Ejemplo de Configuración de Certificados de Importancia Local (LSC) con WLC y Windows Server 2012

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Configuración de Microsoft Windows Server Configurar la WLC Verificación Troubleshoot

Introducción

Este documento describe cómo configurar certificados de significación local (LSC) con un controlador de LAN inalámbrica (WLC) y un Microsoft Windows Server 2012 R2 recientemente instalado.

Nota: Las implementaciones reales pueden diferir en muchos puntos y debería tener un control y un conocimiento completos de los ajustes de Microsoft Windows Server 2012. Este ejemplo de configuración sólo se proporciona como una plantilla de referencia para que los clientes de Cisco implementen y adapten su configuración de Microsoft Windows Server para que LSC funcione.

Prerequisites

Requirements

Cisco recomienda que comprenda todos los cambios realizados en Microsoft Windows Server y compruebe la documentación pertinente de Microsoft si es necesario.

Nota: El LSC en el WLC no es soportado con el intermedio-CA, ya que la CA raíz se perderá del WLC ya que el controlador sólo obtiene la CA intermedia.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC versión 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.

Configurar

Configuración de Microsoft Windows Server

Esta configuración se muestra como realizada en un Microsoft Windows Server 2012 recientemente instalado. Debe adaptar los pasos a su dominio y a su configuración.

Paso 1. Instale los Servicios de dominio de Active Directory para el asistente de funciones y funciones.



Paso 2. Después de la instalación, debe promocionar el servidor al controlador de dominio.

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 Role 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 loois	~
	You can close this wizard without interrupting running tasks. View task pr page again by clicking Notifications in the command bar, and then Task E Export configuration settings	ogress or open this Jetails.
	< <u>P</u> revious <u>N</u> ext > Cl	ose Cancel

Paso 3. Dado que se trata de una nueva configuración, se configura un nuevo bosque; pero normalmente en implementaciones existentes, simplemente configure estos puntos en un controlador de dominio. Aquí, usted elige el dominio **LSC2012.com**. Esto también activa la función Servidor de nombres de dominio (DNS).

Paso 4. Después de reiniciar, instale el servicio de autoridad de certificados (CA) así como la inscripción en la Web.

- **D** 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	Certification Authority	Certification Authority Web
Server Roles	Certificate Enrollment Policy Web Service	interface that allows users to
Features	Certificate Enrollment Web Service	perform tasks such as request and
AD CS	Certification Authority Web Enrollment	revocation lists (CRLs), and enroll for
Role Services	Network Device Enrollment Service	smart card certificates.
Web Server Role (IIS)	Online Responder	
Role Services		
Confirmation		
Results		
	R	
		_
	< <u>P</u> revious <u>N</u>	ext > Install Cancel

Paso 5.Configure.

Select role services

b	Add Roles and Features Wizard
Installation progre	SS DESTINATION SERVER WIN-ODEF7N1GRUB.LSC2012.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
	Web Server (IIS)
	web server (iis)
	You can close this wizard without interrupting running tasks. View task progress or open this
	page again by clicking Notifeations in the command bar, and their rask Details.
	export configuration settings
	< Previous Next > Close Cancel

Paso 6. Elija Enterprise CA y deje todo como predeterminado.

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

Paso 7. Haga clic en el menú Microsoft Windows/Start.

Paso 8. Haga clic en Herramientas administrativas.

Paso 9. Haga clic en Usuarios y equipos de Active Directory.

Paso 10. Expanda el dominio, haga clic con el botón derecho en la carpeta Users y elija New Object > User.

	New Object - User	_ D X
File Action View Help	Create in: LSC2012.com/Users	
 ▷ Saved Queries ▲ ∰ LSC2012.com ▷ ☐ Builtin ▷ ☐ Computers ▷ ☐ Domain Controllers 	Eirst name: AP Initials: Last name: USER Full name: AP USER	
 ForeignSecurityPrincipa Managed Service Accound to the service Account to the service Ac	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	

Paso 11. En este ejemplo, se denomina **APUSER**. Una vez creado, debe editar el usuario y hacer clic en la **ficha MemberOf**, y convertirlo en miembro del grupo IIS_IUSRS

Las asignaciones de derechos de usuario necesarias son:

- Permitir inicio de sesión localmente
- Inicie sesión como servicio

Paso 12. Instale el servicio de inscripción de dispositivos de red (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

• Elija el miembro de cuenta del grupo IIS_USRS, **APUSER** en este ejemplo, como la cuenta de servicio para NDES.

Paso 13. Vaya a Administrative Tools (Herramientas administrativas).

Paso 14. Haga clic en Servicios de Internet Information Server (IIS).

Paso 15. Expanda el Servidor > Sitios > Sitio Web predeterminado > Cert Srv.

