AnyConnect Version 4.0 und NAC Posture Agent führen keine Fehlerbehebung für ISE durch

Inhalt

Einführung

Identity Services Engine (ISE) bietet Statusfunktionen, die die Verwendung des Network Admission Control (NAC)-Agenten (für Microsoft Windows, Macintosh oder über Webagent) oder AnyConnect Version 4.0 erfordern. Das ISE-Statusmodul der AnyConnect Version 4.0 funktioniert genau wie der NAC-Agent und wird daher in diesem Dokument als NAC-Agent bezeichnet. Das häufigste Symptom eines Statusfehlers für einen Client besteht darin, dass der NAC-Agent nicht angezeigt wird, da ein funktionierendes Szenario immer dazu führt, dass das NAC-Agentenfenster angezeigt und den Computer analysiert. Dieses Dokument hilft Ihnen, die vielen Ursachen einzugrenzen, die zum Ausfall der Statusanzeige führen können, d. h. der NAC-Agent wird nicht angezeigt. Sie ist nicht vollständig, da die NAC-Agentenprotokolle nur vom Cisco Technical Assistance Center (TAC) dekodiert werden können und die möglichen Ursachen zahlreich sind. Es zielt jedoch darauf ab, die Situation zu klären und das Problem weiter zu bestimmen, als einfach "der Agent springt nicht mit der Statusanalyse auf" und wird Ihnen wahrscheinlich helfen, die häufigsten Ursachen zu lösen.

Voraussetzungen

Anforderungen

Die in diesem Dokument aufgeführten Szenarien, Symptome und Schritte wurden geschrieben, um Probleme zu beheben, nachdem die Ersteinrichtung bereits abgeschlossen ist. Informationen

zur Erstkonfiguration finden Sie im Status-Services im Cisco ISE-Konfigurationshandbuch auf Cisco.com.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ISE Version 1.2.x
- NAC Agent für ISE Version 4.9.x
- AnyConnect Version 4.0

Hinweis: Die Informationen sollten auch auf andere ISE-Versionen angewendet werden, es sei denn, die Versionshinweise weisen auf wesentliche Verhaltensänderungen hin.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Fehlerbehebungsmethode

Wie kann der Agent angezeigt werden?

Der Agent wird angezeigt, wenn er einen ISE-Knoten erkennt. Wenn der Agent das Gefühl hat, dass er nicht über vollen Netzwerkzugriff verfügt und sich in einem Umleitungs-Szenario befindet, sucht er ständig nach einem ISE-Knoten.

Es gibt ein Dokument auf Cisco.com, in dem die Details des Agent Discovery-Prozesses erläutert werden: Network Admission Control (NAC) Agent Discovery Process für Identity Services Engine. Um eine Vervielfältigung von Inhalten zu vermeiden, werden in diesem Dokument nur die Schlüsselaspekte behandelt.

Wenn ein Client eine Verbindung herstellt, wird eine RADIUS-Authentifizierung (MAC-Filterung oder 802.1x) durchgeführt, an deren Ende die ISE die Umleitungskontrollliste (ACL) und die Umleitungs-URL an das Netzwerkgerät (Switch, Adaptive Security Appliance (ASA) oder Wireless Controller) zurückgibt, um den Client-Datenverkehr so einzuschränken, dass er nur eine IP-Adresse und DNS-Auflösungen erhält. Der gesamte HTTP(S)-Datenverkehr vom Client wird an eine eindeutige URL auf der ISE umgeleitet, die mit CPP endet (Client Posture and Provisioning), mit Ausnahme des Datenverkehrs, der für das ISE-Portal selbst bestimmt ist. Der NAC-Agent sendet ein reguläres HTTP GET-Paket an das Standard-Gateway. Erhält der Support-Mitarbeiter keine Antwort oder eine andere Antwort als eine CPP-Umleitung, gilt er als vollständig verbunden und fährt nicht mit dem Status fort. Wenn eine HTTP-Antwort empfangen wird, die eine Umleitung zu einer CPP-URL am Ende eines bestimmten ISE-Knotens darstellt, wird der Statusprozess fortgesetzt und der ISE-Knoten wird kontaktiert. Die Analyse wird nur dann gestartet, wenn sie die Statusinformationen von diesem ISE-Knoten erfolgreich erhält.

