The bridge to possible

A Custom Compliance

Implementing with Cisco NSO

Fatih Ayvaz, Software Architect
Cisco CX

Cisco Live!

DEVNET-2572

Cisco Webex App

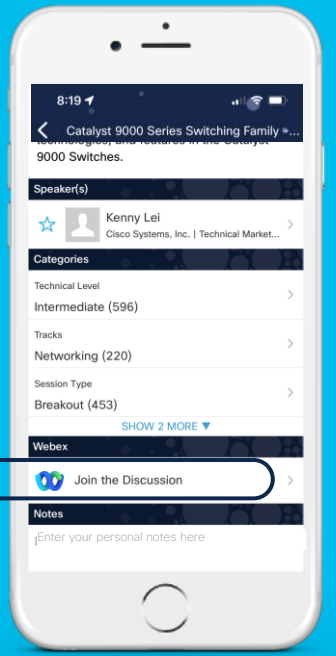
Questions?

Use Cisco Webex App to chat
with the speaker after the session

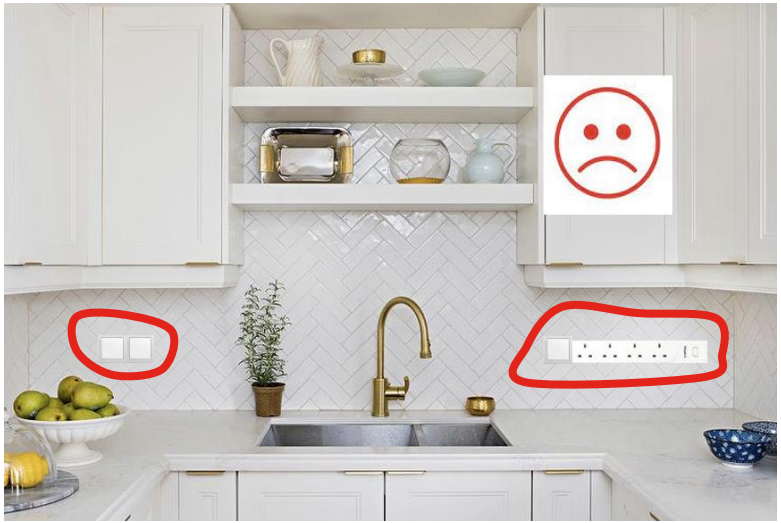
How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated until February 24, 2023.



What we got!



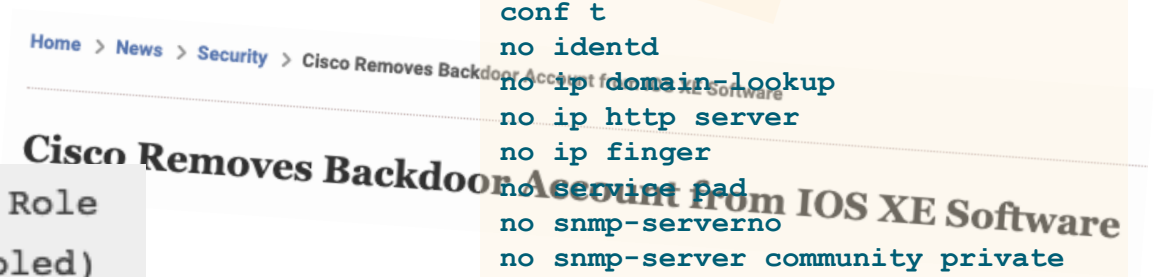
```
username admin privilege 15 password 7 0…9
username cisco …
```

```
router bgp
 no sync

router isis 1
 net 49.0000.0000.0001.00
 is-type level-1
```

Risks of Default Passwords on the Internet

https://www.cisa.gov/uscert/ncas/alerts/TA13-175A




```
switch#show vstack config | inc Role
 Role: Client (SmartInstall enabled)
```


```
conf t
no identd
no ip domain-lookup
no ip http server
no ip finger
no service pad
no snmp-serverno
no snmp-server community private
no snmp-server community public
no service tcp-small-servers
no service udp-small-servers
no ip gratuitous-arps
…
interface GigabitEthernet 0/1
 ip redirects
 ip directed-broadcast
```

