WLC および Windows サーバ 2012 でのローカ ルで有効な証明書(LSC)の設定例

内容

概要 <u>前提条件</u> <u>要件</u> 使用するコンポーネント</u> <u>設定</u> <u>Microsoft Windows Serverの設定</u> <u>WLC の設定</u> 確認 トラブルシュート

概要

このドキュメントでは、ワイヤレスLANコントローラ(WLC)と新しくインストールされた Microsoft Windows Server 2012 R2を使用して、ローカルで有効な証明書(LSC)を設定する方法に ついて説明します。

注:実際の導入は多くの点で異なる場合があり、Microsoft Windows Server 2012の設定を 完全に制御し、知識を持っている必要があります。この設定例は、シスコのお客様がLSCを 機能させるためにMicrosoft Windows Serverの設定を実装および適応するための参照テンプ レートとしてのみ提供されています。

前提条件

要件

Microsoft Windows Serverで行われたすべての変更を理解し、必要に応じて関連するMicrosoftの ドキュメントを確認することをお勧めします。

注:コントローラが中間CAを取得するだけなので、WLC上のLSCは中間CAではサポートされません。これは、ルートCAがWLCから欠落するためです。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

• WLC バージョン 7.6

Microsoft Windows Server 2012 R2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

設定

Microsoft Windows Serverの設定

この設定は、新しくインストールされたMicrosoft Windows Server 2012で実行されたとおりに表示されます。手順をドメインと設定に合わせる必要があります。

ステップ1:役割と機能ウィザードのActive Directoryドメインサービスをインストールします。

Before You Begin	Select one or more roles to install on the selected server.		
Installation Type	Roles	Description	
Server Selection Server Roles Features AD DS Confirmation	Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted	
Results	 □ Application Server □ DHCP Server □ 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 	resources anywhere on the network through a single logon process.	

ステップ2:インストール後、サーバをドメインコントローラに昇格する必要があります。

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

ステップ3:これは新しい設定であるため、新しいフォレストを設定します。ただし、通常は既存の展開では、ドメインコントローラ上でこれらのポイントを設定するだけです。ここでは、 LSC2012.comドメインを選択します。これにより、ドメインネームサーバ(DNS)機能もアクティブになります。

ステップ4:リビート後、認証局(CA)サービスとWeb登録をインストールします。

DESTINATION SERVER

- **D** X

WIN-ODEF7N1GRUB.LSC2012.com

Before You Begin	Select the role services to install for Active Directory Certific	cate Services
Installation Type	Role services	Description
Server Selection Server Roles	Certification Authority	Certification Authority Web Enrollment provides a simple Web interface that allows users to
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		
	Le Contraction de la contracti	
	< <u>P</u> revious	Jext > Install Cancel

ステップ5:設定します。

Select role services

à	Add Roles and Features Wizard	D X
Installation progre	DESTINATION WIN-ODEF7N1GRUB.LSC	N SERVER 2012.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)	-
	You can close this wizard without interrupting running tasks. View task progress or oper page again by clicking Notifications in the command bar, and then Task Details.	n this
	Export configuration settings	
	anyon contractings	
	< Previous Next > Close C	Cancel

ステップ6:[エンタープライズCA]を選択し、すべてデフォルトのままにします。

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	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	> <u>Configure</u> Cancel

ステップ7:Microsoft Windows/スタートメニューをクリックします。

ステップ8:[管理ツール]をクリックします。

ステップ9:[Active Directory Users and Computers]をクリックします。

ステップ10:ドメインを展開し、[Users]フォルダを右クリックして、[**New Object] > [User]を選** 択します。

	New Object - User	×
File Action View Help ← ➡ 2 III ¥ III ¥ □ Active Directory Users and Con	Create in: LSC2012.com/Users	
 Saved Queries LSC2012.com Builtin Computers Domain Controllers ForeignSecurityPrincipa Managed Service Accound Users 	First name: AP Last name: USER Full name: AP USER User logon name: @LSC2012.com User logon name (pre-Windows 2000): User logon name (pre-Windows 2000):	
< III >	Liscourt Arosen < Back	

