
cisco
You make possible

Want a self-driving Data Center Network?

Try Cisco ACI with NAE

Camillo Rossi
Technical Marketing Engineer

DEVNET-2089

cisco Live!
Barcelona | January 27-31, 2020

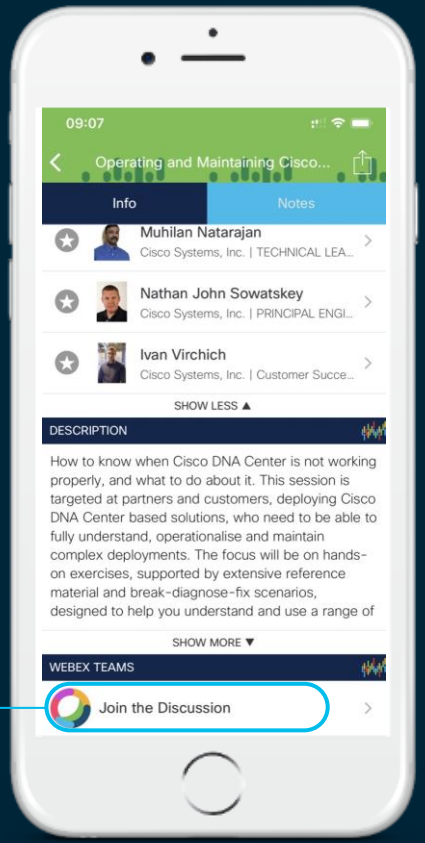
Cisco Webex Teams

Questions?

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

How

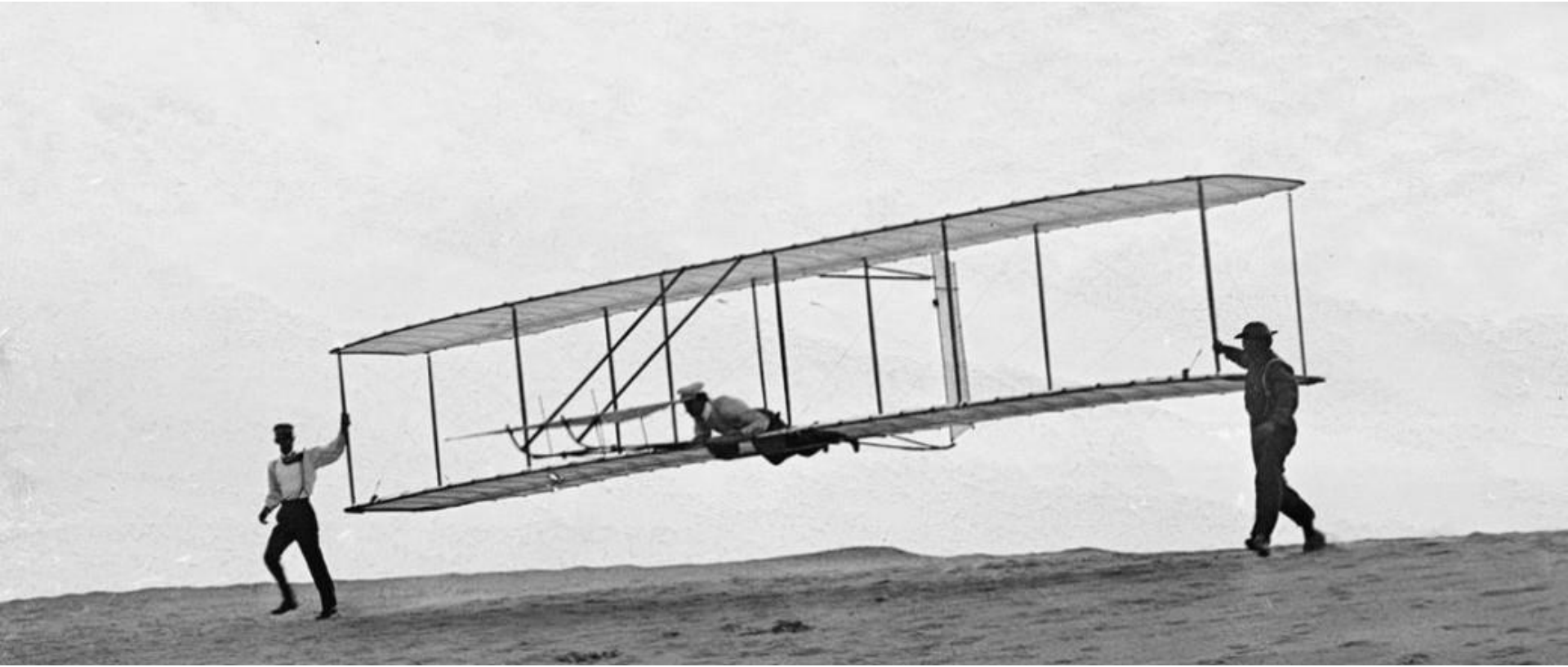
1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



