Configuración de MDS LDAP

Contenido

Introducción

Este documento proporciona una configuración de ejemplo para la configuración básica LDAP (protocolo ligero de acceso a directorios) en switches de datos multicapa (MDS). También se enumeran algunos comandos para mostrar cómo probar y validar la configuración en los switches MDS que ejecutan NX-OS.

El LDAP proporciona validación centralizada de los usuarios que intentan obtener acceso a un dispositivo Cisco MDS. Los servicios LDAP se mantienen en una base de datos en un daemon LDAP que normalmente se ejecuta en una estación de trabajo UNIX o Windows NT. Debe tener acceso a y configurar un servidor LDAP antes de que las funciones LDAP configuradas en su dispositivo Cisco MDS estén disponibles.

LDAP proporciona para las instalaciones de autenticación y autorización independientes. LDAP permite un único servidor de control de acceso (el daemon LDAP) para proporcionar cada autenticación y autorización de servicio de forma independiente. Cada servicio se puede vincular a su propia base de datos para aprovechar otros servicios disponibles en ese servidor o en la red, según las capacidades del demonio.

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

Prerequisites

Requirements

Cisco afirma que la cuenta de usuario de Active Directory (AD) debe configurarse y validarse. Actualmente, Cisco MDS admite Description y MemberOf como nombres de atributo. Configure el rol de usuario con estos atributos en el servidor LDAP.

Componentes Utilizados

La información de este documento se probó en un MDS 9148 que ejecuta NX-OS versión 6.2(7).

La misma configuración debería funcionar para otras plataformas MDS así como para las versiones NX-OS. El servidor LDAP de prueba se encuentra en 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

Ingrese este comando en el switch MDS para asegurarse de que tiene acceso de consola en el switch para la recuperación:

```
aaa authentication login console local
```

Habilite la función LDAP y cree un usuario que se utilizará para el enlace raíz. "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 punto en el servidor LDAP debe crear un usuario (como cpam). En el atributo description, agregue esta entrada:

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

A continuación, en el switch debe crear un mapa de búsqueda. Estos ejemplos muestran Description y MemberOf como atributo-name:

Para Descripción:

```
ldap search-map s1

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

Para MiembroDe:

```
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 grupo abc en el servidor AD, entonces el switch MDS debe tener el nombre de rol abc creado con los permisos requeridos.

Usuario1: miembro del grupo abc
Usuario 2: miembro del grupo abc
Usuario3 - Miembro del 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
```

Ahora, si User1 inicia sesión en el switch y el miembro del atributoOf se configura para LDAP , al usuario1 se le asigna la función abc que tiene todos los derechos de administrador.

También hay dos requisitos cuando se configura el atributo memberOf.

1. El nombre de rol de cada switch debe coincidir con el nombre del grupo de servidores AD, O
2. Cree un grupo en el servidor AD con el nombre "network-admin" y configure todos los usuarios requeridos como miembro del grupo de administradores de red.

Notas:
-El memberOf sólo es compatible con el servidor LDAP de Windows AD. El servidor OpenLDAP no admitirá el atributo memberOf.
- La configuración memberOf sólo se admite en NX-OS 6.2(1) y posteriores.

A continuación, cree un grupo de autenticación, autorización y contabilidad (AAA) con un nombre adecuado y enlace un mapa de búsqueda LDAP creado anteriormente. Como se ha indicado anteriormente, puede utilizar Description o MemberOf según sus preferencias. En el ejemplo que se muestra aquí, s1 se utiliza para la Descripción para la autenticación de usuario. Si la autenticación se debe completar con MemberOf, se puede utilizar s2 en su lugar.

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

aaa authentication login default group ldap2
```

Además, esta configuración revertirá la autenticación a local en caso de que el servidor LDAP sea inalcanzable. Esta es una configuración opcional:

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

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Para verificar si el LDAP funciona correctamente desde el propio switch MDS, utilice esta prueba:

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

MDSA#
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

El Analizador de Cisco CLI (solo clientes registrados) admite determinados comandos show.
Utilice el Analizador de Cisco CLI para ver un análisis de los resultados del comando show.

Aquí se muestran algunos comandos útiles que se pueden utilizar para resolver problemas:

- 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#
```

Información Relacionada

- Guía de Configuración de Seguridad de la Familia Cisco MDS 9000 NX-OS - Configuración de LDAP
- Soporte Técnico y Documentación - Cisco Systems