Secunetics

where science meets art

NSO in the Enterprise

Weaving the Old into the New

June, 2020

Allen Chen, Samuel Coome

Secunetics

- Engineering consultancy based in Washington, DC area
- Network engineering services for large networks:
  - Architecture, design, and deployment
  - Automation and orchestration
  - Performance engineering and management
  - Security engineering, analysis, and response
- Serving government and commercial organizations

Our Brownfield Enterprise

- 10+ departments with independently managed networks
- Around 1200 network infrastructure devices across many vendors (Cisco, Juniper, F5, etc.)
- Wide range of device models and OS versions

The Enterprise Use Case

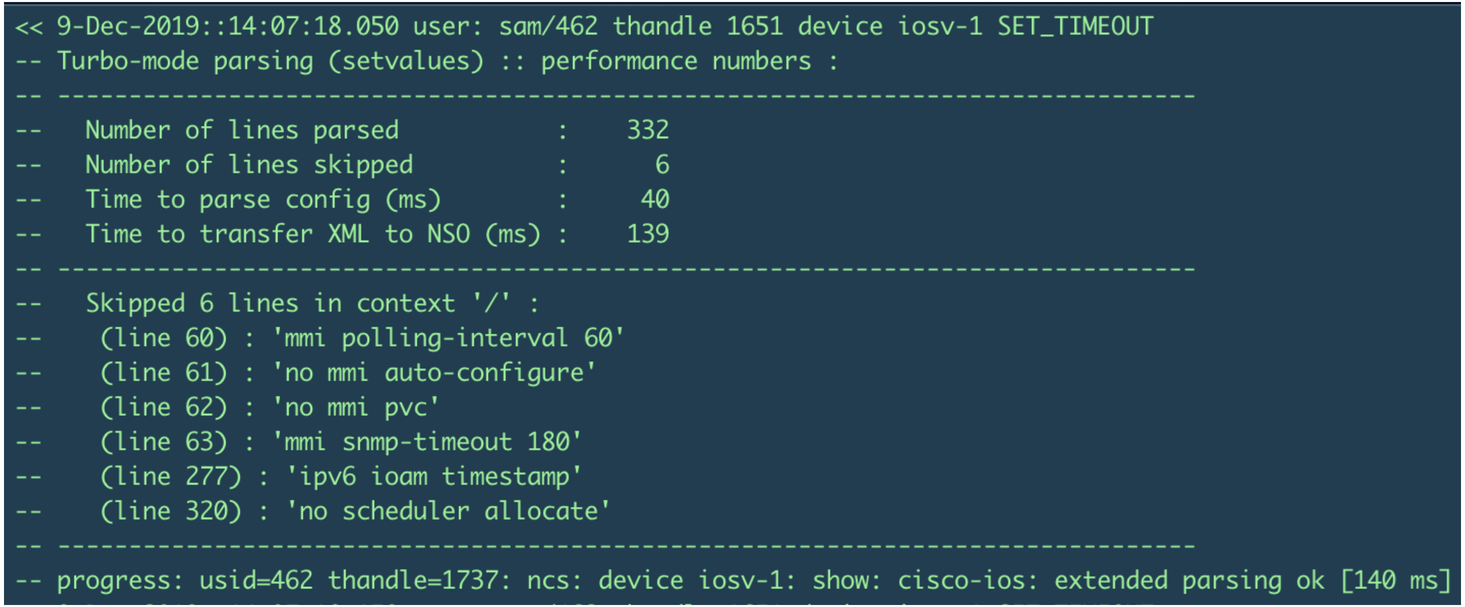
- Unify entire agency's network
- Mostly centrally managed now, but via a team of CLI cowboys
- Strategy
  - Develop official network configuration standards
  - Implement as NSO services
  - Deploy services to network
  - Repeat

Challenges

- NEDs often lacked support for the configurations we needed
- Lack of representative test environment
- Virtual test devices are not good enough
- Most configurations are currently OOB of NSO
- Wide variety of vendors/models
- Very wide variation of devices under one NED
    - Compatibility of a command depends on device model, OS version, and licensing
    - >200 unique combinations of model OS pairings for cisco-ios NED alone

