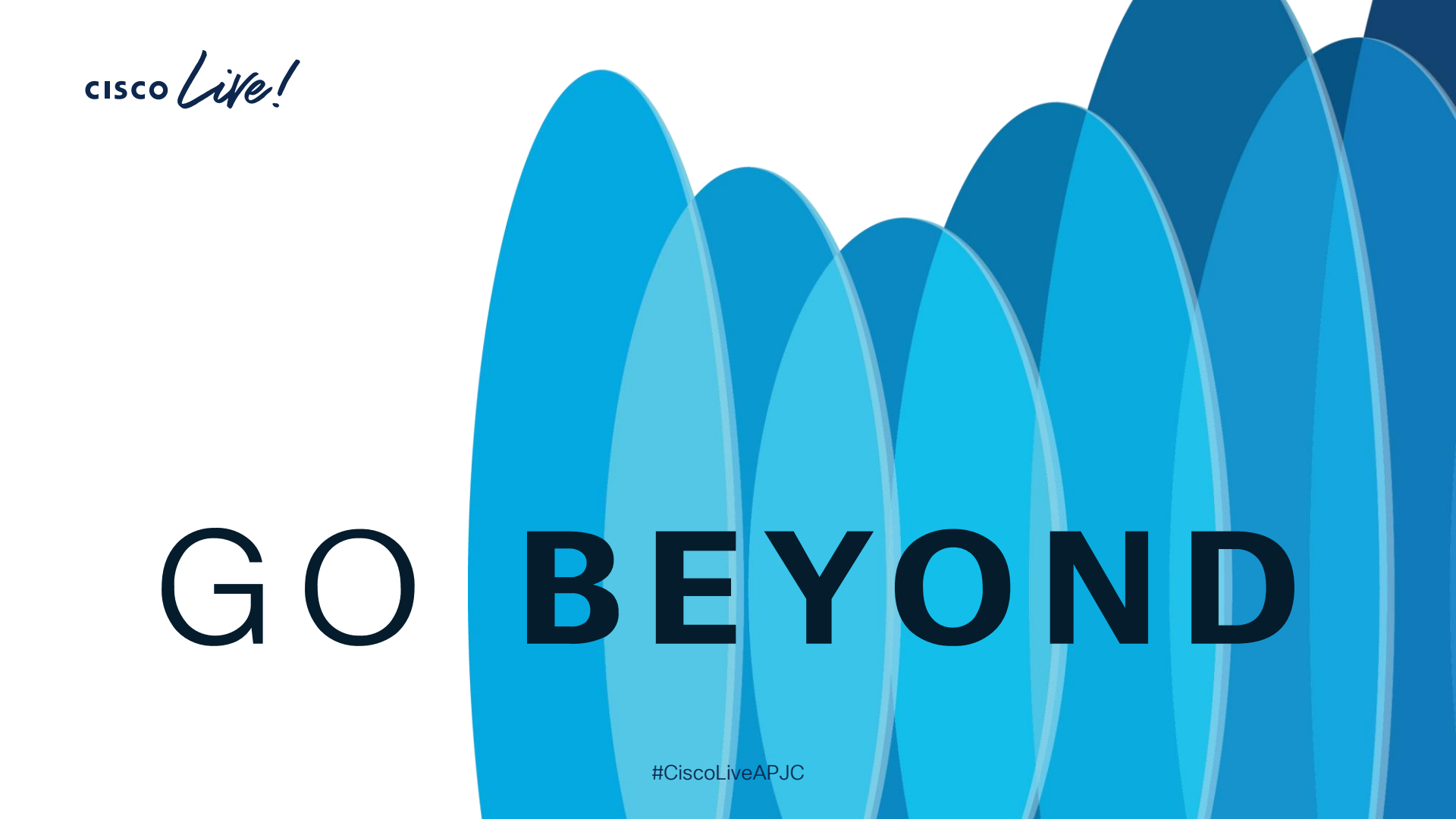

cisco Live!
GO BEYOND
#CiscoLiveAPJC

Programmability, Automation Model Driven Telemetry on Cisco IOS XE with a dash of YANG Suite

Story DeWeese, Technical Marketing
@StoryDeWeese
DEVNET-1283

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-1283

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

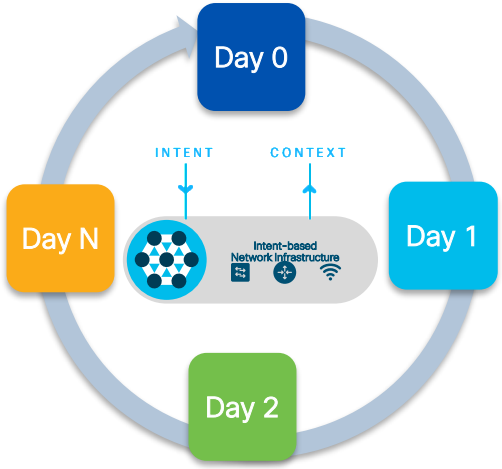
Webex spaces will be moderated by the speaker until November 15, 2024.

cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

Intro to Programmability and Automation

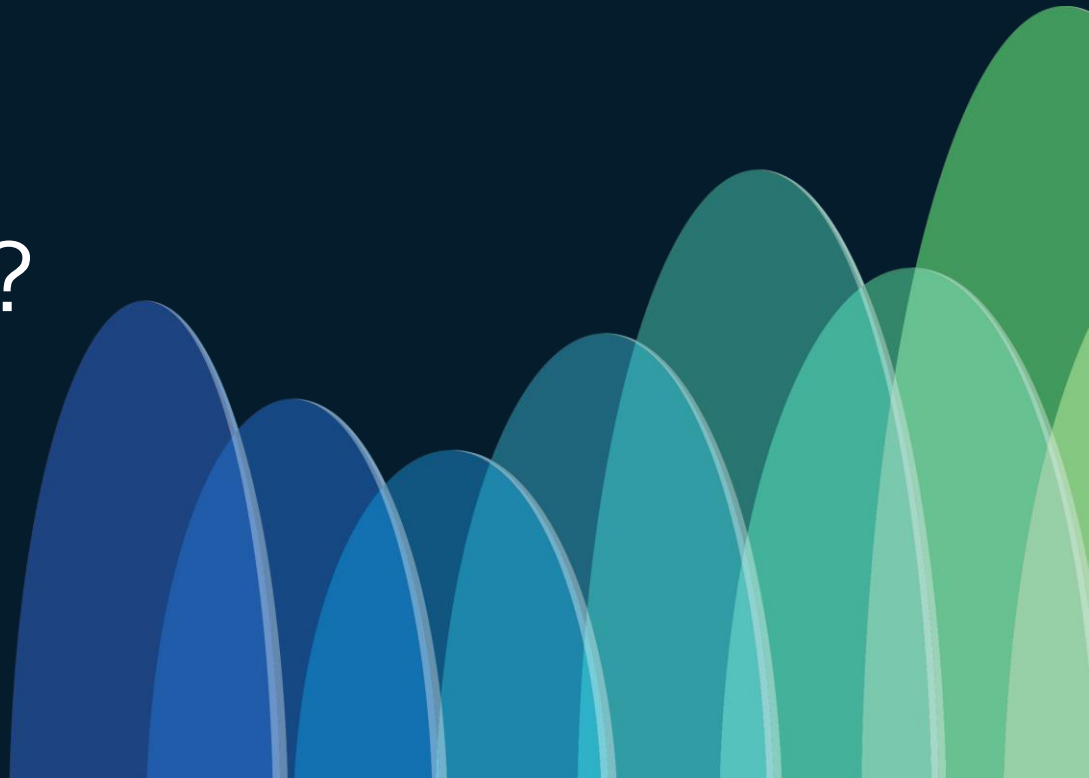


Tooling

Resources

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Why do we use programmability?

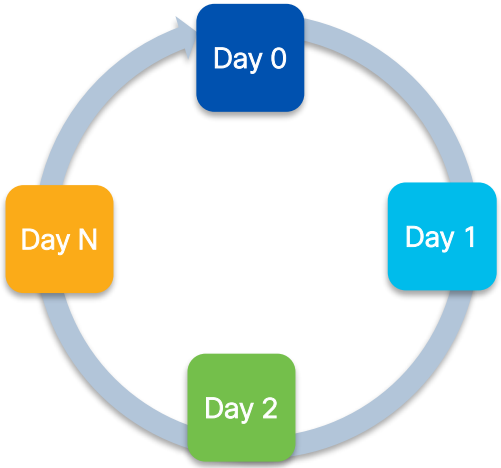


Programmability solutions for complex networks

Efficient	Consistent	Scalable	Secure	Seamless	Smart
Managing infrastructure as code while lowering OPEX	Repeatable and precise intent-based outcomes	Reduce time and effort with large network automation requirements	Secure APIs and integrations	Create value integrating with 3rd party platforms	Real time event notifications, AI/ML capabilities, and streaming telemetry

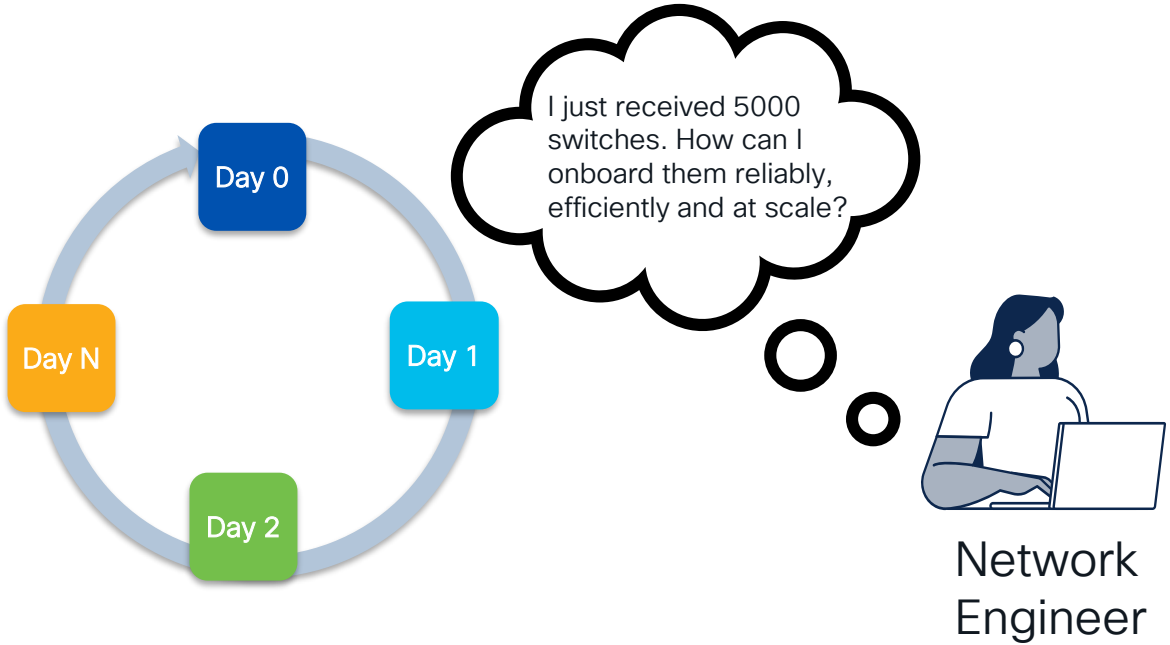
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS XE Programmability & Automation Lifecycle



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS XE Programmability & Automation Lifecycle



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS XE Programmability & Automation Lifecycle

Pre-boot Execution Environment (iPXE)

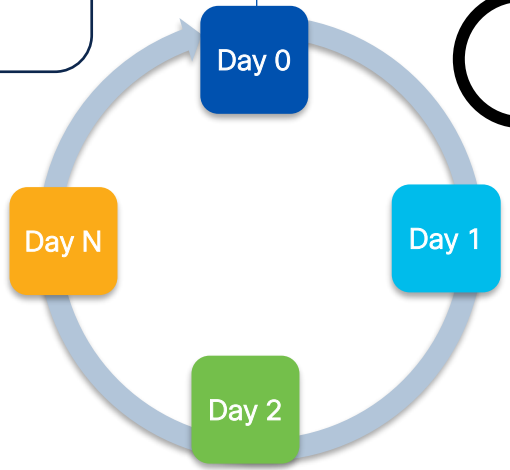
RFC8572 Secure Zero Touch Provisioning ZTP

VM Automation

Provisioning Automation

python™

Device Onboarding

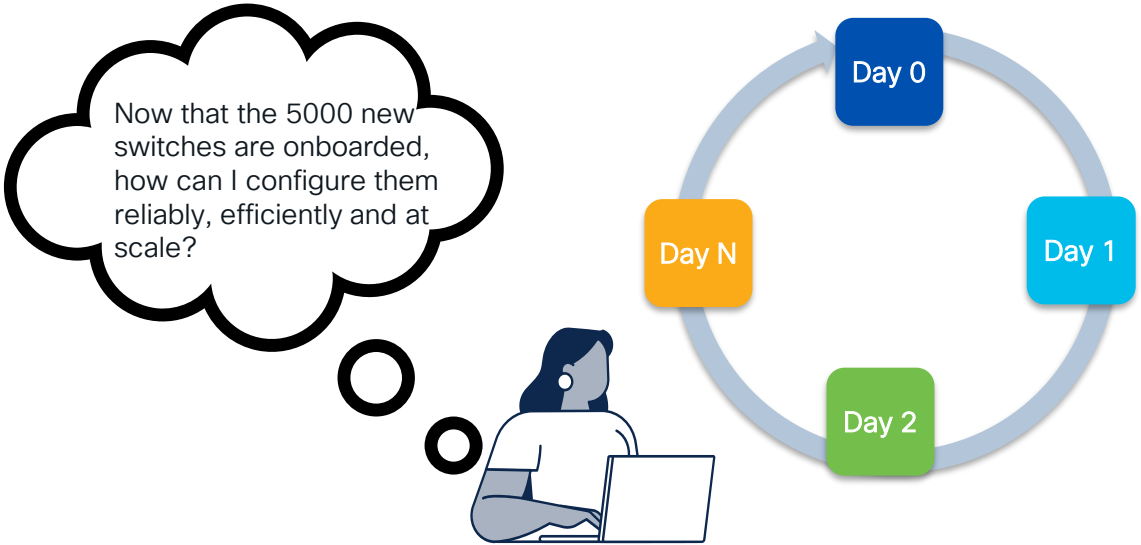


Nice! All 5000 switches are onboarded using Secure Zero Touch Provisioning

Network Engineer

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS XE Programmability & Automation Lifecycle

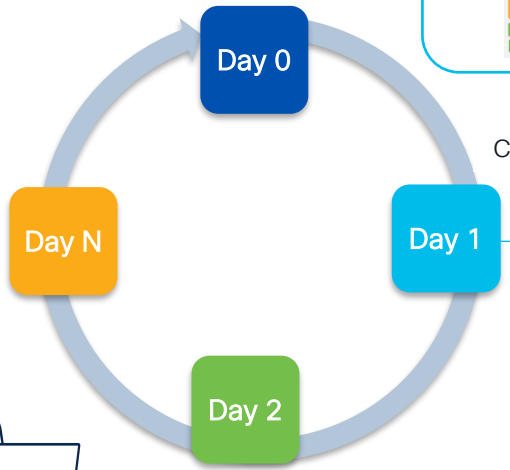


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS XE Programmability & Automation Lifecycle

I can use a tooling such as Ansible or Terraform to configure my 5000 switches at once

Network Engineer



Model Driven Programmability

Device Configuration

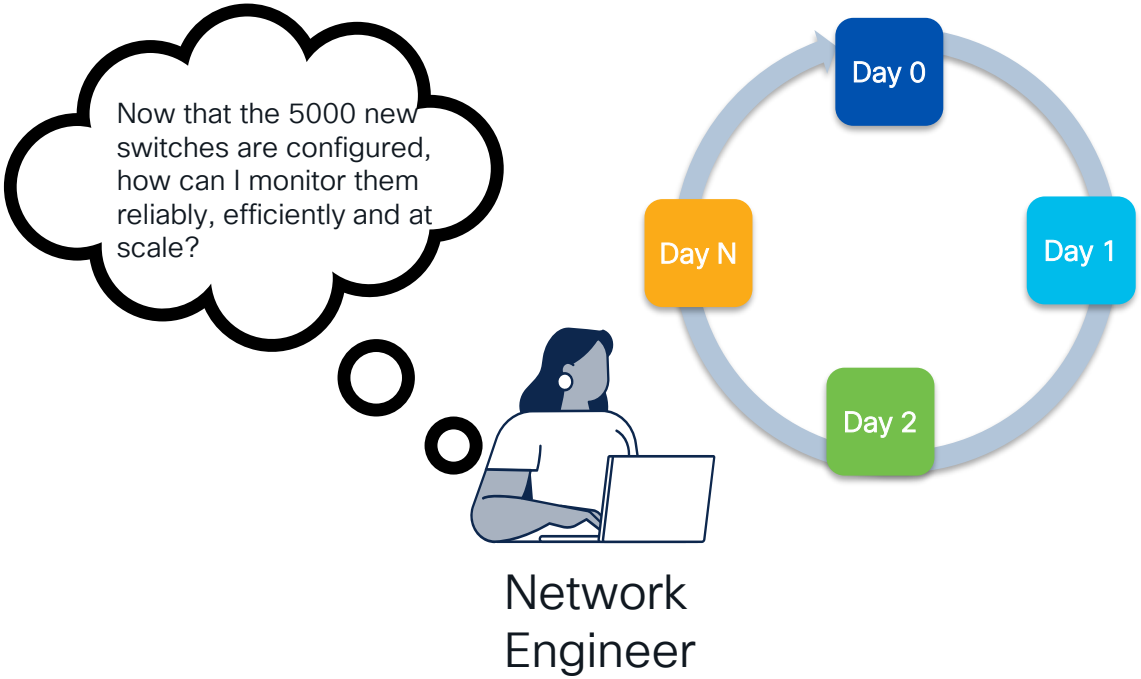
Network Configuration Protocol (NETCONF), RESTCONF, gNMI

YANG “native” Data Models, OpenConfig,

YANG Suite, Terraform, Ansible, pyATS tooling

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS XE Programmability & Automation Lifecycle

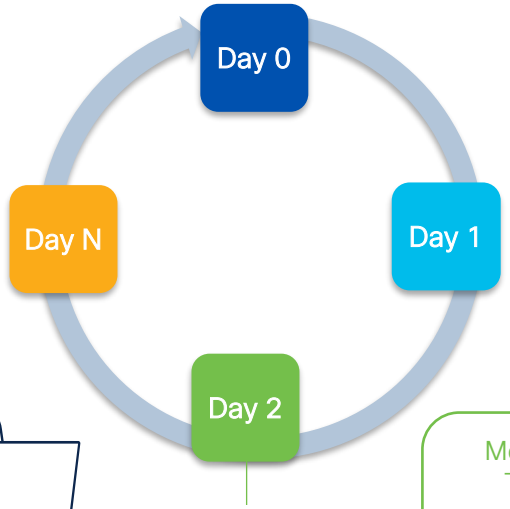


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS XE Programmability & Automation Lifecycle

