UCCE \ PCCE - Procédure pour obtenir et télécharger le - d'individu de Windows Server signé ou les serveurs de certificat d'Autorité de certification (CA) le 2008

Contenu

Introduction Conditions préalables Conditions requises Composants utilisés Configurer Étape 1. Générez le CSR du gestionnaire de l'Internet Information Services (IIS) Étape 2. Téléchargez le certificat signé CA au gestionnaire de l'Internet Information Services (IIS) Étape 3. Liez le certificat de CA signé au site Web par défaut Vérifier Dépanner Cisco relatif prennent en charge des discussions de la Communauté

Introduction

Ce document décrit comment configurer certificat Auto-signée ou d'Autorité de certification (CA) sur Unified Contact Center Enterprise (UCCE) Windows 2008 serveurs R2.

Conditions préalables

Exigences

Cisco recommande que vous ayez la connaissance du processus signé et Auto-signé de certificat.

Composants utilisés

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

- Windows 2008 R2
- UCCE 10.5(1)

Configurer

L'installation du certificat pour la transmission HTTPS sur le serveur de fenêtres est un processus en trois étapes

• Générez la demande de signature de certificat (CSR) du gestionnaire de l'Internet Information

Services (IIS)

- Téléchargez le certificat signé CA au gestionnaire de l'Internet Information Services (IIS)
- Liez le certificat de CA signé au site Web par défaut

Étape 1. Générez le CSR du gestionnaire de l'Internet Information Services (IIS)

1. Ouvrez une session à Windows, **Start > Run de** clic **> tous les programmes > outils d'administration > gestionnaire de l'Internet Information Services (IIS)**, suivant les indications de cette image. Ne sélectionnez pas la version 6 IIS si elle existe.

Active Directory Domains and Trusts Active Directory Module for Windows Po Active Directory Sites and Services Active Directory Users and Computers	
ADSI Edit	administrator
 Component Services Computer Management Data Sources (ODBC) 	Documents
Event Viewer Internet Information Services (IIS) 6.0 [Computer
Internet Information Services (IIS) Man	Network
Local Security Policy	Control Panel
Security Configuration Wizard	Devices and Printers
Services	Administrative Tools
Storage Explorer	Help and Support
🕘 Task Scheduler 📃 🗾	Run
 ■ Back 	Windows Security
Search programs and files	Log off

2. Dans le volet de fenêtre de connexions vers le gauche, sélectionnez le nom du serveur, suivant les indications de cette image.



3. Dans le volet de fenêtre du milieu, choisi **Certificats IIS > de serveur**. Double-cliquer sur des Certificats de serveur pour générer la fenêtre de certificat, suivant les indications de cette image.

Connections	Sin Ici	MWORK H	ome					
Start Page ICMWORK (ORA\administrator) Application Pools	Filter:		• 🗰 Go 🕞 👽	Show All G	iroup by: Area		▼ ■■ ▼	_
±	IIS							
	<u></u>	Ą			404	2		
	Authentication	n Compression	Default Document	Directory Browsing	Error Pages	Handler Mappings	HTTP Redirect	
	-		3			4		
	HTTP Respo	ISAPI and CGI Restrictions	ISAPI Filters	Logging	MIME Types	Modules	Output Caching	
	Sequest Filtering	Server Certificates	Worker Processes					

4. Sur le volet de droite, cliquez sur en fonction les **actions > créent la demande de certificat**, suivant les indications de cette image.

Ac	tions
	Import
	Create Certificate Request
	Complete Certificate Request
	Create Domain Certificate
	Create Self-Signed Certificate
?	Help
	Online Help

5. Pour se terminer la demande de certificat, entrez le nom, l'unité d'organisation, d'organisation, à ville/localité, l'état/province et le pays/région communs, suivant les indications de cette image.

Request Certificate		? ×
Distinguis	hed Name Properties	
Specify the required info as official names and the	ormation for the certificate. State/province and City/locality must be specified ay cannot contain abbreviations.	
Common name:		
Organization:		
Organizational unit:		
City/locality		
State/province:		
Country/region:	US	
	·	
	Previous Next Finish Cano	:el

6. Le clic à côté de modifient le cryptographique et longueur de bit de Sécurité, il est recommandé d'utiliser au moins 2048 pour une meilleure Sécurité, suivant les indications de cette image.

P	Cryptographic Service Provider Properties
Select a c determine However,	ryptographic service provider and a bit length. The bit length of the encryption key s the certificate's encryption strength. The greater the bit length, the stronger the security. a greater bit length may decrease performance.
Cryptogra	phic service provider:
Microsoft	RSA SChannel Cryptographic Provider
Bit length	

7. Sauvegardez la demande de certificat dans l'emplacement désiré qui sera enregistré comme format .TXT, suivant les indications de cette image.

8. Fournissez ce fichier à signer par l'équipe qui gère le CA interne ou la demande de service externe CA, suivant les indications de cette image.

Étape 2. Téléchargez le certificat signé CA au gestionnaire de l'Internet Information Services (IIS)

1. Login à Windows, **Start > Run de** clic **> tous les programmes > outils d'administration > gestionnaire de l'Internet Information Services (IIS),** suivant les indications de cette image. Ne sélectionnez pas la version 6 IIS si elle existe.