*Nipper for performing config reviews for security to identify such *known* security problems

Agenda

- Our compliance requirement
- Compliance tool in NSO
- Running NSO compliance report
- Implementation using NSO py
- Q&A

Session Objectives

- Main goals
- Introduce compliance tool on NSO
- Feature a business requirement to explore development on NSO
- Design custom compliance
- Demonstrate the implemented python logic with a sample NSO action package

- This session does not include
- Python training
- NSO training
- YANG training
- Coding skills and best practices

Compliance Requirement

- all the ios devices must have below logging settings:

```
config
  logging buffered 12345
  logging 1.1.1.1
  logging 2.2.2.2
 !
```

devIOS-1

```
config
 logging buffered 12345
 logging 1.1.1.1
 logging 2.2.2.2
!
```

```
config
 logging buffered 12345
 logging 1.1.1.1
 logging 2.2.2.2
 logging 3.3.3.3
!
```

devIOS-2

Compliance Tool in NSO

- Verify the network has the *correct* configuration!
  - Useful when network connectivity is broken
  - For audit reporting, health checks, preparations for critical operations
  - For comparison of current network vs. what supposed to be configured
- NSO Compliance Tool and Reporting
  - Refer to: “Compliance Reporting” in nso_user_guide-5.7.6.pdf
- NSO compliance can:
  - check the live devices against NSO stored device configuration
  - compare live devices against templates

How to run compliance on NSO

- Create device template
- Create device groups
- Run/schedule the compliance tool
- View the compliance report

Key highlights of the compliance

- Template based
- Variables
- xpath
- Scales with device-groups
- Comparison
- Reporting
  - html, text, xml
  - historical results

Template creation

```
set devices template template_ios_logging ned-id cisco-ios-cli-6.46 config logging buffered buffer-size
"{$buffer_size}"
set devices template template_ios_logging ned-id cisco-ios-cli-6.46 config logging hostname "{$host1_ip}"
set devices template template_ios_logging ned-id cisco-ios-cli-6.46 config logging hostname "{$host2_ip}"
commit
```

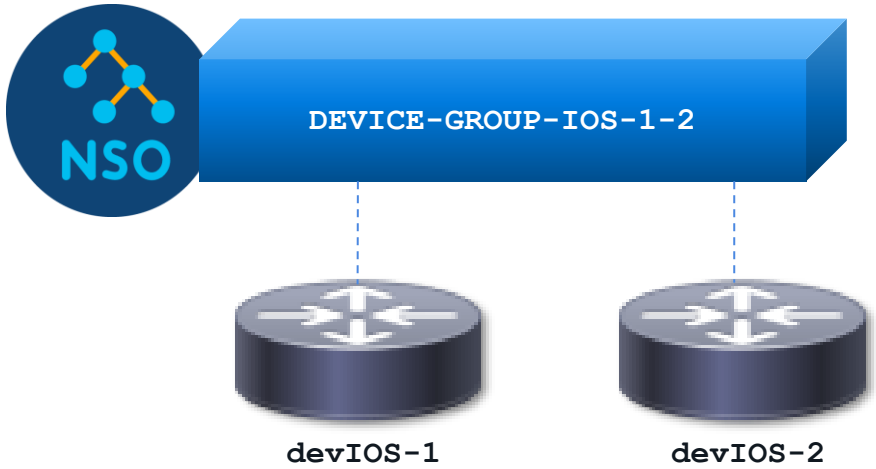
device template

```
nsoadmin@ncs% show devices template
template_ios_logging
ned-id cisco-ios-cli-6.46 {
    config {
        logging {
            buffered {
                buffer-size "{$buffer_size}";
            }
            hostname "{$host1_ip}";
            hostname "{$host2_ip}";
        }
    }
}
```

Device-group

```
nsoadmin@ncs% set devices device-group DEVICE-GROUP-IOS-1-2 device-name [ devIOS-1 devIOS-2 ]
[ok][2023-02-01 23:18:12]

[edit]
nsoadmin@ncs% show devices device-group DEVICE-GROUP-IOS-1-2
device-name [ devIOS-1 devIOS-2 ];
```



