配置MDS LDAP

目录

简介

本文档提供了多层数据交换机(MDS)上基本LDAP（轻量级目录访问协议）配置的示例配置。还列出了一些命令，以展示如何测试和验证运行NX-OS的MDS交换机上的配置。

LDAP为尝试访问Cisco MDS设备的用户提供集中验证。LDAP服务在通常在UNIX或Windows NT工作站上运行的LDAP守护程序的数据库中维护。在Cisco MDS设备上配置的LDAP功能可用之前，您必须有权访问并配置LDAP服务器。

LDAP提供单独的身份验证和授权设施。LDAP允许单个访问控制服务器（LDAP守护程序），以独立提供每个服务身份验证和授权。每个服务都可以绑定到自己的数据库，以便利用该服务器或网络上可用的其他服务，具体取决于守护程序的功能。

LDAP客户端/服务器协议使用TCP（TCP端口389）来满足传输要求。Cisco MDS设备使用LDAP协议提供集中身份验证。

先决条件

要求

思科规定应配置和验证Active Directory(AD)用户帐户。目前，Cisco MDS支持Description和MemberOf作为属性名称。在LDAP服务器中使用这些属性配置用户角色。

使用的组件

本文档中的信息已在运行NX-OS版本6.2(7)的MDS 9148上测试。 相同的配置应适用于其他MDS平台和NX-OS版本。测试LDAP服务器位于10.2.3.7。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

在MDS交换机上输入以下命令，以确保您能够通过控制台访问交换机进行恢复：

```
aaa authentication login console local
```

启用LDAP功能并创建将用于根绑定的用户。本例中使用“Admin”：

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

此时，您应在LDAP服务器上创建用户（如cpam）。 在description属性中，添加以下条目：

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

接下来，在交换机中，您需要创建搜索映射。以下示例将Description和MemberOf显示为attribute-name:

对于说明：

```
ldap search-map s1

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

对于MemberOf:

```
ldap search-map s2

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

例如，如果这三个用户是AD服务器中组abc的成员，则MDS交换机必须具有使用所需权限创建的角色名称abc。

用户1 — 组abc的成员
用户2 — 组abc的成员
用户3 — 组成员abc

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

现在，如果User1登录到交换机，并且为LDAP配置了属性memberOf，则为User1分配了具有所有管理员权限的角色abc。

配置memberOf属性时还有两个要求。

1. 交换机的角色名称应与AD服务器组名称匹配，或
2. 在AD服务器上创建名为“network-admin”的组，并将所有必需用户配置为network-admin组的成员。

注意：

- memberOf属性仅受Windows AD LDAP服务器支持。OpenLDAP服务器将不支持memberOf属性。
— 仅NX-OS 6.2(1)及更高版本支持memberOf配置。

接下来，使用适当的名称创建身份验证、授权和记帐(AAA)组，并绑定之前创建的LDAP搜索映射。如前所述，您可以根据首选项使用Description或MemberOf。在此处显示的示例中，s1用于用户身份验证的说明。如果要使用MemberOf完成身份验证，则可以改用s2。

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

aaa authentication login default group ldap2
```

此外，此配置将在LDAP服务器无法访问时将身份验证恢复为本地。这是可选配置：

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

验证

使用本部分可确认配置能否正常运行。

要从MDS交换机本身验证LDAP是否正常工作，请使用以下测试：

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

MDSA#
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

思科 CLI 分析器（仅适用于注册客户）支持某些 show 命令。要查看对 show 命令输出的分析，请使用思科 CLI 分析器。

用于排除故障的一些有用命令如下所示：

- 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#
```

相关信息

- Cisco MDS 9000系列NX-OS安全配置指南 — 配置LDAP
- 技术支持和文档 - Cisco Systems