配置ISE SCEP集成的HTTPS支持

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u> 配置 <u>NDES服务器证书配置</u> <u>NDES服务器IIS绑定配置</u> <u>ISE服务器配置</u> <u>验证</u> <u>故障排除</u> <u>相关信息</u>

简介

本文描述要求的步骤配置Secure证书登记协议(SCEP)集成的超文本传输协议安全(HTTPS)支持用身份服务引擎(ISE)。

<u>先决条件</u>

<u>要求</u>

Cisco 建议您了解以下主题:

- Microsoft的互联网信息服务(IIS) Web服务器基础知识
- •体验在SCEP和证书的配置里在ISE

使用的组件

本文档中的信息基于以下软件和硬件版本:

• ISE版本1.1.x

•与ICM Hotfixes的Windows服务器2008 R2企业安装的<u>KB2483564</u>和<u>KB2633200的</u> 本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。 对Microsoft证书服务提供相关的信息,当一个指南思科的特别地带来您自己的设备(BYOD)。参考的 Microsoft的TechNet作为真相明确来源Microsoft证书颁发机构、网络设备登记服务(NDES)和 SCEP的涉及服务器配置。

背景信息

在BYOD部署,其中一核心组件是有安装的NDES角色的Microsoft 2008 R2企业服务器。 此服务器 是激活目录(AD)森林的成员。 在NDES时初始安装, Microsoft的IIS Web服务器自动地安装并且配 置支持SCEP的HTTP终端。 使用HTTPS,在一些BYOD部署,客户也许要进一步巩固ISE和 NDES之间的通信。 此步骤选派要求的步骤请求和安装SCEP网站的一安全套接字层SSL证书。

配置

NDES服务器证书配置

注意: 您必须配置IIS的一新证书(只要求,当IIS集成与第三方PKI例如Verisign时或,当认证 机构(CA)和NDES服务器角色被分离在独立服务器上)时。在安装,如果NDES角色在一个当前 Microsoft CA服务器,IIS使用在CA设置期间创建的服务器身份证书。 对于独立配置例如此 ,请跳到直接地在本文的NDES服务器IIS绑定的配置部分。

- 1. 连接到NDES服务器通过控制台或RDP。
- 2. 点击Start > Administrative Tools >互联网信息服务(IIS)管理器。
- 3. 突出显示IIS服务器名并且点击**服务器证书**图标。

 WIN66FEV37056M + 														1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
rectors	🧐 WIR	-B6FEVJ7D	56M Hom	e									Ad	tons Hanage Server
View core and control (See Addy) demonstrator) Application Pocie Sites	115			Show Al G	mpbr: Area			21	là.	*	5			Hassant Diart Ship View Application Pools View Sites
	MDHE Types	All Modules	Output Cathing	Document Bocument Request Filtering	Browsing Server Certificates	Worker Processes	Tracing Rules	Happings	HI IF REDPECT	Respo	Restrictions	Loggra	•	Help Online Help
	Hanageme	et.												

4. 点击Create证书请求,并且填入字段。

-						
1	Internet Information Services (IIS) Hanager					
i	(3) (1) WIN-86FEV37D56M →					0 = 0 10 -
	Connections	0				Actions
1	Q.• 🗔 🖄 😥	Serve	r Certificates			Import
	Start Page	Use this feature b	o request and manage certific	ates that the Web server	can use with Web sites	Create Certificate Request
	Application Pools	configured for SS	Ico and To		Innuel By	Complete Certificate Request
	🖻 😡 Sites	- The -	W2N-86F	EV37D56M.bn-lab.local	bn-lab-WIIN-86FEV37D56M-CA	Create Domain Certificate
ł		IISCERT	bn-lab-W WDN-86F	EV37D56M-CA EV37D56M.bn-lab.local	bn-lab-WIN-86FEV37D56M-CA bn-lab-WIN-86FEV37D56M-CA	Create Ser-Signed Certificate
		1 Contributio				× Remove
	Reque	a Certificate				😢 Help
		Distinguishe	d Name Properties			Online Help
	-					
	Special of the special	ify the required informa ficial names and they co	tion for the certificate. State/ mot contain abbreviations.	province and City/locality	nust be specified	
	Com	non name:	hn-lah-WIN-BGEEV17DSGM	LCA.	_	
1	Orga	nization:	Cisco		_	
	Orga	nizational unit:	bn-lab			
	Oty)	locality	Montreal			
	Stab	Nprovince:	QC			
		in firegeric	1pm		-	
					1	
J						
11					-	
			Previous	Next	Finish Cancel	
						-
	Request Certificate					? ×
	Ele Name					
	rie name					
	Specify the file name for the cert	ficate request.	This information ca	an be sent to a o	ertification	
	autionity for signing.					
	Specify a file name for the certific	ate request:				
	Dewcert cer			_		
	hence cont					
	Period deal					
	President states (
	President					
	hered areas					
	hered areas					
			Previous	Next	Finish Can	xel la

리비즈

5. 打开在与文本编辑的上一步创建的.cer文件并且复制内容对剪贴板。

📕 newcert - Notepad	
File Edit Format View Help	
BEGIN NEW CERTIFICATE REQUEST MIIDazCCAtQCAQAwdTELMAkGA1UEBhMCQ0ExCzAJBGNVBAGMA1FDMREwDwYDVQQ DAhNb250cmVhbDEOMAwGA1UECgwFQ21zY28xDzANBGNVBASMBmJuLwxhYjE1MCM A1UEAwwcV010LU12RkVwSjdENTZNLmJuLwxhYi5sb2NhbDCBnzANBgkqhkiG9W0B AQEFAAOBjQAwgYKCgYEAjyQYLLhwQH9v49+EHztwa001mAq63isaRG8hzn3ixnu1 9wGkHhUQBwPNhyCI510HYhsD8GZRIG5yLpp1vq8cAhAIOnxhaZ9//kSgpFv8rN03 fd9fa7onoq0h+jHNxaYdLTjxMqTNDCOkok0vFLqZR9FXuGEeGCo22LA3jF10XX00 AwEAAaCCAbQwGgYKKwYBBAGCNw0CAzEMFg02LjEuNzYwMS4yMFAGCSsGAQQBgjcV FDFDMEECAQUMHFdJTi1CNkZFVko3RDU2TS5ibi1sYWIUbG9jYNwMFUJ0LUxBQjJ0 YWRtaW5pc3RyYXRvcgwHTU1DLkVYRTByBgorBgEEAYI3DQICMWQWYgIBAR5AAE0A aQBjAHIAbwBzAG8AZgB0ACAAUgBTAEEAIABTAEMAAABhAGAAbgB1AGwAIABDAHI eQBwAHQAbwBnAHIAYQBWAGgAaQBjACAAUAByAG8AdgBpAGQA2QByAwEAMIHPBgk0 hkiG9w0BCQ4xgcEwgb4wDgYDVR0PAQH/BAQDAgTwMBMGA1UdJQQMMAoGCCSGAQUF bKgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQM AgIAgDALBg1ghkgBZQMEASowCwYJYIZIAWUDBAETMASGCMGGSAF1AwQBAjALBg10 hkgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcWQYDVR00BBYEFLgkonC7Y+N9 dDrCREpo8/D/seatMA0GCSqGSIb3DQEBBQUAA4GBAHHCHBDd02+byxWFCm95XU2Y xpITWbkjxbmr0T+q3rcI0jLNQireDB57Has8WdgCoCrLJs8ncm40dzuzan1xYPP1 +EthsI0YgtdLS1gNJb35qAjLTCyDfNZEVP2P1FQNuM9DetkZkjuWLh8zqe0XJyxV +F80YWP06CWPj3PWiZ2Y	
<u> </u>	► //,

6. 访问Microsoft CA Web登记网站并且点击**请求证书**。示例URL :http://yourCAIP/certsrv

	nonre billettal Centinate Services Thinsters
G .	http://10.85.137.156/certsrv/
🚖 Favorites	🙀 🔊 Suggested Sites 🔹 🍘 Web Sice Gallery 🔹
6 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 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. 单击提交证书请求通过使用.....粘贴在从剪贴板的证书内容,并且选择Web服务器模板。

Microsoft Active Directory Certificate Serv Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

-- bn-lab-WIN-B6FEVJ7D56M-CA

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,

R

8. 单击提交然后保存证书文件到桌面。

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

ourca negacor.

	· · · ·	
	AgIAgDALBglghkgBZQMEASow	CwYJYIZIAWUDBAEt
Base-64-encoded	hkgBZQMEAQUwBwYFKw4DAgcw0	CgYIKoZIhvcNAwcw
certificate request	dDrCREpo8/D/seatMA0GCSqG	SIb3DQEBBQUAA4GB
(CMC or	xpITWbkjxbmrOT+q3rcIOjLN(QireDB57Has8WdgC
PKCS #10 or	+EthsI0YgtdL51gNJb35qAjL3	CyDfNzEvP2P1FQN
PKCS #7):	+F80YwPo6CWPj3PWiz2y	•
	4	•

Certificate Temp	plate:	
	Web Server	
Additional Attrib	utes:	
Attributes:	4 7	
	Submit >	\square

9. 返回到NDES服务器并且打开utilty IIS的管理器。点击服务器名然后单击**完整证书请求**为了导入新建立的服务器证书。

Internet Information Services (IIS) Manager				
A Sector				😐 🖂 🔂 I 😣 -
Connections Connections Start Page Start Page Achication Pools	Server Certificate	S age certificates that the Web server	can use with Web sites	Actions Import Create Certificate Request Complete Certificate Request
E- Stes	Name +	Issued To	Issued By	Create Domain Certificate
🗈 😔 Default Web Site		WDV-86FEV37D56M.bn-lab.local	bn-lab-WIN-86FEV37D56M-CA	
		bn-lab-WIN-86FEV37D56M-CA	bn-lab-WIN-B6FEVJ7D56M-CA	Create Self-Signed Certificate
	IISCERT	WIN-86FEV37D56M.bn-lab.local	bn-lab-WDV-86PEV37D56M-CA	Vew

NDES服务器IIS绑定配置

- 1. 展开**服务器名**,展开**站点**,点击**默认网站**。
- 2. 点击在右上角的捆绑。
- 3. 单击添加,更改Typeto HTTPS,并且从下拉列表选择证书。
- 4. 单击 Ok。



ISE服务器配置

1. 连接对CA服务器的Web登记接口并且下载CA证书一系列。

G Hicrosoft Active Directory Certificate Services - Windows Internet Explorer				
👷 Pavorites 🛛 🎪 🔊 Suggested Sites * 🍘 Web Site Gallery *				
6 Microsoft Active Directory Certificate Services				
Microsoft Active Directory Certificate Services - Dn-lab-WIN-B&PEVJ/Dobini-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 <u>Download a CA certificate, certificate chain, or CRL</u>

2. 从ISE GUI,请导航对**管理- >证书- >证书存储**并且导入CA证书一系列到ISE存储。

CISCO Identity Services Engine	
A Home Operations Policy Policy	Administration
Deployment Licensing Certificates	Logging Maintenance Admin Access Settings
Certificate Operations	Certificate Store
Certificate Store Certificate Store SCEP CA Profiles OCSP Services	Friendly Name BN-LAB-vISE1.BN-LAB.local#BN-LAB-vISE1.BN-LAB WIN-B6FEVJ7D56M-MSCEP-RA#bn-lab-WIN-B6FEVJ bn-lab-WIN-B6FEVJ7D56M-CA#bn-lab-WIN-B6FEVJ

 9. 导航对管理->证书->SCEP CA配置文件并且配置HTTPS的URL。点击测验连接然后单击 "Save"。

CISCO Identity Services Engine			
🛕 Home Operations * Policy * Adm	inistration 🔻		
🔆 System 🖞 Identity Management	Network Resources 🛛 🛃 Web Portal Mana	agement	
Deployment Licensing Certificates Logo	ging Maintenance Admin Access Sr	ettings	
Certificate Operations Certificates Certificate Signing Requests Certificate Store SCEP CA Profiles	SCEP Certificate Authority Certificates > BN_LAB_ Edit Profile SCEP Certificate Authority * Name Description	SCEP_SSL BN_LAB_SCEP_SSL]
OCSP Services	* URL	https://10.85.137.156/certsrv/mscep/	Test Connectivity
	Certificate Request Agent Certificate Save Reset	WIN-B6FEVJ7D56M-MSCEP-RA	

<u>验证</u>

使用本部分可确认配置能否正常运行。

•导航对管理->证书->证书Storeand验证CA证书一系列和NDES服务器注册机关(RA)证书存在。

•请使用Wireshark或TCP转储监控在ISE admin节点和NDES服务器之间的初始SSL交换。

<u>命令输出解释程序工具(仅限注册用户</u>)支持某些 **show** 命令。请使用Output Interpreter Tool为了 查看show命令输出分析。

<u>故障排除</u>

本部分提供的信息可用于对配置进行故障排除。

- •为逻辑小站划分BYOD网络拓扑为了帮助识别调试和捕获沿路径的点这些终端之间-ISE、 NDES和CA。
- •保证TCP 443允许双向在ISE和NDES服务器之间。
- 监控注册错误的CA和NDES服务器应用日志并且请使用谷歌或TechNet研究那些错误。

- •请使用在ISE PSN的TCP转储工具并且到/从NDES服务器监控流量。这查找在**操作>诊断工具** >General下**工具**。
- 安装在NDES服务器的Wireshark或在中介交换机的使用SPAN为了到/从ISE PSN捕获SCEP流量。

<u>命令输出解释程序工具(仅限注册用户</u>)支持某些 **show** 命令。请使用Output Interpreter Tool为了 查看show命令输出分析。

注意: 使用 debug 命令之前,请参阅<u>有关 Debug 命令的重要信息</u>。

相关信息

- <u>配置BYOD的SCEP支持</u>
- <u>技术支持和文档 Cisco Systems</u>