Compliance report creation

```
set compliance reports report report_ios_logging compare-template template_ios_logging DEVICE-GROUP-IOS-1-2 variable buffer_size value 12345
set compliance reports report report_ios_logging compare-template template_ios_logging DEVICE-GROUP-IOS-1-2 variable host1_ip value '1.1.1.1'
set compliance reports report report_ios_logging compare-template template_ios_logging DEVICE-GROUP-IOS-1-2 variable host2_ip value '2.2.2.2'
```

commit dry-run

compliance report

```
reports {
+        report report_ios_logging {
+            compare-template template_ios_logging DEVICE-GROUP-IOS-1-2 {
+                variable buffer_size {
+                    value 12345;
+                }
+                variable host1_ip {
+                    value '1.1.1.1';
+                }
+                variable host2_ip {
+                    value '2.2.2.2';
+                }
+            }
+        }
    }
```

Compliance report run

```
nsoadmin@ncs% request compliance reports report
report_ios_logging run outformat html
..
location http://localhost:8080/compliance-
reports/report_36_nsoadmin_1_2023-2-6T11:53:25:0.html
```

```
devices device devIOS-1
 config
  logging buffered 12345
  logging 1.1.1.1
  logging 2.2.2.2
 !
!
```

```
devices device devIOS-2
 config
  logging 1.1.1.1
 !
!
```

devIOS-1

devIOS-2

cisco Live!

localhost:8080/compliance-reports/report_36_nsoadmin_1_2023-2-6T11:53:25:0.html

Imported | Cisco Admin | CISCO CX | Common Cisco To... | PATENT | CISCO PRODUCTS

Publication date : 2023-2-6 11:53:25

Produced by user : nsoadmin

Summary

Compliance result titled "" defined by report "report_ios_logging"

Resulting in **violations**

Checking 2 devices and no services

Produced 2023-2-6 11:53:25

From : Oldest available information

To : 2023-2-6 11:53:25

Template discrepancies

template_ios_logging

Discrepancies in device

devIOS-2

Details

Template discrepancies details

template_ios_logging

Device devIOS-2

```
 config {
     logging {
         buffered {
+            buffer-size 12345;
         }
+        hostname 2.2.2.2 {
+        }
     }
 }
```

compliant!

```
nsoadmin@ncs% request compliance reports report
report_ios_logging run outformat html
..
location http://localhost:8080/compliance-
reports/report_40_nsoadmin_0_2023-2-6T19:25:45:0.html
```

```
devices device devIOS-1
 config
  logging buffered 12345
  logging 1.1.1.1
  logging 2.2.2.2
 !
!
```

```
devices device devIOS-2
 config
  logging buffered 12345
  logging 1.1.1.1
  logging 2.2.2.2
  logging 3.3.3.3
 !
!
```

devIOS-1

devIOS-2

localhost:8080/compliance-reports/report_40_nsoadmin_0_2023-2-6T19:25:45:0.html

Imported | Cisco Admin | CISCO CX | Common Cisco To... | PATENT | CISCO PRODUCTS

Publication date : 2023-2-6 19:25:45

Produced by user : nsoadmin

Summary

Compliance result titled "" defined by report "report_ios_logging"

Resulting in **no-violation**

Checking 2 devices and no services

Produced 2023-2-6 19:25:45

From : Oldest available information

To : 2023-2-6 19:25:45

Template discrepancies

template_ios_logging

No discrepancies found

Details

Template discrepancies details

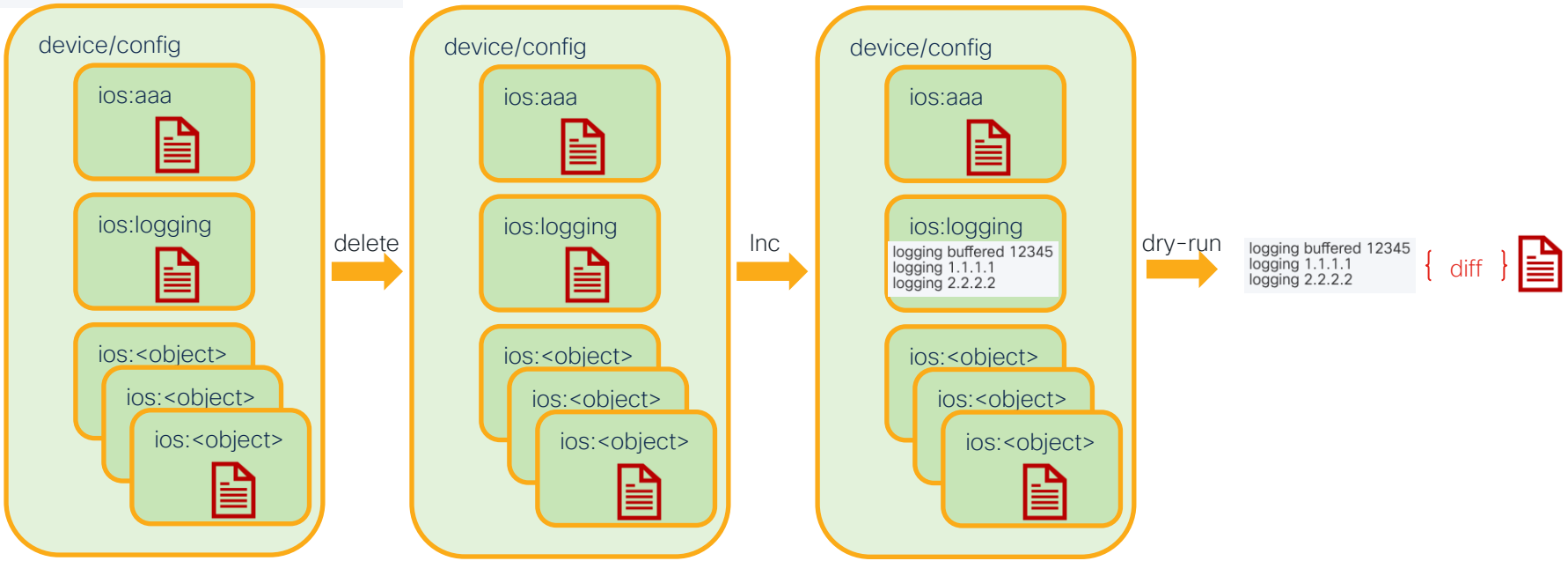
template_ios_logging

No device diffs found

Strict Compliance Action Design

Expected config (golden template):

```
logging buffered {{buffer_size}}
logging {{host1_ip}}
logging {{host2_ip}}
```



NSO action package

- Model (YANG)

```
module compliance-action {

namespace "http://cisco.com/compliance-action";
prefix compliance-action;

import tailf-ncs {
prefix ncs;
}

description
"Custom compliance tool";

revision 2023-02-09 {
description
"Initial revision.";
}

container compliance-action {
tailf:action run-compliance {
```

- Logic (python)

```
import ncs
from ncs.application import Service
from ncs.dp import Action
…
class run_complianceAction(Action):
   @Action.action
   def cb_action(self, uinfo, name, kp, input, output, trans):
   …
   with ncs.maapi.single_write_trans('admin', 'system',
groups=['ncsadmin']) as trans:
      root = ncs.maagic.get_root(trans)
      for dev in devicelist:
         #paths = get_ios_paths() + get_xr_paths()
         paths = configtarget
         delete_configs(paths, trans, dev)
         load_native_config(root, device=dev,
config=compliance_config)
      raw_output = get_dry_run_raw_output(trans,
outformat="cli")
      print(parse_dry_run_output(raw_output, outformat="cli"))
      output.compliance_action_info +=
      parse_dry_run_output(raw_output, outformat="cli") + "\n"
```

Custom compliance run and result

```
nsoadmin@ncs% request compliance-action run-compliance ned-id cisco-ios-cli-6.46 device-selection { device-group-
list [ DEVICE-GROUP-IOS-1-2 ] } config-targets [ logging ] variable-values { variable-value-list { variable-name
buffer_size variable-value 12345 } variable-value-list { variable-name host1_ip variable-value 1.1.1.1 } variable-
value-list { variable-name host2_ip variable-value 2.2.2.2 } } config-lines
Value for 'config-lines' (<string>):
[Multiline mode, exit with ctrl-D.]
> logging buffered {{buffer_size}}
> logging {{host1_ip}}
> logging {{host2_ip}}
>
```

```
devices device devIOS-1
 config
  logging buffered 12345
  logging 1.1.1.1
  logging 2.2.2.2
 !
!
```

```
devices device devIOS-2
 config
  logging buffered 12345
  logging 1.1.1.1
  logging 2.2.2.2
  logging 3.3.3.3
 !
!
```

