LDAP の設定

この章では、Cisco NX-OS デバイス上で Lightweight Directory Access Protocol（LDAP）を設定する方法について説明します。次の項が含まれています。

LDAP について

Lightweight Directory Access Protocol（LDAP）は、Cisco NX-OS 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います。LDAP サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する LDAP デーモンのデータベースで管理されます。Cisco NX-OS 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使用できます。

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（ポート 389）を使用します。Cisco NX-OS 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。

LDAP 認証および許可

クライアントは、簡易バインド（ユーザ名とパスワード）を使用して LDAP サーバとの TCP 接続および認証セッションを確立します。許可プロセスの一環として、LDAP サーバはそのデータベースを検索し、ユーザ プロファイルやその他の情報を取得します。

バインドしてから検索する（認証を行ってから許可する）か、または検索してからバインドするように、バインド操作を設定できます。デフォルトでは、検索してからバインドする方式が使用されます。

検索してからバインドする方式の利点は、baseDN の前にユーザ名（cn 属性）を追加することで認定者名（DN）を形成するのではなく、検索結果で受け取った DN をバインディング時にユーザ DN として使用できることです。この方式は、ユーザ DN がユーザ名と baseDN の組み合わせとは異なる場合に特に役立ちます。ユーザ バインドのために、bindDN が baseDN + append-with-baseDN として構成されます。ここで、append-with-baseDN は cn=$userid のデフォルト値です。

（注） バインド方式の代わりに、比較方式を使用して LDAP 認証を確立することもできます。比較方式では、サーバでユーザ入力の属性値を比較します。たとえば、ユーザ パスワード属性を比較して認証を行うことができます。デフォルトのパスワード属性タイプは userPassword です。

ユーザ ログインにおける LDAP の動作

LDAP を使用する Cisco NX-OS デバイスに対して、ユーザがパスワード認証プロトコル（PAP）ログインを試みると、次の処理が行われます。

1. Cisco NX-OS デバイスは接続が確立されると、ユーザ名とパスワードを取得するために LDAP デーモンに接続します。
2. Cisco NX-OS デバイスは、最終的に LDAP デーモンから次のいずれかの応答を得ます。
   - ACCEPT：ユーザの認証に成功したので、サービスを開始します。Cisco NX-OS デバイスがユーザ許可を必要とする場合は、許可処理が始まります。
   - REJECT：ユーザ認証は失敗します。LDAP デーモンは、ユーザに対してそれ以上のアクセスを拒否するか、ログイン操作を再試行するように要求します。
   - ERROR：デーモンによる認証サービスの途中でエラーが発生したか、またはデーモンと Cisco NX-OS デバイスの間のネットワーク接続でエラーが発生しました。Cisco NX-OS デバイスは ERROR 応答を受信した場合、別の方法でユーザの認証を試行します。

   認証が終了し、Cisco NX-OS デバイスで許可がイネーブルになっていれば、続いてユーザの許可フェーズに入ります。LDAP 許可に進むには、まず LDAP 認証を正常に終了する必要があります。
3. LDAP 許可が必要な場合、Cisco NX-OS デバイスは再び LDAP デーモンに接続し、デーモンから ACCEPT または REJECT 応答が返されます。ACCEPT 応答には、ユーザに対する EXEC または NETWORK セッションの送信に使用される属性が含まれます。また ACCEPT

応答により、ユーザがアクセス可能なサービスが決まります。この場合のサービスは次のとおりです。

- Telnet、rlogin、ポイントツーポイントプロトコル（PPP）、シリアルラインインターネットプロトコル（SLIP）、EXEC サービス
- 接続パラメータ（ホストまたはクライアントの IP アドレス（IPv4 または IPv6）、アクセス リスト、ユーザ タイムアウト）

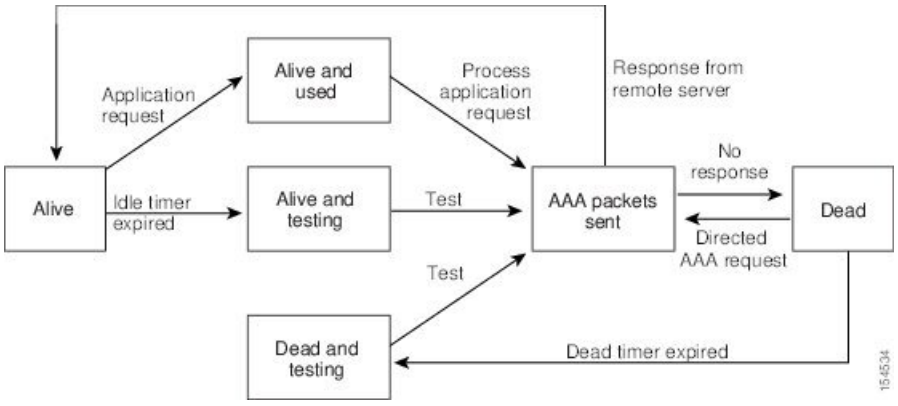
（注） LDAP では、デーモンがユーザを認証するために十分な情報を得られるまで、デーモンとユーザとの自由な対話を許可します。通常、デーモンはユーザ名とパスワードの組み合わせを入力するよう求めますが、他の項目を求めることもできます。

（注） LDAP では、認証の前に許可を行うことができます。

LDAP サーバのモニタリング

応答を返さない LDAP サーバがあると、AAA 要求の処理に遅延が発生することがあります。AAA 要求の処理時間を短縮するために、LDAP サーバを定期的にモニタして LDAP サーバが応答している（アライブ）かどうかを調べることができます。Cisco NX-OS デバイスは、応答の遅い LDAP サーバをデッド（dead）としてマークし、デッド LDAP サーバには AAA 要求を送信しません。Cisco NX-OS デバイスはデッド LDAP サーバを定期的にモニタし、応答があればアライブ状態に戻します。このモニタリング プロセスでは、実際の AAA 要求が送信される前に、LDAP サーバが稼働状態であることを確認します。LDAP サーバがデッドまたはアライブの状態に変わると、簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、Cisco NX-OS デバイスは、パフォーマンスに影響が出る前に、障害が発生していることをエラーメッセージで表示します。次の図に、LDAP サーバ モニタリングのサーバの状態を示します。

図 *1 : LDAP* サーバの状態



（注） 稼働中のサーバと停止中のサーバのモニタリング間隔はそれぞれ別で、ユーザが設定できます。LDAP サーバ モニタリングを実行するには、テスト認証要求を LDAP サーバに送信します。

LDAP のベンダー固有属性

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）ドラフト標準には、ネットワーク アクセス サーバと LDAP サーバ間での Vendor-Specific Attribute（VSA; ベンダー固有属性）の通信方法が規定されています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、一般的な用途には適さない独自の拡張属性をサポートできます。

LDAP 用の Cisco VSA 形式

シスコの LDAP 実装では、IETF 仕様で推奨される形式を使用したベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダー タイプは 1（名前付き cisco-av-pair）です。値は次の形式のストリングです。

```
protocol : attribute separator value *
```

protocol は、特定の許可タイプを表すシスコの属性です。separator は、必須属性の場合は =（等号）、オプションの属性の場合は *（アスタリスク）です。Cisco NX-OS デバイス上の認証に LDAP サーバを使用した場合、LDAP では LDAP サーバに対して、認証結果とともに権限付与情報などのユーザ属性を返すように指示します。この許可情報は、VSA で指定されます。Cisco NX-OS ソフトウェアでは、次の VSA プロトコル オプションをサポートしています。

- shell：ユーザ プロファイル情報を提供する access-accept パケットで使用されるプロトコル。

Cisco NX-OS ソフトウェアは、次の属性をサポートしています。

- roles：ユーザが属するすべてのロールの一覧です。値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。

LDAP のバーチャライゼーション サポート

Cisco NX-OS デバイスは、仮想ルーティング/転送（VRF）インスタンスを使用して LDAP サーバにアクセスします。VRF の詳細情報については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

LDAP の前提条件

LDAP の前提条件は次のとおりです。

- LDAP サーバの IPv4 または IPv6 アドレスまたはホスト名を取得すること
- Cisco NX-OS デバイスが AAA サーバの LDAP クライアントとして設定されていること

