تاقاطبلا ئراقو CAC مادختساب VCS نيوكت ةيكذلا

تايوتحملا

<u>قمدق ملا</u> <u>قمدق ملا</u> <u>قيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>مدختسملا تانوكملا</u> <u>مدختسملا تامولعم</u> <u>تيولام مام</u> <u>تيوكتلا</u> <u>محصلا نم ققحتلا</u> <u>اهحالص او عاطخالا فاش كتسا</u>

ةمدقملا

لوخدلا ليجستو ةيكذلاا ةقاطبلا ئراق تيبثتل ةوطخب ةوطخ تاداشرا دنتسملا اذه فصي نم (VCS) ويديفلا تالاصتا مداخ عم امهمادختساو ةكرتشملا لوصولا ةقاطبل وأ كونبلا لثم VCS ةئيبل لماوعلا ةيئانث ةقداصم بلطتت يتلا تاسسؤملل ةنمآلا تآشنملا تاذ تاموكحاا وأ تايفشتسملا

ةيساسألا تابلطتملا

تابلطتملا

دنتسملا اذهل ةصاخ تابلطتم دجوت ال.

ةمدختسملا تانوكملا

Cisco Expressway (X14.0.2). لوؤسم ىلٍ دنتسملا اذه يف ةدراولا تامولعملا دنتست

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

ةيساسأ تامولعم

مث نمو ،ةبولطملا ةقداصملا ةيساسألا ةينبلا ىلا لوصولا يف مكحتلا ةيقافتإ رفوتو عاوس ةيساسألا ةينبلا نم عزج يأو اهتئيب ىلإ لوصولا نم نكمت يذلا نم "ةمظنألا" فرعت ،ةنمآلا تاكبشلا نم اهريغو ،ايموكح ةفنصملا تائيبلا نمضو .اينورتكلإ وأ ايدام ناك لجس مادختسإ صخش يأل نكمي ."ةفرعملا ىلإ ةجاحلا" وأ "اظح لقألا لوصولا" دعاوق دوست اضيأ ةفورعملا ملا بلطتتو ،لوخدلا تناك عاوس ،ةددعتم قزهجأ ىلإ درفلا جاتحي ال يتح 2000 ماع يف ،كرتشمل لوصولا قاطب .هتناك عاوس ،ةددعتم قزهجأ يل إدص ل الحاصول تاقح لو أي الال وصولا قاطبب .متناك عاوس ،قدام ما لوصول التاقح ال يت عام من من الما القاطر وا ما الما الما ما الما الما ال

؟ةيكذلا ةقاطبلا يه ام

يتلا (PKI) ماعلا حاتفملل ةيساسألا ةينبلل ايساسأ انوكم ةيكذلا تاقاطبلا دعت نسحت ةيكذلا تاقاطبلا نأل يساسألا Windows ماظن يف جمدلل Microsoft اممدختست ينورتكلإلا ديربلاو لوخدلا ليجستو ليمعلا ةقداصم لثم ،طقف جماربلاب ةصاخلا لولحلا ةطبترملا حيتافملاو ةماعلا حيتافملا تاداهشل براقت ةطقن يه ةيكذلا تاقاطبلا .نمآلا :اهنأل

- لاكشأ نم اەريغو ةصاخلا حيتافملا ةيامحل ثبعلل ةمواقم نيزخت تادحو ريفوت ةيصخشلا تامولعملا.
- تاعيقوتلاو ةقداصملا نمضتت يتلاو ،نامألل ةيويحلا ةيباسحلا تايلمعلا لزع .ةفرعم ىلٍ جاتحت ال ٍيتلا ماظنلا نم ىرخألا ءازجألا نع حيتافملا لدابتو ةيمقرلا
- رتويبمكلا ةزهجأ نيب ىرخألا ةصاخلا تامولعملاو دامتعالا تانايب لقن ةيناكمإ نيكمت لقنتلا ءانثأ وأ لزنملا وأ لمعلا يف.

نأل Windows ليغشتلا ماظنل يساسألا ماظنلا نم أزجتي ال اءزج ةيكذلا ةقاطبلا تحبصاً رتويبمكلا ةعانصل ةبسنلاب للحلا وه امك ةبوغرمو ةديدج تازيم رفوت ةيكذلا تاقاطبلا تقولا يف ةيلخاد PKI ةيساسأ ةينب كيدل نكت مل اذإ جمدملا صرقلا وأسواملا ميدقت دنع يف رودلا اذه تيبثت دنتسملا اذه يطغي ال الوأ كلذب مايقلا نم دكأتلا كمزليف ،يلاحل انه ءارجإلا اذه ذيفنت ةيفيك لوح تامولعم يلع روثعلا نكمي نكلو ةددحملا قلاقملا هذه <u>http://technet.microsoft.com/en-us/library/hh831740.aspx.</u>

نيوكتلا

ليجست مەنكمي نيمدختسم كيدل نأو VCS عم LDAP جمدب تمق كنأ ربتخملا اذه ضرتفي LDAP. دامتعا تانايب مادختساب لوخدلا

- <u>ربتخملا تادعم</u> 1
- <u>ةيكذلا ةقاطبلا تيبثت</u> 2.
- <u>قدصملا عجرملا بلاوق نيوكت</u> .3
- <u>ليجستلا ليكو ةداەش ليجست</u> 4.
- <u>...نع ةباين ليجستلا</u> .5
- <u>كرتشملا لوصولا ةقاطبل VCS نيوكت</u> .6

:ةبولطملا تادعملا

:ةتبثملا جماربلا/راودألا هذه ىلع يوتحي يذلا Windows 2012R2 لاجم مداخ

- ةداەشلا حنم ةەج •
- مدخ Active Directory
- DNS
- ةيكذ ةقاطبب قڧرم Windows رتويبمك •
- vSEC: ةيكذلا ةقاطبلا ةرادإل CMS K-Series ةرادإلا جمانرب:



