aruba
a Hewlett Packard Enterprise company

SOLUTION BRIEF

ROOT CAUSE ANALYSIS WITH ARUBA NETWORK ANALYTICS ENGINE

Automate Network Monitoring and Troubleshooting

INTRODUCTION

Network engineers face challenges when managing and maintaining the networks they operate. These challenges range from delivering new capabilities to ensuring the network is always available to support their business. Addressing the demands of high availability requires better visibility and tools for troubleshooting, root cause analysis and diagnostics.

To meet these needs, Aruba has an industry-leading portfolio of switches for the campus network. In particular, Aruba developed the Network Analytics Engine (NAE) as part of the ArubaOS-CX network operating system. With a fully programmable and database-driven design, only ArubaOS-CX is capable of supporting the advanced visibility enabled by the NAE.

NAE DESIGN AND COMPONENTS

Aruba designed NAE to be a highly flexible engine to enable a wide range of solutions to the various problems and challenges faced by network operators. In particular, the NAE helps operators quickly find root causes to problems using a sophisticated diagnostic capture system with deep analytics including machine-learning technologies.

From Problem to Root Cause

There are many disparate tasks involved to find root causes to problems (see Figure 1).

NAE agents perform intelligent monitoring at all times. For example, operators may continually monitor system health on the switch, network analytics at Layers 1-3, or application traffic.

NAE also provides automated diagnostics and data collection. This data enables generating time series graphs that help provide context surrounding problems or anomalies. Based on this context, the NAE performs further diagnostic actions.

In this way, NAE enables rapid drill down into root causes. Upon determining the root cause, NAE can either automate a resolution or provide the network operator with the needed information to quickly solve the problem.

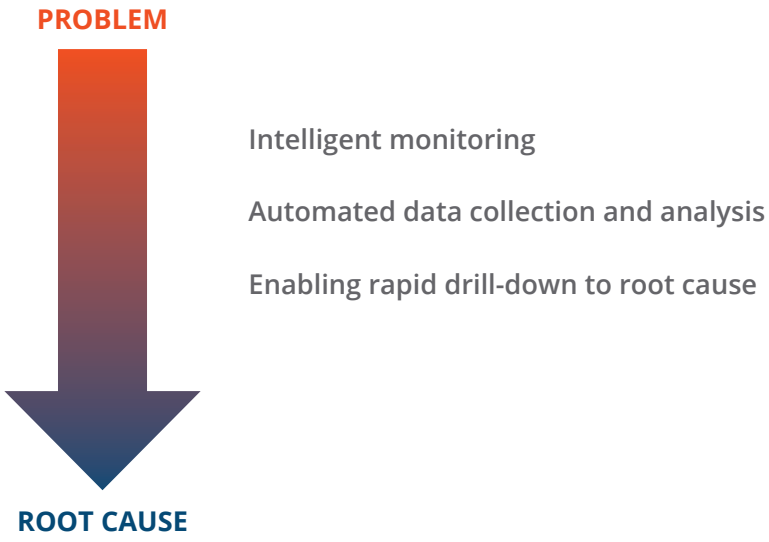

Figure 1: Faster Time to Root Cause with Monitoring, Data Collection and Analytics

NAE Components

NAE runs within the ArubaOS-CX operating system on supported platforms such as the Aruba 8000 series. Figure 2 depicts a high-level diagram of NAE.

Engineers can easily access the NAE through a Web interface, and REST APIs allow access to individual agents (which run securely in Linux containers) and to NAE databases. When a problem arises, these agents notify IT staff of the issue and provide results of the analysis.

NAE accesses two key databases within ArubaOS-CX:

- The Configuration and State Database provides NAE agents with full access to configuration, protocol state, and network statistics—all fully exposed through REST APIs.
- The Time Series Database contains relevant historical data correlated with configuration changes. This provides operators with the ability to capture and archive the network context surrounding a network event.

