The bridge to possible

Secure Data Center in Record Time

Using Cisco to Automate, Deliver and Validate your Pipeline

Jeff Comer, Data Center Architect (CCIE 3943)
Kelly Jones, Solutions Engineer (CCNA DevNet)
@JeffreyLComer & @kelly_jones15

BRKCLD-2731

cisco Live!

#CiscoLive

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCLD-2731

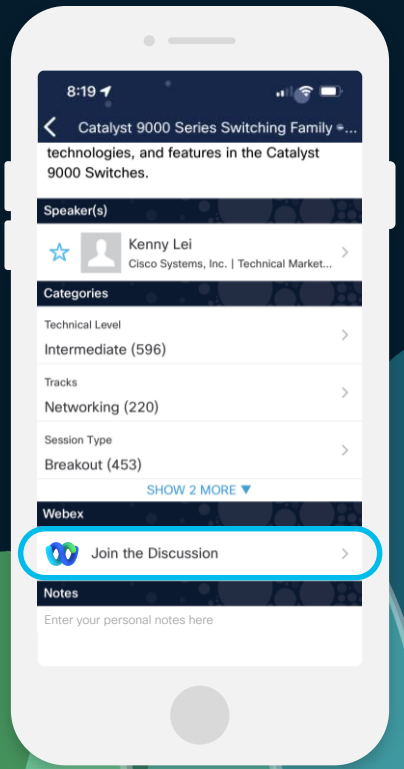
Questions?

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 June 7, 2024.



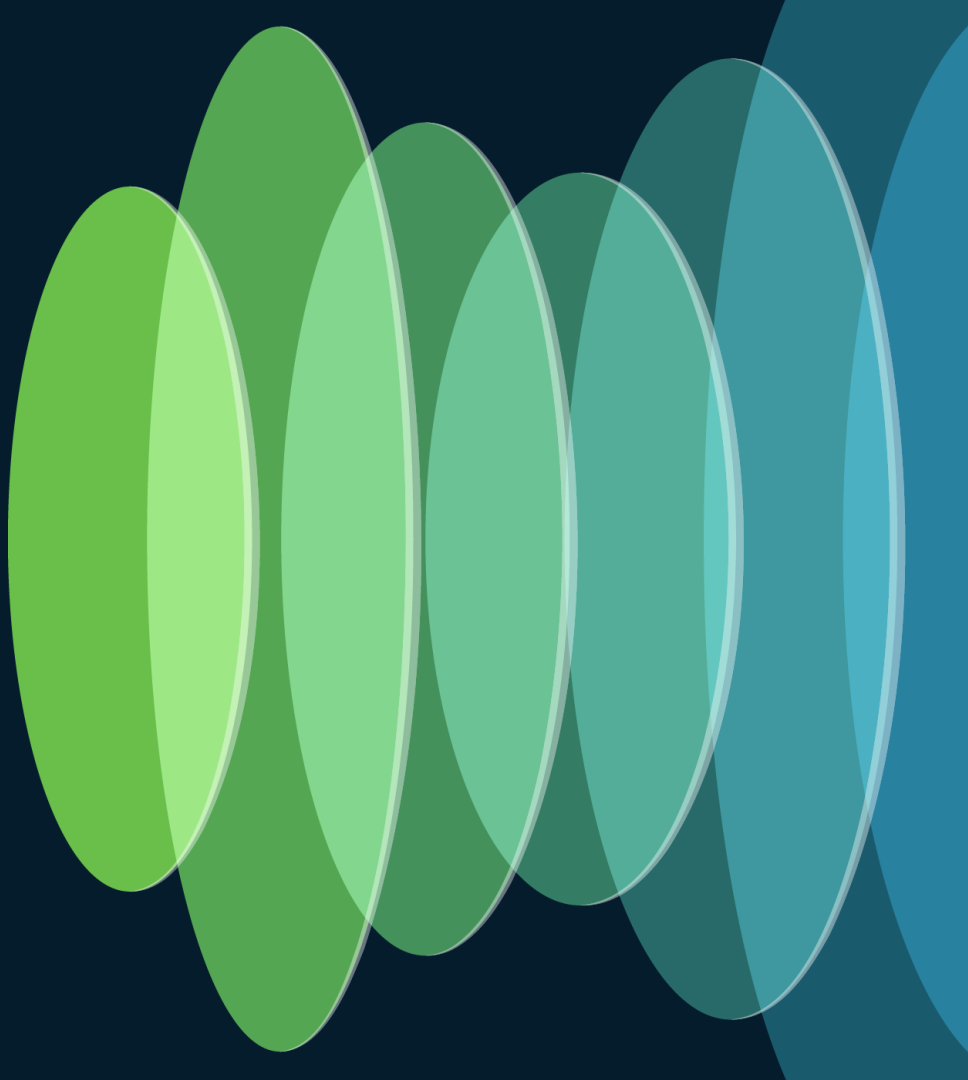
Agenda

- Introduction
- What is an Infrastructure as Code Pipeline
- Pushbutton Data Center (ACI, Nexus Dashboard)
- Auto-Provision Compute and Storage (Intersight)
- Continued Compliance (NSO, AppDynamics, Secure Network Analytics)
- Conclusion

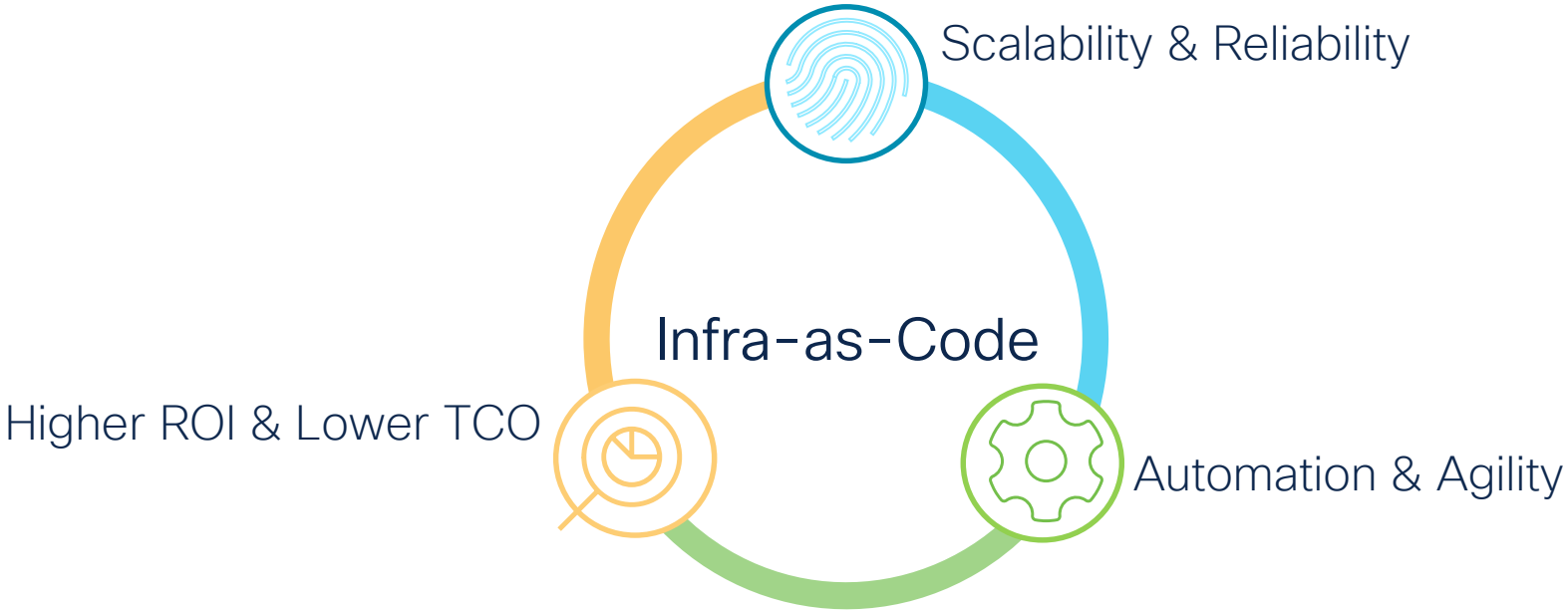
Why Infrastructure as Code (IAC)?

In a world where cars drive themselves, why are we still configuring Data Centers by CLI?

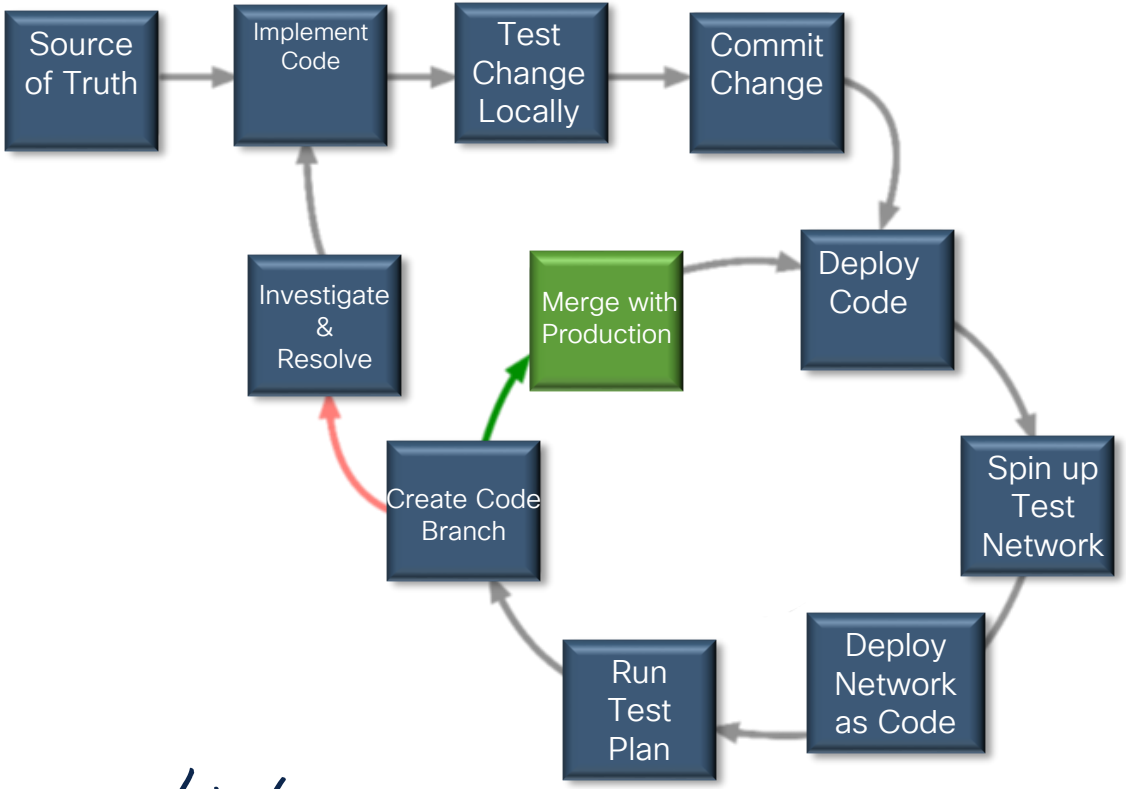
What is an Infrastructure as Code (IAC) Pipeline?