اسريف تاقاطب ئراق جمارب

ةيكذلا ةقاطبلا تيبثت

تالباك يأ ليصوت ةيفيك لوح تاميلعتب ةدوزم ةيكذلا تاقاطبلا ةءارق ةزهجأ يتأت ام قداع نيوكتلا اذه تيبثت ىلع لاثم يلي اميف .قيرورض

ةيكذلا ةقاطبلا ئراقل زاهج ليغشت جمانرب تيبثت ةيفيك

ىلإ لوخدلا ليجست ةشاش نإف ،ەتيبثتو ةيكذلا ةقاطبلا ئراق فاشتكا مت اذإ Windows ىلإ لوخدلا ليجست قشاش ناف ،ەتيبثتو نكت مل اذإ .كلذب فرتعت يتلا:

- Windows رتويبمك ىلع دوجوملا USB ذفنمب ةيكذلا ةقاطبلا ليصوتب مق .1
- بلطتي .زاهجلا ليغشت جمانرب تيبثتل ةشاشلا ىلع رهظت يتلا تاهيجوتلا عبتا .2 وأ ةيكذلا ةقاطبلل ةعنصملا ةهجلا فاشتكا مت يتلا ليغشتلا جمانرب طئاسو كلذ نم ةعنصملا ةقاوسلا جمانرب تلمعتسا يتلاح يف انا .Windows يف ليغشتلا جمانرب قوم **لانت ال** .مهعبت ليزنتلا عقوم
- **ةرادإ** قوف رقناو بتكملا حطس ىلع **رتويبمكلا زامج** زمر قوف نميألا سواملا رزب رقناً .3 ةيعرفلا ةمئاقلا يف.

- . **تامدخلا** قوف رقناو ،**تاقيبطتلاو تامدخلا** ةدقع عيسوتب مق .4
- **صئاصخ** قوف رقنا .**ةيكذلا ةقاطبلا** ىلع نميألا سواملا رزب رقنا ،نميألاا ءزجلا يف .5 ةيعرفلا ةمئاقلا يف.
- رقناو .**ليغشتلا ءدب عون** ةلدسنملا ةمئاقلا يف **يئاقلت** ددح ،**ماع** بيوبتلا ةمالع ىلع .6 قوف OK.
- .كلذب مايقلل كدشري ةزهجألا جلاعم ناك اذإ زاهجلا ليغشت دعأ .7

قدصملا عجرملا بلاوق نيوكت

- .ةيرادإلا تاودألا نم قدصملا MMC ليغشت .1
- . **ةرادا**ٍ ددحو **تاداەشلا بلاوق** ةدقع ددح وأ رقنا .2
- ا **ةفعاضم** ددح مث **ةيكذلا ةقاطبلا مدختسم** ةداهش بلاق ددح وأ نميألا سواملا رزب رقنا .3 ةروصلا يف حضوم وه امك.

a	Console1 - [C	onsole Root\Certifica	te Temp	lates (2012DC-	AD.jajanson.local)]		
http://www.sevorites.com/action/linear-tende	P						- 8 ×
Console Root	Template Display Name	Schema Version	Versi	Intended Purpos	es	~	Actions
Certification Authority (Local)	Administrator	1	4.1				Certificate Templates (2012DC-AD iai
Certificate Templates (2012DC-AD.jajanson.loc	Authenticated Session	1	3.1				Man Astron
	Basic EFS	1	3.1				More Actions
	CA Exchange	2	106.0	Private Key Archi	ival		Smartcard User
	CEP Encryption	1	4.1				More Actions
	Code Signing	1	3.1				indic School P
	Computer	1	5.1				
	Cross Certification Authority	2	105.0				
	Directory Email Replication	2	115.0	Directory Service	Email Replication		
	Domain Controller	1	4.1				
	Domain Controller Authentication	2	110.0	Client Authentica	ation, Server Authentication, Smart Card Logon		
	EFS Recovery Agent	1	6.1				
	Enrollment Agent	1	4.1			_	
	Enrollment Agent (Computer)	1	5.1			-	
	Exchange Enrollment Agent (Offline requ	1	4.1				
	Exchange Signature Only	1	6.1				
	Exchange User	1	7.1				
	2 IPSec	1	8.1				
	IPSec (Offline request)	1	7.1				
	Kerberos Authentication	2	110.0	Client Authentica	ation, Server Authentication, Smart Card Logon, KD		
	Key Recovery Agent	2	105.0	Key Recovery Ag	jent		
	OCSP Response Signing	3	101.0	OCSP Signing			
	RAS and IAS Server	2	101.0	Client Authentic	ation, Server Authentication		
	Root Certification Authority	1	5.1				
	Router (Offline request)	1	4.1				
	Smartcard Logon	1	6.1				
	Smartcard User	1	11.1		Duplicate Template		
	Smartcard User_VCS	4	101.6	Secure Email	ogon		
	Subordinate Certification Authority	1	5.1		All Tasks		
	Trust List Signing	1	3.1		Properties		
	2 User	1	3.1		Help	$\overline{}$	
< III >	Contraction of the Contraction o				>		

لاجملاب مكحتلا ةدحو تاداهش بلاوق

. رمألا مزل اذإ هرييغتب مقو ديدحتلا عجار ،**قدصم عجرم** تحت ،**قفاوت** بيوبتلا ةمالع يف .4

Smartcard	User_VCS	Properties	? X					
Subject Name	Subject Name Issuance Requirements							
Superseded Templates	Extensions	Extensions Security Server						
General Compatibility Requ	est Handling	Cryptography	Key Attestation					
The template options available versions set in Compatibility Se	e are based on t ettings.	the earliest oper	rating system					
Show resulting changes								
Compatibility Settings								
Certification Authority								
Windows Server 2012 R2		~						
Certificate recipient								
Windows 8.1 / Windows	Server 2012 R.	~						
These settings may not prevent template.	nt earlier operat	ing systems fron	n using this					
ОК	Cancel	Apply	Help					

ةيكذلا ةقاطبلا

5. **ماع** بيوبتلا ةمالع ىلع:

أ. لثم ،امسا ددح SmartCard User_VCS.