Assumptions Going In

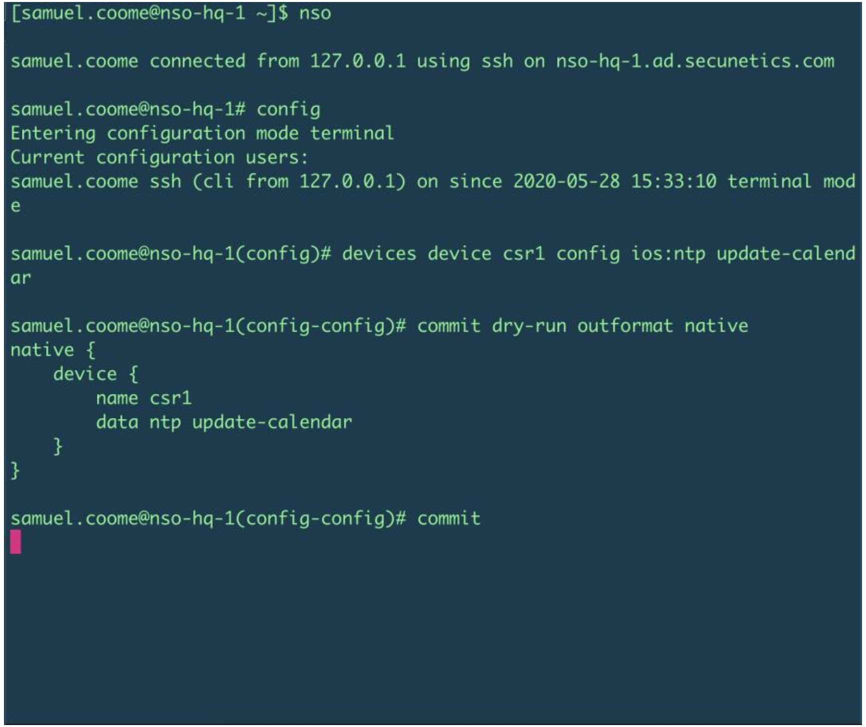
We assumed NEDs would be able to configure and parse all configuration



```
<< 9-Dec-2019::14:07:18.050 user: sam/462 thandle 1651 device iosv-1 SET_TIMEOUT
-- Turbo-mode parsing (setvalues) :: performance numbers :
-- --------------------------------------------------------------------------------
--   Number of lines parsed           :    332
--   Number of lines skipped          :      6
--   Time to parse config (ms)        :     40
--   Time to transfer XML to NSO (ms) :    139
-- --------------------------------------------------------------------------------
--   Skipped 6 lines in context '/' :
--    (line 60) : 'mmi polling-interval 60'
--    (line 61) : 'no mmi auto-configure'
--    (line 62) : 'no mmi pvc'
--    (line 63) : 'mmi snmp-timeout 180'
--    (line 277) : 'ipv6 ioam timestamp'
--    (line 320) : 'no scheduler allocate'
-- --------------------------------------------------------------------------------
-- progress: usid=462 thandle=1737: ncs: device iosv-1: show: cisco-ios: extended parsing ok [140 ms]
```

Assumptions Going In

We assumed NEDs would not allow you to configure commands the device didn’t support



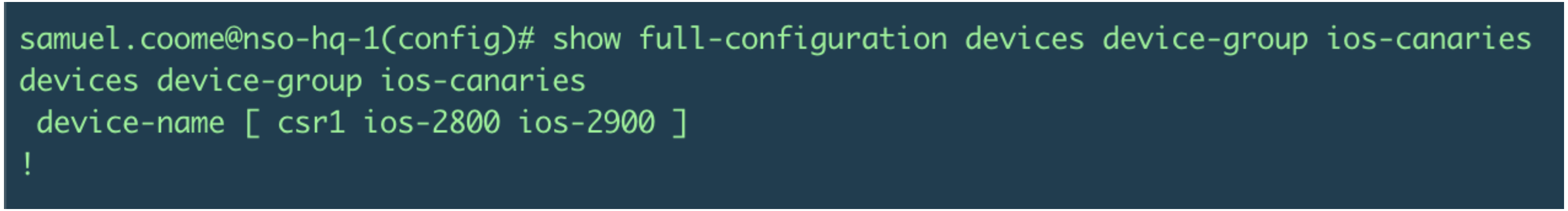
```
[samuel.coome@nso-hq-1 ~]$ nso

samuel.coome connected from 127.0.0.1 using ssh on nso-hq-1.ad.secunetics.com

samuel.coome@nso-hq-1# config
Entering configuration mode terminal
Current configuration users:
samuel.coome ssh (cli from 127.0.0.1) on since 2020-05-28 15:33:10 terminal mod
e

samuel.coome@nso-hq-1(config)# devices device csr1 config ios:ntp update-calend
ar

samuel.coome@nso-hq-1(config-config)# commit dry-run outformat native
native {
    device {
        name csr1
        data ntp update-calendar
    }
}

samuel.coome@nso-hq-1(config-config)# commit
```

First Encounter of *Old* meets *New*

- In testing, a cisco-ios CSR1000V did <u>not</u> support *ntp update-calendar*
- In production, ran into same problem with some physical devices
- First service deployment failed

Canary Devices

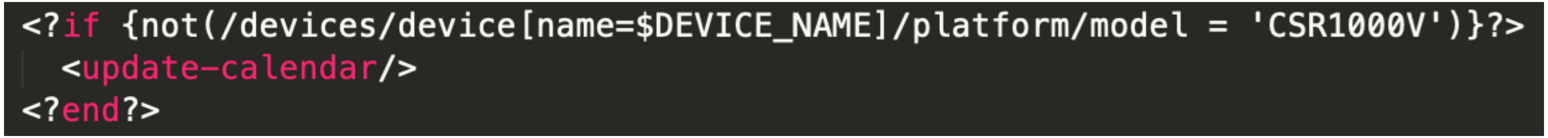
- Create a device-group of canary devices
- Device-group consists of one of each device model per NED
- Canary device-group acts as the initial compatibility test for the service



```
samuel.coome@nso-hq-1(config)# show full-configuration devices device-group ios-canaries
devices device-group ios-canaries
 device-name [ csr1 ios-2800 ios-2900 ]
!
```