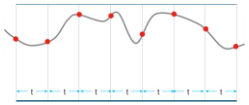
I'll use gRPC for Model Driven Telemetry to monitor changes on my device and quickly find any anomalies

Network Engineer



Device Monitoring

Model Driven Telemetry



TIG_MDT container + guide

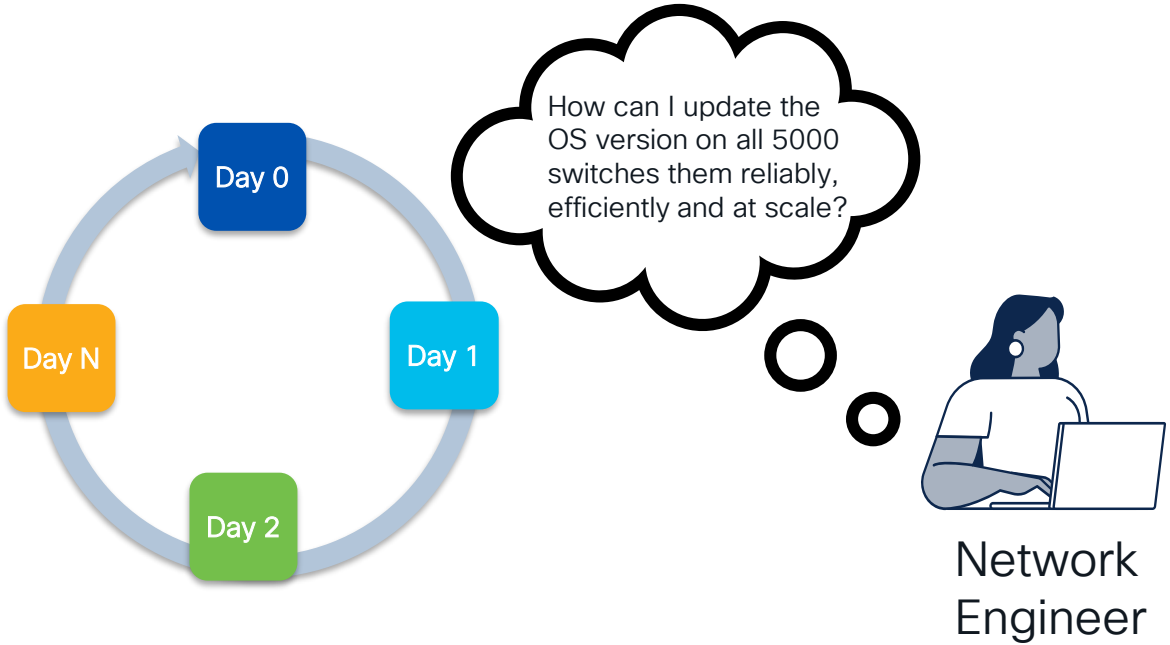
YANG On-Change support

gRPC Dial-Out + DNS + mTLS

gNMI/NETCONF Dial-In

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS XE Programmability & Automation Lifecycle



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS XE Programmability & Automation Lifecycle

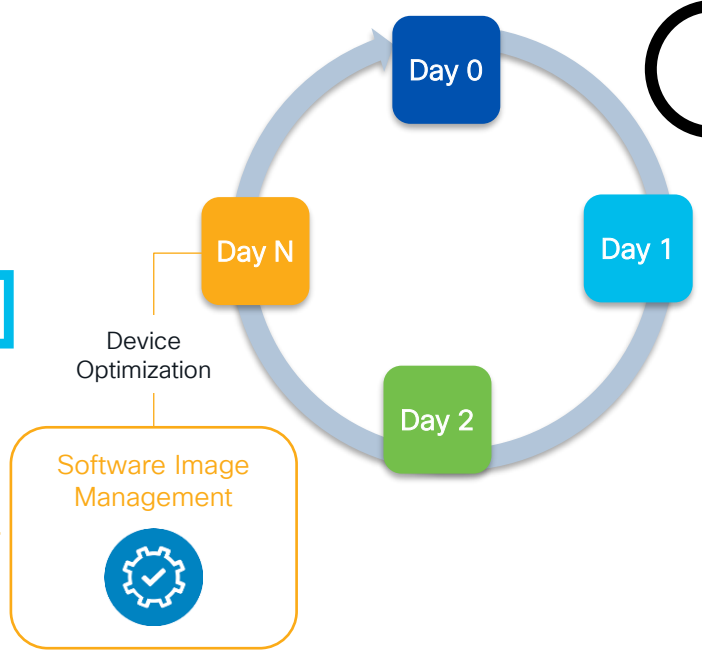
gNOI cert/os/reset proto

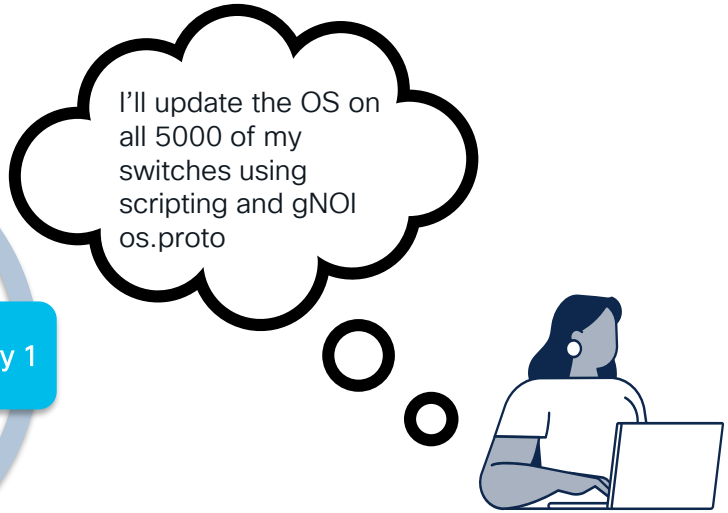
Guest Shell + Python/NETCONF

CentOS 8 Python 3

Application Hosting with Docker

“show run” CLI to YANG

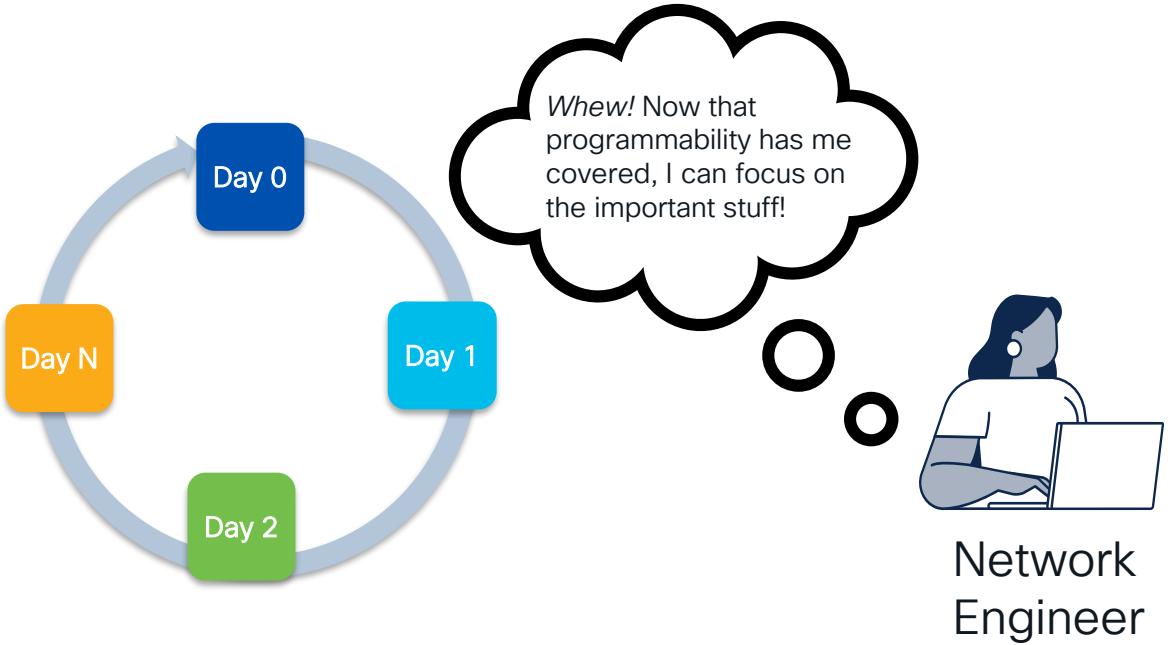




Network Engineer

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS XE Programmability & Automation Lifecycle



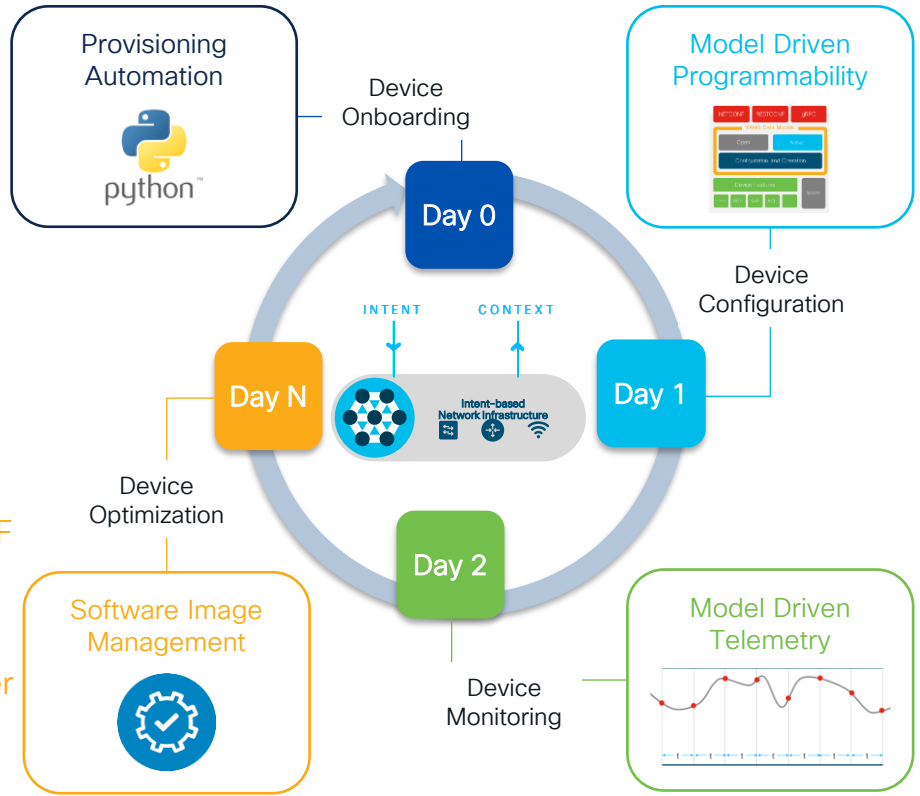
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS XE Programmability & Automation Lifecycle

Pre-boot Execution Environment (iPXE)

RFC8572 Secure Zero Touch Provisioning ZTP

VM Automation



Network Configuration Protocol (NETCONF), RESTCONF, gNMI

YANG “native” Data Models, OpenConfig,

YANG Suite, Terraform, Ansible, pyATS tooling

gNOI cert/os/reset proto

Guest Shell + Python/NETCONF

CentOS 8 Python 3

Application Hosting with Docker

“show run” CLI to YANG

TIG_MDT container + guide

YANG On-Change support

gRPC Dial-Out + DNS + mTLS

gNMI/NETCONF Dial-In

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IOS XE programmability and Telemetry “Stack”

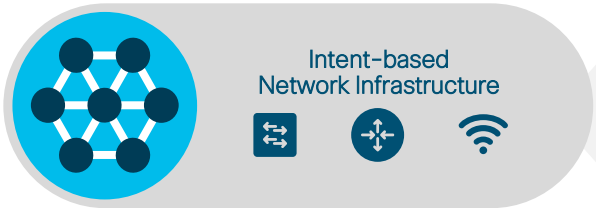
CLI

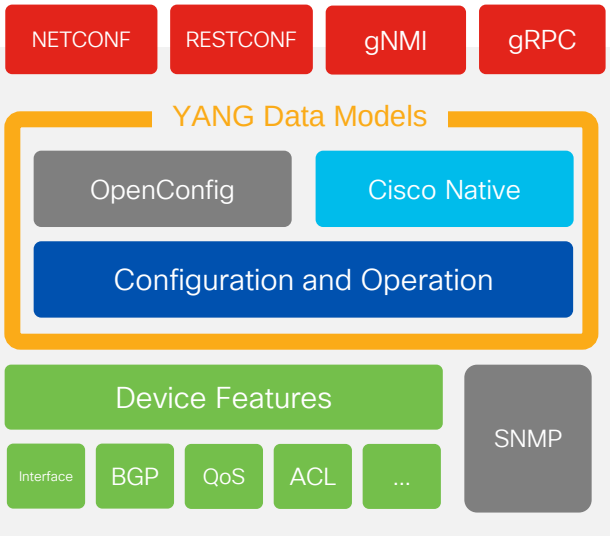
SNMP

WebUI

The NETCONF, RETCONF, gNMI and gRPC are programmatic interfaces that provide additional methods for interfacing with the IOS XE device – Just like the CLI, SNMP, and WebUI is used for configuration changes and operational metrics so can the programmatic interfaces of NETCONF, RESTCONF, gNMI, and gRPC.

YANG data models define the data that is available for configuration and streaming telemetry





IETF OPENCONFIG

IEEE

cisco

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Model Driven Programmability Interface Comparison

Network architecture, security posture and policy, YANG data modules, tools and language preferences are some considerations when leveraging the various MDP interfaces

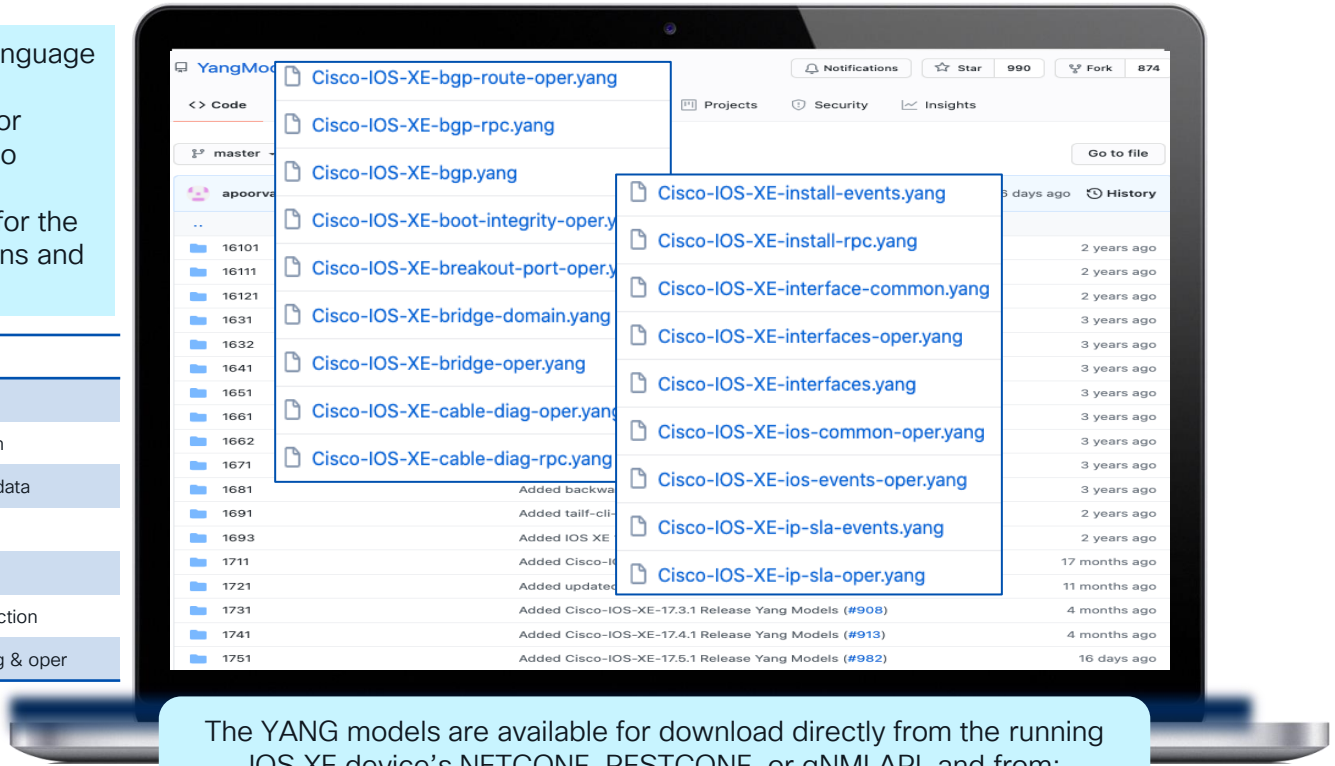
	NETCONF	RESTCONF	gNMI
Minimum IOS XE Version	16.6	16.7	16.8
Recommended Version	17.6	17.6	17.7
Default Port	830	443	9339
Operations	<get>,<get-config>,<edit-config>,<establish-subscription>	GET, POST, PUT, PATCH, DELETE	GET, SET, SUBSCRIBE
Encoding	XML	XML or JSON	RFC7951 JSON_IETF
Security	SSH + PKI certificate or password	HTTPS user/pass	TLS certificate with user authentication
Transport Protocol	SSH	HTTPS	HTTP/2
Tooling	YANG Suite, ncclient, Netconf-console	YANG Suite*, Postman, python	YANG Suite*, gnmic, gnmi_cli
Content	YANG	YANG	YANG + Protobuf

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS XE - YANG models on GitHub

- RFC 7950 YANG data modelling language are the API definitions for IOS XE
- The YANG modules are available for download from the API and are also published on Github.com
- Notable modules are listed below for the running-config, feature oper, actions and event notifications