.ق**بطي** ةقطقط .ةبوغرملا ةميقلا ىلع ةيحالصلا ةرتف نييعتب مق .ب

ةيكذلا ةقاطبلل ماعلا تقولا

6. **بلطلا ةجلاعم** بيوبتلا ةمالع يف:

.**ةيكذلاا ةقاطبلاا ىل| لوخدلا ليجستو عيقوتلا** ىلع **ضرغلا** نييعت.أ

.قربطي ةقطقط .ليجستلا ءانثأ مدختسملا ةبلاطم قوف رقنا .ب

Server Issuance Requirements perseded Templates Extensions Security bility General Request Handling Cryptography Key Attestation we: Signature and smartcard logon v Delete revoked or expired certificates (do not archive) Include symmetric algorithms allowed by the subject d) Include symmetric algorithms allowed by the subject Archive subject's encryption private key ww private key to be exported automatic renewal of smart card certificates, use the existing key if a v key cannot be created (*) following when the subject is enrolled and when the private key ated with this certificate is used: oil subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the rate key is used rol is disabled due to compatibility settings. settings.	Cubicat Name	Course of the							
bility General Request Handling Cryptography Key Attestation bility General Signature and smartcard logon ✓ Clelete revoked or expired certificates (do not archive) Include symmetric algorithms allowed by the subject Include symmetric algorithms allowed by the subject Archive subject's encryption private key w Archive subject's encryption private key automatic renewal of smart card certificates, use the existing key if a v key cannot be created (*) following when the subject is enrolled and when the private key ated with this certificate is used: oll subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the rate key is used rol is disabled due to compatibility settings.	Superceded Templa	Server	Issuance Requirements						
billing Centerial Hereiter Halling Cyptography Hey Attestation ee: Signature and smartcard logon v Delete revoked or expired certificates (do not archive) Include symmetric algorithms allowed by the subject Delete revoked or expired certificates (do not archive) Delete revoked or expired certificates (do not archive) Delete revoked or expired certificates (do not archive) Delete symmetric algorithms allowed by the subject Archive subject's encryption private key we with the same key (") automatic renewal of smart card certificates, use the existing key if a v key cannot be created (") following when the subject is enrolled and when the private key ated with this certificate is used: oll subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the rate key is used rol is disabled due to compatibility settings.	Compatibility General	Request Handling		Key Attestation					
e: Signature and smattcard logon Delete revoked or expired certificates (do not archive) Include symmetric algorithms allowed by the subject Archive subject's encryption private key we private key to be exported new with the same key (") automatic renewal of smart card certificates, use the existing key if a v key cannot be created (") following when the subject is enrolled and when the private key ated with this certificate is used: oll subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the rate key is used rol is disabled due to compatibility settings.			ciyptography	They recordion					
Delete revoked or expired certificates (do not archive) Delete revoked or expired certificates (do not archive) Archive subject's encryption private key w private key to be exported hew with the same key (") automatic renewal of smart card certificates, use the existing key if a v key cannot be created (") following when the subject is enrolled and when the private key ated with this certificate is used: oll subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the rate key is used ol is disabled due to compatibility settings.	urpose: Signa	ture and smartcard	logon	~					
 Include symmetric algorithms allowed by the subject Archive subject's encryption private key Inverse key to be exported Inverse key is used Inv	De	lete revoked or exp	ired certificates (o	do not archive)					
Archive subject's encryption private key w private key to be exported hew with the same key (") automatic renewal of smart card certificates, use the existing key if a v key cannot be created (") following when the subject is enrolled and when the private key ated with this certificate is used: oll subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the vate key is used rol is disabled due to compatibility settings.		lude symmetric algo	orithms allowed by	the subject					
w private key to be exported new with the same key (") automatic renewal of smart card certificates, use the existing key if a w key cannot be created (") following when the subject is enrolled and when the private key ated with this certificate is used: roll subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the rate key is used rol is disabled due to <u>compatibility settings.</u>	Arc	hive subject's encr	yption private key	/					
w private key to be exported new with the same key (*) automatic renewal of smart card certificates, use the existing key if a v key cannot be created (*) following when the subject is enrolled and when the private key ated with this certificate is used: oll subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the rate key is used rol is disabled due to <u>compatibility settings.</u>									
w private key to be exported new with the same key (*) automatic renewal of smart card certificates, use the existing key if a v key cannot be created (*) following when the subject is enrolled and when the private key ated with this certificate is used: roll subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the rate key is used rol is disabled due to <u>compatibility settings.</u>									
w private key to be exported new with the same key (") automatic renewal of smart card certificates, use the existing key if a v key cannot be created (") following when the subject is enrolled and when the private key ated with this certificate is used: roll subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the vate key is used rol is disabled due to <u>compatibility settings.</u>									
w private key to be exported new with the same key (") automatic renewal of smart card certificates, use the existing key if a v key cannot be created (") following when the subject is enrolled and when the private key ated with this certificate is used: roll subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the rate key is used rol is disabled due to <u>compatibility settings.</u>									
new with the same key (*) automatic renewal of smart card certificates, use the existing key if a v key cannot be created (*) following when the subject is enrolled and when the private key ated with this certificate is used: oll subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the vate key is used rol is disabled due to <u>compatibility settings.</u>	Allow private key to	be exported							
automatic renewal of smart card certificates, use the existing key if a v key cannot be created (*) following when the subject is enrolled and when the private key ated with this certificate is used: oll subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the vate key is used rol is disabled due to <u>compatibility settings.</u>	Renew with the san	ne key (*)							
following when the subject is enrolled and when the private key ated with this certificate is used: oll subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the rate key is used rol is disabled due to <u>compatibility settings.</u>	For automatic renew new key cannot be	val of smart card ce created (*)	rtificates, use the	existing key if a					
roll subject without requiring any user input mpt the user during enrollment mpt the user during enrollment and require user input when the rate key is used rol is disabled due to <u>compatibility settings.</u>	Do the following when a associated with this cer	the subject is enrolle tificate is used:	ed and when the	private key					
mpt the user during enrollment mpt the user during enrollment and require user input when the rate key is used rol is disabled due to <u>compatibility settings.</u>	O Enroll subject without	ut requiring any use	rinput						
mpt the user during enrollment and require user input when the rate key is used rol is disabled due to <u>compatibility settings.</u>	Prompt the user duri	ing enrollment							
rol is disabled due to <u>compatibility settings.</u>	 Prompt the user during enrollment and require user input when the private key is used 								
	* Control is disabled du	e to <u>compatibility se</u>	ttings.						
OK Cancel Apply Help	ОК	Cancel	Apply	Help					

