# Exemple de configuration de certificats d'importance locale (LSC) avec WLC et Windows Server 2012

## Contenu

Introduction Conditions préalables Conditions requises Components Used Configuration Configuration de Microsoft Windows Server Configurer le WLC Vérification Dépannage

### Introduction

Ce document décrit comment configurer des certificats d'importance locale (LSC) avec un contrôleur de réseau local sans fil (WLC) et un Microsoft Windows Server 2012 R2 récemment installé.

**Note**: Les déploiements réels peuvent différer sur plusieurs points et vous devez avoir un contrôle et une connaissance complets des paramètres de Microsoft Windows Server 2012. Cet exemple de configuration n'est fourni qu'en tant que modèle de référence permettant aux clients Cisco de mettre en oeuvre et d'adapter leur configuration Microsoft Windows Server afin de faire fonctionner LSC.

### Conditions préalables

#### **Conditions requises**

Cisco vous recommande de comprendre toutes les modifications apportées à Microsoft Windows Server et de consulter la documentation Microsoft appropriée si nécessaire.

**Note**: LSC sur WLC n'est pas pris en charge avec l'autorité de certification intermédiaire, car l'autorité de certification racine sera manquée du WLC puisque le contrôleur obtient seulement l'autorité de certification intermédiaire.

#### **Components Used**

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC version 7.6
- Microsoft Windows Server 2012 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Configuration

#### Configuration de Microsoft Windows Server

Cette configuration s'affiche comme effectuée sur un Microsoft Windows Server 2012 récemment installé. Vous devez adapter les étapes à votre domaine et à votre configuration.

Étape 1. Installer les services de domaine Active Directory pour l'Assistant Fonctions et rôles.

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 objects on the network and maker
Features	Active Directory Federation Services	this information available to users
AD DS	Active Directory Lightweight Directory Services	and network administrators. AD D
Confirmation	Active Directory Rights Management Services	network users access to permitted
lesults	Application Server	resources anywhere on the network
	DHCP Server	<ul> <li>through a single logon process.</li> </ul>
	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	

Étape 2. Après l'installation, vous devez promouvoir le serveur au contrôleur de domaine.

<b>i</b>	Add Roles and Features Wizard	- 0 ×
Installation progr	ess	DESTINATION SERVER WIN-ODEF7N1GRUB
Before You Begin	View installation progress	
Installation Type	Feature installation	
Server Selection Server Roles	Configuration required. Installation succeeded on WIN-ODEF7N1GRUB.	
Features	Active Directory Domain Services 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	
	Role Administration Tools	=
	Active Directory module for Windows PowerShell	
	AD DS Tools	
	AD DS Snap-Ins and Command-Line Tools	~
	You can close this wizard without interrupting running tasks. View task pripage again by clicking Notifications in the command bar, and then Task D Export configuration settings	ogress or open this letails.
	< <u>P</u> revious <u>N</u> ext > Cl	Cancel

**Étape 3.** Comme il s'agit d'une nouvelle configuration, vous configurez une nouvelle forêt ; mais généralement dans les déploiements existants, il suffit de configurer ces points sur un contrôleur de domaine. Choisissez ici le domaine **LSC2012.com**. Ceci active également la fonctionnalité DNS (Domain Name Server).

**Étape 4.** Après un redémarrage, installez le service Autorité de certification (CA) ainsi que l'inscription Web.



- -

х

DESTINATION SERVER WIN-ODEF7N1GRUB.LSC2012.com

Installation Type	Role services	Description
Server Selection Server Roles Features AD CS Role Services Web Server Role (IIS) Role Services Confirmation Results	<ul> <li>Certification Authority</li> <li>Certificate Enrollment Policy Web Service</li> <li>Certificate Enrollment Web Service</li> <li>Certification Authority Web Enrollment</li> <li>Network Device Enrollment Service</li> <li>Online Responder</li> </ul>	Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.
	R	
	< <u>P</u> revious No.	ext > Install Cancel

Étape 5.Configurez-les.

Select role services

à	Add Roles and Features Wizard	- • ×
Installation progre	SS DESTINA WIN-ODEF7N1GRUE	TION SERVER
Before You Begin	View installation progress	
Installation Type	Feature installation	
Server Selection		
Server Roles	Configuration required. Installation succeeded on WIN-ODEF7N1GRUB.LSC2012.com	n.
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)	Configure Active Directory Certificate Services on the destination server	
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

Étape 6. Choisissez Entreprise CA et laissez tout comme valeur par défaut.

<b>b</b>	AD CS Configuration	
Role Services		DESTINATION SERVER WIN-ODEF7N1GRUB.LSC2012.com
Credentials Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Select Role Services to configure	
	More about AD CS Server Roles	> Configure Cancel

Étape 7. Cliquez sur le menu Microsoft Windows/Démarrer.

