ACS 5.x : Exemple de configuration de serveur LDAP

Contenu

Introduction

Le Protocole LDAP (Lightweight Directory Access Protocol) est un protocole de réseau pour questionner et modifier les services d'annuaire qui s'exécutent sur le TCP/IP et l'UDP. Le LDAP est un mécanisme léger pour accéder à un serveur de répertoire x.500-based. RFC 2251 définit le LDAP.

Le Système de contrôle d'accès sécurisé Cisco (ACS) 5.x intègre avec une base de données externe de LDAP (également appelée une mémoire d'identité) à l'aide du protocole de LDAP. Il y a deux méthodes utilisées pour se connecter au serveur LDAP : texte brut (simple) et connexion SSL (chiffré). ACS 5.x peut être configuré pour se connecter au serveur LDAP utilisant chacun des deux méthodes. Ce document fournit un exemple de configuration pour connecter ACS 5.x à un serveur LDAP utilisant une connexion simple.

Conditions préalables

Conditions requises

Ce document suppose que l'ACS 5.x a une connexion IP au serveur LDAP et que le TCP 389 de port est ouvert.

Par défaut, le serveur LDAP de Microsoft Active Directory est configuré pour recevoir des

connexions de LDAP sur le TCP 389 de port. Si vous utilisez n'importe quel autre serveur LDAP, assurez-vous qu'il est en service et recevant des connexions sur le TCP 389 de port.

Composants utilisés

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

- Cisco Secure ACS 5.x
- Serveur LDAP de 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.

Informations générales

Service d'annuaire

Le service d'annuaire est une application logicielle ou un ensemble de demandes utilisées pour stocker et organiser des informations sur les utilisateurs et les ressources de réseau d'un réseau informatique. Vous pouvez utiliser le service d'annuaire afin de gérer l'accès client à ces ressources.

Le service de répertoire LDAP est basé sur un client-server model. Un client se connecte à un serveur LDAP afin de commencer une session de LDAP, et envoie des demandes d'exécution au serveur. Le serveur envoie alors ses réponses. Un ou plusieurs serveurs LDAP contiennent des données de l'arborescence de répertoire LDAP ou de la base de données de partie postérieure de LDAP.

Le service d'annuaire gère le répertoire, qui est la base de données qui tient les informations. Les services d'annuaire emploient un modèle distribué afin de stocker les informations, et ces informations sont habituellement répliquées entre les serveurs de répertoire.

Un répertoire LDAP est organisé dans une hiérarchie simple d'arborescence et peut être distribué parmi beaucoup de serveurs. Chaque serveur peut avoir une version répliquée de tout le répertoire qui est synchronisé périodiquement.

Une entrée dans l'arborescence contient un ensemble d'attributs, où chaque attribut a un nom (un type d'attribut ou une description d'attribut) et un ou plusieurs valeurs. Les attributs sont définis dans un schéma.

Chaque entrée a un identifiant unique appelé le son nom unique (DN). Ce nom contient le nom unique relatif (RDN) construit des attributs dans l'entrée, suivie du DN de l'entrée de parent. Vous pouvez penser au DN comme plein nom du fichier, et au RDN comme nom du fichier relatif dans

un répertoire.

Authentification utilisant le LDAP

ACS 5.x peut authentifier un principal contre une mémoire d'identité de LDAP en exécutant une exécution de grippage sur le serveur de répertoire afin de trouver et authentifier le principal. Si l'authentification réussit, ACS peut récupérer les groupes et les attributs qui appartiennent au principal. Les attributs à récupérer peuvent être configurés dans l'interface web ACS (pages de LDAP). Ces groupes et attributs peuvent être utilisés par ACS afin d'autoriser le principal.

Afin d'authentifier un utilisateur ou questionner la mémoire d'identité de LDAP, ACS se connecte au serveur LDAP et met à jour un groupe de connexion. Voir la Gestion de connexion de LDAP.

Gestion de connexion de LDAP

ACS 5.x prend en charge de plusieurs connexions simultanées de LDAP. Les connexions sont à la demande ouvert au moment de la première authentification LDAP. Le nombre maximal de connexions est configuré pour chaque serveur LDAP. Ouvrir des connexions raccourcit à l'avance le temps d'authentification.

Vous pouvez placer le nombre maximal de connexions pour utiliser pour les connexions obligatoires simultanées. Le nombre de connexions ouvertes peut être différent pour chaque serveur LDAP (primaire ou secondaire) et est déterminé selon le nombre maximal de connexions de gestion configurées pour chaque serveur.

ACS retient une liste de connexions ouvertes de LDAP (informations y compris de grippage) pour chaque serveur LDAP qui est configuré dans ACS. Pendant la procédure d'authentification, les tentatives de gestionnaire de connexion de trouver une connexion ouverte du groupe.

Si une connexion ouverte n'existe pas, un neuf est ouvert. Si le serveur LDAP fermait la connexion, le gestionnaire de connexion signale une erreur pendant le premier appel pour rechercher le répertoire, et des tentatives de renouveler la connexion.

Après que la procédure d'authentification soit complète, le gestionnaire de connexion libère la connexion au gestionnaire de connexion. Le pour en savoir plus, se rapportent au guide utilisateur ACS 5.X.

Configurez

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

Configurez ACS 5.x pour le LDAP

Terminez-vous ces étapes afin de configurer ACS 5.x pour le LDAP :

1. Choisissez les **utilisateurs et l'identité enregistre > identité externe enregistre > LDAP**, et le clic **créent** afin de créer une nouvelle connexion de LDAP.
2. Dans l'onglet Général, fournissez le **nom** et la **description** (facultatifs) pour le nouveau LDAP, et cliquez sur Next.

3. Dans l'onglet de connexion au serveur sous la section Serveur primaire, fournissez le **DN d'adresse Internet**, de **port**, d'**admin**, et le **mot de passe**. **Grippage de test de** clic au **serveur**.**Remarque:** Le numéro de port assigné par IANA pour le LDAP est le TCP 389. Cependant, confirmez le numéro de port que votre serveur LDAP utilise de votre admin de LDAP. Le DN et le mot de passe d'admin devraient t'être fournis par votre admin de LDAP. Votre DN d'admin devrait avoir indiqué toutes les autorisations sur tout l'OUs sur le serveur LDAP.
4. Cette image prouve que le **grippage de test de connexion au serveur** était réussi.**Remarque:** Si le grippage de test n'est pas réussi, re-vérifiez le **DN d'adresse Internet**, de **numéro de port**, d'**admin**, et le **mot de passe de** votre administrateur de LDAP.
5. Cliquez sur **Next** (Suivant).
6. Fournissez les détails requis dans l'onglet d'organisation de répertoire sous la section de schéma. De même, fournissez l'information requise sous la section de structure de répertoire de la manière prévue par votre admin de LDAP. **Configuration de test de** clic.
7. Cette image prouve que le **test de configuration** est réussi.**Remarque:** Si le test de configuration n'est pas réussi, re-vérifiez les paramètres fournis dans le **schéma** et la **structure de répertoire de** votre administrateur de LDAP.
8. Cliquez sur **Finish** (Terminer).
9. **Le serveur LDAP** est créé avec succès.

Configurez la mémoire d'identité

Concurrencent les étapes afin de configurer la mémoire d'identité :

1. Choisissez les **stratégies d'Access** > les **services d'accès** > les **règles de sélection de service**, et les vérifiez que le service va utiliser le serveur LDAP pour l'authentification. Dans cet exemple, l'authentification de serveur LDAP utilise le service **par défaut d'accès au réseau**.
2. Une fois que vous avez vérifié le service dans l'étape 1, allez au service particulier et cliquez sur les **protocoles permis**. Assurez-vous que **permettez PAP/ASCII** est sélectionné, et clique sur Submit.**Remarque:** Vous pouvez avoir d'autres Protocoles d'authentification sélectionnés avec pour permettre PAP/ASCII.
3. Cliquez sur en fonction le service identifié dans l'étape 1, et cliquez sur l'**identité**. Clic **choisi** à la droite du champ de source d'identité.
4. Sélectionnez le serveur LDAP de création récente (**myLDAP**, dans cet exemple), et cliquez sur OK.
5. **Modifications de sauvegarde de** clic.
6. Allez à la section d'autorisation du service identifié dans l'étape 1, et assurez-vous qu'il y a au moins une règle qui permet l'**authentification**.

Dépannez

ACS envoie une demande de grippage d'authentifier l'utilisateur contre un serveur LDAP. La demande de grippage contient le DN et le mot de passe utilisateur de l'utilisateur en texte clair. Un utilisateur est authentifié quand le DN et le mot de passe de l'utilisateur apparie le nom d'utilisateur et mot de passe dans le répertoire LDAP.

- **Erreurs d'authentification** - ACS se connecte des erreurs d'authentification dans les fichiers

journal ACS.

- **Erreurs d'initialisation** - Employez les configurations de délai d'attente de serveur LDAP afin de configurer le nombre de secondes qu'ACS attend une réponse d'un serveur LDAP avant de déterminer cela la connexion ou l'authentification sur ce serveur a manquée. Les possibles raison pour qu'un serveur LDAP renvoie une erreur d'initialisation sont :Le LDAP n'est pas pris en chargeLe serveur est en panneLe serveur est hors de mémoireL'utilisateur n'a aucun privilègeDes qualifications incorrectes d'administrateur sont configurées
- **Erreurs de grippage** - Les possibles raison pour qu'un serveur LDAP renvoie des erreurs de grippage (authentification) sont :Erreurs de filtrageUne recherche utilisant des critères de filtre échoueErreurs de paramètreDes paramètres non valides ont été entrésLe compte utilisateur est limité (désactivé, verrouillé, expiré, le mot de passe a expiré, et ainsi de suite)

Ces erreurs sont enregistré en tant qu'erreurs de ressource externe, indiquant un problème éventuel avec le serveur LDAP :

- Une erreur de connexion s'est produite
- Le délai d'attente a expiré
- Le serveur est en panne
- Le serveur est hors de mémoire

`L'utilisateur A n'existe pas dans l'erreur de base données` est enregistré comme erreur utilisateur inconnue.

`Un mot de passe incorrect était` erreur `écrite` est enregistré comme erreur de mot de passe incorrect, où l'utilisateur existe, mais le mot de passe envoyé est non valide.

Informations connexes

- Système de contrôle d'accès sécurisé Cisco
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems