

服务器证书安装配置指南

IBM Http Server 6

Q/ GlobalSign China-QI-XX-YY

GlobalSign 数字证书颁发机构 环玺信息科技(上海)有限公司 2018年1月

1.	创建证书请求	. 3
	1.1 运行 ikeyman	. 3
	1.2 创建密钥库文件	3
	1.3 生成证书请求	. 4
2.	导入服务器证书	. 5
	2.1 获取并导入服务器证书中级 CA 证书	5
	2.2 获取服务器证书	6
3.	安装服务器证书	. 7
4.	服务器证书的备份及恢复	. 7
	4.1 服务器证书的备份	7
	4.2 服务器证书的恢复	. 7

目 录



服务器证书安装配置指南(IBM Http Server)

1. 创建证书请求

1.1 运行 ikeyman

点击"开始"→"所有程序"→"IBM HTTP Server V6.1"→"Start Key Management Utility", 运行 I Key Manager

1.2 创建密钥库文件

密钥库类型选择"CMS"

新建		×
密钥数据库类型	CMS 💌	
交件名 :	key.kdb	浏览
位置:	C:\Program Files\IBM\SSLKeyDB	
	确定 取消	

注意: 请选中"将密码存储到文件"选项,此选项将把密码加密保存到扩展名为. sth 的 文件中。IHS 启动时,会自动从该. sth 文件中读取密码,如果不选择此项启动 HTTP SERVER 时会报错。





请留意"确定"后弹出的信息提示信息,并检查是否生成.sth文件。



1.3 生成证书请求

IHS6下的 ikeyman 最高支持创建 1024 位密钥,而 EV 服务器要求 2048 位密钥。您可以下载 IHS7 版本,使用 IHS7 试用版 ikeyman 创建含 2048 位密钥的密钥库文件,在 IHS6 下仍然可以正常应用。

🌆 创建新密钥和证书请求	×	
请提供以下信息:		
密钥标签(<u>K</u>)	cn.globa EV 证书要求 2048	
密钥大小(E)	2048 💌	
签名算法(<u>S</u>)	SHA1WithRSA 💌	
共用名(<u>M</u>) (可选)	cn.globalsign.com	
组织(<u>G</u>) (可选)	GlobalSign China Co.,Ltd.	
组织单元(<u>A</u>) (可选)	Sales	
市/县/区(L) (可选)	Shanghai	
省/直辖市(<u>T</u>) (可选)	Shanghai	
邮政编码(<u>Z</u>) (可选)	200060	
国家或地区(U)(可选)	CN 🖵	
输入存储证书请求的文件	牛的名称(<u>H</u>):	
/opt/IBM/certreq.arm	浏览(8)	
确定(<u>0</u>)	重新设置(R) 取消(C)	
导出证书签名请求	文件 certreq.arm,并稍后发送给 Globa	lSign, 等待证书的签发。
信息	×	
新证书请求已在 C:\Program Fil 您必须发送文件	E交件: les\IBM\SSLKeyDB\certreq.arm 中成功创建。 H到认证中心来请求证书。	
	确定	



2. 导入服务器证书

2.1 获取并导入服务器证书中级 CA 证书

为保障服务器证书在 IE7 以下客户端的兼容性,服务器证书需要安装两张中级 CA 证书。 从邮件中获取中级 CA 证书:

将证书签发邮件中的从 BEGIN 到 END 结束的两张中级 CA 证书内容(包括"-----BEGIN CERTIFICATE-----"和"----END CERTIFICATE-----")分别粘贴到记事本文本文档中。修改文件扩展名,保存为 intermediate1.cer 和 intermediate2.cer 文件。

运行 ikeyman 并打开您的 kdb 文件, 切换到"签署人证书"视图, 并选择"添加"

📅 IBM 密钥管理 - [C:\Program Files\IBM\? - D × 密钥数据库文件(F) 创建(C) 查看(V) 帮助(H) 🗅 🚄 🖬 😤 🕵 🗔 密钥数据库信息 DB 类型: CMS 密钥数据库文件 文件名: C:\Program Files\IBM\SSLKeyDB\key.kdb 令牌标号: 密钥数据库内容 从文件添加 CA 证书 X 签署人证书 添加.. 数据类型 Base64 编码的 ASCII 数据 💌 Entrust.net Glob: 删除 Entrust.net Glob: 证书文件名: intermediate1.cer 浏览... Entrust.net Clien 「看/编辑」 Entrust.net Certi C:\Program Files\IBM\SSLKeyDB\ 位置: Entrust.net Secu 解压缩. VeriSign Class 3 确定 取消 VeriSign Class 3 VeriSign Class 2 Public Primary Certification Authority VeriSign Class 1 Public Primary Certification Authority VeriSign Class 4 Public Primary Certification Authority - G2 VeriSign Class 3 Public Primary Certification Authority - G2 VeriSign Class 2 Public Primary Certification Authority - G2 VeriSign Class 1 Public Primary Certification Authority - G2 VeriSign Class 4 Public Primary Certification Authority - G3 VeriSign Class 3 Public Primary Certification Authority - G3 *

分别添加两张中级 CA 证书,并输入证书的标号





2.2 获取服务器证书

将证书签发邮件中的从 BEGIN 到 END 结束的服务器证书内容(包括"-----BEGIN CERTIFICATE-----"和"-----END CERTIFICATE-----") 粘贴到记事本等文本编辑器中,保存为 server.cer 文件

切换到"个人证书"视图,选择"接收",选择并导入您的服务器证书文件。

and and		密钥数据库信息		
DB 类型: CMS 密钥数据库文件 CtHCarman Files\IBM\SSLKeyDB\key.kdb				
		密钥数据库内容		
人证书	从文件接收证书	5	×	接收
	数据类型	Base64 编码的 ASCII 数据 🔻		删除
	证书交件名:	server.cer	浏览	看/编辑
	位置:	C:\Program Files\IBM\SSLKeyDB\		导入
		确定 取消		断创建请求
				<u></u>

证书导入完成

IBE 密钥管理 密钥数据库立件	- [C:\Program Files\IBH\SSLKeyDB\key.kdb]	
DB 类型: C 文件名: C	密钥数据库信息 MS 密钥数据库文件 \Program Files\IBM\SSLKeyDB\key.kdb	
- C. (2014)	密钥数据库内容	
个人证书	•	接收
* server	个人证书列表。用*指明缺省值	删除 查看/编辑 导出/导入 重新创建请求
请求的操作已成		新建自签署 抽取证书



3. 安装服务器证书

打开 IHS 安装目录下 conf 目录中的 httpd. conf 文件,在所有已存在的 Load Module 条 目下方添加如下条目以加载 IBM SSL 模块

完成 HIS 的设置后,您还需要登录 Websphere 控制台,检查"环境"→"虚拟主机"检查 配置中 default_host 或您自定义的虚拟主机项,"主机别名"下,是否已正确启用 443 端口。

4. 服务器证书的备份及恢复

在您成功的安装和配置了服务器证书之后,请务必依据下面的操作流程,备份好您的服务 器证书,以防证书丢失给您带来不便。

4.1 服务器证书的备份

备份服务器证书密钥库文件 key. kdb、key. rdb、key. sth 即可完成服务器证书的备份操作。

4.2 服务器证书的恢复

请参照服务器证书配置部分,将服务器证书密钥文件恢复到您的服务器上,并修改配置文件,恢复服务器证书的应用。

