Couche de Cisco NAC 3 OOB utilisant Vrf-Lite pour la localisation du trafic

Contenu

Introduction

Ce guide décrit une implémentation du Cisco Network Admission Control (NAC) dans un déploiement hors bande de la couche 3 (OOB) qui est basé sur l'expédition de route virtuelle (VRF) - Lite.

Présentation de la solution

Cette section donne une brève introduction pour poser 3 OOB suivre des méthodes de Vrf-Lite afin d'implémenter une architecture NAC.

Synthèse

Le Cisco NAC impose les stratégies de sécurité réseau d'une organisation sur tous les périphériques qui recherchent l'accès au réseau. Le Cisco NAC permet seulement les périphériques d'extrémité conformes et de confiance, tels que des PC, des serveurs, et des PDA, sur le réseau. Le Cisco NAC limite l'accès des périphériques noncompliant, qui limite le possible détérioration des menaces et des risques de Sécurité d'émergeant. Le Cisco NAC donne à des organismes une méthode puissante et basée sur rôles afin d'empêcher l'accès non autorisé et améliorer la résilience de réseau.

La solution de Cisco NAC fournit ces avantages pour l'entreprise :

- **Conformité de stratégie de sécurité** — S'assure que les points finaux se conforment à la stratégie de sécurité ; protège la productivité d'infrastructure et d'employés ; sécurise les ressources géré et en non pris en charge ; environnements internes et accès invité de supports ; conçoit en fonction des stratégies votre niveau de risque
- **Protège des investissements existants** — Est compatible avec de tiers applications d'administration ; les options de déploiement flexible réduisent le besoin de mises à jour d'infrastructure
- **Atténue des risques des virus, des vers, et des contrôles d'accès non autorisés** et réduit des interruptions de grande puissance d'infrastructure ; réduit des dépenses d'exploitation en entreprenant des démarches, ajoute, et change dynamique et automatisé, de ce fait activant une efficacité informatique plus élevée ; intègre avec d'autres composants de Cisco Self-Defending Network afin de fournir la protection de Sécurité complète

Description de la solution

Le Cisco NAC est utilisé dans l'infrastructure réseau afin d'imposer la conformité de stratégie de sécurité sur tous les périphériques qui recherchent l'accès aux ressources de réseau. Le Cisco NAC permet à des administrateurs réseau pour authentifier et autoriser les utilisateurs et pour les évaluer et le remediate leurs ordinateurs associés avant qu'on leur accorde l'accès au réseau. Vous pouvez employer plusieurs méthodes de configuration pour accomplir cette tâche. Ce document se concentre spécifiquement sur l'implémentation basée sur vrf du Cisco NAC dans un déploiement de la couche 3 OOB où le serveur de Cisco NAC (serveur de Cisco Clean Access) est configuré en vrai mode de passerelle IP (conduite).

La couche 3 OOB est l'une des méthodologies de déploiement les plus populaires pour le NAC. Cette variation dans la popularité est basée sur les plusieurs dynamics qui incluent une meilleure utilisation des ressources en matériel. En déployant le Cisco NAC dans une méthodologie de la couche 3 OOB, une appliance simple de Cisco NAC peut mesurer pour rendre service à plus d'utilisateurs. Il permet également des appliances de Cisco NAC à situer centralement plutôt que distribuées à travers le campus ou l'organisation. Par conséquent, les déploiements de la couche 3 OOB sont plus rentables chacun des deux d'un point de vue de capital et de frais d'exploitation.

Ce guide décrit une implémentation de Cisco NAC dans un déploiement de la couche 3 OOB qui est basé sur Vrf-Lite.

Définition simple de VRF

Une manière de regarder la virtualisation de périphérique de VRF est de l'égaliser à l'apparition des VLAN. Les VLAN ont créé les Commutateurs virtuels hors d'un commutateur physique simple. Les vrf étendent cette virtualisation après la borne de la couche 2, et permettent la création des Routeurs virtuels. Les Routeurs virtuels prévoient les réseaux plein-virtualisés de bout en bout.

Une autre manière de regarder la conception de VRF est que chaque VRF agit juste comme un VPN ou un tunnel. Le trafic qui est placé dans un VRF ne peut pas communiquer en dehors de du VRF (tunnel) jusqu'à ce que le trafic traverse le périphérique qui termine le tunnel (le routeur VPN de destination).

Remarque: Ces définitions sont censées pour aider à introduire un nouveau concept. Ces définitions ne sont pas les représentations précises ou les définitions officielles du VRF.

La figure 1 affiche une illustration de virtualisation de périphérique avec des vrf. Chaque couche

colorée dans le diagramme représente un routeur virtuel différent, ou le VRF. La méthodologie de VRF fournit l'isolation de chemin d'avion et de plan de données de contrôle, avec la capacité d'avoir les plans de données d'isolement par multiple. En d'autres termes, il fournit la possibilité pour un routeur virtuel distinct ou le réseau pour chaque type de trafic qui est prévu dans un environnement qui utilise le Cisco NAC. Les types de trafic typiques sont :

- Le trafic d'utilisateur Unauthenticated
- Le trafic authentifié d'utilisateur
- Le trafic de sous-traitant
- Le trafic d'invité

Figure 1 – ***Virtualisation de périphérique***

Architecture de solution

Les serveurs de Cisco NAC ont été au commencement conçus pour être des appliances d'intrabande. L'utilisation des appliances de Cisco NAC sur une infrastructure réseau de Cisco te permet pour prendre une appliance qui a été conçue pour être intrabande à tout le trafic réseau, et le déploie avec une méthodologie OOB.

L'architecture de solution (voyez que le schéma 2) identifie les composants de la solution et le point principaux d'intégration du serveur de Cisco NAC.

Remarque: Dans ce document, les termes « affilent le commutateur » et le « commutateur d'accès » sont utilisés l'un pour l'autre.

Figure 2 – ***Architecture de solution***

Les sections suivantes décrivent l'accès, la distribution, le noyau, et les couches de centre de traitement des données qui composent une architecture typique de campus.

Couche d'accès

La solution de Cisco NAC de la couche 3 OOB s'applique à une conception campus conduite d'Access. Dans le mode d'accès conduit, les interfaces virtuelles commutées de la couche 3 (SVI) sont configurées sur le commutateur d'accès. Pendant que la figure 3 affiche, l'accès VLAN de la couche 3 (par exemple, VLAN 100) est configuré sur le commutateur de périphérie, posent 3 que le routage est pris en charge du commutateur au commutateur de distribution ou au routeur ascendant, et le gestionnaire de Cisco NAC gère les ports sur le commutateur d'accès.

Figure 3 – ***Commutateurs d'accès avec la couche 3 à la périphérie***

Couche de distribution

La couche de distribution est responsable du routage de la couche 3 et de l'agrégation des Commutateurs de couche d'accès. Tandis que vous pouvez placer les serveurs de Cisco NAC dans cette couche dans une conception de la couche 2 OOB, vous ne les localisez pas ici dans une conception de la couche 3 OOB. Au lieu de cela, placez les serveurs de Cisco NAC centralement au bloc de service de Data Center, comme l'architecture de solution affiche (le schéma 2).

Principale couche

La principale couche utilise les Routeurs basés sur IOS de Cisco. La principale couche est réservée pour le routage ultra-rapide, sans aucun services. Placez les services sur un commutateur de service au centre de traitement des données.

Couche de services de Data Center

La couche de services de centre de traitement des données utilise les Routeurs et les Commutateurs basés sur IOS de Cisco dans le réseau campus. Le gestionnaire de Cisco NAC et le serveur de Cisco NAC sont centralement situés au bloc de service de Data Center dans cette conception de la couche 3 OOB.

Composants de la solution

Gestionnaire de Cisco NAC

Le gestionnaire de Cisco NAC est le serveur de gestion et la base de données qui centralise la configuration et la surveillance de tous les serveurs, utilisateurs, et stratégies de Cisco NAC dans un déploiement d'appareils de Cisco NAC. Pour un déploiement de Cisco NAC OOB, le gestionnaire de Cisco NAC fournit la Gestion OOB afin d'ajouter et des commutateurs de commande dans le domaine du gestionnaire de Cisco NAC et configurer des ports de commutateur.

Serveur de Cisco NAC

Le serveur de Cisco NAC est le point d'application entre le réseau (géré) non approuvé et le réseau (interne) de confiance. Le serveur impose maintient l'ordre défini dans le gestionnaire de Cisco NAC, et les points finaux communiquent avec le serveur pendant l'authentification. Dans cette conception, le serveur sépare logiquement les réseaux non approuvés et de confiance, et elle sert de point centralisé d'application à toutes les Listes d'accès (ACLs) et à limitations de la bande passante pour des périphériques dans le réseau non approuvé. Voyez le pour en savoir plus de section Mode OOB.

Agent de Cisco NAC

L'agent de Cisco NAC est un composant facultatif de la solution de Cisco NAC. Quand l'agent est activé pour votre déploiement de Cisco NAC, il s'assure que les ordinateurs qui accèdent à votre rassemblement de réseau les conditions requises de posture de système vous spécifient. L'agent est un en lecture seule, facile à utiliser, le programme d'encombrement réduit qui réside sur des ordinateurs d'utilisateur. Quand les tentatives d'un utilisateur d'accéder au réseau, l'agent vérifie le système client pour le logiciel vous avez besoin, et vous aidez à saisir n'importe quelles mises à jour ou logiciel manquantes. Voir l'étape 6 : Mettez à jour les stratégies de Cisco.com sur le pour en savoir plus de gestionnaire de Cisco NAC.

Considérations de conception

Quand vous considérez un déploiement de la couche 3 OOB NAC, passez en revue plusieurs considérations de conception. Ces considérations sont répertoriées en ces paragraphes, avec une brève discussion de leur importance.

