NAC(CCA) 4.x : Exemple de configuration du mappage d'utilisateurs à certains rôles à l'aide de LDAP

Contenu

Introduction

Ce document décrit le Protocole LDAP (Lightweight Directory Access Protocol) traçant la caractéristique afin de tracer les utilisateurs à certains rôles dans l'appliance de Contrôle d'admission au réseau (NAC) ou le Cisco Clean Access (CCA).

L'appliance de Cisco NAC (autrefois Cisco Clean Access) est un produit facilement déployé NAC qui emploie l'infrastructure réseau pour imposer la conformité de stratégie de sécurité sur tous les périphériques qui recherchent à accéder au réseau calculant des ressources. Avec l'appliance NAC, les administrateurs réseau peuvent authentifier, autorisent, évaluent, et remediate de câble, radio, et utilisateurs distants et leurs ordinateurs avant accès au réseau. Il identifie si les périphériques en réseau tels que des ordinateurs portables, des Téléphones IP, ou des consoles de jeux sont conformes avec les stratégies de sécurité de votre réseau et répare toutes les vulnérabilités avant de permettre l'accès au réseau.

Conditions préalables

Conditions requises

Ce document suppose que le gestionnaire de CCA, le serveur de CCA et le serveur LDAP sont installés et fonctionnent correctement.

Composants utilisés

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

- Gamme 3300 d'appareils de Cisco NAC - Clean Access Manager 4.0
- Gamme 3300 d'appareils de Cisco NAC - Clean Access Server 4.0

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.

Authentification contre le Répertoire actif principal

Plusieurs types de fournisseurs d'authentification dans Clean Access Manager peuvent être utilisés pour authentifier des utilisateurs contre un serveur de Répertoire actif (AD), le service d'annuaire de propriété industrielle de Microsoft. Ceux-ci incluent Windows NT(NTLM), Kerberos et LDAP (préférés).

Si vous employez le LDAP pour se connecter à l'AD, le plein nom unique de Search(Admin) (DN) typiquement doit être placé au DN d'un compte avec des privilèges d'administrateur ou des privilèges des utilisateurs de base. La première entrée commune du nom (NC) devrait être un administrateur de l'AD, ou un utilisateur avec des privilèges lus. Notez que le filtre de recherche, SAMAccountName, est le nom d'ouverture de session utilisateur dans le schéma par défaut d'AD.

Exemple de configuration AD/LDAP

Ceci illustre une configuration d'échantillon utilisant le LDAP pour communiquer avec le Répertoire actif principal :

1. Créez un utilisateur d'admin de domaine dans des utilisateurs et des ordinateurs de Répertoire actif. Placez cet utilisateur dans le répertoire d'utilisateurs.
2. Dans des utilisateurs et des ordinateurs de Répertoire actif, sélectionnez la **découverte du** menu d'actions.Assurez-vous que vos résultats affichent la colonne d'adhésion à des associations pour l'utilisateur créé. Vos résultats de la recherche devraient afficher l'**utilisateur** et l'**adhésion à des associations** associée dans le Répertoire actif. C'est les informations que vous devrez transférer dans Clean Access Manager.
3. De la console Web de Clean Access Manager, allez à la **gestion des utilisateurs > les serveurs authentiques > nouveau** formulaire de **serveur**.
4. Choisissez le **LDAP** comme type de serveur.
5. Pour les **pleins champs de base de contexte de DN** et de **recherche de Search(Admin)**, entrez les résultats de la découverte dans des utilisateurs et des ordinateurs de Répertoire actif.
6. Ces champs sont tout ce qui est nécessaire pour installer correctement ce serveur

authentique dans le CAM :**ServerURL** : ldap://192.168.137.10:389 - C'est le port en mode écoute d'adresse IP et de LDAP de contrôleur de domaine.**Plein DN de Search(Admin)** : Muir de CN=sheldon, CN=Users, DC=domainname, DC=com**Contexte de base de recherche** : DC=domainname, DC=com**Rôle par défaut** : Sélectionnez le rôle par défaut qu'un utilisateur sera mis dans une fois authentifié.**Description** : Utilisé juste pour la référence.**Nom de fournisseur** : C'est le nom du serveur LDAP utilisé pour la page utilisateur installée sur le CAM.**Mot de passe de recherche** : mot de passe du domaine des muir de sheldon**Filtre de recherche** : SAMAccountName=$user$

7. Cliquez sur Add le **serveur**.En ce moment, votre test authentique devrait fonctionner.
8. Test d'authentification :**De la gestion des utilisateurs > les serveurs authentiques > onglet authentique de test**, sélectionnent le fournisseur contre lequel vous voulez tester des qualifications dans la liste de **fournisseur**. Si le fournisseur n'apparaît pas, assurez-vous qu'il est correctement configuré dans la **liste d'**onglet de **serveurs**.Écrivez le nom d'utilisateur et mot de passe pour l'utilisateur et si requis une valeur d'ID DE VLAN.Le clic **authentifient**.Les résultats de test apparaissent au bas de la fenêtre.**Authentification réussie :**Pour tout type de fournisseur, résultat : L'authentification réussie et le rôle de l'utilisateur sont affichés quand le test authentique réussit.Pour des serveurs LDAP/RADIUS, quand l'authentification est réussie et des règles de mappage sont configurés, les attributs/valeurs spécifiées dans la règle de mappage sont également affichés si le serveur authentique (LDAP/RADIUS) renvoie ces valeurs. Exemple :`Result: Authentication successful`
`Role: <role name>`
`Attributes for Mapping:`
`<Attribute Name>=<Attribute value>` **Échec de l'authentification :**Quand l'authentification échoue, les affichages de message avec l'échec de l'authentification résultent comme affiché.

Utilisateurs de carte aux rôles utilisant des attributs ou des IDs de VLAN

Les formes de règles de **mappage** peuvent être utilisées pour tracer des utilisateurs dans le rôle de l'utilisateur basé sur ces paramètres :

- L'ID DE VLAN du trafic d'utilisateur qui provient du côté non approuvé de CAS (tous les types de serveur authentiques)
- Les attributs d'authentification ont passé des serveurs authentiques de LDAP et de RAYON (et des attributs RADIUS passés des concentrateurs de Cisco VPN)

Par exemple, si vous avez deux ensembles d'utilisateurs sur le même IP de sous-réseau mais avec différents privilèges d'accès au réseau, tels que les employés Sans fil et les étudiants, vous pouvez employer un attribut d'un serveur LDAP pour tracer un ensemble d'utilisateurs dans un rôle de l'utilisateur particulier. Vous pouvez alors créer des stratégies de trafic pour permettre l'accès au réseau à un rôle et pour refuser l'accès au réseau à d'autres rôles.

L'appliance de Cisco NAC exécute l'ordre de mappage comme affiché :

L'appliance de Cisco NAC permet à l'administrateur pour spécifier des expressions booléennes complexes en définissant le mappage ordonne pour le Kerberos, le LDAP et les serveurs d'authentification RADIUS. Traçant des règles sont décomposées en conditions et vous pouvez employer des expressions booléennes pour combiner des attributs de plusieurs utilisateurs et des id de VLAN multiple afin de tracer des utilisateurs dans des rôles de l'utilisateur. La cartographie

des règles peut être créée pour une plage des IDs de VLAN, et des correspondances d'attribut peuvent être rendues ne distinguant pas majuscules et minuscules. Ceci permet de plusieurs conditions à configurer avec souplesse pour une règle de mappage.

Une règle de mappage comporte un type authentique de fournisseur, une expression de règle, et le rôle de l'utilisateur dans laquelle pour tracer l'utilisateur. L'expression de règle comporte un ou une combinaison des conditions que les paramètres d'utilisateur doivent apparier pour être tracés dans le rôle de l'utilisateur spécifié. Une condition est composée d'un type de condition, d'un nom d'attribut de source, d'un opérateur, et de la valeur d'attribut contre laquelle l'attribut particulier est apparié.

Afin de créer une règle de mappage, vous ajoutez d'abord des états (de sauvegarde) pour configurer une expression de règle. Puis, une fois une expression de règle est créée, vous peut ajouter la règle de mappage au serveur authentique pour le rôle de l'utilisateur spécifié.

La cartographie des règles peut monter en cascade. Si une source a plus d'une règle de cartographie, les règles sont évaluées dans la commande dans laquelle elles apparaissent dans la liste de règles de mappage. Le rôle pour la première règle positive de mappage est utilisé. Une fois une règle est rencontrée, d'autres règles ne sont pas testées. Si aucune règle n'est vraie, le rôle par défaut pour cette source d'authentification est utilisé.

Configurez la règle de mappage

Procédez comme suit :

1. Allez à la **gestion des utilisateurs > les serveurs authentiques > les règles de mappage** et cliquez sur le lien de **règle de mappage d'ajouter** pour le serveur d'authentification.La forme de **règle de mappage d'ajouter** apparaît.
2. Configurez les conditions pour tracer la règle (a) :**Nom de fournisseur** — Le nom de fournisseur place les champs des règles de mappage forment pour ce type de serveur d'authentification. Par exemple, la forme permet seulement la configuration de règle de mappage d'ID DE VLAN les types pour de Kerberos, de Windows NT, de Windows Netbios SSO, et S/Ident serveur authentiques. La forme permet la configuration de règle de mappage d'ID DE VLAN ou d'attribut pour le RAYON, le LDAP, et les types authentiques de Cisco VPN SSO.**Type de condition** — Configurez et ajoutez les conditions d'abord (font un pas **A** dans la figure) avant d'ajouter la règle de mappage. Choisissez un de ces derniers du menu déroulant afin de placer les champs de la forme de condition :**Attribut** — Pour le LDAP, RAYON, fournisseurs authentiques de Cisco VPN SSO seulement.**ID DE VLAN** — Tous les types de serveur authentiques.Pour un type de condition d'ID DE VLAN (voyez la figure), ce champ s'appelle le **nom de propriété**. Par défaut, ceci est rempli avec le « ID DE VLAN » (et désactivé pour éditer).**Nom d'attribut** — Pour des serveurs LDAP (voyez la figure), le **nom d'attribut** est un champ texte dans lequel vous écrivez l'attribut de source que vous voulez tester. Le nom doit être identique (case-sensitive) au nom de l'attribut passé par la source d'authentification, à moins que vous choisissiez les **égaux ignoriez l'**opérateur de **cas** pour créer la condition.**Valeur d'attribut** — Écrivez la valeur à tester contre le **nom d'attribut de** source.**Opérateur (attribut)** — Choisissez l'opérateur qui définit le test de la chaîne d'attribut de source :**égaux** — Rectifiez si la valeur du **nom d'attribut** apparie la **valeur d'attribut**.**pas égaux** — Rectifiez si la valeur du **nom d'attribut** n'apparie pas la **valeur d'attribut**.**contient** — Rectifiez si la valeur du **nom d'attribut** contient la **valeur d'attribut**.**débuts avec** — Rectifiez si la valeur du **nom d'attribut** commence par la **valeur d'attribut**.**finit avec** — Rectifiez si la valeur

du **nom d'attribut** finit avec la **valeur d'attribut**.**les égaux ignorent le cas** — Rectifiez si la valeur du **nom d'attribut** apparie la chaîne de **valeur d'attribut**. Il n'importe pas si la chaîne soit majuscule ou minuscule.**Opérateur (ID DE VLAN)** — Si vous choisissez l'ID DE VLAN comme **type de condition**, choisissez un de ces opérateurs pour définir une condition cette des tests contre des entiers d'ID DE VLAN :**égaux** — Rectifiez si l'ID DE VLAN apparie l'ID DE VLAN dans le domaine de **valeur d'une propriété**.**pas égaux** — Rectifiez si l'ID DE VLAN n'apparie pas l'ID DE VLAN dans le domaine de **valeur d'une propriété**.**appartient à** — Rectifiez si l'ID DE VLAN fait partie de la marge des valeurs configurées pour le champ de **valeur d'une propriété**. La valeur devrait être un ou plusieurs IDs de VLAN séparés par virgule. Des plages des IDs de VLAN peuvent être spécifiées par trait d'union (-), par exemple, [2,5,7,100-128,556-520]. Seulement des entiers peuvent être écrits, pas des chaînes. Notez que les crochets sont facultatifs.**Exemple :Ajoutez la condition (l'état de sauvegarde)** — Veillez à configurer la condition, puis cliquez sur Add la **condition** afin d'ajouter la condition à l'expression de règle (autrement votre configuration n'est pas enregistrée).

3. Ajoutez la règle de mappage au rôle (b) : Ajoutez la règle de mappage (étape **B** dans la figure) après que vous ayez configuré et ayez ajouté les conditions.**Role name** — Après que vous ayez ajouté au moins une condition, choisissez le rôle de l'utilisateur auquel vous appliquerez le mappage à partir du menu déroulant.**Priorité** — Sélectionnez une priorité du déroulant pour déterminer la commande dans laquelle des règles de mappage sont testées. La première règle qui évalue pour rectifier est utilisée pour assigner à l'utilisateur un rôle.**Expression de règle** — Afin de faciliter en configurant des déclarations conditionnelles pour la règle de mappage, ce champ affiche le contenu de la dernière condition à ajouter. Après avoir ajouté les conditions, vous devez cliquer sur Add la **règle de mappage** afin de sauvegarder toutes les conditions à la règle.**Description** — Une description facultative de la règle de mappage.**Ajoutez le mappage (le mappage de sauvegarde)** — Cliquez sur ce bouton une fois fait en ajoutant des conditions pour créer la règle de mappage pour le rôle. Vous devez ajouter ou sauvegarder le mappage pour un rôle spécifié, ou votre configuration et vos conditions ne seront pas enregistrées.

Éditez les règles de mappage

- **Priorité** — Afin de changer la priorité d'une règle de mappage plus tard, cliquez sur la flèche haut/bas à côté de l'entrée en **gestion des utilisateurs > les serveurs authentiques > la liste de serveurs**. La priorité détermine la commande dans laquelle les règles sont testées. La première règle qui évalue pour rectifier est utilisée pour affecter l'utilisateur à un rôle.
- **Éditez** — Cliquez sur le bouton d'éditer à côté de la règle de modifier la règle de mappage, ou supprimez les conditions de la règle. Notez qu'en éditant un état composé, les conditions dessous (créé plus tard) ne sont pas affichés. C'est d'éviter des boucles.
- **Effacement** — Cliquez sur le bouton d'effacement à côté de l'entrée de règle de mappage pour qu'un serveur authentique supprime que règle individuelle de mappage. Cliquez sur le bouton d'effacement à côté d'une condition sur la forme de règle de mappage d'éditer pour retirer que condition de la règle de mappage. Notez que vous ne pouvez pas retirer une condition qui dépend d'une autre règle dans une instruction composée. Afin de supprimer un état individuel, vous devez supprimer l'état composé d'abord.

Dépannez

Si la cartographie de l'utilisateur d'AD au rôle de l'utilisateur de CCA ne fonctionne pas, alors assurez-vous que vous tracez des utilisateurs à un rôle basé sur des attributs avec le memberof, l'Operator=contains, et l'attribut Value= (nom de Names= d'attribut de groupe).

Informations connexes

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