# ASA 8.x:Windows用のAnyConnect SSL VPN CACスマートカードの設定

内	容
<u>はじ≀</u>	<u> かに</u>
<u>前提</u>	<u>条件</u>
要	性
<u>使</u>	<u>用するコンポーネント</u>
<u>Ciscc</u>	<u>ASA の設定</u>
<u> </u>	<u>入に関する考慮事項</u>
認証、	<u>許可、アカウンティング(AAA)設定</u>
	<u>IAP サーバの設定</u>
<u>証明</u>	<u>書の管理</u>
土	<u>一の生成</u>
<u>ル</u>	ート CA 証明書のインストール
<u>A</u> S	A の登録と ID 証明書のインストール
<u>AnyC</u>	<u>onnect VPN の設定</u>
<u>IP</u>	<u>アドレス プールの作成</u>
F	<u>ンネル グループおよびグループ ポリシーの作成</u>
F	ンネル グループ インターフェイスおよびイメージの設定
証	明書の照合ルール(OCSP が使用される場合)
<u>OCS</u>	<u>この設定</u>
<u>0</u> 0	CSP レスポンダ証明書の設定
<u>0</u> 0	<u>CSP を使用するための CA の設定</u>
<u>0</u> 0	CSP ルールの設定
<u>Ciscc</u>	<u>AnyConnect Client の設定</u>
<u>Ci</u>	sco Anyconnect VPN Client のダウンロード - Windows
<u>Ci</u>	sco Anyconnect VPN Client の起動 - Windows
<u>新</u>	<u>規接続</u>
<u>U</u>	モート アクセスの開始
<u>付録</u>	A:LDAP マッピングおよび DAP
<u>シ</u> 許	ナリオ1:リモートアクセス許可ダイヤルインを使用したActive Directoryの強制:アクセスの <u>可/拒否</u>
<u>Ac</u>	tive Directory の設定
<u>A8</u>	<u>A の設定</u>
<u>シ</u> 用	ナリオ2:グループメンバーシップを使用したアクセスの許可/拒否によるActive Directoryの適
<u>Ac</u>	tive Directory の設定
<u>A</u> 8	A の設定
シ	ナリオ3:複数のmemberOf属性のダイナミックアクセスポリシー
<u>A</u> S	<u>A の設定</u>

 付録 B: ASA CLI 設定

 付録 C: トラブルシューティング

 AAA および LDAP のトラブルシューティング

 例1: 正しい属性マッピングを使用した接続の許可

 例2: 誤って設定されたCisco属性マッピングによる接続の許可

 DAP のトラブルシューティング

 例1:DAPで許可される接続

 例2:DAPとの接続の拒否

 認証局および OCSP のトラブルシューティング

 付録 D: MS 内の LDAP オブジェクトの確認

 LDAP Viewer

 Active Directory サービス インターフェイス エディタ

 付録 E

 関連情報

## はじめに

このドキュメントでは、認証用の Common Access Card(CAC)を使用して Windows 用の AnyConnect VPN リモート アクセスを実現する、Cisco 適応型セキュリティ アプライアンス (ASA)上でのサンプル設定について説明します。

このドキュメントでは、Cisco ASA と Adaptive Security Device Manager (ASDM)、Cisco AnyConnect VPN Client、Microsoft Active Directory (AD) および Lightweight Directory Access Protocol (LDAP)の設定について扱います。

このガイドの設定では、Microsoft AD および LDAP サーバを使用します。またこのドキュメント では、OCSP、LDAP 属性マップ、ダイナミック アクセス ポリシー(DAP)などの高度な機能に ついても扱います。

### 前提条件

### 要件

Cisco ASA、Cisco AnyConnect Client、Microsoft AD/LDAP、および公開キー インフラストラク チャ(PKI)についての基本的な理解があれば、完全な設定を理解するために有益です。AD グル ープ メンバシップ、ユーザ プロパティ、および LDAP オブジェクトについて理解していれば、 証明書属性と AD/LDAP オブジェクトの間での許可プロセスの関連付けに役立ちます。

### 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いています。

- ・ ソフトウェア バージョン 8.0(x) 以降が稼働する Cisco 5500 シリーズ適応型セキュリティ アプライアンス(ASA)
- ・ ASA 8.x 用の Cisco Adaptive Security Device Manager (ASDM) バージョン 6.x

• Cisco AnyConnect VPN Client (Windows 版)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在 的な影響について確実に理解しておく必要があります。

### Cisco ASA の設定

このセクションでは、ASDM を使用した Cisco ASA の設定について扱います。ここでは、SSL AnyConnect 接続を経由した VPN リモート アクセス トンネルを配備するために必要なステップ について説明します。認証には CAC 証明書が使用され、証明書内のユーザ プリンシパル名 (UPN)属性が、許可のために Active Directory に取り込まれます。

#### 導入に関する考慮事項

 このガイドでは、インターフェイス、DNS、NTP、ルーティング、デバイス アクセス、 ASDM アクセスなどの基本的な設定については扱いません。ネットワーク オペレータはこ れらの設定をよく理解しているものとします。

|詳細は、『<u>マルチファンクション セキュリティ アプライアンス</u>』を参照してください。

- 赤色で強調表示されているセクションは、基本的な VPN アクセスのために必要な必須の設定です。たとえば、VPN トンネルは CAC カードで設定でき、OCSP チェック、LDAP マッピング、ダイナミック アクセス ポリシー(DAP)チェックを行う必要はありません。DoDでは OCSP チェックが規定されていますが、OCSP を設定しなくてもトンネルは機能します。
- ・ 青色で強調表示されているセクションは、設計にセキュリティを追加するために含めること ができる高度な機能です。
- ASDM と AnyConnect/SSL VPN は、同じインターフェイスの同じポートを使用できません。 一方または他方のポートを変更してアクセスすることを推奨します。たとえば、ASDM をポート 445 にし、AC/SSL VPN は 443 のままにします。ASDM への URL アクセスは、 8.x で変更されました。https://<ip\_address>:<port>/admin.html を使用してください。
- ・ 必要な ASA イメージは最低 8.0.2.19 で、ASDM 6.0.2 です。
- AnyConnect/CAC は Vista でサポートされています。
- ポリシーを強制するための LDAP およびダイナミック アクセス ポリシーのマッピングの例
   については、<u>付録 A を参照してください。</u>
- ・ LDAPオブジェクトをMSでチェックする方法については、「<u>付録D</u>」を参照してください。
- ファイアウォール設定のためのアプリケーション ポートのリストについては、『<u>関連情報</u> 』を参照してください。

## 認証、許可、アカウンティング(AAA)設定

Common Access Card (CAC)内の証明書の使用は、DISA 認証局(CA)サーバまたは自分の組織の CA サーバを通じて認証されます。証明書はネットワークへのリモート アクセス用に有効である必要があります。認証に加えて、Microsoft Active Directory または Lightweight Directory Access Protocol (LDAP)の使用が許可されている必要もあります。米国国防総省(DoD)では、ユーザ プリンシパル名(UPN)属性を許可用に使用することを求めていますが、これは証明書の Subject Alternative Name (SAN)セクションの一部です。UPN または EDI/PI は、1234567890@mil のフォーマットである必要があります。これらの設定では、ASA 内の AAA サーバを LDAP サーバと一緒に許可用に構成する方法を示しています。LDAP オブジェクト マッピングの追加の設定については、付録 A を参照してください。

LDAP サーバの設定

次のステップを実行します。

- 1. [Remote Access VPN] > [AAA Setup] > [AAA Server Group] を選択します。
- 2. AAA サーバ グループ テーブルで、[Add 3] をクリックします。
- サーバ グループ名を入力し、プロトコル オプション ボタンで [LDAP] を選択します。図 1 を参照してください。
- 4. 選択されたグループ テーブルで、[Add] をクリックします。作成したサーバが前のテーブル で強調表示されていることを確認します。
- 5. AAA サーバの編集ウィンドウで、次の手順を実行します。図 2 を参照してください。

注:このタイプの接続にLDAP/ADが設定されている場合は、Enable LDAP over SSLオプションを選択します。

- a. LDAP が配置されるインターフェイスを選択します。このガイドでは、インターフェ イスの内側であることを示しています。
- b. サーバの IP アドレスを入力します。
- c. [Server Port] を入力します。デフォルトの LDAP ポートは 389 です。
- d. [Server Type] を選択します。
- e. [Base DN] を入力します。これらの値は AD/LDAP 管理者に問い合わせてください。

🕵 Add AAA Serve	r Group	<u> </u>
Configure an AAA se for RADIUS and TAC	rver group. The Ac ACS+ protocols.	counting Mode attribute is only applicable
Server Group:	AD-LDAP	
Protocol:	LDAP	
Accounting Mode:	C Simultaneous	() Single
Reactivation Mode:	<ul> <li>Depletion</li> </ul>	🔿 Timed
Dead Time: 10	minul	tes
Max Failed Attempts:	3	
_		

- f. [Scope] オプションで、該当する回答を選択します。これはベース DN によって異なります。AD/LDAP 管理者に連絡して支援を求めてください。
- g. [Naming Attribute] に、userPrincipalName と入力します。これは AD/LDAP サーバ内 でユーザ許可に使用する属性です。
- h. [Login DN] に管理者 DN を入力します。

注:ユーザには、ユーザオブジェクトとグループメンバーシップを含むLDAP構造を表示または検索する管理者権限または権限があります。

- i. [Login Password] に管理者のパスワードを入力します。
- j. LDAP 属性は [None] のままにします。

#### 図 2

## 🛸 Add AAA Server

Server Group:		AD-LDAP		
Interface Name:		outside	~	
Server Name or IP Addr	ess:	172.18.120.160		
Timeout:		10		seconds
LDAP Parameters				
Enable LDAP over	r SSL			
Server Port:	389			
Server Type:	D6	etect: Automatically/Use Generic: Type 😒		
Base DN:	CN=	Users,DC=ggsgseclab,DC=org		
Scope:	One	level beneath the Base DN		
Naming Attribute(s):	user	PrincipalName	]	
Login DN:	Iminis	strator, CN=Users, DC=ggsgseclab, DC=org	]	
Login Password:		•••••		
LDAP Attribute Map:	No	one 🛛 👻		
SASL MD5 auther	nticati	n		
5ASL Kerberos au	uthent	ication		

X

注:このオプションは、後で設定で使用して、認可のために他のAD/LDAPオブ ジェクトを追加します。

k. [OK] を選択します。

6. [OK] を選択します。

## 証明書の管理

ASA に証明書をインストールするには、2 つのステップがあります。最初に、必要な CA 証明書

(ルートおよび追加の認証局)をインストールします。次に、ASA を特定の CA に登録し、ID 証 明書を取得します。DoD PKI では、Root CA2、Class 3 Root、ASA の登録先の CA## 中間証明書 、ASA ID 証明書、および OCSP 証明書を使用します。ただし OCSP を使用しない場合は、 OCSP 証明書をインストールする必要はありません。

注:ルート証明書と、デバイスのID証明書の登録方法を取得するには、セキュリティ POCに連絡してください。ASA のリモート アクセスの場合、SSL 証明書で十分です。デュ アル SAN 証明書は必要ありません。

注:ローカルマシンにもDoD CAチェーンがインストールされている必要があります。証明 書は Internet Explorer を使用して Microsoft 証明書ストアから表示できます。DoD は、すべ ての CA を自動的にマシンに追加するバッチ ファイルを提供しています。詳細については 、お客様の PKI POC にお問い合わせください。