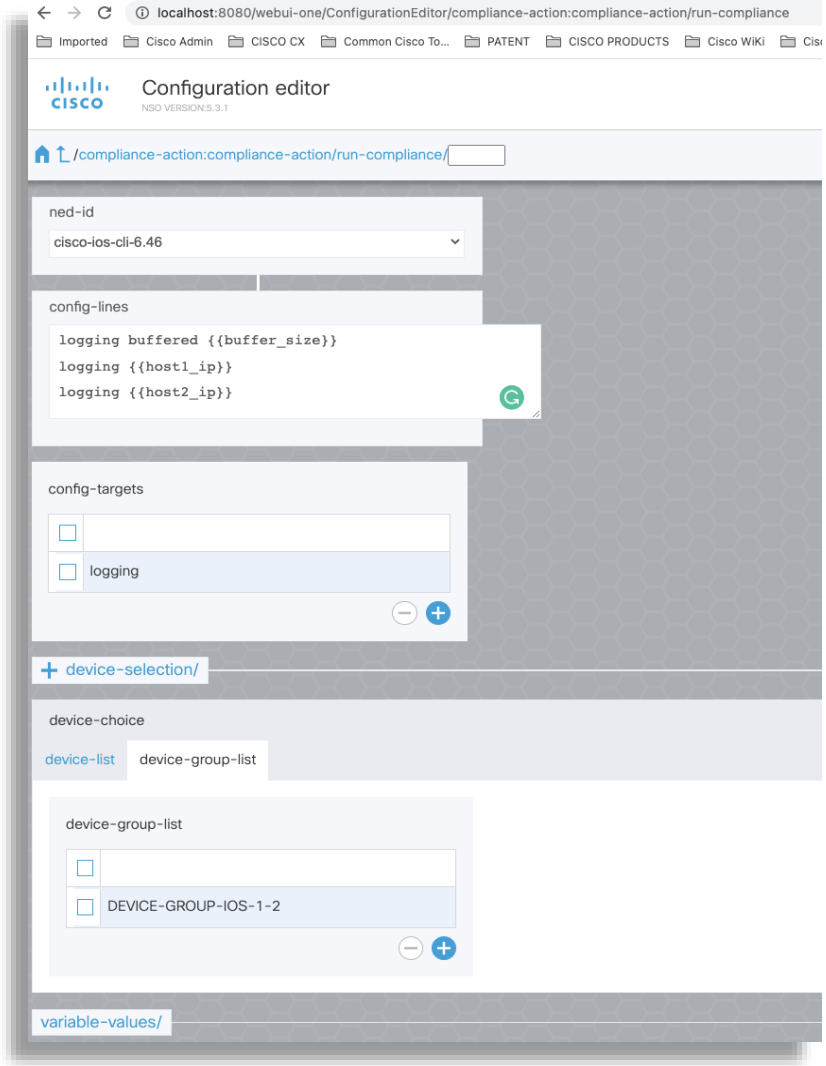
devIOS-1

devIOS-2

```
…
COMPLIANCE REPORT:

 devices {
     device devIOS-2 {
         config {
             logging {
-                hostname 3.3.3.3 {
-                }
             }
         }
     }
 }
…
```

NSO GUI


localhost:8080/webui-one/ConfigurationEditor/compliance-action:compliance-action/run-compliance
Imported
Cisco Admin
CISCO CX
Common Cisco To...
PATENT
CISCO PRODUCTS
Cisco WiKi
Configuration editor
NSO VERSION:5.3.1
/compliance-action:compliance-action/run-compliance/
ned-id
cisco-ios-cli-6.46
config-lines
logging buffered {{buffer_size}}
logging {{host1_ip}}
logging {{host2_ip}}
config-targets
logging
device-selection/
device-choice
device-list
device-group-list
device-group-list
DEVICE-GROUP-IOS-1-2
variable-values/