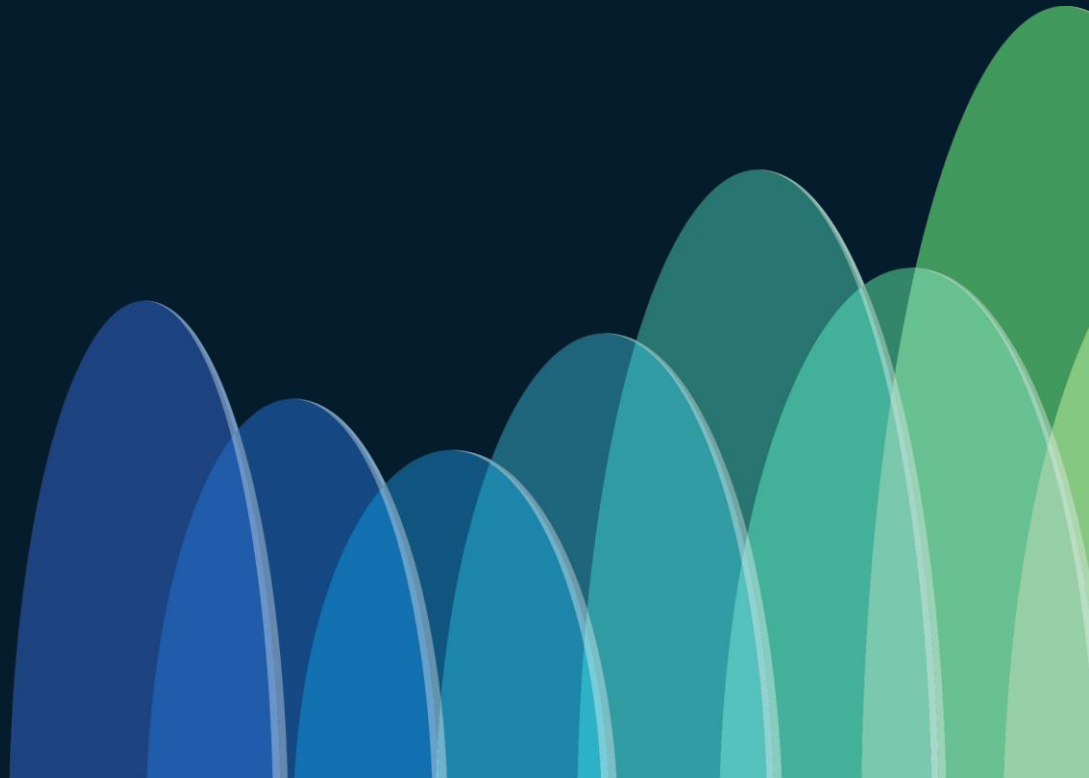
YANG module name.yang	Description
Cisco-IOS-XE-native	running-config
Cisco-IOS-XE-{feature}-cfg	Feature configuration
Cisco-IOS-XE-{feature}-oper	Feature operational data
Cisco-IOS-XE-{feature}-rpc	Actions
Cisco-IOS-XE-{feature}-events	Telemetry Events
Cisco-evpn-service	EVPN service abstraction
OpenConfig-{feature}	abstraction for config & oper



The YANG models are available for download directly from the running IOS XE device's NETCONF, RESTCONF, or gNMI API, and from: https://github.com/YangModels/yang/tree/main/vendor/cisco/xe

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Day 0

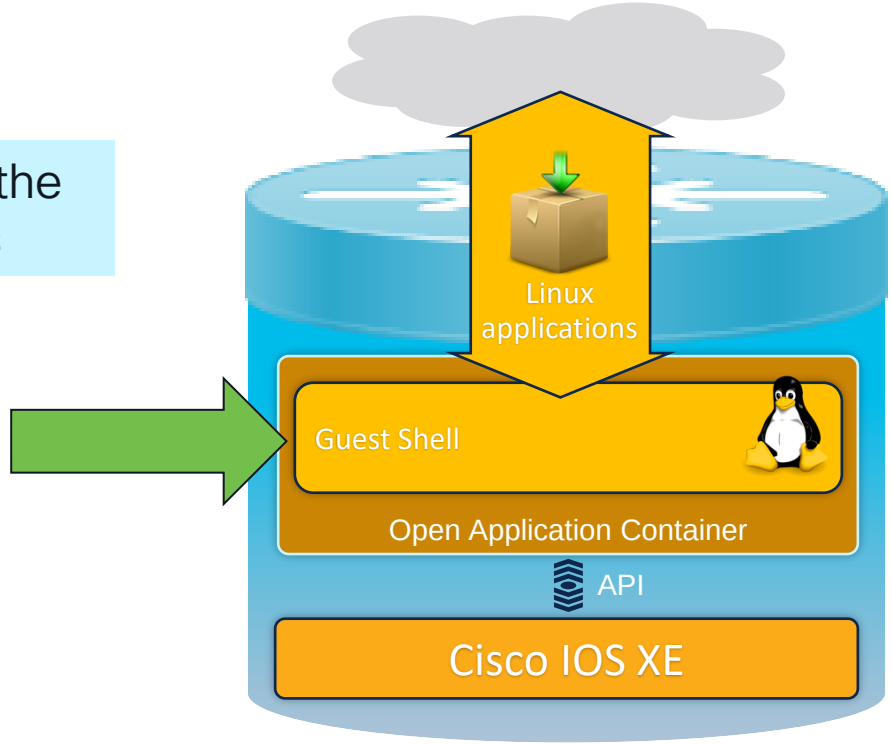


Linux Shell Environment on Cisco IOS XE devices

Cisco IOS XE devices can access the on-box Guest Shell using API calls

This Linux shell can be used for

- Scripting
- Hosting Applications
- Zero Touch Provisioning
- & so much more!

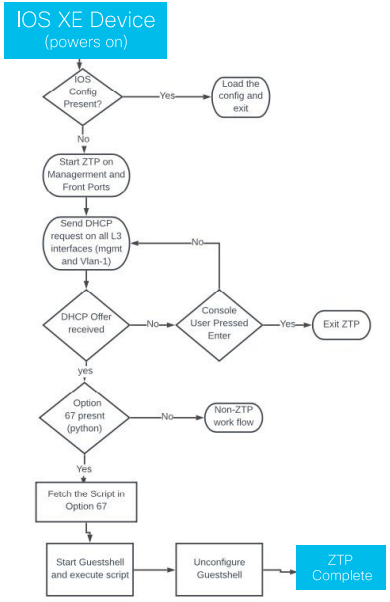


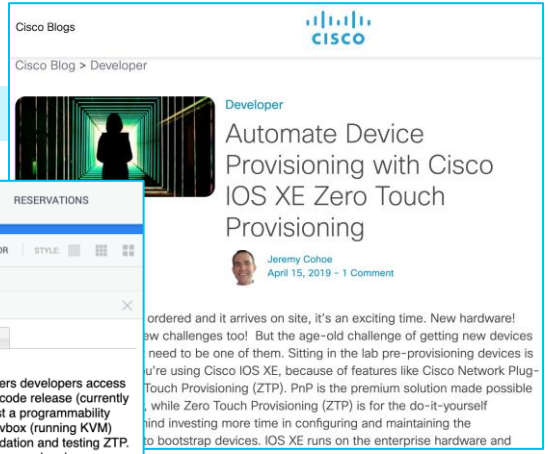
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

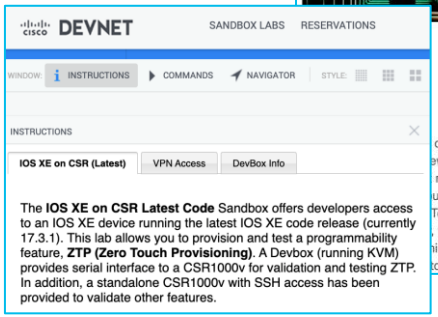
Day 0 – Classic ZTP Overview

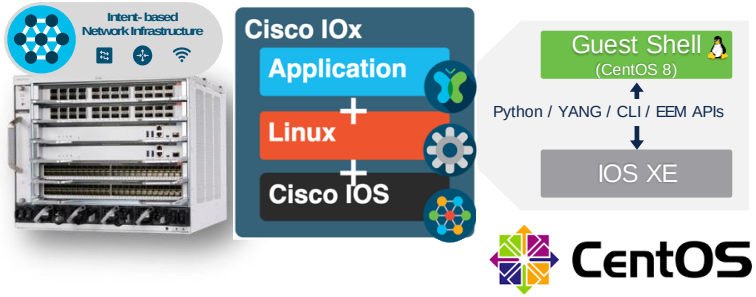
The Day 0 ZTP features are used to automatically configure and provision network devices

1. When an IOS XE device boots and no configuration is present, the device will issue a DHCP request on the management port and on the front panel port.
2. If the DHCP response contains option 67 then ZTP is initiated and the device will retrieve and execute the python script from within the Guest Shell
3. Guest Shell is started and networking is automatically configured







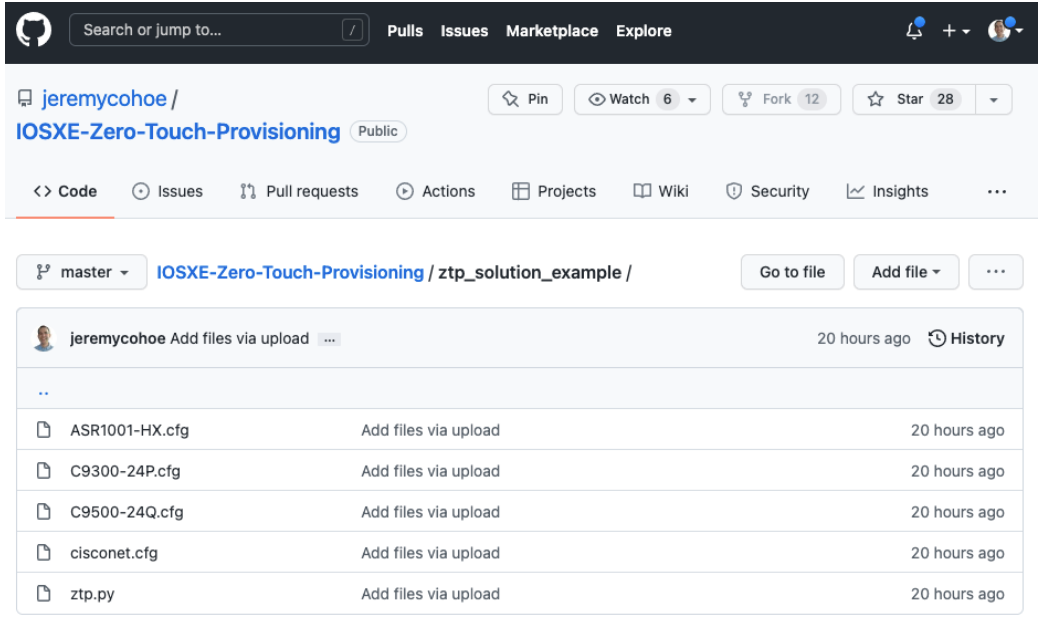


https://www.youtube.com/watch?v=EAXnftG6odg
https://blogs.cisco.com/developer/device-provisioning-with-ios-xe-zero-touch-provisioning
https://devnetsandbox.cisco.com/DevNet
Secure ZTP blog https://blogs.cisco.com/developer/secureztp01

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

ZTP customer use case – code samples

https://github.com/jeremycohoe/IOSXE-Zero-Touch-Provisioning/tree/master/ztp_solution_example

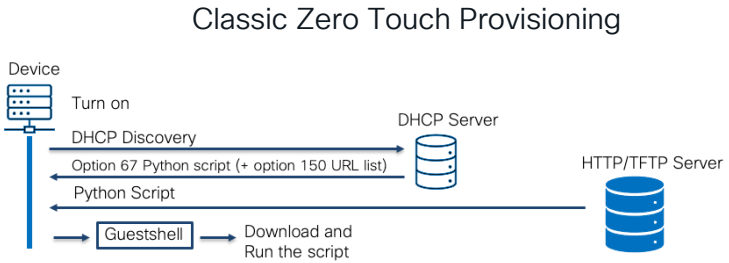


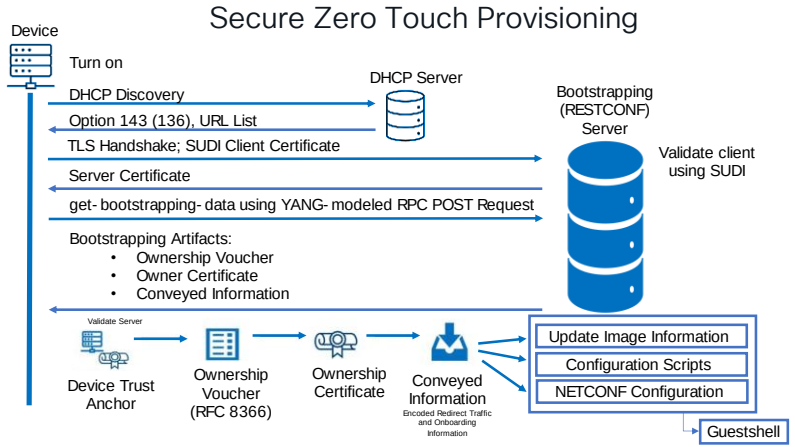
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

RFC8572 Secure ZTP

RFC details: https://www.rfc-editor.org/rfc/rfc8572.html

1. Conveyed Information: used to encode the redirect information and onboarding information (switch config)
2. Ownership Certificate: used by a device to verify the signature over the conveyed information
3. Ownership Voucher: used to verify a device owner as defined by the manufacturer (from the MASA)



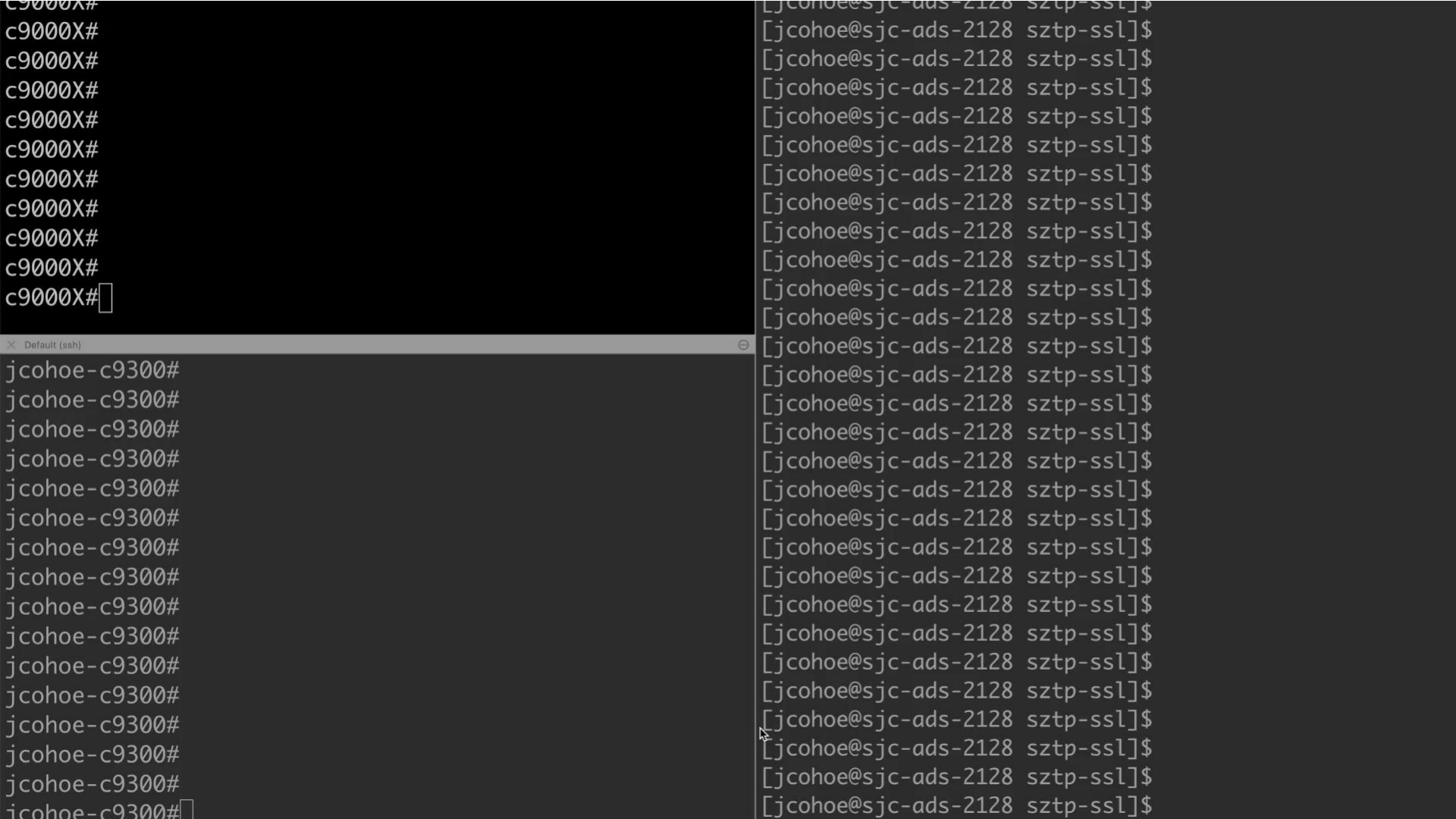


Some security requirements for classic ZTP are resolved using Secure ZTP:

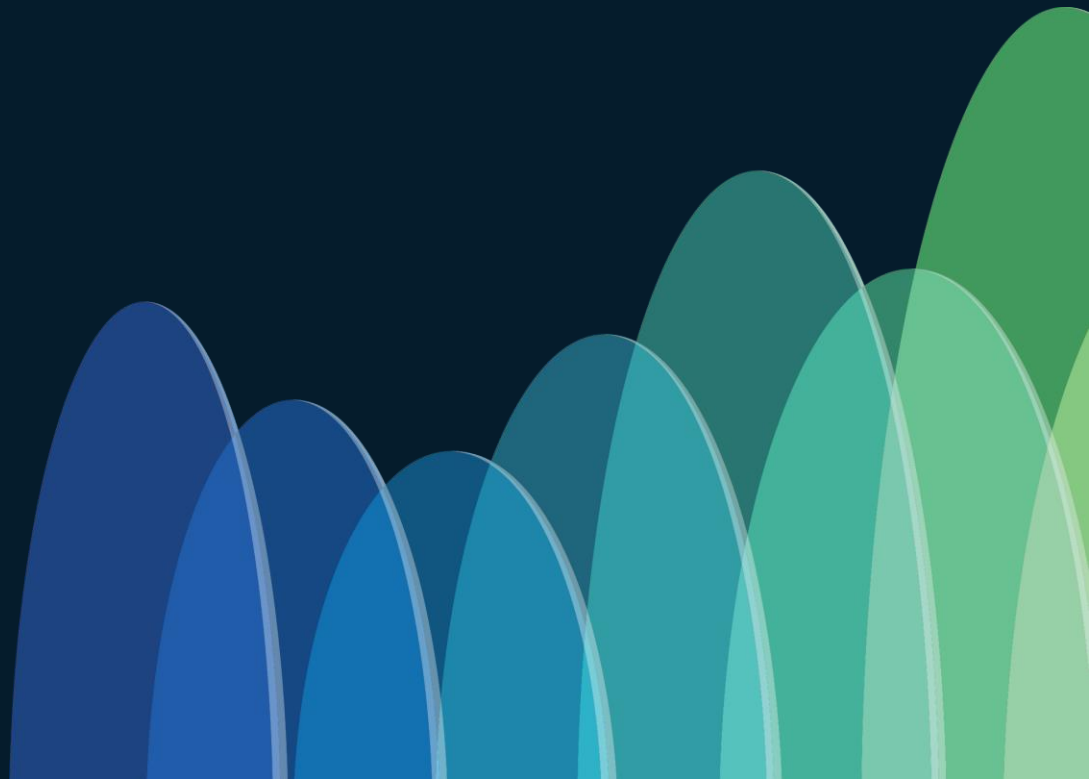
- Management system needs to validate the device
- Device needs to validate the server
- Device must validate the data is what server sent

As part of the SZTP RFC, the device supports image upgrade as part of the conveyed information

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public


c9000X#
c9000X#
c9000X#
c9000X#
c9000X#
c9000X#
c9000X#
c9000X#
c9000X#
c9000X#
c9000X#
Default (ssh)
jcohoe-c9300#
jcohoe-c9300#
jcohoe-c9300#
jcohoe-c9300#
jcohoe-c9300#
jcohoe-c9300#
jcohoe-c9300#
jcohoe-c9300#
jcohoe-c9300#
jcohoe-c9300#
jcohoe-c9300#
jcohoe-c9300#
jcohoe-c9300#
jcohoe-c9300#
jcohoe-c9300#
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$
[jcohoe@sjc-ads-2128 sztp-ssl]$

Day 1



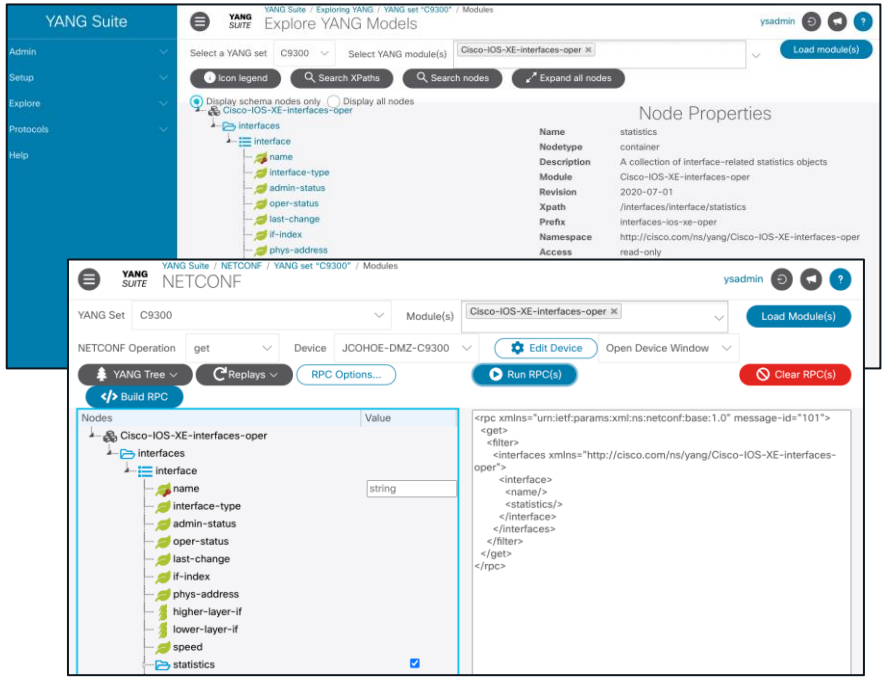
cisco Live!