ステップ11:この例では、APUSERという名前**で**す。作成したら、ユーザを編集し、 [MemberOf]タブをクリックして、IIS_IUSRSグループのメンバにする必要があります

必要なユーザ権限の割り当ては次のとおりです。

– ローカルでログオンを許可

- サービスとしてログオン

ステップ12:ネットワークデバイス登録サービス(NDES)をインストールします。

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	
	< <u>P</u> revious <u>N</u> e	ext > Configure Cancel

• IIS_USRSグループのアカウントメンバー(この例では**APUSER)**をNDESのサービスアカウン トとして選択します。

ステップ13:[管理ツール]に移動します。

ステップ14:[インターネットインフォメーションサービス(IIS)]をクリックします。

ステップ15:[Server] > [Sites] > [Default web site] > [Cert Srv]の順に展開します。

ステップ16:mscepと**mscep_admin**の両方の**場合は**、[authentication]をクリ**ックします**。匿名認証 が有効になっていることを確認します。

ステップ17:Windows認証を右クリックし、[Providers]を**選択します**。NT LAN Manager(NTLM)が リストの最初にあることを確認します。

ステップ18:レジストリ設定で認証チャレンジを無効にする。そうしないと、Simple Certificate Enrollment Protocol(SCEP)でチャレンジパスワード認証が必要になり、WLCではサポートされま せん。

ステップ19:regeditアプリケーションを開きます。

ステップ20:HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\に移動します。

ステップ21: EnforcePasswordを0に設定します。

đ			Re	gistry Editor		×
File	Edit	View Favorites Help				
		👂 🌗 Advanced INF 🔺	Name	Туре	Data	
		Þ- 퉲 ALG	ab (Default)	REG_SZ	(value not set)	
		🔒 AllUserinstallA	88 EnforcePassword	REG_DWORD	0x00000000 (0)	
		👂 🍌 Assistance 🦳				
		⊳- 🍌 AuthHost 🛛 😑				
		BestPractices				
		BidInterface				
		þ - 🍌 Chkdsk				
		р - 📙 СОМЗ				
		Command Prc		N		
		4 🎳 Cryptography		13		
		AutoEnroll				
		D - Calais				
		CatalogDB				
		CatDBTem				
		Defaults				
		A MSCEP				
		- CAType				
		Certsin				
		- Enforce				
<	1	III >				
Comp	outer\H	KEY_LOCAL_MACHINE\SOF	TWARE\Microsoft\Cryp	tography\MSCEP\I	EnforcePassword	Activate Wind

ステップ22:[Microsoft Windows/スタートメニュー]をクリックします。

ステップ23:MMCと入力します。

ステップ24:[ファイル]メニューで、[スナップインの追加と削除]を選択します。[Certification Authority]を選択します。

ステップ25:[証明書テンプレート]フォルダを右クリックし、[管理]をクリックします。

ステップ26:「ユーザー」などの既存のテンプレートを右クリックし、「テンプレートの複製」**を** 選択します。

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
	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	
	Reb Server	1	4.1	Activat
	Workstation Authentication	2	101.0	Client Authent
	1			

