LÖSUNGSÜBERBLICK

ARUBA NETWORK ANALYTICS ENGINE

Schnellere Fehlerbehebung und Ursachenanalyse

Die digitale Welt von heute stellt Netzwerkoperatoren vor zahlreiche Herausforderungen. Mit dem IoT nimmt die Anzahl von Geräten, die von der IT eingebunden und gesichert werden müssen, exponentiell zu. Die Einführung der Cloud hat für unterschiedliche Muster im Netzwerkverkehr gesorgt, und dadurch verlieren Operatoren häufig die Übersicht über die Leistung. Zudem bringt es die Mobilität der Mitarbeiter mit sich, dass diese über verschiedene Netzwerke mit jeweils unterschiedlicher Leistung und Sicherheit auf Anwendungen zugreifen.

Ein unterbrechungsfrei und hoch verfügbares Netzwerk ist für Unternehmen heute von geschäftskritischer Bedeutung. Die genannten Technologietrends machen es jedoch schwieriger, dieses Ziel zu erreichen, da sie für mehr Stress und Fehlerquellen im Netzwerk sorgen.

Netzwerkoperatoren benötigen jetzt mehr Transparenz, um schnell auf Probleme reagieren zu können, sobald diese auftreten. Um diesem Bedarf gerecht zu werden, hat Aruba die Network Analytics Engine (NAE) als Teil des Netzwerkbetriebssystems AOS-CX entwickelt.

NAE bietet ein integriertes Framework für die Überwachung und Fehlerbehebung von Netzwerken. Netzwerkereignisse werden automatisch abgefragt und analysiert, um so ein beispielloses Maß an Einblick in Ausfälle und Anomalien zu erhalten. Anhand dieses Einblicks kann die IT Probleme in Echtzeit erkennen und Trends analysieren, um zukünftige Sicherheits- und Leistungsprobleme vorherzusagen oder sogar vermeiden zu können.

WESENTLICHE VORTEILE

- **Schnellere und vollständige Transparenz:** Die integrierte Zeitreihen-Datenbank liefert Daten zum Ereignis- und Korrelationsverlauf und Echtzeit-Zugriff auf netzwerkweite Einblicke, um den Operatoren bei der Bereitstellung besserer Erlebnisse für die Benutzer zu helfen.
- **Schnelle MTTR:** Regelbasierte Echtzeitüberwachung und intelligente Benachrichtigungen korrelieren automatisch mit Konfigurationsänderungen, um Diagnoseroutinen zu beschleunigen.
- **Vereinfachtes Management:** Die Integration mit Aruba NetEdit und Drittanbieter-Tools wie ServiceNow und Slack bietet die Informationen, um detaillierte NAE Warnungen in IT-Servicemanagementprozesse zu integrieren.
- **Fortlaufende Innovation:** Zugriff auf eine stetig wachsende Bibliothek aus von Aruba kuratierten NAE-Lösungen sowie eine Community aus Experten, die an weiteren Innovationen arbeiten

VOM PROBLEM ZUR URSACHE

Die Suche nach der Ursache eines Netzwerkproblems ist gewöhnlich mit vielen unterschiedlichen Aufgaben verbunden. Zunächst einmal können Netzwerkoperatoren eine Reihe von Befehlen nutzen, um den aktuellen Status des Netzwerks zu ermitteln, oder sie führen Untersuchungen durch, um zu versuchen, das Problem zu reproduzieren.

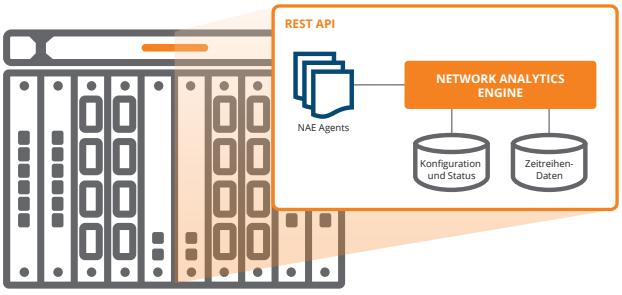

Abbildung 1: Aruba NAE erfasst erweiterte Netzwerkanalysen nativ am Switch

Aruba NAE stellt folgendes bereit:

- Relevante historische Daten im Zusammenhang mit Konfigurationsänderungen
- Automatisierte Serviceauswirkungs- und Ursachenanalyse
- Intelligente, jederzeit verfügbare Überwachungs-Agents
- Vollständige Telemetriedaten für alle Systeminformationen
- Informationen aus benachbarten Infrastrukturen
- Benachrichtigungen mit automatischer Diagnose