Why Infrastructure as Code?



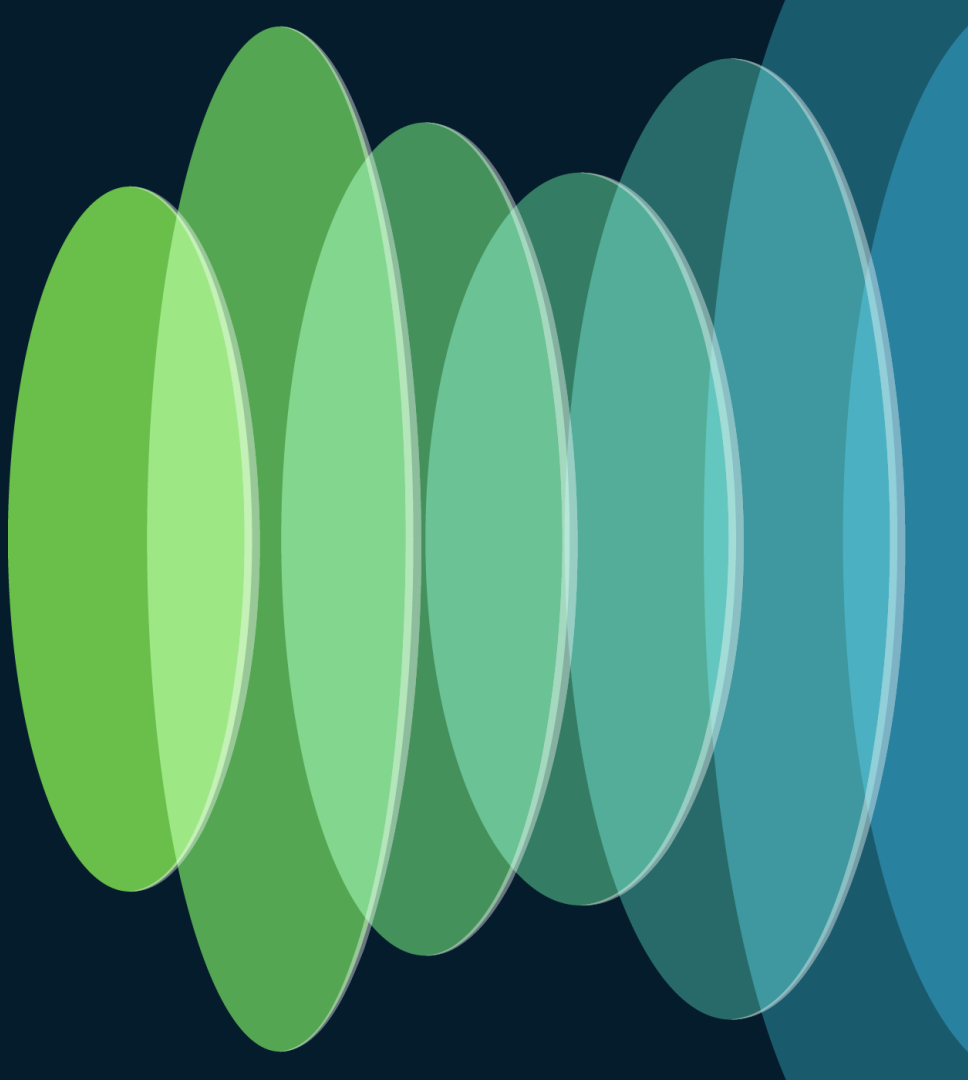
Infrastructure Testing Pipeline Elements



- Source of Truth
- Model-based infrastructure
- Digital Twin Pre-Test
- Validation Pipeline
- Post-Deployment Visibility
- Configuration Management

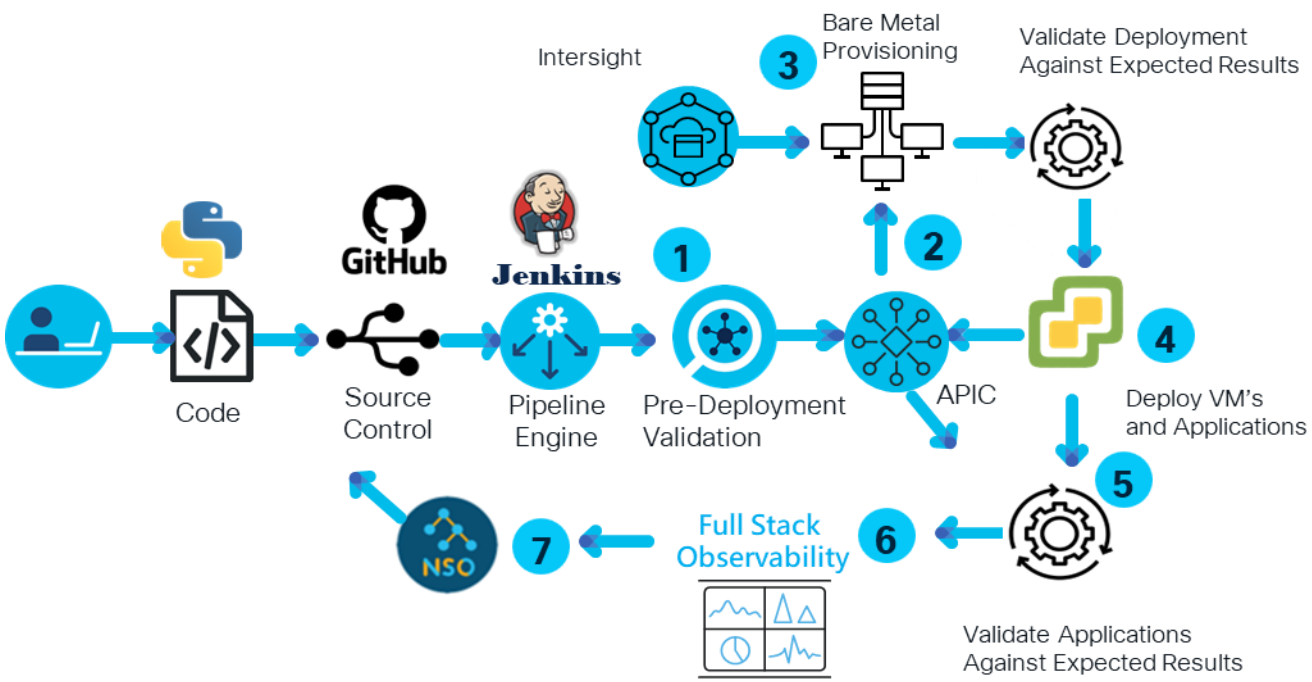
One-Click Data Center

ACI and Nexus Dashboard



cisco Live!

Automated Deployment and Compliance Pipeline



Jenkins Pipeline:

1. **Pre-Deployment Validation**
   - Nexus Dashboard Insights
   - ACI Simulator
2. **Build ACI Fabric**
3. **Deploy Bare Metal Hosts**
   - Intersight
4. **Validate against Expected Results**
   - CXTA
5. **Deploy VMs and Applications**
   - Intersight Cloud Orchestrator
6. **Validate Against Expected Results**
   - CXTA
7. **Full Stack Observability**
   - AppDynamics, SNA
   - Intersight, Nexus Dashboard
   - Skylight
   - Splunk
8. **Compliance Check**
   - NSO
   - Nexus Dasboard Insights
   - Secure Network Analytics

Source of Truth to Code

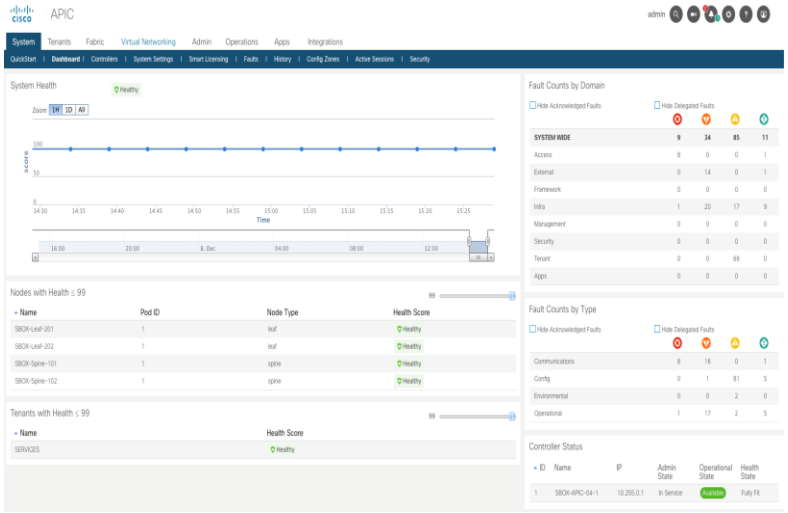
ACI Variables in .csv format

```
bridgeDomain,gateway,prefixLength,tenant,vrf,appProfile,descriptioin,epg,domain,domainType,contract,vlanEncaps,encapsType,filter,l3Out,multivrf,rp,dhcpRelay,c
BD_1200,172.16.115.254,22,SERVICES,services-vrf,Management,ESXi Management EPG,EPG_1200,Infrastructure,phys,SERVICES-Contract,1200,vlan,services-allow_all,out
BD_1201,172.16.116.254,24,SERVICES,services-vrf,Management,HX Storage Data EPG HX-1,EPG_1201,Infrastructure,phys,SERVICES-Contract,1201,vlan,services-allow_a
BD_1202,172.16.117.254,24,SERVICES,services-vrf,Management,ESXi vMtion EPG,EPG_1202,Infrastructure,phys,SERVICES-Contract,1202,vlan,services-allow_all,NA,NA,N
BD_1200,172.16.115.254,22,SERVICES,services-vrf,Management,ESXi Management EPG,EPG_1200,HX-VMM,vmm,SERVICES-Contract,1200,vlan,services-allow_all,out-L3Out_SB
BD_1202,172.16.117.254,24,SERVICES,services-vrf,Management,ESXi vMtion EPG,EPG_1202,HX-VMM,vmm,SERVICES-Contract,1202,auto,services-allow_all,NA,NA,NA,NA,NA,N
BD_5,172.16.125.14,28,SERVICES,services-vrf,Management,Security EPG,EPG_5,HX-VMM,vmm,SERVICES-Contract,1205,vlan,services-allow_all,out-L3Out_SBOX,NA,NA,YES,
BD_1225,172.16.118.254,24,SERVICES,services-vrf,Management,Security EPG,EPG_1225,HX-VMM,vmm,SERVICES-Contract,1225,vlan,services-allow_all,out-L3Out_SBOX,NA,N
```

