# ASA 8.x: نيوكت AnyConnect SSL VPN CAC-Smart Cards معد عم MAC

### المحتويات

المقدمة المتطلبات ال<u>أساسية</u> المتطلبات المكونات المستخدمة الاصطلاحات تكوين ASA من Cisco اعتبارات النشر تكوين المصادقة والتفويض والمحاسبة (AAA) <u>تكوين خادم LDAP</u> إدارة الشهادات إنشاء المفاتيح <u>تثبيت شهادات المرجع المصدق الجذر</u> <u>تسجيل ASA وتثبيت شهادة الهوية</u> تكوين AnyConnect VPN <u>إنشاء تجمع عناوين IP</u> إنشاء مجموعة النفق ونهج المجموعة واجهة مجموعة النفق واعدادات الصورة قواعد مطابقة الشهادة (إذا كان سيتم إستخدام OCSP) تكەين OCSP تكوين شهادة المستجيب <u>OCSP</u> تكوين CA لاستخدام OCSP تكوين قواعد OCSP تكوين عميل AnyConnect من Cisco تنزيل, Cisco AnyConnect VPN Client - Mac OS X بدء تشغيل AnyConnect VPN Client من Cisco - نظام التشغيل Mac OS X اتصال جديد بدء الوصول عن بعد الملحق أ - تخطيط LDAP و DAP <u>السيناريو 1: تطبيق Active Directory باستخدام الطلب الهاتفي لأذن الوصول عن بعد - السماح بالوصول/رفضه</u> Active Directory تكوين ASA السيناريو 2: تطبيق Active Directory باستخدام عضوية المجموعة للسماح بالوصول أو رفضه Active Directory <u>Jack</u> تكوين ASA <u>السيناريو 3: سياسات الوصول الديناميكي للعديد من سمات الأعضاء</u> تكوين ASA الملحق ب - تكوين LDA و الملحق ج - أستكشاف الأخطاء وإصلاحها أستكشاف أخطاء AAA و LDA وإصلاحها المثال 1: الاتصال المسموح به مع تعيين السمة الصحيحة أستكشاف أخطاء PAD وإصلاحها مثال 1: الاتصال المسموح به مع DAP مثال 2: التصال المسموح به مع DAP مثال 2: الاتصال المسموح به مع DAP مثال 3: الاتصال المسموح به مع DAP مثال 3: الاتصال المسموح به مع DAP مثال 3: الاتصال المسموح به مع DAP مثال 4: الاتصال المسموح به مع DAP معلومات ذات صلة مثال 3: مثل 1: مثل 1: الملحق 4: الملحق 5: مثل 1: الالملحق 5: مثل 1: الملحق 5: مثل 5:

### <u>المقدمة</u>

يقدم هذا المستند نموذجا لتكوين على جهاز الأمان القابل للتكيف (ASA) من Cisco للوصول عن بعد إلى AnyConnect VPN لدعم MAC باستخدام بطاقة الوصول المشترك (CAC) للمصادقة.

يغطي هذا المستند تكوين Cisco ASA باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM) و Cisco AnyConnect VPN Client و Microsoft Active Directory/بروتوكول الوصول إلى الدليل خفيف الوزن (LDAP).

يستخدم التكوين الموجود في هذا الدليل خادم Microsoft AD/LDAP. يغطي هذا المستند أيضا الميزات المتقدمة مثل OCSP وخرائط سمات LDAP وسياسات الوصول الديناميكي (DAP).

# <u>المتطلبات الأساسية</u>

### <u>المتطلبات</u>

يكون الفهم الأساسي ل Cisco ASA و Cisco AnyConnect Client و Microsoft AD/LDAP وبنية المفتاح العام (PKI) مفيدا في فهم الإعداد الكامل. تساعد الإلمام بعضوية مجموعة AD وخصائص المستخدم وكذلك كائنات LDAP في ربط عملية التخويل بين سمات الشهادة وكائنات AD/LDAP.

### <u>المكونات المستخدمة</u>

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهاز الأمان القابل للتكيف (ASA) من Cisco 5500 Series الذي يشغل الإصدار x)8.0) من البرنامج والإصدارات الأحدث
  - ASA 8.x الإصدار (Cisco Adaptive Security Device Manager (ASDM
    - MAC مع دعم Cisco AnyConnect VPN Client 2.2 •

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

### <u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

## <u>تکوین ASA من Cisco</u>

يغطي هذا القسم تكوين Cisco ASA عبر ASDM. وهو يغطي الخطوات الضرورية لنشر نفق وصول عن بعد لشبكة VPN من خلال اتصال SSL AnyConnect. يتم إستخدام شهادة CAC للمصادقة، كما يتم ملء السمة User Principal Name (UPN) في الشهادة في Active Directory للتخويل.

### <u>اعتبارات النشر</u>

- لا يغطي هذا الدليل التكوينات الأساسية مثل الواجهات و DNS و NTP والتوجيه والوصول إلى الجهاز والوصول إلى ASDM وما إلى ذلك. من المفترض أن مشغل الشبكة على دراية بهذه التكوينات.راجع <u>أجهزة الأمان متعددة</u> <u>الوظائف</u> للحصول على مزيد من المعلومات.
  - والأقسام المبرزة في RED هي تكوينات إلزامية مطلوبة للوصول الأساسي إلى الشبكة الخاصة الظاهرية (VPN). على سبيل المثال، يمكن إعداد نفق VPN باستخدام بطاقة CAC دون إجراء فحوصات OCSP وتخطيطات LDAP وفحوصات سياسة الوصول الديناميكي (DAP). يقوم DoD بتفويض فحص OCSP ولكن يعمل النفق بدون تكوين OCSP.
    - الأقسام المبرزة بالأزرق هي ميزات متقدمة يمكن تضمينها لإضافة المزيد من التأمين للتصميم.
- لا يمكن أن يستخدم ASDM و ANyConnect/SSL VPN المنافذ نفسها على الواجهة نفسها. يوصى بتغيير المنافذ على أحدها أو الآخر للحصول على حق الوصول. على سبيل المثال، أستخدم المنفذ 445 ل ASDM وترك AC/SSL VPN ل A43 في x.8. أستخدم (ip-address>:<port>/admin.html.
  - صورة ASA المطلوبة هي 8.0.2.19 و ASDM 6.0.2 على الأقل.
    - AnyConnect/CAC مدعوم مع Vista.
  - راجع <u>الملحق (أ)</u> للحصول على أمثلة لرسم خرائط سياسة الوصول الديناميكي و LDAP لتنفيذ السياسات الإضافية.
    - راجع <u>الملحق (د</u>) حول كيفية التحقق من كائنات LDAP في MS.
    - راجع المعلومات ذات الصلة للحصول على قائمة بمنافذ التطبيق لتكوين جدار الحماية.

### <u>تكوين المصادقة والتفويض والمحاسبة (AAA)</u>

تتم مصادقتك باستخدام الشهادة الموجودة في بطاقة الوصول المشترك (CAC) من خلال خادم مرجع مصدق البيانات (CA) أو خادم CA الخاص بمنظمتهم. يجب أن تكون الشهادة صالحة للوصول عن بعد إلى الشبكة. بالإضافة إلى المصادقة، يجب أن تكون مخولا أيضا لاستخدام كائن Microsoft Active Directory أو Vicrosight Directory (LDAP) المصادقة، يجب أن تكون مخولا أيضا لاستخدام كائن Microsoft Active Directory أو UPN) للتخويل، والتي (LDAP) المصادقة، يجب أن تكون منولا أيضا لاستخدام كائن Microsoft Active Directory أو UPN) للتخويل، والتي تعد جزءا من قسم "الاسم البديل للموضوع (SAN)" في الشهادة. يجب أن يكون UPN أو EDI/ال التخويل. راجع (أي للحصول على تكوين إضافي باستخدام تعيين كائن ASA في ASA باستخدام خادم LDAP للتخويل. راجع (أي للحصول على تكوين إضافي الستخدام تعيين كائن LDAP في المعاد.

#### <u>تکوین خادم LDAP</u>

أكمل الخطوات التالية:

- 1. أختر Remote Access VPN (الوصول عن بعد) > إعداد AAA > مجموعة خوادم AAA.
  - 2. في جدول مجموعات خوادم AAA، انقر فوق **إضافة 3**.

3. دخلت نادل مجموعة إسم واخترت LDAP في البروتوكول لاسلكي زر. راجع الشكل 1.

- 4. في الخوادم الموجودة في جدول المجموعة المحدد، انقر فوق **إضافة**. تأكد من أن الخادم الذي أنشأته مبرز في الجدول السابق.
- 5. في نافذة تحرير خادم AAA، أكمل الخطوات التالية. راجع الشكل 2.**ملاحظة:** أختر خيار **تمكين LDAP عبر SSL** في حالة تكوين LDAP/AD لهذا النوع من الاتصال.أخترت القارن حيث ال LDAP يكون موقع. يظهر هذا الدليل داخل الواجهة.أدخل عنوان IP الخاص بالخادم.أدخل **منفذ الخادم**. التقصير LDAP ميناء 389.أختر **نوع الخادم**.أدخل M **الأساسي**. اسأل مسؤول AD/LDAP عن هذه القيم.**شكل-1**

rver group. The Accounting Mode attribute is only applicab ACS+ protocols.
AD-LDAP
LDAP
Simultaneous 💿 Single
O Depletion O Timed
initial minutes
3.11.11.11.11.11.11.11.11.11.11.11

النطاق، أختر الإجابة المناسبة. يعتمد ذلك على DN الأساسي. اطلب المساعدة من مسؤول AD/LDAP.في سمة التسمية، أدخل userPrincipalName. هذه هي السمة المستخدمة لتخويل المستخدم في خادم AD/LDAP.دخلت في ال login DN، المسؤول DN.**ملاحظة:** لديك حقوق أو حقوق إدارية لعرض/البحث في بنية LDAP التي تتضمن كائنات المستخدم وعضوية المجموعة.في كلمة مرور تسجيل الدخول، أدخل كلمة مرور المسؤول.أترك سمة LDAP إلى **بلا.شكل-2** 

🖆 Add AAA Server		X
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:	Detect Automatically/Use Generic Type 💟	
Base DN:	CN=Users,DC=ggsgseclab,DC=org	
Scope:	One level beneath the Base DN 🛛 😽	
Naming Attribute(s):	userPrincipalName	
Login DN:	lministrator, CN=Users, DC=ggsgseclab, DC=org	
Login Password:	•••••	
LDAP Attribute Map:	None 💉	
SASL MD5 authen	tication	
5ASL Kerberos au	thentication	
Kerberos Server G	roup:	

يمكنك إستخدام هذا الخيار لاحقا في التكوين لإضافة كائن AD/LDAP آخر للتخويل.أختر OK. 6. أختر OK.

