AAA の LDAP サーバ

この章では、AAA で使用される LDAP サーバの設定方法について説明します。

LDAP および ASA について

Cisco ASA はほとんどの LDAPv3 ディレクトリ サーバと互換性があり、それには次のものが含まれます。

- Sun Microsystems JAVA System Directory Server（現在は Oracle Directory Server Enterprise Edition の一部、旧名 Sun ONE Directory Server）
- Microsoft Active Directory
- Novell
- OpenLDAP

デフォルトでは、ASA によって Microsoft Active Directory、Sun LDAP、Novell、OpenLDAP、または汎用 LDAPv3 ディレクトリ サーバに接続しているかどうかが自動検出されます。ただし、LDAP サーバ タイプの自動検出による決定が失敗した場合は、手動で設定できます。

LDAP での認証方法

認証中、ASA は、ユーザの LDAP サーバへのクライアント プロキシとして機能し、プレーン テキストまたは Simple Authentication and Security Layer（SASL）プロトコルのいずれかを使って LDAP サーバに対する認証を行います。デフォルトで、ASA は、通常はユーザ名とパスワードである認証パラメータを LDAP サーバにプレーン テキストで渡します。

ASA では、次の SASL メカニズムをサポートしています。次に、強度の低い順番に示します。

- Digest-MD5：ASA は、ユーザ名とパスワードから計算した MD5 値を使用して LDAP サーバに応答します。
- Kerberos：ASA は、GSSAPI Kerberos メカニズムを使用して、ユーザ名とレルムを送信することで LDAP サーバに応答します。

ASA と LDAP サーバは、これらの SASL メカニズムの任意の組み合わせをサポートします。複数のメカニズムを設定した場合、ASA ではサーバに設定されている SASL メカニズムのリストが取得され、認証メカニズムは ASA とサーバの両方に設定されているメカニズムのなかで最も強力なものに設定されます。たとえば、LDAP サーバと ASA の両方がこれら両方のメカニズムをサポートしている場合、ASA は、強力な方の Kerberos メカニズムを選択します。

ユーザ LDAP 認証が成功すると、LDAP サーバは認証されたユーザの属性を返します。VPN 認証の場合、通常これらの属性には、VPN セッションに適用される認可データが含まれます。この場合、LDAP の使用により、認証と許可を 1 ステップで実行できます。

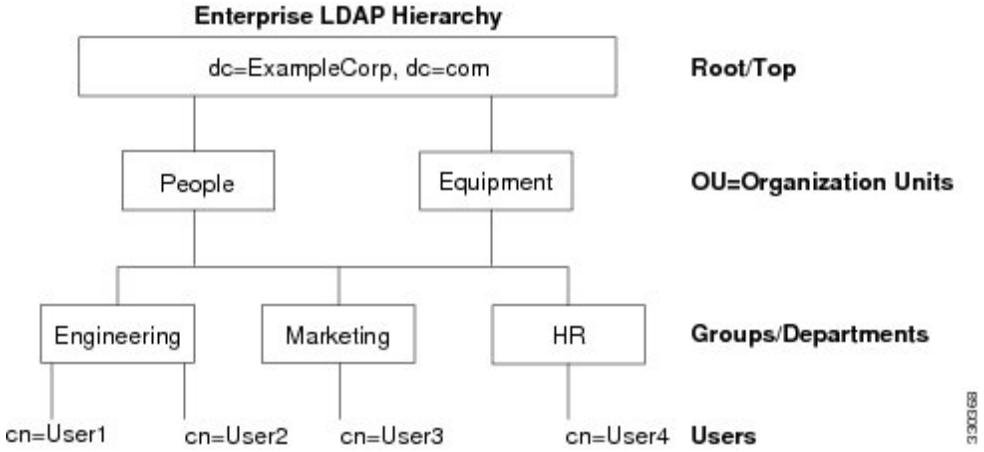
（注） LDAP プロトコルの詳細については、RFC 1777、2251、および 2849 を参照してください。

LDAP 階層

LDAP コンフィギュレーションは、組織の論理階層が反映されたものにする必要があります。たとえば、Example Corporation という企業の従業員 Employee1 を例に考えてみます。Employee1 は Engineering グループに従事しています。この企業の LDAP 階層は 1 つ以上のレベルを持つことができます。たとえば、シングルレベル階層をセットアップします。この中で、Employee1 は Example Corporation のメンバーであると見なされます。あるいは、マルチレベル階層をセットアップします。この中で、Employee1 は Engineering 部門のメンバーであると見なされ、この部門は People という名称の組織ユニットのメンバーであり、この組織ユニットは Example Corporation のメンバーです。マルチレベル階層の例については、次の図を参照してください。