LDAP の注意事項と制約事項

LDAP に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS デバイス上には最大 64 の LDAP サーバを設定できます。
- Cisco NX-OS は LDAP バージョン 3 だけをサポートします。
- Cisco NX-OS は次の LDAP サーバだけをサポートします。
  - OpenLDAP
  - Microsoft Active Directory
- Secure Sockets Layer（SSL）上の LDAP は、SSL バージョン 3 および Transport Layer Security（TLS）バージョン 1.2 のみをサポートします。
- Cisco NX-OS リリース 10.4(3)F 以降、Secure Sockets Layer（SSL）を介した LDAP は、Cisco Nexus スイッチで TLS バージョン 1.3 および 1.2 をサポートします。TLS v1.1 は廃止されました。
- LDAP over SSL の場合、LDAP クライアント設定では、LDAP サーバ証明書のサブジェクトとしてホスト名を含める必要があります。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。
- Cisco NX-OS リリース 10.3(1)F 以降、LDAP は Cisco Nexus 9808 スイッチでサポートされます。
  - Cisco NX-OS リリース 10.4(1)F 以降、LDAP は、Cisco Nexus X98900CD-A および X9836DM-A ライン カードを搭載した Cisco Nexus 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、LDAP は Cisco Nexus 9804 スイッチ、Cisco Nexus X98900CD-A および X9836DM-A ライン カードでサポートされます。
- Cisco NX-OS リリース 10.4(2)F 以降、構成の置換機能は Cisco NX-OS デバイスの LDAP でサポートされます。

LDAP のデフォルト設定

次の表に、LDAP パラメータのデフォルト設定を示します。

パラメータ	デフォルト
LDAP	ディセーブル

パラメータ	デフォルト
LDAP 認証方式	検索してからバインド
LDAP 認証メカニズム	プレーン
デッドタイム間隔	0 分
タイムアウト間隔	5 秒
アイドル タイマー間隔	60 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	Cisco

LDAP の設定

ここでは、Cisco NX-OS デバイスで LDAP を設定する手順を説明します。

LDAP サーバの設定プロセス

process_workflow

次の設定プロセスに従って、LDAP サーバを設定できます。

1. LDAP をイネーブルにします。
2. LDAP サーバと Cisco NX-OS デバイスの接続を確立します。
3. 必要に応じて、AAA 認証方式用に、LDAP サーバのサブセットを使用して LDAP サーバ グループを設定します。
4. （任意）TCP ポートを設定します。
5. （任意）LDAP サーバにデフォルト AAA 認証方式を設定します。
6. （任意）LDAP 検索マップを設定します。
7. （任意）必要に応じて、LDAP サーバの定期モニタリングを設定します。

関連トピック

LDAP 機能の有効化 （7 ページ）
LDAP サーバー ホストの構成 （8 ページ）
LDAP サーバの rootDN の設定 （9 ページ）
LDAP サーバ グループの設定 （10 ページ）
TCP ポートの設定 （14 ページ）
LDAP 検索マップの構成 （15 ページ）

LDAP サーバの定期的モニタリングの設定 （16 ページ）

LDAP 機能の有効化

LDAP は最初は NX- OS デバイス上で無効です。認証に関するコンフィギュレーション コマンドと検証コマンドを使用するには、LDAP 機能を明示的に有効にする必要があります。

LDAP 機能を有効にするには、次の手順を実行します。

手順

ステップ 1 **configure terminal** コマンドでグローバル コンフィギュレーション モードに入ります。

例：

```
switch# configure terminal
```

ステップ 2 **feature ldap** コマンドで LDAP を有効にします。これを無効化するには、このコマンドの no 形式を入力します。

例：

```
switch(config)# feature ldap
```

（注）
LDAP を無効化にすると、関連するすべての構成が削除されます。

ステップ 3 **copy running-config startup-config** で実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

例：

```
switch(config)# copy running-config startup-config
```

LDAP 機能が有効になり、認証コンフィギュレーション コマンドが利用可能になります。

関連トピック

LDAP サーバの設定プロセス （6 ページ）
LDAP サーバー ホストの構成 （8 ページ）
LDAP サーバの rootDN の設定 （9 ページ）
LDAP サーバ グループの設定 （10 ページ）
グローバルな LDAP タイムアウト間隔の設定 （12 ページ）
LDAP サーバのタイムアウト間隔の設定 （13 ページ）
TCP ポートの設定 （14 ページ）
LDAP 検索マップの構成 （15 ページ）
LDAP サーバの定期的モニタリングの設定 （16 ページ）
LDAP デッド タイム間隔の設定 （17 ページ）

LDAP サーバでの AAA 許可の設定 （18 ページ）

LDAP サーバー ホストの構成

Cisco NX-OS デバイスがユーザー認証を目的としてリモート LDAP サーバーにアクセスできるように、LDAP サーバー ホストを構成します。LDAP サーバーの IP またはホスト名を追加し、必要に応じてセキュアな通信のために SSL を有効にするには、次の手順を活用します。

（注） デフォルトでは、LDAP サーバの IP アドレスまたはホスト名を Cisco NX-OS デバイスで設定すると、LDAP サーバがデフォルトの LDAP サーバ グループに追加されます。LDAP サーバを別の LDAP サーバ グループに追加することもできます。

LDAP サーバー ホストを構成するには、次の手順を実行します：

始める前に

- デバイスの LDAP を有効にします。
- LDAP サーバーの IPv4 または IPv6 アドレスまたはホスト名を取得します。
- SSL を有効にする場合は、デバイスで LDAP サーバー証明書が手動で構成されていることを確認します。

手順

ステップ 1 **configure terminal** コマンドを使用して、グローバル構成モードを開始します。。

例：

```
switch# configure terminal
switch(config)#
```

ステップ 2 次のコマンドを使用して、LDAP サーバーの IP アドレスまたはホスト名を指定します：**ldap-server host** 。

- オプションで、 `enable-ssl` キーワードを使用して通信を暗号化します。
- オプションで、 `referral-disable` キーワードを使用して参照リンクを無効にします。

例：

```
switch(config)# switch(config)# ldap-server host 10.10.2.2 enable-ssl
```

ステップ 3 （オプション） **show ldap-server** を使用して LDAP サーバーの構成を確認します。 コマンドを使用します。

例：

```
switch(config)# show ldap-server
```

ステップ 4 **copy running-config startup-config** コマンドを使用して構成を保存します。

例：

```
switch(config)# copy running-config startup-config
```

LDAP サーバー ホストが構成され、認証操作を行える状態になっています。

関連トピック

LDAP サーバの設定プロセス （6 ページ）
LDAP 機能の有効化 （7 ページ）
LDAP サーバ グループの設定 （10 ページ）
LDAP サーバの rootDN の設定 （9 ページ）
LDAP サーバ グループの設定 （10 ページ）
LDAP サーバの定期的モニタリングの設定 （16 ページ）
LDAP サーバのモニタリング （21 ページ）
LDAP サーバ統計情報のクリア （22 ページ）

LDAP サーバの rootDN の設定

LDAP サーバ データベースのルート指定名（DN）を設定できます。rootDN は、LDAP サーバにバインドしてそのサーバの状態を確認するために使用します。

始める前に

LDAP を有効にします。

リモートの LDAP サーバの IPv4 または IPv6 アドレスまたはホスト名を取得します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	[**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **rootDN** *root-name* [**password** *password* [**port** *tcp-port* [**timeout** *seconds*] | **timeout** *seconds*]] 例： `switch(config)# ldap-server host 10.10.1.1 rootDN cn=manager,dc=acme,dc=com password Ur2Gd2BH timeout 60`	LDAP サーバ データベースの rootDN を指定し、ルートのパスワードをバインドします。 任意で、サーバに送る LDAP メッセージに使用する TCP ポートを指定します。有効な範囲は 1 ～ 65535 です。デフォルトの TCP ポートはグローバル値です（グローバル値が設定されていない場合は

	コマンドまたはアクション	目的
		389）。また、サーバのタイムアウト間隔も指定します。値の範囲は 1 ～ 60 秒です。デフォルトのタイムアウト値はグローバル値です（グローバル値が設定されていない場合は 5 秒）。
ステップ 3	（任意） **show ldap-server** 例： `switch(config)# show ldap-server`	LDAP サーバの設定を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP サーバの設定プロセス （6 ページ）
LDAP 機能の有効化 （7 ページ）
LDAP サーバー ホストの構成 （8 ページ）

LDAP サーバ グループの設定

サーバ グループを使用して、1 台または複数台のリモート AAA サーバによるユーザ認証を指定することができます。グループのメンバはすべて、LDAP を使用するように設定する必要があります。設定した順序に従ってサーバが試行されます。

これらのサーバ グループはいつでも設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。

Before you begin

LDAP を有効にします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	[**no**] **aaa group server ldap** *group-name* **Example:**	LDAP サーバ グループを作成し、そのグループの LDAP サーバ グループ コ

