AnyConnect versie 4.0 en NAC Posture Agent verschijnt niet op ISE Troubleshooter

Inhoud

Inleiding

Identity Services Engine (ISE) biedt mogelijkheden voor het stellen van de functies waarvoor het gebruik van de Network Admission Control (NAC)-agent (voor Microsoft Windows, Macintosh of via een webagent) of AnyConnect versie 4.0 vereist is. De AnyConnect versie 4.0 ISE-postmodule werkt precies zoals de NAC-agent en wordt daarom in dit document de NAC-agent genoemd. Het meest voorkomende symptoom van een postuur-falen voor een client is dat de NAC-agent niet naar boven komt omdat een werkscenario er altijd voor zorgt dat het NAC-agensvenster verschijnt en uw PC analyseert. Dit document helpt u de vele oorzaken te verminderen die de houding kunnen leiden tot mislukken, wat betekent dat de NAC-agent niet opduikt. Het is niet bedoeld om volledig te zijn, omdat de logbestanden van de NAC-agents alleen kunnen worden gedecodeerd door het Cisco Technical Assistance Center (TAC) en de mogelijke oorzaken van de problemen zijn talrijk; het wil echter de situatie verduidelijken en het probleem verder uitlijnen dan " de agent komt niet naar voren met de postertieanalyse " en zal u waarschijnlijk helpen de meest voorkomende oorzaken op te lossen .

Voorwaarden

Vereisten

De scenario's, symptomen en stappen in dit document worden geschreven zodat u problemen met de oplossing kunt oplossen nadat de eerste instellingen al zijn voltooid. Raadpleeg voor de eerste

configuratie de Postservices van Cisco ISE Configuration Guide op Cisco.com.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ISE versie 1.2.x
- NAC Agent voor ISE versie 4.9.x
- AnyConnect versie 4.0

  Opmerking: De informatie dient ook van toepassing te zijn op andere releases van ISE, tenzij de vrijgavekeningen duiden op belangrijke gedragsveranderingen.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Methode voor probleemoplossing

Waarom komt de agent naar boven?

De agent verschijnt wanneer hij een ISE-knooppunt ontdekt. Als de agent opmerkt dat het geen volledige netwerktoegang heeft en in een houding omrichtingsscenario is, zoekt het constant een ISE knooppunt.

Er is een Cisco.com-document dat de details van het proces voor het opsporen van de agent verklaart: Agent-detectieproces (Network Admission Control) voor Identity Services Engine. Om overlapping van content te voorkomen, wordt in dit document alleen het kernpunt besproken.

Wanneer een client verbinding maakt, wordt er een RADIUS-verificatie (MAC-filtering of 802.1x) uitgevoerd aan het einde waarvan ISE de toegangscontrolelijst (ACL) en de URL-omleiding naar het netwerkapparaat (switch, adaptieve security applicatie (ASA) of draadloze controller) retourneert om het clientverkeer alleen te beperken zodat deze een IP-adres en DNS-resoluties (Domain Name Server) kan verkrijgen. Alle HTTP(S)-verkeer dat van de client komt, wordt opnieuw gericht naar een unieke URL op ISE die eindigt met CPP (Client Posture and Provisioning), behalve verkeer dat bestemd is voor het ISE-portal zelf. De NAC agent stuurt een regelmatig HTTP pakket naar de standaardgateway. Als de agent geen antwoord of een ander antwoord dan een CPP-omleiding ontvangt, is hij van mening dat hij volledige connectiviteit heeft en gaat hij niet verder met posteren. Als er een HTTP-respons wordt ontvangen die een omleiding naar een CPP-URL aan het einde van een specifiek ISE-knooppunt is, dan gaat dit het postproces en de contacten die ISE-knooppunt kennen voort. Het komt slechts op en begint de analyse wanneer het met succes de postdetails van dat ISE knooppunt ontvangt.

De NAC-agent bereikt ook het geconfigureerde IP-adres van de zoekhost (er wordt niet meer dan één verwacht dat het wordt geconfigureerd). Hij verwacht daar ook omgeleid te worden om de omleiding van URL met de sessie-ID te krijgen. Als het IP-adres van discovery is een ISE-knooppunt, dan heeft dit niet de bedoeling omdat het erop wacht om opnieuw te worden gericht om de juiste sessie-ID te krijgen. Dus is de discovery host gewoonlijk niet nodig, maar kan handig zijn wanneer deze is ingesteld als een IP-adres in het bereik van de opnieuw directie ACL om een omleiding te activeren (zoals in VPN-scenario's bijvoorbeeld).

