具有WLC和Windows Server 2012的本地有效证 书(LSC)配置示例

目录

简介 <u>先决条件</u> 要求 使用的组件 配置 Microsoft Windows Server配置 配置 WLC 验证 故障排除

简介

本文档介绍如何使用无线局域网控制器(WLC)和新安装的Microsoft Windows Server 2012 R2配置本 地有效证书(LSC)。

注意:实际部署可能在很多方面有所不同,您应完全控制并了解Microsoft Windows Server 2012上的设置。此配置示例仅作为参考模板提供,供思科客户实施和调整其Microsoft Windows Server配置以使LSC工作。

先决条件

要求

思科建议您了解在Microsoft Windows Server中所做的每次更改,并在需要时检查相关的 Microsoft文档。

注意:中间CA不支持WLC上的LSC,因为根CA将从WLC丢失,因为控制器仅获取中间CA。

使用的组件

本文档中的信息基于以下软件和硬件版本:

•WLC版本7.6

Microsoft Windows Server 2012 R2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

齔, 「

Microsoft Windows Server配置

此配置显示为在新安装的Microsoft Windows Server 2012上执行。您必须根据域和配置调整步骤。

步骤1.为角色和功能向导安装Active Directory域服务。

Select server roles

DESTINATION SERVER WIN-ODEF7N1GRUB

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 network
	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	~

步骤2.安装后,必须将服务器升级到域控制器。

a	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

步骤3.由于这是新设置,因此您配置了新林;但通常在现有部署中,只需在域控制器上配置这些点 。此处,您选择**LSC2012.com**域。这也会激活域名服务器(DNS)功能。

步骤4.重新启动后,安装证书颁发机构(CA)服务和Web注册。

DESTINATION SERVER WIN-ODEF7N1GRUB.LSC2012.com

_ 0 X

Before You Begin	Select the role services to install for Active Directory Certificate Services					
Installation Type	Role services	Description				
Server Selection Server Roles Features AD CS Role Services Web Server Role (IIS) Role Services Confirmation	 Certification Authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certification Authority Web Enrollment Network Device Enrollment Service Online Responder 	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				

步骤5.配置它们。

Select role services

à	Add Roles and Features Wizard	
Installation progre	DESTINATION WIN-ODEF7N1GRUB.LSC2	SERVER 012.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	i this
	< Previous Next > Close Co	ancel

步骤6.选择企业CA并保留所有默认值。

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

步骤7.单击"Microsoft Windows/开始"菜单。

步骤8.单击管理工具。

步骤9.单击"Active Directory用户和计算机"。

步骤10.展开域,右键单击"用户"文**件夹**,然后选择**"新建对象">"用户**"。

	New Object - User	X
File Action View Help	Create in: LSC2012.com/Users	
 Saved Queries Saved Queries ESC2012.com Builtin Computers 	Erst name: AP Initials: USER	
Domain Controllers ForeignSecurityPrincipa Managed Service Accounts	Full name: AP USER	
🔐 Users	APUSER @LSC2012.com User logon name (pre- <u>Windows 2000):</u> LSC2012\ APUSER	
	< <u>B</u> ack <u>N</u> ext > Cancel	
	Image: Security Group Built-in account for gue Image: Security Group Members of this group Image: Security Group Servers in this group can Image: Security Group Servers in this group can Image: Security Group Members of this group Image: Security Group Members of this group Image: Security Group Designated administrato Image: Security Group Members of this group	
	winkmikem Security Group Members of this group	

步骤11.在本例中,它命名为APUSER。创建后,必须编辑用户并单击MemberOf选项卡,并将其设置为IIS_IUSRS组的成员

所需的用户权限分配包括:

— 允许本地登录

— 以服务身份登录

步骤12.安装网络设备注册服务(NDES)。

b	AD CS Configuration	
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 Online Responder Network Device Enrollment Service Certificate Enrollment Policy Web Service 	
	NOTE BOOK AD CO SERVET NOTES	
	< <u>P</u> revious <u>N</u> e	xt > Configure Cancel

•在本例中,选择IIS_USRS组的帐户成员APUSER作为NDES的服务帐户。

步骤13.导航至Administrative Tools。

步骤14.单击"Internet信息服务(IIS)"。

步骤15.展开Server > Sites > Default web site > Cert Srv。

步骤16.对于mscep和mscep_admin,单击身份验证。确保已启用匿名身份验证。

步骤17.右键单击Windows身**份验**证并选择**提供程**序。确保NT LAN Manager(NTLM)在列表中处于 首位。

步骤18.在注册表设置中禁用身份验证质询,否则简单证书注册协议(SCEP)需要质询密码身份验证 ,WLC不支持该身份验证。 步骤20.转到HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\。