## إدارة الشهادات

هناك إثنان steps in order to ركبت شهادة على ال ASA. أولا، قم بتثبيت شهادات المرجع المصدق (المرجع المصدق الأساسي والثانوي) المطلوبة. ثانيا، تسجيل مكتب المساعدة القانونية في مرجع مصدق محدد والحصول على شهادة الهوية. تستخدم وحدة PKI من DoD هذه الشهادات وشهادة ASA ID وشهادة OCSP ذات الجذر CA2 والفئة 3 و CA# متوسطة التي تم تسجيل ASA بها وشهادة DSA ID وشهادة OCSP. ولكن، إذا أخترت عدم إستخدام OCSP، *فلا* يلزم تثبيت شهادة PSP.

**ملاحظة:** اتصل ب POC للأمان للحصول على الشهادات الجذر بالإضافة إلى التعليمات حول كيفية التسجيل لشهادة الهوية للجهاز. يجب أن تكون شهادة SSL كافية ل ASA للوصول عن بعد. لا *يلزم* إستخدام شهادة شبكة منطقة تخزين (SAN*)* مزدوجة.

**ملاحظة:** يجب أيضا تثبيت سلسلة DoD CA على الجهاز المحلي. يمكن عرض الشهادات في "مخزن شهادات

Microsoft" باستخدام Internet Explorer. أنتج DoD ملف دفعة يقوم تلقائيا بإضافة كافة CAs إلى الجهاز. اطلب PKI POC الخاص بك للحصول على مزيد من المعلومات.

**ملاحظة:** يجب أن يكون جذر DoD CA2 والفئة 3 وكذلك معرف ASA ومعرف CA الوسيط الذي أصدر شهادة ASA هو المرجع المصدق الوحيد المطلوب لمصادقة المستخدم. تنضوي جميع الواسطات CA الحالية تحت سلسلة جذر CA2 والفئة 3 ويتم الوثوق بها طالما تمت إضافة جذور CA2 والفئة 3.

### إنشاء المفاتيح

أكمل الخطوات التالية:

- 1. أختر Remote Access VPN (الوصول عن بعد) > إدارة الشهادات > شهادة الهوية > إضافة.
  - 2. أختر **إضافة شهادة معرف جديدة** ثم **جديد** بواسطة خيار زوج المفاتيح.
- 3. في نافذة إضافة زوج المفاتيح، أدخل اسم مفتاح، DoD-1024. انقر على الراديو لإضافة مفتاح جديد. راجعٍ

Name:	O Use default key pair name	
	Enter new key pair name:	DoD-1024
Size:	1024	
Usage:	💽 General purpose	🚫 Special
	Generate Now Cancel	Help

- الشكل 3.**شكل 3 ا**4. 4. أختر حجم المفتاح.
- 5. الاحتفاظ بالاستخدام **للأغراض العامة**.
- 6. انقر فوق **إنشاء الآن.ملاحظة:** يستخدم المرجع المصدق (CA) الجذري 2 ل DoD مفتاح إصدار 2048 بت. يجب إنشاء مفتاح ثان يستخدم زوج مفاتيح 2048 بت ليكون قادرا على إستخدام المرجع المصدق هذا. أتمت ال سابق steps in order to أضفت مفتاح ثاني.

### تثبيت شهادات المرجع المصدق الجذر

أكمل الخطوات التالية:

- 1. أختر **Remote Access VPN (الوصول عن بعد) > إدارة الشهادات > شهادة CA > إضافة**.
  - 2. أختر **تثبيت من ملف** واستعرض إلى الشهادة.
  - 3. أختر **شهادة التثبيت.الشكل 4: تثبيت الشهادة الجذر**

<ol> <li>Install from a file:</li> </ol>	C:\CAC\DOD-CERTS\ca13-jitc.cer	Browse
🚫 Paste certificate in	PEM format:	
Use SCEP:		
SCEP URL: http://		
Retry Period:	1	minutes
Retry Count:	0	(Use 0 to indicate unlimited retries)
		More Optiops
Install Ce	rtificate Cancel	Help Million
	.شكل 5	ب أن تظهر هذه النافذة. انظر الشكل 5.
	🕵 CA Certificate Ins	tallation
	CA certif	ficate installed successfully.

لكل شهادة تريد تثبيتها. يتطلب DoD PKI شهادة لكل مما يلي: جذر CA 2، جذر الفئة 3، CA# متوسط، مُعرف ASA وخادم OCSP. لا تكون شهادة OCSP مطلوبة إذا لم تستخدم OCSP.**الشكل 6: تثبيت الشهادة الجذر** 

Ele giew Club Wigerds wincow	Falt		LcovFor	
🕝 Hamm 🍕 : střigikaarth 💽 Mich	terine 🔛 stvn 🔇 R	nimth 🕜 Katk 💮 K-Iweld 🗌	🥐 нар	
Remote Access VPN # .s	<b>Configuration &gt; Report</b>	n Access VPN > Certificate Man	agement > CA Certificates	
hetwork (Clienk) Access     Cliendess 55L VPN Access	kaudie	The start By	Friender Ikan	cd
in in a see is p	Dot Dach CA 2	June D. D. Root CA 2. Long M. L. Human	15:01:10 UTC Senature	
🦕 🔛 ) estricatri Management	DoD/CLASS 3 Ploof CA	[m=91001495 FRont (Ayou=100	nan-ammini General Purpose	t dit
🖓 🗛 Callitaes	вор згла са-13	[ui=010 DITE Rolf CA 2, 10=PK2	C2:55:53.UTC Signation	how petals
- Anglidonticy Continents - Anglidontics - Anglidon				(
Det Local Certificate Authority				Ked esti ki
primela Telencing				Delete
Frank BHCP 5erver ■ max				
🗟 🦉 Advanced				
And the second se				
💑 Device Setup				
🚰 firsest				
440 ·····				
CALE Carrote Access VPN				

### <u>تسجيل ASA وتثبيت شهادة الهوية</u>

- 1. أختر Remote Access VPN (الوصول عن بعد) > إدارة الشهادات > شهادة الهوية > إضافة.
  - 2. أختر **إضافة شهادة معرف جديدة**.
  - 3. <u>أ</u>ختر زوج المفاتيح **DoD-1**024. انظر الشكل 7**الشكل 7: معلمات شهادة الهوية**

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

- 4. انتقل إلى مربع DN لموضوع الشهادة وانقر فوق **تحديد**.
- 5. في نافذة DN موضوع الشهادة، أدخل معلومات الجهاز. راجع الشكل 8 على سبيل المثال.**شكل 8: تحرير DN**

			Attribute	Value
	1- L- 111-1		Common Name (CN)	asa80
DN Attribute	to be Added		Department (OU)	PKI
Attribute:	Select Attribute 🔽	Add>>	Department (OU)	DoD
Universit		Conservation	Company Name (O)	U.S. Government
value:		Delete	Country (C)	US

- 6. أختر O**K.ملاحظة:** تأكد من إستخدام اسم المضيف للجهاز الذي تم تكوينه في نظامك عند إضافة اسم المضيف DN للموضوع. يمكن أن يخبرك PKI POC بالحقول الإلزامية المطلوبة.
  - 7. أختر **إضافة شهادة**.
  - 8. <u>انقر فوق **إستعراض** لتحديد الدليل الذي تريد حفظ الطلب فيه. راجع الشكل 9.**شكل 9 طلب شهادة**</u>

🖆 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 clicking the Install button in the Identity Certificates panel.	
Save CSR to file:	)
OK Cancel Help	

9. افتح الملف باستخدام WordPad، وانسخ الطلب إلى الوثائق المناسبة ثم قم بإرساله إلى PKI POC. راجع الشكل 10.**الشكل 10: طلب التسجيل** 



10. ما إن يستلم أنت الشهادة من ال CA مدير، أختر Remote Access VPN > إدارة الشهادة > شهادة المعرف > تثبيت. راجع الشكل 11.الشكل 11: إستيراد شهادة الهوية

The Ten Tools wizerds Window	Tieth	es de la social de la compañía de la social de la compañía de la social de la compañía de la compañía de la com	CHARLES AND AN ADDRESS OF	A DEPENDENCE OF A DEPENDENCE	NO FEND FEND FEND
🚯 Home 🚱 Configuration 📴 Mon	nitoring 🔲 Sav	ve 📿 Refresh	G Back O For	werd 🢡 Help	
Remote Access VPN 🗗 🕂 🗡	Configuration	> Remote Acce	ss VPN > Certifical	e Management > Iden	tity Certificate:
Detwork (Client) Access     Gientless 55L VPN Access	Issued To	Issued By	Expiry Date	Usage	Add
🗄 🖓 Secure Desktop Manager	[asa80]	[Not Available]	Pending	Unknown	
🖃 🛃 Certificate Management					Show Det
CA Certificates					Delete
Code Signer					Export
Coll Certificate Authority					· · · · · · · · · · · · · · · · · · ·
BHCP Server					Instal
🛃 DNS					
0	Televitter enstition	to one he used to	- Abasticate UDU sees	a through the generative of	atanan Vauana
Device Setup	configuration.	te can be used to	authenticate vPN acce	ss chrough the security ap	plance, rou can
🚯 Firowall					
2 Remote Access VPN					

11. في نافذة "تثبيت شهادة"، استعرض للوصول إلى شهادة المعرف واختر **تثبيت الشهادة**. راجع الشكل 12 على سبيل المثال.**الشكل 12: تثبيت شهادة الهوية** 

🖆 Install Identity certificate	×
Identity Certificate  Install from a file: C:\CAC\DOD-CERTS\asa80.txt	Browse
O Paste the certificate data in base-64 format:	
Install Certificate Cancel Help	

**لاحظة:** يوصى بتصدير Id Certificate TrustPoint لحفظ أزواج الشهادات والمفتاح الصادرة. وهذا يسمح لمسؤول ASA باستيراد أزواج الشهادات والمفتاح إلى ASA جديد في حالة حدوث عطل في RMA أو في الجهاز. راجع <u>تصدير نقاط الثقة واستيرادها</u> للحصول على مزيد من المعلومات.**ملاحظة:** انقر فوق **حفظ** لحفظ التكوين في ذاكرة Flash (الذاكرة المؤقتة).

# <u>تكوين AnyConnect VPN</u>

هناك خياران لتكوين معلمات VPN في ASDM. الخيار الأول هو إستخدام معالج SSL VPN. هذه أداة سهلة الاستخدام للمستخدمين الجدد في تكوين VPN. الخيار الثاني هو أن تفعل ذلك يدويا وتمضي خلال كل خيار. يستخدم دليل التكوين هذا الطريقة اليدوية.

**ملاحظة:** هناك طريقتان لإيصال عميل AC إلى المستخدم:

1. يمكنك تنزيل العميل من موقع Cisco على الويب وتثبيته على الجهاز الخاص به.

2. يمكن للمستخدم الوصول إلى ASA عبر مستعرض ويب ويمكن تنزيل العميل.

**ملاحظة:** على سبيل المثال، https://asa.test.com. يستخدم هذا الدليل الطريقة الثانية. بمجرد تثبيت عميل AC على جهاز العميل بشكل دائم، فما عليك سوى تشغيل عميل AC من التطبيق.

<u>إنشاء تجمع عناوين IP</u>

هذا إختياري إذا كنت تستخدم طريقة أخرى مثل DHCP.