Deployment YAML

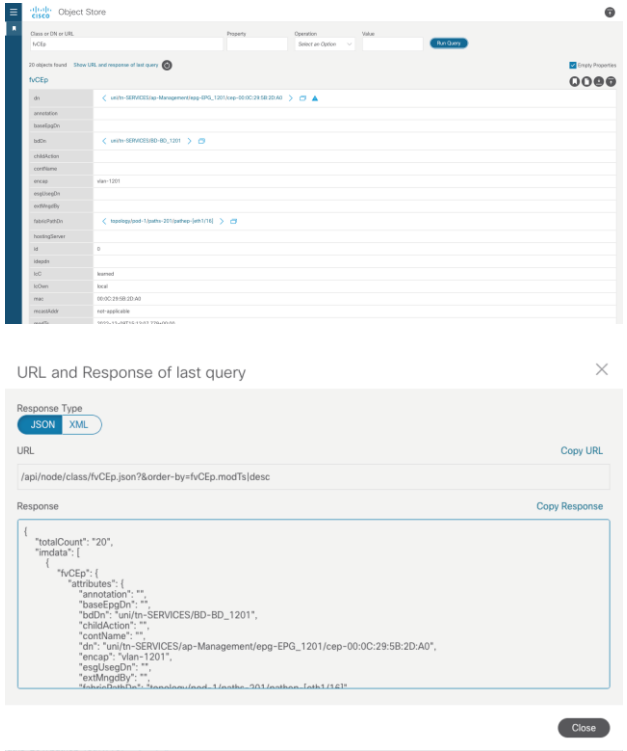
```yaml
tenants:
  - tenant: SERVICES
vrfs:
  - vrf: services-vrf
    tenant: SERVICES
    rp: 172.16.115.254
aps:
  - ap: Management
    tenant: SERVICES
bridge_domains:
  - bd: BD_1200
    gateway: 172.16.115.254
    mask: 22
    tenant: SERVICES
    vrf: services-vrf
    scope: public,shared
    L3Out: out-L3Out_SBOX
  - bd: BD_1201
    gateway: 172.16.116.254
    mask: 24
    tenant: SERVICES
    vrf: services-vrf
    scope: public,shared
    L3Out: NA
  - bd: BD_1202
    gateway: 172.16.117.254
    mask: 24
    tenant: SERVICES
    vrf: services-vrf
    scope: public,shared
    L3Out: NA
  - bd: BD_1200
    gateway: 172.16.115.254
    mask: 22
```

Application Centric Infrastructure (ACI) Role in the Pipeline



- **Application Centric Infrastructure**
  - Software Defined Network
    - Application Programmable Interface Controller (APIC)
    - Nexus 9000 Switches
  - Zero-trust
  - Model-based
  - Open API's

ACI DevOps Tools– REST API's



- ACI Visore
  - Object store browser
  - Query Managed Objects (MO) and display the results.
- Display the URL and Response for API calls in automation scripts.
- Enable '**Show Debug Info**' to determine applicable Class Name or DN.

ACI DevOps Tools – Ansible and Terraform

- Ansible

```yaml
- name: TASK 01 - ENSURE TENANT EXISTS
  aci_tenant:
    host: "{{ inventory_hostname }}"
    username: "{{ username }}"
    private_key: ../creds/ansible.key
    state: "present"
    validate_certs: False
    tenant: "{{ item.tenant }}"
  with_items: "{{ tenants }}"
  tags: tenant
```

- Terraform

```hcl
terraform {
  required_providers {
    aci = {
      source = "ciscodevnet/aci"
    }
  }
}

#configure provider with your cisco aci credentials.
provider "aci" {
  # cisco-aci user name
  username = "admin"
  # cisco-aci password
  password = "password"
  # cisco-aci url
  url      = "https://my-cisco-aci.com"
  insecure = true
}

resource "aci_tenant" "test-tenant" {
  name        = "test-tenant"
  description = "This tenant is created by terraform"
}

resource "aci_application_profile" "test-app" {
  tenant_dn   = aci_tenant.test-tenant.id
  name        = "test-app"
  description = "This app profile is created by terraform"
}
```

ACI DevOps Tools – Ansible and Terraform

Ansible

Open-source tool for cross-platform deployment.

- Extensive library of modules that leverages existing ACI API's.
- The aci_rest module provides the ability to deploy configurations that do not have modules.

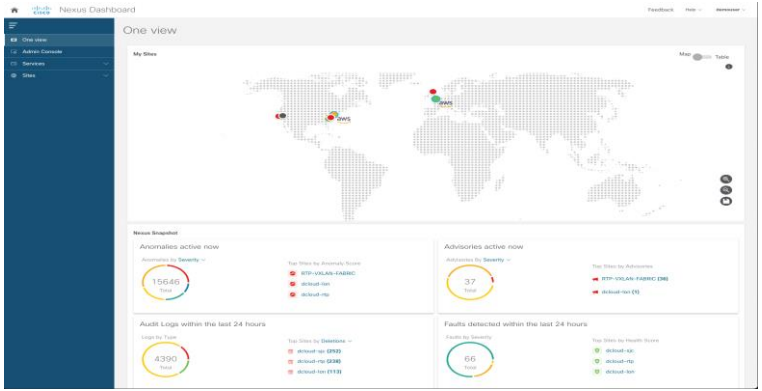
https://docs.ansible.com/ansible/devel/scenario_guides/guide_aci.html

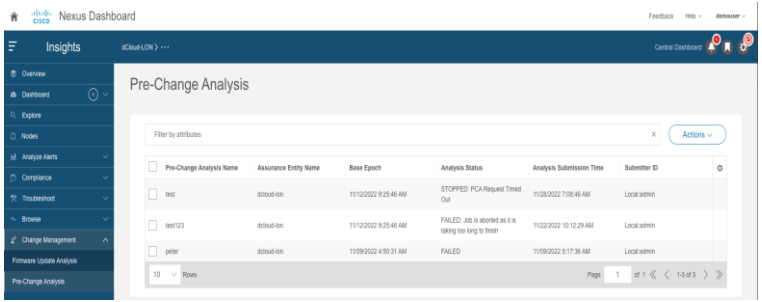
Terraform

- Open-source infrastructure as code software tool designed for safe and predictable infrastructure creation and change
- Extensive library of modules that leverages existing ACI API's
- Maintains state data for the infrastructure and configuration and refreshes this state prior to an operation