Mode OOB

Dans le déploiement des appareils OOB de Cisco NAC, le serveur NAC communique avec l'hôte d'extrémité seulement pendant la procédure d'authentification, pose l'estimation, et la correction. Après que l'hôte d'extrémité soit certifié, il ne communique pas avec le serveur.

En mode OOB, le gestionnaire de Cisco NAC utilise des commutateurs de commande de Protocole SNMP (Simple Network Management Protocol) et des affectations de set vlan pour des ports. Quand le Cisco NAC Manager and Server sont installés pour OOB, le gestionnaire peut contrôler les ports de commutateur des Commutateurs pris en charge. Le contrôle des ports de commutateur est connu comme avion de contrôle SNMP. Pour une liste de modèles de commutateur pris en charge, référez-vous à la section de *Commutateurs prise en charge par OOB de* soutien de commutateur d'appliance de Cisco NAC.

Le mode OOB est principalement utilisé pour des déploiements de câble. Quand la méthode de VRF de couche 3 OOB est utilisée, tout le trafic des VLAN (modifiés) non approuvés, y compris le trafic d'agent, atteint le serveur centralisé de Cisco NAC où toute l'application a lieu. L'application du trafic au serveur est un différentiateur principal entre la méthode de VRF et la méthode d'ACL de couche 3 OOB.

Remarque: Le serveur de Cisco NAC a été initialement machiné pour être un périphérique d'intrabande. En d'autres termes, le serveur a été conçu pour faire le traverser tout le trafic, qui permettrait au serveur pour être le point de contrôle. Quand vous utilisez la méthode de VRF de couche 3 OOB, tout le trafic d'utilisateur unauthenticated traverse le serveur exactement comme si c'étaient un déploiement d'intrabande. Cette circulation tient compte d'un environnement cohérent et prévisible.

Classification de point final

Plusieurs facteurs contribuent à la classification de point final, et incluent des types de périphérique et des rôles de l'utilisateur. Le type de périphérique et le rôle de l'utilisateur affectent le rôle de point final.

Ce sont les types de périphérique possibles :

- Périphériques entreprise
- périphériques Non-entreprise
- Périphériques Non-PC

Ce sont les rôles de l'utilisateur possibles :

- Employé
- Sous-traitant
- Invités

Au commencement, tous les points finaux sont assignés au VLAN unauthenticated. Access aux autres rôles est permis après l'identité et le processus de posture est complet.

Rôles de point final

Le rôle de chaque type de point final doit être au commencement déterminé. Un déploiement typique de campus inclut plusieurs rôles, tels que des employés, des invités, des sous-traitants, et d'autres points finaux tels que des imprimantes, des points d'accès sans fil, et des caméras IP.

Des rôles sont tracés au commutateur VLAN de périphérie.

Remarque: Un rôle supplémentaire est exigé pour l'authentification à laquelle tous les points finaux appartiennent au commencement. Ce rôle trace à un VLAN « modifié » unauthenticated.

Isolation de rôle

Pour ce type de conception NAC, le trafic classifié en tant que « modifié » doit circuler dans le côté « non approuvé » du serveur de Cisco NAC. Maintenez ce principe dans l'esprit tandis que vous concevez une implémentation de Cisco NAC. Supplémentaire, ne permettez pas « nettoient » et les réseaux « modifiés » pour communiquer directement les uns avec les autres.

La figure 4 prouve que quand les vrf d'utilisations d'une conception de la couche 3 OOB, le VRF s'assure que les restes unauthenticated du trafic d'isolement dans son propre réseau virtuel. Le serveur de Cisco NAC agit en tant que point d'application ou le contrôleur qui s'assure la ségrégation et la communication protégée entre « nettoient » et les réseaux « modifiés ».

Figure 4 – *Le serveur de Cisco NAC se connecte aux côtés modifiés et propres*

La circulation

Le processus NAC commence quand un point final est connecté à un switchport NAC-géré. Le trafic classifié en tant que « modifié » ou « unauthenticated » est isolé dans le reste des réseaux pendant qu'il est dans le VRF « modifié ». Ce trafic est localisé et envoyé dans l'interface non approuvée sur le serveur de Cisco NAC. Voir la figure 4.

Remarque: L'appliance de Cisco NAC est inconsciente à la façon dont le trafic lui est présenté. En d'autres termes, l'appliance elle-même n'a aucune préférence si le trafic arrive par un tunnel d'Encapsulation de routage générique (GRE) ou est réorienté par une configuration basée sur la politique de routage, Vrf-conduite, ou d'autres méthodes de redirection.

Mode de serveur de Cisco NAC

Vous pouvez déployer un serveur de Cisco NAC dans un de ces deux modes :

- Mode virtuel de passerelle (passerelle)
- Vrai mode de passerelle IP (conduite)

Mode virtuel de passerelle (passerelle)

Le mode virtuel de passerelle (passerelle) est typiquement utilisé quand le serveur de Cisco NAC est la couche 2 à côté des points finaux. En ce mode, le serveur agit en tant que passerelle et n'est pas impliqué dans la décision de routage du trafic réseau.

Remarque: Ce mode s'applique pas applicable pour cette conception particulière d'ACL.

Mode de la passerelle Vrai-IP (conduite)

Le mode de la passerelle vrai-IP (conduite) s'applique dans une conception où le serveur de Cisco NAC est de plusieurs sauts de la couche 3 à partir du point final, tel que la couche 3 OOB. Quand vous utilisez le serveur comme passerelle vrai-IP, spécifiez les adresses IP de ses deux interfaces

: un pour le côté de confiance (administration de serveurs) et un pour le côté (modifié) non approuvé. Les deux adresses doivent être sur des différents sous-réseaux. L'IP non approuvé d'interface est utilisé pour communiquer avec le point final sur le sous-réseau non approuvé. Le mode que ce guide utilise est la passerelle vrai-IP.

Expérience utilisateur (avec l'agent de Cisco NAC)

Typiquement, les entités entreprises ont l'agent de Cisco NAC déployé à l'avance vers les clients d'extrémité. La configuration d'hôte de détection dans l'agent déclenche des paquets de détection à envoyer à l'interface non approuvée du serveur de Cisco NAC, qui continue automatiquement le point final par le processus NAC.

Dans une couche 3 OOB avec le modèle de VRF, l'hôte de détection est typiquement placé pour être le nom DNS ou l'adresse IP du gestionnaire de Cisco NAC. Le gestionnaire existe dans le réseau propre. Puisque tout le trafic des réseaux « modifiés » est conduit par défaut par le serveur de Cisco NAC, les paquets de détection traversent automatiquement le serveur. La circulation décrite ici est l'un des avantages à la méthode de VRF. Cette circulation prévoit une expérience cohérente et prévisible. Voir le pour en savoir plus d'écoulements de processus de Cisco NAC.

Expérience utilisateur (sans agent de Cisco NAC)

La capacité de fonctionner sans agent de Cisco NAC est un autre avantage du modèle de VRF. Tout le trafic des réseaux « modifiés » est conduit naturellement par le serveur de Cisco NAC. Ceci signifie qu'un utilisateur sur un ordinateur sans agent de Cisco NAC seulement doit ouvrir un navigateur Web et parcourir à n'importe quel site Web valide. Les tentatives du trafic de navigateur de traverser le serveur, qui consécutivement capture la session du navigateur et la réoriente à un portail de captif. Voir le pour en savoir plus d'écoulements de processus de Cisco NAC.

Remarque: Pour la meilleure expérience utilisateur possible, Certificats d'utilisation qui sont de confiance par le navigateur de l'utilisateur. des Certificats Auto-générés sur le serveur de Cisco NAC et le gestionnaire de Cisco NAC ne sont pas recommandés pour un environnement de production.

Remarque: Générez toujours le certificat pour le serveur de Cisco NAC avec l'adresse IP de son interface non approuvée.

Écoulements de processus de Cisco NAC

Cette section explique l'écoulement d'opération de base pour une solution NAC OOB. Les scénarios sont des deux décrits avec et sans un agent de Cisco NAC installé sur la machine cliente. Cette section affiche comment le gestionnaire de Cisco NAC contrôle les ports de commutateur utilisant le SNMP comme support de contrôle. Ces écoulements de processus sont macroanalytiques en nature et contiennent seulement les étapes fonctionnelles de décision. Les écoulements de processus n'incluent pas chaque option ou font un pas qui se produit et n'incluent pas les décisions d'autorisation qui sont basées sur des critères d'estimation de point final.

Référez-vous à l'organigramme de processus dans la figure 6 pour les étapes cerclées qui sont dans la figure 5.

Figure 5 – *Écoulement de processus NAC pour la solution de Cisco NAC de la couche 3 OOB*

Figure 6 – *Schéma de bloc d'écoulement de processus de Cisco NAC*

Implémentation de solution de Cisco NAC

Cette section décrit comment implémenter une solution de Cisco NAC.

Topologie

La figure 7 affiche la topologie utilisée pour la création de ce guide. Le réseau interne, qui se compose de VLAN 200 et 210, est conduit à l'aide de la table de routage globale. Le réseau interne n'a aucun VRF associé avec lui.

Le VRF modifié contient seulement le VLAN MODIFIÉ et les réseaux associés de transit qui sont nécessaires afin de créer un réseau virtuel simple pour que tout le trafic modifié circule au côté modifié du serveur centralisé de Cisco NAC.

Le VRF d'invité contient les INVITÉS VLAN et les réseaux associés de transit qui sont nécessaires afin de terminer toutes les données originaires des INVITÉS VLAN sur une sous-interface séparée sur le Pare-feu. Chacun des trois réseaux virtuels (MODIFIÉS, des INVITÉS, et GLOBAL) est porté sur la même infrastructure physique et fournit l'isolation complète du trafic et de chemin.

Figure 7 – *Topologie utilisée de ce guide*

Commande des exécutions

La commande des exécutions pour le déploiement d'une solution de Cisco NAC est facilement pour la discussion. Configurez-vous la partie NAC de la solution avant que le réseau soit préparé ? Ou, préparez-vous le réseau avant que vous configuriez les périphériques de Cisco NAC ?

Aux fins de l'organisation, ce guide se concentre sur la configuration réseau d'abord. Ceci s'assure que le réseau est prêt pour le NAC, puis la configuration des Produits de Cisco NAC.

Configuration du réseau

Ce guide se concentre sur Vrf-Lite de bout en bout pour l'isolation de chemin. Il est important de noter que vous pouvez employer des vrf avec un tunnel GRE afin de permettre l'isolation de chemin par une distribution existante et une principale couche, sans exiger n'importe quelle configuration dans des ces périphériques. Pour plus d'informations sur quand et pourquoi utiliser des tunnels GRE comparés à un VRF de bout en bout concevez, voyez que l'étendre qu'un VRF entre deux périphériques sectionnent. Vous pouvez également se référer à la couche 3 NAC sur le guide de conception de bande qui utilise Vrf-Lite pour la localisation du trafic.

Ce document est un plein guide de conception concentré sur le Vrf-Lite avec la méthode GRE.

Supplémentaire, la pleine commutation de balise peut être utilisée au lieu de Vrf-Lite le cas échéant. La commutation de balise est considérée -de-portée aux fins de ce document.

Importantes considérations pour Vrf-Lite

Remarque: Vrf-Lite est une caractéristique qui te permet de prendre en charge des réseaux deux ou plus virtuels. Vrf-Lite tient compte également des adresses IP superposantes parmi les réseaux virtuels. Cependant, la superposition d'adresse IP n'est pas recommandée pour une

implémentation NAC, parce que tandis que l'infrastructure elle-même prend en charge les adresses superposantes, elle peut créer des complexités de dépannage et l'enregistrement incorrect.

Les détails fournis dans les étapes ont fourni dans ce contour de section les étapes nécessaires afin de configurer votre réseau pour l'isolation de chemin utilisant Vrf-Lite. La configuration exigée pour insérer l'appliance de Cisco NAC dans votre réseau comme passerelle vrai-IP de la couche 3 OOB est également fournie.

Les interfaces d'entrée d'utilisations de Vrf-Lite afin de distinguer des artères pour différents réseaux virtuels et formes séparent des tables de routage virtuel en associant un ou plusieurs interfaces de la couche 3 avec chaque VRF. Les interfaces dans un VRF peuvent être ou examen médical, tel que des ports Ethernet, ou elles peuvent être ou logique, comme des sous-interfaces, des interfaces de tunnel, ou des interfaces virtuelles de commutateur VLAN (SVI).

Remarque: Une interface de la couche 3 ne peut pas appartenir à plus d'un VRF à la fois.

Notez ces considérations de Vrf-Lite :

- Vrf-Lite est localement - significatif seulement au commutateur où il est défini, et à l'adhésion de VRF est déterminé par l'interface d'entrée. Aucune manipulation d'en-tête ou de charge utile de paquet n'est exécutée.
- Un commutateur avec Vrf-Lite est partagé par de plusieurs réseaux virtuels (domaines de sécurité), et tous les domaines de sécurité ont leurs propres seules tables de routage.
- Tous les domaines de sécurité doivent avoir leurs propres VLAN.
- Vrf-Lite ne prend en charge pas tout le Commutation multiprotocole par étiquette (MPLS) - La fonctionnalité de VRF telle que l'échange d'étiquette, la contiguïté du protocole de distribution d'étiquette (LDP), ou les paquets étiquetés qui sont également savent comme balise-commutation).
- La ressource associative ternaire en mémoire de la couche 3 (TCAM) est partagée entre tous les vrf. Afin de s'assurer que n'importe quel un VRF a le suffisamment d'espace associatif de mémoire (CAM), utilisez la commande de **maximum routes**.
- Un commutateur de Catalyst qui utilise Vrf-Lite peut prendre en charge un réseau global et jusqu'à 64 vrf. Le nombre total d'artères prises en charge est limité par la taille du TCAM.
- Vous pouvez utiliser la plupart des protocoles de routage tels que le Protocole BGP (Border Gateway Protocol), le Protocole OSPF (Open Shortest Path First), le Protocole EIGPR (Enhanced Interior Gateway Routing Protocol), le Protocole RIP (Routing Information Protocol), et le routage statique entre les périphériques qui exécutent Vrf-Lite.
- Dans la plupart des cas, il n'y a aucun besoin d'exécuter le BGP avec Vrf-Lite.
- Vrf-Lite n'affecte pas le débit de commutation par paquets.
- Vous ne pouvez pas configurer la Multidiffusion et le Vrf-Lite sur la même chose interface de la couche 3 en même temps.
- Utilisez la commande secondaire de **capability vrf-lite** sous le router ospf quand vous configurez l'OSPF comme protocole de routage entre les périphériques de réseau.

Définissez un VRF

Dans cet exemple de projet, l'isolation de chemin doit être donnée pour les utilisateurs et les invités unauthenticated ou modifiés. On permet au tout autre trafic pour utiliser le réseau interne. Vous devez définir deux vrf pendant que cette configuration affiche :

Exemple de configuration de VRF

```
!--- This command creates a VRF for the DIRTY virtual
network: ! ip vrf DIRTY ! !--- This command names the
VRF and places you into VRF configuration mode: !
description DIRTY_VRF_FOR_NAC ! !--- Gives the VRF a
user friendly description field for documentation ! rd
100:3 ! !--- Creates a VRF table by specifying a route
distinguisher. !--- Enter either an AS number and an
arbitrary number (xxx:y) or an IP !--- address and
arbitrary number (A.B.C.D:y). ! !--- This document uses
the Autonomous System number and a unique router-id in
that AS. !--- This example signifies AS 100:Router-ID 3
!
```

Remarque: Le moteur de distinction de route n'est pas une configuration exigée pour Vrf-Lite. Cependant, c'est considéré une pratique recommandée de configurer le moteur de distinction de route à l'avenir, de sorte que cela fonctionne sans faille avec la commutation de balise.

```
! -- Here we create a VRF for the GUEST Virtual Network: ! ip vrf GUESTSdescription
GUESTS_VRF_FOR_VISITORSrd 600:3 !
```

Associez un VLAN ou une interface avec un VRF

Après que le VRF soit défini sur le commutateur ou le routeur de la couche 3, vous devez associer les interfaces qui vont participer à la configuration de Vrf-Lite avec le VRF où elles appartiennent. Vous pouvez associer l'examen médical ou les interfaces virtuelles avec un VRF. Cette section fournit des exemples d'une interface physique, une sous interface, une interface virtuelle commutée, et une interface de tunnel qui toutes sont associées avec un VRF.

Remarque: Les exemples sont des échantillons seulement, et n'ont pas été utilisés dans la topologie de ce document.

Exemple de configuration d'interface physique

```
interface FastEthernet0/1
ip vrf forwarding GUESTS
!--- Associates the interface with the appropriate VRF
defined in Step 1. ip address 192.168.39.1
255.255.255.252
```

Exemple de configuration de sous-interface

```
interface FastEthernet3/1.10
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
```

Exemple commuté de configuration d'interface virtuelle

```
interface Vlan100
ip vrf forwarding DIRTY
ip address 192.168.100.1 255.255.255.0
```

Exemple de configuration d'interface de tunnel

```
interface Tunnel0
ip vrf forwarding GUESTS
ip address 192.168.38.2 255.255.255.252
tunnel source Loopback0
tunnel destination 192.168.254.1
```

Étendez un périphérique de VRF entre deux périphériques

Il y a plusieurs méthodologies acceptables que vous pouvez employer afin d'étendre un VRF entre deux parties d'infrastructure. Assurez-vous que la méthode que vous choisissez est basée sur ces critères :

- Considérez les capacités de la plate-forme. Tout le Cisco en cours support posent de l'entreprise 3-capable de commutation et de routage Plateformes Vrf-Lite. Ces Plateformes incluent, mais ne sont pas limitées à, 4500, 3750, et 3560 les Plateformes de Catalyst 6500.
- Une plate-forme de routage doit exécuter l'IOS approprié. Les Plateformes incluent, mais ne sont pas limitées à, les 7600, les 3900, le 3800, 2900, 2800, 1900, 1800, et les Routeurs de Services intégrés de gamme 800 (ISR).
- Considérez le nombre de sauts de la couche 3 entre les parties appropriées d'infrastructure. Afin de déterminer le nombre de sauts de la couche 3, maintenez le déploiement aussi simple comme possible. Par exemple, si cinq sauts de la couche 3 existent entre l'infrastructure qui héberge les périphériques de signalisation CAS (Channel Associated Signaling) et les clients, il peut créer des frais d'administration.

Avec la solution incorrecte :

- La jonction de la couche 2 crée une topologie très suboptimale de la couche 2.
- Les sous-interfaces de la couche 3 créent beaucoup d'interfaces supplémentaires pour configurer. Plus d'interfaces à configurer peuvent créer les questions supplémentaires d'adressage IP de temps système et de potentiel de Gestion. Avec la supposition qu'il n'y a aucune Redondance dans l'infrastructure, chaque couche du réseau a un d'entrée et l'interface physique de sortie. Le calcul pour le nombre de subi-nterfaces est alors (2 * nombre de niveaux dans le réseau * nombres de vrf). Notre exemple a deux vrf, ainsi la formule est (2 *5 * 2) ou 20 sous-interfaces. Après que la Redondance soit ajoutée, ce nombre de plus que double. Comparez ceci à l'extension GRE, où seulement quatre interfaces sont exigées avec le même résultat final. Cette comparaison illustre comment GRE réduit l'incidence de configuration.

Jonction de la couche 2

La jonction de la couche 2 est préférée dans les scénarios où les périphériques de couche d'accès ne prennent en charge pas des sous-interfaces. 3750, et 4500 les Plateformes de Catalyst 3560, ne prennent en charge pas des sous-interfaces.

Dans un accès de la couche 3 modèle qui se connecte à une plate-forme qui ne prend en charge pas des sous-interfaces à une plate-forme qui fait, seulement jonction de la couche 2 d'utilisation d'un côté et sous-interfaces d'utilisation de l'autre côté. Cette configuration met à jour tous les avantages d'une architecture de local de la couche 3 et surmonte toujours la limite sans prise en charge de sous-interface sur quelques Plateformes.

Un des avantages principaux de configurer la jonction de la couche 2 de seulement un côté du lien est que le spanning-tree n'est pas introduit de nouveau dans l'environnement de la couche 3. Voyez l'exemple approprié de la configuration 3750 où un commutateur d'accès de 3750. ce qui ne prend en charge pas GRE ou sous-interfaces, est connecté à un commutateur de distribution 6500. Le commutateur de distribution 6500 prend en charge GRE et sous-interfaces.

Configuration 3750 appropriée

Dans cette configuration, la valeur par défaut pour le VLAN INDIGÈNE est VLAN 1 sur FastEthernet 1/0/1. Cette configuration n'a pas été changée. Cependant, on ne permet pas au VLAN 1 pour être trunked à travers le lien. Les VLAN permis sont limités seulement aux VLAN qui sont étiquetés.

Il n'y a aucun besoin de négociation de jonction de commutateur à commutateur ou de trafic de protocole VTP (VLAN Trunk Protocol) dans cette topologie de la couche 3. Par conséquent, il n'y a également aucun besoin de n'importe quel trafic non-marqué d'être transmis sur ce lien. Cette configuration augmente le choix de sécurité de l'architecture parce qu'elle n'ouvre pas les failles de sécurité inutiles de la couche 2.

Exemple approprié de la configuration 3750

```
!--- 3750 Switch configuration, related to connecting it
to a !--- sub-interface capable switch (Catalyst 6500):
! ip vrf DIRTY rd 100:1 ! ip vrf GUEST rd 600:1 !
interface GigabitEthernet1/0/48 description Uplink to
Cat6k switchport trunk encapsulation dot1q switchport
trunk allowed vlan 901-903,906 switchport mode trunk
spanning-tree portfast trunk ! !--- Since the 3750 does
not support sub-interfaces, !--- you must configure one
SVI per transit network: ! interface Vlan901 description
DIRTY_TRANSIT ip vrf forwarding DIRTY ip address
172.26.120.2 255.255.255.252 ! interface Vlan902
description GLOBAL_TRANSIT ip address 172.26.120.6
255.255.255.252 ! interface Vlan906 description
GUEST_TRANSIT ip vrf forwarding GUEST ip address
172.26.120.14 255.255.255.252 ! !--- This configuration
uses EIGRP as the routing protocol !--- of choice in
this document. !--- Each VRF is defined as a separate !-
-- Autonomous System under the Global AS. ! router eigrp
26 ! address-family ipv4 vrf DIRTY network 172.26.120.0
0.0.0.255 autonomous-system 100 no auto-summary exit-
address-family ! address-family ipv4 vrf GUEST
redistribute static network 172.26.120.0 0.0.0.255
autonomous-system 600 no auto-summary exit-address-
family network 172.26.0.0
```

Configuration 6500 appropriée

Dans cette configuration, l'encapsulation dot1q est utilisée afin d'étiqueter les trames avec VLAN 901, 902, et 906. Quand vous sélectionnez les balises VLAN pour utiliser sur une sous-interface, vous ne pouvez pas utiliser un nombre VLAN qui est déjà défini localement dans la base de données VLAN sur le commutateur.

Exemple approprié de la configuration 6500

```
!--- 6500 Switch configuration, related to connecting it
!--- to a non-sub-interface capable switch (Catalyst
3750): ! ip vrf DIRTY rd 100:26 ! ip vrf GUEST rd 600:26
! interface FastEthernet1/34 description NAC LAB - 3750
no ip address ! interface FastEthernet1/34.901
encapsulation dot1Q 901 ip vrf forwarding DIRTY ip
address 172.26.120.1 255.255.255.252 ! interface
FastEthernet1/34.902 encapsulation dot1Q 902 ip address
172.26.120.5 255.255.255.252 ! interface
FastEthernet1/34.906 encapsulation dot1Q 906 ip vrf
forwarding GUEST ip address 172.26.120.13
```

```
255.255.255.252 ! !--- EIGRP is the routing protocol of
choice in this document. !--- Each VRF is defined as a
!--- separate Autonomous System under the Global AS. !--
- See Configure Routing for the VRF for more
information. ! router eigrp 26 network 172.26.0.0
0.0.255.255 no auto-summary passive-interface Vlan1
redistribute static ! address-family ipv4 vrf DIRTY
autonomous-system 100 network 172.26.120.0 0.0.0.3
network 172.26.160.0 0.0.0.255 no auto-summary no
default-information out redistribute static route-map
gw-route exit-address-family ! address-family ipv4 vrf
GUEST redistribute static network 172.26.120.0 0.0.0.255
autonomous-system 600 no auto-summary exit-address-
family !
```

Configurez le routage pour le VRF

Comme discuté plus tôt dans les importantes considérations pour la section d'utilisation Vrf-Lite, Vrf-Lite prend en charge le BGP, l'OSPF, et l'EIGRP. Dans cet exemple de configuration, l'EIGRP est sélectionné parce que c'est le protocole de routage que Cisco recommande pour l'implémentation sur des réseaux campus où la convergence rapide est exigée.

Remarque: L'OSPF fonctionne aussi bien avec Vrf-Lite, de même que fait BGP.

Remarque: Le BGP est exigé si la conception exige que le trafic « soit coulé » entre les vrf.

Routage pour un VRF avec l'exemple de configuration EIGRP

```
!
!--- This base routing protocol configuration handles
the routing !--- for the Global Routing Table. ! router
eigrp 26 network 172.26.50.0 0.0.0.255 network
172.26.51.0 0.0.0.255 network 172.26.52.0 0.0.0.255
network 172.26.55.0 0.0.0.255 network 172.26.60.0
0.0.0.255 network 172.26.61.0 0.0.0.255 network
172.26.62.0 0.0.0.255 network 172.26.120.4 0.0.0.3
network 172.26.176.0 0.0.0.255 network 172.26.254.1
0.0.0.0 no auto-summary passive-interface Vlan1
redistribute static ! !--- You must define an address
family for each VRF !--- that is to be routing using the
routing protocol. !--- Routing protocol options such as
auto-summarization, !--- AS number, and router id are
all configured under the !--- address family. EIGRP does
not form a neighbor !--- relationship without the AS
specified under the address family. !--- Also, this AS
number needs to be unique for !--- each VRF and cannot
be the same as the global AS number. ! address-family
ipv4 vrf DIRTY autonomous-system 100 network
172.26.120.0 0.0.0.3 network 172.26.160.0 0.0.0.255 no
auto-summary no default-information out redistribute
static route-map gw-route exit-address-family ! address-
family ipv4 vrf GUEST redistribute static network
172.26.120.0 0.0.0.255 autonomous-system 600 no auto-
summary exit-address-family !
```

Le trafic d'artère entre le Tableau de routage global et le VRF modifié

Selon les conditions requises de déploiement NAC, il peut être nécessaire de passer le trafic du

côté non approuvé ou modifié du réseau à la faire confiance ou de nettoyer le côté du réseau. Par exemple, les services de correction peuvent potentiellement vivant du côté de confiance de l'appliance de Cisco NAC. Dans le cas des déploiements simples d'ouverture de session de Répertoire actif, il est nécessaire de passer un sous-ensemble du trafic au Répertoire actif afin de permettre l'échange interactif de ticket Kerberos de connexions, et ainsi de suite.

Quoi qu'il arrive, il est très important que la table de routage globale sache atteindre le VRF modifié, et que le VRF modifié sait atteindre la table de routage globale si n'importe quelles données doivent passer entre les deux. Ceci est typiquement manipulé par la méthodologie dans la figure 8.

Le VRF modifié se transfère sur l'interface non approuvée ou modifiée de l'appliance de Cisco NAC. Le global a les artères statiques seulement aux sous-réseaux qui sont considérés des VLAN modifiés. Ces artères de charge statique indiquent l'interface (de confiance) propre du serveur de Cisco NAC comme prochain saut.

Figure 8 – *Acheminement des écoulements*

Le premier saut de la couche 3 du côté non approuvé ou modifié de l'appliance de Cisco NAC redistribue un default route dans un processus de routage ces points à l'appliance de Cisco NAC. Le premier saut de la couche 3 du côté de confiance ou propre de l'appliance de Cisco NAC redistribue une artère statique pour les sous-réseaux qui appartiennent au VLAN modifié dans la couche d'accès (dans ce cas 172.26.123.0/26).

Remarque: Le premier saut de la couche 3 des bords opposés de l'appliance de Cisco NAC peut être sur le même périphérique physique, mais dans différents vrf.

Remarque: Dans la topologie utilisée pour ce document, le côté non approuvé ou modifié du serveur de Cisco NAC est dans un VRF, alors que le côté de confiance ou propre de l'appliance de Cisco NAC demeure dans la table globale de routage. Cependant, les deux interfaces sont connectées au même contact central de centre de traitement des données.

Exemple de configuration de la couche 3 OOB Vrf-Lite de Cisco NAC

Afin de déployer avec succès une solution du Cisco NAC OOB, vous devez configurer les composants NAC afin d'apparier l'architecture désirée. La figure 9 est un diagramme de réseau logique du Cisco NAC OOB de la couche 3 qui est utilisé dans cette section afin d'afficher la configuration appropriée du gestionnaire de Cisco NAC, du serveur de Cisco NAC, et du commutateur de périphérie pour une couche NAC 3 OOB avec le déploiement de Vrf-Lite.

Figure 9 – *Topologie logique de la couche 3 OOB de Cisco NAC*

Terminez-vous les étapes dans ces sections afin de configurer un déploiement de Cisco NAC de VRF vrai-IP OOB de la couche 3 :

Étape 1 : Configurez le commutateur de périphérie

Comme ces exemples de configuration affichent, créez deux VLAN supplémentaires (MODIFIÉS et INVITÉ) sur le commutateur de périphérie.

La production existante VLAN (VLAN 200) est utilisée pour tous les systèmes entreprise. Cet exemple crée les VLAN, leurs réseaux associés de transit, et assigne chacun des deux aux vrf

corrects. L'application a lieu au serveur de Cisco NAC, ainsi vous n'avez pas besoin de s'appliquer ACLs à chaque VLAN sur le commutateur.

Rôle Unauthenticated : VLAN 100, exemple modifié de configuration de VRF
`!--- Define the DIRTY VRF.` ip vrf DIRTY rd 100:3 `!--- Create the SVI for the DIRTY VLAN.` interface Vlan100 ip vrf forwarding DIRTY ip address 172.26.123.1 255.255.255.224 ip helper-address vrf DIRTY 172.26.51.11 `!--- Create the SVI for the DIRTY_TRANSIT_NETWORK.` interface Vlan301 ip vrf forwarding DIRTY ip address 172.26.120.50 255.255.255.252 `!--- Set the allowed VLAN on the trunk.` interface FastEthernet1/0/48 switchport trunk allowed vlan add 301 `!--- Set up the routing for the VRF.` router eigrp 26 address-family ipv4 vrf DIRTY network 172.26.0.0 autonomous-system 100 no auto-summary exit-address-family
Rôle d'invité : VLAN 600, exemple de configuration de VRF d'INVITÉ
`!--- Define the GUEST VRF.` ip vrf GUEST rd 600:3 `!--- Create the SVI for the GUEST VLAN.` interface Vlan600 ip vrf forwarding GUEST ip address 172.26.123.193 255.255.255.224 `!--- Create the SVI for the DIRTY_TRANSIT_NETWORK.` interface Vlan306 ip vrf forwarding GUEST ip address 172.26.120.62 255.255.255.252 `!--- Set the allowed VLAN on the trunk.` interface FastEthernet1/0/48 switchport trunk allowed vlan add 306 `!--- Set up the routing for the VRF.` router eigrp 26 address-family ipv4 vrf GUEST network 172.26.0.0 autonomous-system 600 no auto-summary exit-address-family

Étape 2 : Configurez le principal commutateur

Les exemples de configuration dans cette section affichent la simulation d'un noyau réduit avec un commutateur du Catalyst 3750-E. Dans la plupart des environnements, ce n'est pas un commutateur de périphérie-classe. Cependant, le commutateur a été établi dans l'environnement de travaux pratiques utilisé pour ce document.

Créez quatre VLAN supplémentaires pour des réseaux de transit, deux pour le VLAN MODIFIÉ et deux pour l'INVITÉ VLAN. Voir la figure 10.

- VLAN MODIFIÉVLAN 301 MODIFIÉ de la périphérie à creuserVLAN 901 MODIFIÉ du noyau au centre de traitement des données
- INVITÉ VLANINVITÉ VLAN 306 de la périphérie à creuserINVITÉ VLAN 906 de noyau au centre de traitement des données

Un transit network est établi de la périphérie au noyau, et d'une seconde pour le noyau au centre de traitement des données. Les réseaux de transit doivent être terminés afin des vrf MODIFIÉS et d'INVITÉ. Si la commutation de balise est activée au lieu de Vrf-Lite, ce n'est pas nécessaire.

Remarque: Ce document se concentre sur Vrf-Lite, et la commutation de balise est considérée - de-portée.

Figure 10 – *Réseaux de transit*

: :

VLAN 301 MODIFIÉ de la périphérie à creuser ; VLAN 901 MODIFIÉ du noyau à l'exemple de configuration de Data Center
!--- This is the core switch. !--- Define the DIRTY VRF. ip vrf DIRTY rd 100:1 *!--- Create the SVI for the DIRTY VLANs.* interface Vlan301 desc This is the Transit Network between the Edge & Core ip vrf forwarding DIRTY ip address 172.26.120.49 255.255.255.252 interface Vlan901 desc This is the Transit Network between the Core and the DC ip vrf forwarding DIRTY ip address 172.26.120.2 255.255.255.252 *!--- Set the allowed VLAN on the trunks.* interface GigabitEthernet1/0/3 switchport trunk allowed vlan add 301 interface GigabitEthernet1/0/48 switchport trunk allowed vlan add 901 *!--- Set up the routing for the VRF.* router eigrp 26 address-family ipv4 vrf DIRTY network 172.26.0.0 autonomous-system 100 no auto-summary exit-address-family exit-address-family

INVITÉ VLAN 306 de la périphérie à creuser ; INVITÉ VLAN 906 de noyau à l'exemple de configuration de Data Center
!--- This is the core switch. ! *!--- Define the GUEST VRF.* ip vrf GUEST rd 600:1 *!--- Create the SVI for the GUEST VLANS.* interface Vlan306 desc This is the transit network between the Edge & Core ip vrf forwarding GUEST ip address 172.26.120.61 255.255.255.252 interface Vlan906 description Transit Network between Core & DC ip vrf forwarding GUEST ip address 172.26.120.14 255.255.255.252 *!--- Set the allowed VLAN on the trunks.* interface GigabitEthernet1/0/3 switchport trunk allowed vlan add 306 interface GigabitEthernet1/0/48 switchport trunk allowed vlan add 906 *!--- Set up the routing for the VRF.* router eigrp 26 address-family ipv4 vrf GUEST network 172.26.0.0 autonomous-system 600 no auto-summary exit-address-family

Étape 3 : Configurez le commutateur de Data Center

Pendant que l'exemple de configuration affiche, le serveur de Cisco NAC a les deux interfaces connectées au même contact central de centre de traitement des données 6500. L'interface de confiance est dans VLAN 60, et l'interface non approuvée est dans VLAN 160, qui est dans le VRF MODIFIÉ.

1. Créez quatre VLAN supplémentaires pour la connexion au noyau :Un VLAN modifié (160)Un VLAN propre (60)Un transit network modifié (901)Un transit network propre (906)Ajoutez le VLAN MODIFIÉ au VRF MODIFIÉ.Terminez le VRF d'INVITÉ dans un INVITÉ DMZ (999) ce des utilisations un Pare-feu de Cisco ASA (hors de la place pour ce document) afin de connecter des utilisateurs d'invité à l'Internet et remplir des fonctions de Traduction d'adresses de réseau (NAT).
2. Créez les sous-interfaces MODIFIÉES et d'INVITÉ de transit.Les commandes affichées dans l'exemple de configuration de commutateur de Data Center effectuent ces tâches :Définissez

les vrf MODIFIÉS et d'INVITÉ.Créez les réseaux MODIFIÉS et PROPRES pour le serveur de Cisco NAC.

Exemple de configuration de commutateur de Data Center

```
!--- Define the DIRTY and GUEST VRFs. ip vrf DIRTY rd
100:26 ip vrf GUEST rd 600:26 !--- Create the sub-
interface and switched virtual interface (SVI) !--- for
the DIRTY and GUEST VLANs. interface
FastEthernet1/34.901 desc Transit Network from Core to
DC for DIRTY traffic encapsulation dot1Q 901 ip vrf
forwarding DIRTY ip address 172.26.120.1 255.255.255.252
interface FastEthernet1/34.906 desc Transit Network from
Core to DC for GUEST traffic encapsulation dot1Q 906 ip
vrf forwarding GUEST ip address 172.26.120.13
255.255.255.252 interface Vlan60 desc Trusted (CLEAN)
side of the NAC Server ip address 172.26.60.1
255.255.255.0 interface Vlan160 desc Untrusted (DIRTY)
side of the NAC Server ip vrf forwarding DIRTY ip
address 172.26.160.1 255.255.255.0 interface Vlan999
description GUEST VLAN SVI ip vrf forwarding GUEST ip
address 192.168.26.254 255.255.255.0 !--- Set up the
routing for the VRFs. router eigrp 26 network
172.26.60.0 0.0.0.255 no auto-summary redistribute
static address-family ipv4 vrf DIRTY autonomous-system
100 network 172.26.120.0 0.0.0.3 network 172.26.160.0
0.0.0.255 no auto-summary redistribute static exit-
address-family address-family ipv4 vrf GUEST network
172.26.0.0 network 192.168.26.0 autonomous-system 600 no
auto-summary redistribute static exit-address-family !--
- Set up the static routes for redistribution for the
VRFs. ip route 172.26.123.0 255.255.255.192 172.26.60.2
ip route vrf DIRTY 0.0.0.0 0.0.0.0 172.26.160.2 ip route
vrf GUEST 0.0.0.0 0.0.0.0 192.168.26.1
```

Étape 4 : Exécutez la première installation du Cisco NAC Manager and Server

L'installation de Cisco NAC Manager and Server est exécutée par l'accès de console. L'installer de service vous guide par la configuration initiale pour le gestionnaire et le serveur. Allez à installer Clean Access Manager et Clean Access Server afin d'exécuter la première installation.

Étape 5 : Appliquez un permis au gestionnaire de Cisco NAC

Après que vous exécutiez la première installation par la console, accédez au GUI de gestionnaire de Cisco NAC afin de continuer de configurer le Cisco NAC Manager and Server. Téléchargez d'abord les permis de gestionnaire et de serveur qui ont été livré avec les appliances. Pour plus d'informations sur la façon télécharger les permis, allez à *Access la* section de *console Web de CAM d'*installer Clean Access Manager et Clean Access Server.

Remarque: Tous les permis de Cisco NAC Manager and Server sont basés sur l'adresse MAC eth0 du gestionnaire. Dans une installation de Basculement, les permis sont basés sur l'adresse MAC eth0 des gestionnaires primaires et secondaires de Cisco NAC.

Étape 6 : Stratégies de mise à jour de Cisco.com sur le gestionnaire de Cisco NAC

Le gestionnaire de Cisco NAC doit être configuré afin de récupérer des mises à jour régulières du serveur central de mise à jour situé à Cisco. La liste des produits prise en charge par appliance du Cisco NAC AV/AS est un fichier XML versioned distribué d'un serveur centralisé de mise à jour qui fournit la matrice la plus en cours des constructeurs pris en charge d'antivirus et d'antispyware et des versions du produit utilisées pour configurer des règles d'antivirus ou d'antispyware et des conditions requises de mise à jour de définition d'antivirus ou d'antispyware pour l'estimation et la correction de posture. Cette liste est mise à jour régulièrement pour l'antivirus et les Produits et les versions d'antispyware pris en charge dans chaque agent de Cisco NAC sortent et incluent des produits nouveaux pour de nouvelles versions d'agent. La liste fournit les informations de version seulement. Quand le gestionnaire de Cisco NAC télécharge la liste des produits prise en charge d'antivirus et d'antispyware, elle télécharge les informations sur ce que sont les dernières versions pour des Produits d'antivirus et d'antispyware. Il ne télécharge pas les fichiers de correctif réels ou les fichiers de définition de virus. Basé sur ces informations, l'agent peut alors déclencher l'application indigène d'antivirus ou d'antispyware afin d'exécuter des mises à jour. Pour plus d'informations sur la façon dont des mises à jour sont récupérées, allez à la *connexion de l'agent d'exigence pour la* section de *machines cliente de* configurer l'appliance de Cisco NAC pour l'estimation de posture de connexion de l'agent et de client.

Étape 7 : Installez les Certificats d'un tiers Autorité de certification (CA)

Pendant l'installation, le script d'utilitaire de configuration pour le gestionnaire de Cisco NAC et le serveur de Cisco NAC exige de vous de générer un certificat ssl provisoire. Pour l'environnement de travaux pratiques, vous pouvez continuer à utiliser les Certificats auto-signés. Cependant, ils ne sont pas recommandés pour un réseau de production.

Pour plus d'informations sur installer des Certificats sur le gestionnaire de Cisco NAC d'une tierce partie CA, allez à l'*heure système de positionnement* et aux sections *d'accès direct de console Web de Clean Access Server de* gérer le CAM.

Remarque: Si vous utilisez les Certificats d'auto-signe dans l'environnement de travaux pratiques, le gestionnaire de Cisco NAC et le serveur de Cisco NAC chaque besoin de faire confiance au certificat de l'autre. Ceci exige que vous téléchargez les Certificats pour chacun des deux en tant qu'autorité de certification de confiance sous **SSL** > les **autorités de certification de confiance**.

Étape 8 : Configuration du serveur de Cisco NAC d'examen

La plupart de chose importante à se souvenir pour une conception réussie NAC est que le trafic classifié en tant qu'écoulement modifié de nécessité dans le côté non approuvé du serveur NAC, comme figure 11 affiche :

Figure 11 – ***Déploiement de serveur de Cisco NAC***

Étape 9 : Ajoutez le serveur de Cisco NAC au gestionnaire de Cisco NAC

Terminez-vous ces étapes afin d'ajouter le serveur de Cisco NAC au gestionnaire de Cisco NAC :

1. **Serveurs de CCA de** clic sous le volet de Gestion de périphériques. Voir la figure 12.
2. Cliquez sur le nouvel onglet de serveur.
3. Utilisez la case d'adresse IP du serveur afin d'ajouter l'adresse IP de l'interface de confiance du serveur de Cisco NAC.
4. Dans la case d'emplacement de serveur, présentez le **serveur de Cisco NAC OOB** comme emplacement de serveur.

5. Choisissez la Vrai-IP-**passerelle hors bande de la** liste déroulante de type de serveur.
6. Cliquez sur Add **Clean Access Server**.

Figure 12 – ***Ajouter le serveur de Cisco NAC au gestionnaire de Cisco NAC***

Remarque: Le gestionnaire de Cisco NAC et le serveur de Cisco NAC doivent faire confiance au CA de chacun pour que le gestionnaire ajoute avec succès le serveur.

Après que vous ajoutiez le serveur de Cisco NAC, il apparaît dans la liste sous la liste d'onglet de serveurs. Voir la figure 13.

Étape 10 : Configurez le serveur de Cisco NAC

Terminez-vous ces étapes afin de configurer le serveur de Cisco NAC :

1. Cliquez sur la liste d'onglet de serveurs.
2. Cliquez sur l'icône de gérer pour le serveur de Cisco NAC afin de continuer la configuration.

Figure 13 – ***Serveur de Cisco NAC géré par le gestionnaire de Cisco NAC***

Après que vous cliquiez sur le graphisme de gérer, l'écran affiché dans la figure 14 apparaît.

Étape 11 : Support de la couche 3 d'enable

Terminez-vous ces étapes afin d'activer le support de la couche 3 :

1. Sélectionnez l'onglet de réseau.
2. Vérifiez la case à cocher de **support de l'enable L3**.
3. Vérifiez le **mode strict de l'enable L3 pour bloquer les périphériques NAT avec la** case à cocher d'**agent NAC**.
4. Cliquez sur **Update**.
5. Redémarrez le serveur de Cisco NAC comme instruit.

Figure 14 – ***Détails de réseau serveur de Cisco NAC***

Remarque: Générez toujours le certificat pour le serveur de Cisco NAC avec l'adresse IP de son interface non approuvée. Pour un certificat basé sur nom, les besoins de nom de résoudre à l'adresse IP non approuvée d'interface. Quand le point final communique avec l'interface non approuvée du serveur afin de commencer le processus NAC, le serveur réoriente l'utilisateur à l'adresse Internet de certificat ou à l'IP. Si le certificat indique l'interface de confiance, le processus de procédure de connexion ne fonctionne pas correctement.

Étape 12 : Configurez les artères statiques

Terminez-vous ces étapes afin de configurer les artères statiques :

1. Après que les réinitialisations de serveur de Cisco NAC, reviennent au serveur et continuent la configuration.Le serveur de Cisco NAC doit employer l'interface non approuvée afin de communiquer avec des points d'extrémité sur le VLAN unauthenticated.
2. **Artères avancées > statiques** choisies afin d'ajouter des artères au VLAN unauthenticated.
3. Complétez les sous-réseaux appropriés pour les VLAN unauthenticated.
4. Cliquez sur Add l'**artère**.

5. **Interface non approuvée** choisie **[eth1]** pour ces derniers artères.

Figure 15 – *Ajoutez une artère statique pour atteindre le sous-réseau de l'utilisateur ONU-authentifié*

Étape 13 : Profils d'installation pour des Commutateurs dans le gestionnaire de Cisco NAC

Terminez-vous ces étapes afin d'installer des profils pour des Commutateurs dans le gestionnaire de Cisco NAC :

1. **La Gestion** choisie **OOB > profile > périphérique > éditent**.
2. Complétez les informations de profil de périphérique. Figure 16 d'utilisation comme guide.Chaque commutateur est associé avec un profil. Ajoutez un profil pour chaque type de commutateur de périphérie que le gestionnaire de Cisco NAC gèrera. Dans cet exemple, un commutateur 3750 est géré.**Figure 16 – *Profil SNMP utilisé pour gérer le commutateur***
3. Installez la configuration de commutateur pour le SNMP.Configurez le commutateur de périphérie pour les mêmes chaînes lecture/écriture de la communauté SNMP qui sont configurées sur le gestionnaire de Cisco NAC.`snmp-server community Cisco123 RO`
`snmp-server community Cisco1234 RW`
4. **Gestion** choisie **> profils > port OOB > nouveau**. Voir la figure 17.Pour le contrôle de port individuel, configurez un profil de port sous la **Gestion >** les **profils >** le **port OOB** qui inclut l'accès unauthenticated par défaut VLAN VLAN et de par défaut. Dans la partie VLAN d'accès, spécifiez le rôle de l'utilisateur VLAN utilisant Access VLAN déroulant. Le gestionnaire de Cisco NAC change le VLAN unauthenticated à l'accès VLAN basé sur le VLAN défini dans le rôle où l'utilisateur appartient.Définissez le profil de port afin de contrôler le VLAN du port basé sur les rôles de l'utilisateur et les VLAN mis en application.Le VLAN authentique est le VLAN UNAUTHENTICATED (VLAN 17) auquel des périphériques unauthenticated sont au commencement assignés.Access par défaut VLAN est les EMPLOYÉS VLAN (VLAN 14). Ce VLAN est utilisé si l'utilisateur authentifié ne fait pas définir un VLAN basé sur rôle.Access VLAN peut ignorer le par défaut VLAN à un rôle de l'utilisateur VLAN, qui est défini sous le rôle de l'utilisateur. Pour plus d'informations sur des rôles de l'utilisateur d'établissement, voir l'étape 17 : Configurez les rôles de l'utilisateur. Des mappages de LDAP peuvent être utilisés afin de tracer des rôles de l'utilisateur dans le NAC aux groupes de LDAP. Le pour en savoir plus, se rapportent à NAC(CCA) 4.x : Utilisateurs de carte à certains rôles utilisant l'exemple de configuration de LDAP.**Figure 17 – *Profil de port pour gérer le port de commutateur*** **Remarque:** Vous pouvez également définir des noms VLAN au lieu des id. Si vous définissez des noms VLAN, vous pouvez avoir des IDs de VLAN sur différents Commutateurs à travers le campus. Cependant, le même nom VLAN est relié à un rôle particulier.Les options supplémentaires sont disponibles sous le profil de port pour la release IP et renouvellent des options. Faites descendre l'écran la page affichée dedans afin de voir ces options.Si l'utilisateur est derrière un téléphone IP, décochez le **rebond le port après que le VLAN soit** case à cocher **changée**. Si ceci est vérifié, il peut probablement redémarrer le téléphone IP quand le port est rebondi.**Figure 18 – *Profil de dessous disponible de port de diverses options***