- 1. أختر Remote Access VPN (الشبكة الخاصة الظاهرية (VPN) < ((VPN) (العميل) Access > Address (تعيين العناوين) > مجموعات العناوين.
  - 2. انقر فوق **إضافة (Add)**.
- 3. في نافذة إضافة تجمع IP، أدخل اسم تجمع IP، حيث تقوم بتشغيل عنوان IP ونهايته واختر قناع شبكة فرعية. انظر الشكل 13.**الشكل 13: إضافة تجمع I**P

🖆 Add IP Pool	X
Name:	CAC-USERS
Starting IP Address:	192.168.1.1
Ending IP Address:	192,168.1,254
Subnet Mask:	255.255.255.0
ОК	Cancel Help

- 4. أختر **موافق**.
- 5. أختر Remote Access VPN (الوصول عن بعد) > Network (العميل) Remote Access VPN (تعيين العنوان) > Access كالعميل) Access Address Assignment (تعيين العنوان) > Access Address Assignment
- 6. حدد أسلوب تعيين عنوان IP المناسب. يستخدم هذا الدليل تجمعات العناوين الداخلية. انظر الشكل 14.**الشكل** 14**: أسلوب تعيين عنوان I**P



7. طقطقة **يطبق**.

### <u>إنشاء مجموعة النفق ونهج المجموعة</u>

#### نهج المجموعة

**ملاحظة:** إذا لم تكن ترغب في إنشاء نهج جديد، يمكنك إستخدام النهج الافتراضي المضمن في المجموعة.

- 1. أختر الوصول عن بعد إلى VPN -> الوصول إلى الشبكة (العميل) -> نهج المجموعة.
  - 2. انقر فوق **إضافة** واختر **نهج المجموعة الداخلي**.
- 3. في نافذة "إضافة نهج مجموعة داخلي"، أدخل اسم "نهج المجموعة" في مربع النص "الاسم". راجع الشكل 15. **الشكل 15: إضافة سياسة مجموعة داخلية**

verc	Name: AC-USER:	5				
Advanced	Banner: 🔽 Inheri	:				
	Address Pools: 🔲 Inheri	CAC-USE	RS			Select
	More Options					
	Tunneling Protocols:	🔲 Inherit	Clientless SSL VPN	SSL VPN Client	IPsec	L2TP/IPs
	Filter:	🗹 Inherit				Manage
	NAC Policy:	🔽 Inherit			· · · · · ·	Manage
	Access Hours:	🔽 Inherit				Manage
	Simultaneous Logins:	🕑 Inherit				
	Restrict access to VLAN:	🔽 Inherit				
	Maximum Connect Time:	🔽 Inherit	Unimited	mnutes		
	Idle Timeout:	🔽 Inherit	Unlimited	mnubes		

في علامة التبويب "عام"، أختر SSL VPN Client في خيار **بروتوكولات** الاتصال النفقي، إلا إذا كنت تستخدم بروتوكولات أخرى مثل SSL بدون عميل.في قسم الخوادم، قم بإلغاء تحديد خانة الاختيار Inherit وأدخل عنوان IP الخاص بخوادم DNS و WINS. أدخل نطاق DHCP إذا كان ذلك ممكنا.في قسم الخوادم، قم بإلغاء تحديد خانة الاختيار **توريث** في المجال الافتراضي وأدخل اسم المجال المناسب.في علامة التبويب "عام"، قم بإلغاء تحديد خانة الاختيار **توريث** في المجال الافتراضي وأدخل اسم المجال المناسب.في علامة التبويب "عام"، الخطوة السابقة. إذا كنت تستخدم طريقة أخرى لتعيين عنوان IP، فاترك هذه الطريقة للوراثة وقم بإجراء التغيير المناسب.تترك كل علامات تبويب التكوين الأخرى للإعدادات الافتراضية. ميل AC إلى المستخدمين النهائيين. تتمثل أولاهما في الانتقال إلى Cisco.com وتنزيل عميل AC. الطريقة الثانية هي أن يقوم ASA بتنزيل العميل إلى المستخدم عندما يحاول المستخدم الاتصال. والمراتة وقم بإجراء عميل AC إلى المستخدمين النهائيين. تتمثل أولاهما في الانتقال إلى Cisco.com وتنزيل عميل AC. الطريقة الثانية هي أن يقوم ASA بتنزيل العميل إلى المستخدم عندما يحاول المستخدم الاتصال. ولائيل المتول

4. بعد ذلك، أختر **متقدم > SSL VPN Client > إعدادات تسجيل الدخول**. انظر الشكل 16.**الشكل 16: إضافة** سياسة مجموعة داخلية

📬 Edit Internal Group Poli	icy: AC-USERS	×
General Servers Advanced Split Tunneling E Browser Proxy SSL VPN Client Cogn Setting Dead Peer Detecti Customization Customization TPsec Client	After successfully logging in, user can have the choice to download the clent software, or go to clentless SSL VPN portal 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 Logn Selecton below is taken: Default Post Logn Selecton O to Clentless SSL VPN portal O to Clentless SSL VPN clent	

قم بإلغاء تحديد خانة الاختيار **توريث**.أختر الإعداد المناسب ل Post Login (تسجيل الدخول إلى الموقع) الذي يناسب بيئتك.أختر تحديد مادة النشر الافتراضي المناسب الذي يناسب بيئتك.أختر O**K**.

### واجهة مجموعة النفق وإعدادات الصورة

**ملاحظة:** إذا كنت لا تريد إنشاء مجموعة جديدة، يمكنك إستخدام المجموعة المدمجة الافتراضية.

- 1. أختر Remote Access VPN (الوصول عن بعد) > Network (العميل) Access > ملف تعريف اتصال VPN ل SSL.
  - 2. أختر **تمكين عميل Cisco AnyConnect...** 
    - 3. يظهر مربع حوار مع السؤال svc
      - 4. أختر **نعم**.
- 5. إذا كان هناك صورة بالفعل، أختر الصورة التي تريد إستخدامها مع تصفح Flash. إذا لم تكن الصورة متوفرة، أختر **تحميل** واستعرض الملف على الكمبيوتر المحلي. انظر الشكل 17. يمكن تنزيل الملفات من Cisco.com، <u>هناك ملف Windows و Mac و Linux.**شكل 17: إضافة صورة عميل VPN**</u>

🚰 Add SSL VPN Client Image	X
Flash SVC Image:	Browse Flash
	Upload
OK Cancel	Help

6. التمكين التالي **يسمح بالوصول**، **يتطلب شهادة عميل** و**تمكين DTLS إختياريا**. انظر الشكل 18.**الشكل 18: تمكين الوصول** 

🔓 Cisco ASDM 6.0 for ASA - 17	2.18.120.225					
File View Icols Wigards Windo	w <u>H</u> eb Aonitoring 🔚 Sav	e 💽 Refresh 🚺	Look For: Back OFor	eerd 🦻 Help	ing in the second	uhuhu cisco
Remote Access V       P         Network (Clent) Access       A         SSL VPN Connection Profiles       IPsec Connection Profiles	Configuration > F The security app users upon corru- VPN Client suppo	Remote Access Vi lance automatically action. The initial clie rts the HTTP5/TCP (	PN > Network (Cl deploys the Osco Ar nt deployment requi SSL) and Datagram	ient) Access > S wConnect VPN Clen res end-user admini Transport Layer Sec	SL VPN Connection t or legary SSL VPN C strative rights. The C: unity (DTLS) tunneling	n Profiles  ient to remote sco AnyConnect aptions.
Group Policies     Dynamic Access Policies     Address Assignment     Assignment Policy	(More client-rela	ted parameters, suc	h as client images ar	nd client profiles, car	n be found at <u>Client Se</u>	<u>etinos</u> .)
Address Paols     Advanced     Chendless SSL VPN Access	Access Interfaces	AnyConnect VPN Cli	ent or legacy SSL VP	N Client access on t	he interfaces selected	in the table below
Device Setup	Interface outside	Allow Access	Require Cli	ent Certificate	Enable DTLS	
Remate Access VPN	Access Port: 44 Click here to Ass	3 DTLS con Certificate to Inf	5 Port: 443			
Device Management	Connection Profiles	rism	Apply	Reset		307 2:09:48 AM LI

- 7. طقطقة **يطبق**.
- 8. بعد ذلك، قم بإنشاء ملف تعريف اتصال/مجموعة نفق. أختر Remote Access VPN (الوصول عن بعد) > Network (العميل) Access > ملف تعريف اتصال VPN ل SSL.
  - 9. في قسم توصيفات التوصيل، انقر على **إضافة.شكل 19: إضافة ملف تعريف الاتصال**

🖆 Add SSL VPN Connect	ion Profile		
Basic Cold Cold Cold Cold Cold	Name:	AC-USERS	
Advanced	Aliases:		
	Authentication		
	Method:	🔿 AAA 💿 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-USERS	Manage
	SSL VPN Client Protocol:	Enabled	
	ОК	Cancel Help	

قم بتسمية المجموعة.أختر **شهادة** في طريقة المصادقة.أختر نهج المجموعة الذي تم إنشاؤه مسبقا.تأكد من تمكين SSL VPN Client.أترك الخيارات الأخرى كافتراضي.

10. بعد ذلك، **أختر متقدم > التخويل**. راجع الشكل 20**الشكل 20: الترخيص** 

🖆 Edit SSL VPN Connect	ction Profile: AC-USERS	
Basic	Default Authorization Server Group	
-Advanced	Server Group: AD-LDAP Manage	
Client Addressing Authentication	Users must exist in the authorization database to connect	
Authorization	Interface-specific Authorization Server Groups	
-SSL VPN	Add 📷 Edt 📋 Delete	
	Interface Server Group	
	User Name Mapping O Use the entire DN as the username	
	<ul> <li>Specify individual DN fields as the username</li> </ul>	
	Primary DN Field: UPN (User's Principal Name)	
	Secondary DN Field: None	
	OK Cancel Help	

أختر مجموعة AD-LDAP التي تم إنشاؤها مسبقا.تحقق من **أنه يجب وجود المستخدمين... للاتصال.**في حقول التعيين، أختر **UPN** للأساسي و**none** للثانوي.

- 11. أخترت ال **SSL VPN** قسم من القائمة.
- 12. في قسم الأسماء المستعارة للاتصال، أكمل الخطوات التالية:**الشكل 21: الأسماء المستعارة للاتصال**

🖆 Edit SSL VPN Connect	ion Profile: AC-USERS		X
Basic	Portal Page Customization:	DfltCustomization	Manage
General	CSD Alternate Group Policy:	DfltGrpPolicy	Manage
- Client Addressing - Authentication - Authorization	Enable the display of Rad	dius Reject-Message on the login screen when authent	ication is rejected
Accounting	Connection Aliases		
SSL VPN	💠 Add 🗹 Delete		
	Alias	Enabled	
	Group URLs		
	URL	Enabled	
	OK (	Cancel Help	

أختر **إضافة**.أدخل الاسم المستعار للمجموعة التي تريد إستخدامها.تأكد من أن **ممكن** يكون محددا. انظر الشكل 21.