Der NAC-Agent erreicht außerdem die konfigurierte IP-Adresse des Discovery-Hosts (es wird nicht erwartet, dass mehr als eine konfiguriert wird). Er soll auch dort umgeleitet werden, um die Umleitungs-URL mit der Sitzungs-ID abzurufen. Wenn die Erkennungs-IP-Adresse ein ISE-Knoten ist, wird sie nicht weiterverfolgt, da sie auf eine Umleitung wartet, um die richtige Sitzungs-ID zu

erhalten. Der Discovery-Host wird also in der Regel nicht benötigt, kann aber nützlich sein, wenn er als eine beliebige IP-Adresse im Bereich der umgeleiteten ACL festgelegt wird, um eine Umleitung auszulösen (z. B. in VPN-Szenarien).

Mögliche Ursachen

Umleitung erfolgt nicht

Dies ist die weit häufigste Ursache. Öffnen Sie zum Validieren oder für ungültig erklären einen Browser auf dem PC, auf dem der Agent nicht angezeigt wird, und überprüfen Sie, ob Sie zur Download-Seite des Status-Agenten weitergeleitet werden, wenn Sie eine URL eingeben. Sie können auch eine zufällige IP-Adresse wie http://1.2.3.4 eingeben, um ein mögliches DNS-Problem zu vermeiden (wenn eine IP-Adresse umgeleitet wird, ein Website-Name jedoch nicht, können Sie DNS anzeigen).

Wenn Sie umgeleitet werden, sollten Sie die Agentenprotokolle und das ISE-Support-Paket (mit dem Status- und Schweizer-Modul zum Debugging-Modus) sammeln und sich an das Cisco TAC wenden. Dies weist darauf hin, dass der Agent einen ISE-Knoten erkennt, aber etwas beim Abrufen der Statusdaten fehlschlägt.

Wenn keine Umleitung erfolgt, haben Sie die erste Ursache, die noch weiter untersucht werden muss. Ein guter Anfang ist, die Konfiguration auf dem Netzwerkzugriffsgerät (Wireless LAN Controller (WLC) oder Switch) zu überprüfen und mit dem nächsten Element in diesem Dokument zu beginnen.

Auf dem Netzwerkgerät sind keine Attribute installiert.

Dieses Problem ist ein Teilfall des Szenarios **"Umleitung findet nicht statt"**. Wenn die Umleitung nicht erfolgt, muss zunächst überprüft werden (da das Problem auf einem bestimmten Client auftritt), ob der Client vom Switch oder der Wireless Access Layer korrekt in den richtigen Status gesetzt wurde.

Im Folgenden finden Sie ein Beispiel für die Ausgabe des Befehls **show access-session interface <Schnittstellennummer> detail** (Sie müssen möglicherweise **Details** am Ende auf einigen Plattformen hinzufügen) auf dem Switch, mit dem der Client verbunden ist. Sie müssen überprüfen, ob der Status "Authz Success" lautet, dass die URL die ACL richtig auf die beabsichtigte Umleitungszugriffskontrollliste verweist und dass die URL auf den erwarteten ISE-Knoten verweist, der **CPP** am Ende der URL verwendet. Das ACS ACL-Feld ist nicht obligatorisch, da es nur angezeigt wird, wenn Sie eine herunterladbare Zugriffsliste im Autorisierungsprofil für die ISE konfiguriert haben. Es ist jedoch wichtig, sich die ACL anzuschauen und zu überprüfen, ob sie nicht mit der umgeleiteten ACL kollidiert (siehe Dokumente zur Statuskonfiguration im Zweifelsfall).

```
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
```

Geben Sie zur Fehlerbehebung bei einem WLC, der AireOS ausführt, **show wireless client detail <mac address>** und geben Sie **show wireless client mac-address <mac address> detail ein,** um einen WLC, der Cisco IOS-XE ausführt, zu beheben. Ähnliche Daten werden angezeigt, und Sie müssen die Umleitungs-URL und die ACL überprüfen und ob der Client den Status "POSTURE_REQD" oder Ähnliches hat (dieser Wert variiert je nach Softwareversion).

