# 使用WLC和Windows Server 2012的本地重要證 書(LSC)配置示例

### 目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>設定</u> <u>Microsoft Windows Server配置</u> <u>設定WLC</u> <u>驗證</u> 疑難排解

## 簡介

本文說明如何使用無線LAN控制器(WLC)和新安裝的Microsoft Windows Server 2012 R2設定本機重 要憑證(LSC)。

**附註**:實際部署在很多方面可能有所不同,您應該對Microsoft Windows Server 2012上的設 定擁有完全的控制和知識。此配置示例僅作為思科客戶實施並調整其Microsoft Windows Server配置以使LSC正常工作的參考模板提供。

## 必要條件

#### 需求

思科建議您瞭解Microsoft Windows Server中的每一項更改,如果需要,請檢視相關Microsoft文檔 。

**附註**:中間CA不支援WLC上的LSC,因為控制器僅取得中間CA,WLC會遺失根CA。

#### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

•WLC版本7.6

Microsoft Windows Server 2012 R2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

設定

#### Microsoft Windows Server配置

此配置顯示為在新安裝的Microsoft Windows Server 2012上執行。您必須根據您的域和配置調整步驟。

步驟1.為角色和功能嚮導安裝Active Directory域服務。

Before You Begin	Select one or more roles to install on the elected server.		
Installation Type	Roles		Description
Server Selection	Active Directory Cartificate 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		

< Previous

<u>N</u>ext >

Install

Cancel

**步驟2.安**裝後,必須將伺服器升級為域控制器。

<b>a</b>	Add Roles and Features Wizard	
Installation progre	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	^
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 DS Shap-Ins and Command-Line Tools	×
	You can close this wizard without interrupting running tasks. View task propage again by clicking Notifications in the command bar, and then Task D Export configuration settings	ogress or open this Netails.
	< <u>P</u> revious <u>N</u> ext > Cla	Ose Cancel

**步驟3.**由於這是新設定,因此請配置新的林;但在現有部署中,通常只需在域控制器上配置這些點 即可。在這裡,您選擇LSC2012.com域。這也會啟用域名伺服器(DNS)功能。

步驟4.重新開機後,安裝憑證授權單位(CA)服務和Web註冊。

\_ 0 X

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 Server Roles Features AD CS Role Services Web Server Role (IIS) Role Services	<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.		
Results	R			
	< <u>P</u> revious <u>N</u> e	ext > Install Cancel		

**步驟5.**進行設定。

Select role services

<b>a</b>	Add Roles and Features Wizard	×
Installation progre	DESTINATION S DESTINATION S WIN-ODEF7N1GRUB.LSC20	SERVER 12.com
Before You Begin	View installation progress	
Installation Type	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)	<u> </u>
	You can close this wizard without interrupting running tasks. View task progress or open page again by clicking Notifications in the command bar, and then Task Details. Export configuration settings	this
	< Previous Next > Close Ca	ncel

**步驟6.選**擇企業CA,並將所有內容保留為預設值。

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

步驟7.按一下Microsoft Windows/開始選單。

#### 步驟8.單擊管理工具。

步驟9.單擊Active Directory使用者和電腦。

**步驟10**.展開域,按一下右鍵**Users資料夾**,然後選擇**New Object > User**。

	New Object - User	X
File Action View Help ← ➡ 2   ↓ 2   ↓   ↓   ★	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 Accou</li> <li>Users</li> </ul>	Full name: AP USER User logon name: APUSER @LSC2012.com	
	User logon name (pre- <u>Wi</u> ndows 2000): LSC2012\ APUSER	
	< <u>B</u> ack <u>N</u> ext > Cancel	
	Image: Source of the second	
	winkwikem Security Group Members of this group	

