Konfigurieren der HTTPS-Unterstützung für ISE SCEP-Integration

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren NDES-Serverzertifikatkonfiguration IIS-Bindungskonfiguration des NDES-Servers ISE-Serverkonfiguration Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument werden die Schritte beschrieben, die zur Konfiguration der Hypertext Transfer Protocol Secure (HTTPS)-Unterstützung für die Integration des Secure Certificate Enrollment Protocol (SCEP) in die Identity Services Engine (ISE) erforderlich sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse des Internetinformationsdienste-Webservers (IIS) von Microsoft
- Erfahrung in der Konfiguration von SCEP und Zertifikaten auf ISE

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

ISE Version 1.1.x

• Windows Server 2008 R2 Enterprise mit Hotfixen für installierte <u>KB2483564</u> und <u>KB2633200</u> Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Die Informationen zu Microsoft-Zertifikatsdiensten werden als Leitfaden speziell für Cisco Bring Your Own Device (BYOD) bereitgestellt. Weitere Informationen finden Sie im Microsoft TechNet als Quelle der Wahrheit für Microsoft-Zertifizierungsstellen, Network Device Enrollment Service (NDES) und SCEP-bezogene Serverkonfigurationen.

Hintergrundinformationen

Bei einer BYOD-Bereitstellung ist eine der Kernkomponenten ein Microsoft 2008 R2 Enterprise-Server, auf dem die NDES-Rolle installiert ist. Dieser Server ist Teil des Active Directory-Waldes (AD). Während der Erstinstallation von NDES wird der IIS-Webserver von Microsoft automatisch installiert und konfiguriert, um die HTTP-Beendigung des SCEP zu unterstützen. In einigen BYOD-Bereitstellungen möchten Kunden möglicherweise die Kommunikation zwischen ISE und NDES mithilfe von HTTPS weiter sichern. In diesem Verfahren werden die erforderlichen Schritte zum Anfordern und Installieren eines SSL-Zertifikats (Secure Socket Layer) für die SCEP-Website beschrieben.

Konfigurieren

NDES-Serverzertifikatkonfiguration

Hinweis: Sie müssen ein neues Zertifikat für IIS konfigurieren (nur erforderlich, wenn IIS in eine PKI eines Drittanbieters wie Verisign integriert ist oder wenn die CA- und NDES-Serverrollen auf separate Server aufgeteilt werden). Wenn sich die NDES-Rolle bei der Installation auf einem aktuellen Microsoft CA-Server befindet, verwendet IIS das beim Einrichten der CA erstellte Serveridentitätszertifikat. Bei Standalone-Konfigurationen wie diesen können Sie direkt zum Abschnitt NDES-Server IIS Binding Configuration in diesem Dokument wechseln.

- 1. Herstellen einer Verbindung zum NDES-Server über Konsole oder RDP.
- 2. Klicken Sie auf Start -> Verwaltung -> Internetinformationsdienste (IIS)-Manager.
- 3. Markieren Sie den IIS-Servernamen, und klicken Sie auf das Symbol Serverzertifikate.



4. Klicken Sie auf Zertifikatsanforderung erstellen, und füllen Sie die Felder aus.

Ī	Internet Information Services (IIS) Manager		
	(3) (1) WIN-BOFEV37DSOM >		😐 🖂 🔂 I 🔒 •
	Connections Connections Start Page Connection Page Co	Server Certificates Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL. Name ^ Issued To Issued By WID+66FEV37D56M-bn-lab.local bn-lab-WID+66FEV37D56M-CA bn-lab-WID+66FEV37D56M-bn-lab.local bn-lab-WID+66FEV37D56M-CA IISCERT WID+66FEV37D56M-bn-lab.local bn-lab-WID+66FEV37D56M-CA	Actions Import Create Certificate Request Conplete Certificate Request Create Domain Certificate Create Self-Signed Certificate View Xemove
•		Distinguished Name Properties Of the required information for the certificate. State/province and City/locality must be specified efficial names and they cannot contain abbreviations. entry in the required information for the certificate. State/province and City/locality must be specified efficial names and they cannot contain abbreviations. entry in the information for the certificate. State/province and City/locality must be specified efficial names and they cannot contain abbreviations. entry in the information in the certificate. State/province and City/locality must be specified efficial names and they cannot contain abbreviations. entry integration Classical contained in the certificate. garizational unit: pn-lab ty/locality Montreal ats/province: QC unitry/region: CA	Heb Orine Heb
l			
		Previous Next Pinish Cancel	

equest Certifica	te						? :
File	Name						
Specify the file n authority for sign	ame for the certining.	ficate reque	st. This informa	ation can be	e sent to a	certification	
Specify a file nam	te for the certific	ate request:					
			Previous	Nex	đ	Finish	Cancel

5. Öffnen Sie die im vorherigen Schritt erstellte Cer-Datei mit einem Texteditor, und kopieren Sie den Inhalt in die Zwischenablage.



6. Rufen Sie die Microsoft CA Web Enrollment-Website auf, und klicken Sie auf **Zertifikat anfordern**.Beispiel-URL: http://yourCAIP/certsrv

Hicrosoft Active Directory Certificate Services - Windows Internet Explorer					
(> < 10) + 10.85, 137.156/certary/					
👷 Pavorites 🔹 🏚 Suggested Sites 👻 🙋 Web Sice Gallery 🗝					
Horosoft Active Directory Certificate Services					
Microsoft Active Directory Certificate Services bri-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 re					

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. Klicken Sie auf **Zertifikatsanforderung senden mit...** Fügen Sie den Zertifikatsinhalt aus der Zwischenablage ein, und wählen Sie die **Webserver-**Vorlage aus.

Microsoft Active Directory Certificate Services bn-lab-WIN-B6FEVJ7D56M-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 CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base	oded PKCS #7 file.

8. Klicken Sie auf Senden, und speichern Sie die Zertifikatsdatei auf dem 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+q3rcIOjLNQireDB57Has8WdgC +EthsI0YgtdL51gNJb35qAjLTCyDfNzEvP2P1FQN +F80YwPo6CWPj3PWiz2y			
Certificate Temp	ate: Web Server			
Additional Attribu	ites:			
Attributes:	× V V			
	Submit >	La Car		

9. Kehren Sie zum NDES-Server zurück, und öffnen Sie das IIS-Manager-Dienstprogramm. Klicken Sie auf den Servernamen und anschließend auf **Zertifikatsanforderung abschließen**, um das neu erstellte Serverzertifikat zu importieren.



IIS-Bindungskonfiguration des NDES-Servers

- 1. Erweitern Sie den Servernamen, erweitern Sie Sites, und klicken Sie auf Standardwebsite.
- 2. Klicken Sie in der rechten oberen Ecke auf **Bindungen**.
- 3. Klicken Sie auf **Hinzufügen**, ändern Sie den Typ in HTTPS, und wählen Sie das Zertifikat aus der Dropdown-Liste aus.

5 3

4. Klicken Sie auf OK.

ections	C De bille Contra	Actions
Dant hoge Una thoge Win 6075/UTO509 (SN-LA32/pdministrator) Application Pools Sola Default lineb Sta	Default Web Site Home Him Image: Configuration ADP Based	Defore Edit Termission Edit Stic Dedings Texis Settings Texis Settings Texis Settings Texis Settings Texis Settings Sape Texase Web Stic Texase Texase Web Stic Texase Texase Web Stic Texase Texase Stic Texase Web Stic Texase Texase Stic Texase Stic Texase Texase Texase Stic Texase Texase Texase Stic Texase Stic
	Add Site Backey Pros Pactor Pactor Pactor Pactor Pactor Pactor Pactor	Innto- Proto Online Help

ISE-Serverkonfiguration

1. Stellen Sie eine Verbindung zur Web Enrollment-Schnittstelle des CA-Servers her, und laden Sie die Zertifizierungsstellenkette herunter.

