



SDDC/Cloud 네트워크 패브릭의 자동화 진단 솔루션 Cisco NAE

시스코 코리아
유승만 차장

목차



- 데이터센터 네트워크 트렌드
- 되돌아 보는 SDN 현황
- Cisco NAE 소개
- 요약



데이터센터 네트워크 트렌드

빠른 변화와 새로운 요구에 직면한 데이터 센터 네트워크



확장성

10,000이상의 VMs, 100개 이상의 분산형 앱, 백만개 이상의 정책들



복잡성

멀티 데이터 센터, 멀티 테넌트, 하이브리드, 가상화, 다양한 인프라 환경



변동성

VM 이동성, 앱 마이그레이션, 다이내믹한 확장성, 셀프 서비스 포털

우리의 현실은,,,

“ 의도와는 상관 없는
변경 작업들,,, ”

운영 이슈 >

보안 이슈 >

컴플라이언스 >

변경작업 >

“ 수동적인 변경 작업,,, ”

트러블 슈팅

무작위의 정책 적용

감사

원복 작업

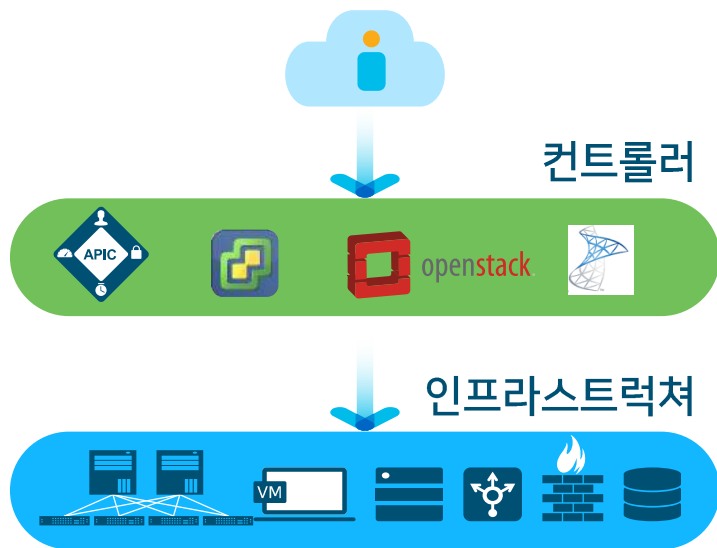


“결국은,,,”

의도한 대로
선제적인
조치 불가

더욱 깊어져 가는 고민들,,,

고객의 의도



1 구성변경 이후, **에러**가 없는 것만으로 정상인지를 어떻게 확인하죠?

2 전체 인프라의 **상태**를 쉽게 이해하려면 어떻게 해야합니까?

3 네트워크를 신속하게 **분석**하여 문제를 식별하려면 어떻게 합니까?

되돌아 보는 SDN 현황

시스코의 SDN 적용 그 이후... Pros



손쉬운 자원이동과 구성



대규모 패치 작업 편의성



물리적 디자인 간편성



유연성 높은 디자인과 고성능

시스코의 SDN 적용 그 이후... Cons



운영 방식의 변화



장애 발생시 대처 요령 부족



논리적인 복잡도

Cisco NAE 소개

INTENT ASSURANCE

인프라가

당신이 의도 한대로,

운영되고 있다는 자신감 !!!

구성, 변경, 라우팅, 가상화, 보안, 컴플라이언스, 감사

시스코 Network Assurance Engine 소개



Cisco NAE



네트워크의 수학적 모델 기반



전체 네트워크에 대한 지속적인 검증 / 유효성 점검



네트워크 정상 동작에 대한 확신 근거 제공

포괄적

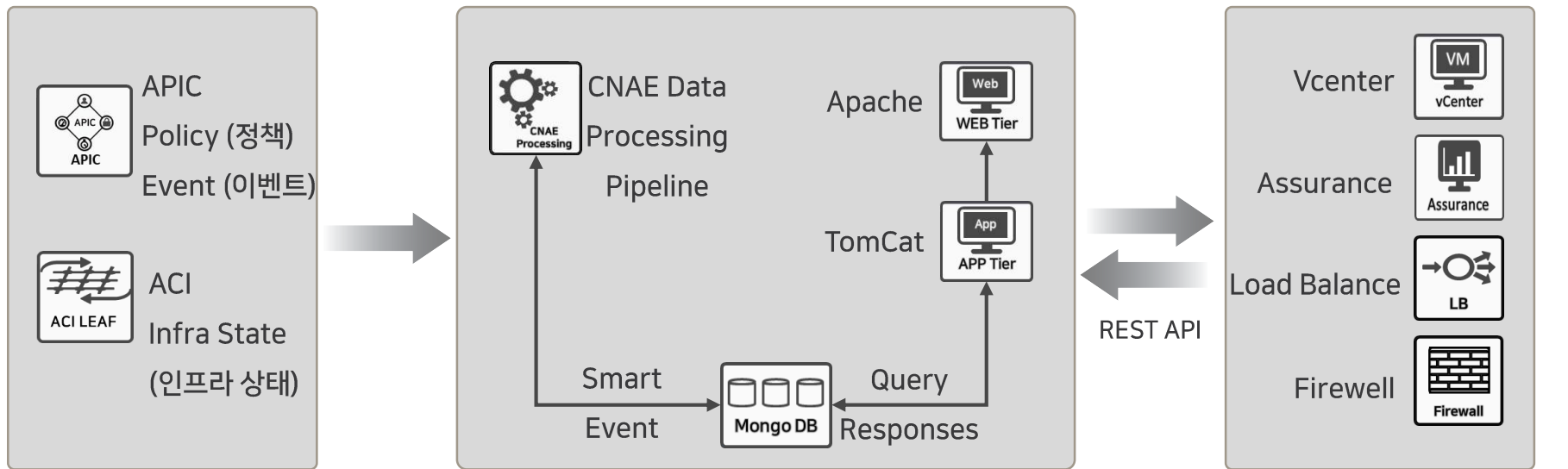
지능적

지속성

시스코 Network Assurance Engine 아키텍처



CNAE 아키텍처 구조

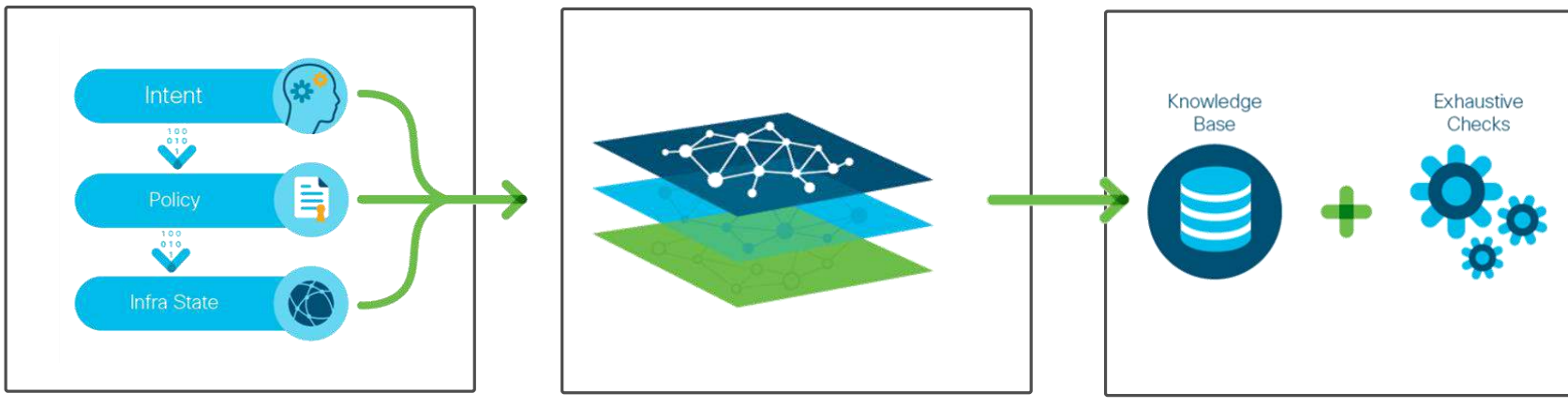


[Intent]

[CNAE - DataCenter Assurance Engine]

[Ecosystem Partner]

시스코 Network Assurance Engine 동작 방식



데이터 수집

데이터 센터
네트워크 전반
의도, 정책, 상태

포괄적인 네트워크 모델링

언더 레이, 오버레이
가상화 레이어 전반의
수학적으로 정확한 모델

지능형 분석

5000 개 이상의 지식 기반
분석 시나리오 내장
스마트한 해결책 제시 방식



Cisco Network Assurance Engine

Deployment Model

센서 필요 없음.
Read Only 권한 접근

Time to Value

30 mins 안에 설치
60 mins 안에 가치 증명

Form Factors

VM 기반의 Software
(3개 VMs - 최대 100개 LEAFs)

Available Now

30 Day Free Trial

Subscription 기반 라이선싱

시스코 Network Assurance Engine 핵심 요약



포괄적인 네트워크 진단

보안 정책, 포워딩, 엔드 포인트,
TCAM 활용, 컨트롤러 정책 등
전반에 걸친 **전체 네트워크 상태**
분석 및 상호 연관성 분석



지능형 분석

5000+ 이상의 위협 및
장애 시나리오 분석
30년 이상의 시스코
네트워크 지식 DB 기반
분석



지속적인 검증

실시간 수집 및 모델링
분석, 해결책 제시

시스코 Network Assurance Engine 핵심 기능

변경 관리

컴플라이언스 및 시각화

이상 및 문제 해결 관리

The screenshot displays the 'Configuration & Audit' section of the Cisco Network Assurance Engine. A table lists configuration items with columns for Severity, Name, App EPG, and Count. Two items are highlighted with red warning icons: 'OVERLAPPING_SUBNETS_ACROSS_VRFs_ID' and 'PERMIT_POLICY_SHADOWED_BY_DENY_PO'. A detailed view of the 'PERMIT_POLICY_SHADOWED_BY_DENY_PO' item is shown below, including its description, affected objects (Provider EPG: EPG_11, Consumer EPG: EPG_6), and failure conditions.

Severity	Name	App EPG	Count
Warning	OVERLAPPING_SUBNETS_ACROSS_VRFs_ID	Communications	1
Warning	PERMIT_POLICY_SHADOWED_BY_DENY_PO	Deny policy is overl...	1

Description: EPGs cannot communicate due to a deny rule overriding a permit rule.

Affected Objects:

Provider EPG	Consumer EPG
EPG_11	EPG_6

Failure Condition: Deny policy is overriding Permit policy between two EPGs.

The screenshot shows the 'View Control' section of the Cisco Network Assurance Engine. It features a large, circular network visualization with nodes and connecting lines. A circular callout highlights a specific area of the network, showing a 'Policies' layer and 'Endpoints' layer. The interface includes navigation buttons for 'View Control' and 'View Details'.

The screenshot displays the 'Tenant Endpoints Events' section of the Cisco Network Assurance Engine. It shows a list of events with columns for Severity, Name, and Count. A detailed view of an event is shown below, including its description, affected objects, and suggested next steps.

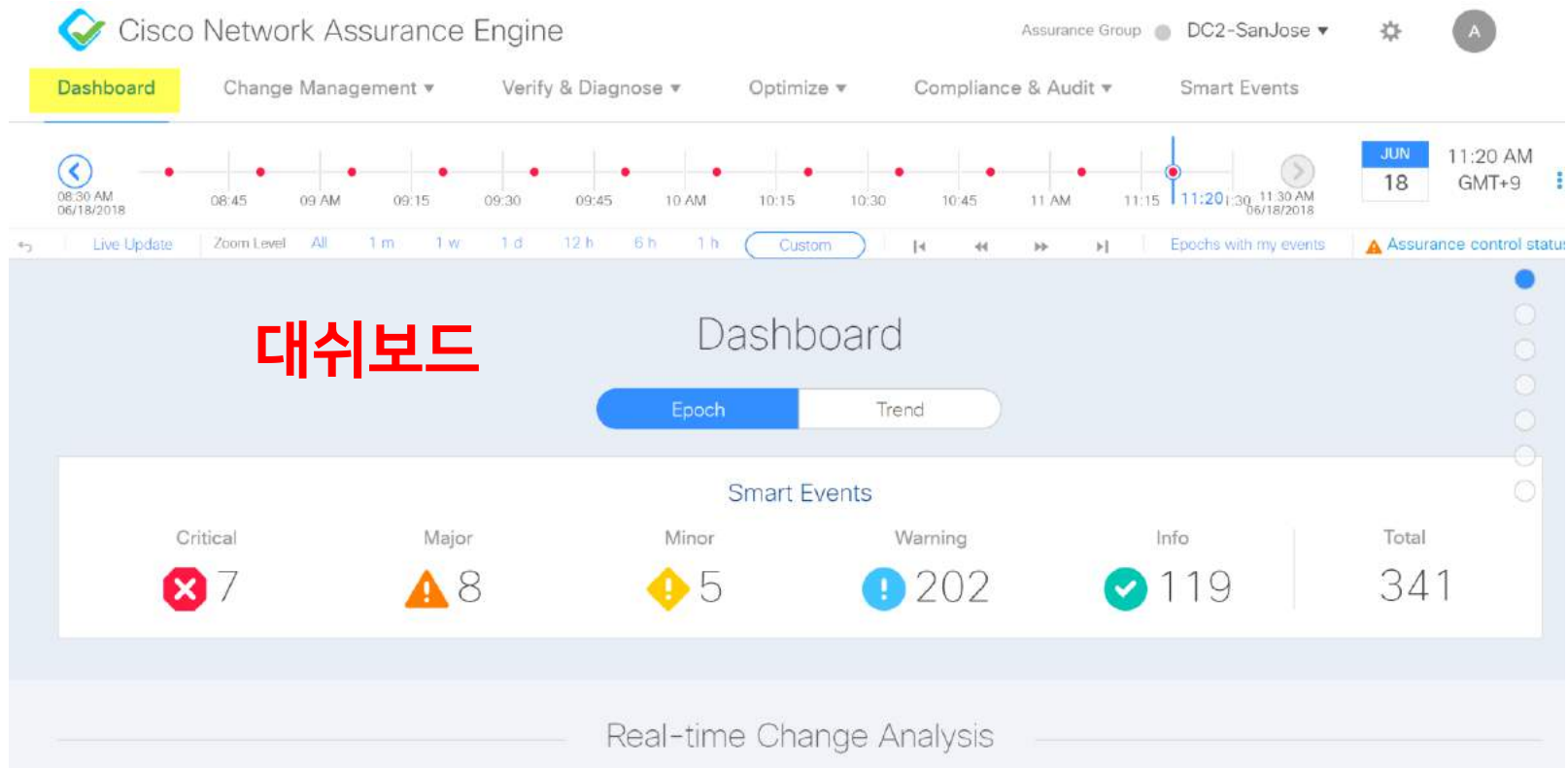
Description: IP address not present by VRF.

Affected Objects: List of duplicate IP's in VRF.

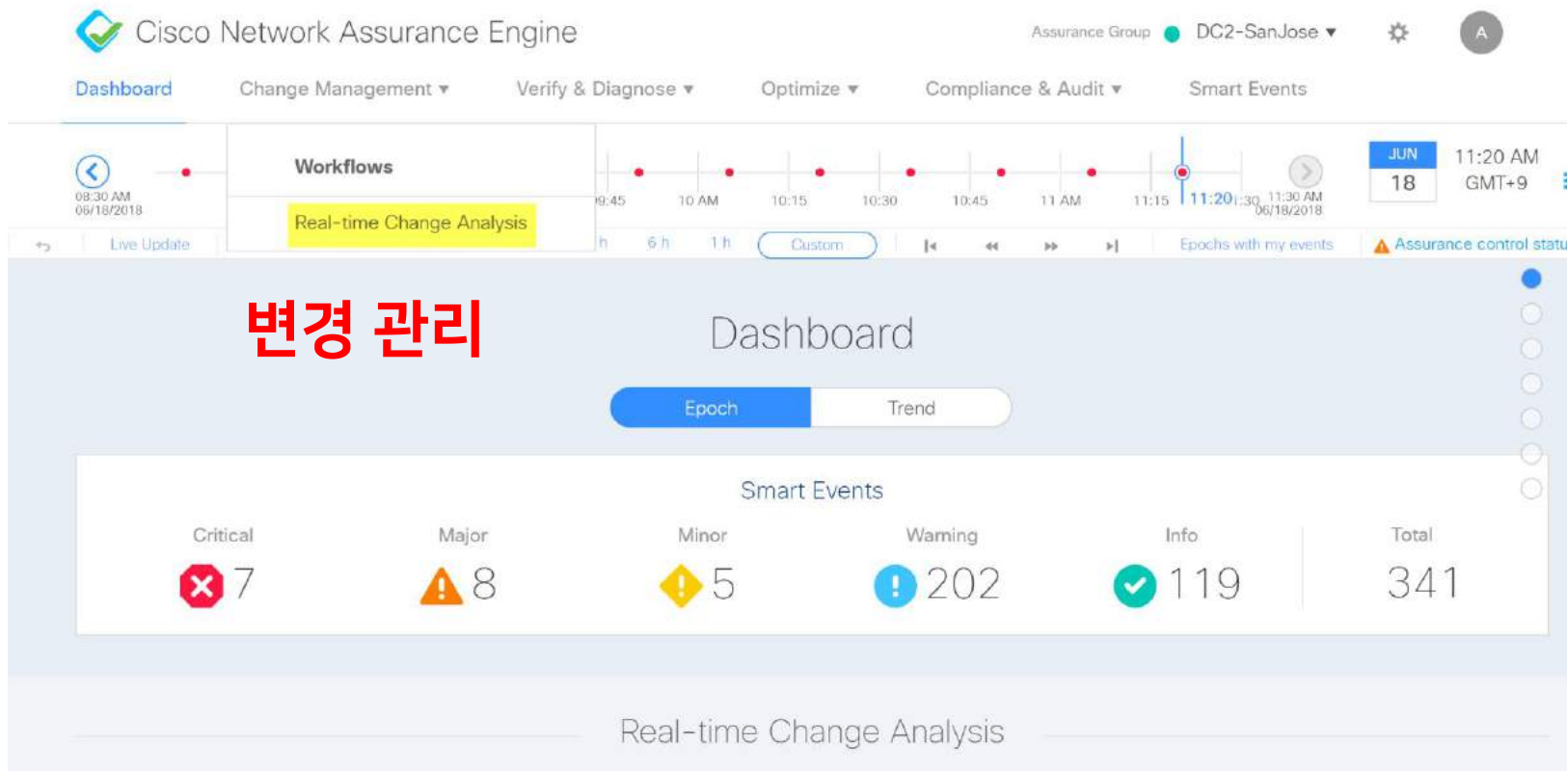
Suggested Next Steps:

- Login into the APIC UI and verify the presence of the endpoints in the operational tabs of the EPGs.
- Identify the EPGs that actually own the IPs and change the IP address on the host/device that has the incorrect IP address.
- Clear the endpoint on the leaf by opening a SSH session to each leaf and entering the following command:
leaf# clear system internal epm endpoint command

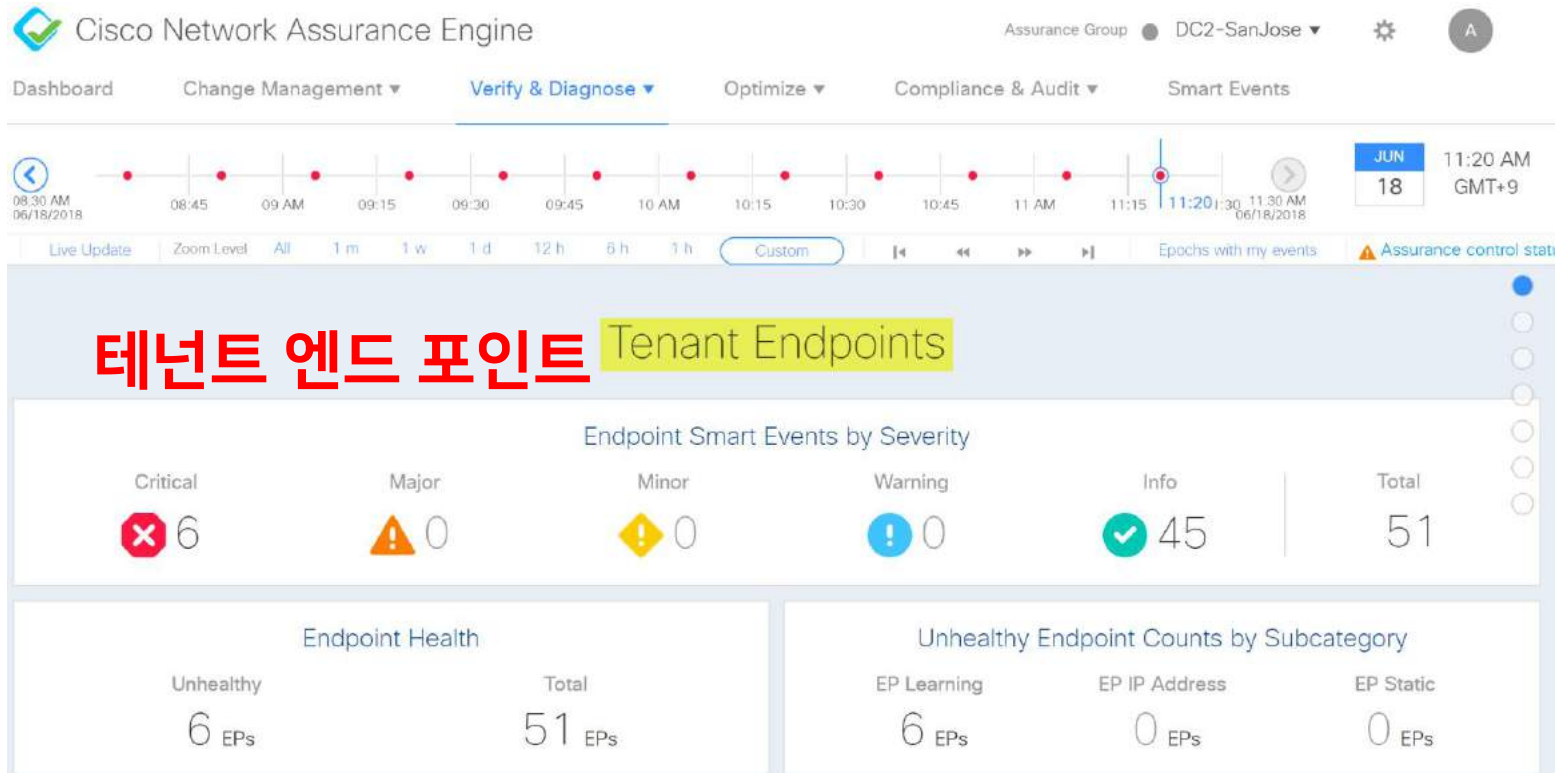
시스코 Network Assurance Engine 핵심 기능



시스코 Network Assurance Engine 핵심 기능



시스코 Network Assurance Engine 핵심 기능



시스코 Network Assurance Engine 핵심 기능

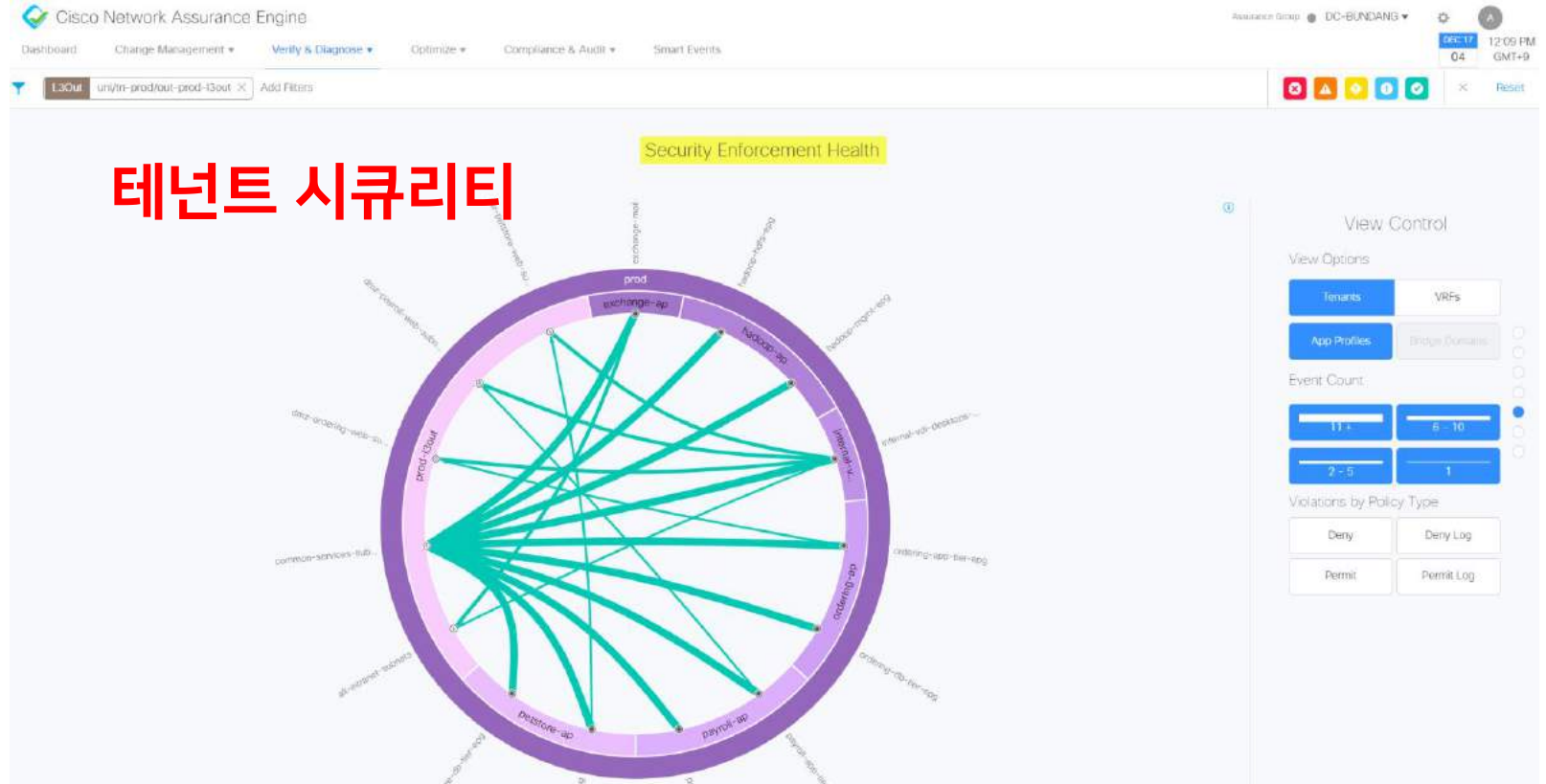
Cisco Network Assurance Engine Assurance Group DC2-SanJose JUN 18 11:20 AM GMT+9

Dashboard Change Management **Verify & Diagnose** Optimize Compliance & Audit Smart Events

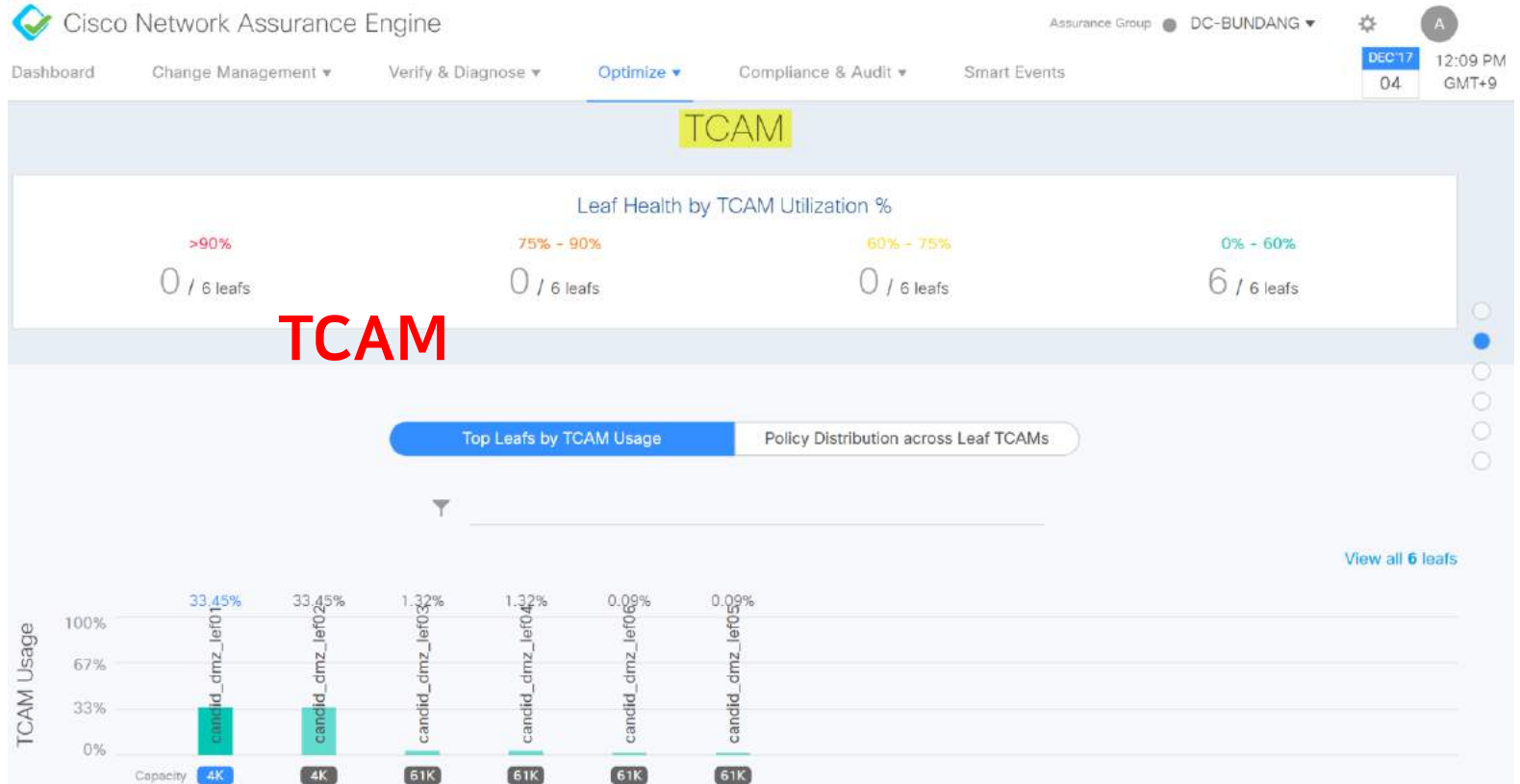
Add Filters **테넌트 엔드 포인트** [Icons] [Reset]

Severity	MAC	IP	EPG	BD	VRF	Encap
	Search	192.168.101	X Search	Search	Search	Search
✖	00:50:56:AA:06:48	192.168.101.13	unknownepg	101NET	A	-
✖	00:50:56:AA:27:71	192.168.101.14	unknownepg	101NET	A	-
✖	00:50:56:AA:2B:54	192.168.101.15	unknownepg	101NET	A	-
✖	00:50:56:AA:3D:94	192.168.101.16	unknownepg	101NET	A	-
✖	00:50:56:AA:D8:9C	192.168.101.12	unknownepg	101NET	A	-
✖	00:50:56:AA:F3:2F	192.168.101.11	unknownepg	101NET	A	-
✔	00:22:BD:F8:19:FF	192.168.101.1	-	101NET	A	0 0
✔	00:50:56:A0:11:61	192.168.101.113	Thanos-APP	101NET	A	2225 2225

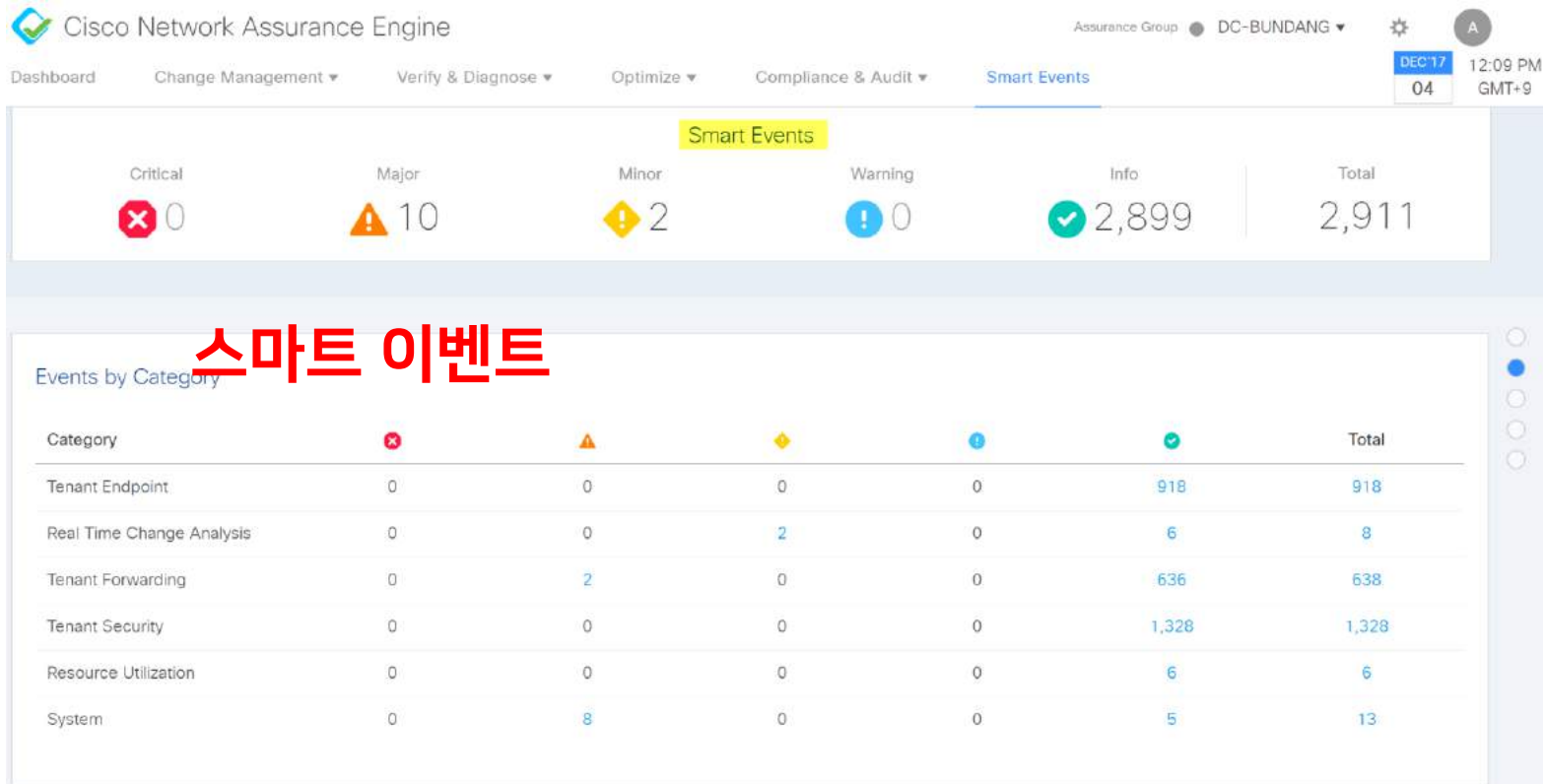
시스코 Network Assurance Engine 핵심 기능



시스코 Network Assurance Engine 핵심 기능



시스코 Network Assurance Engine 핵심 기능



시스코 Network Assurance Engine 핵심 기능

Severity ▾ 1	Event Category	Event Subcategory	Event Name ▲ 2	Event Description
Search		Search		=BD_WITH_SUBNET_MARKED_EXTERNAL_HAS_L ×
1	CHANGE_ANALYSIS	FORWARDING_POLICY	BD_WITH_SUBNET_MARKED_EXTERNAL_HAS_L3OUT_B...	VRF is in enforced mode and externally via an L3Out but th do not have any contract with the L3Out.

스마트 트러블 슈팅

Description	VRF is in enforced mode and BD subnet is advertised externally via an L3Out but the EPG(s) belonging to the BD do not have any contract with the External EPG belonging to the L3Out.							
Impact	BD subnets will not be advertised.							
Affected Objects	<table><thead><tr><th>VRF's Tenant</th><th>VRF</th><th>BD Subnet</th></tr></thead><tbody><tr><td>non-prod</td><td>non-prod-vrf</td><td>10.11.0.0/24</td></tr></tbody></table>		VRF's Tenant	VRF	BD Subnet	non-prod	non-prod-vrf	10.11.0.0/24
VRF's Tenant	VRF	BD Subnet						
non-prod	non-prod-vrf	10.11.0.0/24						
Checks	<table><thead><tr><th>Failing Condition</th><th>Suggested Next Steps</th></tr></thead><tbody><tr><td>BD has a subnet marked external and associated with L3Out but none of the EPGs that belong to this BD has contract with the External EPG.</td><td><ol style="list-style-type: none">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.</td></tr></tbody></table>		Failing Condition	Suggested Next Steps	BD has a subnet marked external and associated with L3Out but none of the EPGs that belong to this BD has contract with the External EPG.	<ol style="list-style-type: none">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.		
Failing Condition	Suggested Next Steps							
BD has a subnet marked external and associated with L3Out but none of the EPGs that belong to this BD has contract with the External EPG.	<ol style="list-style-type: none">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.							

시스코 Network Assurance Engine 핵심 기능

Cisco Network Assurance Engine

Assurance Group ● DC-BUNDANG

Dashboard Change Management Verify & Diagnose

Critical 0 Major 10 Minor 1

오프라인 분석

Events by Category

Category	Critical	Major	Minor
Tenant Endpoint	0	0	0
Real Time Change Analysis	0	0	0
Tenant Forwarding	0	0	2

Settings Menu:

- Assurance Group Configuration
- Download Offline Collection Script
- Offline File Management
- Offline Analysis**
- Appliance Administration
- Appliance Status
- User Management
- Download Tech Support Logs
- REST API Documentation
- Download Appliance Documentation
- About Network Assurance Engine

12:09 PM GMT+9

636

요약

고객 사용 사례 및 효과



구성변경에 따른 변화 예측

- IT 민첩성 확대
- 휴먼 에러 최소화
- 마이그레이션 가속화



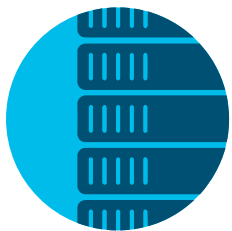
네트워크 전반에 대한 Proactive 검증

- 네트워크 커넥티비티
- 잠재적인 네트워크 위협에 대한 취약점을 사전에 제거
- 시스템 기반의 향상된 SLA 기술 제거



네트워크 보안정책 및 준수 확인

- 보안 위협 감소
- 지속적인 Intent 네트워크 설계 기준 감사



Cisco Data Center Product Portfolio

Cisco ACI

- 네트워크 최적화 및 자동화
- 네트워크 보안, 가용성
- Multicloud Networking

Network Assurance Engine

- 예측 변경 관리
- 광범위한 네트워크 검증
- 네트워크 보안 정책 및 규정 준수 보장

Tetration

- 워크로드 보안 (제로 트러스트)
- 응용 프로그램 연관성 매핑 / 정책 검색
- 실시간 가시성 / 인사이트