	Command or Action	Purpose
	`switch(config)# aaa group server ldap LDAPServer1` `switch(config-ldap)#`	ンフィギュレーションモードを開始します。
ステップ 3	[**no**] **server** {*ipv4-address* | *ipv6-address* | *host-name*} **Example:** `switch(config-ldap)# server 10.10.2.2`	LDAP サーバを、LDAP サーバ グループのメンバとして設定します。 指定した LDAP サーバが見つからなかった場合は、**ldap-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	(Optional) [**no**] **authentication** {**bind-first** [**append-with-baseDN** *DNstring*] | **compare** [**password-attribute** *password*]} **Example:** `switch(config-ldap)# authentication compare password-attribute TyuL8r`	バインド方式または比較方式を使用して LDAP 認証を実行します。デフォルトの LDAP 認証方式は、検索してからバインドするバインド方式です。
ステップ 5	(Optional) [**no**] **enable user-server-group** **Example:** `switch(config-ldap)# enable user-server-group`	グループ検証を有効にします。LDAP サーバでグループ名を設定する必要があります。ユーザは、ユーザ名がLDAP サーバで設定されたこのグループのメンバとして示されている場合にだけ、公開キー認証を通じてログインできます。
ステップ 6	(Optional) [**no**] **enable Cert-DN-match** **Example:** `switch(config-ldap)# enable Cert-DN-match`	ユーザ プロファイルでユーザ証明書のサブジェクト DN がログイン可能と示されている場合にだけユーザがログインできるようにします。
ステップ 7	(Optional) **no** [**use-vrf** *vrf-name*] **Example:** `switch(config-ldap)# use-vrf vrf1`	サーバ グループ内のサーバとの接続に使用する VRF を指定します。

ステップ 8	**exit**
	Example:
	`switch(config-ldap)# exit`
	`switch(config)#`
		LDAP サーバ グループ コンフィギュレーション モードを終了します。

ステップ 9	(Optional) **show ldap-server groups** **Example:** `switch(config)# show ldap-server groups`	LDAP サーバ グループの設定を表示します。

	Command or Action	Purpose
ステップ 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

LDAP サーバの設定プロセス （6 ページ）
LDAP サーバー ホストの構成 （8 ページ）
LDAP 機能の有効化 （7 ページ）
LDAP サーバー ホストの構成 （8 ページ）

グローバルな LDAP タイムアウト間隔の設定

Cisco NX-OS デバイスがすべての LDAP サーバからの応答を待つ時間を決定するグローバル タイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。

始める前に

LDAP をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	[**no**] **ldap-server timeout** *seconds* 例： `switch(config)# ldap-server timeout 10`	LDAP サーバのタイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒です。有効な範囲は 1 ～ 60 秒です。
ステップ 3	（任意） **show ldap-server** 例： `switch(config)# show ldap-server`	LDAP サーバの設定を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP 機能の有効化 （7 ページ）
LDAP サーバのタイムアウト間隔の設定 （13 ページ）
LDAP サーバのタイムアウト間隔の設定 （13 ページ）

LDAP サーバのタイムアウト間隔の設定

Cisco NX-OS デバイスが LDAP サーバからの応答を待つ時間を決定するタイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。

始める前に

LDAP をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	[**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **timeout** *seconds* 例： `switch(config)# ldap-server host server1 timeout 10`	特定のサーバのタイムアウト間隔を指定します。デフォルトはグローバル値です。 （注） 特定の LDAP サーバに指定したタイムアウト間隔は、すべての LDAP サーバで使用されるグローバルなタイムアウト間隔を上書きします。
ステップ 3	（任意） **show ldap-server** 例： `switch(config)# show ldap-server`	LDAP サーバの設定を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

グローバルな LDAP タイムアウト間隔の設定 （12 ページ）

LDAP 機能の有効化 （7 ページ）
グローバルな LDAP タイムアウト間隔の設定 （12 ページ）

TCP ポートの設定

別のアプリケーションとポート番号が競合している場合は、LDAP サーバ用に別の TCP ポートを設定できます。デフォルトでは、Cisco NX-OS デバイスはすべての LDAP 要求に対しポート 389 を使用します。

始める前に

LDAP をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	[**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **port** *tcp-port* [**timeout** *seconds*] 例： `switch(config)# ldap-server host 10.10.1.1 port 200 timeout 5`	サーバに送る LDAP メッセージに使用する TCP ポートを指定します。デフォルトの TCP ポートは 389 です。有効な範囲は 1 ～ 65535 です。 任意でサーバのタイムアウト間隔を指定します。値の範囲は 1 ～ 60 秒です。デフォルトのタイムアウト値はグローバル値です（グローバル値が設定されていない場合は 5 秒）。 （注） 特定の LDAP サーバに指定したタイムアウト間隔は、すべての LDAP サーバで使用されるグローバルなタイムアウト間隔を上書きします。
ステップ 3	（任意） **show ldap-server** 例： `switch(config)# show ldap-server`	LDAP サーバの設定を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例：	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
	`switch(config)# copy running-config startup-config`	

