ACS 5.X : Sécurisez l'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 serveur de contrôle d'accès (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 à connecter au serveur LDAP : texte brut (simple) et connexion SSL (chiffré). ACS 5.x peut être configuré pour se connecter au serveur LDAP utilisant les les deux les méthodes. Dans ce document l'ACS 5.x est configuré pour se connecter à un serveur LDAP utilisant la connexion cryptée.

Conditions préalables

Conditions requises

Ce document suppose qu'ACS 5.x a une connexion IP au serveur LDAP et le TCP 636 de port est ouvert.

Le serveur LDAP de Répertoire actif de Microsoft® doit être configuré pour recevoir les connexions sécurisées de LDAP sur le TCP 636 de port. Ce document suppose que vous avez le certificat racine de l'autorité de certification (CA) qui a fourni le certificat de serveur au serveur LDAP de Microsoft. Pour plus d'informations sur la façon configurer le serveur LDAP, référez-vous

à comment activer le LDAP au-dessus du SSL avec une tiers autorité de certification.

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, d'enregistrer et d'informations de organisation sur les utilisateurs et les ressources de réseau d'un réseau informatique. Vous pouvez utiliser le service d'annuaire pour gérer l'accès client à ces ressources.

Le service de répertoire LDAP est basé sur un client-server model. Un client commence une session de LDAP par se connecter à un serveur 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 utilisent un modèle distribué pour 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 : 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 pour 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 pour 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.

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 essais pour 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.

Installez le certificat de CA de racine sur ACS 5.x

Terminez-vous ces étapes afin d'installer un certificat de CA de racine sur le Cisco Secure ACS 5.x :

Remarque: Assurez-vous que le serveur LDAP est préconfiguré pour recevoir des connexions cryptées sur le TCP 636 de port. Pour plus d'informations sur la façon configurer le serveur LDAP de Microsoft, référez-vous à comment activer le LDAP au-dessus du SSL avec une tiers autorité de certification.

1. Choisissez les **utilisateurs et l'identité enregistre** > des **autorités de certification**, puis clique

sur Add afin d'ajouter le certificat racine du CA qui a fourni le certificat de serveur au serveur LDAP de Microsoft.
2. Àpartir du **fichier du certificat pour importer la** section, le clic **parcourent** à côté du **fichier du certificat** afin de rechercher le fichier du certificat.
3. Choisissez le **fichier du certificat** requis (le certificat racine du CA qui a fourni le certificat de serveur au serveur LDAP de Microsoft) et cliquez sur **ouvert**.
4. Fournissez une **description** dans l'espace prévu à côté de la description et cliquez sur Submit.Cette image prouve que le certificat racine a été correctement installé :

Configurez ACS 5.X pour le LDAP sécurisé

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

1. Choisissez les **utilisateurs et l'identité enregistre > identité externe enregistre > LDAP** et le clic **créent** pour créer une nouvelle connexion de LDAP.
2. **De l'onglet Général** fournissez le **nom** et le **Description(optional)** pour le nouveau LDAP, puis cliquez sur Next.
3. De 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**. Assurez-vous que la case à cocher à côté de l'**authentification sécurisée d'utilisation** est vérifiée et choisissez le **certificat de CA** récemment installé de **racine**. **Grippage de test de** clic au **serveur**.**Remarque:** Le numéro de port assigné par IANA pour le LDAP sécurisé est le TCP 636. Cependant, confirmez le numéro de port que votre serveur LDAP utilise de votre admin de LDAP.**Remarque:** Le DN et le mot de passe d'admin devraient t'être fournis par votre admin de LDAP. Le DN d'admin doit avoir indiqué toutes les autorisations sur tout l'OUs sur le serveur LDAP.La prochaine image prouve que le **grippage de test de connexion au serveur** était réussi.**Remarque:** Si le grippage de test n'est pas réussi puis re-vérifiez le **DN d'adresse Internet, de numéro de port, d'admin, le mot de passe** et la **racine CA de** votre administrateur de LDAP.
4. Cliquez sur **Next** (Suivant).
5. De l'onglet d'**organisation de répertoire** sous la section de **schéma**, fournissez les détails requis. 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.La prochaine image prouve que le **test de configuration** est réussi.**Remarque:** Si le test de configuration n'est pas réussi puis re-vérifiez les paramètres fournis dans le **schéma** et la **structure de répertoire de** votre administrateur de LDAP.
6. Cliquez sur **Finish** (Terminer).**Le serveur LDAP** est créé avec succès.

Configurez la mémoire d'identité

Concurrencent ces 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 sécurisent le serveur LDAP pour l'authentification. Dans cet exemple le service est **accès au réseau par défaut**.
2. Après que vous ayez vérifié le service dans l'étape 1, allez au service particulier et cliquez sur les **protocoles permis**. Assurez que qui **laissent PAP/ASCII** est sélectionné, puis clique sur Submit.**Remarque:** Vous pouvez avoir d'autres Protocoles d'authentification sélectionnés avec pour permettre PAP/ASCII.

3. Cliquez sur le service identifié dans l'étape 1, puis cliquez sur l'**identité**. Clic **choisi** à côté de la **source d'identité**.
4. Sélectionnez le de création récente **sécurisent le serveur LDAP** (**myLDAP** dans cet exemple), puis cliquent 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

L'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 pour configurer le nombre de secondes que l'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, qui indique 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

Cette erreur est enregistré comme erreur utilisateur inconnue : `Un utilisateur n'existe pas dans la base de données.`

Cette erreur est enregistré comme erreur de mot de passe incorrect, où l'utilisateur existe, mais le mot de passe envoyé est non valide : `Un mot de passe incorrect a été entré.`

Informations connexes

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