Service Template Lookups for Platform

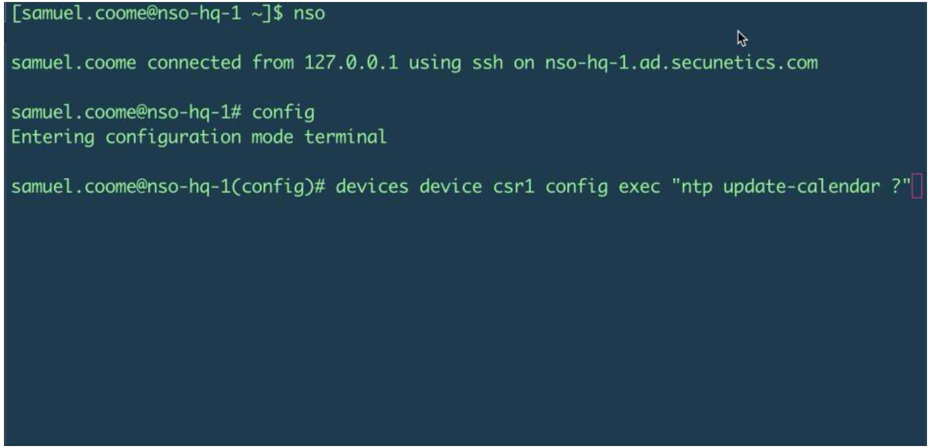
- Enumerate a list of all of the devices that failed a command
- Add their models to an <?if?> statement to skip the command
  - deploy a minimum mandatory configuration and the rest is *best-effort*
- Reload the packages & re-deploy the service



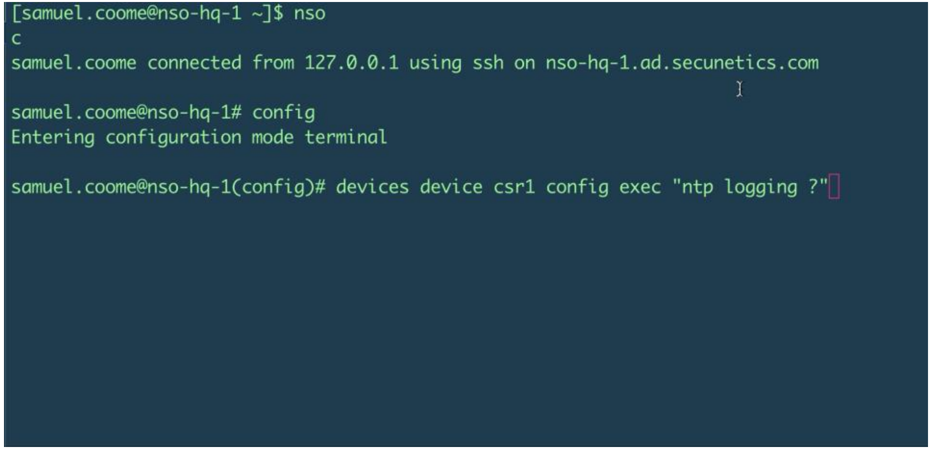
```
<?if {not(/devices/device[name=$DEVICE_NAME]/platform/model = 'CSR1000V')}?>
  <update-calendar/>
<?end?>
```