https://registry.terraform.io/providers/CiscoDevNet/aci/latest/docs

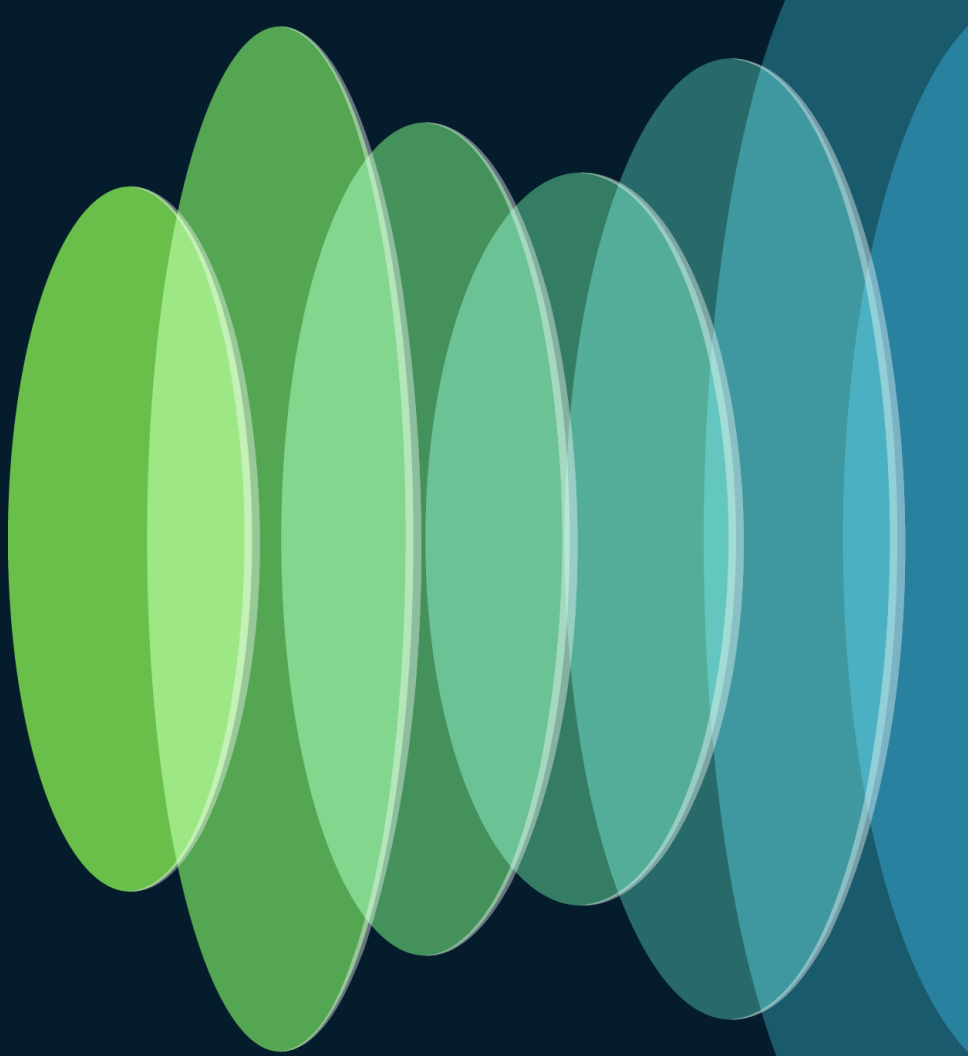
Nexus Dashboard - Insights





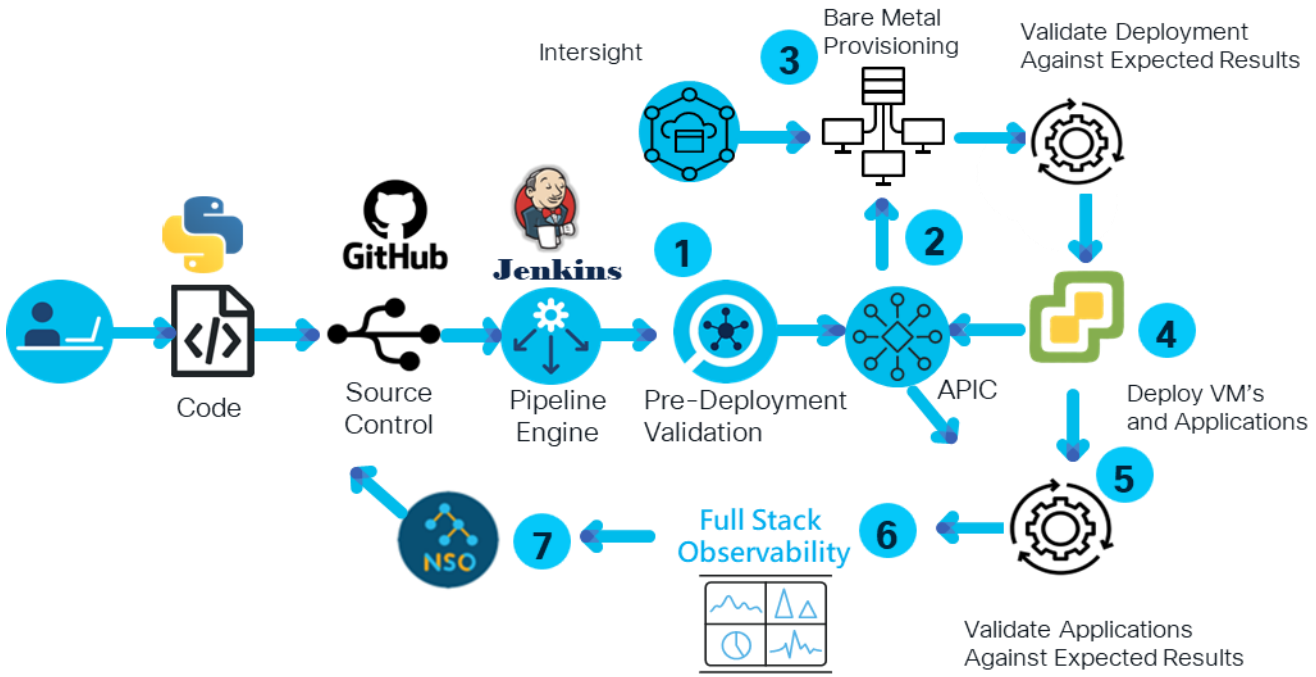
- Monitors, maintain, troubleshoot, and manage multiple data center fabrics.
- Extensive API's supporting pre- and post-change analysis
  - Test Code
  - Validate changes to a fabric prior to deployment.
  - Monitor performance post-deployment

Auto-Provision Compute and Storage with Intersight



cisco Live!

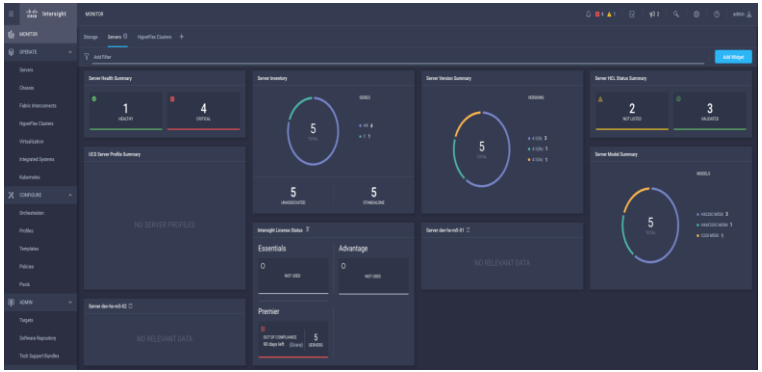
Automated Deployment and Compliance Pipeline



Jenkins Pipeline:

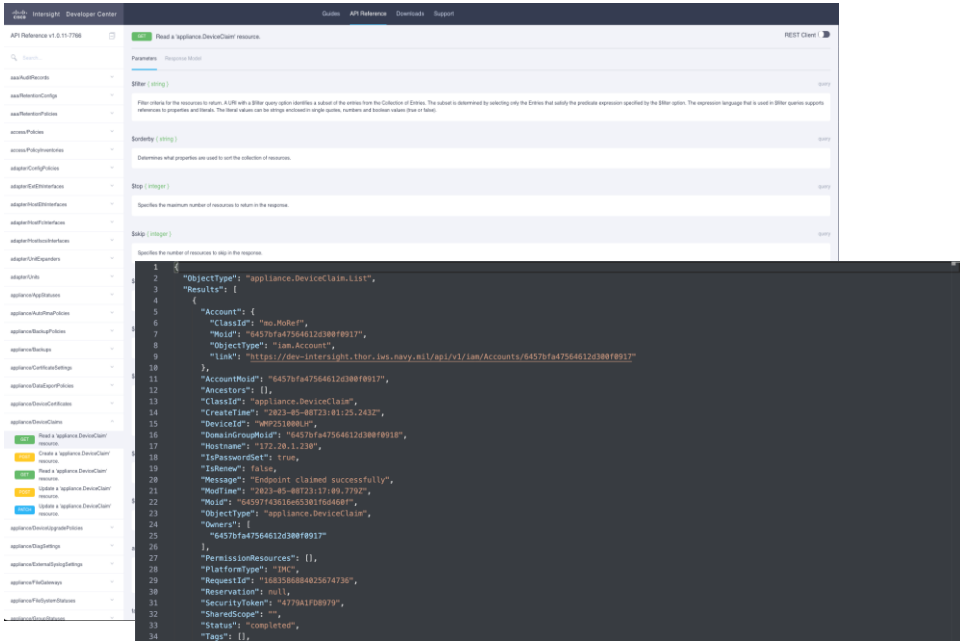
1. **Pre-Deployment Validation**
   - Nexus Dashboard Insights
   - ACI Simulator
2. **Build ACI Fabric**
3. **Deploy Bare Metal Hosts**
   - Intersight
4. **Validate against Expected Results**
   - CXTA
5. **Deploy VMs and Applications**
   - Intersight Cloud Orchestrator
6. **Validate Against Expected Results**
   - CXTA
7. **Full Stack Observability**
   - AppDynamics, SNA
   - Intersight, Nexus Dashboard
   - Skylight
   - Splunk
8. **Compliance Check**
   - NSO
   - Nexus Dasboard Insights
   - Secure Network Analytics

Intersight Role in the Pipeline



- Orchestration, Automation, Visibility
  - Workloads
  - Compute
  - BareMetal
  - Converged Compute
- Centralized Firmware Management
- Bulk OS deployment
- Robust workflow engine to orchestrate tasks across platforms via http API endpoints, ansible executor, etc.
- Workload Optimization

Intersight API's

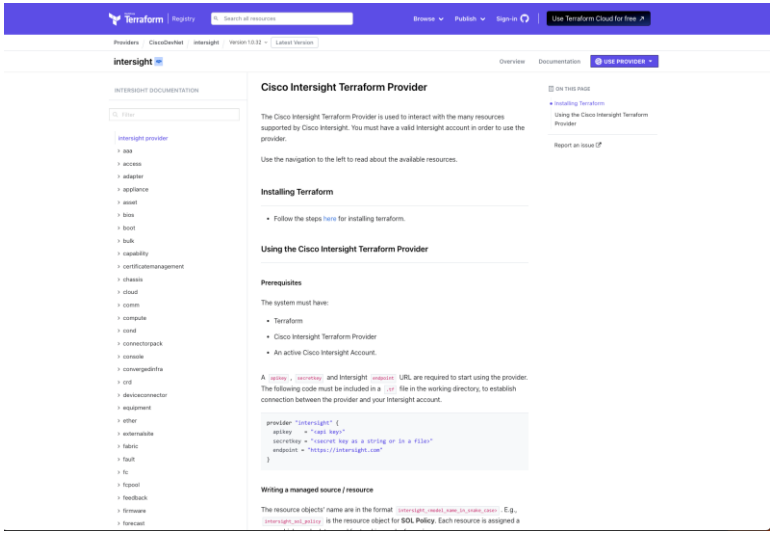


- All functions available in the GUI exposed via API's.
- Can be executed directly from the api explorer.
- Supports CI/CD pipelines
  - Deployment
  - Verification
  - Continuous compliance

Intersight Developer Center

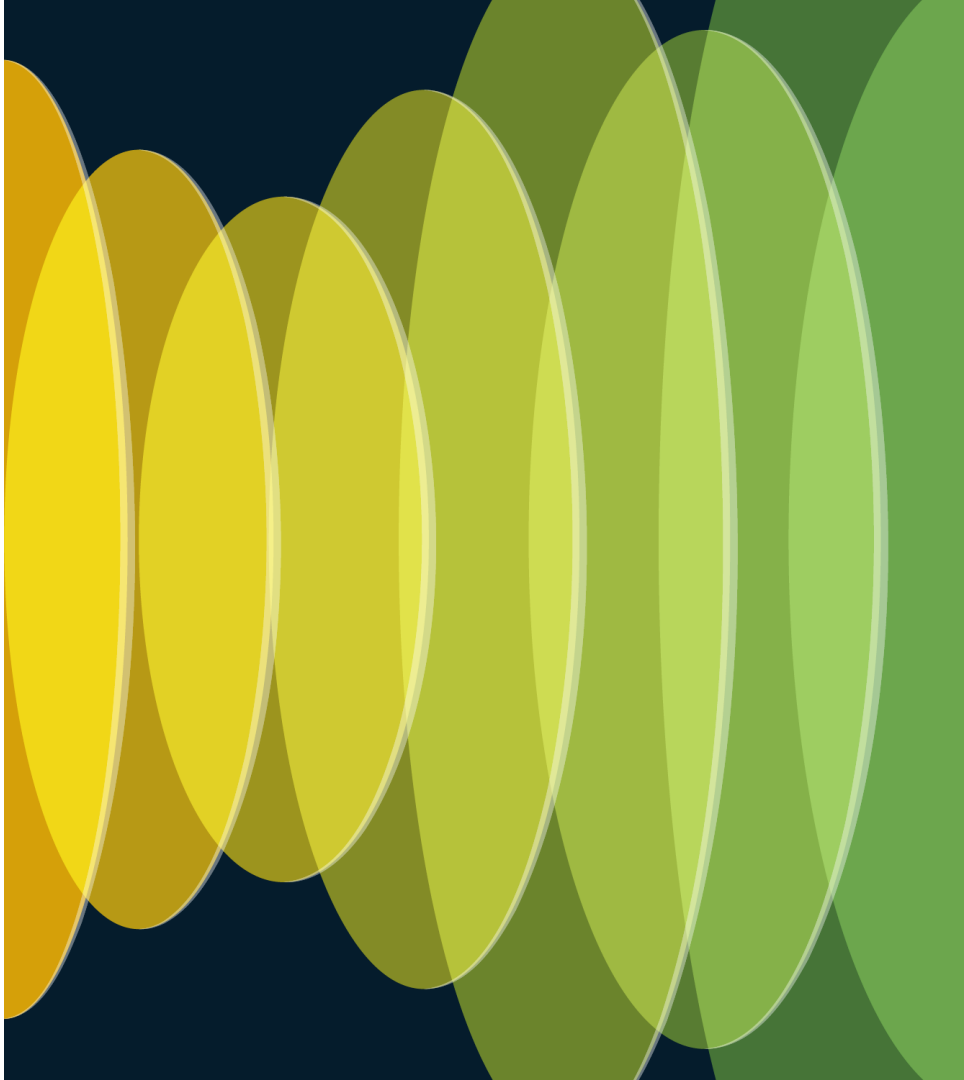
https://intersight.com/apidocs/introduction/overview/#intersight-api-overview

Intersight and Terraform



- Terraform is an infrastructure as code tool that simplifies provisioning of resources with minimal code expertise.
- Terraform utilizes the API's available from various resources through the use of providers.
- The Intersight Terraform provider leverages the API's provided by Intersight to automate infrastructure tasks with low code overhead.

