Configurazione del supporto HTTPS per l'integrazione ISE SCEP

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Configurazione Configurazione certificato server NDES Configurazione binding IIS NDES Server Configurazione server ISE Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene descritto come configurare il supporto HTTPS (Hypertext Transfer Protocol Secure) per l'integrazione SCEP (Secure Certificate Enrollment Protocol) con ISE (Identity Services Engine).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base del server Web Microsoft Internet Information Services (IIS)
- Esperienza nella configurazione di SCEP e certificati su ISE

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

• ISE release 11.1.x

 Windows Server 2008 R2 Enterprise con aggiornamenti rapidi per <u>KB2483564</u> e <u>KB2633200</u> installati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Le informazioni relative ai servizi certificati Microsoft sono fornite come guida specifica per Cisco Bring Your Own Device (BYOD). Per informazioni dettagliate sulle configurazioni dei server relative a Microsoft, NDES (Network Device Enrollment Service) e SCEP, vedere il sito Web TechNet di Microsoft.

Premesse

In una distribuzione BYOD, uno dei componenti principali è un server Microsoft 2008 R2 Enterprise con il ruolo NDES installato. Il server è un membro della foresta di Active Directory (AD). Durante l'installazione iniziale di NDES, il server Web IIS di Microsoft viene installato e configurato automaticamente per supportare la terminazione HTTP di SCEP. In alcune implementazioni BYOD, i clienti potrebbero voler proteggere ulteriormente le comunicazioni tra ISE e NDES utilizzando HTTPS. In questa procedura vengono descritti in dettaglio i passaggi necessari per richiedere e installare un certificato SSL (Secure Sockets Layer) per il sito Web SCEP.

Configurazione

Configurazione certificato server NDES

Nota: È necessario configurare un nuovo certificato per IIS (richiesto solo quando IIS è integrato con una PKI di terze parti, ad esempio Verisign o quando i ruoli dell'Autorità di certificazione (CA) e del server NDES sono separati in server separati). Durante l'installazione, se il ruolo NDES si trova su un server CA Microsoft corrente, IIS utilizza il certificato di identità del server creato durante l'installazione della CA. Per configurazioni autonome come questa, passare direttamente alla sezione **Configurazione binding IIS di NDES Server** in questo documento.

- 1. Connettersi al server NDES tramite console o RDP.
- 2. Fare clic su Start -> Strumenti di amministrazione -> Gestione Internet Information Services (IIS).
- 3. Evidenziare il nome del server IIS e fare clic sull'icona Certificati server.



4. Fare clic su Crea richiesta certificato e completare i campi.

-	To be and the formation of the States and							
	Internet Information Services (IIS) Planager							
	WIN-BGFEV37D5GM +	Q Q 10 × WIN-66FEV37DS6M →						
	Connections Connections Connections Connections Connections Connections Connections Connectio	Serve Use this feature to configured for SSR Name A IISCERT t Certificate Distinguisher	er Certificate	PS hage certificates that the Web server Issued To WIN-86FEVJ7D56M.bn-lab.local bn-lab.WIN-86FEVJ7D56M.bn-lab.local WIN-86FEVJ7D56M.bn-lab.local wrties	can use with Web sites Issued By bn-lab-WIDH-86FEV37D59M-CA bn-lab-WIDH-86FEV37D59M-CA bn-lab-WIDH-86FEV37D59M-CA Ph-lab-WIDH-86FEV37D59M-CA	Actions Import Create Certificate Request Conplete Certificate Request Create Domain Certificate Create Self-Signed Certificate Vew Xennove Help Online Help Online Help		
	Spec as of Orga Orga Oty/ State Court	fy the required informa ficial names and they ca non names nizations nizational unit: locality l/province: try/regions	tion for the certifi annot contain abb Dn-lab-WIN-ĐG Cisco Dn-lab Montreal QC CA	cate. State.jprovince and City,locality reviations. SFEV17D56M-CA	must be specified			
1				Previous. Next	Frish Cancel			

equest Certif	cate					?	X
a 1	le Name						
Specify the file name for the certificate request. This information can be sent to a certification authority for signing.							
Specify a file	name for the c	ertificate reques	t:				
			Previous	Next	Finish	Cancel	

5. Aprire il file con estensione cer creato nel passaggio precedente con un editor di testo e copiare il contenuto negli Appunti.



6. Accedere al sito Web di registrazione della CA Microsoft e fare clic su **Richiedi certificato**.URL di esempio: http://yourCAIP/certsrv

C Hicrosoft Active Directory Certificate Services - Windows Internet Explorer						
C C = 0 http://10.85.137.156/certarv/						
👷 Pavorites 🔹 🏚 Suggested Sites 🔹 🔊 Web Site Callery 🔹						
6 Microsoft Active Directory Certificate Services						
IR annual Antin Diseases And State Contains - Inclusive DECONDECT AN						
ancrosok nowe birectory certificate services — binabinimited Evaluation						
Welcome						
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communic upon the type of certificate you request, perform other security tasks.						
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending method.						
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.						

Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

7. Fare clic su **Invia una richiesta di certificato utilizzando...** Incollare il contenuto del certificato dagli Appunti e scegliere il modello **Server Web**.