ステップ27:Microsoft Windows 2012 R2にするCAを選択します。

ステップ28: [General]タブで、WLCなどの表示名と有効期間を追加します。

ステップ29:[Subject Name]タブで、[Supply in the request]が選択されていることを確認します。

	Prop	erties	of New	Template		x
Superseded T	emplat	es	Ext	ensions	Secur	ity
Compatibility Gen	eral	Request	Handling	Cryptograph	y Key Atte	estation
Subject Name		Sen	ver	Issuance	Requirement	nts
• Supply in the r	equest					
Use subje	ct infor	mation fro	om existing	certificates fo	r autoenrolln	nent
irenewal re	quests					
O Build from this	Active	Directory	informativ	n		
Select this ontic	on to e	nforce co	nsistency	among subject	t names and	to
simplify certifica	te adm	ninistration	1.			
Subject <u>n</u> ame f	format:					
None					~	
Include e-m	ail nam	ne in subje	ect name			
	ormatio	n in alterr	nate subje	ct name:		
E-mail name	9					
DNS name						
User princip	al nam	ie (UPN)				
Service prin	icipal n	ame (SPI	N)			\mathbb{R}
						Ť
	OK		Cancel	Apply		lelo
	OIN		Jancer			ыр

ステップ30:[発行要件]タブ**をクリック**します。一般的な階層型CA環境では、発行ポリシーを空白 のままにしておくことを推奨します。

Supersec	perseded Template		Exte	Extensions Security	
Compatibility	General	Request	Handling	Cryptography Key Attesta	
Subject Name Server Issuance Requirements					Requirements
Require the following for enrollment:					
If you re	quire more	than one :	signature, a	utoenrollmen	t is not allowed.
Policy ty	pe required	in signatu	ire:		
					\sim
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 exis	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

ステップ31:[Extensions]タブ、[**Application Policies**]、[**Edit**]の順にクリックします。[Add] をクリ ックして、[Client Authentication] がアプリケーション ポリシーとして追加されていることを確認 します。[OK] をクリックします。

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

ステップ32:[セキュリティ]タブを**クリック**し、[**追加…]をクリックします。**.NDESサービスのイン ストールで定義されたSCEPサービスアカウントがテンプレートを完全に制御していることを確 認し、[**OK**]をクリック**します**。

Subject N	Sen	ver	Issuance	quirements						
Compatibility	General	Request	Handling	Cryptograph	ıy	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 User	rs)						
Enterprise Admins (LSC2012\Enterprise Admins)										
\searrow										
Add <u>R</u> emove										

ステップ33:Certification Authority GUIインターフェイスに戻ります。Certificate Templatesディレクトリを右**クリックします**。[New] [Certificate Template to Issue] に移動します。以前に設定したWLCテンプレートを選択し、[**OK**]をクリック**します。**

···· ····	ion nen rorones minori	, nop		-
(= 🔿 🖄				
sole Root		Enable Certificate Templates	× —	-
Certification / wlaaan201 Revoko Issued Pendir	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>	e enable on this Certification Authority. was recently created does not appear on this list, you may ne s been replicated to all domain controllers. ne organization may not be available to your CA. tificate Template Concepts.	ed to wait until ctions	-
Eailed	Name Rey Recovery Agent CCSP Response Signing RAS and IAS Server Router (Offline request) Smartcard Logon Smartcard User Trust List Signing User Signature Only	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		
	WLC Workstation Authentication	Client Authentication Secure Email, Encrypting File System Client Authentication	✓	
<		III		

ステップ34:[Computer] > [HKEY_LOCAL_MACHINE] > [SOFTWARE] > [Microsoft] >

[Cryptography] > [MSCEP]の下のレジストリ設定で、デフォルトのSCEPテンプレートを変更しま す。EncryptionTemplate、GeneralPurposeTemplate、およびSignatureTemplateキーをIPsec(オ フライン要求)から以前作成したWLCテンプレートに変更します。