13. وانقر فوق **OK**.

**ملاحظة:** انقر فوق **حفظ** لحفظ التكوين في ذاكرة Flash (الذاكرة المؤقتة).

قواعد مطابقة الشهادة (إذا كان سيتم إستخدام OCSP)

1. أخترت Remote Access VPN > **متقدم > شهادة إلى SSL VPN توصيل خرائط**. انظر الشكل 22.أختر **إضافة** في قسم خرائط توصيفات التوصيل.يمكنك الاحتفاظ بالخريطة الموجودة كخريطة DefaultCertificateMap في قسم الخريطة أو إنشاء خريطة جديدة إذا كنت تستخدم بالفعل خرائط الثقة ل IPsec.حافظ على أولوية القاعدة.تحت مجموعة معينة، أترك باسم — **غير معين** —. انظر الشكل 22.ا**لشكل 22: إضافة قاعدة مطابقة الشهادات** 

Configure a certificate matchin rule priority uniquely identifies to the rule with lower values h will be ignored.	ng rule and associ the certificate ma aving greater pric	ate it with a connection profile. Th atching rule and assigns a priority prity. Rules that are not mapped
Map:	<ul> <li>Existing</li> </ul>	DefaultCertificateMap
	🚫 New	
Priority:	20	

فوق OK.

- 2. انقر فوق **إضافة** في الجدول السفلي.
- 3. في نافذة "معيار إضافة قاعدة مطابقة الشهادة"، أكمل الخطوات التالية:**الشكل 23: معيار قاعدة مطابقة الشهادة**

Add Certificate Match	ing Rule Criterion		
Configure a certificate matc	hing rule criterion		
Rule Priority: Mapped to Connection Profi	20 e: Not Mapped		
Field	Component	Operator Does Not Equal	Value
	OK Cancel	Help	

الاحتفاظ بعمود الحقل إلى **الموضوع**.الاحتفاظ بعمود المكون في **الحقل بأكمله**.قم بتغيير عمود عامل التشغيل إلى **لا يساوي**.في عمود القيمة، أدخل علامتي اقتباس ".طقطقة ok و**يطبق**. راجع الشكل 23 على سبيل المثال.

# <u>تکوین OCSP</u>

يمكن أن يختلف تكوين OCSP ويتوقف على مورد مستجيب OCSP. اقرأ دليل المبشرين لمزيد من المعلومات.

<u>تكوين شهادة المستجيب OCSP</u>

- 1. الحصول على شهادة تم إنشاؤها ذاتيا من المستجيب OCSP.
- 2. أكمل الإجراءات المذكورة سابقا وقم بتثبيت شهادة لخادم OSCP.**ملاحظة:** تأكد من تحديد **عدم التحقق من شهادات الإلغاء** لنقطة الثقة لشهادة OCSP.

<u>تكوين CA لاستخدام OCSP</u>

1. أختر **إدارة شهادات الوصول عن بعد > شهادات CA**.

- 2. ركزت OCSP in order to أخترت CA أن يشكل أن يستعمل OCSP.
  - 3. انقر فوق **تحرير**.
  - 4. تأكد من التحقق من **شهادة الإبطال**.
- 5. في قسم طرق الإبطال، قم بإضافة OCSP. انظر الشكل 24.**التحقق من إبطال OCSP**

dit Options for CA Cert Revocation Check CRL Retr	ificate	dvanced
O Do not check certificates	for revocation	
<ul> <li>Check certificates for re Revocation Methods</li> <li>Specify the methods u method will be used or</li> </ul>	vocation sed for revocation checking and their order. If both r ily if the first one returns error.	nethods are selected, the second
CRL	Add>> OCSP	Move Up
	< <remove< th=""><th>Move Down</th></remove<>	Move Down
Consider certificat	e valid if revocation information cannot be retrieved	
	OK Cancel Help	

6. تأكد من أن **إعتبار الشهادة صالحة... لا يمكن إستردادها** إذا كنت تريد اتباع فحص OCSP الصارم. **ملاحظة:** تكوين/تحرير جميع خادم CA الذي يستخدم OCSP للإبطال.

### <u>تکوین قواعد OCSP</u>

**ملاحظة:** تحقق من إنشاء نهج مطابقة لمجموعة الشهادات ومن تكوين المستجيب OCSP قبل إكمال هذه الخطوات.

**ملاحظة:** في بعض عمليات تنفيذ OCSP، قد تكون هناك حاجة إلى سجل DNS A و PTR لمكتب خدمات الدعم التقني. يتم إجراء هذا التحقق للتحقق من أن ASA من موقع mil.

#### 1. أخترت Remote Access VPN> شهادة إدارة>CA شهادة 2.

- 2. ركزت OCSP in order to أخترت CA أن يشكل أن يستعمل OCSP.
  - 3. أختر **تحرير**.
  - 4. انقر فوق علامة التبويب **قاعدة OCSP**.
    - 5. انقر فوق **إضافة (Add).**
- 6. في نافذة إضافة قاعدة OCSP، أكمل الخطوات التالية. راجع الشكل 25.**الشكل 25: إضافة قواعد OCSP**

Certificate Map:	DefaultCertificateMap
Certificate:	[cn=OCSP, ou=AMHS, o=Army, c=us]:[cn=OCSP, ou=AMHS.
Index:	10
URL:	http://ocsp.disa.mil

خريطة الشهادة، أختر DefaultCertificateMap أو خريطة تم إنشاؤها مسبقا.في خيار الشهادة، أختر **المستجيب OCSP**.في خيار الفهرس، قم بإدخال 10.في خيار عنوان الربط، أدخل عنوان IP أو اسم المضيف الخاص بالمستجيب OCSP. إذا كنت تستخدم اسم المضيف، فتأكد من تكوين خادم DNS على ASA.وانقر فوق OK.طقطقة **يطبق**.

# <u>تکوین عمیل AnyConnect من Cisco</u>

يغطي هذا القسم تكوين عميل Cisco AnyConnect VPN.

**الافتراضات**— تم تثبيت عميل AnyConnect VPN من Cisco وتطبيق Middleware بالفعل في الكمبيوتر المضيف. تم إختبار ActiveCard Gold و ActiveClient.

**ملاحظة:** يستخدم هذا الدليل أسلوب URL المجموعة للتثبيت الأولي لعميل AC فقط. بمجرد تثبيت عميل AC، تقوم بتشغيل تطبيق AC تماما مثل عميل IPsec.

**ملاحظة:** يلزم تثبيت سلسلة شهادات DoD على الجهاز المحلي. ارجع إلى PKI POC للحصول على ملف الشهادات/الدفعة.

**ملاحظة:** برنامج تشغيل قارئ البطاقة ل Mac OSX مثبت بالفعل ومتوافق مع إصدار نظام التشغيل الحالي الذي تستخدمه.

### <u> Cisco AnyConnect VPN Client - Mac OS X تنزيل</u>

- 1. إطلاق موقع جلسة إلى ال ASA من خلال Safari. ينبغي أن يكون العنوان على شكل -https://Outside Interface. على سبيل المثال، https://172.18.120.225.
  - 2. إطار منبثق يطلب التحقق من شهادة ASA. انقر فوق **متابعة**.
- 3. يظهر نافذة منبثقة أخرى لإلغاء تأمين سلسلة مفاتيح CAC. أدخل رقم التعريف الشخصي (PIN). راجع الشكل 31.**شكل 31: أدخل رمز PIN**

	Unlock	Keychain
a	Please enter your	keychain password.
	Safari wants to use "CAC-2050-5000-1	ceychain 028-0004-5279".
	Password:	
▶ Details		
?		Cancel OK

- 4. بعد أن تظهر صفحة ويب SSL VPN-service، انقر فوق **متابعة**.
- 5. بعد إلغاء تأمين سلسلة المفاتيح، يطالبك المستعرض إذا كنت تثق في الشهادة من ASA. انقر فوق **الثقة**.
  - 6. أدخل كلمة مرور الجذر لإلغاء تأمين سلسلة المفاتيح لإنشاء اتصال آمن، ثم انقر على **موافق**.
    - 7. أختر الشهادة التي تريد إستخدامها لمصادقة العميل، ثم انقر على **موافق**.
    - 8. ثم يطلب المستعرض كلمة مرور الجذر/المستخدم للسماح بتنزيل عملاء AnyConnect.
- 9. إذا تمت المصادقة عليه، يبدأ عميل AnyConnect في التنزيل. راجع الشكل 32. **شكل 32: تنزيل AnyConnect**

B WebLaunch	Using Sun Java for Installation
	Launching Cisco AnyConnect VPN Client
V _ Platform	If the software does not start properly, Click her
Time Left: 1 sec (1.3) Transfer rate: 646 KE	7 MB of 2.47 MB copied) I/Sec

- 10. بعد تنزيل التطبيق، يطالبك المستعرض بقبول شهادة ASA. انقر فوق **قبول**.
  - 11. تم تأسيس الاتصال. شكل 33.**شكل AnyConnect:33 متصل**

	😑 😑 🔿 🦳 Cisco AnyCo	nnect VPN Client
WebLaunch	Connected to	ाsco
- Platform Detection	Duration: 00:00:29	Disconnect
- ActiveX	Client Address 20.1.1.1 Server Address 20.1.1.1	6
- Java Detection	Bytes Sent 6675 Bytes Received 680	0
- Sun Java	Connection Log	

### بدء تشغيل AnyConnect VPN Client من Cisco - نظام التشغيل Mac OS X

من Finder—Applications > عميل AnyConnect VPN من

**ملاحظة:** راجع الملحق (ه) للحصول على تكوين ملف تعريف عميل AnyConnect الاختياري.

### <u>اتصال جديد</u>

تظهر نافذة التيار المتردد. انظر الشكل 37.

شکل 37: اتصال VPN جدید

AC الاتصال تلقائيا.		Version 2.1.01
AC الاتصال تلقائيا.		Version 2.1.01
AC الاتصال تلقائيا.		Version 2.1.01
AC الاتصال تلقائيا.		Version 2.1.01
AC الاتصال تلقائيا.		Version 2.1.01
AC الاتصال تلقائيا.		
. راجع الشکل 38 <b>. شکل 38: أدخل رمز PIN</b> Unlock Keychain	ب إذا لم يحاول ا يطلب منك ذلك	ختر المضيف المناسر دخل رمز PIN عندما
Please enter your keychain	password.	
Cisco AnyConnect VPN Client wa CAC-4090-0029-8400-0005-	ints to use k 60C1".	eychain
Password:		
etails		

### <u>بدء الوصول عن بعد</u>

- 1. أختر المجموعة والمضيف اللذين تريد الاتصال بهما.
- 2. أخترَت بما أنّ شهّادات استعملت، **يربط** in order to أسست ال VPN. راجع الشكل 39.**ملاحظة:** نظرا لأن الاتصال يستخدم الشهادات، فلا حاجة لإدخال اسم مستخدم وكلمة مرور.**شكل 39: التوصيل**

Connect to:	10.86.95.252	. (C. ana ana ana	CISCO
VPN session and	ad.		
Group:	SVC	÷	
Username:	CACUSER		
Password:		· · · · · · · · · ·	
		Get Cer	tificate

الملحق (ه) للحصول على تكوين ملف تعريف عميل AnyConnect الاختياري.

# <u>الملحق أ - تخطيط LDAP و DAP</u>

في الإصدار x)7.1 من ASA/PIX والإصدارات الأحدث، تم تقديم ميزة تسمى تخطيط LDAP. هذه ميزة قوية توفر تعيين بين سمة Cisco وكائنات/سمة LDAP، مما ينفي الحاجة إلى تغيير مخطط LDAP. لتنفيذ مصادقة CAC، يمكن أن يدعم هذا فرض سياسات إضافي على اتصال الوصول عن بعد. هذا مثال من LDAP يخطط. اعلم أنك تحتاج إلى حقوق المسؤول لإجراء تغييرات في خادم AD/LDAP. في برنامج ASA 8.x، تم تقديم ميزة سياسة الوصول الديناميكي (DAP). يمكن أن يعمل بروتوكول DAP بالاقتران مع CAC للنظر في مجموعات AD متعددة بالإضافة إلى سياسات الدفع وقوائم التحكم في الوصول وما إلى ذلك.

<u>السيناريو 1: تطبيق Active Directory باستخدام الطلب الهاتفي لأذن الوصول عن بعد - السماح</u> بالوصول/رفضه

يخطط هذا المثال سمة AD msNPAllowDailin إلى سمة Cisco cVPN3000-tunneling- البروتوكول.

• قيمة سمة AD: صواب = السماح؛ خطأ = رفض • قيمة سمة IPsec + 16 WebVPN) = true 4) أو 20 (Cisco: 1 = false، 4 (IPSec + 16 WebVPN، للشرط "السماح"، قم بتعيين:

> • صحيح = 20 لرفض الطلب الهاتفي، تقوم بتعيين:

• خطأ = 1 **ملاحظة:** تأكد من أن TRUE و FALSE في كل الحروف كبيرة. راجع <u>تكوين خادم خارجي لتفويض مستخدم جهاز</u> <u>الأمان</u> للحصول على مزيد من المعلومات.

### **Active Directory**

1. في خادم Active Directory، انقر فوق **ابدأ > تشغيل**. 2. في مربع النص المفتوح، اكتب **dsa.msc** ثم انقر **موافق**. يقوم هذا بتشغيل وحدة تحكم إدارة Active

.Directory

- 3. في وحدة تحكم إدارة Active Directory Users and، انقر فوق علامة الجمع لتوسيع Active Directory Users and. Computers.
  - 4. انقر فوق علامة الجمع لتوسيع اسم المجال.
- 5. إذا كان لديك وحدة تخزين تم إنشاؤها للمستخدمين، فقم بتوسيع وحدة التحكم لعرض كافة المستخدمين، وإذا كان لديك كافة المستخدمين الذين تم تعيينهم في مجلد المستخدمين، فقم بتوسيع هذا المجلد لعرضهم. راجع الشكل A1.**الشكل A1: وحدة تحكم ادارة Active Directory**

🚡 labrat - [Console Root\Active Dire	ectory Users and Computers	[Ciscojax-2k3.labrat.com]\la	brat.com\MIL]	- O ×
File Action Yew Favorites Y     ← →	lindow Help 13 12 10 10 10 10 10 10 10 10 10 10 10 10 10	č		_ ® ×
Console Root Active Directory Users and Comp Active Directory Users and Comp Builtin Computers Domain Controllers Domain	Name Clark Kent Ethan Hunt Pater Parker	User User User	Description	
	•			•

6. انقر نقرا مزدوجا فوق المستخدم الذي تريد تحريره.انقر فوق علامة التبويب "الطلب الهاتفي" في صفحة خصائص المستخدم وانقر فوق **السماح** أو **الرفض**. راجع الشكل أ 2.ا**لشكل ألف 2: خصائص المستخدم** 

ark Kent Properties	?
Environment   Sessions   Remote control   1 General   Address   Account   Profile Published Certificates   Member Of	Terminal Services Profile   COM   Telephones   Organization Dial-in   Object   Security
Remote Access Permission (Dial-in or VPN)	I
Allow access	
C Deny access	
C Control access through Remote Access	Bolicy
L Verify Caller ID:	
Callback Options	
No Callback	
Set by Caller (Routing and Remote Acc	ess Service only)
C Always Callback to:	
C Assign a Static IP Address	
Apply State Boutes	, 
Define routes to enable for this Dial-in connection.	Static Roytes
OK	Cancel Apply

7. ثم انقر فوق **OK**.

### <u>تکوین ASA</u>

- 1. في ASDM، أختر **إعداد AAA للوصول عن بعد VPN> > خريطة سمة LDAP**.
  - 2. انقر فوق **إضافة (Add)**.
- 3. في نافذة خريطة إضافة سمة LDAP، أكمل الخطوات التالية. انظر الشكل أ 3.**الشكل A3: إضافة تعيين سمة** LDAP

🖆 Add LDAP Attribute Map				X
Name: msNPAllowOlalin (Sector)				
Customer Name: InsNPAllowDialin Control Contro	Add >>	Customer Name	Cisco Name	
	K Cencel	Help		

أدخل اسما في مربع نص الاسم.في علامة التبويب "اسم الخريطة"، اكتب msNPAllowDialin في مربع النص "اسم العميل".في علامة التبويب اسم الخريطة، أختر **بروتوكولات** الاتصال النفقي في الخيار المنسدل في اسم Cisco.انقر فوق **إضافة (Add)**.أختر علامة التبويب **تعيين قيمة**.انقر فوق **إضافة (Add)**.في نافذة قيمة خريطة LDAP للسمة المضافة، اكتب TRUE في مربع النص اسم العميل واكتب 20 في مربع النص قيمة Oisco.انقر فوق **إضافة (Add)**.اكتب FALSE في مربع نص اسم العميل واكتب 1 في مربع نص قيمة Oisco. راجع الشكل أ4

ustomer Name: InsNPAlowDialn				
		Customer Value	Cisco Value	
Customer Value:	Add >>	TRUE	1 20	
Cisco Value:	<< Remove			

وانقر فوق OK.وانقر فوق OK.طقطقة **يطبق**.يجب أن يبدو التكوين مثل الشكل A5.**الشكل A5: تكوين تعيين سمة LDAP** 

🗱 Cisco ASDM 6.0 for ASA - 172	.18.120.225	
<u>File View Tools Wizards Windo</u>	الطاعة المراجع	alulu
Home 🖧 Configuration 💽 M	onitoring 🔚 Save 🔇 Refresh 🔇 Back 💭 Forward 🢡 Help	CISCO
Remote Access V @ 9 ×	Configuration > Remote Access VPN > AAA Setup > LDAP Attribute Map	
Image: Network (Client) Access		
AAA Setup	Add and configure attribute map used by LDAP server.	
DAP Attribute Map	Name Attribute Marchines	
🖉 Local Users	mstDAlouCiplo mstDAlouCiplo_Tuppelog.2xstocols	
a 🔥 Secure Desktop Manager 🞽		
Device Setup		D
🕄 Firewall		
Remote Access VPN		
Site-to-Site VPN		
Device Management		
». ·	Apply as Reset	
Device configuration loaded	cisco 15 🐻 🛃 💽 7/17	7/07 1:56:07 PM UTC

4. أختر **إعداد AAA للوصول عن بعد VPN> > مجموعات خوادم AAA**. انظر الشكل ألف 6.**الشكل A6:** مجموعات خوادم AAA

📸 Cisco ASDM 6.0 for ASA - 172	2.18.120.225				
File Yew Tools Wigards Windo	w Help	Look For:	and Assessed	Find +	abab
Remote Access V a 9 ×	Configuration > Ren	note Access VP	N > AAA Setup > AAA	Server Groups	
Clientless SSL VPN Access     AAA Setup	AAA Server Groups Server Group	Protocol	Accounting Mode	Reactivation M	Add
Local Users	AD-LDAP LOCAL	LDAP		Depletion	Edit
R A Secure Desktop Manager ≥	C Servers in the Selector	() (Crosp		<u>)</u>	Delete
Device Setup	Server Name or IP	Address	Interface	Timeout	Add
Firewall	172-18-120-160		outside		Edit
Remote Access VPN					Delete
Device Management					Move Down
×			Apply Reset		
Device configuration loaded	cis	co 15		7/17/	07 1:59:07 PM UT

- 5. انقر فوق مجموعة الخوادم التي تريد تحريرها. في الخوادم الموجودة في قسم المجموعة المحددة، أختر عنوان IP الخاص بالخادم أو اسم المضيف، ثم انقر فوق **تحرير**.
- 6. في نافذة Edit AAA Server، في مربع نص خريطة سمة LDAP، أختر خريطة سمة LDAP التي تم إنشاؤها في القائمة المنسدلة. راجع الشكل A7**الشكل A7: إضافة تعيين سمة LDAP**

🚰 Edit AAA Server							
Server Group:	AD-LDAP						
Interface Name:	outside						
Server Name or IP Addr	ess: 172.18.120.160						
Timeout:	10 sec						
LDAP Parameters							
Enable LDAP over	SSL						
Server Port:	389						
Server Type:	Detect Automatically/Use Generic Type						
Base DN:	CN=Users,DC=ggsgseclab,DC=org						
Scope:	One level beneath the Base DN						
Naming Attribute(s):	userPrincipalName						
Login DN:	CN=Administrator,CN=Users,DC=ggsgseclab,DC=o						
Login Password:	•••••						
LDAP Attribute Map:	msNPAllowDialin						
SASL MD5 authentication							
🔄 SASL Kerberos au	SASL Kerberos authentication						
Kerberos Server G	roup; [						
	ЭК	Cancel Help					

7. وانقر فوق OK.

**ملاحظة:** قم بتشغيل تصحيح LDAP بينما تقوم بالاختبار للتحقق من عمل ربط LDAP وتخطيط السمات بشكل صحيح. راجع الملحق (ج) للحصول على أوامر أستكشاف الأخطاء وإصلاحها.

<u>السيناريو 2: تطبيق Active Directory باستخدام عضوية المجموعة للسماح بالوصول أو رفضه</u>

يستخدم هذا المثال تعيين عضو سمة LDAP لسمة بروتوكول الاتصال النفقي لإنشاء عضوية مجموعة كشرط. لكي تنجح هذه السياسة، يجب أن تتوفر لديك هذه الشروط:

- أستخدم مجموعة موجودة بالفعل أو قم بإنشاء مجموعة جديدة لمستخدمي ASA VPN ليكونوا عضوا في شروط السماح.
- أستخدم مجموعة موجودة بالفعل أو قم بإنشاء مجموعة جديدة لمستخدمي غير ASA لتكون عضوا في شروط الرفض.
  - تأكد من إيداع عارض LDAP الذي يتوفر لديك DN الصحيح للمجموعة. انظر الملحق د. إن يكون ال DN خطأ، ال يخطط لا يعمل بشكل صحيح.

