

DESCRIPCIÓN GENERAL DE LA SOLUCIÓN

MOTOR DE ANÁLISIS DE RED ARUBA

Solución de problemas y análisis de causas raíz a gran velocidad

En el mundo digital actual, los operadores de red se enfrentan a numerosos retos. El IoT está introduciendo un número exponencial de dispositivos que la TI debe incorporar y proteger. La adopción de la nube ha creado patrones de tráfico diferentes en la red y, con frecuencia, los operadores pierden la visibilidad del rendimiento. Por último, la movilidad de los empleados significa acceso a aplicaciones en multitud de redes, cada una de las cuales con niveles de seguridad y rendimiento diferentes.

Una red siempre en funcionamiento y de alta disponibilidad resulta crucial para las empresas actuales. No obstante, estas tendencias tecnológicas suelen complicar la consecución de este objetivo, pues generan más tensión y puntos de fallo en la red.

Ahora, los operadores de red precisan mayor visibilidad para abordar con rapidez los problemas en el momento en que se producen. Para hacer frente a esta necesidad, Aruba ha desarrollado el motor de análisis de red (NAE), que forma parte del sistema operativo de red AOS-CX.

El NAE proporciona un marco integrado para la supervisión y la solución de problemas de red. Interroga y analiza de forma automática los eventos de red para proporcionar una visibilidad sin precedentes de las interrupciones y las anomalías. Utilizando estos conocimientos, la TI puede detectar problemas en tiempo real y analizar tendencias para predecir o incluso evitar problemas de seguridad y rendimiento futuros.

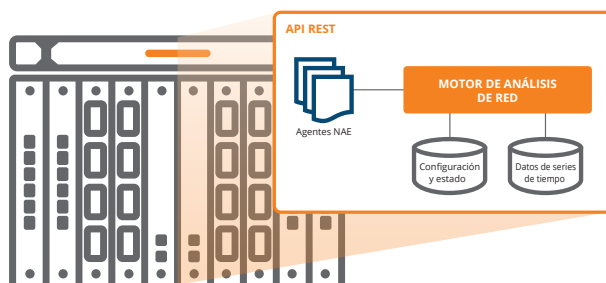


Figura 1: El NAE de Aruba recopila análisis de red avanzados de forma nativa en el switch

VENTAJAS PRINCIPALES

- **Visibilidad completa y más rápida:** La base de datos de series de tiempo integrada ofrece un historial de correlaciones y eventos, además de acceso en tiempo real a conocimientos a escala de la red para ayudar a los operadores a mejorar la experiencia.
- **Tiempo medio hasta la resolución reducido:** La supervisión en tiempo real basada en reglas y las notificaciones inteligentes correlacionan automáticamente los cambios en la configuración para ayudar a acelerar las rutinas de diagnóstico.
- **Gestión simplificada:** Las integraciones con Aruba NetEdit y herramientas de terceros, como ServiceNow y Slack, proporcionan los conocimientos necesarios para incorporar alertas NAE enriquecidas en los procesos de gestión del servicio de TI.
- **Innovación continua:** El acceso a una creciente biblioteca de soluciones NAE perfeccionadas por Aruba y a una comunidad de expertos que trabajan en innovaciones adicionales.

DESDE EL PROBLEMA A LA CAUSA RAÍZ

Tradicionalmente, encontrar la causa raíz de un problema de red solía implicar la realización de muchas tareas dispares. Para empezar, los operadores de red podían utilizar una serie de comandos de demostración para investigar el

El NAE Aruba ofrece:

- Datos históricos relevantes correlacionados con cambios de configuración
- Análisis automatizados de impacto en el servicio y causas raíz
- Agentes de supervisión inteligentes siempre en funcionamiento
- Telemetría completa para toda la información del sistema
- Información de infraestructura cercana
- Notificaciones con diagnóstico automático

estado actual de la red o incluso enviar sondas para intentar recrear el problema.