Cisco YANG Suite

YANG API Testing and Validation Environment

Construct and test YANG based APIs over NETCONF, RESTCONF, gRPC and gNMI

IOS XE / IOS XR / NX OS platforms



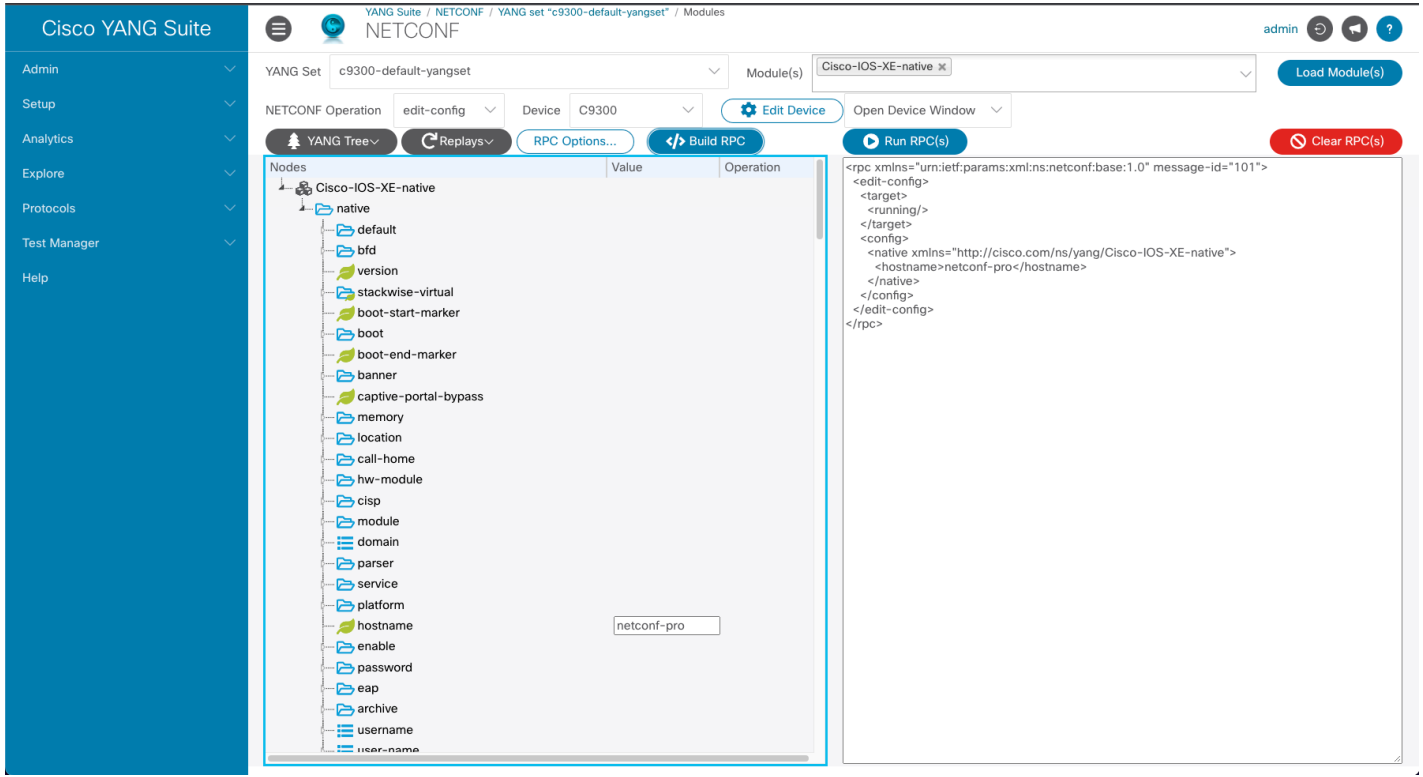
developer.cisco.com/yangsuite

github.com/CiscoDevNet/yangsuite

Get hands-on using the new learning lab!
https://developer.cisco.com/learning/labs/intro-yangsuite/
Docker container innovation 1 container

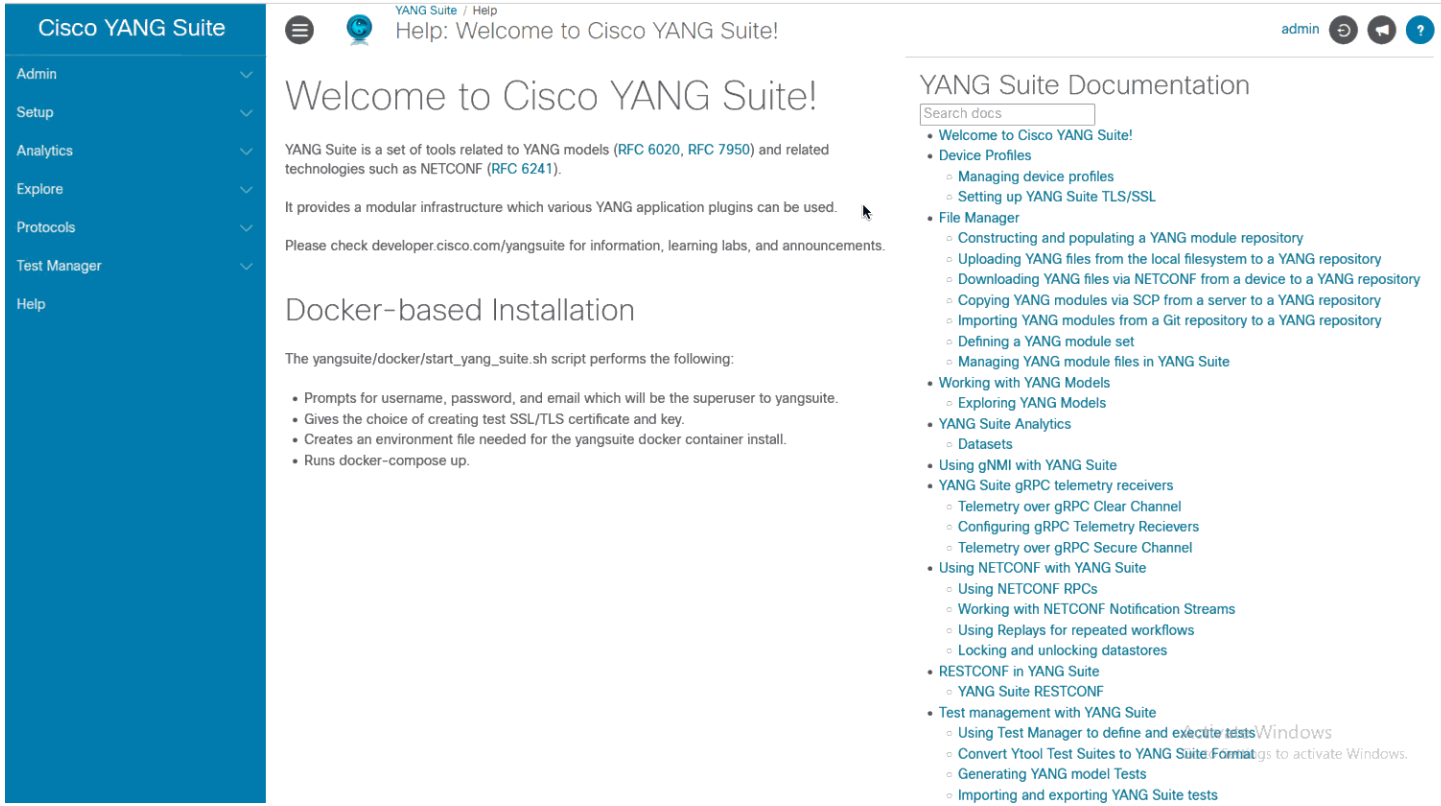
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Build NETCONF XML Payload to SET Hostname



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

YANG Suite RESTCONF Demo



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

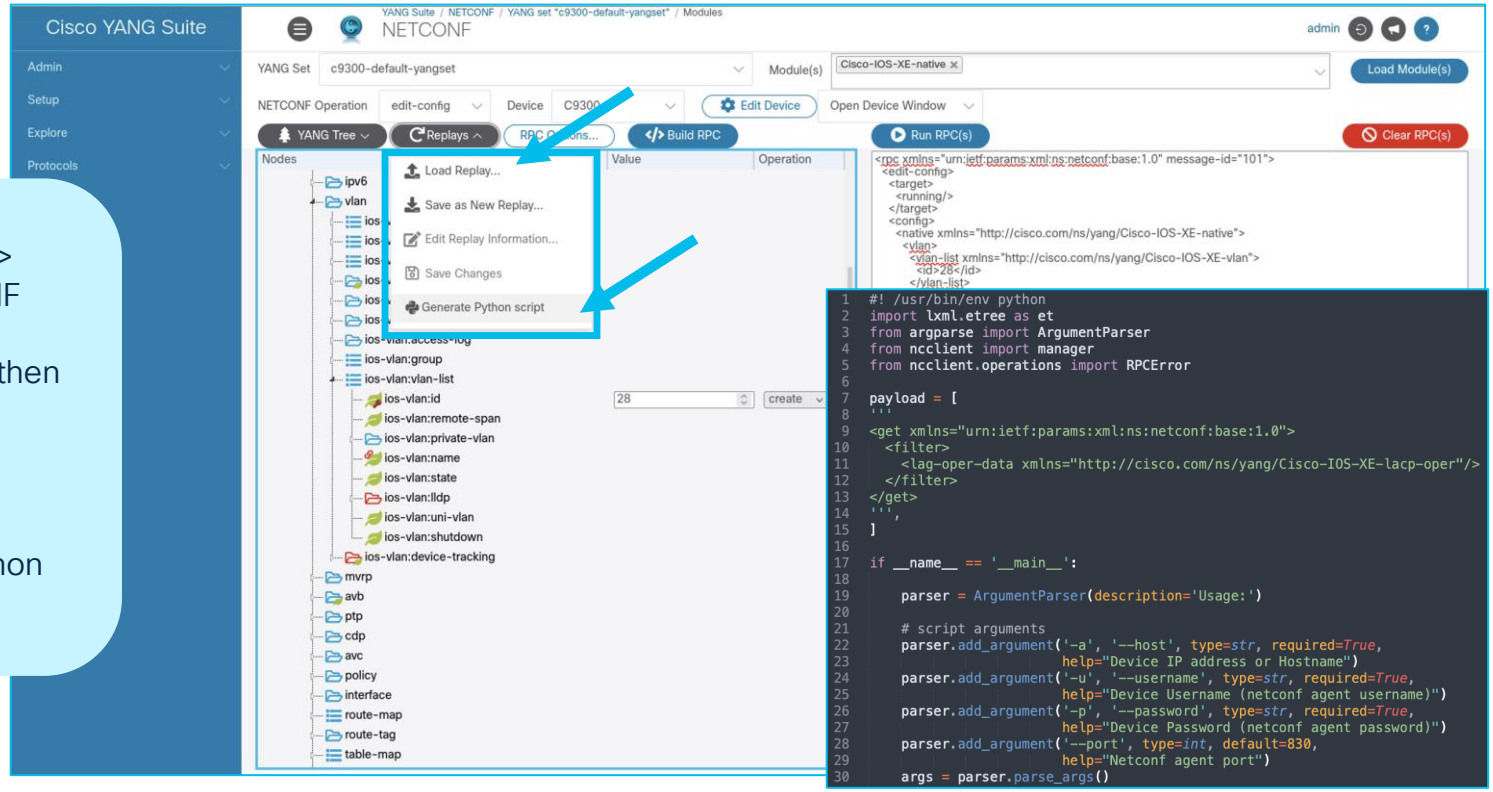
Demo: Generate Python from NETCONF

Access YANG Suite > Protocols > NETCONF

Select YANG model then Build RPC payload

Select Replays

Select Generate Python script



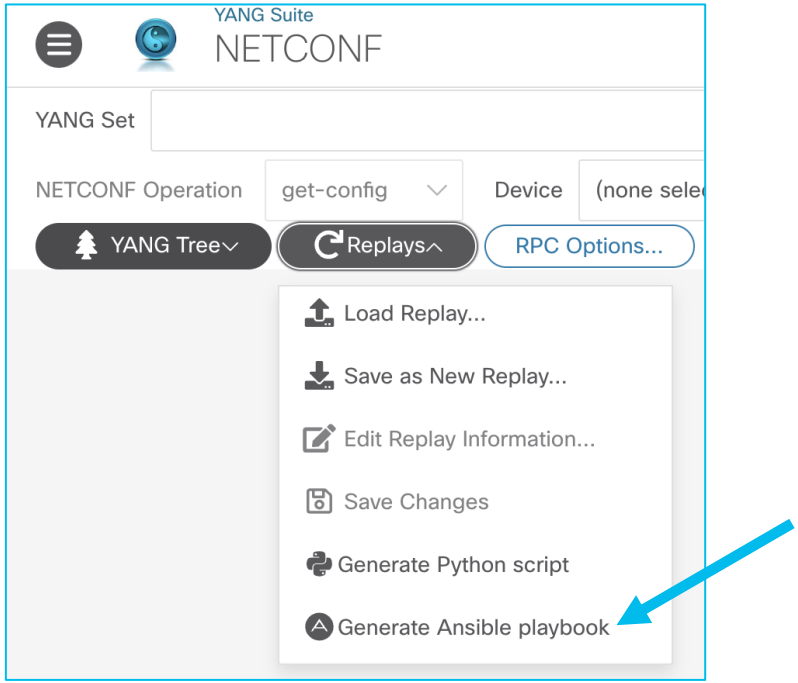
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

NETCONF + Ansible

Similar to the “Generate Python” functionality, a new functionality generates YAML formatted for Ansible.

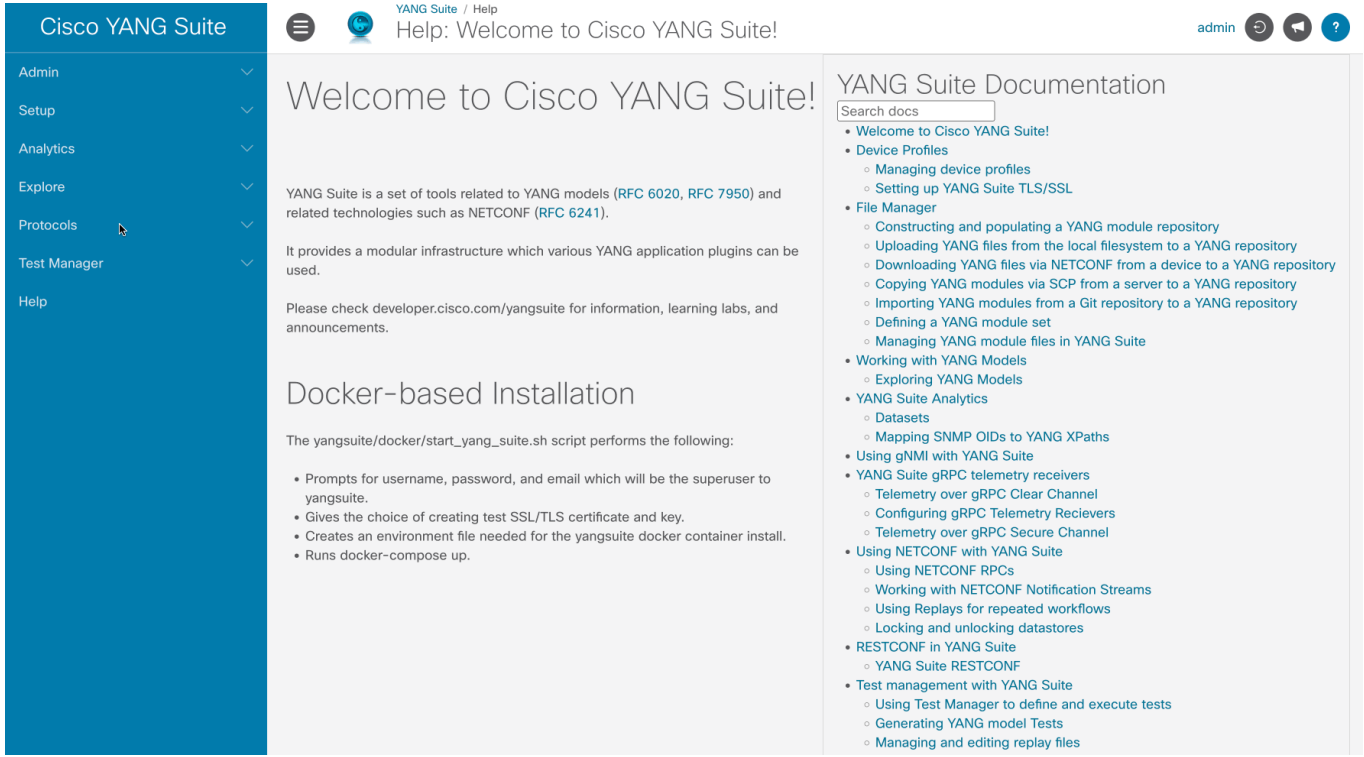
Requirements
1. Install Ansible
2. Install NETCONF collection:
   `ansible-galaxy collection install NETCONF`

```
- name : conf-host
  hosts: c9300
  connection: netconf
  gather_facts: no

  tasks:
    - name: hostname-conf
      netconf_config:
        xml: |
            <config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
              <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
                <hostname>c9300-pod29</hostname>
              </native>
            </config>
```



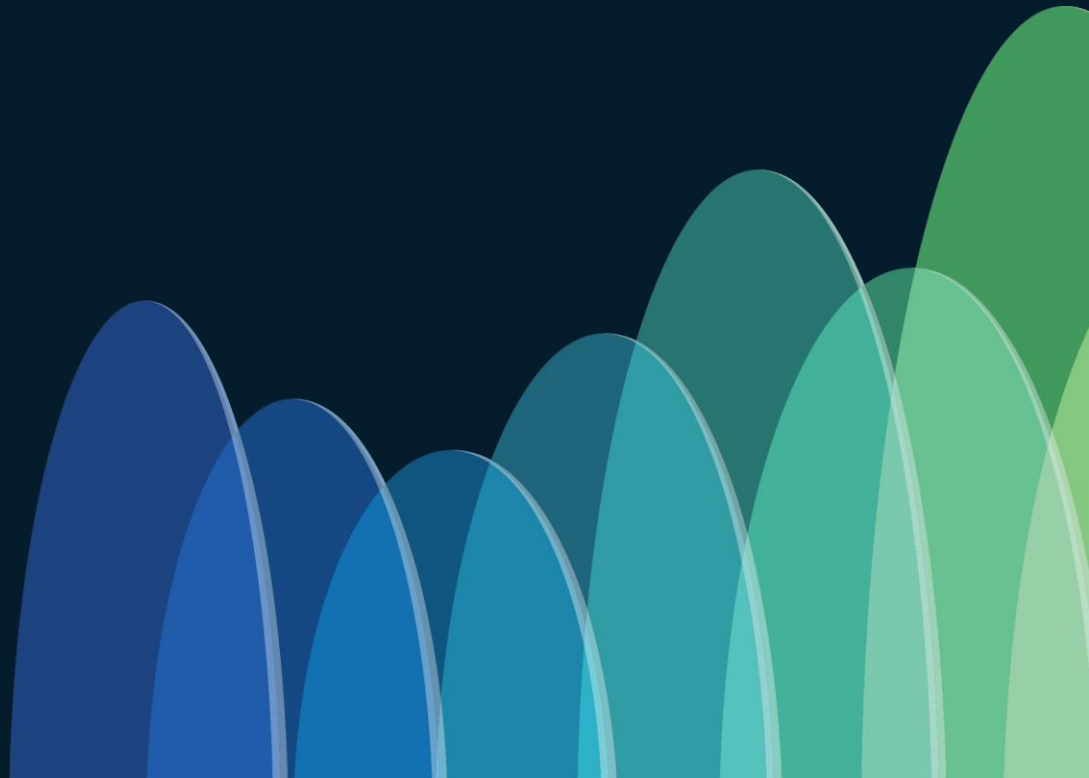
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

NETCONF + Ansible Update Interface Description Demo



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Day 2



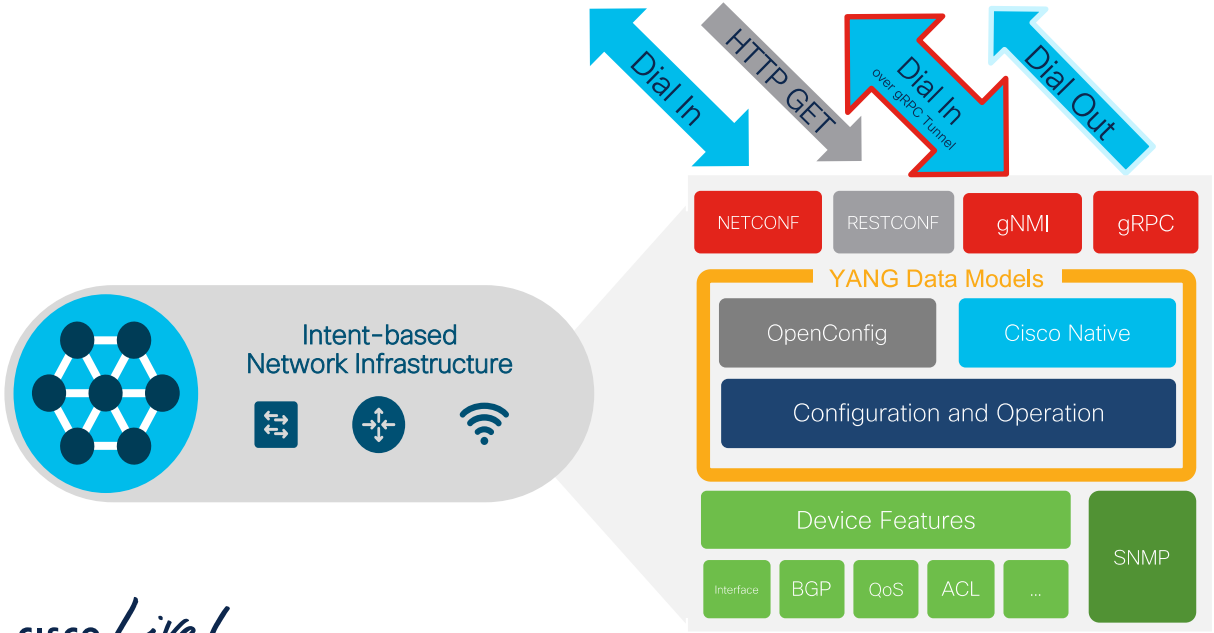
cisco Live!

Model Driven Telemetry Interfaces

Dial In: Collector establishes a connection to the device then subscribes to telemetry (pub/sub)

Dial Out: Telemetry is pushed from the device to the collector based off configuration (push)

Publication / Subscription



XML, JSON, proto and kvGPB encoding

Consistent YANG data models between interfaces

On-change event and time-based publication options

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Updated TIG_MDT container now available!

Recently updated!

```
docker pull jeremycohoe/tig_mdt
docker run -ti -p 3000:3000 -p 57500:57500 jeremycohoe/tig_mdt
```

Upgrade coming to Telegraf, Influx, and Grafana Model Driven Telemetry (TIG_MDT) Docker container
Making it easier to consume telemetry in production

Upgraded Telegraf, InlfuxDB, and Grafana tools
Additional dashboards for
Device Health, Wireless Client, Wireless AP, RF etc
Examples for device CLI configuration for telemetry
Details of scale and data storage requirements

Cisco IOS XE Devices

Collector/Receiver
Decodes to text

telegraf™

Storage
Time Series Database

InfluxDB

Monitoring and Visualizations

Grafana

https://hub.docker.com/r/jeremycohoe/tig_mdt https://github.com/jeremycohoe/cisco-ios-xe-mdt
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/179/b_179_programmability_cg/m_179_prog_ietf_telemetry.html

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

FYI

Model Driven Telemetry Interface Comparison

	NETCONF	gRPC (Dial-Out)	gNMI
Minimum IOS XE Version	16.6	16.10	Dial-In: 16.12 over gRPC tunnel: 17.11
Recommended Version	17.9	17.9	Dial-In: 17.9 over gRPC tunnel 17.11
Telemetry Direction	Dial-In, IOS XE is server	Dial-Out IOS XE is client	Dial-In IOS XE is server Dial-Out gRPC Tunnel
Configuration	Dynamic per session	Static per configuration	Dynamic per session
Telemetry Collector	Client	Server	Client
Encoding	XML	KV GPB	JSON_IETF + PROTO
Security	SSH + PKI certificate or password	mTLS or plain-text	mTLS certificates mTLS cert only or mTLS cert + user/pass authentication
Transport Protocol	SSH	HTTP2	HTTP2
Data Models	YANG	YANG	YANG

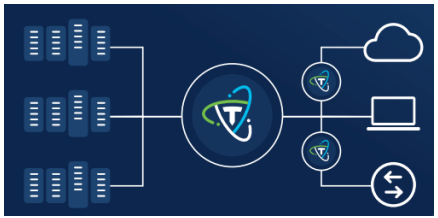
Network architecture, security posture and policy, YANG data modules, tools and language preferences, and standards, and software version, are some considerations when leveraging the various MDT interfaces

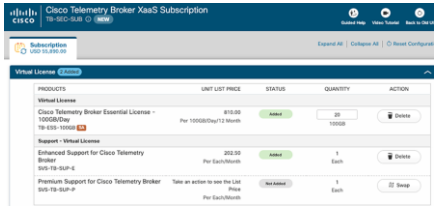
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Telemetry Data Broker (Telegraf)

Cisco Telemetry Broker provides many benefits include brokering, filtering, and transforming data. It provides the ability to replicate telemetry data.

- Cisco Secure Network Analytics (Stealthwatch) UDP Director (UDPD) replicates UDP traffic to multiple destinations.
- Cisco Telemetry Broker
  - Builds upon UDPD
  - Optimizes telemetry pipelines for the hybrid cloud
  - Simplifies the consumption of telemetry data for customers' business-critical tools by brokering hybrid cloud data, filtering unneeded data, and transforming data to a usable format





Brokering Data:
The ability to route and replicate telemetry data from a source location to multiple destination consumers.

Quickly onboard new telemetry-based tools!

Filtering Data:
The ability to filter data that is being replicated to consumers for fine grain control over what consumers are able to see and analyze.

Save money sending data to expensive tools!

Transforming Data:
The ability to transform data protocols from the exporter to the consumer's protocol of choice.

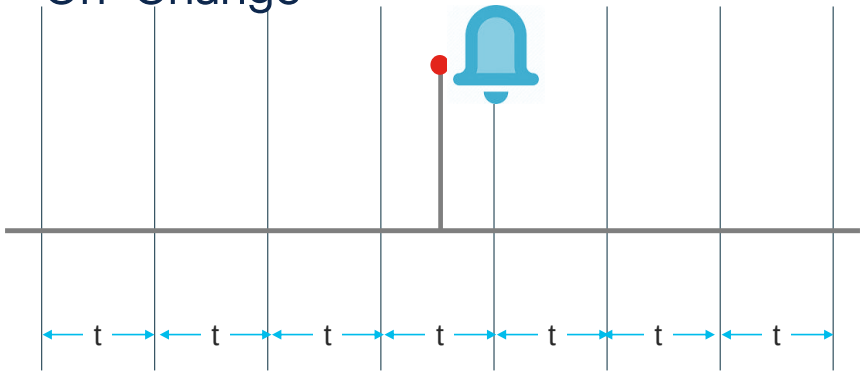
Enable tools to consume multiple data formats!

https://cs.co/telemetrybroker aka https://www.cisco.com/c/en/us/products/security/telemetry-broker/index.html
https://blogs.cisco.com/security/taking-full-control-of-your-telemetry-with-the-intelligent-telemetry-plane

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

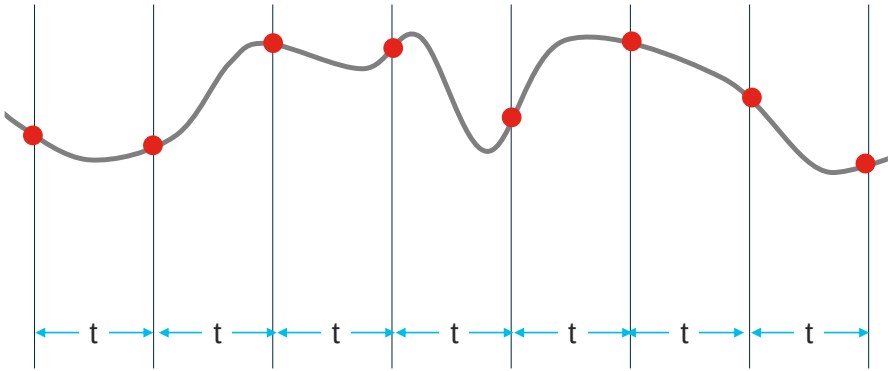
Publication options

On-Change



Feature Model “On-Change” Notifications
Event Notifications (failed login, optic fault, etc)
State and Configuration

Periodic



Feature Model “Periodic” Notifications
Time based publication
Minimum interval 100 centiseconds (1s)

OpenConfig YANG with GNXI, not NETCONF

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Configure a gRPC Telemetry Subscription

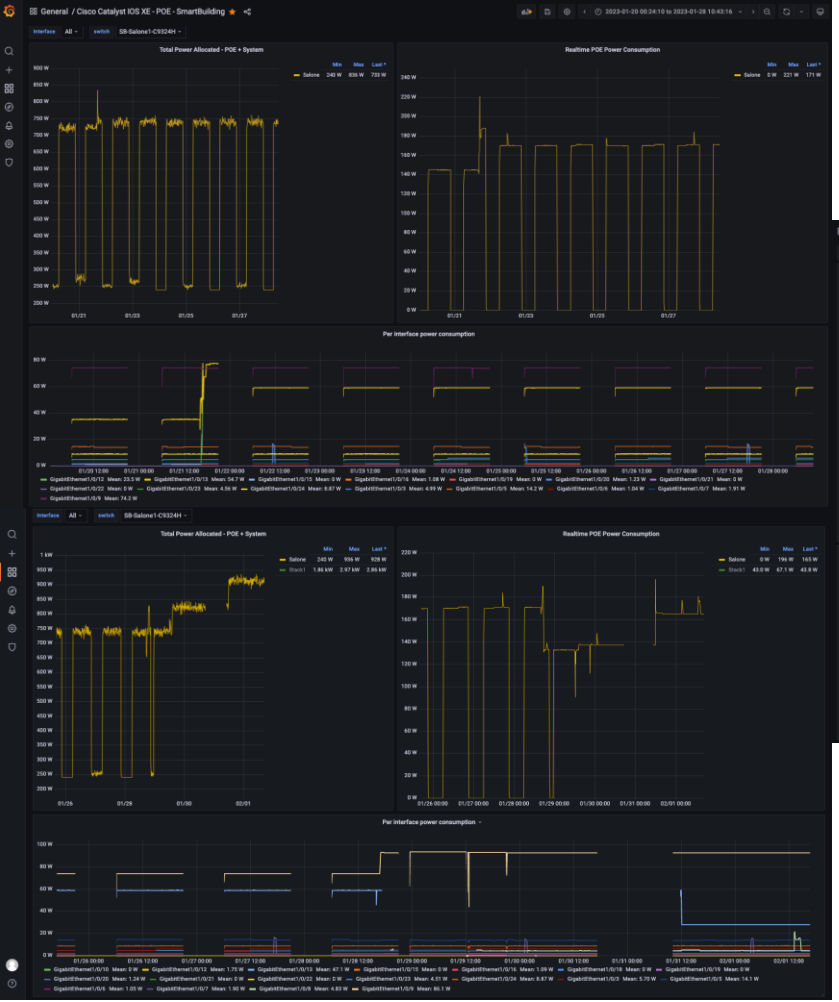
Configuring telemetry subscriptions like the following to collect CPU data over time

On Cisco IOS XE Device:

```
configure terminal
telemetry ietf subscription 1
 encoding encode-kvgpb
 filter xpath /process-cpu-ios-xe-oper:cpu-usage/cpu-utilization
 stream yang-push
 update-policy periodic 60000
 receiver ip address 10.1.1.3 57500 protocol grpc-tcp
```

See more examples at: https://github.com/jeremycohoe/cisco-ios-xe-mdt

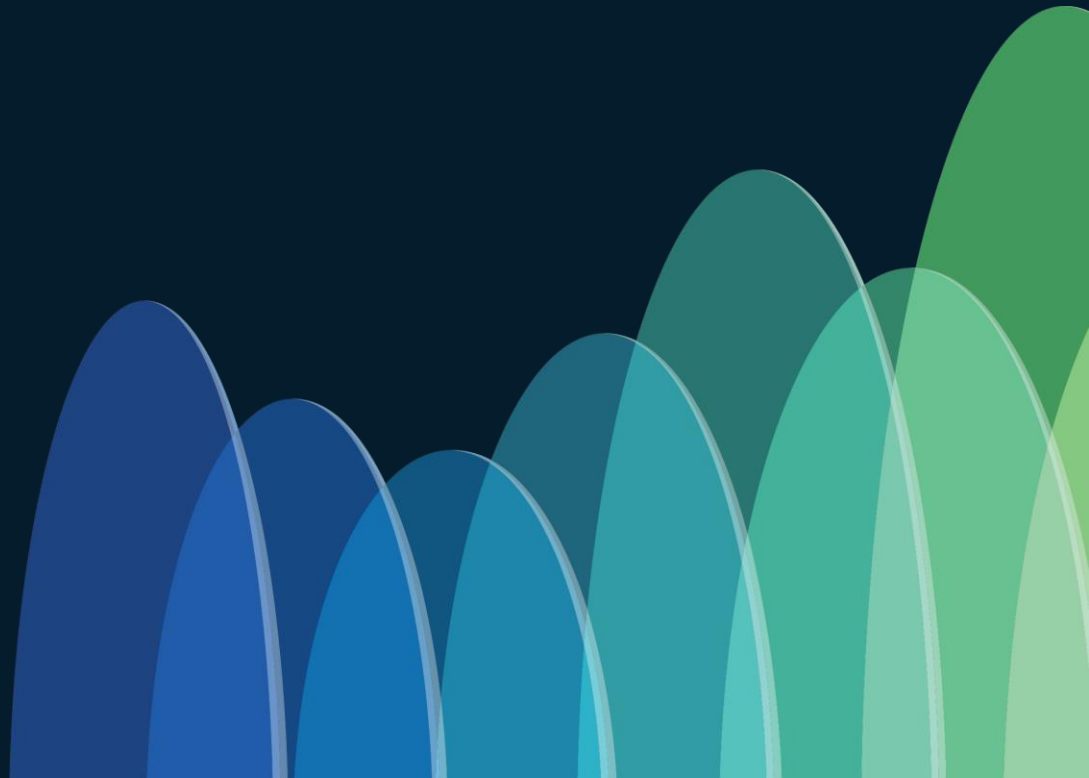
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



Interested in learning more?
Attend tomorrow's sustainability session
BRKAPP-2245

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Day N



cisco Live!

gNOI – gRPC Network Operations Interface

1. gRPC Network Operations Interface, or gNOI, is a set of gRPC-based microservices, used for executing operational commands on network devices
2. gNOI operations are executed against the gNMI API interface
3. gNOI is defined and implemented on a per proto basis
4. There are many protos defined - some are more mature and evolve and different pace

