Configurez le LDAP MDS

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour la configuration de base de LDAP (protocole LDAP) sur les commutateurs de données multicouche (MDS). Quelques commandes sont également répertoriées afin d'afficher comment tester et valider la configuration sur les Commutateurs MDS qui exécutent NX-OS.

Le LDAP fournit la validation centralisée des utilisateurs qui tentent d'accéder à un périphérique de Cisco MDS. Des services de LDAP sont mis à jour dans une base de données sur un démon de LDAP qui s'exécute typiquement sur un poste de travail UNIX ou de Windows NT. Vous devez avoir accès à et devez configurer un serveur LDAP avant que les caractéristiques configurées de LDAP sur votre périphérique de Cisco MDS soient disponibles.

Le LDAP prévoit les équipements distincts d'authentification et d'autorisation. Le LDAP tient compte d'un serveur simple de contrôle d'accès (le démon de LDAP) afin de fournir chaque authentification et autorisation de service indépendamment. Chaque service peut être attaché dans sa propre base de données afin de tirer profit d'autres services disponibles sur ce serveur ou sur le réseau, dépendant sur les capacités du démon.

Le protocole de client/serveur de LDAP utilise le TCP (port TCP 389) pour des conditions requises de transport. Les périphériques de Cisco MDS fournissent à l'authentification centralisée l'utilisation du protocole de LDAP.

Conditions préalables

Conditions requises

Cisco déclare que le compte utilisateur de Répertoire actif (AD) devrait être configuré et validé. Actuellement, description de supports de Cisco MDS et MemberOf en tant que noms d'attribut. Configurez le rôle de l'utilisateur avec ces attributs dans le serveur LDAP.

Composants utilisés

Les informations dans ce document ont été testées sur un MDS 9148 qui exécute la version 6.2(7)

NX-OS. La même configuration devrait fonctionner pour d'autres Plateformes MDS aussi bien que versions NX-OS. Le serveur LDAP de test se trouve chez 10.2.3.7.

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.

Configurez

Sélectionnez cette commande sur le commutateur MDS afin de vous veiller pour avoir accès de console dans le commutateur pour la reprise :

```
aaa authentication login console local
```

Activez la caractéristique de LDAP et créez un utilisateur qui sera utilisé pour l'attache de racine. Le « 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
```

En ce moment sur le serveur LDAP vous devriez créer un utilisateur (tel que le cpam). Dans l'attribut de description ajoutez cette entrée :

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

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

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 des membres d'ABC de groupe dans le serveur d'AD, puis le commutateur MDS doit avoir l'ABC de role name créé avec des autorisations exigées.

User1 - Membre d'ABC de groupe
User2 - Membre d'ABC de groupe
User3 - Membre d'ABC de groupe

```
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 User1 ouvre une session au commutateur et le memberOf d'attribut est configuré pour le LDAP, puis User1 est assigné l'ABC de rôle qui a tous les droits d'admin.

Il y a également deux conditions requises quand vous configurez l'attribut de memberOf.

1. La role name de l'un ou l'autre de commutateur devrait s'assortir avec le nom de groupe de serveurs d'AD, OU
2. Créez un groupe sur le serveur d'AD avec le nom « réseau-admin » et configurez tous les utilisateurs requis en tant que membre du groupe de réseau-admin.

   Remarques :
   - L'attribut de memberOf est seulement pris en charge par le serveur LDAP d'AD de Windows. Le serveur d'OpenLDAP ne prendra en charge pas l'attribut de memberOf.
   - La configuration de memberOf est seulement prise en charge dans NX-OS 6.2(1) et plus tard.

Ensuite, créez un groupe d'Authentification, autorisation et comptabilité (AAA) avec un nom approprié et liez une carte précédemment créée de recherche de LDAP. Comme précédemment remarquable, vous pouvez utiliser la description ou le MemberOf basé sur votre préférence. Dans l'exemple présenté ici, le S1 est utilisé pour la description pour l'authentification de l'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 retournera l'authentification aux gens du pays au cas où le serveur LDAP serait inaccessible. C'est une configuration facultative :

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

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

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

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

MDSA#
```

Dépannez

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

L'analyseur de Cisco CLI (clients enregistrés seulement) prend en charge certaines **commandes show**. Employez l'analyseur de Cisco CLI afin de visualiser une analyse de sortie de commande show.

Quelques commandes utiles de utiliser pour dépanner des questions sont affichées ici :

- **show ldap-server**
- **groupes de show ldap-server**

- statistiques 10.2.3.7 de show ldap-server
- 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 sécurité de la famille NX-OS du Cisco MDS 9000 - Configurer le LDAP
- Support et documentation techniques - Cisco Systems