CHAPTER 38

# AAA サーバとローカル データベースの設定

この章では、認証、許可、アカウンティング（AAA 、「トリプル エー」と発音）のサポート、および AAA サーバとローカル データベースの設定方法について説明します。

この章は、次の項目を取り上げます。



## AAA について

AAA によって、ASA が、ユーザが誰か（認証）、ユーザが何を実行できるか（許可）、およびユーザが何を実行したか（アカウンティング）を判別することが可能になります。

AAA には、ユーザ アクセスに対して、アクセス リストだけを使用する場合よりもレベルの高い保護および制御機能が用意されています。たとえば、すべての外部ユーザが DMZ ネットワークのサーバ上の Telnet にアクセスできるようにするアクセス リストを作成できます。一部のユーザだけがサーバにアクセスできるようにする際に、そのユーザの IP アドレスを常に認識しているとは限らない場合、AAA を使用すると、認証済みまたは許可済みのユーザだけに ASA を介した接続を許可することができます（Telnet サーバもまた、認証を実行します。ASA は、許可されないユーザがサーバにアクセスできないようにします）。

認証だけで使用することも、許可およびアカウンティングとともに使用することもできます。許可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングだけで使用することも、認証および許可とともに使用することもできます。

この項では、次のトピックについて取り上げます。

# 認証について

認証では、有効なユーザ クレデンシャルを要求してアクセスを制御します。このクレデンシャルは通常、ユーザ名とパスワードです。次の項目を認証するように、ASA を設定できます。

- ASA へのすべての管理接続（この接続には、次のセッションが含まれます）
  - Telnet
  - SSH
  - シリアル コンソール
  - ASDM（HTTPS を使用）
  - VPN 管理アクセス
- **enable** コマンド
- ネットワーク アクセス
- VPN アクセス

# 許可について

ユーザの認証後、許可によって*ユーザごと*にアクセスが制御されます。次の項目を許可するように、ASA を設定できます。

- 管理コマンド
- ネットワーク アクセス
- VPN アクセス

許可によって、各認証済みユーザが使用できるサービスおよびコマンドが制御されます。許可をイネーブルにしていない場合は、認証だけで、すべての認証済みユーザがサービスに同じようにアクセスできます。

許可で提供される制御を必要とする場合は、広範な認証ルールを設定してから、詳細な許可を設定できます。たとえば、外部ネットワーク上のサーバにアクセスする内部ユーザを認証して、特定のユーザがアクセスできる外部サーバを許可によって制限できます。

ASA はユーザあたり最初の 16 件の許可要求をキャッシュするため、ユーザが現在の認証セッション中に同じサービスにアクセスした場合、ASA は許可サーバに要求を再送信しません。

# アカウンティングについて

アカウンティングは、ASA を通過するトラフィックを追跡して、ユーザ アクティビティを記録できるようにします。トラフィックの認証をイネーブルにすると、ユーザごとにトラフィックをアカウンティングできます。トラフィックを認証しない場合は、IP アドレスごとにトラフィックをアカウンティングできます。ASA アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、そのセッションでを経由したバイト数、使用されたサービス、各セッションの継続時間が含まれます。

# サーバ サポートの要約

表 38-1 に、各 AAA サービスのサポート状況の要約を AAA サーバ タイプ（ローカル データベースを含む）別に示します。特定の AAA サーバ タイプのサポートの詳細については、表に続く項目を参照してください。

**表 38-1　AAA サポートの要約**

| | データベース タイプ | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **AAA サービス** | **ローカル** | **RADIUS** | **TACACS+** | **SDI（RSA）** | **NT** | **Kerberos** | **LDAP** | **HTTP Form** |
| **認証** | | | | | | | | |
| VPN ユーザ[1] | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes[2] |
| ファイアウォール セッション | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| 管理者 | Yes | Yes | Yes | Yes[3] | Yes | Yes | Yes | No |
| **許可** | | | | | | | | |
| VPN ユーザ | Yes | Yes | No | No | No | No | Yes | No |
| ファイアウォール セッション | No | Yes[4] | Yes | No | No | No | No | No |
| 管理者 | Yes[5] | No | Yes | No | No | No | No | No |
| **アカウンティング** | | | | | | | | |
| VPN 接続 | No | Yes | Yes | No | No | No | No | No |
| ファイアウォール セッション | No | Yes | Yes | No | No | No | No | No |
| 管理者 | No | Yes[6] | Yes | No | No | No | No | No |

1. SSL VPN 接続では、PAP または MS-CHAPv2 のいずれかを使用できます。
2. HTTP Form プロトコルでは、クライアントレス SSL VPN ユーザ セッションの場合に限り、認証と SSO 操作の両方がサポートされます。
3. RSA/SDI は、ASA 5500 ソフトウェア バージョン 8.2(1) 以降を使用した ASDM HTTP 管理アクセス用にサポートされています。
4. ファイアウォール セッションの場合、RADIUS 許可はユーザ固有のアクセス リストでだけサポートされます。このアクセス リストは RADIUS 認証応答で受信または指定されます。
5. ローカル コマンド許可は、特権レベルに限りサポートされます。
6. コマンド アカウンティングは、TACACS+ でのみ使用できます。

（注）　表 38-1 に記載されているネイティブ プロトコル認証のほか、ASA ではプロキシ認証がサポートされています。たとえば、ASA は RADIUS サーバ経由で RSA/SDI または LDAP サーバ、あるいはその両方へのプロキシとして動作することができます。デジタル証明書、またはデジタル証明書と表内の AAA の組み合わせ、あるいはその両方による認証もサポートされます。

# RADIUS サーバのサポート

ASA は AAA について、次の RFC 準拠 RADIUS サーバをサポートしています。

- Cisco Secure ACS 3.2、4.0、4.1、4.2、および 5.x
- Cisco Identity Services Engine（ISE）
- RSA 認証マネージャ 5.2、6.1 および 7.x の RSA Radius
- Microsoft

## 認証方法

ASA は、RADIUS で次の認証方法をサポートします。

- PAP：すべての接続タイプの場合。
- CHAP および MS-CHAPv1：L2TP-over-IPsec 接続の場合。
- MS-CHAPv2：L2TP-over-IPsec 接続の場合。また、パスワード管理機能がイネーブルで、通常の IPsec リモート アクセス接続の場合。MS-CHAPv2 は、クライアントレス接続でも使用できます。
- 認証プロキシ モード：RADIUS から Active Directory、RADIUS から RSA/SDI、RADIUS からトークンサーバ、および RSA/SDI から RADIUS 接続。

（注）　MS-CHAPv2 を、ASA と RADIUS サーバの間の VPN 接続で使用されるプロトコルとしてイネーブルにするには、トンネル グループ一般属性でパスワード管理をイネーブルにする必要があります。パスワード管理をイネーブルにすると、ASA から RADIUS サーバへの MS-CHAPv2 認証要求が生成されます。詳細については、**password-management** コマンドの説明を参照してください。

二重認証を使用し、トンネル グループでパスワード管理をイネーブルにした場合は、プライマリ認証要求とセカンダリ認証要求に MS-CHAPv2 要求属性が含まれます。RADIUS サーバが MS-CHAPv2 をサポートしない場合は、**no mschapv2-capable** コマンドを使用して、そのサーバが MS-CHAPv2 以外の認証要求を送信するように設定できます。

## 属性のサポート

ASA は、次の RADIUS 属性のセットをサポートします。

- RFC 2138 に定義されている認証属性
- RFC 2139 に定義されているアカウンティング属性
- RFC 2868 に定義されているトンネル プロトコル サポート用の RADIUS 属性
- Cisco IOS ベンダー固有属性（VSA）は、RADIUS ベンダー ID 9 で識別されます。
- RADIUS ベンダー ID 3076 によって識別される Cisco VPN 関連 VSA
- RFC 2548 に定義されている Microsoft VSA

- Cisco VSA（Cisco-Priv-Level）。特権の標準ランキングである 0 ～ 15 の数値を指定します。1 が最低レベルを示し、15 が最高レベルを示します。0 レベルは特権がないことを示します。第 1 レベル（login）では、このレベルで使用可能なコマンドに対する特権 EXEC アクセスが許可されます。第 2 レベル（enable）では CLI コンフィギュレーション特権が許可されます。
- 属性の一覧については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/ref_extserver.html#wp1605508

### RADIUS 許可機能

ASA では RADIUS サーバを使用して、ダイナミック アクセス リストまたはユーザごとのアクセス リスト名を使用する VPN リモート アクセスおよびファイアウォール カットスルー プロキシ セッションのユーザ許可を実行できます。ダイナミック アクセス リストを実装するには、これをサポートするように RADIUS サーバを設定する必要があります。ユーザを認証する場合、RADIUS サーバによってダウンロード可能なアクセス リスト、またはアクセス リスト名が ASA に送信されます。所定のサービスへのアクセスがアクセス リストによって許可または拒否されます。認証セッションの有効期限が切れると、ASA によってアクセス リストが削除されます。

アクセス リストに加え、ASA では、その他多数の許可属性、VPN リモート アクセスおよびファイアウォール カットスルー プロキシ セッションに対する許可の設定をサポートします。許可属性すべての一覧については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/ref_extserver.html#wp16055508

## TACACS+ サーバのサポート

ASA は、ASCII、PAP、CHAP、および MS-CHAPv1 で TACACS+ 認証をサポートします。

## RSA/SDI サーバのサポート

RSA SecureID サーバは、SDI サーバとも呼ばれます。

この項では、次のトピックについて取り上げます。

- 「RSA/SDI バージョンのサポート」（P.38-5）
- 「2 ステップ認証プロセス」（P.38-6）
- 「RSA/SDI プライマリ サーバおよびレプリカ サーバ」（P.38-6）

### RSA/SDI バージョンのサポート

ASA は、SDI バージョン 5.x、6.x、および 7.x をサポートします。SDI は、SDI プライマリ サーバおよび SDI レプリカ サーバの概念を使用します。各プライマリおよびそのレプリカは、シングル ノード秘密ファイルを共有します。そのノード シークレット ファイルの名前は、.sdi が付加された ACE またはサーバ IP アドレスの 16 進数値に基づきます。

ASA に設定するバージョン 5.x、6.x、または 7.x SDI サーバは、プライマリでも、レプリカのいずれか 1 つでもかまいません。ユーザ認証のための SDI エージェントによるサーバの選択方法の詳細については、「RSA/SDI プライマリ サーバおよびレプリカ サーバ」（P.38-6）を参照してください。

### 2 ステップ認証プロセス

SDI バージョン 5.x、6.x、または 7.x は 2 ステップのプロセスを使用して、侵入者が RSA SecurID 認証要求から情報を取り込み、それを使用して別のサーバに認証を証明しないように防止します。エージェントはまず、SecurID サーバにロック要求を送信してから、ユーザ認証要求を送信します。サーバはユーザ名をロックして、別の（レプリカ）サーバがユーザ名を受信できないようにします。このアクションは、同じユーザが、同じ認証サーバを同時に使用して、2 つの ASA に認証を証明することができないことを意味します。ユーザ名のロックに成功すると、ASA はパスコードを送信します。

### RSA/SDI プライマリ サーバおよびレプリカ サーバ

ASA は、最初のユーザが設定済みサーバ（プライマリでもレプリカでもかまいません）に認証を証明するときに、サーバ リストを取得します。次に、ASA はリスト上の各サーバにプライオリティを割り当て、その後のサーバ選択では、この割り当てられたプライオリティのサーバから無作為に抽出します。最もプライオリティの高いサーバが選択される可能性が高くなります。

## NT サーバのサポート

ASA では、NTLM バージョン 1 をサポートしている Microsoft Windows Server オペレーティング システム（ひとまとめにして「NT サーバ」と呼びます）がサポートされています。

（注）　NT サーバでは、ユーザ パスワードの最大長は 14 文字です。それより長いパスワードは、NTLM バージョン 1 の制限により切り捨てられます。

## Kerberos サーバのサポート

ASA は、3DES、DES、および RC4 暗号タイプをサポートしています。

（注）　ASA は、トンネル ネゴシエーション中のユーザ パスワードの変更はサポートしていません。この状況が意図せずに発生することを回避するために、ASA に接続するユーザの Kerberos/Active Directory サーバでのパスワード期限切れをディセーブルにします。

単純な Kerberos サーバ コンフィギュレーションの例については、例 38-2（P.38-16）を参照してください。

## LDAP サーバのサポート

ASA では LDAP をサポートしています。この項では、次のトピックについて取り上げます。

- 「LDAP による認証」（P.38-7）
- 「LDAP サーバのタイプ」（P.38-7）

## LDAP による認証

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。

これらの SASL メカニズムの任意の組み合わせをサポートするように、ASA と LDAP サーバを設定できます。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、より強力な方の 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許可データが含まれます。したがって、LDAP を使用すると、認証と許可が 1 つのステップで行われます。

## LDAP サーバのタイプ

ASA では LDAP バージョン 3 がサポートされており、Sun Microsystems JAVA System Directory Server（従来の Sun ONE Directory Server）、Microsoft Active Directory、Novell、OpenLDAP、およびその他の LDAPv3 ディレクトリ サーバとの互換性があります。

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、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。

サーバ タイプを設定する際には、次のガイドラインに注意してください。

- Sun ディレクトリ サーバにアクセスするように ASA で設定されている Distinguished Name（DN; 認定者名）は、その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 では、Novell、OpenLDAP、およびその他の LDAPv3 ディレクトリ サーバを使用したパスワード管理はサポートされません。
- ASA では、ログイン識別名（DN）とログイン パスワードを使用して、LDAP サーバとの信頼関係（バインド）が確立されます。詳細については、「ASA と LDAP サーバのバインディング」（P.C-4）を参照してください。

# クライアントレス SSL VPN に対する HTTP Form 認証

ASA では、クライアントレス SSL VPN ユーザ セッションの認証と SSO 操作だけに HTTP Form プロトコルを使用できます。設定については、「クライアントレス SSL VPN でのシングル サインオンの使用」（P.78-17）を参照してください。

# ローカル データベース サポート（フォールバック方式としての機能を含む）

ASA は、ユーザ プロファイルを取り込むことができるローカル データベースを管理します。

ローカル データベースは、複数の機能のフォールバック方式として動作できます。この動作は、ASA から誤ってロックアウトされないようにすることを意図しています。

フォールバック サポートを必要とするユーザについては、ローカル データベース内のユーザ名およびパスワードと、AAA サーバ上のユーザ名およびパスワードとを一致させることを推奨します。これにより、透過フォールバックがサポートされます。ユーザは、AAA サーバとローカル データベースのどちらがサービスを提供しているかが判別できないので、ローカル データベースのユーザ名およびパスワードとは異なるユーザ名およびパスワードを AAA サーバで使用することは、指定するべきユーザ名とパスワードをユーザが確信できないことを意味します。

ローカル データベースでサポートされているフォールバック機能は次のとおりです。

- コンソールおよびイネーブル パスワード認証：グループ内のサーバがすべて使用できない場合、ASA ではローカル データベースを使用して管理アクセスを認証します。これには、イネーブル パスワード認証が含まれる場合があります。
- コマンド許可：グループ内の TACACS+ サーバがすべて使用できない場合、特権レベルに基づいてコマンドを許可するためにローカル データベースが使用されます。
- VPN 認証および許可：VPN 認証および許可は、通常この VPN サービスをサポートしている AAA サーバが使用できない場合、ASA へのリモート アクセスをイネーブルにするためにサポートされます。管理者である VPN クライアントが、ローカル データベースへのフォールバックを設定されたトンネル グループを指定する場合、AAA サーバ グループが使用できない場合でも、ローカル データベースが必要な属性で設定されていれば、VPN トンネルが確立できます。

# グループ内の複数のサーバを使用したフォールバックの仕組み

サーバ グループ内に複数のサーバを設定し、サーバ グループのローカル データベースへのフォールバックをイネーブルにしている場合、ASA からの認証要求に対してグループ内のどのサーバからも応答がないと、フォールバックが発生します。次のシナリオで例証します。

サーバ 1、サーバ 2 の順で、LDAP サーバ グループに 2 台の Active Directory サーバを設定します。リモート ユーザがログインすると、ASA によってサーバ 1 に対する認証が試みられます。

サーバ 1 から認証エラー（「*user not found*」など）が返されると、ASA によるサーバ 2 に対する認証は試みられません。

タイムアウト期間内にサーバ 1 から応答がないと（または認証回数が、設定されている最大数を超えている場合）、ASA によってサーバ 2 に対する認証が試みられます。

グループ内のどちらのサーバからも応答がなく、ASA にローカル データベースへのフォールバックが設定されている場合、ASA によってローカル データベースに対する認証が試みられます。

# 証明書とユーザ ログイン クレデンシャルの使用

この項では、認証と許可に証明書およびユーザ ログイン クレデンシャル（ユーザ名とパスワード）を使用する、さまざまな方法について説明します。これらの方式は、IPSec、AnyConnect、およびクライアントレス SSL VPN に適用されます。

すべての場合において、LDAP 許可では、パスワードをクレデンシャルとして使用しません。RADIUS 許可では、すべてのユーザの共通パスワードまたはユーザ名のいずれかを、パスワードとして使用します。

この項では、次のトピックについて取り上げます。



## ユーザ ログイン クレデンシャルの使用

認証および許可のデフォルトの方法では、ユーザ ログイン クレデンシャルを使用します。

- 認証
  - トンネル グループ（ASDM 接続プロファイルとも呼ばれます）の認証サーバ グループ設定によりイネーブルにされます。
  - ユーザ名とパスワードをクレデンシャルとして使用します。
- 許可
  - トンネル グループ（ASDM 接続プロファイルとも呼ばれます）の許可サーバ グループ設定によりイネーブルにされます。
  - ユーザ名をクレデンシャルとして使用します。

## 証明書の使用

ユーザ デジタル証明書が設定されている場合、ASA によって最初に証明書が検証されます。ただし、証明書の DN は認証用のユーザ名として使用されません。

認証と許可の両方がイネーブルになっている場合、ASA によって、ユーザの認証と許可の両方にユーザ ログイン クレデンシャルが使用されます。

- 認証
  - 認証サーバ グループ設定によってイネーブルにされます。
  - ユーザ名とパスワードをクレデンシャルとして使用します。
- 許可
  - 許可サーバ グループ設定によってイネーブルにされます。
  - ユーザ名をクレデンシャルとして使用します。

認証がディセーブルで許可がイネーブルになっている場合、ASA によって許可にプライマリ DN のフィールドが使用されます。

- 認証
  - 認証サーバ グループ設定によってディセーブル（[None] に設定）になります。
  - クレデンシャルは使用されません。
- 許可

- 許可サーバ グループ設定によってイネーブルにされます。
- 証明書のプライマリ DN フィールドのユーザ名の値をクレデンシャルとして使用します。

（注）　証明書にプライマリ DN のフィールドが存在しない場合、ASA では、セカンダリ DN のフィールド値が許可要求のユーザ名として使用されます。

次のサブジェクト DN フィールドと値が含まれるユーザ証明書を例に挙げます。

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

プライマリ DN = EA（電子メール アドレス）およびセカンダリ DN = CN（一般名）の場合、許可要求で使われるユーザ名は anyuser@example.com になります。

# AAA サーバのライセンス要件

| モデル | ライセンス要件 |
|---|---|
| すべてのモデル | 基本ライセンス |

# 注意事項と制限事項

この項では、この機能のガイドラインと制限事項について説明します。

### コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

### ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

### IPv6 のガイドライン

IPv6 をサポートします。

# AAA の設定

この項では、次のトピックについて取り上げます。

- 「AAA サーバ グループの設定」（P.38-11）
- 「VPN のための LDAP での許可の設定」（P.38-16）
- 「LDAP 属性マップの設定」（P.38-17）
- 「ユーザ アカウントのローカル データベースへの追加」（P.38-20）
- 「SSH 公開キーによるユーザの認証」（P.38-24）
- 「AAA によるユーザ ロールの区別」（P.38-24）

# AAA を設定するためのタスク フロー

**ステップ 1**　次のいずれかまたは両方を実行します。

- AAA サーバ グループを追加します。「AAA サーバ グループの設定」（P.38-11）を参照してください。
- ローカル データベースにユーザを追加します。「ユーザ アカウントのローカル データベースへの追加」（P.38-20）を参照してください。

**ステップ 2**　（任意）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 のための LDAP での許可の設定」（P.38-16）を参照してください。

**ステップ 3**　LDAP サーバの場合は、LDAP 属性マップを設定します。「LDAP 属性マップの設定」（P.38-17）を参照してください。

**ステップ 4**　（任意）認証時に管理ユーザとリモート アクセス ユーザを区別します。「AAA によるユーザ ロールの区別」（P.38-24）を参照してください。

# AAA サーバ グループの設定

認証、許可、またはアカウンティングに外部 AAA サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの AAA サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。AAA サーバ グループは名前で識別されます。各サーバ グループは、Kerberos、LDAP、NT、RADIUS、SDI、または TACACS+ というサーバの 1 つのタイプ専用となります。

## ガイドライン

- シングル モードで最大 100 個のサーバ グループ、またはマルチ モードでコンテキストごとに 4 つのサーバ グループを持つことができます。
- 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これらのサーバが 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（管理認証および許可限定）。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 AAA サーバにアクセスしようとします。

## 手順の詳細

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **aaa-server** *server_tag* **protocol** {**kerberos** \| **ldap** \| **nt** \| **radius** \| **sdi** \| **tacacs+**}<br><br>**例：**<br>`hostname(config)# aaa-server servergroup1 protocol ldap`<br>`hostname(config-aaa-server-group)#`<br><br>`hostname(config)# aaa-server servergroup1 protocol radius`<br>`hostname(config-aaa-server-group)# interim-accounting-update`<br><br>`hostname(config)# aaa-server servergroup1 protocol radius`<br>`hostname(config-aaa-server-group)# ad-agent-mode` | サーバ グループ名とプロトコルを識別します。たとえば、RADIUS を使用してネットワーク アクセスを認証し、TACACS+ を使用して CLI アクセスを認証するには、RADIUS サーバ用に 1 つ、TACACS+ サーバ用に 1 つというように、最低 2 つのサーバ グループを作成する必要があります。<br><br>シングル モードで最大 100 個のサーバ グループ、またはマルチ モードでコンテキストごとに 4 つのサーバ グループを持つことができます。各グループには、シングルモードで最大 15 台、マルチ モードで最大 4 台のサーバを含めることができます。<br><br>**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。<br><br>**interim-accounting-update** オプションは、クライアントレス SSL セッションおよび AnyConnect セッションに対して、マルチセッション アカウンティングをイネーブルします。このオプションを選択すると、開始レコードと終了レコード以外に中間アカウンティング レコードが RADIUS サーバに送信されます。<br><br>**ヒント** Clean Access SSO を使用して VPN 接続を完了できないという問題がユーザに発生している場合は、このオプションを選択します。この問題は ASA に対してクライアントレス接続または AnyConnect 接続を直接行う場合に発生する可能性があります。<br><br>**ad-agent-mode** オプションで、ASA と AD エージェント間の共有秘密を指定し、RADIUS サーバ グループがフル機能の RADIUS サーバではない AD エージェントを含めるよう指示します。ユーザ ID と関連付けることができるのは、**ad-agent-mode** オプションを使用して設定された RADIUS サーバ グループだけです。結果として、**ad-agent-mode** オプションを使用して設定されていない RADIUS サーバ グループを指定すると **test aaa-server** {**authentication** \| **authorization**} *aaa-server-group* コマンドが使用できなくなります。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 2 | **merge-dacl** {**before-avpair** \| **after-avpair**}<br><br>**例：**<br>hostname(config)# aaa-server servergroup1 protocol radius<br>hostname(config-aaa-server-group)# merge-dacl before-avpair | ダウンロード可能 ACL と、RADIUS パケットから Cisco AV ペアで受信した ACL を結合します。デフォルト設定は **no merge dacl** で、ダウンロード可能な ACL は Cisco AV ペア ACL と結合されません。AV ペアおよびダウンロード可能な ACL の両方を受信した場合は、AV ペアが優先し、使用されます。<br><br>**before-avpair** オプションは、ダウンロード可能な ACL エントリが Cisco-AV-Pair エントリの前に配置されるように指定します。<br><br>**after-avpair** オプションは、ダウンロード可能な ACL エントリが Cisco-AV-Pair エントリの後に配置されるように指定します。このオプションは、VPN 接続にのみ適用されます。VPN ユーザの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および ASA で設定される ACL の形式になります。このオプションでは、ダウンロード可能 ACL と AV ペア ACL が結合されているどうかを判断します。ASA で設定される ACL には適用されません。 |
| ステップ 3 | **max-failed-attempts** *number*<br><br>**例：**<br>hostname(config-aaa-server-group)# max-failed-attempts 2 | 次のサーバを試す前にグループ内の AAA サーバに送信する要求の最大数を指定します。*number* 引数の範囲は 1 ～ 5 です。デフォルトは 3 です。<br><br>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は、「ローカル コマンド許可の設定」（P.43-24）および「TACACS+ コマンド許可の設定」（P.43-29）を参照してフォールバック メカニズムを設定）、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。<br><br>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 4 | **reactivation-mode** {**depletion** [**deadtime** *minutes*] \| **timed**}<br><br>**例：**<br>hostname(config-aaa-server-group)# reactivation-mode deadtime 20 | 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。<br><br>**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。<br><br>**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。<br><br>**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。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 5 | **accounting-mode simultaneous**<br><br>**例：**<br>`hostname(config-aaa-server-group)# accounting-mode simultaneous` | グループ内のすべてのサーバにアカウンティング メッセージを送信します（RADIUS または TACACS+ のみ）。<br>アクティブ サーバだけ送信メッセージをデフォルトに戻すには、**accounting-mode single** コマンドを入力します。 |
| ステップ 6 | **aaa-server** *server_group* [*interface_name*] **host** *server_ip*<br><br>**例：**<br>`hostname(config)# aaa-server servergroup1 outside host 10.10.1.1` | 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。<br>**aaa-server host** コマンドを入力すると、AAA サーバのホスト コンフィギュレーション モードを開始します。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。<br>ホスト コンフィギュレーション モードでのコマンドは、すべての AAA サーバ タイプに適用されるわけではありません。表 38-2 に、使用可能なコマンド、適用先のサーバ タイプ、および新規 AAA サーバ定義にそのコマンドのデフォルト値が指定されているかどうかを示します。コマンドが、指定したサーバ タイプに適用可能で、デフォルト値が用意されていない場合は（「—」で示す）、コマンドを使用して値を指定します。 |

**表 38-2　ホスト モード コマンド、サーバ タイプ、およびデフォルト**

| コマンド | 適用可能な AAA サーバ タイプ | デフォルト値 | 説明 |
|---|---|---|---|
| **accounting-port** | RADIUS | 1646 | |
| **acl-netmask-convert** | RADIUS | 標準 | |
| **authentication-port** | RADIUS | 1645 | |
| **kerberos-realm** | Kerberos | — | |
| **key** | RADIUS | — | |
| | TACACS+ | — | |
| **ldap-attribute-map** | LDAP | — | |
| **ldap-base-dn** | LDAP | — | |
| **ldap-login-dn** | LDAP | — | |
| **ldap-login-password** | LDAP | — | |
| **ldap-naming-attribute** | LDAP | — | |
| **ldap-over-ssl** | LDAP | 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** | LDAP | — | |

表 38-2　ホスト モード コマンド、サーバ タイプ、およびデフォルト （続き）

| コマンド | 適用可能な AAA サーバ タイプ | デフォルト値 | 説明 |
|---|---|---|---|
| **mschapv2-capable** | RADIUS | enabled | |
| **nt-auth-domain-controller** | NT | — | |
| **radius-common-pw** | RADIUS | — | |
| **retry-interval** | Kerberos | 10 秒 | |
| | RADIUS | 10 秒 | |
| | SDI | 10 秒 | |
| **sasl-mechanism** | LDAP | — | |
| **server-port** | Kerberos | 88 | |
| | LDAP | 389 | |
| | NT | 139 | |
| | SDI | 5500 | |
| | TACACS+ | 49 | |
| **server-type** | LDAP | auto-discovery | 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** | All | 10 秒 | |

## 例

例 38-1 に、1 つのプライマリ サーバと 1 つのバックアップ サーバを持つ 1 つの TACACS+ グループ、単一のサーバを持つ 1 つの RADIUS グループ、および 1 つの NT ドメイン サーバを追加する方法を示します。

**例 38-1　複数の AAA サーバ グループおよびサーバ**

```
hostname(config)# aaa-server AuthInbound protocol tacacs+
hostname(config-aaa-server-group)# max-failed-attempts 2
hostname(config-aaa-server-group)# reactivation-mode depletion deadtime 20
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthInbound (inside) host 10.1.1.1
hostname(config-aaa-server-host)# key TACPlusUauthKey
hostname(config-aaa-server-host)# exit
hostname(config)# aaa-server AuthInbound (inside) host 10.1.1.2
hostname(config-aaa-server-host)# key TACPlusUauthKey2
hostname(config-aaa-server-host)# exit
hostname(config)# aaa-server AuthOutbound protocol radius
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key RadUauthKey
hostname(config-aaa-server-host)# exit
hostname(config)# aaa-server NTAuth protocol nt
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server NTAuth (inside) host 10.1.1.4
hostname(config-aaa-server-host)# nt-auth-domain-controller primary1
hostname(config-aaa-server-host)# exit
```

例 38-2 に、watchdogs という名前の Kerberos AAA サーバ グループを設定し、そのグループに AAA サーバを追加して、そのサーバの Kerberos 領域を定義する方法を示します。例 38-2 では、リトライ インターバルと Kerberos サーバがリスンするポートを定義していないため、ASA は、これら 2 つのサーバ固有のパラメータにデフォルト値を使用します。表 38-2 に、すべての AAA サーバ ホスト モード コマンドのデフォルト値を示します。

（注）　Kerberos 領域名では数字と大文字だけを使用します。ASA は領域名に小文字を受け入れますが、小文字を大文字に変換しません。大文字だけを使用してください。

**例 38-2　Kerberos サーバ グループおよびサーバ**

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(config)#
```

# VPN のための LDAP での許可の設定

VPN アクセスのためのユーザ LDAP 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許可データが含まれます。したがって、LDAP を使用すると、認証と許可が 1 つのステップで行われます。

ただし、場合によっては、許可メカニズムとは別の異なる許可を 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、許可情報は返されません。この場合、ユーザ許可では、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、認証と許可は 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。

## 手順の詳細

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **aaa-server** *server_group* **protocol** {**kerberos** \| **ldap** \| **nt** \| **radius** \| **sdi** \| **tacacs+**}<br><br>**例：**<br>hostname(config)# aaa-server servergroup1 protocol ldap<br>hostname(config-aaa-server-group) | AAA サーバ グループを作成します。 |
| ステップ 2 | **tunnel-group** *groupname*<br><br>**例：**<br>hostname(config)# tunnel-group remotegrp | 「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。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | **tunnel-group** *groupname* **general-attributes**<br><br>**例：**<br>hostname(config)# tunnel-group remotegrp general-attributes | サーバ グループとトンネル グループを関連付けます。 |
| ステップ 4 | **authorization-server-group** *group-tag*<br><br>**例：**<br>hostname(config-general)# authorization-server-group ldap_dir_1 | 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。 |

**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。

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

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

# LDAP 属性マップの設定

ASA では、LDAP ディレクトリを使用して、VPN リモート アクセス ユーザまたはファイアウォール ネットワーク アクセス セッションおよびカットスルー プロキシ セッションの認証を行えます。また、ACL、ブックマーク リスト、DNS 設定または WINS 設定、セッション タイマーといったポリシー権限（許可属性とも呼ばれます）の設定も行えます。つまり、外部から LDAP サーバを介して、ローカル グループ ポリシーに含まれる主要な属性を設定できるということです。

許可プロセスは LDAP 属性マップ（ベンダー固有属性を定義する RADIUS ディクショナリに類似しています）によって行われます。このプロセスにより、ネイティブ LDAP ユーザ属性が Cisco ASA 属性名に変換されます。それらの属性マップを LDAP サーバにバインドしたり、必要に応じて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。

## ガイドライン

LDAP 属性マップでは、マルチ値の属性に制限があります。たとえば、ユーザが複数の AD グループのメンバであり、LDAP 属性マップが複数のグループで一致する場合、マップされる値は、一致したエントリのアルファベット順配列に基づいて選択されます。

属性マッピング機能を適切に使用するには、Cisco 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。LDAP 属性マップの詳細については、「Active Directory/LDAP VPN リモート アクセス許可の例」（P.C-16）を参照してください。

頻繁にマッピングされるシスコの 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）：ディレクトリの部門またはユーザ 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、および SSL に適用されるアクセス コントロール リスト（ACL）。
- 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 サーバには 1 つの ldap 属性のみを割り当てることができます。

LDAP 機能を正しくマップするには、次の手順を実行します。

## 手順の詳細

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **ldap attribute-map** *map-name*<br><br>**例：**<br>`hostname(config)# ldap attribute-map att_map_1` | 空の LDAP 属性マップ テーブルを作成します。 |
| ステップ 2 | **map-name** *user-attribute-name Cisco-attribute-name*<br><br>**例：**<br>`hostname(config-ldap-attribute-map)# map-name department IETF-Radius-Class` | 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。 |
| ステップ 3 | **map-value** *user-attribute-name Cisco-attribute-name*<br><br>**例：**<br>`hostname(config-ldap-attribute-map)# map-value department Engineering group1` | 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。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | **aaa-server** *server_group* [*interface_name*] **host** *server_ip*<br><br>**例：**<br>hostname(config)# aaa-server ldap_dir_1 host 10.1.1.4 | 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。 |
| ステップ 5 | **ldap-attribute-map** *map-name*<br><br>**例：**<br>hostname(config-aaa-server-host)# ldap-attribute-map att_map_1 | 属性マップを LDAP サーバにバインドします。 |

## 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 属性の有効な値は次の 3 つです。

- 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。

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

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

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

```
hostname(config-ldap-attribute-map)#
```

# ユーザ アカウントのローカル データベースへの追加

ここでは、ローカル データベース内のユーザの管理方法について説明します。

ユーザをローカル データベースに追加するには、次の手順を実行します。

## ガイドライン

次の各機能は、ローカル データベースを使用して実行されます。

- ASDM ユーザごとのアクセス
- コンソール認証
- Telnet 認証および SSH 認証
- **enable** コマンド認証

  この設定は、CLI アクセスにだけ使用され、ASDM ログインには影響しません。
- コマンド許可

  ローカル データベースを使用するコマンド許可を有効にすると、ASA では、ユーザ特権レベルを参照して、どのコマンドが使用できるかが特定されます。コマンド許可がディセーブルの場合は通常、特権レベルは参照されません。デフォルトでは、コマンドの特権レベルはすべて、0 または 15 のどちらかです。
- ネットワーク アクセス認証
- VPN クライアント認証

マルチ コンテキスト モードの場合、システム実行スペースでユーザ名を設定し、**login** コマンドを使用して CLI で個々にログインできます。ただし、システム実行スペースではローカル データベースを参照する AAA ルールは設定できません。

## 制限事項

ローカル データベースはネットワーク アクセス許可には使用できません。

## 手順の詳細

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **username** *username* {**nopassword** \| **password** *password* [**mschap**]} [**privilege** *priv_level*]<br><br>**例：**<br>`hostname(config)# username exampleuser1 privilege 1` | ユーザ アカウントを作成します。**username** *username* キーワードは、4 ～ 64 文字の文字列です。<br><br>**password** *password* キーワードは、3 ～ 32 文字の文字列です。**mschap** キーワードは、パスワードを入力した後に、そのパスワードが Unicode に変換され、MD4 を使用してハッシュされることを示します。このキーワードは、ユーザを MS-CHAPv1 または MS-CHAPv2 を使用して認証する場合に使用します。**privilege** *level* 引数では、0 ～ 15 の特権レベルを設定します。デフォルトは 2 です。この特権レベルは、コマンド許可で使用されます。<br><br>**注意**　コマンド許可（**aaa authorization console LOCAL** コマンド）を使用していない場合、デフォルトのレベル 2 を使用して特権 EXEC モードにアクセスできます。特権 EXEC モードへのアクセスを制限する場合、特権レベルを 0 または 1 に設定するか、または **service-type** コマンドを使用します（ステップ 5 を参照）。<br><br>**nopassword** キーワードは、パスワードを指定しないユーザ アカウントを作成します。<br><br>通常、**encrypted** および **nt-encrypted** キーワードは表示専用です。**username** コマンド内のパスワードを定義すると、ASA はセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するときに暗号化します。**show running-config** コマンドを入力すると、**username** コマンドは実際のパスワードを表示しません。このコマンドは暗号化されたパスワードを表示し、次に **encrypted** または **nt-encrypted** キーワード（**mschap** を指定する場合）を表示します。たとえば、パスワードに「test」と入力すると、**show running-config** の出力には次のように表示されます。<br><br>`username user1 password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted`<br><br>実際に CLI で **encrypted** または **nt-encrypted** キーワードを入力するのは、あるコンフィギュレーション ファイルを他の ASA にカット アンド ペーストして、同じパスワードを使用している場合だけです。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 2 | **aaa authorization exec authentication-server**<br><br>**例：**<br>`hostname(config)# aaa authorization exec authentication-server` | （任意）管理アクセスを認証するユーザに、ユーザ固有のアクセス レベルを強制します（**aaa authentication console LOCAL** コマンドを参照）。このコマンドは、ローカル、RADIUS、LDAP（マッピング済み）、および TACACS+ の各ユーザの管理許可をイネーブルにします。<br><br>**aaa authorization exec LOCAL** コマンドを使用して、ローカル データベースから属性を取得できるようにします。AAA サーバのユーザを管理許可が有効になるように設定する方法については、「管理許可によるユーザ CLI および ASDM アクセスの制限」（P.43-22）を参照してください。<br><br>次に示すユーザ タイプごとの前提条件を確認してください。<br>• **username** コマンドを使用して、0 ～ 15 の特権レベルでローカル データベースでユーザを設定します。**service-type** コマンドを使用して、アクセスのレベルを設定します。<br>• RADIUS ユーザに Cisco VSA CVPN3000-Privilege-Level の 0 ～ 15 の値を設定します。<br>• LDAP ユーザを特権レベル 0 ～ 15 を使用して設定し、**ldap map-attributes** コマンドを使用して LDAP 属性を Cisco VAS CVPN3000-Privilege-Level にマッピングします。<br>• コマンド特権レベルの設定については、**privilege** コマンドを参照してください。 |
| ステップ 3 | **username** *username* **attributes**<br><br>**例：**<br>`hostname(config)# username exampleuser1 attributes` | （任意）ユーザ名属性を設定します。*username* 引数はステップ 1 で作成したユーザ名です。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | **service-type** {**admin** \| **nas-prompt** \| **remote-access**}<br><br>**例：**<br>hostname(config-username)# service-type admin | （任意）ステップ 2 で管理許可を設定した場合は、ユーザ レベルを設定します。**admin** キーワードは、**aaa authentication console LOCAL** コマンドによって指定されたサービスへのフル アクセスを許可します。デフォルトは **admin** キーワードです。<br><br>**nas-prompt** キーワードは、**aaa authentication** {**telnet** \| **ssh** \| **serial**} **console LOCAL** コマンドを設定しているときに CLI へのアクセスを許可しますが、**aaa authentication http console LOCAL** コマンドを設定しているときは ASDM へのコンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console LOCAL** コマンドを使用して認証をイネーブルにしている場合、ユーザは、**enable** コマンド（または **login** コマンド）を使用して特権 EXEC モードにアクセスできません。<br><br>**remote-access** キーワードは管理アクセスを拒否します。ユーザは、**aaa authentication console LOCAL** コマンドで指定されているいずれのサービスも使用できません（**serial** キーワードは除きます。この場合、シリアル アクセスは許可されます）。<br><br>（任意）VPN 認証にこのユーザ名を使用している場合、そのユーザに多くの VPN 属性を設定できます。詳細については、「個々のユーザの属性の設定」（P.71-94）を参照してください。 |

### 例

次の例では、admin ユーザ アカウントに対して特権レベル 15 を割り当てます。

