SOLUTION OVERVIEW

ARUBA NETWORK ANALYTICS ENGINE

Accelerated troubleshooting and root cause analysis

Network operators face a number of challenges in today's digital world. IoT is introducing an exponential number of devices that IT must onboard and secure. Cloud adoption has created different traffic patterns on the network, and operators often lose visibility into performance. Lastly, workforce mobility means employees access apps over multiple networks, each delivering different levels of performance and security.

A highly available, always-on network is mission-critical for businesses today. However, these technology trends make this objective harder to achieve, as they create more stress and points of failure on the network.

Network operators now require better visibility to swiftly address issues as they are occurring. To meet this need, Aruba has developed the Network Analytics Engine (NAE), which is part of the AOS-CX network operating system.

NAE provides a built-in framework for monitoring and troubleshooting networks. It automatically interrogates and analyzes network events to provide unprecedented visibility into outages and anomalies. Using these insights, IT can detect problems in real time and analyze trends to predict or even avoid future security and performance issues.

FROM PROBLEM TO ROOT CAUSE

Finding the root cause of a network issue has traditionally involved many disparate tasks. To begin with, network operators may use a series of show commands to investigate the current status of the network, or they may run probes to try and recreate the problem.

KEY BENEFITS

- **Faster, complete visibility:** Built-in, time series database delivers event and correlation history and real-time access to network-wide insights to help operators deliver better experiences
- **Rapid MTTR:** Rules-based, real-time monitoring and intelligent notifications automatically correlate to configuration changes to help accelerate diagnostic routines
- **Simplified management:** Integrations with Aruba NetEdit and third-party tools such as ServiceNow and Slack provide the intelligence to integrate rich NAE alerts into IT service management processes
- **Continued innovation:** Access to an always-growing library of Aruba-curated NAE solutions and a community of experts working on additional innovations

If telemetry is available from the moment the problem occurred, manual configurations with external tools are often required to conduct proper analysis. But these data pipelines are often unfiltered, creating delays in transferring and processing data. Secondly, third-party monitoring tools often sample data, rather than capturing full detail, creating additional gaps in visibility.

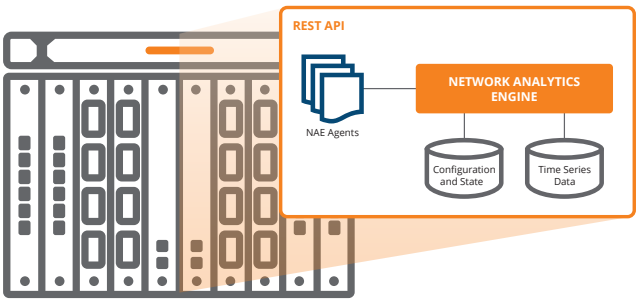

Figure 1: Aruba NAE collects advanced network analytics natively on the switch

Aruba NAE provides:

- Relevant historical data correlated with configuration changes
- Automated service impact and root cause analysis
- Intelligent monitoring agents 'always on'
- Complete telemetry for all system information
- Information from neighboring infrastructure
- Notifications with automatic diagnostics

Conversely, NAE performs intelligent monitoring directly on each switch, giving operators distributed analytics and actionable insights into network-wide health, without delays or loss of information.

With NAE, operators can proactively set rules to monitor specific traffic of interest, collect that data, and correlate it to events that trigger service alerts—all in an automated fashion. This allows NAE to rapidly drill down into an issue, accelerating service impact and root cause analysis for faster mean time to resolution (MTTR).

NAE COMPONENTS

NAE runs within the AOS-CX operating system on supported platforms such as Aruba CX 6000 and Aruba CX 8000 Switch Series (figure 2). It monitors a switch's configuration using agents that pull data from two key databases:

- Configuration and state database: Provides NAE agents with full access to configuration, protocol state, and network statistics—all fully exposed through REST APIs.
- Time series database: Contains relevant historical data correlated to configuration changes. This provides operators with the ability to capture, archive, and quickly access the state of the network surrounding a network event.

NAE agents test for conditions on the switch, its neighboring devices, or on traffic that is passing through the network, and then take actions based on the results of the test.

For example, a high hit count on an ACL that is triggered by an unknown host is an indication of a possible security breach. In this case, NAE could alert operators to the issue by creating a Syslog message or generating a custom report with results of the analysis, which is easily accessible through a web interface.

