LDAP の IPv6 サポートの設定

LDAP の IPv6 サポートを構成するための制限

- バインド、検索、および比較操作のみがサポートされます。
- Lightweight Directory Access Protocol（LDAP）の参照はサポートされていません。
- LDAP サーバからの割り込みメッセージまたは通知は処理されません。

LDAP の IPv6 サポートの設定に関する情報

LDAP の IPv6 サポート

IPv6 を介した Lightweight Directory Access Protocol （LDAP）をサポートするために、IPv6 ネットワークを介した通信中の認証と承認に関して、認証、承認、およびアカウンティング（AAA）トランザクションに変更が加えられます。IPv6 ネットワーク上で LDAP をサポートするために、サーバー構成に基づいて IPv4 と IPv6 の両方をサポートするようにトランスポート呼び出しが変更されました。

Transport Layer Security

Transport Layer Security（TLS）は、プライバシー、認証、およびデータ整合性によるデータのセキュアトランザクションを可能にするアプリケーションレベルプロトコルです。証明書、公開キー、および秘密キーに基づいて、クライアントの身元を証明します。証明書は、認証局（CA）によって発行されます。各証明書には、発行した機関の名前、証明書の発行先エンティティの名前、エンティティの公開キー、および証明書の有効期限を示すタイムスタンプが含まれます。TLS による LDAP のサポートについては、LDAP プロトコルの拡張として RFC 2830 で説明されています。

LDAP 操作

バインド

バインド操作は、サーバーに対してユーザーを認証するために使用されます。LDAP サーバーとの接続を開始するために使用されます。LDAP はコネクション型プロトコルです。クライアントはプロトコルバージョンとクライアント認証情報を指定します。LDAP は次のバインドをサポートします。

- 認証済みバインド
- 匿名バインド

認証済みバインドは、ルートの認定者名（DN）とパスワードが使用できる場合に実行されます。ルート DN とパスワードがない場合、匿名バインドが実行されます。LDAP 環境では、検索操作が実行されてから、バインド操作が実行されます。これは、パスワード属性が検索操作の一部として返される場合、パスワードの確認を LDAP クライアントのローカルで実行できるためです。したがって、余計なバインド操作を実行する必要がなくなります。パスワード属性が返されない場合、バインド操作を後で実行できます。検索操作を先に実行してバインド操作を後で実行するもう 1 つの利点は、ユーザー名（cn 属性）の前にベース DN を付けることで DN を構成するのではなく、検索結果で受信した DN をユーザー DN として使用できることです。LDAP サーバーに保存されているすべてのエントリには、固有の DN があります。DN は、Relative Distinguished Name（RDN）と、レコードが存在する LDAP サーバー内の場所の 2 つの部分で構成されます。

LDAP サーバーに保存されているエントリのほとんどには名前があり、多くの場合、名前は Common Name（cn）属性で保存されます。すべてのオブジェクトには名前があるため、LDAP に保存されているほとんどのオブジェクトは RDN のベースとして cn 値を使用します。

比較

認証のために、比較操作を使用して、バインド要求を比較要求で置換します。比較操作によって、接続のための最初のバインド パラメータを維持できます。

検索

検索操作は、LDAP サーバーを検索するために使用されます。クライアントは検索の開始点（ベース DN）、検索範囲（オブジェクト、その子、またはそのオブジェクトをルートとするサブツリー）、およびサーチ フィルタを指定します。

認可要求の場合、検索操作はバインド操作なしで直接実行されます。検索操作を正常に実行するには、LDAP サーバを特定の特権で設定します。この特権レベルは、バインド操作で設定します。

LDAP 検索操作は、特定のユーザーについて複数のユーザー エントリを返す可能性があります。このような場合、LDAP クライアントは適切なエラー コードを AAA に返します。このようなエラーを回避するために、単一のエントリに一致することができる適切なサーチフィルタを設定する必要があります。

LDAP の IPv6 サポートを構成する方法

デバイスと LDAP サーバーの通信の設定

Lightweight Directory Access Protocol（LDAP）ホストは、Active Directory（Microsoft）や OpenLDAP などの LDAP サーバーソフトウェアを実行するマルチユーザーシステムです。デバイスから LDAP サーバーへの通信の構成には、いくつかのコンポーネントがあります。

