AnyConnect versione 4.0 e NAC Posture Agent non vengono visualizzati nella Guida alla risoluzione dei problemi ISE

Sommario

Introduzione

Identity Services Engine (ISE) fornisce funzionalità di postura che richiedono l'uso dell'agente NAC (Network Admission Control) (per Microsoft Windows, Macintosh o tramite webagent) o di AnyConnect versione 4.0. Il modulo di postura ISE di AnyConnect versione 4.0 funziona esattamente come l'agente NAC e nel presente documento viene quindi chiamato agente NAC. Il sintomo più comune di errore di postura per un client è che l'agente NAC non viene visualizzato poiché uno scenario di lavoro causa sempre la visualizzazione della finestra dell'agente NAC e l'analisi del PC. Questo documento aiuta a limitare le molte cause che possono portare la postura a fallire, il che significa che l'agente NAC non compare. Non deve essere esaustivo in quanto i registri degli agenti NAC possono essere decodificati solo dal Cisco Technical Assistance Center (TAC) e le possibili cause principali sono numerose; tuttavia ha lo scopo di chiarire la situazione e di individuare il problema più lontano che semplicemente "l'agente non viene fuori con l'analisi della postura" e probabilmente aiuterà a risolvere le cause più comuni.

Prerequisiti

Requisiti

Gli scenari, i sintomi e i passaggi elencati in questo documento consentono di risolvere i problemi

al termine dell'installazione iniziale. Per la configurazione iniziale, fare riferimento a Posture Services nella Guida alla configurazione di Cisco ISE all'indirizzo Cisco.com.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ISE versione 1.2.x
- NAC Agent per ISE versione 4.9.x
- AnyConnect versione 4.0

Nota: Le informazioni devono essere valide anche per altre versioni di ISE, a meno che le note non indichino cambiamenti di comportamento importanti.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Metodologia di risoluzione dei problemi

Cosa fa saltare fuori l'agente?

L'agente viene visualizzato quando rileva un nodo ISE. Se l'agente rileva di non avere accesso completo alla rete e si trova in uno scenario di reindirizzamento della postura, cerca costantemente un nodo ISE.

Èdisponibile un documento Cisco.com in cui vengono illustrati i dettagli del processo di individuazione dell'agente: Processo di individuazione dell'agente NAC (Network Admission Control) per Identity Services Engine. Per evitare la duplicazione dei contenuti, questo documento tratta solo il punto chiave.

Quando un client si connette, viene sottoposto a un'autenticazione RADIUS (filtro MAC o 802.1x) alla fine della quale, ISE restituisce l'elenco di controllo di accesso (ACL) di reindirizzamento e l'URL di reindirizzamento al dispositivo di rete (switch, appliance di sicurezza adattiva (ASA) o controller wireless) in modo da limitare il traffico del client e consentirgli di ottenere solo un indirizzo IP e risoluzioni DNS (Domain Name Server). Tutto il traffico HTTP(S) proveniente dal client viene reindirizzato a un URL univoco su ISE che termina con CPP (Client Posture and Provisioning), ad eccezione del traffico destinato al portale ISE stesso. L'agente NAC invia un normale pacchetto HTTP GET al gateway predefinito. Se l'agente non riceve risposte o non riceve risposte diverse dal reindirizzamento della CPP, considera di avere una connettività completa e non procede con la postura. Se riceve una risposta HTTP che è un reindirizzamento a un URL CPP alla fine di un nodo ISE specifico, continua il processo di postura e contatta il nodo ISE. Viene visualizzato e inizia l'analisi solo quando riceve correttamente i dettagli della postura da quel nodo ISE.

L'agente NAC raggiunge anche l'indirizzo IP dell'host di rilevamento configurato (non si prevede che ne venga configurato più di uno). Prevede di essere reindirizzato anche lì per ottenere l'URL di reindirizzamento con l'ID sessione. Se l'indirizzo IP di rilevamento è un nodo ISE, non viene eseguito perché attende di essere reindirizzato per ottenere l'ID sessione corretto. Pertanto, l'host

di rilevamento in genere non è necessario, ma può essere utile quando impostato come qualsiasi indirizzo IP nell'intervallo dell'ACL di reindirizzamento per attivare un reindirizzamento (ad esempio, in scenari VPN).

