Configuratievoorbeeld voor lokale belangrijke certificaten (LSC) met WLC en Windows Server 2012

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Configuratie Microsoft Windows-server De WLC configureren Verifiëren Problemen oplossen

Inleiding

Dit document beschrijft hoe u lokaal belangrijke certificaten (LSC) kunt configureren met een draadloze LAN-controller (WLC) en een nieuw geïnstalleerd Microsoft Windows Server 2012 R2.

Opmerking: Reële implementaties kunnen op veel punten verschillen. U dient volledige controle en kennis te hebben over de instellingen op Microsoft Windows Server 2012. Dit configuratievoorbeeld wordt alleen geleverd als een referentiesjabloon voor Cisco-klanten om hun Microsoft Windows Server-configuratie te implementeren en aan te passen om LSC te laten werken.

Voorwaarden

Vereisten

Cisco raadt u aan elke wijziging te begrijpen die in Microsoft Windows Server is gemaakt en indien nodig de relevante Microsoft documentatie te controleren.

Opmerking: LSC op WLC wordt niet ondersteund met intermediair-CA, omdat de basis-CA wordt gemist vanuit WLC omdat de controller alleen de intermediaire CA krijgt.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

• WLC versie 7.6

Microsoft Windows Server 2012 R2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Configuratie Microsoft Windows-server

Deze configuratie wordt weergegeven zoals uitgevoerd op een nieuw geïnstalleerd Microsoft Windows Server 2012. U moet de stappen aan uw domein en uw configuratie aanpassen.

Stap 1.Installeer de actieve Domeinservices van de Map voor de rollen en eigenschappen wizard.

Before You Begin	Select one or more roles to install on the elected server.	
Installation Type	Roles	Description
Server Selection	Active Directory Certificate Services	Active Directory Domain Services
Server Roles	Active Directory Domain Services	(AD DS) stores information about
Features	Active Directory Federation Services	this information available to users
AD DS	Active Directory Lightweight Directory Services	and network administrators. AD DS
Confirmation	Active Directory Rights Management Services	uses domain controllers to give network users access to permitted
Results	Application Server	= resources anywhere on the networ
	DHCP Server	through a single logon process.
	DNS Server	
	Fax Server	
	File and Storage Services (1 of 12 installed)	
	Hyper-V	
	Network Policy and Access Services	
	Print and Document Services	
	Remote Access	
	Remote Desktop Services	

Stap 2.Na de installatie moet u de server naar de domeincontroller promoten.

a	Add Roles and Features Wizard	
Installation progr	ess	DESTINATION SERVER WIN-ODEF7N1GRUB
Before You Begin	View installation progress	
Installation Type	Feature installation	
Server Selection		I IIII
Server Roles	Configuration required. Installation succeeded on WIN-ODEF7N1GRUB.	
Features	Active Directory Domain Services	^
AD DS	Additional steps are required to make this machine a domain controller.	
Confirmation	Promote this server to a domain controller	
Results	Group Policy Management	
	Remote Server Administration Tools	=
	AD DS and AD LDS Tools	
	Active Directory module for Windows PowerShell	
	AD DS Tools	
	Active Directory Administrative Center	
	AD D3 Shap-ins and Command-Line tools	~
	You can close this wizard without interrupting running tasks. View task pr page again by clicking Notifications in the command bar, and then Task I Export configuration settings	ogress or open this Jetails.
	< Previous Next > Cl	Cancel

Stap 3. Aangezien dit een nieuwe instelling is, kunt u een nieuw bos configureren. maar meestal in bestaande implementaties, moet u deze punten gewoon op een domeincontroller configureren. Hier kiest u het **LSC2012.com-**domein. Hiermee wordt ook de DNS-functie (Domain Name Server) geactiveerd.

Stap 4. Nadat u het programma opnieuw hebt opgestart, installeert u zowel de certificaatdienst (CA) als de webinschrijving.



- -

х

DESTINATION SERVER WIN-ODEF7N1GRUB.LSC2012.com

Before You Begin	Select the role services to install for Active Directory Certifica	ate Services
Installation Type	Role services	Description
Server Selection	Cartification Authority	Certification Authority Web
Server Roles	Certificate Enrollment Policy Web Service	Enrollment provides a simple Web
Features	Certificate Enrollment Web Service	perform tasks such as request and
AD CS	Certification Authority Web Enrollment	renew certificates, retrieve certificate
Role Services	Network Device Enrollment Service	smart card certificates.
Web Server Role (IIS)	Online Responder	
Role Services		
Confirmation		
Results		
	~	
	< <u>Previous</u>	ext > Install Cancel

Stap 5.Configureer ze.

