MDS LDAP configureren

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor de basis-LDAP-configuratie (Lichtgewicht Directory Access Protocol) op Multilayer Data Switches (MDS). Een paar opdrachten zijn ook in de lijst opgenomen om te laten zien hoe de configuratie op MDS-switches moet worden getest en gevalideerd die NX-OS uitvoeren.

De LDAP biedt gecentraliseerde validatie van gebruikers die toegang tot een Cisco MDS-apparaat proberen te verkrijgen. De diensten van LDAP worden onderhouden in een database op een LDAP-datum die doorgaans op een UNIX- of Windows NT-werkstation draait. U moet toegang hebben tot en een LDAP server configureren voordat de geconfigureerde LDAP-functies op uw Cisco MDS-apparaat beschikbaar zijn.

LDAP voorziet in aparte echtheids- en vergunningsfaciliteiten. LDAP maakt het mogelijk één enkele toegangscontroleserver (de LDAP-datum) te gebruiken om elke verificatie en autorisatie op onafhankelijke wijze te waarborgen. Elke dienst kan in zijn eigen database worden gebonden om gebruik te maken van andere diensten die beschikbaar zijn op die server of op het netwerk, afhankelijk van de mogelijkheden van de daemon.

Het LDAP client/server protocol gebruikt TCP (TCP poort 389) voor transportvereisten. Cisco MDS-apparaten bieden gecentraliseerde verificatie met behulp van het LDAP-protocol.

Voorwaarden

Vereisten

Cisco stelt dat de AD-gebruikersaccount (Active Directory) moet worden geconfigureerd en gevalideerd. Op dit moment ondersteunt Cisco MDS Beschrijving en LidOf als attributennamen. Configureer de gebruikersrol met deze eigenschappen in de LDAP server.

Gebruikte componenten

De informatie in dit document is getest op een MDS 9148 met NX-OS versie 6.2(7). Dezelfde configuratie dient te werken voor andere MDS-platforms en NX-OS-versies. De test LDAP server

bevindt zich op 10.2.3.7.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Typ deze opdracht in de MDS-schakelaar om er zeker van te zijn dat u toegang tot de console hebt voor herstel:

```
aaa authentication login console local
```

Schakel de LDAP-functie in en maak een gebruiker die voor de wortelbinding wordt gebruikt. "Admin" wordt in dit voorbeeld gebruikt:

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

Op dit punt op de LDAP server moet u een gebruiker (zoals SCM) maken. Voeg in de eigenschap beschrijving deze vermelding toe:

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

Daarna, in de switch moet je een zoekkaart maken. Deze voorbeelden geven een beschrijving en een lid van de eigenschap aan:

Omschrijving:

```
ldap search-map s1

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

Voor lidVan:

```
ldap search-map s2

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

Als deze drie gebruikers bijvoorbeeld leden van groep abc in de AD server zijn, moet de MDS switch de rolnaam abc hebben gemaakt met de vereiste rechten.

Gebruiker1 - Lid van groep abc
Gebruiker2 - Lid van groep abc
Gebruiker3 - Lid van groep abc

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

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

Als Gebruiker1 inlogt op de schakelaar en het attribuut lidOf wordt ingesteld voor LDAP, dan wordt Gebruiker1 toegewezen aan de rollenbank die alle adminerechten heeft.

Er zijn ook twee vereisten wanneer u het lidOf attribuut vormt.

1. Ofwel dient de rolnaam van de switch overeen te komen met de naam van de AD-servergroep, ofwel
2. Maak een groep op de AD server met de naam "netwerk-beheerder" en stel alle vereiste gebruikers in als lid van de netwerk-beheerder groep.

   Opmerkingen:
   - de LidOf-eigenschap wordt alleen ondersteund door de Windows AD LDAP-server. De OpenLDAP-server ondersteunt de eigenschap LidOf niet.
   - Het lid van de configuratie wordt alleen ondersteund in NX-OS 6.2(1) en hoger.

Maak vervolgens een AAA-groep (Verificatie, autorisatie en accounting) met een juiste naam en verbind een eerder gemaakte LDAP-zoekkaart. Zoals eerder opgemerkt, kunt u ofwel Beschrijving ofwel LidOf op basis van uw voorkeur gebruiken. In het hier weergegeven voorbeeld wordt s1 gebruikt voor de Beschrijving voor gebruikersverificatie. Indien de echtheidscontrole met LidOf moet worden voltooid, kan s2 in plaats daarvan worden gebruikt.

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

aaa authentication login default group ldap2
```

Ook zal deze configuratie de verificatie terugbrengen naar de lokale taal voor het geval de LDAP server onbereikbaar is. Dit is een optionele configuratie:

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

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Gebruik deze test om te controleren of de LDAP vanuit de MDS-schakelaar zelf werkt:

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

MDSA#
```

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

De Cisco CLI Analyzer (alleen geregistreerde klanten) ondersteunt bepaalde **show-**opdrachten.

Gebruik de Cisco CLI Analyzer om een analyse van de opdrachtoutput te bekijken.

Hier worden enkele nuttige opdrachten weergegeven die moeten worden gebruikt voor problemen met probleemoplossing:

- IP-server tonen
- LAN-servergroepen weergeven
- statistische gegevens van bladeservers weergeven 10.2.3.7
- vertonen

```
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#
```

Gerelateerde informatie

- Cisco MDS 9000 hele reeks NX-OS security configuratiegids - met LBP configureren
- Technische ondersteuning en documentatie – Cisco Systems