

PANORAMICA DELLA SOLUZIONE

ARUBA NETWORK ANALYTICS ENGINE

Accelerazione della risoluzione dei problemi e analisi delle cause alla radice

Nel mondo digitale di oggi gli operatori di rete devono affrontare molte sfide. IoT lancia un numero esponenziale di dispositivi che il settore IT deve integrare e garantire. L'adozione della tecnologia Cloud ha creato nella rete differenti modelli di traffico e gli operatori spesso perdono visibilità nelle prestazioni. Infine, la mobilità della forza lavoro significa che i dipendenti possono accedere alle applicazioni attraverso reti multiple, ciascuna caratterizzata da differenti livelli di prestazione e di sicurezza.

Di conseguenza una rete altamente affidabile e sempre disponibile si rivela mission-critical per le aziende di oggi. Tuttavia, queste tendenze della tecnologia rendono questo obiettivo più difficile da raggiungere, poiché creano maggiore stress e punti di guasto sulla rete.

Adesso gli operatori di rete richiedono una migliore visibilità per risolvere immediatamente i problemi che si presentano. Per soddisfare tali esigenze, Aruba ha sviluppato Network Analytics Engine (NAE), che è integrato nel sistema operativo di rete AOS-CX.

NAE fornisce un framework integrato per le reti di monitoraggio e di risoluzione dei problemi. Il sistema interroga e analizza automaticamente gli eventi di rete per fornire una visibilità senza precedenti su interruzioni di servizio e relative anomalie. Grazie a questi insight, il dipartimento IT può individuare i problemi in tempo reale e analizzare le tendenze per prevedere o persino evitare problemi futuri di prestazioni e sicurezza.

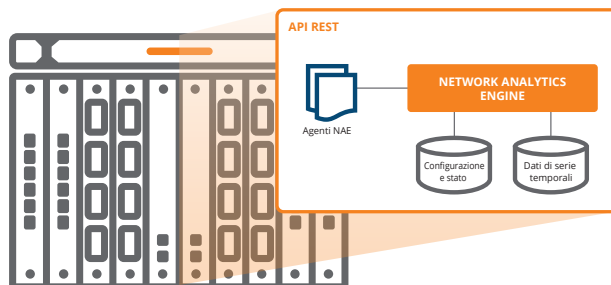


Figura 1: Aruba NAE raccoglie avanzate analisi di rete in modalità nativa sullo switch

VANTAGGI PRINCIPALI

- **più veloce, visibilità completa:** il Database basato su serie temporali (Time Series Database) come elemento integrato fornisce lo storico degli eventi e delle correlazioni e l'accesso in tempo reale agli insight sull'intera rete, per consentire agli operatori di offrire esperienze migliori
- **MTTR rapido:** basato su regole, il monitoraggio in tempo reale e le notifiche intelligenti sono automaticamente correlate alle modifiche di configurazione per consentire di velocizzare le routine diagnostiche
- **gestione semplificata:** le integrazioni con NetEdit di Aruba e strumenti di terze parti come ServiceNow e Slack forniscono l'intelligenza necessaria per integrare segnalazioni NAE avanzate nei processi di IT service management
- **innovazione continua:** accesso a una libreria in costante crescita di soluzioni NAE curate da Aruba e una community di esperti al lavoro su ulteriori innovazioni

DAL PROBLEMA ALLE CAUSE ALLA RADICE

L'individuazione delle cause alla radice di un problema di rete ha richiesto tradizionalmente molte attività disparate tra loro. Per cominciare, gli operatori di rete possono utilizzare una serie di comandi "show" per indagare lo stato corrente della

Aruba NAE offre:

- Dati storici rilevanti in correlazione con le modifiche apportate alla configurazione
- Impatto automatizzato dei servizi e analisi della root cause
- Agenti di monitoraggio intelligente 'always on'
- Telemetria completa per tutte le informazioni di sistema
- Informazioni dall'infrastruttura adiacente
- Notifiche con diagnostiche automatiche

rete oppure possono eseguire i probe per tentare di ricreare il problema.

