ASA 8.x: نيوكت AnyConnect SSL VPN CAC-SmartCards ل Windows

تايوتحملا

<u>ةمدقملا</u> <u>قىساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسمالا تانوكمالا</u> <u>Cisco نم ASA نىوكت</u> رش ن ل ا ت ار ا ت ع ا <u>(AAA) ةبساحمل او ضي،وفتل او ةقداصمل اني،وكت</u> <u>LDAP مداخ نېوكت</u> <u>تاداەشلا قرادا</u> <u>جيتافملا ءاشنا</u> <u>رذجلا قدصملا عجرملا تاداهش تيبثت</u> <u>قىوەلا قداەش تېپېتو ASA لىجس ت</u> AnyConnect VPN نیوکت <u>IP نېوانع عمجت ءاشنا</u> <u>قعومجملا جەنو قەنلا قعومجم ءاشنا</u> <u>ةروصلا تادادعاو قفنلا قعومجم قمجاو</u> (OCSP مادختسا متيس ناك اذا) ةداهشال ققباطم دعاوق OCSP نىوكت <u>OCSP بيجتسملا ةداەش نىوكت</u> <u>OCSP مادختسال CA نېوكت</u> <u>OCSP دعاوق نېوكت</u> <u>Cisco نم AnyConnect لىمع نىوكت</u> <u>Lisco AnyConnect VPN Client - Windows</u> Cisco - Windows نم AnyConnect VPN ليمع ليغشت عدب <u>دیدج لاصتا</u> <u>دعب نع لوصولا ءدت</u> DAP و LDAP طيطخت - أ ق حل مل <u>- دعب نع لوصول انذأل يفتامل بلطل مادختس اب Active Directory قيبطت 1: ويرانيس ل ا</u> <u>مضفر/لوصولات جامسلا</u> Active Directory دادع <u>ASA نېوكت</u> <u>وأ لوصولاب جامسلل ةعومجملا فيوضع مادختساب Active Directory قيبطت :2 ويرانيسلا</u> <u>ەض ف ر</u> Active Directory دادع ASA نىوكت <u>ءاضءألا تامس نم ديدعل يكيمانيدلا لوصولا تاسايس :3 ويرانيسلا</u> <u>ASA نيوكت</u>

ةمدقملا

نم (ASA) فيكتال لباقلا نامألا زامج ىلع نيوكتال اجذومن دنتسملا اذه مدقي Cisco نم (ASA) فيكتال لباقل نامألا زامج كل كرتشملا لوصولا ةقاطب مادختساب Windows ل AnyConnect VPN ىلإ دعب نع لوصولل (CAC) .ةقداصمل

نيوكت دنتسملا اذه يطغي Cisco ASA فيكتلل لباقلا نامألا ةزهجأ ريدم مادختساب Cisco ASA نيوكت دنتسملا اذه يطغي (ASDM و Microsoft Active Directory (AD/ و Disco AnyConnect VPN Client و LDAP) و نزولا فيفخ

اضيأ دنتسملا اذه يطغي .Microsoft AD/LDAP مداخ ليلدلا اذه يف دوجوملا نيوكتلا مدختسي (DAP) يكيمانيدلا لوصولا تاسايسو LDAP تامس طئارخو OCSP لثم ةمدقتملا تازيملا

ةيساسألا تابلطتملا

تابلطتملا

ةينبو Microsoft AD/LDAP و Cisco AnyConnect Client و Cisco ASA ل يساسألاا مەفلاا نوكي AD ةعومجم ةيوضعب ماملإلاا دعاست .لماكلا دادعإلاا مەف يف اديفم (PKI) ماعلاا حاتفملاا ةداەشلا تامس نيب ليوختلاا ةيلمع طبر يف LDAP تانځاك كلذكو مدختسملا صځاصخو ماكرلا تانځاكو

ةمدختسملا تانوكملا

ةيلاتا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- نم (ASA) رادصإلا لغشي يذلا Cisco 5500 Series نم (ASA) فيكتلل لباقلا نامألا زاهج ثدحألا تارادصإلاو جمانربلا
- Cisco Adaptive Security Device Manager (ASDM)، رادصإلاا 6.x ل ASA 8.x

• ل Sisco ل Mindows ل يمع Windows

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ةرشابم كتكبش.

Cisco نم ASA نيوكت

قفن رشنل ةيرورضلا تاوطخلا يطغي وهو .ASDM ربع Cisco ASA نيوكت مسقلا اذه يطغي CAC ةداهش مادختسإ متي .SSL AnyConnect لاصتا لللخ نم VPN ةكبشل دعب نع لوصو مدانه شادختسل يف قداهشلا يف User Principal Name (UPN) قمسلا علم متي امك ،ةقداصملل ليوختلل.

رشنلا تارابتعا

• ميجوتلاو NTP و DNS و تامجاولا لثم ةيساسألا تانيوكتلا ليلدلا اذه يطغي ال ةكبشلا لغشم نأ ضرتفملا نم .كلذ ىلإ امو ASDM ىلإ لوصولاو زامجلا ىلإ لوصولاو تانيوكتلا مذمب ةيارد ىلع.

تامولعملا نم ديزم ىلع لوصحلل <u>فئاظولا ةددعتم نامألاا ةزهجاً</u> عجار.

- ى الي عن الله عن الله عن المال المعن الماس الله عن الله عن الله عن الله عن الله عن الله عن الماس الله عن المال مادختساب VPN قفن دادعإ نكمي ،لاثملا ليبس علع .(VPN) ةيرهاظلا قصاخلا ةكبشلا لوصولا ةسايس تاصوحفو LDAP تاطيطختو OCSP تاصوحف ءارجإ نود CAC ةقاطب نودب قفنلا لمعي نكلو OCSP صحف ضيوفتب DoD موقي .(DAP) يكيمانيدلا نيوكت
- نم ديزملا ةفاضإل اەنيمضت نكمي ةمدقتم تازيم يە قرزألاب ةزربملا ماسقألا ميمصتلل نيمأتلا.
- .لقألاا ىلع ASDM 6.0.2 و 8.0.2.19 يه ةبولطملا ASA ةروص
- AnyConnect/CAC عم موعدم Vista.
- DAP و يكيمانيدلا لوصولا ةسايس طئارخ مسرل ةلثمأ ىلع لوصحلل (أ) قحلملا عجار
 ديفاضإلا تاسايسلا ذيفنتل
- يف LDAP تانئاك نم ققرحتالا ةيفيك يلع فرعتال (<u>د) قرطا</u> عجار MS.
- رادج نيوكتل قيبطتلا ذفانمب ةمئاق ىلع لوصحلل <u>قلصلا تاذ تامولعملا</u> عجار ةيامحلا

(AAA) ةبساحملاو ضيوفتلاو ةقداصملا نيوكت

لالخ نم (CAC) كرتشملا لوصولا ةقاطب يف ةدوجوملا قداهشلا مادختساب كتقداصم متت قحلاص قداهشلا نوكت نأ بجي .مهتمظنمب صاخلا AA مداخ وأ (CA) تانايبلا قدصم عجرم مداخ اضيأ الوخم نوكت نأ بجي ،ةقداصملا ىلا قفاضإلاب .قكبشلا ىلا دعب نع لوصولل الميأ الوخم نوكت نا مجي ،ققداصملا ولا قفاضالاب .قكبشلا ىلا دعب نع لوصولل المجت يتلو ،ليوختلل (UPN) يساسألا مدختسملا مسا قمس مادختسا عافدلا قرازو بلطتت اذهب EDI/P1 وأ لاوكي نا بجي .قداهشلا يف "(SAN) عوضوملل ليدبلا مسالا" مسق نم اءزج المجت العام المحالي المحالي المحت المالي مراح من المال مريب موادي موالي المولي المالي المالي المالي المحت المحت يتلو المحت المالي المالي من المالي من المالي ماليات مالي من المالي من المالي مولي المالي الم

LDAP مداخ نيوكت

ةيلاتلا تاوطخلا لمكأ

- .AAA مداوخ ةعومجم < AAA دادعإ < (دعب نع لوصولI) Remote Access VPN رتخأ .1
- .3 ةفاضإ قوف رقنا ،AAA مداوخ تاعومجم لودج يف .2
- .1 لكشلا عجار .رز يكلسال لوكوتوربلا يف LDAP ترتخاو مسإ ةعومجم لدان تلخد .3
- يذلا مداخلا نأ نم دكأت .ةفاضإ قوف رقنا ،ددحملا ةعومجملا لودج يف ةدوجوملا مداوخلا يف .4 قباسلا لودجلا يف زربم هتأشنأ.
- .2 لكشلا عجار .ةيلاتلا تاوطخلا لمكأ ،AAA مداخ ريرحت ةذفان يف .5

نم عونلا اذهل LDAP/AD نيوكت ةلاح يف SSL ربع LDAP نيكمت رايخ رتخأ :ةظحالم لاصتال.

- a. ةەجاولا لخاد ليلدلا اذه رەظي عقوم نوكي LDAP لا ثيح نراقلا ترتخأ.
- .مداخلاب صاخلا IP ناونع لخدأ
- c. دان تلخد LDAP ديصقتلا. المان عانيم الدان ال
- .مداخلا عون رتخأ .d
- e. ميقلا هذه نع AD/LDAP لوؤسم لأسا .يساسألا DN لخدأ.

1-لكش

🞼 Add AAA Serve	r Group		X
Configure an AAA se for RADIUS and TAC/	ver group. The Acc ACS+ protocols.	ounting Mo	de attribute is only applicable
Server Group:	AD-LDAP]
Protocol:	LDAP	~]
Accounting Mode:	🔅 Simultaneous	🛞 Single	
Reactivation Mode:	 Depletion 	🔿 Timed	
Dead Time: 10	minut	es	
Max Failed Attempts:	3]
_		(

- f. بلطا .يساسألا DN ىلع كلذ دمتعي .ةبسانملا ةباجإلا رتخأ ،قاطنلا رايخ تحت لوؤسم نم ةدعاسملا AD/LDAP.
- g. ليوختل ةمدختسملاً قمسلاً يه هذه userPrincipalName لخدأ ،ةيمستلاً قمس يف مداخ يف مدختسملاً AD/LDAP.
- h. لوؤسملا اlogin DN لا يف تلخد DN.

يتلا LDAP ةينب يف ثحبلا/ضرعل ةيرادإ قوقح وأ قوقح كيدل :ةظحالم ةعومجملا ةيوضعو مدختسملا تانئاك نمضتت.

- i. لوؤسملا رورم ةملك لخدأ ،لوخدلا ليجست رورم ةملك يف.
- .الب ىلإ LDAP ةمس كرتأ .

2-لكش

🛸 Add AAA Server

conds
conds
conds
000000000000000000000000000000000000000

х

رخآ AD/LDAP نﺉاك ةفاضإل نﻱﻭﻙﺕﻝﺍ ﻱﻑ ﺍﻕﺡﺍﻝ ﺭﺍﻱﺥﻝﺍ ﺍﺫﻩ ﻣﺩﺧﺖﺱﺕ :ﺓڟﺡﺍﻝﻣ ﻝﻱﻭﺧﺖﻝﻝ.

k. رتخأ OK.

.0K رتخأ

تاداەشلا ةرادإ

عجرملا تاداەش تيبثتب مق ،الوأ .ASA لا ىلع ةداەش تبكر steps in order to نانثإ كانە

ةدعاسملا بتكم ليجست ،ايناث .ةبولطملا (يوناثلاو يساسألا قدصملا عجرملا) قدصملا هذه Dod نم PKI قدحو مدختست .ةيوهلا قداهش ىلع لوصحلاو ددحم قدصم عجرم يف قينوناقلا مت يتلا قطسوتم #CA و 3 ةئفلاو CA2 رذجلا تاذ OCSP قداهشو DI ASA قداهشو تاداهشلا الف ،OCSP مادختسإ مدع ترتخأ اذإ ،نكلو .OCSP قداهشو ASA ID قداهشو اهب ASA ليجست زلي

لوح تاميلعت ىلا ةفاضإلاب رذجلا تاداەش ىلع لوصحلل نامألل POC ب لصتا :ةظحالم ASA ل ةيفاك SSL ةداەش نوكت نأ بجي .زامجلل ةيوەلا ةداەشل ليجستلا ةيفيك ةجودزم (SAN) نيزخت ةقطنم ةكبش ةداەش مادختسا مزلي ال .دعب نع لوصولل.