Possibili cause

Il reindirizzamento non viene eseguito

Questa è di gran lunga la causa più comune. Per convalidare o invalidare, apri un browser sul PC dove l'agente non compare e vedi se sei reindirizzato alla pagina di download dell'agente di postura quando digiti un URL. È inoltre possibile digitare un indirizzo IP casuale, ad esempio http://1.2.3.4, per evitare possibili problemi DNS. Se un indirizzo IP viene reindirizzato ma il nome di un sito Web non viene reindirizzato, è possibile controllare il DNS.

Se il reindirizzamento viene eseguito, è necessario raccogliere i log dell'agente e il bundle di supporto ISE (con il modulo di postura e svizzero in modalità debug) e contattare Cisco TAC. Ciò indica che l'agente rileva un nodo ISE ma qualcosa si guasta durante il processo per ottenere i dati di postura.

Se non si verifica alcun reindirizzamento, si ha la prima causa che richiede ulteriori indagini sulla causa principale. Per iniziare, occorre controllare la configurazione sul dispositivo di accesso alla rete (Wireless LAN Controller (WLC) o sullo switch) e passare alla voce successiva di questo documento.

Attributi non installati nel dispositivo di rete

Questo problema è una sottocartella dello scenario **Redirection Does Not Happen**. Se il reindirizzamento non viene eseguito, la prima cosa da verificare (poiché il problema si verifica su un determinato client) è che il client sia posizionato correttamente dallo switch o dal livello di accesso wireless.

