Contents

Introduction

This document provides a sample configuration for basic LDAP (Lightweight Directory Access Protocol) configuration on Multilayer Data Switches (MDS). A few commands are also listed in order to show how to test and validate the configuration on MDS switches that run NX-OS.

The LDAP provides centralized validation of users who attempt to gain access to a Cisco MDS device. LDAP services are maintained in a database on an LDAP daemon that typically runs on a UNIX or Windows NT workstation. You must have access to and must configure an LDAP server before the configured LDAP features on your Cisco MDS device are available.

LDAP provides for separate authentication and authorization facilities. LDAP allows for a single access control server (the LDAP daemon) in order to provide each service authentication and authorization independently. Each service can be tied into its own database in order to take advantage of other services available on that server or on the network, dependent upon the capabilities of the daemon.

The LDAP client/server protocol uses TCP (TCP port 389) for transport requirements. Cisco MDS devices provide centralized authentication with use of the LDAP protocol.

Prerequisites

Requirements

Cisco states that the Active Directory (AD) user account should be configured and validated. Currently, Cisco MDS supports Description and MemberOf as attribute names. Configure the user role with these attributes in the LDAP server.

Components Used

The information in this document was tested on an MDS 9148 that runs NX-OS Version 6.2(7). The same configuration should work for other MDS platforms as well as NX-OS versions. The test LDAP server is located at 10.2.3.7.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Enter this command on the MDS switch in order to make sure you have console access into the switch for recovery:

```
aaa authentication login console local
```

Enable the LDAP feature and create a user that will be used for root binding. "Admin" is used in this example:

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

At this point on the LDAP server you should create a user (such as cpam). In the description attribute add this entry:

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

Next, in the switch you need to create a search map. These examples show Description and MemberOf as the attribute-name:

For Description:

```
ldap search-map s1

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

For MemberOf:

```
ldap search-map s2

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

For example, if these three users are members of group abc in the AD server, then the MDS switch must have the role name abc created with required permissions.

User1 - Member of Group abc
User2 - Member of Group abc
User3 - Member of Group abc

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

Now, if User1 logs in to the switch and the attribute memberOf is configured for LDAP , then User1 is assigned the role abc which has all admin rights.

There are also two requirements when you configure the memberOf attribute.

1. Either switch's role name should match with the AD server group name, OR
2. Create a group on the AD server with the name "network-admin" and configure all required users as a member of the network-admin group.

Notes:

- The memberOf attribute is only supported by the Windows AD LDAP server. The OpenLDAP server will not support the memberOf attribute.
- The memberOf configuration is only supported in NX-OS 6.2(1) and later.

Next, create an Authentication, Authorization, and Accounting (AAA) group with an appropriate name and bind a previously created LDAP search map. As previously noted, you can use either Description or MemberOf based on your preference. In the example shown here, s1 is used for the Description for user authentication. If authentication is to be completed with MemberOf, then s2 can be used instead.

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

aaa authentication login default group ldap2
```

Also, this configuration will revert authentication to local in case the LDAP server is unreachable. This is an optional configuration:

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

Verify

Use this section in order to confirm that your configuration works properly.

In order to verify if the LDAP works properly from the MDS switch itself, use this test:

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

MDSA#
```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

The Cisco CLI Analyzer (registered customers only) supports certain **show** commands. Use the Cisco CLI Analyzer in order to view an analysis of **show** command output.

Some useful commands to use to troubleshoot issues are shown here:

- **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#
```

Related Information

- [Cisco MDS 9000 Family NX-OS Security Configuration Guide - Configuring LDAP]
- [Technical Support & Documentation - Cisco Systems]