تاداەشلا ضرع نكمي .يلحملا زاەجلا ىلع DoD CA ةلسلس تيبثت اضيأ بجي :ةظحالم موقي ةعفد فلم DoD جتنأ .Internet Explorer مادختساب "Microsoft تاداەش نزخم" يف ديزم ىلع لوصحلل كب صاخلا PKI POC بلطا .زاەجلا ىلإ CAs ةفاك ةفاضإب ايئاقلت .تامولعملا نم

طيسولا CA فرعمو ASA فرعم كلذكو 3 ةئفلاو DoD CA2 رذج نوكي نأ بجي :ةظحالم مدختسملا ةقداصمل بولطملا ديحولا قدصملا عجرملا وه ASA ةداهش ردصأ يذلا. اهب قوثولا متيو 3 ةئفلاو CA2 رذج ةلسلس تحت ةيلاحل CA تاطساولا عيمج يوضنت 3. ةئفلاو CA2 روذج ةفاضإ تمت املاط

حيتافملا ءاشنإ

:ةيلاتلا تاوطخلا لمكأ

- .ةفاضإ < ةيوهلا ةداهش < تاداهشلا ةرادإ < (دعب نع لوصولا) Remote Access VPN رتخأ .1
- .حيتافملا جوز رايخ ةطساوب ديدج مث ةديدج فرعم ةداهش ةفاضإ رتخأ .2
- ةفاضإل ويدارلا ىلع رقنا. DoD-1024 ،حاتفم مسا لخدأ ،حيتافملا جوز ةفاضإ ةذفان يف .3 لكشلا عجار .ديدج حاتفم 3.

3 لكش

🕵 Add K	iey Pair	
Name:	🚫 Use default key pair name	
	💿 Enter new key pair name:	DoD-1024
Size:	1024	

- .حاتفملا مجح رتخأ
- 5. ةماعلا ضارغألل مادختسالاب ظافتحالا.
- .نآلا ءاشنإ قوف رقنا .6

2048 رادصإ حاتفم DoD ب صاخلا 2 يرذجلا (CA) قدصملا عجرملا مدختسي :ةظحالم ىلع ارداق نوكيل تب 2048 حيتافم جوز مدختسي ناث حاتفم ءاشنإ بجي .تب .يناث حاتفم تفضأ steps in order to قباس لا تمتأ .اذه قدصملا عجرملا مادختسإ

رذجلا قدصملا عجرملا تاداهش تيبثت

:ةيلاتلا تاوطخلا لمكأ

- .ةفاضإ < CA ةداهش < تاداهشلا ةرادإ < (دعب نع لوصولا) Remote Access VPN رتخأ .1
- .ةداەشلا ىلإ ضرعتساو فلم نم تيبثت رتخأ .2
- .تيبثتلا ةداەش رتخأ .3

رذجلا ةداەشلا تيبثت :4 لكشلا

💕 Install Certificate		
 Install from a file: 	C:\CAC\DOD-CERTS\ca13-jitc.ce	Browse
O Paste certificate in	PEM format:	
O Use SCEP:		
SCEP URL: http://		
Retry Period:	1	minutes
Retry Count:	0	(Use 0 to indicate unlimited retries)
		More Options
	verse Consul	
		Heip

.5 لكشلا رظنا .ةذفانلا هذه رهظت نأ بجي .4

5 لكش

🕵 CA Certi	icate Installation
¢	CA certificate installed successfully.
	ОК

بلطتي .اهتيبثت ديرت ةداهش لكل 3 ىلإ 1 نم تاوطخلا ررك :ةظحالم DoD PKI بلطتي .اهتيبثت ديرت ةداهش لكل 3 ىلإ 1 نم تاوطخلا ررك :ةظحالم OCSP مداخو ASA فرعم ،طسوتم #OCSP مدختست مل اذإ ةبولطم OCSP ةداهش نوكت ال

رذجلا ةداەشلا تيبثت :6 لكشلا

 Activativ (Clerk) Access Clendess S3L VPN Access AAA Seh p Sourd Tc Isourd Tc <liisour< th=""><th>Remote Access VPN 🚽 🖉 🔬</th><th>Configuration ></th><th>Remot</th><th>n Annens VP</th><th>Contificate</th><th>Manag</th><th>ement > EA</th><th>Certificates</th><th></th></liisour<>	Remote Access VPN 🚽 🖉 🔬	Configuration >	Remot	n Annens VP	Contificate	Manag	ement > EA	Certificates	
ADA Setup Isoued TC Isoued Sy Excity Date:: Usage::	Network (Client) Access								
Secure Deskou Manager DoC POSIC CA 2 [u=>] D Root CA 2, u=P(1, u), 15001000 Constal Publics Deb C.ASD 0 2pod CA (m=>) CLASS - Root CA 2, u=P(1, u), CLA	t 📊 222 Setup	Issued To		Issued By		E E	Evuiry Date	Usaya	br6
DOD JITC C/-13 [ui=D_P JITC Roul CA 2, Lu=PK1 C2:55:53 UTC Signature Main Local Certificates Main Local Certificates Authority Main Local Certificates Authority Main Local Certificates Dod JITC C/-13 [ui=D_P JITC Roul CA 2, Lu=PK1 C2:55:53 UTC Signature Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certificates Main Local Certi	🖌 🦰 Secure Deskup, Manager 🔊 🖻 Hortiñkath Management	DeD CLASS 0 P	bol CA] <mark>[ui=DLD Root</mark> [m≓DHCC A	CA 2, LuHPUL, . S F Roht (Aylo)	_u l 	5:01:10 UTC 391-900000	Signature General Purpose	(I dt
Core Signer Kenn Kenn Kenn Kenn Kenn Kenn Kenn De De De De De De De De De		000 JEC CO-1	.3	[ui=0_0 JITC	Roll CA 2; lu=	PK1 C	2:55:53 UTC	Sgrabue	how Pete
Device Set_p									Keq estal
Device Set_p	Thed Telepring								Delete
	ENS SCIENCE								
Device Set_p	F2 havened								
- Tiskel	Device Setup								
	firevel								

ةيوەلا ةداەش تيبثتو ASA ليجست

- .ةفاضإ < ةيوهلا ةداهش < تاداهشلا ةرادإ < (دعب نع لوصولا) Remote Access VPN رتخأ .1
- .ةديدج فرعم ةداەش ةفاضإ رتخأ .2
- 7 لكشلا رظنا .DoD-1024 حيتافملا جوز رتخأ .3

ةيوەلا ةداەش تاملعم :7 لكشلا

🖆 Add Identity Certificat	e 🔀
🚫 Import the identity certif	icate from a file:
Decryption Passphrase:	
File to Import From:	Browse
 Add a new identity certif 	icate:
Key Pair:	DoD-1024 Show New
Certificate Subject DN:	Select
Generate self-signed	l certificate
Act as local certif	icate authority and issue dynamic certificates to TLS-Proxy
	Advanced
Add Certifi	icate Cancel Help

- 4. ديدحت قوف رقناو ةداهشلا عوضومل DN عبرم ىلإ لقتنا.
- .لاثملا ليبس ىلع 8 لكشلا عجار .زاهجلا تامولعم لخدأ ،ةداهشلا عوضوم DN ةذفان يف .5

DN ريرحت :8 لكش

DN Attribute to be Added Add>> Common Name (CN) asa80 Attribute: Select Attribute Add>> Department (OU) PKI Value: Delete Company Name (O) U.S. Government			Attribute	Value
Attribute: Select Attribute Y Add>> Department (OU) PKI Value: Delete Company Name (O) U.S. Government	Second and a second second		Common Name (CN)	asa80
Attribute: Select Attribute Y Add>> Department (OU) DoD Value: Delete Company Name (O) U.S. Government	DIN Attribute to be Added		Department (OU)	PKI
Value: Delete Company Name (O) U.S. Governmer	Attribute: Select Attribute 🔽	Add>>	Department (OU)	DoD
value: Delete		C	Company Name (O)	U.S. Government
Country (C) US	value;	Delete	Country (C)	US

.0K رتخأ

ماظنلاا يف ەنيوكت مت يذلا زاەجلل فيضملا مسا مادختسا نم دكأت :ةظحالم لوقحلاب PKI POC كربخي نأ نكمي .عوضوملل DN مقر ةفاضا دنع كب صاخلا .ةبولطملا ةيمازلإلا

- .ةداەش ةفاضإ رتخأ .7
- .9 لكشلا عجار .هيف بلطلا ظفح ديرت يذلا ليلدلا ديدحتل ضارعتسإ قوف رقنا .8

ةداەشلا بلط :9 لكشلا



مادختساب فلملا حتفا .9 مادختساب فلملا حتفا .9 مادختساب فلمل حتفا .9 مق مث ةبسانمل BKI POC مادختساب فلمل عتفا .0

ليجستلا بلط :10 لكشلا



ا ان م ةداەشلا تنأ ملتسي نإ ام .10 Remote Access VPN ج ةداەشلا ا قرادإ < 10. 11. لكشلا عجار .تيبثت < فرعملا قداەش

ةيوەلا ةداەش داريتسإ :11 لكشلا

- 1 ¹				
	6.000	C 100	1.0.20	R Service I
				2010
10000 C	1.000			i serer s



Starting IP Address:192.168.1.1Ending IP Address:192.168.1.254
Ending IP Address: 192,168.1,254
Subnet Mask:

تيبثت رتخاو فرعملا ةداەش ىلإ لوصولل ضرعتسا ،"ةداەش تيبثت" ةذفان يف .11 لاثملا ليبس ىلع 12 لكشلا عجار .ةداەشلا.

ةيوەلا ةداەش تيبثت :12 لكشلا

🖆 Install Identity ce	rtificate 🔀
Identity Certificate	
 Install from a file: 	C:\CAC\DOD-CERTS\asa80.txt Browse
Paste the certificat	e data in base-64 format:
Install Cert	ificate Cancel Help

ريدصتب ىصوي :ةظحالم الا حاتفملاو تاداەشلا جاوزأ ظفحل Id Certificate TrustPoint ريدصتب ىصوي :ةظحالم ىلإ حاتفملاو تاداەشلا جاوزأ داريتساب ASA لوؤسمل حمسي اذەو .اەرادصإ مت يتلا ASA ق<u>قثلا طاقن ريدصت</u> عجار .زاەجلا يف وأ RMA يف لطع ثودح ةلاح يف ديدج ديامولعملا نم ديزم ىلع لوصحلل <u>اەداريتساو</u>.

ة القرم المرابقة القرب المرابقة المربقة المربقة المربقة المربقة (المربقة المربقة ا

AnyConnect VPN نيوكت

ةادأ هذه .SSL VPN جلاعم مادختسإ وه لوألا رايخلا .ASDM يف VPN تاملعم نيوكتل نارايخ كانه ايودي كلذ لعفت نأ وه يناثلا رايخلا. VPN نيوكت يف ددجلا نيمدختسملل مادختسالا ةلهس .ةيوديلا ةقيرطلا اذه نيوكتلا ليلد مدختسي .رايخ لك لالخ يضمتو

مدختسملا ىل AC ليمع لاصيال ناتقيرط كانه :ةظحالم

.هب صاخلا زاهجلا ىلع ەتيبثتو بيولا ىلع Cisco عقوم نم ليمعلا ليزنت كنكمي .1

2. ليمعلا ليزنت نكميو بيو ضرعتسم ربع ASA كلإ لوصولا مدختسملل نكمي.