Protobuf RPC	Use	Related CLI	Release
Cert.proto	TLS Certificate management	`crypto pki …`	17.3
Os.proto	Network Operating System management	`install add file …`	17.5
Reset.proto	Factory Reset and secure wipe	`write erase …`	17.7
File.proto	Not implemented on IOS XE, use YANG	`copy, delete`	N/A
System.proto	Not implemented on IOS XE, use YANG	`reload, set boot`	N/A

https://github.com/openconfig/gnoi
https://github.com/jeremycohoe/cisco-catalyst-gnoi-reset.proto Factory Reset API Lab Guide
https://github.com/jeremycohoe/cisco-catalyst-gnoi-cert.proto Certificate Management API Lab Guide
https://www.youtube.com/watch?v=cGxgBAlefOQ GNOI OS.proto - Operating System API demo

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

GNOI OS.proto demo

```
jcohoe@jcohoe-ubuntu18-lab:~$ cd ~/certs-jcohoe-c9300-2/ ; gnoi_os -insecure -target_addr 10.85.134.92:9339 -op install -target_name c9300 -alsologtostderr -cert ./cli
ent.crt -ca ./rootCA.pem   -key ./rootCA.key -version 17.06.01.0.135639.1618187331 -time_out 999s -os /tftpboot/cat9k_iosxe.17.06.01-20210411.bin
jcohoe@jcohoe-ubuntu18-lab:~/certs-jcohoe-c9300-2$ cd
jcohoe@jcohoe-ubuntu18-lab:~$
jcohoe@jcohoe-ubuntu18-lab:~$ cd ~/certs-jcohoe-c9300-2/ ; gnoi_os -insecure -target_addr 10.85.134.92:9339 -op activate -target_name c9300 -alsologtostderr -cert ./cl
ient.crt -ca ./rootCA.pem   -key ./rootCA.key -version 17.06.01.0.135639.1618187331 -time_out 999s -os /tftpboot/cat9k_iosxe.17.06.01-20210411.bin
jcohoe@jcohoe-ubuntu18-lab:~/certs-jcohoe-c9300-2$
jcohoe@jcohoe-ubuntu18-lab:~/certs-jcohoe-c9300-2$ cd ~/certs-jcohoe-c9300-2/ ; gnoi_os -insecure -target_addr 10.85.134.92:9339 -op verify -target_name c9300 -alsolog
tostderr -cert ./client.crt -ca ./rootCA.pem   -key ./rootCA.key
I0418 11:57:10.555504   29388 gnoi_os.go:98] Running OS version: 17.06.01.0.135639.1618187331
jcohoe@jcohoe-ubuntu18-lab:~/certs-jcohoe-c9300-2$
```

```
telnet
C9300#
*Apr 18 18:29:46.613: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine: Started install remove
*Apr 18 18:32:09.394: %PLATFORM_FEP-1-FRU_PS_ACCESS: Switch 1: power supply A is not responding
*Apr 18 18:32:11.246: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_engine: Completed install remove
*Apr 18 18:35:21.621: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine: Started install add flash:gNOI_iosxe_17.06.01.0.135639.1618187331.bin
*Apr 18 18:38:28.711: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_engine: Completed install add PACKAGE flash:gNOI_iosxe_17.06.01.0.135639.1618187331.bin
*Apr 18 18:38:58.711: %ISSU-3-ISSU_COMP_CHECK_FAILED: Switch 1 R0/0: install_engine: ISSU compatibility check failed for 17.06.01.0.135639
C9300#
C9300#
*Apr 18 18:44:28.608: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine: Started install activate
*Apr 18 18:44:28.608: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0: install_mgr: Install auto abort timer will expire in 7200 seconds
```

```
C9300#show gnxi os summary
Mode: Install Mode
Current Operation: No operation in progress
No image has been added as Inactive
Current Activated Version: 17.05.01.0.144.1617180620
C9300#show gnxi os summary
Mode: Install Mode
Current Operation: No operation in progress
No image has been added as Inactive
Current Activated Version: 17.06.01.0.135639.1618187331
Last Executed RPC: Verify, Success
```

Demo video on YouTube

Verify:
cd ~/certs-jcohoe-c9300-2/ ; gnoi_os -insecure -target_addr 10.85.134.92:9339 -op verify -target_name c9300 -alsologtostderr -cert ./client.crt -ca ./rootCA.pem -key ./rootCA.key
Running OS version: 17.05.01.0.144.1617180620

Install:
cd ~/certs-jcohoe-c9300-2/ ; gnoi_os -insecure -target_addr 10.85.134.92:9339 -op install -target_name c9300 -alsologtostderr -cert ./client.crt -ca ./rootCA.pem -key ./rootCA.key -version 17.06.01.0.135639.1618187331 -time_out 999s -os /tftpboot/cat9k_iosxe.17.06.01-20210411.bin

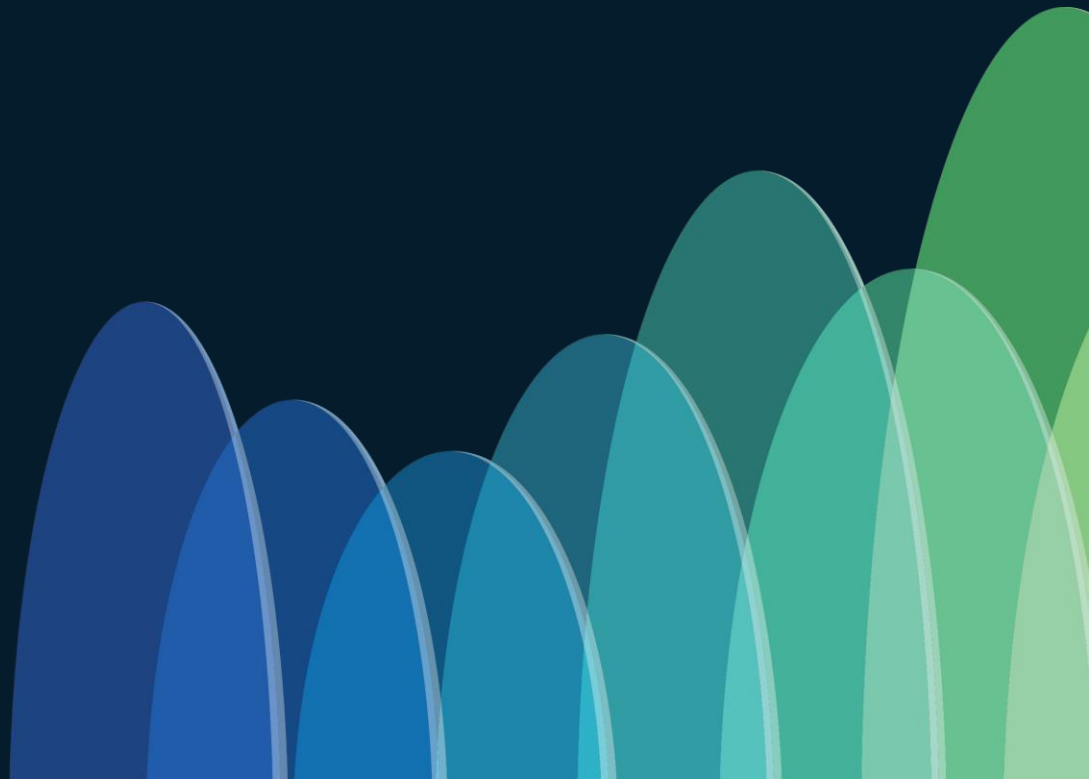
Activate:
cd ~/certs-jcohoe-c9300-2/ ; gnoi_os -insecure -target_addr 10.85.134.92:9339 -op activate -target_name c9300 -alsologtostderr -cert ./client.crt -ca ./rootCA.pem -key ./rootCA.key -version 17.06.01.0.135639.1618187331 -time_out 999s -os /tftpboot/cat9k_iosxe.17.06.01-20210411.bin

Verify:
Running OS version: 17.06.01.0.135639.1618187331

show CLI: show gnxi os summary

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Tooling

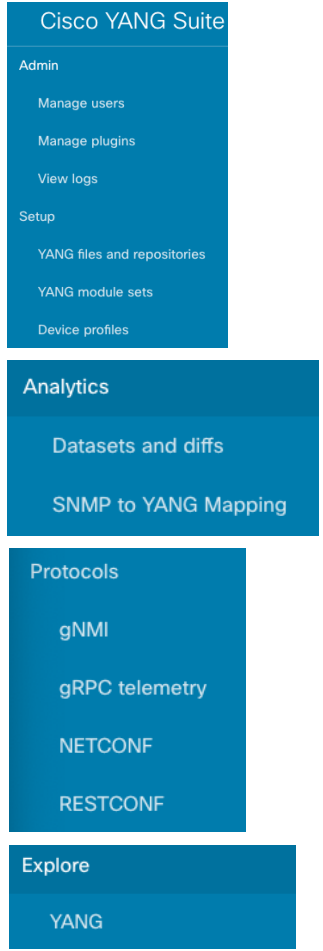


YANG Suite Capabilities

- Initial Release:
  - Plugin and YANG File Manager, Datasets and diffs
  - Device Manager
  - NETCONF (Python), gRPC Telemetry
  - Docker install support with HTTPS
- Second Release:
  - RESTCONF
  - gNMI
  - Python Integrations
- Third Release:
  - gRPC Telemetry with TLS Support
  - SNMP OID to YANG Xpath Mapping
  - Ansible Integrations
  - Pip install support

Core plugins

Additional plugins



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is Ansible?

- Open-source configuration management tool
- Commercially supported by Red Hat
- Declarative and idempotent
- Ansible can be Imperative when needed
- Can manage a wide range of systems:
  VMs, network devices, cloud instances, etc.
- Agentless: no requirement for installation of application software to run
- Has Python server-side dependencies

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

They can coexist… it's not an either/or story

- Terraform keeps state locally
- Terraform knows what is configured vs desired end-state
- Terraform can automatically destroy/recreate resources

- Ansible mutates the infrastructure
- Ansible does not keep state (mostly)
- Terraform can call Ansible to perform tasks post resource deployment (e.g., on VMs deployed)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Create a MDT Subscription using Ansible

CLI

```
configure terminal
telemetry ietf subscription 1
 encoding encode-kvgpb
 filter xpath /process-cpu-ios-xe-oper:cpu-usage/cpu-utilization
 stream yang-push
 update-policy periodic 60000
 receiver ip address 10.1.1.3 57500 protocol grpc-tcp
```

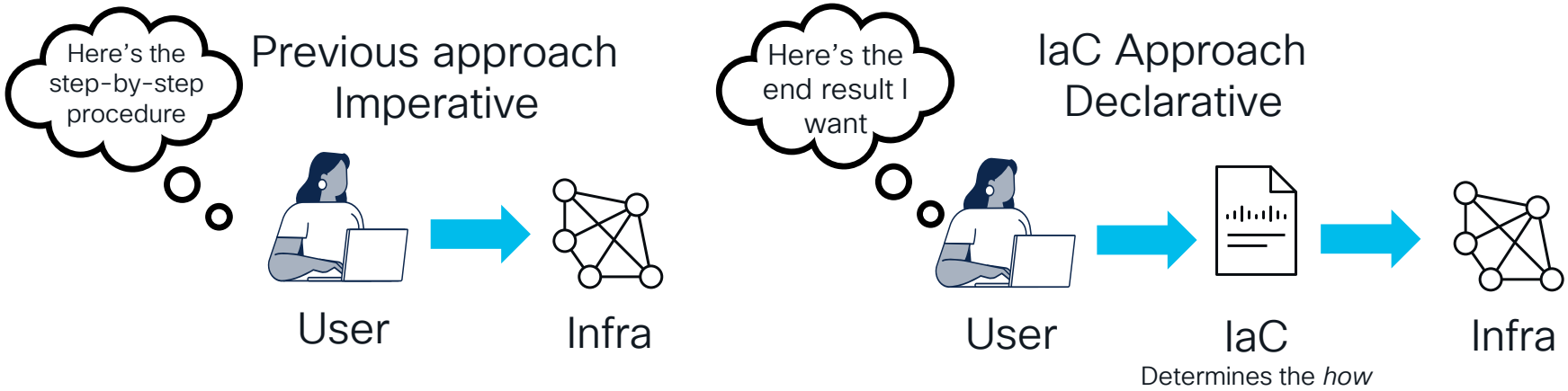
```
- name: add telemetry subscriptions
  hosts: c9300
  connection: netconf
  gather_facts: no

  tasks:
  - name: establish subscription
    netconf_config:
      xml: |
        <config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
          <mdt-config-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-mdt-cfg">
            <mdt-subscription>
              <subscription-id>1</subscription-id>
              <base>
                <stream>yang-push</stream>
                <encoding>encode-kvgpb</encoding>
                <source-address>10.1.1.5</source-address>
                <source-vrf>Mgmt-vrf</source-vrf>
                <period>2000</period>
                <xpath>/process-cpu-ios-xe-oper:cpu-usage/cpu-utilization/five-seconds</xpath>
              </base>
              <mdt-receivers>
                <address>10.1.1.3</address>
                <port>57500</port>
                <protocol>grpc-tcp</protocol>
              </mdt-receivers>
            </mdt-subscription>
          </mdt-config-data>
        </config>
```

https://github.com/jeremycohoe/ansible-config-samples/blob/master/add_sub_17.7.yaml

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What's IaC?

Infrastructure as Code (IaC) is the process of managing changes through code, rather than a manual process



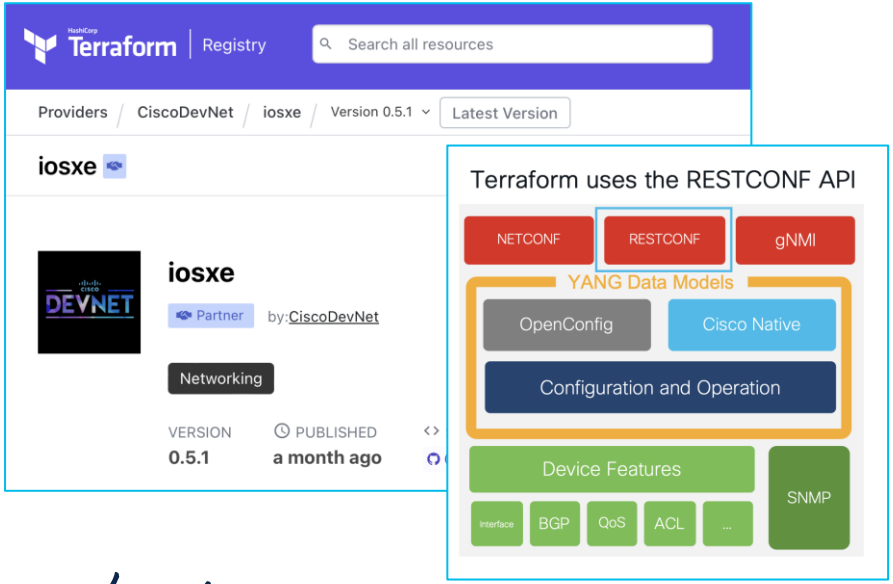
Learn more about IaC here:
https://developer.cisco.com/iac/#:~:text=Adopting%20Infrastructure%20as%20Code%20allows,data%20center%20to%20the%20edge.

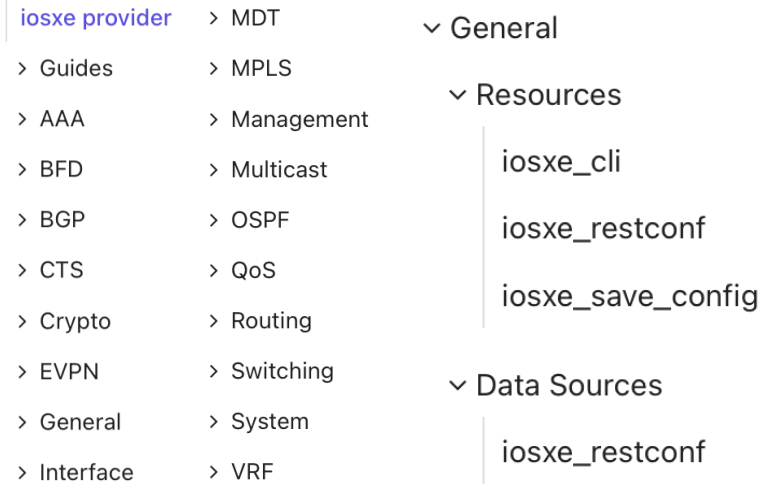
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS XE Terraform Provider

Infrastructure as Code (IaC) Software Tool providing a consistent CLI workflow to manage hundreds of cloud services. Terraform codifies cloud APIs into declarative configuration files.

Documentation and details about the provider are available on the Hashicorp Registry
https://registry.terraform.io/providers/CiscoDevNet/iosxe/latest
Source code in GitHub Repository: https://github.com/CiscoDevNet/terraform-provider-iosxe/





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Terraform for Model Driven Telemetry

Enable gRPC Dial-Out telemetry subscriptions for the POE and Basic Device Monitoring use cases

```
auto@pod22-xelab:~/mdt_example$ terraform plan -var-file="var.tfvars"

Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the following symbols:
  + create

Terraform will perform the following actions:

  # iosxe_mdt_subscription.cpu_subs["100"] will be created
  + resource "iosxe_mdt_subscription" "cpu_subs" {
      + encoding          = "encode-kvgpb"
      + filter_xpath      = "/process-cpu-ios-xe-oper:cpu-usage/cpu-utilization/five-seconds"
      + id                = (known after apply)
      + receivers         = [
          + {
              + address  = "10.1.1.3"
              + port     = 57500
              + protocol = "grpc-tcp"
            },
        ]
      + stream            = "yang-push"
      + subscription_id   = 100
      + update_policy_periodic = 3000
    }

  # iosxe_mdt_subscription.cpu_subs["101"] will be created
  + resource "iosxe_mdt_subscription" "cpu_subs" {
      + encoding          = "encode-kvgpb"
      + filter_xpath      = "/process-cpu-ios-xe-oper:cpu-usage/cpu-utilization/one-minute"
      + id                = (known after apply)
      + receivers         = [
          + {
              + address  = "10.1.1.3"
              + port     = 57500
              + protocol = "grpc-tcp"
            },
        ]
      + stream            = "yang-push"
      + subscription_id   = 101
      + update_policy_periodic = 3000
    }
```

Lab Guide Steps:

1. Introduction
2. IOS XE CLI pre-req
3. Terraform Install & headers, device variables
4. Variables and config for MDT subscription
5. Terraform configuration for device monitoring
6. TF Workflow: init, plan, apply & destroy
7. Validation with TF and CLI
8. Conclusion

iosxe_mdt_subscription (Resource)

This resource can manage the MDT Subscription configuration.

