La version 4.0 d'AnyConnect et l'agent de position du NAC ne s'affiche pas sur ISE dépannent le guide

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Dépannage de la méthodologie](#)
[Qu'incite l'agent à s'afficher ?](#)
[Causes possibles](#)
[La redirection ne se produit pas](#)
[Des attributs ne sont pas installés sur le périphérique de réseau](#)
[Les attributs sont en place mais le périphérique de réseau ne réoriente pas](#)
[Liste d'accès téléchargeable de intervention (DACL)](#)
[Mauvaise version d'agent NAC](#)
[Le proxy de Web de HTTP est en service par des clients](#)
[Des hôtes de détection sont configurés dans l'agent NAC](#)
[L'agent NAC ne s'affiche pas parfois](#)
[Renversez le problème : L'agent s'affiche à plusieurs reprises](#)
[Informations connexes](#)

Introduction

Le Cisco Identity Services Engine (ISE) fournit les capacités posantes qui exigent l'utilisation de l'agent de Contrôle d'admission au réseau (NAC) (pour Microsoft Windows, Macintosh, ou par l'intermédiaire de webagent) ou de la version 4.0 d'AnyConnect. Le module de posture de la version 4.0 ISE d'AnyConnect fonctionne exactement comme l'agent NAC et est donc mentionné comme l'agent NAC dans ce document. La plupart de symptôme commun de panne de posture pour un client est que l'agent NAC ne s'affiche pas puisqu'un scénario fonctionnant fait toujours afficher et analyser la fenêtre d'agent NAC votre PC. Ce document vous aide à rétrécir vers le bas les nombreuses causes qui peuvent mener la posture échouer, qui signifie que l'agent NAC ne s'affiche pas. On ne le cense pas être exhaustif parce que les logs d'agent NAC peuvent seulement être décodés par le centre d'assistance technique Cisco (TAC) et les causes principales possibles sont nombreuses ; cependant il vise à clarifier la situation et à indiquer exactement le problème plus loin que simplement « l'agent ne s'affiche pas avec l'analyse de posture » et vous aidera probablement à résoudre les la plupart des causes classiques.

Conditions préalables

Conditions requises

Les scénarios, les symptômes, et les étapes répertoriées dans ce document écrits pour que vous dépanniez des questions après que la première installation sont soit déjà terminée. Pour la configuration initiale, référez-vous aux services de posture sur le guide de configuration de Cisco ISE sur Cisco.com.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ISE Version1.2.x
- Agent NAC pour la version 4.9.x ISE
- Version 4.0 d'AnyConnect

  Remarque: Les informations devraient également s'appliquer à d'autres releases d'ISE à moins que les notes de mise à jour indiquent les modifications comportementales importantes.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Dépannage de la méthodologie

Qu'incite l'agent à s'afficher ?

L'agent s'affiche quand il découvre un noeud ISE. Si l'agent sent qu'il n'a pas le plein accès au réseau et est dans un scénario de redirection de posture, il recherche constamment un noeud ISE.

Là nous un document de Cisco.com qui explique les détails du processus de découverte d'agent : Processus de découverte d'agent de Contrôle d'admission au réseau (NAC) pour le Cisco Identity Services Engine. Afin d'éviter la duplication satisfaite, ce document discute seulement le point clé.

Quand un client se connecte, il subit une authentification de RAYON (filtrage MAC ou 802.1x) à l'extrémité dont, ISE renvoie la liste de contrôle d'accès de redirection (ACL) et l'URL de redirection au périphérique de réseau (commutateur, appliance de sécurité adaptable (ASA), ou

contrôleur sans-fil) afin de limiter le trafic de client pour lui permettre seulement pour obtenir des résolutions d'une adresse IP et de Domain Name Server (DN). Tout le trafic http qui provient le client est réorienté à un seul URL sur ISE qui finit avec **CPP** (posture et ravitaillement de client), excepté le trafic destiné au portail ISE lui-même. L'agent NAC envoie un HTTP régulier OBTIENNENT le paquet à la passerelle par défaut. Si l'agent reçoit le pas de réponse ou tout autre réponse qu'une redirection de CPP, il se considère avoir la connectivité complète et ne continue pas de poser. S'il reçoit une réponse de HTTP qui est une redirection à un URL de CPP à l'extrémité d'un noeud de la particularité ISE, alors il continue le processus et les contacts de posture ce noeud ISE. Il seulement s'affiche et commence l'analyse quand il reçoit avec succès les détails de posture de celui noeud ISE.

L'agent NAC atteint également à l'adresse IP configurée d'hôte de détection (il ne prévoit pas plus d'une à configurer). Il compte être réorienté là aussi bien afin d'obtenir l'URL de redirection avec l'ID de session. Si l'adresse IP de détection est un noeud ISE, alors elle ne poursuit pas parce qu'elle attend d'être réorientée afin d'obtenir le bon ID de session. Ainsi l'hôte de détection n'est habituellement pas nécessaire, mais peut être utile une fois réglé en tant que toute adresse IP de l'ordre de l'ACL de réorientation afin de déclencher une redirection (comme dans des scénarios VPN, par exemple).

Causes possibles

La redirection ne se produit pas

C'est la plupart de cause classique de loin. Afin de valider ou infirmer, ouvrent un navigateur sur le PC où l'agent ne s'affiche pas et voit si vous êtes réorienté à la page de téléchargement d'agent intermédiaire quand vous tapez n'importe quel URL. Vous pouvez également taper une adresse IP aléatoire telle que **http://1.2.3.4** afin d'éviter une question possible de DN (si une adresse IP réoriente mais un nom de site Web ne fait pas, vous pouvez regarder des DN).

Si vous obtenez réorienté, vous devriez collecter le paquet de logs d'agent et de support ISE (avec la posture et le module de Suisse pour mettre au point le mode) et contacter Cisco TAC. Ceci indique que l'agent découvre un noeud ISE mais quelque chose échoue pendant le processus pour obtenir les données de posture.

Si aucune redirection ne se produit, vous avez votre première cause, qui exige toujours des recherches plus approfondies de la cause principale. Un bon début est de vérifier la configuration sur le périphérique d'accès au réseau (contrôleur LAN Sans fil (WLC) ou commutateur) et de se déplacer au prochain élément dans ce document.

Des attributs ne sont pas installés sur le périphérique de réseau

Cette question est un subcase de la **redirection ne se produit pas** scénario. Si la redirection ne se produit pas, la première chose est de vérifier (car le problème se pose sur un client donné) que le client est correctement placé dans le bon état par la couche d'accès de commutateur ou de radio.

Voici l'exemple de sortie de la commande de **number> de <interface de la session international de**

show authentication (vous pourriez devoir ajouter le **détail à l'**extrémité sur quelques Plateformes) prise sur le commutateur où le client est connecté. Vous devez vérifier que l'état est « succès d'Authz », que l'URL réorientent l'ACL correctement indique destiné réorientent l'ACL, et que l'URL réorientent des points au noeud prévu ISE avec **CPP à l'**extrémité de l'URL. Le champ d'ACL ACS n'est pas obligatoire parce qu'il affiche seulement si vous configuriez une liste d'accès téléchargeable sur le profil d'autorisation sur ISE. Il est, cependant, important de le regarder et de le vérifier qu'il n'y a aucun conflit avec l'ACL de réorientation (voir les documents au sujet de la configuration de posture en cas de doute).

```
01-SW3750-access#show auth sess int gi1/0/12
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
```

Afin de dépanner un WLC qui exécute AireOS, présentez le **petit groupe < MAC address > de client sans fil d'exposition** et écrivez le **détail de < MAC address > de mac-address de client sans fil d'exposition** afin de dépanner un WLC qui exécute le Cisco IOS XE. Les affichages de données et vous semblables devez vérifier l'URL de réorientation et l'ACL et si le client est dans l'état « POSTURE_REQD » ou semblable (il varie selon la version de logiciel).

Si les attributs ne sont pas présents, vous devez ouvrir les détails d'authentification dans l'ISE du client que vous dépanniez (naviguez vers des **exécutions > des authentifications**) et les vérifier dans la section de résultat que les attributs de redirection ont été envoyée. S'ils n'étaient pas envoyés, vous devriez passer en revue la stratégie d'autorisation pour comprendre pourquoi les attributs n'ont pas été retournés pour ce client particulier. Probablement, une des conditions ne s'est pas assortie, ainsi c'est une bonne idée de les dépanner un.

Souvenez-vous que, concernant l'ACL de réorientation, le Cisco IOS® réoriente sur des déclarations d'autorisation (ainsi les adresses IP ISE et de DN devez être refusé) tandis qu'AireOS sur le WLC réoriente là-dessus des instructions de refus (ainsi est tenu compte d'ISE et de DN).

Les attributs sont en place mais le périphérique de réseau ne réoriente pas

La principale cause est dans ce cas une question de configuration. Vous devriez passer en revue la configuration du périphérique de réseau contre les exemples de guide de configuration et de configuration sur Cisco.com. Si c'est le cas, le problème existe typiquement dans tous tous les ports ou Points d'accès (aps) du périphérique de réseau. Sinon, le problème pourrait seulement se poser sur quelques switchports ou quelques aps. Si c'est le cas, vous devriez comparer la configuration de ceux où le problème se pose comparé aux ports ou aux aps où la posture fonctionne bien.

FlexConnect aps sont sensible parce qu'ils peuvent chacun avoir une seule configuration et il est facile de faire une erreur dans un ACL ou un VLAN dans quelques aps et pas d'autres.

Un autre problème courant est que le client VLAN n'a pas un SVI. Ceci applique seulement aux Commutateurs et est discuté en détail dans la redirection du trafic ISE sur la gamme Catalyst 3750 commutent. Tout pourrait sembler bon du point de vue d'attributs.

Liste d'accès téléchargeable de intervention (DACL)

Si, en même temps que les attributs de redirection, vous poussent un DACL de nouveau au commutateur (ou l'Airespace-ACL pour un contrôleur sans-fil), alors il pourrait bloquer votre redirection. Le DACL est appliqué d'abord et détermine ce qui est complètement relâché et ce qui continue pour être traité. Alors l'ACL de réorientation est appliqué et détermine ce qui est réorienté.

Ce que signifie concrètement ceci est celui le plus souvent, vous voudrez permettre tout le trafic de HTTP et HTTPS dans votre DACL. Si vous le bloquez, il ne sera pas réorienté puisqu'il sera relâché avant cela. Ce n'est pas un problème de sécurité, parce que ce trafic sera réorienté en grande partie sur l'ACL de réorientation après, ainsi on ne lui permet pas vraiment sur le réseau ; cependant, vous devez permettre à ces deux types de trafic dans le DACL afin qu'ils puissent pour avoir une occasion de frapper l'ACL de réorientation juste après.

Mauvaise version d'agent NAC

Il est facile d'oublier que des versions spécifiques d'agent NAC sont validées contre des versions spécifiques d'ISE. Beaucoup d'administrateurs améliorent leur batterie ISE et oublient de télécharger la version relative d'agent NAC dans la base de données de résultats de ravitaillement de client.

Si vous utilisez une version périmée d'agent NAC pour votre code ISE, rendez-vous compte qu'il pourrait fonctionner mais il ne pourrait pas également. Ainsi il n'est aucune surprise que quelques clients travaillent et d'autres ne font pas. Une manière de vérifier est d'aller à Cisco.com la section téléchargement de votre version et de contrôle ISE qui les versions d'agent NAC sont là. En général il y a plusieurs pris en charge pour chaque version ISE. Cette page Web recueille toutes les matrices : Les informations sur la compatibilité de Cisco ISE.

Le proxy de Web de HTTP est en service par des clients

Le concept d'un proxy de Web de HTTP est que les clients ne résolvent pas les adresses IP de

DN de site Web elles-mêmes ni entrent en contact avec les sites Web directement ; en revanche, ils envoient simplement leur demande au serveur proxy, qui prend soin de elle. Le problème typique avec une configuration habituelle est que le client résout un site Web (tel que www.cisco.com) en envoyant directement le HTTP OBTIENNENT pour lui au proxy, qui obtient intercepté et légitime réorienté au portail ISE. Cependant, au lieu d'envoyer alors le prochain HTTP OBTENEZ à l'adresse IP portaile ISE, le client continue à envoyer cette demande au proxy.

Au cas où vous décideriez de ne pas réorienter le trafic http destiné au proxy, vos utilisateurs ont l'accès direct à tout le Internet (puisque tout le trafic passe par le proxy) sans authentifier ou poser. La solution est réellement de modifier les configurations du navigateur des clients et d'ajouter une exception pour l'adresse IP ISE dans les paramètres de proxy. De cette façon, quand le client doit atteindre ISE, il envoie la demande directement à l'ISE et pas au proxy. Ceci évite la boucle infinie où le client obtient constamment réorienté mais ne voit jamais la page de connexion.

Notez que l'agent NAC n'est pas affecté par les paramètres de proxy écrits dans le système et il continue à agir normalement. Ceci signifie que si vous utilisez un proxy de Web, vous ne pouvez pas avoir le fonctionnement de détection d'agent NAC (parce qu'il utilise le port 80) et avoir l'installation automatique d'utilisateurs l'agent une fois qu'ils sont réorientés à la page de posture quand ils parcourent (puisque ce utilise le port de proxy et les Commutateurs typiques ne peuvent pas réorienter sur des plusieurs ports).

Des hôtes de détection sont configurés dans l'agent NAC

Particulièrement après version 1.2 ISE, il est recommandé pour ne pas configurer n'importe quel serveur de détection sur l'agent NAC à moins que vous ayez l'expertise sur ce qu'il fait et ne fait pas. L'agent NAC est censé découvrir le noeud ISE qui a authentifié le périphérique de client par la détection de HTTP. Si vous comptez sur des hôtes de détection, vous pourriez faire entrer en contact avec à l'agent NAC un autre noeud ISE que celui qui a authentifié le périphérique et qui ne fonctionne pas. La version 1.2 ISE rejette un agent qui découvre le noeud par le processus de serveur de détection parce qu'il veut que l'agent NAC obtienne l'ID de session de l'URL de réorientation ainsi cette méthode est découragée.

Dans certains cas, vous pourriez vouloir configurer un hôte de détection. Alors il devrait être configuré avec n'importe quelle adresse IP (même si non-existant) qui sera réorientée par l'ACL de réorientation, et il ne devrait pas idéalement être dans le même sous-réseau que le client (autrement le client ARP indéfiniment pour lui et ne jamais envoyer le paquet de détection de HTTP).

L'agent NAC ne s'affiche pas parfois

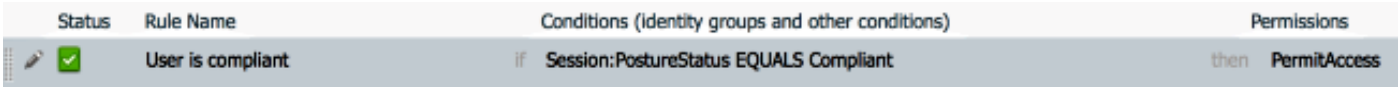
Quand la question est plus intermittente et les actions telles que débrancher/replugging la Connectivité de câble/wifi la font fonctionner, c'est un problème plus subtil. Ce pourrait être un problème avec les id de session de RAYON où l'ID de session est supprimé sur l'ISE par la comptabilité de RAYON (comptabilité de débronchement pour voir si elle change quelque chose).

Si vous utilisez ISE Version1.2, une autre possibilité est que le client envoie beaucoup de paquets de HTTP de sorte qu'aucun ne provienne un navigateur ou l'agent NAC. La version 1.2 ISE balaye

le champ d'utilisateur-agent en paquets de HTTP pour voir si elle provient l'agent NAC ou un programme de lecture, mais beaucoup d'autres applications envoient le trafic de HTTP avec un champ d'utilisateur-agent et ne mentionnent pas n'importe quel système d'exploitation ou informations utiles. La version 1.2 ISE envoie alors une modification de l'autorisation de déconnecter le client. La version 1.3 ISE n'est pas affectée par ce beause de question que cela fonctionne d'une manière différente. La solution est d'améliorer à la version 1.3 ou de permettre toutes les applications détectées dans l'ACL de réorientation de sorte qu'elles ne soient pas réorientées vers ISE.

Renversez le problème : L'agent s'affiche à plusieurs reprises

Le problème opposé peut surgir où l'agent s'affiche, fait l'analyse de posture, valide le client, et puis s'affiche de nouveau peu de temps après au lieu de permettre la connexion réseau et de rester silent. Ceci se produit parce que, même après une posture réussie, le trafic http est encore réorienté au portail de CPP sur ISE. Il est une bonne idée de passer alors par la stratégie d'autorisation ISE et contrôle que vous avez une règle qui envoie un accès d'autorisation (ou la règle semblable avec ACLs et VLAN possibles) quand il revoit un client conforme et PAS une redirection de CPP.



Informations connexes

- Services de posture sur le guide de configuration de Cisco ISE
- Processus de découverte d'agent NAC pour ISE
- Redirection du trafic ISE sur le commutateur de gamme Catalyst 3750
- Support et documentation techniques - Cisco Systems