Operators can also combine multiple actions into existing workflows to perform more selective diagnostics or recommendations. This includes the ability to deliver notifications to IT service management systems such as ServiceNow or collaboration tools like Slack when an issue of interest occurs.

Besides providing the ability to monitor the status of a switch, the Web UI also allows networking teams to view and configure NAE agents, scripts, and alerts.

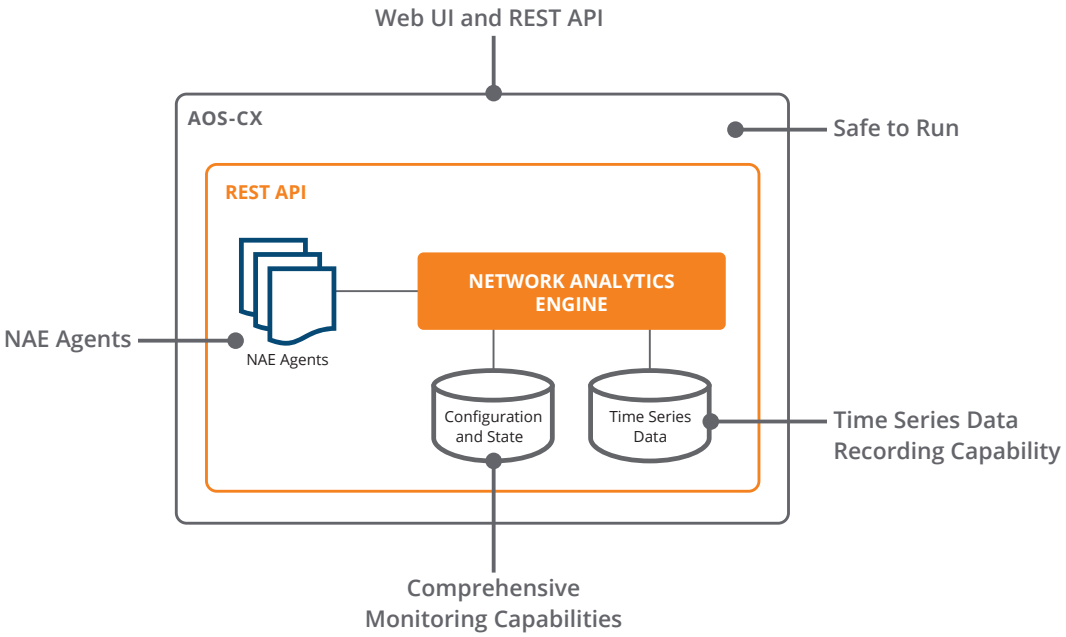

Figure 2: NAE Components

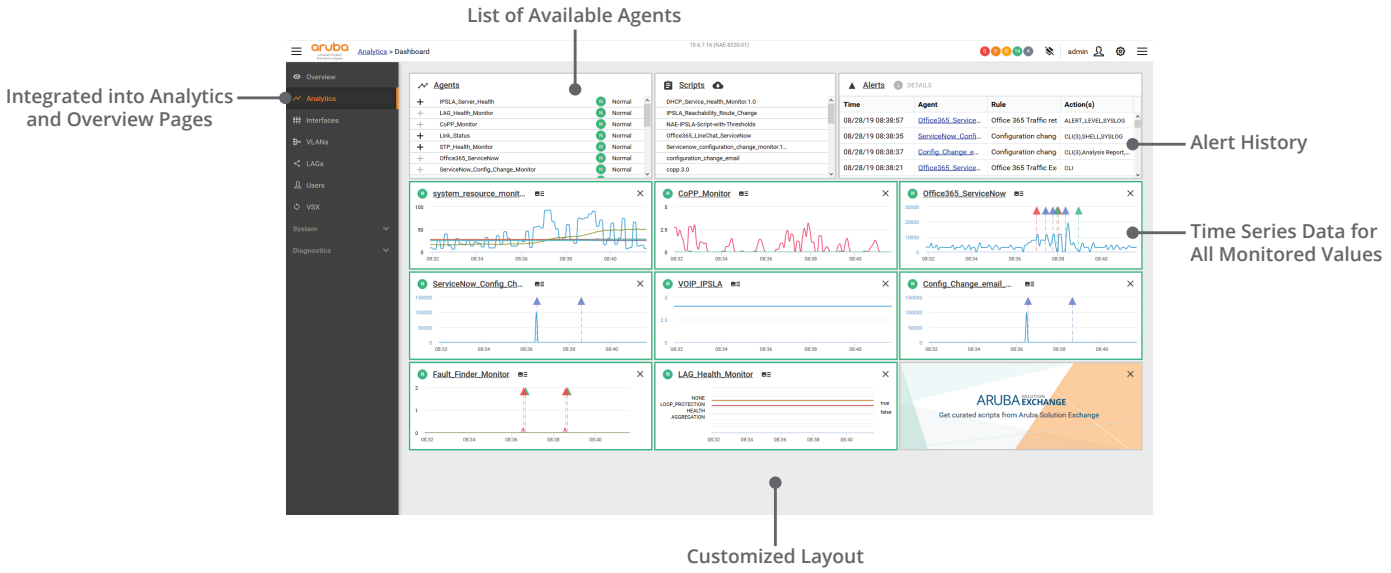

Figure 3: Aruba NAE Dashboard

EXAMPLE USE CASES

NAE maps network problems to their common root causes, accelerating troubleshooting routines by predetermining many first- and second-order diagnostics so operators can focus on a more targeted set of issues.

At a broader level, the use cases for NAE agents are:

1. System Health
2. Network Analytics
3. Security
4. Application Visibility
5. Network Optimization

System Health

Organizations need reliable intelligence on the status and performance of their switches. Relevant NAE agents monitor the health of the control plane's system resources, such as CPU and memory usage, and track this over time. When operators receive alerts due to an anomaly, NAE captures and archives detailed system information at the time of the spike.

System health agents also ensure availability for critical services such as TACACS+ and Syslog. These agents perform network diagnostics or take other appropriate actions (such as out-of-band notifications) if they are not.

Network Analytics

NAE can integrate all network statistics made available in AOS-CX with the time series database for analysis. The breadth of capabilities in this category cuts across everything from Layer 1 transceiver monitoring to Layer 3 health of BGP peers.

A wide range of use cases unfolds from the ability to monitor nearly every statistic in the system. Examples include:

- Transceiver Health: By monitoring transceiver TX and RX power levels, NAE can detect several different problems with the health of a connection. If power levels suddenly change, NAE compares these levels to a known baseline and provides high-probability guidance as to what happened with the fiber links between the two transceivers.
- OSPF Route Health: Routing protocols such as OSPF have a huge bearing on the operation of the network. NAE provides context into changes in OSPF tables. For example, NAE monitors link state advertisement (LSA) counters, providing insight into the number of routes available in the system. A sudden drop in an LSA number may mean that an OSPF neighbor is unavailable or is no longer supplying a normal number of routes. This often indicates a reachability problem, and NAE provides rapid insight into its origin.