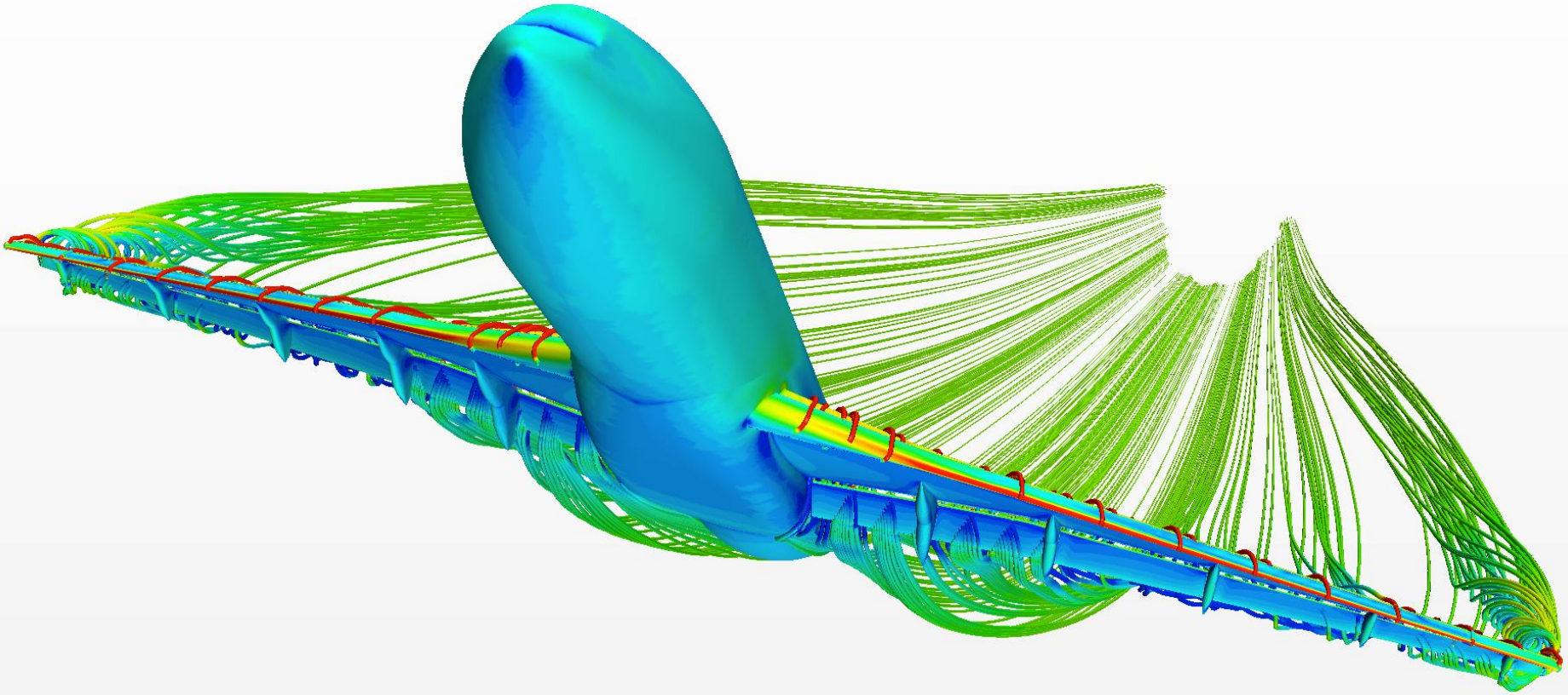
Agenda

- Challenges In A Modern Data Center
- A Solution
- A NetOps Approach
- A Use Case
- Conclusion