**ملاحظة:** اعلم أنه يمكن ل ASA قراءة السلسلة الأولى من السمة memeberOf فقط في هذا الإصدار. تأكد من أن المجموعة الجديدة التي تم إنشاؤها موجودة في أعلى القائمة. الخيار الآخر هو أن تضع حرف خاص أمام الاسم عندما ينظر AD إلى الحروف الخاصة أولا. للعمل حول هذا التحذير، أستخدم DAP في برنامج x.8 للنظر في مجموعات متعددة.

**ملاحظة:** تأكد من أن المستخدم جزء من مجموعة الرفض أو على الأقل مجموعة أخرى بحيث يتم إرسال العضو مرة أخرى إلى ASA دائما. لا يتوجب عليك تحديد شرط الرفض الكاذب ولكن أفضل ممارسة هي القيام بذلك. إذا كان اسم المجموعة الموجود أو اسم المجموعة يحتوي على مسافة، فأدخل السمة بهذه الطريقة:

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

**ملاحظة:** يسمح DAP لمكتب المحاسبة المستقل بالنظر إلى مجموعات متعددة في السمة memberOf والتفويض الأساسي لهذه المجموعات. راجع قسم DAP.

رسم الخرائط

• قيمة سمة AD:عضو CN=AsauSers،CN=Users،DC=ggsgseclab،DC=orgعضو CN=TelnetClient،CN=Users،DC=Labrat،DC=com • قيمة سمة Cisco: 1 خطأ، true = 20،

من أجل شرط **السماح**، تقوم بالتعيين:

• عضو CN=AsauSers،CN=Users،DC=ggsgseclab،DC=org= 20

بالنسبة لشرط **الرفض**، تقوم بتعيين:

• عضو CN=TelnetClient،CN=Users،DC=ggsgseclab،DC=org = 1

**ملاحظة:** في الإصدار المستقبلي، هناك سمة Cisco للسماح بالاتصال ورفضه. راجع <u>تكوين خادم خارجي لتفويض</u> <u>مستخدم جهاز الأمان</u> للحصول على مزيد من المعلومات حول سمات Cisco.

### Active Directory إعداد

- 1. في خادم Active Directory، أختر **ابدأ > تشغيل**.
- 2. في مربع النص المفتوح، اكتب **dsa.msc**، ثم انقر **موافق**. يقوم هذا بتشغيل وحدة تحكم إدارة Active Directory.
- 3. في وحدة تحكم إدارة Active Directory Users and، انقر فوق علامة الجمع لتوسيع Active Directory Users and Computers. انظر الشكل أ 8**الشكل A8: مجموعات Active Directory**

PACTIVE DIrectory Users and Compo	uters				
Eile Action Yew Window He	lp .			_82	
> 🗈 📧 👗 🗙 😭	8 2 2 2 2 2 2 2	E Contra de			
Active Directory Users and Computer Saved Queries Big Iabrat.com Builtin	Users 23 objects				
	Name	Туре	Description	1	
	🖸 Administrator	User	Built-in account for administering the co		
	2 artperez	User			
Computers	ASAUsers	Security Group	VPN Remote Access Users	0.000	
+ O Doman Controlers	Cert Publishers	Security Group	Members of this group are permitted to		
PoregroecunkyPrincipas	CERTSVC_DCOM_ACCESS	Security Group			
a linere	2 Dris Admins	Security Group	DNS Administrators Group		
	DhsUpdateProxy Security Group DNS clients who a		DNS clients who are permitted to perfor		
	Domain Admins	Security Group	Designated administrators of the domain		
	Domain Computers	Domain Computers Security Group All workstations and servers joined			
	Domain Controllers	Security Group	All domain controllers in the domain		
	Domain Guests	Security Group	All domain guests		
	Domain Users	Security Group	All domain users		
	Enterprise 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		
	RAS and IAS Servers	Security Group	Servers in this group can access remote		
	Schema Admins	Security Group	Designated administrators of the schema		
	5UPPORT_388945a0	User	This is a vendor's account for the Help a		
1	# Teinet Clients	Security Group	Members of this group have access to T	1999	

- 4. انقر فوق علامة الجمع لتوسيع اسم المجال.
- 5. انقر بزر الماوس الأيمن فوق المجلد **المستخدمون** واختر **جديد > مجموعة**.
  - 6. أدخل اسم مجموعة. على سبيل المثال: AsauSers.
    - 7. وانقر فوق O**K**.
- 8. انقر فوق المجلد **المستخدمون**، ثم انقر نقرا مزدوجا فوق المجموعة التي أنشأتها للتو.
  - 9. أختر علامة التبويب **أعضاء**، ثم انقر فوق **إضافة**.
  - 10. اكتب اسم المستخدم الذي تريد إضافته، ثم انقر فوق **موافق**.

### <u>تکوین ASA</u>

- 1. في ASDM، أختر **Remote Access VPN (الوصول عن بعد) > إعداد AAA > خريطة سمة LDAP**.
  - 2. انقر فوق **إضافة (Add)**.
- 3. في نافذة خريطة إضافة سمة LDAP، أكمل الخطوات التالية. انظر الشكل أ 3.أدخل اسما في مربع نص الاسم.في علامة التبويب "اسم الخريطة"، اكتب عضو في مربع النص "ج" الخاص ب "اسم العميل".في علامة التبويب اسم الخريطة، أختر بروتوكولات الاتصال النفقي في مربع النص "ج" الخاص ب "اسم العميل".في علامة وقو علامة التبويب اسم الخريطة، أختر إضافة. اكتب عضو في مربع النص "ج" الخاص ب "اسم العميل".في علامة التبويب اسم الخريطة، أختر بروتوكولات الاتصال النفقي في الخيار المنسدل في اسم Oisco.أختر إضافة.انقر فوق علامة التبويب تعيين قيمة.أختر إضافة.في نافذة قيمة خريطة LDAP لسمة الإضافة، اكتب فوق علامة التبويب تعيين قيمة.أختر إضافة.في نافذة قيمة خريطة LDAP لسمة الإضافة، اكتب فوق علامة التبويب تعيين قيمة.أختر إضافة.في نافذة قيمة خريطة LDAP لسمة الإضافة، اكتب Oisco.أختر إضافة.انقر فوق علامة التبويب تعيين قيمة.أختر إضافة.في نافذة قيمة خريطة LDAP لسمة الإضافة، اكتب أولافة.انقر فوق علامة التبويب تعيين قيمة.أختر إضافة.في نافذة قيمة خريطة LDAP لسمة الإضافة، اكتب Cisco فوق علامة التبويب تعيين وقيمة.أختر إضافة.في نافذة قيمة خريطة Cisco لصم المم العميل واكتب O في مربع نص المام العميل واكتب O. في مربع نص قيمة O. المام العميل واكتب 10 في مربع نص قيمة مربع النص اسم العميل واكتب 10 في مربع في مربع قيمة O. المام العميل واكتب 1 في مربع نص قيمة O. الماك O. الحم الماك أ4.وانقر فوق إضافة (Add). كتب Cisco مادع الشكل أ4.وانقر فوق Add).وانقر فوق إضافة O. المكل Add ماك ملاحيل أ4.وانقر فوق Add).وانقر فوق Add).وانقر فوق Add).وانقر فوق Add) وم Add ماك أ4.وانقر فوق مال.وانقر فوق Add).وانقر فوق Add).وانقر فوق المالي 20.00.ملي مالم Add). يطبق.يجب أن يبدو التكوين مثل الشكل Add).

Cisco ASDM 6.0 for ASA - 172	2.18.120.225			
Ele Yew Tools Wigards Windo	w Help Ionitoring 📊 Save	Look For:	Serverd ? He	
Remote Access V 🗗 🕈 🗡	Configuration > Re	mote Access VPN > AA	A Setup > LDAP Attrit	oute Map 🗆
Network (Client) Access     AAA Setup     AAA Setup     AAA Setver Groups	Add and configure	a attribute map used by LD	AP server.	
LOAP Attribute Map	Name	Attribute Map Nam	e	
€ 👫 Secure Desktop Manager ≚ <	memberOf	memberOf-Tunnein	ig-Protocols	
Revice Setup				D
Firewall				
Remote Access VPN				
Site-to-Site VPN				
Device Management				
<u>ه</u> ۲		Apply	Reset	
Configuration changes say	d	sco 15	li 🛃 🔂	7/17/07 2:14:47 PM UTC

- 4. أختر **إعداد AAA للوصول عن بعد VPN> > مجموعات خوادم AAA**.
- 5. انقر فوق مجموعة الخوادم التي تريد تحريرها. في الخوادم الموجودة في قسم المجموعة المحددة، حدد عنوان IP الخاص بالخادم أو اسم المضيف، ثم انقر فوق

ne Customer to Cisco Map Value	
CN—Telnet Clients, CN—Users, DC—ggsgsedab, DC—org—1 CN—ASAUsers, CN—Users, DC—apsosedab, DC—ara—20	
len vergensler 19.5 service og en	Edit
	Delete

6. في نافذة Edit AAA Server، في مربع نص خريطة سمات LDAP، حدد خريطة سمات LDAP التي تم إنشاؤها في القائمة المنسدلة.

7. وانقر فوق OK.

**ملاحظة:** قم بتشغيل تصحيح LDAP بينما تقوم بالاختبار للتحقق من أن ربط LDAP وتعيينات السمات تعمل بشكل صحيح. راجع الملحق (ج) للحصول على أوامر أستكشاف الأخطاء وإصلاحها.

### <u>السيناريو 3: سياسات الوصول الديناميكي للعديد من سمات الأعضاء</u>

يستخدم هذا المثال DAP للنظر في سمات أعضاء متعددين للسماح بالوصول بناء على عضوية مجموعة Active Directory. قبل x.8، كان ASA يقرأ أول سمة عضو فقط. مع x.8 والإصدارات الأحدث، يمكن أن يقوم ASA بالنظر إلى جميع سمات أعضاء Of.

- أستخدم مجموعة موجودة بالفعل أو قم بإنشاء مجموعة جديدة (أو مجموعات متعددة) لمستخدمي ASA VPN ليكونوا أعضاء في شروط السماح.
- أستخدم مجموعةً موجودة بالفعلّ أو قم بإنشاء مجموعة جديدة لمستخدمي غير ASA لتكون عضوا في شروط الرفض.
- تأكد من إيداع عارض LDAP الذي يتوفر لديك DN الصحيح للمجموعة. انظر الملحق د. إن يكون ال DN خطأ، ال يخطط لا يعمل بشكل صحيح.

