Configuración MDS LDAP

Contenido

Introducción

Este documento proporciona una configuración de muestra para la configuración básica LDAP (protocolo lightweight directory access) en los switches de datos de múltiples capas (MDS). Algunos comandos también se enumeran para mostrar cómo probar y validar la configuración en el Switches MDS que ejecuta NX-OS.

El LDAP proporciona la validación centralizada de los usuarios que intentan acceder a un dispositivo de Cisco MDS. Mantienen a los servicios LDAP en una base de datos en una daemon LDAP que se ejecute típicamente en UNIX o un puesto de trabajo del Windows NT. Usted debe tener acceso a y debe configurar a un servidor LDAP antes de que las características configuradas LDAP en su dispositivo de Cisco MDS estén disponibles.

El LDAP prevé los recursos separados de la autenticación y autorización. El LDAP permite un solo Access Control Server (la daemon LDAP) para proporcionar cada autenticación y autorización del servicio independientemente. Cada servicio se puede atar en su propia base de datos para aprovecharse de los otros servicios disponibles en ese servidor o en la red, dependiente sobre las capacidades de la daemon.

El protocolo del cliente LDAP/del servidor utiliza TCP (puerto TCP 389) para los requisitos del transporte. Los dispositivos de Cisco MDS proporcionan la autenticación centralizada con el uso del protocolo LDAP.

Prerrequisitos

Requisitos

Estados de Cisco que la cuenta de usuario del Active Directory (AD) debe ser configurada y ser validada. Actualmente, descripción de los soportes de Cisco MDS y MemberOf como nombres del atributo. Configure el rol del usuario con estos atributos en el servidor LDAP.

Componentes Utilizados

La información en este documento fue probada en un MDS 9148 que funciona con la versión

6.2(7) NX-OS. La misma configuración debe trabajar para otras plataformas MDS así como las versiones NX-OS. El servidor LDAP de la prueba está situado en 10.2.3.7.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Ingrese este comando en el Switch MDS para aseegurarse le tener acceso a la consola en el Switch para la recuperación:

```
aaa authentication login console local
```

Habilite la característica LDAP y cree a un usuario que sea utilizado para el atascamiento de la raíz. El “Admin” se utiliza en este ejemplo:

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

En este momento en el servidor LDAP usted debe crear a un usuario (tal como cpam). En el atributo de la descripción agregue esta entrada:

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

Después, en el Switch usted necesita crear una correspondencia de la búsqueda. Estos ejemplos muestran la descripción y MemberOf como el atributo-nombre:

Para la descripción:

```
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 ejemplo, si estos tres usuarios son miembros del ABC del grupo en el servidor AD, después el Switch MDS debe tener el ABC del nombre de la función creado con los permisos requeridos.

User1 - Miembro del ABC del grupo
User2 - Miembro del ABC del grupo
User3 - Miembro del ABC del grupo

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

Ahora, si el user1 abre una sesión al Switch y el memberOf del atributo se configura para el LDAP, después user1 se asigna el ABC del papel que tiene todos los derechos admin.

Hay también dos requisitos cuando usted configura el atributo del memberOf.

1. El nombre de la función de cualquier Switch debe hacer juego con el nombre de grupo de servidores AD, O
2. Cree a un grupo en el servidor AD con el nombre “red-admin” y configure a todos los usuarios requeridos como un miembro del grupo red-admin.

   Notas:
   - El atributo del memberOf es soportado solamente por el servidor LDAP de Windows AD. El servidor de OpenLDAP no soportará el atributo del memberOf.
   - La configuración del memberOf se soporta solamente en NX-OS 6.2(1) y posterior.

Después, cree a un grupo del Authentication, Authorization, and Accounting (AAA) con un nombre apropiado y ate una correspondencia previamente creada de la búsqueda LDAP. Según lo observado previamente, usted puede utilizar la descripción o MemberOf basado en su preferencia. En el ejemplo mostrado aquí, el s1 se utiliza para la descripción para la autenticación de usuario. Si se va la autenticación a ser completada con MemberOf, después el s2 se puede utilizar en lugar de otro.

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

aaa authentication login default group ldap2
```

También, esta configuración invertirá la autenticación al local en caso de que el servidor LDAP sea inalcanzable. Esto es una configuración optativa:

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

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Para verificar si el LDAP trabaja correctamente del Switch sí mismo MDS, utilice esta prueba:

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

MDSA#
```

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

El analizador del CLI de Cisco (clientes registrados solamente) apoya los ciertos comandos show. Utilice el analizador del CLI de Cisco para ver una análisis de la salida del comando show.

Muestran algunos comandos útiles de utilizar para resolver problemas los problemas aquí:

- **muestre al servidor LDAP**
- **muestre a los grupos de servidor LDAP**
- **muestre las estadísticas 10.2.3.7 del servidor LDAP**

- muestre la autenticación 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#
```

Información Relacionada

- Guía de configuración de seguridad de la familia NX-OS del Cisco MDS 9000 - Configurar el

LDAP

- Soporte Técnico y Documentación - Cisco Systems