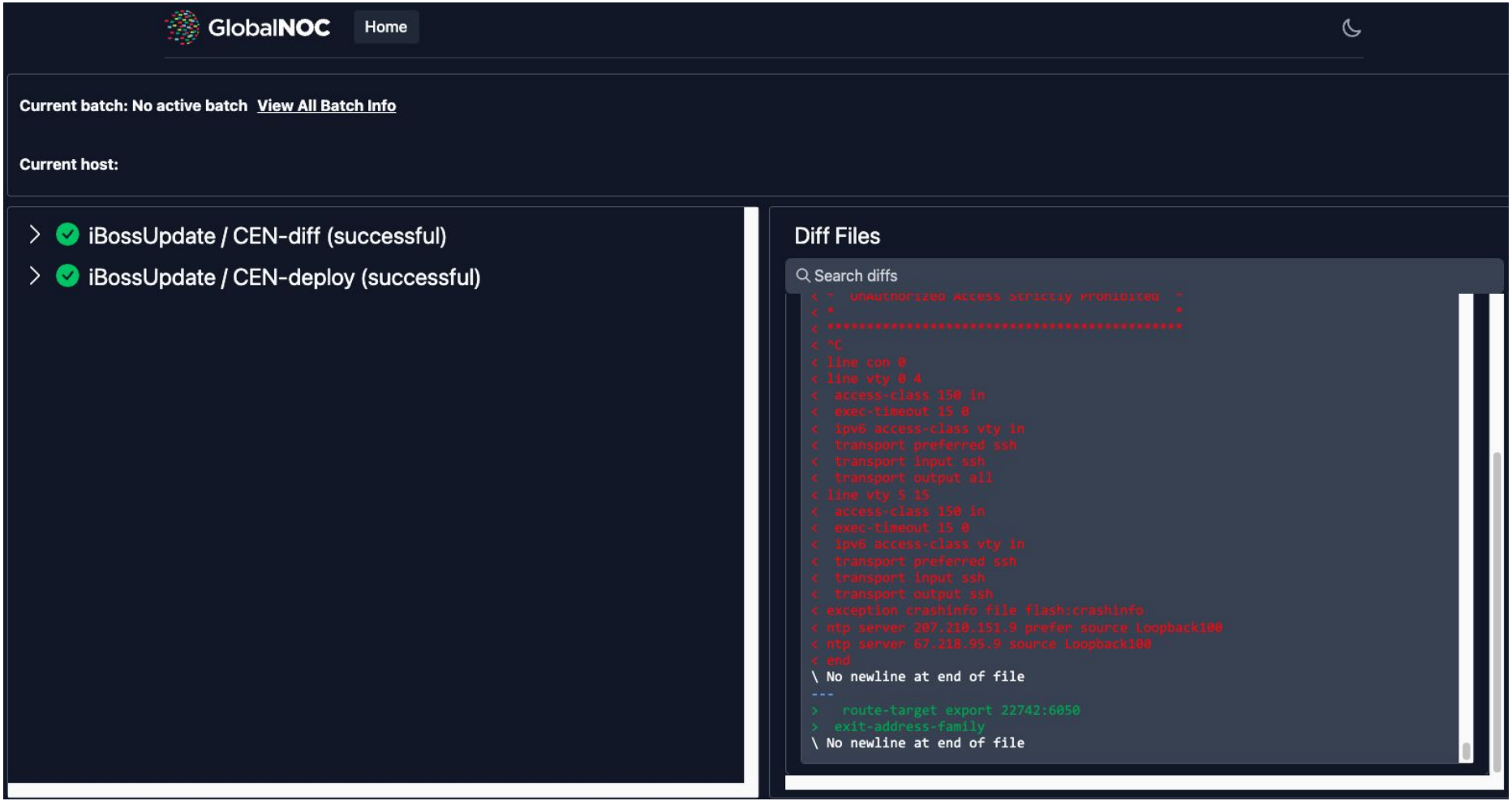
Network Automation - Are we there yet? - GlobalNOC

