aruba
a Hewlett Packard Enterprise company

PRÉSENTATION GÉNÉRALE DE LA SOLUTION

MOTEUR D'ANALYSE DE RÉSEAU ARUBA

Accélération du dépannage et de l'analyse des causes profondes

Les opérateurs de réseau sont confrontés à un certain nombre de défis dans le monde numérique d'aujourd'hui. L'IoT implique l'introduction d'un nombre exponentiels d'appareils qui doivent être intégrés et sécurisés par les équipes informatiques. La mise en place du cloud a généré différents modèles de trafic sur le réseau, et les opérateurs perdent souvent de la visibilité en termes de performances. Enfin, la mobilité de la main-d'œuvre signifie que les employés accèdent à des applications sur plusieurs réseaux, chacun offrant différents niveaux de performance et de sécurité.

Un réseau toujours en service, hautement disponible est aujourd'hui un élément stratégique pour les entreprises. Cependant, cet objectif est plus difficile à atteindre en raison de ces tendances technologiques, qui créent davantage de contrainte et de de points de défaillance sur le réseau.

Les opérateurs réseau ont désormais besoin d'une meilleure visibilité pour traiter rapidement les problèmes au fur et à mesure qu'ils apparaissent. Pour répondre à ce besoin, Aruba a développé le moteur d'analyse de réseau (NAE), qui fait partie du système d'exploitation réseau AOS-CX.

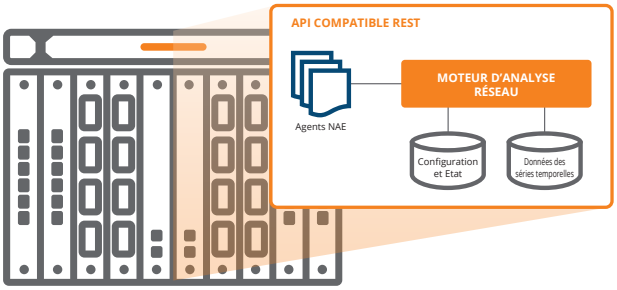
Le NAE fournit un cadre intégré pour la surveillance et le dépannage des réseaux. Il interroge et analyse automatiquement les événements réseau et fournit une visibilité sans précédent sur les interruptions et les anomalies. Grâce à ces informations, les équipes informatiques peuvent détecter les problèmes en temps réel et analyser les tendances afin de prévoir ou même d'éviter les futurs problèmes de sécurité et de performance.

PRINCIPAUX AVANTAGES

- **Visibilité plus complète et rapide :** La base de données intégrée de séries temporelles fournit un historique des événements et des corrélations ainsi qu'un accès en temps réel à des informations à l'échelle du réseau afin d'aider les opérateurs à offrir de meilleures expériences
- **Accélération de la durée moyenne de résolution des problèmes (MTTR) :** Une surveillance en temps réel basée sur des règles et des notifications intelligentes sont automatiquement corrélées aux changements de configuration pour accélérer les routines de diagnostic
- **Administration simplifiée :** Les intégrations avec Aruba NetEdit et des outils tiers tels que ServiceNow et Slack fournissent les caractéristiques intelligentes nécessaires pour intégrer des alertes NAE détailles dans les processus de gestion des services informatiques
- **Innovation continue :** Accès à une bibliothèque en constante évolution de solutions NAE organisées par Aruba et à une communauté d'experts travaillant sur des innovations supplémentaires

DU PROBLÈME À LA CAUSE PROFONDE

Pour rechercher la cause profonde d'un problème de réseau, cela implique généralement de nombreuses tâches disparates. Pour commencer, les opérateurs réseau utilisent une série de commandes d'affichage pour étudier l'état actuel du réseau, ou bien ils effectuent des tests pour essayer de recréer le problème.



Le moteur NAE Aruba offre :

- Des données historiques pertinentes corrélées aux changements de configuration
- Une analyse automatisée des causes profondes et de l'impact sur le service
- Des agents de surveillance intelligents "toujours en service"
- Une télémétrie complète pour tous les systèmes d'information
- Des informations provenant des infrastructures voisines
- Des notifications comprenant des diagnostics automatiques

Figure 1 : Le NAE d'Aruba assure une collecte native des analyses réseau avancées sur le commutateur

Si la technologie de télémétrie est disponible au moment de la survenue du problème, des configurations manuelles combinées à des outils externes sont souvent nécessaires pour effectuer une analyse appropriée. Mais ces pipelines de données sont souvent configurés sans filtres, ce qui entraîne des retards dans le transfert et le traitement des données. Deuxièmement, les outils de surveillance tiers procèdent souvent à un échantillonnage des données, plutôt qu'à une capture des détails complets, ce qui crée des lacunes supplémentaires au niveau de la visibilité.

À l'inverse, le NAE effectue une surveillance intelligente directement sur chaque commutateur. Il fournit ainsi aux opérateurs des analyses distribuées et des informations exploitables sur l'état d'intégrité de l'ensemble du réseau, sans retard ni perte d'informations.

Avec le NAE, les opérateurs peuvent définir de manière proactive des règles de surveillance d'un trafic spécifique d'intérêt, de collecte de ces données et de rapprochement de celles-ci avec des événements qui déclenchent des alertes de service, le tout de manière automatisée. Cela permet au NAE d'explorer rapidement un problème, d'accélérer l'impact du service et l'analyse des causes profondes pour une durée moyenne de résolution des problèmes (MTTR) plus rapide.

COMPOSANTS NAE

Le NAE s'exécute dans le système d'exploitation AOS-CX sur des plates-formes prises en charge telles que la gamme de commutateurs Aruba CX 6000 et Aruba CX 8000 (figure 2). Il surveille la configuration d'un commutateur à l'aide d'agents qui extraient des données de deux bases de données principales :

- Base de données des configurations et des états : Elle fournit aux agents NAE un accès complet à la configuration, à l'état du protocole et aux statistiques réseau, grâce à l'exposition complète fournie par les API REST.
- Base de données des séries temporelles : Elle contient des données historiques pertinentes liées aux changements de configuration. Cela permet aux opérateurs de capturer, d'archiver et d'accéder rapidement à l'état du réseau existant lors d'un événement réseau.

Les agents NAE testent l'état du commutateur, ses appareils voisins ou du trafic qui traverse le réseau, puis prennent des mesures en fonction des résultats du test.

Par exemple, un nombre élevé d'alertes sur une liste ACL déclenchées par un hôte inconnu signale une possible faille de sécurité. Dans ce cas, le NAE peut alerter les opérateurs de la présence de ce problème en créant un message Syslog ou en générant un rapport personnalisé avec les résultats de l'analyse, facilement accessible via une interface web.

Les opérateurs peuvent également combiner plusieurs actions dans des workflows existants pour effectuer des diagnostics ou des recommandations plus sélectifs. Cela inclut la possibilité de transmettre des notifications aux systèmes de gestion des services informatiques, tels que ServiceNow ou aux outils de collaboration tels que Slack en cas de survenue d'un problème d'intérêt.

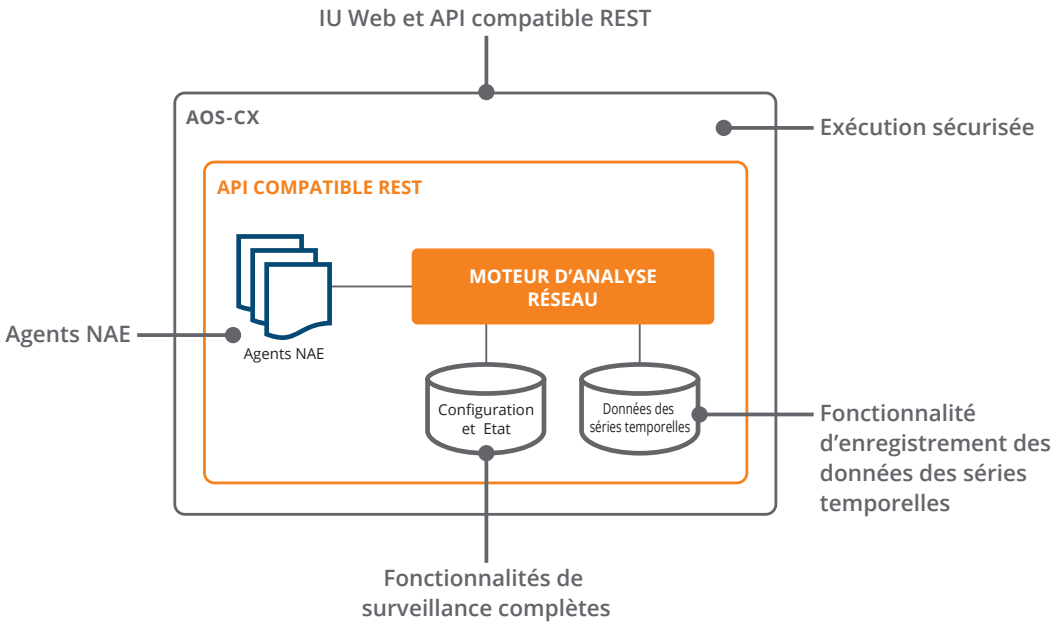


Figure 2 : Les composants NAE

Figure 3 : Le tableau de bord NAE Aruba

Outre la capacité d'une surveillance de l'état d'un commutateur, l'interface Web permet également aux équipes réseau de visualiser et de configurer les agents NAE, les scripts et les alertes.

EXEMPLES DE CAS D'UTILISATION

Le NAE cartographie les problèmes réseau en fonction de leurs causes profondes communes, ce qui accélère les routines de dépannage en prédéterminant de nombreux diagnostics de premier et de second ordre et ce qui permet aux opérateurs de se concentrer sur un ensemble plus ciblé de problèmes.

À un niveau plus large, les cas d'utilisation des agents NAE sont les suivants :

1. État du système
2. Analytique réseau
3. Sécurité
4. Visibilité des applications
5. Optimisation du réseau

État du système

Les organisations ont besoin de renseignements fiables sur l'état et la performance de leurs commutateurs. Les agents NAE concernés surveillent l'état d'intégrité des ressources système du panneau de commande, telles que l'utilisation du processeur et de la mémoire, et en assurent le suivi au fil du temps. Lorsque les opérateurs reçoivent des alertes liées à une anomalie, le NAE capture et archive des informations système détaillées au moment du pic.

Les agents en charge de l'intégrité du système assurent également la disponibilité des services stratégiques tels que TACACS+ et Syslog. Ces agents effectuent des diagnostics réseau ou prennent d'autres mesures appropriées (telles que des notifications hors bande) si nécessaire.

Analytique réseau

Le NAE peut intégrer toutes les statistiques réseau disponibles dans AOS-CX dans la base de données des séries temporelles pour analyse. L'étendue des fonctionnalités de cette catégorie couvre tous les domaines, de la surveillance de l'émetteur-récepteur de couche 1 à l'état d'intégrité de couche 3 des homologues BGP.

Un large éventail de cas d'utilisation se traduit par une possible surveillance de quasiment toutes les statistiques dans le système. Quelques exemples :

- État d'intégrité de l'émetteur-récepteur : En surveillant les niveaux de puissance de l'émetteur-récepteur TX et RX, le NAE peut détecter plusieurs problèmes différents au niveau de l'état d'une connexion. En cas de changement soudain de la puissance, le NAE compare ces niveaux à un référentiel connu et assure un guidage haute probabilité sur les incidents survenus au niveau des liaisons par fibre entre les deux émetteurs-récepteurs.
- État d'intégrité de la route OSPF : Les protocoles de routage tels que le protocole OSPF ont une énorme

influence sur le fonctionnement du réseau. Le NAE fournit le contexte des changements dans les tables OSPF. Par exemple, le NAE assure la surveillance des compteurs LSA (Link State Advertisement, annonce de l'état de la liaison), et fournit des renseignements sur le nombre de routes disponibles dans le système. Une chute soudaine d'un nombre LSA peut signifier qu'un voisin OSPF n'est pas disponible ou ne fournit plus un nombre normal de routes. Cela indique souvent un problème d'accessibilité et le NAE fournit des renseignements rapides sur son origine.

D'autres agents d'analyse de réseau comprennent des dispositifs de surveillance de l'intégrité du protocole VRRP (Virtual Router Redundancy Protocol), de l'intégrité de l'agrégation de liens (LAG) ou le protocole STP (Spanning Tree Protocol) ainsi que des dispositifs de surveillance des statistiques d'interface.

Sécurité

Le NAE peut également identifier et inspecter le trafic erratique circulant à travers les commutateurs AOS-CX au niveau des couches d'accès, d'intégration et de cœur du réseau. Lorsque cela se produit, le NAE peut alors intervenir sur le trafic, ou bien le diriger vers un dispositif de sécurité pour une inspection plus approfondie.

Par exemple, supposez un système CVC, qui généralement interagit uniquement avec un contrôleur CVC. Si le NAE détecte un trafic provenant de ce système et interagissant avec un référentiel de code source ou un serveur de base de données, il s'agit probablement d'un dispositif piraté. Le NAE peut diriger ce trafic vers Aruba IntroSpect, une solution d'analyse UEBA (User and Entity Behavior Analytics), pour des diagnostics complets et approfondis des terminaux. Après examen, l'administrateur peut ajuster la politique qui a autorisé cette communication indésirable, ou mettre automatiquement en place des mesures de quarantaine contre l'appareil corrompu en utilisant Aruba ClearPass.

D'autres agents de sécurité comprennent un dispositif de surveillance des changements de configuration et un dispositif de surveillance COPP (Control Plane Policing).

Visibilité des applications

Le NAE fournit également une visibilité sur le trafic des applications lors de son passage à travers le cœur du réseau. Cela inclut le suivi des performances des applications cloud telles qu'Office 365 ou Google Suite.

Dès la détection de la moindre dégradation, l'agent NAE effectue des diagnostics de réseau robustes. Par exemple, si un Fournisseur d'accès à Internet (FAI) assure un service dégradé, le NAE fournit des renseignements sur le moment où le service a commencé à se dégrader, ce qui réduit considérablement le temps nécessaire pour isoler et résoudre la cause profonde.

D'autres agents de visibilité d'application comprennent

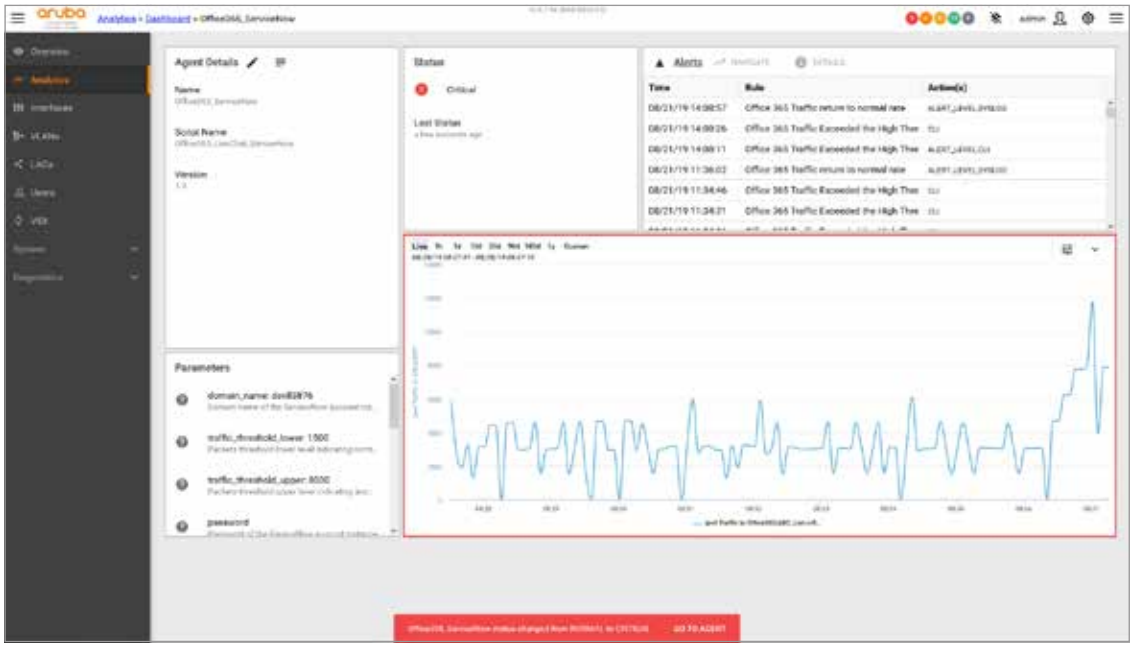


Figure 4 : Alerte critique relative à une dégradation du service d'Office 365

l'intégrité de la file d'attente VoIP afin de surveiller le taux de file d'attente pour les anomalies, ainsi que des statistiques de relais DHCP, afin de surveiller des taux de demandes et de proposer des causes profondes expliquant ces disparités.

Optimisation du réseau

En plus d'accélérer l'analyse des causes profondes, le NAE peut également optimiser les flux de trafic au sein d'un réseau. En tirant parti des statistiques portant sur l'utilisation de l'interface et les performances des applications, le NAE ajuste les pondérations des routes pour diriger le trafic des applications vers d'autres liaisons ou des fournisseurs différents. Le NAE peut également prévenir ou corriger les déséquilibres au niveau de l'agrégation des liens en surveillant les ratios de trafic et en veillant à ce que les agrégations de liens soient utilisées de façon presque égale. De telles fonctionnalités assurent une amélioration de la classe de service pour l'entreprise et ses utilisateurs.

INTÉGRATION AVEC NETEDIT POUR UNE SIMPLICITÉ ACCRUE DE LA GESTION

Le NAE est étroitement intégré à NetEdit, l'outil de configuration et d'orchestration des commutateurs Aruba. NetEdit permet aux équipes informatiques de coordonner de manière flexible les déploiements de service de la périphérie au cloud, d'automatiser les modifications rapides à l'échelle du réseau et d'assurer la conformité des politiques après les mises à jour du réseau.

Grâce aux analyses intégrées de NAE, NetEdit fournit également aux opérateurs réseau des renseignements pour surveiller et résoudre les problèmes à partir d'une console unique.

En s'abonnant au statut de l'agent NAE, NetEdit collecte des données lorsqu'un problème d'intérêt survient et envoie une notification à l'opérateur via Slack ou un autre outil ITSM. En cliquant sur NetEdit, l'opérateur voit immédiatement les appareils et services touchés et dispose de tous les détails de diagnostic liés à l'heure de survenue de l'événement.

De cette manière, NetEdit et NAE réduisent considérablement la quantité de données collectées et corrélées manuellement, qui sont générées lors du dépannage de problèmes via des moyens traditionnels. On obtient également une réduction de la charge sur le réseau, de sorte que les performances ne sont pas affectées par le processus de collecte de la télémétrie.

DÉVELOPPEMENT COMMUNAUTAIRE

Pour aider les clients à tirer pleinement parti du NAE, Aruba a créé une solide bibliothèque d'agents et de scripts partagés, fournis aux clients et à la communauté avec une licence open source. Ceux-ci sont disponibles sur Aruba Solutions Exchange et GitHub.

La communauté Aruba Airheads encourage également le développement par crowdsourcing en fournissant un forum en ligne pour les développeurs et les ingénieurs réseau pour discuter, construire et partager des agents NAE pour d'autres cas d'utilisation personnalisés.

CONCLUSION

Les équipes informatiques ont besoin d'une meilleure visibilité sur l'état d'intégrité du réseau afin de répondre aux exigences de résilience, de performance et d'agilité. Avec le NAE, les clients ont accès en temps réel à des analyses distribuées à l'échelle du réseau, ainsi qu'à une bibliothèque en perpétuelle croissance de scripts qui automatisent les tâches de diagnostic, ce qui permet d'accélérer le dépannage et d'améliorer l'expérience de l'opérateur réseau.

Pour en savoir plus sur le moteur NAE et d'autres solutions de commutation, visitez le site Web d'Aruba pour obtenir des fiches techniques produits, des présentations techniques etc.

Vous pouvez consulter la bibliothèque complète des agents NAE disponibles de la gamme de commutateurs Aruba CX 6000 et Aruba CX 8000 sur Aruba Solutions Exchange ou sur GitHub.

aruba
a Hewlett Packard Enterprise company

SO_NAE_092519 a00059004fre