Year 1909



Year 2020



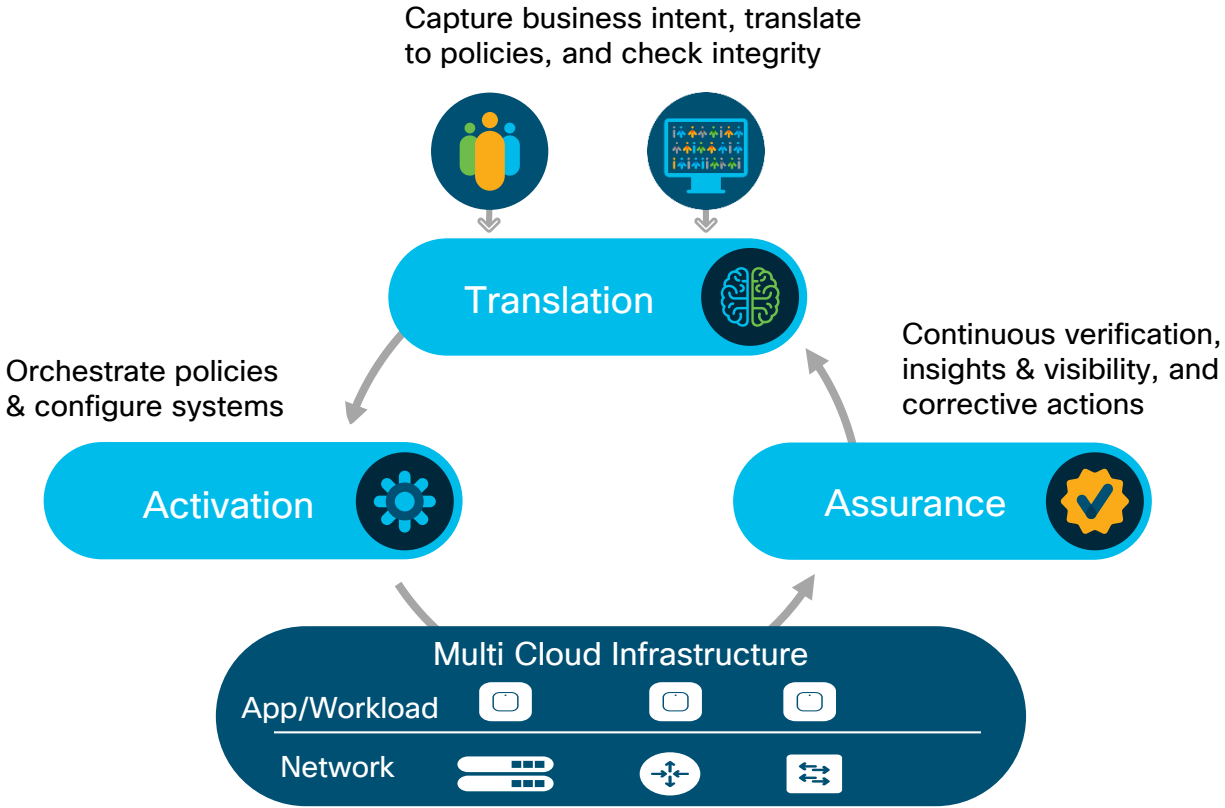
Year 1983

Can you reach the Mainframe ?

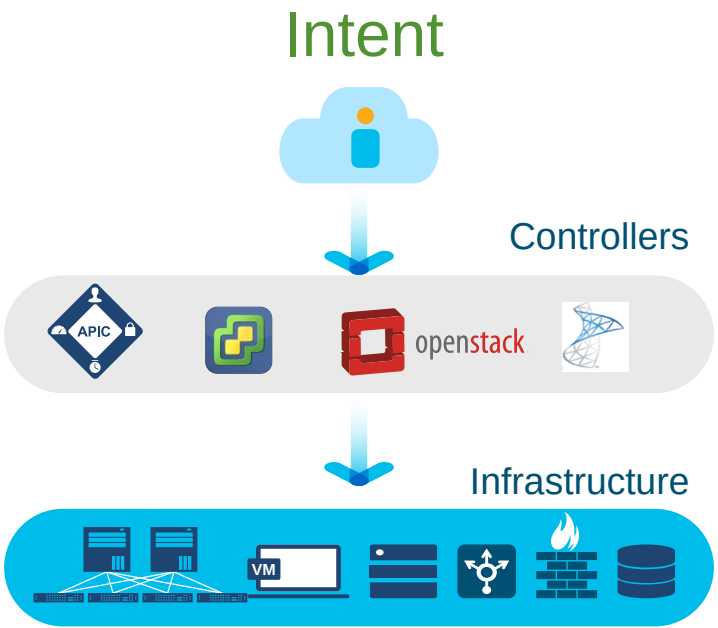
Year 2019

Can you Ping the IP of the Server ?

