Konfigurieren von MDS LDAP

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für eine grundlegende LDAP-Konfiguration (Lightweight Directory Access Protocol) auf Multilayer Data Switches (MDS). Es sind auch einige Befehle aufgelistet, um zu zeigen, wie die Konfiguration auf MDS-Switches getestet und validiert wird, auf denen NX-OS ausgeführt wird.

Das LDAP bietet eine zentralisierte Validierung von Benutzern, die versuchen, auf ein Cisco MDS-Gerät zuzugreifen. LDAP-Dienste werden in einer Datenbank auf einem LDAP-Daemon verwaltet, der in der Regel auf einer UNIX- oder Windows NT-Workstation ausgeführt wird. Sie müssen über Zugriff auf einen LDAP-Server verfügen und diesen konfigurieren, bevor die konfigurierten LDAP-Funktionen auf Ihrem Cisco MDS-Gerät verfügbar sind.

LDAP bietet separate Authentifizierungs- und Autorisierungsfunktionen. LDAP ermöglicht einen einzelnen Zugriffskontrollserver (den LDAP-Daemon), um jede Service-Authentifizierung und -Autorisierung unabhängig voneinander bereitzustellen. Jeder Dienst kann in seine eigene Datenbank eingebunden werden, um andere Dienste nutzen zu können, die auf diesem Server oder im Netzwerk verfügbar sind, abhängig von den Funktionen des Daemons.

Das LDAP-Client-/Serverprotokoll verwendet TCP (TCP-Port 389) für die Transportanforderungen. Cisco MDS-Geräte ermöglichen eine zentralisierte Authentifizierung mithilfe des LDAP-Protokolls.

Voraussetzungen

Anforderungen

Cisco gibt an, dass das Active Directory-Benutzerkonto (AD) konfiguriert und validiert werden soll. Derzeit unterstützt Cisco MDS Description und MemberOf als Attributnamen. Konfigurieren Sie die Benutzerrolle mit diesen Attributen im LDAP-Server.

Verwendete Komponenten

Die Informationen in diesem Dokument wurden auf einem MDS 9148 getestet, auf dem NX-OS Version 6.2(7) ausgeführt wird. Dieselbe Konfiguration sollte für andere MDS-Plattformen und NX-

OS-Versionen verwendet werden. Der Test-LDAP-Server befindet sich unter 10.2.3.7.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Geben Sie den folgenden Befehl auf dem MDS-Switch ein, um sicherzustellen, dass Sie über Konsolenzugriff auf den Switch verfügen, um ihn wiederherzustellen:

```
aaa authentication login console local
```

Aktivieren Sie die LDAP-Funktion, und erstellen Sie einen Benutzer, der für die Root-Bindung verwendet wird. In diesem Beispiel wird "Admin" verwendet:

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

An diesem Punkt auf dem LDAP-Server sollten Sie einen Benutzer (z. B. cpam) erstellen. Fügen Sie im description-Attribut diesen Eintrag hinzu:

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

Als Nächstes müssen Sie im Switch eine Suchzuordnung erstellen. In diesen Beispielen werden Description und MemberOf als Attributname angezeigt:

Zur Beschreibung:

```
ldap search-map s1

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

Für Mitglied von:

```
ldap search-map s2

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

Wenn diese drei Benutzer z. B. Mitglieder der Gruppe abc im AD-Server sind, muss der MDS-Switch über den Namen abc verfügen, der mit den erforderlichen Berechtigungen erstellt wurde.

Benutzer1 - Mitglied der Gruppe abc
User2 - Mitglied der Gruppe abc
Benutzer3 - Mitglied der Gruppe abc

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

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

Wenn sich Benutzer1 nun beim Switch anmeldet und das Attribut memberOf für LDAP konfiguriert ist, wird User1 die Rolle abc zugewiesen, die über alle Administratorrechte verfügt.

Beim Konfigurieren des memberOf-Attributs gibt es auch zwei Anforderungen.

1. Der Rollenname eines Switches muss mit dem AD-Servergruppennamen übereinstimmen, ODER
2. Erstellen Sie auf dem AD-Server eine Gruppe mit dem Namen "network-admin", und konfigurieren Sie alle erforderlichen Benutzer als Mitglied der Netzwerk-Admin-Gruppe.

Hinweise:
- die memberOf-Attribut wird nur vom Windows AD-LDAP-Server unterstützt. Der OpenLDAP-Server unterstützt das memberOf-Attribut nicht.
- Der MemberOf-Konfiguration wird nur in NX-OS 6.2(1) und höher unterstützt.

Erstellen Sie anschließend eine AAA-Gruppe (Authentication, Authorization, and Accounting) mit einem entsprechenden Namen, und binden Sie eine zuvor erstellte LDAP-Suchzuordnung. Wie bereits erwähnt, können Sie je nach Präferenz entweder Description (Beschreibung) oder MemberOf verwenden. Im hier gezeigten Beispiel wird s1 für die Beschreibung zur Benutzerauthentifizierung verwendet. Wenn die Authentifizierung mit MemberOf abgeschlossen werden soll, kann stattdessen s2 verwendet werden.

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

aaa authentication login default group ldap2
```

Diese Konfiguration setzt die Authentifizierung auch dann auf lokal zurück, wenn der LDAP-Server nicht erreichbar ist. Dies ist eine optionale Konfiguration:

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

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Verwenden Sie den folgenden Test, um zu überprüfen, ob das LDAP vom MDS-Switch selbst ordnungsgemäß funktioniert:

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

MDSA#
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Der Cisco CLI Analyzer (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie den Cisco CLI Analyzer, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Hier sind einige nützliche Befehle zur Fehlerbehebung aufgeführt:

- **show ldap-server**
- **LDAP-Servergruppen anzeigen**
- **ldap-server statistics 10.2.3.7 anzeigen**
- **Authentifizierung anzeigen**

```
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#
```

Zugehörige Informationen

- Cisco MDS 9000-Produktfamilie - NX-OS-Sicherheitskonfigurationsleitfaden - Konfigurieren von LDAP
- Technischer Support und Dokumentation - Cisco Systems