マルチレベル階層の方が詳細ですが、検索結果が速く返されるのはシングルレベル階層の方です。

図 *1* : マルチレベルの *LDAP* 階層



LDAP 階層の検索

ASA は、LDAP 階層内での検索を調整できます。ASA に次の 3 種類のフィールドを設定すると、LDAP 階層での検索開始場所とその範囲、および検索する情報のタイプを定義できます。これらのフィールドは、ユーザの権限が含まれている部分だけを検索するように階層の検索を限定します。

- LDAP Base DN では、サーバが ASA から認可要求を受信したときに LDAP 階層内のどの場所からユーザ情報の検索を開始するかを定義します。
- Search Scope では、LDAP 階層の検索範囲を定義します。この指定では、LDAP Base DN よりもかなり下位のレベルまで検索します。サーバによる検索を直下の 1 レベルだけにするか、サブツリー全体を検索するかを選択できます。シングルレベルの検索の方が高速ですが、サブツリー検索の方が広範囲に検索できます。
- Naming Attribute では、LDAP サーバのエントリを一意に識別する RDN を定義します。一般的な名前属性には、cn（一般名）、sAMAccountName、および userPrincipalName を含めることができます。

次の図に、Example Corporation の LDAP 階層の例を示します。この階層が指定されると、複数の方法で検索を定義できます。次の表に、2つの検索コンフィギュレーションの例を示します。

最初のコンフィギュレーションの例では、Employee1 が IPSec トンネルを確立するときに LDAP 認可が必要であるため、ASA から LDAP サーバに検索要求が送信され、この中で Employee1 を Engineering グループの中で検索することが指定されます。この検索は短時間でできます。

2 番目のコンフィギュレーションの例では、ASA から送信される検索要求の中で、Employee1 を Example Corporation 全体の中で検索することが指定されています。この検索には時間がかかります。

表 *1*: 検索コンフィギュレーションの例

番号	LDAP Base DN	検索範囲	名前属性	結果
1	group=Engineering,ou=People,dc=ExampleCorporation,dc=com	1 レベル	cn=Employee1	検索が高速
2	dc=ExampleCorporation,dc=com	サブツリー	cn=Employee1	検索に時間がかかる

LDAP サーバへのバインド

ASA は、ログイン DN とログイン パスワードを使用して、LDAP サーバとの信頼（バインド）を築きます。Microsoft Active Directory の読み取り専用操作（認証、許可、グループ検索など）を行うとき、ASA では特権の低いログイン DN でバインドできます。たとえば、Login DN には、AD の「Member Of」の指定が Domain Users の一部であるユーザを指定することができます。VPN のパスワード管理操作では、Login DN にはより高い特権が必要となり、AD の Account Operators グループの一部を指定する必要があります。

次に、Login DN の例を示します。

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

ASA は次の認証方式をサポートしています。

- 暗号化されていないパスワードを使用したポート 389 での簡易 LDAP 認証
- ポート 636 でのセキュアな LDAP（LDAP-S）
- Simple Authentication and Security Layer（SASL）MD5
- SASL Kerberos

ASA は匿名認証をサポートしていません。

（注） LDAP クライアントとしての ASA は、匿名のバインドや要求の送信をサポートしていません。

LDAP 属性マップ

ASA では、次の目的での認証のために LDAP ディレクトリを使用できます。

- VPN リモート アクセス ユーザ
- ファイアウォール ネットワークのアクセス/カットスルー プロキシ セッション
- ACL、ブックマーク リスト、DNS または WINS 設定、セッション タイマーなどのポリシーの権限（または許可属性と呼ばれる）の設定

- ローカル グループ ポリシーのキー属性の設定

ASA は、LDAP 属性マップを使用して、ネイティブ LDAP ユーザ属性を Cisco ASA 属性に変換します。それらの属性マップを LDAP サーバにバインドしたり、削除したりすることができます。また、属性マップを表示または消去することもできます。

LDAP 属性マップは複数値属性をサポートしません。たとえば、あるユーザが複数の AD グループのメンバで、LDAP 属性マップが複数のグループと一致する場合、選択される値は一致するエントリのアルファベット順に基づくものです。