Si hay disponibles datos telemétricos desde el momento en que tiene lugar el problema, suelen ser necesarias configuraciones manuales con herramientas externas para llevar a cabo un análisis adecuado. Sin embargo, estos canales de datos con frecuencia no tienen filtros, por lo que producen demoras en la transferencia y el procesamiento de los datos. En segundo lugar, las herramientas de supervisión de terceros suelen tomar muestras de datos, en lugar de captar detalles completos, creando lagunas adicionales en la visibilidad.

Por el contrario, el NAE lleva a cabo una supervisión inteligente directamente en cada switch, para ofrecer a los operadores un análisis distribuido y unos conocimientos de gran utilidad sobre el estado general de la red, sin demoras ni pérdidas de información.

Con el NAE, los operadores pueden establecer reglas de forma proactiva para supervisar tráfico específico de interés, recopilar esos datos y correlacionarlos con los eventos que activan las alertas de servicio... todo ello de manera automatizada. Esto permite que el NAE identifique rápidamente un problema, acelerando el impacto del servicio y el análisis de la causa raíz para acortar el tiempo medio de resolución (MTTR).

COMPONENTES DEL NAE

NAE se ejecuta en el seno del sistema operativo AOS-CX en plataformas compatibles, como la serie de switches Aruba CX 6000 y Aruba CX 8000 (figura 2). Supervisa la configuración de un switch utilizando agentes que extraen esos datos de dos bases de datos claves:

- Base de datos de configuración y estado: Proporciona a los agentes del NAE un acceso total a las estadísticas de red, configuración y estado del protocolo, totalmente visibles a través de las API REST.
- Base de datos de series de tiempo: Contiene datos históricos relevantes correlacionados con cambios en la configuración. Esto proporciona a los operadores la capacidad para captar, archivar y acceder con rapidez al estado de la red en el contexto de un evento de red.

Los agentes del NAE comprueban ciertas condiciones en el switch, sus dispositivos vecinos o en el tráfico que está circulando por la red y, entonces, toman decisiones sobre la base de los resultados de la prueba.

Por ejemplo, un recuento elevado de resultados en una ACL activado por un host desconocido indica un posible fallo de seguridad. En este caso, el NAE podría alertar a los operadores de la existencia de un problema mediante la creación de un mensaje de Syslog o la generación de un informe personalizado con resultados del análisis, al cual se podrá acceder fácilmente a través de una interfaz web.