Paso 16. Para mscep y **mscep_admin**, haga clic en **authentication**. Asegúrese de que la autenticación anónima esté habilitada.

Paso 17. Haga clic con el botón derecho del ratón en autenticación de Windows y elija Proveedores. Asegúrese de que NT LAN Manager (NTLM) sea el primero en la lista.

Paso 18. Inhabilite el desafío de autenticación en la configuración del Registro; de lo contrario, Simple Certificate Enrollment Protocol (SCEP) espera la autenticación de contraseña de desafío,

que no es compatible con el WLC.

Paso 19. Abra la aplicación regedit.

Paso 20. Vaya a HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\.

Paso 21. Establezca EnforcePassword en 0.

đ			Re	gistry Editor		
File	Edit	View Favorites Help				
		🛛 🍌 Advanced INF 🔨	Name	Туре	Data	
		🔉 - 🍌 ALG	ab) (Default)	REG_SZ	(value not set)	
		🐌 AllUserInstallA	EnforcePassword	REG_DWORD	0x00000000 (0)	
		👂 🍌 Assistance 👘				
		⊳- 🍌 AuthHost 🛛 🛓				
		BestPractices				
		b BidInterface				
		D - Low Chkdsk				
		р - 📕 СОМЗ				
		Command Prc		N		
		4 🎳 Cryptography		6		
		AutoEnroll				
		D- Calais				
		CatDB lem				
		Catype				
		Parriero				
<		III >				
Comp	outer\ł	KEY_LOCAL_MACHINE\SOF	TWARE\Microsoft\Cryp	tography\MSCEP\En	forcePassword	Activate Wind

Paso 22. Haga clic en el menú Microsoft Windows/Start.

Paso 23. Escriba MMC.

Paso 24. En el menú Archivo, elija Agregar o quitar complemento. Elija Autoridad de Certificación.

Paso 25. Haga clic con el botón derecho en la carpeta Plantilla de certificado y haga clic en Administrar.

Paso 26. Haga clic con el botón derecho del ratón en una plantilla existente, como Usuario, y elija Duplicar plantilla.

File Action View Help				
Þ 🔿 🖬 🖬 🖬 🔽 🖬				
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	
	Rechange Enrollment Agent (Offline requ	1	4.1	
	Exchange Signature Only	1	6.1	
	R 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	
	Irust List Signing	1	3.1	
	Juser Land Land Land Land Land Land Land Land	1	3.1	
	I User Signative Only	1	4.1	
	Web Server	1	4.1	Activat
	Workstation Authentication	2	101.0	Client Authent

Paso 27. Elija la CA como Microsoft Windows 2012 R2.

Paso 28. En la ficha General, agregue un nombre de visualización como WLC y un período de validez.

Paso 29. En la ficha Nombre del asunto, confirme que se ha seleccionado Suministrar en la solicitud.

Properties of New Template							
Superseded Templates Extensions Security							
Compatibility General	Request	Handling	Cryptograph	y Key Attesta	tion		
Subject Name	Sen	ver	Issuance	Requirements			
Supply in the request							
Use subject infor renewal requests	mation fro	m existing	certificates fo	r autoenrolimen			
 <u>B</u>uild from this Active Select this option to ensimplify certificate adm Subject name formation 	Directory nforce co iinistratior	information nsistency 1.	on among subjec	t names and to			
None				~			
				Ŧ			
lnclude e-mail nam	ie in subje	ect name					
Include this informatio	n in alterr	nate subje	ct name:				
E-mail name							
DNS name							
User principal nam	e (UPN)						
Service principal name (SPN)							
ОК	(Cancel	Apply	Help			

Paso 30. Haga clic en la pestaña **Requisitos de emisión**. Cisco recomienda dejar las políticas de emisión en blanco en un entorno de CA jerárquico típico:

Supersec	Security								
Compatibility	General	Request	Handling	Cryptograph	y Key Attestation				
Subject N	Name	Sen	ver	Issuance	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.	Allow key based renewal Requires subject information to be provided within the certificate request.								
[ОК	(Cancel	<u>A</u> pply	Help				

Paso 31. Haga clic en la ficha Extensiones, Políticas de aplicación y, a continuación, en Editar. Haga clic en Agregar y asegúrese de que la autenticación de cliente se agrega como política de aplicación. 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							

Paso 32. Haga clic en la **ficha Seguridad** y, a continuación, haga clic en **Agregar...** Asegúrese de que la cuenta de servicio SCEP definida en la instalación del servicio NDES tenga control total de la plantilla y haga clic en **Aceptar**.

Subject N	lame	Sen	ver	Issuance Requirements		
Compatibility	General	Request	Handling	Cryptograph	ny Key Attestatio	n
Supersec	led 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)			
용 Domain	Admins (L	SC2012\D	omain Ad	mins)		
👫 Domain	Users (LS	C2012\Do	main User	rs)		
🔏 Enterpri	ise Admins	(LSC2012	\Enterpris	e Admins)		
\mathbb{R}^{2}						
				A <u>d</u> d] <u>R</u> emove]

Paso 33. Vuelva a la interfaz gráfica de usuario de Certification Authority. Haga clic con el botón derecho del ratón en el **directorio Plantillas de certificado**. Vaya a **New > Certificate Template para emitir**. Seleccione la plantilla WLC configurada previamente y haga clic en **Aceptar**.

· · · · · · · · ·		·		- 1-
(= e) 🖄				
sole Root		Enable Certificate Templates	× –	
Certification A Wlaaan201 Certification A Certification A Certificatio	Select one Certificate Template to Note: If a certificate template that information about this template ha All of the certificate templates in the For more information, see <u>Certificate</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. he organization may not be available to your CA. rtificate Template Concepts.	ed to wait until tions	n
🦳 Failed	Name	Intended Purpose	~	
Certifi	Image: Construction Image: Construction Image: Construction Image: Construction	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 Secure Email, Client Authentication Client Authentication Client Authentication		
		ОК	Cancel	
<	III > <	III		

Paso 34. Cambie la plantilla SCEP predeterminada en la configuración del Registro en **Equipo > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Criptografía > MSCEP**. Cambie las claves EncryptionTemplate, GeneralPurposeTemplate y SignatureTemplate de IPsec (solicitud sin conexión) a la plantilla WLC creada anteriormente.

đ			Re	gistry Editor		_ _ ×
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew F <u>a</u> vorites <u>H</u> elp				
		👂 - 퉲 Advanced INF 🔿	Name	Туре	Data	
		Þ - 퉲 ALG	ab (Default)	REG_SZ	(value not set)	
			EncryptionTem	REG_SZ	WLC	
		Assistance	eneralPurpose	REG_SZ	WLC	
		Þ- 퉲 AuthHost 🛛 🚊	a Signature Template	REG_SZ	WLC	
		BestPractices	6			
		BidInterface				
		b - Chkdsk				
		D- COM3				
		Command Prc				
		CatalogDB				
		CatDRTem				
		Defaults				
		MSCEP				
		CAType				
		Certsin				
		Passwo				
<						
					、	
Com	puter\H	IKEY_LOCAL_MACHINE\SOF	TWARE\Microsoft\Cryp	tography\MSCEP	,	Activate Wind

Paso 35. Reinicie el sistema.

Configurar la WLC

Paso 1. En el WLC, navegue al menú Security . Haga clic en Certificados > LSC.

Paso 2. Marque la casilla Enable LSC on Controller.

Paso 3. Introduzca la URL de Microsoft Windows Server 2012. De forma predeterminada, se agrega con /certsrv/mscep/mscep.dll.

Paso 4. Introduzca sus detalles en la sección Params.

Paso 5. Aplique el cambio.

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	

Paso 6. Haga clic en la flecha azul de la línea CA superior y elija **Agregar**. Debería cambiar el estado de **No presente** a **presente**.

Paso 7. Haga clic en la pestaña AP provisioning.

Paso 8. Marque la casilla de verificación Enable bajo AP Provisioning y haga clic en Update.

Paso 9. Reinicie los puntos de acceso si no se han reiniciado.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

El punto de acceso, después de reiniciar, se une y se muestra con LSC como el tipo de certificado en el menú Inalámbrico.

CISCO	MONITOR WLANS	CONTROLLER WIRELESS SECURITY	MANAGENENT COMMANDS	HELP EEEDBACK			
Wireless	All APs					Entries	1-2012 A
Access Points All APs Rodics R02.tis/n S02.tis/n Doub-Band Racks	Current Filter Number of APs	None 2	(Chance Filter) (Clear Filter	a			
Global Configuration	AP Name	AP Nodel	AP NAC AP Up 1	lime Admin Status	Operational Status Port	AP Node	Certificate Type
Mesh	CAP15011-1	AIR-CAP3501I-E-K9	c8:9c:id:6e:a3:cd 0 d, 00 l	h 35 m 21 s Disabled	R0G 1	Local	LSC
RF Profiles	LAF1142-1	AIR-LAP1142N-1-K9	ac:12:c5:73:33:ce 0 d, 00	h 02 m 35 s Enabled	ROG 1	Local	LSC
RF Profiles FlexConnect Groups FlexConnect ACLs b 802.111a/n b 802.111a/n b Media Stream b Application Visibility And Control Country Timers b Netflow b Qo5							
	2				- 10) 😪 👍 ENG	> 6:41 PM

Nota: Después de 8.3.112, los AP MIC no pueden unirse en absoluto una vez que LSC está habilitado. Por lo tanto, la función de recuento de "intentos de LSC" se vuelve de uso limitado.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.