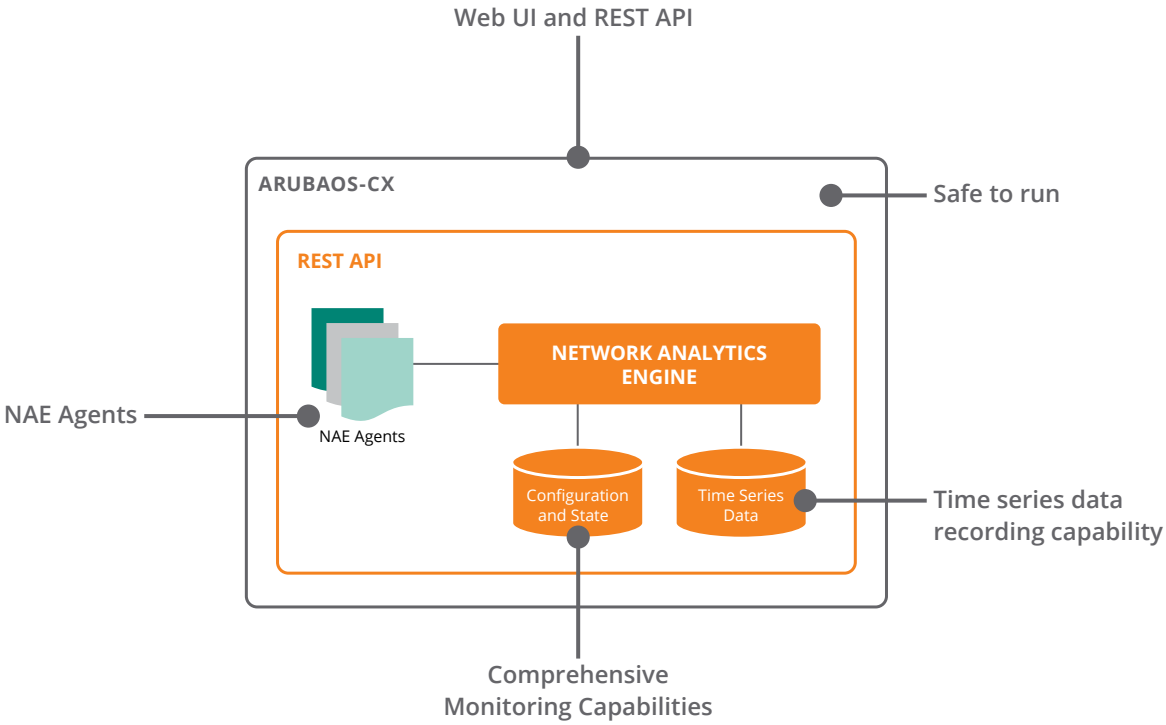

Figure 2: NAE Components

NAE agents test for conditions and take actions based on the results the condition. An example of a condition might be a high hit count on an ACL, which would trigger an action to generate an alert and create a Syslog message or a custom report. Operators can also combine multiple actions into workflows to perform more selective diagnostics or recommendations.

The ArubaOS-CX Web UI (Figure 3) provides quick and easy visibility.

Besides providing the ability to monitor the status of a switch, the Web UI allows you to view and configure NAE agents, scripts, and alerts. Automatically generated graphs enable additional context that is required for troubleshooting networks.

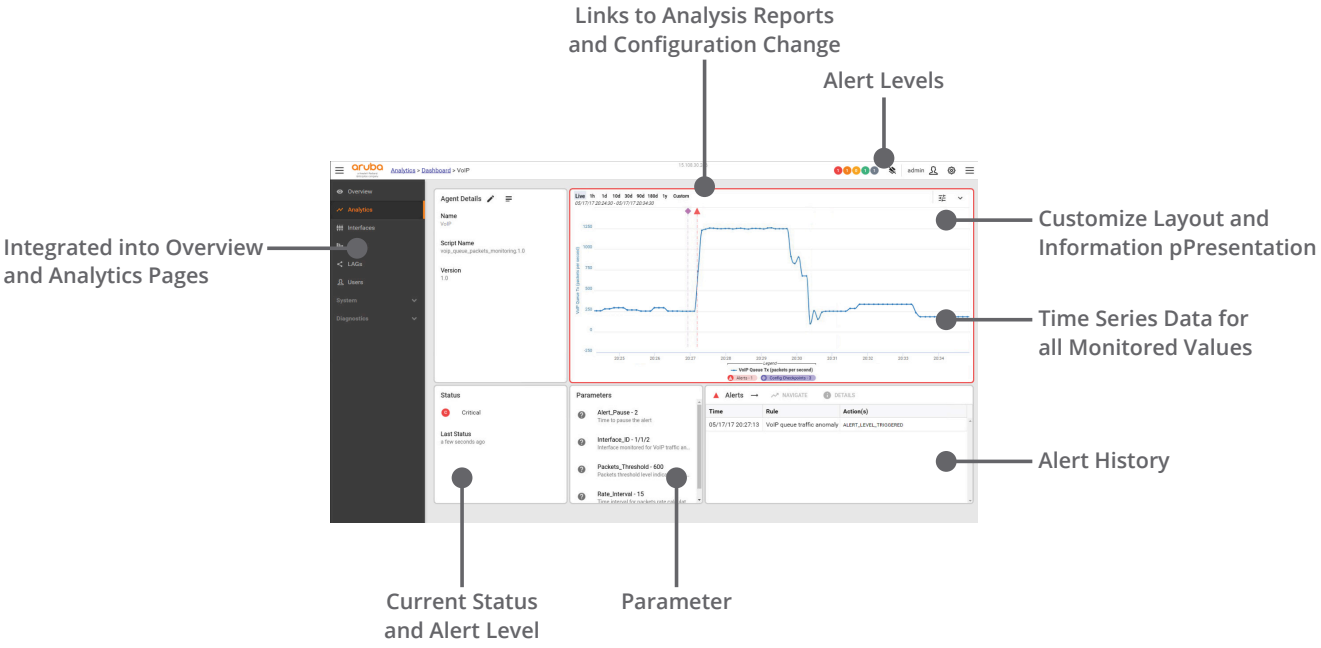

Figure 3: ArubaOS-CX Web UI

NAE USE CASE CATEGORIES WITH EXAMPLES

NAE maps user problems to root causes by automating common diagnostic routines that often lead directly to the exact problem. Using built-in monitors and data collection agents, the NAE predetermines many first and second order diagnostics, allowing operators to focus on a smaller and more targeted set of root causes.

