NAC (CCA) : Configurez l'authentification sur Clean Access Manager avec ACS 5.x et plus tard

Contenu

Introduction

Ce document fournit des informations comment configurer l'authentification sur Clean Access Manager (CAM) avec le Système de contrôle d'accès sécurisé Cisco (ACS) 5.x et plus tard. Pour une configuration semblable utilisant des versions plus tôt qu'ACS 5.x, référez-vous à NAC (CCA) : Configurez l'authentification sur Clean Access Manager (CAM) avec ACS.

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.

Note: 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 :

Configurez l'authentification sur le CCA avec ACS 5.x

Procédez comme suit :

1. **Ajoutez les nouveaux rôles Créez un rôle d'admin**Du 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**Du 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**Du 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 ACS5.x

1. Choisissez les **ressources de réseau > les périphériques de réseau et les clients d'AAA**, puis cliquez sur **créent** afin d'ajouter le **CAM** en tant que **client d'AAA**.
2. Fournissez le **nom, adresse IP** et choisissez le **RAYON** sous des options d'authentification. Puis, fournissez le **secret partagé** pour le **CAM** et cliquez sur Submit.
3. Choisissez les **ressources de réseau > les périphériques de réseau et les clients d'AAA**, puis cliquez sur **créent** afin d'ajouter **CAS** en tant que **client d'AAA**.
4. Fournissez le **nom, adresse IP** et choisissez le **RAYON** sous des options d'authentification. Puis, fournissez le **secret partagé** pour **CAS** et cliquez sur Submit.
5. Choisissez les **ressources de réseau > les périphériques de réseau et les clients** et le clic d'**AAA créent** afin d'ajouter l'**ASA** en tant que **client d'AAA**.
6. Fournissez le **nom, adresse IP** et choisissez le **RAYON** sous des options d'authentification. Puis, fournissez le **secret partagé** pour l'**ASA** et cliquez sur Submit.
7. Choisissez les **utilisateurs et l'identité enregistre > des groupes d'identité** et le clic **créent** afin de créer un nouveau groupe d'identité.
8. Fournissez le **nom de groupe** et cliquez sur Submit.
9. Choisissez les **utilisateurs et l'identité enregistre > des groupes d'identité** et le clic **créent** afin de créer un nouveau groupe d'identité.
10. Fournissez le **nom de groupe** et cliquez sur Submit.
11. Choisissez les **utilisateurs et l'identité enregistre > identité interne enregistre > des utilisateurs** et le clic **créent** afin de créer un nouvel utilisateur.
12. Fournissez le **nom d'utilisateur** et changez l'adhésion à des associations au groupe d'**admin**. Puis, fournissez le **mot de passe** et confirmez le mot de passe. Cliquez sur **Submit**.
13. Choisissez les **utilisateurs et l'identité enregistre > identité interne enregistre > des utilisateurs** et le clic **créent** afin de créer un nouvel utilisateur.
14. Fournissez le **nom d'utilisateur** et changez l'adhésion à des associations aux **users group**. Puis, fournissez le **mot de passe** et confirmez le mot de passe. Cliquez sur **Submit**.
15. Choisissez les **éléments > l'autorisation de stratégie et les autorisations > l'accès au réseau > les profils** et le clic d'**autorisation créent** afin de créer un nouveau **profil d'autorisation**.
16. Fournissez le **nom de profil** et cliquez sur les **attributs RADIUS**.
17. **Des attributs RADIUS** tabulez, choisissez **RADIUS-IETF** comme **type de dictionnaire**. Puis, clic **choisi** à côté de l'**attribut RADIUS**.
18. Choisissez l'attribut de **classe** et cliquez sur OK.
19. Assurez-vous que la **valeur d'attribut** est **statique** et entrez dans l'**admin** comme valeur. Cliquez sur Add, puis cliquez sur Submit.

20. Choisissez les **éléments > l'autorisation de stratégie et les autorisations > l'accès au réseau > les profils** et le clic d'**autorisation créent** afin de créer un nouveau **profil d'autorisation**.
21. Fournissez le **nom de profil** et cliquez sur les **attributs RADIUS**.
22. **Des attributs RADIUS** tabulez, choisissez **RADIUS-IETF** comme **type de dictionnaire**. Puis, clic **choisi** à côté de l'**attribut RADIUS**.
23. Choisissez l'attribut de **classe** et cliquez sur OK.
24. Assurez-vous que la **valeur d'attribut** est **statique** et présentez les **utilisateurs** comme valeur. Cliquez sur Add, puis cliquez sur Submit.
25. Choisissez les **stratégies d'Access > les services d'accès > les règles de sélection de service** et identifiez quel service traite la **demande RADIUS**. Dans cet exemple, le service est **accès au réseau par défaut**.
26. Choisissez les **stratégies d'Access > les services d'accès > l'accès au réseau de par défaut** (le service l'a identifié dans l'étape précédente qui a traité la demande RADIUS) **> autorisation**. Le clic **personnalisent**.
27. Déplacez le **groupe d'identité de disponible à la** colonne **sélectionnée**. Cliquez sur **OK**.
28. Le clic **créent** afin de créer une nouvelle règle.
29. Assurez-vous que la case de **groupe d'identité** est cochée, puis cliquent sur **choisi** à côté du **groupe d'identité**.
30. Sélectionnez le groupe d'**admin** et cliquez sur OK.
31. Clic **choisi** dans la section de **profils d'autorisation**.
32. Sélectionnez le profil d'autorisation d'**admin** et cliquez sur OK.
33. Le clic **créent** afin de créer une nouvelle règle.
34. Assurez-vous que la case de **groupe d'identité** est cochée et cliquez sur **choisi** à côté du groupe d'identité.
35. Sélectionnez les **users group** et cliquez sur OK.
36. Clic **choisi** dans la section de **profils d'autorisation**.
37. Sélectionnez le profil d'autorisation d'**utilisateurs** et cliquez sur OK.
38. Cliquez sur **OK**.
39. **Modifications de sauvegarde de** clic.

Dépannez

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

Informations connexes

- Support d'appareils de Cisco NAC
- Système de contrôle d'accès sécurisé Cisco
- Support et documentation techniques - Cisco Systems