Se la telemetria è disponibile dal momento in cui il problema si verifica, per condurre analisi adeguate occorrono spesso configurazioni manuali con strumenti esterni. Tuttavia queste pipeline di dati spesso non sono filtrati e creano ritardi nel trasferimento e nell'elaborazione dei dati. Secondariamente, gli strumenti di monitoraggio di terze parti spesso campionano i dati invece di catturare i dettagli completi, creando così ulteriori mancanze di visibilità.

Al contrario, NAE esegue il monitoraggio intelligente direttamente su ciascuno switch, offrendo agli operatori analisi distribuite e insight fruibili sullo stato di salute dell'intera rete, senza ritardi o mancanza di informazioni.

Con NAE gli operatori possono stabilire regole in modo proattivo per monitorare specifici traffici di interesse, raccogliere i relativi dati e metterli in relazione con gli eventi che azionano gli avvisi di servizio: tutto in modo automatico. Ciò consente a NAE di eseguire rapidi drill-down di un problema, velocizzando l'intervento di assistenza e l'analisi delle cause alla radice in vista di tempi medi di risoluzione più rapidi (MTTR).

COMPONENTI NAE

NAE gira funziona all'interno del sistema operativo AOS-CX su piattaforme supportate come gli switch Aruba serie CX 6000 e CX 8000 (figura 2). Esso monitorizza la configurazione di uno switch utilizzando agenti che estraggono i dati da due database principali:

- Database di stato e configurazione: Fornisce agenti NAE con accesso completo a configurazione, stato del protocollo e statistiche di rete: tutto completamente esposto attraverso API REST.
- Database basato su serie temporali (Time Series Database): Contiene dati storici rilevanti in correlazione con le modifiche apportate alla configurazione. Ciò fornisce agli operatori la capacità di catturare, archiviare e accedere rapidamente ai dati sullo stato della rete al momento in cui l'evento si verifica.

Gli agenti NAE verificano le condizioni sullo switch e i dispositivi adiacenti oppure sul traffico in transito attraverso la rete, per eseguire quindi le azioni necessarie in base ai risultati del test.

Ad esempio, un conteggio elevato di risultati su un ACL che è azionato da un host sconosciuto è un'indicazione di possibile violazione della sicurezza. In tale caso, il NAE può segnalare agli operatori il problema attraverso la creazione di un messaggio Syslog oppure generando un report su misura