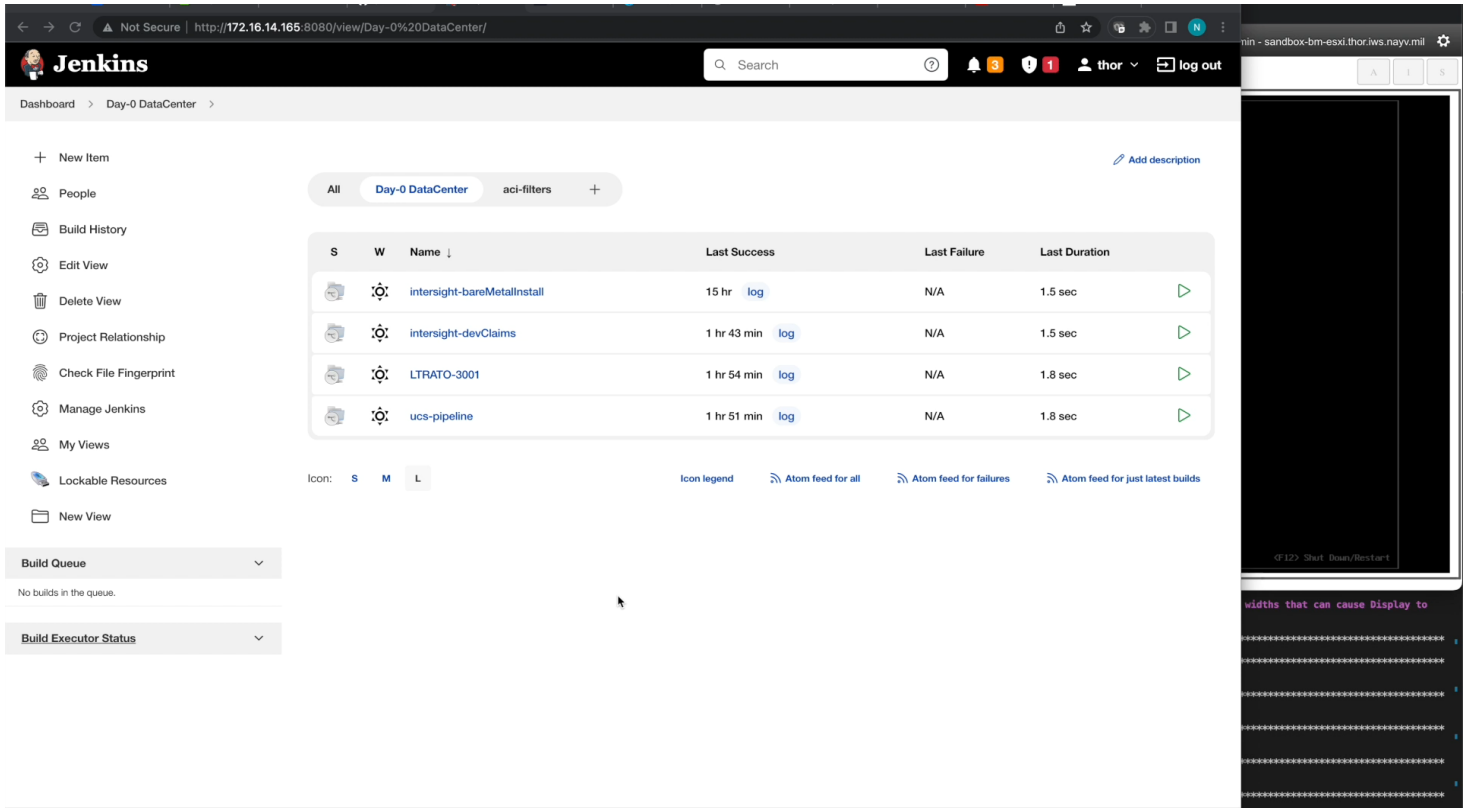
Demo: Putting it all together



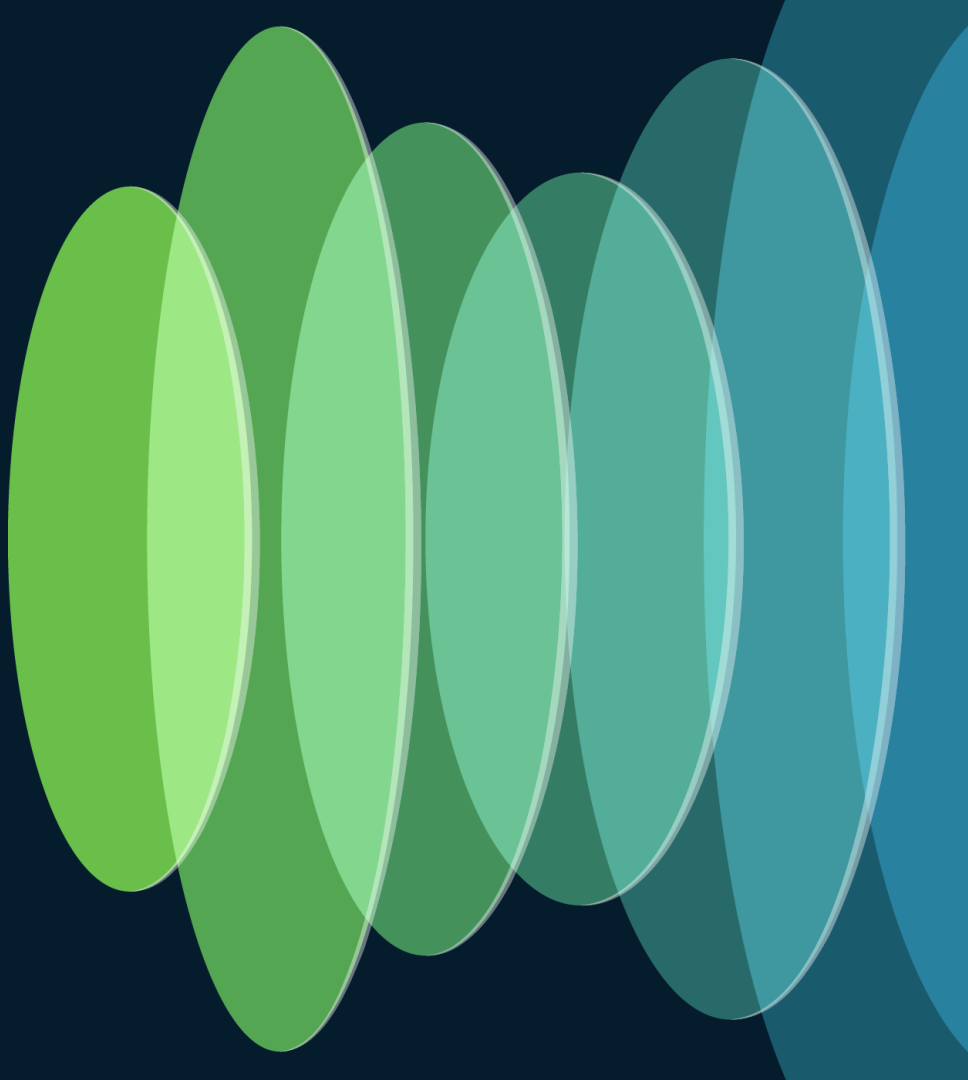
Demo: Putting it all together

- ACI Day-0 Build
  - Fabric discovery, Port and Policy creation
  - VMM Integration with vCenter
  - Tenant, Context, Bridge Domain, End Point Groups, Contract, and Filters
- Compute stack Day-0 Build
  - UCS device claims using Terraform Intersight Provider
  - Bare-metal provisioning of ESXi hosts using Terraform Intersight Provider
  - Hyperflex DC-No-FI cluster creation and deployment using Terraform Intersight

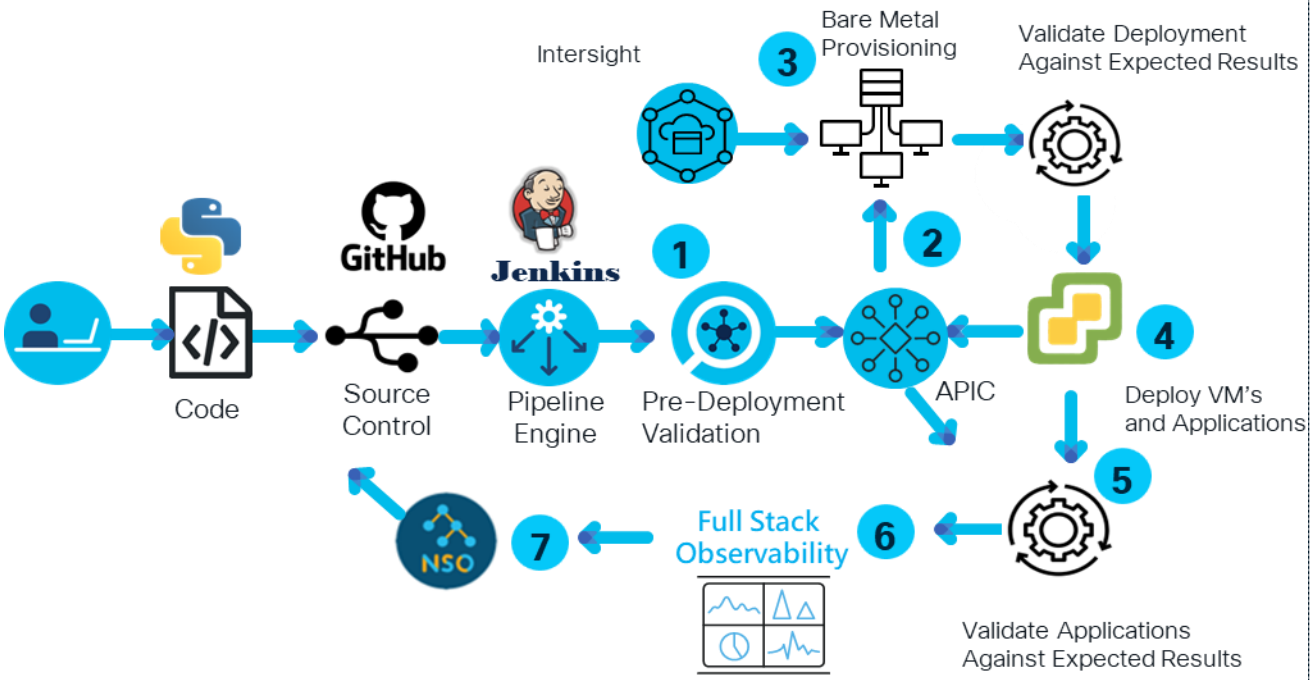
Demo: Putting it all together



Continued Visibility and Compliance



Automated Deployment and Compliance Pipeline



Jenkins Pipeline:

1. **Pre-Deployment Validation**
   - Nexus Dashboard Insights
   - ACI Simulator
2. **Build ACI Fabric**
3. **Deploy Bare Metal Hosts**
   - Intersight
4. **Validate against Expected Results**
   - CXTA
5. **Deploy VMs and Applications**
   - Intersight Cloud Orchestrator
6. **Validate Against Expected Results**
   - CXTA
7. **Full Stack Observability**
   - AppDynamics, SNA
   - Intersight, Nexus Dashboard
   - Skylight
   - Splunk
8. **Compliance Check**
   - NSO
   - Nexus Dasboard Insights
   - Secure Network Analytics

Continued Visibility and Compliance

NSO, AppDynamics, Secure Network Analytics

NSO
Network Services Orchestrator

NSO is a model driven orchestration platform that supports over 170 vendors. NSO also tracks device state and changes.