Intent-Based Networking in the Datacenter



Infrastructure Provisioning has Evolved with Mature Orchestration Engines



- Automated, Agile
- Highly Scalable
- Policy Based
- Virtualized

NAE Overview

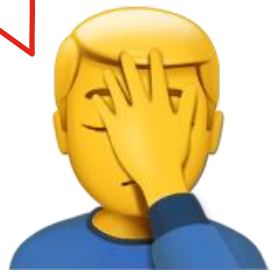
Problem: DC Paradigms Are Fundamentally Reactive

Intent Frequently Breaks …		We Always React …
Operational	→	Troubleshoot
Security	→	Scramble to fix it
Compliance	→	Fail audits
Change	→	Undo change

Leaving Us With …

An Inability to Assure Intent Proactively.

We are always in a reactive mode!



Intent Assurance

The confidence that the infrastructure is doing what you intended it to do

Intent Encompasses Data Center Operations

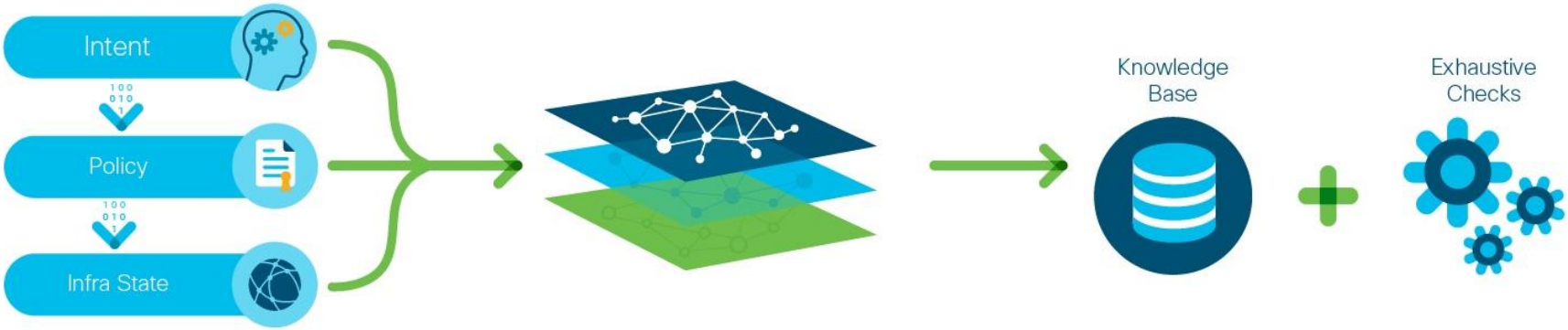
Configs, Changes, Routing, VMs, Security, … Compliance, Audits

Network Assurance Engine

Precise formal mathematical models allow you to transform network operations from re-active to pro-active

