ISE SCEP لماكتل HTTPS معد نيوكت

المحتويات

<u>المقدمة</u> <u>المتطلبات الأساسية</u> <u>المكونات المستخدمة</u> <u>معلومات أساسية</u> <u>التكوين</u> <u>تكوين شهادة خادم NDES Server IIS</u> <u>تكوين زبط NDES Server IIS</u> <u>تكوين خادم ISE</u> <u>التحقق من الصحة</u> <u>استكشاف الأخطاء وإصلاحها</u> <u>معلومات ذات صلة</u>

المقدمة

يصف هذا المستند الخطوات المطلوبة لتكوين دعم بروتوكول نقل النص التشعبي الآمن (HTTPS) لتكامل بروتوكول تسجيل الشهادة الآمن (SCEP) مع محرك خدمات الهوية (ISE).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بخادم ويب لخدمات معلومات الإنترنت (IIS) من Microsoft
 - الخبرة في تكوين SCEP والشهادات على ISE

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

• ISE الإصدار x.1.1

• Windows Server 2008 R2 Enterprise مع تثبيت الإصلاحات العاجلة ل <u>KB2483564</u> و<u>KB2633200</u> وWindows Server 2008 R2 Enterprise تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر. يتم توفير المعلومات المتعلقة بخدمات شهادات Microsoft كدليل خاص ب Cisco Bring your your device BYOD)). ارجع إلى TechNet من Microsoft كمصدر نهائي للحقيقة الخاصة بهيئة شهادة Microsoft وخدمة تسجيل أجهزة الشبكة (NDES) وتكوينات الخوادم ذات الصلة SCEP.

معلومات أساسية

في نشر BYOD، يكون أحد المكونات الأساسية هو خادم Microsoft 2008 R2 Enterprise المثبت عليه دور NDES. هذا الخادم عضو في غابة Active Directory (AD). أثناء التثبيت الأولي ل NDES، يتم تثبيت خادم ويب IIS الخاص ب Microsoft وتكوينه تلقائيا لدعم إنهاء HTTP ل SCEP. في بعض عمليات نشر BYOD، قد يرغب العملاء في زيادة تأمين الاتصالات بين ISE و NDES باستخدام HTTPS. يوضح هذا الإجراء بالتفصيل الخطوات المطلوبة لطلب شهادة طبقة مأخذ التوصيل الآمنة (SSL) وتثبيتها لموقع SCEP على الويب.

التكوين

تكوين شهادة خادم NDES

ملاحظة: يجب تكوين شهادة جديدة ل IIS (مطلوبة فقط عندما يتم دمج IIS مع PKI خاص بجهة خارجية مثل Verisign أو عندما يتم فصل أدوار خادم مرجع التصديق (CA) و NDES على خوادم منفصلة). في التثبيت، إذا كان دور NDES على خادم Microsoft CA حالي، يستخدم IIS شهادة هوية الخادم التي تم إنشاؤها أثناء إعداد CA. بالنسبة للتكوينات المستقلة مثل هذا، قم بالتخطي مباشرة إلى قسم **تكوين ربط NDES Serve** في هذا المستند.

- 1. الاتصال بخادم NDES عبر وحدة التحكم أو RDP.
- انقر على بدء -> أدوات إدارية -> إدارة خدمات معلومات الإنترنت (IIS).
 - 3. قم بتمييز اسم خادم IIS وانقر على أيقونة **شهادات الخادم**.

emet Information Services (IIS) Manager												a = 9
exections State Tage Application Pode State State State State Configure	win-B6FEVJ	7D56M Hon Million Congression Congression Congression Cathory Saved	Show Al Q Default Document Request Filtering	Directory Brooding Server Certificates	Error Pages Vooker Processes	Faled Reset	Harder Happings	HTTP Redrect	HTTP Respo	EAPT and GEI Restrictions	Loggra	Actoos Hanage Server Restert b Start Stop Ver Application Prob Ver Stos P Indp Coline Help

4. انقر على **إنشاء طلب شهادة**، وأكمل الحقول.