### <u>تکوین ASA</u>

- 1. في ASDM، أختر **الوصول عن بعد إلى شبكة VPN> (العميل) > سياسات الوصول الديناميكية**.
  - 2. انقر فوق **إضافة (Add)**.
- 3. في نهج إضافة الوصول الديناميكي، أكمل الخطوات التالية:أدخل اسما في مربع نص الاسم ب.في قسم الأولوية، أدخل 1، أو رقم أكبر من 0.في فئة التحديد، انقر فوق **إضافة**.في سمة إضافة AAA، أختر LDAP .في قسم معرف السمة، أدخل memberOf.في قسم القيمة، أختر = وأدخل اسم مجموعة الإعلان. كرر هذه الخطوة لكل مجموعة تريد الإشارة إليها. راجع الشكل A10.**شكل خريطة سمة AAA10**

🛤 Add AAA	A Attribute 🛛 🔀
AAA Attribut	te Type: LDAP
Attribute ID:	memberOf
Value:	= ASAUsers
	Cancel Help
وانقر فوق OK.في قسم سمات	

الوصول، **أختر إستمرار**. انظر الشكل أ 11.**الشكل A11 إضافة سياسة ديناميكية** 

ziption: Multi-Group Membership Check			Priority: 1	
ection Offeria refine the AAA and endpoint attributes used to select this access elow and every endpoint attribute has been satisfied. These att pedity the logical expression text.	spolicy. A policy ributes can be or	is used when a user's a nated using the tables	uthorization attributes match the AA below and/or by expanding the Adv	A attribute oriteria anced option to
User has ANY of the following AAA Attributes values		and the following end	ipoint attributes are satisfied.	
AAA Attribute Operation/Value	Add	Endpoint ID	Name/Operation/Value	Add
dap.memberOf = _ACAUSers dap.memberOf = YPNUsers	Edit			Edit
	Delete			Delete
4				Logical Op.
Advanced				(8)
Action Network ACL Filters Web-Type ACL Filters Functions Action:   Continue Terminate	Port Forward	ng Lists URL Lists Ad	cess Method	
Specify the message that will be displayed when this record is a	selected.			
User Message:				

- 5. أختر **نهج الوصول الافتراضي** واختر Edit **(تحرير)**.
- 6. يجب تعيين الإجراء الافتراضي على **إنهاء**. انظر الشكل أ 12.**الشكل A12 تحرير السياسة الديناميكية**

🗯 Edit D	ynamic <i>I</i>	ccess Policy	,			×
Policy N	lame: DfltA	ccessPolicy				
Descrip	tion:					
Con	<mark>is Policy Att</mark> ifigure acce	ribut <del>es</del> ss policy attribu	tes for this policy. Attrib	utes values	specified here will override those values obtained from the AAA system.	1
Ac	tion Netw	ork ACL Filters	Web-Type ACL Filters	Functions	Port Forwarding Lists URL Lists Access Method	
S	action: ipeofy the r	Continue	• • Terminate	record is s	elected.	
U	Jser Messag	le:				
			OK		Cancel Help	

7. وانقر فوق **OK**.

**ملاحظة:** إذا لم يتم تحديد **إنهاء**، يتم السماح لك بالدخول حتى إذا لم تكن في أي مجموعات لأن الافتراضي هو المتابعة.



#### ASA 5510

```
ciscoasa#show running-config
                                           Saved :
                                  (ASA Version 8.0(2
                                                 !
                                     hostname asa80
                                domain-name army.mil
            enable password 8Ry2YjIyt7RRXU24 encrypted
                                             names
                                                 !
                         interface GigabitEthernet0/0
                                     nameif outside
                                   security-level 0
                   ip address x.x.x.x 255.255.255.128
                                                 !
                        interface GigabitEthernet0/1
                                      nameif inside
                                 security-level 100
                                      no ip address
                                                 1
                     boot system disk0:/asa802-k8.bin
                                   ftp mode passive
                         dns server-group DefaultDNS
                                domain-name army.mil
                                                 !
       -----ACL's------
                                       _____
            access-list out extended permit ip any any
                _____
                                       _____
                                     pager lines 24
                           logging console debugging
                                   mtu outside 1500
                                                 1
  -----VPN Pool------
                                       _____
 ip local pool CAC-USERS 192.168.1.1-192.168.1.254 mask
                                      255.255.255.0
      _____
                                                 1
                                       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
                                                    1
           -----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 3082037a a0030201 02020231 9e300d06 092a8648 30820411 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 a0030201 02020105 300d0609 2a864886 30820258 30820370 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 5a170d32 39313230 35313530 30303130 31333135 30343132 3031305a 305b310b 0355040a 130f552e 18301606 02555331 55040613 30090603 532e2047 6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b 1303504b 0403130d 446f4420 526f6f74 20434120 14060355 49311630 32308201 crypto ca certificate chain ASDM\_TrustPoint4 certificate ca 04 308201d0 a0030201 02020104 300d0609 2a864886 30820267 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 ! -----SSL/WEBVPN-----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 -----VPN Group/Tunnel Policy-----group-policy CAC-USERS internal ggroup-policy AC-USERS internal group-policy AC-USERS attributes vpn-tunnel-protocol svc address-pools value CAC-USERS webvpn 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-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

# الملحق ج- أستكشاف الأخطاء وإصلاحها

### أستكشاف أخطاء AAA و LDAP وإصلاحها

- **debug Idap 255 -**يعرض تبادلات LDAP
- debug aaa شائع 10—يعرض تبادلات AAA

المثال 1: الاتصال المسموح به مع تعيين السمة الصحيحة

يوضح هذا المثال إخراج debug ldap وdebug **aaa شائع** أثناء اتصال ناجح بالسيناريو 2 الموضح في الملحق (أ).

### الشكل C1: تصحيح أخطاء LDAP و debug aaa إخراج مشترك -تعيين صحيح 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 Session Start [78] New request Session, context 0x26f1c44, reqType = 0 [78] Fiber started [78] Creating LDAP context with uri=ldap:// [78] 172.18.120.160:389 Binding as administrator [78] Performing Simple authentication for Administrator [78] to 172.18.120.160 Connect to LDAP server: ldap:// 172.18.120.160, [78] = status Successful :LDAP Search [78] [Base DN = [CN=Users, DC=ggsgseclab, DC=org [Filter = [userPrincipalName=1234567890@mil [Scope = [SUBTREE :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 [78] .....com1.0 ...d,...& = userCertificate: value [78] t.....50....\*.H......0@1.0.....&....,d../......0'..0 .....com1.0 ...d,...& givenName: value = Ethan [78] distinguishedName: value = CN=Ethan [78] Hunt, OU=MIL, DC=labrat, DC=com 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 = [78] CN=ASAUsers, CN=Users, DC=ggsgseclab, DC=org 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] 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 [78]
                   = callback_aaa_task: status = 1, msg
                       AAA FSM: In aaa_backend_callback
      aaa_backend_callback: Handle = 39, pAcb = 2ae115c
   Fiber exit Tx=147 bytes Rx=4821 bytes, status=1 [78]
                                       Session End [78]
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-USERS ,
          ,AAA_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
                      Tunnelling-Protocol(4107) 20 20 1
                                :user policy attributes
                                                   None
                              :tunnel policy attributes
                  Primary-DNS(4101) 4 IP: 10.0.10.100 1
```

```
Secondary-DNS(4102) 4 IP: 0.0.0.0 2

Tunnelling-Protocol(4107) 4 4 3

"Default-Domain-Name(4124) 10 "ggsgseclab.org 4

List of address pools to assign addresses from(4313) 5

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
```

<u>المثال 2: الاتصال المسموح به بتعيين سمة Cisco التي تم تكوينها بشكل غير منتظم</u>

يوضح هذا المثال إخراج debug Idap وdebug **aaa شائع** أثناء اتصال مسموح به مع السيناريو 2 الموضح في الملحق (أ).

> الشكل C2: تصحيح أخطاء LDAP و debug aaa إخراج مشترك -تعيين غير صحيح

```
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
                                                       Ω
                     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
                                     Session Start [82]
New request Session, context 0x26f1c44, reqType = 0 [82]
                                     Fiber started [82]
                        Creating LDAP context with [82]
                           uri=ldap://172.18.120.160:389
                           Binding as administrator [82]
Performing Simple authentication for Administrator [82]
                                                      to
                                         172.18.120.160
Connect to LDAP server: ldap:// 172.18.120.160:389, [82]
                                                = status
                                              Successful
                                       :LDAP Search [82]
               [Base DN = [CN=Users, DC=ggsgseclab, DC=org
             [Filter = [userPrincipalName=1234567890@mil
                                       [Scope = [SUBTREE
                              :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 [82]
.....com1.0
                                              ...d,...&
                          = userCertificate: value [82]
t.....50....*.H......0@1.0.....&...,d../.....0'..0
                                        .....com1.0
                                              ...d,...&
                          givenName: value = Ethan [82]
               distinguishedName: value = CN=Ethan [82]
                           Hunt, OU=MIL, DC=labrat, DC=com
                           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 = [82]
              CN=ASAUsers, CN=Users, DC=ggsgseclab, DC=org
    = mapped to cVPN3000-Tunneling-Protocols: value [82]
              CN=ASAUsers, CN=Users, DC=ggsgseclab, DC=org
                         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....my [82]
       accountExpires: value = 9223372036854775807 [82]
                            logonCount: value = 25 [82]
                sAMAccountName: value = 1234567890 [82]
                 sAMAccountType: value = 805306368 [82]
         userPrincipalName: value = 1234567890@mil [82]
                           = objectCategory: value [82]
CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=or
                                                      q
               mail: value = Ethan.Hunt@labrat.com [82]
                   = callback_aaa_task: status = 1, msq
                       AAA FSM: In aaa_backend_callback
      aaa_backend_callback: Handle = 41, pAcb = 2ae115c
    Fiber exit Tx=147 bytes Rx=4821 bytes, status=1 [82]
                                       Session End [82]
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(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 = <none>, author svr = AD-= LDAP, user pol tunn pol = CAC-USERS , ,AAA\_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 Tunnelling-Protocol(4107) 20 0 1 :user policy attributes None :tunnel policy attributes Primary-DNS(4101) 4 IP: 10.0.10.100 1 Secondary-DNS(4102) 4 IP: 0.0.0.0 2 Tunnelling-Protocol(4107) 4 4 3 "Default-Domain-Name(4124) 10 "ggsgseclab.org 4 List of address pools to assign addresses from(4313) 5 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

# <u>أستكشاف أخطاء DAP وإصلاحها</u>

• تصحيح أخطاء DAP—يعرض أخطاء DAP • debug dap trace—يعرض تتبع وظيفة DAP

مثال 1: الاتصال المسموح به مع DAP

يوضح هذا المثال إخراج **أخطاء تصحيح الأخطاء** و**debug dap trace** أثناء اتصال ناجح بالسيناريو 3 الموضح في الملحق أ. لاحظ العديد من سمات الأعضاء. يمكنك الانضمام إلى كل من \_ASAUsers و VPNUsers أو tp أي من المجموعتين، والتي تعتمد على تكوين ASA.

#### شكل c3: debug dap