C Microsoft Active Directory Certificate Services - Windows Internet Explorer
🔆 🕑 🗢 🔊 http://10.85.137.156/certarv/
👷 Pavorites 🛛 🎪 🔊 Suggested Sites 🔹 🖉 Web Sice Gallery 🔹
6 Microsoft Active Directory Certificate Services
Microsoft Active Directory Certificate Services — bri-lab-WIN-B6FEVU7D58M-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 re-

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

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

2. Navigieren Sie in der ISE-GUI zu Administration -> Certificates -> Certificate Store, und importieren Sie die Zertifizierungsstellenkette der Zertifizierungsstelle in den ISE-Store.

CISCO Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻	Administration 🔻
🔆 System 🔮 Identity Management	Network Resources 🛃 Web Portal Management
Deployment Licensing Certificates	Logging Maintenance Admin Access Settings
Certificate Operations	Certificate Store
Certificate Signing Requests	✓ Edit Import Export X Delete
SCEP CA Profiles	BN-LAB-vISE1.BN-LAB.local#BN-LAB-vISE1.BN-LAB.
Services	bn-lab-WIN-B6FEVJ7D56M-CA#bn-lab-WIN-B6FEVJ

3. Navigieren Sie zu **Administration -> Certificates -> SCEP CA Profiles**, und konfigurieren Sie den URL für HTTPS. Klicken Sie auf **Verbindung testen** und dann auf **Speichern**.

A Hore Destrict a Dalloy a Ma	valdediae v		
nome operations + Policy + Adn	unioradon •		
🔆 System 🔁 Identity Management	Network Resources 4 Web Portal Man	agement	
Deployment Licensing Certificates Log	ging Maintenance Admin Access S	iettings	
Certificate Operations	SCEP Certificate Authority Certificates > BN_LAB_	SCEP_SSL	
Local Certificates	Edit Profile		
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 Certificate	WIN-B6FEVJ7D56M-MSCEP-RA	
	Paul Beest		
	Save Neper		

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

• Navigieren Sie zu Administration -> Certificates -> Certificate Store, und überprüfen Sie, ob

die Zertifizierungsstellenkette der Zertifizierungsstelle und das Zertifikat der NDES Server Registration Authority (RA) vorhanden sind.

• Verwenden Sie Wireshark oder TCP Dump, um den ersten SSL-Austausch zwischen dem ISE-Admin-Knoten und dem NDES-Server zu überwachen.

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

- Unterteilen Sie die BYOD-Netzwerktopologie in logische Wegpunkte, um Debug- und Erfassungspunkte entlang des Pfads zwischen diesen Endpunkten ISE, NDES und CA zu identifizieren.
- Stellen Sie sicher, dass TCP 443 bidirektional zwischen der ISE und dem NDES-Server zugelassen ist.
- Überwachen Sie die CA- und NDES-Serveranwendungsprotokolle auf Registrierungsfehler, und verwenden Sie Google oder TechNet, um diese Fehler zu untersuchen.
- Verwenden Sie das TCP-Dump-Dienstprogramm auf dem ISE-PSN, und überwachen Sie den Datenverkehr zum und vom NDES-Server. Diese finden Sie unter Operations > Diagnostic Tools > General Tools.
- Installieren Sie Wireshark auf dem NDES-Server, oder verwenden Sie SPAN auf zwischengeschalteten Switches, um SCEP-Datenverkehr vom und zum ISE-PSN zu erfassen.

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Hinweis: Bevor Sie **Debug-**Befehle verwenden, lesen Sie die <u>wichtigen Informationen zu</u> <u>Debug-Befehlen</u>.

Zugehörige Informationen

- Konfigurieren der SCEP-Unterstützung für BYOD
- <u>Technischer Support und Dokumentation Cisco Systems</u>