ةيكذلا ةقاطبلا

7. 2048 ىلإ حاتفملا مجحل ىندألا دحلا نييعتب مق ،**ريفشتلا** بيوبتلا ةمالع يف

ر**يفشت رفوم** ددح مث ،**نييلاتان نيرفوملا دحأ مدختست نأ بجي تابلطلا** قوف رقنا .أ هدعاقل هيكذلاا هقاطبلا

.**قبطي** ةقطقط .ب

	Prop	perties	of New	/ Template		X
Subject N	Name	Sen	ver	Issuance F	Requirement	s
Supersec	ded Templa	tes	Ext	tensions	Securit	у
Compatibility	General	Request	t Handling Cryptography Key Attestation			
Provider Ca	tegory:	Lega	acy Crypto	ographic Service	Provider	~
Algorithm na	ime:	Dete	ermined by	y CSP		~
Minimum key	y size:	2048	3			
Choose whic	ch cryptogra	aphic prov	riders can	be used for requ	iests	
○ Request:	s can use a	iny provide	er availab	le on the subject	's computer	
Providers:	s must use (one of the	tollowing	providers:		
Microsoft	Base Sma	rt Card Cry	/pto Provi	der	^	ᠿ
Microsoft	DH SChar	nel Crypto	ographic I	Provider vider v 1.0	≡	
Microsoft	Enhanced	DSS and	Diffie-He	llman Cryptograp	hic Pr	
Microsoft	Enhanced	RSA and	AES Cry	ptographic Provid	ler 🗹	♣
Request ha	sh:	Dete	ermined by	y CSP		~
Use alter	nate signat	ure format				
	nato olginat					
Г			_			
L	ОК	(Cancel	Apply	He	lp

ةداەشلا

ليجستلا ىلإ لوصولا قح حنم ديرت يتلا نامألا ةعومجم فضأ ،"نامأ" بيوبتلا ةمالع يف .8 ددحف ،نيمدختسملا عيمج ىلإ لوصولا قح حنم يف بغرت تنك اذإ ،لاثملا ليبس ىلع .اهل .مهل **ليجستلا** تانوذأ ددح مث ،مهيلع قدصملا نيمدختسملا ةعومجم

P	roperties of Nev	v Template	X
• •	iopenties of Nev	v remplate	_
Compatibility Gener	al Request Handling	Cryptography	Key Attestation
Subject Name	Server	Issuance R	equirements
Superseded Terr	nplates Ex	tensions	Security
Group or user names	3:		
& Authenticated	Users		
🤱 Administrator (A	dmin@jajanson.local)		
Section Administration Administratio Administration Administration Administration Administration	(JAJANSON\Domain	Admins)	
Manual Enterprise Admi	ins (JAJANSON\Enter	prise Admins)	
		Add	Remove
Permissions for Auth	enticated Users	Allow	Deny
Full Control			
Read		~	
Write			
Enroll			
Autoenroll			
For special permissio Advanced	ons or advanced settin	gs, click	Advanced
, arenove.			
OH	(Cancel	Apply	Help

ديدجلا بلاقلا رەظي نأ بجي .ديدجلا بلاقلا ءاشناو كتارييغت ءاەنال **قفاوم** قوف رقنا .9 تاداەشلا بلاوق" ةمئاق يف نآلا.

a	Console1 - [C	onsole Root\Certific	ate Templ	lates (2012DC-AD.jajanson.local)]		
🙀 File Action View Favorites Window H	lp					- 8 ×
			Luc 1		_	
Console Root	Template Display Name	Schema Version	Versi	Intended Purposes	-	Actions
Certification Authority (Local)	Code Signing	1	3.1			Certificate Templates (2012DC-AD.jaj 🔺
Certificate Templates (2012DC-AD-Jajanson.io	Computer	1	5.1			More Actions
	Cross Certification Authority	2	105.0			
	Directory Email Replication	2	115.0	Directory Service Email Replication		Smartcard User_VCS
	Domain Controller	1	4.1			More Actions
	Domain Controller Authentication	2	110.0	Client Authentication, Server Authentication, Smart Card Logon		
	EFS Recovery Agent	1	6.1			
	Enrollment Agent	1	4.1			
	Enrollment Agent (Computer)	1	5.1			
	Exchange Enrollment Agent (Offline requ	1	4.1			
	Exchange Signature Only	1	6.1			
	Exchange User	1	7.1			
	@ IPSec	1	8.1			
	IPSec (Offline request)	1	7.1			
	Kerberos Authentication	2	110.0	Client Authentication, Server Authentication, Smart Card Logon, H	D	
	Key Recovery Agent	2	105.0	Key Recovery Agent		
	CCSP Response Signing	3	101.0	OCSP Signing		
	RAS and IAS Server	2	101.0	Client Authentication, Server Authentication	-	
	Root Certification Authority	1	5.1			
	Router (Offline request)	1	4.1			
	Smartcard Logon	1	6.1			
	Smartcard User	1	11.1			
	Smartcard User_VCS	4	101.6	Secure Email, Client Authentication, Smart Card Logon		
	Subordinate Certification Authority	1	5.1			
	I Trust List Signing	1	3.1			
	2 User	1	3.1			
	Ser Signature Only	1	4.1			
	VCS_Login_SMART	2	100.8	Smart Card Logon, Client Authentication		
	Web Server	1	4.1			
	Webclientandserver	2	100.4	Client Authentication, Server Authentication		
	Workstation Authentication	2	101.0	Client Authentication	v	
< III >	<	ш				
36 certificate templates						