関連トピック

LDAP サーバの設定プロセス （6 ページ）
LDAP 機能の有効化 （7 ページ）

LDAP 検索マップの構成

検索クエリーをLDAPサーバーに送信するようにLDAP検索マップを構成できます。サーバはそのデータベースで、検索マップで指定された基準を満たすデータを検索します。

始める前に

LDAP をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ldap search-map** *map-name*
	例：
	`switch(config)# ldap search-map map1`
	`switch(config-ldap-search-map)#`
		LDAP 検索マップを設定します。

ステップ 3	（任意） [**userprofile** | **trustedCert** | **CRLLookup** | **user-certdn-match** | **user-pubkey-match** | **user-switch-bind**] **attribute-name** *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name* 例： `switch(config-ldap-search-map)# userprofile attribute-name att-name search-filter (&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com`	ユーザ プロファイル、信頼できる証明書、CRL、証明書DN一致、公開キー一致、または user-switchgroup ルックアップ検索操作の属性名、検索フィルタ、およびベースDNを設定します。これらの値は、検索クエリーを LDAP サーバに送信するために使用されます。 *Attribute-name* 引数は Nexus ロール定義を含む LDAP サーバ属性の名前です。

ステップ 4	（任意） **exit**
	例：
	`switch(config-ldap-search-map)# exit`
	`switch(config)#`
		LDAP検索マップ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 5	（任意） **show ldap-search-map** 例： `switch(config)# show ldap-search-map`	設定された LDAP 検索マップを表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP サーバの設定プロセス （6 ページ）
LDAP 機能の有効化 （7 ページ）

LDAP サーバの定期的モニタリングの設定

LDAP サーバの可用性をモニタリングできます。設定パラメータには、サーバに対して使用するユーザ名とパスワード、サーバにバインドして状態を確認するための rootDN、およびアイドル タイマーがあります。アイドル タイマーには、LDAP サーバで何の要求も受信されない状態の時間を指定します。これを過ぎると Cisco NX-OS デバイスはテスト パケットを送信します。このオプションを設定して定期的にサーバをテストしたり、1 回だけテストを実行したりできます。

（注） ネットワークのセキュリティを保護するために、LDAP データベースの既存のユーザ名と同じものを使用しないことを推奨します。

始める前に

LDAP をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	必須: [**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **test rootDN** *root-name* [**idle-time** *minutes* | **password**	サーバ モニタリング用のパラメータを指定します。デフォルトのユーザ名は

	コマンドまたはアクション	目的
	password [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]] 例： `switch(config)# ldap-server host 10.10.1.1 test rootDN root1 username user1 password Ur2Gd2BH idle-time 3`	test、デフォルトのパスワードは Cisco です。アイドル タイマーのデフォルト値は 60 分です。有効な範囲は 1 ～ 1,440 分です。 （注） LDAP サーバデータベースの既存のユーザでないユーザを指定することを推奨します。
ステップ 3	[**no**] **ldap-server deadtime** *minutes* 例： `switch(config)# ldap-server deadtime 5`	以前に応答の遅かった LDAP サーバを Cisco NX-OS デバイスがチェックを始めるまでの分数を指定します。デフォルト値は 0 分です。そして、有効な範囲は 0 ～ 60 分です。
ステップ 4	（任意） **show ldap-server** 例： `switch(config)# show ldap-server`	LDAP サーバの設定を表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP サーバの設定プロセス （6 ページ）
LDAP 機能の有効化 （7 ページ）
LDAP サーバー ホストの構成 （8 ページ）

LDAP デッド タイム間隔の設定

すべての LDAP サーバのデッド タイム間隔を設定できます。デッド タイム間隔では、Cisco NX-OS デバイスが LDAP サーバをデッドであると宣言した後、そのサーバがアライブになったかどうかを確認するためにテスト パケットを送信するまでの時間を指定します。

（注） デッド タイム間隔に 0 分を設定すると、LDAP サーバは、応答を返さない場合でも、デッドとしてマークされません。デッド タイム間隔はグループ単位で設定できます。

始める前に

LDAP をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	[**no**] **ldap-server deadtime** *minutes* 例： `switch(config)# ldap-server deadtime 5`	グローバルなデッド タイム間隔を設定します。デフォルト値は0分です。範囲は 0 ～ 60 分です。
ステップ 3	（任意） **show ldap-server** 例： `switch(config)# show ldap-server`	LDAP サーバの設定を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP 機能の有効化 （7 ページ）