Demo

- NSO compliance
- NSO python action

```
nsoadmin@ncs%

[edit]
nsoadmin@ncs%

[edit]
nsoadmin@ncs% # TEAR-DOWN:
[ok][2023-02-07 13:20:56]

[edit]
nsoadmin@ncs% # delete compliance report:
[ok][2023-02-07 13:20:56]

[edit]
nsoadmin@ncs% delete compliance reports report report_ios_logging
[ok][2023-02-07 13:20:56]

[edit]
nsoadmin@ncs%

[edit]
nsoadmin@ncs% # delete device group:
[ok][2023-02-07 13:20:56]

[edit]
nsoadmin@ncs% delete devices device-group DEVICE-GROUP-IOS-1-2
[ok][2023-02-07 13:20:56]

[edit]
nsoadmin@ncs%

[edit]
nsoadmin@ncs% # delete devices logging
[ok][2023-02-07 13:20:56]

[edit]
nsoadmin@ncs% delete devices device devIOS-1 config logging
[ok][2023-02-07 13:20:56]

[edit]
nsoadmin@ncs% delete devices device devIOS-2 config logging
[ok][2023-02-07 13:20:56]

[edit]
nsoadmin@ncs% commit
Commit complete.
[ok][2023-02-07 13:20:59]

[edit]
nsoadmin@ncs%
```

localhost:8080/compliance-reports/report_46_nsoadmin_0_2023-2-7T13:10:39:0.html

Publication date : 2023-2-7 13:10:39

Produced by user : nsoadmin

Summary

Compliance result titled "" defined by report "report_ios_logging"