Migration | Change Mgmt. | Ongoing Optimization

Network Assurance Engine: How It Works



Data Collection

Captures all non-packet data: intent, policy, state across data center network

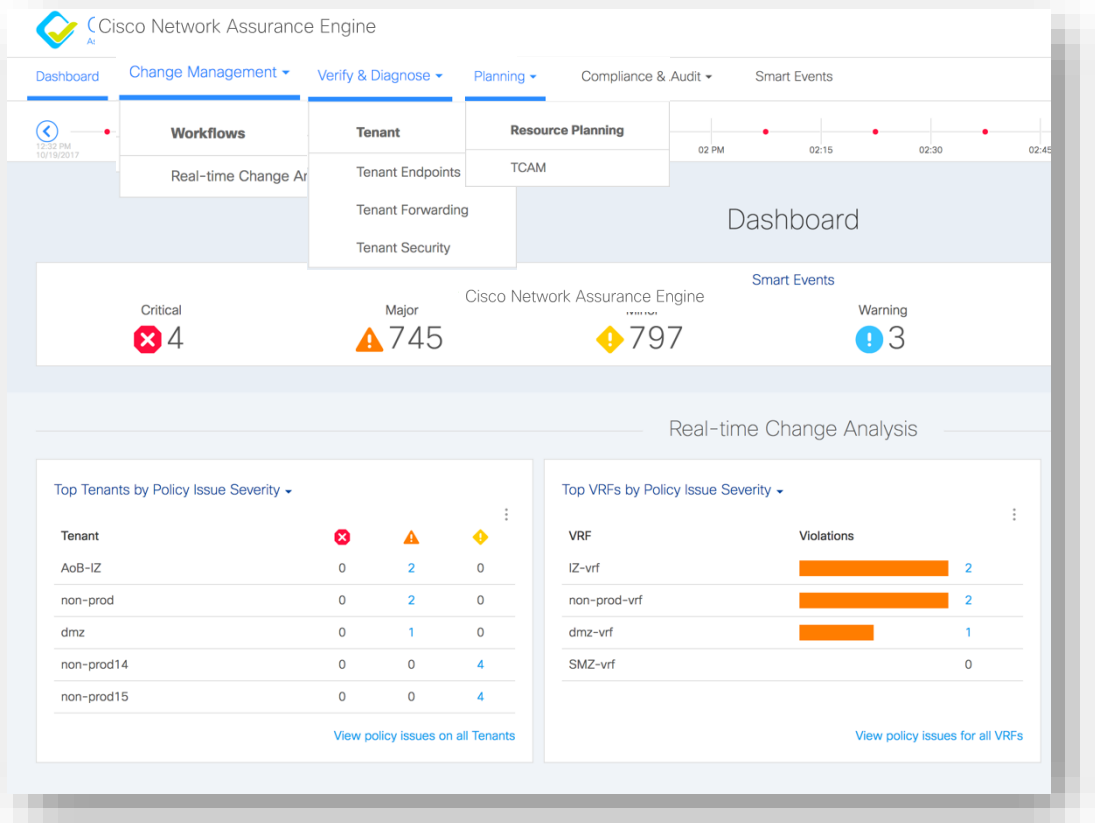
Comprehensive Network Modeling

Mathematically accurate models spanning underlay, overlay and virtualization layers

Intelligent Analysis

5000+ domain knowledge-based error scenarios built-in, codified remediation steps