A.J. Ragusa - Manager Network Automation and Performance Team

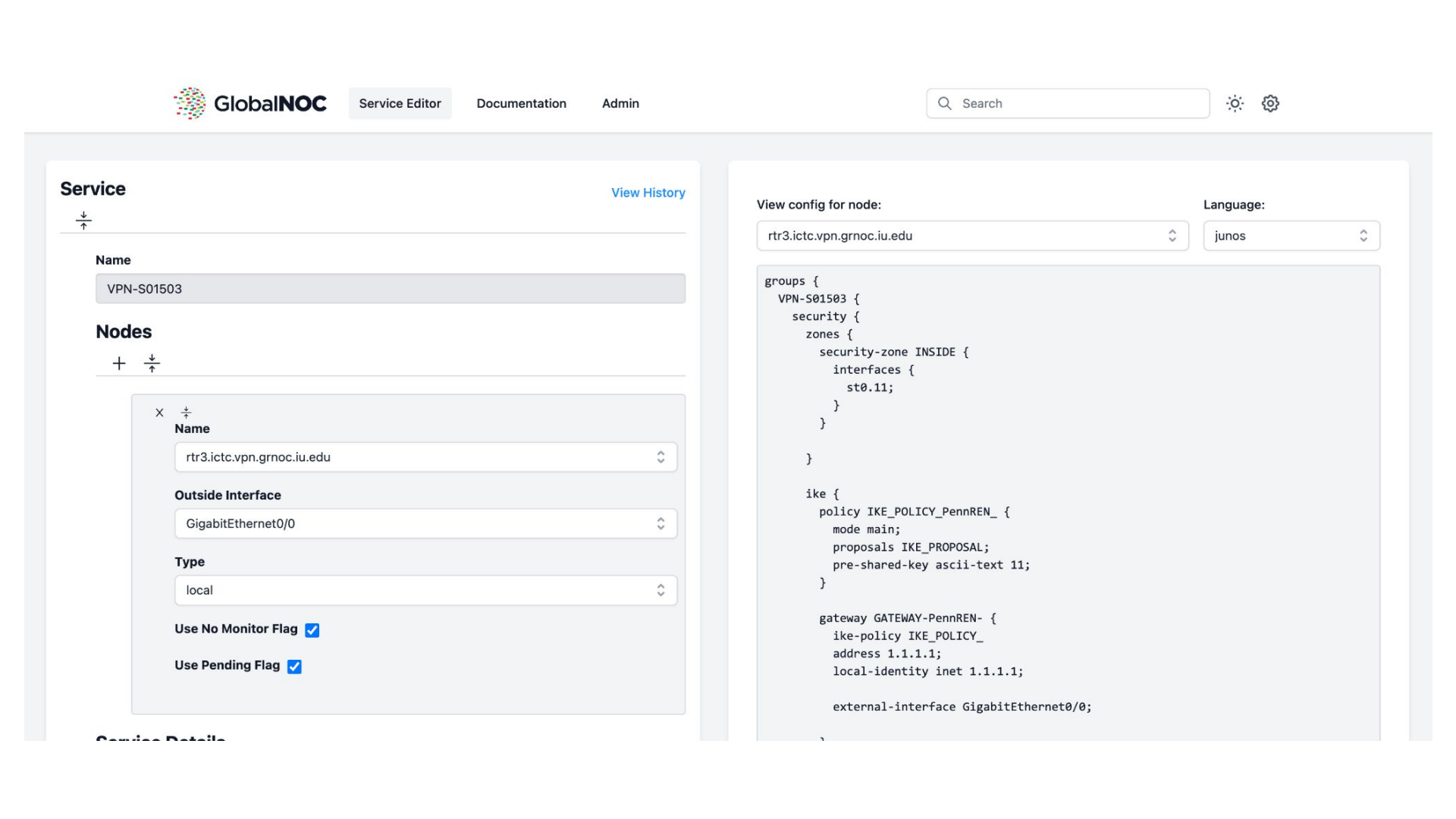
Automation at the GlobalNOC

- GNAT - GlobalNOC Network Automation tool
  - AWX/Ansible, Git/GitHub, GlobalNOC DB, and custom playbooks with a WebUI
  - “Things that are the same across devices” - Think Radius Config, NTP, Syslog, root passwords, ACLs,etc… (this is a surprising size of configuration on many devices)
  - Periodic network configuration validation (verify devices are configured as expected)
- GSCS - GlobalNOC Service Configuration System
  - YANG based configuration tool to generate templates on “services”
  - “Things that are different” - BGP peerings, VLAN configs, VRFs, VPN configurations, etc..
  - GSCS pushes changes into GNAT
- Network Troubleshooter
  - Ultimate goal - automatically fix the network when its possible… currently this is in its first steps


GlobalNOC
Home
Render and Diff
Only Diff
Diff and Deploy
Project
OSHEAN
Branch
core-and-mp
Description
AJ Demo
Git Token
Default Device Execution Order
Submit
Selected Devices
Filter:
Show all
Search
ncs-core
ncs-core1.nav400min.mgmt.oshean.org active
ncs-core1.ner1summer.mgmt.oshean.org active
ncs-core1.osh210benef.mgmt.oshean.org active
ncs-core1.osh235prome.mgmt.oshean.org active
ncs-core1.sto320washn.mgmt.oshean.org active
ncs-core1.ton10beacha.mgmt.oshean.org install
ncs-core1.uri1bairdhi.mgmt.oshean.org active
ncs-core1.whe26emain.mgmt.oshean.org active
ncs-core2.nav400min.mgmt.oshean.org active
ncs-core2.ner1summer.mgmt.oshean.org active
ncs-core2.osh210benef.mgmt.oshean.org active
ncs-core2.osh235prome.mgmt.oshean.org active
ncs-core2.sto320washn.mgmt.oshean.org install
ncs-core2.ton10beacha.mgmt.oshean.org install
ncs-core3.osh210benef.mgmt.oshean.org install
ncs-core3.osh235prome.mgmt.oshean.org active