Splunk

Comprehensive full-stack observability solution across a multi-cloud hybrid, environment.

SNA
Secure Network Analytics

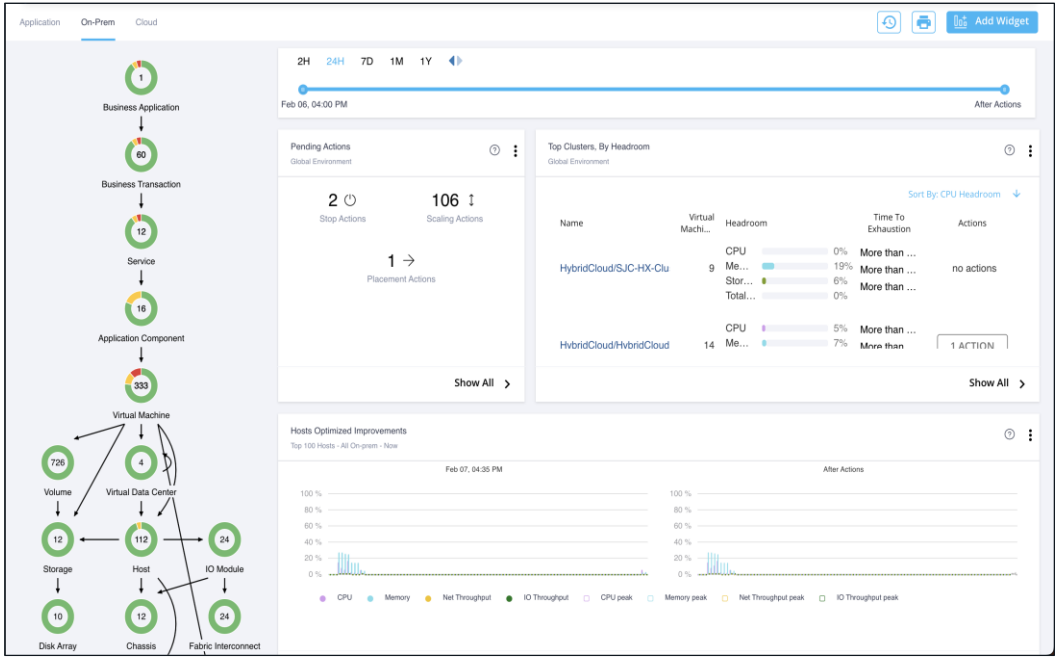
Continuous monitoring of devices, applications, and users throughout infrastructure through flow data

AppDynamics

Dynamic application performance baselines based on machine learning and artificial intelligence

Intersight Workload Optimizer (IWO)

Give Workload Resources When and Where Needed



- Continuously analyze workload consumption, costs and compliance constraints in real time
- Automatically re-allocate compute and storage resources in real-time based on demand or consumption
- Integrates with AppDynamics to provide a common view of Applications in both business and infrastructure perspective

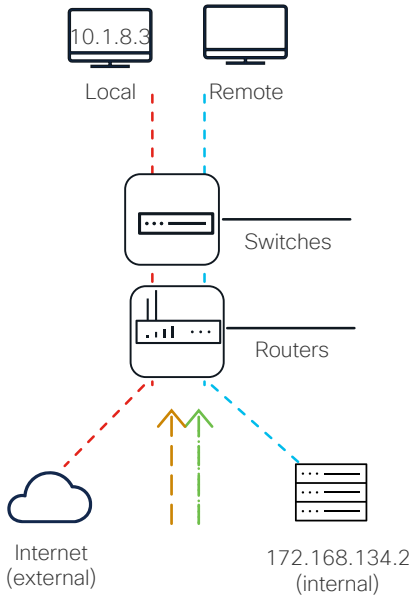
Sample Use Cases:

- Tie components of an application to a specific Data Center Rack
- Auto-scale resources
- Roll-back poor performing application upgrade

Secure Network Analytics (SNA):

The network as the source of truth

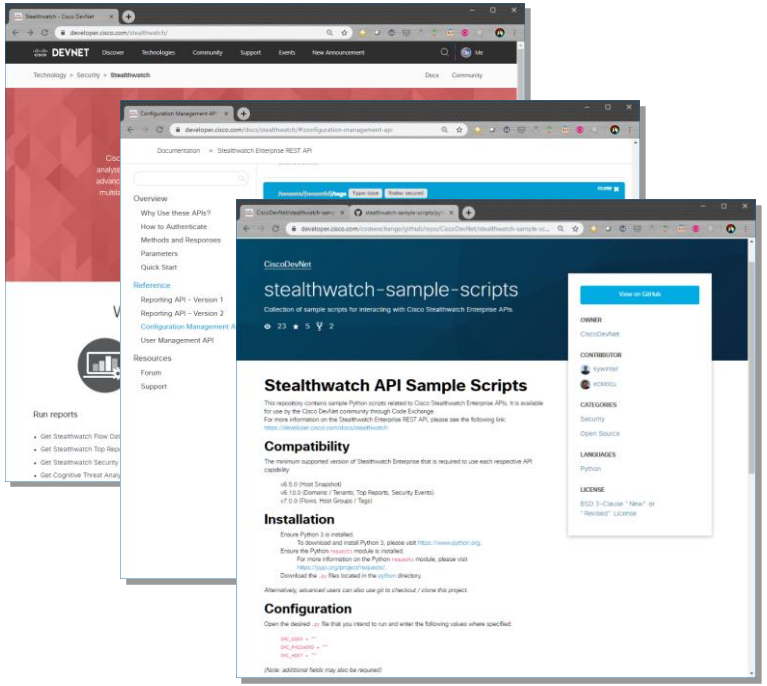
- A Trace of every conversation
- Agentless information collection
- Remote worker endpoint data collection
- Cloud Telemetry ingest
- East-west and north-south visibility
- Light meta data collection using the existing infrastructure
- Capture enhanced NetFlow for encrypted traffic analysis from Cisco ASR, ISR and Catalyst 9000 platforms



Flow information	Packets
Source address	10.1.8.3
Destination address	172.168.134.2
Source port	47321
Destination port	443
Interface	Gi0/0/1
IP TOS	0x00
IP protocol	6
Next hop	172.168.25.1
TCP flags	0x1A
Source SGT	100
:	:
ETA meta data	IDP | SPLT
Application name	NBAR SECURE-HTTP
Process Name	chrome.exe
Process Account User	Acme/john

Automate with Secure Network Analytics APIs

- Secure Network Analytics has REST API capabilities available to get, add, modify, and delete host groups.
- These APIs provide an easy programmatic mechanism to maintain host group configurations.
- Sample scripts are provided via DevNet to enable customers to use these API capabilities with success.



Run reports

- Get Secure Network Analytics Flow Data
- Get Secure Network Analytics Top Reports
- Get Secure Network Analytics Security Events

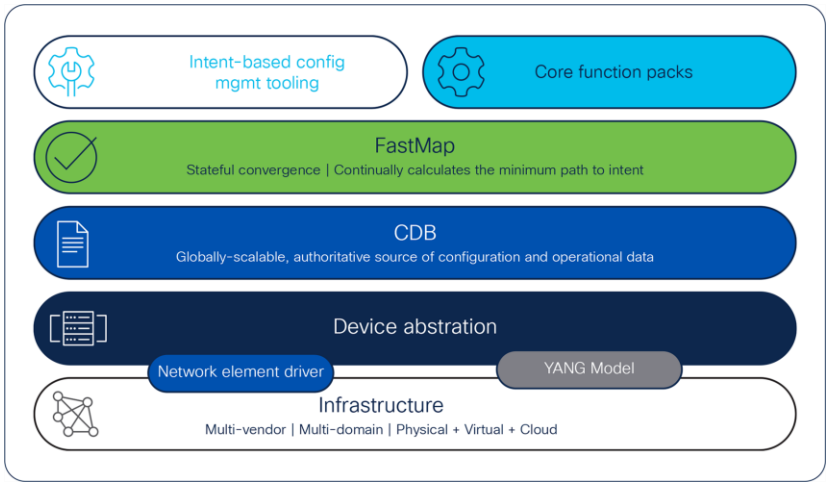
Manage configurations

- Get & Modify Host Groups / Tags
- Get & Modify Core / Relationship Policy
- Get & Modify Custom Security Events

Manage users

- Get & Modify User Information
- Get & Modify User Roles
- Modify Users Passwords

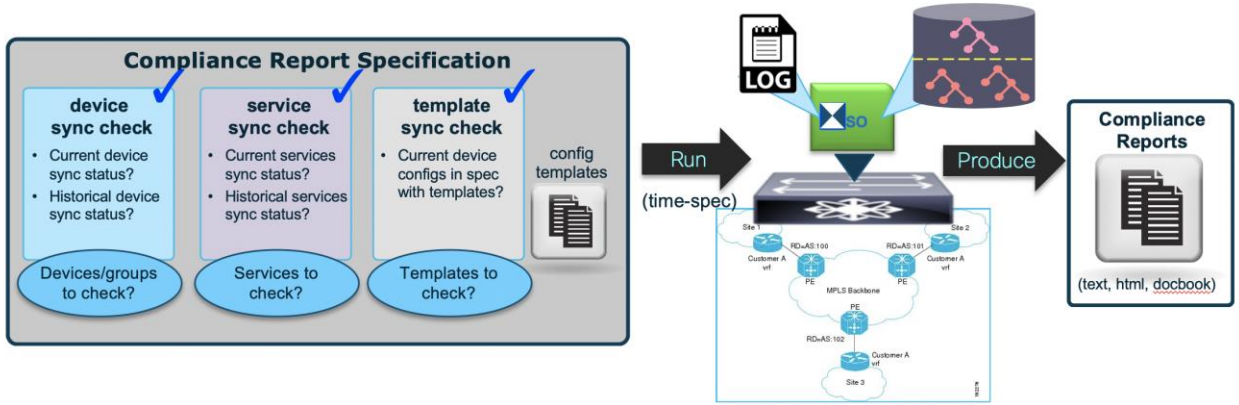
Cisco Network Services Orchestrator (NSO)



- Single datastore for all network elements under management
- Applies YANG as service-layer abstraction to model intent
- Network Element Drivers (NEDs):
  - Abstracts underlying protocol and data-models
  - Normalize Device Configurations
  - 170+ vendors supported
- Tracks State

Cisco Network Services Orchestrator (NSO):