Mogelijke oorzaken

Er is geen omleiding

Dit is veruit de meest voorkomende zaak. Om te valideren of ongeldig te maken, opent u een browser op de PC waar de agent niet verschijnt en ziet u of u opnieuw wordt gericht naar de downloadpagina van de postbeambte wanneer u een URL typt. U kunt ook een willekeurig IP-adres, zoals http://1.2.3.4, typen om een mogelijke DNS-kwestie te voorkomen (als een IP-adres opnieuw wordt gericht maar een website-naam niet, kunt u DNS-instellingen bekijken).

Als u herleiding krijgt, moet u de agent loggen en de ISE-ondersteuningsbundel verzamelen (met de houding en zwitserse module om de modus te reinigen) en contact opnemen met Cisco TAC. Dit geeft aan dat de agent een ISE-knooppunt ontdekt, maar dat er tijdens het proces iets niet in staat is om de postgegevens te verkrijgen.

Als er geen omleiding gebeurt, heb je je eerste doel, dat nog steeds nader onderzoek van de oorzaak vereist. Een goed begin is om de configuratie op het apparaat voor netwerktoegang (Wireless LAN Controller) of -schakelaar te controleren en naar het volgende item in dit document te verplaatsen.

De kenmerken worden niet op het netwerkapparaat geïnstalleerd

Dit is een subgeval van het scenario van de omleiding. Als de omleiding niet gebeurt, is het eerste ding om te verifiëren (zoals het probleem op een bepaalde client voorkomt) dat de client correct in de juiste status geplaatst wordt door de switch of draadloze toegangslaag.

Hier is voorbeelduitvoer van de **show access-sessie interface <interface number> detail** opdracht (u kunt **details** aan het eind op sommige platforms **moeten toevoegen**) genomen op de switch waar de client is aangesloten. U moet verifiëren dat de status "Auteur succes" is, dat de URL ACL correct omricht naar de bedoelde omleiding ACL, en dat de URL naar het verwachte ISE-knooppunt wijst met **CPP** aan het eind van de URL. Het veld ACS ACL is niet verplicht, omdat het alleen toont dat u een downloadbare toegangslijst in het autorisatieprofiel op ISE hebt ingesteld. Het is echter belangrijk om ernaar te kijken en te controleren of er geen conflict is met de omleiding van ACL (zie documenten over de configuratie van de houding in geval van twijfel).

```
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
```

Als u een WLC-oplossing wilt problemen oplossen die AireOS uitvoert, **toont u** het **draadloze adres <mac-adres>**en voert u **Wireless client-mac-adres <mac-adres> in** om een WLC-oplossing te vinden die Cisco IOS-XE uitvoert. Gelijkaardige datadisplays en u moet de URL en ACL opnieuw sturen en als de client in "POSTURE_REQD" staat of vergelijkbaar is (deze varieert afhankelijk van de softwareversie).

Als eigenschappen niet aanwezig zijn, moet u de authenticatiedetails in ISE van de client openen die u oplossen was (navigeer naar **Operations > Authenticaties**) en in de sectie Resultaat controleren dat de omrichtingseigenschappen werden verzonden. Indien ze niet werden verstuurd, dient u het vergunningsbeleid te herzien om te begrijpen waarom de eigenschappen voor deze specifieke cliënt niet werden teruggegeven. Waarschijnlijk kwam één van de voorwaarden niet overeen, dus het is een goed idee om hen één voor één in de problemen te brengen.

Onthoud dat, wat betreft het doorsturen van ACL, Cisco IOS® omleidingen op vergunningsverklaringen (zodat de ISE en DNS IP adressen moeten worden ontkend) terwijl AireOS op de WLC op ontkenningsverklaringen (dus is het toegestaan voor ISE en DNS).

Eigenschappen zijn op zijn plaats maar het netwerkapparaat richt zich niet op

De belangrijkste oorzaak in dit geval is een configuratieprobleem. U dient de configuratie van het netwerkapparaat te bekijken aan de hand van de configuratiehandleiding en configuratievoorbeelden op Cisco.com. Als dit het geval is, bestaat het probleem gewoonlijk door alle poorten of toegangspunten (APs) van het netwerkapparaat. Als dit niet het geval is, kan het probleem zich alleen voordoen bij sommige luchthavens of AP's. Als dit het geval is, zou u de configuratie van die moeten vergelijken waar het probleem zich voordoet vergeleken met de havens of APs waar de houding prima werkt.