لاجملاب مكحتلا يف ەتدەاشم تمت يذلا بلاقلا

عيسوتب مق مث ،(يلحملا) قدصملا عجرملا عيسوتب مق ،MMC نم رسيألاا عزجلا يف 10. قدصملا عجرملا ةمئاق نمض كب صاخلا قدصملا عجرمل.

بلاق قوف رقنا مث **"ديدج"** قوف رقنا مث ،"تاداهشلا بلاوق" قوف نميألا سواملا رزب رقنا اثيدح هؤاشناٍ مت يذلا ةيكذلا ةقاطبلا بلاق رتخأ مث .هرادصإل **قداهشلا**.

ä		C	onsole1 - [Console Roo	t\Certification Authority (Local)\jajanson-2012DC-AD-CA\Certificate Templates]		_ D X
File Action View Favorites	Window Help	þ				- 8 ×
🗢 🔿 🙇 📷 🙆 🖬 🖬	1					
Console Root		Name		Intended Purpose	Actions	
D Certificate Templates		Exchange	Enrollment Agent (Offline r	Certificate Request Agent	Certificate Templates	
A Certification Authority (Local)	0	IPSec (Offi	ine request)	IP security IKE intermediate	Marchatians	
a jajanson-2012DC-AD-CA		Webclient	andserver	Client Authentication, Server Authentic	More Actions	,
Revoked Certificates		Exchange	Signature Only	Secure Email		
Issued Certificates		CEP Encry	ption	Certificate Request Agent		
Pending Requests		Smartcard	User_VCS	Secure Email, Client Authentication, Sm		
Failed Requests		VCS_Login	SMART	Smart Card Logon, Client Authentication		
Certificate Fer	Aanage		Agent	Certificate Request Agent		
			mail Replication	Directory Service Email Replication		
N	vew	,	ontroller Authentication	Client Authentication, Server Authentic		
Vi	fiew	•	uthentication	Client Authentication, Server Authentic		
N	New Window from I	Here	try Agent	File Recovery		
N	Jaw Tacknad View			Encrypting File System		
14	vew raskpau view		ontroller	Client Authentication, Server Authentic		
Re	lefresh		r	Server Authentication		
Ð	oport List			Client Authentication, Server Authentic		
н	ielo			Encrypting File System, Secure Email, Cl		
			e Certification Authority	<all></all>		
		Administra	ator	Microsoft Trust List Signing, Encrypting		

ديدج بلاق رادصإ

عجرملا ةمئاق ددح وأ نميألا سواملا رزب رقنا ،MMC يف ،بلاقلل لثامتملا خسنلا دعب .11 نميألا سواملا رزب رقنا مث .**قمدخلا فاقيا** قوف رقنا مث ،**ماهملا عيمج** قوف رقناو ،قدصملا .**قمدخلا ءدب** قوف رقنا مث ،**ماهملا عيمج** قوف رقناو ،ىرخأ ةرم قدصملا عجرملا مسا قوف



تاداەشلا تامدخ ليغشت ءدب مث فقوتلا

ليجستلا ليكو ةداهش يف ليجستلا

(تامولعملا ةينقت يلوئسم بتكم حطس) ليمع زاهج ىلع كلذب مايقلا نسحتسملا نمو.

.**يب صاخلا مدختسملا باسحل** تاداهش مث **ةفاضإ** قوف رقنا ،**تاداهش** رتخأ MMC ليغشت .1

a		Console1	- [Console Root]			_ 🗆 X
File Action View Favorites Window He	elp					- 8 ×
Console Root	Name				Actions	
		There are no ite	ms to show in this view.		Console Root More Actions	
		Add or R You can select snap-ins for this console from those available or extensible snap-ins; you can configure which extensions are er Available snap-ins; Yendor Active Directory Da Microsoft Cor Active Directory Ste Microsoft Cor Active Directory Ste Microsoft Cor Active Control Microsoft Cor Active Control Microsoft Cor Computer Manager Microsoft Cor Computer Manager Microsoft Cor Description: Description:	emove: Snap-ins your computer and configure the selected set of snap-ins. For abiled. Selected snap-ins: Certificates sna This snap-in will always manage certificates for:	v or pp-in	More Actions	

تاداەش ةڧاضإ

3. **ةداەش بلط** ددح مث **ماەملا ةفاك** ددحو ،**ةيصخشلا ةدقعلا** ددح وأ نميألا سواملا رزب رقنا **قديدج**.



ةديدج تاداهش بلط

3. **يلاتلا** قوف رقنا مث Active Directory ليجست جەن ددح مث ،جلاعملا يف **يلاتلا** قوف رقنا. ىرخأ ةرم.

a	Concola 1 - Concola Doot/Cartificator - Current Ucar/Darconall X	_ 🗆 X
File Action View	Certificate Enrollment	×
Console Root Certificates - Curren Certificates - Curren P Personal P Trusted Root Certificates - Curren D Enterprise Trust D Intermediate Certificates	Select Certificate Enrollment Policy Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.	s Inal A Iore Actions
Active Directory	Configured by your administrator	
Trusted Publishe	Active Directory Enrollment Policy 🗸	
 ▷ □ Untrusted Certifi ▷ □ Third-Party Root ▷ □ Trusted People ▷ □ Client Authentic ▷ □ Certificate Enroll ▷ □ Smart Card Trust ⊿ □ Certification Author ▷ □ jajanson-2012DC 	Configured by you Add New	
< III Personal store contains 9 cer	Next Cancel]

Active Directory ليجست



ليجستلا ةداەش ليكو

حيتي اذهو ،ليجست ةطحمك نآلاا كيدل تامولعملا ةينقت يلوؤسمل بتكملا حطس دادعإ مت نيرخآلا نيمدختسملا نع ةباين ةديدج ةيكذ تاقاطب ليجست كل.

<u>...نع ةباين ليجستلا</u>

ءاشنإو مەليجست بجي ،ةقداصملل ةيكذ تاقاطبب نيفظوملا ديوزت نم نآلا نكمتت يكل ةيكذلا ةقاطبلا ىلإ كلذ دعب اەداريتسإ متي يتلا قداەشلا.



1. داريتساو MMC داريتساو Certificates Module & Manger Certificates for My User Account.

<mark>تايلمعلا < ماەملا ةفاك</mark> ددحو **تاداەش < يصخش** ددح وأ قوف نميألا سواملا رزب رقنا .2 ...<mark>نع ةباينلاب ليجستل</mark>ا قوف رقناو **ةمدقتملا**

3. **يلاتلا** قوف رقنا مث Active Directory ليجست جەن رتخاو ،جلاعملا يف.



<u>مدقتم ةباينلاب ليجستلا</u>

a		Console1 - [Console Root\Certif	icates - Current U	er/Personal/Certific	cates]				= 0 X
File Action View Favorites Window He	P								_ 0 ×
Console Root Console Root Certificates - Consent User Certificates Cer	Issued To	I tourd By jajanean-2012DC-AD-CA jajanean-2012DC-AD-CA ficate Encollment Hore You Begin ar following steps will help you install certific toucks, protect content, establish identsy, fore requesting a certificate, verify the following in tension of the establish identsy.	Expiration Date 10/14/2019 10/12/2018 isates, which are digit and do other sourfly- wing: y-your right to obtain	Intended Pulposes Certificate Repard Microsoft Trust List Al credentials used to cer- related tasks. the certificate	Friendly Nome «None» • None» • O X meet to windex	Status 1	Ceti Enro 1.3.6 Sma Sma Sma	Actions Certificates More Actions	,
Personal store contains 9 certificates.									

4. **يلاتلا** قوف رقنا مث ةداەشلا ليجست جەن ددح.

-		Console1 - [Console Root\Certifica	tes - Current Us	er\Personal\Certifi	cates]				- 🗆 X
Tile Action View Favorites Window Help									_ 8 ×
(+ +) 2 🗊 🗓 🤉 🗳 🖬 🔟									
Console Root Issue	Jed To A	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certi	Actions	
a 💭 Certificates - Current User	Administrator	jajanson-2012DC-AD-CA	10/14/2019	Certificate Request	<none></none>		Enro	Certificates	
Certificates	Administrator Administrator	jajanson-2012DC-AD-CA	10/12/2018	Microsoft Trust List	<none></none>		Adm	More Actions	۲.
Trusted Root Certification Authorities	Administrator				_ _ ×		Enro		
Enterprise Trust Intermediate Certification Authorities	🗔 jajanson-2012 📮 Certificate Enrollment								
Active Directory User Object	PIVKey BD9A5						1.3.6 Sma		
D I Trusted Publishers Si So	Scott Lang S	Select Certificate Enrollment Policy					Sma		
D Third-Party Root Certification Authorities	Scott Lang	Certificate enrollment policy enables enrollment	for certificates base	ed on predefined certific	ate templates.		Sma		
Trusted People	C C	Certificate enrollment policy may already be con	figured for you.						
D Client Authentication Issuers D Certificate Enrollment Requests		Configured by your administrator							
Smart Card Trusted Roots		Active Directory Enrollment Policy			v				
		Configured by you			Add New				
				Next	Cancel				
5							>		
Personal store contains 9 certificates.							141	,	

ليجستلا ةسايس

.اقبسم اەتبلط يتلا ليجستلا ةداەش يە ەذە .**عيقوتلا ةداەش** ديدحت نآلا كنم بلطي .5



عيقوتلا ةداەش ديدحت

يف بغرت يتلاا ةداەشلا ىلا لوصولل ضارعتسالا ىل جاتحت ،ةيلاتلا ةشاشلا يف .6 اقبسم ەتأشنا يذلا بلاقلا وە SmartCard User_VCS ناف ،ةلاحلا ەذە يفو ،اەبلط.

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]								_ 🗆 X	
🖀 File Action View Favorites Window He	lp								- 8 ×
Console Root Certificates Cert	Issued To	lssued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA	Expiration Date 10/14/2019 10/12/2018	Intended Purposes Certificate Request Microsoft Trust List	Friendly Name <none> - X</none>	Status Certi Enro Adm Enro	Certi Enro Adm Enro	Actions Certificates More Actions	
 Enterprise Irust Enterprise Irust Active Directory User Object Trusted Publishers Untrusted Certificates Third-Party Root Certification Authorities Trusted Paople Client Authentication Issuers Client Authentication Requests Smart Card Trusted Roots 	G jajanson-2012 DPIVKey BD9A5 Scott Lang Scott Lang	Certificate Enrollment Request Certificates You can request the following types of certifica click Net. Exchange Enrollment Agent (Offline request) More information is required to enr Exchange Signature Only More information is required to enr © Smartcard User_VCS User Show all templates	Les. Select the certificates and the certificates of the certi	cates you want to reques ole . Click here to configure ole . Click here to configure ole . Next	st, and then Details		1.3.6 Sma Sma Sma		
Personal store contains 9 certificates.	<	ш					>		

VCS ةيكذلا ةقاطبلا رتخاً

7. قوف رقنا .ەنع ةباين ليجستلا يف بغرت يذلا مدختسملا ديدحت ىلإ جاتحت ،كلذ دعب إركان مدختسمل مسا بتكاو **ضارعتس]**،ةلاحلا مدە يف .ليجستلا يف بغرت يذلا فظوملاب صاخلا مدختسملا مسا بتكاو **ضارعتس]** مدختسي غنال توكس 'antman@jajanson.local account'.

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]								_ 🗆 X
File Action View Favorites Window Hel	lp							_ <i>5</i> ×
Console Root Console Root Certificates - Current User Certificates Certificates Certificates Certification Authorities Certification Authorities Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Serificate Authorities Certificates Serificate Authorities Serificate Authorities Serificate Authorities Certificate Authoriti	Issued To	Issued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA Select User Select this object type: User From this location: [siganson local Enter the object name to select (assencing): Scott Lans (antman@asanson local) Advanced	Ехрігаtion Date 10/14/2019 10/12/2018 Обіе Спе ОК	Intended Purposes Certificate Request Microsoft Trust List x t Types ations x n name of ations cancel	Friendly Name <none> of that user. For o be installed is Browse</none>	Status C E S S S S S	Certi Actions Certificates More Actions I.3.6 Imma Imma Imma Imma Imma Imma Imma Imm	
Personal store contains 9 certificates	<u>`</u>							
Personal store contains 9 certificates.								

مدختسملا رايتخإ

8. جاردإب مق ،نآلاا .**لوخدلا ليجست** قوف رقنلاب ليجستلا يف رمتسا ،ةيلاتا ةشاشلا يف .8 كب صاخلا عراقلا يف ةيكذ ةقاطب.



انيودت

9. يلي امك اەنع فشكلا متي ،ةيكذلا ةقاطبلا لاخدا درجمب

Reques	W	indows Security	×	
The enrol	Enrolling for the user Select a smart card device	certificate.		
®¥ak	Axaito O Genuito U The smart o	yptoflex .NET 8 Smart Card Reader 0 ed is ready for use.	Cover	

اي يصخشلا فيرعتلا مقر) ةيكذلا ةقاطبلاب صاخلا PIN مقر ةباتك كلذ دعب كنم بلطي .10 يضارتفالا.

-	Con	sole1 - [Console Root\Certifica	tes - Current Us	er\Personal\Certifi	cates]			_ 🗆 X
Tile Action View Favorites Window He	lp							_ 8 ×
◆ ➡ 2 📷 🛍 🖻 🖶 🖬 🖬								
Console Root Gertificates - Current User Certificates - Current User	Issued To	Issued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA	Expiration Date 10/14/2019 10/12/2018	Intended Purposes Certificate Request Microsoft Trust List	<pre>Friendly Name <none> <none></none></none></pre>	Status C E	Certi Actions Enro Adm Certificates	
Certificates Gertificates Gertificate Certification Authorities Gertificates Gertificates Gertificates Gertificate Certification Authorities Gertificate Certification Authorities Gertificate Certification Authorities Gertificate Certificates Gertif	Certificate Administrato Administrato PIVKey B0AS Scott Lang Scott Lang Scott Lang Scott Lang Scott Lang	Enrollment Enrolling for the user certil Please enter your authentication Pl PlN PlN Click here for mer	vs Security icate. N. einformation	Cancel	Cancel	4 E S S S	More Actions	

PIN زمر لخدأ

ةقاطبلا هذه مادختسإ كلذ دعب كنكمي ،**ليجستلا حاجن** ةشاش ىرت نأ درجمب ،اريخأ .11 فيرعت مقرو طقف ةقاطبلا عم VCS لثم ،لاجملاب لصتم مداخ ىلا لوخدلا ليجستل ةيكذلا تابلط هيجوت ةداعإل VCS دادعإ ىلا ةجاحب تلزام ،معن كلذ متي مل ،كلذ عمو .فورعم يصخش ةقاطبلا ةداهش رادصإل كرتشملا لوصولا ةقاطب مادختساو ةيكذلا ةقاطبلا ىل قنادمارا .

etificate Enrollment		_ 0 X	
ertificate Installation Results			
he following certificates have been env Active Directory Earstment Policy	oiled and initialied on this computer.		
Wakkundig Smartcard User	🖌 STATUS: Succeeded	Details 🛩	
	_		
		iest user Oose	س العجير بتا المت

كرتشملا لوصولا ةقاطبل VCS نيوكت

VCS يف ةقث قدصملا عجرملا تاداهش ةمئاق ىلإ رذجلا قدصملا عجرملا ليمحتب مق **. المثال المثال المثال المثال المثال المثال المثال المثال المثال** المتالي المتالي المتالي المتالي المتالي المتال ال

2. لقتنا VCS ىلإ يسيئرلا قدصملا عجرملا لبق نم ةعقوملا ةداەشلا ءاغلإ ةمئاق ليمحت. قراد**إ < نامألا < ةنايصلا** ىلإ C**RL.**

مسا بحسي يذلا كب صاخلا لجسلا لباقم كب ةصاخلا ليمعلا ةداهش رابتخاب مق .3 متيس .يلحملا مدختسملا وأ LDAP لباقم ةقداصملل اهمادختسال ةداهشلا نم مدختسملا كديرب وأ كب ةصاخلا ةكبشلا هذه نوكت نأ نكمي .ةداهشلا **عوضوم** عم regex ةقباطم بولطملا ينورتكلإلا ديربلا مادختسا مت ،لمعملا اذه يف .كلذ ىلإ ام وأ ينورتكلإلا .

搹 Certificate	\times
General Details Certification Path	
Show: <all></all>	\sim
Field Signature hash algorithm Issuer Valid from	Value ^ sha512 jajanson-2012DC-AD-CA, jaja Tuesday, October 17, 2017 5: Thursday, October 17, 2019 5
Subject Public key Public key parameters Certificate Template Inform	antman@jajanson.local, Scott RSA (1024 Bits) 05 00 Template=1 3 6 1 4 1 311 21
E = antman@jajanson.local CN = Scott Lang OU = Heroes DC = jajanson DC = local	
Ed	it Properties Copy to File
	OK

ليمعلا ةداهش عوضوم

4. بولطملا ليمعلا قدامش ددح .**ليمعلا قدامش رابتخا < نيمأتلا < قنايصلا** ىلإ لقتنا ج**ذامن** مسق يف .رابتخالا ققطنم ىلإ امليمحتب مق ،antman.pem يربتخم يف تناك ،امرابتخإ كب صاخلا regex قصلا **صيخرتلا ققباطمل Regex** تحت **قدامشلا ىل قدنتسملا ققداصملاً** متال لقح ريغةت مقت ال .مرابتخا متيل

CISCO Clsco TelePresence Video Communication Server Expres	soway	This system that if all					
Status System Configuration Applications Users Maintenance							
Client certificate testing		You are here: <u>Mantematics</u> + <u>Security certificates</u>					
Client certificate							
	This tests whether a client certificate is valid when checked against the VCS's current trusted CA list	and, if loaded, the revocation list					
Certificate source	Uploaded test file (PEM format) 📿 🙏	Copicades searching (MSD) formany /					
Belect the file you want to text	Browne No file selected.	Browne. No file selected. I/					
Currently uploaded text file							
Certificate based authentication pattern							
	This section applies only if your certificate contains authentication condentials and you vant to use to the nominated certificants to see if the certificant's condentials (the usemanne) can be scinated.	inficate-based authentication as your client certificate-based security setting. It less you test the outcome of applying regax and username format combinations to					
Regex to match against certificate	dutjact: "emailAddresen("roaptureCommonName=")@jajaneon.localim	<i>u</i>					
Usemanie format	AceptureCommonName#						
	Make these settings permanent						

VCS يف كتبقر ربتخا

Check certificate						
Certificate test results						
Valid certificate:		OK .				
Source: Filename: Test pattern (as entered above):		Uploaded test file (PEM format) antman.pem		regex we are than which is in . Actaan was		
	Regex Template Resulting string (username)	/Subject:nemalAddressn(HosptureCommonNameh:n)@jajanson.localim #captureCommonName# antman		issued the smartcard cer	tificate on his CAC card.	
Stored pattern (current VCS config	ration):				1	
	Regex	/Subject: *CN+(7 <capturecommonname>([*,\])(\.))*)/m</capturecommonname>				
	Template	#captureCommonName#				
	Resulting string (usernar	me) Regex Invalid				
Centopia a para terz	vocuncee	Cert(fright) Detail Tring, 1 (not) Signature A (perting) that Interface Signature A (perting) that Interface (ref Signature A (perting) that Interface (ref) that Int	17:00:00:00:00:00:17 ns:on.0C=1oca1 ca1.0V=fcctt Lang.0V=Hs drfg:19:15:4c-00-41 drfg:19:15:4c-00-41 drfg:19:15:4c-00-41 drfg:19:15:4c-00-41 drfg:19:15:4c-00-41 drfg:19:15:4c-00-41 drfg:19:15:4c-00-41 fc:10:15:4	rres .00-is ten on.00-i oca1	\bigtriangledown	Here we see the uploaded certificate and the current configuration of the regex on the server. Once you have verified that the regex is working then you can permentantly change the Regex. So do not worry that this section shows a failure because this is the current configuration not your test configuration above.

رابتخالا جئاتن

Cisco Expressway-E

Status System Configuration A	pplications Users	Maintenance	
System administration			
Ephemeral port range end			* 49999
Services]		
Serial port / console			0n 🗸 (j)
SSH service			
Web interface (over UTTOC)			
web interface (over h11PS)			
Session limits	1		
Consist time out (minutes)			* 30
Session time out (minutes)			
Per-account session limit			* 0
System session limit			* 0
System protection]		
Automated protection service			On V
Automatic discovery protection			
· · · · · · · · · · · · · · · · · · ·			
Web server configuration			
Redirect HTTP requests to HTTPS	1		
HTTP Strict Transport Security (HSTS)			
Web edministration and			()
web administrator port			
Client certificate-based security			Not required V
Save			Drop down the above box and choose Client-Based Authentication
Related tasks			
Upload a CA certificate file for HTTPS			
Test client certificates			

ليمعلا ىل قدنتسملا ةقداصملا نيكمت

!!!سوبحم انأ !ةدجنلا

،ناك ببس يأل ةداەشلا VCS ضفرو ليمعلا ىلإ ةدنتسملا ةقداصملا نيكمتب تمق اذا بيولل (GUI) ةيموسرلا مدختسملا ةەجاو مادختساب لوخدلا ليجست نم نكمتت نلف نكمي .كماظن ىلإ ةدوعلل ةقيرط دوجو نم قلقت ال ،نكلو .نآلا دعب ةيديلقتلا ةقيرطلاب ةيفيك لوح تامولعم مدقيو بيولا ىلع Cisco عقوم ىلع قفرملا دنتسملا ىلع روثعلا .يرذجلا لوصولا نم ليمعلا ىل ةدنتسملا ةقداصملا ليطعت

ةحصلا نم ققحتلا

نيوكتلا اذه ةحص نم ققحتلل ءارجإ اًيلاح دجوي ال.

اهحالصإو ءاطخألا فاشكتسا

نيوكتلا اذهل اهحالصإو ءاطخألا فاشكتسال ةددحم تامولعم أَيلاح رفوتت ال.

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