Query Devices

- Use ? to check if the command is supported



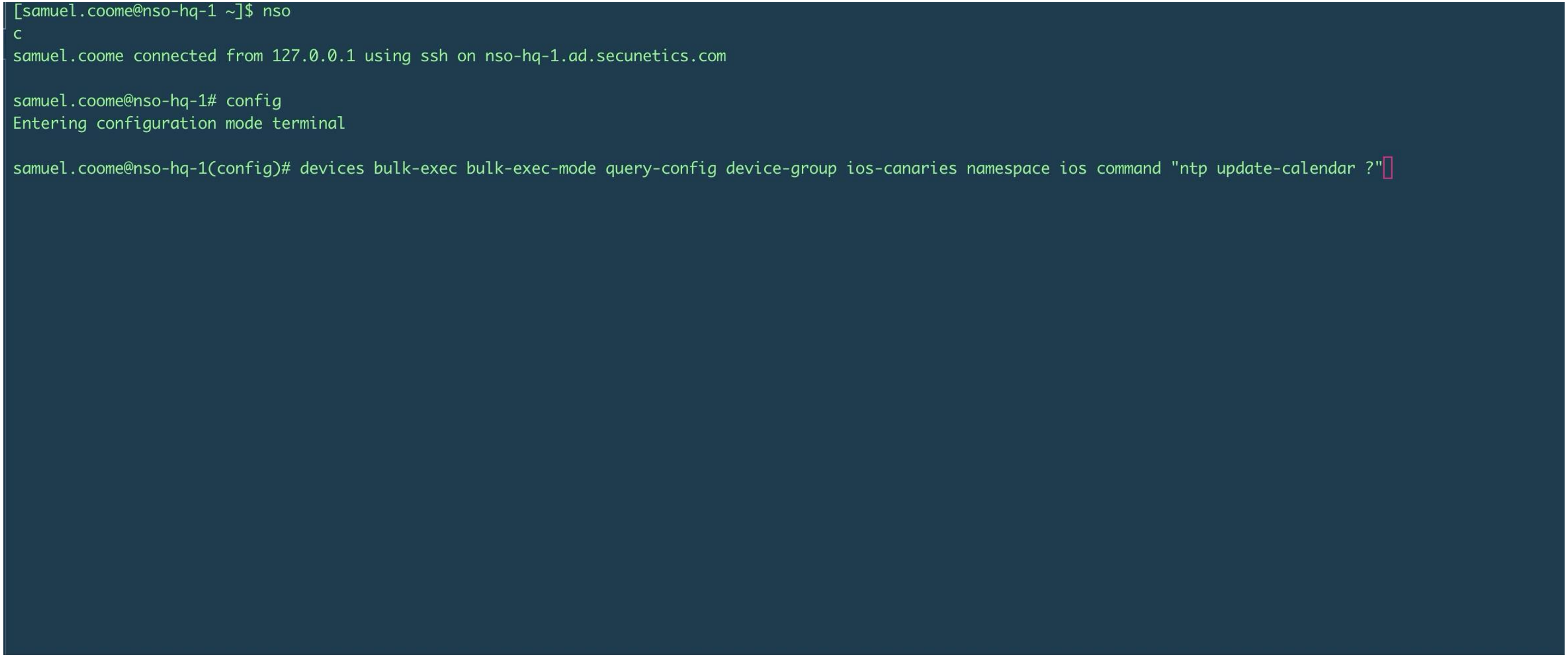
```
[samuel.coome@nso-hq-1 ~]$ nso

samuel.coome connected from 127.0.0.1 using ssh on nso-hq-1.ad.secunetics.com

samuel.coome@nso-hq-1# config
Entering configuration mode terminal

samuel.coome@nso-hq-1(config)# devices device csr1 config exec "ntp update-calendar ?"
```



```
[samuel.coome@nso-hq-1 ~]$ nso
c
samuel.coome connected from 127.0.0.1 using ssh on nso-hq-1.ad.secunetics.com

samuel.coome@nso-hq-1# config
Entering configuration mode terminal

samuel.coome@nso-hq-1(config)# devices device csr1 config exec "ntp logging ?"
```

Bulk Execution (bulk-exec)

- Augment NSO’s existing capabilities!
- Multi-threaded Python action
- Iterate through devices (group, list, etc.)
- Run *live-status* or *config exec* on each device



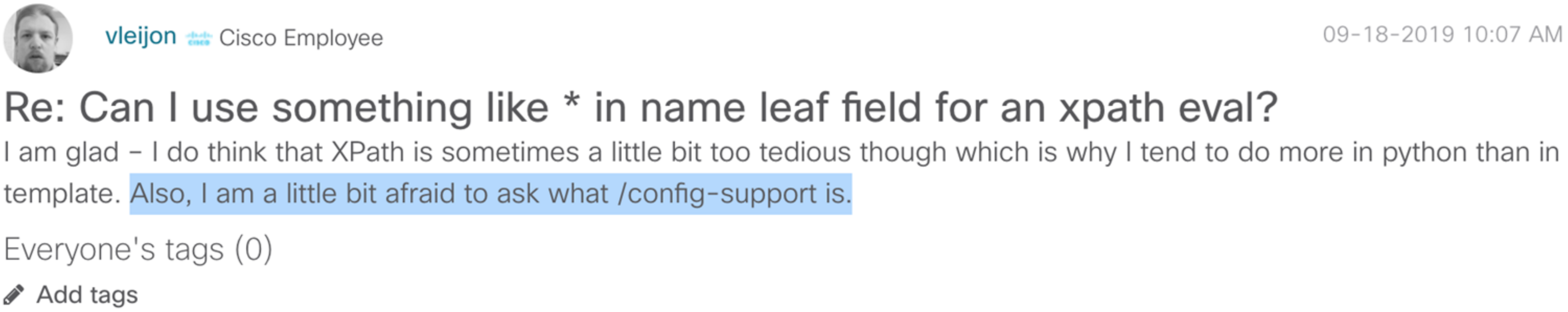
```
[samuel.coome@nso-hq-1 ~]$ nso
c
samuel.coome connected from 127.0.0.1 using ssh on nso-hq-1.ad.secunetics.com

samuel.coome@nso-hq-1# config
Entering configuration mode terminal

samuel.coome@nso-hq-1(config)# devices bulk-exec bulk-exec-mode query-config device-group ios-canaries namespace ios command "ntp update-calendar ?"
```

Edge Cases

- Not just device model
    - OS
    - Licenses
- New devices in the network bring new model/OS combinations
    - New failures require updates to the service

Config-support

- Modification to the NSO CDB schema
- Associates device-name to command
- Mark if the command is not supported