注:ユーザ認証に必要なCAは、DoD CA2とクラス3のルート、およびASA証明書を発行し たASA IDとCA中間証明書のみです。現行のすべての CA 中間証明書は CA2 および Class 3 Root チェーンに該当するため、CA2 および Class 3 Root が追加される限り信頼されます。

キーの生成

次のステップを実行します。

- 1. [Remote Access VPN] > [Certificate Management] > [Identity Certificate] > [Add] を選択します。
- 2. [Add a new id certificate] を選択し、キー ペア オプションの [New] を選択します。
- [Add Key Pair] ウィンドウで、キー名に DoD-1024 と入力します。新しいキーを追加するオ プション ボタンをクリックします。図 3 を参照してください。

図 3

🚰 Add Key Pair	
Name: 🔘 Use default key pair name	
Enter new key pair name:	DoD-1024
Size: 1024	

- 4. キーのサイズを選択します。
- 5. [Usage] は [General Purpose] のままにします。
- 6. [Generate Now] をクリックします。

注: DoDルートCA 2は2048ビットキーを使用します。この CA を使用できるようにす るには、2048 ビットのキー ペアを使用する 2 番目のキーを生成する必要があります 。上記の手順を使用して、2 番目のキーを追加してください。

ルート CA 証明書のインストール

次のステップを実行します。

- 1. [Remote Access VPN] > [Certificate Management] > [CA Certificate] > [Add] を選択します。
- 2. [Install from File] を選択し、証明書を参照します。
- 3. [Install Certificate] を選択します。
  - 図4:ルート証明書のインストール

🖆 Install Certificate		
<ol> <li>Install from a file:</li> </ol>	C:\CAC\DOD-CERTS\ca13-jitc.cer	Browse
🔘 Paste certificate in	PEM format:	
O Use SCEP:		
SCEP URL: http://		
Retry Period:	1	minutes
Retry Count:	0	(Use 0 to indicate unlimited retries)
		More Options
Install Cer	tificate Cancel	Help

4. このウィンドウが表示されます。図5を参照してください。

図5:

🕵 CA Cert	ificate Installation 🛛 🔀
¢	CA certificate installed successfully.
	OK

注:インストールするすべての証明書について、手順1 ~ 3を繰り返します。DoD PKIでは、ルートCA 2、クラス3ルート、CA##中間、ASA ID、およびOCSPサーバの それぞれの証明書が必要です。OCSP を使用しない場合、OCSP 証明書は不要です。

図6:ルート証明書のインストール

conntr. Access VPN 🚊 🗸 🔬	Configuration > Report	e Access VPN > Certificate Man	agement > EA Certificates	
Ketwork (Client) Access				
The cleases size in the case	Issued To	Issued By	ExcityDate Usage	ard
🔏 Secure Deskud Manager 🔝 Kosträcete Monogeniest	DeD CLAST CA 2 DeD CLAST 0 Poet CA	[arroub Root CA2, LarPH, La [m=0:1001 ASS - Root ( Ayo)= 100	15:01:10 UTC Signature DB1-90100C General Purpose	th I
CA Callitates	DOD JITE CA-13	[ui=010 0010 Rol( CA 2; lu≓PK0	C2:55:53.UTC Signature	how set
				Req esta
The local Telencing				Delete
Advanced				
Dev ca Set_p				

ASA の登録と ID 証明書のインストール

- 1. [Remote Access VPN] > [Certificate Management] > [Identity Certificate] > [Add] を選択します。
- 2. [Add a new id certificate] を選択します。
- 3. DoD-1024 キーペアを選択します。図7を参照してください。

### 図7:ID証明書のパラメータ

🛸 Add Identity Certificat	e	
O Import the identity certif	icate from a file:	
Decryption Passphrase:		
File to Import From:		Browse
<ul> <li>Add a new identity certif</li> </ul>	icate:	
Key Pair:	DoD-1024	Show New
Certificate Subject DN:		Select
Generate self-signed	certificate	
Act as local certif	icate authority and issue dynamic ce	rtificates to TLS-Proxy
		Advanced
Add Certifi	cate Cancel	Help

- 4. [Certificate Subject DN] ボックスに移動し、[Select] を選択します。
- 5. [Certificate Subject DN] ウィンドウで、デバイスの情報を入力します。図 8 の例を参照して ください。

図8:DNの編集

DN Attribute to be Added       Add>>>       Attribute       Value       Common Name (CN)       asa80         Attribute:       Select Attribute        Add>>>       Department (OU)       PKI         Value:       Delete       Delete       Company Name (O)       U.S. Government	Certificate Sul	oject DN			
DN Attribute to be Added       Common Name (CN)       asa80         Attribute:       Select Attribute        Add>>>       Department (OU)       PKI         Value:       Delete       Department (OU)       DoD         Company Name (O)       U,S. Government         Company Name (O)       U,S. Government         Country (C)       US				Attribute	Value
Attribute:     Select Attribute Y       Value:     Delete         Delete   Department (OU) PKI Department (OU) DoD Company Name (O) U.S. Government Country (C) US	Distantial and			Common Name (CN)	asa80
Attribute:       Select Attribute Y       Add>>       Department (OU)       DoD         Value:       Delete       Delete       Company Name (O)       U.S. Government         Country (C)       US	DN Attribute t	o be Added		Department (OU)	PKI
Value:     Delete     Company Name (O)     U.S. Government.       Country (C)     US	Attribute:	Select Attribute 🔽	Add>>	Department (OU)	DoD
Value: Delete Country (C) US	United I			Company Name (O)	U.S. Government
	value;		Delete	Country (C)	US
			Delete	Country (C)	US

6. [OK] を選択します。

注:サブジェクトDNを追加するときは、システムに設定されているデバイスのホスト 名を使用していることを確認してください。必須フィールドについては PKI POC か ら聞き取ることができます。

- 7. [Add Certificate] を選択します。
- 8. 要求を保存するディレクトリを選択するには、[Browse] をクリックします。図 9 を参照し てください。

図9:証明書要求

🖾 Identity Certificate Request	
To complete the enrollment process, please save the PKCS10 enrollment request (CSR) and send it to the CA.	
You will then need to install the certificate that is returned from the CA by	

9. ファイルを WordPad で開き、適切なドキュメントに要求をコピーして、お客様の PKI POC に送信します。図 10 を参照してください。

図10:登録要求



10. CA 管理者から証明書を受け取ったら、[Remote Access VPN] > [Certificate Management] > [ID Certificate] > [Install] を選択します。図 11 を参照してください。

図11:ID証明書のインポート

2 <b>2 2 2 2 2 2 2</b> 2 2 2 2 2 2 2 2 2 2 2	PE (PE (PE )	10 7 B 10 7	er. er. 1
Second Sec.		202	
	and and the		



Starting IP Address:	192 168 1 1
	172,100,1,1
Ending IP Address:	192,168.1,254
Subnet Mask:	255.255.255.0

11. 証明書のインストール ウィンドウで、ID 証明書を参照し、[Install Certificate] を選択します 。図 12 の例を参照してください。

図12:ID証明書のインストール

🚰 Install Identity ce	rtificate 🔀
Identity Certificate	
<ul> <li>Install from a file:</li> </ul>	C:\CAC\DOD-CERTS\asa80.txt Browse
Paste the certificat	e data in base-64 format:
Install Cert	tificate Cancel Help

注:発行された証明書とキーペアを保存するために、ID証明書トラストポイントをエ クスポートすることをお勧めします。これによって ASA 管理者は、RMA またはハー ドウェア障害の場合に証明書およびキー ペアを新しい ASA にインポートすることが できます。詳細は、『<u>トラストポイントのエクスポートおよびインポート</u>』を参照し てください。

注:フラッシュメモリに設定を保存するには、SAVEをクリックします。

### AnyConnect VPN の設定

ASDM で VPN パラメータを設定するには 2 つのオプションがあります。最初のオプションは SSL VPN ウィザードを使用することです。これは VPN 設定が初めてのユーザにとって、使いや すいツールです。2 つ目のオプションは、手動で各オプションを設定することです。この設定ガ イドでは、手動による方法を使用します。

注:ACクライアントをユーザに提供する方法は2つあります。

1. Cisco の Web サイトからクライアントをダウンロードし、マシンにインストールすること ができます。

2. Web ブラウザ経由で ASA にアクセスすると、クライアントをダウンロードできます。

注:たとえば、<u>https://asa.test.com</u>です。このガイドでは 2 番目の方法を使用します。AC クライアントがクライアント マシンに完全にインストールされたら、AC クライアントをア プリケーションから起動します。 IP アドレス プールの作成

DHCP などの他の方法を使用する場合、これはオプションです。

- 1. [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools] を選択します。
- 2. [Add] をクリックします。
- 3. [Add IP Pool] ウィンドウで、IP プールの名前、開始および終了 IP アドレスを入力し、サブ ネット マスクを選択します。図 13 を参照してください。

図13:IPプールの追加

🛸 Add IP Pool	
	· · · · · · · · · · · · · · · · · · ·
Name:	CAC-USERS
Starting IP Address:	192.168.1.1
Enaing IP Adaress:	192,168,1,254
Subnet Mask:	255.255.255.0
ΟΚ	Cancel Help

- 4. [OK] を選択します。
- 5. [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy] を選択します。

適切な IP アドレス割り当て方法を選択します。このガイドでは、内部アドレス プールを使用します。図 14 を参照してください。

図14:IPアドレス割り当て方法



7. [APPLY] をクリックします。

### トンネル グループおよびグループ ポリシーの作成

グループ ポリシー

注:新しいポリシーを作成しない場合は、デフォルトの組み込みグループポリシーを使用で きます。

- 1. [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。
- 2. [Add] をクリックして、[Internal Group Policy] を選択します。
- 3. [Add Internal Group Policy] ウィンドウで、[Name] テキスト ボックスにグループ ポリシー の名前を入力します。図 15 を参照してください。

図15:内部グループポリシーの追加

General	Name: A	C-USERS					
Advanced	Banner:	Inherit					
	Address Pools: [	Inherit	CAC-USE	ণ্ড			Select
	More Options	More Options					
	Tunneling Proto	cols: [	🗌 Inherit	Clientless SSL VPN	SSL VPN Client	IPsec	L2TP/IPsec
	Filter:	[	🗹 Inherit				Manage
	NAC Policy:	[	🖌 Inherit			×.	Manage
	Access Hours:	[	🖌 Inherit			2	Manage
	Simultaneous Lo	gins: [	🗹 Inherit				
	Restrict access	to VLAN: [	Inherit				
	Maximum Conne	ect Time: [	🖌 Inherit	Unimited	mnutes		
	Ide Timeout:	[	🔽 Inherit	Unimited	mnubes		

- a. [General] タブの [Tunneling Protocols] で [SSL VPN Client] オプションを選択します (Clientless SSL などの他のプロトコルを使用しない場合)。
- b. [Servers] セクションで、[inherit] チェック ボックスのチェックを外し、DNS サーバお よび WINS サーバの IP アドレスを入力します。該当する場合は DHCP の範囲を入力 します。
- c. [Servers] セクションで、デフォルト ドメインの [inherit] チェック ボックスを選択解 除し、適切なドメイン名を入力します。
- d. [General] タブで、アドレス プール セクションの [inherit] チェックを選択解除し、前 の手順で作成されたアドレス プールを追加します。IP アドレス割り当てに別の方法を 使用する場合、これを [inherit] のままにして、適宜変更します。
- e. 他のすべての設定タブは、デフォルト設定のままにします。

注:エンドユーザにACクライアントを提供する方法は2つあります。1 つの方法 は、Cisco.com にアクセスして AC クライアントをダウンロードすることです。 別の方法は、ユーザが接続を試行したときに ASA でクライアントをユーザにダ ウンロードすることです。この例では後者の方法を示します。

4. 次に、[Advanced] > [SSL VPN Client] > [Login Settings] を選択します。図 16 を参照してく ださい。

#### 図16:内部グループポリシーの追加

🛸 Edit Internal Group Pol	icy: AC-USERS
General Servers Advanced Split Tunneling IE Browser Proxy SSL VPN Client Cogn Secting Key Regeneration Dead Peer Detecti - Customization I - IPsec Client	After successfully logging in, user can have the choice to download the client software, or go to clientless SSL VPN partal page. The following settings decides what will happen. Inherit Post Logn Setting O to not prompt user to choose User has seconds to choose, or Default Post Login Selection below is tolker: Default Post Login Selection Go to Clientless SSL VPN portal O bownload SSL VPN Client
	OK Cancel Help

- a. [Inherit] チェックボックスを選択解除します。
- b. [Post Login Setting] は、ご使用の環境に合ったほうを選択します。
- c. [Post Login Selection] は、ご使用の環境に合ったほうを選択します。
- d. [OK] を選択します。

### トンネル グループ インターフェイスおよびイメージの設定

注:新しいグループを作成しない場合は、デフォルトの組み込みグループを使用できます。

- 1. [Remote Access VPN] > [Network (Client) Access] > [SSL VPN Connection Profile] を選択します。
- 2. [Enable Cisco AnyConnect Client.....]を選択します。
- 3. [Would you like to designate an SVC image?]という質問を示すダイアログ ボックスが表示 されます。
- 4. [Yes] を選択します。

5. 画像がすでに存在する場合、Browse Flash で使用する画像を選択します。画像が使用できない場合、[Upload] を選択してローカル コンピュータ上のファイルを参照します。図 17 を参照してください。ファイルはCisco.comからダウンロードできます。Windows、MAC、およびLinuxのファイルがあります。

図17:SSL VPNクライアントイメージの追加

🛸 Add SSL VPN Client Image	
Flash SVC Image:	Browse Flash
	Upload

6. 次に、[Allow Access]、[Require Client Cert] をオンにし、オプションで [Enable DTLS] をオ ンにします。図 18 を参照してください。

図18:アクセスの有効化

🛍 Cisco ASDM 6.0 for ASA - 17	2.18.120.225				
File View Tools Wigards Windo	w Help Yonitoring 🔛 Save -	🕞 Refresh 🔇	Look For: Back OF Forward ? Help	And +	ahaha cisco
Remote Access V 🗗 🗘 🗙	Configuration > Ren	note Access VPN	> Network (Client) Access > S	SL VPN Connectio	n Profiles 🛛
Network (Client) Access     SSL VPN Connection Profiles     IPsec Connection Profiles     Group Policies	The security applian users upon connecti VPN Client supports	ce automatically dep ion. The initial client i the HTTPS/TCP (SSL	lays the Osco AnyConnect VPN Cler deployment requires end-user admin .) and Datagram Transport Layer Ser	nt or legacy SSL VPN C istrative rights. The C curity (DTLS) tunneling	Jient to remote isco AnyConnect 3 options.
Address Assignment     Assignment Policy	(More client-related	i parameters, such a	s client images and client profiles, ca	n be found at <u>client s</u>	ettinos.)
IP Address Pools	Access Interfaces —				
Clentless SSL VPN Access	C Enable Cisco An	yConnect VPN Client	or legacy SSL VPN Client access on I	the interfaces selecte	d in the table below
Connection Profiles	Interface	Allow Access	Require Client Certificate	Enable DTLS	
	outside	2		<u></u>	
S Device Setup					
Frewall	1	-			
Remote Access VPN	Access Fort: 445	DICSPO	Jrt: [443]		
Ste-to-Site VPN	Click nere to Assure	Certricate to Intern	305,		
Device Management	Connection Profiles				
?			ADDIY Keset	0.00.000	
Configuration changes saved successful	<i>w.</i>	CISCO	15 🐻 🌌 🖡	101	23/07 2:09:48 AM UTC

- 7. [APPLY] をクリックします。
- 8. 次に、接続プロファイルおよびトンネル グループを作成します。[Remote Access VPN] > [Network (Client) Access] > [SSL VPN Connection Profile] を選択します。
- 9. [Connection Profiles] セクションで、[Add] をクリックします。

図19:接続プロファイルの追加

E	Add SSL VPN Connecti	on Profile		X
	Basic	Name:	AC-USERS	
	H-Advanced	Aliases:		
		Authentication		
		Method:	◯ AAA ④ Certificate ◯ Both	
		AAA Server Group:	LOCAL	Manage
			Use LOCAL if Server Group Fails	
		Client Address Assignent		
		DHCP Servers:		
		Client Address Pools:		Select
		Default Group Policy		
		Group Policy:	AC-USER5	Manage
		SSL VPN Client Protocol:	C Enabled	
		OK	Cancel Help	

a. グループに名前を付けます。

- b. 認証方法で [Certificate] を選択します。
- c. 以前作成したグループポリシーを選択します。
- d. [SSL VPN Client] がオンになっていることを確認します。
- e. 他のオプションはデフォルトのままにします。
- 10. 次に、[Advanced] > [Authorization] を選択します。詳細については、図 20 を参照してくだ さい。

図20:許可

🖆 Edit SSL VPN Connecti	on Profile: AC-USERS			
Basic	Default Authorization Server	Group		
General	Server Group: AD-LDAP		Manage	
Client Addressing     Authentication     Authorization     Accounting	Users n	nust exist in the auth	orization database to connect	
Accounting SSL VPN	💠 Add 🛒 Edt 👔 De	lete		
	Interface		Server Group	
	Licer Name Married			
	O Use the entire DN as t	he username		
	<ul> <li>Specify individual DN f</li> </ul>	ields as the username	,	
	Primary DN Field:	UPN (User's Principal I	Name)	
	Secondary DN Field:	- None	×	
	ОК	Cancel	Help	

- a. 以前作成した AD-LDAP グループを選択します。
- b. [Users must exist....to connect] にチェックマークを付けます。
- c. マッピング フィールドで、プライマリについては [UPN] を、セカンダリについては [None] を選択します。
- 11. メニューから [SSL VPN] セクションを選択します。
- 12. [Connection Aliases] セクションで、次の手順を実行します。

図21:接続エイリアス

🖆 Edit SSL VPN Connecti	on Profile: AC-USERS					
Basic	Portal Page Customization:	DfltCustomization	Manage			
General	CSD Alternate Group Policy:	DfltGrpPolicy	Manage			
Client Addressing Authentication	Enable the display of Radius Reject-Message on the login screen when authentication is rejected					
Accounting	Connection Aliases					
SSL VPN	💠 Add 🖪 Delete					
	Alias	Enabled				
	AC-USERS	✓				
	Group URLs					
	💠 Add 📷 Delete					
	URL	Enabled				
	ОК	Cancel Help				

a. [Add] を選択します。

- b. 使用するグループ エイリアスを入力します。
- c. [Enabled] にチェックマークが付いていることを確認します。図 21 を参照してください。

13. [OK] をクリックします。

注:フラッシュメモリに設定を保存するには、Saveをクリックします。

証明書の照合ルール(OCSP が使用される場合)

- 1. [Remote Access VPN] > [Advanced] > [Certificate to SSL VPN Connection Profile Maps] を 選択します。図 22 を参照してください。
  - a. [Certificate to Connection Profile Maps] セクションで [Add] を選択します。
  - b. [Map] セクションでは、既存のマップを DefaultCertificateMap として保持するか、あ るいは IPsec 用の証明書マップをすでに使用している場合は新しいマップを作成する ことができます。
  - c. ルールのプライオリティはそのままにします。

d. マップ対象グループは、[-- Not Mapped --] のままにします。図 22 を参照してください。

図22:証明書照合ルールの追加

rule and associate e certificate matc ing greater priorit	e it with a connection profile. The hing rule and assigns a priority :y. Rules that are not mapped
Existing	DefaultCertificateMap 🛛 🖌
) New	
20	
- Not Mapped	· · · · · · · · · · · · · · · · · · ·
(massion)	
	rule and associate e certificate matc ing greater priorit Existing New O - Not Mapped

e. [OK] をクリックします。

- 2. 下の表にある [Add] をクリックします。
- 3. [Add Certificate Matching Rule Criterion] ウィンドウで、次の手順を実行します。

図23:証明書照合ルールの基準

Choose a	<b>digital certificate</b> ation The Web site you want b	o view requests	? 🗙
	Name POOLE.JUSTIN.ALLE MCGINTY.JIMMY.11 POOLE.JUSTIN.ALLE MCGINTY.JIMMY.11	ose a certificate. Issuer DOD CLASS 3 EMAIL CA-10 DOD JITC CA-15 DOD CLASS 3 CA-10 DOD JITC EMAIL CA-15	
	Mo	re Info View Certifical	te

- a. [Field] カラムは [Subject] のままにします。
- b. [Component] カラムは [Whole Field] のままにします。
- c. [Operator] カラムを [Does Not Equal] に変更します。
- d. [値]列に2つの二重引用符""を入力します。
- e. [OK] および [Apply] をクリックします。図 23 の例を参照してください。

### OCSP の設定

OCSP の設定はさまざまであり、OCSP レスポンダ ベンダーによって異なります。詳細は、ベン ダーのマニュアルをお読みください。

OCSP レスポンダ証明書の設定

1. OCSP レスポンダから自己生成された証明書を取得します。

2. 以前説明した手順を実行して、OSCP サーバの証明書をインストールします。

注:OCSP証明書のトラストポイントで、Do not check certificates for revocationが選 択されていることを確認します。

OCSP を使用するための CA の設定

- 1. [Remote Access VPN] > [Certificate Management] > [CA Certificate] を選択します。
- 2. OCSP を使用するように CA を設定するために、OCSP を強調表示します。
- 3. [Edit] をクリックします。
- 4. [Check certificate for revocation] がチェックされていることを確認します。
- 5. [Revocation Methods] セクションで、OCSP を追加します。図 24 を参照してください。

OCSP 失効チェック

Revocation Check	CDI Debrieusl Delicu	CDL Detrieval Method	OCCD Dulas	Adusteed	
torocadori cricer	CRE Retrieval Pulicy	CRE Recrieval Metriou	OC3P Rules	Auvanceu	
O Do not check	certificates for revocal	tion			
• Check certifica	ates for revocation				
Revocation Me	ethods				
Specify the method will	methods used for revo be used only if the firs	cation checking and the t one returns error.	ir order. If bo	th methods are sel	ected, the second
CRL		Add>>	CSP		Move Up
		< <remove< td=""><td></td><td></td><td>Move Down</td></remove<>			Move Down
Conside	r certificate valid if rev	ocation information can	not be retriev	ed	

6. 厳密な OCSP チェックを行う場合、[Consider Certificate valid…cannot be retrieved] のチェ ックマークを外してください。 OCSP ルールの設定

注:次の手順を実行する前に、証明書グループ照合ポリシーが作成されていること、および OCSPレスポンダが設定されていることを確認します。

注:一部のOCSP実装では、DNSのAおよびPTRレコードがASAに必要になる場合がありま す。このチェックは、ASA が .mil のサイトからのものであることを確認するために実行さ れます。

- 1. [Remote Access VPN] > [Certificate Management] > [CA Certificates 2] を選択します。
- 2. OCSP を使用するように CA を設定するために、OCSP を強調表示します。
- 3. [Edit] を選択します。
- 4. [OCSP Rule] タブをクリックします。
- 5. [Add] をクリックします。
- 6. [Add OCSP Rule] ウィンドウで、次の手順を実行します。図 25 を参照してください。

図25:OCSPルールの追加

🕵 Add OCSP I	Rule	
Certificate Map:	DefaultCertificateMap	~
Certificate:	[cn=OCSP, ou=AMHS, o=Army, c=us]:[cn=OCSP, ou=AMHS	×

- a. [Certificate Map] オプションで、[DefaultCertificateMap] を選択するか、以前作成した マップを選択します。
- b. [Certificate] オプションで、[OCSP responder] を選択します。
- c. [Index] オプションに、10 と入力します。

- d. [URL] オプションに、OCSP レスポンダの IP アドレスまたはホスト名を入力します。 ホスト名を使用する場合、ASA に DNS サーバが設定されていることを確認します。
- e. [OK] をクリックします。
- f. [APPLY] をクリックします。

### Cisco AnyConnect Client の設定

このセクションでは、Cisco AnyConnect VPN Client の設定について扱います。

前提条件:Cisco AnyConnect VPN ClientおよびミドルウェアアプリケーションがホストPCにすで にインストールされている。ActivCard Gold および ActivClient がテスト済みである。

注:このガイドでは、ACクライアントの初期インストールにのみグループURL方式を使用 します。AC クライアントのインストールが済んだら、IPsec クライアントと同じように AC アプリケーションを起動します。

注:DoD証明書チェーンはローカルマシンにインストールする必要があります。PKI POC に 問い合わせて証明書またはバッチ ファイルを取得してください。

Cisco Anyconnect VPN Client のダウンロード - Windows

- 1. Internet Explorer 経由で ASA への Web セッションを起動します。アドレスは https://Outside-Interface という形式になります。たとえば、https://172.18.120.225 と指定 します。
- 2. アクセスに使用する署名証明書を選択します。図 26 を参照してください。

図26:正しい証明書の選択

Choose a Identific	digital certificate ation The Web site you want t identification. Please cho	o view requests ose a certificate.
	Name POOLE.JUSTIN.ALLE MCGINTY.JIMMY.11 POOLE.JUSTIN.ALLE MCGINTY.JIMMY.11	Issuer DOD CLASS 3 EMAIL CA-10 DOD JITC CA-15 DOD CLASS 3 CA-10 DOD JITC EMAIL CA-15
	Mc	ore Info View Certificate OK Cancel

3. プロンプトが表示されたら、PIN を入力します。

図27:暗証番号の入力

ActivCa	ard Gold - Enter	PIN
	Enter PIN code:	
	OK	Cancel

- 4. [Yes] を選択してセキュリティ警告に同意します。
- 5. SSL ログイン ページで、[Login] を選択します。クライアント証明書がログインに使用され ます。図 28 を参照してください。

図28:SSLログイン

SSL VPN Service - Microsoft Internet Explorer provided by Cisco Systems, Inc.		
Ele Edit yew Fgyorites Tools Help		: 🍂
🔾 Back 🔹 🜍 🔹 📓 ổ 🔎 Search 🤺 Favorites 🧭 🍰 🖉 🔛 💭	18	
Address a https://172.18.120.225/+CSCOE+/lagon.html	🖌 🄁 😡	unis 🎽 📆 🔹
CISCO SSL VPN Service		

6. AnyConnect はクライアントのダウンロードを開始します。図 29 を参照してください。

図29:AnyConnectのインストール

Installation - Microsoft Internet Explorer prov	rided by Cisco Systems , Inc.	
Ble Edit Vew Favorites Iools Help		<b>**</b>
🌀 Back 🔹 🐑  📓 🚮 🔎 Search	👷 Favorites 🔞 🍰 🧕 💌 🔹 🗾 🗱 🦓	
Address Address https://172.18.120.225/CAOHE/stc/1/index.htm	ni 🔽 🄁 😡	Unis 🎽 👬 -
		1
diate Cisco	AnyConnect VPN Client	
🔏 WebLaunch	Using ActiveX for Installation	
Platform Detection	Security Warning Attempting to launch ActiveX, which is digitally signed by Cisco Systems. In order to properly use the ActiveX control, be sure to click "Yes" on the	
- ActiveX	security pop-up.	
Texe Detection	Yes No No	
🔲 Niccosoft Java		
📋 - Sun Java		
🛄 - Download		
🖸 - Connected	Help Cancel	
Dpening page https://172.18.120.225/CACHE/stc/1/binar	ies/ocx.htm 🔒 💣 Inter	met

7. 使用する適切な証明書を選択します。図 30 を参照してください。AnyConnect はインスト ールを続行します。ASA 管理者は、クライアントを永続的にインストールするか、ASA 接 続のたびにインストールすることができます。

図30:証明書



Cisco Anyconnect VPN Client の起動 - Windows

ホスト PC から、[Start] > [All Programs] > [Cisco] > [AnyConnect VPN Client] を選択します。

注:オプションのAnyConnectクライアントプロファイル設定については、付録Eを参照し てください。

### 新規接続

1. AC ウィンドウが表示されます。図 34 を参照してください。

図34:新しいVPN接続



2. AC が接続を自動的に試行しない場合、適切なホストを選択します。

3. プロンプトが表示されたら、PIN を入力します。図 35 を参照してください。

図35:暗証番号の入力

ActivCa	ard Gold - Enter PIN	
	Enter PIN code:	
	OK Cance	

リモート アクセスの開始

接続先となるグループおよびホストを選択します。

証明書が使用されるため、[Connect] を選択して VPN を確立します。図 36 を参照してください。

図36:接続



注:接続には証明書が使用されるため、ユーザ名とパスワードを入力する必要はありません 。

注:オプションのAnyConnectクライアントプロファイル設定については、付録Eを参照し てください。

### 付録 A:LDAP マッピングおよび DAP

ASA/PIX リリース 7.1(x) 以降では、LDAP マッピングと呼ばれる機能が導入されました。これは Cisco 属性と LDAP オブジェクトまたは属性の間のマッピングを提供する高度な機能で、LDAP スキーマ変更が不要になります。CAC 認証を実装する場合、これはリモート アクセス接続への 追加のポリシー適用をサポートすることができます。これらは LDAP マッピングの例です。 AD/LDAP サーバを変更するには、管理者権限が必要であることに注意してください。ASA 8.x ソ フトウェアでは、ダイナミック アクセス ポリシー (DAP)機能が導入されました。DAP は CAC と一緒に機能して、複数の AD グループを参照したり、ポリシーや ACL などをプッシュしたりす ることができます。

シナリオ1:リモートアクセス許可ダイヤルインを使用したActive Directoryの強制 :アクセスの許可/拒否

この例では AD 属性 msNPAllowDailin を Cisco 属性 cVPN3000-Tunneling- Protocol にマッピング します。

- AD属性值:TRUE=許可、FALSE=拒否
- Cisco属性値:1=FALSE、4(IPSec)または20(4 IPSEC + 16 WebVPN)=TRUE、

ALLOW 条件について、次のようにマップします。

• TRUE = 20

DENY ダイヤルイン条件の場合、次のようにマップします。

• FALSE = 1

注:TRUEとFALSEはすべて大文字にしてください。詳細は、『<u>セキュリティ アプライアン</u> <u>ス ユーザ許可のための外部サーバの設定</u>』を参照してください。

#### Active Directory の設定

- 1. Active Directory サーバで、[Start] > [Run] をクリックします。
- 2. 開いたテキスト ボックスに dsa.msc と入力して、[Ok] をクリックします。これで Active Directory 管理コンソールが起動します。
- 3. Active Directory 管理コンソールでプラス記号をクリックして、Active Directory のユーザお

よびコンピュータを展開します。

- 4. プラス記号をクリックして、ドメイン名を展開します。
- 5. ユーザのOUが作成されている場合は、すべてのユーザを表示するためにOUを展開します。 すべてのユーザがUsersフォルダに割り当てられている場合は、それらのユーザを表示する ためにフォルダを展開します。図 A1 を参照してください。

図A1: Active Directory管理コンソール



6. 編集するユーザをダブルクリックします。

ユーザのプロパティ ページで [Dial-in] タブをクリックし、[Allow] または [Deny] をクリック します。図 A2 を参照してください。

図A2:ユーザのプロパティ

	- Col 10 10 10 10	
	20 - 20 - 20 - 20 - 20 - 20 - 20 - 20 -	

Remote Access Permission (Dial-	in or VPN)
Allow access	
C Deny access	
C Control access through Remo	le Access Policy
🗌 Velićy Coller ID:	
Callback Options	
No Callback	
Set by Caller (Routing and Re	mote Access Service only)
C Always Callback to:	
🗖 Assigo a Static IP Address 👘	
- Andu Otska Rautaa arrester	1

 $\mathbf{7}$ 

7. 次に [OK] をクリックします。

### ASA の設定

- 1. ASDM で、[Remote Access VPN] > [AAA Setup] > [LDAP Attribute Map] を選択します。
- 2. [Add] をクリックします。
- 3. Add LDAP Attribute Map ウィンドウで、次の手順を実行します。図 A3 を参照してください

#### 図A3:LDAP属性マップの追加

o

🖆 Add LDAP Attribute Map				X
Name: msNPAllowOlalin				
Map Name Map Value				-
		Customer Name	Cisco Name	
Customer Name:				
msNPAllowDialm	Add >>			
Cisco Name:	< Remove			
Tunneling-Protocols				
	K Cancel	Help		

- a. 「名前」テキストボックスに名前を入力します。
- b. [Map Name] タブの [Customer Name] テキストボックスに msNPAllowDialin と入力し ます。
- c. [Map Name] タブの [Cisco Name] ドロップダウン オプションで [Tunneling-Protocols] を選択します。
- d. [Add] をクリックします。
- e. [Map Value] タブを選択します。
- f. [Add] をクリックします。
- g. [Add Attribute LDAP Map Value] ウィンドウの [Customer Name] テキストボックスに TRUE と入力し、[Cisco Value] テキストボックスに 20 と入力します。
- h. [Add] をクリックします。
- i. [Customer Name] テキストボックスに FALSE と入力し、[Cisco Value] テキストボッ クスに 1 と入力します。図 A4 を参照してください。

istomer Name: Ins/IPAlowOlein			
		Customer Value	Cisco Value
		FALSE	1
Customer Value:	Add >>		

- j. [OK] をクリックします。
- k. [OK] をクリックします。
- I. [APPLY] をクリックします。
- m. 設定は図 A5 のようになります。

図A5:LDAP属性マップの設定

📬 Cisco ASDM 6.0 for ASA - 17.	.18.120.225	
File View Tools Wigards Windo	W Help Look For: Find -	alulu
Home Configuration	onitoring 🔚 Save 🔇 Refresh 🔇 Back 💭 Forward 🦿 Help	CISCO
Remote Access V @ 9 ×	Configuration > Remote Access VPN > AAA Setup > LDAP Attribute Map	
Setwork (Client) Access     Access     Clientless SSL VPN Access		
AAA Setup	Add and configure attribute map used by LDAP server.	
LDAP Attribute Map	Name Attribute Map Name	
E 🖓 Secure Desktop Manager ⊻	msNPAllowDialn msNPAllowDialn=Tunneling-Protocols	
<		E E
Revice Setup		
🕵 Firewall		
Remote Access VPN		
Site-to-Site VPN		
Device Management		
ş	Reset 1	

4. [Remote Access VPN] > [AAA Setup] > [AAA Server Groups] を選択します。図 A6 を参照し てください。

図A6:AAAサーバグループ

🚰 Cisco ASDM 6.0 for ASA - 17	2.18.120.225				
Ele View Tools Wigards Winds	ow Help Monitoring 🛄 Save (	Look For:	Badk 🚫 Forward	Find -	dhalla cisco
Remote Access V @ P ×	Configuration > Ren	note Access VP	N > AAA Setup > AA	AA Server Groups	
Image: Set Web Access	AAA Server Groups				
AAA Setup	Server Group	Protocol	Accounting Mod	e Reactivation M	Add
AAA Server Groups LDAP Attribute Map	AD-LDAP LOCAL	LDAP LOCAL		Depletion	Edit
🖶 🔏 Local Users	<	10	[]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]	>	Delete
	Servers in the Selected	f Group			
Device Setup	Server Name or IP	Address	Interface	Timeout	Add
🚮 Firewall	172.18.120.160		outside	10	Edit
Remote Access VPN				(	Delete
Site-to-Site VPN					Move Up
Device Management					Maye Down III
». ·			Apply	t	
Device configuration loaded	cis	00 15	6	7/17	7/07 1:59:07 PM UTC

- 5. 編集するサーバ グループをクリックします。[Servers in the Selected Group] セクションか らサーバの IP アドレスまたはホスト名を選択して、[Edit] をクリックします。
- 6. [Edit AAA Server] ウィンドウの [LDAP Attribute Map] テキストボックスで、作成された LDAP 属性マップをドロップダウン メニューから選択します。図 A7 を参照してください。

図A7:LDAP属性マップの追加

## 🕵 Edit AAA Server

Server Group:		AD-LDAP		
Interface Name:		outside	*	
Server Name or IP Addr	ess:	172.18.120.160		
Timeout:		10		seconds
LDAP Parameters				
Enable LDAP over	SSL			
Server Port:	389			
Server Type:	D6	etect Automatically/Use Generic Type		1
Base DN:	CN=	Users,DC=ggsgseclab,DC=org		
Scope:	One	level beneath the Base DN		

7. [OK] をクリックします。

注:LDAPバインディングと属性マッピングが正しく機能しているかどうかを確認するには、テスト中にLDAPデバッグをオンにします。トラブルシューティング コマンドについては 付録 C を参照してください。

シナリオ2:グループメンバーシップを使用したアクセスの許可/拒否によるActive

#### Directoryの適用

この例では、グループ メンバシップを条件として設定するために、LDAP 属性 memberOf を使用 してトンネリング プロトコル属性にマッピングします。このポリシーを機能させるには、次の条 件が必要です。

- ALLOW 条件のメンバになる ASA VPN ユーザについて、すでに存在するグループを使用するか、新しいグループを作成します。
- DENY 条件のメンバになる ASA 以外のユーザについて、すでに存在するグループを使用す るか、新しいグループを作成します。
- LDAP Viewer 内で、グループの DN が正しいことを確認します。「付録 D」を参照してく ださい。DN が正しくない場合、マッピングは正しく動作しません。

注:このリリースでは、ASAはmemeberOf属性の最初の文字列だけを読み取ることができ ることに注意してください。作成された新しいグループがリストの先頭になるようにしてく ださい。他のオプションは、特殊文字を名前の前に配置して、AD が特殊文字を最初に参照 できるようにすることです。この制約を回避するには、複数のグループを参照する 8.x ソフ トウェアの DAP を使用してください。

注:ユーザが拒否グループの一部であるか、memberOfが常にASAに送り返されるように別の1つ以上のグループの一部であるかを確認してください。FALSE 拒否条件を指定する必要 はありませんが、そうすることがベスト プラクティスです。既存のグループ名にスペース が含まれる場合は、次の方法で属性を入力します。

CN=Backup Operators,CN=Builtin,DC=ggsgseclab,DC=orgです。

注:DAPを使用すると、ASAはmemberOf属性の複数のグループを参照し、それらのグルー プに基づいて許可を行うことができます。DAP のセクションを参照してください。

マッピング

- AD 属性の値:
  - memberOf CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
  - memberOf CN=TelnetClients,CN=Users,DC=labrat,DC=com
- Cisco属性值:1=FALSE、20=TRUE、

ALLOW 条件について、次のようにマップします。

memberOf CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org= 20

DENY 条件について、次のようにマップします。

memberOf CN=TelnetClients,CN=Users,DC=ggsgseclab,DC=org = 1

注:今後のリリースでは、接続を許可および拒否するためのCisco属性が追加されます。 Cisco 属性についての詳細は、『<u>セキュリティ アプライアンス ユーザ許可のための外部サ</u> <u>ーバの設定</u>』を参照してください。

### Active Directory の設定

- 1. Active Directory サーバで、[Start] > [Run] を選択します。
- 2. 開いたテキスト ボックスに dsa.msc と入力して、[Ok] をクリックします。これで Active Directory 管理コンソールが起動します。
- 3. Active Directory 管理コンソールでプラス記号をクリックして、Active Directory のユーザお よびコンピュータを展開します。図 A8 を参照してください。

図A8:Active Directoryグループ

Sile Action View Window He	łp			_8×
← → 🗈 📧 👗 🗙 😭 🖳	3 20 1 7 4 2	<u>r</u> ita in transfer		
Active Directory Users and Computer	Users 23 objects			
Saved Queries     Jabrat.com     Diabrat.com     Diabrat.com	Name	Туре	Description	1
	Administrator	User	Built-in account for administering the co	
E Computers	12 artperez	User		
🗉 🥝 Domain Controllers	ASAUsers	Security Group	VPN Remote Access Users	- 1919 - 1919
ForeignSecurityPrincipals	CERTSVC_DCOM_ACCESS	Security Group	Members of this group are permitted to	
MIL Contraction	DonsAdmins	Security Group	DNS Administrators Group	
Users	2 DnsUpdateProxy	Security Group	DNS clients who are permitted to perfor	
	Domain Admins	Security Group	Designated administrators of the domain	
	Domain Computers	ain Computers Security Group All workstations and servers joined to		
	Domain Controllers	Security Group	All domain controllers in the domain	
	Domain Guests	Security Group	All domain guests	
	Domain Users	Security Group	All domain users	
	TEnterprise Admins	Security Group	Designated administrators of the enterp	
	Group Policy Creator Owners	Security Group	Members in this group can modify group	· · · · · · · · · · · · · · · · · · ·
	Guest	User	Built-in account for guest access to the	
	HelpServicesGroup	Security Group	Group for the Help and Support Center	
	TIIS_WPG	Security Group	IIS Worker Process Group	
	1USR_CISCOJAX-2K3	User	Buik-in account for anonymous access t	
	IWAM_CISCOJAX-2K3	User	Built-in account for Internet Information	
	TRAS and IAS Servers	Security Group	Servers in this group can access remote	
	Schema Admins	Security Group	Designated administrators of the schema	
	SUPPORT_388945aD	User	This is a vendor's account for the Help a	
	TeinetClients	Security Group	Members of this group have access to T	

- 4. プラス記号をクリックして、ドメイン名を展開します。
- 5. [Users] フォルダを右クリックし、[New] > [Group] を選択します。
- 6. グループ名を入力します。例:ASAUsers。
- 7. [OK] をクリックします。

- 8. [Users] フォルダをクリックし、上記で作成したグループをダブルクリックします。
- 9. [Members] タブを選択して、[Add] をクリックします。
- 10. 追加するユーザの名前を入力して、[Ok] をクリックします。

#### ASA の設定

- 1. ASDM で、[Remote Access VPN] > [AAA Setup] > [LDAP Attribute Map] を選択します。
- 2. [Add] をクリックします。
- 3. Add LDAP Attribute Map ウィンドウで、次の手順を実行します。図 A3 を参照してください。
  - a.「名前」テキストボックスに名前を入力します。
  - b. [Map Name] タブの [Customer Name] テキストボックス c に memberOf と入力します。
  - c. [Map Name] タブの [Cisco Name] ドロップダウン オプションで [Tunneling-Protocols] を選択します。
  - d. [Add] を選択します。
  - e. [Map Value] タブをクリックします。
  - f. [Add] を選択します。
  - g. [Add Attribute LDAP Map Value] ウィンドウの [Customer Name] テキストボックスに CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org と入力し、[Cisco Value] テキスト ボックスに 20 と入力します。
  - h. [Add] をクリックします。
  - i. [Customer Name] テキストボックスに CN=TelnetClients,CN=Users,DC=ggsgseclab,DC=org と入力し、[Cisco Value] テキス トボックスに 1 と入力します。図 A4 を参照してください。
  - j. [OK] をクリックします。
  - k. [OK] をクリックします。
  - I. [APPLY] をクリックします。
  - m. 設定は図 A9 のようになります。

図 A9 : LDAP 属性マップ

🖀 Cisco ASDM 6.0 for ASA - 172.	18.120.225		
Ele Yew Icols Wigards Window	ritoring 📊 Save	Look For:	
Remote Access V  P P X P Network (Client) Access P Glientless SSL VPN Access AAA Setup AAA Setup AAA Server Groups	Configuration > Rea	note Access VPN > AAA Setup > LDAP Attr attribute map used by LDAP server.	nibute Map 🗖
ChAP Attribute Map Cocal Users Cocal User	Name memberOf	Attribute Map Name memberOf—Tunneing-Protocols	
Erewall  Remote Access VPN  Ste-to-Site VPN			
Device Management		Apply Reset	A 7/12/07 2:14:47 PM LITC

- 4. [Remote Access VPN] > [AAA Setup] > [AAA Server Groups] を選択します。
- 5. 編集するサーバ グループをクリックします。[Servers in the Selected Group] セクションか らサーバの IP アドレスまたはホスト名を選択して、[Edit] をクリックします。

lame: memberOf		
p Name Map Value		
Customer Name	Customer to Gisco Map Value	boa
memberOf	CN=Teinet Clients, CN=Users, DC=ggsgsedab, DC=org=1	
	jen-Askuses,en-uses,ex-ggsgeenadee-uig-zu	Edit
		Delete

6. [Edit AAA Server] ウィンドウの [LDAP Attribute Map] テキストボックスで、作成された LDAP 属性マップをドロップダウン メニューから選択します。 7. [OK] をクリックします。

注:LDAPバインディングと属性マッピングが正しく動作していることを確認するために、 テスト中はLDAPデバッグをオンにします。トラブルシューティング コマンドについては付 録 C を参照してください。

シナリオ3:複数のmemberOf属性のダイナミックアクセスポリシー

この例では、Active Directory グループ メンバシップに基づくアクセスを可能にするために、 DAP を使用して複数の memberOf 属性を参照します。8.x よりも前では、ASA は最初の memberOf 属性のみを読み取っていました。8.x 以降では、ASA はすべての memberOf 属性を参 照できます。

- ALLOW 条件のメンバになる ASA VPN ユーザについて、すでに存在するグループを使用するか、新しいグループ(1つまたは複数)を作成します。
- DENY 条件のメンバになる ASA 以外のユーザについて、すでに存在するグループを使用するか、新しいグループを作成します。
- LDAP Viewer 内で、グループの DN が正しいことを確認します。「付録 D」を参照してく ださい。DN が正しくない場合、マッピングは正しく動作しません。

ASA の設定

- 1. ASDM で、[Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] を選択します。
- 2. [Add] をクリックします。
- 3. [Add Dynamic Access Policy] で、次の手順を実行します。
  - a.「名前」テキストボックスに名前を入力します。b.
  - b. プライオリティ セクションに、1 などの 0 より大きい数を入力します。
  - c. 選択基準で、[Add] をクリックします。
  - d. [Add AAA Attribute] で、[LDAP] を選択します。
  - e. [Attribute ID] セクションで、memberOf と入力します。
  - f. [Value] セクションで、[=] を選択し、AD グループ名を入力します。参照する各グルー プについてこの手順を繰り返します。図 A10 を参照してください。

図 A10 : AAA 属性マップ

🛸 Add AAA Attrib	ute 🔀
AAA Attribute Type:	LDAP
Attribute ID: membe	rOF
Value: 🛁 🔽	ASAUsers

- g. [OK] をクリックします。
- h. [Access Policy Attributes] セクションで、[Continue] を選択します。図 A11 を参照し てください。

図 A11 : ダイナミック ポリシーの追加

			in the second	
soription: Multi-Group Membership Check			Priority: 1	
Selection Oriteria				
Define the AAA and endpoint attributes used to select this accele below and every endpoint attribute has been satisfied. These a specify the logical expression text.	ss policy. A policy itributes can be o	is used when a user's i reated using the tables	authorization attributes match the A4 s below and/or by expanding the Adv	AA attribute oriteria vanced option to
User has ANY of the following AAA Attributes values 😽		and the following en	idpoint attributes are satisfied.	
AAA Attribute Operation/Value	Add	Endpoint ID	Name/Operation/Value	Add
Idap.memberOf = _ASAUsers	Ert			7.0
Idap.memberOf — YPNUsers				
	Delete			Delete
				Logical Op.
4		a second second		
Advanced				٤
Advanced Access Policy Attributes Configure access policy attributes for this policy. Attributes val Action Network ACL Filters Web-Type ACL Filters Function	ues specified here	will override those val. ng Lists    URL Lists    A	ues obtained from the AAA system. ccess Mathod	8
Advanced Access Policy Attributes Configure access policy attributes for this policy. Attributes val Action Network ACL Filters Web-Type ACL Filters Function Action:  Continue Terminate	ues specified here	will override those val. Ing Lists   URL Lists   A	ies obtained from the AAA system. ccess Method	8)
Advanced  Access Policy Attributes Configure access policy attributes for this policy. Attributes val  Action Network ACL Filters Web-Type ACL Filters Function  Action:   Continue  Terminate  Specify the message that will be displayed when this record is	ues specified here ns   Port Forward s selected.	will override those val. Ing Lists   URL Lists   A	ues obtained from the AAA system. ccess Melthod	8)
Advanced  Access Policy Attributes Configure access policy attributes for this policy. Attributes val  Action Retwork ACL Filters Web-Type ACL Filters Function Action: Continue Specify the message that will be displayed when this record in	ues specified here ns Port Forward s selected,	will override those val. ng Lists   URL Lists   A	ues obtained from the AAA system. ccass Mathod	8
Advanced  Access Policy Attributes  Configure access policy attributes for this policy. Attributes val  Action  Action  Network ACL Fitters  Web-Type ACL Fitters  Function  Action:  Continue  Terminate  Specify the message that will be displayed when this record is  User Message:	ues specified here ins Port Forward s selected.	will override those val. ng Lists    URL Lists    A	ues obtained from the AAA system. access Method	8
Advanced Access Policy Attributes Configure access policy attributes for this policy. Attributes val Action Network ACL Filters Web-Type ACL Filters Function Action:  O Continue  Terminate Specify the message that will be displayed when this record in User Message:	ues specified here ns Port Forward s selected.	will override those val. ng Lists   URL Lists   A	ies obtained from the AAA system. ccess Method	3
Advanced Access Folcy Attributes Configure access policy attributes for this policy. Attributes val Action Network ACL Filters Web-Type ACL Filters Function Action:  O Continue  Terminate Specify the message that will be displayed when this record in User Message:	ues specified here ns Port Forward s selected.	will override those val. ng Lists    URL Lists    A	ues obtained from the AAA system. occess Method	3
Advanced Access Policy Attributes Configure access policy attributes for this policy. Attributes val Action Network ACL Filters Web-Type ACL Filters Function Action:  O Continue  Terminate Specify the message that will be displayed when this record is User Message:	ues specified here ns Port Forward s selected.	will override those val. ng Lists   URL Lists   A	ies obtained from the AAA system. ccess Method	۲

- 4. ASDM で、[Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] を選択します。
- 5. [Default Access Policy] を選択し、[Edit] を選択します。
- 6. デフォルト アクションは [Terminate] に設定されます。図 A12 を参照してください。

図 A12:ダイナミック ポリシーの編集

	DIRACCESSPORCY
escription:	
Access Poli Configure	cy Attributes access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA system.
Action	Network ACL Filters Web-Type ACL Filters Functions Port Forwarding Lists URL Lists Access Method
Specif	r the message that will be displayed when this record is selected.
User M	essage:

注:デフォルトでは「続行」が選択されているため、「終了」が選択されていない場合は、 どのグループにも属していなくても許可されます。

## 付録 B:ASA CLI 設定

ASA 5510
<#root>
ciscoasa#
show running-config
: Saved : ASA Version 8.0(2) ! hostname asa80 domain-name army.mil enable password 8Ry2YjIyt7RRXU24 encrypted
names !
interface GigabitEthernetO/O nameif outside security-level O ip address x.x.x.x 255.255.128
interface GigabitEthernetO/1 nameif inside security-level 100 no ip address
! boot system disk0:/asa802-k8.bin ftp mode passive dns server-group DefaultDNS domain-name army.mil
! ACL'sACL's access-list out extended permit ip any any
pager lines 24 logging console debugging mtu outside 1500 !
ip local pool CAC-USERS 192.168.1.1-192.168.1.254 mask 255.255.255.0
! no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400
access-group out in interface outside route outside 0.0.0.0 0.0.0.0 172.18.120.129 1

timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute -----LDAP Maps & DAP----ldap attribute-map memberOf map-name memberOf Tunneling-Protocols March 11, 2008 ASA - CAC Authentication for AnyConnect VPN Access Company Confidential. A printed copy of this document is considered uncontrolled. 49 map-value memberOf CN=\_ASAUsers,CN=Users,DC=ggsgseclab,DC=org 20 ldap attribute-map msNPAllowDialin map-name msNPAllowDialin Tunneling-Protocols map-value msNPAllowDialin FALSE 1 map-value msNPAllowDialin TRUE 20 dynamic-access-policy-record CAC-USERS description "Multi-Group Membership Check" priority 1 dynamic-access-policy-record DfltAccessPolicy action terminate -----LDAP Server----aaa-server AD-LDAP protocol ldap aaa-server AD-LDAP (outside) host 172.18.120.160 ldap-base-dn CN=Users,DC=ggsgseclab,DC=org ldap-scope onelevel ldap-naming-attribute userPrincipalName ldap-login-password \* ldap-login-dn CN=Administrator,CN=Users,DC=ggsgseclab,DC=org \_\_\_\_\_ aaa authentication http console LOCAL http server enable 445 http 0.0.0.0 0.0.0.0 outside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart -----CA Trustpoints----crypto ca trustpoint ASDM\_TrustPoint0 revocation-check ocsp enrollment terminal keypair DoD-1024 match certificate DefaultCertificateMap override ocsp trustpoint ASDM\_TrustPoint5 10 url http://ocsp.disa.mil crl configure crypto ca trustpoint ASDM\_TrustPoint1 revocation-check ocsp enrollment terminal fqdn asa80 subject-name CN=asa80,OU=PKI,OU=DoD,O=U.S. Government,C=US keypair DoD-1024 match certificate DefaultCertificateMap override ocsp trustpoint ASDM\_TrustPoint5 10 url http://ocsp.disa.mil no client-types crl configure crypto ca trustpoint ASDM\_TrustPoint2

revocation-check ocsp enrollment terminal keypair DoD-2048 match certificate DefaultCertificateMap override ocsp trustpoint ASDM\_TrustPoint5 10 url http://ocsp.disa.mil no client-types crl configure crypto ca trustpoint ASDM\_TrustPoint3 revocation-check ocsp none enrollment terminal crl configure -----Certificate Map----crypto ca certificate map DefaultCertificateMap 10 subject-name ne "" ------CA Certificates (Partial Cert is Shown)-----crypto ca certificate chain ASDM\_TrustPoint0 certificate ca 37 3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101 05050030 60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53 2e20476f 7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603 55040b13 03504b49 311b3019 06035504 03131244 6f44204a 49544320 526f6f74 crypto ca certificate chain ASDM\_TrustPoint1 certificate 319e 30820411 3082037a a0030201 02020231 9e300d06 092a8648 86f70d01 01050500 305c310b 30090603 55040613 02555331 18301606 0355040a 130f552e 532e2047 6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b crypto ca certificate chain ASDM\_TrustPoint2 certificate ca 37 3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101 05050030 60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53 2e20476f 7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603 55040b13 f766e045 f15ddb43 9549d1e9 a0ea6814 b64bcece 089e1b6e 1be959a5 6fc20a76 crypto ca certificate chain ASDM\_TrustPoint3 certificate ca 05 30820370 30820258 a0030201 02020105 300d0609 2a864886 f70d0101 05050030 5b310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53 2e20476f 7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603 55040b13 03504b49 31163014 06035504 03130d44 6f442052 6f6f7420 43412032 301e170d 30343132 31333135 30303130 5a170d32 39313230 35313530 3031305a 305b310b 30090603 55040613 02555331 18301606 0355040a 130f552e 532e2047 6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b 1303504b 49311630 14060355 0403130d 446f4420 526f6f74 20434120 32308201 crypto ca certificate chain ASDM\_TrustPoint4 certificate ca 04

```
30820267 308201d0 a0030201 02020104 300d0609 2a864886 f70d0101
05050030
61310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 311c301a 06035504 03131344 6f442043 4c415353 20332052
6f6f7420
class-map inspection_default
match default-inspection-traffic
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
service-policy global_policy global
      -----windows-----
ssl certificate-authentication interface outside port 443
webvpn
enable outside
svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
svc enable
tunnel-group-list enable
        _____
 -----PN Group/Tunnel Policy------VPN Group/Tunnel Policy-------
group-policy CAC-USERS internal
ggroup-policy AC-USERS internal
group-policy AC-USERS attributes
vpn-windows-tunnel-protocol svc
address-pools value CAC-USERS
web∨pn
svc ask none default svc
tunnel-group AC-USERS type remote-access
tunnel-group AC-USERS general-attributes
authorization-server-group AD-LDAP
default-group-policy AC-USERS
authorization-required
authorization-dn-attributes UPN
tunnel-group AC-USERS webvpn-windows-attributes
authentication certificate
group-alias AC-USERS enable
tunnel-group-map enable rules
```

```
no tunnel-group-map enable ou
no tunnel-group-map enable ike-id
no tunnel-group-map enable peer-ip
```