đ						Re	egistry Edi	tor		_ _ X
<u>F</u> ile	Edit	<u>V</u> iew	F <u>a</u> vorite	es <u>H</u> elp						
		Þ-	📙 Advar	nced INF	^	Name	Туре	[Data	
		Þ-	📕 ALG			ab (Default)	REG_SZ	((value not set)	
			🗼 AllUse	erinstallA		EncryptionTem	REG_SZ	١	WLC	
		Þ-	🗼 Assist	ance		💩 GeneralPurpose	REG_SZ	١	WLC	
		Þ-	📕 Auth	lost	≡	al Signature Templat	e REG_SZ	١	WLC	
		₽-	BestPi	ractices						
		Þ-	BidInt	erface						
		Þ-	Chkds	sk						
		▶-	COM:	3						
		-	Com	nand Pro	9					
		4-	Crypto	ography						
				ItoEnroll						
				stale e DP						
				artificate						
				faults						
			A M	SCEP						
			1	CATvp						
				Certsin						
				Enforce						
				Passwo						
				UseSin	<u> </u>					
			- n ~	n	_					
				/						
Com	puter\H	IKEY_L	OCAL_M/	ACHINE	SOF	TWARE\Microsoft\Cryp	otography\N	ISCEP		Activate Wind

ステップ35:システムを再起動します。

WLC の設定

ステップ1:WLCで、[Security]メニューに移動します。[Certificates] > [LSC]をクリックします。

ステップ2:[Enable LSC on Controller]チェックボックスをオンにします。

ステップ3:Microsoft Windows Server 2012のURLを入力します。デフォルトでは、/certsrv/mscep/mscep.dllが付加さ**れます**。

ステップ4:「パラメータ」セクションに詳細を入力します。

ステップ5:変更を適用します。

Local Significant Certificates (LSC)

E-mail

Key Size

General	AP Provisioning		
Certificate	Туре	Status	í
CA		Present 🔽	
General			
Enable L	SC on Controller	\checkmark	
CA Server			
CA serve	r 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	
Organiza	tion	Cisco	
Departm	ent	R&D	

rmanchur@wlaaan.com

Apply

ステップ6:上のCA行の青い矢印をクリックし、[**Add**]を選択**します**。ステータスが[Not present]から[**present**]に変**更されるよ**うになっ**ています**。

2048

ステップ7:[AP provisioning]タブをクリックします。

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 AP Policies Password Policies Local EAP 	General AP Provis Enable Update Numbe	AP Pr sioning	ts to LSC (0 to 25	5) 3					
Priority Order									
 Certificate LSC SSC 	MAC Add	ress							
Access Control Lists									
Wireless Protection Policies									
Web Auth									
TrustSec SXP									
▶ Advanced									

ステップ8:[AP Provisioning]の下の[Enable]チェックボックスをオンにし、[Update]をクリッ**クし** ます。

ステップ9:アクセスポイントがリブートされていない場合は、リブートします。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アクセスポイントは、リブート後に再び参加し、[Wireless]メニューに証明書タイプとしてLSCが 表示されます。

	CISCO	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGENERT	COMMANDS	нер	FEEDBACK						
Wire	less	All APs												Entries	1 - 2 of 2	~
- A	scess Points I APs dote 802.15a/n 802.15b/g/n Duel-Band Radies	Current Fill	lar I APa		None 2		[Change Fil	er) (Clear Fiber)	1							
G	lobal Configuration	AR Name			lindel			AD III. T	-	Admin Status	Operational	Beet	AP Mode		Certificat	-
) A	lvanced esh	CAPISOLI-J	L.	AIR	CAP35011-8-K	9	cB:Pc:id:6e:a3:cd	0 d, 00 h	35 m 21 /	a Disabled	ROG	1	Local		LSC	-
R	Profiles	and a state of a			0011111-1-6		SC.12.12.72.22.04	00,001	G2 11 201		100	-	Cords.			
EI B	exConnect Groups ExConnect ACLs															
F 80	2.11a/n															
► 80	2.11b/g/n															
F M	edia Stream															
• 2	aplication Visibility ad Control															
6	suntry															
т	mers															
F N	stflow															
⊧ Q	15															
		<					-	0					-	ENG	6.41 DM	
+		2			ö.	e II	i 🔒 🛛 🕅	P				- 😼	Si 🕼	UK	12/16/2014	4

注:8.3.112以降、MIC APはLSCが有効になると一度にまったく参加できません。したがって、「LSCへの試行」カウント機能は限られた使用になります。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。