配置MD LDAP

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[配置](#)
[验证](#)
[故障排除](#)
[相关信息](#)

简介

本文为基本LDAP (轻量级目录访问协议)配置提供一配置示例在多层数据交换(MD)。也列出一些命令为了显示如何测试和验证在运行NX-OS的MD交换机的配置。

LDAP提供尝试获得访问到Cisco MDS设备用户的集中化验证。LDAP服务在UNIX或Windows NT工作站典型地运行在LDAP守护程序的一个数据库保养。在您的Cisco MDS设备的已配置的LDAP功能是可用的前，您必须访问并且必须配置LDAP服务器。

独立的认证和授权设施的LDAP提供。LDAP允许单个访问控制服务器(LDAP守护程序)为了独立地提供每个服务认证和授权。每服务可以被关联到其自己的数据库为了利用其他服务可用在该服务器或在网络，从属在守护程序的功能。

LDAP客户端/服务器协议使用TCP (TCP端口389)传输需求。Cisco MDS设备提供集中认证使用LDAP协议。

先决条件

要求

思科阐明，应该配置和验证激活目录(AD)用户帐户。目前， Cisco MDS支持说明和MemberOf作为属性名称。配置与这些属性的用户角色在LDAP服务器。

使用的组件

本文档中的信息在运行NX-OS版本6.2(7)的MD 9148测试了。相同的配置应该为其他MD平台以及NX-OS版本工作。测验LDAP服务器查找在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

输入此on命令MD交换机为了确保您访问控制台访问到恢复的交换机：

```
aaa authentication login console local
```

启用LDAP功能并且创建将使用绑定的根的用户。“Admin”用于此示例：

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

这时在LDAP服务器您应该创建用户(例如cpam)。在说明属性请添加此条目：

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

其次，在交换机您需要创建搜索地图。这些示例显示说明和MemberOf作为属性名称：

说明：

```
ldap search-map s1

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

MemberOf ：

```
ldap search-map s2

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

例如，如果这三个用户是组abc的成员在AD服务器的，然后MD交换机必须有角色名称abc创建与需要的权限。

User1 -组abc的成员
User2 -组abc的成员
用户3 -组abc的成员

```
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登陆到交换机，并且属性memberOf为LDAP配置，然后User1分配角色有所有管理权限的abc。

当您配置memberOf属性时，也有两个需求。

1. 任一交换机的角色名称应该配比与AD服务器组组名或者
2. 创建AD服务器的一组有命名“网络Admin的”并且配置全部必需用户作为网络Admin组的成员。

   注意：
   - Windows AD LDAP服务器只支持memberOf属性。OpenLDAP服务器不会支持memberOf属性。
   - NX-OS 6.2(1)只支持memberOf配置及以后。

其次，请创建有适当的名称的一验证、授权和统计(AAA)组并且绑定一张以前已创建LDAP搜索地图。如以前注释，您能使用根据您的首选或MemberOf的说明。在显示的示例中此处， s1使用用户认证的说明。如果验证将完成与MemberOf，则可以使用s2。

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

aaa authentication login default group ldap2
```

并且，万一LDAP服务器是不可得到的，此配置将恢复验证对本地。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。

为了验证，如果LDAP从MD交换机适当地运作，请使用此测验：

```
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。

确定Cisco CLI分析器(仅限注册用户)支持**显示**命令。请使用Cisco CLI分析器为了查看show命令输出分析。

一些有用的命令使用排除故障问题显示此处：

- **show ldap server**
- **show ldap server组**
- **show ldap server统计信息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