Exemple de configuration d'authentification LDAP pour le central UCS

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour l'authentification de Protocole LDAP (Lightweight Directory Access Protocol) pour le central du Système d'informatique unifiée Cisco (UCS). Les procédures utilisent l'interface utilisateur graphique centrale UCS (GUI), un domaine d'exemple de bglucs.com, et un nom d'utilisateur d'exemple de testuser.

Dans la version 1.0 du logiciel central UCS, le LDAP est le seul protocole pris en charge d'authentification à distance. La version 1.0 a très la prise en charge limitée pour l'authentification à distance et la configuration de LDAP pour le central UCS elle-même. Cependant, vous pouvez employer le central UCS afin de configurer toutes les options pour les domaines d'UCS Manager gérés par le central UCS.

Les limites d'authentification à distance centrale UCS incluent :

- Le RAYON et les TACACS ne sont pas pris en charge.
- Des groupes de mappage d'adhésion à des associations de LDAP pour l'affectation de rôle et de fournisseur de LDAP pour des contrôleurs de plusieurs domaines ne sont pas pris en charge.
- Le LDAP emploie seulement l'attribut de CiscoAVPair ou n'importe quel attribut inutilisé afin de passer le rôle. Le rôle passé est l'un des rôles de prédéfinis dans la base de données locale de central UCS.
- De plusieurs domaines/protocoles d'authentification ne sont pas pris en charge.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Le central UCS est déployé.
- La Microsoft Active Directory est déployée.

Composants utilisés

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

- Version 1.0 de central UCS
- Microsoft Active Directory

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.

Les informations de rassemblement

Cette section récapitule les informations que vous devez recueillir avant que vous commenciez la configuration.

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

Petits groupes d'utilisateur de grippage

L'utilisateur de grippage peut être n'importe quel utilisateur de LDAP dans le domaine qui a l'accès en lecture au domaine ; un utilisateur de grippage est prié pour la configuration de LDAP. Le central UCS emploie le nom d'utilisateur et mot de passe de l'utilisateur de grippage afin de

connecter et questionner le Répertoire actif (AD) pour l'authentification de l'utilisateur et ainsi de suite. Cet exemple utilise le compte administrateur en tant qu'utilisateur de grippage.

Cette procédure décrit comment un administrateur de LDAP peut employer l'éditeur des interfaces de service de Répertoire actif (ADSI) afin de trouver le DN.

1. Ouvrez l'éditeur ADSI.
2. Trouvez l'utilisateur de grippage. L'utilisateur est dans le même chemin que dans l'AD.
3. Cliquez avec le bouton droit l'utilisateur, et choisissez Properties.
4. Dans la boîte de dialogue Properties, **distinguishedName de** double clic.
5. Copiez le DN du champ de valeur.
6. **Annulation de** clic afin de fermer toutes les fenêtres.

Pour obtenir le mot de passe pour l'utilisateur de grippage, contactez l'administrateur d'AD.

Détails de base de DN

Le DN de base est le DN de l'unité organisationnelle (OU) ou du conteneur où le rechercher l'utilisateur et les petits groupes d'utilisateur commence. Vous pouvez utiliser le DN d'une OU créée dans l'AD pour le central UCS ou UCS. Cependant, vous pouvez le trouver plus simple pour utiliser le DN pour la racine de domaine lui-même.

Cette procédure décrit comment un administrateur de LDAP peut employer l'éditeur ADSI afin de trouver le DN de base.

1. Ouvrez l'éditeur ADSI.
2. Trouvez l'OU ou le conteneur à utiliser comme DN de base.
3. Cliquez avec le bouton droit l'OU ou le conteneur, et choisissez Properties.
4. Dans la boîte de dialogue Properties, **distinguishedName de** double clic.
5. Copiez le DN du champ de valeur, et notez tous les autres détails que vous avez besoin.
6. **Annulation de** clic afin de fermer toutes les fenêtres.

Détails de fournisseur

Le fournisseur joue une fonction clé dans l'authentification LDAP et l'autorisation au central UCS. Le fournisseur est l'un des serveurs d'AD qui des requêtes centrales UCS afin de rechercher et authentifier l'utilisateur et afin d'obtenir des petits groupes d'utilisateur tels que les informations de rôle. Soyez sûr de recueillir l'adresse Internet ou l'adresse IP du serveur d'AD de fournisseur.

Propriété de filtre

Le champ de filtre ou la propriété est utilisé afin de rechercher la base de données d'AD. L'user-id écrit à la procédure de connexion est passé de nouveau à l'AD et comparé contre le filtre.

Vous pouvez utiliser sAMAccountName=$userid comme valeur de filtre. le sAMAccountName est un attribut dans l'AD et a la même valeur que l'user-id d'AD, qui est utilisé afin d'ouvrir une session au GUI central UCS.

