MDS LDAP の設定

内容

概要

このドキュメントでは、マルチレイヤ データ スイッチ（MDS）上の基本的な LDAP（Lightweight Directory Access Protocol）設定に関する設定例について説明します。NX-OS を実行する MDS スイッチ上の設定をテストおよび検証する方法を示すために、いくつかのコマンドも一覧表示されています。

LDAP は、Cisco MDS デバイスにアクセスしようとするユーザの検証を集中的に行うことができます。LDAP サービスは、一般に UNIX または Windows NT ワークステーションで稼働する LDAP デーモン上のデータベースに保持されます。Cisco MDS デバイスに設定した LDAP 機能を使用可能にするには、LDAP サーバにアクセスして設定しておく必要があります。

LDAP では、認証と認可のファシリティが別々に提供されます。LDAP では、1 台のアクセス コントロール サーバ（LDAP デーモン）で各サービス認証と認可を個別に提供できます。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを活用できます。

LDAP クライアント/サーバ プロトコルでは、トランスポート要件を満たすために、TCP（TCP ポート 389）を使用します。Cisco MDS デバイスは、LDAP プロトコルを使用して集中型の認証を行います。

前提条件

要件

Active Directory（AD）ユーザ アカウントを設定し、検証する必要があります。現在、Cisco MDS は、属性名として description および memberOf をサポートしています。LDAP サーバでこれらの属性を持つユーザ ロールを設定します。

使用するコンポーネント

このドキュメントに記載されている情報は、NX-OS バージョン 6.2(7) を実行する MDS 9148 でテストされました。 他の MDS プラットフォームだけでなく、NX-OS の各バージョンでも同じ設定が機能するはずです。テスト LDAP サーバは 10.2.3.7 にあります。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

MDS スイッチで次のコマンドを入力し、リカバリするスイッチにコンソールからアクセスできることを確認します。

```
aaa authentication login console local
```

LDAP 機能を有効にし、ルート バインドに使用されるユーザを作成します。この例では「Admin」を使用します。

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

この時点で、LDAP サーバ上にユーザ（cpam など）を作成する必要があります。 description 属性に次のエントリを追加します。

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

次に、スイッチ内に検索マップを作成する必要があります。次の例では、属性名として description および memberOf を使用しています。

description の場合：

```
ldap search-map s1

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

memberOf の場合：

```
ldap search-map s2

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

たとえば、これらの3人のユーザがADサーバのグループabcのメンバーである場合、MDSスイッチには必要な権限を持つロール名abcが作成されている必要があります。

ユーザ1：グループabcのメンバー
ユーザ2：グループabcのメンバー
ユーザ3：グループabcのメンバー

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

ここで、User1がスイッチにログインし、属性memberOfがLDAP（UserGroupの場合）に設定されている場合、User1にはすべての管理者権限を持つロールabcが割り当てられます。

memberOf属性を設定する際には、2つの要件があります。

1. スイッチのロール名がADサーバグループ名と一致している必要があります。または、
2. ADサーバ上に「network-admin」という名前のグループを作成し、必要なすべてのユーザをnetwork-adminグループのメンバとして設定します。

注：
-その memberOf属性は、Windows AD LDAPサーバでのみサポートされています。
OpenLDAPサーバーはmemberOf属性をサポートしません。
- memberOf設定は、NX-OS 6.2(1)以降でのみサポートされています。

次に、適切な名前で認証、許可、アカウンティング(AAA)グループを作成し、以前に作成したLDAP検索マップをバインドします。前述のように、好みに応じて description または memberOf のいずれかを使用できます。次の例では、ユーザ認証用の description には s1 が使用されています。認証が memberOf を使用して完了される場合、代わりに s2 を使用できます。

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

aaa authentication login default group ldap2
```

また、この設定は、LDAP サーバに到達できない場合は、認証をローカルに戻します。これはオプションの設定です。

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

確認

ここでは、設定が正常に機能しているかどうかを確認します。

LDAP が MDS スイッチ自体から正常に動作するか確認するためには、次のテストを使用します。

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

MDSA#
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

Cisco CLI アナライザ（登録ユーザ専用）は、特定の show コマンドをサポートします。show コマンド出力の分析を表示するには、Cisco CLI アナライザを使用します。

次のいくつかのコマンドは、問題のトラブルシューティングに役立ちます。

- 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#
```

関連情報

- Cisco MDS 9000 ファミリ NX-OS セキュリティの設定ガイド - LDAP の設定
- テクニカル サポートとドキュメント – Cisco Systems