Configurar MDS LDAP

Índice

Introdução

Este documento fornece uma configuração de exemplo para a configuração básica LDAP (protocolo lightweight directory access) nos switch de dados Multilayer (MDS). Alguns comandos são alistados igualmente a fim mostrar como testar e validar a configuração no Switches MDS que executa NX-OS.

O LDAP fornece a validação centralizada dos usuários que tentam aceder a um dispositivo de Cisco MDS. Os serviços LDAP são mantidos em um base de dados em um demônio LDAP que seja executado tipicamente em UNIX ou em uma estação de trabalho do Windows NT. Você deve ter o acesso a e deve configurar um servidor ldap antes que as características configuradas LDAP em seu dispositivo de Cisco MDS estejam disponíveis.

O LDAP prevê facilidades separadas da authentication e autorização. O LDAP permite um único Access Control Server (demônio LDAP) a fim fornecer independentemente cada authentication e autorização do serviço. Cada serviço pode ser amarrado em seu próprio base de dados a fim aproveitar-se dos outros serviços disponíveis nesse server ou na rede, dependente das capacidades do demônio.

O protocolo do cliente de LDAP/server usa TCP (porta TCP 389) para exigências do transporte. Os dispositivos de Cisco MDS fornecem a autenticação centralizada o uso do protocolo ldap.

Pré-requisitos

Requisitos

Cisco indica que a conta de usuário do diretório ativo (AD) deve ser configurada e validado. Atualmente, descrição dos apoios de Cisco MDS e MemberOf como nomes do atributo. Configurar o papel de usuário com estes atributos no servidor ldap.

Componentes Utilizados

A informação neste documento foi testada em um MDS 9148 que executasse a versão 6.2(7) NX-OS. A mesma configuração deve trabalhar para outras plataformas MDS assim como versões

NX-OS. O servidor ldap do teste é ficado situado em 10.2.3.7.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Incorpore este comando no interruptor MDS a fim certificar-se de você ter o acesso de console no interruptor para a recuperação:

```
aaa authentication login console local
```

Permita a característica LDAP e crie um usuário que seja usado para o emperramento da raiz. O “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
```

Neste momento no servidor ldap você deve criar um usuário (tal como o cpam). No atributo da descrição adicionar esta entrada:

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

Em seguida, no interruptor você precisa de criar um mapa da busca. Estes exemplos mostram a descrição e o MemberOf como o atributo-nome:

Para a descrição:

```
ldap search-map s1

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

Para MemberOf:

```
ldap search-map s2

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

Por exemplo, se estes três usuários são membros do ABC do grupo no server AD, a seguir o interruptor MDS deve ter o ABC do nome do papel criado com as permissões exigidas.

Usuário1 - Membro do ABC do grupo
User2 - Membro do ABC do grupo
User3 - Membro do ABC do grupo

```
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 o usuário1 entra ao interruptor e o memberOf do atributo está configurado para o LDAP, a seguir usuário1 é atribuído o ABC do papel que tem todos os direitos admin.

Há igualmente duas exigências quando você configura o atributo do memberOf.

1. O nome do papel de um ou outro interruptor deve combinar com o nome de grupo de servidor AD, OU
2. Crie um grupo no server AD com o nome “rede-admin” e configurar todos os usuários exigidos como um membro do grupo rede-admin.

   Notas:
   - O atributo do memberOf é apoiado somente pelo servidor ldap de Windows AD. O server de OpenLDAP não apoiará o atributo do memberOf.
   - A configuração do memberOf é apoiada somente em NX-OS 6.2(1) e mais atrasado.

Em seguida, crie um grupo do Authentication, Authorization, and Accounting (AAA) com um nome apropriado e ligue um mapa previamente criado da busca LDAP. Como notável previamente, você pode usar a descrição ou o MemberOf baseada em sua preferência. No exemplo mostrado aqui, o S1 é usado para a descrição para a autenticação de usuário. Se a autenticação deve ser terminada com MemberOf, a seguir s2 pode ser usado pelo contrário.

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

aaa authentication login default group ldap2
```

Também, esta configuração reverterá a autenticação ao local caso que o servidor ldap é inacessível. Esta é uma configuração opcional:

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

Verificar

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

A fim verificar se o LDAP trabalha corretamente do interruptor próprio MDS, use este teste:

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

MDSA#
```

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

O analisador do CLI Cisco (clientes registrados somente) apoia determinados comandos de exibição. Use o analisador do CLI Cisco a fim ver uma análise do emissor de comando de execução.

Alguns comandos úteis usar-se para pesquisar defeitos edições são mostrados aqui:

- **mostre o servidor ldap**
- **mostre grupos de servidor ldap**
- **mostre as estatísticas 10.2.3.7 do servidor ldap**

- mostre a autenticação aaa

```
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 da família NX-OS do Cisco MDS 9000 - Configurando o

LDAP

- Suporte Técnico e Documentação - Cisco Systems