Ajoutez et configurez les attributs

Cette section récapitule les informations que vous devez afin d'ajouter l'attribut de CiscoAVPair (s'il y a lieu) et mettre à jour l'attribut ou autre de CiscoAVPair, attribut de prédéfinis avant que vous commenciez la configuration de LDAP.

Le champ d'attribut spécifie l'attribut d'AD (sous la propriété d'utilisateur), qui passe de retour le rôle à assigner à l'utilisateur. Dans la version 1.0a du logiciel central UCS, l'attribut personnalisé CiscoAVPair ou n'importe quel autre attribut inutilisé dans l'AD peut être transformé en unités afin de passer ce rôle.

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

Ajoutez l'attribut de CiscoAVPair

Afin d'ajouter un nouvel attribut au domaine, développer le schéma du domaine, et ajouter l'attribut à la classe (qui, dans cet exemple, est utilisateur).

Cette procédure décrit comment développer le schéma sur un serveur d'AD de Windows et ajouter l'attribut de CiscoAVPair.

1. Procédure de connexion à un serveur d'AD.
2. Cliquez sur le **Start > Run**, tapez le **MMC**, et l'appuyez sur **entrent** afin d'ouvrir une console vide de Microsoft Management Console (MMC).
3. Dans le MMC, le **fichier** > l'**ajout/suppression de** clic SNAP-**dans > ajoutent**.
4. Dans l'ajouter autonome SNAP-dans la boîte de dialogue, sélectionnez le **schéma de Répertoire actif**, et cliquez sur Add.
5. Dans le MMC, développez le **schéma de Répertoire actif**, cliquez avec le bouton droit les **attributs**, et choisissez **créent l'attribut**.La nouvelle boîte de dialogue d'attribut de création apparaît
6. Créez un attribut nommé CiscoAVPair dans le service d'authentification à distance.Dans les zones d'identification communes de nom et d'affichage de LDAP, entrez dans **CiscoAVPair**.Dans le seul domaine de l'object id 500, écrivez **1.3.6.1.4.1.9.287247.1**.Dans le champ description, entrez dans le **rôle et le paramètre régional UCS**.Dans le domaine de syntaxe, **chaîne** choisie d'**Unicode de la** liste déroulante.Cliquez sur OK afin de sauvegarder l'attribut et fermer la boîte de dialogue.Une fois l'attribut est ajouté au schéma, il doit être tracé ou inclus dans la classe d'utilisateurs. Ceci te permet pour éditer la propriété d'utilisateur et pour spécifier la valeur le rôle à passer.
7. Dans le même MMC utilisé pour l'extension de schéma d'AD, développez les **classes**, cliquez avec le bouton droit l'**utilisateur**, et choisissez Properties.
8. Dans la boîte de dialogue Properties d'utilisateur, cliquez sur l'onglet d'**attributs**, et cliquez sur Add.
9. Dans la boîte de dialogue choisie d'objet de schéma, cliquez sur **CiscoAVPair**, et cliquez sur OK.
10. Dans la boîte de dialogue Properties d'utilisateur, cliquez sur Apply.
11. Cliquez avec le bouton droit le **schéma de Répertoire actif**, et choisissez la **recharge le schéma** afin d'inclure les nouvelles modifications.
12. S'il y a lieu, employez l'éditeur ADSI pour mettre à jour le schéma. Cliquez avec le bouton droit **Localhost**, et choisissez le **schéma de mise à jour maintenant**.

Attribut de CiscoAVPair de mise à jour

Cette procédure décrit comment mettre à jour l'attribut de CiscoAVPair. La syntaxe est `shell : roles= " <role> »`.

1. Dans l'ADSI éditez la boîte de dialogue, localisent l'utilisateur qui a besoin de l'accès au central UCS.
2. Cliquez avec le bouton droit l'utilisateur, et choisissez Properties.
3. Dans la boîte de dialogue Properties, cliquez sur l'onglet d'**éditeur d'attribut**, cliquez sur **CiscoAVPair**, et cliquez sur Edit.
4. Dans la boîte de dialogue à valeurs multiples d'éditeur de chaîne, écrivez le **shell de** valeur **: le roles= " admin »** dans le domaine de valeurs et cliquent sur OK.
5. Cliquez sur OK afin de sauvegarder les modifications et fermer la boîte de dialogue Properties.

Attribut de prédéfinis de mise à jour

Cette procédure décrit comment mettre à jour un attribut de prédéfinis, où le rôle est l'un des rôles de l'utilisateur de prédéfinis au central UCS. Cet exemple utilise la *société d'*attribut afin de passer le rôle. La syntaxe est `shell : roles= " <role> »`.

1. Dans l'ADSI éditez la boîte de dialogue, localisent l'utilisateur qui a besoin de l'accès au central UCS.
2. Cliquez avec le bouton droit l'utilisateur, et choisissez Properties.
3. Dans la boîte de dialogue Properties, cliquez sur l'onglet d'**éditeur d'attribut**, cliquez sur la **société**, et cliquez sur Edit.
4. Dans la boîte de dialogue d'éditeur d'attribut de chaîne, écrivez le **shell de** valeur **: le roles= " admin »** dans le domaine de valeur, et cliquent sur OK.
5. Cliquez sur OK afin de sauvegarder les modifications et fermer la boîte de dialogue Properties.