Select role services

à	Add Roles and Features Wizard
Installation progre	DESTINATION SERVER WIN-ODEF7N1GRUB.LSC2012.com
Before You Begin	View installation progress
Installation Type	1 Feature installation
Server Selection	
Server Roles	Configuration required. Installation succeeded on WIN-ODEF7N1GRUB.LSC2012.com.
Features	Active Directory Certificate Services
AD CS	Additional steps are required to configure Active Directory Certificate Services on the
Role Services	destination server
Web Server Role (IIS)	Certification Authority
Role Services	Certification Authority Web Enrollment
Confirmation	Remote Server Administration Tools
Results	Role Administration Tools
	Active Directory Certificate Services Tools
	Certification Authority Management Tools
	Web Server (IIS)
	You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
	Export configuration settings
	< Previous Next > Close Cancel

Stap 6. Kies Enterprise CA en laat alles standaard achter.

a	AD CS Configuration	
Role Services		DESTINATION SERVER WIN-ODEF7N1GRUB.LSC2012.com
Credentials Role Services Setup Type CA Type Private Key	Select Role Services to configure Certification Authority Certification Authority Web Enrollment Online Responder Network Daries Forellment Service]
Cryptography CA Name Validity Period Certificate Database	Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service	
Confirmation Progress Results		
	More about AD CS Server Roles	<u>Configure</u>

Stap 7. Klik op het menu Microsoft Windows/Start.

Stap 8. Klik op Administratieve hulpmiddelen.

Stap 9. Klik op Active Directory Gebruikers en computers.

Stap 10. Vouw het domein uit, klik met de rechtermuisknop op de gebruikersmap en kies Nieuw object > Gebruiker.

3	New Object - User	- D X
File Action View Help ← ➡ 2	Create in: LSC2012.com/Users	
 ▷ Saved Queries ▲ SC2012.com ▷ Builtin ▷ Computers ▷ Domain Controllers ▷ EoreionSecurityPrincipa 	First name: AP Initials: Last name: USER Full name: AP USER	
 Managed Service Accou Users 	User logon name: APUSER @LSC2012.com ✓ User logon name (pre- <u>W</u> indows 2000): LSC2012\ APUSER	
< III >	< Back Next > Cancel Image: Guest User Built-in account for gue Image: Protected Us Security Group Members of this group Image: RAS and IAS Security Group Servers in this group can Image: Read-only D Security Group Members of this group Image: Schema Ad Security Group Designated administrato Image: WinRMRem Security Group Members of this group	

Stap 1. In dit voorbeeld wordt het **APUSER** genoemd. Als deze optie eenmaal is gemaakt, moet u de gebruiker bewerken en op het **tabblad LidOf** klikken, en er een lid van de groep IS_IUSRS van maken

De vereiste gebruikersrechten opdrachten zijn:

- Lokaal loggen toestaan

- Log in als service

Stap 12. Installeer de Inschrijvingsservice voor het netwerkapparaat (NDES).

b	AD CS Configuration	_ _ X
Role Services		DESTINATION SERVER WIN-ODEF7N1GRUB.wlaaan2012.com
Credentials Role Services Service Account for NDES RA Information Cryptography for NDES Confirmation Progress Results	Select Role Services to configure Certification Authority Certification Authority Web Enrollment Conline Responder Certificate Enrollment Veb Service Certificate Enrollment Policy Web Service	
	< <u>P</u> revious <u>N</u> e	ext > Configure Cancel

• Kies het rekeninglid van de groep IS_USRS, **APUSER** in dit voorbeeld, als de servicekening voor NDES.

Stap 13. Navigeer naar administratieve hulpmiddelen.

Stap 14. Klik op Internet Information Services (IS).

Stap 15. Uitbreidt de server > Sites > Standaardwebsite > Cert Srv.

Stap 16. Klik voor zowel **mscep** als **mscep_admin** op **verificatie**. Zorg ervoor dat anonieme verificatie is ingeschakeld.

Stap 17. Klik met de rechtermuisknop op **Windows-verificatie** en kies **providers**. Zorg ervoor dat NT LAN Manager (NTLM) eerst in de lijst staat.

Stap 18. Schakel de authenticatie-uitdaging uit in de registerinstellingen, anders verwacht Simple certificaatinschrijving Protocol (SCEP) dat de WLC-versie niet ondersteunt.

Stap 19. Open de toepassing.

Stap 20. Ga naar HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\.

Stap 21. Stel het wachtwoord in op 0.

đ					Re	gistry Editor		
File	Edit	View	Favorites H	elp				
		Þ-4	💧 Advanced II	NF 🔼	Name	Туре	Data	
		Þ-1	🔓 ALG		ab (Default)	REG_SZ	(value not set)	
			💧 AllUserinsta	IIA	認 EnforcePassword	REG_DWORD	0x00000000 (0)	
		Þ-4	Assistance					
		Þ-1	🔓 AuthHost	≡				
		Þ-1	BestPractice	s				
		Þ-4	BidInterface					
		Þ-	🔓 Chkdsk					
		Þ-	COM3					
			Command	Prc		•		
		4-	Cryptograp	י אי		6		
			🔈 - 🏭 AutoEnr	oll				
			🗅 - 鷆 Calais					
			📔 Catalog	DB				
			🔒 CatDBT	m				
			🗅 - 🎽 Certifica	te				
			👂 - 🎽 Defaults					
			A 🏭 MSCEP					
			CAT	/p				
			🎍 Cert	iln				
			🏄 Enfo	rce				
			🕌 Pass	wo				
			Uses	ing				
<				>				
Comp	outer\H	IKEY_LO	CAL_MACHIN	E\SOF	TWARE\Microsoft\Cryp	tography\MSCEP	\EnforcePassword	Activate Wind

Stap 2. Klik op het menu Microsoft Windows/Start.

Stap 23. Type MMC.

Stap 2. Kies in het menu Bestand de optie Magnetisch toevoegen/verwijderen. Kies certificeringsinstantie.

Stap 25. Klik met de rechtermuisknop op de map certificaatsjabloon en klik op beheren.

Stap 2. Klik met de rechtermuisknop op een bestaande sjabloon zoals Gebruiker en kies **Dubbele** sjabloon.

File Action View Help				
🏟 📅 📰 🗟 🚺				
Certificate Templates (WIN-ODE	Template Display Name	Schema Version	Versi	Intended Purp
	CA Exchange	2	106.0	Private Key Arc
	CEP Encryption	1	4.1	
	🗵 Code Signing	1	3.1	_
	Computer	1	5.1	
	Cross Certification Authority	2	105.0	
	Directory Email Replication	2	115.0	Directory Servi
	Domain Controller	1	4.1	
	Domain Controller Authentication	2	110.0	Client Authent
	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 Authent
	Key Recovery Agent	2	105.0	Key Recovery A
	OCSP Response Signing	3	101.0	OCSP Signing
	RAS and IAS Server	2	101.0	Client Authent
	Root Certification Authority	1	5.1	
	Router (Offline request)	1	4.1	
	🗟 Smartcard Logon	1	6.1	
	🚇 Smartcard User	1	11.1	
	Subordinate Certification Authority	1	5.1	
	Trust List Signing	1	3.1	
	🚇 User	1	3.1	
	User Signative Only	1	4.1	
	B Web Server	1	4.1	Activat
	Workstation Authentication	2	101.0	Client Authent

Stap 27. Kies de CA om Microsoft Windows 2012 R2 te zijn.

Stap 28. Voeg in het tabblad Algemeen een weergavenaam toe, zoals WLC, en een validatieperiode.

Stap 29. Bevestig in het tabblad Onderwerp dat Levering in het verzoek is geselecteerd.

Prop	oerties (of New	Template		x	
Superseded Templat	tes	Exte	ensions	Security		
Compatibility General	Request	Handling	Cryptograph	y Key Attesta	tion	
Subject Name Server Issuance Requirements						
Supply in the request	•					
- Use subject infer	nation for	m aviation	oortificantee fe	r autoonrallmoot		
renewal requests	mation no s	m existing	centificates to	rautoenroliment		
O Build from this Active	Directory	informatio	n			
Select this option to e	nforce co	nsistency	among subjec	t names and to		
simplify certificate add	ninistratior	1.				
Subject name format:						
None				~		
<u>I</u> nclude e-mail nan	ne in subje	ect name				
Include this informatio	n in alterr	nate subje	ct name:			
E-mail name		-				
DNS name						
User principal nam	ne (UPN)					
Service principal r	name (SPI	(V		Ν		
				4		
					-	
ОК	(Cancel	Apply	Help		