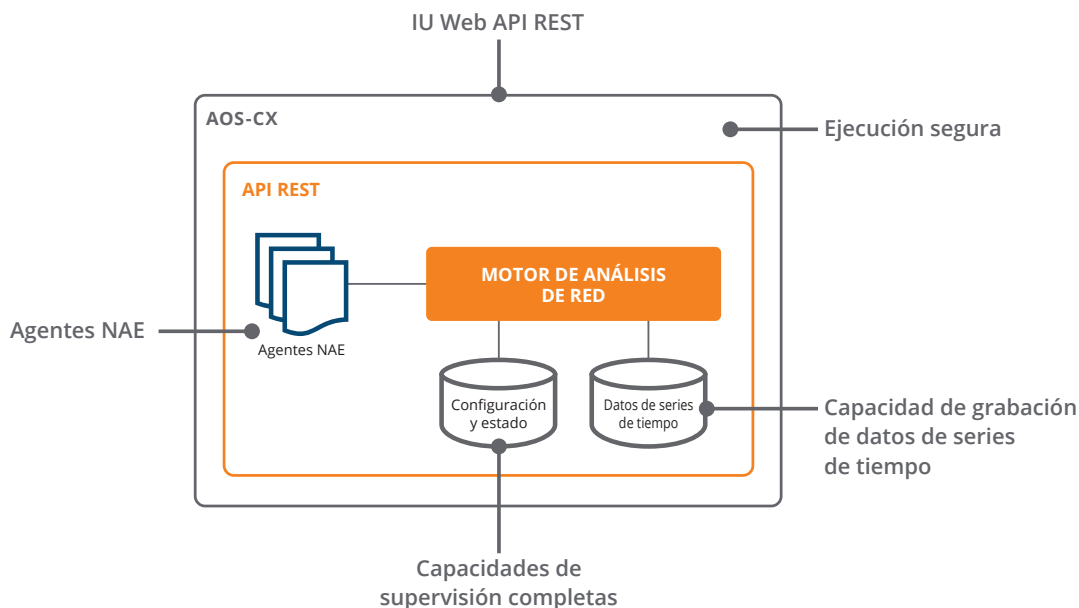


Figura 2: Componentes del NAE



Figura 3: Panel principal del NAE de Aruba

Los operadores también pueden combinar varias acciones en los flujos de trabajo existentes para elaborar diagnósticos o recomendaciones más selectivos. Aquí se incluye la capacidad para enviar notificaciones a los sistemas de gestión del sistema de TI, como ServiceNow, o las herramientas de colaboración, como Slack, cuando ocurre un problema de interés.

Además de proporcionar la capacidad para supervisar el estado de un switch, la IU web también permite que los equipos interconectados visualicen y configuren las alertas, los scripts y los agentes del NAE.

EJEMPLOS DE CASOS DE USO

El NAE asigna problemas de red a sus problemas raíz comunes, acelerando las rutinas de solución de problemas al predeterminar muchos diagnósticos de primer y segundo orden, para que los operadores puedan centrarse en un conjunto de problemas más específico.

A un nivel más amplio, los casos de uso de los agentes del NAE son:

1. Estado del sistema
2. Análisis de red
3. Seguridad
4. Visibilidad de las aplicaciones
5. Optimización de red

Estado del sistema

Las organizaciones precisan conocimientos fiables sobre el estado y el rendimiento de sus switches. Los agentes del NAE relevantes supervisan el estado de los recursos del sistema del plano de control, como el uso de la CPU y la memoria, y realizan un seguimiento a lo largo del tiempo. Cuando los operadores reciben alertas debido a una anomalía, el NAE capta y archiva información detallada del sistema cuando se produce un pico.

Los agentes del estado del sistema también garantizan la disponibilidad de servicios cruciales como TACACS+ u Syslog. Estos agentes llevan a cabo diagnósticos de red o toman otras medidas pertinentes (como notificaciones fuera de banda) si no lo son.

Análisis de red

El NAE puede integrar todas las estadísticas de red disponibles en AOS-CX con la base de datos de series de tiempo para su análisis. El alcance de las capacidades en esta categoría abarca todo desde la supervisión de transceptores en la capa 1 hasta el estado de los homólogos del BGP de la capa 3.

Una amplia gama de casos de uso se deriva de la capacidad de supervisar prácticamente cualquier estadística en el sistema. Estos son algunos ejemplos:

- Estados de los transceptores: Al supervisar los niveles de alimentación de los transceptores TX y RX, el NAE puede detectar varios problemas diferentes con el estado de una conexión. Si los niveles de alimentación cambian de

manera repentina, el NAE compara estos niveles con una línea de base conocida y proporciona directrices de alta probabilidad respecto a lo ocurrido con los enlaces de fibra entre los dos transceptores.

- Estado de la ruta OSPF: Los protocolos de enrutamiento, como OSPF, tienen un gran impacto en el funcionamiento de la red. El NAE proporciona contexto para los cambios en las tablas de OSPF. Por ejemplo, el NAE supervisa los contadores de los avisos de estado de enlace (LSA), para ofrecer información sobre el número de rutas disponibles en el sistema. Una caída repentina en un número de LSA puede significar que un OSPF vecino no está disponible o que ya no suministra un número normal de rutas. Esto suele indicar un problema de accesibilidad y el NAE ofrece información rápida relativa a su origen.

Otros agentes de análisis de red incluyen los monitores de estado para el protocolo de redundancia del enrutador virtual (VRRP), el estado de la agregación de enlaces (LAG) o el protocolo de árbol de expansión (STP), además de los monitores de las estadísticas de interfaz.

Seguridad

El NAE también puede identificar e inspeccionar tráfico errante a través de los switches AOS-CX en las capas de acceso, agregación y de núcleo de la red. Cuando ocurre esto, el NAE puede tomar medidas respecto al tráfico o dirigirlo hacia un dispositivo de seguridad para una inspección detallada.

Por ejemplo, tomemos un sistema HVAC, que solo suele interaccionar con un controlador HVAC. Si el NAE detecta tráfico desde este sistema que interactúa con un repositorio de códigos fuente o un servidor de base de datos, suele tratarse de un dispositivo pirateado. El NAE puede dirigir este tráfico hacia Aruba IntroSpect, una solución de análisis de comportamientos de usuarios y entidades (UEBA), para obtener diagnósticos de punto final completos e intensivos. Tras la pertinente investigación, el administrador podrá ajustar la política que permitió la comunicación no deseada o tomar medidas de cuarentena contra el dispositivo comprometido de forma automática gracias a Aruba ClearPass.

Otros agentes de seguridad incluyen un monitor de cambios de configuración y un monitor de políticas de plano de control (COPP).

Visibilidad de las aplicaciones

El NAE también proporciona visibilidad del tráfico de las aplicaciones, pues atraviesa el núcleo de la red. Aquí se incluye el seguimiento del rendimiento de las aplicaciones en la nube, como Office 365 o Google Suite.

Tras la detección de cualquier anomalía, el agente del NAE lleva a cabo un sólido diagnóstico de red. Por ejemplo, si un proveedor de servicios de internet (ISP) está prestando un servicio deteriorado, el NAE ofrece conocimientos sobre el momento en el que el servicio comenzó a presentar

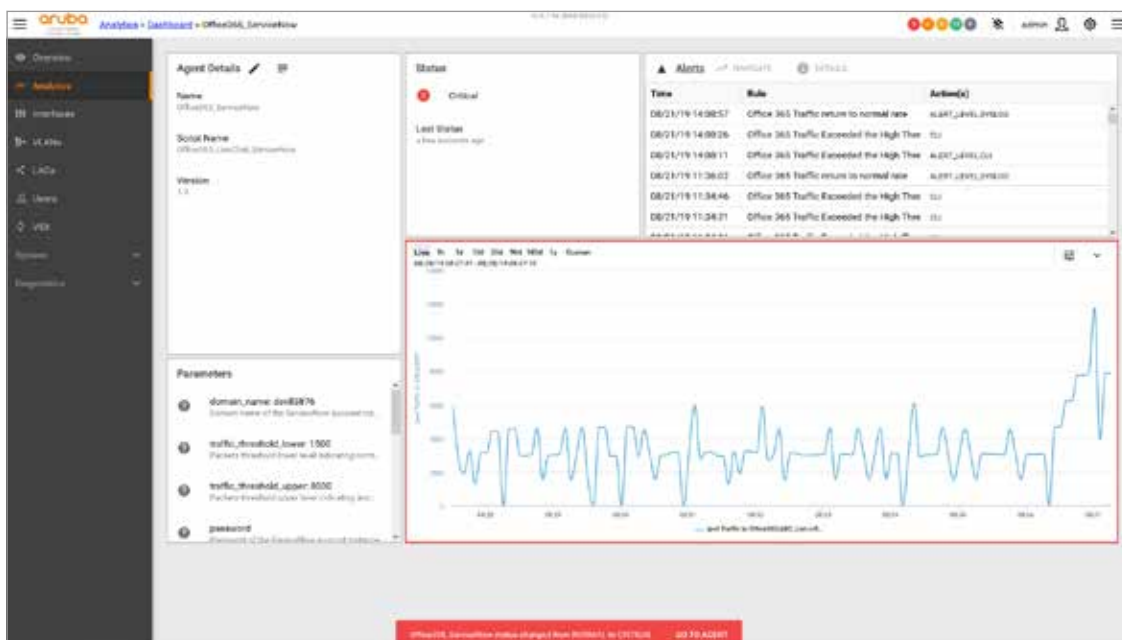


Figura 4: Alerta crítica sobre deterioro de servicio de Office 365

síntomas de deterioro, reduciendo drásticamente el tiempo necesario para aislar y abordar la causa raíz.