prompt hostname context

## 付録 C:トラブルシューティング

AAA および LDAP のトラブルシューティング

- debug Idap 255: LDAP データ交換を表示します
- debug aaa common 10: AAA データ交換を表示します

例1:正しい属性マッピングを使用した接続の許可

この例は、付録 A に示すシナリオ 2 を使用した接続の成功における debug ldap および debug aaa common の出力を示します。

図C1:debug LDAPおよびdebug aaa commonの出力:正しいマッピング AAA API: In aaa\_open AAA session opened: handle = 39 AAA API: In aaa\_process\_async aaa\_process\_async: sending AAA\_MSG\_PROCESS AAA task: aaa\_process\_msg(1a87a64) received message type 0 AAA FSM: In AAA\_StartAAATransaction AAA FSM: In AAA\_InitTransaction Initiating authorization query (Svr Grp: AD-LDAP) AAA FSM: In AAA\_BindServer AAA\_BindServer: Using server: 172.18.120.160 AAA FSM: In AAA\_SendMsg User: 1234567890@mil Pasw: 1234567890@mil Resp: [78] Session Start [78] New request Session, context 0x26f1c44, reqType = 0 [78] Fiber started [78] Creating LDAP context with uri=ldap:// 172.18.120.160:389 [78] Binding as administrator [78] Performing Simple authentication for Administrator to 172.18.120.160 [78] Connect to LDAP server: ldap:// 172.18.120.160, status = Successful [78] LDAP Search: Base DN = [CN=Users,DC=ggsgseclab,DC=org] Filter = [userPrincipalName=1234567890@mil] Scope = [SUBTREE] [78] Retrieved Attributes: [78] objectClass: value = top [78] objectClass: value = person [78] objectClass: value = organizationalPerson

```
[78] objectClass: value = user
[78] cn: value = Ethan Hunt
[78] sn: value = Hunt
[78] userCertificate: value =
0..50....../.....60....*.H.....0@1.0.....&...,d....com1.0.....
&...,d...
[78] userCertificate: value =
0...'0................./..t......50....*.H.......0@1.0.....&...,d.....com1.0.....
&...,d...
[78] givenName: value = Ethan
[78] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[78] instanceType: value = 4
[78] whenCreated: value = 20060613151033.0Z
[78] whenChanged: value = 20060622185924.0Z
[78] displayName: value = Ethan Hunt
[78] uSNCreated: value = 14050
[78] memberOf: value = CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[78] mapped to cVPN3000-Tunneling-Protocols: value = 20
[78] uSNChanged: value = 14855
[78] name: value = Ethan Hunt
[78] objectGUID: value = ..9...NJ..GU..z.
[78] userAccountControl: value = 66048
[78] badPwdCount: value = 0
[78] codePage: value = 0
[78] countryCode: value = 0
[78] badPasswordTime: value = 127954717631875000
[78] lastLogoff: value = 0
[78] lastLogon: value = 127954849209218750
[78] pwdLastSet: value = 127946850340781250
[78] primaryGroupID: value = 513
[78] objectSid: value = .....q....q....mY....
[78] accountExpires: value = 9223372036854775807
[78] logonCount: value = 25
[78] sAMAccountName: value = 1234567890
[78] sAMAccountType: value = 805306368
[78] userPrincipalName: value = 1234567890@mil
[78] objectCategory: value =
[78] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
[78] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[78] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
  _____
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(CAC-USERS)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB)
  _____
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
```

User: CAC-USER Pasw: Resp: grp\_policy\_ioctl(12f1b20, 114698, 1a870b4) grp\_policy\_ioctl: Looking up CAC-USERS callback\_aaa\_task: status = 1, msg = AAA FSM: In aaa\_backend\_callback aaa\_backend\_callback: Handle = 39, pAcb = 2ae115c AAA task: aaa\_process\_msg(1a87a64) received message type 1 AAA FSM: In AAA\_ProcSvrResp Back End response: Tunnel Group Policy Status: 1 (ACCEPT) AAA FSM: In AAA\_NextFunction AAA\_NextFunction: i\_fsm\_state = IFSM\_TUNN\_GRP\_POLICY, auth\_status = ACCEPT AAA\_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol = , tunn pol = CAC-USERSAAA\_NextFunction: New i\_fsm\_state = IFSM\_DONE, AAA FSM: In AAA\_ProcessFinal Checking time simultaneous login restriction for user 1234567890@mil AAA FSM: In AAA\_Callback user attributes: 1 Tunnelling-Protocol(4107) 20 20 user policy attributes: None tunnel policy attributes: 1 Primary-DNS(4101) 4 IP: 10.0.10.100 2 Secondary-DNS(4102) 4 IP: 0.0.0.0 3 Tunnelling-Protocol(4107) 4 4 4 Default-Domain-Name(4124) 10 "ggsgseclab.org" 5 List of address pools to assign addresses from(4313) 10 "CAC-USERS" Auth Status = ACCEPT AAA API: In aaa\_close AAA task: aaa\_process\_msg(1a87a64) received message type 3 In aaai\_close\_session (39) AAA API: In aaa\_send\_acct\_start AAA API: In aaa\_send\_acct\_stop CAC-Test#

### 例2:誤って設定されたCisco属性マッピングによる接続の許可

この例は、付録 A に示すシナリオ 2 を使用した接続の許可における debug ldap および debug aaa common の出力を示します。

図C2:debug LDAPおよびdebug aaa commonの出力: 誤ったマッピング AAA API: In aaa\_open AAA session opened: handle = 41 AAA API: In aaa\_process\_async aaa\_process\_async: sending AAA\_MSG\_PROCESS AAA task: aaa\_process\_msg(1a87a64) received message type 0 AAA FSM: In AAA\_StartAAATransaction AAA FSM: In AAA\_InitTransaction Initiating authorization query (Svr Grp: AD-LDAP)

```
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[82] Session Start
[82] New request Session, context 0x26f1c44, reqType = 0
[82] Fiber started
[82] Creating LDAP context with uri=ldap://172.18.120.160:389
[82] Binding as administrator
[82] Performing Simple authentication for Administrator to
172.18.120.160
[82] Connect to LDAP server: ldap:// 172.18.120.160:389, status =
Successful
[82] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[82] Retrieved Attributes:
[82] objectClass: value = top
[82] objectClass: value = person
[82] objectClass: value = organizationalPerson
[82] objectClass: value = user
[82] cn: value = Ethan Hunt
[82] sn: value = Hunt
[82] userCertificate: value =
0...50......./.........60....*.H.......0@1.0.....&...,d....com1.0....
&...,d...
[82] userCertificate: value =
0...'0......./..t.....50....*.H......0@1.0.....&...,d....com1.0.....
&...,d...
[82] givenName: value = Ethan
[82] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[82] instanceType: value = 4
[82] whenCreated: value = 20060613151033.0Z
[82] whenChanged: value = 20060622185924.0Z
[82] displayName: value = Ethan Hunt
[82] uSNCreated: value = 14050
[82] memberOf: value = CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[82] mapped to cVPN3000-Tunneling-Protocols: value =
CN=ASAUsers, CN=Users, DC=ggsgseclab, DC=org
[82] uSNChanged: value = 14855
[82] name: value = Ethan Hunt
[82] objectGUID: value = ..9...NJ..GU..z.
[82] userAccountControl: value = 66048
[82] badPwdCount: value = 0
[82] codePage: value = 0
[82] countryCode: value = 0
[82] badPasswordTime: value = 127954717631875000
[82] lastLogoff: value = 0
[82] lastLogon: value = 127954849209218750
[82] pwdLastSet: value = 127946850340781250
[82] primaryGroupID: value = 513
[82] objectSid: value = .....q.....q.....
[82] accountExpires: value = 9223372036854775807
[82] logonCount: value = 25
[82] sAMAccountName: value = 1234567890
[82] sAMAccountType: value = 805306368
[82] userPrincipalName: value = 1234567890@mil
```

[82] objectCategory: value = CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=org [82] mail: value = Ethan.Hunt@labrat.com callback\_aaa\_task: status = 1, msg = AAA FSM: In aaa\_backend\_callback aaa\_backend\_callback: Handle = 41, pAcb = 2ae115c [82] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1 [82] Session End AAA task: aaa\_process\_msg(1a87a64) received message type 1 AAA FSM: In AAA\_ProcSvrResp Back End response: \_\_\_\_\_ Authorization Status: 1 (ACCEPT) AAA FSM: In AAA\_NextFunction AAA\_NextFunction: i\_fsm\_state = IFSM\_AUTHORIZE, auth\_status = ACCEPT AAA\_NextFunction: authen  $svr = \langle none \rangle$ , author svr = AD-LDAP, user pol = , tunn pol = CAC-USERS AAA\_NextFunction: New i\_fsm\_state = IFSM\_TUNN\_GRP\_POLICY, AAA FSM: In AAA\_InitTransaction aaai\_policy\_name\_to\_server\_id(USAFE) Got server ID 0 for group policy DB Initiating tunnel group policy lookup (Svr Grp: GROUP\_POLICY\_DB) AAA FSM: In AAA\_BindServer AAA\_BindServer: Using server: <Internal Server> AAA FSM: In AAA\_SendMsg User: CAC-USERS Pasw: Resp: grp\_policy\_ioctl(12f1b20, 114698, 1a870b4) grp\_policy\_ioctl: Looking up CAC-USERS callback\_aaa\_task: status = 1, msg = AAA FSM: In aaa\_backend\_callback aaa\_backend\_callback: Handle = 41, pAcb = 2ae115c AAA task: aaa\_process\_msg(1a87a64) received message type 1 AAA FSM: In AAA\_ProcSvrResp Back End response: \_\_\_\_\_ Tunnel Group Policy Status: 1 (ACCEPT) AAA FSM: In AAA\_NextFunction AAA\_NextFunction: i\_fsm\_state = IFSM\_TUNN\_GRP\_POLICY, auth\_status = ACCEPT AAA\_NextFunction: authen  $svr = \langle none \rangle$ , author svr = AD-LDAP, user pol =, tunn pol = CAC-USERSAAA\_NextFunction: New i\_fsm\_state = IFSM\_DONE, AAA FSM: In AAA\_ProcessFinal Checking time simultaneous login restriction for user 1234567890@mil AAA FSM: In AAA\_Callback user attributes: 1 Tunnelling-Protocol(4107) 20 0 user policy attributes: None tunnel policy attributes: 1 Primary-DNS(4101) 4 IP: 10.0.10.100 2 Secondary-DNS(4102) 4 IP: 0.0.0.0 3 Tunnelling-Protocol(4107) 4 4 4 Default-Domain-Name(4124) 10 "ggsgseclab.org" 5 List of address pools to assign addresses from(4313) 10 "CAC-USERS" Auth Status = ACCEPT AAA API: In aaa\_close AAA task: aaa\_process\_msg(1a87a64) received message type 3

In aaai\_close\_session (41) AAA API: In aaa\_send\_acct\_start AAA API: In aaa\_send\_acct\_stop

## DAP のトラブルシューティング

- debug dap errors: DAP エラーを表示します
- debug dap trace : DAP 機能のトレースを表示します

例1:DAPで許可される接続

この例は、付録Aに示すシナリオ3を使用した接続の成功におけるdebug dap errorsおよびdebug dap traceの出力を示します。複数のmemberOf属性に注目してください。ユーザは \_ASAUsers と VPNUsers の両方に属することも、いずれかのグループに属することもでき、ASA 構成によって 決まります。

```
図C3:デバッグDAP
<#root>
debug dap errors
debug dap errors enabled at level 1
debug dap trace
debug dap trace enabled at level 1
The DAP policy contains the following attributes for user:
1241879298@mil
1: action = continue
DAP_TRACE: DAP_open: C8EEFA10
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged =
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.displayName = 1241879298
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.1 = VPNUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.2 = _ASAUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged = 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =
....+..F.."5....
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet =
128273494546718750
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid = ..
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectCategory =
CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298, CN=Users, DC=ggsgseclab, DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["1"] =
"VPNUsers":
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["2"] =
```

```
"_ASAUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] = "TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] = "CACUSERS";
DAP_TRACE: dap_add_to_lua_tree:endpoint["application"]["clienttype"] =
"IPSec";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs: CAC-USERS
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr: rec_count = 1
DAP_TRACE: Username: 1241879298@mil, DAP_close: C8EEFA10
d.
```

例2:DAPとの接続の拒否

この例は、付録 A に示すシナリオ 3 を使用した接続の失敗における debug dap errors および debug dap trace の出力を示します。