Configurez l'authentification LDAP sur le central UCS

La configuration de LDAP au central UCS est terminée sous la Gestion d'exécutions.

1. Procédure de connexion au central UCS sous un compte local.
2. Cliquez sur la **Gestion d'exécutions**, développez les **groupes de domaine**, et cliquez sur les **stratégies** > la **Sécurité opérationnelles**.
3. Afin de configurer l'authentification LDAP, prenez ces mesures :Configurez le fournisseur de LDAP.Configurez le groupe de fournisseur de LDAP (non disponible dans la version 1.0a).Changez la règle indigène d'authentification.

Configurez le fournisseur de LDAP

1. Cliquez sur le **LDAP**, cliquez avec le bouton droit les **fournisseurs**, et choisissez **créent le fournisseur de LDAP**.
2. Dans la boîte de dialogue de fournisseur de LDAP de création, ajoutez ces détails, qui ont

été recueillis plus tôt.Adresse Internet ou IP du fournisseurDN de grippageDN de baseFiltreAttribut (CiscoAVPair ou un attribut de prédéfinis tel que la sociétéMot de passe (mot de passe de l'utilisateur utilisé dans le DN de grippage)
3. Cliquez sur OK afin de sauvegarder la configuration et fermer la boîte de dialogue.

Remarque: Aucune autre valeur ne doit être modifiée sur cet écran. Les règles de groupe de LDAP ne sont pas prises en charge pour l'authentification centrale UCS dans cette release.

Configurez le groupe de fournisseur de LDAP

Remarque: Dans la version 1.0a, des groupes de fournisseur ne sont pas pris en charge. Cette procédure décrit comment configurer un groupe factice de fournisseur pour utiliser dans la configuration plus tard.

1. Cliquez sur le **LDAP**, cliquez avec le bouton droit le **groupe de fournisseur**, et choisissez **créent le groupe de fournisseur de LDAP**.
2. Dans la boîte de dialogue de groupe de fournisseur de LDAP de création, écrivez le nom pour le groupe dans la zone d'identification.
3. De la liste de fournisseurs disponibles du côté gauche, sélectionnez le fournisseur, et cliquez sur le plus grand que le symbole (**>**) afin de déplacer ce fournisseur aux fournisseurs assignés du côté droit.
4. Cliquez sur OK afin de sauvegarder les modifications et fermer l'écran.

Règle indigène d'authentification de modification

La version 1.0a ne prend en charge pas de plusieurs domaines d'authentification comme dans les UCS Manager. Afin de fonctionner autour de ceci, vous devez modifier la règle indigène d'authentification.

L'authentification indigène a l'option de modifier l'authentification pour des procédures de connexion par défaut ou des ouvertures de session de console. Puisque des plusieurs domaines ne sont pas pris en charge, vous pouvez utiliser le compte local ou un compte de LDAP, mais pas chacun des deux. Changez la valeur du royaume afin d'utiliser des gens du pays ou le LDAP comme source d'authentification.

1. Cliquez sur l'**authentification**, cliquez avec le bouton droit l'**authentification indigène**, et choisissez Properties.
2. Déterminez si vous voulez l'authentification par défaut, l'authentification de console, ou chacun des deux. Utilisez l'authentification par défaut pour le GUI et l'interface de ligne de commande (CLI). Utilisez l'authentification de console pour la vue basée sur noyau du virtual machine du virtual machine (VM) (KVM).
3. Choisissez le **LDAP de la** liste déroulante de royaume. La valeur du royaume détermine si les gens du pays ou le LDAP sont la source d'authentification.
4. Cliquez sur OK afin de fermer la page.
5. Sur les stratégies paginez, cliquez sur la **sauvegarde** s'il y a lieu afin de sauvegarder les modifications.

Remarque: Ne vous déconnectez de pas votre session en cours ou modifiez l'authentification de console jusqu'à ce que vous vérifiiez que l'authentification LDAP fonctionne correctement. L'authentification de console fournit une manière de retourner à la configuration précédente. Référez-vous à la section de vérifier.

Vérifiez

Cette procédure décrit comment tester l'authentification LDAP.

1. Ouvrez une nouvelle session au central UCS, et écrivez le nom d'utilisateur et mot de passe. Vous n'avez pas besoin d'inclure un domaine ou un caractère avant le nom d'utilisateur. Cet exemple utilise des testucs en tant qu'utilisateur du domaine.
2. L'authentification LDAP est réussie si vous voyez le tableau de bord de central UCS. L'utilisateur est affiché au bas de page.

Dépannez

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

Informations connexes

- Support et documentation techniques - Cisco Systems