Étape 8. Cliquez sur Outils d'administration.

Étape 9. Cliquez sur Utilisateurs et ordinateurs Active Directory.

Étape 10. Développez le domaine, cliquez avec le bouton droit sur le dossier Utilisateurs, puis choisissez Nouveau objet > Utilisateur.

	New Object - User	X
File Action View Help	Create in: LSC2012.com/Users	
<ul> <li>▷ Saved Queries</li> <li>▲ ∰ LSC2012.com</li> <li>▷ 📫 Builtin</li> <li>▷ 📫 Computers</li> </ul>	Erst name: AP Initials:	
<ul> <li>Domain Controllers</li> <li>ForeignSecurityPrincipa</li> <li>Managed Service Account</li> </ul>	Full name: AP USER	
🖺 Users	APUSER @LSC2012.com V User logon name (pre- <u>W</u> indows 2000):	
l	<u>Reack</u> <u>Next</u> > <u>Cancel</u> Cancel     Guest   User     Built-in account for gue	
	Security Group       Members of this group         RAS and IAS       Security Group         Read-only D       Security Group         Members of this group can         Read-only D         Security Group	
< III >	Schema Ad Security Group Designated administrato WinRMRem Security Group Members of this group	

Étape 11. Dans cet exemple, il est nommé APUSER. Une fois créé, vous devez modifier l'utilisateur et cliquer sur l'onglet MemberOf, puis en faire un membre du groupe IIS\_IUSRS.

Les affectations de droits d'utilisateur requises sont les suivantes :

- Autoriser la connexion localement
- Se connecter en tant que service

Étape 12. Installez le service NDES (Network Device Enrollment Service).

<b>b</b>	AD CS Configuration	- <b>-</b> ×
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

• Choisissez le membre de compte du groupe IIS\_USRS, **APUSER** dans cet exemple, comme compte de service pour NDES.

Étape 13. Accédez à Outils d'administration.

Étape 14. Cliquez sur IIS (Internet Information Services).

Étape 15. Développez Serveur > Sites > Site Web par défaut > Cert Srv.

Étape 16. Pour mscep et mscep\_admin, cliquez sur authentication. Assurez-vous que l'authentification anonyme est activée.

**Étape 17.** Cliquez avec le bouton droit sur **authentification Windows** et choisissez **Fournisseurs**. Assurez-vous que NT LAN Manager (NTLM) figure en premier dans la liste.

**Étape 18.** Désactivez le défi d'authentification dans les paramètres du Registre, sinon le protocole SCEP (Simple Certificate Enrollment Protocol) attend l'authentification par mot de passe de défi,

qui n'est pas pris en charge par le WLC.

Étape 19. Ouvrez l'application regedit.

Étape 20. Accédez à HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\.

Étape 21. Définissez EnforcePassword sur 0.

đ			Re	gistry Editor		
File	Edit	View Favorites Help				
		👂 - 🎳 Advanced INF 🔨	Name	Туре	Data	
		🔉 - 퉲 ALG	ab) (Default)	REG_SZ	(value not set)	
		🔒 AllUserinstallA	EnforcePassword	REG_DWORD	0x00000000 (0)	
		👂 🍌 Assistance 🦳				
		⊳- 🎍 AuthHost 🛛 😑				
		BestPractices				
		👂 퉬 BidInterface 🦳				
		þ- 🍌 Chkdsk				
		р - 🍌 СОМЗ				
		Command Prc		N		
		4 🎳 Cryptography		13		
		AutoEnroll				
		D - 🎽 Calais				
		CatalogDB				
		CatDBTem				
		Defaults				
		Catype				
		Decours				
<	1					
Comp	uter\H	KEY_LOCAL_MACHINE\SOF	TWARE\Microsoft\Cryp	tography\MSCEP\	EnforcePassword	ctivate Wind

Étape 22. Cliquez sur le menu Microsoft Windows/Démarrer.

Étape 23. Tapez MMC.

Étape 24. Dans le menu Fichier, sélectionnez Ajouter/Supprimer un composant logiciel enfichable. Sélectionnez Autorité de certification.

Étape 25. Cliquez avec le bouton droit sur le dossier Modèle de certificat et cliquez sur Gérer.

**Étape 26.** Cliquez avec le bouton droit sur un modèle existant, tel que Utilisateur, et choisissez **Modèle en double**.

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 Signat 👷 Only	1	4.1	
	Reb Server	1	4.1	Activat
	Workstation Authentication	2	101.0	Client Authent 🛶

Étape 27. Choisissez l'autorité de certification Microsoft Windows 2012 R2.