属性マッピング機能を適切に使用するには、LDAP 属性の名前と値およびユーザ定義の属性の名前と値を理解する必要があります。

頻繁にマッピングされる LDAP 属性の名前と、一般にマッピングされるユーザ定義の属性のタイプは次のとおりです。

- IETF-Radius-Class（ASA バージョン 8.2 以降における Group_Policy）：ディレクトリ部門またはユーザ グループ（たとえば、Microsoft Active Directory memberOf）属性値に基づいてグループ ポリシーを設定します。ASDM バージョン 6.2/ASA バージョン 8.2 以降では、IETF-Radius-Class 属性の代わりに group-policy 属性が使用されます。
- IETF-Radius-Filter-Id：VPN クライアント、IPSec、SSL に対するアクセス コントロール リスト（ACL）に適用されます。
- IETF-Radius-Framed-IP-Address：VPN リモート アクセス クライアント、IPSec、および SSL にスタティック IP アドレスを割り当てます。
- Banner1：VPN リモート アクセス ユーザのログイン時にテキスト バナーを表示します。
- Tunneling-Protocols：アクセス タイプに基づいて、VPN リモート アクセス セッションを許可または拒否します。

（注） 1 つの LDAP 属性マップに、1 つ以上の属性を含めることができます。特定の LADP サーバからは、1 つの LDAP 属性のみをマップすることができます。

AAA の LDAP サーバのガイドライン

この項では、AAA の LDAP サーバを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

IPv6

AAA サーバは IPv4 アドレスを使用する必要がありますが、エンドポイントは IPv6 を使用できます。

その他のガイドライン

- Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN が、サーバのデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACL を設定できます。
- Microsoft Active Directory および Sun サーバでのパスワード管理をイネーブルにするために LDAP over SSL を設定する必要があります。
- ASA は、Novell、OpenLDAP およびその他の LDAPv3 ディレクトリ サーバによるパスワード管理をサポートしません。
- バージョン 7.1（x）以降、ASA はネイティブ LDAP スキーマを使用して認証および認可を行うため、Cisco スキーマは必要なくなりました。
- シングルモードの場合は最大 100 台の LDAP サーバ グループを使用でき、マルチモードの場合は各コンテキストで最大 4 台の LDAP サーバ グループを使用できます。
- 各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台の LDAP サーバを含めることができます。
- ユーザがログインすると、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまで LDAP サーバが 1 つずつアクセスされます。グループ内のすべてのサーバが使用できない場合、ASA は、ローカル データベースがフォールバック方式として設定されていると、ローカル データベースに接続しようとします（管理認証および認可限定）。フォールバック メソッドとして設定されていない場合、ASA は LDAP サーバに引き続きアクセスしようとします。

AAA の LDAP サーバの設定

この項では、AAA に LDAP サーバを設定する方法について説明します。

手順

ステップ 1 LDAP 属性マップを設定します。LDAP 属性マップの設定 （6 ページ）を参照してください。

ステップ 2 LDAP サーバ グループを追加します。LDAP サーバ グループの設定 （8 ページ）を参照してください。

ステップ 3 （オプション）認証メカニズムとは別の異なる、LDAP サーバからの許可を設定します。「VPN の LDAP 認証の設定 （11 ページ）」を参照してください。

LDAP 属性マップの設定

LDAP 属性マップを設定するには、次の手順を実行します。

手順

ステップ 1 空の LDAP 属性マップ テーブルを作成します。

ldap-attribute-map *map-name*

例：

```
ciscoasa(config)# ldap-attribute-map att_map_1
```

ステップ 2 ユーザ定義の属性名 department を、シスコの属性にマッピングします。

map-name *user-attribute-name Cisco-attribute-name*

例：

```
ciscoasa(config-ldap-attribute-map)# map-name department IETF-Radius-Class
```

ステップ 3 ユーザ定義のマップ値である department をユーザ定義の属性値とシスコの属性値にマッピングします。

map-value *user-attribute-name Cisco-attribute-name*

例：

```
ciscoasa(config-ldap-attribute-map)# map-value department Engineering group1
```

ステップ 4 サーバと、そのサーバが属する AAA サーバ グループを識別します。

aaa-server *server_group* [*interface_name*] **host** *server_ip*

例：

```
ciscoasa(config)# aaa-server ldap_dir_1 host 10.1.1.4
```

ステップ 5 属性マップを LDAP サーバにバインドします。

ldap-attribute-map *map-name*

例：

```
ciscoasa(config-aaa-server-host)# ldap-attribute-map att_map_1
```

例

次の例は、accessType という名前のLDAP 属性に基づいて管理セッションを ASA に制限する方法を示しています。accessType 属性には、以下の値のいずれかが含まれる可能性があります。

- [VPN]
- admin
- helpdesk

次の例では、各値が、ASA でサポートされる有効な IETF-Radius-Service-Type 属性のいずれかにマッピングされる方法を示します。有効なタイプには、remote-access（Service-Type 5）発信、admin（Service-Type 6）管理、および nas-prompt（Service-Type 7）NAS プロンプトがあります。

```
ciscoasa(config)# ldap attribute-map MGMT
ciscoasa(config-ldap-attribute-map)# map-name accessType IETF-Radius-Service-Type
ciscoasa(config-ldap-attribute-map)# map-value accessType VPN 5
ciscoasa(config-ldap-attribute-map)# map-value accessType admin 6
ciscoasa(config-ldap-attribute-map)# map-value accessType helpdesk 7

ciscoasa(config-ldap-attribute-map)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 10.1.254.91
ciscoasa(config-aaa-server-host)# ldap-base-dn CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-password test
ciscoasa(config-aaa-server-host)# ldap-login-dn CN=Administrator,CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# server-type auto-detect
ciscoasa(config-aaa-server-host)# ldap-attribute-map MGMT
```

次の例では、シスコの LDAP 属性名の全リストを表示します。

```
ciscoasa(config)# ldap attribute-map att_map_1
ciscoasa(config-ldap-attribute-map)# map-name att_map_1?

ldap mode commands/options:
cisco-attribute-names:
  Access-Hours
  Allow-Network-Extension-Mode
  Auth-Service-Type
  Authenticated-User-Idle-Timeout
  Authorization-Required
  Authorization-Type
 :
 :
  X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

LDAP サーバ グループの設定

LDAP サーバ グループを作成して設定し、LDAP サーバをそのグループに追加するには、次の手順を実行します。

始める前に

LDAP サーバを LDAP サーバ グループに追加する前に、属性マップを追加する必要があります。

手順

ステップ 1 サーバ グループ名とプロトコルを指定します。

aaa-server *server_tag* **protocol ldap**

例：

```
ciscoasa(config)# aaa-server servergroup1 protocol ldap
ciscoasa(config-aaa-server-group)#
```

aaa-server protocol コマンドを入力する場合は、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 次のサーバを試す前にグループ内の LDAP サーバでの AAA トランザクションの失敗の最大数を指定します。

max-failed-attempts *number*

例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 引数の範囲は 1 ～ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式を設定し（管理アクセスだけの場合）、グループ内のすべてのサーバが応答できなかった場合、グループは非応答と見なされ、フォールバック方式が試行されます。サーバ グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、ASA は引き続きグループ内のサーバにアクセスしようとします。

ステップ 3 グループ内で障害の発生したサーバを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

depletion キーワードを指定すると、グループ内のすべてのサーバが非アクティブになった後に、障害の発生したサーバが再度アクティブ化されます。

deadtime *minutes* キーワード引数のペアには、グループ内の最後のサーバをディセーブルにしてから、次にすべてのサーバを再度イネーブルにするまでの経過時間を分単位で 0 ～ 1440 から指定します。デフォルトは 10 分です。

timed キーワードは、30 秒間のダウンタイムの後に障害が発生したサーバを再度アクティブ化します。

ステップ 4 LDAP サーバと、そのサーバが属する AAA サーバ グループを識別します。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

例：

```
ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1
```

(*interface_name***)** を指定していない場合、ASA はデフォルトで**内部**インターフェイスを使用します。

aaa-server host コマンドを入力すると、aaa-server ホスト コンフィギュレーション モードが開始します。必要に応じて、ホスト コンフィギュレーション モード コマンドを使用して、さらに AAA サーバを設定します。

LDAP サーバで使用できるコマンドと、新しい LDAP サーバ定義にそのコマンドのデフォルト値があるかどうかを、次の表に示します。デフォルト値が指定されていない場合（「—」で表示）、コマンドを使用して値を指定します。

表 *2:* ホスト モード コマンドとデフォルト値

コマンド	デフォルト値	説明
ldap-attribute-map	—	—
ldap-base-dn	—	—
ldap-login-dn	—	—
ldap-login-password	—	—
ldap-naming-attribute	—	—
ldap-over-ssl	636	設定されていない場合は、ASA では LDAP 要求に sAMAccountName を使用します。SASL とプレーン テキストのどちらを使用する場合でも、ASA と LDAP サーバの間での通信のセキュリティは SSL で確保されます。SASL を設定しない場合、SSL で LDAP 通信を保護することを強くお勧めします。
ldap-scope	—	—
sasl-mechanism	—	—
server-port	389	—

コマンド	デフォルト値	説明
server-type	自動検出	自動検出により LDAP サーバのタイプが特定できなくても、そのサーバが、Microsoft Active Directory、Sun LDAP ディレクトリ サーバ、それ以外の LDAP サーバのいずれであるかがわかっている場合は、そのサーバタイプを手動で設定できます。
timeout	10 秒	—

例

次の例では、watchdogs という名前の LDAP サーバ グループを設定し、そのグループに LDAP サーバを追加する方法を示します。この例では、この例ではリトライ インターバルや LDAP サーバがリスンするポートを定義しないため、ASA はこの 2 つのサーバ固有パラメータにデフォルト値を使用します。

```
ciscoasa(config)# aaa-server watchdogs protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

VPN の LDAP 認証の設定

VPN アクセスのための LDAP ユーザ認証が成功すると、ASA は、LDAP 属性を返す LDAP サーバのクエリーを実行します。通常これらの属性には、VPN セッションに適用される認可データが含まれます。このように LDAP を使用すると、1 つのステップで認証および認可を完了できます。

ただし、場合によっては、認可メカニズムとは別の異なる認可を LDAP ディレクトリ サーバから取得する必要があります。たとえば、認証に SDI または証明書サーバを使用している場合、認可情報は返されません。この場合、ユーザ認可では、認証の成功後に LDAP ディレクトリのクエリーを実行するため、認証と認可は 2 つのステップで行われます。

LDAP を使用した VPN ユーザ許可を設定するには、次の手順を実行します。

手順

ステップ 1 remotegrp という名前の IPsec リモート アクセス トンネル グループを作成します。

tunnel-group *groupname*

例：

```
ciscoasa(config)# tunnel-group remotegrp
```

ステップ 2 サーバ グループとトンネル グループを関連付けます。

tunnel-group *groupname* **general-attributes**

例：

```
ciscoasa(config)# tunnel-group remotegrp general-attributes
```

ステップ 3 以前作成した認証のための AAA サーバ グループに新しいトンネル グループを割り当てます。

authorization-server-group *group-tag*

例：

```
ciscoasa(config-general)# authorization-server-group ldap_dir_1
```

例

特定の要件で使用できる許可関連のコマンドとオプションは他にもありますが、次の例では、LDAP でのユーザ許可をイネーブルにするコマンドを示します。この例では、remote-1 という名前の IPsec リモート アクセス トンネル グループを作成し、すでに作成してある許可用の ldap_dir_1 AAA サーバ グループにその新しいトンネル グループを割り当てています。

```
ciscoasa(config)# tunnel-group remote-1 type ipsec-ra
ciscoasa(config)# tunnel-group remote-1 general-attributes
ciscoasa(config-general)# authorization-server-group ldap_dir_1
ciscoasa(config-general)#
```

この設定が完了したら、次のコマンドを入力して、ディレクトリ パスワード、ディレクトリ検索の開始点、ディレクトリ検索の範囲など、追加の LDAP 許可パラメータを設定できます。

```
ciscoasa(config)# aaa-server ldap_dir_1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
ciscoasa(config-aaa-server-host)# ldap-login-dn obscurepassword
ciscoasa(config-aaa-server-host)# ldap-base-dn starthere
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)#
```

AAA の LDAP サーバのモニタリング

AAA の LDAP サーバのモニタリングについては、次のコマンドを参照してください。

- **show aaa-server**

  このコマンドは、設定されたAAAサーバの統計情報を表示します。AAAサーバコンフィギュレーションをクリアするには、**clear aaa-server statistics** コマンドを入力します。

- **show running-config aaa-server**

  このコマンドは、AAA サーバの実行コンフィギュレーションを表示します。AAA サーバの統計情報をクリアするには、**clear configure aaa-server** コマンドを使用します。

AAA の LDAP サーバの履歴

表 *3 : AAA* サーバの履歴

機能名	プラットフォーム リリース	説明
AAA の LDAP サーバ	7.0(1)	LDAP サーバの AAA のサポートと LDAP サーバの設定方法について説明します。 次のコマンドを導入しました。 **username**、**aaa authorization exec authentication-server**、**aaa authentication console LOCAL**、**aaa authorization exec LOCAL**、**service-type**、**ldap attribute-map**、**aaa-server protocol**、**aaa authentication telnet | ssh | serial} console LOCAL**、**aaa authentication http console LOCAL**、**aaa authentication enable console LOCAL**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**authorization-server-group**、**tunnel-group**、**tunnel-group general-attributes**、**map-name**、**map-value**、**ldap-attribute-map**。