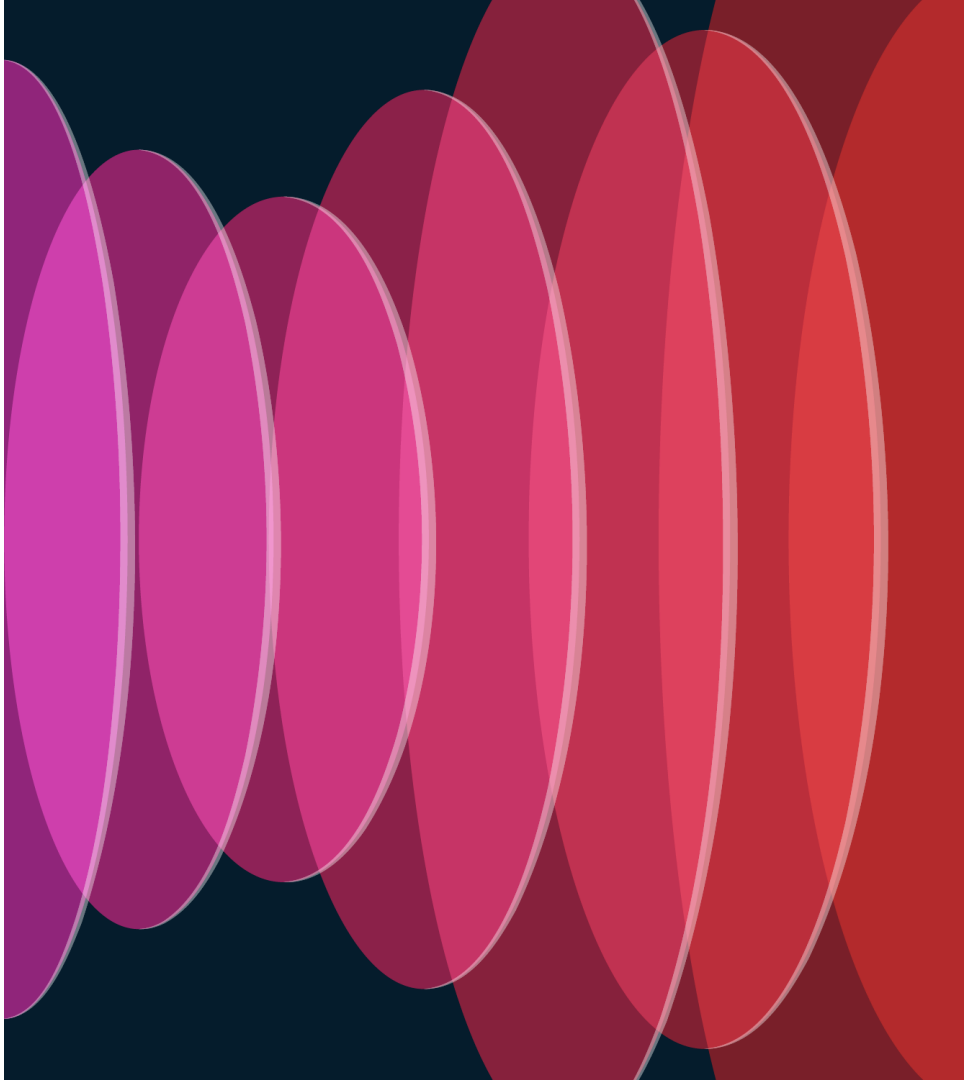
Model-driven, Stateful compliance



- Create device configuration “golden template”
- NSO identifies delta between golden template and current device config
- Deltas saved as artifact
- Process can be fed into automated validation pipeline

Demo

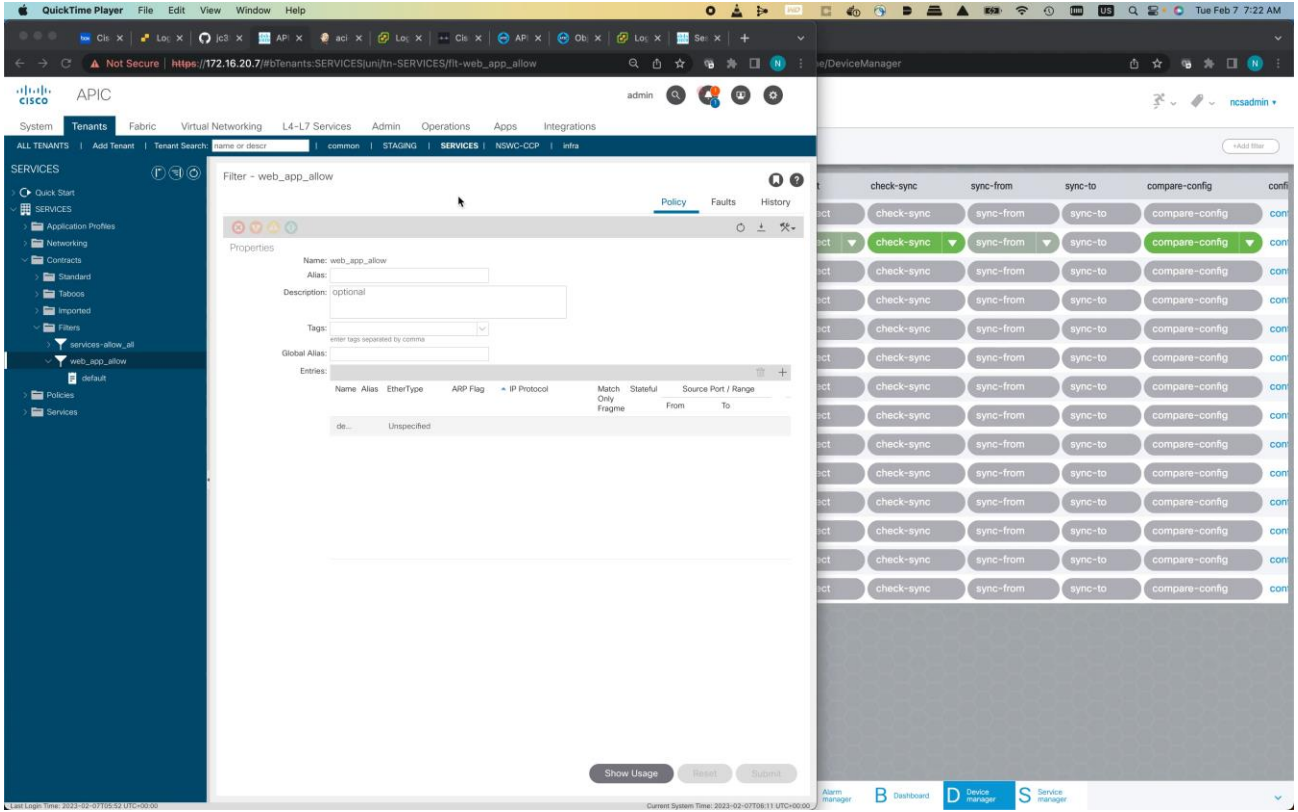
Management and Visibility



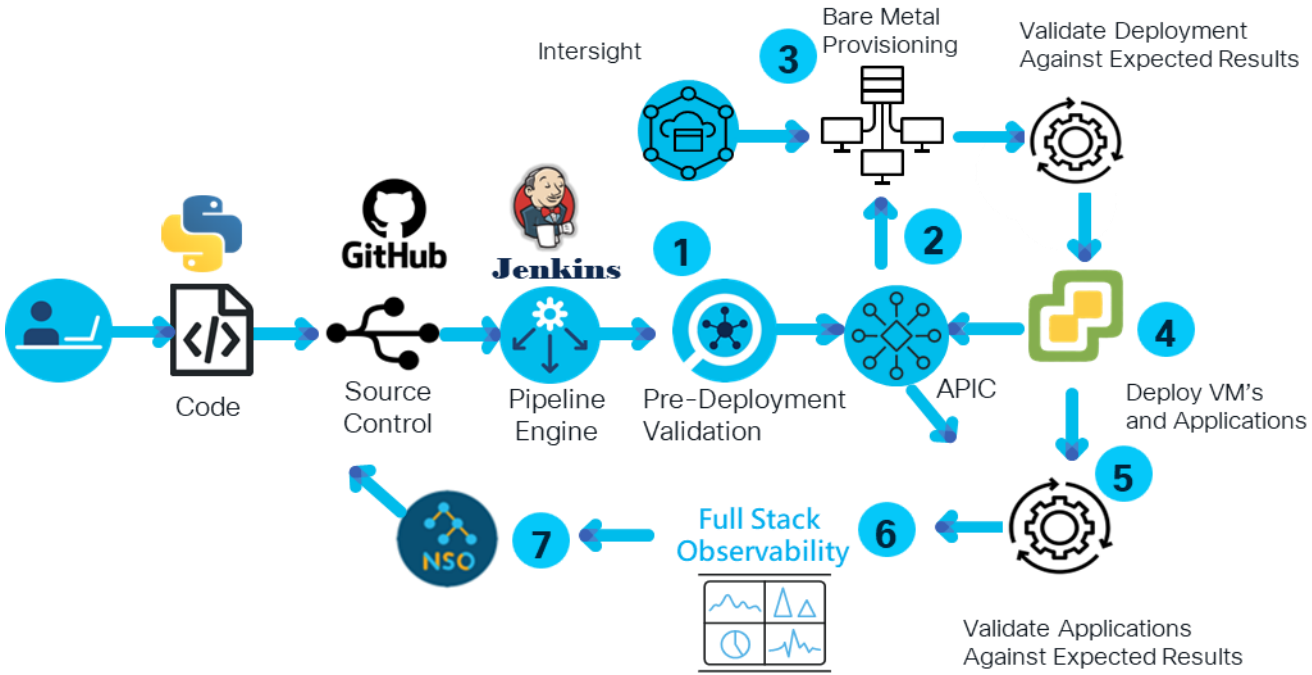
Demo: Management and Visibility

- NSO Synchronized to Devices
- Automated Pipeline Applies ACI Contract
- NSO Detects Change and reports out-of-sync
- Configuration Compare shows changes
- NSO Reverts device to previous config