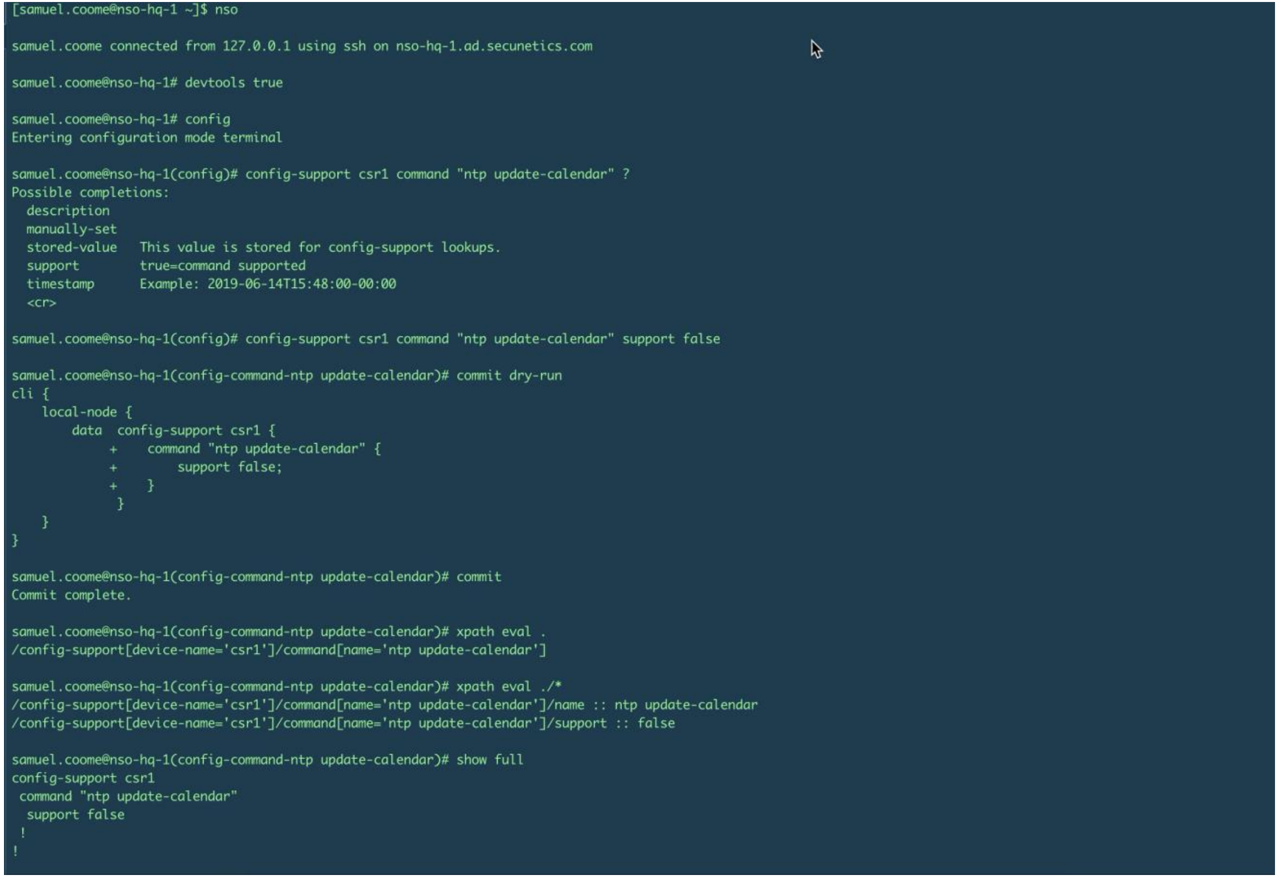
vleijon Cisco Employee 09-18-2019 10:07 AM

Re: Can I use something like * in name leaf field for an xpath eval?

I am glad – I do think that XPath is sometimes a little bit too tedious though which is why I tend to do more in python than in template. Also, I am a little bit afraid to ask what /config-support is.

Everyone's tags (0)

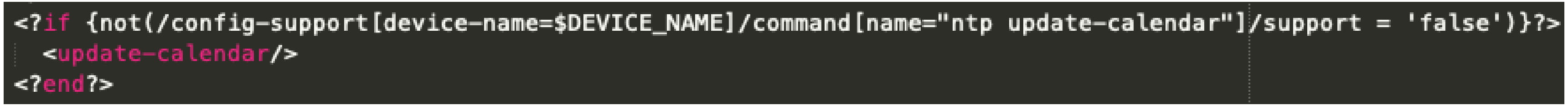
Add tags



```
[samuel.coome@nso-hq-1 ~]$ nso

samuel.coome connected from 127.0.0.1 using ssh on nso-hq-1.ad.secunetics.com

samuel.coome@nso-hq-1# devtools true

samuel.coome@nso-hq-1# config
Entering configuration mode terminal

samuel.coome@nso-hq-1(config)# config-support csr1 command "ntp update-calendar" ?
Possible completions:
  description
  manually-set
  stored-value   This value is stored for config-support lookups.
  support        true=command supported
  timestamp      Example: 2019-06-14T15:48:00-00:00
  <cr>

samuel.coome@nso-hq-1(config)# config-support csr1 command "ntp update-calendar" support false

samuel.coome@nso-hq-1(config-command-ntp update-calendar)# commit dry-run
cli {
    local-node {
        data  config-support csr1 {
             +    command "ntp update-calendar" {
             +        support false;
             +    }
              }
    }
}

samuel.coome@nso-hq-1(config-command-ntp update-calendar)# commit
Commit complete.

samuel.coome@nso-hq-1(config-command-ntp update-calendar)# xpath eval .
/config-support[device-name='csr1']/command[name='ntp update-calendar']

samuel.coome@nso-hq-1(config-command-ntp update-calendar)# xpath eval ./*
/config-support[device-name='csr1']/command[name='ntp update-calendar']/name :: ntp update-calendar
/config-support[device-name='csr1']/command[name='ntp update-calendar']/support :: false

samuel.coome@nso-hq-1(config-command-ntp update-calendar)# show full
config-support csr1
 command "ntp update-calendar"
  support false
 !
!
```