Di seguito è riportato un esempio di output del comando **show access-session interface <interface number> detail** (su alcune piattaforme potrebbe essere necessario aggiungere **alcuni dettagli**) eseguito sullo switch a cui è connesso il client. È necessario verificare che lo stato sia "Autorizzazione riuscita", che l'ACL di reindirizzamento dell'URL punti correttamente all'ACL di reindirizzamento desiderato e che il reindirizzamento dell'URL punti al nodo ISE previsto con **CPP** alla fine dell'URL. Il campo ACS ACL non è obbligatorio perché visualizza solo se è stato configurato un elenco degli accessi scaricabile nel profilo di autorizzazione su ISE. Tuttavia, è importante esaminarlo e verificare che non ci siano conflitti con l'ACL di reindirizzamento (vedere i documenti sulla configurazione della postura in caso di dubbio).

```
01-SW3750-access#show access-sess gi1/0/12 det
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
```

```
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cpp
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

Per risolvere i problemi di un WLC con AireOS, immettere **show wireless client detail <mac address>** e **show wireless client mac-address <mac address> detail** per risolvere i problemi di un WLC con Cisco IOS-XE. Vengono visualizzati dati simili ed è necessario verificare l'URL di reindirizzamento e l'ACL e se il client si trova nello stato "POSTURE_REQD" o simile (varia a seconda della versione del software).

Se gli attributi non sono presenti, è necessario aprire i dettagli di autenticazione nell'ISE del client in fase di risoluzione dei problemi (passare a **Operazioni > Autenticazioni**) e verificare nella sezione Risultati che gli attributi di reindirizzamento siano stati inviati. Se non sono stati inviati, è necessario esaminare i criteri di autorizzazione per comprendere il motivo per cui gli attributi non sono stati restituiti per questo particolare client. È probabile che una delle condizioni non corrisponda, quindi è consigliabile risolverla singolarmente.

Tenere presente che, per quanto riguarda l'ACL di reindirizzamento, Cisco IOS® reindirizza le istruzioni di autorizzazione (quindi gli indirizzi IP ISE e DNS devono essere rifiutati) mentre AireOS sul WLC reindirizza le istruzioni di negazione (quindi è consentito per ISE e DNS).

Gli attributi sono presenti ma il dispositivo di rete non reindirizza

La causa principale è un problema di configurazione. Esaminare la configurazione del dispositivo di rete in base alla guida alla configurazione e agli esempi di configurazione disponibili su Cisco.com. In questo caso, il problema in genere si verifica in tutte le porte o i punti di accesso (AP) del dispositivo di rete. In caso contrario, il problema potrebbe verificarsi solo su alcune porte switch o su alcuni access point. In questo caso, confrontare la configurazione di quelli in cui si è verificato il problema con le porte o i punti di accesso in cui la postura funziona correttamente.

I punti di accesso FlexConnect sono sensibili perché possono avere ciascuno una configurazione univoca ed è facile commettere un errore in un ACL o in una VLAN in alcuni punti di accesso e non in altri.

Un altro problema comune è che la VLAN del client non ha una SVI. Ciò si applica solo agli switch e viene descritto in dettaglio in ISE Traffic Redirection sugli switch Catalyst serie 3750. Dal punto di vista degli attributi, tutto può risultare bello.

Interferenza con DACL (Downloadable Access-list)

Se, contemporaneamente agli attributi di reindirizzamento, si spinge nuovamente un DACL sullo switch (o Airespace-ACL per un controller wireless), il reindirizzamento potrebbe essere bloccato.

L'elenco DACL viene applicato per primo e determina cosa viene completamente eliminato e cosa viene elaborato. Quindi, viene applicato l'ACL di reindirizzamento e determina cosa viene reindirizzato.

Ciò significa che, nella maggior parte dei casi, si desidera autorizzare tutto il traffico HTTP e HTTPS nel DACL. Se lo si blocca, non verrà reindirizzato poiché verrà eliminato prima di tale operazione. Non rappresenta un problema di sicurezza, in quanto il traffico verrà reindirizzato principalmente sull'ACL di reindirizzamento dopo il reindirizzamento, quindi non è realmente consentito sulla rete; tuttavia, è necessario autorizzare questi due tipi di traffico nell'elenco DACL in modo che possano individuare l'ACL di reindirizzamento subito dopo.

Versione agente NAC non valida

Èfacile dimenticare che le versioni degli agenti NAC sono convalidate rispetto alle versioni specifiche di ISE. Molti amministratori aggiornano il proprio cluster ISE e dimenticano di caricare la versione dell'agente NAC correlata nel database dei risultati del provisioning client.

Se si utilizza una versione non aggiornata dell'agente NAC per il codice ISE, tenere presente che potrebbe funzionare, ma potrebbe anche non funzionare. Non sorprende quindi che alcuni clienti lavorino e altri no. Per verificare, visitare la sezione Cisco.com download della versione ISE e verificare quali versioni dell'agente NAC sono disponibili. In genere, per ciascuna versione ISE sono supportate diverse versioni. In questa pagina Web vengono raccolte tutte le matrici: Informazioni sulla compatibilità con Cisco ISE.

Proxy Web HTTP in uso dai client

Il concetto di proxy Web HTTP è che i client non risolvono gli indirizzi IP DNS dei siti Web né contattano direttamente i siti Web; ma semplicemente al server proxy, che si occupa della gestione della richiesta. Il problema tipico di una configurazione comune è che il client risolve un sito Web (ad esempio www.cisco.com) inviando direttamente il comando HTTP GET per il proxy, che viene intercettato e correttamente reindirizzato al portale ISE. Tuttavia, invece di inviare il successivo HTTP GET all'indirizzo IP del portale ISE, il client continua a inviare la richiesta al proxy.

Nel caso in cui si decida di non reindirizzare il traffico HTTP destinato al proxy, gli utenti hanno accesso diretto all'intero Internet (poiché tutto il traffico passa attraverso il proxy) senza autenticazione o postura. La soluzione è modificare le impostazioni del browser dei client e aggiungere un'eccezione per l'indirizzo IP ISE nelle impostazioni del proxy. In questo modo, quando il client deve raggiungere l'ISE, invia la richiesta direttamente all'ISE e non al proxy. In questo modo si evita il loop infinito in cui il client viene costantemente reindirizzato ma non viene mai visualizzata la pagina di accesso.

Notare che l'agente NAC non è influenzato dalle impostazioni proxy immesse nel sistema e continua a funzionare normalmente. Ciò significa che se si utilizza un proxy Web, non è possibile avere sia il rilevamento agente NAC funzionante (in quanto utilizza la porta 80) sia l'installazione automatica dell'agente da parte degli utenti una volta reindirizzati alla pagina della postura durante la navigazione (in quanto utilizza la porta proxy e gli switch tipici non possono reindirizzare su più porte).

Gli host di individuazione sono configurati nell'agente NAC

Soprattutto dopo ISE versione 1.2, si consiglia di non configurare alcun host di rilevamento sull'agente NAC a meno che non si abbia esperienza sulle sue funzioni e sulle sue operazioni. L'agente NAC deve individuare il nodo ISE che ha autenticato il dispositivo client tramite il rilevamento HTTP. Se ci si affida agli host di rilevamento, è possibile che l'agente NAC contatti un nodo ISE diverso da quello che ha autenticato il dispositivo e che non funzioni. ISE versione 1.2 rifiuta un agente che individua il nodo attraverso il processo di individuazione host perché desidera che l'agente NAC ottenga l'ID sessione dall'URL di reindirizzamento, pertanto questo metodo è sconsigliato.

In alcuni casi, è possibile configurare un host di individuazione. Quindi deve essere configurato con qualsiasi indirizzo IP (anche se non esistente) che verrà reindirizzato dall'ACL di reindirizzamento e idealmente non deve trovarsi nella stessa subnet del client (in caso contrario, il client eseguirà l'ARP indefinitamente per tale indirizzo e non invierà mai il pacchetto di rilevamento HTTP).

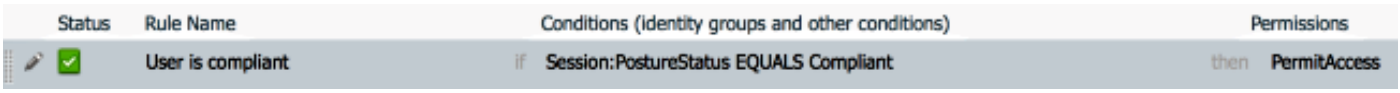
L'agente NAC non viene visualizzato a volte

Quando il problema è più intermittente e azioni quali lo scollegamento/ricollegamento del cavo o la connettività wifi lo rendono possibile, è un problema più sottile. Potrebbe trattarsi di un problema con gli ID sessione RADIUS in cui l'ID sessione viene eliminato sull'ISE dall'accounting RADIUS (disabilitare l'accounting per verificare se viene modificato qualcosa).

Se si usa ISE versione 1.2, è possibile anche che il client invii molti pacchetti HTTP in modo che nessuno provenga da un browser o dall'agente NAC. ISE versione 1.2 analizza il campo user-agent nei pacchetti HTTP per vedere se proviene dall'agente NAC o da un browser, ma molte altre applicazioni inviano il traffico HTTP con un campo user-agent e non menzionano alcun sistema operativo o informazioni utili. ISE versione 1.2 invia quindi una modifica di autorizzazione per disconnettere il client. ISE versione 1.3 non è interessata dal problema, in quanto funziona in modo diverso. La soluzione è aggiornare alla versione 1.3 o consentire a tutte le applicazioni rilevate nell'ACL di reindirizzamento in modo che non vengano reindirizzate all'ISE.

Problema inverso: L'agente viene riattivato ripetutamente

Il problema opposto può sorgere quando l'agente compare, esegue l'analisi della postura, convalida il client e poi riappare poco dopo invece di consentire la connettività di rete e rimanere in silenzio. Questo accade perché, anche dopo una postura corretta, il traffico HTTP viene ancora reindirizzato al portale CPP su ISE. È quindi consigliabile analizzare la policy di autorizzazione ISE e verificare di disporre di una regola che invii un'autorizzazione di accesso (o una regola simile con possibili ACL e VLAN) quando vede un client conforme e NON un nuovo reindirizzamento CPP.



Informazioni correlate

- Servizi di postura nella guida alla configurazione di Cisco ISE
- Processo di rilevamento agente NAC per ISE
- ISE Traffic Redirection sugli switch Catalyst serie 3750
- Documentazione e supporto tecnico – Cisco Systems