Étape 14 : Configurez les configurations de récepteur SNMP

En plus d'installer la chaîne de caractères de la communauté SNMP pour la lecture/écriture, vous

devez également configurer le gestionnaire de Cisco NAC afin de recevoir des déroutements SNMP du commutateur. Ces déroutements sont envoyés quand l'utilisateur se connecte et des démonter du port. Quand le serveur de Cisco NAC envoie les informations d'adresse IP MAC/d'un point final particulier au gestionnaire, le gestionnaire peut construire une table de mappage intérieurement pour le MAC/IP et le port de commutateur.

1. **La Gestion** choisie **OOB > profile > récepteur SNMP**.
2. Configurez les configurations de déroutement SNMP comme cette figure affiche :**Figure 19 – *La configuration de récepteur SNMP de gestionnaire de Cisco NAC pour collecter des déroutements SNMP et informe***
3. Afin de configurer les positions de commutateur pour des déroutements SNMP, augmentez le compteur d'annulation de Clean Access Manager de commutateur par défaut (CAM) à 1 heure par recommandations de pratique recommandée Cisco pour NAC OOB. L'échantillon CLI affiche l'ensemble de paramètres de `mac-address-table aging-time à` 3600.L'établissement du temporisateur à 1 heure ramène la fréquence des notifications de MAC envoyées hors déjà des périphériques connectés au gestionnaire de Cisco NAC. Employez la commande de **déroutement de source** afin de spécifier l'adresse source qui est utilisée pour envoyer les déroutements.Sur option, configurez les déroutements de lien et de linkdown afin d'envoyer au gestionnaire de Cisco NAC (non affiché dans l'échantillon CLI). Ces déroutements sont utilisés seulement dans un scénario de déploiement où les hôtes d'extrémité ne sont pas connectés derrière un téléphone IP.**Remarque:** Des snmps inform sont recommandés parce qu'ils sont plus fiables que les déroutements SNMP. En outre, considérez le Qualité de service (QoS) pour le SNMP dans un environnement de réseau du trafic élevé.

Étape 15 : Ajoutez les Commutateurs comme périphériques dans le gestionnaire de Cisco NAC

Terminez-vous ces étapes afin d'ajouter des Commutateurs comme périphériques dans le gestionnaire de Cisco NAC :

1. **Gestion** choisie **> périphériques > périphériques OOB > nouveau**.Utilisez le profil de commutateur créé dans l'étape 13 afin d'ajouter le commutateur.
2. Sous le profil de périphérique, utilisez le profil que vous avez créé. Ne changez pas la valeur par défaut de profil de port quand vous ajoutez le commutateur.**Figure 20 – *Ajoutez le commutateur de périphérie dans le gestionnaire de Cisco NAC pour contrôler par l'intermédiaire du SNMP***
3. Après que le commutateur soit ajouté au gestionnaire de Cisco NAC, vous pouvez sélectionner les ports que vous voulez gérer.

Étape 16 : Configurez les ports de commutateur pour que les périphériques soient gérés par NAC

Terminez-vous ces étapes afin de configurer les ports de commutateur pour que les périphériques soient gérés par NAC.

1. **Gestion OOB > commutateur de périphériques** choisis **[adresse IP] > ports > liste** afin de voir les ports de commutateur disponibles que vous pouvez gérer.**Figure 21 – *Sélection de***

contrôle de port disponible pour un commutateur géré **Remarque:** Ne laissez pas le profil par défaut en tant que « incontrôlé » jusqu'à ce que vous puissiez marquer les interfaces appropriées statiquement en tant que « incontrôlé ». Après les ports uplinks, et tous les autres ports marche-arrêt qui doivent rester incontrôlés sont placés ; changez alors le par défaut à votre profil commandé de port. Le manque de faire ainsi dans cette commande peut avoir comme conséquence des résultats moins que desirables.
2. **La Gestion OOB >** le **commutateur de périphériques** choisis **[adresse IP] >** des **ports > parviennent** afin de gérer plusieurs ports immédiatement.

Figure 22 – *Gérez les plusieurs ports avec l'option de joindre*

Étape 17 : Configurez les rôles de l'utilisateur

Dans cet exemple, les VLAN qui correspondent à chaque rôle sont déjà créés dans le commutateur de périphérie.

1. **La gestion des utilisateurs >** les **rôles de l'utilisateur** choisis **> éditent le rôle** et créent un rôle des employés pendant que cette figure affiche :**Figure 23 –** *Créez un rôle des employés et tracez les DONNÉES VLAN*
2. **La gestion des utilisateurs >** les **rôles de l'utilisateur** choisis **> éditent le rôle** et créent un rôle d'invité pendant que cette figure affiche :**Figure 24 –** *Créez un rôle d'invité et tracez l'INVITÉ VLAN*

Étape 18 : Ajoutez les utilisateurs et les assignez pour s'approprier le rôle de l'utilisateur

Dans un campus universitaire, vous intègrerez avec un serveur d'authentification externe et tracerez l'utilisateur à un rôle particulier au moyen de l'attribut de LDAP. Cet exemple utilise un utilisateur local et des associés cet utilisateur local avec un rôle.

Étape 19 : Personnalisez la page d'ouverture de session utilisateur pour la procédure de connexion de Web

Une page de connexion par défaut est déjà créée dans le gestionnaire de Cisco NAC. Vous pouvez sur option personnaliser la page de connexion afin de changer l'apparence du portail web. Pour une solution de la couche 3 OOB NAC, vous devez télécharger le composant d'ActiveX ou de Javas au client d'extrémité afin d'effectuer ces tâches :

- Cherchez l'adresse MAC de la machine cliente.
- Effectuez la release d'adresse IP et la renouvelez.

1. **Gestion > pages utilisateur** choisies.
2. Éditez la page afin d'activer les options comme cette figure affiche :

Figure 25 – *Mises en page d'utilisateur pour la procédure de connexion de Web*

Étape 20 : Personnalisez l'agent de Cisco NAC pour les rôles de l'utilisateur

Terminez-vous ces étapes afin de personnaliser l'agent de Cisco NAC pour des rôles de l'utilisateur :

1. **Gestion de périphériques** choisie > **Clean Access > configuration générale > connexion de l'agent**.Vous pouvez configurer le gestionnaire de Cisco NAC afin de rendre l'agent obligatoire pour n'importe quel rôle de l'utilisateur. Dans cet exemple, l'agent est obligatoire pour le rôle des employés. Les rôles de sous-traitant et d'invité doivent utiliser la procédure de connexion de Web.
2. Vérifiez l'**utilisation d'exigence de la** case à cocher d'**agent**.

Figure 26 – ***Connexion de l'agent requise pour le rôle des employés***

Étape 21 : Distribuez l'hôte de détection pour l'agent de Cisco NAC

La distribution de logiciel agent de Cisco NAC, l'installation, et la configuration sont couvertes dedans configurent l'appliance de Cisco NAC pour l'estimation de posture de connexion de l'agent et de client. Cet exemple configure l'hôte de détection sur le gestionnaire de Cisco NAC.

Gestion de périphériques choisie > **Clean Access > Clean Access Agent > installation** :

Figure 27 – ***Découvrez le serveur pour un agent de Cisco NAC***

Le champ Host de détection pré-est rempli si l'agent de Cisco NAC est téléchargé du serveur de Cisco NAC. Voir la figure 27.

Remarque: Dans une couche 3 OOB avec le modèle de VRF, l'hôte de détection est typiquement placé pour être le nom DNS ou l'adresse IP du gestionnaire de Cisco NAC, qui existe dans le réseau propre. Puisque tout le trafic des réseaux « modifiés » est conduit par défaut par le serveur de Cisco NAC, les paquets de détection traversent automatiquement le serveur. La circulation décrite ici est l'un des avantages à la méthode de VRF. Il prévoit une expérience cohérente et prévisible. Voir le pour en savoir plus d'écoulements de processus de Cisco NAC.