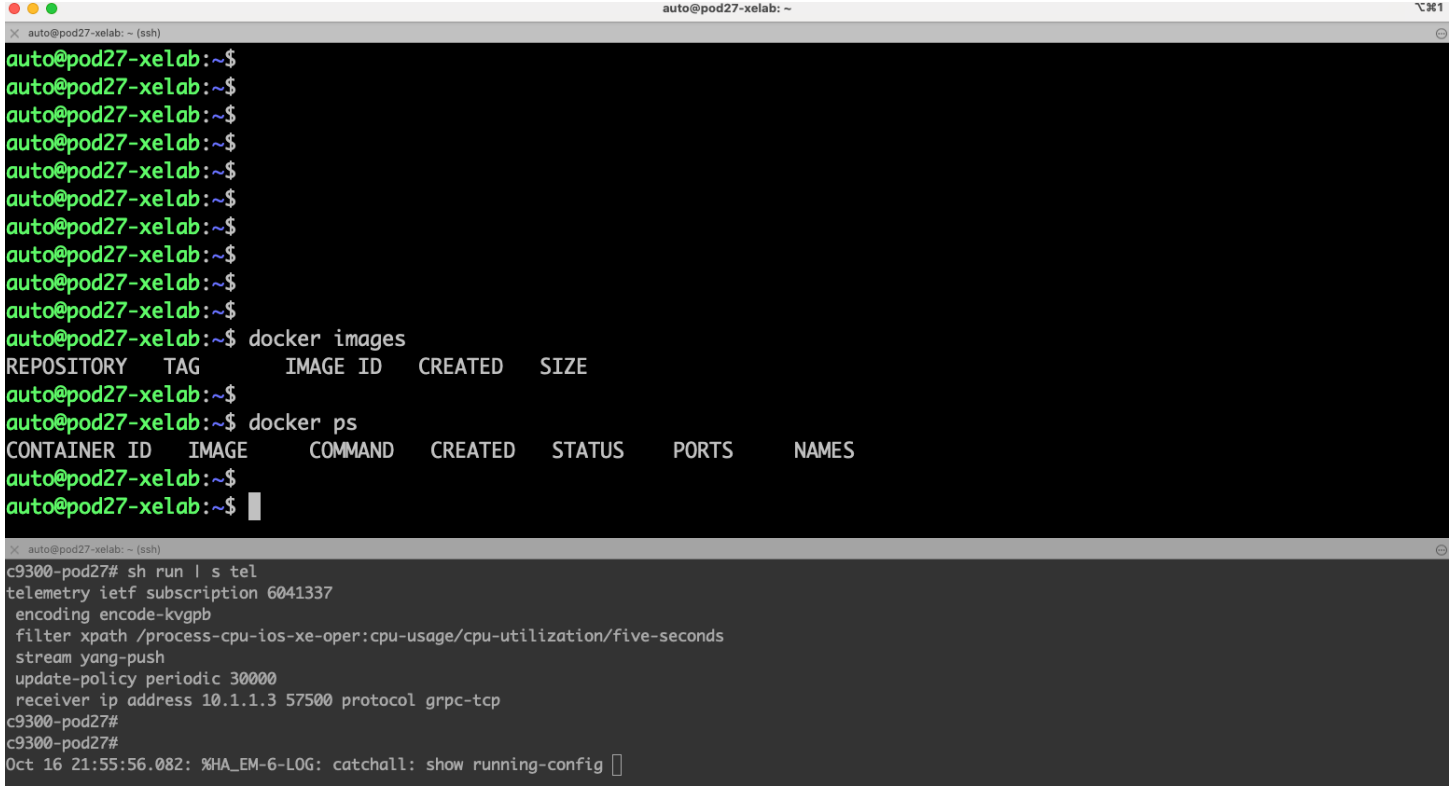
Example Usage

```
resource "iosxe_mdt_subscription" "example" {
  subscription_id         = 101
  stream                  = "yang-notif-native"
  encoding                = "encode-kvgpb"
  source_vrf              = "Mgmt-vrf"
  source_address          = "1.2.3.4"
  update_policy_on_change = true
  filter_xpath            = "/ios-events-ios-xe-oper
  receivers = [
    {
      address  = "5.6.7.8"
      port     = 57600
      protocol = "grpc-tcp"
    }
  ]
}
```

https://registry.terraform.io/providers/CiscoDevNet/iosxe/latest/docs/resources/mdt_subscription
https://registry.terraform.io/providers/CiscoDevNet/iosxe/latest/docs/data-sources/mdt_subscription
https://github.com/jeremycohoe/cisco-ios-xe-panda-lab-terraform

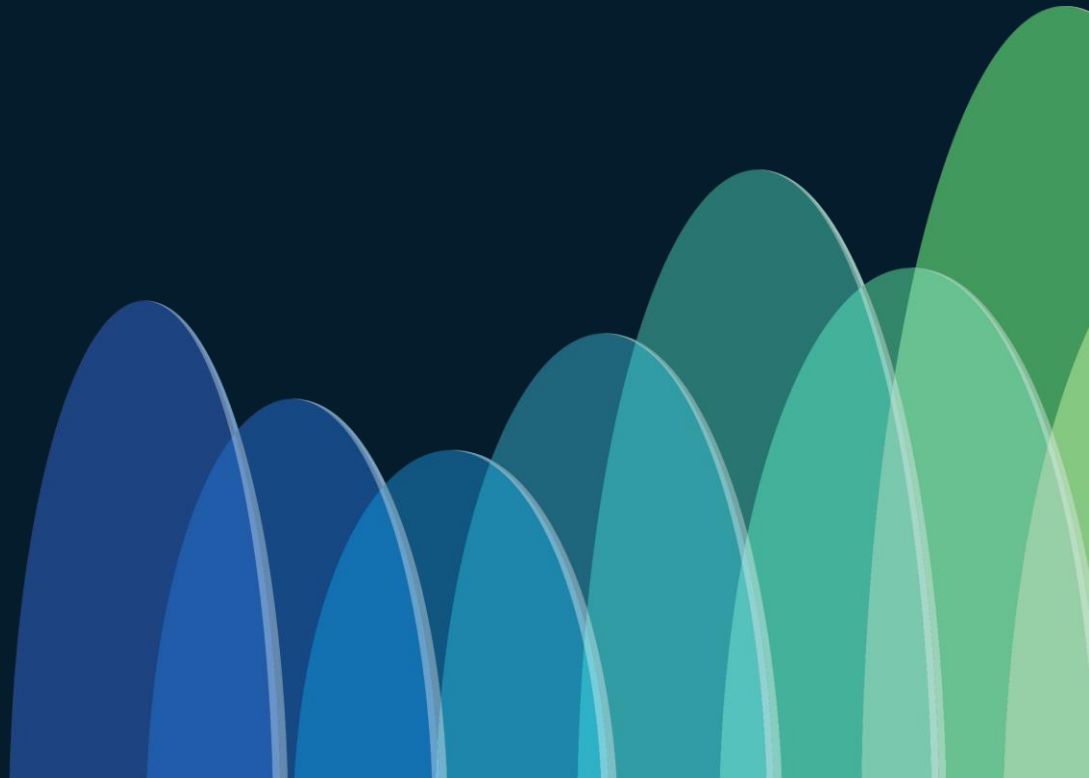
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

DEMO – install docker container and use Terraform files to configure telemetry subscriptions



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Resources



Cisco Catalyst Programmability Sessions at Cisco Live APJC 2024

Sunday Nov 10	Monday Nov 11	Tuesday Nov 12	Wednesday Nov 13	Thursday Nov 14
Session Levels: Beginner Intermediate	4:15 PM DEVNET-2385 Atomic Config Replace with Cisco Catalyst 9000	2:00 PM DEVNET-1249 Secure Zero Touch Provisioning (SZTP) with Cisco Catalyst Switches	11:30 AM DEVNET-1283 Programmability, Automation Model Driven Telemetry on Cisco IOS XE with a dash of YANG Suite?	8:30 AM BRKAPP-2245 Programmability on Catalyst 9000 enabling Sustainability Telemetry Dashboards

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure ZTP Blog

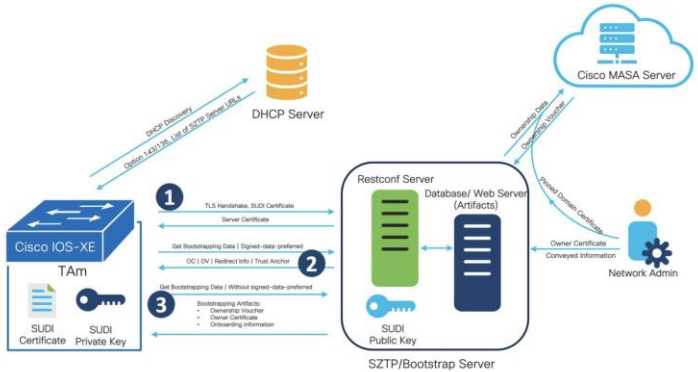
Developer

Building Trust from the Ground Up: The Role of Secure ZTP in Zero Trust Networks

6 min read

Ashil Parekh

Secure ZTP employs three-step validation, including device validation, server validation, and artifact validation, to securely onboard the device. The diagram provided below illustrates the various steps involved in the device onboarding and provisioning process within a secure ZTP framework. Let's take a closer look at each of these steps:



https://blogs.cisco.com/developer/secureztp01

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

ZTP in Action

Start the hands-on lab for Day 0

Module: Zero Touch Provisioning

In this module, you will verify and confirm the prerequisites for Zero Touch Provisioning (ZTP), the feature of IOS XE on the Catalyst 9300 switch. At the end of this module, you will issue the 'write erase' command, reload the switch, and watch as the ZTP process completes and the switch is configured programmatically and automatically.

What is ZTP? When a device that supports Zero-Touch Provisioning boots up, and does not find the startup configuration (during initial installation), the device enters the Zero-Touch Provisioning mode. The device searches for an IP from a DHCP server and bootstraps itself by enabling the Guest Shell. The device then obtains the IP address or URL of an HTTP/TFTP server, and downloads a Python script from an server to configure the device.

```
write erase
reload
```

ping

https://github.com/sdeweese/CLUS22-LTROPS-1836-programmabilty-and-automation/blob/main/ZTP2.md

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Open Programmable Infrastructure (OPI) SZTP

Ready to create your own bootstrapping server, consider the OPI one to get started

Device Getting Onboarding Information

Read the configuration back and validate it is correct:

```
docker run --rm --network sztp_opi docker.io/curlimages/curl:8.5.0 --silent --fail-with-body -
```

Get onboarding info (from device perspective)

```
$ docker run --rm --user 0 --network sztp_opi -v sztp_clie
{
  "ietf-sztp-bootstrap-server:output": {
    "conveyed-information": "MIIDfwYLKoZIhvcNAQkQASugggNul
  }
}
```

Decode payload

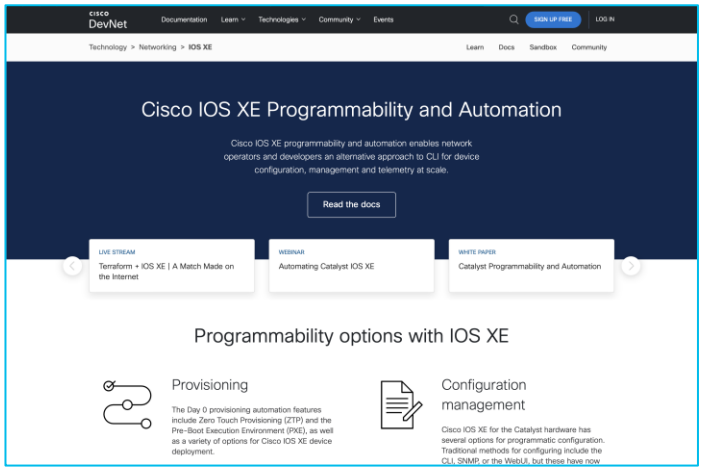
```
$ jq -r .\"ietf-sztp-bootstrap-server:output\".\"conveyed-information\" /tmp/post_rpc_input.js
{
  "ietf-sztp-conveyed-info:onboarding-information": {
    "boot-image": {
      "download-uri": [
        "https://web:443/my-boot-image.img",
        "ftps://web:990/my-boot-image.img"
      ],
      "image-verification": [
        {
          "hash-algorithm": "ietf-sztp-conveyed-info:sha-256",
          "hash-value": "7b:ca:e6:ac:23:06:d8:79:06:8c:ac:03:80:e2:16:44:7e:40:6a:65:fa:d4:69:
        }
      ]
    },
    "pre-configuration-script": "IyEvYmluL2Jhc2gKZWNobyAiaW5zaWRlIHRoZSBwcmUtY29uZmlndXJhdGlvb
    "configuration-handling": "merge",
    "configuration": "PHRvcCB4bWxucz0iaHR0cHM6L2V4YW1wbGUuY29tL2NvbmZpZyI+CiAgPGFueS14bWwtY29u
    "post-configuration-script": "IyEvYmluL2Jhc2gKZWNobyAiaW5zaWRlIHRoZSBwb3N0LWNvbmZpZ3VyYXRp
  }
}
```

https://github.com/opiproject/sztp

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Programmability Website

The one-stop-shop for Cisco IOS XE Programmability resources including videos, white papers, labs and more!



- Community Forum
- IOS XE FAQ
- White Papers
- Code Exchange
- IOS XE Docs & Guide
- Learning Tracks and Labs
- Sandboxes
  - … and more !

https://developer.cisco.com/iosxe/

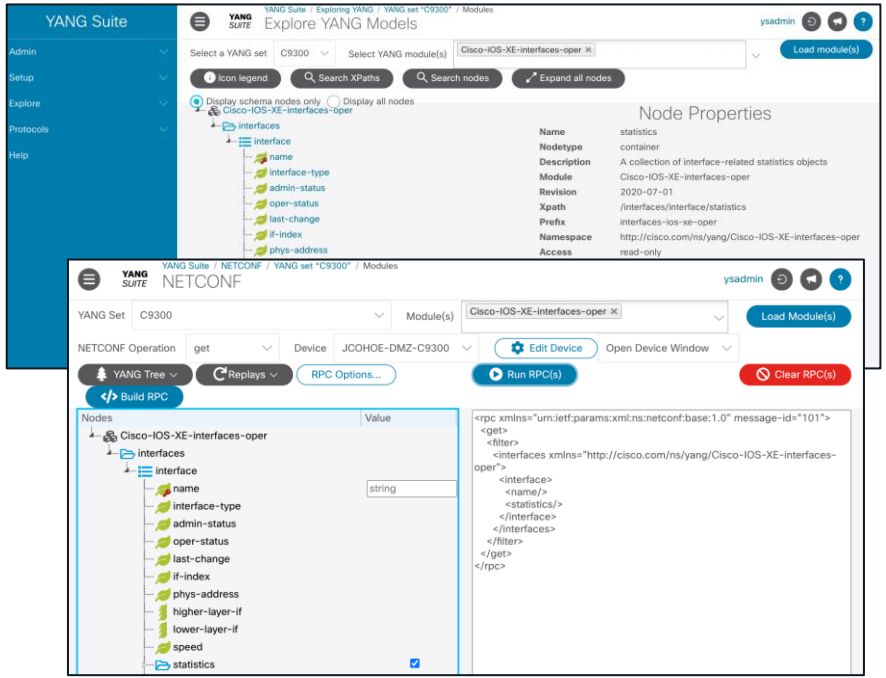
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco YANG Suite

YANG API Testing and Validation Environment

Construct and test YANG based APIs over NETCONF, RESTCONF, gRPC and gNMI

IOS XE / IOS XR / NX OS platforms



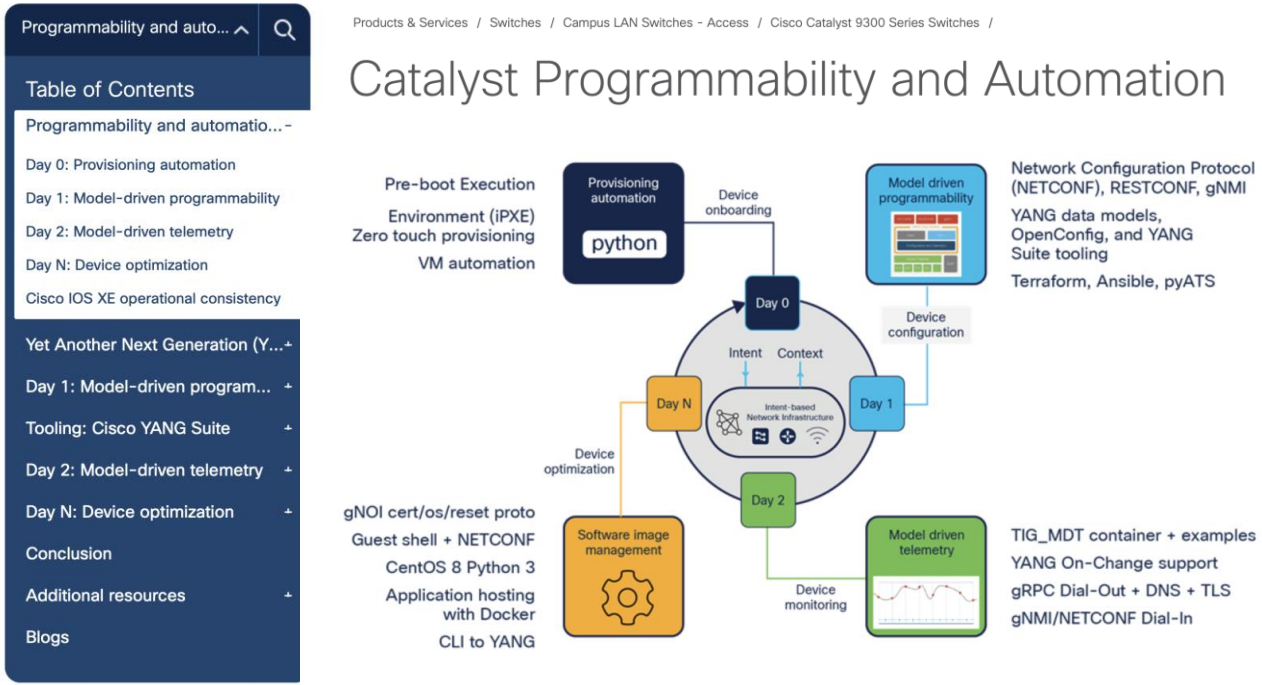
developer.cisco.com/yangsuite

github.com/CiscoDevNet/yangsuite

Get hands-on using the new learning lab!
https://developer.cisco.com/learning/labs/intro-yangsuite/
Docker container innovation 1 container

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

API White Paper



Website: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-catalyst-programmability-automation-wp.html
PDF: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-catalyst-programmability-automation-wp.pdf
Webinar with live demos & examples: https://www.youtube.com/watch?v=LdcK5PnPu2I

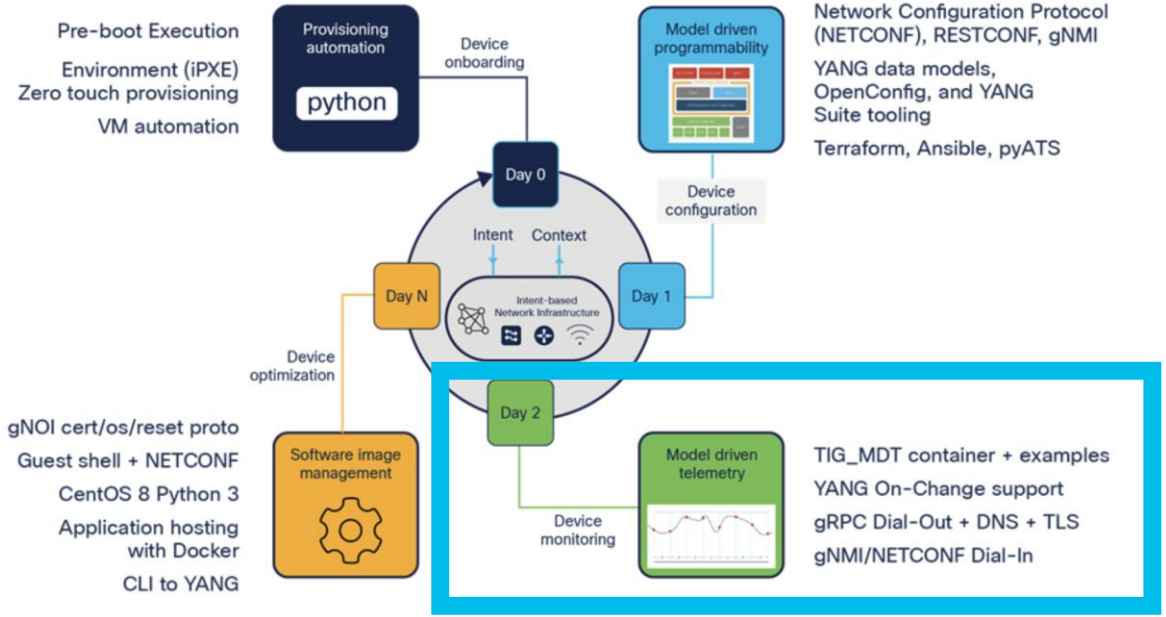
http://cs.co/apiwp

http://cs.co/apiwppdf

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Model Drive Telemetry (MDT) White Paper

The Model Driven Telemetry White Paper includes examples, use cases and tooling related to telemetry. This paper is now available online and in PDF form!



