Configurez l'ISE pour l'intégration avec un serveur LDAP

Contenu

Introduction

Ce document décrit comment configurer un Logiciel Cisco Identity Services Engine (ISE) pour l'intégration avec un serveur de Protocole LDAP (Lightweight Directory Access Protocol) de Cisco.

> **Note**: Ce document est valide pour les installations qui utilisent le LDAP comme source extérieure d'identité pour l'authentification et l'autorisation ISE.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Les informations ce document sont basées sur des ces logiciel et versions de matériel :

- Version 1.3 de Cisco ISE avec le correctif 2
- La version 7 x64 de Microsoft Windows avec OpenLDAP a installé
- Version 8.0.100.0 Sans fil du contrôleur LAN de Cisco (WLC)
- Version 3.1 de Cisco AnyConnect pour Microsoft Windows
- Éditeur de profil de gestionnaire d'accès au réseau de Cisco

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.

Informations générales

Ces méthodes d'authentification sont prises en charge avec le LDAP :

- Generic Token Card (EAP-GTC) du Â d'âÂ d'Extensible Authentication Protocol
- Transport Layer Security de du Â d'âÂ d'Extensible Authentication Protocol (EAP-TLS)
- Transport Layer Security de du Â d'âÂ de Protected Extensible Authentication Protocol (PEAP-TLS)

Configurez

Cette section décrit comment configurer les périphériques de réseau et intégrer l'ISE avec un serveur LDAP.

Diagramme du réseau

Dans cet exemple de configuration, le point final utilise un adaptateur Sans fil afin de s'associer avec le réseau Sans fil. Le RÉSEAU LOCAL Sans fil (WLAN) sur le WLC est configuré afin d'authentifier les utilisateurs par l'intermédiaire de l'ISE. Sur l'ISE, le LDAP est configuré comme mémoire externe d'identité.

Cette image illustre la topologie du réseau qui est utilisée :

Configurez OpenLDAP

L'installation de l'OpenLDAP pour Microsoft Windows est terminée par l'intermédiaire du GUI, et elle est simple. L'emplacement par défaut est **C : > OpenLDAP**. Après installation, vous devriez voir ce répertoire :

Notez deux répertoires en particulier :

- Le du Â d'âÂ de **ClientTools** ce répertoire inclut un ensemble de binaires qui sont utilisées afin d'éditer la base de données de LDAP.

- le du Â d'âÂ de **ldifdata** ceci est l'emplacement dans lequel vous devriez enregistrer les fichiers avec des objets de LDAP.

Ajoutez cette structure à la base de données de LDAP :

Sous le répertoire racine, vous devez configurer deux unités organisationnelles (OUs). L'OU d'*OU=groups* devrait avoir un groupe enfants (**cn=domainusers** dans cet exemple). L'OU d'*OU=people* définit les deux comptes utilisateurs qui appartiennent au groupe de *cn=domainusers*.

Afin de remplir base de données, vous devez créer le fichier de *ldif* d'abord. La structure précédemment mentionnée a été créée à partir de ce fichier :

```
dn: ou=groups,dc=maxcrc,dc=com
changetype: add
ou: groups
description: All groups in organisation
objectclass: organizationalunit

dn: ou=people,dc=maxcrc,dc=com
changetype: add
ou: people
description: All people in organisation
objectclass: organizationalunit

dn: uid=john.doe,ou=people,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: john.doe
givenName: John
sn: Doe
cn: John Doe
mail: john.doe@example.com
userPassword: password

dn: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: jan.kowalski
givenName: Jan
sn: Kowalski
cn: Jan Kowalski
mail: jan.kowalski@example.com
userPassword: password

dn: cn=domainusers,ou=groups,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: posixGroup
gidNumber: 678
memberUid: uid=john.doe,ou=people,dc=maxcrc,dc=com
```

```
memberUid: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
```

Afin d'ajouter les objets à la base de données de LDAP, vous pouvez utiliser la binaire de **ldapmodify** :

```
C:\OpenLDAP\ClientTools>ldapmodify.exe -a -x -h localhost -p 389 -D "cn=Manager,
dc=maxcrc,dc=com" -w secret -f C:\OpenLDAP\ldifdata\test.ldif
ldap_connect_to_host: TCP localhost:389
ldap_new_socket: 496
ldap_prepare_socket: 496
ldap_connect_to_host: Trying ::1 389
ldap_pvt_connect: fd: 496 tm: -1 async: 0
attempting to connect:
connect success
adding new entry "ou=groups,dc=maxcrc,dc=com"

adding new entry "ou=people,dc=maxcrc,dc=com"

adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

adding new entry "uid=jan.kowalski,ou=people,dc=maxcrc,dc=com"

adding new entry "cn=domainusers,ou=groups,dc=maxcrc,dc=com"
```

Intégrez OpenLDAP avec l'ISE

Utilisez les informations qui sont fournies dans les images dans toute cette section afin de configurer le LDAP comme mémoire externe d'identité sur l'ISE.

Vous pouvez configurer ces attributs de l'*onglet Général* :

- Le **soumis du** Â d'âÂ d'**Objectclass** ce champ correspond à la classe d'objets des comptes utilisateurs dans le fichier de *ldif*. Selon la configuration de LDAP, vous pouvez utiliser une de quatre classes ici :

  Dessus

  Personne

  OrganizationalPerson

  InetOrgPerson

- Le du Â d'âÂ d'**attribut de nom du sujet** ceci est l'attribut qui est récupéré par le LDAP quand l'ISE s'enquiert si un nom d'utilisateur spécifique est inclus dans une base de données. Dans ce scénario, vous devez utiliser **john.doe ou** jan.kowalskias le nom d'utilisateur sur le point final.

- Le du Â d'âÂ d'**Objectclass de groupe** ce champ correspond à la classe d'objets pour un groupe dans le fichier de *ldif*. Dans ce scénario, la classe d'objets pour le groupe de *cn=domainusers* est **posixGroup**.

- Le du Â d'âÂ d'**attribut de carte de groupe** cet attribut définit comment les utilisateurs sont tracés aux groupes. Sous le groupe de *cn=domainusers* dans le fichier de *ldif*, vous pouvez voir deux attributs de *memberUid* qui correspondent aux utilisateurs.

L'ISE offre également quelques schémas préconfigurés (Microsoft Active Directory, Sun, Novell) :

Après que vous placiez l'adresse IP et le nom corrects de domaine administratif, vous pouvez *tester le grippage au* serveur. En ce moment, vous ne devriez récupérer aucun sujets ou groupes parce que les bases de recherche ne sont pas encore configurées.

Dans le prochain onglet, vous pouvez configurer la base de recherche de sujet/groupe. C'est le point de *joindre* pour l'ISE au LDAP. Vous pouvez récupérer seulement les sujets et les groupes qui sont des enfants de votre point se joignant. Dans ce scénario, les sujets de l'*OU=people* et les groupes de l'*OU=groups* sont récupérés :

Des groupes onglet, vous pouvez importer les groupes du LDAP sur l'ISE :

Configurez le WLC

Utilisez les informations qui sont fournies dans ces images afin de configurer le WLC pour l'authentification de 802.1x :

Configurez EAP-GTC

Une des méthodes d'authentification prises en charge pour le LDAP est EAP-GTC. Il est disponible dans le Cisco AnyConnect, mais vous devez installer l'éditeur de profil de gestionnaire d'accès au réseau afin de configurer le profil correctement. Vous devez également éditer la configuration du gestionnaire d'accès au réseau, qui par défaut se trouve ici :

C : > ProgramData > Cisco > Client à mobilité sécurisé Cisco AnyConnect > gestionnaire d'accès au réseau > système > fichier configuration.xml

Utilisez les informations qui sont fournies dans ces images afin de configurer l'EAP-GTC sur le point final :

Utilisez les informations qui sont fournies dans ces images afin de changer les stratégies d'authentification et d'autorisation sur l'ISE :

Après que vous appliquiez la configuration, vous devriez pouvoir se connecter au réseau :

Vérifiez

Afin de vérifier les configurations de LDAP et ISE, vous devriez pouvoir récupérer les sujets et les groupes avec une connexion de test au serveur :

Ces images illustrent un état d'échantillon de l'ISE :

Dépannez

Cette section décrit quelques erreurs communes qui sont produites avec cette configuration et comment les dépanner :

- Après installation de l'OpenLDAP, vous pourriez rencontrer une erreur pour indiquer qu'un **gssapi.dll** manque. Afin d'éliminer l'erreur, vous devez redémarrer Microsoft Windows.

- Il ne pourrait pas être possible d'éditer le *fichier configuration.xml* pour le Cisco AnyConnect directement. Sauvegardez votre nouvelle configuration dans un autre emplacement et puis employez-la pour remplacer l'ancien fichier.

- Dans l'état d'authentification, vous pourriez voir ce message d'erreur :

  `Authentication method is not supported by any applicable identity store`
  Ce message d'erreur indique que la méthode que vous avez sélectionnée n'est pas prise en charge par LDAP. Assurez-vous que l'*authentification Protocol* dans le même état affiche une des méthodes prises en charge (EAP-GTC, EAP-TLS, ou PEAP-TLS).

- Dans l'état d'authentification, vous pourriez noter que le sujet n'a pas été trouvé dans la mémoire d'identité. Ceci signifie que le nom d'utilisateur de l'état n'apparie pas l'*attribut de nom du sujet* pour aucun utilisateur dans la base de données de LDAP. Dans ce scénario, la valeur a été placée à l'**uid** pour cet attribut, ainsi il signifie que l'ISE regarde aux valeurs d'*uid* pour l'utilisateur de LDAP quand il tente de trouver une correspondance.

- Les sujets et les groupes ne pourraient pas être récupérés correctement pendant un *grippage au* test de *serveur*. La cause la plus probable de cette question est une configuration incorrecte pour les bases de recherche. Souvenez-vous que la hiérarchie de LDAP doit être spécifiée de la feuille-à-racine et du *C.C* (peut se composer de plusieurs mots).

  Conseil : Afin de dépanner l'authentification EAP du côté WLC, référez-vous à l'authentification EAP avec le document Cisco d'exemple de configuration des contrôleurs WLAN (WLC).