Étape 22 : Procédure de connexion de Web

Terminez-vous ces étapes afin d'ouvrir une session par le Web :

1. Connectez la machine cliente utilisant un des ports de périphérie contrôlés par le gestionnaire de Cisco NAC.La machine cliente est placée dans le VLAN unauthenticated. Assurez-vous que l'ordinateur reçoit une adresse IP du sous-réseau unauthenticated VLAN.
2. Ouvrez le navigateur afin d'exécuter la procédure de connexion.La supposition est que cette machine cliente n'a pas un agent de Cisco NAC déjà installé. Si toutes les entrées DNS sont réorientées à l'interface non approuvée du serveur de Cisco NAC, de navigateur les redirect to automatiquement une page de connexion. S'il ne fait pas, aller à un URL de particularité tel que guest.nac.local afin d'exécuter la procédure de connexion :

Figure 28 – ***Page Web Login***

Étape 23 : Connexion de l'agent

Vous pouvez distribuer l'agent de Cisco NAC juste comme n'importe quelle autre application logicielle aux utilisateurs finaux ou vous pouvez la forcer utilisant le serveur de Cisco NAC.

Remarque: Plus d'informations détaillées sur la distribution et l'installation d'agent sont disponibles dans l'appliance de Cisco NAC - guide de configuration de Clean Access Manager.

Cette figure affiche l'écran qui apparaît quand l'agent est lancé :

Figure 29 – *Connexion de l'agent*

1. Sélectionnez le serveur de la liste déroulante de serveur.
2. Écrivez le nom d'utilisateur.
3. Entrez le mot de passe.
4. **Procédure de connexion de** clic.Les figures 30 et 31 affiche les écrans qui apparaissent :.**Figure 30 – *L'agent de Cisco NAC exécutant la version IP ou renouvellent* Figure 31 – *L'agent de Cisco NAC indiquant le plein accès de réseau après IP régénèrent***
5. Cliquez sur **OK**.

Annexe

Haute disponibilité

Chacun des différents gestionnaires de Cisco NAC et serveurs de Cisco NAC dans la solution peut être configuré en mode facilement disponible, signifiant qu'il y a deux appliances qui agissent dans une configuration d'actif-standby.

Gestionnaire NAC

Vous pouvez configurer le gestionnaire de Cisco NAC en mode facilement disponible où il y a deux gestionnaires NAC qui agissent dans une configuration d'actif-standby. La configuration entière sur un gestionnaire est enregistrée dans une base de données. Le gestionnaire de réserve synchronise sa base de données avec la base de données sur le gestionnaire actif. Toutes les modifications de configuration apportées au gestionnaire actif sont immédiatement poussées au gestionnaire de réserve. Ces points clé fournissent un résumé de haut niveau d'exécution facilement disponible de gestionnaire :

- Le mode facilement disponible de gestionnaire de Cisco NAC est une configuration active ou passive de deux-serveur dans laquelle un gestionnaire de réserve agit en tant que sauvegarde à un gestionnaire actif.
- Le gestionnaire actif de Cisco NAC effectue toutes les tâches pour le système. Le gestionnaire de standby surveille le gestionnaire actif et maintient sa base de données synchronisée avec la base de données du gestionnaire actif.
- Les deux gestionnaires de Cisco NAC partagent un IP virtuel de service pour l'interface de confiance par Eth0. Utilisez cet IP de service pour le certificat ssl.
- Les gestionnaires primaires et secondaires de Cisco NAC permutent des paquets de pulsation d'UDP toutes les 2 secondes. Si le temporisateur de pulsation expire, le basculement dynamique se produit.
- Afin d'assurer un gestionnaire actif de Cisco NAC est toujours disponible, son interface de confiance (Eth0) doit être. Vous devez éviter la situation où un gestionnaire est en activité mais n'êtes pas par accessible son interface de confiance. Cette condition se produit si le gestionnaire de réserve reçoit des paquets de pulsation du gestionnaire actif, mais l'interface Eth0 du gestionnaire actif échoue. Le mécanisme de lien-détecter permet au gestionnaire de réserve pour connaître quand l'interface Eth0 du gestionnaire actif devient indisponible.
- Vous pouvez choisir « configurez automatiquement » l'interface Eth1 dans la page de **gestion** > de **gestionnaire** > de **Basculement de CCA**. Cependant, vous devez manuellement configurer d'autres (Eth2 ou Eth3) interfaces facilement disponibles avec une adresse IP et un netmask avant que vous configuriez la Haute disponibilité sur le gestionnaire de Cisco NAC.

- Les interfaces Eth0, Eth1, et Eth2/Eth3 peuvent être utilisées pour la synchronisation de paquets et de base de données de pulsation. En outre, n'importe quelle interface (COM) séquentielle disponible peut également être utilisée pour des paquets de pulsation. Si vous utilisez plus d'un de ces interfaces, le Basculement se produit seulement si toutes les interfaces de pulsation échouent.

Remarque: Les paires facilement disponibles de gestionnaire de Cisco NAC ne peuvent pas être séparées par un lien de la couche 3.

Pour plus de détails, référez-vous à la documentation de gestionnaire de Cisco NAC à configurer la Haute disponibilité.

Serveur de Cisco NAC

Afin d'assurer la protection contre un point de défaillance unique, vous pouvez configurer le serveur de Cisco NAC en mode facilement disponible. Le mode facilement disponible pour le serveur de Cisco NAC est semblable à celui du gestionnaire de Cisco NAC et utilise également une configuration d'actif-standby. Les serveurs de Cisco NAC partagent toujours une adresse IP virtuelle (appelée un IP de service), mais ils ne partagent pas les adresses MAC virtuelles.

Ces points clé fournissent une vue d'ensemble à niveau élevé du fonctionnement du serveur facilement disponible de Cisco NAC :

- Le mode facilement disponible de serveur de Cisco NAC est une configuration actif-passive de deux-serveur dans laquelle un ordinateur hôte de réserve de Cisco NAC agit en tant que sauvegarde à un serveur actif de Cisco NAC.
- Le serveur actif de Cisco NAC effectue toutes les tâches pour le système. Puisque la majeure partie de la configuration du serveur est enregistrée sur le gestionnaire de Cisco NAC, quand le Basculement de serveur se produit, le gestionnaire pousse la configuration au serveur nouveau-actif.
- Le serveur de réserve de Cisco NAC n'expédie aucun paquet entre ses interfaces.
- Le serveur de Cisco NAC de standby surveille les santés du serveur actif par une interface de pulsation (interface série et un ou plusieurs interfaces d'UDP). Des paquets de pulsation peuvent être envoyés sur l'interface série, l'interface Eth2 dédiée, l'interface Eth3 dédiée, ou l'interface Eth0/Eth1 (si aucune interface Eth2 ou Eth3 n'est disponible).
- Les serveurs primaires et secondaires de Cisco NAC permutent des paquets de pulsation d'UDP toutes les deux secondes. Si le temporisateur de pulsation expire, le basculement dynamique se produit.
- En plus du Basculement basé sur pulsation, le serveur de Cisco NAC fournit également le Basculement basé sur lien basé sur la panne du lien Eth0 ou Eth1. Le serveur envoie des paquets de ping d'ICMP à une adresse IP externe par l'interface Eth0 et/ou Eth1. Le Basculement se produit seulement si un serveur de Cisco NAC peut cingler les adresses externes.

Pour plus de détails, référez-vous à la documentation de serveur de Cisco NAC à configurer la Haute disponibilité.

Répertoire actif SingleSignOn (Répertoire actif SSO)

Le répertoire actif SSO de Windows est la capacité pour une appliance de Cisco NAC automatiquement aux utilisateurs de connexion déjà authentifiés à un contrôleur de domaine

principal de Kerberos (serveur de Répertoire actif). Cette capacité élimine la nécessité de se connecter dans le serveur de Cisco NAC après que vous soyez déjà connecté dans le domaine. Pour plus de détails au sujet de configurer le répertoire actif SSO sur une appliance de Cisco NAC, allez à configurer l'ouverture de session simple de Répertoire actif.

Considérations d'environnement de domaine windows

En vue d'un déploiement NAC, des modifications à la stratégie de script de connexion peuvent être exigées. Des scripts de connexion de Windows peuvent être classifiés comme scripts de startup ou d'arrêt et de connexion ou de déconnexion. Passages startup de Windows et scripts d'arrêt dans un « contexte d'ordinateur. » Exécuter les scripts fonctionne seulement si l'appliance de Cisco NAC ouvre les ressources de réseau appropriées exigées par le script pour le rôle particulier quand ces scripts sont exécutés à l'amorce ou à l'arrêt PC, qui sont typiquement le rôle unauthenticated. Des scripts de connexion et de déconnexion sont exécutés dans un « contexte d'utilisateur, » qui signifie que le script de connexion exécute après que l'utilisateur ait ouvert une session la cuvette Windows GINA. Le script de connexion peut pour exécuter si l'authentification ou l'estimation de posture de machine cliente ne se termine pas et l'accès au réseau n'est pas accordé à temps. Ces scripts peuvent également être interrompus par l'adresse IP régénèrent initié par l'agent de Cisco NAC après qu'un événement de connexion OOB. Pour plus d'informations sur des modifications nécessaires aux scripts de connexion, allez à Windows GPO les scripts et l'Interopérabilité de Cisco NAC.

Configurez l'appliance de Cisco NAC pour l'estimation de posture de connexion de l'agent et de client

L'agent de Cisco NAC et l'agent de Web de Cisco NAC fournissent l'estimation locale et la correction de posture pour des machines cliente. Les utilisateurs téléchargent et installent l'agent de Cisco NAC ou l'agent de Web de Cisco NAC (logiciel client en lecture seule), qui peuvent vérifier le registre, les processus, les applications, et les services d'hôte. Pour plus de détails au sujet de l'agent et l'estimation et la correction de posture, allez à configurer l'appliance de Cisco NAC pour l'estimation de posture de connexion de l'agent et de client.

Informations connexes

- Page de support d'appareils de Cisco NAC
- Support et documentation techniques - Cisco Systems