Other network analytics agents include health monitors for Virtual Router Redundancy Protocol (VRRP), link aggregation (LAG) health, or spanning tree protocol (STP), as well as monitors for interface statistics.

Security

NAE can also identify and inspect errant traffic passing through AOS-CX switches at the access, aggregation, and core layers of the network. When this occurs, NAE can then take action on the traffic, or direct it to a security device for detailed inspection.

For example, consider an HVAC system, which typically only interacts with an HVAC controller. If NAE sees traffic from this system interacting with a source code repository or a database server, it is likely a hacked device. Upon detection, NAE can help quarantine the traffic and compromised devices by automatically communicating with Aruba ClearPass, which responds with predetermined, policy-based actions to cut off the threat before it extends to other parts of the network.

Other security agents include a configuration change monitor and a Control Plane Policing (COPP) monitor.

Application Visibility

NAE also provides visibility into application traffic as it traverses the core of the network. This includes tracking the performance of cloud applications such as Office 365 or Google Suite.

Upon detecting any degradation, the NAE agent performs robust network diagnostics. For example, if an Internet Service Provider (ISP) is delivering a degraded service, NAE provides insight into when the service started suffering, sharply reducing the time needed to isolate and address root cause.

Other application visibility agents include VoIP queue health to monitor the queue rate for anomalies, as well as DHCP relay statistics, which monitors the rates of requests and suggests root causes of mismatches.

Network Optimization

In addition to accelerating root cause analysis, NAE can also optimize traffic flows across a network. By leveraging interface usage and application performance statistics, NAE adjusts the weights of routes to direct application traffic over different links or to different providers. NAE can also prevent or correct LAG imbalances by monitoring traffic ratios and ensuring LAGs are at near-equal utilization. Such capabilities ensure a better class of service for the business and its users.

INTEGRATION WITH NETEDIT FOR ADDED MANAGEMENT SIMPLICITY

NAE is tightly integrated with NetEdit, Aruba's switch configuration and orchestration tool. NetEdit arms IT teams with the power to smoothly coordinate end-to-end service roll outs, automate rapid network-wide changes, and ensure policy conformance after network updates.

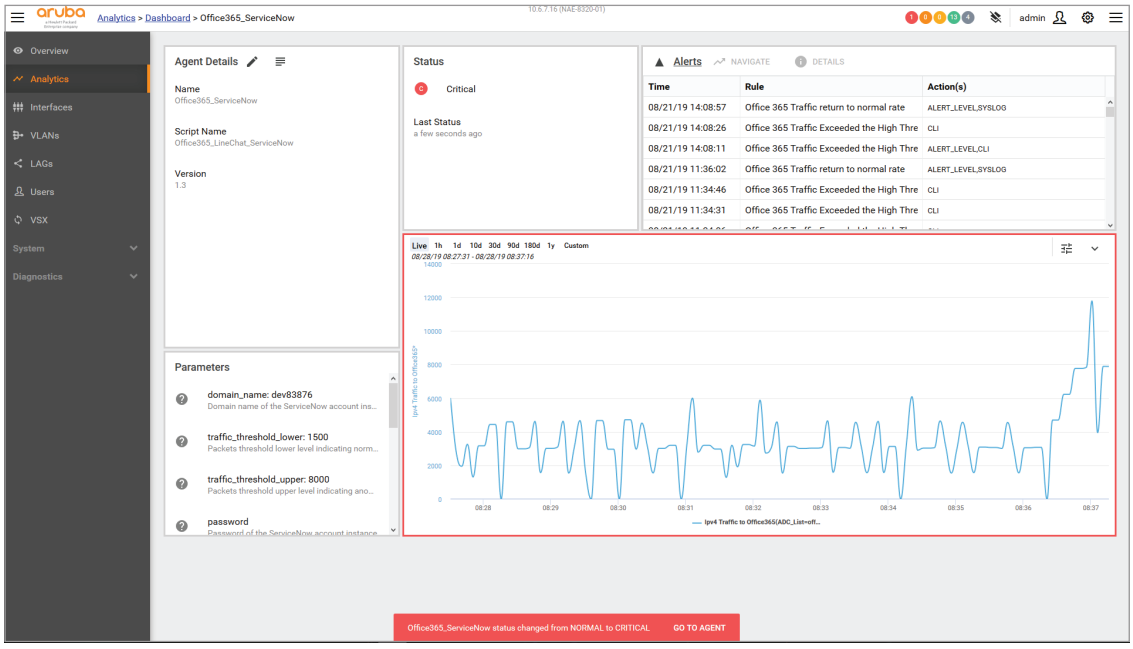

Figure 4: Critical Alert to Office 365 Service Degradation

With embedded analytics from NAE, NetEdit also gives network operators the insights to monitor and troubleshoot issues from a single console.

By subscribing to the status of the NAE agent, NetEdit collects data when an issue of interest occurs, and submits a notification to the operator via Slack or another ITSM tool. Upon clicking into NetEdit, the operator immediately sees the impacted devices and services, with full diagnostic details correlated to the time the event occurred.

In this manner, NetEdit and NAE significantly reduce the amount of manual data collection and correlation that occur when troubleshooting problems through traditional means. It also produces less load on the network, so performance is not impacted in the process of collecting telemetry.

COMMUNITY DEVELOPMENT

To help customers take full advantage of NAE, Aruba has created a robust library of shared agents and scripts, provided to customers and the community with an open source license. These are available on both the Aruba Solutions Exchange and GitHub.

The Aruba Airheads community also fosters crowdsourced development by providing an online forum for developers and network engineers to discuss, build, and share NAE agents for other custom use cases.

CONCLUSION

IT teams need greater visibility into network health to satisfy requirements for resiliency, performance, and agility. With NAE, customers get real-time access to distributed, network-wide analytics—along with an ever-growing library of scripts that automate diagnostic tasks—to speed troubleshooting and enhance the network operator experience.

To learn more about NAE and other switching solutions, visit the Aruba website for product data sheets, technical overviews, and more.

You can also view the complete library of NAE agents available on Aruba CX 6000 and Aruba CX 8000 Switch Series on the Aruba Solutions Exchange or on GitHub.

SO_NAE_SK_121119 a00059004enw