Configurar MDS LDAP

Contents

Introduction

Este documento fornece uma configuração de exemplo para a configuração básica LDAP (Lightweight Diretory Access Protocol) em MDS (Multilayer Data Switches). Alguns comandos também são listados para mostrar como testar e validar a configuração em switches MDS que executam NX-OS.

O LDAP fornece validação centralizada de usuários que tentam obter acesso a um dispositivo Cisco MDS. Os serviços LDAP são mantidos em um banco de dados em um daemon LDAP que normalmente é executado em uma estação de trabalho UNIX ou Windows NT. Você deve ter acesso e configurar um servidor LDAP antes que os recursos LDAP configurados em seu dispositivo Cisco MDS estejam disponíveis.

O LDAP oferece autenticação e autorização separadas. O LDAP permite um único servidor de controle de acesso (o daemon LDAP) para fornecer cada autenticação e autorização de serviço de forma independente. Cada serviço pode ser vinculado ao seu próprio banco de dados para aproveitar outros serviços disponíveis nesse servidor ou na rede, dependendo dos recursos do daemon.

O protocolo cliente/servidor LDAP usa TCP (porta TCP 389) para requisitos de transporte. Os dispositivos Cisco MDS fornecem autenticação centralizada com o uso do protocolo LDAP.

Prerequisites

Requirements

A Cisco afirma que a conta de usuário do Ative Diretory (AD) deve ser configurada e validada. Atualmente, o Cisco MDS suporta Descrição e Membro de como nomes de atributo. Configure a função de usuário com esses atributos no servidor LDAP.

Componentes Utilizados

As informações neste documento foram testadas em um MDS 9148 que executa o NX-OS versão 6.2(7). A mesma configuração deve funcionar para outras plataformas MDS, bem como para as

versões NX-OS. O servidor LDAP de teste está localizado em 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.

Configurar

Insira este comando no switch MDS para garantir que você tenha acesso de console ao switch para recuperação:

```
aaa authentication login console local
```

Ative o recurso LDAP e crie um usuário que será usado para a associação raiz. "Admin" é usado neste exemplo:

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

Nesse ponto do servidor LDAP, você deve criar um usuário (como cpam). No atributo de descrição, adicione esta entrada:

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

Em seguida, no switch, você precisa criar um mapa de pesquisa. Estes exemplos mostram Description e MemberOf como o nome do atributo:

Para descrição:

```
ldap search-map s1

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

Para Membro De:

```
ldap search-map s2

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

Por exemplo, se esses três usuários forem membros do grupo abc no servidor AD, o switch MDS deverá ter o nome da função abc criado com permissões necessárias.

Usuário1 - Membro do grupo abc
Usuário 2 - Membro do grupo abc
Usuário 3 - Membro do grupo abc

```
role name abc
   rule 1 permit clear
   rule 2 permit config
   rule 3 permit debug
```

```
  rule 4 permit exec
  rule 5 permit show
```

Agora, se User1 faz login no switch e o atributo memberOf está configurado para LDAP , então User1 recebe a função abc que tem todos os direitos de administrador.

Há também dois requisitos ao configurar o atributo memberOf.

1. O nome da função do comutador deve corresponder ao nome do grupo de servidores AD OU
2. Crie um grupo no servidor AD com o nome "network-admin" e configure todos os usuários necessários como um membro do grupo network-admin.

Notas:
-O o atributo memberOf só é suportado pelo servidor LDAP do Windows AD. O servidor OpenLDAP não suportará o atributo memberOf.
- A configuração memberOf só é suportada no NX-OS 6.2(1) e posterior.

Em seguida, crie um grupo de Autenticação, Autorização e Contabilidade (AAA) com um nome apropriado e vincule um mapa de pesquisa LDAP criado anteriormente. Como observado anteriormente, você pode usar a Descrição ou o Membro de com base em sua preferência. No exemplo mostrado aqui, s1 é usado para a Descrição da autenticação do usuário. Se a autenticação deve ser concluída com MemberOf, então s2 pode ser usado.

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

aaa authentication login default group ldap2
```

Além disso, essa configuração reverterá a autenticação para local caso o servidor LDAP não possa ser alcançado. Esta é uma configuração opcional:

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

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para verificar se o LDAP funciona corretamente a partir do próprio switch MDS, use este teste:

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

MDSA#
```

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

O Cisco CLI Analyzer (somente clientes registrados) aceita alguns comandos show. Use o Cisco CLI Analyzer para visualizar uma análise da saída do comando show.

Alguns comandos úteis a serem usados para solucionar problemas são mostrados aqui:

- 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#
```

Informações Relacionadas

- Guia de configuração de segurança do NX-OS da família Cisco MDS 9000 - Configuração do LDAP
- Suporte Técnico e Documentação - Cisco Systems