For example, increased latency due to congestion or packet drops causes poor VoIP quality. However, the root cause could be at the physical layer (a bad cable), link state issues at Layers 2 or 3, or an MTU misconfiguration.

Similarly, connection difficulties to a network or peripherals could also be due to any of the above causes cited in the VoIP example, but could also be an ISP service failure. In addition, application access issues into email, SharePoint, or cloud systems could be due to problems with DHCP reachability, or simply due to configuration errors.

A relatively new class of problems involves IoT devices including projectors, cameras, or other building systems such as door locks. In addition to lower-layer network problems, these problems could indicate security issues (a hacked device).

The NAE includes built-in agents to help monitor, diagnose and resolve all of the above issues and more. At a broad level, the use case categories for NAE agents are:

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

System Health

Enterprises need reliable intelligence of 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 customers receive NMS alerts due to an anomaly such as high CPU usage, the NAE captures and archives detailed system information at the time of the spike. This helps ensure rapid root cause analysis and timely resolution.

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 ArubaOS-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, the 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. Another class of problems involves fading power on transceivers. If RX power slowly trends to zero, or TX power slowly rises, a threshold-crossing alert (TCA) informs the network engineer that the transceiver is fading and will soon need replacement, thus enabling a planned resolution/upgrade instead of a random outage.
- **OSPF Route Health:** Routing protocols such as OSPF have a huge bearing on the efficient operation of the network. NAE monitors and provides context and insight 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.

Upon detection of anomalies, the NAE helps diagnose root causes. For instance, a sudden drop in an LSA number may mean that an OSPF neighbor is unavailable or no longer supplying as many routes as is normal. In many cases, this will indicate a reachability problem—the NAE provides rapid insight into the origin of the problem.

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

Using the ability of the Aruba 8000 series to locate traffic passing through the aggregation and core portions of the network, NAE inspects and identifies errant traffic. 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 would only interact with an HVAC controller. If NAE sees traffic from this system interacting with (for instance) a source code

repository or a database server, it is likely to be a hacked device. NAE can direct this traffic to Aruba Introspect, a User and Entity Behavior Analytics (UEBA) solution, for complete and intensive endpoint diagnostics. After investigation, the admin can adjust the threshold or take quarantine action against the compromised device automatically using Aruba ClearPass.

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

Application Visibility

In our cloud and mobile world, being able to monitor business critical network services is key. NAE's application data collectors enable visibility at Layers 3 and 4 into application traffic as it traverses the core of the network. NAE monitors cloud applications such as Office365 or Google Suite, tracking their performance across time. Upon detecting the degradation, NAE agent performs robust network diagnostics.

For example, if an Internet Service Provider (ISP) is delivering degraded service, NAE immediately provides insight when the event was discovered, sharply reducing the time of the network engineering team to isolate, respond and address root cause.

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

Network Optimization

This category diverges from root cause analysis and directs the focus at optimizing traffic by using NAE's analytics capability in conjunction with automation. By leveraging interface usage and application performance statistics, NAE can adjust the weights of routes to direct application traffic out different links or to different providers. This ensures a better class of service for the business and users, and an optimal network for the IT team. NAE can also prevent or correct LAG imbalances by monitoring traffic ratios and ensuring LAGs are near equal utilization.

COMMUNITY

To help customers take advantage of the powerful automation capabilities within the Aruba 8400 and 8320 Switches, Aruba provides an ecosystem with shared scripts created and provided to our customers and the community with an open source license.

Aruba has created many NAE agents based on the popular Python language; these are available on both the Aruba Solutions Exchange (ASE) and GitHub, ensuring a wide availability of automation examples. The Aruba Airheads community allows developers and network engineers to come together online, and discuss and build NAE agents and custom solutions for relevant use cases.

CONCLUSION

NAE is a powerful solution designed to meet the current and evolving needs of network operators. By leveraging the power of ArubaOS-CX, the NAE creates a flexible and valuable solution to rapidly drill down from high-level network problems and enable quick root cause discovery and resolution. There are many compelling use cases already available, from ensuring that Aruba 8000-series switches are online and operating at peak performance, to enhancing the security profile of your IoT network and locating potentially dangerous and previously hidden attacks.

Aruba is embracing the community and has built a highly flexible solution for the future. Developers and network operators can use tools relevant to their background and communicate on the Aruba Airheads community to build unique solutions directly relevant to their unique networks.

TO LEARN MORE

The Aruba Campus Switches main page contains product datasheets and technical overviews.

Aruba NAE Agents are available here at the Aruba Solutions Exchange and on GitHub.

SB_NetworkAnalyticsEngine_102518 a00059004enw