Cisco NSO 5 Update

Carl Moberg
Director, Product Management, CPSG
June 2019
What’s New Around NSO 5

- Virtually unlimited horizontal scaling
- Concurrent heterogenous environments

- 500,000 physical and virtual devices under management
- In production in all top 10 service providers

- ETSI SOL003 Support in NFVO
- Swagger/OpenAPI
- NED Builder tool

- Secure Call-Home
- Service Tracking
- Audit Trails
- Continued platform hardening

© 2019 Cisco and/or its affiliates. All rights reserved.
"I have an issue with growth. While it’s a good problem to have, the number of physical and virtual devices I need to orchestrate is exploding and not all my services have consistent operational environments”

- Virtually unlimited horizontal scaling [4.5, 4.6]
- Multiple name spaces and NED versioning allow easy accommodation of multiple, concurrent disparate operational environments [5.0]
Layered Services Architecture (LSA)

- Horizontal scale-out architecture
- Improved performance through parallel service execution
- Device nodes can be organized by service type, device location, etc.
- Rolling and granular upgrades
Multiple Version Runtime Namespaces

• Allow NSO to runtime-load the same YANG module (as defined by namespace) of different versions

• Supports broader span of vendor versions found in very large networks

• Runtime analysis of version change impact across versions. I.e. what-if analysis on service code based on NED upgrades

✔ Robust support for emerging NETCONF/YANG platforms
Open: NSO as unified cross-vendor, cross-domain programmatic interface

“My environment is always going to have a diversity of vendors—I will maintain control of my toolchain and I need tooling that will work with whatever I have today and whatever I might buy tomorrow—both up and down the stack.”

- Swagger/OpenAPI support [4.7]
- ETSI SOL003 support in both our NFV Orchestration Function Pack and ESC [5.1]
- NED Builder tool empowers customers to create their own NETCONF NEDs [5.2]
- Support for 177 NEDs beyond Cisco
Swagger/OpenAPI for RESTCONF

- Offline generation of Swagger 2.0 specifications from YANG for RESTCONF
- Provides a mapping between YANG schema constructs to JSON Schema to the extent possible
- Opens up for all tooling built around Swagger to access RESTCONF-exposed resources in NSO

✔️ Unlocking the use of OpenAPI tools ecosystem for NSO
NETCONF NED Builder

• A tool for NSO users to automatically generate, build and load YANG-based NETCONF NEDs

• Significantly reduces the manual steps, and time spent on enabling never-seen devices to be completely managed by NSO

• Fine grained control over the process with steps including
  • Downloading and validating the YANG module content
  • Install and uninstall NEDs based on the specific combination YANG modules

✔ Truly automated, zero-touch device integration
NED Builder

1. Configure connectivity and log into new device

2. Initiate NED Builder Script

3a. Script pulls models from device...

3b. ...and generates a new NED

4. Formally unknown device now fully manageable in NSO
100+ NEDs supported—customization available
“With great power comes great responsibility—how do I make sure that my orchestration tooling is not turned against me?”

Trusted: NSO makes sure you can trust your infra so your customers can trust you

- Secure call home [5.0]
- Audit trails [4.7]
- Service tracking [4.7]
- Secure key management [5.0]
NETCONF call home

• RFC 8071 - *Enable a NETCONF or RESTCONF server to initiate a secure connection to a NETCONF or RESTCONF client, respectively*

• Allows network elements to securely call-home for management after cold start

• Client-initiated operations provide *stealth-mode* removing the need for open ports on the device

• Supports both NAT and direct scenarios

✅ Standardized and secure call-home
Audit Trails

• Provides the fundamental audit trails for regulated environments
• Trails include complete per-change information, including:
  • The nature and content of all changes performed through NSO
  • Both on the services layer, as well as any resulting device-layer changes
  • All changes mapped to the user triggering the changes

✓ Fine-grained, transparent audit trails to support compliance
Monitoring Dashboard

- Connected devices and types
- Active user sessions
- Service instances
- Service progress monitoring

Overview of the running administrative status
Service Progress Monitoring

- Enable monitoring of service delivery times
- Service models are associated with:
  - Expression on the plan
  - Time to jeopardized state
  - Time to violated state
- The expression is evaluated at the jeopardized and violated times
- Alarms are generated for jeopardized or violated SLAs

✔ No-code, declarative tracking of service delivery
Plan and Commit Queue UI Applications

- Plan viewer in the configuration editor
- Commit queue content viewer in the commit manager
- Upload-and-merge of configuration data

✓ New custom representations of configuration and state
Proven: NSO is a strategic choice

“Orchestration at scale is hard. My people don’t have the expertise and the tech seems to have a half-life measured in months. I don’t need products, I need a strategic partner.”

- In production since 2010 – 8 years of accumulated wisdom
- In production at the top 10 carriers
- Several customer networks have NSO managing more than 50k devices
- Pre-engineered solutions like MSX, ESC and Core Function Packs shorten time-to-value
- CX professional services and an active developer community provide hand-holding as needed
The NSO Ecosystem

Services
- Advisory
- Implementation
- Optimization
- Technical
- Business Critical
- BPA

Extensions

Core Function Packs
- Crossworks
- Itential
- Netrounds
- Telco Cloud

Solutions
What is a Core Function Pack?

- Ready-made implementations for specific features
- Productized and commercially supported
- 80/20 rule – reduce implementation cost and time to market
- Evolves with solution requirements
Core Function Packs – Brief Overview

- **NFVO CFP** – ETSI NFV MANO standards compliant multi-vendor NFV Orchestrator
- **vBranch CFP** – scalable, multi-tenant, multi-vendor virtual branch orchestration
- **T-SDN CFP** – Transport network automation for SR-TE
- **SAE CFP** – virtualized, multi-vendor demilitarized zone (DMZ) managing security between consumers and providers of data and applications
- **SDWAN CFP** – scalable, multi-tenant, on-premise SDWAN orchestration with multi-vendor branch
NSO Developer Days, June 18–20 2019

Annual community event in Stockholm for Orchestration and Automation Professionals. Focus on increasing knowledge through valuable content. Promote experience sharing, active and vivid discussions on the NSO Developer Hub

Recorded Powerful technical workshops

Gather attendees from 200 companies managing complex networks world wide

Register at www.cisco.com/go/nso2019

Experience Sweden during the lightest time of the year. Join the most popular festival in Sweden raising of the grand Maypole with ring dance at Skansen park or take a boat tour in the archipelago.
Questions?