Service Template Lookups Revisited

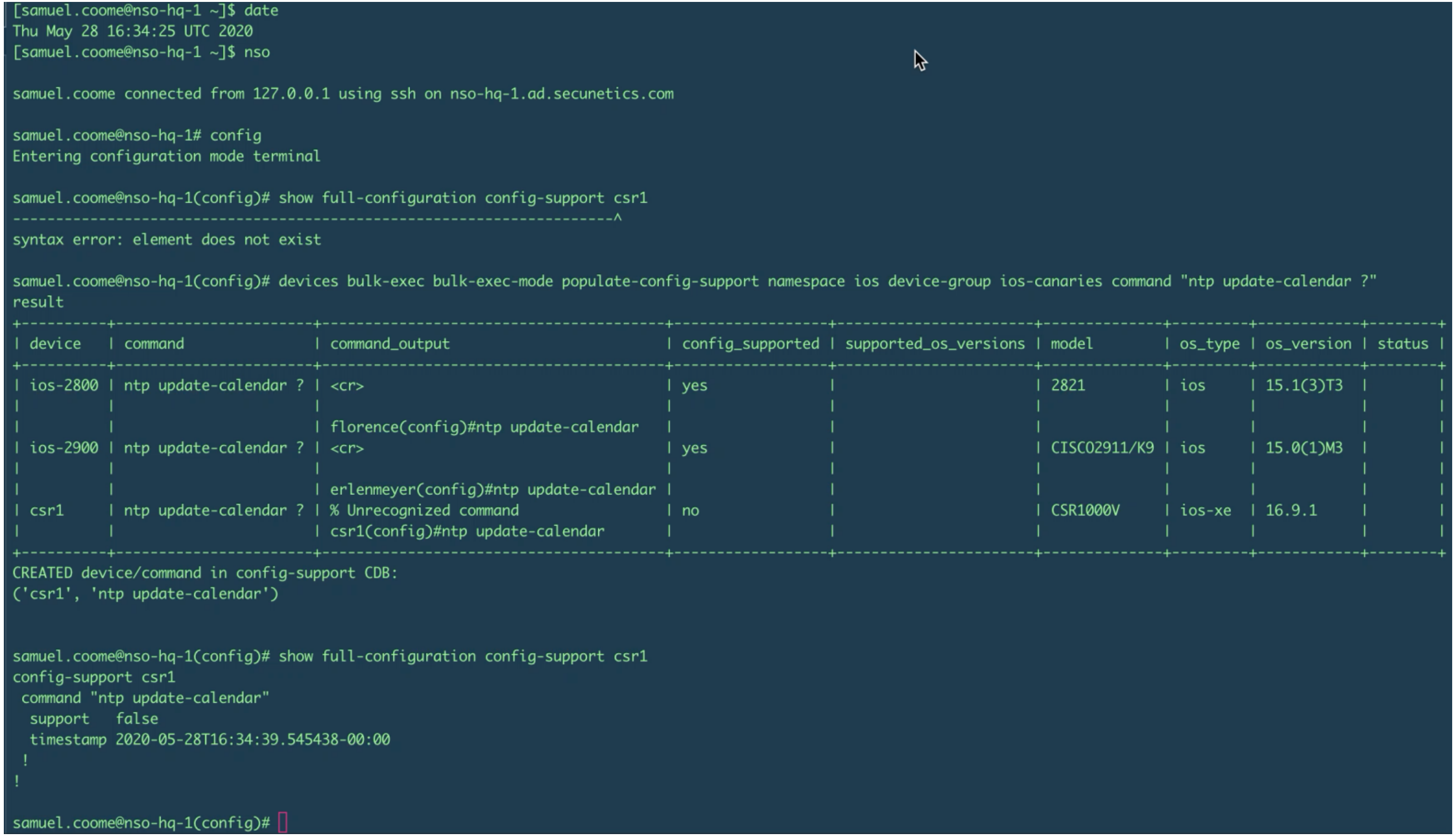
- Same methodology used for looking up the platform
- But one lookup covers all devices for a service regardless of platform or license



```
<?if {not(/config-support[device-name=$DEVICE_NAME]/command[name="ntp update-calendar"]/support = 'false')}?>
  <update-calendar/>
<?end?>
```

Bulk-exec and Config-support

- Store results from the bulk-exec command in config-support
- Update support for a service by running bulk-exec
  - No longer have to modify the template and reload the packages
- Re-deploying the service re-checks the config-support lookup