GlobalNOC
Home
Current batch: No active batch View All Batch Info
Current host:
iBossUpdate / CEN-diff (successful)
iBossUpdate / CEN-deploy (successful)
Diff Files
Search diffs
< " Unauthorized Access Strictly Prohibited "
< *   *
< **
< ^C
< line con 0
< line vty 0 4
< access-class 150 in
< exec-timeout 15 0
< ipv6 access-class vty in
< transport preferred ssh
< transport input ssh
< transport output all
< line vty 5 15
< access-class 150 in
< exec-timeout 15 0
< ipv6 access-class vty in
< transport preferred ssh
< transport input ssh
< transport output ssh
< exception crashinfo file flash:crashinfo
< ntp server 207.210.151.9 prefer source Loopback100
< ntp server 67.218.95.9 source Loopback100
< end
\ No newline at end of file

> route-target export 22742:6050
> exit-address-family
\ No newline at end of file


GlobalNOC
Service Editor
Documentation
Admin
Search
Service
View History
Name
VPN-S01503
Nodes
Name
rtr3.ictc.vpn.grnoc.iu.edu
Outside Interface
GigabitEthernet0/0
Type
local
Use No Monitor Flag
Use Pending Flag
View config for node:
rtr3.ictc.vpn.grnoc.iu.edu
Language:
junos
groups {
VPN-S01503 {
security {
zones {
security-zone INSIDE {
interfaces {
st0.11;
}
}
}
ike {
policy IKE_POLICY_PennREN_ {
mode main;
proposals IKE_PROPOSAL;
pre-shared-key ascii-text 11;
}
gateway GATEWAY-PennREN- {
ike-policy IKE_POLICY_
address 1.1.1.1;
local-identity inet 1.1.1.1;
external-interface GigabitEthernet0/0;

GlobalNOC Troubleshooter Home

INC0121887

Alarm1 Alarm2

Critical since Tue Nov 01 11:11:00 EDT 2022

core1.atla.net.internet2.edu

BGP to [RE] MISSION ~ AS396926 &#124 I2-S12530 is down (State: Last down time is within threshold of 30 minutes.).[CLEARED]

Log messages

Show the log matched on keywords 'BGP' and 2607:f4a0:5010:8::1
Command: show logging | include 2607:f4a0:5010:8::1 | include BGP

RP/0/RP0/CPU0:Nov 29 15:57:50.363 UTC: locald_DLRSC[136]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "show logging | include 2607:f4a0:5010:8::1 | include BGP" by ansible from TTY /dev/pts/4 140.182.45.18
RP/0/RP0/CPU0:Nov 29 16:37:30.607 UTC: locald_DLRSC[136]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "show logging | include 2607:f4a0:5010:8::1 | include BGP" by ansible from TTY /dev/pts/4 140.182.45.18
RP/0/RP0/CPU0:Nov 29 16:42:11.903 UTC: locald_DLRSC[136]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "show logging | include 2607:f4a0:5010:8::1 | include BGP" by ansible from TTY /dev/pts/5 140.182.45.18

Commit History

Show commit history to determine if any recent changes affected the BGP status
Command: show configuration history last 15

Sno. Event Info Time Stamp
~~~~ ~~~~~ ~~~~ ~~~~~~~~~~
1 backup Periodic ASCII backup Mon Nov 28 23:54:07 2022
2 commit id 1000001063 Mon Nov 28 23:43:08 2022
3 commit id 1000001062 Mon Nov 28 23:39:00 2022
4 backup Periodic ASCII backup Mon Nov 28 21:09:05 2022
5 commit id 1000001061 Mon Nov 28 21:07:56 2022
6 commit id 1000001060 Mon Nov 28 21:01:09 2022
~~~~

Automation at the GlobalNOC cont.

- GlobalNOC Network Maintenance Sanity Checker
  - Runs a set of commands and stores the results before and after the maintenance and compares the results to verify the status of the network before and after maintenances (can be integrated into GNAT)
- Lots of “one off” automation pieces
  - DDoS remediation for Indiana GigaPOP
  - Version validation
  - Juniper device upgrades - NWave process
  - Cisco IOS-XR upgrades - OSHEAN process
  - Interface Description updates
  - IPv6 Deployments

Sounds great does it work?

- Ya, mostly…
  - Currently support over 400 devices at 80% configured via Automation
  - Another 200 devices at about 20%
  - More devices and networks every day
- Constantly trying to add features and work with network engineers to improve workflows
- Starting is the hard part!

How did we get there?

- Dedicated team of developers
  - Lots of interacting with network engineers at different organizations to get requirements, feedback, and improvements
- Already had experience with NetConf, working with device configurations
- Already had a Centralized Database (GlobalNOC DB) of network devices, and other information to start with
- Testlab is critical!

Lessons Learned from Automation Deployments

- Starting is the hardest part
  - Lots of excuses on why not (time, experience, not ready, etc)
  - Pick something small and easy that is a time saver (changing root password)
  - Don’t need NSO/Ansible/Puppet/Chef, can just start with a perl Script
- Try different things
  - What works for one task might not work for another
- Re-evaluate and move forward
  - What has been successful? What hasn’t and why?
  - Pick one more thing to work towards
    - ACL updates, Prefix-List updates, Firmware upgrade
- Just START! You need to gain some experience to figure out what tools you want to use, and get ideas on how to go forward.