MDS LDAP 구성

목차

소개

이 문서에서는 MDS(Multilayer Data Switches)의 기본 LDAP(Lightweight Directory Access Protocol) 컨피그레이션에 대한 샘플 컨피그레이션을 제공합니다.NX-OS를 실행하는 MDS 스위치에서 컨피그레이션을 테스트하고 검증하는 방법을 보여 주기 위해 몇 가지 명령도 나열되어 있습니다.

LDAP는 Cisco MDS 디바이스에 대한 액세스를 시도하는 사용자를 중앙에서 검증합니다.LDAP 서비스는 일반적으로 UNIX 또는 Windows NT 워크스테이션에서 실행되는 LDAP 데몬의 데이터베이스에서 유지 관리됩니다.Cisco MDS 디바이스에서 구성된 LDAP 기능을 사용하려면 먼저 LDAP 서버에 대한 액세스 권한이 있어야 하며 이를 구성해야 합니다.

LDAP는 별도의 인증 및 권한 부여 기능을 제공합니다.LDAP는 각 서비스 인증 및 권한 부여를 독립적으로 제공하기 위해 단일 액세스 제어 서버(LDAP 데몬)를 허용합니다.각 서비스는 해당 서버 또는 네트워크에서 사용 가능한 다른 서비스를 이용하기 위해 해당 데몬의 기능에 따라 자체 데이터베이스에 연결될 수 있습니다.

LDAP 클라이언트/서버 프로토콜은 전송 요구 사항에 TCP(TCP 포트 389)를 사용합니다.Cisco MDS 디바이스는 LDAP 프로토콜을 사용하여 중앙 집중식 인증을 제공합니다.

사전 요구 사항

요구 사항

Cisco는 AD(Active Directory) 사용자 계정을 구성하고 검증해야 한다고 말합니다.현재 Cisco MDS는 Description 및 MemberOf를 특성 이름으로 지원합니다.LDAP 서버에서 이러한 특성을 사용하여 사용자 역할을 구성합니다.

사용되는 구성 요소

이 문서의 정보는 NX-OS 버전 6.2(7)를 실행하는 MDS 9148에서 테스트되었습니다. NX-OS 버전은 물론 다른 MDS 플랫폼에서도 동일한 컨피그레이션이 작동해야 합니다.테스트 LDAP 서버는 10.2.3.7에 있습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

복구를 위해 스위치에 콘솔 액세스 권한이 있는지 확인하려면 MDS 스위치에 이 명령을 입력합니다 .

```
aaa authentication login console local
```

LDAP 기능을 활성화하고 루트 바인딩에 사용할 사용자를 만듭니다.이 예에서는 "Admin"이 사용됩니다.

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

LDAP 서버에서 이 시점에서 사용자를 생성해야 합니다(예: cpam). description 속성에서 이 항목을 추가합니다.

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

다음으로, 스위치에서 검색 맵을 만들어야 합니다.다음 예에서는 Description 및 MemberOf를 attribute-name으로 보여 줍니다.

설명:

```
ldap search-map s1

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

MemberOf:

```
ldap search-map s2

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

예를 들어 이 세 명의 사용자가 AD 서버의 그룹 abc 멤버인 경우 MDS 스위치에는 필수 권한으로 만든 역할 이름이 abc여야 합니다.

User1 - 그룹 abc의 구성원
User2 - 그룹 abc 멤버
User3 - 그룹 abc 멤버

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

이제 User1이 스위치에 로그인하고 특성 memberOf가 LDAP에 대해 구성된 경우 User1에는 모든 관리자 권한이 있는 역할 abc가 할당됩니다.

memberOf 특성을 구성할 때 두 가지 요구 사항이 있습니다.

1. 스위치의 역할 이름이 AD 서버 그룹 이름 또는 OR과 일치해야 합니다.
2. "network-admin"이라는 이름으로 AD 서버에 그룹을 만들고 필요한 모든 사용자를 네트워크 관리자 그룹의 구성원으로 구성합니다.

참고:
- memberOf 특성은 Windows AD LDAP 서버에서만 지원됩니다.OpenLDAP 서버는 memberOf 특성을 지원하지 않습니다.
- memberOf 컨피그레이션은 NX-OS 6.2(1) 이상에서만 지원됩니다.

그런 다음 적절한 이름으로 AAA(Authentication, Authorization, and Accounting) 그룹을 만들고 이전에 생성한 LDAP 검색 맵을 바인딩합니다.앞에서 설명한 대로 기본 설정에 따라 Description 또는 MemberOf를 사용할 수 있습니다.여기에 표시된 예에서 s1은 사용자 인증에 대한 설명에 사용됩니다.MemberOf를 사용하여 인증을 완료하려면 s2를 대신 사용할 수 있습니다.

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

aaa authentication login default group ldap2
```

또한 이 컨피그레이션은 LDAP 서버에 연결할 수 없는 경우 인증을 로컬으로 되돌립니다.이는 선택적 컨피그레이션입니다.

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

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

MDS 스위치 자체에서 LDAP가 제대로 작동하는지 확인하려면 다음 테스트를 사용합니다.

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

MDSA#
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

Cisco CLI Analyzer(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 Cisco CLI Analyzer를 사용합니다.

문제 해결에 사용할 수 있는 몇 가지 유용한 명령은 다음과 같습니다.

- **ldap 서버 표시**

- ldap-server 그룹 표시
- ldap-server 통계 10.2.3.7 표시
- aaa 인증 표시

```
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#
```

관련 정보

- Cisco MDS 9000 제품군 NX-OS 보안 컨피그레이션 가이드 - LDAP 구성
- 기술 지원 및 문서 – Cisco Systems