Sollten ab dem Zeitpunkt des Auftretens des Problems Telemetriedaten zur Verfügung stehen, sind oft manuelle Konfigurationen mit externen Tools erforderlich, um eine ordnungsgemäße Analyse durchzuführen. Diese Datenpipelines sind jedoch häufig ungefiltert und führen zu Verzögerungen bei der Übertragung und Verarbeitung von Daten. Hinzu kommt, dass Überwachungstools von Drittanbietern oft nur Stichproben nehmen, anstatt alle Details zu erfassen, was zu zusätzlichen Lücken in der Transparenz führt.

NAE hingegen führt intelligente Überwachung direkt am Switch durch und liefert Operatoren so verteilte Analysen und nutzbare Informationen zum netzwerkweiten Status, und das ohne Verzögerungen oder Informationsverluste.

Mit NAE können Operatoren proaktiv Regeln zur Überwachung bestimmten Datenverkehrs festlegen, diese Daten erfassen und mit Ereignissen in Verbindung bringen, die zu Servicewarnungen führen – und das alles automatisch. Auf diese Weise kann NAE schnell eine Aufschlüsselung des Problems vornehmen und so die Serviceauswirkungs- und Ursachenanalyse für eine schnellere Mean Time to Resolution (MTTR) beschleunigen.

NAE KOMPONENTEN

NAE läuft innerhalb des AOS-CX Betriebssystems auf unterstützten Plattformen wie der Aruba CX 6000 und der Aruba CX 8000 Switch-Serie (Abbildung 2). Es überwacht die Konfiguration eines Switches über Agents, die Daten aus zwei zentralen Datenbanken beziehen:

- Konfigurations- und Statusdatenbank: Bietet NAE Agents vollen Zugriff auf Konfiguration, Protokollstatus und Netzwerkstatistiken – alles vollständig zugänglich über REST APIs.
- Zeitreihen-Datenbank: Enthält relevante historische Daten im Zusammenhang mit Konfigurationsänderungen. Dies gibt Operatoren die Möglichkeit, den Zustand des Netzwerks um ein Netzwerkereignis herum zu erfassen, zu archivieren und schnell darauf zuzugreifen.

NAE Agents testen Bedingungen am Switch, an benachbarten Geräten oder im Datenverkehr, der das Netzwerk passiert, und ergreifen je nach Ergebnis entsprechende Maßnahmen.

So ist beispielsweise eine hohe Trefferquote bei einer ACL, die von einem unbekannten Host ausgelöst wird, ein Hinweis auf eine mögliche Sicherheitsverletzung. In diesem Fall könnte NAE Operatoren über das Problem