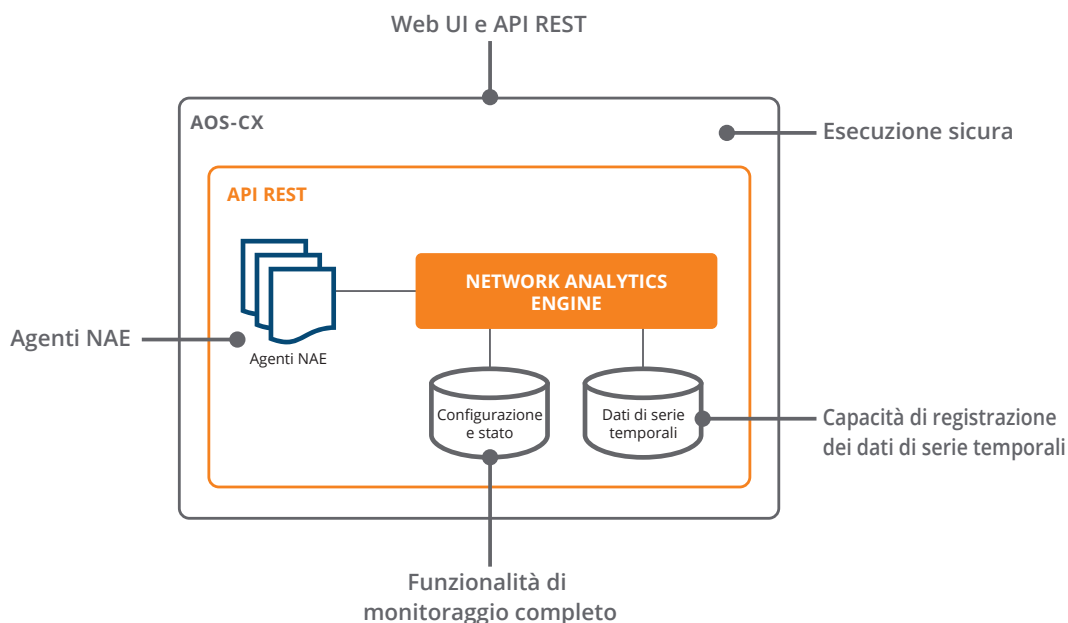


Figura 2: Componenti NAE



Figura 3: Dashboard NAE Aruba

con i risultati dell'analisi, facilmente accessibile attraverso un'interfaccia web.

Gli operatori possono anche riunire tra loro azioni multiple in flussi di lavoro esistenti, per eseguire diagnosi o raccomandazioni più selettive. Ciò include la capacità di inviare notifiche ai sistemi di IT service management come ServiceNow o strumenti di collaborazione come Slack al verificarsi di un problema.

Oltre a fornire la capacità di monitorare lo stato di uno switch, la Web UI consente anche ai team di networking di visualizzare e configurare agenti, script e segnalazioni NAE.

ESEMPI DI CASI D'USO

NAE esegue la mappatura dei problemi di rete fino a individuarne le comuni cause alla radice, accelerando le routine di risoluzione dei problemi grazie alla possibilità di predeterminare molte diagnosi primarie e secondarie in modo che gli operatori possano concentrarsi su una serie di problemi in modo più specifico.

A un livello più ampio, i casi d'uso per gli agenti NAE sono:

1. integrità del sistema
2. analisi di rete
3. sicurezza
4. visibilità delle applicazioni
5. ottimizzazione della rete

Integrità del sistema

Le organizzazioni richiedono una comprensione affidabile dello stato e delle prestazioni dei loro switch. Gli agenti NAE rilevanti monitorano l'integrità delle risorse di sistema del piano di controllo, come CPU e utilizzo della memoria e quindi tracciano queste risorse nel tempo. Quando gli operatori ricevono segnalazioni causate da un'anomalia, il NAE cattura e archivia informazioni dettagliate sul sistema al momento del picco.

Gli agenti di controllo dell'integrità del sistema garantiscono anche la disponibilità di diversi servizi fondamentali come TACACS+ e Syslog. Questi agenti di controllo eseguono diagnostiche di rete oppure altre azioni adeguate (come notifiche fuori banda) nel caso le diagnostiche non lo siano.

Analisi di rete

Il NAE può integrare tutte le statistiche di rete rese disponibili in AOS-CX con il database basato su serie temporali (Time Series Database) per le analisi. L'ampia gamma di funzionalità in questa categoria riguarda ogni aspetto, dal monitoraggio del ricetrasmittitore di Layer 1 all'integrità di Layer 3 dei peer BGP.

Dalla capacità di monitorare quasi ogni statistica sul sistema si sviluppa un'ampia gamma di casi d'uso. Gli esempi comprendono:

- integrità del ricetrasmittitore: Grazie al monitoraggio dei livelli di potenza del ricetrasmittitore TX e RX, il NAE può rilevare numerosi problemi differenti sull'integrità di

un collegamento. Se i livelli di potenza improvvisamente variano, il NAE confronta questi livelli con una baseline nota e fornisce indicazioni di elevata probabilità su ciò che è avvenuto nei collegamenti su fibra ottica tra due ricetrasmittitori.

- integrità del percorso OSPF: protocolli di routing come l'OSPF rivestono una grande importanza nel funzionamento della rete. Il NAE fornisce il contesto in cui sono avvenute le modifiche nelle tabelle OSPF. Ad esempio, il NAE monitora i contatori LSA (link state advertisement) per fornire insight sul numero di percorsi disponibili nel sistema. Un'improvvisa diminuzione del numero di LSA può significare che un elemento OSPF attiguo non è disponibile o non sta più mettendo a disposizione il numero normale di percorsi. Ciò indica spesso un problema di accessibilità e il NAE fornisce un rapido insight sulle sue origini.

Altri agenti nell'analisi di rete comprendono monitor di integrità per Virtual Router Redundancy Protocol (VRRP), LAG (link aggregation) o spanning tree protocol (STP), oltre ad altri monitor delle statistiche di interfaccia.

Sicurezza

Il NAE può anche individuare e ispezionare il traffico in transito attraverso gli switch AOS-CX ai livelli di accesso, aggregazione e nucleo della rete. Quando ciò si verifica, il NAE può intervenire sul traffico oppure dirigerlo verso un

dispositivo di sicurezza per ispezioni dettagliate.

Ad esempio, si consideri un sistema HVAC, che tipicamente interagisce soltanto con un controller HVAC. Se il NAE rileva che il traffico proveniente da questo sistema interagisce con un repository del codice sorgente o con un server database, si tratta probabilmente di un dispositivo hackerato. Il NAE è in grado di dirigere questo traffico verso Aruba IntroSpect, una soluzione UEBA (User and Entity Behavior Analytics) che esegue diagnostiche complete e intensive degli endpoint. Dopo un'indagine, l'amministratore può adeguare la policy che ha consentito la comunicazione indesiderata oppure adottare automaticamente misure di quarantena per il dispositivo compromesso utilizzando Aruba ClearPass.

Altri agenti di sicurezza comprendono un monitor delle modifiche di configurazione e un monitor COPP (Control Plane Policing).

Visibilità delle applicazioni

Il NAE fornisce anche visibilità sul traffico delle applicazioni mentre attraversa il nucleo della rete. Ciò comprende la tracciatura delle prestazioni nelle applicazioni cloud come Office 365 o Google Suite.

Al rilevamento di qualsiasi degrado delle prestazioni, l'agente NAE esegue una robusta diagnostica di network. Ad esempio, se un Internet Service Provider (ISP) sta fornendo un servizio con prestazioni ridotte, il NAE fornisce l'insight sul momento in cui il servizio ha iniziato ad avere problemi,

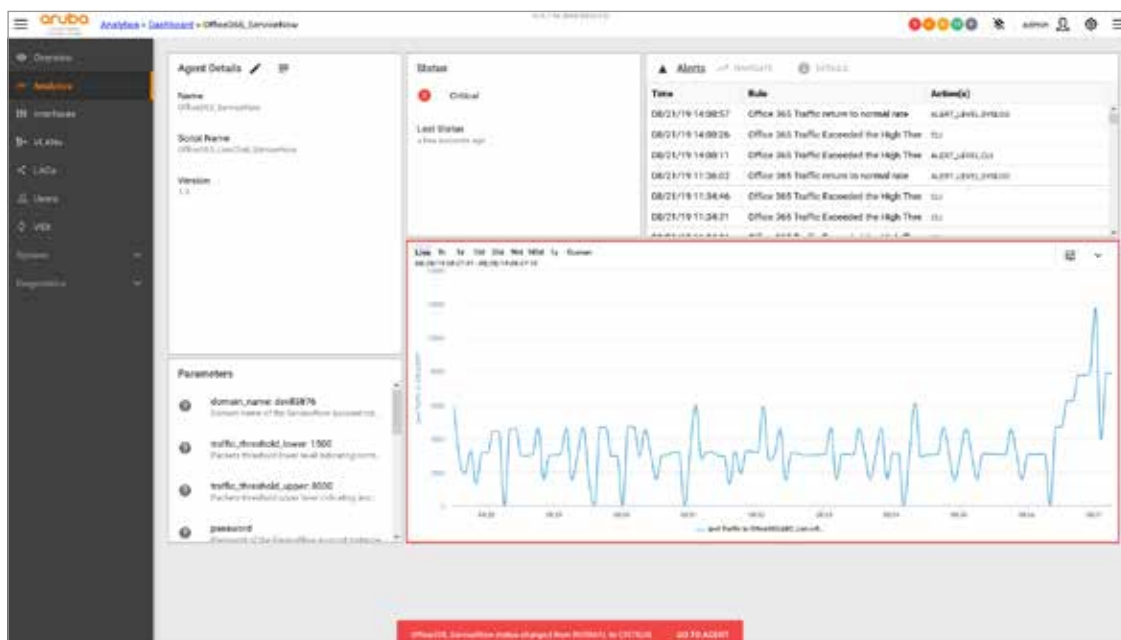


Figura 4: Segnalazione critica sul malfunzionamento del servizio di Office 365

riducendo drasticamente il tempo richiesto per isolare e affrontare la causa alla radice.

Altri agenti di visibilità sulle applicazioni comprendono l'integrità della coda VoIP per monitorare eventuali anomalie nella velocità di smaltimento della coda, oltre a statistiche sul relè DHCP, che si occupa di monitorare la velocità delle richieste e suggerisce cause alla radice del mancato allineamento.

Ottimizzazione della rete

Oltre a velocizzare l'analisi delle cause alla radice, il NAE può anche ottimizzare i flussi di traffico in esecuzione su una rete. Sfruttando le statistiche sull'utilizzo dell'interfaccia e sulle prestazioni applicative, il NAE adatta il peso dei percorsi per dirigere il traffico delle applicazioni su collegamenti diversi oppure verso provider differenti. Il NAE è anche in grado di prevenire o correggere disequilibri LAG monitorando i rapporti di traffico e garantendo che l'utilizzo dei LAG avvenga in condizioni quasi di parità. Tali capacità garantiscono una migliore classe di servizi per l'azienda e i suoi utenti.

INTEGRAZIONE CON NETEDIT PER MAGGIORE SEMPLICITÀ DI GESTIONE

Il NAE è strettamente integrato con NetEdit, lo strumento di Aruba per la configurazione e l'orchestrazione degli switch. NetEdit fornisce ai team IT la capacità di coordinare in modo regolare le esecuzioni dei servizi end-to-end, automatizzare in modo rapido le modifiche sull'intera rete e garantire la conformità alla policy dopo gli aggiornamenti di rete.

Grazie alle analisi integrate del NAE, NetEdit offre agli operatori di rete anche gli insight per monitorare e risolvere i problemi da una sola console.

Attraverso l'iscrizione allo stato dell'agente NAE, NetEdit raccoglie i dati correnti al verificarsi del problema e invia la corrispondente notifica all'operatore attraverso Slack o un altro strumento ITSM. Se si fa click su NetEdit, l'operatore rileva immediatamente i dispositivi e i servizi interessati

dal problema, con i dettagli di diagnosi completi e relativi al momento in cui l'evento si è verificato.

In tal modo, NetEdit e NAE riducono significativamente la raccolta e la correlazione di dati da eseguire manualmente durante la risoluzione dei problemi con i mezzi tradizionali. Inoltre si verifica meno carico sulla rete, così le prestazioni non risentono durante il processo di raccolta della telemetria.

SVILUPPO DI COMMUNITY

Per consentire ai clienti di trarre un vantaggio completo da NAE, Aruba ha creato una robusta libreria di agenti e script da condividere, a disposizione di clienti e community con licenza open source. La libreria è disponibile sia su Aruba Solutions Exchange che su GitHub.

La Airheads community di Aruba promuove anche lo sviluppo in crowdsourcing attraverso un forum online per sviluppatori e ingegneri di rete per discutere, creare e condividere agenti NAE per altro casi d'uso personalizzati.

CONCLUSIONE

I team IT necessitano di maggiore visibilità sull'integrità della rete, per poter soddisfare i requisiti di resilienza, prestazioni e agilità. Con NAE, i clienti hanno accesso in tempo reale alle analisi distribuite sull'intera rete — insieme a una libreria di script in costante crescita che automatizza le attività diagnostiche — per velocizzare la risoluzione dei problemi e potenziare l'esperienza degli operatori di rete.

Per sapere di più su NAE e altre soluzioni di switching, [visitate il sito web di Aruba](#) per consultare le schede tecniche dei prodotti, le caratteristiche tecniche e altro ancora.

È anche possibile visualizzare la libreria completa di agenti NAE disponibile sugli switch Aruba serie CX 6000 e serie CX 8000 su [Aruba Solutions Exchange](#) o su [GitHub](#).