ةيناثلا ةقيرطلا ليلدلا اذه مدختسي .<u>https://asa.test.com</u> ،لاثملا ليبس ىلع :ةظحالم. ليمع ليغشت ىوس كيلع امف ،مئاد لكشب ليمعلا زامج ىلع AC ليمع تيبثت درجمب AC قيبطتلا نم

IP نيوانع عمجت ءاشنإ

.DHCP لثم ىرخأ ةقيرط مدختست تنك اذإ يرايتخإ اذه

- 1. ليمعلا) > Network (ليمعلا) الايمعلا) ميرهاظلا قصاخلا قصاخلا ما محليا مال الايمعلا) Access رتخأ Address Assignment (نيوانعل انعومجم ح (نيوانعل انييعت).
- .(Add) ةفاضإ قوف رقنا .2
- هتياهنو IP ناونع ليغشتب موقت ثيح ،IP عمجت مسا لخدأ ،IP عمجت ةفاضإ ةذفان يف .3 13 لكشلا رظنا .ةيعرف ةكبش عانق رتخاو

IP عمجت ةفاضإ :13 لكشلا

Name:	CAC-USERS
Starting IP Address:	192.168.1.1
Ending IP Address:	192,168.1,254
Subnet Mask:	255.255.255.0

- .قفاوم رتخأ .4
- 5. (دعب نع لوصول Remote Access VPN (ليمعل) > Network (ليمعل) Access > Address Assignment (ناونعلا نييعت) + Assignment (ناونعل نييعت) + Assignment (ا
- . ةيلخادلا نيوانعلا تاعمجت ليلدلا اذه مدختسي .بسانملا IP ناونع نييعت بولسأ ددح. 14. لكشلا رظنا

IP ناونع نييعت بولسأ :14 لكشلا



.قيبطت قوف رقنا .7

ةعومجملا جەنو قڧنلا ةعومجم ءاشنإ

ةعومجملا جەن

يضارتفالاا جەنلا مادختسإ كنكمي ،ديدج جەن ءاشنإ يف بغرت نكت مل اذإ :ةظحالم ةعومجملا يف نمضملا.

- .ةعومجملا جەن <- (ليمعلا) ةكبشلا ىلإ لوصولا <- VPN ىلإ دعب نع لوصولا رتخأ .1
- . يلخادلا ةعومجملا جەن رتخاو ةفاضإ قوف رقنا .2
- عن العبرم يف "ةعومجملا جهن" مسا لخدأ ،"يلخاد ةعومجم جهن ةفاضإ" ةذفان يف .3 15. لكشلا عجار ."مسالا"

ةيلخاد ةعومجم ةسايس ةفاضإ :15 لكشلا

neral	Name: AC-US	ERS				
 Dervers Advanced 	Banner: 🔽 Inh	nerit				
	Address Pools: 🔲 Inh	erit CAC-U	ERS .			Select
	More Options					
	Tunneling Protocols:	🗌 Inheri	Clientless SSI	L VPN 🔽 SSL VP	N Client DIPsec	L2TP/IPsec
	Filter:	🔽 Inheri			×	Manage
	NAC Policy:	🔽 Inheri				Manage
	Access Hours:	🔽 Inheri			V	Manage
	Simultaneous Logins:	🕑 Inheri	:			
	Restrict access to VL	AN: 🔽 Inheri			*	
	Maximum Connect Tir	me: 🔽 Inheri	Unimited	mnutes		
	Ide Timeout:	🔽 Inheri	: Onlimited	mnutes		

- a. لاصتالا تالوكوتورب رايخ يف SSL VPN Client رتخأ ،"ماع" بيوبتلا ةمالع يف ليمع نودب SSL لثم يرخأ تالوكوتورب مدختست تنك اذإ الإ ،يقفنلا.
- صاخلا IP ناونع لخدأو Inherit رايتخالاا ةناخ ديدحت ءاغلإب مق ،مداوخلا مسق يف .b انكمم كلذ ناك اذإ DHCP قاطن لخدأ .WINS و DNS مداوخب.
- c. يضارتفالا لاجملا يف ثيروت رايتخالا ةناخ ديدحت ءاغلإب مق ،مداوخلا مسق يف بسانملا لاجملا مسا لخدأو.
- d. عمجت مسق يف ةثارو رايتخالاا ةناخ ديدحت ءاغلاب مق ،"ماع" بيوبتلا ةمالع يف تنك اذإ .ةقباسلا ةوطخلا يف هؤاشنإ مت يذلا نيوانعلا عمجت فضأو نيوانعلا ءارجإب مقو ةثارولل ةقيرطلا هذه كرتاف ،IP ناونع نييعتل ىرخأ ةقيرط مدختست .بسانملا رييغتلا
- e. ةيضارتفالا تادادعإلل ىرخألا نيوكتلا بيوبت تامالع لك كرتت.

نييئاەنلا نيمدختسملا ىل AC ليمع لقنل ناتقيرط كانە :ةظحالم. ةقيرطلا AC. ليمع ليزنتو Cisco.com ىل لاقتنالا يف امەالوأ لثمتت لواحي امدنع مدختسملا ىل ليمعلا ليزنتب ASA موقي نأ يه ةيناثلا . ريخألا بولسألا لاثملا اذه حضوي .لاصتالا مدختسملا

. 16 لكشلا رظنا .لوخدلا ليجست تادادعإ < SSL VPN Client < مدقتم رتخأ ،كلذ دعب .4

ةيلخاد ةعومجم ةسايس ةفاضإ :16 لكشلا

🗯 Edit Internal Group Pol	icy: AC-USERS	×
General Servers	After successfully logging in, user can have the choice to download the client software, or go to clientless SSL VPN portal page. The following settings decides what will happen.	
Advanced Split Tunneling	Inherit	
IE Browser Proxy	Post Login Setting	
Login Setting	 Do not prompt user to choose 	
Key Regeneration	O Prompt user to choose	
Customization ⊡ IPsec Client	User has seconds to choose, or Default Post Login Selection below is taken.	
	Default Post Login Selection	
	Go to Clientless SSL VPN portal	
	Download SSL VPN Client	
	OK Cancel Help	

- a. ثيروت رايتخالا ةناخ ديدحت ءاغلإب مق.
- b. بساني يذلا (عقوملا ىلإ لوخدلا ليجست) Post Login ل بسانملا دادعإلا رتخأ كتيب.
- .كتىء بساني يذلا بسانملا يضارتفالا رشنلا ةدام ديدحت رتخأ .c
- .OK رتخأ

ةروصلا تادادعإو قفنلا ةعومجم ةهجاو

ةجمدملا ةعومجملا مادختسإ كنكمي ،ةديدج ةعومجم ءاشنإ ديرت ال تنك اذإ :ةظحالم ةيضارتفالا.

- 1. فيرعت فلم < Access VPN (ليمعلا) > Network (دعب نع لوصولا) Access VPN (تعا أ. ل VPN لااصتا
- Cisco AnyConnect..... ليمع نيكمت رتخأ
- SVC، ة روس نيييت ديرت ل، لاؤسلا عم راوح عبرم رهظي. SVC?

- .معن رتخأ .4
- مل اذإ .Flash حفصت عم اهمادختسإ ديرت يتلا ةروصلا رتخأ ،لعفلاب ةروص كانه ناك اذإ .5 رظنا .يلحملا رتويبمكلا ىلع فلملا ضرعتساو ليمحت رتخأ ،ةرفوتم ةروصلا نكت Linux. و Mad و Windows فلم كانه ،Cisco.com نم تافلملا ليزنت نكمي .17 لكشلا

SSL VPN ليمع ةروص ةفاضإ :17 لكش

🚰 Add SSL VPN Client Image	
Flash SVC Image:	Browse Flash
	Upload
[······] [······] [······]	••••••

رظنا .ايرايتخإ DTLS نيكمتو ليمع ةداهش بلطتي ،لوصولاب حمسي يلاتلا نيكمتلا .6 18 لكشلا

لوصولا نيكمت :18 لكشلا

📫 Cisco ASDM 6.0 for ASA - 172	2.18.120.225				
Ele View Tools Wigards Window	w Heb Ionitoring 🔚 Save	Refresh	Look For: Back Of Forward ? Help	Find -	ahaha cisco
Remote Access V Q A × Network (Clent) Access SL VPN Connection Profiles Profiles Croup Policies Address Assignment Address Pools Address Pools Address Pools Address SL VPN Access Clentless SSL VPN Access Clentless SSL VPN Access Connection Profiles	Configuration > Re The security apple users upon connect VPN Clent support (More clent-relate Access Interfaces Interface Sutside	emote Access VPN nce automatically dep tion. The initial clerk of s the HTTPS/TCP (SSL id parameters, such a nyConnect VPN Client Allow Access	Network (Client) Access > S loys the Cisco AnyConnect VPN Cle deployment requires end-user admin) and Datagram Transport Layer Se s client images and client profiles, cr or legacy SSL VPN Client access on Require Client Certificate	SSL VPN Connection int or legacy SSL VPN Cik istrative rights. The Cis- curty (DTLS) tunneling of an be found at <u>Clent Set</u> the interfaces selected in Enable DTLS	Profiles co AnyConnect aptions. thos.) in the table below
	Access Port: 443 Click here to Asso Connection Profiles	DTLS Po n Certificate to Interf	rt: 443 300, Apply Reset	schut 🛐	807 2:09:48 AM UTC

- .قيبطت قوف رقنا .7
- Remote Access VPN رتخأ .قفن ةعومجم/لاصتا فيرعت فلم ءاشنإب مق ،كلذ دعب .8 SSL. ل VPN لاصتا فيرعت فلم < Access (ليمعلا) Network (دعب نع لوصولا)
- .ةفاضإ ىلع رقنا ،ليصوتلا تافيصوت مسق يف .9

لاصتالا فيرعت فلم ةفاضإ :19 لكش

🖆 Add SSL VPN Connect	ion Profile		
Basic	Name:	AC-USERS	
⊞-Advanced	Aliases:		
	Authentication		
	Method:	◯ AAA ③ 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:	C Enabled	
	OK	Cancel Help	

a. ةعومجملا ةيمستب مق.

b. ةقداصملا ةقيرط يف ةداەش رتخأ.

c. اقبسم ەؤاشنإ مت يذلا ةعومجملا جەن رتخأ.

d. نيكمت نم دكأت SSL VPN Client.

e. يضارتفاك ىرخألاا تارايخلا كرتأ.

20 لكشلا عجار .ليوختلا < مدقتم رتخأ ،كلذ دعب .10

صيخرتلا :20 لكشلا

🖆 Edit SSL VPN Connecti	on Profile: AC-USERS				
e Basic	Default Authorization Serve	r Group			
General	Server Group: AD-LDAP		Manage		
Client Addressing Authentication	Users must exist in the authorization database to connect				
Accounting	Interface-specific Authoriza	tion Server Groups			
SSL VPN	Add 📓 Edit 🖀 D	elete			
	Interface		Server Group		
	User Name Mapping				
	O Use the entire DN as	the username			
	 Specify individual DN 	fields as the userna	me		
	Primary DN Field:	UPN (User's Princip	al Name) 🔽 😽		
	Secondary DN Field:	None	~		
	ОК	Cancel	Help		

- a. اقبسم اەۋاشنإ مت يتلا AD-LDAP ةعومجم رتخأ.
- b. لاصتالل ...نيمدختسملا دوجو بجي هنأ نم ققحت.
- c. يوناثلل none يساسألل UPN رتخأ ،نييعتلا لوقح يف
- .ةمئاقلا نم مسق SSL VPN لا ترتخأ .11
- :ةيلاتلا تاوطخلا لمكأ ،لاصتالل ةراعتسملا ءامسألا مسق يف .12

لاصتالل ةراعتسملا ءامسألاا :21 لكشلا

🖆 Edit SSL VPN Connecti	on Profile: AC-USERS					
Basic	Portal Page Customization:	DfltCustomization		Manage		
General	CSD Alternate Group Policy:	DfltGrpPolicy	~	Manage		
Client Addressing Authentication	Enable the display of Radius Reject-Message on the login screen when authentication is rejected					
Authorization	Connection Aliases					
SSL VPN	🗣 Add 🖪 Delete					
	Alias					
	AC-USERS					
	Group 1 PLs					
	🗣 Add 📷 Delete					
	URL	Enabled				
]					
	ОК	Cancel Help				

a. ةفاضإ رتخأ

b. اەمادختسإ ديرت يتلا ةعومجملل راعتسملا مسالا لخدأ.

c. دكأت الكشلار عن المراب المرابع المرابع الم الم الم الم

.OK قوف رقناو .13

(OCSP مادختسإ متيس ناك اذإ) ةداهشلا ةقباطم دعاوق

- لكشلا رظنا. طئارخ ليصوت SSL VPN ىلإ ةداەش < مدقتم < Remote Access VPN ترتخأ .1 22.
 - a. ليصوتلا تافيصوت طئارخ مسق يف ةفاضإ رتخأ.
 - b. مسق يف DefaultCertificateMap ةطيرخك ةدوجوملا ةطيرخلاب ظافتحالا كنكمي ل ةقثلا طئارخ لعفلاب مدختست تنك اذإ ةديدج ةطيرخ ءاشنإ وأ ةطيرخلا
 - .ةدعاقلا ةيولوأ ىلع ظفاح .c
 - d. الكشلار رظنا .— نيعم ريغ مساب كرتأ ،ةنيعم ةعومجم تحت.

تاداەشلا ةقباطم ةدعاق ةفاضإ :22 لكشلا

Configure a certificate Matchi Configure a certificate match rule priority uniquely identifie to the rule with lower values will be ignored.	ing Rule ing rule and associ s the certificate ma having greater pric	ate it with a connection profile. The atching rule and assigns a priority prity. Rules that are not mapped
Мар:	💽 Existing	DefaultCertificateMap
	🔘 New	
Priority:	20	
Mapped to Connection Profile	e: Not Mapped -	
	Canal	

- .OK قوف رقناو .e
- يلفسلا لودجلا يف ةفاضإ قوف رقنا .2
- 3. (العام) تاوطخلا المكأ: "قداهشلا ةقباطم قدعاق قفاضإ رايعم" قذفان يف

ةداەشلا ةقباطم ةدعاق رايعم :23 لكشلا

Choose a	digital certificate		? 🔀
	ation The Web site you want to identification. Please cho	o view requests ose a certificate.	
	Name POOLE.JUSTIN.ALLE MCGINTY.JIMMY.11 POOLE.JUSTIN.ALLE MCGINTY.JIMMY.11	Issuer DOD CLASS 3 EMAIL CA-10 DOD JITC CA-15 DOD CLASS 3 CA-10 DOD JITC EMAIL CA-15	
	Mo	re Info View Certifical	te

- a. عوضوملا يف لقحلا دومعب ظافتحالا.
- b. ەلمكأب لقحلا يف نوكملا دومعب ظافتحالا.
- c. يواسي ال ىلإ ليغشتلا لماع دومع رييغتب مق.
- d. سابتقا يتمالع لخدأ ،ةميقلا دومع يف.
- e. لاثملال ليبس ىلع 23 لكشلا عجار .قبطيو ok ةقطقط.

OCSP نيوكت

نيوكت فلتخي نأ نكمي OCSP. نيوكت فلتخي نأ نكمي تامولعملا نم ديزمل.

OCSP بيجتسملا ةداەش نيوكت

OCSP. بيجتسملا نم ايتاذ اهؤاشنإ مت ةداهش ىلع لوصحلا .1

OSCP. مداخل ةداهش تيبثتب مقو اقباس ةروكذملا تاءارجإلا لمكأ .2

ةداەشل ةقثلاا ةطقنل ءاغلإلاا تاداەش نم ققحتلا مدع ديدحت نم دكأت :ةظحالم OCSP.

OCSP مادختسال CA نيوكت

- .CA تاداهش < دعب نع لوصولا تاداهش ةرادإ رتخأ .1
- 2. تزكر OCSP in order to لمعتسي نأ لكشي نأ CA ترتخأ OCSP in order to تزكر
- .ريرحت قوف رقنا .3
- لاطبإلا ةداەش نم ققحتلا نم دكأت .4.
- .5 لكشلا رظنا. OCSP ةفاضإب مق ،لاطبإلا قرط مسق يف

OCSP لاطبإ نم ققحتلا

CRL RBINBYS	I Policy CRL Retrieval Method OCSP Rules	idvanced
O Do not check certificates for	revocation	
Check certificates for revoca	stion	
Revocation Methods		
Specify the methods used method will be used only if	for revocation checking and their order. If both the first one returns error.	methods are selected, the second
CRL	Add>> OCSP	Nove Up
	< <remove< td=""><td>Move Down</td></remove<>	Move Down
Consider certificate va	alid if revocation information cannot be retrieved	

صحف عابتا ديرت تنك اذإ اهدادرتسإ نكمي ال ...ةحلاص ةداهشلا رابتعإ نأ نم دكأت .6 مراصلا OCSP .لاطبإلل OCSP مدختست يتلا CA مداوخ ةفاك ريرحت/نيوكتب مق :ةظحالم

OCSP دعاوق نيوكت

بيجتسملا نيوكت نمو تاداەشلا ةعومجمل ةقباطم جەن ءاشنإ نم ققحت :ةظحالم OCSP بيجتسملا نيوكت نمو تاداەشلا مخمل المك تاوطخلا ەذە لامكإ لبق.

PTR و DNS A لجس ىلا قجاح كانه نوكت دق ،OCSP ذيفنت تايلمع ضعب يف :ةظحالم mil. عقوم نم ASA نأ نم قرقحتال قرقحتال اذه ءارجا متي .ينوّتال معداا تامدخ بتكمل

- 1. ترتخأ Remote Access VPN<ةرادإ ةداەش <۲۸
- .2 كرمعتسي نأ لكشي نأ CA ترتخأ OCSP in order to تزكر OCSP in order to تركر.
- .ريرحت رتخاً .3
- 4. ةدعاق بيوبتلا ةمالع قوف رقنا.
- 5. أفاضإ قوف رقنا.
- .25 لكشلا عجار .ةيلاتلا تاوطخلا لمكأ ،OCSP ةدعاق ةفاضإ ةذفان يف .6

OCSP دعاوق ةفاضإ :25 لكشلا

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

a. اقبسم اهؤاشنإ مت ةطيرخ وأ DefaultCertificateMap رتخأ ،ةداهشلا ةطيرخ رايخ يف.

b. بيجتسملا رتخأ ،ةداەشلا رايخ يف

- c. لازداب مق ،سرەفلا رايخ يف .
- d. بيجتسملاب صاخلا فيضملا مسا وأ IP ناونع لخدأ ،طبرلا ناونع رايخ يف AS. مداخ نيوك DCSP مداخ نيوكت نم دكأتف ،فيضملا مسا مدختست تنك اذإ

e. قوف رقناو OK.

.قيبطت قوف رقنا .f

Cisco نم AnyConnect ليمع نيوكت

Cisco AnyConnect VPN. ليمع نيوكت مسقلا اذه يطغي

لعفلاب Middleware قيبطتو Cisco نم AnyConnect VPN ليمع تيبثت مت - تاضارتفالا و ActiveCard Gold رابتخإ مت .فيضملا رتويبمكلا يف

طقف AC ليمعل يلوألا تيبثتلل ةعومجملا URL بولسأ ليلدلا اذه مدختسي :ةظحالم. اليمع لثم امامت AC قيبطت ليغشتب موقت ،AC ليمع تيبثت درجمب IPsec.

تاداەش ةلسلس تيبثت مزلي :ةظحالم DoD تاداەش ةلسلس تيبثت مزلي :ةظحالم PKI POC يا عجرا .يل عجرا .يل عرب اي اي عجرا

Cisco AnyConnect VPN Client - Windows ليزنت

- اناونعلا نوكي نأ يغبني .بيقنتلا لجر تنرتنإ لالخ نم ASA لا ىلا قسلج بيو تقلطأ .1 لكش ىلع https://Outside-Interface. لاثملا ليبس ىلع، <u>https://172.18.120.225</u>.
- 26. لكشلا رظنا .لوصولل اهمادختسإ دارملا عيقوتلا ةداهش رتخأ

ةحيحصلا ةداەشلا رتخأ :26 لكش

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

.كلذ كنم بلطي امدنع (PIN) يصخشلا فيرعتلا مقر لخدأ .3

PIN زمر لخدأ :27 لكش

ActivCard Gold - Enter PIN			
	Enter PIN code:		
	OK	Cancel	

- 4. نامألا ەيبنت لوبقل معن رتخأ.
- ليمعلا ةداهش مدختست .لوخدلا ليجست رتخأ ،SSL لوخد ليجست ةحفص يف ةدحاو ةرم .5 28. لكشلا رظنا .لوخدلا ليجستل

SSL لوخد ليجست :28 لكش

SSL VPN Service - Microsoft Internet Explorer provided by Cisco Systems, Inc.				
Ele Edit yew Favorites Look Help				
🔾 Back 🔹 💿 🛛 📓 💰 🔎 Search 🤺 Favorites 🥝 🍙 🛬 🔳 👘 🛄 鑬	**			
Address A https://172.18.120.225/+CSCOE+/logon.html	💌 🔁 😡	unis » 📆 •		
CISCO SSL VPN Service				

.02 لكشلا رظنا .ليمعلا ليزنت يف AnyConnect أدبي .6

AnyConnect تيبثت :29 لكش



7. تيبثت رمتسي .30 لكشلا عجار .مادختسالل ةبسانملا ةداهشلا رتخأ لكشب هتيبثت وأ ASA لاصتا لك تيبثتب ليمعلل ASA لوؤسم حمسي نأ نكمي مئاد

ةداەشلا :30 لكش



Cisco - Windows نم Cisco - Windows ليمع ليغشت ءدب

Cisco > AnyConnect VPN Client. جماربلا عيمج < Startرتخأ ،فيضملا رتويبمكلا نم

ليمع فيرعت فلم نيوكت ىلع لوصحلل (ه) قحلملا عجار :ةظحالم AnyConnect ليمع فيرعت فلم نيوكت ىلع لوصحلل (ه)

ديدج لاصتا

1. لكشلا رظنا .ددرتملا رايتلا ةذفان رهظت.

ديدج VPN لاصتا :34 لكش



- .ايئاقلت لاصتالا AC لواحي مل اذإ بسانملا فيضملا رتخأ .2
- 35. لكشلا عجار .كلذ كنم بلطي امدنع PIN زمر لخدأ

PIN زمر لخدأ :35 لكش

ActivCard Gold - Enter PIN			
Enter PIN code:			
OK	Cancel		

دعب نع لوصولا ءدب

امەب لاصتالا دىرت نيذللا فيضملاو ةعومجملا رتخا.

.36 لكشلا عجار .VPN لا تسسأ in order to طبري ،تلمعتسا تاداهش نأ امب ترتخأ

لاصتالاً :36 لكش


ةملكو مدختسم مسا لاخدال ةجاح الف ،تاداهشلا مدختسي لاصتالا نأل ارظن :ةظحالم رورم

ليمع فيرعت فلم نيوكت ىلع لوصحلل (ه) قحلملا عجار :ةظحالم AnyConnect ليمع فيرعت فلم نيوكت ىلع لوصحلل (ه)

DAP و LDAP طيطخت - أ قحلملا

هذه .LDAP طيطخت ىمست ةزيم ميدقت مت ،ثدحألا تارادصإلاو ASA/PIX نم (x).7 رادصإلاا يف رييغت ىلا ةجاحلا يفني امم ،LDAP قمس/تانئاكو Cisco قمس نيب نييعت رفوت ةيوق ةزيم لاصتا ىلع يفاضإ تاسايس ضرف اذه معدي نأ نكمي ،CAC ققداصم ذيفنتل .LDAP ططخم ءارجإل لوؤسملا قوقح ىلا جاتحت كنأ ملعا .ططخي LDAP نم لاثم اذه .دعب نع لوصولا لوصولا قسايس قزيم ميدقت مت ،ASA 8.x جمانرب يف .AD/LDAP مداخ يف تارييغت تاعومجم يف رظنلل CAC عم نارتقالاب DAP لوكوتورب لمعي نأ نكمي .(DAP) يكيمانيدلا مانيدا مراي قوق عن الماي مي مانيد من ميدقت مي .

لوصولا نذأل يفتاهلا بلطلا مادختساب Active Directory قيبطت :1 ويرانيسلا مضفر/لوصولاب حامسلا - دعب نع

لوكوتوربلا -Cisco cVPN3000-tunneling ةمس ىلإ AD msNPAllowDailin ةمس ل|ثمل| اذه ططخي.

- ضفر = أطخ ؛حامسلا = باوص :AD ةمس ةميق •
- قمس ةميق Cisco: 1 = false، 4 (IPSec) وأ (4 IPsec + 16 WebVPN) = true،

:نييعتب مق ،"حامسلا" طرشلل

20 = حيحص •

نييعتب موقت ،يفتاهلا بلطلا ضفرل:

1 = أطخ •

ِ <u>يچراخ مداخ نيوكت</u> عجار .ةريبك فورحلا لك يف FALSE و TRUE نأ نم دكأت :ةظحالم تامولعملا نم ديزم ىلع لوصحلل <u>نامألا زامج مدختسم ضيوفتل</u>.

Active Directory دادع

- .ليغشت < أدبا قوف رقنا ،Active Directory مداخ يف .1
- ةدجو ليغشتب اذه موقي .قفاوم رقنا مث dsa.msc بتكا ،جوتفملا صنلا عبرم يف .2 ةرادإ مكحت Active Directory.
- 3. عيسوتل عمجلا ةمالع قوف رقنا Active Directory، عيسوتل عمجلا ةمالع قوف رقنا Active Directory قرادإ مكحت ةدحو يف Users and Computers.

- 4. لاجملا مسا عيسوتل عمجلا ةمالع قوف رقنا.
- ضرعل مكحتلا ةدحو عيسوتب مقف ،نيمدختسملل اهؤاشنا مت نيزخت ةدحو كيدل ناك اذا .5 دلجم يف مەنييعت مت نيذلا نيمدختسملا ةفاك كيدل ناك اذاو ،نيمدختسملا ةفاك ماد مەضرعل دلجملا اذه عيسوتب مقف ،نيمدختسملا

Active Directory ةرادإ مكحت ةدحو :A1 لكشلا



.ەريرحت ديرت يذلا مدختسملا قوف اجودزم ارقن رقنا .6

رقناو مدختسملا صئاصخ ةحفص يف "يفتاهلا بلطلا" بيوبتلا ةمالع قوف رقنا 2. أ لكشلا عجار .ضفرلا وأ حامسلا قوف

مدختسملا صئاصخ :2 فلأ لكشلا

	5 B 1 C 1 C	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	120.0400.000			100600-001
100	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		AND DOMESTIC OF	1. C. C. C. C. C.		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
100	10 C 10					
					and the second second	

Remote Access Permission (Dial-in or	(VPN)
Allow access	
C Deny access	
🔿 Control access through Remote A	Access Bolicy
T Veišu Siziecij():	
Callback Options	1
• No Caliback	
Set by Caller (Routing and Remo)	te Access Service only)
C Always Callback to:	
-	
Assign a Static IP Address	J
Andu Statz: Ricutes	

7

.OK قوف رقنا مث .7

ASA نيوكت

.LDAP ةمس ةطيرخ < <VPN دعب نع لوصولل AAA دادعإ رتخأ ،ASDM يف .1

.(Add) ةفاضإ قوف رقنا .2

3. أ لكشلا رظنا .ةيلاتلا تاوطخلا لمكأ ،LDAP ةمس ةفاضإ ةطيرخ ةذفان يف .3

LDAP ةمس نييعت ةفاضإ :A3 لكشلا

🖆 Add LDAP Attribute Map		×
Name: msNPAloxOlain		
	Customer Name	Cisco Name
Customer Name: InsNPAllowDialm Control Contro	Add >> 111	
СПСК	Cancel II Help II	

- .مسالا صن عبرم يف امسا لخدأ .a
- b. مسا" صنلا عبرم يف msNPAllowDialin بتكا ،"ةطيرخلا مسا" بيوبتلا ةمالع يف اليمعل.
- c. رايخلا يف يقفنلا لاصتالا تالوكوتورب رتخأ ،ةطيرخلا مسا بيوبتلا ةمالع يف مسا يف لدسنملا Cisco.
- d. افاضإ قوف رقنا).
- e. ةميق نييعت بيوبتلا ةمالع رتخا.
- f. اةفاضإ قوف رقنا).
- g. صنلا عبرم يف TRUE بتكا ،ةفاضملا ةمسلل LDAP ةطيرخ ةميق ةذفان يف مين مين ا عبرم يف 20 بتكاو ليمعل مسا
- h. اةفاضإ قوف رقنا).
- i. اعجار Cisco. ةميق صن عبرم يف 1 بتكاو ليمعلا مسا صن عبرم يف FALSE بتكا الأ لكشلا

ustomer Name: ms/NPAllowOtalin			
		Customer Value	Cisco Value
		FALSE	1
Customer Value:	Add >>		

- j. قوف رقناو
- k. قوف رقناو OK.
- .قيبطت قوف رقنا .ا
- m. لكشلا لثم نيوكتلا ودبي نأ بجي A5.

LDAP ةمس نييعت نيوكت :A5 لكشلا

🛍 Cisco ASDM 6.0 for ASA - 172	2.18.120.225		
Ele Yew Tools Wigards Window	w Help	Look For: Find	alala
Home Configuration M	lonitoring 🔚 Save 🄇	Refresh 🔇 Back 💭 Forward 🧳 Help	CISCO
Remote Access V 🗗 🕈 ×	Configuration > Rem	ote Access VPN > AAA Setup > LDAP Attribute Map	
E Inetwork (Client) Access A Inetwork (Client) Access			
AAA Setup	Add and configure a	attribute map used by LDAP server.	
DAP Attribute Map	Name	Attribute Map Name	
🕀 🕂 Secure Desktop Manager 👱	msNPAlowDialn	msNPAllowDialn=Tunneling-Protocols	
			E
Service Setup			D
Firewall			
Remote Access VPN			
Site-to-Site VPN			
Device Management	a and a set of the set		
30 *		Reset	
			_

.6 فلأ لكشلا رظنا. AAA مداوخ تاعومجم < <VPN دعب نع لوصولل AAA دادعإ رتخأ .4

AAA مداوخ تاعومجم :A6 لكشلا

🕵 Cisco ASDM 6.0 for ASA - 17	2.18.120.225				
Ele View Tools Wigards Windo	ow Help Monitoring 🛄 Save (Look For:	Back 🚫 Forward 🗌	Find -	dialia cisco
Remote Access V a P ×	Configuration > Ren	note Access VP	> AAA Setup > AAA	Server Groups	
Network (Client) Access	AAA Server Groups				
AAA Setup	Server Group	Protocol	Accounting Mode	Reactivation M	Add
AAA Server Groups	AD-LDAP LOCAL	LDAP		Depletion	Edit
🖶 🚮 Local Users 🕀 🕂 Gecure Desktop Manager 👱	<	U.		>	Delete
< H >	Servers in the Selecte	d Group			
Device Setup	Server Name or IF	Address	Interface	Timeout	Add
🕵 Firewall	172.18.120.160		outside	10	Edit
Remote Access VPN					Delete
Site-to-Site VPN					Move Up
Device Management					Move Down
*			Apply Reset		
Device configuration loaded	d	sco 15	6 🛃 🗖	7/17	/07 1:59:07 PM UTC

- ةعومجملا مسق يف ةدوجوملا مداوخلا يف .اهريرحت ديرت يتلا مداوخلا ةعومجم قوف رقنا .5 ريرحت قوف رقنا مث ،فيضملا مسا وأ مداخلاب صاخلا IP ناونع رتخأ ،ةددحملا.
- الما الما المات المات المات المات المات المات Edit AAA Server، المات المات المات المات المات المات المات المات A7 لك شل المات المات

LDAP ةمس نييعت ةفاضإ :A7 لكشلا

🖆 Edit AAA Server

		ADIDAD		
Server Group:				
Interface Name:		outside	*	
Server Name or IP Addr	ess:	172,18,120,160		
Timeout:		10		seconds
LDAP Parameters				
Enable LDAP over	r SSL			
Server Port:	389			
Server Type:	D6	etect Automatically/Use Generic Type]
Base DN:	CN=	Users,DC=ggsgseclab,DC=org		
Scope:	One	level beneath the Base DN		

.OK قوف رقناو .7

طبر لمع نم ققحتلل رابتخالاب موقت امنيب LDAP حيحصت ليغشتب مق :ةظحالم فاشكتسأ رماوأ ىلع لوصحلل (ج) قحلملا عجار .حيحص لكشب تامسلا طيطختو LDAP اهحالصإو ءاطخألاا.

حامسلل ةعومجملا ةيوضع مادختساب Active Directory قيبطت :2 ويرانيسلا

ەضڧر وأ لوصولاب

ءاشنإل يقفنلا لاصتالا لوكوتورب ةمسل LDAP ةمس وضع نييعت لاثملا اذه مدختسي طورشلا هذه كيدل رفوتت نأ بجي ،ةسايسلا هذه حجنت يكل .طرشك ةعومجم ةيوضع:

- ASA VPN يمدختسمل ةديدج ةعومجم ءاشنإب مق وأ لعفلاب ةدوجوم ةعومجم مدختساً
 حامسلاً طورش يف اوضع اونوكيل.
- ASA ريغ يمدختسمل ةديدج ةعومجم ءاشنإب مق وأ لعفلاب ةدوجوم ةعومجم مدختساً
 ASA ريغ يمدختسمل قديدج تعومجم عاشناب مق وأ لعفل العام العورش يف اوضع نوكتل
- نإ .د قحلملا رظنا .ةعومجملل حيحصلا DN كيدل رفوتي يذلا LDAP ضراع عاديإ نم دكأت حيحص لكشب لمعي ال ططخي لا ،أطخ DN لا نوكي.

يف طقف memeberOf ةمسلاا نم ىلوألاا ةلسلسلا ةءارق ASA ل نكمي هنأ ملعا :ةظحالم ةمئاقلاا ىلعأ يف ةدوجوم اهؤاشنإ مت يتلا ةديدجلا ةعومجملا نأ نم دكأت .رادصإلاا اذه. الوأ ةصاخلا فورحلا ىل AD رظني امدنع مسالا مامأ صاخ فرح عضت نأ وه رخآلا رايخلا. قددعتم تاعومجم يف رظنلل 8.x جمانرب يف DAP مدختسأ ،ريذحتلا اذه لوح لمعلل.

ثيحب ىرخأ ةعومجم لقألاا ىلع وأ ضفرلاا ةعومجم نم ءزج مدختسملاا نأ نم دكأت :ةظحالم بذاكلا ضفرلاا طرش ديدحت كيلع بجوتي ال .امئاد ASA ىلإ ىرخأ ةرم وضعلا لاسرا متي ةعومجملا مسا وأ دوجوملاا ةعومجملا مسا ناك اذإ .كلذب مايقلاا يه ةسرامم لضفأ نكلو ةقيرطلا هذهب ةمسلا لخدأف ،ةفاسم ىلع يوتحي

CN=Builtin،DC=ggsgseclab،DC=org ، يطايتحالا خسين لا لماوع

يف ةددعتم تاعومجم ىلإ رظنلاب لقتسملا ةبساحملا بتكمل DAP حمسي :ةظحالم مسق عجار .تاعومجملا هذهل يساسألا ضيوفتلاو memberOf ةمسلا

طئارخلا مسر

- AD: ةمس ةميق
 - CN=AsauSers،CN=Users،DC=ggsgseclab،DC=org
 - cN=TelnetClient،CN=Users،DC=Labrat،DC=com
- أطخ = 1 cisco: 1، أطخ، 20 = true،

نييعتلاب موقت ،حامسلا طرش لجأ نم:

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

نييعتب موقت ،ضفرلا طرشل ةبسنلاب:

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

عجار .ەضفرو لاصتالاب حامسلل Cisco ةمس كانە ،يلبقتسملا رادصإلا يف :ةظحالم لوح تامولعملا نم ديزم ىلع لوصحلل <u>نامألا زامج مدختسم ضيوفتل يجراخ مداخ نيوكت</u> تامس Cisco.

Active Directory دادع

- . ليغشت < أدبا رتخأ ،Active Directory مداخ يف .
- ا ةدحو ليغشتب اذه موقي .قفاوم رقنا مث ،dsa.msc بتكا ،حوتفملا صنلا عبرم يف .2 قرادإ مكحت Active Directory.
- 3. عيسوتل عمجلا ةمالع قوف رقنا Active Directory، عيسوتل عمجلا ةمالع قوف رقنا Active Directory قرادإ مكحت ةدحو يف Users and Computers. أ لكشلا رظنا 8

Active Directory تاعومجم :A8 لڬشلا

Elle Action View Window H	elp 1 19 19 19 19 19 23 19	,		-16
Active Directory Users and Computer	Users 23 objects			
Saved Queries	Name	Туре	Description	1
🖲 🧾 Builtin	Administrator Artperez	User User	Built-in account for administering the co	
Computers	AGASAUsers	Security Group	VPN Remote Access Users	
Ontain Controllers ForeignSecurityPrincipals	Cert Publishers	Security Group Security Group	Members of this group are permitted to	
MIL	DonsAdmins	Security Group	DNS Administrators Group	
Users	DnsUpdateProxy	Security Group	DNS clients who are permitted to perfor	
	Domain Admins	Security Group	Designated administrators of the domain	
	Domain Computers	Security Group	All workstations and servers joined to th	
	Domain Controllers	Security Group	All domain controllers in the domain	
	Domain Guests	Security Group	All domain guests	
	Domain Users	Security Group	All domain users	
	DEnterprise 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	
	1 HelpServicesGroup	Security Group	Group for the Help and Support Center	
	115_WPG	Security Group	IIS Worker Process Group	
	1USR_CISCOJAX-2K3	User	Built-in account for anonymous access t	
	IWAM_CISCOJAX-2K3	User	Built-in account for Internet Information	
	TRAS and IAS Servers	Security Group	Servers in this group can access remote	
	Schema Admins	Security Group	Designated administrators of the schema	
	SUPPORT_388945a0	User	This is a vendor's account for the Help a	
	78 Teinet Clients	Security Group	Members of this group have access to T	(+)+

- 4. لاجملا مسا عيسوتل عمجلا ةمالع قوف رقنا.
- .ةعومجم < ديدج رتخاو نومدختسملا دلجملا قوف نميألا سواملا رزب رقنا .5
- 6. لائمال ليبس ىلع .ةعومجم مسا لخدأ .AsauSers.
- .OK قوف رقناو .7
- اهتأشنأ يتلا ةعومجملا قوف اجودزم ارقن رقنا مث ،نومدختسملا دلجملا قوف رقنا .8

وتلل.

.ةفاضإ قوف رقنا مث ،ءاضعأ بيوبتلا ةمالع رتخأ .9

.قفاوم قوف رقنا مث ،ەتفاضإ ديرت يذلا مدختسملا مسا بتكا .10

ASA نيوكت

- . LDAP ةمس ةطيرخ < AAA دادعإ < (دعب نع لوصولا) Remote Access VPN رتخأ ،ASDM يف .1
- 2. أفاضإ قوف رقنا).
- .3 أ لكشلا رظنا .ةيلاتلا تاوطخلا لمكأ ،LDAP ةمس ةفاضإ ةطيرخ ةذفان يف .3
 - a. مسالا صن عبرم يف امسا لخدأ.
 - b. مسا" ب صاخلا "ج" صنلا عبرم يف وضع بتكا ،"ةطيرخلا مسا" بيوبتلا ةمالع يف "ليمعلا.
 - c. رايخلا يف يقفنلا لاصتالا تالوكوتورب رتخأ ،ةطيرخلا مسا بيوبتلا ةمالع يف مسا يف لدسنملا
 - .ةفاضإ رتخأ .d
 - e. ةميق نييعت بيوبتلا ةمالع قوف رقنا.
 - .ةفاضإ رتخأ .f
 - g. بتكا ،ةفاضإلا ةمسل LDAP ةطيرخ ةميق ةذفان يف cn=asauSers،cn=Users،dc=ggsgseclab،dc=org بتكاو ليمعلا مسا صنلا عبرم يف 20 Gisco.
 - h. اةفاضإ قوف رقنا).
 - i. ليمعلا مسا صن عبرم يف cn=telnetClient،cn=Users،dc=ggsgseclab،dc=org بتكا ةميق صن عبرم يف 1 بتكاو Cisco. أ لكشلا عجار
 - .)OK قوف رقناو .j
 - .OK قوف رقناو .k
 - .قيبطت قوف رقنا .ا
 - m. لكشلا لثم نيوكتلا ودبي نأ بجي
 - نييعت ةمس A9 LDAP لكش

🖀 Cisco ASDM 6.0 for ASA - 172	2.18.120.225			
Ele Yew Tools Wigards Windo	w Help Ionitoring 📊 Save I	Look For:	Forward ? Help	cisco
Remote Access V Network (Client) Access Clientless SSL VPN Access AAA Setup AAA Setup AAA Setver Groups	Configuration > Ren Add and configure	note Access VPN > AAA So e attribute map used by LDAP se	etup > LDAP Attribute erver.	tap 🗆
Cocal Users Cocal Users Coca	Name memberOf	Attribute Map Name memberOf—Tunneing-Pro	otocols	
Erewall				
Device Management		Apply	Reset	
Configuration changes say	d	sco 15		7/17/07 2:14:47 PM UTC

- AAA مداوخ تاعومجم < <VPN دعب نع لوصولل AAA دادعإ رتخأ .4
- ةعومجملا مسق يف ةدوجوملا مداوخلا يف .اهريرحت ديرت يتلا مداوخلا ةعومجم قوف رقنا .5 ريرحت قوف رقنا مث ،فيضملا مسا وأ مداخلاب صاخلا IP ناونع ددح ،ةددحملا

p Name Map Value		
Customer Name	Customer to Osco Map Value	boa
memberOf	CN=TelnetClients, CN=Users, DC=ggsgsedab, DC=org=1 CN=ASAUsers_CN=Users_DC=ggsgsedab_DC=gra=20	
		Edit
		Delete

6. تامس ةطيرخ ددح ،LDAP تامس ةطيرخ صن عبرم يف ،Edit AAA Server ةذفان يف .DAP تامس ةطيرخ ددح ،LDAP تامس ةطيرخ صن عبرم يف

حيحصت ليغشتب مق :ةظحالم LDAP طبر نأ نم ققحتلل رابتخالاب موقت امنيب LDAP حيحصت ليغشتب مق رماوأ ىلع لوصحلل (ج) قحلملا عجار .حيحص لكشب لمعت تامسلا تانييعتو اهحالصإو ءاطخألاا فاشكتسأ.

ءاضعألاا تامس نم ديدعلل يكيمانيدلا لوصولا تاسايس :3 ويرانيسلا

ىلع ءانب لوصولاب حامسلل نيددعتم ءاضعأ تامس يف رظنلل DAP لاثملا اذه مدختسي قومجم ةيوضع ASA عم .طقف وضع ةمس لوأ أرقي ASA ناك ،8.x لبق .Active Directory قعومجم ةيوضع مرقي نأ نكمي ،ثدحألا تارادصإلاو ASA وقي نا نكمي ،ثدحالا تارادصإل

- (ةددعتم تاعومجم وأ) ةديدج ةعومجم ءاشنإب مق وأ لعفلاب ةدوجوم ةعومجم مدختساً
 حامسلا طورش يف ءاضعا اونوكيل ASA VPN يمدختسمل
- ASA ريغ يمدختسمل ةديدج ةعومجم ءاشنإب مق وأ لعفلاب ةدوجوم ةعومجم مدختساً
 ASA ريغ يمدختسمل قديدج تعومجم عاشناب مق وأ لعفل العام العورش يف اوضع نوكتل
- نإ .د قحلملا رظنا .ةعومجملل حيحصلا DN كيدل رفوتي يذلا LDAP ضراع عاديإ نم دكأت حيحص لكشب لمعي ال ططخي لا ،أطخ DN لا نوكي.

ASA نيوكت

- لوصولاا تاسايس < (ليمعلا) <VPN ةكبش ىلإ دعب نع لوصولا رتخأ ،ASDM يف .1 ةيكيمانيدلا.
- 2. أفاضإ قوف رقنا).
- ةيلاتا تاوطخلا لمكأ ،يكيمانيدلا لوصولا ةفاضإ جەن يف .3:
 - a. ب مسالا صن عبرم يف امسا لخدأ.
 - b. نم ربكأ مقر وأ ،1 لخدأ ،ةيولوألا مسق يف
 - c. ةفاضإ قوف رقنا ،ديدحتاا ةئف يف.
 - . LDAP رتخأ ،AAA ةفاضإ ةمس يف .d
 - e. لخدأ ،ةمسلا فرعم مسق يف
 - f. ةعومجم لكل ةوطخلا هذه ررك .نالعإلاا ةعومجم مسا لخدأو = رتخأ ،ةميقلا مسق يف مسا لخدأو = رتخأ ،ةميقلا مسق يف A10.

AAA10 ةمس ةطيرخ لكش

🛋 Add AAA	Attrib	ute 🔀
AAA Attribute	Type:	LDAP
Attribute ID:	membe	rOF
Value:	= 🗸	_ASAUsers

- .OK قوف رقناو .g
- h. أ لكشلا رظنا .رارمتسإ رتخأ ،لوصولا جەن تامس مسق يف

ةيكيمانيد ةسايس ةفاضإ A11 لكشلا

and the second				
asoription: Multi-Group Membership Check			Priority: 1	a second
Selection Oritoria				
Define the AAA and endpoint attributes used to select this a below and every endpoint attribute has been satisfied. Ther specify the logical expression text.	ccess policy. A policy e attributes can be c	is used when a user's reated using the tables	authorization attributes match the AA s 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 en	idpoint attributes are satisfied.	
AAA Attribute Operation/Value	Add	Endpoint ID	Name/Operation/Value	Add
Idap.memberOf = _ASAUsers	Edt			Fill
dap.memberOf = YPNUsers				
	Delete			Delete
				Logical Op.
Advanced	<u>신</u>			(\$)
Advanced Access Folicy Attributes Configure access policy attributes for this policy. Attributes Action Network ACL Filters Web-Type ACL Filters Fun Action: Continue Terminate	values specified here	will override those valu	ues obtained from the AAA system. vocass Method	\$
Advanced Access Policy Attributes Configure access policy attributes for this policy, Attributes Action: Network ACL Filters Web-Type ACL Filters Fun Action: Continue Terminate Specify the message that will be displayed when this record	values specified here tions Port Forward	will override those val. Ing Lists LRL Lists A	ues obtained from the AAA system. Incress Method	(\$)
Advanced Access Folicy Attributes Configure access policy attributes for this policy. Attributes Action Network ACL Filters Web-Type ACL Filters Fun Action: Continue Terminate Specify the message that will be displayed when this reco User Message:	values specified here ctions Port Forward rd is selected.	will override those val. Ing Lists URL Lists A	ues obtained from the AAA system. vocass Method	 >
Advanced Access Folicy Attributes Configure access policy attributes for this policy. Attributes Action Network ACL Filters Web-Type ACL Filters Fun Action: O Continue Terminate Specify the message that will be displayed when this recor User Message:	values specified here ctions Port Forward rd is selected.	will override those valu	ues obtained from the AAA system. vocess Mathod	•

- لوصولاا تاسايس < (ليمعلا) <VPN ةكبش ىلإ دعب نع لوصولا رتخأ ،ASDM يف .4 .ةيكيمانيدلا
- 5. (ريرحت) Edit رتخاو يضارتفال الوصول اجهن رتخأ.
- .12 أ لكشلا رظنا .ءاەنإ ىلع يضارتڧالا ءارجإلا نييعت بجي .6

ةيكيمانيدلا ةسايسلا ريرحت A12 لكشلا

	DIRACCESSPOICY
escription:	
Access Poli Configure	y Attributes access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA system.
Action	Network ACL Filters Web-Type ACL Filters Functions Port Forwarding Lists URL Lists Access Method
Specify	the message that will be displayed when this record is selected.
1972 P. 1972 P. 1973	
User M	issage:

يأ يف نكت مل اذإ ىتح لوخدلاب كل حامسلا متي ،ءاەنإ ديدحت متي مل اذإ :ةظحالم ةعباتملا وه يضارتفالا نأل تاعومجم.

ASA CLI نيوكت - ب قحلملا

ASA 5510
<#root>
ciscoasa#
show running-config
: Saved
: ASA Version 8.0(2)
! hostname asa80 domain-name army.mil enable password 8Ry2YjIyt7RRXU24 encrypted names !
interface GigabitEthernet0/0 nameif outside
ip address x.x.x.x 255.255.128
interface GigabitEthernetO/1 nameif inside security-level 100
no ip address !
boot system disk0:/asa802-k8.bin ftp mode passive dns server-group DefaultDNS domain-name army.mil
! ACL's
access-list out extended permit ip any any
pager lines 24 logging console debugging mtu outside 1500 I
VPN Pool ip local pool CAC-USERS 192.168.1.1-192.168.1.254 mask 255.255.255.0
! no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400 access-group out in interface outside
route outside 0.0.0.0 0.0.0.0 172.18.120.129 1

timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute -----LDAP Maps & DAP----ldap attribute-map memberOf map-name memberOf Tunneling-Protocols March 11, 2008 ASA - CAC Authentication for AnyConnect VPN Access Company Confidential. A printed copy of this document is considered uncontrolled. 49 map-value memberOf CN=_ASAUsers,CN=Users,DC=ggsgseclab,DC=org 20 ldap attribute-map msNPAllowDialin map-name msNPAllowDialin Tunneling-Protocols map-value msNPAllowDialin FALSE 1 map-value msNPAllowDialin TRUE 20 dynamic-access-policy-record CAC-USERS description "Multi-Group Membership Check" priority 1 dynamic-access-policy-record DfltAccessPolicy action terminate -----LDAP Server----aaa-server AD-LDAP protocol ldap aaa-server AD-LDAP (outside) host 172.18.120.160 ldap-base-dn CN=Users,DC=ggsgseclab,DC=org ldap-scope onelevel ldap-naming-attribute userPrincipalName ldap-login-password * ldap-login-dn CN=Administrator,CN=Users,DC=ggsgseclab,DC=org _____ aaa authentication http console LOCAL http server enable 445 http 0.0.0.0 0.0.0.0 outside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart -----CA Trustpoints----crypto ca trustpoint ASDM_TrustPoint0 revocation-check ocsp enrollment terminal keypair DoD-1024 match certificate DefaultCertificateMap override ocsp trustpoint ASDM_TrustPoint5 10 url http://ocsp.disa.mil crl configure crypto ca trustpoint ASDM_TrustPoint1 revocation-check ocsp enrollment terminal fqdn asa80 subject-name CN=asa80,OU=PKI,OU=DoD,O=U.S. Government,C=US keypair DoD-1024 match certificate DefaultCertificateMap override ocsp trustpoint ASDM_TrustPoint5 10 url http://ocsp.disa.mil no client-types crl configure crypto ca trustpoint ASDM_TrustPoint2

revocation-check ocsp enrollment terminal keypair DoD-2048 match certificate DefaultCertificateMap override ocsp trustpoint ASDM_TrustPoint5 10 url http://ocsp.disa.mil no client-types crl configure crypto ca trustpoint ASDM_TrustPoint3 revocation-check ocsp none enrollment terminal crl configure -----Certificate Map----crypto ca certificate map DefaultCertificateMap 10 subject-name ne "" ------CA Certificates (Partial Cert is Shown)-----crypto ca certificate chain ASDM_TrustPoint0 certificate ca 37 3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101 05050030 60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53 2e20476f 7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603 55040b13 03504b49 311b3019 06035504 03131244 6f44204a 49544320 526f6f74 crypto ca certificate chain ASDM_TrustPoint1 certificate 319e 30820411 3082037a a0030201 02020231 9e300d06 092a8648 86f70d01 01050500 305c310b 30090603 55040613 02555331 18301606 0355040a 130f552e 532e2047 6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b crypto ca certificate chain ASDM_TrustPoint2 certificate ca 37 3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101 05050030 60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53 2e20476f 7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603 55040b13 f766e045 f15ddb43 9549d1e9 a0ea6814 b64bcece 089e1b6e 1be959a5 6fc20a76 crypto ca certificate chain ASDM_TrustPoint3 certificate ca 05 30820370 30820258 a0030201 02020105 300d0609 2a864886 f70d0101 05050030 5b310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53 2e20476f 7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603 55040b13 03504b49 31163014 06035504 03130d44 6f442052 6f6f7420 43412032 301e170d 30343132 31333135 30303130 5a170d32 39313230 35313530 3031305a 305b310b 30090603 55040613 02555331 18301606 0355040a 130f552e 532e2047 6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b 1303504b 49311630 14060355 0403130d 446f4420 526f6f74 20434120 32308201 crypto ca certificate chain ASDM_TrustPoint4 certificate ca 04

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

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

prompt hostname context

اهحالصإو ءاطخألا فاشكتسأ -ج قحلملا

اهحالصإو LDAP و AAA ءاطخأ فاشكتسأ

- debug Idap 255—تالدابت ضرعي—LDAP
- debug aaa تالدابت ضرعي—10 عئاش AAA

ةحيحصلا ةمسلا نييعت عم هب حومسملا لاصتالا 1: لاثملا

جارخإ لـاثمـلا اذه حضوي debug aaa ويرانيسلاب حجان لـاصتا ءانثأ عئاش debug ldap ويرانيسلاب حجان لـاصتا (أ) قحلملا يف حضوملا

حيحص نييعت - كرتشم جارخإ debug aaa و LDAP ءاطخأ حيحصت :C1 لكشلا

```
AAA API: In aaa_open
AAA session opened: handle = 39
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type 0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[78] Session Start
[78] New request Session, context 0x26f1c44, reqType = 0
[78] Fiber started
[78] Creating LDAP context with uri=ldap:// 172.18.120.160:389
[78] Binding as administrator
[78] Performing Simple authentication for Administrator to
172.18.120.160
[78] Connect to LDAP server: ldap:// 172.18.120.160, status =
Successful
[78] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[78] Retrieved Attributes:
[78] objectClass: value = top
[78] objectClass: value = person
[78] objectClass: value = organizationalPerson
```

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

User: CAC-USER Pasw: Resp: grp_policy_ioctl(12f1b20, 114698, 1a870b4) grp_policy_ioctl: Looking up CAC-USERS callback_aaa_task: status = 1, msg = AAA FSM: In aaa_backend_callback aaa_backend_callback: Handle = 39, pAcb = 2ae115c AAA task: aaa_process_msg(1a87a64) received message type 1 AAA FSM: In AAA_ProcSvrResp Back End response: Tunnel Group Policy Status: 1 (ACCEPT) AAA FSM: In AAA_NextFunction AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status = ACCEPT AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol = , tunn pol = CAC-USERSAAA_NextFunction: New i_fsm_state = IFSM_DONE, AAA FSM: In AAA_ProcessFinal Checking time simultaneous login restriction for user 1234567890@mil AAA FSM: In AAA_Callback user attributes: 1 Tunnelling-Protocol(4107) 20 20 user policy attributes: None tunnel policy attributes: 1 Primary-DNS(4101) 4 IP: 10.0.10.100 2 Secondary-DNS(4102) 4 IP: 0.0.0.0 3 Tunnelling-Protocol(4107) 4 4 4 Default-Domain-Name(4124) 10 "ggsgseclab.org" 5 List of address pools to assign addresses from(4313) 10 "CAC-USERS" Auth Status = ACCEPT AAA API: In aaa_close AAA task: aaa_process_msg(1a87a64) received message type 3 In aaai_close_session (39) AAA API: In aaa_send_acct_start AAA API: In aaa_send_acct_stop CAC-Test#

لكشب اەنيوكت مت يتلا Cisco ةمس نييعتب ەب حومسملا لاصتالا :2 لاثملا مظتنم ريغ

جارخإ لـاثملا اذه حضوي debug aaa ويرانيسلا عم هب حومسم لـاصتا ءانثأ عئاش debug aaa ويرانيسلا عم هب حومسم لـاصتا (أ) قحلملا يف حضوملا

حيحص ريغ نييعت - كرتشم جارخإ debug aaa و LDAP ءاطخأ حيحصت :C2 لكشلا

```
AAA API: In aaa_open
AAA session opened: handle = 41
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type 0
AAA FSM: In AAA_StartAAATransaction
```

AAA FSM: In AAA_InitTransaction Initiating authorization query (Svr Grp: AD-LDAP) AAA FSM: In AAA_BindServer AAA_BindServer: Using server: 172.18.120.160 AAA FSM: In AAA_SendMsg User: 1234567890@mil Pasw: 1234567890@mil Resp: [82] Session Start [82] New request Session, context 0x26f1c44, reqType = 0 [82] Fiber started [82] Creating LDAP context with uri=ldap://172.18.120.160:389 [82] Binding as administrator [82] Performing Simple authentication for Administrator to 172.18.120.160 [82] Connect to LDAP server: ldap:// 172.18.120.160:389, status = Successful [82] LDAP Search: Base DN = [CN=Users,DC=ggsgseclab,DC=org] Filter = [userPrincipalName=1234567890@mil] Scope = [SUBTREE][82] Retrieved Attributes: [82] objectClass: value = top [82] objectClass: value = person [82] objectClass: value = organizationalPerson [82] objectClass: value = user [82] cn: value = Ethan Hunt [82] sn: value = Hunt [82] userCertificate: value = 0..50....../.....60...*.H.....0@1.0.....&...,d....com1.0..... &...,d... [82] userCertificate: value = 0...'0....../..t.....50....*.H......0@1.0.....&...,d....com1.0..... &...,d... [82] givenName: value = Ethan [82] distinguishedName: value = CN=Ethan Hunt,OU=MIL,DC=labrat,DC=com [82] instanceType: value = 4 [82] whenCreated: value = 20060613151033.0Z [82] whenChanged: value = 20060622185924.0Z [82] displayName: value = Ethan Hunt [82] uSNCreated: value = 14050[82] memberOf: value = CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org [82] mapped to cVPN3000-Tunneling-Protocols: value = CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org [82] uSNChanged: value = 14855 [82] name: value = Ethan Hunt [82] objectGUID: value = ..9...NJ..GU..z. [82] userAccountControl: value = 66048 [82] badPwdCount: value = 0 [82] codePage: value = 0 [82] countryCode: value = 0 [82] badPasswordTime: value = 127954717631875000 [82] lastLogoff: value = 0 [82] lastLogon: value = 127954849209218750 [82] pwdLastSet: value = 127946850340781250 [82] primaryGroupID: value = 513 [82] objectSid: value =q.....q.....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 =
CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=org
[82] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
[82] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[82] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
  _____
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status = ACCEPT
AAA_NextFunction: authen svr = <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:
1 Tunnelling-Protocol(4107) 20 0
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313) 10
"CAC-USERS"
Auth Status = ACCEPT
```

```
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type 3
In aaai_close_session (41)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
```

اهحالصإو DAP ءاطخأ فاشكتسأ

- DAP ءاطخاً ضرعي—DAP ءاطخاً حيحصت •
- DAP ةفيظو عبتت ضرعي—DAP

DAP عم ہب حومسملا لاصتالا :1 لاثم

ويرانيسلاب حجان للاصتا ءانثأ debug dap traceو ءاطخألاا حيحصت ءاطخأ جارخإ لـاثملاا اذه حضوي نم لـك ىلإ مامضنالـا كنكمي .ءاضعألـا تـامس نم ديدعلـا ظحال .أ قحلملاا يف حضوملا 3 _ASA. نيوكت ىلع دمتعت يتلاو ،نيتعومجملـا نم يأ tp وأ VPNUsers و

```
c3: debug dap لكش
<#root>
debug dap errors
debug dap errors enabled at level 1
debug dap trace
debug dap trace enabled at level 1
The DAP policy contains the following attributes for user:
1241879298@mil
1: action = continue
DAP_TRACE: DAP_open: C8EEFA10
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged =
20070718151143.0Z
```

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

```
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["2"] =
"_ASAUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368":
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person, CN=Schema, CN=Configuration, DC=ggsgseclab, DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] = "TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] = "CACUSERS";
DAP_TRACE: dap_add_to_lua_tree:endpoint["application"]["clienttype"] =
"IPSec";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs: CAC-USERS
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr: rec_count = 1
DAP_TRACE: Username: 1241879298@mil, DAP_close: C8EEFA10
d.
```

DAP ب لاصتالا ضفر :2 لاثملا

3 ويرانيسلاب حجان ريغ لـاصتا ءانثأ debug dap traceو DAP ءاطخأ جارخإ يلااتلا لـاثملا حضوي. أ قحلملا يف حضوملا.

	DAP ءاطخألا حيحصت :C4 لكشلا	
<#root>		
#		

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

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

```
"1241879298@mil";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs:
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
```

OCSP / امحالصإو ءاطخألا فاشكتسأ ةداهش ةئيه

- debug crypto ca 3
- (تقۇملا نزخملا وأ) ةئفلل CA مكحت ةدحو ءاطخاً حيحصت—نيوكتلا عضو يف ليجستلل

ةقباطم جەنو OCSP بيجتسم مادختساب حاجنب ةداەشلا ةحص نم ققحتلا ةلثمألا ەذە رەظت ةلشافلا تاداەشلا قعومجم.

اەتحص نم ققحتلا مت ةداەش ىلع يوتحي يذلا ءاطخألا حيحصت جارخإ C3 لكشلا حضوي جەنلا قباطت ةلماع تاداەش ةعومجمو.

لكشب اەنيوكت مت تاداەش ةعومجم ةقباطم جەنل ءاطخألا حيحصت جارخإ حضوي C4 لكشلا حيحص ريغ.

ةاغلم ةداهشب مدختسمل ءاطخألاا حيحصت جارخإ C5 لكشلا حضوي.

حاجنب ةداەشلا نم ققحتلا - OCSP ءاطخاً حيحصت :C5 لكشلا

CRYPTO_PKI: Found a suitable authenticated trustpoint ASDM_TrustPoint11. CRYPTO_PKI: Allocated OCSP data handle 0xca2d27b8 CRYPTO_PKI: Certificate validation: Successful, status: 0. Attempting to retrieve revocation status if necessary CRYPTO_PKI: status = 0: poll revocation status CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial number: OF192B, subject name: cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S. Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-15,ou=PKI,ou=DoD,o=U.S. Government,c=US. CRYPTO_PKI: Processing map rules for SSL. CRYPTO_PKI: Processing map SSL sequence 20... CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field: = cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S. Government,c=US, map rule: subject-name ne "". CRYPTO_PKI: Peer cert has been authorized by map: SSL sequence: 20. CRYPTO_PKI: Found OCSP override match. Override URL: http://198.154.68.90, Override trustpoint: ASDM_TrustPoint12 CRYPTO_PKI: crypto_pki_get_cert_record_by_subject() CRYPTO_PKI: Destroying OCSP data handle 0xca2d27b8 Crypto CA thread sleeps! CRYPTO_PKI: Attempting to find tunnel group for cert with serial number: OF192B, subject name: cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S. Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-

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

ةلشافلا تاداەشلا ةعومجم ةقباطم جەن جارخإ :C5 لكشلا

ةاغلم ةداەش جارخإ :5ميج لكشلا

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

number: 2FB5FC7400000000035, subject name: cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org CRYPTO_PKI: Certificate not validated

MS يف LDAP تانئاك نم ققحتلا - د قحلملا

ب صاخلا طوغضملا صرقلا يف Microsoft Server 2003، ب صاخلا طوغضملا صرقلا يف معدلا ليلد يلإ لقتنا ،تاودألا هذه تيبثتل .LDAP تامس/تانئاك كلذكو LDAP ةينب ضرعل تيبثت .تاودألا مث طوغضملا صرقلا يف

LDAP ضراع

.ليغشت < ءدب رتخأ ،تيبثتلا دعب 1

- 2. العن المثان الحية الحيف الما المثان المثان المثان الكا الكا الكا المثان المثان المثان المثان المثان المثان ا
- .ليصوت < ليصوت رتخأ .3
- .قفاوم قوف رقنا مث مداخلا مسا لخدأ .4
- .طبر < ليصوت رتخأ .5
- رورم ةملكو مدختسم مسا لخدأ .6.

لوؤسملا قوقح ىلإ جاتحت :ةظحالم.

- .OK قوف رقناو .7
- .01 لكشلا عجار .LDAP تانئاك ضرع .8

LDAP ضراع :D1 لكشلا



Active Directory تامدخ ةەجاو ررحم

- مداخ يف Active Directory، ليغشت < أدبا رتخأ.
- اررحملا أدبي اذه adsiedit.msc. بتكا.
- . صئاصخ قوف رقناو نئاك قوف نميألا سوامل رزب رقنا

.D2 لكشلا عجار .ةنيعم تانئاكل صئاصخلا لك ةادألا هذه رهظت

ADSI ريرحت :D2 لكشلا

🕗 ADSI Edir		S. A. A. 18. 17			_ [D] ×
😔 Elle Action Yew With 🗢 🔿 🗈 💽 🗙 😭	N=Clark Kent Properties		1	?×	<u>=161 ×</u>
ADSI Edit Domain [Oscojax-2k3.lal DC=labrat,DC=com CN=Bultin CN=Computers CN=Computers DC=Lobrat,DC=com	Show mandatory attrib Show only attributes th Attributes:	utes es hat have <u>v</u> alues		ss) show in th	Distinguished Name
CN=ForeignSec. CN=LostAndFou CN=LostAndFou CN=Clark Ke CN=Clark Ke CN=Ch=Peter Pc CN=NTDS Quotz CN=Program Da CN=System CN=Users Configuration [Ciscojax- Schema [Ciscojax-2k3.la CN=Ethan Hunt [Ciscoja	Attribute unicodePwd url userAccountControl userCert userCertFicate userParameters userPassword userPAssword userPAssword userSharedFolder userSharedFolder userSharedFolder userSharedFolder userSharedFolder userShitMECertificate userWorkstations 4	Syntax Octet String Unicode String Integer Octet String Octet String Octet String Octet String Unicode String Unicode String Unicode String Unicode String Unicode String Unicode String	Value CNot Setb CNot Setb GE048 CNot Setb Dx30 0x82 0x06 0x27 0x3 mc dl CNot Setb CNot		
	Edt	к	Cancel Apply		2

ە قحلملا

ىلإ فيصوتلا ريشي نأ نكمي .لمع ةطحم ىلإ ەتفاضإو AnyConnect فيصوت ءاشنإ نكمي .ردصملا وأ زيمملا مسالا لثم ةداەشلا ةقباطم تاملعم وأ ASA يفيضم لثم ةفلتخم ميق قفاضإ نكمي .Notepad مادختساب ەريرحت نكميو xml. فلمك فيرعتلا فلم نيزخت متي :يف فلملا نيزخت متي .ةعومجم جەن لالخ نم ASA لا نم ەعفد وأ ايودي ليمع لك ىلإ فلمل

```
C:\Documents and Settings\All Users\Application Data\Cisco\Cisco
AnyConnect VPN Client\Profile
```

ةيلاتلا تاوطخلا لمكأ

- 1. مادختساب فلملاحتفاو AnyConnectProfile.tmpl رتخأ
- عجار .فيضملا IP ناونع وأ ردصملا لثم فلملا ىلع ةبسانملا تاليدعتلا ءارجإب مق .2 لاثملا ليبس ىلع F1 لكشلا.
- .xml. ةئيه ىلع فلملا ظفحا ،ءاەتنالا دنع .3

:راصتخابو .فيرعتلا فلم ةرادإب قلعتي اميف Cisco AnyConnect قئاثو عجار

· دائم ،كتكرشل ديرف لكشب فيرعت فلم ةيمست بجي · CiscoProfile.xml

• ةيدرفلا تاعومجملل افلتخم ناك ولو ىتح ەسفن وە فيرعتلا فلم مسا نوكي نأ بجي ةكرشلا لخاد.

عم ەعيزوت متي مث ةنمآ ةرابع لوؤسم ةطساوب ەب ظافتحالا متيل فلملا اذه ميمصت مت تقو يأ يف ءالمعلا ىلع اذه XML ىلإ دنتسملا فيصوتلا عيزوت نكمي .ليمعلا جمانرب. ليزنتلا ةيلآ نم ءزجك وأ جماربلا عيزوت عم عمجم فلمك يه ةموعدملا عيزوتلا تايلآ نم نامألا ةرابع تاجتنم ضعب عم طقف ةيئاقلتلا ليزنتلا ةيلآ رفوتت .قيئاقلتلا

يذلاا XML فيرعت فلم نم ققحتلا ىلع ةدشب نيلوؤسملا عيجشت متي :ةظحالم ةفيظو لالخ نم وأ تنرتنإلا ربع ةحصلا نم ققحت ةادأ مادختساب هئاشنإب نوموقي مادختساب ةحصلا نم ققحتلا قيقحت نكمي .ASDM يف فيرعتلا فلم داريتسإ AnyConnectProfile.xsd اليرذجلا ارصنعلا وه AnyConnectProfile ليما دادي ما دوجوملا مارخيا يرذجلا رصنعا ول

.Cisco نم AnyConnect VPN ليمع فيرعت فلمل XML فلم نم ةنيع هذه

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

<pre>! Certificate Distinguished Name matching allows ! for exact match criteria in the choosing of au - <distinguishedname> - <distinguishedname> <rattern>DoD-Issuer-ABC </rattern></distinguishedname> <th><certificatematch></certificatematch></th></distinguishedname></pre>	<certificatematch></certificatematch>
<pre>- <distinguishedname> - <distinguishedname>EsSUER-CN Pattern>DoD-Issuer-ABC </distinguishedname>Essuer-ABC </distinguishedname> <th>! Certificate Distinguished Name matching allows ! for exact match criteria in the choosing of a</th></pre>	! Certificate Distinguished Name matching allows ! for exact match criteria in the choosing of a
- <serverlist> / This is the data needed to attempt a connection to ! a specific host. >></serverlist>	<pre>- <distinguishedname> - <distinguishednamedefinition operator="Equal" wildcard="Disabled"> ISSUER-CN DoD-Issuer-ABC </distinguishednamedefinition> </distinguishedname> <!--/CertificateMatch--> <!--/ClientInitialization--> - / This section contains the list of hosts from which / the user is able to select.</pre>
<pre><serverlist> / This is the data needed to attempt a connection to ! a specific host> <hostentry> <hostname>host-02</hostname> <kostaddress>host-02.dod.gov </kostaddress></hostentry> - <hostentry> <hostentry> <hostentry> <gostaddress>192.168.1.1 <!--/HostAddress--> <!--/HostEntry--></gostaddress></hostentry></hostentry></hostentry></serverlist></pre>	
<pre>! This is the data needed to attempt a connection to ! a specific host> <(HostEntry> <(HostName>host-02 <(HostAddress>host-02.dod.gov - <hostentry> <(HostEntry> <(HostName>host-01 <(HostAddress>192.168.1.1 </hostentry> </pre>	<serverlist></serverlist>
> - <hostname>host-02</hostname> <hostaddress>host-02.dod.gov</hostaddress> - <hostentry> <hostname>host-01</hostname> <hostaddress>192.168.1.1</hostaddress> </hostentry>	! This is the data needed to attempt a connection to ! a specific host.
<hostentry> <hostname>host-02</hostname> <hostaddress>host-02.dod.gov</hostaddress> </hostentry> - <hostentry> <hostname>host-01</hostname> <hostaddress>192.168.1.1</hostaddress> </hostentry>	>
	<hostentry> <hostname>host-02</hostname> <hostaddress>host-02.dod.gov</hostaddress> </hostentry> - <hostentry> <hostname>host-01</hostname> <hostaddress>192.168.1.1</hostaddress> </hostentry>

ةلص تاذ تامولعم

- RFC 3280 و X.509 قطساوب ةددجملا RFC و تاداهشلا
- <u>RFC 2560 ةطساوب ددحملا OCSP </u>
- <u>ماعلا حاتفمل مي ماسألاً مي من الما مي ما ما مع</u>
- <u>ةدوسملار ايعم بسح حضوم "نزول فيفخ OCSP"</u> •
- <u>SSL / TLS ةطساوب ددحمل RFC 2246</u>
- <u>Cisco Systems</u> <u>تادنتسمل او ينقتل امعدل ا</u>

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