FlexConnect APs zijn gevoelig omdat zij elk een unieke configuratie kunnen hebben en het gemakkelijk is om een fout in ACL of een VLAN in sommige APs en niet anderen te maken.

Een ander algemeen probleem is dat de client-VLAN geen SVI heeft. Dit is alleen van toepassing op switches en wordt in detail besproken in ISE Traffic ReRichting op Catalyst 3750 Series switch. Alles kan er goed uitzien vanuit het oogpunt van de eigenschappen.

Interveniënt Downloadable Access-List (DACL)

Als u, op het zelfde moment als omleidingseigenschappen, een DACL terug naar de schakelaar (of Airespace-ACL voor een draadloze controller) duw, dan zou het uw omleiding kunnen blokkeren. DACL wordt eerst toegepast en bepaalt wat volledig wordt ingetrokken en wat er verder wordt verwerkt. Vervolgens wordt ACL-richting (ombuigen) toegepast en bepaalt wat opnieuw wordt gericht.

Wat dit concreet betekent is dat je meestal al HTTP- en HTTPS-verkeer in je DACL's wilt toestaan. Als je het blokkeert, wordt het niet opnieuw gericht, want het wordt eerder laten vallen. Het gaat niet om de veiligheid, want dat verkeer zal vooral worden omgeleid naar de achteruitrijdende ACL,

zodat het niet echt op het netwerk is toegestaan; echter, moet u deze twee types van verkeer in de DACL toestaan om hen een kans te hebben om ACL onmiddellijk na te leiden.

Bad NAC Agent versie

Het is makkelijk om te vergeten dat specifieke NAC-agent versies gevalideerd zijn tegen specifieke versies van ISE. Vele beheerders verbeteren hun ISE-cluster en vergeten de verwante NAC Agent-versie te uploaden in de database van de klantprovisioning.

Als u een verouderde NAC Agent versie voor uw ISE code gebruikt, let op dat het kan werken maar ook niet. Het is dus geen verrassing dat sommige klanten werken en andere niet. Eén manier om te controleren is om naar het download-gedeelte van Cisco.com van uw ISE-versie te gaan en te controleren welke NAC-versies er zijn. Meestal worden er meerdere ondersteund voor elke ISE-versie. Op deze webpagina worden alle matrixen verzameld: Cisco ISE-compatibiliteitsinformatie.

HTTP Web Proxy is in gebruik bij clients

Het concept van een HTTP-webproxy is dat cliënten de DNS-adressen van de website niet zelf oplossen en evenmin rechtstreeks contact opnemen met de websites; in plaats daarvan sturen ze hun verzoek gewoon naar de proxy server , die er zorg voor draagt . Het typische probleem met een gebruikelijke configuratie is dat de client een website (zoals www.cisco.com) oplost door direct de HTTP GET for it naar de proxy te verzenden, die wordt onderschept en terecht wordt hergeleid naar het ISE portal. In plaats van dan het volgende HTTP GET naar het ISE portal IP adres te verzenden, blijft de client dat verzoek naar de proxy verzenden.

Heeft u besloten om het HTTP-verkeer dat voor de proxy is bestemd niet opnieuw te richten, dan hebben uw gebruikers directe toegang tot het hele internet (omdat al het verkeer via de proxy verloopt) zonder dat u de proxy of de positie authentiek heeft. De oplossing is om de browser instellingen van de cliënten daadwerkelijk te veranderen en een uitzondering voor het ISE IP adres in de volmachtsinstellingen toe te voegen. Op deze manier, wanneer de cliënt ISE moet bereiken, stuurt hij het verzoek rechtstreeks naar de ISE en niet naar de gevolmachtigde. Dit vermijdt de oneindige lus waar de klant constant wordt hergericht maar nooit de logpagina ziet.