Demo: Management and Visibility



Automated Deployment and Compliance Pipeline

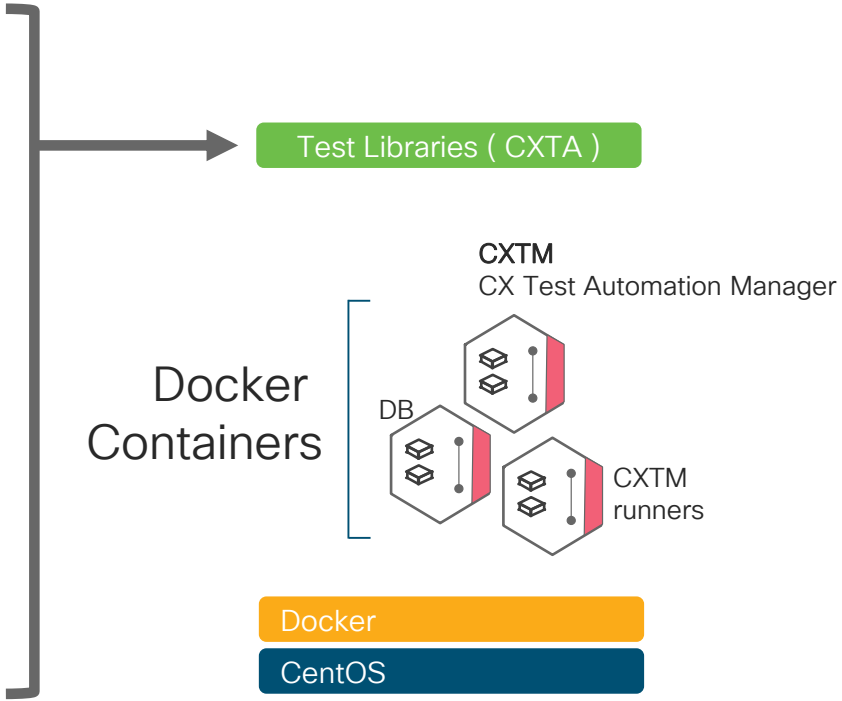


Jenkins Pipeline:

1. Deploy ACI Fabric
   -
2. Deploy Bare Metal Hosts
3. Validate against Expected Results
4. Deploy VMs and Applications
5. Validate Against Expected Results
6. Full Stack Visibility
   - Intersight, AppD, SNA
7. Compliance Check
   - NSO,
   - AppDynamics
   - Secure Network Analytics

Cisco Continuous Automation & Integration Testing (CAIT) Solution Validation Services

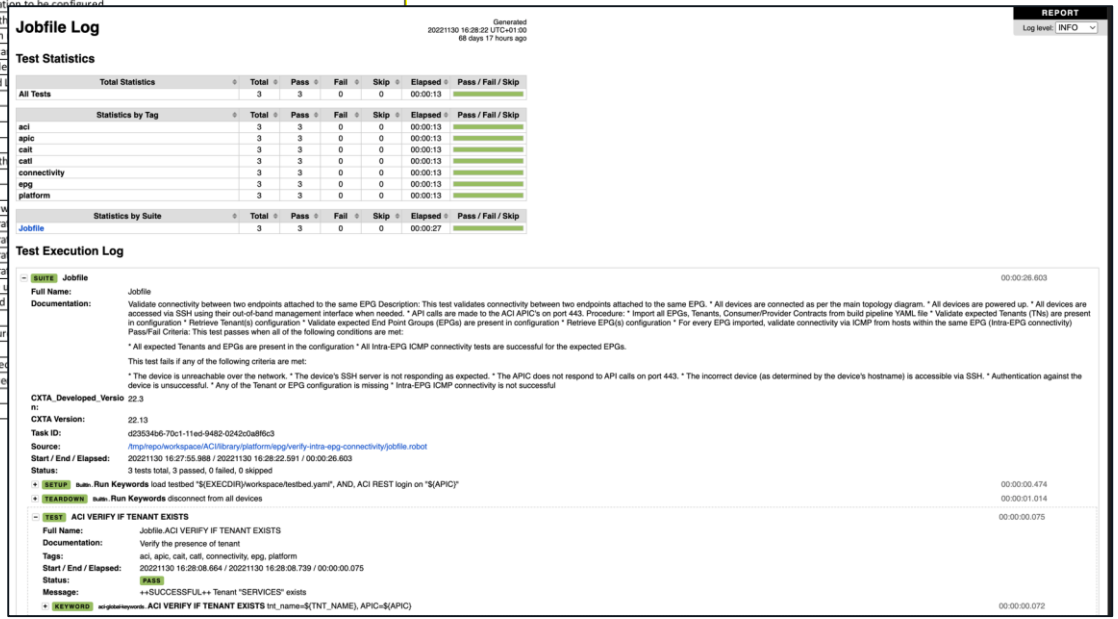
- Over 1,000 keywords developed by our test consulting engineers that accelerate creation of test case logic
- Utilizes the open-source Robot Framework to build test case logic using easy to understand English sentences
- Capable of controlling packet generation from many vendors including Spirent and IXIA
- Support for all of Cisco devices and third-party network devices via CLI and ReST interfaces



CAIT Solution Validation Service

Over 100 ACI Standard Tests

Test Case Number	Description	Requirement
3.0.0.0	ACI - Validate ACI Default Gateway Functionality	Requires at least 2 Endpoints that are available for ssh to ping from
3.0.1.0	ACI - Validate ACI Fabric as L2 GW MP	Requires at least 1 Endpoint that are available for ssh to ping from
3.0.2.0	ACI - Validate ACI L2 Gateway	Requires at least 1 Endpoint that are available for ssh to ping from
3.0.3.0	ACI - Validate ACI L3 Gateway	Requires at least 2 Endpoints that are available for ssh to ping from with l3 out
3.1.4.1	ACI - Validate Import/Export Remote Location	Requires External Backup Location to be configured
3.1.5.0	ACI - Validate Intra EPG Connectivity	Requires at least 2 Endpoints th
3.1.7.1	ACI - Validate NXOS IPN Link Failure Behavior	Requires IPN Connectivity with
3.1.11.0	ACI - Validate Uplink Port Tracking	Port Tracking enabled and para
3.1.12.0	ACI - Validate Switch Profile Interface Profile Association Spine	Requires Spine Interface Profile
3.1.13.1	ACI - Validate IPN Multicast	Requires Multicast Source and L
3.1.16.0	ACI - Validate Switch and APIC Software Version	Requires finalized version
3.2.1.0	ACI - Validate BFD Sessions on Border Leaf Switches	Requires BFD Configuration
3.2.3.0	ACI - Validate External Routes Learned on Border Leafs	Requires L3out
3.2.4.0	ACI - Validate L3Out EIGRP Configuration and Adjacency	Requires L3out and EIGRP
3.2.5.0	ACI - ACI Fabric as L3 GW MP	Requires at least 2 Endpoints th
3.2.6.0	ACI - Validate L3 Domain Configuration	Requires L3out
3.2.7.0	ACI - Validate OSPF Functionality Between IPN and ACI Switch	Requires L3out and OSPF
3.2.8.0	ACI - Validate VRF Configuration	Requires VRF Configured fully w
3.3.0.0	ACI - Validate AAA Authentication Policies Configuration	Requires TACACS/ISE Configurat
3.3.2.0	ACI - Validate Authentication Fallback	Requires TACACS/ISE Configurat
3.3.2.1	ACI - Validate TACACS Authentication	Requires TACACS/ISE Configurat
3.3.2.2	ACI - Validate TACACS Local Authentication	Requires TACACS/ISE Configurat
3.4.0.0	ACI - Validate CDP Configuration and Functionality	Requires devices attached the u
3.4.1.0	ACI - Validate IPN Device's DHCP Relay Configuration	Requires IPN Device connected
3.4.3.0	ACI - Validate Global Miscabling Protocol Configuration	Requires MCP Configured
3.4.5.0	ACI - Validate Port-Channel Interface Policy Configuration	Requires Port-Channel configur
3.4.6.0	ACI - Validate ACI SNMP Configuration	Requires SNMP Server
3.4.7.0	ACI - Validate APIC Console Reachability	Requires Console Server connec
3.4.7.2	ACI - Validate APIC Inband SSH Reachability	Inband Management Configure
3.4.8.0	ACI - Validate APIC Syslog Configuration	Requires Syslog Server
3.4.9.0	ACI - Validate Global DNS Configuration	Requires DNS Server



REPORT

Log level: INFO

Jobfile Log

Generated
20221130 16:28:22 UTC+01:00
68 days 17 hours ago

Test Statistics

Total Statistics	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
All Tests	3	3	0	0	00:00:13	

Statistics by Tag	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
aci	3	3	0	0	00:00:13	
apic	3	3	0	0	00:00:13	
cait	3	3	0	0	00:00:13	
catl	3	3	0	0	00:00:13	
connectivity	3	3	0	0	00:00:13	
epg	3	3	0	0	00:00:13	
platform	3	3	0	0	00:00:13	

Statistics by Suite	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
Jobfile	3	3	0	0	00:00:27	

Test Execution Log

SUITE **Jobfile** 00:00:26.603

Full Name: Jobfile

Documentation: Validate connectivity between two endpoints attached to the same EPG Description: This test validates connectivity between two endpoints attached to the same EPG. * All devices are connected as per the main topology diagram. * All devices are powered up. * All devices are accessed via SSH using their out-of-band management interface when needed. * API calls are made to the ACI APIC's on port 443. Procedure: * Import all EPGs, Tenants, Consumer/Provider Contracts from build pipeline YAML file * Validate expected Tenants (TNs) are present in configuration * Retrieve Tenant(s) configuration * Validate expected End Point Groups (EPGs) are present in configuration * Retrieve EPG(s) configuration * For every EPG imported, validate connectivity via ICMP from hosts within the same EPG (Intra-EPG connectivity) Pass/Fail Criteria: This test passes when all of the following conditions are met:

* All expected Tenants and EPGs are present in the configuration * All Intra-EPG ICMP connectivity tests are successful for the expected EPGs.

This test fails if any of the following criteria are met:

* The device is unreachable over the network. * The device's SSH server is not responding as expected. * The APIC does not respond to API calls on port 443. * The incorrect device (as determined by the device's hostname) is accessible via SSH. * Authentication against the device is unsuccessful. * Any of the Tenant or EPG configuration is missing * Intra-EPG ICMP connectivity is not successful

CXTA_Developed_Version: 22.3

CXTA Version: 22.13

Task ID: d23534b6-70c1-11ed-9482-0242c0a8f6c3

Source: /tmp/repo/workspace/ACI/library/platform/epg/verify-intra-epg-connectivity/jobfile.robot

Start / End / Elapsed: 20221130 16:27:55.988 / 20221130 16:28:22.591 / 00:00:26.603

Status: 3 tests total, 3 passed, 0 failed, 0 skipped

SETUP Suite. **Run Keywords** load testbed "${EXECDIR}/workspace/testbed.yaml", AND, ACI REST login on "${APIC}" 00:00:00.474

TEARDOWN Suite. **Run Keywords** disconnect from all devices 00:00:01.014

TEST **ACI VERIFY IF TENANT EXISTS** 00:00:00.075

Full Name: Jobfile.ACI VERIFY IF TENANT EXISTS

Documentation: Verify the presence of tenant

Tags: aci, apic, cait, catl, connectivity, epg, platform

Start / End / Elapsed: 20221130 16:28:08.664 / 20221130 16:28:08.739 / 00:00:00.075

Status: PASS

Message: ++SUCCESSFUL++ Tenant "SERVICES" exists

KEYWORD acl-global-keywords. **ACI VERIFY IF TENANT EXISTS** tnt_name=${TNT_NAME}, APIC=${APIC} 00:00:00.072

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

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

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer 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

Contact us at:
kellyjon@cisco.com
jcomer@cisco.com

Thank you