Resulting in **no-violation**

Checking 2 devices and no services

Produced 2023-2-7 13:10:39

From : Oldest available information

To : 2023-2-7 13:10:39

Template discrepancies

template_ios_logging

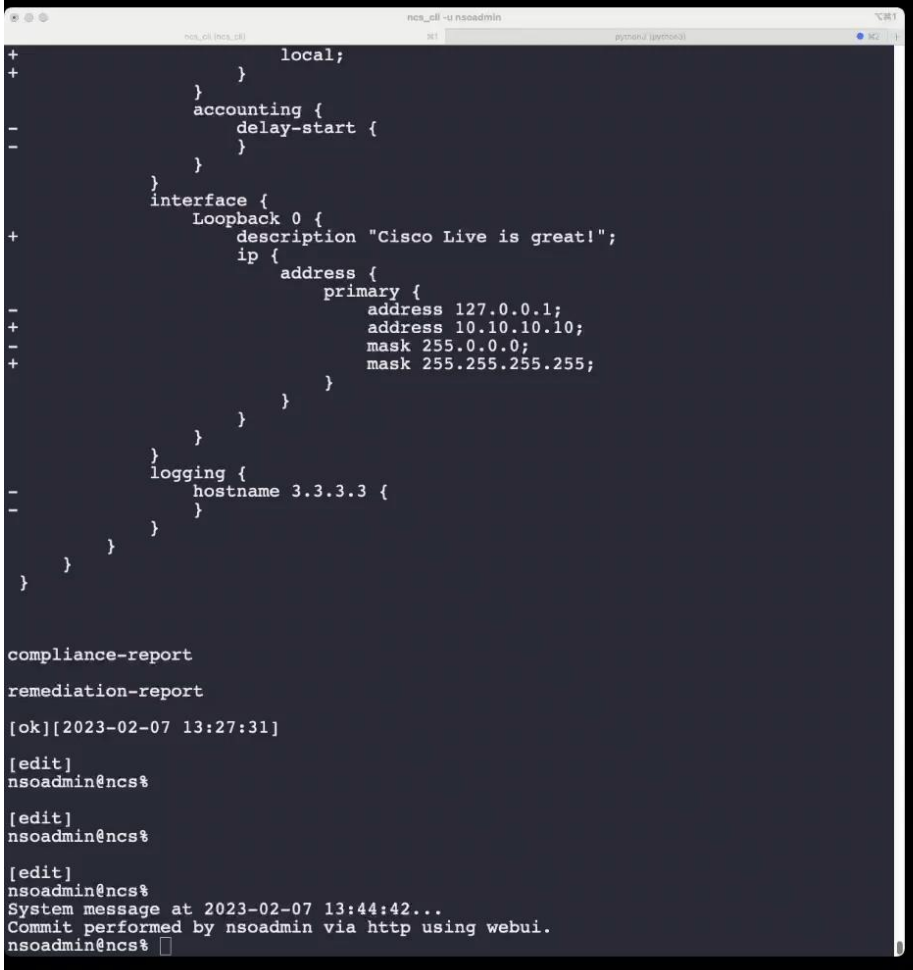
No discrepancies found

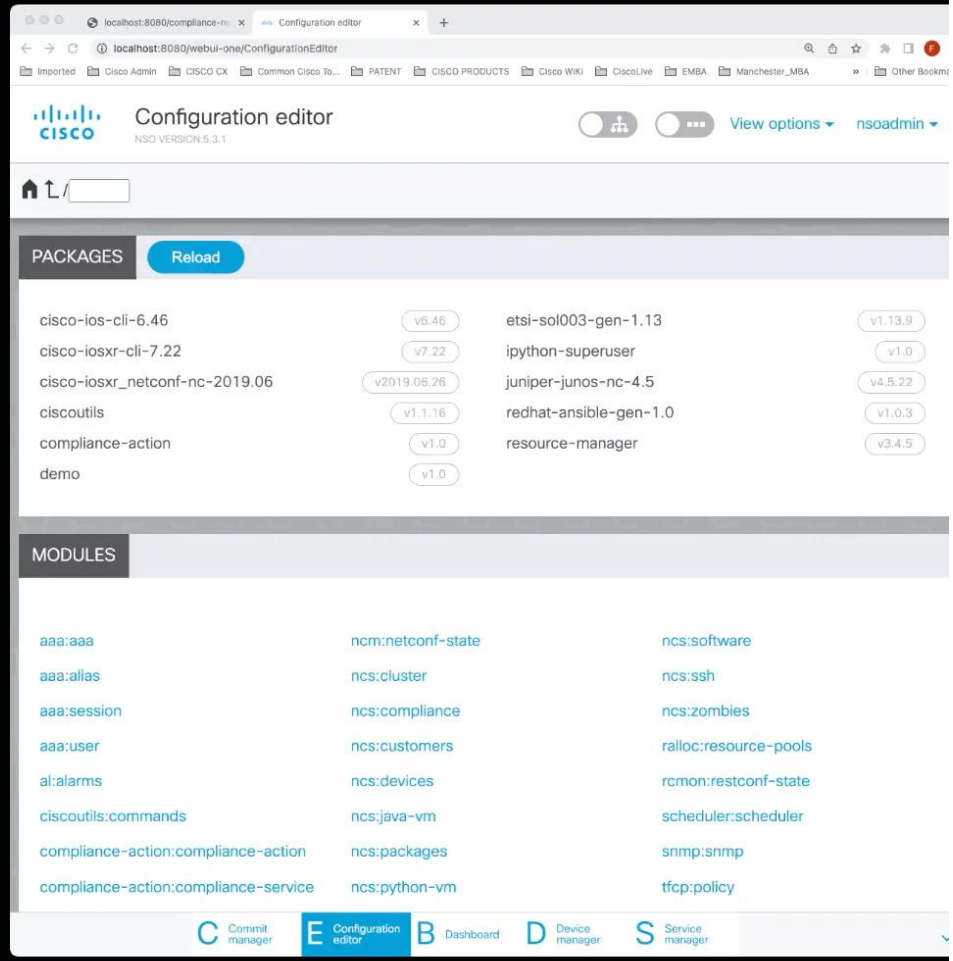
Details

Template discrepancies details

template_ios_logging

No device diffs found


ncs_cli -u nsoadmin
+   local;
+   }
            }
            accounting {
-               delay-start {
-               }
            }
        }
        interface {
            Loopback 0 {
+   description "Cisco Live is great!";
                ip {
                    address {
                        primary {
-                           address 127.0.0.1;
+   address 10.10.10.10;
-                           mask 255.0.0.0;
+   mask 255.255.255.255;
                        }
                    }
                }
            }
        }
        logging {
-           hostname 3.3.3.3 {
-           }
        }
    }
}
compliance-report
remediation-report
[ok][2023-02-07 13:27:31]
[edit]
nsoadmin@ncs%
[edit]
nsoadmin@ncs%
[edit]
nsoadmin@ncs%
System message at 2023-02-07 13:44:42...
Commit performed by nsoadmin via http using webui.
nsoadmin@ncs%