Active Directory Domains and Trusts Active Directory Module for Windows Po Active Directory Sites and Services Active Directory Users and Computers	
Z ADSI Edit	administrator
Somponent Services	Documents
Event Viewer	Computer
Internet Information Services (IIS) Man	Network
Local Security Policy	Control Panel
🚡 Security Configuration Wizard 📃	Devices and Printers
🔍 Services	Administrative Tools
Storage Explorer	Help and Support
🕑 Task Scheduler 🗾 🗾	Run
 ● Back 	Windows Security
Search programs and files	Log off

2. Dans le volet de fenêtre de connexions vers le gauche, sélectionnez le nom du serveur, suivant les indications de cette image.



3. Dans le volet de fenêtre du milieu, choisi Certificats IIS > de serveur. Double-cliquer sur des

Certificats de serveur pour générer la fenêtre de certificat, suivant les indications de cette image.



4. Sur le volet de droite, cliquez sur en fonction les **actions > demande complète de certificat**, suivant les indications de cette image.

Act	tions
	Import
	Create Certificate Request
	Complete Certificate Request
	Create Domain Certificate
	Create Self-Signed Certificate
?	Help
	Online Help

5. Avant cette étape, assurez-vous que le certificat signé est dans le format .CER et a été téléchargé au serveur local. Cliquez sur... le bouton pour parcourir le fichier .CER. À l'intérieur du nom amical, utilisez le FQDN du serveur, suivant les indications de cette image.

Complete C	ertificate Request	? ×
P	Specify Certificate Authority Response	
Complete authority's	a previously created certificate request by retrieving the file that contains the certificate s response.	
File name	containing the certification authority's response:	
Friendly n	ame:	

6. Cliquez sur OK pour télécharger le certificat. Si complet, confirmez le certificat apparaît maintenant dans la fenêtre de Certificats de serveur, suivant les indications de cette image.

Server Certificate	S age certificates that the Web ser	ver can use with Web sites con	figured for SSL.
Name A	Issued To	Issued By	Expir
Cisco ICM Diagnostic Framework	icmwork.	icmwork	6/30
Cisco ICM SSL Certificate	ICMWORK	ICMWORK	6/25
	A CONTRACTOR OF A CONTRACTOR A	InCommon RSA Server CA	6/2/2018 6:59

Étape 3. Liez le certificat de CA signé au site Web par défaut

1. Dans le gestionnaire IIS sous l'avion de fenêtre de connexions, la main gauche, cliquent sur en fonction le **<server_name> > les sites > le site Web de par défaut**, suivant les indications de cette image.



2. Sous le volet de fenêtre d'actions du côté droit, cliquez sur en fonction les attaches, suivant les indications de cette image.



3. À la fenêtre d'obligatoirex de site, cliquez sur en fonction les https pour mettre en valeur plus d'options. Cliquez sur en fonction Edit pour continuer, suivant les indications de cette image.

js				?
Host Name	Port 80	IP Address *	Binding 808:* * localho:	Add Edit Remove
	443		localho:	Browse
	Host Name	Host Name Port 80 443	Host Name Port IP Address 80 * 443	Host Name Port IP Address Binding 80 * 808:* * localhos localhos

4. Sous le paramètre de certificat ssl, cliquez sur en fonction vers le bas la flèche pour sélectionner le certificat signé téléchargé précédemment. Visualisez le certificat signé pour vérifier le chemin de certification et évaluez des correspondances le serveur local. Quand OK terminé de presse, puis près de sortie hors de la fenêtre d'obligatoirex de site, suivant les indications de cette image.

dit Site Binding		? ×
Type: https	IP address: All Unassigned	Port:
Host name:		
SSL certificate:		
Not selected	•	View
Cisco ICM SSL Certin Cisco ICM Diagnostic	cace Framework service certificate	Cancel

5. Redémarrez le service d'admin IIS sous les services MMC SNAP-dans par cliquer sur sur le **Start > Run > le services.msc.**, suivant les indications de cette image.

Help				
) 🗟 🛛 🖬 🕨 🖿	II I)			
Name 🔺	Description	Status	Startup Type	Log On As
Q Diagnostic Service	The Diagno		Manual	Local Service
🧛 Diagnostic System	The Diagno		Manual	Local System
🎑 Disk Defragmenter	Provides Di		Manual	Local System
🔍 Distributed Link Tra	Maintains li	Started	Automatic	Local System
Q Distributed Transac	Coordinate	Started	Automatic (D	Network S
Q DNS Client	The DNS Cl	Started	Automatic	Network S
Encrypting File Syst	Provides th		Manual	Local System
Extensible Authenti	The Extens		Manual	Local System
Runction Discovery	The FDPH		Manual	Local Service
Runction Discovery	Publishes t		Manual	Local Service
Group Policy Client	The servic	Started	Automatic	Local System
Realth Key and Cer	Provides X		Manual	Local System
O-Human Interface D	Enables de		Manual	Local System
IIS Admin Service	Enables thi	Charl	natic	Local System
SA IKE and AuthIP IPs.	The IKEEX		hatic	Local System

6. Si réussi, le navigateur Web de client ne devrait inciter aucun avertissement d'erreur de certificat en entrant dans l'URL FQDN pour le site Web.

Note: Si le service d'admin IIS manque à reprise le service d'édition de World Wide Web.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépanner

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