LDAP サーバでの AAA 許可の設定

LDAP サーバのデフォルトの AAA 許可方式を設定できます。

始める前に

LDAP を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	
ステップ 2	**aaa authorization** {**ssh-certificate** | **ssh-publickey**} **default** {**group** *group-list* | **local**} 例： `switch(config)# aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2`	LDAP サーバのデフォルトの AAA 許可方式を設定します。 **ssh-certificate** キーワードは証明書認証を使用した LDAP 許可またはローカル許可を設定し、**ssh-publickey** キーワードは SSH 公開キーを使用した LDAP 許可またはローカル許可を設定します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。 *group-list* 引数には、LDAP サーバ グループ名をスペースで区切ったリストを指定します。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。**local** 方式はローカル データベースを使用して許可を行います。
ステップ 3	（任意） **show aaa authorization** [**all**] 例： `switch(config)# show aaa authorization`	AAA 許可設定を表示します。**all** キーワードを指定すると、デフォルト値が表示されます。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP 機能の有効化 （7 ページ）

LDAP SSH 公開キー認証の設定

AAA 認証は、LDAP サーバーのユーザーエントリに保存されているユーザーの公開キーを使用して、LDAP サーバーを介して実行されます。

LDAP SSH 公開キー認証を設定する前に、次の点を考慮したことを確認してください。

- ユーザーの公開キーをユーザー属性として LDAP サーバーに保存します。
- SSH クライアントからの秘密キーを使用してサインインします。

（注） SSH サインイン時に提示した秘密キーは、LDAP サーバーに保存されている公開キーを使用して検証されます。

次の例は、サンプルの LDAP クライアントの設定を示しています。

次の例では、ユーザーの公開キーが、 **user-pubkey-match** 構成で指定された属性（以下の場合は **sshPublicKeys** 属性）で LDAP サーバーに保存されます。

```
ldap-server host fully qualified domain name.com rootDN
"CN=ucsadmin1,CN=Users,DC=PI-Sec-DT,DC=com"  password 7 password1
ldap search-map Map1
  userprofile attribute-name "description" search-filter "(cn=$userid)" base-DN
"DC=PI-Sec-DT,DC=com"
  user-pubkey-match attribute-name "sshPublicKeys" search-filter "(cn=$userid)" base-DN
 "DC=PI-Sec-DT,DC=com"
aaa group server ldap ldap1
  server fully qualified domain name.com
  use-vrf management
  ldap-search-map Map1

aaa authorization ssh-publickey default group ldap1
```

次に、ユーザの SSH クライアント秘密キーを使用して、スイッチ管理 IP アドレスにサインインする例を示します。

```
ssh ldapuser@10.0.0.1 -i ldap_pub_key_test
```

LDAP SSH 証明書許可の設定

AAA 許可は、LDAP サーバーのユーザー属性に保存されている証明書と証明書の DN を使用して、LDAP サーバーを介して実行されます。

LDAP SSH 証明書の許可中に、次のことが処理されます。

- スイッチにインストールされている CA 証明書を使用して、SSH クライアントを介して提示されたユーザー証明書の検証。
- **enable cert-dn-match** 設定はデフォルトで有効になっているため、証明書を検証するための、LDAP サーバーに保存されている DN との cert-DN-match は、自動的に処理されます。

次の例は、サンプルの LDAP クライアントの設定を示しています。

- 次の例は、**user-certdn-match** 構成で指定された特定の属性の下で LDAP サーバーに証明書 DN を保存する方法を示しています。

  形式は「x509v3-sign-rsa DN /DC=com, DC=PI-Sec-DT, CN=Users, CN=username1」です。

  ```
  ldap-server host fully qualified domain name.com rootDN
  "CN=ucsadmin1,CN=Users,DC=PI-Sec-DT,DC=com"  password 7 password1
  ldap search-map Map24
    userprofile attribute-name "description" search-filter "(cn=$userid)" base-DN
  "DC=PI-Sec-DT,DC=com"
    user-certdn-match attribute-name <attribute> search-filter "(cn=$userid)" base-DN
   "DC=PI-Sec-DT,DC=com"
  ```

```
aaa group server ldap ldap24
  server fully qualified domain name.com
  enable Cert-DN-match
  use-vrf management
  ldap-search-map Map24

aaa authorization ssh-certificate default group ldap24
```

- 次の show コマンドは、ボックスにインストールされている rootCA 証明書の詳細を表示します。

```
switch# show crypto ca certificates
Trustpoint: ldap
CA certificate 0:
subject=C = IN, ST = KAR, L = BGL, O = Cisco, OU = DCBG-Cert, CN = RootCA
issuer=C = IN, ST = KAR, L = BGL, O = Cisco, OU = DCBG-Cert, CN = RootCA
serial=82EE7603BF7E74A9
notBefore=May 29 07:12:30 2023 GMT
notAfter=May 26 07:12:30 2033 GMT
SHA1 Fingerprint=D5:AE:75:8E:A1:4F:79:1E:80:3E:5E:67:C5:42:44:10:13:C6:F7:1D
purposes: sslserver sslclient

n7700-DE#
```

- 次の例は、SSH クライアントからユーザー サインインを実行する方法を示しています。
  - SSHクライアントでは、入力証明書には秘密キーとユーザー証明書の両方が含まれており、結合されて「<user> .crt」という単一のファイルになっています。
  - rootCA.crt は rootCA 証明書ファイルです。
  - IP アドレスはスイッチの管理 IP アドレスです。

```
ssh username1@10.0.0.1 -i username1.crt -vvv -oCACertificateFile=rootCA.crt
```

LDAP サーバのモニタリング

Cisco NX-OS デバイスが保持している LDAP サーバのアクティビティに関する統計情報をモニタリングできます。

始める前に

Cisco NX-OS デバイスに LDAP サーバを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**show ldap-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} 例： `switch# show ldap-server statistics 10.10.1.1`	LDAP サーバの統計情報を表示します。

関連トピック

LDAP サーバー ホストの構成 （8 ページ）
LDAP サーバ統計情報のクリア （22 ページ）
LDAP サーバ統計情報のクリア （22 ページ）

LDAP サーバ統計情報のクリア

Cisco NX-OS デバイスが保持している LDAP サーバのアクティビティに関する統計情報を表示します。

始める前に

Cisco NX-OS デバイスに LDAP サーバを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	（任意） **show ldap-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} 例： `switch# show ldap-server statistics 10.10.1.1`	LDAP サーバの統計情報を表示します。
ステップ 2	**clear ldap-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} 例： `switch# clear ldap-server statistics 10.10.1.1`	LDAP サーバ統計情報をクリアします。

関連トピック

LDAP サーバのモニタリング （21 ページ）
LDAP サーバー ホストの構成 （8 ページ）
LDAP サーバのモニタリング （21 ページ）

LDAP 設定の確認

LDAP 設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show running-config ldap [**all**]	実行コンフィギュレーションの LDAP 設定を表示します。

コマンド	目的
show startup-config ldap	スタートアップ コンフィギュレーションの LDAP 設定を表示します。
show ldap-server	LDAP 設定情報を表示します。
show ldap-server groups	LDAP サーバ グループの設定情報を表示します。
show ldap-server statistics {*hostname* | *ipv4-address* | *ipv6-address*}	LDAP 統計情報を表示します。
show ldap-search-map	設定されている LDAP 属性マップに関する情報を表示します。

LDAP の設定例

次に、LDAP サーバ ホストおよびサーバ グループを設定する例を示します。

```
feature ldap
ldap-server host 10.10.2.2 enable-ssl
aaa group server ldap LdapServer
server 10.10.2.2
exit
show ldap-server
show ldap-server groups
```

次に、LDAP 検索マップを設定する例を示します。

```
ldap search-map s0
userprofile attribute-name att-name search-filter "
(&(objectClass=Person)(sAMAccountName=$userid))" base-DN dc=acme,dc=com
exit
show ldap-search-map
```

次に、LDAP サーバに対する証明書認証を使用して AAA 許可を設定する例を示します。

```
aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2
exit
show aaa authorization
```

次の例は、認証を検証する方法を示しています。

```
failing
test aaa group LdapServer user <user-password>
user has failed authentication

! working
test aaa group LdapServer user <user-password>
user has been authenticated
```

次の作業

これで、サーバ グループも含めて AAA 認証方式を設定できるようになります。

LDAP に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『*Cisco NX-OS* ライセンス ガイド』
VRF コンフィギュレーション	『*Cisco Nexus 9000* シリーズ *NX-OS* ユニキャスト ルーティング設定ガイド』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
LDAP に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。