**步驟11.**在本範例中,它命名為APUSER。建立後,必須編輯使用者並按一下MemberOf頁籤,並使 其成為IIS\_IUSRS組的成員

#### 所需的使用者許可權分配包括:

— 允許在本地登入

— 作為服務登入

步驟12.安裝網路裝置註冊服務(NDES)。

<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 Service Certificate Enrollment Policy Web Service	
	< <u>P</u> revious <u>N</u> ex	t > <u>C</u> onfigure Cancel

• 選擇IIS\_USRS組的帳戶成員(在本例中為APUSER),作為NDES的服務帳戶。

步驟13.導覽至Administrative Tools。

步驟14.單擊Internet Information Services(IIS)。

步驟15.展開Server > Sites > Default web site > Cert Srv。

步驟16.對於mscep和mscep\_admin,請按一下authentication。確保啟用了匿名身份驗證。

**步驟17.右**鍵按一下**windows authentication並**選擇**Providers**。確保NT LAN Manager(NTLM)在清單 中位於首位。

**步驟18.在**登錄檔設定中禁用身份驗證質詢,否則簡單證書註冊協定(SCEP)要求質詢密碼身份驗證 ,而WLC不支援該身份驗證。

步驟19.開啟regedit application。

步驟20.前往HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\。

步驟21.將EnforcePassword設定為0。

Ċ)		Registry Editor					- • ×
File	Edit	View Favorites	Help				
		👂 🏭 Advance	ed INF 🔨	Name	Туре	Data	
		Þ - 퉲 ALG		ab (Default)	REG_SZ	(value not set)	
		🕌 AllUserl	nstallA	8 EnforcePassword	REG_DWORD	0x00000000 (0)	
		👂 - 퉲 Assistan	ice				
		👂 - 鷆 AuthHo	st ≘				
		👂 - 🌽 BestPra	ctices				
		þ 퉬 BidInter	face				
		Þ- 🎍 Chkdsk					
		þ- 퉲 СОМЗ					
		🕌 Comma	and Pro		•		
		🛛 🎍 Cryptog	raphy		13		
		Þ - 🏰 Auto	Enroll				
		👂 - 🏰 Cala	is				
		🌆 Cata	logDB				
		Catl	DBTem				
		D- Cert	ificate				
		Defa	oults				
		⊿ - <u>∥</u> MSC	LEP				
			Cartype				
			Certsin				
			Enforce				
			rasswo				
			v Sesing				
<	1		>				
Comp	uter\H	IKEY_LOCAL_MAC	HINE\SOF	TWARE\Microsoft\Cryp	tography\MSCEP\Enfo	rcePassword	ctivate Wind

步驟22.按一下Microsoft Windows/開始選單。

步驟23.鍵入MMC。

步驟24.在「檔案」選單上,選擇「新增/刪除管理單元」。選擇Certification Authority。

步驟25.右鍵點選Certificate Template資料夾,然後點擊Manage。

步驟26.按一下右鍵現有模板(如User),然後選擇「複製**模板」**。

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	
	I User Signatt ve Only	1	4.1	
	B Web Server	1	4.1	Activat
	Workstation Authentication	2	101.0	Client Authent

步驟27.選擇CA作為Microsoft Windows 2012 R2。

步驟28.在「General」索引標籤上,新增顯示名稱,例如WLC和有效期。

**步驟29.在**「使用者名稱」標籤中,確認已選**擇了請求中的**「供應」。

Proj	perties	of New	Template		x	
Superseded Templa	ites	Exte	ensions	Security		
Compatibility General	Request	Handling	Cryptography	/ Key Attesta	tion	
Subject Name	Subject Name Server Issuance Requirements					
Supply in the request	+					
Use subject info						
renewal request	mation no s	mexisting	centificates for	autoenrolimen		
Build from this Active	e Directory	informatio	n			
Select this option to a	enforce co	nsistency	among subject	names and to		
simplify certificate ad	ministration	1.				
Subject name format						
None				~		
lnclude e-mail na	me in subje	ect name				
Include this informati	on in alterr	nate subje	ct name:			
E-mail name		-				
DNS name						
User principal nar	me (UPN)					
Service principal	name (SPI	N)		N		
				45		
					-	
ОК	(	Cancel	<u>A</u> pply	Help		