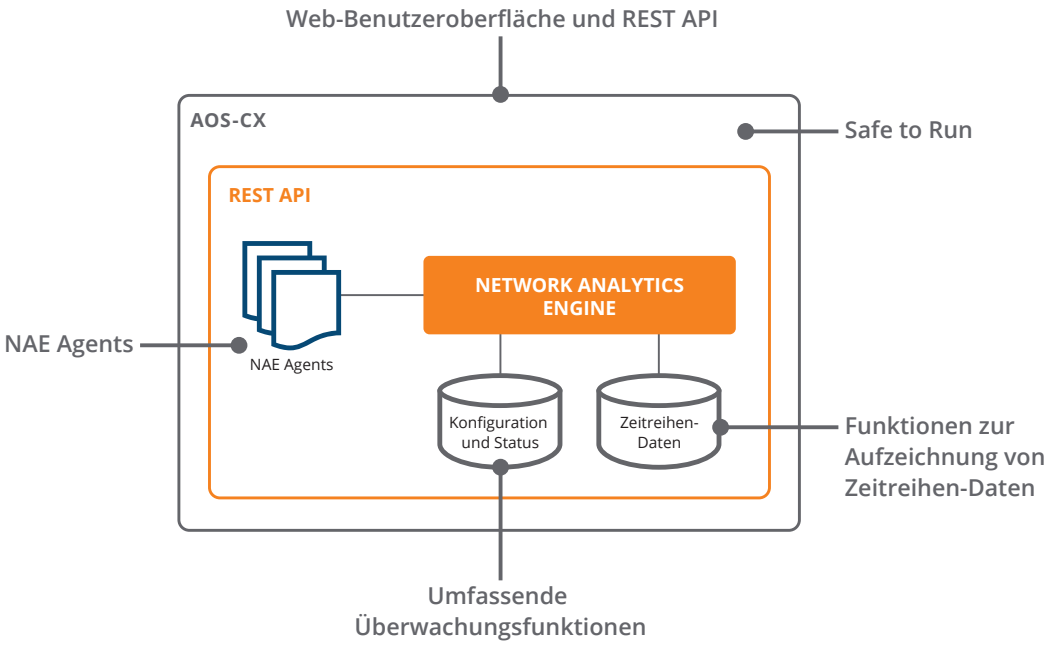

Abbildung 2: NAE Komponenten

Abbildung 3: Aruba NAE Dashboard

informieren, indem es eine Syslog-Meldung erstellt oder einen benutzerdefinierten Bericht mit den Ergebnissen der Analyse generiert, der über eine Weboberfläche einfach zugänglich ist.

Operatoren können mehrere Aktionen auch in vorhandenen Workflows kombinieren, um eine selektivere Diagnose oder Empfehlung auszuführen. Dazu gehört auch die Möglichkeit, Benachrichtigungen an IT-Service-Managementsysteme wie ServiceNow oder Collaboration-Tools wie Slack bereitzustellen, wenn ein Problem von Interesse auftritt.

Neben der Möglichkeit, den Status eines Switches zu überwachen, können Netzwerkteams über die Web-Benutzeroberfläche auch NAE Agents, Skripts und Warnungen anzeigen und konfigurieren.

FALLBEISPIELE

NAE ordnet Netzwerkprobleme den gemeinsamen Ursachen zu und beschleunigt Fehlerbehebungsroutinen, indem es zahlreiche Diagnosen erster und zweiter Ordnung bestimmt, damit sich die Operatoren gezielter auf bestimmte Probleme konzentrieren können.

Allgemein gibt es für NAE Agents folgende Anwendungsfälle:

1. Systemstatus
2. Netzwerkanalyse
3. Sicherheit
4. Anwendungstransparenz
5. Netzwerkoptimierung

Systemstatus

Unternehmen benötigen verlässliche Informationen über den Status und die Leistung ihrer Switches. Relevante NAE Agents überwachen den Status der Systemressourcen der Steuerungsebene, wie CPU- und Speicherauslastung, und verfolgen diesen im Zeitablauf. Wenn Operatoren aufgrund einer Anomalie Warnmeldungen erhalten, erfasst und archiviert NAE detaillierte Systeminformationen zum Zeitpunkt der Störung.

Systemstatus-Agents gewährleisten auch die Verfügbarkeit kritischer Services wie TACACS+ und Syslog. Diese Agents führen Netzwerkdiagnosen durch oder ergreifen ansonsten andere geeignete Maßnahmen (z. B. Out-of-Band-Benachrichtigungen).

Netzwerkanalyse

NAE kann alle in AOS-CX verfügbaren Netzwerkstatistiken zu Analysezwecken mit der Zeitreihen-Datenbank integrieren. Die Bandbreite der Funktionen in dieser Kategorie erstreckt sich von der Überwachung von Layer-1-Transceivern bis hin zur Überwachung des Layer-3-Status von BGP-Peers.

Aus der Möglichkeit, nahezu jede Statistik im System zu überwachen, ergibt sich eine Vielzahl von Anwendungsfällen. Beispiele:

- Transceiver-Status: Durch die Überwachung der TX- und RX-Leistung von Transceivern kann NAE verschiedene Probleme mit dem Status einer Verbindung erkennen. Im Falle plötzlicher Leistungsschwankungen vergleicht

NAE die jeweilige Werte mit einer bekannten Baseline und liefert Hinweise darauf, was mit den Glasfaserverbindungen zwischen den beiden Transceivern höchstwahrscheinlich passiert ist.

- OSPF-Routenstatus: Routingprotokolle wie OSPF haben einen großen Einfluss auf den Betrieb des Netzwerks. NAE liefert Kontext zu Änderungen in OSPF-Tabellen. So überwacht NAE beispielsweise LSA-Zähler (Link State Advertising), um Aufschluss über die Anzahl der im System verfügbaren Routen zu geben. Ein plötzlicher Abfall einer LSA-Zahl kann bedeuten, dass ein OSPF-Nachbar nicht verfügbar ist oder keine normale Anzahl von Routen mehr liefert. Dies weist häufig auf ein Erreichbarkeitsproblem hin, und NAE liefert einen schnellen Einblick in dessen Ursache.

Zu den weiteren Netzwerkanalyse-Agents gehören Statusmonitore für VRRP (Virtual Router Redundancy Protocol), Link Aggregation (LAG) oder STP (Spanning Tree Protocol) sowie Monitore für Schnittstellenstatistiken.

Sicherheit

NAE kann auch fehlerhaften Datenverkehr, der AOS-CX Switches in den Zugriffs-, Aggregations- und Kernschichten des Netzwerks durchläuft, identifizieren und überprüfen. Ist dies der Fall, kann NAE Maßnahmen für den Verkehr durchführen oder diesen zur genaueren Überprüfung an ein Sicherheitsgerät weiterleiten.

Beispiel: ein HLK-System, das typischerweise nur mit einem HLK-Controller interagiert. Wenn NAE bemerkt, dass Datenverkehr von diesem System mit einem Quellcode-Repository oder einem Datenbankserver interagiert, wurde das Gerät vermutlich gehackt. NAE kann diesen Verkehr an Aruba IntroSpect leiten, eine UEBA-Lösung (User and Entity Behavior Analytics) um eine vollständige und umfassende Endpunktdiagnose durchführen zu lassen. Nach der Untersuchung kann der Administrator die Richtlinie anpassen, die die unerwünschte Kommunikation zugelassen hat, oder unter Verwendung von Aruba ClearPass automatisch Quarantänemaßnahmen für das betroffene Gerät ergreifen.

Zu den weiteren Sicherheits-Agents gehören ein Konfigurationsänderungsmonitor und ein COPP-Monitor (Control Plane Policing).

Anwendungstransparenz

NAE bietet auch Einblick in den Anwendungsverkehr, wenn dieser den Kern des Netzwerks durchquert. Dazu gehört auch die Verfolgung der Leistung von Cloud-Anwendungen wie Office 365 oder Google Suite.

Sobald es zu Leistungseinbußen kommt, führt der NAE-Agent eine robuste Netzwerkdiagnose durch. Wenn beispielsweise ein Internetdienstanbieter einen beeinträchtigten Service bereitstellt, gibt NAE Aufschluss darüber, wann die Serviceverschlechterung eingesetzt hat, wodurch die zur

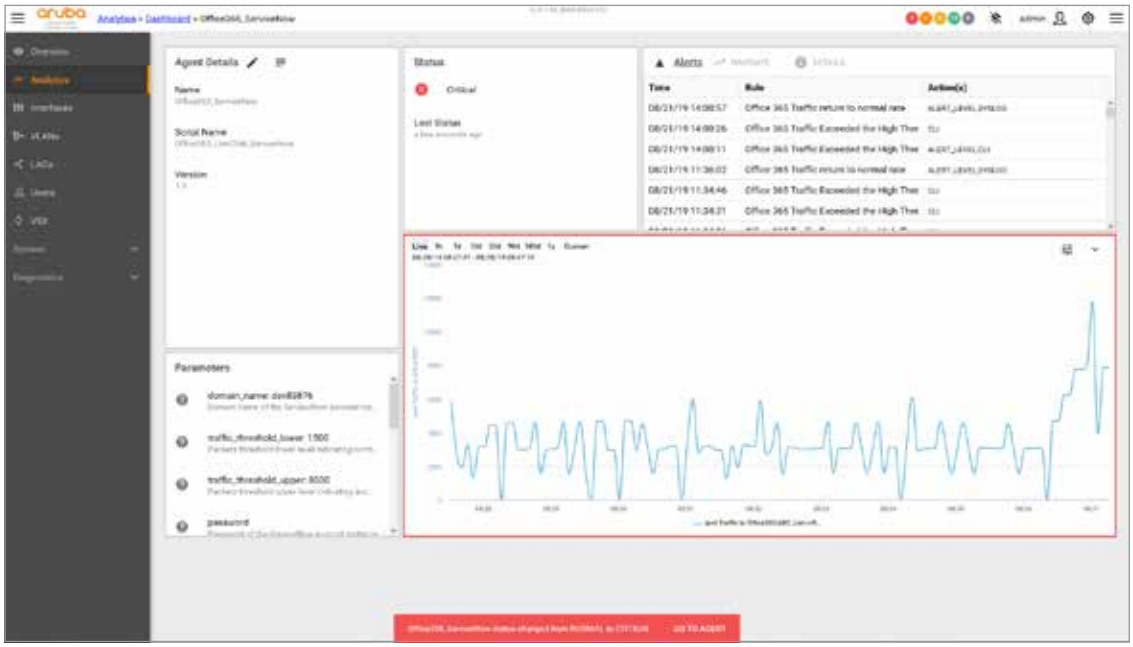

Abbildung 4: Kritische Warnung wegen Verschlechterung des Office 365 Services

Isolierung und Behebung der Ursache erforderliche Zeit beträchtlich reduziert wird.

Andere Agents für die Anwendungstransparenz umfassen den Status der VoIP-Warteschlange, um die Warteschlange auf Anomalien zu überwachen, sowie DHCP-Relay-Statistiken, um die Anzahl von Anfragen zu überwachen und auf mögliche Ursachen von Diskrepanzen hinzuweisen.

Netzwerkoptimierung

Neben der Beschleunigung der Ursachenanalyse kann NAE auch Datenverkehrsflüsse in einem Netzwerk optimieren. Durch die Nutzung der Statistiken zu Schnittstellenauslastung und Anwendungsleistung passt NAE die Gewichtung der Routen an, um Anwendungsverkehr über verschiedene Links oder an verschiedene Provider zu leiten. NAE kann auch LAG-Ungleichgewichte verhindern oder korrigieren, indem es die Datenverkehrsquoten überwacht und sicherstellt, dass LAGs möglichst gleichberechtigt genutzt werden. Derartige Funktionen gewährleisten eine bessere Serviceklasse für Unternehmen und Benutzer.

INTEGRATION IN NETEDIT FÜR EIN EINFACHERES MANAGEMENT

NAE ist eng in NetEdit integriert, dem Tool für die Switch-Konfiguration und -Orchestrierung von Aruba. NetEdit verschafft IT-Teams die Möglichkeit zur reibungslosen Koordination von End-to-End-Service-Rollouts, zur schnellen Automatisierung netzwerkweiter Änderungen und zur Gewährleistung der Richtlinienkonformität nach Netzwerkaktualisierungen.

Mit den eingebetteten Analysen von NAE bietet NetEdit Operatoren auch den nötigen Einblick, um Probleme von einer einzelnen Konsole aus zu überwachen und zu beheben.

NetEdit abonniert den Status des NAE Agent, erfasst so Daten, wenn ein Problem von Interesse auftritt, und übermittelt über Slack oder ein anderes ITSM-Tool eine Benachrichtigung an den Operator Wenn der Operator in NetEdit klickt, sieht er sofort, welche Geräte und Services betroffen sind, und erhält umfassende Diagnosedetails vom Zeitpunkt des Auftretens des zugrunde liegenden Ereignisses.

Auf diese Weise tragen NetEdit und NAE signifikant dazu bei, die Menge an manueller Datenerfassung und -korrelation, die bei der Fehlerbehebung durch herkömmliche Methoden üblicherweise anfällt, zu reduzieren. Außerdem wird das Netzwerk weniger belastet, so dass die Leistung bei der Erfassung der Telemetriedaten nicht beeinträchtigt wird.

AUSBAU DER COMMUNITY

Damit Kunden die Vorteile von NAE voll ausschöpfen können, hat Aruba eine solide Bibliothek aus gemeinsamen Agents und Skripts erstellt, die Kunden und der Community mit einer Open-Source-Lizenz zur Verfügung gestellt werden. Die Bibliothek ist sowohl über Aruba Solutions Exchange als auch über GitHub verfügbar.

Die Aruba Airheads Community fördert auch die Crowdsourcing-Entwicklung, indem sie ein Online-Forum für Entwickler und Netzwerktechniker bietet, in dem NAE-Agents für andere kundenspezifische Anwendungsfälle diskutiert, erstellt und ausgetauscht werden können.

FAZIT

IT-Teams benötigen mehr Einblick in den Netzwerkstatus, um die Anforderungen an Resilienz, Leistung und Agilität zu erfüllen. Mit NAE erhalten Kunden Echtzeit-Zugriff auf verteilte, netzwerkweite Analysen – zusammen mit einer stetig wachsenden Bibliothek aus Skripts zur Automatisierung von Diagnoseprogrammen –, um die Fehlerbehebung zu beschleunigen und die Bedienerfreundlichkeit zu verbessern.

Weitere Informationen zu NAE und anderen Switching-Lösungen, darunter Produktdatenblätter, technische Übersichten und mehr, finden Sie auf der Aruba-Website.

Eine vollständige Ansicht der Bibliothek aus verfügbaren NAE Agents der Aruba CX 6000 und der Aruba CX 8000 Switch-Serie finden Sie auch auf Aruba Solutions Exchange oder auf GitHub.

a Hewlett Packard Enterprise company

SO_NAE_092519 a00059004dee