Merk op dat de NAC-agent niet wordt beïnvloed door de proxy-instellingen die in het systeem zijn ingevoerd, en dat de agent gewoon blijft handelen. Dit betekent dat als u een web proxy gebruikt, u niet beide de NAC agent discovery working kunt hebben (omdat deze poort 80 gebruikt) en gebruikers zelf-installeren de agent zodra ze teruggestuurd zijn naar de poster pagina wanneer ze doorbladeren (omdat dat de proxy poort gebruikt en typische switches niet opnieuw kunnen richten op meerdere poorten).

Discovery Hosts worden ingesteld in de NAC Agent

Vooral na versie 1.2 van ISE wordt aangeraden om geen discovery host op de NAC-agent te configureren tenzij u over expertise beschikt wat wel en niet doet. De NAC agent zou het ISE knooppunt moeten ontdekken dat het client-apparaat voor de eerst ontdekte HTTP. Als u op ontdekkingshosts vertrouwen, kunt u de NAC-agent contact hebben met een ander ISE-knooppunt dan het knooppunt dat het apparaat heeft geauthentificeerd en dat niet werkt. ISE versie 1.2 wijst een agent af die het knooppunt door het zoekhostproces ontdekt, omdat de NAC-agent de sessie-ID uit de URL-omleiding wil halen, zodat deze methode wordt ontmoedigd.

In sommige gevallen kunt u een discovery host configureren. Dan zou het met om het even welk IP adres (zelfs als niet bestaand) moeten worden gevormd die door het herleiden ACL opnieuw zal worden gericht, en het zou idealiter niet in zelfde voorwerp als de client moeten zijn (anders zal de client ARP voor onbepaalde tijd en nooit het HTTP discovery Packet verzenden).

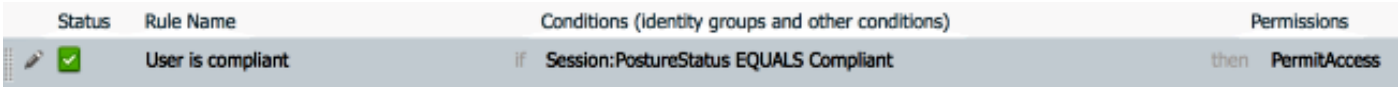
NAC-agent soms niet omhoog

Wanneer het om een intermitterende kwestie gaat en de acties zoals het uit de stekker halen/het opnieuw aansluiten van de kabel/WiFi connectiviteit het werk maken, is het een subtieler probleem. Het kan een probleem zijn met de RADIUS-sessie-ID's, waarbij de sessie-ID op ISE wordt verwijderd door RADIUS-accounting (rekenschap uitschakelen om te zien of er iets aan verandert).

Als u ISE Versie 1.2 gebruikt, is een andere mogelijkheid dat de client veel HTTP-pakketten verstuurt zodat er geen van een browser of de NAC-agent komt. ISE Versie 1.2 scant het veld user-agent in HTTP-pakketten om te zien of het van de NAC-agent of een browser komt, maar veel andere toepassingen verzenden HTTP-verkeer met een user-agent-veld en vermelden geen besturingssysteem of nuttige informatie. ISE versie 1.2 stuurt vervolgens een wijziging in de autorisatie om de client los te koppelen van de elektriciteit. ISE versie 1.3 heeft geen invloed op deze kwestie omdat het op een andere manier werkt. De oplossing is om te upgraden naar versie 1.3 of om alle gedetecteerde toepassingen in het doorsturen van ACL toe te staan zodat ze niet opnieuw naar ISE worden gericht.

Probleem omgekeerd: Agent pint herhaaldelijk

Het tegenovergestelde probleem kan zich voordoen waar de agent omhoog komt, de posteranalyse uitvoert, de client bevestigt, en dan weer verschijnt kort daarna in plaats van netwerkconnectiviteit toe te staan en stil te blijven. Dit gebeurt omdat, zelfs na een succesvolle opstelling, het HTTP-verkeer nog steeds wordt herbestemd voor het CPP-portaal op ISE. Het is een goed idee om dan door het ISE vergunningbeleid te gaan en te controleren dat u een regel hebt die een vergunning toegang (of gelijkaardige regel met mogelijke ACLs en VLANs) verstuurt wanneer het een conforme client en NIET een CPPomleiding ziet.



Gerelateerde informatie

- Postservices in de Cisco ISE Configuration Guide
- NAC Agent-detectieproces voor ISE
- ISE Traffic Redirectie op Catalyst 3750 Series-switch
- Technische ondersteuning en documentatie – Cisco Systems