

IIS 服务器证书部署

环境说明

- 建议使用 IIS8 (支持 SNI),一个站点一个端口允许同时部署多张证书
- Win7, server 2008 r2, win8, win2012 系统上关于加密套件的补丁 https://technet.microsoft.com/zh-CN/library/security/3042058.aspx?f=255&MSPPError=-21 47217396
- 对于 IIS6,IIS7,IIS8,操作具体通用性

获取证书

这里需要 pfx/p12 (pkcs12) 格式的证书.

MPKI 方式:

- 1. 登录 https://mpki.trustasia.com
- 2. 证书下载 pkcs12 格式(得到一个 pfx 后缀的证书文件)。此 pfx 文件密码就是证书密码

非 MPKI

- 1. CSR 对应的 key 文件
- 2. 证书邮件里提取代码,里面可能有多段代码,把第一段-----BEGIN CERTIFICATE-----到 -----END CERTIFICATE------(包括开头和结尾,不用换行)复制到 txt 文本文件里,然后保 存为 cer 后缀,得到证书文件。注意证书链部分不使用。
- 3. 使用工具 https://myssl.com/cert_convert.html,进行格式转换,选择 pem 转 pkcs12.

导入证书

IIS 使用的是系统证书库中的证书。所以证书是要导入系统的。导入到 mmc 中

1. 运行 mmc



控制台1 - [控制台根节点]		
💊 文件(F) 操作(A) 查看(V) 收縮 (← ⇔ 🗊 📄 🛛 🗊	硖(O) 窗口(W) 帮助(H)	- 8 ×
🤷 控制台根节点	名称	操作
	此视图中没有可显示的项目。	控制台根节点▲
		更多操作

2. 使用计算机账户添加证书单元。主要是计算机账户,其他保持默认设置即可。

添加或删除管理单元	X	
您可以在计算机上为, 哪些扩展项。	此控制合选择可用的管理单元并配置所选的一组管理单元。对于可扩展的管理单元,您可以配置要启用 证书管理	E
 ○方市町省理年70(3). 管理単印 管理単印管理 源長 會高级安全 Windows 國共享文件夹 公子学れ管理 ② 任务计划程序 過设备管理器 國授权管理器 國大件夹 ③ 性能监视器 ③ 建策略对象编辑器 ● 组件服务 描述: 证书管理单元允许您 	 该管理单元将始终为下列帐户管理证书: ⑦ 我的用户帐户(M) ⑦ 服务帐户(S) ⑧ 计算机帐户(C) 	
	< 上一步(B) 下一步(X) > 取消	

- 3. 在"个人"下面的证书中导入 pfx 文件。
- 4. 所有任务-->导入证书





🔄 控制台1 - [控制台根节点\证书(2	[地计算机]\个人\证书]						
➡ 文件(E) 操作(A) 查看(V) 收	蔵夹(Q) 窗口(₩) 帮助(L	±)					- 6 ×
□ 控制台根节点	颁发给	颁发者	截止日期	预期目的	友好名称	状态 证=	操作
▲ 🖓 证书(本地计算机)	www.trustasia.com	Symantec Class 3 EC	2018/12	服务器身份	<无>		证书 🔺
 							更多操作
	•	111				۱. F	
个人存储含有一个证书。							

5. 调整证书链。将中级证书剪切到 "中级证书颁发机构"下的"证书"中。

SSL 配置

到 IIS 中绑定导入的证书

			Ø	贴绑定	? >
类型	主机名	第口	IP 地址	绑定信息)3740(A)
http		80	•		45 9時間(E)
					删除(R)
					读型范(B)

添加网站绑定	? X
类型(T): https ↓ IP 地址(I): 全部未分配 主机名(H): 主机名(H): □ 需要服务器名称指示(N)	端囗(O): ✔ 443
SSL 证书(F): Trustasia	选择(L) 查看(V) 确定 取消

优化 SSL

运行工具: <u>http://www.trustasia.com/down/ssltools.zip</u> 协议部分:只勾选 TLS1.0 TLS1.1 TLS1.2 套件部分:去掉带 DHE,RC4,NULL,MD5(ECDHE 的保留) 然后重启系统。





ss 📀	SL Tools for IIS	a							٢
	SSL Tools	for IIS			川	亞洲詞 TRU	┆信 ST <mark>↓</mark>	(sia	
欢迎	证书 安全 关于								
日安	全协议·重启系统生效]								
#	协议 启用	说明							
1	SSL 2.0	建议关闭,存在大量安全漏洞!							
2	SSL 3.0								
3	TLS 1.0								
4	TLS 1.1 🔍								
5	TLS 1.2 📝								
	应告供 的时来会 声扬动	田安江井井 2日1							
	密套件·I即时生效、可把动) 一	周奎伉先级」					1	-1.54	_
#	套件		启用	支持协议	FIPS	交换	加密	哈希	
11	TLS_ECDHE_RSA_WITH_AE	S_256_CBC_SHA_P256	1	TLS 1.2, TLS 1.1, TLS 1.0	是	ECDH_P256	AES	SHA1	
4	TLS_ECDHE_RSA_WITH_AE	.5_128_UBU_SHA256_P256	v	TLS 1.2	是	ECDH_P256	AES	SHA256	
1	TLS_RSA_WITH_AES_128_U	BC_SHA256	v	1L5 1.2 TIC 1.2 TIC 1.1 TIC 1.0	定日	H5A DCA	AES	SHA256	
2	TLS_RSA_WITH_AES_128_U		V	TLS 1.2, TLS 1.1, TLS 1.0	定日	R5A DCA	AES	SHAT	
3	TLS_RSA_WITH_AES_206_0	BC_SHA206	V	TE 12 TE 11 TE 10	定日	H5A DCA	AES	SHA256	
4	TLS_BSA_WITH_AES_206_0		v	TLS 1.2, TLS 1.1, TLS 1.0	定不	DCA	AE3	CUA1	
6	TIS DEA WITH 2DES EDE			TIC 1 2 TIC 11 TIC 10 SOL 30		DCA	2DEC	CUA1	
0	TIS ECOHE BSA WITH AE	5 128 CBC SHA256 P394	V	TIS 1 2	正旦	FCDH P394	AES	SHA256	
9	TIS ECOHE BSA WITH AE	S 128 CBC SHA P256	V	TIS12 TIS11 TIS10	正見	ECDH P256	AES	SHA1	
10	TIS ECOHE BSA WITH AE	S 128 CBC SHA P384		TIS12 TIS11 TIS10	足	ECDH P384	AES	SHA1	
12	TLS ECDHE BSA WITH AF	S 256 CBC SHA P384		TIS12 TIS11 TIS10	是	ECDH P384	AES	SHA1	
13	TLS ECDHE ECDSA WITH	AES 128 GCM SHA256 P256		TLS 1.2	是	ECDH P256	AES	SHA256	
14	TLS ECDHE ECDSA WITH	AES 128 CBC SHA256 P256	1	TLS 1.2	是	ECDH P256	AES	SHA256	Ξ
15	TLS ECDHE ECDSA WITH	AES 128 GCM SHA384 P384		TLS 1.2	是	ECDH P384	AES	SHA384	
16	TLS ECDHE ECDSA WITH	AES 128 CBC SHA384 P384		TLS 1.2	是	ECDH P384	AES	SHA384	
17	TLS_ECDHE_ECDSA_WITH	AES_128_CBC_SHA_P256	1	TLS 1.2, TLS 1.1, TLS 1.0	是	ECDH_P256	AES	SHA1	
18	TLS_ECDHE_ECDSA_WITH_	AES_128_CBC_SHA_P384	V	TLS 1.2, TLS 1.1, TLS 1.0	是	ECDH_P384	AES	SHA1	
19	TLS_ECDHE_ECDSA_WITH_	AES_256_CBC_SHA_P256	1	TLS 1.2, TLS 1.1, TLS 1.0	是	ECDH_P256	AES	SHA1	
20	TLS_ECDHE_ECDSA_WITH_	AES_256_CBC_SHA_P384	1	TLS 1.2, TLS 1.1, TLS 1.0	是	ECDH_P384	AES	SHA1	
21	TLS_DHE_DSS_WITH_AES_	128_CBC_SHA256		TLS 1.2	是	DH	AES	SHA256	
22	TLS_DHE_DSS_WITH_AES_	128_CBC_SHA		TLS 1.2, TLS 1.1, TLS 1.0	是	DH	AES	SHA1	
23	TLS_DHE_DSS_WITH_AES_	256_CBC_SHA256		TLS 1.2	是	DH	AES	SHA256	
24	TLS_DHE_DSS_WITH_AES_	256_CBC_SHA		TLS 1.2, TLS 1.1, TLS 1.0	是	DH	AES	SHA1	
25	TLS_DHE_DSS_WITH_3DES	_EDE_CBC_SHA		TLS 1.2, TLS 1.1, TLS 1.0, SSL 3.0	是	DH	3DES	SHA1	
26	TLS_RSA_WITH_RC4_128_N	4D5		TLS 1.2, TLS 1.1, TLS 1.0, SSL 3.0	否	RSA	RC4	MD5	
29	TLS_RSA_WITH_NULL_SHA	256		TLS 1.2	台	HSA	NULL	SHA256	
30	TLS_RSA_WITH_NULL_SHA			TES 1.2, TES 1.1, TES 1.0, SSE 3.0	百	HSA	NULL	SHAT	
									- T

http 跳转 https (建议非强制)

安装 rewrite 模块,下载模块 https://www.iis.net/downloads/microsoft/url-rewrite





类型	模式	添加
与模式匹配	^OFF\$	
		上移
	类型 与模式匹配	

\square	跨条件跟踪捕获组	(<u>K</u>)
-----------	----------	--------------

	1
ſſ	(
 操作类型(Y):	
操作属性	
重定向 URL:	
https://(HTTP HOST)/(R:1)	
☑ 附加查询字符串 @)	
重完向类型·	
金河其他 (303)	
· · · · · · · · · · · · · · · · · · ·	



检测

MvSSL.com	myssl.com Q	DNS诊断工
	myssl.com	
A	IP地址: 54.223.178.8:443 (北京) 服务器: openresty	
V	站点标题: SSL/TLS安全评估报告	
	检测时间:2017-09-26 10:51:04 (耗时:16秒)	
7 \.h		
. 既述		
ξ 述 检测部署SSL/TL	.S的服务是否符合行业最佳实践,PCI DSS支付卡行业安全标准,Apple ATS规范。	
乱述 检测部署SSL/TL	.S的服务是否符合行业最佳实践,PCI DSS支付卡行业安全标准,Apple ATS规范。	
5 述 检测部署SSL/TL	S的服务是否符合行业最佳实践,PCI DSS支付卡行业安全标准,Apple ATS规范。	
乱 述 检测部署SSL/TL 评级	-S的服务是否符合行业最佳实践,PCI DSS支付卡行业安全标准,Apple ATS规范。 A* A A B C D E F T	
ま 歴 歴 運 部署SSL/TL 详級 PCI DSS	S的服务是否符合行业最佳实践, PCI DSS支付卡行业安全标准, Apple ATS规范。 ▲ A A B C D E F T	
<mark>我 述</mark> 检测部署SSL/TL 评级 PCI DSS	_S的服务是否符合行业最佳实践,PCI DSS支付卡行业安全标准,Apple ATS规范。 A ⁺ A A ⁺ B C D E F T 合规	
K 述 检测部署SSL/TL 评级 PCI DSS ATS	S的服务是否符合行业最佳实践, PCI DSS支付卡行业安全标准, Apple ATS规范。 A ⁺ A A ⁻ B C D E F T 合规 合规 合规	
<mark>张 述</mark> 检测部署SSL/TL 评级 PCI DSS ATS	S的服务是否符合行业最佳实践, PCI DSS支付卡行业安全标准, Apple ATS规范。 A* A A ⁻ B C D E F T 合规 合规	
私 述 检测部署SSL/TL 评级 PCI DSS ATS	SS的服务是否符合行业最佳实践, PCI DSS支付卡行业安全标准, Apple ATS规范。 A* A A B C D E F T 合规 合规	•