図C4:デバッグDAP	
<#root>	
#	
debug dap errors	

```
debug dap errors enabled at level 1
debug dap trace
debug dap trace enabled at level 1
The DAP policy contains the following attributes for user:
1241879298@mil
1: action = terminate
DAP_TRACE: DAP_open: C91154E8
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName =
CN=1241879298, CN=Users, DC=ggsgseclab, DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged =
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.displayName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf = DnsAdmins
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged = 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =
....+..F.."5....
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet =
128273494546718750
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid = ...
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectCategory =
CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=org
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298, CN=Users, DC=ggsgseclab, DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"] = "DnsAdmins";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] = "TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs:
```

## 認証局および OCSP のトラブルシューティング

- debug crypto ca 3
- ・コンフィギュレーション モードで logging class ca console (または buffer) debugging

これらの例では、OCSP レスポンダによる証明書検証の成功と、証明書グループ照合ポリシーの 失敗を示します。

図 C3 は、検証された証明書と、動作中の証明書グループ照合ポリシーのデバッグ出力を示しま す。

図 C4 は、設定を誤った証明書グループ照合ポリシーのデバッグ出力を示します。

図 C5 は、無効になった証明書を持つユーザのデバッグ出力を示します。

図C5:OCSPデバッグ – 正常な証明書検証 CRYPTO\_PKI: Found a suitable authenticated trustpoint ASDM TrustPoint11. CRYPTO\_PKI: Allocated OCSP data handle 0xca2d27b8 CRYPTO\_PKI: Certificate validation: Successful, status: 0. Attempting to retrieve revocation status if necessary CRYPTO\_PKI: status = 0: poll revocation status CRYPTO\_PKI: Attempting to find OCSP override for peer cert: serial number: OF192B, subject name: cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S. Government,c=US, issuer\_name: cn=DOD JITC EMAIL CA-15,ou=PKI,ou=DoD,o=U.S. Government,c=US. CRYPTO\_PKI: Processing map rules for SSL. CRYPTO\_PKI: Processing map SSL sequence 20... CRYPTO\_PKI: Match of subject-name field to map PASSED. Peer cert field: = cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S. Government,c=US, map rule: subject-name ne "". CRYPTO\_PKI: Peer cert has been authorized by map: SSL sequence: 20. CRYPTO\_PKI: Found OCSP override match. Override URL: http://198.154.68.90, Override trustpoint: ASDM\_TrustPoint12 CRYPTO\_PKI: crypto\_pki\_get\_cert\_record\_by\_subject() CRYPTO\_PKI: Destroying OCSP data handle 0xca2d27b8 Crypto CA thread sleeps! CRYPTO\_PKI: Attempting to find tunnel group for cert with serial number: OF192B, subject name: cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S. Government,c=US, issuer\_name: cn=DOD JITC EMAIL CA-15,ou=PKI,ou=DoD,o=U.S. Government,c=US. CRYPTO\_PKI: Processing map rules for DefaultCertificateMap. CRYPTO\_PKI: Processing map DefaultCertificateMap sequence 10... CRYPTO\_PKI: Match of subject-name field to map PASSED. Peer cert field: = cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.

Government,c=US, map rule: subject-name ne "". CRYPTO\_PKI: Peer cert has been authorized by map: DefaultCertificateMap sequence: 10. CRYPTO\_PKI: Ignoring match on map DefaultCertificateMap, index 10 for WebVPN group map processing. No tunnel group is configured. CRYPTO\_PKI: Peer cert could not be authorized with map: DefaultCertificateMap. CRYPTO\_PKI: Processing map rules for SSL. CRYPTO\_PKI: Processing map SSL sequence 20... CRYPTO\_PKI: Match of subject-name field to map PASSED. Peer cert field: = cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S. Government,c=US, map rule: subject-name ne "". CRYPTO\_PKI: Peer cert has been authorized by map: SSL sequence: 20. CRYPTO\_PKI: Ignoring match on map SSL, index 20 for WebVPN group map

図C5:失敗した証明書グループ照合ポリシーの出力

図C5:失効した証明書の出力

n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled uvalidation=. CMertifiIcLa, ted ccha=inl ais eibtrhaer tin, valdid cor =noct oamuthori,zed. map rule: subject-name ne "". CRYPTO\_PKI: Peer cert has been authorized by map: DefaultCertificateMap sequence: 10. Tunnel Group Match on map DefaultCertificateMap sequence # 10. Group name is CAC-USERS CRYPTO\_PKI: Checking to see if an identical cert is already in the database... CRYPTO\_PKI: looking for cert in handle=2467668, digest= CRYPTO\_PKI: Cert record not found, returning E\_NOT\_FOUND CRYPTO\_PKI: Cert not found in database. CRYPTO\_PKI: Looking for suitable trustpoints... CRYPTO\_PKI: Found a suitable authenticated trustpoint trustpoint0. CRYPTO\_PKI: Certificate validation: Successful, status: 0. Attempting to retrieve revocation status if necessary CRYPTO\_PKI: Attempting to find OCSP override for peer cert: serial number: 2FB5FC7400000000035, subject name: cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org, issuer\_name: cn=ggsgseclab,dc=ggsgseclab,dc=org. CRYPTO\_PKI: Processing map rules for DefaultCertificateMap. CRYPTO\_PKI: Processing map DefaultCertificateMap sequence 10... CRYPTO\_PKI: Match of subject-name field to map PASSED. Peer cert field: = cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org, map rule: subject-name ne "". CRYPTO\_PKI: Peer cert has been authorized by map: DefaultCertificateMap sequence: 10. CRYPTO\_PKI: Found OCSP override match. Override URL: http://ocsp.disa.mil, Override trustpoint: OCSP CRYPTO\_PKI: crypto\_pki\_get\_cert\_record\_by\_subject() CRYPTO\_PKI: Found a subject match ERROR: Certificate validation failed, Certificate is revoked, serial number: 2FB5FC7400000000035, subject name: cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org CRYPTO\_PKI: Certificate not validated

## 付録 D: MS 内の LDAP オブジェクトの確認

Microsoft Server 2003 の CD には、LDAP 構造と、LDAP オブジェクトおよび属性を表示するためにインストールできる追加のツールがあります。これらのツールをインストールするには、CD の Support ディレクトリに移動し、Tools ディレクトリを選択します。SUPTOOLS.MSI をインストールします。

#### LDAP Viewer

- 1. インストールした後、[Start] > [Run] を選択します。
- 2. Idp と入力し、[Ok] をクリックします。これで LDAP Viewer が始動します。
- 3. [Connection] > [Connect] を選択します。
- 4. サーバ名を入力して [Ok] をクリックします。
- 5. [Connection] > [Bind] を選択します。
- 6. ユーザ名とパスワードを入力します。

注:管理者権限が必要です。

7. [OK] をクリックします。

8. LDAP オブジェクトを表示します。図 D1 を参照してください。

図D1:LDAPビューア



Active Directory サービス インターフェイス エディタ

- Active Directory サーバで、[Start] > [Run] を選択します。
- adsiedit.msc と入力します。これでエディタが始動します。
- ・オブジェクトを右クリックし、[Properties] をクリックします。

このツールは特定のオブジェクトのすべての属性を表示します。図 D2 を参照してください。

図D2:ADSI Edit

🕗 ADS1 Edir		S. A. A. 18 12			
Ele Action Yew Wine	N=Clark Kent Properties		20	3	<u>_101</u> >
ADSI Edit Domain [Oscotax-2k3.lal DC=labrat, DC=com DC=labrat, DC=com DC=labrat, DC=com DC=Computers B OU=Domain Cor	Show mandatory attrib     Show optional attribute     Show only attributes th     Attributes:	utes es hat have <u>v</u> alues		ss Disting	uished Name
CN=ForeignSec. CN=LostAndFou CN=Clark Ke CN=Clark Ke CN=Clark Ke CN=Peter Pc CN=Program Da CN=System CN=Users Configuration [Ciscojax- Schema [Ciscojax-2k].la CN=Ethan Hunt [Ciscoja	Attribute unicodePvd url userAccountControl userCent userCentricate userParameters user	Syntax Octet String Unicode String Integer Octet String Octet String Octet String Octet String Unicode String Unicode String Unicode String Octet String Unicode String Unicode String	Value   CNot Setb CNot Setb G6048 CNot Setb Gx30 0x62 0x06 0x27 0x3 mix G1 CNot Setb C		
		ок.	Cancel Apply		

### 付録 E

AnyConnect プロファイルを作成してワークステーションに追加することができます。このプロ ファイルは、ASA ホストなどのさまざまな値や、識別名あるいは発行者などの証明書照合パラメ ータを参照できます。このプロファイルは.xml ファイルとして保存され、Notepad で編集できま す。このファイルは各クライアントに手動で追加したり、グループ ポリシーを通じて ASA から プッシュしたりすることができます。ファイルは次の場所に保存されます。

 $\label{eq:locuments} C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile$ 

次のステップを実行します。

- 1. AnyConnectProfile.tmpl を選択し、ファイルを Notepad で開きます。
- 2. ファイルに対して発行者やホスト IP などの変更を行います。図 F1 の例を参照してください。
- 3. 完了したら、ファイルを.xml として保存します。

プロファイル管理については、Cisco AnyConnect のドキュメントを参照してください。つまり、

次のようになります。

- プロファイルには、ユーザ企業に固有の名前を付ける必要があります。例
   : CiscoProfile.xml
- 会社内の個々のグループについて異なっていたとしても、プロファイル名は同じである必要 があります。

このファイルは Secure Gateway 管理者によって保守され、クライアント ソフトウェアと一緒に 配布されるためのものです。この XML に基づくプロファイルは、クライアントにいつでも配布 できます。サポートされる配布メカニズムは、ソフトウェア配布のバンドル ファイルとしての配 布か、自動ダウンロード メカニズムの一部としての配布です。自動ダウンロード メカニズムは、 一部の Cisco Secure Gateway 製品でのみ使用できます。

注:管理者は、作成したXMLプロファイルをオンライン検証ツールで検証するか、ASDMの プロファイルインポート機能で検証することを強く推奨します。検証は、このディレクトリ にある AnyConnectProfile.xsd を使用して実行できます。AnyConnectProfile は AnyConnect Client Profile を表すルート要素です。

これは、Cisco AnyConnect VPN クライアント プロファイル XML ファイルの例です。

<#root> xml version="1.0" encoding="UTF-8" - < AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"</p> xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd"> !--- The ClientInitialization section represents global settings !--- for the client. In some cases, for 1 - --> <ClientInitialization> !--- The Start Before Logon feature can be used to activate !--- the VPN as part of the logon sequence <UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon> !--- This control enables an administrator to have a one time !--- message displayed prior to a users <ShowPreConnectMessage>false</ShowPreConnectMessage>

```
!-- This section enables the definition of various attributes !--- that can be used to refine client c
-->
<CertificateMatch>
--- Certificate Distinguished Name matching allows !--- for exact match criteria in the choosing of a
 <DistinguishedName>
 <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled">
<Name>ISSUER-CN</Name>
<Pattern>DoD-Issuer-ABC</Pattern>
</DistinguishedNameDefinition>
</DistinguishedName>
</CertificateMatch>
</ClientInitialization>
!-- This section contains the list of hosts from which !--- the user is able to select.
<ServerList>
!--- This is the data needed to attempt a connection to !--- a specific host.
-->
<HostEntry>
<HostName>host-02</HostName>
<HostAddress>host-02.dod.gov</HostAddress>
</HostEntrv>
<HostEntry>
<HostName>host-01</HostName>
<HostAddress>192.168.1.1</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

## 関連情報

- <u>Certificates & CRLs specified by X.509 and RFC 3280</u>
- OCSP specified by RFC 2560
- Public Key Infrastructure Introduction
- <u>"Lightweight OCSP" profiled by draft standard</u>
- <u>SSL / TLS specified by RFC 2246</u>
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。