Configurer MDS LDAP

Contenu

Introduction

Ce document fournit un exemple de configuration pour la configuration LDAP de base (Lightweight Directory Access Protocol) sur les commutateurs de données multicouches (MDS). Quelques commandes sont également répertoriées afin de montrer comment tester et valider la configuration sur les commutateurs MDS qui exécutent NX-OS.

Le protocole LDAP fournit une validation centralisée des utilisateurs qui tentent d'accéder à un périphérique Cisco MDS. Les services LDAP sont gérés dans une base de données sur un démon LDAP qui s'exécute généralement sur une station de travail UNIX ou Windows NT. Vous devez avoir accès à un serveur LDAP et le configurer avant que les fonctionnalités LDAP configurées sur votre périphérique Cisco MDS ne soient disponibles.

LDAP fournit des fonctions d'authentification et d'autorisation distinctes. LDAP permet un serveur de contrôle d'accès unique (le démon LDAP) afin de fournir chaque authentification et autorisation de service indépendamment. Chaque service peut être lié à sa propre base de données afin de tirer parti des autres services disponibles sur ce serveur ou sur le réseau, en fonction des capacités du démon.

Le protocole client/serveur LDAP utilise TCP (port TCP 389) pour les besoins de transport. Les périphériques Cisco MDS fournissent une authentification centralisée avec l'utilisation du protocole LDAP.

Conditions préalables

Conditions requises

Cisco indique que le compte utilisateur Active Directory (AD) doit être configuré et validé. Actuellement, Cisco MDS prend en charge Description et MemberOf en tant que noms d'attribut. Configurez le rôle utilisateur avec ces attributs dans le serveur LDAP.

Components Used

Les informations de ce document ont été testées sur un MDS 9148 qui exécute NX-OS Version

6.2(7). La même configuration doit fonctionner pour les autres plates-formes MDS ainsi que pour les versions NX-OS. Le serveur LDAP de test se trouve à l'adresse 10.2.3.7.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Entrez cette commande sur le commutateur MDS afin de vous assurer que vous avez accès à la console dans le commutateur pour la récupération :

```
aaa authentication login console local
```

Activez la fonctionnalité LDAP et créez un utilisateur qui sera utilisé pour la liaison racine. « Admin » est utilisé dans cet exemple :

```
feature ldap
ldap-server host 10.2.3.7 rootDN "cn=Admin,cn=Users,dc=ciscoprod,dc=com"
password fewhg port 389
```

Àce stade sur le serveur LDAP, vous devez créer un utilisateur (tel que cpam). Dans l'attribut description, ajoutez cette entrée :

```
shell:roles="network-admin"
```

Ensuite, dans le commutateur, vous devez créer une carte de recherche. Ces exemples montrent Description et MemberOf comme nom-attribut :

Pour la description :

```
ldap search-map s1

   userprofile attribute-name "description" search-filter "cn=$userid"
base-DN "dc=ciscoprod,dc=com"
```

Pour MemberOf :

```
ldap search-map s2

  userprofile attribute-name "memberOf" search-filter "cn=$userid"
base-DN "dc=ciscoprod,dc=com"
```

Par exemple, si ces trois utilisateurs sont membres du groupe abc dans le serveur AD, le commutateur MDS doit avoir le nom de rôle abc créé avec les autorisations requises.

Utilisateur1 - Membre du groupe abc
Utilisateur2 - Membre du groupe abc
Utilisateur3 - Membre du groupe abc

```
role name abc
   rule 1 permit clear
   rule 2 permit config
```

```
   rule 3 permit debug
   rule 4 permit exec
   rule 5 permit show
```

Maintenant, si l'utilisateur 1 se connecte au commutateur et que l'attribut memberOf est configuré pour LDAP , alors l'utilisateur 1 se voit attribuer le rôle abc qui possède tous les droits d'administrateur.

Il existe également deux conditions requises lorsque vous configurez l'attribut memberOf.

1. Le nom de rôle de chaque commutateur doit correspondre au nom du groupe de serveurs AD, OU
2. Créez un groupe sur le serveur AD avec le nom « network-admin » et configurez tous les utilisateurs requis en tant que membres du groupe network-admin.

Remarques :
-Les memberOf est pris en charge uniquement par le serveur LDAP Windows AD. Le serveur OpenLDAP ne prend pas en charge l'attribut memberOf.
- La configuration memberOf n'est prise en charge que dans NX-OS 6.2(1) et versions ultérieures.

Ensuite, créez un groupe AAA (Authentication, Authorization, and Accounting) avec un nom approprié et associez un mappage de recherche LDAP précédemment créé. Comme indiqué précédemment, vous pouvez utiliser Description ou MemberOf en fonction de vos préférences. Dans l'exemple présenté ici, s1 est utilisé pour la description de l'authentification utilisateur. Si l'authentification doit être terminée avec MemberOf, alors s2 peut être utilisé à la place.

```
aaa group server ldap ldap2
server 10.2.3.7
ldap-search-map s1

aaa authentication login default group ldap2
```

En outre, cette configuration rétablit l'authentification en local en cas d'inaccessibilité du serveur LDAP. Il s'agit d'une configuration facultative :

```
aaa authentication login default fallback error local
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Afin de vérifier si LDAP fonctionne correctement à partir du commutateur MDS lui-même, utilisez ce test :

```
MDSA# test aaa group ldap2 cpam Cisco_123
user has been authenticated

MDSA#
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Certaines commandes d'affichage (« **show** ») sont offertes par l'outil « Cisco CLI Analyzer » réservé aux clients inscrits. Utilisez cet outil pour obtenir une analyse des rapports produits par ces commandes.

Voici quelques commandes utiles à utiliser pour résoudre les problèmes :

- **show ldap-server**
- **show ldap-server groups**
- **show ldap-server statistics 10.2.3.7**
- **show aaa authentication**

```
MDSA# show ldap-server
timeout : 5
port : 389
deadtime : 0
total number of servers : 1

following LDAP servers are configured:
10.2.3.7:
idle time:0
test user:test
test password:********
test DN:dc=test,dc=com
timeout: 5 port: 389 rootDN: cn=Admin,cn=Users,dc=ciscoprod,dc=com
enable-ssl: false

MDSA# show ldap-server groups
total number of groups: 1

following LDAP server groups are configured:
group ldap2:
Mode: UnSecure
Authentication: Search and Bind
Bind and Search : append with basedn (cn=$userid)
Authentication: Do bind instead of compare
Bind and Search : compare passwd attribute userPassword
Authentication Mech: Default(PLAIN)
server: 10.2.3.7 port: 389 timeout: 5
Search map: s1

MDSA# show ldap-server statistics 10.2.3.7
Server is not monitored

Authentication Statistics
failed transactions: 2
successful transactions: 11
requests sent: 36
requests timed out: 0
responses with no matching requests: 0
responses not processed: 0
responses containing errors: 0
MDSA# show ldap-search-map
total number of search maps : 1

following LDAP search maps are configured:
SEARCH MAP s1:
User Profile:
BaseDN: dc=ciscoprod,dc=com
Attribute Name: description
Search Filter: cn=$userid
```

```
MDSA# show aaa authentication
default: group ldap2
console: local
dhchap: local
iscsi: local
MDSA#
```

Informations connexes

- Guide de configuration de la sécurité NX-OS de la gamme Cisco MDS 9000 - Configuration de LDAP
- Support et documentation techniques - Cisco Systems