Étape 28. Dans l'onglet Général, ajoutez un nom d'affichage tel que WLC et une période de validité.

Étape 29. Dans l'onglet Nom du sujet, vérifiez que Approvisionnement dans la demande est sélectionné.

Prop	perties	of New	Template		x
Superseded Templa	tes	Ext	ensions	Security	
Compatibility General	Request	Request Handling Cryptography Key Attest			
Subject Name	Sen	ver	Issuance	Requirements	
Supply in the request	+				
_ il les subject infe	mation for	m evieties	. aatifiaataa fa		
renewal request	s	in existing	centificates for	autoeniroiimen	
○ <u>B</u> uild from this Active Select this option to e	e Directory enforce co	informationsistency	on among subject	names and to	
Subject name format	ninistratior :	1.			
None				~	
Include e-mail nar	me in subie	ect name			
Include this information	on in alterr	nate subje	ct name:		
Uses ariseis al any					
<u>U</u> ser principal nar	ILE (UFIN)	un l			
	name (SPI	N)		6	
OK	(	Cancel	Apply	Help	

Étape 30. Cliquez sur l'onglet Conditions d'émission. Cisco recommande de laisser les stratégies d'émission vides dans un environnement CA hiérarchique typique :

Supersec	Superseded Templates		Exte	Extensions Security	
Compatibility	General	Request	Handling	Cryptograph	y Key Attestation
Subject N	Subject Name Server Issuance Requirements				Requirements
Require the following for enrollment:					
lf you re	quire more	than one	signature, a	autoenrollment	is not allowed.
Policy ty	pe required	in signati	ire:		
Applicati	an naliau				Y
Applicati	on policy.				~
l <u>s</u> suance	e policies:				
					A <u>d</u> d
					<u>R</u> emove
Require the f	following fo	r reenrollm	ent:		
Same crit	teria as for (	enrollment			
⊖ Valid <u>e</u> xis	ting certific	ate			
Allow	key based	renewal			
Requires request.	subject inf	omation t	o be provid	led within the	certificate
[	ОК	(	Cancel	<u>A</u> pply	Help

Étape 31. Cliquez sur l'onglet Extensions, Stratégies d'application, puis Modifier. Cliquez sur Add, et assurez-vous que l'authentification du client est ajoutée en tant que stratégie d'application. Click 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

Étape 32. Cliquez sur l'onglet Sécurité, puis sur Ajouter.... Assurez-vous que le compte de service SCEP défini dans l'installation du service NDES contrôle entièrement le modèle, puis cliquez sur OK.

Subject Name		Server		Issuance	e Requirements			
Compatibility	General	Request	Handling	Cryptograph	y Key Attestation			
Supersec	led Templa	tes	Exte	ensions	Security			
<u>G</u> roup or use	rnames:							
& Authent	ticated Use	rs						
🔏 Adminis	trator							
🔏 AP USE	ER (APUSE	R@LSC2	012.com)					
👫 Domain	Admins (L	SC2012\D	omain Ad	mins)				
👫 Domain	Users (LS	C2012\Do	main User	rs)				
👫 Enterpri	se Admins	(LSC2012	\Enterpris	e Admins)				
$\searrow$								
Add <u>R</u> emove								

Étape 33. Revenez à l'interface graphique de l'autorité de certification. Cliquez avec le bouton droit de la souris sur le répertoire Certificate Templates. Accédez à Nouveau > Modèle de certificat à émettre. Sélectionnez le modèle WLC configuré précédemment, puis cliquez sur OK.

	on nen rarones million			
(= => 🖄	🖬 🛕 📑 🖪			_
sole Root	•	Enable Certificate Templates	x	<u> </u>
Certification A Welaaan201 Revoku Ssued Pendir	Select one Certificate Template to Note: If a certificate template that information about this template has All of the certificate templates in to For more information, see <u>Ce</u>	o enable on this Certification Authority. t was recently created does not appear on this list, you may ne as been replicated to all domain controllers. the organization may not be available to your CA. artificate Template Concepts.	ed to wait until	Tem tions
Failed Certific	Name Rev Recovery Agent	Intended Purpose Key Recovery Agent	^	
	R OCSP Response Signing	OCSP Signing		
	RAS and IAS Server	Client Authentication, Server Authentication		
	Router (Offline request)	Client Authentication		
	Smartcard User	Secure Email, Client Authentication, Smart Card Logon		
	Trust List Signing	Microsoft Trust List Signing		
	R User Signature Only	Secure Email, Client Authentication	=	
	WLC	Client Authentication, Secure Email, Encrypting File System		
	Workstation Authentication	Client Authentication 1%	~	
		ОК	Cancel	
٢	III > <	III	>	

Étape 34. Modifiez le modèle SCEP par défaut dans les paramètres de Registre sous Ordinateur > HKEY\_LOCAL\_MACHINE > LOGICIEL > Microsoft > Cryptographie > MSCEP. Modifiez les clés EncryptionTemplate, GeneralPurposeTemplate et SignatureTemplate d'IPsec (Offline Request) au modèle WLC précédemment créé.

Ø						Re	egistry Edi	tor		X
<u>F</u> ile	Edit	<u>V</u> iew	F <u>a</u> vorite	s <u>H</u> elp	•					
		Þ-(	📔 Advan	ced INF	^	Name	Туре	Data		
		Þ-	ALG			赴 (Default)	REG_SZ	(value not s	set)	
			AllUse	rinstallA		EncryptionTem	REG_SZ	WLC		
		Þ-	Assista	ince		💩 GeneralPurpose	REG_SZ	WLC		
		Þ-	📙 AuthH	ost	≡	Signature Template	REG_SZ	WLC		
		₽- <u> </u>	BestPr	actices		- R				
		Þ-	BidInte	erface						
		Þ-	Chkds	ĸ						
		₽- <b> </b>	COM3							
			Comm	land Pro						
		4-	Crypto	graphy						
				toEnroll	1					
				idis taleeDE						
				+DRT arr						
			Ce	rtificate						
			b - De	faults						
			MS MS	CEP						
			T]]	CATyp						
				CertsIn						
				Enforce						
				Passwo						
			L	UseSin	<u> </u>					
<					<b>–</b>					
Com	outer) H				SOF	TWARE\Microsoft\Cove	tography\M	SCEP		A 12 1 147 1
com	aren (i		CHC_MM		301	t the (microsoft (cryp	in dial and in the second			Activate Wind

Étape 35. Redémarrez le système.

#### **Configurer le WLC**

Étape 1. Sur le WLC, accédez au menu Sécurité. Cliquez sur Certificats > LSC.

Étape 2. Cochez la case Activer LSC sur le contrôleur.

Étape 3. Saisissez votre URL Microsoft Windows Server 2012. Par défaut, il est ajouté à /certsrv/mscep/mscep.dll.

Étape 4. Entrez vos détails dans la section Params.

Étape 5. Appliquer la modification.

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				

Apply

Étape 6.Cliquez sur la flèche bleue sur la ligne CA supérieure et choisissez Ajouter. Il doit changer le statut de Non présent à présent.

Étape 7. Cliquez sur l'onglet Approvisionnement AP.

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

Étape 8. Cochez la case Activer sous Approvisionnement AP et cliquez sur Mettre à jour.

Étape 9. Redémarrez vos points d'accès s'ils n'ont pas redémarré eux-mêmes.

### Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Le point d'accès, après le redémarrage, se reconnecte et s'affiche avec LSC comme type de certificat dans le menu Wireless.

CISCO	MONITOR WLANS	CONTROLLER WIRELESS SECU	URITY MANAGEMENT CO	MMANDS HELP	EEEDBACK			
Wireless	All APs						Entries	1-2012
Access Points     All APs     Redice     R02.tis/n     S02.tis/n     Dual-Band Radies     Construction	Current Filter Number of APa	lkone 2	(Charlos Filter)	Clear Filter)				
Global Configuration	AP Name	AP Nodel	AP HAC	AP Up Time	Admin Status	Operational Status Port	AP Mode	Certificate Type
Mesh	CAP15011-1	AIR-CAP35011-8-K9	c8:9c:id:6e:a3:cd	0 d, 00 h 35 m 21 s	Disabled	R0G 1	Local	LSC
RF Profiles	LAP1142-1	AIR-LAP1142N-1-K9	ac:12:c5:73:33:ce	0 d, 00 h 02 m 35 s	Enabled	R6G 1	Local	LSC
RF Profiles FlexConnect Groups FlexConnect ACLS B02.11a/n B02.11b/g/n Media Stream Application Visibility And Control Country Timers Netflow Q05	LAPILAZ-1	AIR-LAP1142N-1-K9	ac:12:c5:73:33:ce	_ 0 d, 00 h 02 m 35 s	i Enabled	REG 1	Local	LSC
	<		111 <b></b> 11	1			516	>
	2		🛛 🚺 🙀			- 10	( 😼 🕼 - uk	12/16/2014

**Note**: Après la version 8.3.112, les points d'accès MIC ne peuvent pas se joindre du tout une fois que LSC est activé. Par conséquent, la fonction de comptage « tentatives de LSC » devient d'usage limité.

# Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.