Simple GUI with direct access to the information

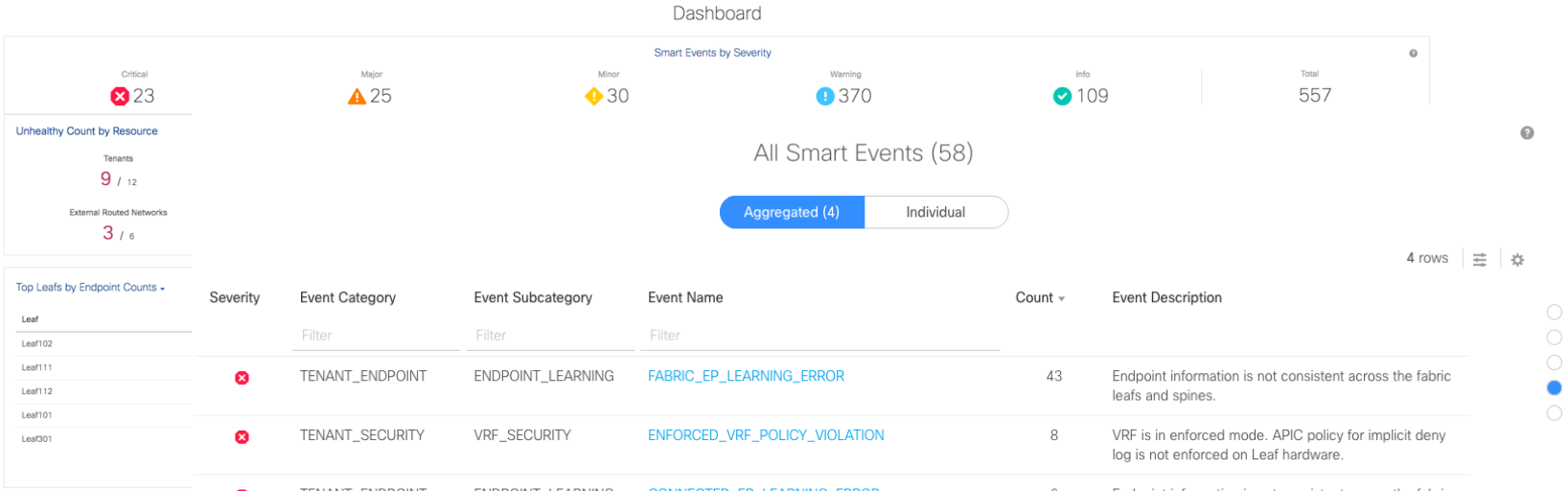


4 Main Tabs:

- Dashboard (Summary)
- Change Mgmt
- Tenant Diagnose (EP/FW/Sec)
- Planning (HW resources)

Admin Tabs & functions

- Compliance & Audit
- Smart Events



Driving Operator Confidence

What is wrong ?

Overlapping subnets

Where is the impact?

In VRF 2

What is the fix ?

Specific subnetting

Why is it wrong ?

Subnets learnt from VRF 1

Description	Communication between EPGs across VRFs is failing due to an overlapping subnet address.
Impact	Overlapping subnet configuration is causing an intermittent connectivity problem between Provide and Consumer EPGs.

Affected Objects

VRF's Tenant	VRF	Prefix
overlapErrorsNavRoutingTenant86	across_vrf_2	30.30.30.30/32

Checks

Failing Condition	Suggested Next Steps
Provider BD's/EPG's subnets or Consumer BD's/EPG's subnets are not unique across both VRFs.	• Check if Provider and Consumer EPGs are required to communicate with each other using the listed contracts. • If connectivity is required, ensure that the Provider EPG's subnet or Consumer EPG's subnet are unique across the VRFs. • If connectivity is not required, determine if you can remove the consumer (not the provider) side of the imported contract relationship.

Subnet	EPG Type	Contract	Parent EPG	Parent BD	Parent BD's VRF
30.30.30.30/32	Provider	navtest_cont_0	Across_vrf_epg2	across_vrf_bd_2	across_vrf_2
30.30.30.30/32	Consumer	navtest_cont_0	pepg1	-	across_vrf_1

Prefix	Owner BD	Owner BD's Tenant	Owner EPG	Owner L3Out	External Route	Owner VRF	Owner VRF's Tenant
30.30.30.30/32	-	-	-	L3overlapL3_across_vrf	-	across_vrf_2	overlapErrorsNavRoutingTenant86
30.30.30.30/32	-	-	-	across_vrf_l3out_1	-	across_vrf_1	overlapErrorsNavRoutingTenant86

Smart Events with Remedial Steps!

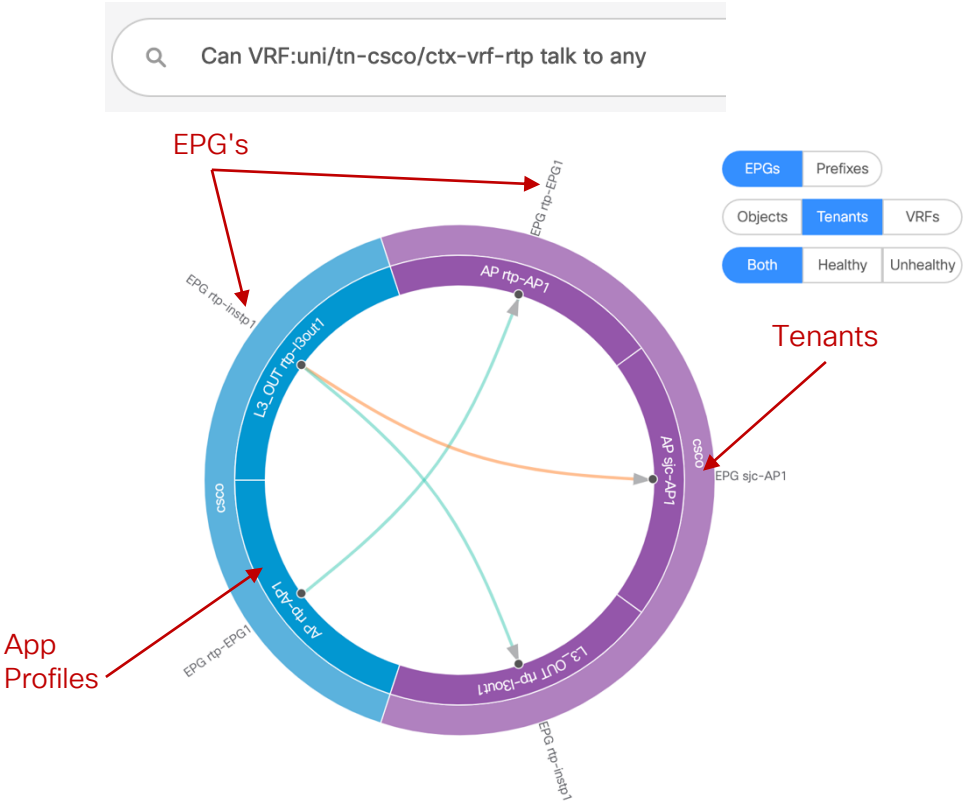
	Code
72eec6dc-1708-3c65-946f-e1e33c09cfe8-17725b858620e1e30e1086f2060baef9	4003

Policy Explorer

Policy Explorer

- Explore the ACI object models and associations
- Verify connectivity and segmentation between network assets
- The Explorer feature is based on natural language query interface. The types of queries supported by the feature include:
  - What Query: Answers how the different ACI networking entities are related to each other.
  - Can Query: Answers whether the entities in the ACI policy can communicate with each other. Can queries can also be used to determine if the entities in the ACI policy can communicate using protocols such as TCP, UDP, or ICMP and the source and destination ports used for communication.
  - How Query: Provides details on the communication between the entities in the ACI policy.
  - View Query: Provides the visual indication of the interface status for any leaf switch in the assurance group.

Ability to Explore your policies

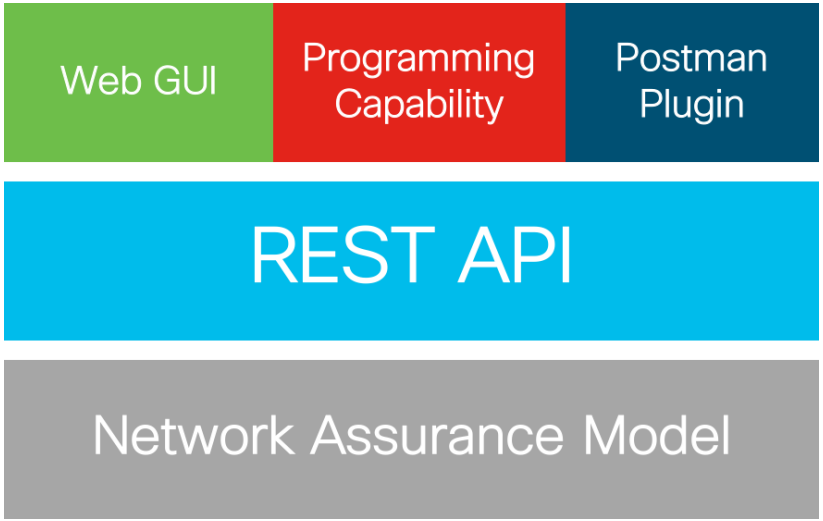


- **Value**: NAE allows to easily analyze the policy space to answer the question:
  - Are all necessary policies against EPG-n correctly configured ?
  - Can EPG-A talk to EPG-B based on policies within my Tenant?
  - Are all the contracts required correctly configured or are there any missing?
  - Do we have consistency among all policies to provide the expected Tenant security?
  - Color coded to easy point out issues

Network Assurance Engine APIs

NAE APIs

- Same objects irrespective of interface
- True REST API targeting “resources”
- Programmatic access to all assurance models
- Fully automatable management of NAE

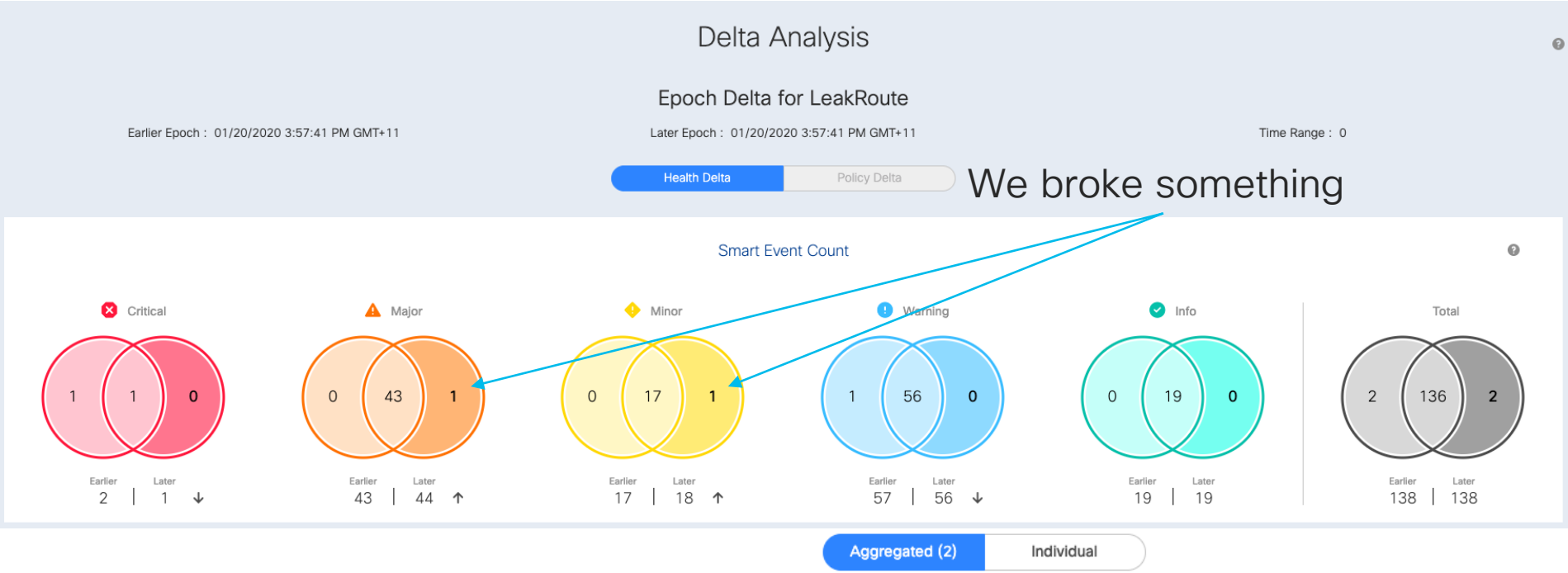


Demo Time!
Will my Change be successful?

Pre-Change Analysis

- Pre-change analysis (PCA) allows modelling the intended changes in Cisco NAE, and verify if the changes generate the desired results.
- The Changes can be modelled:
  - On the GUI, in cases where no ACI pre-prod/test environment is present
  - Imported as a JSON/XML file, where an ACI pre-prod/test environment is present
- A Special PCA Epoch Delta is generated to inform the user of potential impacts

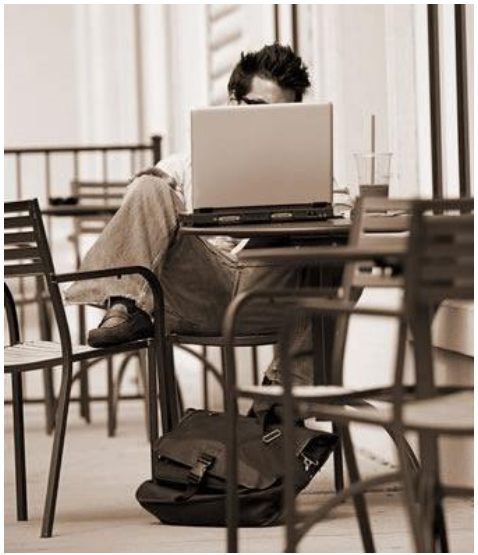
Pre-Change Analysis – Result Example



Severity	Event Category	Event Subcategory	Event Name	Epoch	Count
⚠	CHANGE_ANALYSIS	FORWARDING_POLICY	OVERLAPPING_SUBNETS_ACROSS_BDS_ACROSS_VRFS_DUE_TO_CONTRACT		1
⚠	CHANGE_ANALYSIS	FORWARDING_POLICY	BD_WITH_NO_L3OUT_HAS_SUBNET_MARKED_EXTERNAL		1

Design

In the café



Feedback

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

cisco Live!

Continue your education

Demos in the Cisco campus

Walk-in self-paced labs

Meet the engineer 1:1 meetings

Related sessions

Thank you

cisco Live!

You make **possible**