Microsoft Active Directory Certificate Services bn-lab-WIN-B6HEVJ/D56M-CA	
Advanced Certificate Request	
The policy of the CA determines the types of certificates you can request. Click one of the following options to:	
Create and submit a request to this CA.	
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by	using a base-64-encoded PKCS #7 file.
12	

8. Fare clic su Invia, quindi salvare il file del certificato sul desktop.

Microsoft Active Directory Certificate Services -- bn-lab-WIN-B6FEVJ7D56M-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate requ

Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	AgIAgDALBglghkgBZQMEASowCwYJYIZIAWUDBAEt hkgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcw dDrCREpo8/D/seatMA0GCSqGSIb3DQEBBQUAA4GB xpITWbkjxbmrOT+q3rcI0jLNQireDB57Has8WdgC +EthsI0YgtdL51gNJb35qAjLTCyDfNzEvP2P1FQN +F80YwPo6CWPj3PWiz2y	
Certificate Temp	ate: Web Server	
Additional Attribu	ites:	
Attributes:	× • •	
	Submit >	A

9. Tornare al server NDES e aprire l'utilità Gestione IIS. Per importare il certificato server appena creato, fare clic sul nome del server e quindi su **Completa richiesta certificato**.



Configurazione binding IIS NDES Server

- 1. Espandere il nome del server, Siti, quindi fare clic su Sito Web predefinito.
- 2. Fare clic su Binding nell'angolo superiore destro.
- 3. Fare clic su **Add** (Aggiungi), impostare Type (Tipo) su HTTPS e scegliere il certificato dall'elenco a discesa.
- 4. Fare clic su OK.

enclines		Actions
excloses Seri-Tape 1989-1990(705091 (BH-LASI)administrator) Series Series Series District web Series District web Series Provide Seri	Pefault Web Site Home Her Image: Constraint Compression AD Authentication Compression Output Default Modules Output Output Request Modules Output Configuration SD. Entropy Maggeresent SD. Entropy Configuration SD. Entropy Maggeresent SD. Entropy Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configurat	Actions Depice Edit Sec Back Setings Back Setings Back Setings Here Applications Here Applic
	Type: P address: Parts Feb:s Add Unassigned W Feb:s Add Unassigned W SR. certification: V Foot selected W Vite-cord V Vite-cord Cancel Ext selected Cancel	54

x 5 2

Configurazione server ISE

1. Connettersi all'interfaccia di registrazione Web del server CA e scaricare la catena di certificati CA.

G Hicrosoft Active Directory Certificate Services - Windows Internet Explorer						
👷 Pavorites 🛛 🎪 😰 Suggested Sites 👻 🖉 Web Sice Gallery 🔹						
S Microsoft Active Directory Certificate Services						
Microsoft Active Directory Certificate Services - bn-lab-WIN-B6FEVJ7D56M-CA						
Welcome						
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communic upon the type of certificate you request, perform other security tasks.						
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending r						
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.						

Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

 Dalla GUI di ISE, selezionare Administration > Certificates > Certificate Store (Amministrazione > Certificati > Archivio certificati), quindi importare la catena di certificati CA nell'archivio ISE.



3. Passare a Amministrazione -> Certificati -> Profili CA SCEP e configurare l'URL per HTTPS. Fare clic su Test connettività e quindi su Salva.

CISCO Identity Services Engine			
🛕 Home Operations * Policy * Admit	nistration 🔻		
🔆 System 🕂 Identity Management 🔛	Nebwork Resources 🛛 🛃 Web Portal Mana	agement	
Deployment Licensing Certificates Loggi	ing Maintenance Admin Access Sr	iettings	
Certificate Operations	SCEP Certificate Authority Certificates > BN_LAB_1 Edit Profile	SCEP_SSL	
Certificate Signing Requests	SCEP Certificate Authority		_
Certificate Store	* Name	BN_LAB_SCEP_SSL	
SCEP CA Profiles	Description		
OCSP Services	* URL	https://10.85.137.156/certsrv/mscep/	Test Connectivity
Certificate Request Agent Certifica		WIN-B6FEVJ7D56M-MSCEP-RA	
	Save Reset		

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

- Passare a Amministrazione -> Certificati -> Archivio certificati e verificare che la catena di certificati CA e il certificato RA (Registration Authority) del server NDES siano presenti.
- Usare Wireshark o TCP Dump per monitorare lo scambio SSL iniziale tra il nodo di amministrazione ISE e il server NDES.

Lo <u>strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi</u> **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

- Suddividere la topologia di rete BYOD in punti di riferimento logici per identificare i punti di debug e di acquisizione sul percorso tra questi endpoint, ISE, NDES e CA.
- Verificare che TCP 443 sia consentito in modo bidirezionale tra ISE e il server NDES.
- Monitorare i registri delle applicazioni server CA e NDES per individuare eventuali errori di registrazione e utilizzare Google o TechNet per ricercarli.
- Usare l'utility TCP Dump sul PSN ISE e monitorare il traffico da e verso il server NDES. È disponibile in Operazioni > Strumenti diagnostici > Strumenti generali.
- Installare Wireshark sul server NDES o usare SPAN sugli switch intermedi per acquisire il traffico SCEP da e verso il PSN su ISE.

Lo <u>strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi</u> **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> prima di usare i comandi di **debug**.

Informazioni correlate

- <u>Configurazione del supporto SCEP per BYOD</u>
- Documentazione e supporto tecnico Cisco Systems