Otros agentes de visibilidad de las aplicaciones incluyen el estado de la cola VoIP para supervisar la velocidad de la cola en busca de anomalías, además de las estadísticas de relé DHCP, que supervisa las tasas de consultas y sugiere causas raíz para las faltas de coincidencia.

Optimización de red

Además de acelerar el análisis de las causas raíz, el NAE también puede optimizar los flujos de tráfico por la red. Haciendo un uso provechoso de las estadísticas de rendimiento de las aplicaciones y de uso de la interfaz, el NAE ajusta los pesos de las rutas para dirigir el tráfico de las aplicaciones hacia diferentes enlaces o proveedores. El NAE también puede evitar o corregir desequilibrios de LAG mediante la supervisión de los coeficientes de tráfico y al garantizar que los LAG se encuentren cerca de una utilización cuasi equilibrada. Dichas capacidades garantizan una clase de servicio superior para la empresa y sus usuarios.

INTEGRACIÓN CON NETEDIT PARA MAJOR FACILIDAD DE GESTIÓN

El NAE está perfectamente integrado con NetEdit, la herramienta de configuración y organización de switches de Aruba. NetEdit brinda a los equipos de TI el poder de coordinar con fluidez los despliegues de servicio extremo a extremo, de automatizar cambios rápidos a escala de la red y de garantizar la conformidad con las políticas tras las actualizaciones de red.

Con el análisis integrado de NAE, NetEdit también proporciona a los operadores de red los conocimientos necesarios para supervisar y resolver problemas desde un único panel de control.

Mediante la suscripción al estado del agente del NAE, NetEdit recopila datos cuando se produce un problema de interés y envía una notificación al operador a través de Slack u otra herramienta ITSM. Al hacer clic en NetEdit, el operador

visualiza inmediatamente los servicios y dispositivos afectados, con detalles de diagnóstico completos correlacionados con el momento en que se produce el error.

De este modo, NetEdit y NAE reducen de manera significativa la cantidad de recopilación y correlación de datos manuales que tiene lugar cuando se resuelven problemas a través de medios tradicionales. También genera menos carga en la red, para que el rendimiento no se vea afectado durante el proceso de recopilación de la telemetría.

DESARROLLO DE COMUNIDADES

Para ayudar a los clientes a sacar el máximo partido del NAE, Aruba ha creado una completa biblioteca de agentes y scripts compartidos, que se pone a disposición de los clientes y la comunidad con una licencia de código abierto. Estos están disponibles en Aruba Solutions Exchange y GitHub.

La comunidad Aruba Airheads también promueve el desarrollo mediante crowdsourcing al ofrecer un foro en línea para que los desarrolladores y los ingenieros de red puedan debatir, construir y compartir agentes de NAE para otros casos de uso específicos.

CONCLUSIÓN

Los equipos de TI precisan mayor visibilidad del estado de la red para cumplir los requisitos de resiliencia, rendimiento y agilidad. Con el NAE, los clientes acceden en tiempo real a análisis distribuidos y a escala de la red —y a una biblioteca creciente de scripts que automatizan las tareas de diagnóstico— para acelerar la solución de problemas y mejorar la experiencia del operador de red.

Para acceder a información adicional sobre el NAE y otras soluciones de conmutación, [visita el sitio web de Aruba](#) para acceder a hojas de datos de producto, descripciones técnicas y mucho más.

También puedes ver la biblioteca completa de agentes de NAE disponible para las series de switches Aruba CX 6000 y Aruba CX 8000 en [Aruba Solutions Exchange](#) o [GitHub](#).