Internet Information Services (IIS) Manager				
(3) (1) + WIN-86FEV37D56M →				10 × 10 •
Connections	Conve	r Castificator		Actions
Q,• 🔒 2 8.	Serve	r Certificates		Import
HIN-BOPEV17D56M (DN-LAD2/administrator)	Use this feature to configured for SS	request and manage certificates that the Web server o	an use with Web sites	Create Certificate Request
□ Application Pools □ 0 Sites	Name +	Issued To	Issued By	Create Domain Certificate
E 🔮 Default Web Site		bn-lab-WIN-86FEV37056M-bn-lab.local bn-lab-WIN-86FEV37056M-CA	bn-lab-WIN-86FEVJ7D56M-CA bn-lab-WIN-86FEVJ7D56M-CA	Create Self-Signed Certificate
	IISCERT	WIN-86FEV37D56M.bn-lab.local	bn-lab-WIIN-86FEV37D56M-CA	Vew
R	squest Certificate		2 X	P Help
	Distinguished	I Name Properties		Online Help
	Specify the required informal as official names and they ca	ion for the certificate. State, province and City/locality monot contain abbreviations.	ust be specified	
	Common name:	ho-lah-WIN-REEV17DSEM-CA	_	
'	Organization:	Cisco	_	
	Organizational unit:	bn-lab		
	City/locality	Montreal		
	Country/region:	loc CA	-	
		-		
			ย	
		Previous Next /	with Cancel	
Request Certifica	te			? ×
(common)				
File	Name			
Lee by				
Specify the file n	ame for the certific	ate request. This information can be	sent to a certification	
authority for sign	ing.			
Specify a file nam	e for the certificat	e request:		
newcert.cer				
,				
		President	t Ench	1 canal

5. افتح ملف .cer الذي تم إنشاؤه في الخطوة السابقة باستخدام محرر نصي وانسخ المحتوى إلى الحافظة.



6. قم بالوصول إلى موقع ويب تسجيل Microsoft CA على الويب وانقر فوق **طلب شهادة**.مثال على :URL http://yourCAIP/certsrv

Controsont Active Directory Certificate Services - Hilloows Directory
3 + 1 http://10.85.137.156/certarv/
👷 Favorites 🙀 🔊 Suggested Sites * 🖉 Web Sice Gallery *
Hicrosoft 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 re

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

Select a task:

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

7. انقر على **إرسال طلب شهادة باستخدام..**.. الصق في محتوى الشهادة من الحافظة، واختر قالب **خادم الويب**.

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 PKCS #7 file,

6

8. انقر على **إرسال** ثم احفظ ملف الشهادة على سطح المكتب.

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:

			_
	AgIAgDALBglghkgBZOMEASowC	WYJYIZIAWUDBAEt	
Base-64-encoded	hkgBZOMEAOUwBwYFKw4DAgcw0	GYIKoZIhvcNAwcw	
certificate request	dDrCREpo8/D/seatMA0GCSgGS	Ib3DOEBBOUAA4GB	
(CMC or	xpITWbkjxbmr0T+g3rcI0jLN0	ireDB57Has8WdgC	
PKCS #10 or	+EthsI0YgtdL51gNJb35gAjLT	CyDfNzEvP2P1FQN-	_
PKCS #7):	+F80YwPo6CWPj3PWiz2y	-	,
-	4		

Certificate Tem	olate:		
	Web Server		
Additional Attrib	utes:		
Attributes	्	A V	
		Submit	>

9. ارجع إلى خادم NDES وافتح وحدة إدارة IIS. انقر على اسم الخادم ثم انقر على **إكمال طلب الشهادة** لاستيراد شهادة الخادم التي تم إنشاؤها حديثا.

Internet Information Services (IIS) Manager					
				😐 🖂 🔂 I 🗑 -	
Connections Q, • I	Server Certificates Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.			Actions Import Create Certificate Request Complete Certificate Request	
E- a Sites ⊛-	Name A	Issued To WIN-86FEVJ7D56M.bn-lab.local bn-lab-WIN-86FEVJ7D56M-CA	Issued By bn-lab-WDN-86FEV37D56M-CA bn-lab-WDN-86FEV37D56M-CA	Create Domain Certificate Create Self-Signed Certificate	
	IISCERT	WIN-86FEV37D56M.bn-lab.local	bn-lab-WIN-86FEV37D56M-CA	Vew	

تكوين ربط NDES Server IIS

- 1. قم بتوسيع **اسم الخادم**، وتوسيع **المواقع**، وانقر فوق **موقع ويب الافتراضي**.
 - 2. انقر فوق **روابط** في الزاوية العلوية اليمنى.

