Configura LDAP MDS

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per la configurazione di base di LDAP (Lightweight Directory Access Protocol) su MDS (Multilayer Data Switch). Sono inoltre elencati alcuni comandi per mostrare come verificare e convalidare la configurazione sugli switch MDS con NX-OS.

Il protocollo LDAP fornisce la convalida centralizzata degli utenti che tentano di accedere a un dispositivo Cisco MDS. I servizi LDAP vengono gestiti in un database su un daemon LDAP che in genere viene eseguito su una workstation UNIX o Windows NT. È necessario disporre dell'accesso a e configurare un server LDAP prima che le funzionalità LDAP configurate sul dispositivo Cisco MDS siano disponibili.

LDAP fornisce funzioni di autenticazione e autorizzazione separate. LDAP consente di utilizzare un singolo server di controllo dell'accesso (il daemon LDAP) per fornire in modo indipendente l'autenticazione e l'autorizzazione di ogni servizio. Ciascun servizio può essere collegato al proprio database per sfruttare altri servizi disponibili sul server o sulla rete, a seconda delle funzionalità del daemon.

Il protocollo client/server LDAP utilizza TCP (porta TCP 389) per i requisiti di trasporto. I dispositivi Cisco MDS offrono l'autenticazione centralizzata con l'utilizzo del protocollo LDAP.

Prerequisiti

Requisiti

Cisco indica che l'account utente di Active Directory (AD) deve essere configurato e convalidato. Al momento, Cisco MDS supporta i nomi Description e MemberOf come attributi. Configurare il ruolo utente con questi attributi nel server LDAP.

Componenti usati

Le informazioni di questo documento sono state testate su un MDS 9148 con NX-OS versione 6.2(7). La stessa configurazione dovrebbe funzionare per altre piattaforme MDS e versioni NX-

OS. Il server LDAP di prova si trova nella posizione 10.2.3.7.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Immettere questo comando sullo switch MDS per verificare di disporre dell'accesso da console allo switch per il ripristino:

```
aaa authentication login console local
```

Attivare la funzionalità LDAP e creare un utente da utilizzare per l'associazione radice. Nell'esempio viene utilizzato "Admin":

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

A questo punto sul server LDAP è necessario creare un utente (ad esempio cpam). Nell'attributo description aggiungere la voce seguente:

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

Quindi, nello switch occorre creare una mappa di ricerca. In questi esempi vengono illustrati Description e MemberOf come nome-attributo:

Per Descrizione:

```
ldap search-map s1

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

Per MemberOf:

```
ldap search-map s2

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

Ad esempio, se questi tre utenti sono membri del gruppo abc nel server AD, lo switch MDS deve avere il nome del ruolo abc creato con le autorizzazioni richieste.

Utente1 - Membro del gruppo abc
Utente2 - Membro del gruppo abc
Utente3 - Membro del gruppo abc

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

```
rule 3 permit debug
rule 4 permit exec
rule 5 permit show
```

Ora, se l'utente 1 accede allo switch e l'attributo memberOf è configurato per LDAP, all'utente 1 viene assegnato il ruolo abc con tutti i diritti di amministratore.

Quando si configura l'attributo memberOf, sono previsti anche due requisiti.

1. Il nome del ruolo dello switch deve corrispondere al nome del gruppo di server AD oppure
2. Creare un gruppo sul server AD con il nome "network-admin" e configurare tutti gli utenti necessari come membri del gruppo network-admin.

Note:
-OSPF (Open Shortest Path First) L'attributo memberOf è supportato solo dal server LDAP AD di Windows. Il server OpenLDAP non supporta l'attributo memberOf.
- La configurazione memberOf è supportata solo in NX-OS 6.2(1) e versioni successive.

Creare quindi un gruppo di autenticazione, autorizzazione e accounting (AAA) con un nome appropriato e associare una mappa di ricerca LDAP creata in precedenza. Come indicato in precedenza, è possibile utilizzare Description o MemberOf in base alle proprie preferenze. Nell'esempio riportato di seguito, s1 viene utilizzato per la descrizione dell'autenticazione utente. Se l'autenticazione deve essere completata con MemberOf, è possibile utilizzare s2.

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

aaa authentication login default group ldap2
```

Inoltre, questa configurazione ripristinerà l'autenticazione locale nel caso in cui il server LDAP non sia raggiungibile. Questa è una configurazione opzionale:

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

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Per verificare se il protocollo LDAP funziona correttamente dallo switch MDS, utilizzare questo test:

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

MDSA#
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Cisco CLI Analyzer (solo utenti registrati) supporta alcuni comandi show. Usare Cisco CLI

Analyzer per visualizzare un'analisi dell'output del comando **show**.

Di seguito sono riportati alcuni comandi utili per la risoluzione dei problemi:

- **show ldap-server**
- **mostra gruppi di server ldap**
- **show ldap-server statistics 10.2.3.7**
- **mostra autenticazione 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#
```

Informazioni correlate

- Guida alla configurazione della protezione di Cisco MDS 9000 NX-OS - Configurazione di LDAP
- Documentazione e supporto tecnico – Cisco Systems