```
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
                                          mil@1241879298
                                              _____
                                         _____
                                    action = continue :1
                           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
                                           mil@1241879298
                    DAP_TRACE: Username: 1241879298@mil,
                                = aaa.ldap.objectCategory
CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=or
                                                        q
                    DAP_TRACE: Username: 1241879298@mil,
                         aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username
                                           mil@1241879298
                    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"]["physicalDeliveryOfficeN
                                                  = ["ame
                                              ; "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
                                        ;"mil@1241879298"
                                               DAP_TRACE:
     = ["dap_add_to_lua_tree:aaa["ldap"]["objectCategory
CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=o"
                                                      ;"rq
                                               DAP_TRACE:
    dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] =
                                                   ; " " TRUE
 ["DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username
                                        ;"mil@1241879298"
                                               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
```

### <u>المثال 2: رفض الاتصال ب DAP</u>

يوضح المثال التالي إخراج **أخطاء DAP** وdebug dap trace أثناء اتصال غير ناجح بالسيناريو 3 الموضح في الملحق أ.

#### الشكل C4: تصحيح الأخطاء DAP

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 = 1241879298DAP\_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 20070626163734.02 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 = 33691DAP\_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
                                           mil@1241879298
                    DAP_TRACE: Username: 1241879298@mil,
                                = aaa.ldap.objectCategory
CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=or
                                                        g
                    DAP_TRACE: Username: 1241879298@mil,
                         aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username
                                           mil@1241879298
                    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"]["physicalDeliveryOfficeN
                                                  = ["ame
                                              ;"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=qqsqseclab, DC=orq"
                                               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
                                        ;"mil@1241879298"
                                               DAP_TRACE:
     = ["dap_add_to_lua_tree:aaa["ldap"]["objectCategory
CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=o"
                                                     ;"rg
                                               DAP_TRACE:
    dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] =
                                                   ; " " TRUE
 ["DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username
                                                         =
                                        ;"mil@1241879298"
```

:DAP\_TRACE: Username: 1241879298@mil, Selected DAPs DAP\_TRACE: dap\_request: memory usage = 33% DAP\_TRACE: dap\_process\_selected\_daps: selected 0 records DAP\_TRACE: Username: 1241879298@mil, dap\_aggregate\_attr: rec\_count = 1

# <u>هيئة شهادة أستكشاف الأخطاء وإصلاحها / OCSP</u>

#### debug crypto ca 3 •

• في وضع التكوين**—تصحيح أخطاء وحدة تحكم CA للفئة** (**أو المخزن المؤقت) للتسجيل** 

تظهر هذه الأمثلة التحقق من صحة الشهادة بنجاح باستخدام مستجيب OCSP ونهج مطابقة مجموعة الشهادات الفاشلة.

يوضح الشكل C3 إخراج تصحيح الأخطاء الذي يحتوي على شهادة تم التحقق من صحتها ومجموعة شهادات عاملة تطابق النهج.

الشكل C4 يوضح إخراج تصحيح الأخطاء لنهج مطابقة مجموعة شهادات تم تكوينها بشكل غير صحيح.

يوضح الشكل C5 إخراج تصحيح الأخطاء لمستخدم بشهادة ملغاة.

#### الشكل C5: تصحيح أخطاء OCSP - التحقق من الشهادة بنجاح

```
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: 0F192B, 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
               .ou=PKI,ou=DoD,o=U.S. Government,c=US,15
              .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
               .ou=PKI,ou=DoD,o=U.S. Government,c=US,15
                   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

#### الشكل C5: إخراج نهج مطابقة مجموعة الشهادات الفاشلة

#### الشكل جيم5: إخراج شهادة ملغاة

n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta, in faioled .=uvalidation CMertifilcLa,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: 2FB5FC740000000035, 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: 2FB5FC740000000035, subject name: cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org CRYPTO\_PKI: Certificate not validated

# <u>الملحق د - التحقق من كائنات LDAP في MS</u>

في القرص المضغوط الخاص ب Microsoft Server 2003، هناك أدوات إضافية يمكن تثبيتها لعرض بنية LDAP وكذلك كائنات/سمات LDAP. لتثبيت هذه الأدوات، انتقل إلى دليل **الدعم** في القرص المضغوط ثم **الأدوات**. تثبيت SUPTOOLS.MSI.

#### <u> عارض LDAP</u>

- بعد التثبيت، أختر **بدء > تشغيل**.
- اکتب l**dp**، ثم انقر **موافق**. يقوم هذا بتشغيل عارض LDAP.
  - أختر **توصيل > توصيل**.
  - أدخل اسم الخادم ثم انقر فوق **موافق**.
    - أختر **توصيل > ربط**.
- أدخل اسم مستخدم وكلمة مرور.**ملاحظة:** تحتاج إلى حقوق المسؤول.
  - وانقر فوق OK.
  - عرض كائنات LDAP. راجع الشكل D1.**الشكل D1: عارض LDAP**

[ 🚰 ldap://Ciscojax-2k3.labrat.com/DC=labrat,DC=com	
Connection growse Yew Options Utilities	Elek
DC=labrat,DC=com     CN=Computers,DC=labrat,DC=com     CN=Computers,DC=labrat,DC=com     CN=Computers,DC=labrat,DC=com     CN=Computers,DC=labrat,DC=com     CN=Computers,DC=labrat,DC=com     CN=Computers,DC=labrat,DC=com     CN=Computers,DC=labrat,DC=com     CN=Computers,DC=labrat,DC=com     CN=Computers,DC=labrat,DC=com     CN=Computer Parker,OU=MIL,DC=labrat,DC=com     CN=Computer Parker,DC=com     CN=Computer Parker,DC=com     CN=Computer Parker,DC=com     CN=Computer Parker,DC=labrat,DC=com     C	<pre>Expanding base 'CM=Clark Kent_OU=MIL_DC=labrat_DC=com' Result &lt;0&gt;: [null] Matched DNs: Getling 1 entries: &gt;&gt; Dn: CN=Clark Kent_OU=MIL_DC=labrat_DC=com</pre>
Ready	NAM

### محرر واجهة خدمات <u>Active Directory</u>

- في خادم Active Directory، أختر **ابدأ > تشغيل**.
  - اكتب adsiedit.msc. هذا يبدأ المحرر.
- انقر بزر الماوس الأيمن فوق كائن وانقر فوق **خصائص**.

تظهر هذه الأداة كل الخصائص لكائنات معينة. راجع الشكل D2.

الشكل D2: تحرير ADSI

ADSI Edit Domain [Oscojax-2k3.lal DC=labrat,DC=com CN=Bultin CN=Bultin CN=Computers	Attribute Editor   Security   Show mandatory attrib Show optional attribute Show only attributes the	utes es nat have <u>v</u> alues		ss ) show in this	Distinguished Name
OU=Domain Cor ON=ForeignSec. ON=CostAndFou OU=MIL ON=Ethan H ON=Cherk Ke ON=Ethan H ON=NTDS Quote ON=Program Da ON=System ON=System ON=System ON=Users Configuration [Oscojax- Schema [Ciscojax-2k3.la ON=Ethan Hunt [Ciscoja	Attribute unicodePwd uf userAccountControl userCett userCethicate userParameters userPassword userPASsword userPASsword userSharedFolder userSharedFolder userSharedFolder userShiMECertificate userWorkstations 4 Edit	Synkax Octet String Unicode String Inleger Octet String Octet String Octet String Octet String Unicode String Unicode String Unicode String Unicode String Unicode String Unicode String	Value Chot Setb Chot Setb G6048 Chot Setb Dx30 0x82 0x06 0x27 0 mc d1 Chot Setb Chot S		

### <u>الملحق ہ</u>

يمكن إنشاء توصيف AnyConnect وإضافته إلى محطة عمل. يمكن أن يشير التوصيف إلى قيم مختلفة مثل مضيفي ASA أو معلمات مطابقة الشهادة مثل الاسم المميز أو المصدر. يتم تخزين ملف التعريف كملف .xml ويمكن تحريره باستخدام Notepad. يمكن إضافة الملف إلى كل عميل يدويا أو دفعه من ال ASA من خلال نهج مجموعة. يتم تخزين الملف في:

> C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile أكمل الخطوات التالية:

- 1. أختر AnyConnectProfile.tmpl وافتح الملف باستخدام Notepad.
- 2. قم بإجراء التعديلات المناسبة على الملّف مثل المصدر أو عنوان IP المضيف. راجع الشكل F1 على سبيل المثال.
  - 3. عند الانتهاء، احفظ الملف على هيئة .xml.

هذه عينة من ملف XML لملف تعريف عميل AnyConnect VPN من Cisco.

راجع وثائق Cisco AnyConnect فيما يتعلق بإدارة ملف التعريف. وباختصار:

• يجب تسمية ملف تعريف بشكل فريد لشركتك. مثال: CiscoProfile.xml

• يجب أن يكون اسم ملف التعريف هو نفسه حتى ولو كان مختلفا للمجموعة الفردية داخل الشركة.

تم تصميم هذا الملف ليتم الاحتفاظ به بواسطة مسؤول عبارة آمنة ثم يتم توزيعه مع برنامج العميل. يمكن توزيع التوصيف المستند إلى XML هذا على العملاء في أي وقت. آليات التوزيع المدعومة هي كملف مجمع مع توزيع البرامج أو كجزء من آلية التنزيل التلقائية. آلية التنزيل التلقائية متاحة فقط مع بعض منتجات عبارة الأمان من Cisco. **ملاحظة:** يتم تشجيع المسؤولين بشدة على التحقق من ملف تعريف XML الذي يقومون بإنشائه باستخدام أداة تحقق من الصحة عبر الإنترنت أو من خلال وظيفة إستيراد ملف التعريف في ASDM. يمكن تحقيق التحقق من الصحة باستخدام AnyConnectProfile.xsd الموجود في هذا الدليل. AnyConnectProfile هو العنصر الجذري الذي يمثل ملف تعريف عميل AnyConnect.

> "xml version="1.0" encoding="UTF-8 The ClientInitialization section represents global ---! settings !--- for the client. In some cases, for example, BackupServerList, host specific !--- overrides - <-- --! .are possible The Start Before Logon feature can be used to ---! activate !--- the VPN as part of the logon sequence. !--- UserControllable: Does the administrator of this profile allow the user !--- to control this attribute for their own use. Any user setting !--- associated with <-- .this attribute is stored elsewhere This control enables an administrator to have a one ---! time !--- message displayed prior to a users first connection attempt. As an !--- example, the message can be used to remind a user to insert their smart !--- card into its reader. !--- The message to be used with this control is localizable and can be !--- found in the AnyConnect message catalog. !--- (default: "This is a (".pre-connect reminder message This section enables the definition of various --! attributes !--- that can be used to refine client - <-- .certificate selection Certificate Distinguished Name matching allows for ---! exact !--- match criteria in the choosing of acceptable - .client !--- certificates

```
This section contains the list of hosts from which --! -

- .!--- the user is able to select

This is the data needed to attempt a connection to ---!

- <-- .a specific !--- host
```

### <u>معلومات ذات صلة</u>

- الشهادات و CRLs المحددة بواسطة X.509 و X.509
  - <u>OCSP المحدد بواسطة OCSP المحدد بواسطة </u>
    - تقديم البنية الأساسية للمفتاح العام
  - <u>"OCSP خفيف الوزن" موضح حسب معيار المسودة</u>
    - <u>SSL / TLS المحدد بواسطة SSL / TLS </u>
    - الدعم التقني والمستندات Cisco Systems

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما