配置MDS LDAP

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[設定](#)
[驗證](#)
[疑難排解](#)
[相關資訊](#)

簡介

本文檔提供多層資料交換機(MDS)上的基本LDAP（輕量級目錄訪問協定）配置的示例配置。還列出了幾個命令，以便顯示如何在運行NX-OS的MDS交換機上測試和驗證配置。

LDAP為嘗試訪問Cisco MDS裝置的使用者提供集中驗證。LDAP服務在LDAP守護程式的資料庫中維護，該守護程式通常在UNIX或Windows NT工作站上運行。在Cisco MDS裝置上配置的LDAP功能可用之前，您必須擁有對LDAP伺服器的訪問權並對其進行配置。

LDAP提供獨立的身份驗證和授權功能。LDAP允許使用單個訪問控制伺服器（LDAP守護程式），以便獨立提供每個服務的身份驗證和授權。每個服務都可以繫結到其自己的資料庫中，以便利用該伺服器或網路上可用的其他服務，具體取決於守護程式的功能。

LDAP客戶端/伺服器協定使用TCP（TCP埠389）滿足傳輸要求。Cisco MDS裝置使用LDAP協定提供集中身份驗證。

必要條件

需求

思科宣告應配置和驗證Active Directory(AD)使用者帳戶。目前，Cisco MDS支援Description和MemberOf作為屬性名稱。在LDAP伺服器中使用這些屬性配置使用者角色。

採用元件

本檔案中的資訊已在執行NX-OS版本6.2(7)的MDS 9148上測試。 相同的配置應適用於其他MDS平台以及NX-OS版本。測試LDAP伺服器位於10.2.3.7。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

在MDS交換器上輸入以下命令，以確保您可以透過主控台存取交換器以進行復原：

```
aaa authentication login console local
```

啟用LDAP功能並建立將用於根繫結的使用者。本示例中使用「Admin」：

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

此時，您應該在LDAP伺服器上建立一個使用者（如cpam）。 在說明屬性中新增以下條目：

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

接下來，您需要在switch中建立搜尋映像。以下示例將Description和MemberOf顯示為attribute-name:

對於說明：

```
ldap search-map s1

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

對於MemberOf:

```
ldap search-map s2

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

例如，如果這三個使用者是AD伺服器中組abc的成員，則MDS交換機必須具有使用所需許可權建立的角色名稱abc。

使用者1 — 組abc的成員
使用者2 — 組abc的成員
使用者3 — 組abc的成員

```
role name abc
   rule 1 permit clear
   rule 2 permit config
   rule 3 permit debug
   rule 4 permit exec
   rule 5 permit show
```

現在，如果User1登入到交換機，並且為LDAP配置屬性memberOf ，則為User1分配了具有所有管理員許可權的角色abc。

配置memberOf屬性時也有兩個要求。

1. 交換機的角色名稱應與AD伺服器組名稱匹配，或者
2. 在AD伺服器上建立一個名為「network-admin」的組，並將所有必需使用者配置為network-admin組的成員。

附註：

-其 memberOf屬性僅受Windows AD LDAP伺服器支援。OpenLDAP伺服器不支援memberOf屬性。
- memberOf配置僅在NX-OS 6.2(1)及更高版本中受支援。

接下來，使用適當的名稱建立身份驗證、授權和記帳(AAA)組，並繫結以前建立的LDAP搜尋對映。如前所述，您可以根據自己的偏好使用Description或MemberOf。此處顯示的示例中，s1用於說明使用者身份驗證。如果要使用MemberOf完成身份驗證，則可以改用s2。

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

aaa authentication login default group ldap2
```

此外，如果LDAP伺服器無法訪問，此配置會將身份驗證還原為本地。這是選用組態：

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

驗證

使用本節內容，確認您的組態是否正常運作。

為了驗證LDAP是否從MDS交換機本身正常工作，請使用以下測試：

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

MDSA#
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

Cisco CLI Analyzer（僅供已註冊客戶使用）支援某些 show 指令。使用 Cisco CLI Analyzer 檢視 show 指令輸出的分析。

以下是一些用來排查問題的有用命令：

- 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#
```

相關資訊

- Cisco MDS 9000系列NX-OS安全配置指南 — 配置LDAP
- 技術支援與文件 - Cisco Systems