Cisco IT Network Assurance Engine Deployment

This white paper is one in a series of case studies that explain how Cisco IT deployed ACI to deliver improved business performance. These in-depth case studies cover the Cisco IT ACI data center design, migration to ACI, the ACI NetApp storage area network deployment, compute at scale with AVS, UCS, KVM, and VMware, Tetration analytics (parts 1 and 2), ACI OpenStack automation, and Network Assurance Engine. These white papers will enable field engineers and customer IT architects to assess the product, plan deployments, and exploit its application centric properties to flexibly deploy and manage robust highly scalable integrated data center and network resources.

Contributors to this white paper from the Cisco IT include Vishal Soni, Sr Engineer, and Benny Van De Voorde, Principal Engineer.

Version: 1.1, June 2020 – updated with copy edits for clarity.

Americas Headquarters

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

http://www.cisco.com

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

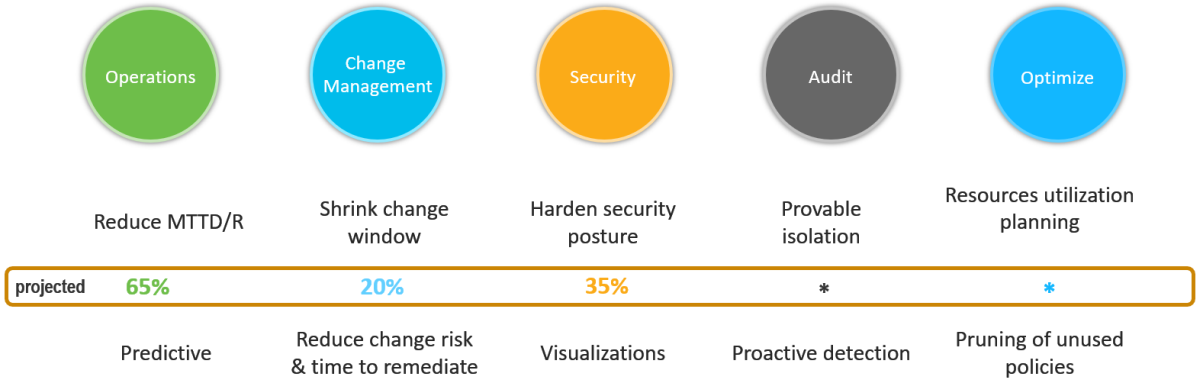
Table of Contents

Cisco IT Network Assurance Engine Deployment

The Cisco IT data center environment deploys thousands of applications that support the enterprise, its partners, and customers. Cisco ACI technology easily provides great value in automating operations of classical networking processes. Cisco ACI enables Cisco IT to use a common application-aware policy-based operating model across their entire physical and virtual environments.

The Cisco Network Assurance Engine (NAE) improves business performance by transforming operations in software-defined datacenters through continuous network verification and analysis.

Cisco IT NAE Business Benefits



Cisco IT uses NAE to transform ACI network operations from a reactive posture to a highly proactive approach. As Cisco IT Sr Engineer Vishal Soni says, "There is simply no other way to drive down MTTR for incidents, shrink change windows, and optimize planning in large scale data centers as effectively." This white paper shows exactly how Cisco IT made this happen with CNAE.

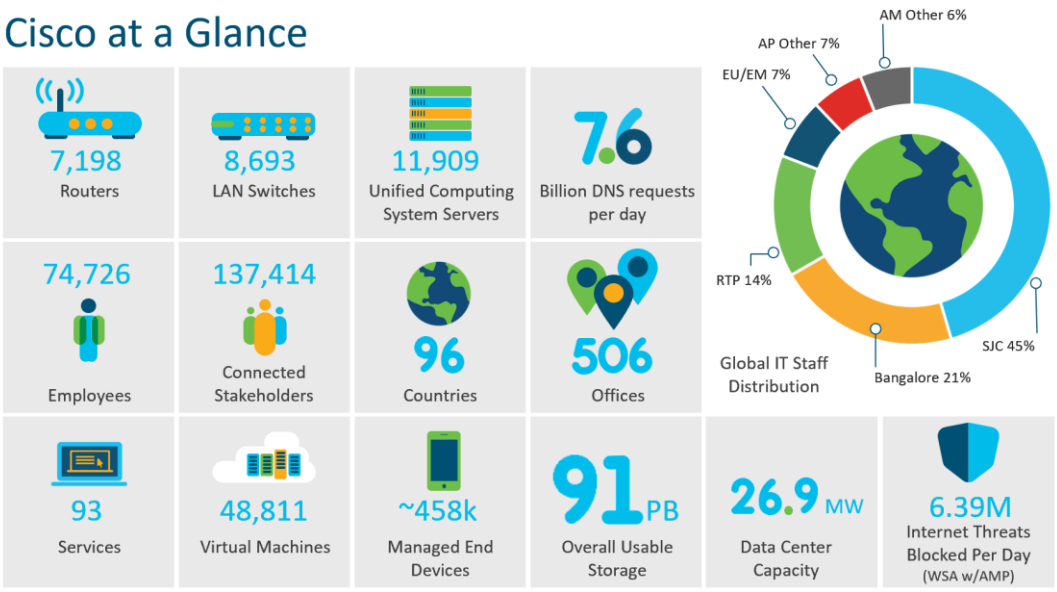
This white paper provides a brief overview of Cisco IT operations, intent-based data centers, NAE, and an in-depth case study of the Cisco IT deployment, including installation insights, operational use cases and incident lifecycle integration with Splunk and ServiceNow. It shows how Cisco IT uses NAE to plan network capacity, and proactively detect and resolve issues before they impact the business.

Cisco Intent Based Data Center at Scale

Business needs have forced a fundamental shift in data center architectures. Data centers are becoming the heart of enterprises, and they are growing rapidly in every dimension. They are increasingly sophisticated, with multiple tenants, and workload placement in hybrid cloud infrastructure. Most of all, they are constantly changing with auto-scaling applications, VM mobility, and self-service portals.

The Cisco IT organization operates multiple business application and engineering development data centers distributed around the world.

Cisco IT Data Center Operations at a Glance



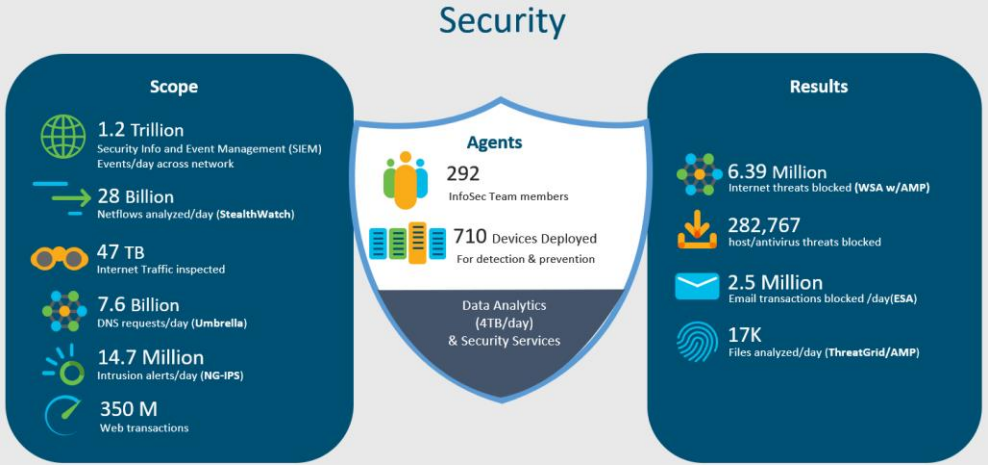
Cisco IT supports more than 100 services, more than 3,000 production and non-production applications and about 200,000 endpoints providing 24x7 support worldwide with nearly five 9s uptime.

The infrastructure for the core Cisco business data centers (DC) is big. For example, the Allen, Texas DC alone includes 856 network devices that support 2300 traditional and private-cloud applications, run 8000 virtual machines, including 1700 Cisco Unified Computing System™ (Cisco UCS®) blades and 710 bare metal servers, with 14.5PB of NAS storage and 12PB of SAN storage. Cisco is driven to migrate to ACI because, as its data centers grow, quick and agile application deployment becomes increasingly challenging.

However, data center operations are typically reactive. Forensics are characterized by long troubleshooting cycles and war-rooms. Rollbacks driven by change mistakes happen often. Frequently, initial audits fail because policies do not comply with business intent. Fundamentally, data center operations lack the ability to proactively assure intent before changes are made.

With Cisco ACI, Cisco IT can deploy an intent-based data center architecture at scale. This enables Cisco IT to enhance its security posture, and deliver the business results the enterprise needs.

Cisco IT Intent-Based Data Center Enables Enhanced Security Posture



Examples of intent are, "Block production applications from communicating with non-production applications" or "export a subnet to a WAN."

Cisco IT Intent-Based Data Center

With ACI as the foundation, Cisco IT chose to use Tetration Analytics and Network Assurance Engine (NAE) to build out its intent-based architecture. Tetration enables knowing *what has already happened* in the data center at scale. Because it learns what is actually happening, it enables enforcing policy across multicloud data centers using consistent segmentation with security policies that minimize lateral movement. Tetration cannot see a problem in a configuration that has not happened yet because no traffic has yet to expose the configuration problem. NAE intent intelligence enables you to know what could happen *before* it occurs and assures that your network will perform exactly as intended. NAE warns you about configuration problems before you deploy them or before traffic has hit them.

The ACI intent-based infrastructure improves network availability and agility. Compared with traditional prescriptive approaches, what makes intent different?

- Intent is "I need to go to the airport"; prescriptive is "turn left here, yield to traffic on the right…"
- Intent is "Allow application XYZ connect to the Internet"; prescriptive is "allow packets matching this specific 5-tuple out of switch port 13"

How we use NAE to realize the intent-based data center:

- Algorithmic validation after pushing new configuration
- Automated and orchestrated provisioning to reduce errors and misconfigurations
- Continuous validation in real-time to detect outages and degradations
- Reduced operating expenses
- Performance optimization

NAE provides lifecycle management – design, implementation, operation, and assurance.

Intent-based data center architecture enables better data center performance at scale:

- Translation and validation – from the business what to infrastructure configuration how and proving the "correctness" of configuration before deploying.
- Automated orchestration/implementation – system can configure changes across existing infrastructure
- Awareness of state – system ingests real-time status
- Assurance and dynamic optimization/remediation – continuous, real-time validation. Mathematical validation that business intent and configurations are in sync; take real-time action if out of sync

These advanced capabilities of the Cisco IT intent-based data center architecture contribute to valuable business outcomes.

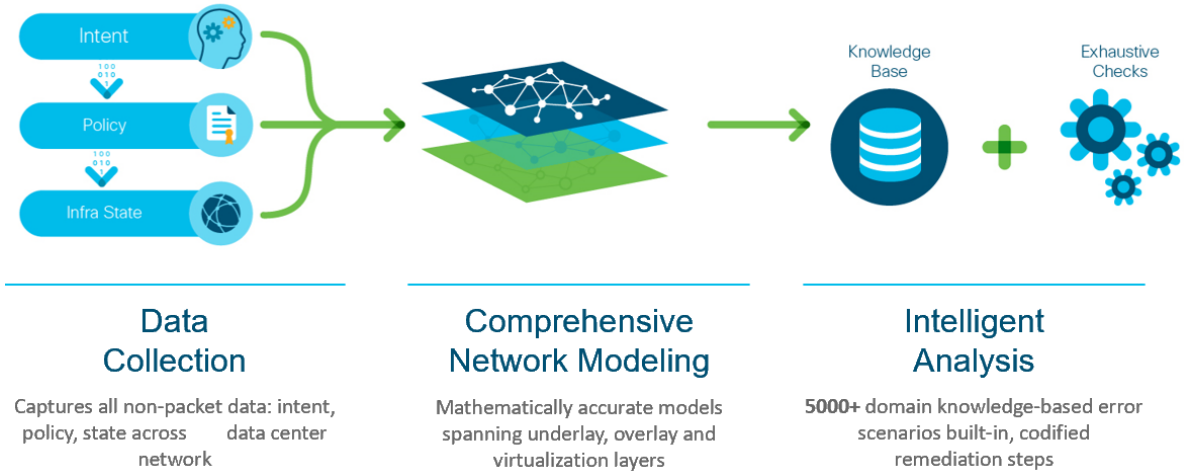
Cisco IT Intent-Based Data Center Contributes to Valuable Business Outcomes

We transitioned to the intent-based data center by enabling existing products to plug into this architecture, and gradually enabled these functionalities.

Cisco Network Assurance Engine Overview

Cisco Network Assurance Engine (NAE) NAE is the critical intent assurance pillar of the Cisco vision for intent-based data center networks. It transforms operations in data center networks to a more proactive model.

Cisco Network Assurance Engine



NAE gives operators the confidence that their network is always operating consistently with their intent by performing the following key functions:

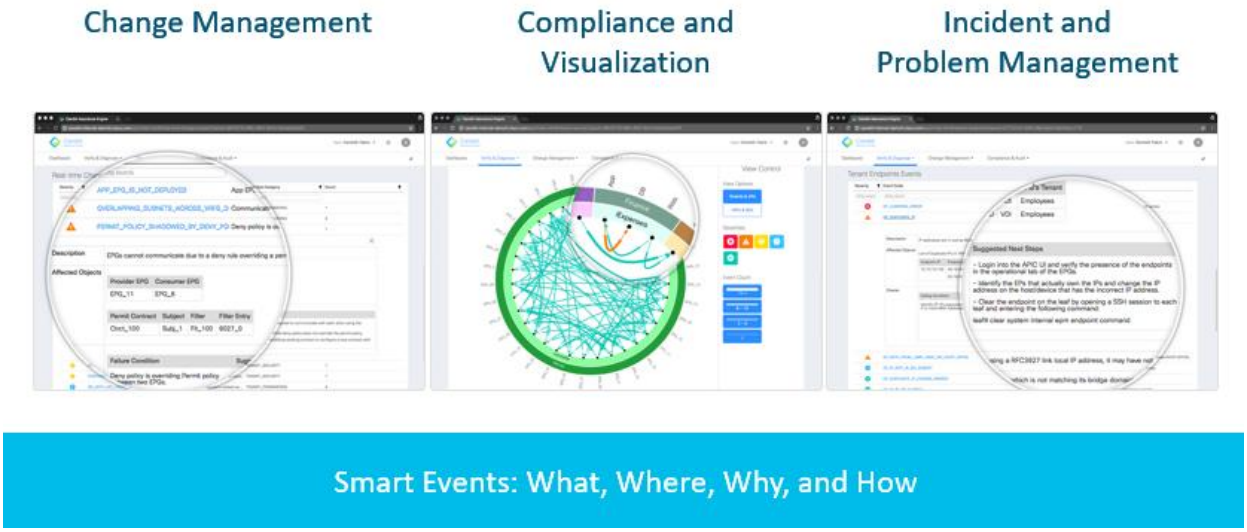
• **Predicts the impact of changes**: Proactively verifies changes for correctness, bringing increased change agility while reducing risk of human error–induced network failures.

• **Verifies network-wide behavior**: Continuously analyzes and verifies the dynamic state of the network against intent and policy to ensure connectivity and eliminate potential network outages and vulnerabilities before any business impact occurs.

• **Assures network security policy and compliance**: Assures network security policies and checks for compliance against business rules to reduce security risk and achieve provable continuous compliance by policy and state.

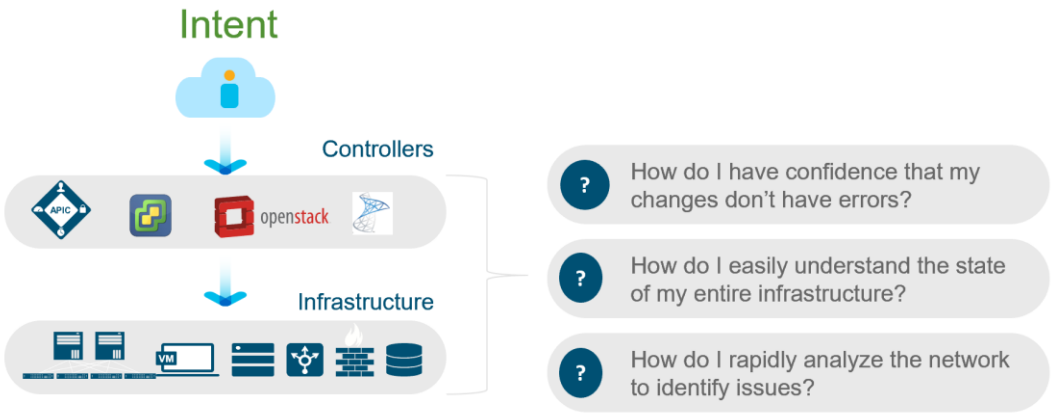
NAE achieves its results by continually reading every configuration, the network-wide state, along with the operator intent from the deployed policies. In periodic intervals it calls epochs, NAE reads ACI logical and concrete model configurations, infrastructure information, routing tables, TCAM entries, and more periodically from ACI controllers and switches. From these, it builds accurate comprehensive mathematical models of network behavior. It then delivers insights into data center operations by combining these models with Cisco's more than 30 years of knowledge of networking.

Cisco Network Assurance Engine Insights



NAE provides insight into what went wrong, and pinpoints issues like bad state, policy conflicts, TCAM waste, routing loops, and security holes. The result is automatically generated smart events that instantly pinpoint any deviations from intended behavior and suggest expert-level remediation.

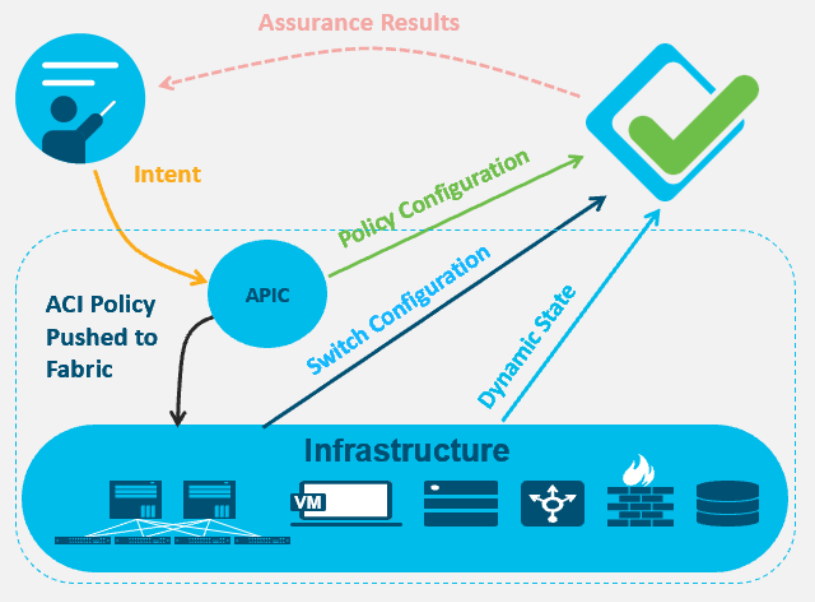
Network Assurance – Configuration



I'm making changes to the network: how do I know that I haven't introduced some latent misconfigurations or errors that will bring down the application a couple of weeks from now? Maybe the security policy I programmed is conflicts with an existing deny policy I don't know about, or I am programming a subnet that overlaps with an existing subnet. Or I migrate 500 VLANs from the legacy network to my new fabric but make typing errors for 5 subnets. Likely, I'll only know about its weeks from now when some apps are not accessible, and it then takes days to debug the errors. NAE proactively analyzes policies

and configurations for correctness and consistency and tells you if you are making mistakes.

Network Assurance – Dynamic Change

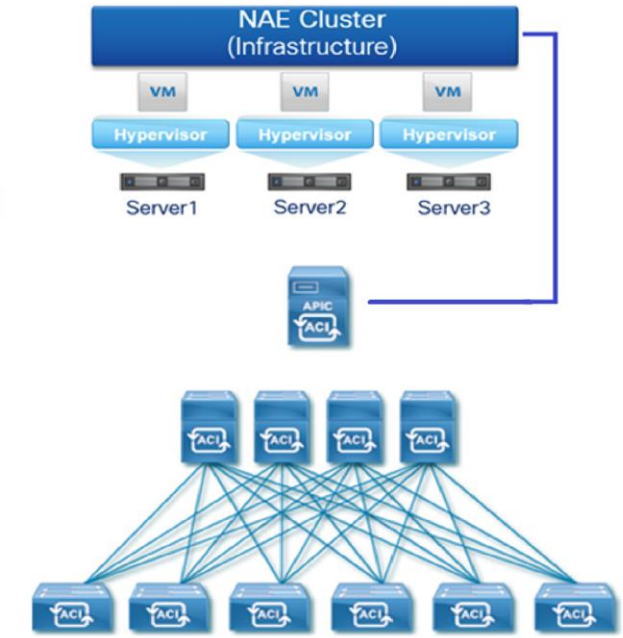


In the ACI framework, with tenants, app profiles and EPGs, it is helpful to be able to quickly identify bridge domain and VLAN sittings, or where EPGs are deployed, or how connectivity is established between A and B. NAE correlates the state of the network to the configured policy, so issues are resolved much faster.

Modern data center systems are dynamic, complex distributed systems. The fabric learns routing prefixes from the outside world; routing loops can develop in the forwarding tables; or we learn a more specific route from the branch so that traffic meant for an internal application is diverted outside. Maybe the default gateway doesn't get correctly programmed due to a connectivity issue, or a leaf switch ran out of TCAM space, so policies aren't deployed correctly. These are transient vulnerabilities. A VMWare admin could create a configuration mismatch by programming port groups that are inconsistent with the APIC. These are extremely hard to find issues, but they are critical to identify because of the problems they cause. NAE addresses this gap by continuously analyzing the dynamic state of the entire network to ensure it is always configured consistently with your intent.

The NAE platform can be deployed on-site as a simple preconfigured 3 VM cluster.

Cisco NAE form factor



NAE is a lightweight, small footprint, set of 3 preconfigured VMs, that takes 30 mins to deploy. No sensors needed - simply point it to the APIC. In one hour, it captures the state of the fabric.

Cisco IT NAE Case Study

Starting in June of 2017 with NAE v1.0, Cisco IT started with assuring the core ACI fabric, and quickly added assurance support for network services such as load balancers, firewalls, as well as virtual machine managers such as vCenter.

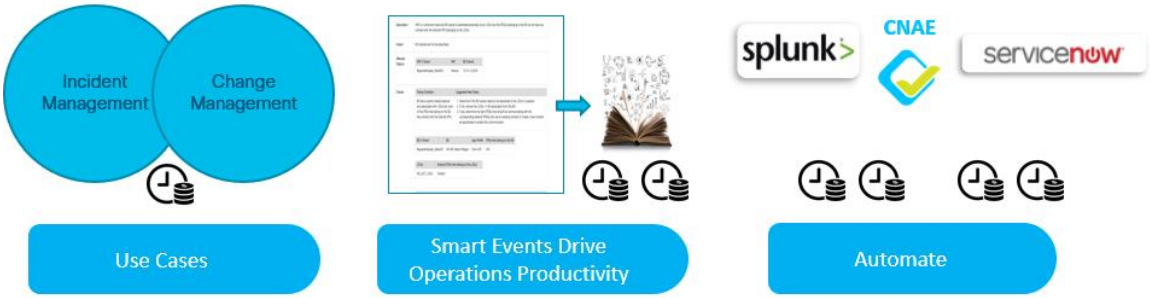
Cisco IT Current NAE Deployments

Fabric	Assuring	Lifecycle	ACI	CNAE Image & Version
Non-Prod Fab 1	Non-Prod Fab2	Non-Prod + DR	3.2 (4e)	IAE-V1000-M10, 3.0(1)
Non-Prod Fab 2	Non-Prod Fab1, Fab 3	Non-Prod + DR, Openstack	3.2 (4e)	IAE-V1000-M10, 3.0(1)
Prod Fab 2 (ALLN)	Prod (RCDN) Fab 1, Fab 3	Prod, Openstack	3.2 (4e)	IAE-V1000-M10, 3.0(1)
Prod Fab 1 (RCDN)	Prod (ALLN) Fab 2, Fab 3	Prod, Openstack	3.2 (4e)	IAE-V1000-M10, 3.0(1)
SVL Fab 6	SVL Fab 7	Lab	3.2 (4e)	IAE-V1000-M10, 3.0(1)
SVL Fab 7	SVL Fab 6	Lab Openstack	3.2 (4e)	IAE-V1000-M10, 3.0(1)

Cisco IT NAE Journey

NAE needs to fit into the broader operational toolchain IT organizations use to operate their data centers. The ecosystem team integrates NAE with key products.

Cisco IT NAE Journey

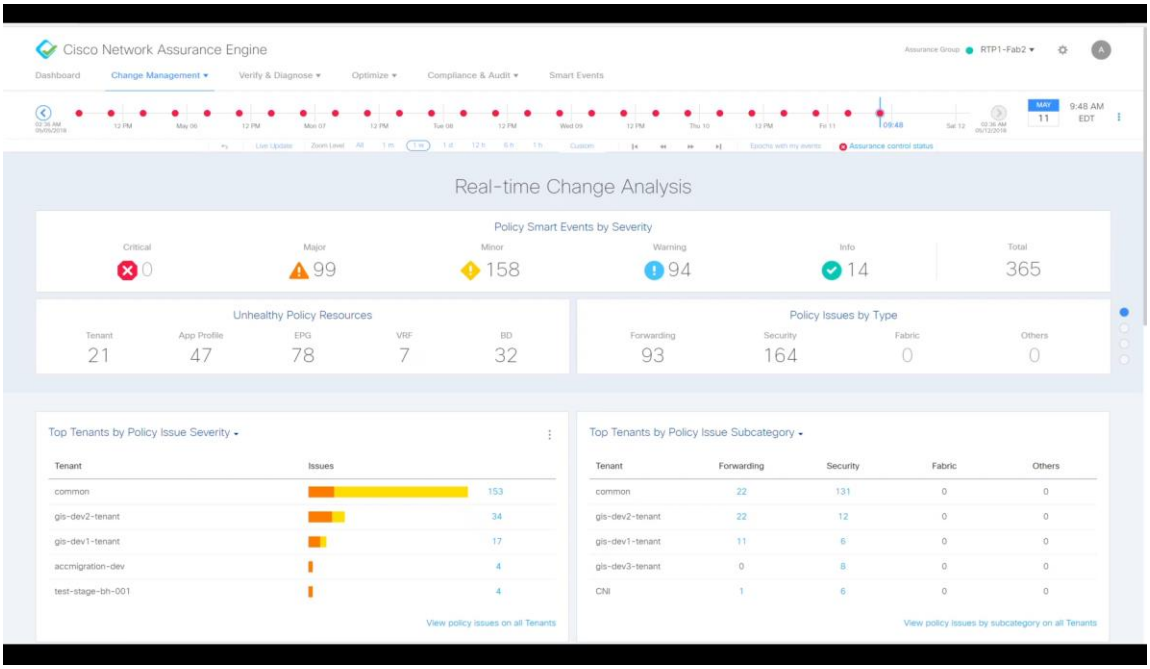


There are certified Splunk and Service Now apps for automating remediation and event correlation, as well as a Turbonomic app for intelligent workload placement.

Conventional troubleshooting methods produce inconsistent results and depend on the skill set of the staff. The ability to uncover the root cause of a problem, and the time it takes to troubleshoot a problem can vary according to the skills of those performing these tasks. Typically, runbooks, job aids, and training are used to address the problem of inconsistency.

NAE improves this process by providing reliable insight into the complete state of the data center and its configuration.

NAE user interface features progressive discovery of network state information



At the very top, NAE presents a summary view of its findings. NAE periodically collects information in time segments it calls an epoch. An epoch can be examined in more detail. Misconfiguration events are organized by severity levels and object type. Examples of events include stale policies, undeployed EPGs, missing contracts or misconfigured contracts. Events can be searched and filtered so that you can quickly get a detailed description of the event, along with clear guidance to resolve the issue.

Change Management with Assurance

Before NAE, the toolset Cisco IT used was seriously lacking - not much more than eyeballing, giving it a soak test, and hoping nothing fell apart. If a change was unsuccessful, roll it back. Multiple change windows were needed to accomplish a change.

Cisco IT Change Management with NAE

Cisco IT integrated NAE in our change management process. Now, after pushing the change, we instantly validate the change with NAE. Validation goes beyond checking configuration issues due to human errors; it gives us confidence that there are no stale configurations that might cause problems.

Cisco IT has been using NAE to systematically remove configuration issues. The result is that the number of NAE Smart Events has gone down by 39%, and the system health score that the APIC reports has gone up from 79% to 88%.

In the future, NAE will be able to model changes before deploying them, which will enable pre-validation, shortening approval times and driving change agility.

Examples of issues NAE flags

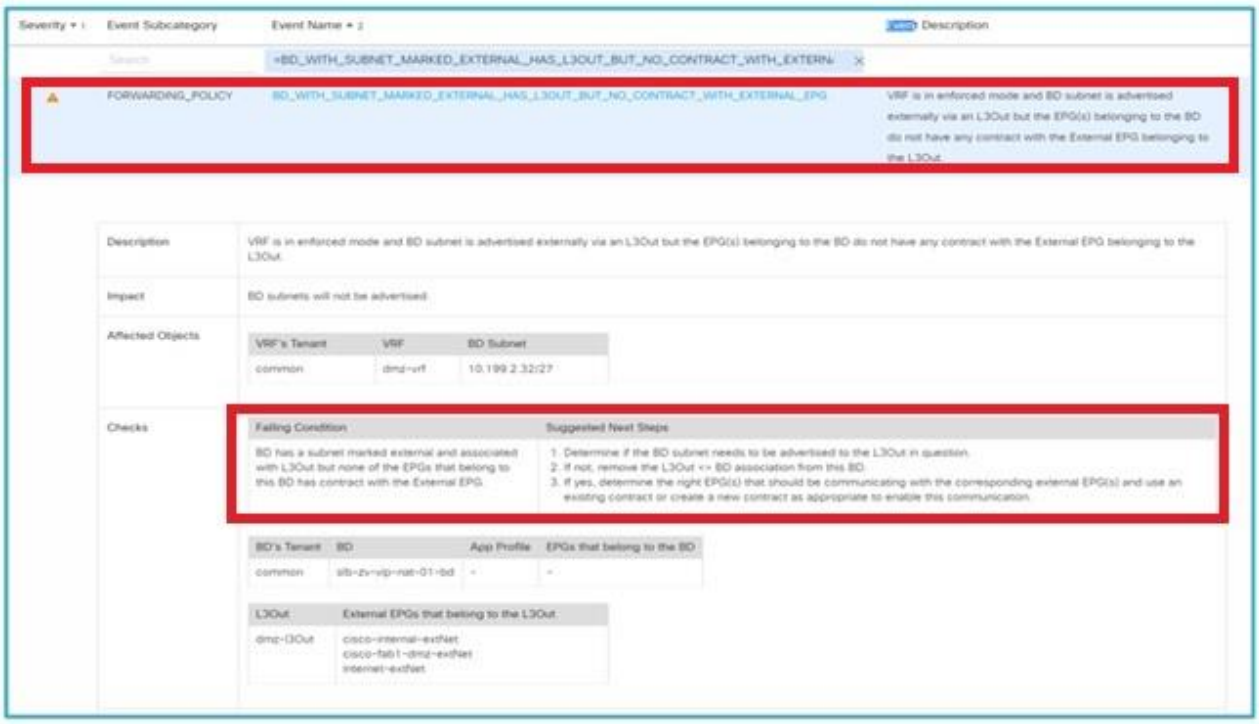
- Tenant Connectivity Loss
  - ✓ PERMIT_POLICY_VIOLATION
- Tenant EP Mobility Impact
  - ✓ EP_DUPLICATE_IP
  - ✓ EP_IP_NOT_IN_BD_SUBNET
  - ✓ EP_DHCP_ERROR
- Tenant Policy Impact
  - ✓ ALLOW_TRAFFIC_ALIASED
  - ✓ POLICY_OVERSPECIED
- Tenant Security Violation
  - ✓ DENY_TRAFFIC_VIOLATION
  - ✓ LOG_TRAFFIC_POLICY_VIOLATION
- Resource Impact
  - ✓ TCAM_OVERFLOW_WARNING
  - ✓ BANDWITH_UTILIZATION_WARNING

NAE proactively provides deep visibility by running 1000s of checks. To call out a few, it can find issues with the network underlay and detect loops. At the virtualization layer, it detects static issues and dynamic issues. This removes a lot of manual effort. Cisco IT modified our run books and now, NAE is the first place we go to validate that the network is behaving as we expect it should. This has greatly improved our operations efficiency and productivity.

The following story illustrates our experience. We migrated an application that needed load balancing which was in the DMZ. We knew how to do this. During the change window, with cutsheets ready, we loaded the load balancer (LB) configuration and the server load balancer (SLB) EPG in 20 mins. Compute migrated the VMs and brought services up on

the backend servers. The virtual IP (VIP) for the SLB did not come up but bypassing the VIP and connecting directly to the backend, the application worked fine. We checked for issues to explain why there was no access to the VIP from outside the fabric. We checked the LB for possible causes. Checked probes. Checked reachability of backend server from LB. The gateway was up, but still the VIP wouldn't ping from outside. Even wiped and re-built the entire LB config, but still no luck. After more than 6 hours, someone on call discovered that a contract was missing. How could we have missed that? We realized this is in the DMZ. All that time spent troubleshooting the LB when we should've been looking elsewhere.

NAE Smart Event identifies failed condition and recommends next steps



Instead of the scenario above, an NAE smart event flags the issue as a "BD has a subnet marked external and associated with L3Out but none of the EPGs that belong to this BD has a contract with the external EPG." Furthermore, NAE provides these suggested next steps: "1. Determine if the BD subnet needs to be advertised to the L3Out in question; 2. If not, remove the L3Out<BD> association from this BD; 3. If yes, determine the right EPG(s) that should be communicating with the corresponding external EPG(s) and use an existing contract or create a new contract as appropriate to enable this communication"

Proactive Incident Management

How can NAE help before users notice degradation in application performance? NAE Smart Events warn of impending incidents.

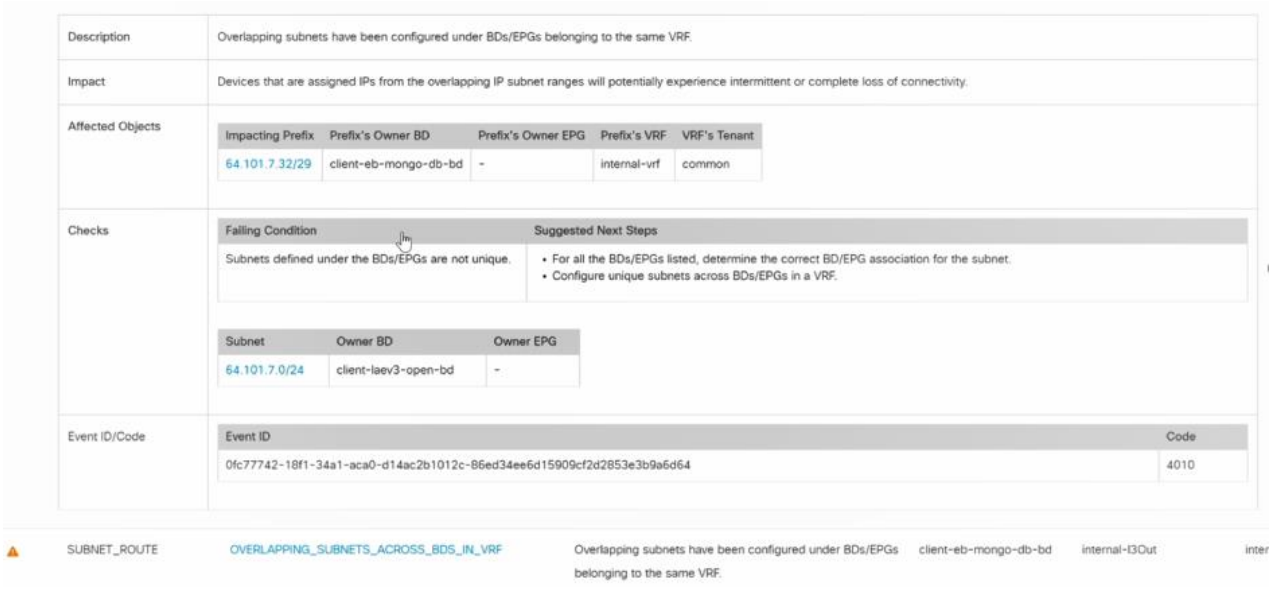
The Cisco IT container platform called CAE hosts multiple applications, some bandwidth sensitive. NAE flags a critical event regarding reduced bandwidth that impacts performance for one or more applications hosted on the CAE platform. While traditional monitoring tools show a link is down, NAE goes on to pinpoint the EPG, application profile, and tenant affected by this event. This enables Cisco IT to fix the problem before users notice any degradation.

Troubleshoot VM reachability – a Forwarding Issue

Conventional troubleshooting of VM reachability includes tools like PING, trace route, the APIC EP Tracker for validating connectivity, checking for packet loss, and locating an endpoint. The default gateway for the subnet of that VM would be examined. APIC has visualization tools. The APIC CLI and MOquery can show the IP, MAC and EPG. The Mongo DB EPG is suspected. Check APIC for learning on the EPG. Notice something interesting – on a leaf node no IPs are being learned. We look for APIC faults. In this case, no flaunts flagged for this EPG. Instead, NAE simplifies this process

Tenant Forwarding Troubleshooting with NAE

Using the NAE GUI, you can drill down from the Dashboard by selecting a collection point called an EPOCH, then select Verify & Diagnose/Tenant forwarding to isolate reachability issues.

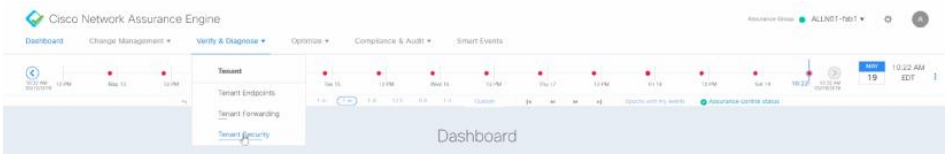


Because this is a layer 3 forwarding issue, we filter NAE events on bridge domain (BD), and specify the BD name. NAE immediately reports an event showing overlapping subnets. NAE identifies devices that are assigned IPs, which shows 70% packet Loss, and goes on to show the impacting prefix, failing condition and that the traffic to devices in the

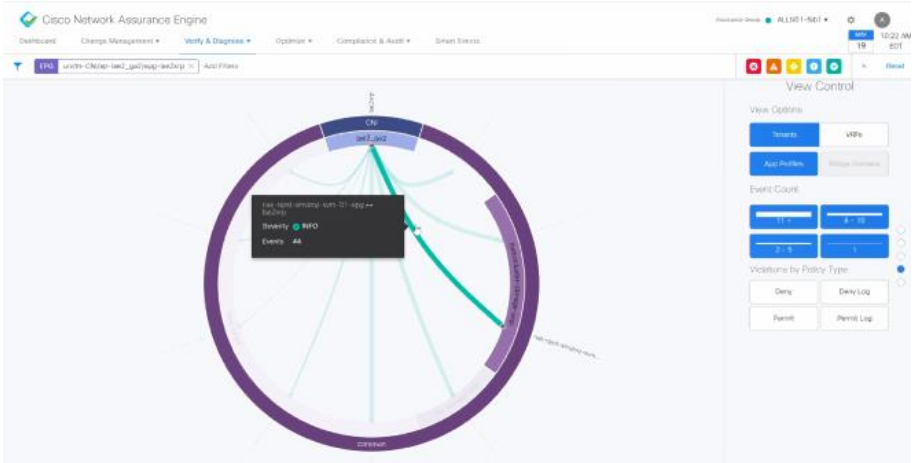
Mongo DB disappear without a trace. This is a needle in a haystack problem to troubleshoot. NAE cut down the time to resolution on this issue and MTTR overall! NAE provides the most accurate and current view of the running state of the data center. This is a fundamentally new way of doing network operations.

Troubleshoot Contract Issues

A user from the application team reports that their host in EPG A cannot communicate with EBG B. In a traditional approach, we used the APIC GUI - log on to APIC > go to Ops Tab > input source/destination endpoints. Once the topology is generated you see leaf switch pairs on which the endpoints are learned and the interface details between the leaf and spine switches and leaf switch and southbound connectivity VMM domain. It generates a complete list of contracts that are deployed between the EPGs. Another way to investigate this is via the CLI to establish whether a certain TCP port is permitted between the EPGs or use creative regex on the switch to verify if the rule is programmed in the hardware. All these steps take time. The stakeholder is anxious about significant dollar loses because of this issue. Custom in-house scripts check for such problems. But, while the script works well, it is a challenge to use well.



In the NAE dashboard, we select the appropriate EPOCH, and drill down on a connectivity issue between EPGs by selecting security (contracts).

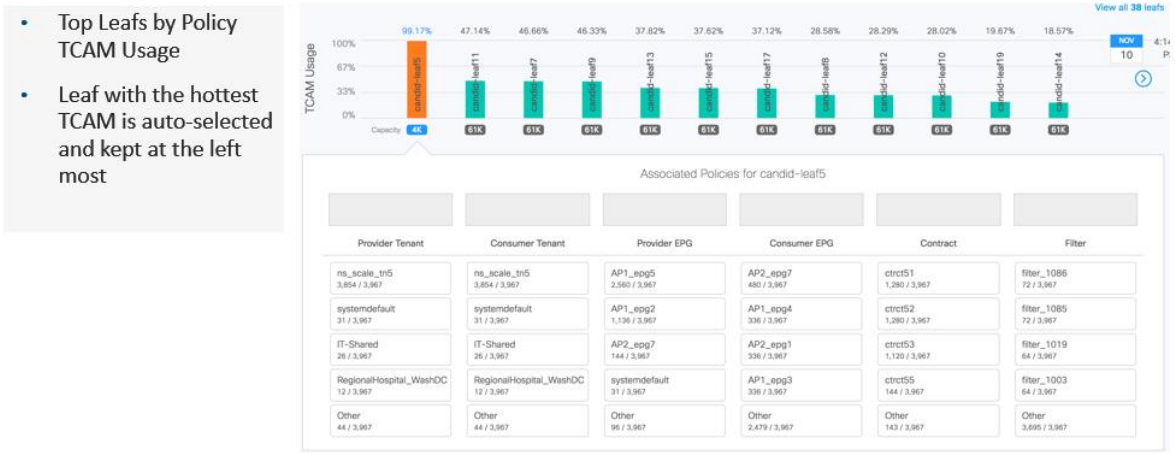


NAE provides a visual representation of all security policies (contracts) for that EPG ... Outer ring / inner ring / dot / arc. A single view provides a complete representation of all policies and enforcement state in the hardware on every leaf across the fabric. Next, with a single click, drill down to examine not just the configured policies, but also the dynamic state between the 2 EPGs in question. This is not only useful for troubleshooting contract issues but can be used for compliance & audit. For example, the finance tenant must be completely isolated. The NAE visualization shows if the isolation is complete or not.

Optimization

NAE provides a holistic view of resource utilization, specifically TCAM.

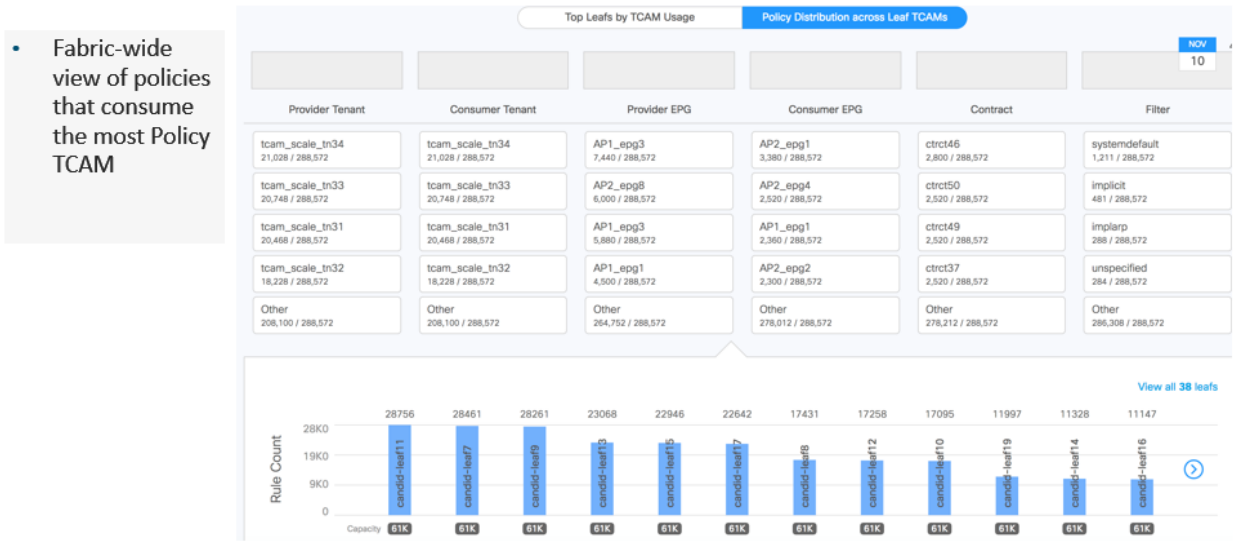
Resource Optimization – using NAE to identify leaf switches with highest TCAM use



After operating ACI for more than 3 years, Cisco IT had streamlined its processes for brownfield migration and successfully migrated several applications, mostly in the application-centric way. Last year, Cisco IT wanted to accelerate the migration process and started using a network centric approach. Typically, this meant doing a mass migration of multiple applications in a dedicated subnet. When migrations were fully in progress, they hit a roadblock. During one change window, the APIC errors led them to discover that the migration was resulting in 170% TCAM utilization. TCAM space is limited. As policies grew with each new EPG, so did TCAM utilization. As a result, they had to pause the application migrations. The manual remediation approach would be to first identify which applications to remove and then identify which to optimize. This would be a huge

task to perform on hundreds of EPGs. As network operators, we don't want to delete

Resource Optimization – using NAE to identify policy distribution across TCAMs



Instead, the NAE visualizations show which policies are not in use and which ones are consuming the most TCAM. This enables Cisco IT to easily plan, and accurately forecast and manage their data center growth.

Integrating NAE with Change and Incident Management Systems

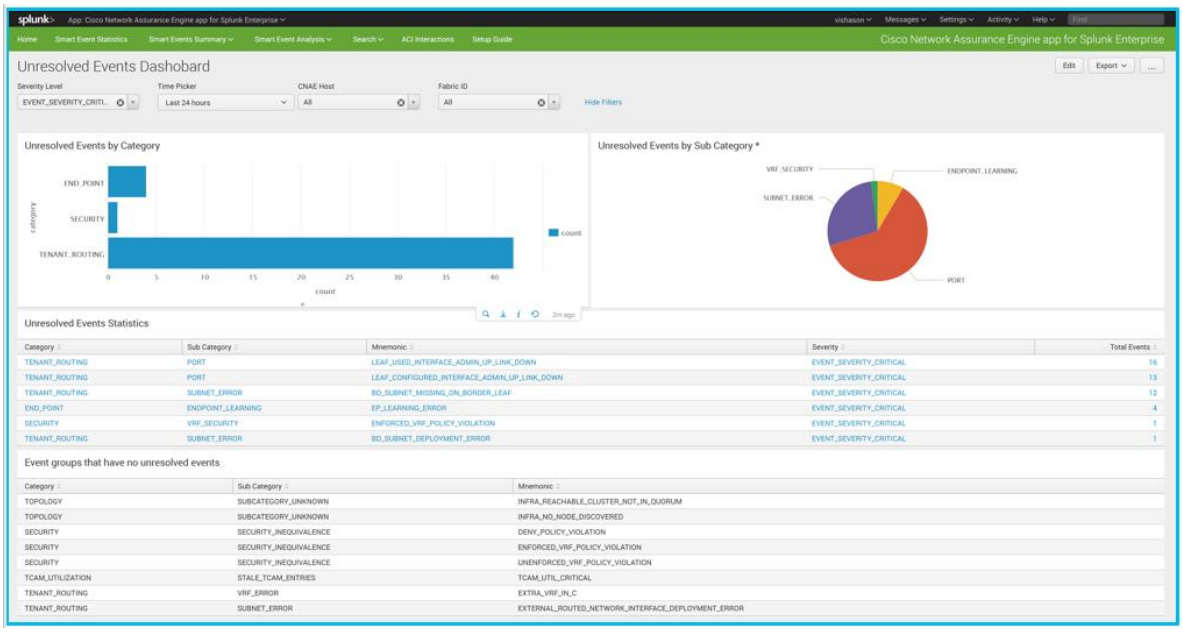
Cisco IT NAE integration roadmap:

- Splunk NAE integration – already done (very easy to implement – run the app, collect the data, and view the reports).
- ServiceNow NAE integration
    1. Use NAE to 'clean' the fabric of issues – already done.
    2. Suppress irrelevant Smart Events from surfacing in SNOW – by Q3 2019.
    3. Handle NAE Smart Events in the SNOW workflow – design done, will deploy by Q4 2019.

Using the new Cisco Network Assurance Engine App for Splunk Enterprise, network

administrators can visualize detailed network configuration and compliance issues in real-time using Splunk software. New, persistent, resolved, and unresolved events are shown across timelines, allowing administrators to quickly determine when an event originated and how long it has persisted.

Splunk integration with NAE



If a VM's status is listed as inaccessible, for example, the network administrator can easily search for events related to that VM's IP address. Cisco Network Assurance Engine will show the changes (or lack thereof) to the network, any underlying problems the changes may have caused, and suggested steps for resolving the problem. Once the issue is fixed, it will be listed as "resolved" in the Splunk Enterprise dashboard, providing assurance that the VM is now operational.

With Splunk software, network configuration and compliance issues can be easily correlated with data across infrastructure tiers and applications for comprehensive, continuous visibility. Correlating the issues raised by Cisco Network Assurance Engine with data from other sources considerably accelerates the root cause analysis and resolution. Administrators can also establish rules that proactively alert on potential configuration, performance and compliance issues in the network. Automating some or all the steps required to respond to known network events raised by Cisco Network Assurance Engine, further reduces the time and cost of network administration and troubleshooting.

With Cisco Network Assurance Engine integration, ServiceNow administrators can orchestrate, automate, and validate network changes through the ServiceNow dashboard. NAE has full visibility of the underlying network and all the variables that can cause service disruptions. When a problem is identified and understood, network administrators must create a ticket, resolve the problem, verify the fix, and close the ticket. These tedious, manual steps can result in unnecessary downtime, hinder user productivity, and pull network administrators away from value-added projects. And if the same problem reappears, all the steps must be repeated. Continuous network assurance and analysis that NAE provides can be coupled with cloud-based service management tools such as ServiceNow.

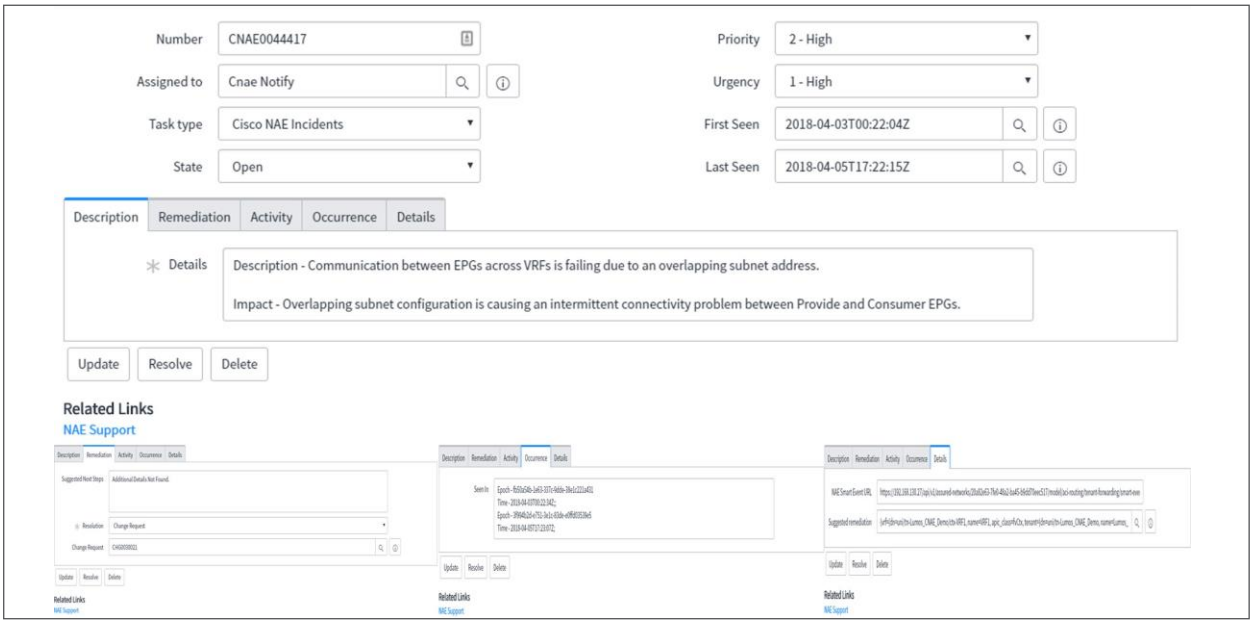
Cisco Network Assurance Engine and ServiceNow integration provides comprehensive and customizable visibility to Smart Events raised by Cisco Network Assurance Engine by allowing categorization and filtering of problems pertaining to areas of expertise such as security, policy analysis, tenant routing, or resource usage. These filtering capabilities enable you to easily have visibility into areas of interest such as:

- Events and incidents within a period of time
- De-duplicated NAE Smart Events
- Incident association with NAE Smart Events

The Cisco Network Assurance Engine with the ServiceNow application automates the incident management process for Smart Events. After each NAE network analysis cycle, Smart Events NAE raises are analyzed and reported as a new ticket or added to an existing ticket, depending on whether it is a completely new Smart Event or one that has been reported in the past.

If Cisco Network Assurance Engine finds an error or conflict within the network, it sends an alert to ServiceNow detailing the problem, its root cause, and recommended resolution. ServiceNow then creates a ticket.

Cisco Network Assurance Engine ServiceNow ticket with all details

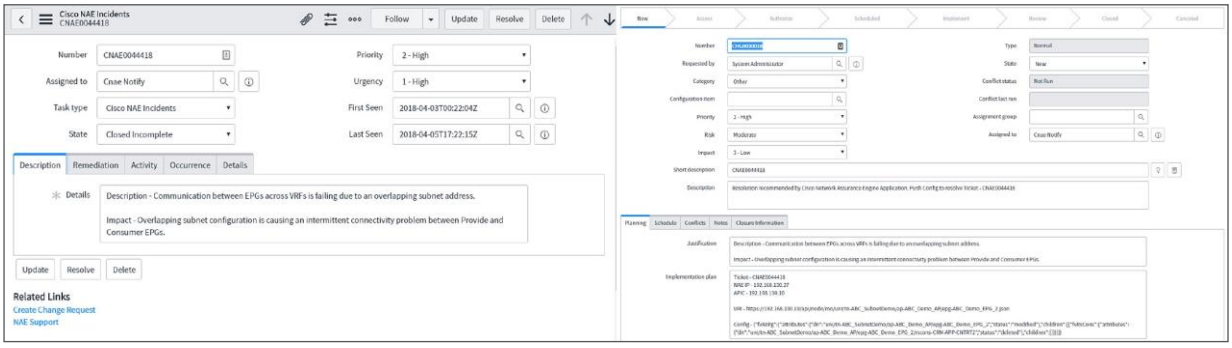


ServiceNow logs these changes by creating a change request that helps the administrators monitor all the changes and, if there is a need to roll back, they know exactly the changes made.

After the incident is assigned to a user, the assignee can just create a change request without having to agree to the auto-resolution the application offers.

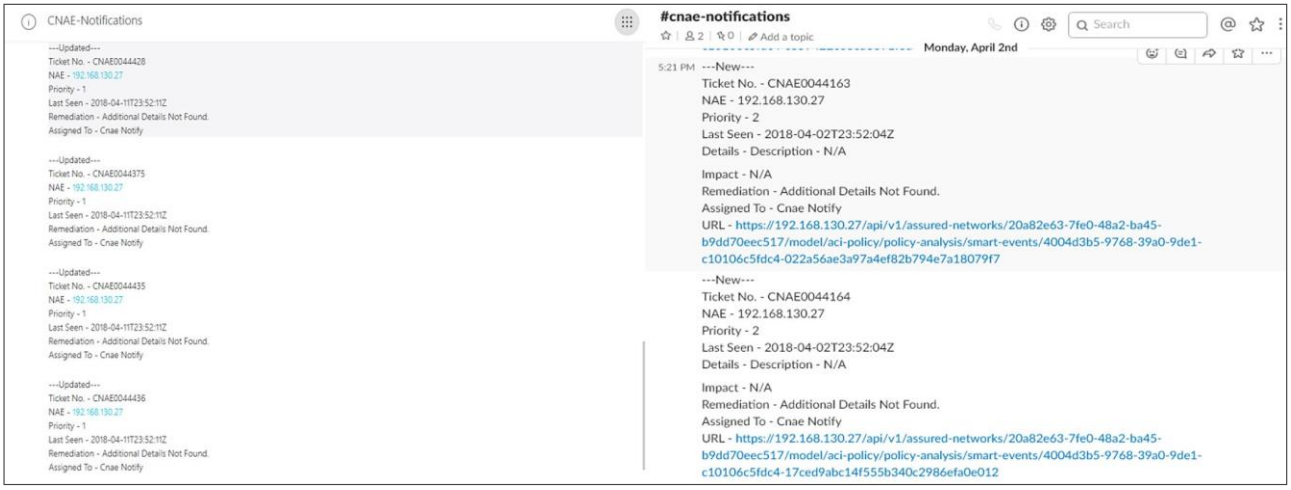
While Cisco IT has not yet done so, you can fully automate all these steps, dramatically reducing the time and cost of network administration, troubleshooting, ticket management, and problem resolution. With automated alerts, ticketing, problem remediation, and validation, the combination of Cisco Network Assurance Engine and ServiceNow enables closed-loop incident management. In doing so, it effectively creates a self-healing network.

Change request management



This workflow helps operations teams manage configuration changes and push them during the change window. This process helps the assignees prioritize their resolution.

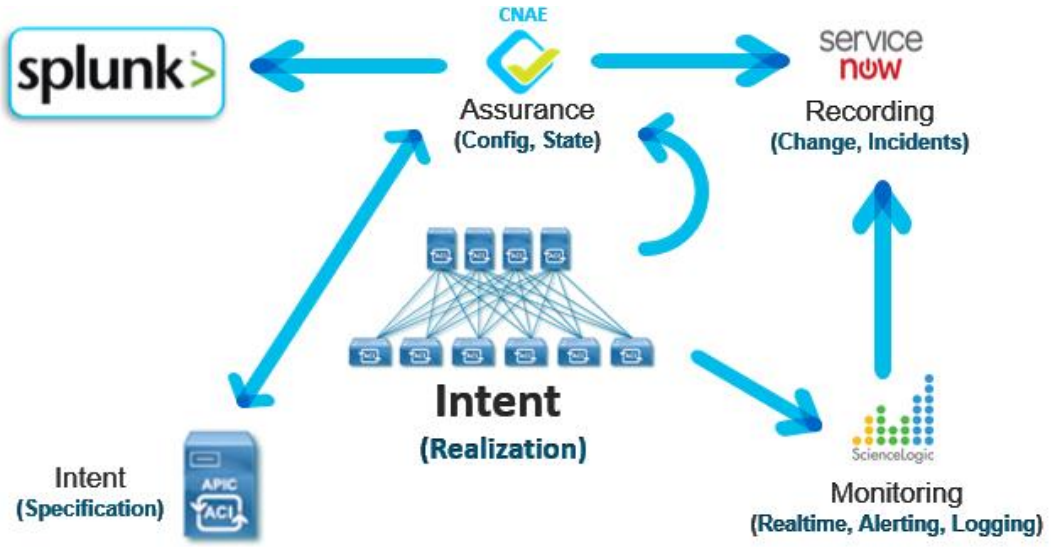
Push notifications



The integration of push notifications helps them be more responsive toward pressing problems, helping ensure less downtime of critical services.

The integration of Cisco Network Assurance Engine and ServiceNow provides visibility and orchestration spanning IT services as well as the network fabric. It not only delivers continuous network verification, but also improves change management, streamlines component configuration, and enables closed-loop incident response—significantly reducing the time and cost of network administration.

Cisco IT Network Policy Approval Workflow



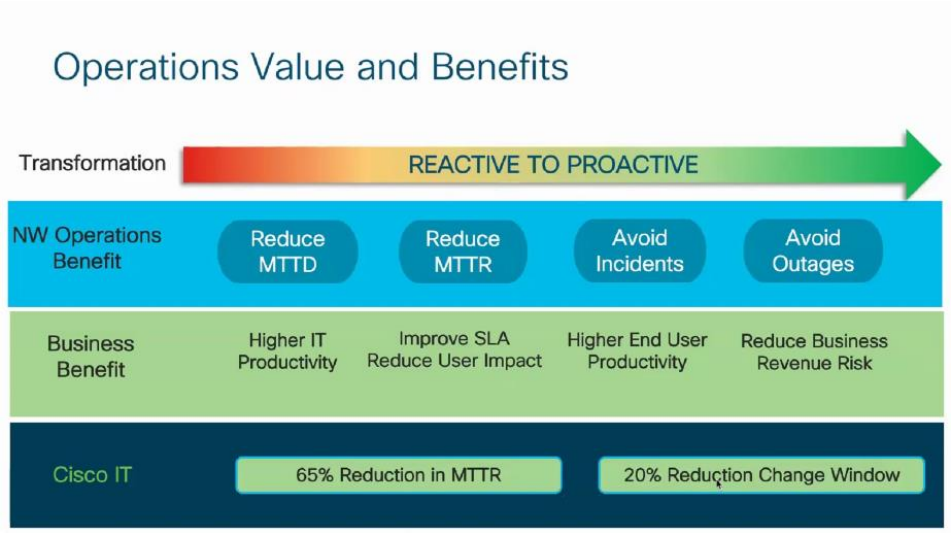
High level summary of a Cisco IT basic approval process is listed below:

1. Client makes a network security policy change request
2. Support case is automatically generated
3. Notification is sent to Infosec
4. Infosec review request and approves or rejects
5. Support case is updated
6. Notification sent to client
7. If approved, the client then chooses a time for the change to be pushed to network
8. Change push to network at the time nominated in step 3

Each change to a workspace is automatically tracked and versioned live as the admin makes the edits. The changes, however, do not get applied to endpoints to be enforced immediately. This is done through a separate process via the "Enforce Latest Policies" button. The idea is that an admin can make changes, then run some analysis in TA to understand what the impact of the change would be should it be implemented. Unintended negative impacts can then be handled by further edits to the policy. Once the admin is happy, they hit the enforce latest policies button at which point the changes are pushed out to the agents on the endpoints and the updated policy is applied.

Best Practices and Lessons Learned

Cisco IT has used NAE for several years and learned that it transformed their data center operations from a reactive to a proactive posture.



Start off focused on the basics: add new features as you go, and test/certify new features and code prior to production deployment. Use lab environments for testing prior to production rollout, and check release notes for any important changes. Create a certification process with standard must have capabilities and verification, and document/track issues found.

Build with automation in mind: create standard and reusable constructs, and document naming conventions for various objects to make readability and troubleshooting easier. Scripting skills will help you on your journey, especially with integrating NAE with existing systems such as ServiceNow. Not all the Smart Events NAE produces will be relevant to your data center. Filtering and prioritizing Smart Events streamlines the relevant data center operations activities.

Changed management: Cisco IT has been using NAE to systematically remove configuration issues. The result is that the number of NAE Smart Events has gone down by 39%, and the system health score that the APIC reports has gone up from 79% to 88%. In the future, NAE will be able to model changes before deploying them, which will enable pre-validation, shortening approval times and driving change agility.