**步驟30.單擊Issuance Requirements選**項卡。Cisco建議您在典型的分層CA環境中將頒發策略留空 :

Supersec	ded Templa	tes	Exte	ensions	Securit	ty		
Compatibility	General	Request	Handling	Cryptograph	Cryptography Key Attestation			
Subject N	lame	Sen	ver	Issuance Requirements				
Require the f	following fo cate manag ber of auth	r enrollmen ger approv orized sigr	nt: rali natures:	Pee: 0				
If you require more than one signature, autoenrollment is not allowed.								
	perequieu	in signatu	iro.			$\overline{}$		
Applicati	on policy:							
						~		
l <u>s</u> suance	e policies:							
					A <u>d</u> d <u>R</u> emov	/e		
Require the f	following fo	r reenrollm	ent:					
<ul> <li>Same crit</li> </ul>	eria as for (	enrollment						
◯ Valid <u>e</u> xis	ting certific	ate						
Allow	key based	renewal						
Requires request.	subject inf	ormation t	o be provid	led within the	certificate			
[	ОК	(	Cancel	Apply	H	elp		

**步驟31.單擊Extensions(擴展)頁籖、Application Policies**,然後Edit。按一下Add,並確保將 Client Authentication新增為應用程式策略。按一下「OK」(確定)。

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

**步驟32.單擊Security選項**卡,然後單**擊Add...**.確保在NDES服務安裝中定義的SCEP服務帳戶完全控 制模板,然後按一下**確定**。

Subject N	Sen	ver	Issuance	Requirements					
Compatibility	Compatibility General			Cryptograph	y Key Attestation				
Supersec	ded Templa	tes	Ext	ensions	Security				
Group or user names:									
& Authent	ticated Use	rs							
🔏 Adminis	trator								
👗 AP USI	er (Apuse	R@LSC2	012.com)						
👫 Domain	Admins (L	SC2012\D	)omain Ad	mins)					
👫 Domain	Users (LS	C2012\Do	main Use	rs)					
🔏 Enterpri	ise Admins	(LSC2012	\Enterpris	e Admins)					
Add <u>R</u> emove									

**步驟33.**返回證書頒發機構GUI介面。按一下右鍵Certificate Templates目錄。導覽至New> Certificate Template to Issue。選擇先前配置的WLC模板,然後點選**確定。** 

	ion nen ratones milaon	,		-1-
(= 🔿 🖄	🖬 🖻 🗟 🔽 🖬			_
sole Root	•	Enable Certificate Templates	x	<u> </u>
Certification A wlaaan201 Revoku Ssued Pendir	Select one Certificate Template to Note: If a certificate template that information about this template ha All of the certificate templates in th For more information, see <u>Cer</u>	o enable on this Certification Authority. was recently created does not appear on this list, you may ne is been replicated to all domain controllers. he organization may not be available to your CA. <u>ttificate Template Concepts.</u>	ed to wait until	Tem tions
E Failed	Name Key Recovery Agent OCSP Response Signing RAS and IAS Server Router (Offline request) Smartcard Logon Smartcard User Trust List Signing User Signature Only WLC Workstation Authentication	Intended Purpose Key Recovery Agent OCSP Signing Client Authentication, Server Authentication Client Authentication, Server Authentication Client Authentication, Smart Card Logon Secure Email, Client Authentication, Smart Card Logon Microsoft Trust List Signing Secure Email, Client Authentication Client Authentication, Secure Email, Encrypting File System Client Authentication		
<		OK	Cancel	

**步驟34.在**「電腦」>「HKEY\_LOCAL\_MACHINE」>「軟體」>「Microsoft」>「加密」>「 MSCEP」下的登錄檔設定中更改預設SCEP模板。將EncryptionTemplate、 GeneralPurposeTemplate和SignatureTemplate金鑰從IPsec(離線請求)更改為先前建立的 WLC模板。

ġ					Re	gistry Edito	or	_ <b>_</b> X
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	F <u>a</u> vorites	<u>H</u> elp				
		Þ-1	Advance	d INF 🔨	Name	Туре	Data	
		Þ - 🔰	ALG		赴 (Default)	REG_SZ	(value not set)	
			AllUserIn	nstallA	EncryptionTem	REG_SZ	WLC	
		Þ-1	Assistan	ce	A General Purpose	REG_SZ	WLC	
		Þ-	AuthHos	st ≣	Signature Template	REG_SZ	WLC	
		Þ-1	BestPrac	tices				
		Þ-1	BidInterf	ace				
		Þ-1	Chkdsk					
		► P - M	COMB					
			Comma	na Pro				
		4-4		Enroll				
			Calai	ie				
			Catal	logDB				
			CatD	BTem				
			Certi	ficate				
			Defa	ults				
			MSC	EP				
			C	АТур				
			- 🝈 o	ertsin				
			🏭 E	nforce				
			]] P	asswo				
			l]] U	JseSing				
<		· · · .		>				
Comp	outer\H	IKEY_LO	CAL_MAC	HINE\SOF	TWARE\Microsoft\Cryp	tography\MS	CEP	Activate Wind

步驟35.重新啟動系統。

#### 設定WLC

步驟1。在WLC上,導覽至Security功能表。按一下「Certificates > LSC」。

步驟2.勾選在控制器上啟用LSC覈取方塊。

**步驟3.**輸入您的Microsoft Windows Server 2012 URL。預設情況下,它會附加在 /certsrv/mscep/mscep.dll中。

步驟4.在「引數」部分輸入您的詳細資訊。

步驟5.應用變更。

Local Significant Certificates (LSC)

-				
Δ	n	n	h	
	μ	μ	- 1	٢.

General AP Provisionin	g					
Certificate Type	Status					
CA	Present 🔽					
General						
Enable LSC on Controller	$\checkmark$					
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					

步驟6.按一下CA上方線上的藍色箭頭並選擇Add。應該將狀態從Not presence更改為presence。

#### 步驟7.單擊AP調配頁籤。

cisco	MONITOR	WLANs	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>Password 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 Presioning	rovision	5) 3						

步驟8.選中AP Provisioning下的Enable覈取方塊,然後點選Update。

步驟9.如果接入點沒有自行重新啟動,請重新啟動它們。

### 驗證

使用本節內容,確認您的組態是否正常運作。

重新引導後,接入點會返回並顯示LSC作為「無線」選單中的證書型別。

	CISCO	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGENERT	COMMANDS	нар	EEEDBACK						
W	fireless	All APs												Entries	1 - 2 of 2	^
•	Access Points All APs Radics 802.11a/n 802.11b/g/n	Current Filt	ar f APa		None 2		Change Fil	ier) (Clear Filter	1							
	Global Configuration										Operational				Certificat	te
•	Advanced Mesh	CAPISOLI-I		AIR-	CAP35011-E-K	9	c8:9c:1d:6e:a3:cd	0 d, 00 l	h 35 m 21	a Disabled	REG	1 Port	AP Node Local		LSC	
	RF Profiles	LAP1142-1		AIR	LAP1142N-1-K	2	ac:12:c5:73:33:ce	0 d, 00	h 02 m 35	s Enabled	REG	1	Local		LSC	- 1
	FlexConnect Groups FlexConnect ACLs															
۲	802.11a/n															
1	802.11b/g/n															
ľ	Media Stream Application Visibility															
1	And Control															
	Country															
	Netflow															
1	005															
																*
		<u> </u>	-	8			- 0	0				-	-	ENG	6:41 PM	
Ŀ		2			ö.	3		P				- 10	97 (b	UK	12/16/201	14

附註:在8.3.112之後,一旦啟用LSC,MIC AP就根本無法加入。因此,「嘗試LSC」計數功 能使用受到限制。

## 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。