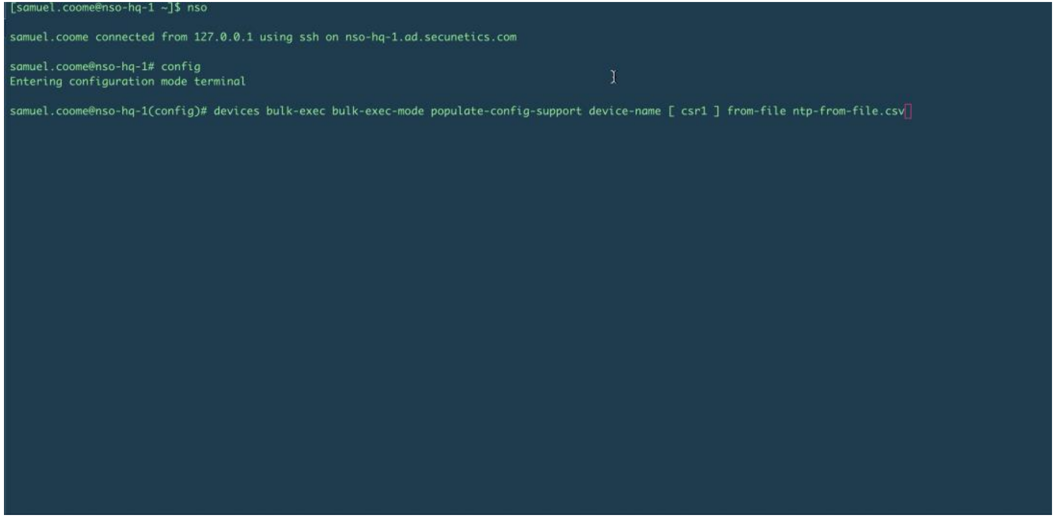
```
[samuel.coome@nso-hq-1 ~]$ date
Thu May 28 16:34:25 UTC 2020
[samuel.coome@nso-hq-1 ~]$ nso

samuel.coome connected from 127.0.0.1 using ssh on nso-hq-1.ad.secunetics.com

samuel.coome@nso-hq-1# config
Entering configuration mode terminal

samuel.coome@nso-hq-1(config)# show full-configuration config-support csr1
----------------------------------------------------------------------^
syntax error: element does not exist

samuel.coome@nso-hq-1(config)# devices bulk-exec bulk-exec-mode populate-config-support namespace ios device-group ios-canaries command "ntp update-calendar ?"
result
+----------+-----------------------+----------------------------------------+------------------+-----------------------+--------------+---------+------------+--------+
| device   | command               | command_output                         | config_supported | supported_os_versions | model        | os_type | os_version | status |
+----------+-----------------------+----------------------------------------+------------------+-----------------------+--------------+---------+------------+--------+
| ios-2800 | ntp update-calendar ? | <cr>                                   | yes              |                       | 2821         | ios     | 15.1(3)T3  |        |
|          |                       |                                        |                  |                       |              |         |            |        |
|          |                       | florence(config)#ntp update-calendar   |                  |                       |              |         |            |        |
| ios-2900 | ntp update-calendar ? | <cr>                                   | yes              |                       | CISCO2911/K9 | ios     | 15.0(1)M3  |        |
|          |                       |                                        |                  |                       |              |         |            |        |
|          |                       | erlenmeyer(config)#ntp update-calendar |                  |                       |              |         |            |        |
| csr1     | ntp update-calendar ? | % Unrecognized command                 | no               |                       | CSR1000V     | ios-xe  | 16.9.1     |        |
|          |                       | csr1(config)#ntp update-calendar       |                  |                       |              |         |            |        |
+----------+-----------------------+----------------------------------------+------------------+-----------------------+--------------+---------+------------+--------+
CREATED device/command in config-support CDB:
('csr1', 'ntp update-calendar')


samuel.coome@nso-hq-1(config)# show full-configuration config-support csr1
config-support csr1
 command "ntp update-calendar"
  support   false
  timestamp 2020-05-28T16:34:39.545438-00:00
 !
!

samuel.coome@nso-hq-1(config)# 
```

Required for Ease of Use

- Know all the commands for a service
- Know which commands are being looked up in the service template
- Be able to perform the compatibility check prior to the error occurring

Feed bulk-exec commands from a file

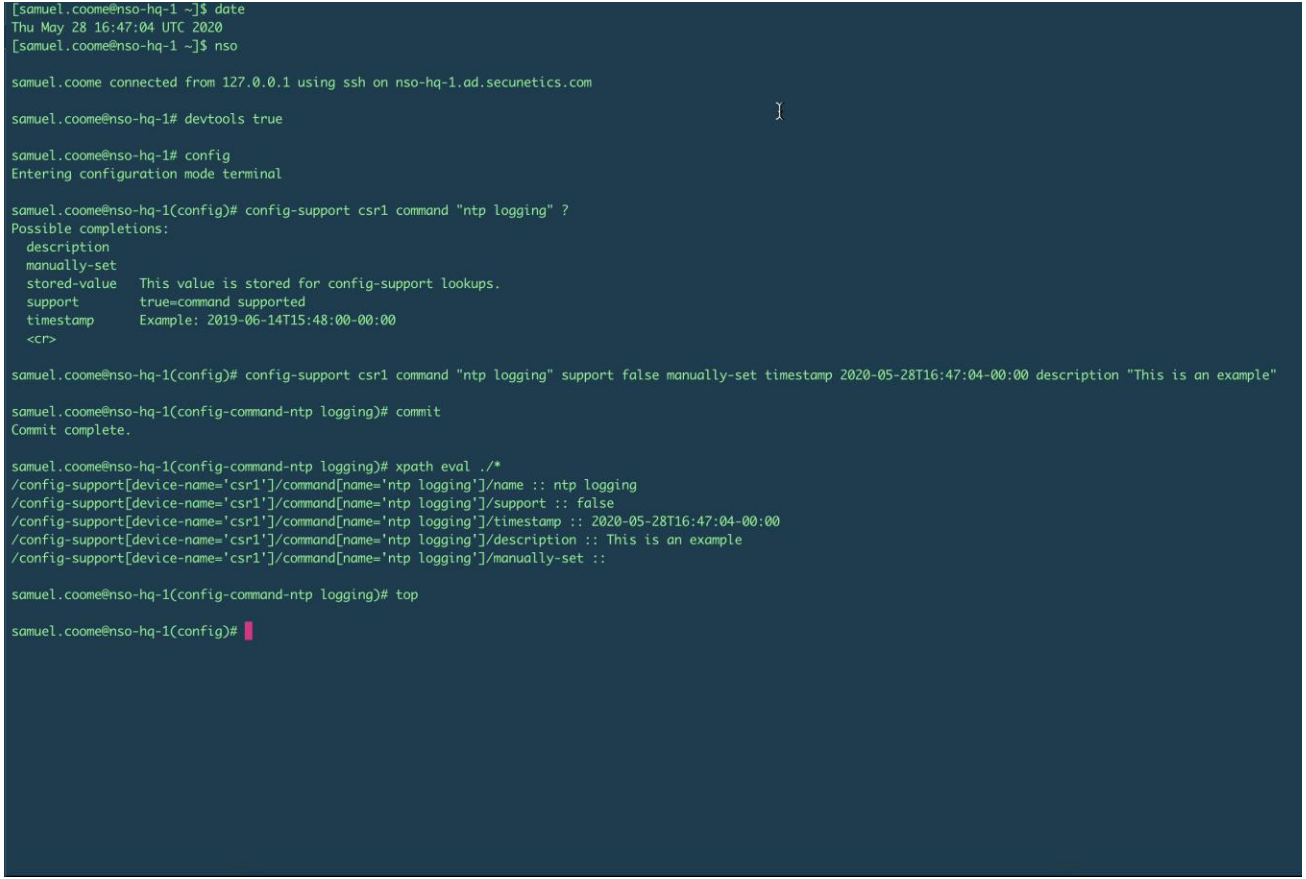
- The file acts as a batch file for testing all commands for a service
- Run the file on all devices for a new service
- Run the file on new devices



```
[samuel.coome@nso-hq-1 ~]$ nso

samuel.coome connected from 127.0.0.1 using ssh on nso-hq-1.ad.secunetics.com

samuel.coome@nso-hq-1# config
Entering configuration mode terminal

samuel.coome@nso-hq-1(config)# devices bulk-exec bulk-exec-mode populate-config-support device-name [ csr1 ] from-file ntp-from-file.csv
```

Manual override

- Automation can only be as good as the information you work with
- Devices lie
  - False positives
  - False negatives
- Need to be able to manually command support for lying devices
  - We called it *manually-set*
  - Marks the command as immutable against automation (e.g., bulk-exec)



```
[samuel.coome@nso-hq-1 ~]$ date
Thu May 28 16:47:04 UTC 2020
[samuel.coome@nso-hq-1 ~]$ nso

samuel.coome connected from 127.0.0.1 using ssh on nso-hq-1.ad.secunetics.com

samuel.coome@nso-hq-1# devtools true

samuel.coome@nso-hq-1# config
Entering configuration mode terminal

samuel.coome@nso-hq-1(config)# config-support csr1 command "ntp logging" ?
Possible completions:
  description
  manually-set
  stored-value   This value is stored for config-support lookups.
  support        true=command supported
  timestamp      Example: 2019-06-14T15:48:00-00:00
  <cr>

samuel.coome@nso-hq-1(config)# config-support csr1 command "ntp logging" support false manually-set timestamp 2020-05-28T16:47:04-00:00 description "This is an example"

samuel.coome@nso-hq-1(config-command-ntp logging)# commit
Commit complete.

samuel.coome@nso-hq-1(config-command-ntp logging)# xpath eval ./*
/config-support[device-name='csr1']/command[name='ntp logging']/name :: ntp logging
/config-support[device-name='csr1']/command[name='ntp logging']/support :: false
/config-support[device-name='csr1']/command[name='ntp logging']/timestamp :: 2020-05-28T16:47:04-00:00
/config-support[device-name='csr1']/command[name='ntp logging']/description :: This is an example
/config-support[device-name='csr1']/command[name='ntp logging']/manually-set ::

samuel.coome@nso-hq-1(config-command-ntp logging)# top

samuel.coome@nso-hq-1(config)#
```

Summary / Takeaways

- Your existing environment may not have been engineered with automation in mind
- NSO is a platform, augment its current capabilities
- For diverse environments you require flexibility, scalability, and tracking from your solution
- It really is a tricky thing to weave the old into the new, but it can be done!

Questions?