Website

PDF

View online: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/model-driven-telemetry-wp.html
View as PDF: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/model-driven-telemetry-wp.pdf

Introduction to Cisco IOS ...

Table of Contents

- Introduction to Cisco IOS XE
- Introduction to telemetry
- Benefits of model driven tele...
- Network monitoring challeng...
- Architecture and databases
- Dial-in and dial-out MDT +
- Publication notification optio...
- YANG data modeling language +
- Benchmarking and comparis... +
- Cisco controller solutions +
- Cloud solutions +
- Tooling +
- Dashboarding and validation +
- Configuration examples +
- Telemetry configuration man... +
- Troubleshooting and validati... +
- Best practices and lessons l... +
- Conclusion
- Resources

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

dCloud Programmability

https://dcloud.cisco.com
"Cisco Catalyst 9000 IOS XE Programmability & Automation Lab v1"
https://dcloud2.cisco.com/demo/catalyst-9000-ios-xe-programmability-automation-lab-v1

Use Cases:

EVPN:
Ansible with CLI deployment of EVPN solutions
EVPN management over RESTCONF/YANG with Postman
Declarative EVPN fabric management with Terraform

Model Driven Telemetry
Telemetry configuration with CLI and YANG Suite Collection with TIG_MDT container and tooling

YANG Programmability
YANG Suite tooling and integrations to YANG API's
Ansible integrations

Tooling and Integrations
YANG Suite
- NETCONF/RESTCONF/gNMI API
  - Ansible integration
- NETCONF/gNMI Dial-In Telemetry
- gRPC Dial-Out Telemetry receiver

Telemetry
- TIG stack in Docker
- Grafana dashboard for device health

Postman / RESTCONF
- EVPN fabric API calls

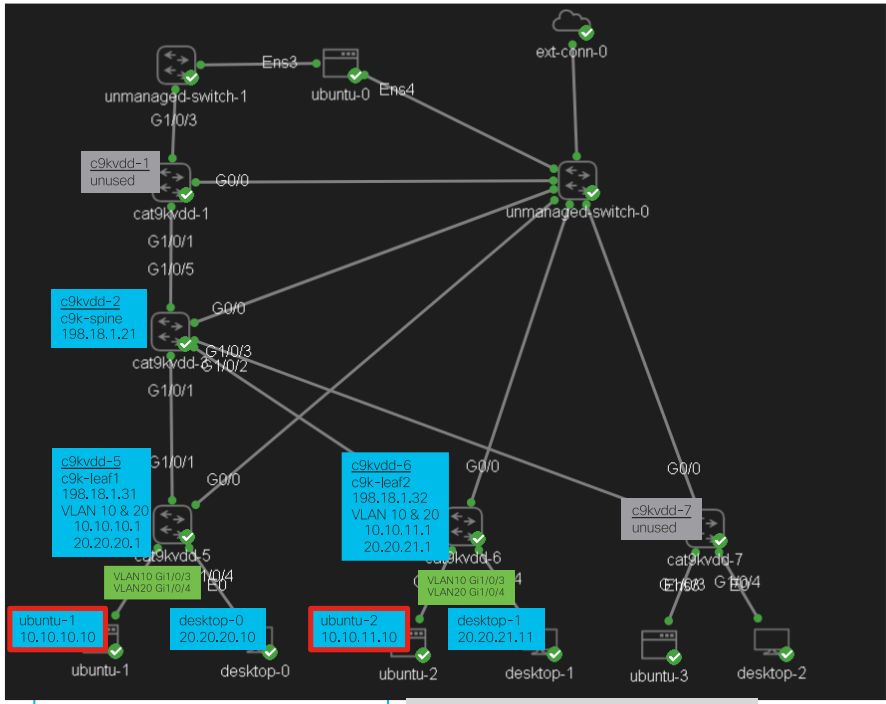
Terraform/RESTCONF
- Declarative EVPN fabric management

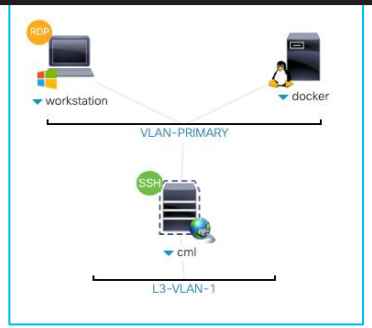
Ansible
- EVPN solution enablement using CLI

Ubuntu VM Details:
Syslog receiver from all switches
TFTP config backup
See slide

Windows VM Details
VS Code
Terraform @ folder
Ansible @ folder
Chrome browser
YANG Suite, Grafana
Bash/PS/Cmd shells
SSH into C9K or Ubuntu
Postman
Workspace for EVPN

C9K VM's





VLAN1
c9k-spine
IP: 198.18.1.21
developer / C1sco12345
c9k-leaf1
IP: 198.18.1.31
developer / C1sco12345
c9k-leaf2
IP: 198.18.1.32
developer / C1sco12345
c9kvdd-1 - unconfigured

c9kvdd-7 - unconfigured

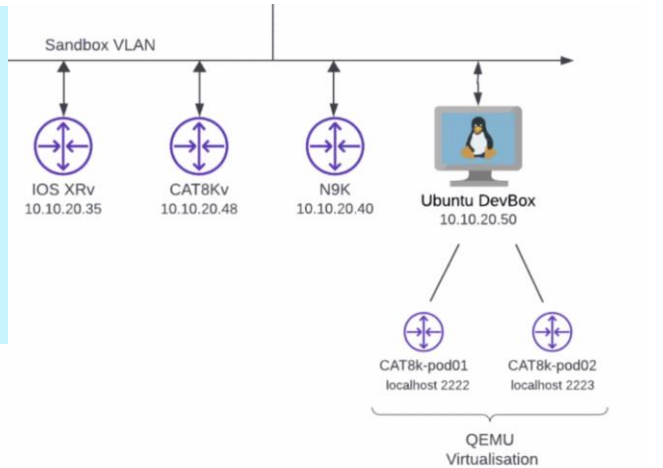
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

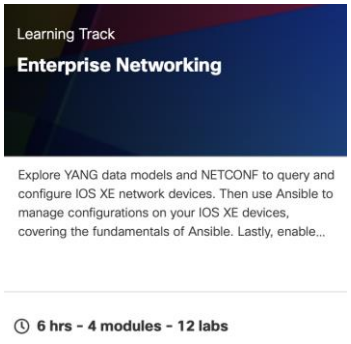
Cisco IOS XE - Reservable Virtual Sandbox

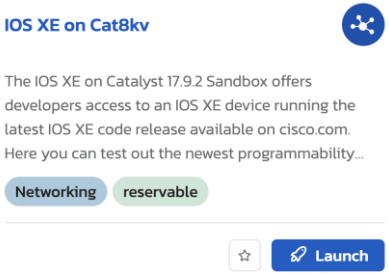
This DevNet reservable sandbox has IOS XRv + N9Kv + IOS XE
The Catalyst 8000V within the DevBox is enabled for Day 0/ZTP usecases

https://devnetsandbox.cisco.com
"IOS XE on Cat8kv"
https://devnetsandbox.cisco.com/DevNet/catalog/IOS%20XE%20on%20Cat8kv

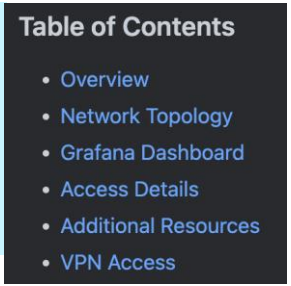
The "Enterprise Networking" Learning Labs contains guides for the supported usecases
https://developer.cisco.com/learning/

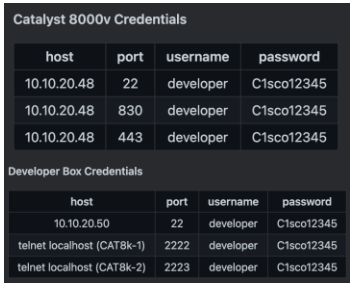






Sandbox Capabilities:
TIG_MDT Telemetry
YANG Suite API
Terraform + Ansible
ZTP & Guest Shell
... and more



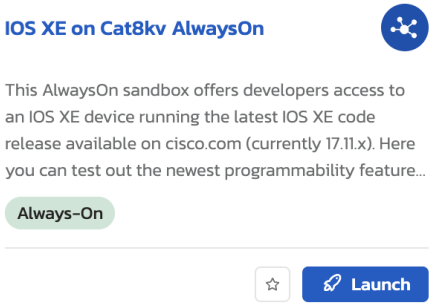


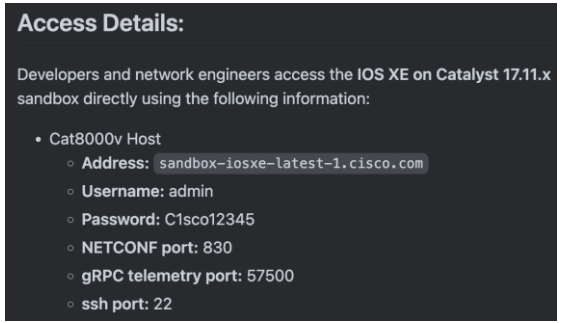
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

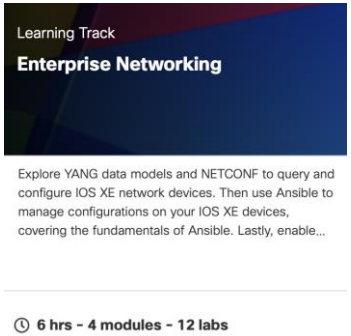
Cisco IOS XE – Always On Virtual Sandbox

The “IOS XE on Cat8kv Always On” virtual sandbox requires no reservation
The c8kv can be accessed with SSH, NETCONF, and RESTCONF
Hostname: sandbox-iosxe-latest-1.cisco.com
Username: admin Password: C1sco12345
SSH port 22, NETCONF port 830, RESTCONF HTTPS
https://devnetsandbox.cisco.com
devnetsandboxiosxe.cisco.com
https://devnetsandbox.cisco.com/DevNet/catalog/ios-xe-always-on

The “Enterprise Networking” Learning Labs contains guides for the supported usecases
https://developer.cisco.com/learning/







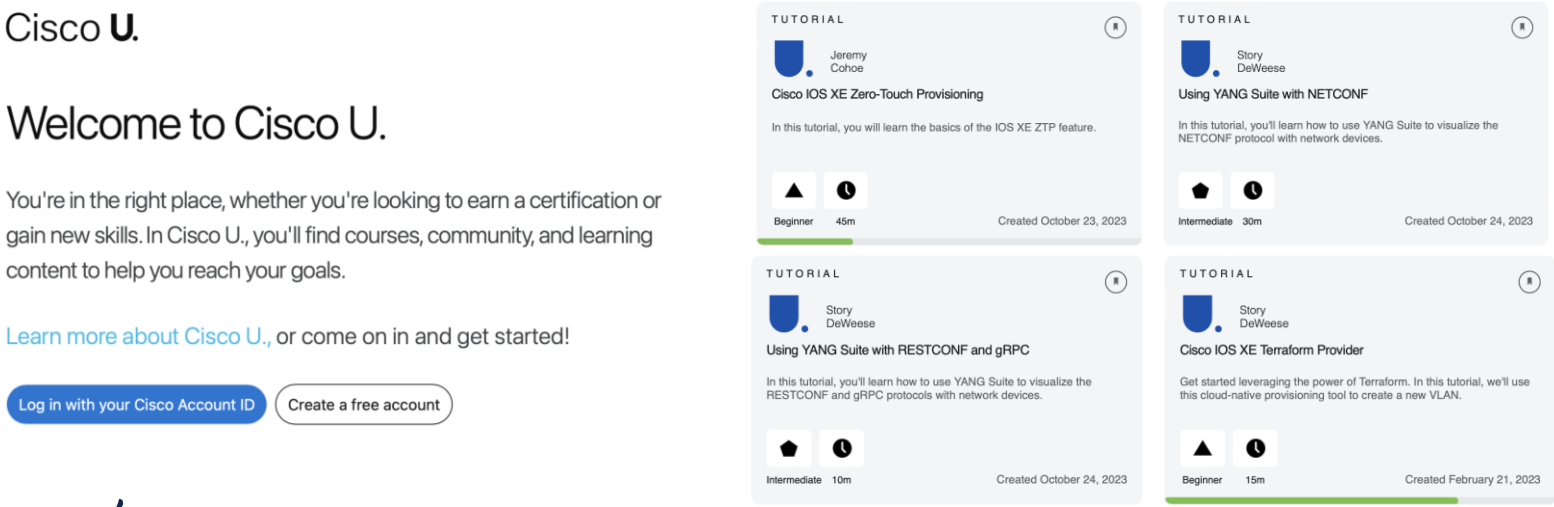
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco University (Cisco U) part of L&D

https://u.cisco.com
https://u.cisco.com/search/tutorial?query=Story%20DeWeese,%20Jeremy%20Coho,%20not%20berry

Direct link to Tutorial, requires login to u.cisco.com first:

1. https://ondemandelearning.cisco.com/apollo-alpha/tc-iosxe-ztp/pages/1
2. https://ondemandelearning.cisco.com/apollo-alpha/tc-terraform-ios-xe/pages/1
3. https://ondemandelearning.cisco.com/apollo-alpha/tc-yangsuite-netconf/pages/1
4. https://ondemandelearning.cisco.com/apollo-alpha/tc-yangsuite-restconf/pages/1



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco Live!

Keynote Deep Dives

Wednesday
10:30am –11:30am

Experiences Amplified: How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106

Smart, Secure, Seamless: Transforming Experiences with Next-Generation Networking

Level 2
Room 204

Harness a Bold New Era: Transform Data Centre and Service Provider Connectivity

Level 2
Room 203

Securing User to Application and Everything in Between

Level 2
Melbourne Room 2

Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

Complete your surveys in the **Cisco Live mobile app**.

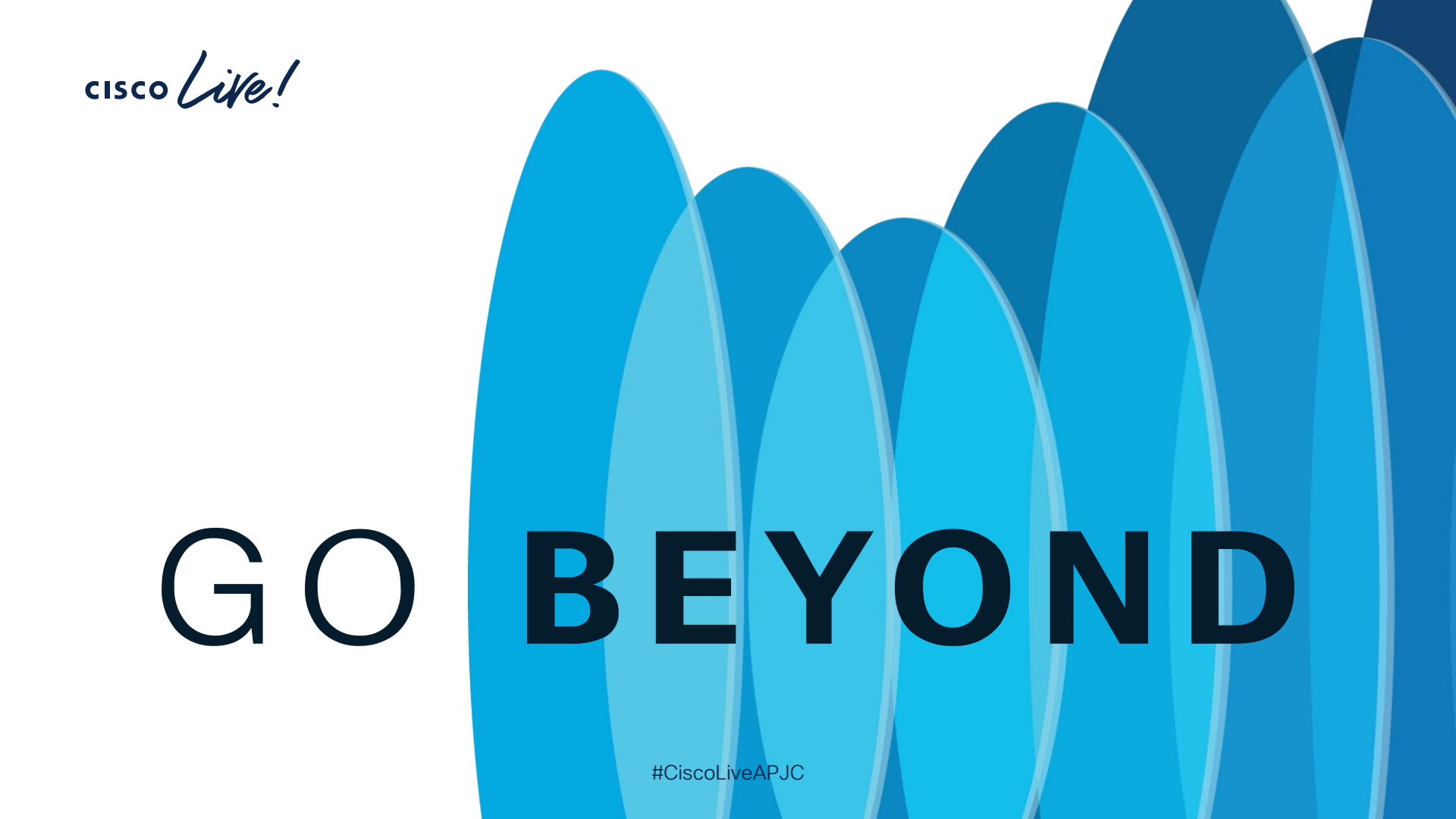
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC