솔루션 오버뷰

# ARUBA 네트워크 분석 엔진

## 신속한 문제 해결 및 근본 원인 분석

네트워크 운영자들은 오늘날 디지털 세계에서 많은 어려움에 직면하고 있습니다. IoT단말의 도입은 IT부서가 네트워크에 안전하게 연결 해야 할 단말의 수를 기하급수적으로 늘리고 있습니다. 클라우드 채택으로 인해 네트워크 상에 다른 트래픽 패턴이 발생한 경우, 운영자들은 성능에 대한 가시성을 잃는 경우도 있습니다. 마지막으로, 모빌리티 업무 환경은 직원들이 각각 다른 수준의 성능과 보안을 제공하는 여러 네트워크를 통해 앱에 액세스한다는 것을 의미합니다.

고가용성의 상시 가동 네트워크는 오늘날 기업에게 미션 크리티컬한 대상입니다. 그러나 이러한 기술 동향으로 인해 네트워크에서 더 많은 스트레스와 장애 지점이 발생하여 이 목표를 달성하기가 더 어려워졌습니다.

이제 네트워크 운영자들은 문제가 발생할 때 신속하게 해결하기 위해 더 나은 가시성이 필요합니다. 이러한 요구를 충족하기 위해 Aruba는 AOS-CX 네트워크 운영체제의 일부인 네트워크 분석 엔진(NAE)을 개발했습니다.

NAE는 네트워크 모니터링 및 문제 해결을 위한 기본 프레임워크를 제공합니다. 네트워크 이벤트를 자동으로 조사하고 분석하여 중단 및 비정상적인 상태에 대한 전례 없는 가시성을 제공합니다. IT팀은 이러한 인사이트를 활용하여 실시간으로 문제를 감지하고 동향을 분석하여 향후 보안 및 성능 문제를 예측하거나 방지할 수 있습니다.

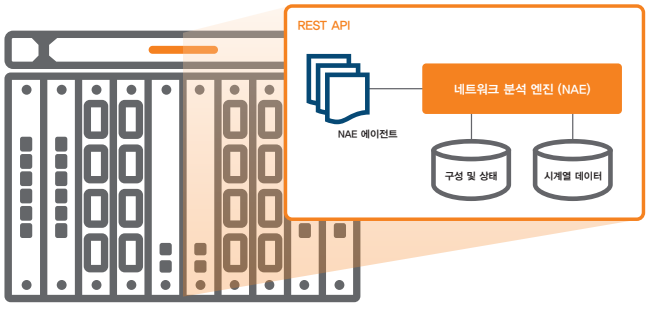
### 주요 이점

- **더욱 빨라지고 완전해진 가시성:** 내장형 시계열 데이터베이스는 운영자가 더 나은 경험을 제공할 수 있도록 이벤트 및 연계 내역과 네트워크 전반의 인사이트에 대한 실시간 액세스를 제공합니다.
- **신속해진 MTTR:** 규칙 기반의 실시간 모니터링과 지능형 알림은 구성 변경과 자동으로 연계되어 빠르게 네트워크를 진단 할 수 있도록 합니다.
- **간편한 관리:** Aruba NetEdit뿐 아니라 ServiceNow, Slack과 같은 타사 도구와의 통합을 통해 다양한 NAE 알림을 IT 서비스 관리 프로세스에 통합할 수 있는 인텔리전스를 제공합니다.
- **지속적인 혁신:** 지속적으로 성장하고 있으며 Aruba가 관리하는 NAE 솔루션 라이브러리와 추가적인 혁신을 추구하는 전문가 커뮤니티에 대한 이용 권한을 제공합니다.

## 문제부터 근본 원인까지

네트워크 문제의 근본 원인을 찾는 일은 전통적으로 여러 가지 많은 작업과 연관되어 왔습니다. 우선 네트워크 운영자들은 일련의 show 명령을 사용하여 네트워크의 현재 상태를 조사하거나 프로브를 실행하여 문제를 시도 및 재현할 수 있습니다.

문제가 발생한 순간부터 텔레메트리를 사용할 수 있는 경우 적절한 분석을 수행하기 위해 외부 도구를 사용한 수동 구성이 필요한 경우가 많습니다. 그러나 이러한 데이터 파이프라인은 종종 필터링되지 않으므로 데이터 전송과 처리가 지연됩니다. 두 번째로, 타사 모니터링 도구는 데이터의 전체적인 세부 정보를 캡처하는 대신 종종 데이터를 샘플링하여 가시성에 추가적인 간극을 유발합니다.




Aruba NAE 제공 기능:

- 구성 변경과 연관된 기록 데이터
- 서비스 영향 및 근본 원인 분석 자동화
- 지능형 모니터링 에이전트 – 'Always On'
- 모든 시스템 정보에 대한 완벽한 원격 측정
- 인접 인프라의 정보
- 자동 진단을 통한 알림

**그림 1: 스위치에서 기본적으로 고급 네트워크 분석을 수집하는 Aruba NAE**

반대로, NAE는 각 스위치에서 직접 지능형 모니터링을 수행하여 지연이나 정보 손실 없이 운영자에게 네트워크 전체 상태에 대한 분산 분석과 실행 가능한 인사이트를 제공합니다.

운영자는 NAE를 통해 자동화된 방식으로 관심을 갖고 있는 특정 트래픽을 모니터링하여 해당 데이터를 수집하고, 이를 서비스 알림을 트리거하는 이벤트와 연결시키는 규칙을 사전에 설정할 수 있습니다. 이를 통해 NAE는 드릴다운 방식으로 문제를 신속하게 확인하고 서비스 영향력과 근본 원인 분석을 가속화하여 MTTR(Mean Time to Resolution)을 줄일 수 있습니다.

## NAE 구성요소

NAE는 Aruba CX 6000 및 Aruba CX 8000 스위치 시리즈(그림 2)와 같은AOS-CX 운영체제를 지원하는 플랫폼 내에서 실행되며 다음과 같은 두 개의 주요 데이터베이스에서 데이터를 가져오는 에이전트를 사용하여 스위치의 구성을 모니터링합니다.

- 구성 및 상태 데이터베이스: REST API를 통해 완전히 확인되는 구성 정보, 프로토콜 상태 및 네트워크 통계에 대한 전체 액세스 권한을 NAE 에이전트에 제공합니다.
- 시계열 데이터베이스: 구성 변경과 연관된 관련 기록 데이터를 포함합니다. 운영자는 이를 통해 네트워크 이벤트를 둘러싼 네트워크 상태를 캡처 및 보관하고 빠르게 액세스할 수 있습니다.

NAE 에이전트는 스위치, 해당 주변 장치 또는 네트워크를 통과하는 트래픽 상태를 테스트한 다음 테스트 결과에 따라 조치를 취합니다.

예를 들어, 알 수 없는 호스트에 의해 ACL에 의해 차단되는 횟수가 높은 경우는 보안 위반 가능성을 나타냅니다. 이 경우, NAE는 Syslog 메시지를 작성하거나 분석 결과가 포함된 사용자 정의 보고서를 생성하여 운영자에게 문제를 알릴 수 있으며, 이는 웹 인터페이스를 통해 쉽게 액세스할 수 있습니다.

또한 운영자는 여러 작업을 기존 워크플로에 결합하여 보다 선별적인 진단 또는 권장사항을 수행할 수도 있습니다. 관심을 갖고 있던 문제가 발생할 때 ServiceNow와 같은 IT 서비스 관리 시스템이나 Slack과 같은 협업 도구에 알림을 전달하는 기능 등이 여기에 해당합니다.

웹 UI는 스위치 상태를 모니터링할 수 있는 기능을 제공하는 것 외에도 네트워크 팀이 NAE 에이전트, 스크립트 및 알림을 보고 구성할 수 있도록 합니다.

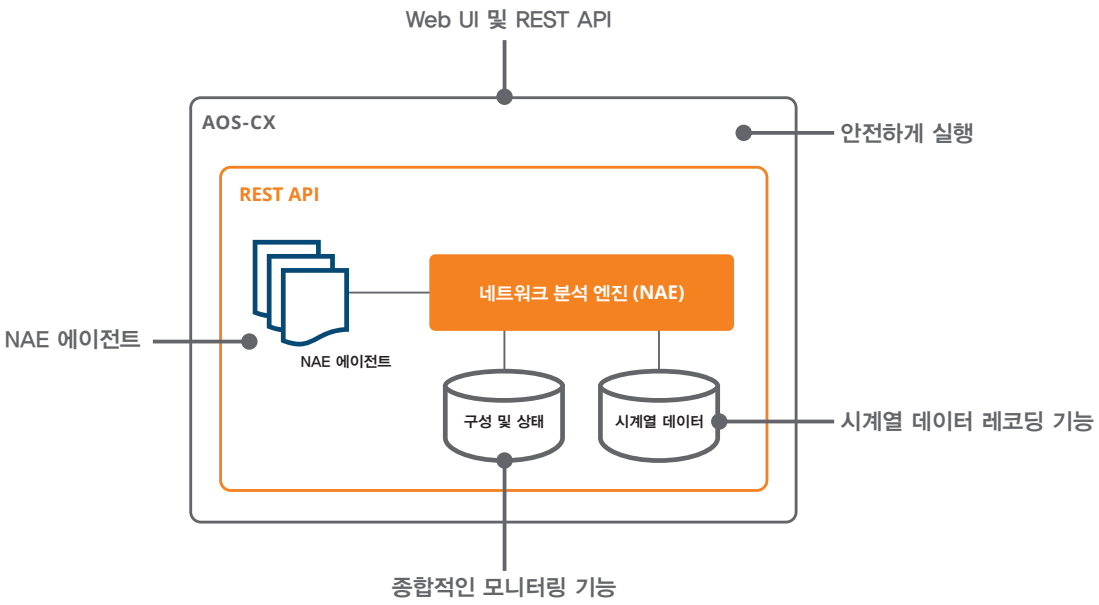



그림 2: NAE 구성요소

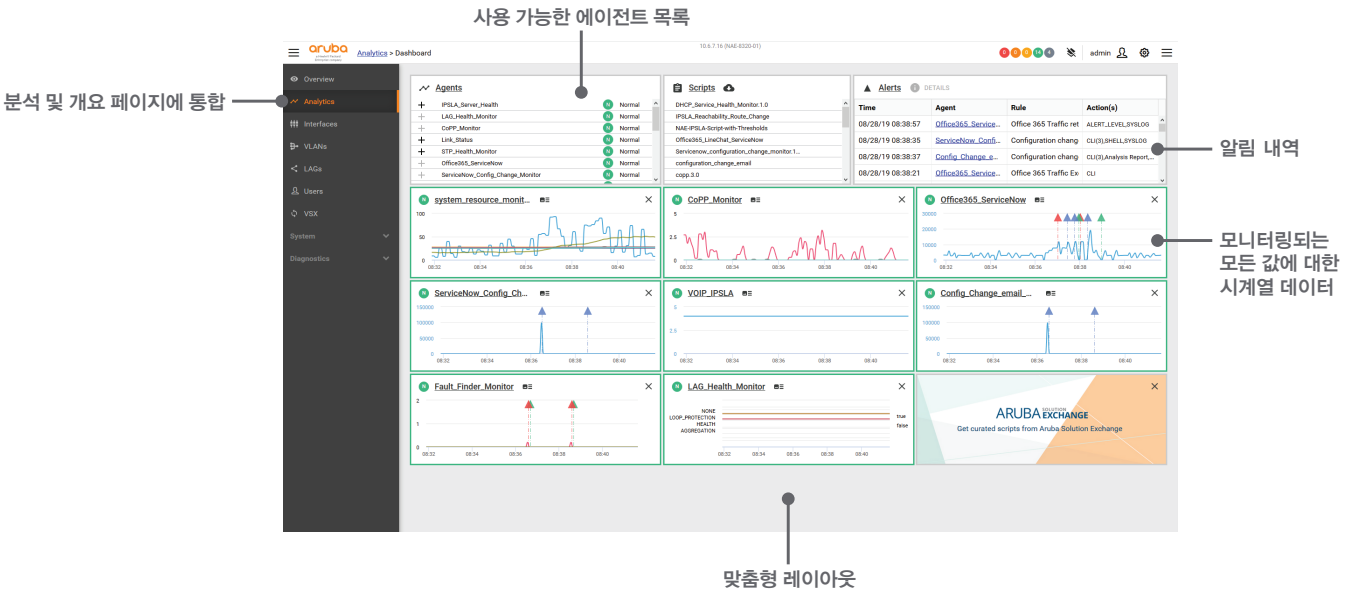



그림 3: Aruba NAE 대시보드

## 사용 사례 예시

NAE는 네트워크 문제를 공통 근본 원인에 매핑하여 다양한 1차 및 2차 진단을 미리 결정함으로써 문제 해결 절차를 가속화하고 운영자가 보다 구체화된 문제들에 집중할 수 있도록 합니다.

보다 광범위한 수준에서 NAE 에이전트의 사용 사례는 다음과 같습니다.

1. 시스템 상태
2. 네트워크 분석
3. 보안
4. 애플리케이션 가시성
5. 네트워크 최적화

### 시스템 상태

조직은 스위치의 상태 및 성능에 대한 신뢰할 수 있는 인텔리전스가 필요합니다. 관련하여 NAE 에이전트는 CPU 및 메모리 사용량과 같은 제어 영역의 시스템 리소스 상태를 모니터링하고 시간의 흐름에 따라 이를 추적합니다. 운영자가 장치의 비정상적인 상태로 인해 알림을 받으면, NAE는 문제 발생 시점의 상세한 시스템 정보를 캡처하여 보관합니다.

또한 시스템 상태 에이전트는 TACACS+ 및 Syslog와 같은 중요한 서비스의 가용성을 보장합니다. 이러한 에이전트는 네트워크 진단을 수행하거나, 수행하지 않을 경우 다른 적절한 조치(예: OOB 알림)를 수행합니다.

### 네트워크 분석

NAE는 분석을 위해 AOS-CX에서 사용 가능한 모든 네트워크 통계를 시계열 데이터베이스와 통합할 수 있습니다. 이 범주의 다양한 기능은 Layer 1 트랜시버 모니터링부터 Layer 3 BGP peer 상태에 이르기까지 모든 것에 영향을 미칩니다.

광범위한 사용 사례는 시스템의 거의 모든 통계를 모니터링하는 기능에서 시작됩니다. 예시:

- 트랜시버 상태: NAE는 트랜시버 TX 및 RX 전력 레벨을 모니터링하여 연결 상태에 대한 다양한 문제를 감지할 수 있습니다. 전력 레벨이 갑자기 변하면 NAE는 이러한 레벨을 알려진 기준과 비교하여 두 트랜시버 간의 광섬유 링크에서 발생한 문제에 대해 높은 확률의 지침을 제공합니다.
- OSPF Route 상태: OSPF와 같은 라우팅 프로토콜은 네트워크 작동에 큰 영향을 미칩니다. NAE는 OSPF 테이블의 변경 사항에 대한 컨텍스트를 제공합니다. 예를 들어 NAE는 LSA(Link State Advertisement) 카운터를 모니터링하여 시스템에서 사용 가능한 경로 수에 대한 인사이트를 제공합니다. LSA 개수의 급격한 감소는 OSPF neighbor를 사용할 수 없거나 더 이상 정상적인 경로 개수를 제공하지 않음을 의미할 수 있습니다. 이것은 종종 연결성 문제를 나타내며, NAE는 해당 근원에 대한 빠른 인사이트를 제공합니다.

다른 네트워크 분석 에이전트에는 VRRP(Virtual Router Redundancy Protocol), LAG(Link Aggregation) 상태 또는 STP(Spanning Tree Protocol)에 대한 상태 모니터링뿐 아니라 인터페이스 통계에 대한 모니터가 포함됩니다.

### 보안

또한 NAE는 네트워크의 액세스, 어그리게이션 및 코어 계층에서 AOS-CX 스위치를 통과하는 잘못된 트래픽을 식별하고 검사할 수 있습니다. 이 경우, NAE는 트래픽에 대한 조치를 취하거나 자세한 검사를 위해 보안 장치로 전달할 수 있습니다.

예를 들어, 일반적으로 HVAC 컨트롤러와만 상호작용하는 HVAC 시스템에 대해 생각해 보십시오. NAE가 이 시스템의 트래픽이 소스 코드 저장소나 데이터베이스 서버와 통신하는 것을 확인하면 해킹된 장치일 가능성이 높습니다. NAE는 완전하고 집중적인 엔드포인트 진단을 위해 이 트래픽을 사용자 및 엔터티 행동 분석(UEBA) 솔루션인 Aruba IntroSpect로 전달할 수 있습니다. 조사 후 관리자는 원치 않는 통신을 허용한 정책을 조정하거나 Aruba ClearPass를 사용하여 손상된 장치에 대해 자동으로 격리 조치를 취할 수 있습니다.

다른 보안 에이전트로는 구성 변경 모니터와 COPP(Control Plane Policing) 모니터가 있습니다.

### 애플리케이션 가시성

또한 NAE는 네트워크 핵심을 통과할 때 애플리케이션 트래픽에 대한 가시성을 제공합니다. 여기에는 Office 365나 Google Suite와 같은 클라우드 애플리케이션의 성능 추적이 포함됩니다.

NAE 에이전트는 성능 저하를 감지하면 강력한 네트워크 진단을 수행합니다. 예를 들어 인터넷 서비스 공급업체(ISP)가 성능이 저하된 서비스를 제공하는 경우 NAE는 서비스가 문제를 겪기 시작한 시기에 대한 인사이트를 제공하여 근본 원인을 격리하고 해결하는 데 필요한 시간을 대폭 단축시킵니다.

다른 애플리케이션의 가시성을 보여주는 에이전트에는 VoIP 대기열 상태의 비정상적인 대기열 수치를 모니터링 하는 것뿐만 아니라 DHCP Relay 통계 수치에서 요청에 따른 응답률이 불일치하는 것 등을 모니터링 할 수 있습니다.

### 네트워크 최적화

NAE는 빠르게 근본 원인을 분석하는 것 외에도 네트워크의 트래픽 흐름을 최적화할 수 있습니다. NAE는 인터페이스 사용 및 애플리케이션 성능 통계를 활용하여 경로의 가중치를 조정하고 애플리케이션 트래픽을 다른 링크나 다른 서비스 공급자에게 전달합니다. 또한 트래픽 비율을 모니터링하고 LAG 활용률이 거의 동일하도록 하여 LAG 불균형을 방지 또는 수정할 수 있습니다. 이러한 기능은 비즈니스와 해당 사용자에게 더 나은 서비스 레벨을 보장합니다.

## NETEDIT 통합을 통한 추가적인 관리 간소화

NAE는 아루바의 스위치 구성 및 오케스트레이션 도구인 NetEdit와 긴밀하게 통합되어 있습니다. NetEdit는 IT 팀이 엔드 투 엔드 서비스 확장을 원활하게 조정하고 네트워크 전반의 변경을 신속하게 자동화하며 네트워크 업데이트 이후 정책 준수를 보장할 수 있도록 역량을 부여합니다.

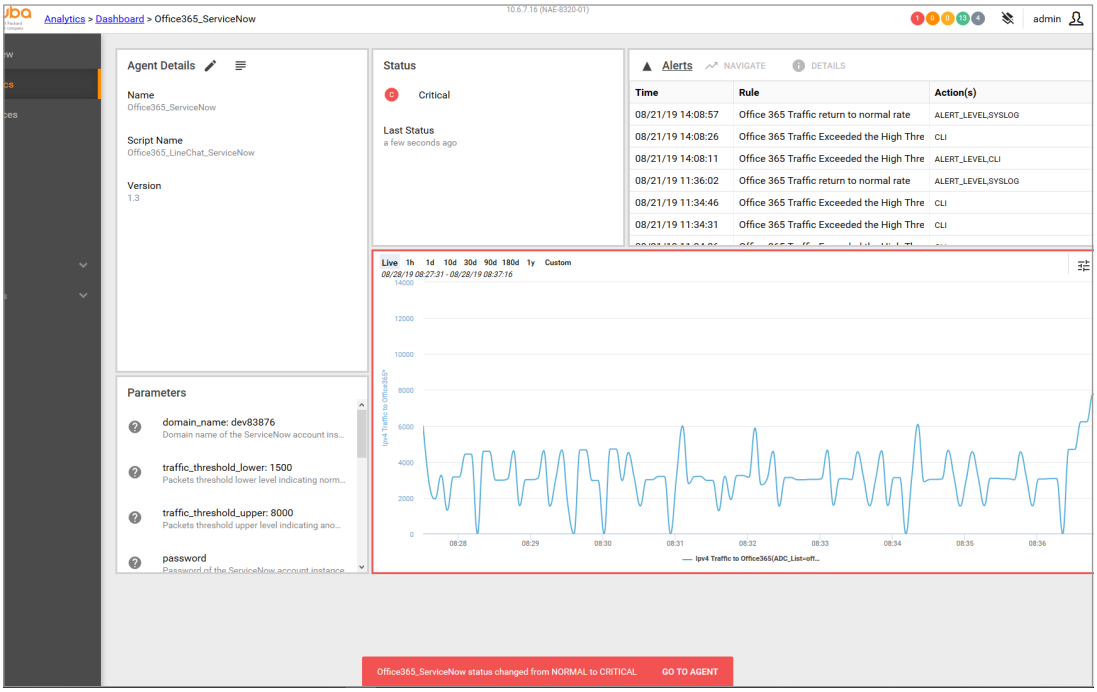



그림 4: Office 365 서비스 성능 저하에 대한 중요 경고

또한 NetEdit는 NAE의 임베디드 분석 기능을 사용하여 네트워크 운영자에게 단일 콘솔의 문제를 모니터링하고 해결할 수 있는 인사이트를 제공합니다.

NetEdit는 NAE 에이전트의 상태를 구독하여 관심을 갖고 있는 문제가 발생할 때 데이터를 수집하고 Slack 또는 다른 ITSM 도구를 통해 운영자에게 알림을 제출합니다. NetEdit를 클릭하면 운영자는 이벤트가 발생한 시간과 전체 진단 세부 정보와 함께 영향을 받은 장치와 서비스를 즉시 볼 수 있습니다.

NetEdit 및 NAE는 기존 방식으로 문제를 해결할 때 대비하여 발생하는 수동 데이터 수집 분량과 연계를 크게 줄입니다. 또한 네트워크에서 부하가 적게 발생하므로 텔레메트리 수집 과정에서 성능에 영향을 주지 않습니다.

## 커뮤니티 개발

Aruba는 고객이 NAE를 최대한 활용할 수 있도록 고객과 커뮤니티에 오픈 소스 라이센스를 제공하는 공유 에이전트 및 스크립트의 강력한 라이브러리를 구축했습니다. 이는 Aruba Solutions Exchange와 GitHub에서 모두 사용할 수 있습니다.

또한 Aruba Airheads 커뮤니티는 개발자와 네트워크 엔지니어가 다른 사용자 정의 사용 사례에 대해 NAE 에이전트를 논의, 구축 및 공유할 수 있는 온라인 포럼을 제공하여 크라우드소싱 개발을 촉진합니다.

## 결론

IT 팀은 탄력성, 성능 및 민첩성에 대한 요구사항을 충족하기 위해 네트워크 상태에 대한 가시성을 강화해야 합니다. 고객은 NAE를 통해 진단 작업을 자동화하고 점차 증가하고 있는 스크립트 라이브러리와 함께 분산된 네트워크 전반의 분석에 실시간으로 액세스하여 문제 해결 시간을 단축하고 네트워크 운영자 환경을 개선할 수 있습니다.

NAE 및 기타 스위칭 솔루션에 대한 자세한 내용은 Aruba 웹사이트를 방문하여 제품 데이터시트, 기술 개요 등을 확인하십시오.

또한 Aruba Solutions Exchange 또는 GitHub의 Aruba CX 6000 및 Aruba CX 8000 스위치 시리즈에서 사용 가능한 NAE 에이전트 전체 라이브러리를 볼 수 있습니다.



SO_NAE_092519 a00059004enw