localhost:8080/webui-one/ConfigurationEditor
Configuration editor
NSO VERSION:5.3.1
View options
nsoadmin
PACKAGES
Reload
cisco-ios-cli-6.46 v6.46
cisco-iosxr-cli-7.22 v7.22
cisco-iosxr_netconf-nc-2019.06 v2019.06.26
ciscoutils v1.1.16
compliance-action v1.0
demo v1.0
etsi-sol003-gen-1.13 v1.13.9
ipython-superuser v1.0
juniper-junos-nc-4.5 v4.5.22
redhat-ansible-gen-1.0 v1.0.3
resource-manager v3.4.5
MODULES
aaa:aaa
aaa:alias
aaa:session
aaa:user
al:alarms
ciscoutils:commands
compliance-action:compliance-action
compliance-action:compliance-service
ncm:netconf-state
ncs:cluster
ncs:compliance
ncs:customers
ncs:devices
ncs:java-vm
ncs:packages
ncs:python-vm
ncs:software
ncs:ssh
ncs:zombies
ralloc:resource-pools
rcmon:restconf-state
scheduler:scheduler
snmp:snmp
tfcp:policy
C Commit manager
E Configuration editor
B Dashboard
D Device manager
S Service manager

Action components

- compliance.yang
  - leaf ned-id {
  - container device-selection {
    - choice device-choice {
      - leaf-list device-list {
      - leaf-list device-group-list {
  - leaf-list config-targets {
  - leaf config-lines {
  - container variable-values {
  - output {
    - leaf compliance-action-info {
    - leaf compliance-report {
    - leaf remediation-report {

- compliance.py
  - def replace_vars(text, parameters):
  - def get_dry_run_raw_output(trans: ncs.maapi.Transaction, outformat: str):
  - def parse_dry_run_output(dry_run_output_raw: dict, outformat: str) -> str:
  - def load_native_config(root, device: str, config: str):
  - def delete_configs(paths, trans, dev):

Key features in strict compliance

- Simplifies usage with one action command
  - no need to create template, compliance report, or device group
- Allows individual devices as well as device groups
- Supports native config
- Detects extra lines
- Allows user to specify config targets
- Supports config path
- Extendible to support multiple NEDs in one report
- Supports parameterization
- Flexible for customized reporting requirements
- Can generate remediation config

Relevant sessions

- CISCOU-2664 Compliance with Ansible
- DEVWKS-3984 Infrastructure-as-a-code & CICD
- DEVNET-2535 Testing & Deployment of NSO
- WoS Cisco CX Booth
- 2022 Automation Developer Days:

https://www.youtube.com/watch?v=0bWm1q6V0qM

Q&A

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN

Backup slides

Try this on a local-install:

```
(base) ➜  NSO pwd
<your path to NSO installation>
(base) ➜  NSO source ncsrc
(base) ➜  NSO cd ncs-run
(base) ➜  ncs-run ncs
echo $PYTHONPATH
<some path>/src/ncs/pyapi
python3
import ncs
import _ncs
from ncs.application import Service
from ncs.dp import Action
m = ncs.maapi.Maapi()
s = ncs.maapi.Session(m, 'nsoadmin', 'system')
t = m.start_write_trans(ncs.RUNNING)
root = ncs.maagic.get_root(t)
help(root.devices.device['devIOS-1'].config.interface.FastEthernet['0/0'])
root.devices.device['devIOS-1'].config.interface.FastEthernet['0/0'].__dir__()
a = root.devices.device['devIOS-1'].config.interface.FastEthernet['0/0']
setattr(a, 'description', 'cisco live is great')
root.devices.device['devIOS-1'].config.interface.FastEthernet['0/0'].description.upper()
```

use NSO installation path
change NSO username
change device name
change interface name