步骤21.将EnforcePassword设置为0。

đ				Re	gistry Editor		- D X
File	Edit	View Favorites	Help				
		👂 퉲 Advanc	ed INF 🔨	Name	Туре	Data	
		Þ- 퉲 ALG		ab (Default)	REG_SZ	(value not set)	
		鷆 AllUserl	nstallA	8 EnforcePassword	REG_DWORD	0x00000000 (0)	
		👂 - 퉲 Assistan	ice				
		👂 - 鷆 AuthHo	st ≣				
		þ - 🎉 BestPra	ctices				
		þ 퉬 BidInter	face				
		Þ- 🎍 Chkdsk					
		þ- 퉲 СОМЗ					
		🕌 Comma	ind Pro		•		
		⊿ 🎳 Cryptog	raphy		13		
		Þ - 🏰 Auto	Enroll				
		👂 - 🏰 Cala	is				
		🎽 Cata	logDB				
		Catl	Blem				
		D- Cert	ficate				
		Defa	ults				
		⊿ - 🏨 MSC	EP				
			ertsin				
			Inforce				
			asswo				
			v v				
<	1		>				
Comp	outer\H	KEY_LOCAL_MAC	HINE	TWARE\Microsoft\Cryp	tography\MSCEP\Enfo	rcePassword	ctivate Wind

步骤22.单击"Microsoft Windows/开始"菜单。

步骤23.键入MMC。

步骤24.在"文件"菜单中,选择"添加/删除管理单元"。选择Certification Authority。

步骤25.右键单击Certificate Template(证书模板)文件夹,然后单击Manage。

步骤26.右键单击现有模板(如用户),然后选择"复**制模板"**。

File	Action	View	Help				
þ		🗎 📑	? 🖬				
a c	ertificate	Template	s (WIN-OD	E Template Display Name	Schema Version	Versi	Intended Purp
				R CA Exchange	2	106.0	Private Key Arc
				CEP Encryption	1	4.1	
				R 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	
				R 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	
				Web Server 8	1	4.1	Activat
				B Workstation Authentication	2	101.0	Client Authent

步骤27.选择CA作为Microsoft Windows 2012 R2。

步骤28.在General选项卡上,添加显示名称(如WLC)和有效期。

步骤29.在"主题名称"选项卡中,确认选**择了"请求中**的供应"。

Superseded Templates Extensions Security Compatibility General Request Handling Cryptography Key Attestation Subject Name Server Issuance Requirements	Properties of New Template							
Compatibility General Request Handling Cryptography Key Attestation Subject Name Server Issuance Requirements Image: Supply in the request Image: Supply in the request Image: Use subject information from existing certificates for autoenrollment renewal requests Image: Build from this Active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration. Subject game format: None Image: I	Superseded Temp	olates	Exte	ensions	Security			
Subject Name Server Issuance Requirements	Compatibility General	Request	Handling	Cryptography	/ Key Attestat	tion		
 Supply in the request Use subject information from existing certificates for autoenrollment tenewal requests Puild from this Active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration. Subject name format: None Include e-mail name in subject name Include this information in alternate subject names: Include this information in alternate subject name: Service principal name (UPN) Service principal name (SPN) OK Cancel Apply Help 	Subject Name	Subject Name Server Issuance Requirements						
Image: Section of the existing certificates for autoenrollment renewal requests Image: Section of the existing certificates for autoenrollment renewal requests Image: Section of the existing certificates for autoenrollment of the existing certificate administration. Subject name format: Image: None Image: Imag	Supply in the reau	est						
Build from this Active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration. Subject name format: None ✓ Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN)	Use subject in renewal reque	formation fro sts	om existing	certificates for	autoenrollment]		
None Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN)	O Build from this Action Select this option to simplify certificate a Subject name form	ive Directory o enforce co administratior at:	r informatio Insistency 1.	on among subject	names and to			
Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN)	None				~			
Include emili name in subject name Include this information in alternate subject name E-mail name DNS name User principal name (UPN) Service principal name (SPN)		ame in subi	actiname					
Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN)		ianie in sabje	eet manne					
E-mail name DNS name User principal name (UPN) Service principal name (SPN) Image: Concelement of the service	Include this informa	ation in alterr	nate subje	ct name:				
DNS name User principal name (UPN) Service principal name (SPN) V V OK Cancel Apply Help	E-mail name							
User principal name (UPN) Service principal name (SPN) Image: Concelement of the service of the servic	DNS name							
OK Cancel Apply Help		ame (UPN)						
OK Cancel <u>A</u> pply Help	Ser <u>v</u> ice principal name (SPN)							
OK Cancel <u>A</u> pply Help								
OK Cancel <u>Apply</u> Help								
Cancer <u>Appiy</u> Help	01		Cancel	Apphy	Hele			
	UK UK		Lancer		Help			

步骤30.单击Issuance Requirements**选项**卡。思科建议您在典型的分层CA环境中将颁发策略留空:

Supersec	ded Templa	ites	Exte	ensions	Security			
Compatibility	General	Request	Handling	Cryptograph	y Key Attestation			
Subject N	lame	Sen	ver	Issuance	Requirements			
Require the following for enrollment:								
If you re	quire more	than one :	signature, a	autoenrollment	t is not allowed.			
<u>P</u> olicy ty	pe required	lin signatu	ire:					
					~			
Applicati	on policy:							
Issuance	e policies:							
					A <u>d</u> d			
	<u>R</u> emove							
Require the f	following fo	r reenrollm	ent:					
Same crit	eria as for (enrollment						
◯ Valid <u>e</u> xis	ting certific	ate						
Allow	key based	renewal						
Requires request.	Requires subject information to be provided within the certificate request.							
[ОК	(Cancel	Apply	Help			

步骤31.单击"扩**展"选**项卡**、"应用**策略"和**"编辑**"。单击Add,并确保将Client Authentication添加为应 用策略。Click OK.

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

步骤32.单击"安**全"选**项卡,然**后单击"添加……**。确保在NDES服务安装中定义的SCEP服务帐户对 模板具有完全控制权,然后单击**OK**。

Subject N	Sen	ver	Issuance	quirements					
Compatibility	General	Request	Handling	Cryptograph	ıy	Key Attestation			
Supersec	ded Templa	Ext	ensions	Security					
Group or user names:									
& 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 Use	rs)					
🔏 Enterpri	ise Admins	(LSC2012	\Enterpris	e Admins)					
Add <u>R</u> emove									

步骤33.返回到证书颁发机构GUI界面。右键单击"证书模**板"目录**。导航至"**新建">"要颁发的证书模板** "。选择之前配置的WLC模板,然后单击**OK。**

	on nen reronces million	n nop		
(= 🔿 🖄	📅 🖪 🔒 🛛 🖬			•
sole Root		Enable Certificate Templates	X	
Certification A Wlaaan201 Revoku Issued	Select one Certificate Template t Note: If a certificate template that information about this template hat All of the certificate templates in t For more information, see Certificate Cer	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. ertificate Template Concepts.	ed to wait until	Tem tions
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 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	

步骤34.在"计算机">"HKEY_LOCAL_MACHINE">"软件">"Microsoft">"加密">"MSCEP"下的注册表设置中更改默认的SCEP模板。将EncryptionTemplate、GeneralPurposeTemplate和 SignatureTemplate密钥从IPsec(脱机请求)更改为先前创建的WLC模板。

ġ			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- 🚹 ALG	ab (Default)	REG_SZ	(value not set)	
		🔒 AllUserInstallA	EncryptionTem	REG_SZ	WLC	
		Assistance	eneralPurpose	REG_SZ	WLC	
		Þ- 🕌 AuthHost 🛛 🚊	a Signature Template	EG_SZ	WLC	
		BestPractices				
		b - BidInterface				
		b - M Chkdsk				
		D- COM3				
		Command Pro				
		AutoEnroll				
		Catalog DR				
		Catalogue				
		Certificate				
		Defaults				
		MSCEP				
		CAType				
		CertsIn				
		Enforce				
		Passwo				
Com	puter\H	KEY_LOCAL_MACHINE\SOF	TWARE\Microsoft\Cryp	tography\MSCEP		Activate Wind

步骤35.重新启动系统。

配置 WLC

步骤1.在WLC上,导航至Security菜单。单击Certificates > LSC。

步骤2.选中Enable LSC on Controller复选框。

步骤3.输入Microsoft Windows Server 2012 URL。默认情况下,会附加/certsrv/mscep/mscep.dll。

步骤4.在"参数"部分输入详细信息。

步骤5.应用更改。

Local Significant Certificates (LSC)

General

CA

General

Certificate Type

cant Certificates (LSC)								
AP Provisioning								
/ре	Status							
	Present							
on Controller								
	. T							

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

步骤6.单击CA上行的蓝色箭头并选择"添加"。它应将状态从"不存在"更改为"存在"

步骤7.单击AP调配选项卡。

cisco	MONITOR	WLANs	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 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 Presioning	rovision	5) 3						

步骤8.选中AP Provisioning下**的**Enable复选框,然后单击**Update**。

步骤9.如果接入点没有自行重新启动,请重新启动它们。

验证

使用本部分可确认配置能否正常运行。

重新启动后,接入点会重新连接并以LSC作为证书类型显示在Wireless(无线)菜单中。

	CISCO	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGENERT	COMMANDS	нер	FEEDBACK						
W	fireless	All APs												Entries	1 - 2 of 2	^
-	Access Points All APs Radics 802.11a/n 802.11b/g/n Dual-Band Radios	Current Filt	lar I APa		None 2		Change Fil	ier) (Clear Filter	1							
	Global Configuration	AR Name			Hodel			AD III- T	in a	Admin Status	Operational	Beet	AP Mode		Certificat	8
`	Advanced Hesh RE Profiles	CAP15011-1		AIR-	CAP35011-8-K	9	c0:9c:id:6e:a3:cd ac:02:c5:73:33:ce	0 4, 00 1	1 35 m 21 1 02 m 35	a Disabled	ROG	1	Local		LSC	-
	FlexConnect Groups															
1	802.11b/g/n															
	Media Stream															
	Application Visibility And Control															
	Country															
	Timers															
•	Netflow															
•	Q05															< 1
F			-	ð 👝 📘			-	2					83.4	ENG	6:41 PM	
Ľ		<u> </u>			0		3- - -	r				- 10	16 VQ	UK	12/16/2014	4

注意:在8.3.112之后,MIC AP在启用LSC后,将无法加入。因此,"尝试LSC"计数功能的使 用有限。

故障排除

目前没有针对此配置的故障排除信息。