Wenn keine Attribute vorhanden sind, müssen Sie die Authentifizierungsdetails in der ISE des Clients öffnen, für den Sie die Fehlerbehebung ausgeführt haben (navigieren Sie zu **Operations > Authentications**), und im Abschnitt Result überprüfen, dass die Umleitungsattribute gesendet wurden. Wenn sie nicht gesendet wurden, sollten Sie die Autorisierungsrichtlinie überprüfen, um zu verstehen, warum die Attribute für diesen Client nicht zurückgegeben wurden. Eine der Bedingungen stimmt wahrscheinlich nicht überein, daher ist es empfehlenswert, die Probleme einzeln zu beheben.

Beachten Sie, dass Cisco IOS® in Bezug auf die Umleitungszugriffskontrollliste auf Genehmigungsanweisungen umleitet (sodass die ISE- und DNS-IP-Adressen abgelehnt werden müssen), während AireOS auf dem WLC auf Ablehnungsanweisungen umleitet (dies ist für ISE und DNS also zulässig).

Attribute sind vorhanden, das Netzwerkgerät wird jedoch nicht umgeleitet.

Die Hauptursache in diesem Fall ist ein Konfigurationsproblem. Sie sollten die Konfiguration des Netzwerkgeräts anhand des Konfigurationsleitfadens und der Konfigurationsbeispiele auf Cisco.com überprüfen. In diesem Fall liegt das Problem in der Regel an allen Ports oder Access Points (APs) des Netzwerkgeräts vor. Andernfalls tritt das Problem möglicherweise nur bei einigen Switch-Ports oder APs auf. In diesem Fall sollten Sie die Konfiguration derjenigen vergleichen, bei denen das Problem auftritt, im Vergleich zu den Ports oder APs, an denen die Schwachstelle gut funktioniert.

FlexConnect-APs sind empfindlich, da sie jeweils über eine eindeutige Konfiguration verfügen können und es leicht ist, in einer ACL oder einem VLAN in einigen APs und nicht in anderen einen Fehler zu machen.

Ein weiteres häufiges Problem ist, dass das Client-VLAN keine SVI hat. Dies gilt nur für Switches und wird ausführlich in ISE Traffic Redirection auf dem Catalyst Switch der Serie 3750 beschrieben. Aus der Sicht der Attribute kann alles gut aussehen.

Integration der herunterladbaren Zugriffsliste (DACL)

Wenn Sie gleichzeitig mit den Umleitungsattributen eine DACL zurück zum Switch drücken (oder eine Air-ACL für einen Wireless-Controller), kann die Umleitung blockiert werden. Die DACL wird zuerst angewendet und bestimmt, was vollständig verworfen wird und was weiter verarbeitet wird. Anschließend wird die Umleitungskontrollliste angewendet und bestimmt, was umgeleitet wird.

Konkret bedeutet dies, dass Sie in der Regel den gesamten HTTP- und HTTPS-Verkehr in Ihrer DACL zulassen möchten. Wenn Sie sie blockieren, wird sie nicht umgeleitet, da sie vorher gelöscht wird. Dies ist kein Sicherheitsbedenken, da der Datenverkehr größtenteils über die nachfolgende Umleitungszugriffskontrollliste umgeleitet wird, sodass er im Netzwerk nicht zugelassen ist. Sie müssen diese beiden Datenverkehrstypen jedoch in der DACL zulassen, damit sie unmittelbar danach auf die Umleitungszugriffskontrollliste zugreifen können.

Ungültige Version des NAC-Agenten

Es ist leicht zu vergessen, dass bestimmte NAC Agent-Versionen für bestimmte ISE-Versionen validiert wurden. Viele Administratoren aktualisieren ihren ISE-Cluster und vergessen, die zugehörige NAC-Agent-Version in die Ergebnisdatenbank der Client-Bereitstellung hochzuladen.

Wenn Sie eine veraltete NAC-Agent-Version für Ihren ISE-Code verwenden, sollten Sie bedenken, dass dieser möglicherweise funktioniert, aber möglicherweise auch nicht. Es ist daher keine Überraschung, dass einige Kunden arbeiten und andere nicht. Eine Möglichkeit zur Verifizierung besteht darin, im Download-Bereich der ISE-Version von Cisco.com zu überprüfen, welche NAC Agent-Versionen vorhanden sind. In der Regel werden für jede ISE-Version mehrere Versionen unterstützt. Diese Webseite sammelt alle Matrixdateien: Informationen zur ISE-Kompatibilität von Cisco.

HTTP-Webproxy wird von Clients verwendet

Das Konzept eines HTTP-Webproxys besteht darin, dass Clients die DNS-IP-Adressen der Website nicht selbst auflösen oder die Websites direkt kontaktieren. sondern senden ihre Anfrage einfach an den Proxy-Server, der sich um sie kümmert. Das typische Problem bei einer normalen Konfiguration besteht darin, dass der Client eine Website (z. B. www.cisco.com) löst, indem er die HTTP GET für diese Website direkt an den Proxy sendet, der abgefangen wird und rechtmäßig an das ISE-Portal umgeleitet wird. Anstatt jedoch die nächste HTTP GET-Anforderung an die IP-Adresse des ISE-Portals zu senden, sendet der Client diese Anforderung weiterhin an den Proxy.

Falls Sie beschließen, HTTP-Datenverkehr, der an den Proxy gerichtet ist, nicht umzuleiten, haben Ihre Benutzer direkten Zugriff auf das gesamte Internet (da der gesamte Datenverkehr den Proxy durchläuft), ohne sich zu authentifizieren oder zu posten. Die Lösung besteht darin, die Browsereinstellungen der Clients zu ändern und in den Proxy-Einstellungen eine Ausnahme für die ISE-IP-Adresse hinzuzufügen. Wenn der Client die ISE erreichen muss, sendet er die Anfrage direkt an die ISE und nicht an den Proxy. Dadurch wird die unendliche Schleife vermieden, in der der Client ständig umgeleitet wird, aber nie die Anmeldeseite sieht.

Beachten Sie, dass der NAC-Agent nicht von den im System eingegebenen Proxy-Einstellungen betroffen ist und weiterhin normal arbeitet. Das bedeutet, dass bei Verwendung eines Webproxys die NAC-Agent-Erkennung nicht funktioniert (weil Port 80 verwendet wird) und die Benutzer den Agent selbst installieren können, sobald sie beim Durchsuchen zur Statusseite umgeleitet werden (da dies den Proxy-Port verwendet und typische Switches nicht auf mehreren Ports umgeleitet werden können).

Discovery-Hosts werden im NAC Agent konfiguriert.

Insbesondere nach ISE Version 1.2 wird empfohlen, keinen Discovery-Host auf dem NAC-Agent zu konfigurieren, es sei denn, Sie verfügen über Fachwissen in Bezug auf die Aktivitäten und Aktivitäten. Der NAC-Agent soll den ISE-Knoten ermitteln, der das Client-Gerät mittels HTTP Discovery authentifiziert hat. Wenn Sie sich auf Discovery-Hosts verlassen, kann der NAC-Agent einen anderen ISE-Knoten kontaktieren als den, der das Gerät authentifiziert hat und der nicht funktioniert. Die ISE Version 1.2 weist einen Agent zurück, der den Knoten durch den Discovery Host-Prozess erkennt, da der NAC-Agent die Session-ID von der Umleitungs-URL abrufen soll, sodass diese Methode nicht empfohlen wird.

In einigen Fällen möchten Sie möglicherweise einen Discovery-Host konfigurieren. Anschließend sollte sie mit jeder IP-Adresse konfiguriert werden (auch wenn sie nicht vorhanden ist), die von der Umleitungszugriffskontrollliste umgeleitet wird. Idealerweise sollte sie sich nicht im gleichen Subnetz wie der Client befinden (ansonsten wird der Client für ihn auf unbestimmte Zeit ARP erstellen und niemals das HTTP Discovery-Paket senden).

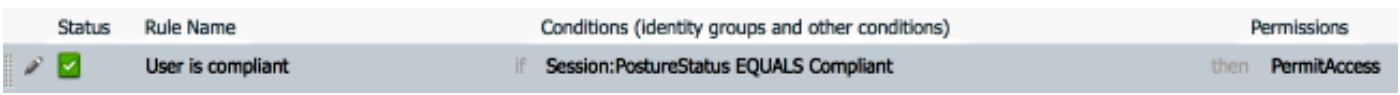
NAC Agent führt manchmal keine Popup-Meldung aus

Wenn das Problem häufiger auftritt und z. B. das Trennen/Trennen der Kabel-/Wi-Fi-Verbindung zum Netz funktioniert, ist es ein Problem, das etwas komplizierter ist. Es könnte ein Problem mit den RADIUS-Session-IDs auftreten, bei denen die Session-ID durch RADIUS Accounting auf der ISE gelöscht wird (deaktivieren Sie Accounting, um festzustellen, ob es etwas ändert).

Wenn Sie ISE Version 1.2 verwenden, besteht eine weitere Möglichkeit darin, dass der Client viele HTTP-Pakete sendet, sodass keine Pakete von einem Browser oder vom NAC-Agent stammen. ISE Version 1.2 überprüft das Benutzeragentenfeld in HTTP-Paketen, um festzustellen, ob es vom NAC-Agenten oder vom Browser stammt. Viele andere Anwendungen senden HTTP-Datenverkehr mit einem Benutzeragentenfeld, ohne Betriebssystem oder nützliche Informationen zu erwähnen. ISE Version 1.2 sendet dann eine Autorisierungsänderung, um die Verbindung zum Client zu trennen. ISE Version 1.3 ist von diesem Problem nicht betroffen, da es auf andere Weise funktioniert. Die Lösung besteht entweder darin, ein Upgrade auf Version 1.3 durchzuführen oder alle erkannten Anwendungen in der Umleitungskontrollliste zuzulassen, damit sie nicht an die ISE umgeleitet werden.

Umkehrproblem: Agenten-Pops wiederholt

Das Gegenteil kann auftreten, wenn der Agent eine Popup-Meldung ausführt, die Statusanalyse durchführt, den Client validiert und dann kurz danach wieder angezeigt wird, anstatt die Netzwerkverbindung zu ermöglichen und den Anruf zu unterdrücken. Dies liegt daran, dass der HTTP-Datenverkehr auch nach einem erfolgreichen Status noch an das CPP-Portal der ISE weitergeleitet wird. Es empfiehlt sich, die ISE-Autorisierungsrichtlinie zu durchlaufen und zu überprüfen, ob eine Regel vorhanden ist, die einen Genehmigungszugriff (oder eine ähnliche Regel mit möglichen ACLs und VLANs) sendet, wenn ein kompatibler Client erkannt wird und KEINE CPP-Umleitung erneut erfolgt.



Zugehörige Informationen

- Statusservices im Cisco ISE-Konfigurationshandbuch
- NAC Agent Discovery Process für ISE
- Umleitung des ISE-Datenverkehrs auf dem Catalyst Switch der Serie 3750
- Technischer Support und Dokumentation - Cisco Systems