R

- 3. انقر فوق **إضافة**، وقم بتغيير TypeTo HTTPS، واختر الشهادة من القائمة المنسدلة.
 - 4. وانقر فوق **OK**.

		1915
Internet Information Services (III) Hanager	fadt Vieb Ster ►	100 × 51 10 •
Connections Con	Default Web Site Home Immediate Site Address in Site Address	Actions Diplore Edit Termission Edit Termission Basic Settings Termission Termission Termission Termission Termission Termission Termission Termission Statut Statut Statut Statut Statut Statut Statut Statut Statut Termission Termission </th

تکوین خادم ISE

1. قم بالاتصال بواجهة تسجيل الويب لخادم CA وقم بتنزيل سلسلة شهادات CA.

FIRITION RATE DECEMPTERMENT AND A DECEMPTER CAPACITY
O → [a] http://10.85.137.156/certarv/
👷 Favorites 🔥 😰 Suggested Sites 🔹 🍘 Web Sice Gallery 🔹
₩ Korosoft Active Directory Certificate Services
Microsoft Active Directory Certificate Services - In-Jab 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

2. من واجهة المستخدم الرسومية ISE، انتقل إلى **الإدارة -> الشهادات -> مخزن الشهادات** واستورد سلسلة شهادات CA إلى مخزن ISE.

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
🔹 Local Certificates	
👰 Certificate Signing Requests	Cur Tribor Schort Colece
💇 Certificate Store	Friendly Name
SCEP CA Profiles	BN-LAB-vISE1.BN-LAB.local#BN-LAB-vISE1.BN-LAB.
OCSP Services	WIN-B6FEVJ7D56M-MSCEP-RA#bn-lab-WIN-B6FEVJ
	bn-lab-WIN-B6FEVJ7D56M-CA#bn-lab-WIN-B6FEVJ.

3. انتقل إلى **الإدارة -> الشهادات -> توصيفات SCEP CA** وقم بتكوين عنوان URL ل HTTPS. انقر على **إختبار الاتصال** ثم انقر على **حفظ**.

CISCO Identity Services Engine			
🛕 Home Operations 🔻 Policy 🔻 Admir	histration 🔻		
🔆 System 🔮 Identity Management 🔛	Network Resources 🔄 Web Portal Mana	agamant	
Deployment Licensing Certificates Loggi	ng Maintenance Admin Access S	ettings	
Certificate Operations	SCEP Certificate Authority Certificates > BN_LAB_ Edit Profile SCEP Certificate Authority	SCEP_SSL	
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	
	Save Reset		

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

- انتقل إلى **الإدارة -> الشهادات ->** مخزن **الشهادات** وتحقق من وجود سلسلة شهادات CA وشهادة هيئة تسجيل خوادم NDES (RA).
 - أستخدم Wireshark أو تفريغ TCP لمراقبة تبادل SSL الأولي بين عقدة مسؤول ISE وخادم NDES.

<u>تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر</u> show. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر show.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- قم بتقسيم مخطط شبكة BYOD إلى نقاط طريق منطقية للمساعدة في تحديد نقاط تصحيح الأخطاء والامساك على طول المسار بين نقاط النهاية هذه - ISE و NDES و CA.
 - تأكد من السماح ل TCP 443 بشكل ثنائي الإتجاه بين ISE وخادم NDES.

- راقب سجلات تطبيقات خادم CA و NDES لأخطاء التسجيل واستخدم Google أو TechNet للبحث عن تلك الأخطاء.
- أستخدم الأداة المساعدة لتفريغ TCP على ISE PSN وأداة مراقبة حركة مرور البيانات من وإلى خادم NDES. ويوجد هذا ضمن **العمليات > أدوات التشخيص > الأدوات العامة**.
 - ركبت Wireshark على ال NDES نادل أو استعملت فسحة بين دعامتين على وسيط مفتاح in order to على قبض SCEP حركة مرور إلى ومن ال ISE PSN.

<u>تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر</u> show. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر show.

ملاحظة: ارجع إلى <u>معلومات مهمة حول أوامر التصحيح</u> قبل إستخدام أوامر debug.

معلومات ذات صلة

- <u>تكوين دعم SCEP ل BYOD</u>
- <u>الدعم التقني والمستندات Cisco Systems</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما