LDAP 属性マップの ASA 使用の設定例

目次

概要

このドキュメントは、適応型セキュリティ アプライアンス（ASA）上できめ細かいダイナミック アクセス ポリシーを設定するために Lightweight Directory Access Protocol（LDAP）属性マップを使用する方法について説明しています。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco IOS® での Secure Sockets Layer VPN（SSL VPN）
- Cisco IOS での LDAP 認証
- ディレクトリ サービス

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- CISCO881-SEC-K9
- Cisco IOS Software, C880 Software (C880DATA-UNIVERSALK9-M), Version 15.1(4)M, RELEASE SOFTWARE (fc1)

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

LDAP は、分散ディレクトリ情報サービスに IP ネットワーク経由でアクセスし維持するための、ベンダーに依存しない開かれた業界標準アプリケーション プロトコルです。 ディレクトリ サービスによって、ユーザ、システム、ネットワーク、サービス、およびアプリケーションに関する情報がネットワークを通して共有できるため、イントラネットやインターネットのアプリケーション開発において重要な役割を果たします。

通常、管理者は、VPN ユーザにさまざまなアクセス権限または WebVPN コンテンツを提供します。 これは、VPN サーバ上で異なる VPN ポリシーを設定し、各ユーザのクレデンシャルに基づいてこれらのポリシー セットを割り当てることで実現されます。 これは手動で行うこともできますが、ディレクトリ サービスを利用してプロセスを自動化すればより効率的です。 LDAP を使用してグループ ポリシーをユーザに割り当てる場合、マップを設定して、Active Directory（AD）属性 **memberOf** などの LDAP 属性を、VPN ヘッドエンドで認識される **IETF-Radius-Class** 属性にマッピングする必要があります。

Cisco IOS では、ドキュメントで説明されているように、異なるポリシー グループを WebVPN コンテキストで設定し、どのポリシー グループにユーザが割り当てられるかを判断するために LDAP 属性マップを使用することで同じことができます。 Cisco IOS ヘッドエンド設定例上で LDAP を使用する AnyConnect クライアントに対するポリシー グループ割り当てを参照してください。

ASA では、これは、さまざまなグループ ポリシーを異なるユーザに割り当てることで実現します。 LDAP 認証が使用されていると、LDAP 属性マップを使用して自動的に実行できます。 LDAP を使用してグループ ポリシーをユーザに割り当てるには、AD 属性 **memberOf** などの LDAP 属性を ASA が認識する**グループ ポリシー**に割り当てます。 属性マッピングが確立されたら、LDAP

サーバで設定された属性値を ASA のグループ ポリシーの名前にマッピングする必要があります。

> **注: memberOf** 属性は、ユーザが Active Directory の一部であるグループに対応します。 ユーザは、Active Directory の複数のグループのメンバになることができます。 この場合、複数の **memberOf** 属性がサーバにより送信されますが、ASA は 1 グループ ポリシーに対して 1 属性だけをマッチングできます。

FAQ

Q. ASA の LDAP 属性マップ数の設定には制限がありますか。

A. いいえ、制限はありません。 LDAP 属性マップは、LDAP 認証/認可を使用する VPN のリモート アクセス セッション中に動的に割り当てられます。

Q. LDAP 属性マップごとにマッピングできる属性の数に制限はありますか。

A. 設定制限はありません。

Q. 特定の LDAP 属性マップを適用できる LDAP サーバの数には制限がありますか。

A. 制限はありません。 LDAP コードは LDAP 属性マップの名前が有効であることのみを検証します。

Q. LDAP 属性マップおよび AD memberOf などの複数の値を持つ属性には制限がありますか。

A. はい。 ここでは、AD についてだけ説明していますが、ポリシーの決定に複数値の属性を使用する LDAP サーバが制限されます。 LDAP 属性マップには、AD memberOf のような複数値の属性に対して制限があります。 ユーザが複数の AD グループのメンバーであり（通常この状態）、LDAP 属性マップが複数のグループに一致する場合、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で選択されます。 この機能は直感的にわかりやすいものではないため、よく理解しておくことが重要です。

要約： LDAP マッピング結果が、1 つの属性に対して複数の値となる場合、最終的な属性値は次のように選択されます。

- 最初に、文字数の最も少ない値を選択します。
- これが複数の値となる場合、アルファベット順で最初の値を選択します。

使用例

Active Directory-LDAP は、ユーザ認証または認可リクエストに対して次の 4 つの memberOf イ

ンスタンスを返します。

```
memberOf: value = CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
memberOf: value = CN=Cisco-Eng,CN=Users,DC=stbu,OU=cisco,DC=com
memberOf: value = CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com
memberOf: value = CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com
```

LDAP-MAP #1: 次の LDAP 属性マップが、memberOf 設定に基づいて異なる ASA グループ ポリシーをマッピングするために設定されているとします。

```
ldap attribute-map Class
map-name memberOf Group-Policy
map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup4
map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup3
map-value memberOf CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup2
map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup1
```

この場合、4 つのグループ ポリシー値すべて（ASAGroup1 - ASAGroup4）が一致します。 ただし、ASAGroup1 がアルファベット順で最初になるため、この接続は、グループ ポリシー ASAGroup1 に割り当てられます。

LDAP-MAP #2： 次の LDAP 属性マップは、最初の memberOf に明示的なマップ値が割り当てられていない（ASAGroup4 がない）ことを除けば同じものです。 マップ値が明示的に定義されていない場合、LDAP から受信した属性のテキストが使用されます。

```
ldap attribute-map Class
map-name memberOf Group-Policy
map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup3
map-value memberOf CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup2
map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup1
```

前のケースと同様に、4 つすべてのエントリが一致します。 この場合、APP-SSL-VPN エントリに関してはマッピングされる値がないため、マッピング値はデフォルトで CN=APP-SSL-VPN Managers、CN=Users、OU=stbu、DC=cisco、DC=com になります。 CN=APP-SSL-VPN がアルファベット順で最初に出現するため、APP-SSL-VPN がポリシー値として選択されます。

詳細については、Cisco Bug ID CSCub64284 を参照してください。 PIX/ASA 8.0：ログイン時に LDAP 認証を使用してグループ ポリシーを割り当てる を参照してください。 ログイン時に LDAP 認証を使用してグループ ポリシーを割り当てるでは、特定の環境で機能する可能性のある memberOf に関するシンプルな LDAP のケースを示しています。

回避策とベスト プラクティス オプション

1. ダイナミック アクセス ポリシー（DAP）の使用：DAP には、複数の値を持つ属性（memberOf など）の解析に関するこの制限はありません。 ただし、DAP は現在、DAP 内でグループ ポリシーを設定することはできません。 そのため、トンネルグループ/グループ ポリシー関連付け方式によってセッションを適切にセグメント化する必要があります。 将来 DAP は、グループ ポリシーも含めた任意の認可属性を設定できるようになるため（Cisco Bug ID CSCsi54718）、DAP の設定のために LDAP 属性マップを使用する必要はなくなります。

2. LDAP 属性マップを使用してクラス属性を設定する必要がある場合、導入シナリオ上可能で

あれば代替手段として、AD 上のグループを区別するための単一値の属性（Department など）を使用することもできます。

注:「CN=Engineering, OU=Office1, DC=cisco,DC=com」のような memberOf DN では、DN の最初、つまり、CN=Engineering でだけこの手段を使用できます。Organizational Unit (OU) ではできません。 任意の DN フィールド上でフィルタを適用するための拡張があります。

設定：使用例

注: このセクションで説明した各例はスタンドアロン設定ですが、それぞれ組み合わせて必要なアクセス ポリシーを作成することができます。

ヒント： 属性名および値では大文字と小文字が区別されます。 正しくマッピングされない場合、Cisco 属性および LDAP の属性の名前と値の***両方***で、LDAP 属性マップのスペルと大文字小文字が正しいことを確認します。

1. ユーザベースの属性ポリシーの適用

任意の標準 LDAP 属性を、良く知られたアプライアンス ベンダー固有属性（VSA）にマッピングすることができます。 1 つ以上の LDAP 属性を 1 つ以上の Cisco LDAP 属性にマッピングできます。 Cisco LDAP VSA の完全なリストについては、LDAP 認可でサポートされる Cisco 属性を参照してください。 この例は、LDAP user1 に対してバナーを適用する方法について示しています。 User1 は、次のいずれかの VPN リモート アクセス タイプが可能です。 IPsec、SVC、または WebVPN Clientless。 この例は、Banner1 を適用するために、[Properties]/[General]/[Office] 属性/フィールドを使用します。

注: ASA/PIX グループ ポリシーからポリシーを適用するため、[AD Department] 属性/フィールドを使用して、Cisco IETF-Radius-Class VSA にマッピングすることができます。 ドキュメントの後の方でこの例を示します。

LDAP（Microsoft AD および Sun の場合）属性マッピングは PIX/ASA バージョン 7.1.x でサポートされています。 Cisco 属性には、任意の Microsoft/AD の属性をマッピングできます。 そのための手順を次に示します。

1. AD/LDAP サーバで次を実行します。user1 を選択します。[> Properties] を右クリックします。属性を設定するために必要なタブを選択します（例： [General] タブ）。たとえば [Office] フィールドのような、時間範囲を適用するために使用するフィールド/属性を選択し、バナー テキストを入力します（例：「LDAP へようこそ!!!!」）。 GUI 上の [Office] 設定は、AD/LDAP 属性 [physicalDeliveryOfficeName] に保存されます。

2. ASA では、LDAP 属性マッピング テーブルを作成するために、AD/LDAP 属性 [physicalDeliveryOfficeName] を ASA 属性 [Banner1] にマッピングします。

```
B200-54(config)# show run ldap
ldap attribute-map Banner
```

```
map-name physicalDeliveryOfficeName Banner1
```

3. LDAP 属性マップを aaa サーバ エントリに関連付けます。

```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map Banner
```

4. Remote Access セッションを確立し、バナー「LDAP へようこそ!!!」を確認します。 これは VPN ユーザに表示されます。

2. 特定のグループ ポリシー内の LDAP ユーザの配置：汎用例

この例は、AD-LDAP サーバ上の user1 の認証を示し、[department] フィールド値を取得して、適用される ASA/PIX グループ ポリシーにマッピングされるようにします。

1. AD/LDAP サーバで次を実行します。user1 を選択します。[> Properties] を右クリックします。属性を設定するために必要なタブを選択します（例： [Organization] タブ）。たとえば [Department] のような、グループ ポリシーを適用するために使用するフィールド/属性を選択し、ASA/PIX にグループ ポリシーの値（Group-Policy1）を入力します。 GUI 上の [Department] 設定は、AD/LDAP 属性 [department] に保存されます。

2. LDAP 属性マップ テーブルを定義します。

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department Group-Policy
5520-1(config)#
```

注: Cisco Bug ID CSCsv43552 の実装の結果として、新規 LDAP 属性マップの属性である Group-Policy が、IETF-Radius-Class に置き換わるものとして導入されました。 ASA Version 8.2 上の CLI は、8.0 の設定ファイルを読み取るために、map-name および map-value コマンドの有効な選択肢として IETF-Radius-Class キーワードをサポートします（ソフトウェア アップグレード シナリオ）。 Adaptive Security Device Manager（ASDM）コードはすでにアップデートされ、属性マップ エントリを設定する際に IETF-Radius-Class は選択肢として表示されなくなりました。 また、ASDM は（8.0 config から読み取られた場合）IETF-Radius-Class 属性を Group-Policy 属性として書き出します。

3. アプライアンスおよび必須ポリシー属性上でグループ ポリシー Group_policy1 を定義します。

4. VPN リモート アクセス トンネルを確立し、セッションが Group-Policy1 から属性（および

デフォルト グループ ポリシーからのその他の該当する属性）を継承することを確認します。

注: 必要に応じてマップに属性をさらに追加します。 この例は、特定の機能を制御するための最小限のものを示しています（ユーザに特定の ASA/PIX 7.1.x グループ ポリシーを設定します）。 3 番目の例では、マップのタイプを示します。

NOACCESS グループ ポリシーの設定

NOACCESS グループ ポリシーを作成して、LDAP グループのメンバでないユーザの VPN 接続を拒否できます。 次に、この設定の一部を例として示します。

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department Group-Policy
5520-1(config)#
```

このグループ ポリシーをデフォルト グループ ポリシーとしてトンネル グループに適用する必要があります。 これにより、目的の LDAP グループに属するユーザなど、LDAP 属性マップからマッピングを取得するユーザは、目的のグループ ポリシーを取得できます。また、たとえば、目的の LDAP グループに属さないユーザなど、マッピングを取得できないユーザは、トンネル グループから NOACCESS グループ ポリシーを取得できます。これにより、これらのユーザのアクセスがブロックされます。

ヒント： ここでは vpn-simultaneous-logins 属性が 0 に設定されているため、他のすべてのグループ ポリシーでも明示的に定義する必要があります。 それ以外の場合は、そのトンネル グループのデフォルト グループ ポリシーから継承されます。この場合は NOACCESS ポリシーです。

3. グループ ベースの属性のポリシーの適用：例

注: ASA を Version 7.2.2 以降で実行するには、Cisco Bug ID CSCse08736 の実装/フィックスが必要です。

1. AD-LDAP サーバで、Active Directory ユーザおよびコンピュータは、VPN 属性が設定されているグループを表すユーザ レコード（VPNUserGroup）を設定します。

2. AD-LDAP サーバでは、Active Directory ユーザおよびコンピュータは、各ユーザ レコードの [Department] フィールドを定義して、group-record（VPNUserGroup）をポイントするようにします。 この例では、ユーザ名は **web1** です。

   注: [department] が論理的にグループ ポリシーを参照する目的のためだけに、Department AD 属性が使用されました。 実際には、どのフィールドを使用することもできます。 必要なのは、この例に示すように、このフィールドが Cisco VPN 属性グループ ポリシーにマッピングすることです。

3. LDAP 属性マップテーブルを定義します。

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department IETF-Radius-Class
map-name description\Banner1
map-name physicalDeliveryOfficeName IETF-Radius-Session-Timeout
5520-1(config)#
```

2 つの AD-LDAP 属性、Description および Office（AD 名前記述および PhysicalDeliveryOfficeName で表される）は、Cisco VPN 属性 Banner1 および IETF-Radius-Session-Timeout にマッピングする、（VPNUSerGroup に対する）グループ レコード属性です。

department 属性は、ユーザ レコードが ASA（VPNUSer）上の外部グループ ポリシーの名前にマッピングするために使用され、次に、属性が定義されている AD-LDAP サーバ上の VPNuserGroup レコードにマッピングされるために使用されます。

注: Cisco 属性（Group Policy）は LDAP 属性マップで定義する必要があります。 マッピングされる AD 属性は、設定可能な AD 属性であれば任意です。 この例では、グループ ポリシーを参照する最も論理的な名前である、department を使用しています。

4. aaa サーバを、LDAP 認証、認可、アカウンティング（AAA）に使用する LDAP 属性マップ名を使用して設定します。

```
5520-1(config)# show runn aaa-server LDAP-AD11
aaa-server LDAP-AD11 protocol ldap
aaa-server LDAP-AD11 host 90.148.1.11
ldap-base-dn cn=Users,dc=nelson,dc=cisco,dc=com
ldap-scope onelevel
ldap-naming-attribute sAMAccountName
ldap-login-password altiga
ldap-login-dn cn=Administrator,cn=Users,dc=nelson,dc=cisco,dc=com
ldap-attribute-map Our-AD-Map
5520-1(config)#
```

5. LDAP 認証または LDAP 認可でトンネル グループを定義します。

LDAP 認可での例： 属性が定義されている場合、認証 +（認可）属性のポリシーを適用します。

```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group LDAP-AD11
accounting-server-group RadiusACS28
5520-1(config)#
```

LDAP 認証での例： デジタル証明書の使用のための設定。

```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
```

```
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group none
authorization-server-group LDAP-AD11
accounting-server-group RadiusACS28
authorization-required
authorization-dn-attributes ea
5520-1(config)#
```

6. 外部グループ ポリシーを定義します。 グループ ポリシーの名前は、グループを表す AD-LDAP ユーザ レコードの値です（VPNUserGroup）。

```
5520-1(config)# show runn group-policy VPNUserGroup
group-policy VPNUserGroup external server-group LDAP-AD11
5520-1(config)#
```

7. トンネルを確立し、属性が適用されていることを確認します。 この場合、Banner および Session-Timeout は、AD 上の VPNuserGroup レコードから適用されます。

4. IPsec および SVC トンネルに対する「静的 IP アドレスの割り当て」の Active Directory の強制

AD の属性は msRADIUSFramedIPAddress です。 属性は、[AD User Properties] の [Dial-in] タブ、[Assign a Static IP Address] で設定されます。

次に手順を示します。

1. AD サーバで、ユーザの [Properties]、[Dial-in] タブ [Assign a Static IP Address] で、IPsec/SVC セッション（10.20.30.6）に割り当てる IP アドレスの値を入力します。

2. このマッピングを使用して ASA で LDAP 属性マップを作成します。

```
5540-1# show running-config ldap
ldap attribute-map Assign-IP
map-name msRADIUSFrameIPAdddress IETF-Radius-Framed-IP-Address
5540-1#
```

3. ASA で、VPN アドレス割り当てが「vpn-addr-assign-aaa」を含むように設定されていることを確認します。

```
5520-1(config)# show runn all vpn-addr-assign
vpn-addr-assign aaa
no vpn-addr-assign dhcp
vpn-addr-assign local
5520-1(config)#
```

4. IPsec/SVC Remote Authority（RA）セッションを確立し、「show vpn-sessiondb

remote|svc」で、[Assigned IP] フィールドが正しいことを確認します。

5. Active Directory での「リモート アクセス許可ダイヤルイン、アクセスの許可/拒否」の適用

次の VPN リモート アクセス セションがすべてサポートされます。 IPsec、WebVPN および SVC。 Allow Access の値は TRUE です。 Deny Acccess の値は FALSE です。 AD の属性名は msNPAllowDialin です。

この例は、Cisco Tunneling-Protocols を使用して Allow Access (TRUE) および Deny (FALSE) 条件を作成する LDAP 属性マップの作成方法を示しています。 たとえば、tunnel-protocol=L2TPover IPsec (8) をマッピングする場合、WebVPN およ びIPsec に対してアクセスを強制する場合に FALSE を作成できます。 逆のロジックも適用されます。

次に手順を示します。

1. AD サーバの user1 の[Properties]、[Dial-In] で、各ユーザに対して適切な [Allow Access] または [Deny access] を選択します。

   注: 3 番目のオプション [Control access through the Remote Access Policy] を選択した場合、AD サーバから値は返されないため、強制される許可は、ASA/PIX の内部 group-policy の設定に基づいたものとなります。

2. ASA でこのマッピングを使用して LDAP 属性マップを作成します。

```
5520-1(config)# show runn all vpn-addr-assign
vpn-addr-assign aaa
no vpn-addr-assign dhcp
vpn-addr-assign local
5520-1(config)#
```

   注: 必要に応じてマップに属性をさらに追加します。 この例は、この特定の機能 ([Dian-In] 設定に基づいたアクセスの許可、または拒否) を制御するための最低限のものだけを示しています。

   ldap-attribute-map は、何を意味し、強制しますか。

   map-value msNPAllowDialin FALSE 8

   user1 に対するアクセスの拒否。 FALSE 値条件は、トンネル プロトコル L2TPoverIPsec (値 8) にマッピングします。

   user2 に対するアクセスの許可。 TRUE 値条件は、トンネル プロトコル WebVPN + IPsec (値 20) にマッピングします。

   AD で user1 として認証される WebVPN/IPsec ユーザは、トンネル プロトコル不一致により失敗します。

AD で user1 として認証される L2TPoverIPsec は、Deny ルールにより失敗します。

AD で user2 として認証される WebVPN/IPsec ユーザは、成功します（Allow ルールの適用およびトンネル プロトコルと一致するため）。

AD で user2 として認証される L2TPoverIPsec ユーザは、トンネル プロトコル不一致により失敗します。
RFC 2867 および 2868 で定義されているトンネル プロトコルをサポートします。

6.「アクセスを許可または拒否するメンバー/グループ メンバーシップ」の Active Directory の強制

このケースは、Case 5 と密接に関連しており、より論理的なフローを提供し、グループ メンバーシップ チェックを条件として確立するため、推奨される方法です。

1. AD のユーザを特定のグループの「Member Of」として設定します。 グループ階層の最上位に位置づける名前を使用します（ASA-VPN-Consultants）。 AD-LDAP で、グループ メンバーシップは AD 属性 [memberOf] で定義されます。

   現時点では、「memberOf」文字列の最初のグループにのみルールを適用できるため、グループがリストの最上位にあることが重要です。 リリース 7.3 では、複数のグループ フィルタリングと強制を実行できます。
2. ASA で、最小限のマッピングを使用して LDAP 属性マップを作成します。

```
5520-1(config)# show runn all vpn-addr-assign
vpn-addr-assign aaa
no vpn-addr-assign dhcp
vpn-addr-assign local
5520-1(config)#
```

注: 必要に応じてマップに属性をさらに追加します。 この例は、この特定の機能（グループ メンバーシップに基づいたアクセスの許可または拒否）を制御するための最低限のものだけを示しています。

ldap-attribute-map は、何を意味し、強制しますか。

AD グループ [ASA-VPN-Consultants] のメンバーである AD の一部の User=joe_consultant は、ユーザが IPsec を使用する場合（tunnel-protocol=4=IPSec）にのみアクセスが許可されます。

AD の一部である User=joe_consultant は、他のリモート アクセス クライアント（PPTP/L2TP、L2TP/IPSec、WebVPN/SVC など）では VPN アクセスに失敗します。

User=bill_the_hacker は、ユーザが AD メンバーシップではないため、許可されません。

7.「ログオン時間/Time-of-Day 規則」の Active Directory の強制

この使用例は、AD/LDAP 上の Time of Day 規則を設定し、強制する方法について説明しています。

これを行う手順を次に示します。

1. AD/LDAP サーバで次を実行します。ユーザを選択します。[> Properties] を右クリックします。属性を設定するために必要なタブを選択します（例： [General] タブ）。[Office] フィールドのような、時間範囲を適用するためのフィールド/属性を選択し、時間範囲の名前（たとえば、Boston）を入力します。 GUI 上の [Office] 設定は、AD/LDAP 属性 [physicalDeliveryOfficeName] に保存されます。

2. ASA 上で次を実行します。

   LDAP 属性マッピング テーブルを作成します。AD/LDAP 属性 [physicalDeliveryOfficeName] を ASA 属性 [Access-Hours] にマッピングします。

   例：

   ```
   B200-54(config-time-range)# show run ldap
   ldap attribute-map TimeOfDay
   map-name physicalDeliveryOfficeName Access-Hours
   ```

3. ASA で、LDAP 属性マップを aaa サーバ エントリと関連付けます。

   ```
   B200-54(config-time-range)# show runn aaa-server microsoft
   aaa-server microsoft protocol ldap
   aaa-server microsoft host audi-qa.frdevtestad.local
   ldap-base-dn dc=frdevtestad,dc=local
   ldap-scope subtree
   ldap-naming-attribute sAMAccountName
   ldap-login-password hello
   ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
   ldap-attribute-map TimeOfDay
   ```

4. ASA で、ユーザに割り当てられる名前値を持つ時間範囲オブジェクト（手順 1 の Office 値）を作成します。

   ```
   B200-54(config-time-range)# show runn time-range
   !
   time-range Boston
   periodic weekdays 8:00 to 17:00
   !
   ```

5. VPN リモート アクセス セッションを設定します。

   時間範囲内の場合、セッションは成功します。時間範囲外の場合、セッションは失敗します。

8. LDAP マップ設定を使用してユーザを特定のグループ ポリシーにマッピングし、二重認証の場合に authorization-server-group コマンドを使用する

1. このシナリオでは、二重認証が使用されます。 最初に使用される認証サーバは RADIUS で、2 番目に使用される認証サーバは LDAP サーバです。

   LDAP サーバと RADIUS サーバを設定します。 次に例を示します。

```
ASA5585-S10-K9# show runn aaa-server
aaa-server test-ldap protocol ldap
aaa-server test-ldap (out) host 10.201.246.130
 ldap-base-dn cn=users, dc=htts-sec, dc=com
 ldap-login-password *****
 ldap-login-dn cn=Administrator, cn=Users, dc=htts-sec, dc=com
 server-type microsoft
 ldap-attribute-map Test-Safenet-MAP
aaa-server test-rad protocol radius
aaa-server test-rad (out) host 10.201.249.102
 key *****
```

   LDAP 属性マップを定義します。 次に例を示します。

```
ASA5585-S10-K9# show runn ldap
ldap attribute-map Test-Safenet-MAP
map-name memberOf IETF-Radius-Class
map-value memberOf "CN=DHCP Users,CN=Users,DC=htts-sec,DC=com" Test-Policy-Safenet
```

   トンネル グループを定義し、認証のために RADIUS サーバと DAP サーバとを関連付けます。 次に例を示します。

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

   トンネル グループ設定で使用するグループ ポリシーを表示します。

```
ASA5585-S10-K9# show runn group-policy
group-policy NoAccess internal
group-policy NoAccess attributes
wins-server none
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 0
```

```
default-domain none
group-policy Test-Policy-Safenet internal
group-policy Test-Policy-Safenet attributes
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 15
vpn-idle-timeout 30
vpn-tunnel-protocol ikev1 ssl-client ssl-clientless
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Safenet-Group-Policy-SplitAcl
default-domain none
```

この設定では、LDAP 属性を使用して正しくマッピングされた AnyConnect ユーザに、グループ ポリシー、Test-Policy-Safenet が割り当てられませんでした。 代わりに、デフォルト グループ ポリシー（この場合は NoAccess）が設定されたままになっています。

デバッグ情報（debug ldap 255）の一部および情報レベルの syslog を参照してください。

```
--------------------------------------------------------------------------------

memberOf: value = CN=DHCP Users,CN=Users,DC=htts-sec,DC=com

[47]                        mapped to IETF-Radius-Class: value = Test-Policy-Safenet

[47]                        mapped to LDAP-Class: value = Test-Policy-Safenet

--------------------------------------------------------------------------------

Syslogs :

%ASA-6-113004: AAA user authentication Successful : server = 10.201.246.130 : user =
test123

%ASA-6-113003: AAA group policy for user test123 is being set to Test-Policy-Safenet

%ASA-6-113011: AAA retrieved user specific group policy (Test-Policy-Safenet) for user =
test123

%ASA-6-113009: AAA retrieved default group policy (NoAccess) for user = test123

%ASA-6-113013: AAA unable to complete the request Error : reason = Simultaneous logins
exceeded for user : user = test123

%ASA-6-716039: Group <DfltGrpPolicy> User <test123> IP <10.116.122.154> Authentication:
rejected, Session Type: WebVPN.
```

syslog から、ユーザが特定のグループ ポリシーを取得したにも関わらず、同時ログインが 0 に設定された NoAccess グループ ポリシーがユーザに割り当てられたため、エラーになったことがわかります。

ユーザが LDAP マップに基づいてグループ ポリシーに割り当てられるにはこのコマンドが必要です。 **authorization-server-group test-ldap**（この場合、**test-ldap** は LDAP サーバ名です）。 次に例を示します。

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
authorization-server-group test-ldap
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

2. ここで、最初の認証サーバ (この例では RADIUS) がユーザ固有の属性、たとえば IEFT クラス属性を送信した場合、ユーザは RADIUS によって送信されたグループ ポリシーにマッピングされます。 したがって、セカンダリ サーバに LDAP マップが設定されており、ユーザの LDAP 属性がユーザを異なるグループ ポリシーにマッピングする場合、最初の認証サーバによって送信されたグループ ポリシーが強制されます。

   LDAP マップ属性に基づいてユーザにグループ ポリシーを割り当てるためには、トンネル グループでこのコマンドを指定する必要があります。 authorization-server-group test-ldap.

3. 最初の認証サーバがユーザ固有の属性を通過させない SDI または OTP の場合、ユーザにはトンネル グループのデフォルトのグループ ポリシーが適用されます。 この場合、LDAP マッピングが正しい場合でも NoAccess となります。

   また、ユーザに正しいグループ ポリシーが割り当てられるためには、トンネル グループでコマンド authorization-server-group test-ldap が必要です。

4. サーバが両方とも同じ RADIUS サーバ、または LDAP サーバの場合、グループ ポリシー ロックが機能するために authorization-server-group コマンドは必要ありません。

確認

```
ASA5585-S10-K9# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : test123                 Index        : 2
Assigned IP  : 10.34.63.1              Public IP    : 10.116.122.154
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : 3DES 3DES 3DES          Hashing      : SHA1 SHA1 SHA1
Bytes Tx     : 14042                   Bytes Rx     : 8872
Group Policy : Test-Policy-Safenet     Tunnel Group : Test_Safenet
Login Time   : 10:45:28 UTC Fri Sep 12 2014
Duration     : 0h:01m:12s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                     VLAN         : none
```

トラブルシューティング

このセクションでは、設定のトラブルシューティングについて説明します。

LDAP トランザクションのデバッグ

これらのデバッグは、DAP 設定で問題を切り分けるために使用できます。

- debug ldap 255
- debug dap trace
- debug aaa authentication

ASA では LDAP サーバからユーザを認証できない

ASA が LDAP サーバからのユーザを認証できない場合のサンプル デバッグは次のとおりです。

```
ASA5585-S10-K9# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : test123                  Index        : 2
Assigned IP  : 10.34.63.1             Public IP    : 10.116.122.154
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : 3DES 3DES 3DES         Hashing      : SHA1 SHA1 SHA1
Bytes Tx     : 14042                  Bytes Rx     : 8872
Group Policy : Test-Policy-Safenet    Tunnel Group : Test_Safenet
Login Time   : 10:45:28 UTC Fri Sep 12 2014
Duration     : 0h:01m:12s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

このデバックでは、LDAP ログイン DN 形式が正しくないか、パスワードが間違っているかのいずれかなので、両方確認して問題を解決します。