- ホスト名または IP アドレス
- ポート番号
- タイムアウト時間
- 基本識別名（DN）

デバイスから LDAP サーバーへの通信を構成するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例**： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **例**： `Device# configure terminal`	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
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**ldap server** *name* 例： `Device(config)# ldap server server1`	デバイスを LDAP プロトコルとして設定し、LDAP サーバ コンフィギュレーション モードを開始します。
ステップ 5	**ipv6** *ipv6-address* 例： `Device(config-ldap-server)# ipv6 2001:DB8:0:0:8:800`	LDAP サーバーへの IPv6 アドレスを指定します。
ステップ 6	**transport port** *port-number* 例： `Device(config-ldap-server)# transport port 200`	LDAP サーバーに接続するためにトランスポートプロトコルを設定します。
ステップ 7	**timeout retransmit** *seconds* 例： `Device(config-ldap-server)# timeout retransmit 20`	デバイスが LDAP 要求への応答を待機してから、要求を再送信する秒数を指定します。
ステップ 8	**exit** 例： `Device(config-ldap-server)# exit`	LDAP サーバー コンフィギュレーション モードを終了し、グローバル コンフィギュレーションモードに入ります。

LDAP プロトコル パラメータの設定

LDAP プロトコルパラメータを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**aaa** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**ldap server** *name* 例： `Device(config)# ldap server server1`	Lightweight Directory Access Protocol（LDAP）サーバーを定義し、LDAP サーバー コンフィギュレーション モードを開始します。
ステップ 5	**bind authenticate root-dn password** [**0** *string* | **7** *string*] *string* 例： `Device(config-ldap-server)# bind authenticate root-dn "cn=administrator,cn=users,dc=rac-blr2,dc=example,dc=com" password"`	デバイスと LDAP サーバー間で使用される共有秘密テキスト文字列を指定します。暗号化されていない共有秘密を設定するには、**0** 回線オプションを使用します。暗号化された共有秘密を設定するには、**7** 回線オプションを使用します。
ステップ 6	**search-filter user-object-type** *string* 例： `Device(config-ldap-server)# search-filter user-object-type string1`	検索要求に使用するサーチ フィルタを指定します。
ステップ 7	**base-dn** *string* 例： `Device(config-ldap-server)# base-dn "dc=sns,dc=example,dc=com"`	検索の基本識別名（DN）を指定します。
ステップ 8	**mode secure** [**no-negotiation**] 例： `Device(config-ldap-server)# mode secure no-negotiation`	トランスポート層セキュリティ（TLS）接続を開始するように LDAP を設定し、セキュアモードを指定します。
ステップ 9	**secure cipher 3des-ede-cbc-sha** 例： `Device(config-ldap-server)# secure cipher 3des-ede-cbc-sha`	安全な接続の場合の暗号スイートを指定します。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： `Device(config-ldap-server)# exit`	LDAP サーバー コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。

認証要求のための検索操作とバインド操作の設定

認証要求の検索およびバインド操作を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**ldap server** *name* 例： `Device(config)# ldap server server1`	Lightweight Directory Access Protocol（LDAP）サーバーを定義し、LDAP サーバー コンフィギュレーション モードを開始します。
ステップ 5	**authentication bind-first** 例： `Device(config-ldap-server)# authentication bind-first`	認証要求のために一連の検索操作とバインド操作を設定します。
ステップ 6	**authentication compare** 例： `Device(config-ldap-server)# authentication compare`	バインド要求を認証の比較要求に置き換えます。

	コマンドまたはアクション	目的
ステップ 7	**exit** 例： `Device(config-ldap-server)# exit`	LDAP サーバー コンフィギュレーション モードを終了します。

LDAP スケーラビリティ機能のモニタリングと保守

次の **show** および **debug** コマンドは任意の順序で入力できます。

手順

ステップ 1 **enable**

例：

```
> enable
```

特権 EXEC モードを有効にします。

パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
# configure terminal
```

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 3 **clear ldap server**

TCP 接続の Lightweight Directory Access Protocol（LDAP）サーバーをクリアします。

例：

```
# clear ldap server
```

ステップ 4 **debug ldap**

LDAP 関連の情報を表示します。

例：

```
# debug ldap
```

ステップ 5 **show ldap server**

LDAP サーバの状態情報など、サーバの多様なカウンタを表示します。

例：

```
# show ldap server
```

ステップ 6 show ldap attributes

デフォルトの LDAP 属性マッピングに関する情報を表示します。

例：

```
Device# show ldap attributes

LDAP Attribute                  Format      AAA Attribute
==============                  ======      =============
airespaceBwDataBurstContract    Ulong       bsn-data-bandwidth-burst-contr
userPassword                    String      password
airespaceBwRealBurstContract    Ulong       bsn-realtime-bandwidth-burst-c
employeeType                    String      employee-type
airespaceServiceType            Ulong       service-type
airespaceACLName                String      bsn-acl-name
priv-lvl                        Ulong       priv-lvl
memberOf                        String DN   supplicant-group
cn                              String      username
airespaceDSCP                   Ulong       bsn-dscp
policyTag                       String      tag-name
airespaceQOSLevel               Ulong       bsn-qos-level
airespace8021PType              Ulong       bsn-8021p-type
airespaceBwRealAveContract      Ulong       bsn-realtime-bandwidth-average
airespaceVlanInterfaceName      String      bsn-vlan-interface-name
airespaceVapId                  Ulong       bsn-wlan-id
airespaceBwDataAveContract      Ulong       bsn-data-bandwidth-average-con
sAMAccountName                  String      sam-account-name
meetingContactInfo              String      contact-info
telephoneNumber                 String      telephone-number
Map: att_map_1
department                      String DN   element-req-qos
```

LDAP の IPv6 サポートの構成例

例：デバイスから LDAP サーバーへの通信

次に、サーバーグループ server1 を作成し、IP アドレス、トランスポートポート 200、および再送信値を指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# ldap server server1
Device(config-ldap-server)# ipv6 2001:DB8:0:0:8:800
Device(config-ldap-server)# transport port 200
Device(config-ldap-server)# timeout retransmit 20
Device(config-ldap-server)# exit
```

例：LDAP プロトコルパラメータ

次の例は、Lightweight Directory Access Protocol（LDAP）パラメータを設定する方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# ldap server server1
Device(config-ldap-server)# bind authenticate root-dn
"cn=administrator,cn=users,dc=nac-blr2,dc=example,dc=com password"
Device(config-ldap-server)# base-dn "dc=sns,dc=example,dc=com"
Device(config-ldap-server)# mode secure no-negotiation
Device(config-ldap-server)# secure cipher 3des-ede-cbc-sha
Device(config-ldap-server)# exit
```

例：認証要求のための検索操作とバインド操作

次に、認証要求のために一連の検索およびバインド操作を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# ldap server server1
Device(config-ldap-server)# authentication bind-first
Device(config-ldap-server)# authentication compare
Device(config-ldap-server)# exit
```

例：LDAP サーバーからのサーバー情報

LDAP サーバーからの出力例を次に示します。

```
Device# show ldap server all

Server Information for server1
============================================
 Server name              :server1
 Server IP                :2001:DB8:0:0:8:800
 Server listening Port    :389
 Connection status        :DOWN
 Root Bind status         :No Bind
 Server mode              :Non-Secure
 Cipher Suite             :0x00
 Authentication Seq       :Search first. Then Bind/Compare      password next
 Authentication Procedure :Bind with user password
 Request timeout          :30
 ------------------------------------------
 * LDAP STATISTICS *
 Total messages  [Sent:0, Received:0]
 Response delay(ms) [Average:0, Maximum:0]
 Total search    [Request:0, ResultEntry:0, ResultDone:0]
 Total bind      [Request:0, Response:0]
 Total extended  [Request:0, Response:0]
 Total compare   [Request:0, Response:0]
 Search [Success:0, Failures:0]
 Bind   [Success:0, Failures:0]
```

```
 Missing attrs in Entry [0]
------------------------------------------
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9600 Series Switches)*

標準および RFC

標準/RFC	タイトル
RFC 4511	*Lightweight Directory Access Protocol*（*LDAP*）
RFC 4513	「*Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms*」

LDAP の IPv6 サポートの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.11.1	LDAP の IPv6 サポート	LDAP の IPv6 サポート機能では、認証、許可、およびアカウンティング（AAA）トランザクションに変更を加えることにより、LDAP プロトコルの IPv6 トランスポートサポートについて説明します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

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。