Stap 30. Klik op het tabblad **Eisen** voor **uitgifte**. Cisco raadt aan om uitgiftebeleid leeg te laten in een typische hiërarchische CA-omgeving:

Supersec	Superseded Templates Extensions Security				Security
Compatibility	General	Request	Handling	Cryptograph	y Key Attestation
Subject N	Subject Name Server Issuance Requirements				Requirements
Require the following for enrollment:					
	ber of auth	onzea sigr	atures:	0	
lf you re	quire more	than one s	signature, a	autoenrollment	t is not allowed.
Policy ty	pe required	in signatu	ire:		
					~
Applicati	on policy:				
					~
l <u>s</u> suance	e policies:				
					A <u>d</u> d
					<u>R</u> emove
Require the	following fo	r reenrollm	ent:		
Same crit	teria as for (enrollment			
○ Valid <u>e</u> xis	ting certific	ate			
Allow	<u>k</u> ey based	renewal			
Requires subject information to be provided within the certificate request.					
[ОК	(Cancel	Apply	Help

Stap 3 1. Klik op het **tabblad Uitbreidingen**, **Toepassingsbeleid** en **Bewerk**. Klik op **Add** en controleer of clientverificatie wordt toegevoegd als toepassingsbeleid. Klik op **OK**.

An application policy defines how a certificate can be used.
Application policies: Client Authentication Encrypting File System Secure Email
Add Edit Remove Make this extension critical
OK Cancel

Stap 3 2. Klik op het **tabblad Beveiliging** en vervolgens op **Toevoegen...** Zorg ervoor dat de SCEP-servicekaart die in de NDES-servicesinstallatie is gedefinieerd, de volledige controle over de sjabloon heeft en klik op **OK**.

Subject N	lame	Sen	ver	Issuance	e Requirements	
Compatibility	General	Request	Handling	Cryptography Key Attestat		
Supersec	ded Templa	tes	Exte	ensions	Security	
<u>G</u> roup or use	rnames:					
& Authen	ticated Use	rs				
🔏 Adminis	trator					
👗 AP US	ER (APUSE	R@LSC2	012.com)			
👫 Domain	Admins (L	SC2012\D)omain Ad	mins)		
👫 Domain	Users (LS	C2012\Do	main User	rs)		
🔏 Enterpri	ise Admins	(LSC2012	\Enterpris	e Admins)		
					8	
			Sum	A <u>d</u> d	<u>R</u> emove	

Stap 3. Ga terug naar de GUI-interface van de certificeringsinstantie. Klik met de rechtermuisknop op de **map certificaatsjablonen**. Navigeer naar **Nieuw > certificaatsjabloon om uit te geven**. Selecteer de eerder ingesteld WLC-sjabloon en klik op **OK**.

· ··· · ···		p		- 1-
(= 🔿 🖄				-
sole Root	•	Enable Certificate Templates	x	<u> </u>
Certification A Wlaaan201 Certification A Revoku Ssued Ssued	Select one Certificate Template to Note: If a certificate template that information about this template has All of the certificate templates in th For more information, see <u>Cer</u>	enable on this Certification Authority. was recently created does not appear on this list, you may new s been replicated to all domain controllers. e organization may not be available to your CA. tificate Template Concepts.	ed to wait until	Tem tions
🣔 Failed	Name	Intended Purpose	^	
Certifi	Key Recovery Agent OCSP Response Signing RAS and IAS Server Router (Offline request) Smartcard Logon Smartcard User Trust List Signing	Key Recovery Agent OCSP Signing Client Authentication, Server Authentication Client Authentication Client Authentication, Smart Card Logon Secure Email, Client Authentication, Smart Card Logon Microsoft Trust List Signing	_	
	W User Signature Only	Client Authentication Secure Email, Encrypting File System	×	
		ОК	Cancel	
<		III	>	_

Stap 34. Verander de standaard SCEP-sjabloon in de registratiesystemen onder **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptografie > MSCEP**. Verander de toetsen EncryptionSjabloon, GeneralPurposeSjabloon en SignatureSjabloon van IPsec (Offline aanvraag) naar de eerder gemaakte WLC-sjabloon.

đ						Re	egistry Edi	itor			-		×
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	F <u>a</u> vorites	<u>H</u> elp									
		Þ-	📗 Advance	ed INF 🛧	Nan	ne	Туре		Data				
		Þ-	📗 ALG		e 🗎 🧶	Default)	REG_SZ		(value not set)				
			📗 AllUserir	nstallA	e 🔊 E	ncryptionTem	REG_SZ		WLC				
		Þ-	Assistan	ce) 🔔 (GeneralPurpose	REG_SZ		WLC				
		Þ-	AuthHos	st ≣	at s	SignatureTemplat	e REG_SZ		WLC				
		Þ-	BestPrace	tices	- 11	13							
		Þ-	BidInterf	ace									
		Þ-	Chkdsk										
		P -		ad Dra									
		1	Auto	Enroll									
			Calai	is									
			Cata	loaDB									
			CatD	BTem									
			- 🚺 Certi	ficate									
			b - 🚺 Defa	ults									
			🖌 🚺 MSC	EP									
			🔒 C	АТур									
				CertsIn									
			}E	inforce									
]] P	asswo									
			j	JseSing 🗸									
<				>	1								
Comp	outer\H	IKEY_L	OCAL_MAC	HINE\SO	FTWAR	E\Microsoft\Cryp	tography\N	ISCEP		A	tivat	o Wi	indi

Stap 35. Herstart het systeem.

De WLC configureren

Stap 1. Navigeer in het menu Beveiliging op de WLC. Klik op Certificaten > LSC.

Stap 2. Controleer het selectieknop LSC inschakelen op controller.

Stap 3. Voer uw Microsoft Windows Server 2012 URL in. Standaard wordt deze toegevoegd aan /certsrv/mscep/mscep.dll.

Stap 4. Voer uw gegevens in het gedeelte Params in.

Stap 5. Pas de wijziging toe.

Local Significant Certificates (LSC)

General AP Provisioning	
Certificate Type	Status
CA	Present
General	
Enable LSC on Controller	
CA Server	
CA server URL	http://10.48.39.197/certsrv/mscep/mscep.dll (Ex: http://10.0.0.1:8080/caserver)
Params	
Country Code	BE
State	Belgium
City	Brussel
Organization	Cisco
Department	R&D
E-mail	rmanchur@wlaaan.com
Key Size	2048

Stap 6. Klik op de blauwe pijl op de bovenste CA-lijn en kies **Add**. Het moet de status veranderen van **niet aanwezig** naar **nu**.

Stap 7. Klik op het tabblad AP-provisioning.

cisco	MONITOR	<u>w</u> lans	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	
Security	Local Sig	nificant	Certificates (LSC)						
 AAA General RADIUS Authentication Accounting Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies P Policies Password Policies Local EAP Priority Order Certificate LSC SSC Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP Advanced 	General AP Provis Enable Update Numbe AP Ethern	AP Pr sioning	ts to LSC (0 to 25	5) 3						

Stap 8.Controleer het selectieteken Enable onder AP Provisioning en klik op Update.

Stap 9.Herstart uw toegangspunten als ze niet zelf zijn herstart.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het toegangspunt, na het opnieuw opstarten, sluit zich aan bij en toont met LSC als het certificaattype in het menu Draadloos.

CISCO	MONETOR WLANS	CONTROLLER WIRELES	s Security May	NAGENERT COMMANDS	HELP FEEDBA	ск			
Wireless	All APs							Ent	ries 1 - 2 of 2
Access Points Al: APs Radice R02.118/n R02.118/n Dual-Band Radice	Current Filter Number of APa	lia 2		(Charge Fiber) (Clear Fiber	1				
Global Configuration	AP Name	AP Nodel	AP P	AC AP Up T	ine A	Operat Idmin Status Status	Ional Port	AP Node	Certificate
Mesh RF Profiles FlexConnect Groups	CAP35011-1 LAP1142-1	AIR-CAPISOLI-E AIR-LAP1142N-1	-K9 c8:94 -K9 ac:12	c:1d:6e:a3:cd 0 d, 00 h 1:c5:73:33:ce 0 d, 00 h	35 m 21 s D 02 m 35 s E	Inabled REG Inabled REG	1	Local	LSC LSC
▶ 802.11a/n									
▶ 802.11b/g/n									
Media Stream									
Application Visibility And Control									
Country									
Timers									
Netflow									
▶ QoS	< .								~
			110						

Opmerking: Na 8.3.112 kunnen MIC APs zich niet bij allen aansluiten wanneer LSC wordt ingeschakeld. Daarom wordt de optie "pogingen tot LSC" tellen beperkt gebruikt.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.