Содержание

Введение

Этот документ предоставляет пример конфигурации для основного LDAP (Упрощенный протокол доступа к каталогам (LDAP)) конфигурация на многоуровневых коммутаторах данных (MDS). Несколько команд также перечислены, чтобы показать, как протестировать и проверить конфигурацию на коммутаторах MDS, которые выполняют NX-OS.

LDAP предоставляет централизованную проверку пользователей, которые пытаются получить доступ к устройству MDS Cisco. Сервисы LDAP поддержаны в базе данных по демону LDAP, который, как правило, работает на UNIX или рабочей станции Windows NT. Вы должны иметь доступ к и должны настроить Сервер LDAP, прежде чем настроенные функции LDAP на вашем устройстве MDS Cisco будут доступны.

LDAP обеспечивает отдельные средства проверки подлинности и авторизация. LDAP обеспечивает сервер контроля за одиночным обращением (демон LDAP) для обеспечения каждой сервисной проверки подлинности и авторизация независимо. Каждый сервис может быть связан в его собственную базу данных для использования преимуществ других сервисов, доступных на том сервере или в сети, зависящей от возможностей демона.

Клиент LDAP / протокол сервера использует TCP (порт TCP 389) для транспортных требований. Устройства MDS Cisco предоставляют централизованной аутентификации использование Протокола LDAP.

Предварительные условия

Требования

Cisco сообщает, что учетная запись пользователя Active Directory (AD) должна быть настроена и проверена. В настоящее время MDS Cisco поддерживает Описание и MemberOf как названия атрибута. Настройте роль пользователя с этими атрибутами в Сервере LDAP.

Используемые компоненты

Сведения в этом документе были протестированы на MDS 9148, который выполняет Версию 6.2 (7) NX-OS. Одинаковая конфигурация должна работать для других платформ MDS, а также версий NX-OS. Тестовый Сервер LDAP расположен в 10.2.3.7.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Введите эту команду в коммутатор MDS, чтобы удостовериться, что у вас есть консольный доступ в коммутатор для восстановления:

```
aaa authentication login console local
```

Активируйте опцию LDAP и создайте пользователя, который будет использоваться для корневой привязки. "Admin" используется в данном примере:

```
feature ldap
```

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

На этом этапе на Сервере LDAP необходимо создать пользователя (такого как cpam). В описании атрибут добавляют эту запись:

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

Затем, в коммутаторе необходимо создать поисковую карту. Эти примеры показывают Описание и MemberOf как название атрибута:

Для описания:

```
ldap search-map s1
userprofile attribute-name "description" search-filter "cn=$userid"
base-DN "dc=ciscoprod,dc=com"
```

Для MemberOf:

```
ldap search-map s2  userprofile attribute-name "memberOf" search-filter "cn=$userid"
base-DN "dc=ciscoprod,dc=com"
```

Затем создайте группу Аутентификации, авторизации и учета (AAA) с соответствующим названием и свяжите ранее созданную карту поиска LDAP. Как ранее обращено внимание, можно использовать или Описание или MemberOf на основе предпочтения. В примере, показанном здесь, s1 используется для Описания для проверки подлинности пользователя. Если аутентификация должна быть завершена с MemberOf, то s2 может использоваться вместо этого.

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

aaa authentication login default group ldap2
```

Кроме того, эта конфигурация вернется аутентификация к локальной переменной в случае, если Сервер LDAP недостижим. Это - произвольная конфигурация:

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

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Чтобы проверить, работает ли LDAP должным образом от самого коммутатора MDS, используйте этот тест:

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

MDSA#
```

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Cisco CLI Анализатор (только зарегистрированные клиенты) поддерживает **некоторые команды show** . Используйте Cisco CLI Анализатор для **просматривания аналитику выходных данных команды show** .

Некоторые полезные команды для использования для решения проблем показывают здесь:

- **show ldap server**
- **группы show ldap-server**
- **статистика show ldap-server 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#
```

Дополнительные сведения

- Руководство по конфигурации системы безопасности NX-OS семейства Cisco MDS 9000 - LDAP Настройки
- Cisco Systems – техническая поддержка и документация