NAC (CCA) : Configurer l'authentification sur Clean Access Manager (CAM) avec ACS

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Configurez
Diagramme du réseau
Étapes pour configurer l'authentification sur le CCA avec ACS
Configuration ACS
Vérifiez
Dépannez
Informations connexes

Introduction

Ce document décrit comment configurer l'authentification sur Clean Access Manager (CAM) avec le Cisco Secure Access Control Server (ACS). Pour une configuration semblable utilisant ACS 5.x et plus tard, référez-vous à NAC (CCA) : Configurez l'authentification sur Clean Access Manager avec ACS 5.x et plus tard.

Conditions préalables

Conditions requises

Cette configuration s'applique à la version 3.5 et ultérieures de CAM.

Composants utilisés

Les informations dans ce document sont basées sur la version 4.1 de CAM.

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.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Étapes pour configurer l'authentification sur le CCA avec ACS

Procédez comme suit :

1. **Ajoutez les nouveaux rôles Créez un rôle d'admin**Dans le CAM, choisissez la **gestion des utilisateurs > les rôles de l'utilisateur > nouveau rôle**.Écrivez un nom unique, **admin**, pour le rôle dans le domaine de role name.Écrivez le **rôle de l'utilisateur d'admin** comme description facultative de rôle.Choisissez le **rôle normal de procédure de connexion** comme type de rôle.Configurez **(OOB) le** rôle de l'utilisateur **hors bande** VLAN avec le VLAN approprié. Par exemple, choisissez l'ID DE VLAN et spécifiez l'ID en tant que 10.Une fois terminé, le clic **créent le rôle**. Afin de restaurer les propriétés par défaut sur la forme, **remise de** clic.Le rôle apparaît maintenant dans la liste d'onglet de rôles suivant les indications de la balise VLAN pour la section basée sur rôle de mappages OOB.**Créez un rôle de l'utilisateur**Dans le CAM, choisissez la **gestion des utilisateurs > les rôles de l'utilisateur > nouveau rôle**.Écrivez un nom unique, des **utilisateurs**, pour le rôle dans le domaine de role name.Écrivez le **rôle de l'utilisateur normal** comme description facultative de rôle.Configurez **(OOB) le** rôle de l'utilisateur **hors bande** VLAN avec le VLAN approprié. Par exemple, choisissez l'ID DE VLAN et spécifiez l'ID en tant que 20.Une fois terminé, le clic **créent le rôle**. Afin de restaurer les propriétés par défaut sur la forme, **remise de** clic.Le rôle apparaît maintenant dans la liste d'onglet de rôles suivant les indications de la balise VLAN pour la section basée sur rôle de mappages OOB.
2. **Balise VLAN pour les mappages basés sur rôle OOB**Dans le CAM, choisissez la **gestion des utilisateurs > les rôles de l'utilisateur > la liste de rôles** afin de voir la liste de rôles jusqu'ici.
3. **Ajoutez le serveur authentique de RAYON (ACS)**Choisissez la **gestion des utilisateurs > les serveurs authentiques > nouveau**.Du menu déroulant de type d'authentification, choisissez le **rayon**.Écrivez le nom de fournisseur comme **ACS**.Écrivez le nom du serveur comme **auth.cisco.com**.**Port de serveur** — Le numéro de port **1812** sur lequel le serveur de RAYON écoute.**Type de rayon** — La méthode d'authentification de RAYON. Les méthodes prises en charge incluent EAPMD5, PAP, CHAP, MSCHAP et MSCHAP2.**Le rôle par défaut** est utilisé si traçant à ACS n'est pas défini ou est placé correctement, ou si l'attribut RADIUS n'est pas défini ou est placé correctement sur l'ACS.**Secret partagé** — Le RAYON a partagé la limite secrète à l'adresse IP du client spécifié.**Nas-IP-adresse** — Cette valeur à envoyer avec tous les paquets d'authentification de RAYON.Cliquez sur Add le **serveur**.

4. **Utilisateurs de la carte ACS aux rôles de l'utilisateur de CCA**Choisissez la **gestion des utilisateurs > les serveurs authentiques > les règles de mappage > ajoutent le lien de mappage** afin de tracer l'utilisateur d'admin dans ACS au rôle de l'utilisateur d'admin de CCA.Choisissez la **gestion des utilisateurs > les serveurs authentiques > les règles de mappage > ajoutent le lien de mappage** afin de tracer l'utilisateur normal dans ACS au rôle de l'utilisateur de CCA.Voici le rôle de l'utilisateur de résumé de mappage :
5. **Fournisseurs alternatifs d'enable sur la page utilisateur**Choisissez la **gestion > les pages utilisateur > la page de connexion > ajoutent > contenu** afin d'activer les fournisseurs alternatifs à la page d'ouverture de session utilisateur.

Configuration ACS

1. Choisissez la **configuration d'interface** afin de s'assurer que l'attribut [025] de classe du RAYON (IETF) est activé.
2. **Ajoutez le client RADIUS au serveur ACS**Choisissez la **configuration réseau** afin d'ajouter le CAM de client d'AAA comme affiché :Cliquez sur Submit **+ reprise**.**Remarque:** Assurez-vous que la clé de RAYON s'assortit avec le client d'AAA et utilise le RAYON (IETF).Choisissez la **configuration réseau** afin d'ajouter le client CAS d'AAA comme affiché :Cliquez sur Submit **+ reprise**.**Remarque:** Pour la comptabilité de RAYON de passerelle VPN, la stratégie de CCA doit permettre à des paquets de comptabilité de RAYON (UDP 1646/1813) de l'adresse IP de CAS pour passer unauthenticated à l'adresse IP de serveur ACS.Choisissez la **configuration réseau** afin d'ajouter le client ASA d'AAA comme affichée :Adresse de gauche d'interface de l'utilisateur PIX/ASA (typiquement interface interne)Set type au RAYON (Cisco IOS/PIX).
3. **Ajoutez les groupes de /Configure sur le serveur ACSCréez le groupe d'admin**Placez l'attribut [025] de classe de RAYON IETF pour s'approprier la valeur de groupe.La valeur doit apparier cela configuré sur la cartographie de CAS.**Créez le groupe d'utilisateurs**Ajoutez/configurez le groupe pour que chaque rôle de l'utilisateur de Clean Access soit tracé.**Ajoutez/configurez les utilisateurs sur le serveur ACS**Ajoutez/configurez l'utilisateur ACS pour que chaque utilisateur de Clean Access soit authentifié par ACS.Placez l'adhésion à des associations ACS.ACS prend en charge également l'authentification de proxy à d'autres serveurs externes.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Dans la section de surveillance ACS, vous pouvez voir les informations sur passées les authentifications comme affichées :

De même, vous pouvez voir le tir d'écran pour la comptabilité de RAYON :

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

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