```
hostname(config)# username admin password password privilege 15
```

次の例では、パスワードを指定しないユーザ アカウントを作成します。

```
hostname(config)# username user34 nopassword
```

次の例では、管理許可をイネーブルにし、パスワードを指定するユーザ アカウントを作成し、ユーザ名属性コンフィギュレーション モードを開始して、**service-type** 属性を指定します。

```
hostname(config)# aaa authorization exec authentication-server
hostname(config)# username user1 password gOgeOus
hostname(config)# username user1 attributes
hostname(config-username)# service-type nas-prompt
```

## ユーザに対する VPN ポリシー属性の設定

### 前提条件

この手順では、既存のユーザを編集する方法について説明します。詳細については、「ユーザ アカウントのローカル データベースへの追加」（P.38-20）を参照してください。

**手順の詳細**

# SSH 公開キーによるユーザの認証

SSH 公開キーを使用してユーザを認証できます。公開キーは、ハッシュ化することも、ハッシュ化しないでおくこともできます。

SSH の公開キーで認証を行うには、次のコマンドを入力します。

| コマンド | 目的 |
|---|---|
| **username** {*user*} **attributes ssh authentication publickey** *key* **[hashed]**<br><br>**例：**<br>`hostname(config)# username anyuser ssh authentication publickey key [hashed]` | 公開キー認証をユーザ単位でイネーブルにします。*key* 引数の値は次のいずれかになります。<br>• *key* 引数が指定され、ハッシュされたタグが指定されていない場合、キーの値は、SSH-RSA の未処理キーを生成することのできる SSH キー生成ソフトウェアによって生成される Base 64 で符号化された公開キーである必要があります（つまり、証明書は使用しません）。Base 64 エンコード公開キーを送信すると、そのキーは SHA-256 によりハッシュ化され、それ以降のすべての比較では対応する 32 バイト ハッシュが使用されます。<br>• *key* 引数が指定され、ハッシュされたタグを指定した場合は、キーの値は、SHA-256 で事前にハッシュされている必要があります。長さは 32 バイトで、各バイトはコロンで区切られている必要があります（解析のため）。<br>設定を保存すると、ハッシュされたキー値はコンフィギュレーションに保存され、ASA のリブート時に使用されます。 |

# AAA によるユーザ ロールの区別

ASA を使用すると、RADIUS、LDAP、TACACS+、またはローカル ユーザ データベースを使用して認証する場合に、管理ユーザとリモート アクセス ユーザを区別することができます。ユーザ ロールを区別することで、リモート アクセス VPN ユーザやネットワーク アクセス ユーザが ASA に管理接続を確立するのを防ぐことができます。

ユーザ ロールを区別するには、ユーザ名コンフィギュレーション モードで **service-type** 属性を使用します。RADIUS および LDAP の場合（**ldap-attribute-map** コマンドを使用）、Cisco ベンダー固有属性（VSA）の Cisco-Priv-Level を使用して、認証済みのユーザに特権レベルを割り当てることができます。

この項では、次のトピックについて取り上げます。


- 「ローカル認証の使用」（P.38-25）
- 「RADIUS 認証の使用」（P.38-25）
- 「LDAP 認証の使用」（P.38-25）
- 「TACACS+ 認証の使用」（P.38-26）

## ローカル認証の使用

ローカル認証を使用している場合、**service-type** 属性および特権レベルを設定する前に、ユーザを作成し、パスワードと特権レベルを割り当てる必要があります。そのためには、次のコマンドを入力します。

```
hostname(config)# username admin password mysecret123 privilege 15
```

**mysecret123** は保存されているパスワードです。15 は割り当てられる権限レベルで、これは管理ユーザを表します。

**service-type** 属性の使用可能な設定オプションには、次のものがあります。

- **admin**：ユーザはコンフィギュレーション モードにアクセスできます。このオプションでは、ユーザにリモート アクセス経由での接続が許可されます。
- **nas-prompt**：ユーザは EXEC モードにアクセスできます。
- **remote-access**：ユーザはネットワークにアクセスできます。

次の例では、admin という名前のユーザに **service-type** として **admin** を指定します。

```
hostname(config)# username admin attributes
hostname(config-username)# service-type admin
```

次の例では、ra-user という名前のユーザに **service-type** として **remote-access** を指定します。

```
hostname(config)# username ra-user attributes
hostname(config-username)# service-type remote-access
```

## RADIUS 認証の使用

RADIUS IETF の **service-type** 属性が、RADIUS 認証および許可要求の結果として access-accept メッセージで送信される場合、この属性は認証されたユーザにどのタイプのサービスを付与するかを指定するために使用されます。サポートされる属性値は、administrative（6）、nas-prompt（7）、Framed（2）、および Login（1）です。認証と許可に使用できるサポートされている RADIUS IETF VSA のリストについては、表 C-8（P.C-37）を参照してください。

RADIUS 認証の使用の詳細については、「外部 RADIUS サーバの設定」（P.C-27）を参照してください。Cisco Secure ACS のための RADIUS 認証の設定については、Cisco.com にある Cisco Secure ACS のマニュアルを参照してください。

RADIUS Cisco VSA **privilege-level** 属性（ベンダー ID 3076、サブ ID 220）が access-accept メッセージで送信される場合は、ユーザの権限レベルを指定するために使用されます。許可に使用できるサポートされている RADIUS VSA のリストについては、表 C-7（P.C-28）を参照してください。

## LDAP 認証の使用

ユーザが LDAP 経由で認証される場合、ネイティブ LDAP 属性およびその値は Cisco ASA 属性にマッピングされ、特定の許可機能を提供します。許可に使用できるサポートされている LDAP VSA のリストについては、表 C-2（P.C-6）を参照してください。

LDAP 許可には、LDAP 属性マッピング機能を使用できます。この機能の例については、「権限および属性のポリシー実施の概要」（P.C-1）を参照してください。

次の例は、LDAP 属性マップを定義する方法を示しています。この例では、セキュリティ ポリシーによって、LDAP によって認証されているユーザが、ユーザ レコードのフィールドまたはパラメータの title と company を、IETF-RADIUS service-type と privilege-level にそれぞれマップすることを指定しています。

LDAP 属性マップを定義するには、次のコマンドを入力します。

```
hostname(config)# ldap attribute-map admin-control
hostname(config-ldap-attribute-map)# map-name title IETF-RADIUS-Service-Type
hostname(config-ldap-attribute-map)# map-name company Privilege-Level
```

次に、**ldap-attribute-map** コマンドの出力例を示します。

```
ldap attribute-map admin-control
    map-name company Privilege-Level
    map-name title IETF-Radius-Service-Type
```

LDAP 属性マップを LDAP AAA サーバに適用するには、次のコマンドを入力します。

```
hostname(config)# aaa-server ldap-server (dmz1) host 10.20.30.1
hostname(config-aaa-server-host)# ldap-attribute-map admin-control
```

（注）　認証されたユーザが ASDM、SSH、または Telnet を使用して ASA に管理アクセスを試みたものの、これを実行するために必要な特権レベルを持っていないと、ASA から syslog メッセージ 113021 が生成されます。このメッセージは、管理者権限が不適切であるためログインに失敗したことをユーザに通知するものです。

## TACACS+ 認証の使用

TACACS+ 認証を設定する方法については、「外部 TACACS+ サーバの設定」（P.C-39）を参照してください。

# AAA サーバのモニタリング

AAA サーバをモニタするには、次のいずれかのコマンドを入力します。

| コマンド | 目的 |
|---|---|
| **show aaa-server** | 設定済みの AAA サーバの統計情報を表示します。<br>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** | AAA サーバ実行コンフィギュレーションを表示します。<br>AAA サーバの統計情報をクリアするには、**clear configure aaa-server** コマンドを入力します。 |
| **show running-config all ldap attribute-map** | 実行コンフィギュレーションのすべての LDAP 属性を表示します。<br>実行コンフィギュレーションのすべての LDAP 属性をクリアするには、**clear configuration ldap attribute-map** コマンドを使用します。 |
| **show running-config zonelabs-integrity** | Zone Labs Integrity サーバ コンフィギュレーションを表示します。<br>Zone Labs Integrity サーバ コンフィギュレーションをクリアするには、**clear configure zonelabs-integrity** コマンドを使用します。 |
| **show ad-groups** *name* [**filter** *string*] | LDAP を使用する AD サーバだけに適用し、AD サーバに登録されているグループを表示します。 |

# その他の参考資料

LDAP マッピングの実装に関するその他の情報については、「RFC」（P.38-27）を参照してください。

## RFC

| RFC | タイトル |
|---|---|
| 2138 | *『Remote Authentication Dial In User Service (RADIUS)』* |
| 2139 | *『RADIUS Accounting』* |
| 2548 | *『Microsoft Vendor-specific RADIUS Attributes』* |
| 2868 | *『RADIUS Attributes for Tunnel Protocol Support』* |

# AAA サーバの機能履歴

表 38-3 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 38-3　AAA サーバの機能履歴

| 機能名 | プラットフォーム リリース | 機能情報 |
|---|---|---|
| AAA サーバ | 7.0(1) | AAA サーバでは、AAA のサポート情報と AAA サーバおよびローカル データベースの設定方法が示されます。<br>次のコマンドを導入しました。<br>**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**、**zonelabs-Integrity server-address**、**zonelabs-integrity port**、**zonelabs-integrity interface**、**zonelabs-integrity fail-timeout**、**zonelabs-integrity fail-close**、**zonelabs-integrity fail-open**、**zonelabs-integrity ssl-certificate-port**、**zonelabs-integrity ssl-client-authentication {enable \| disable}**、**client-firewall {opt \| req} zonelabs-integrity** |
| ASA からの RADIUS アクセス要求パケットおよび RADIUS アカウンティング要求パケットで送信された主なベンダー固有属性（VSA） | 8.4(3) | 4 つの新しい VSA：Tunnel Group Name（146）および Client Type（150）は、ASA からの RADIUS アクセス要求パケットで送信されます。Session Type（151）および Session Subtype（152）は、ASA からの RADIUS アカウンティング要求パケットで送信されます。4 つのすべての属性が、すべてのアカウンティング要求パケット タイプ（開始、中間アップデート、および終了）に送信されます。RADIUS サーバ（ACS や ISE など）は、許可属性やポリシー属性を強制適用したり、アカウンティングや課金のためにそれらの属性を使用したりできます。 |