Processus de découverte d'agent de Contrôle d'admission au réseau (NAC) pour le Cisco Identity Services Engine (ISE)

Contenu

Introduction

Ce document décrit comment l'agent du Cisco Network Admission Control (NAC) découvre un noeud de stratégie du Logiciel Cisco Identity Services Engine (ISE), aussi bien que la configuration exigée pour assurer la transmission réussie entre l'agent NAC et l'ISE.

Conditions préalables

Conditions requises

Cisco recommande que vous répondiez à ces exigences :

- La machine cliente doit provisioned avec l'agent NAC.
- ISE doit être configuré correctement pour l'écoulement de ravitaillement de client.
- Le client d'AAA (commutateur ou WLC) doit être configuré avec approprié réorientent l'ACL. Il est essentiel que cet ACL réoriente n'importe quelle transmission sur le port 80 et ne réoriente pas la transmission sur le port 8905.
- La machine cliente doit pouvoir résoudre l'adresse Internet ISE.

Composants utilisés

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

- Agent 4.9.x du Cisco Network Admission Control (NAC)
- Logiciel Cisco Identity Services Engine (ISE) 1.1.x

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Processus de découverte

Quand les débuts d'agent NAC, il suit cet ordre :

1. Sonde de détection de HTTP sur le port 80 à l'hôte de détection, si on est configuré.
2. Sonde de détection HTTPS sur le port 8905 à l'hôte de détection, si on est configuré.
3. Sonde de détection de HTTP sur le port 80 à la passerelle par défaut.
4. HTTPS rebranchent la sonde sur 8905 au noeud précédemment entré en contact de stratégie ISE.
5. Répétition de 1.

La validation réussie de posture dépend de l'agent atteignant le noeud de stratégie qui a authentifié la session de l'original 802.1x/MAB et recevoir les informations de session. Ces informations sont disponibles au commutateur mais pas à l'agent. Les tentatives d'agent de se connecter à tout noeud quand il monte.

Dans les étapes 1 et 3, notez que le trafic http d'utilisations d'agent NAC au port 80 spécifiquement pour atteindre l'hôte de détection ou la passerelle par défaut. Ce processus se produit parce que l'écoulement de ravitaillement de client ISE exige du port 80 d'être réorienté au noeud de stratégie ISE qui a authentifié la session. Tant que l'écoulement de processeur de chemin de contrôle (CPP) et l'URL réorientent la configuration est correct et fonctionnant, n'importe quel agent NAC dans le réseau devrait ne rencontrer aucun problème atteignant le noeud correct de stratégie. Une mise en garde à se souvenir est que l'URL de réorientation contient l'adresse Internet d'ISE, ainsi la machine cliente devrait pouvoir résoudre cela à l'IP du noeud de stratégie.

Si l'URL réorientent ne fonctionne pas ou n'est pas configuré, alors étapes 2 et 4 sont utilisées comme Basculement. Ces étapes sont utilisées seulement si vous avez configuré un hôte de détection ou si l'agent s'est connecté à ce déploiement ISE précédemment. Même si l'agent obtient à un point de décision politique (PDP) utilisant l'étape 2 ou 4, il ne garantit pas que la validation de posture réussira parce que les informations de session peuvent ne pas être disponibles sur ce PDP.

Afin de fonctionner autour de cette question, des groupes de noeud peuvent être installés pour partager les informations de session. Cependant, il est beaucoup plus simple de configurer et obtenir le fonctionnement de redirection URL.

Vérifiez

Afin de vérifier si l'agent NAC pourra atteindre le noeud de stratégie, ouvre un navigateur sur la machine cliente et va à cet URL : https:// <ise-hostname>:8905/auth/discovery

ISE devrait renvoyer une page qui inclut ce texte : X-Perfigo-CAS=<FQDN d'*ISE*>

Informations connexes

- Support et documentation techniques - Cisco Systems