# 阿里云 SSL证书(CA证书服务、数据安 全)

# 用户指南

文档版本: 20190920

为了无法计算的价值 | [] 阿里云

# <u>法律声明</u>

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读 或使用本文档,您的阅读或使用行为将被视为对本声明全部内容的认可。

- 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档,且仅能用于自身的合法 合规的业务活动。本文档的内容视为阿里云的保密信息,您应当严格遵守保密义务;未经阿里云 事先书面同意,您不得向任何第三方披露本手册内容或提供给任何第三方使用。
- 未经阿里云事先书面许可,任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分 或全部,不得以任何方式或途径进行传播和宣传。
- 3. 由于产品版本升级、调整或其他原因,本文档内容有可能变更。阿里云保留在没有任何通知或者 提示下对本文档的内容进行修改的权利,并在阿里云授权通道中不时发布更新后的用户文档。您 应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
- 4. 本文档仅作为用户使用阿里云产品及服务的参考性指引,阿里云以产品及服务的"现状"、"有缺陷"和"当前功能"的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引,但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的,阿里云不承担任何法律责任。在任何情况下,阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害,包括用户使用或信赖本文档而遭受的利润损失,承担责任(即使阿里云已被告知该等损失的可能性)。
- 5. 阿里云网站上所有内容,包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计,均由阿里云和/或其关联公司依法拥有其知识产权,包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意,任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外,未经阿里云事先书面同意,任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称(包括但不限于单独为或以组合形式包含"阿里云"、Aliyun"、"万网"等阿里云和/或其关联公司品牌,上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司)。
- 6. 如若发现本文档存在任何错误,请与阿里云取得直接联系。

# 通用约定

格式	说明	样例
•	该类警示信息将导致系统重大变更甚至 故障,或者导致人身伤害等结果。	禁止: 重置操作将丢失用户配置数据。
A	该类警示信息可能导致系统重大变更甚 至故障,或者导致人身伤害等结果。	▲ 警告: 重启操作将导致业务中断,恢复业务所需 时间约10分钟。
Ê	用于补充说明、最佳实践、窍门等,不 是用户必须了解的内容。	道 说明: 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定。
courier 字体	命令。	执行 cd /d C:/windows 命令,进 入Windows系统文件夹。
##	表示参数、变量。	bae log listinstanceid Instance_ID
[]或者[a b ]	表示可选项,至多选择一个。	ipconfig[-all -t]
{}或者{a b }	表示必选项,至多选择一个。	<pre>swich {stand   slave}</pre>

# 目录

法律声明	I
通用约定	I
1 概览	1
2 选择并购买证书	
3 申请和提交审核	12
4 已签发证书部署到阿里云云产品	17
5 上传已有证书	20
6 下载证书并安装到其他服务器	
6.1 下载证书	
6.2 Tomcat服务器安装SSL证书	
6.2.1 安装PFX格式证书	
6.2.2 安装IKS格式证书	
6.3 在Apache服务器上安装SSL证书	
6.4 在Nginx/Tengine服务器上安装证书	
6.5 在IIS服务器上安装证书	35
6.6 在GlassFish服务器上安装证书	40
7 吊销证书	42
8 全站HTTPS	43
8.1 全站HTTPS介绍	43
8.2 开启全站HTTPS服务	44
8.3 修改DNS解析记录	53
8.4 阿里云企业邮箱接入全站HTTPS最佳实践	55

# 1概览

本文档介绍阿里云SSL证书服务的操作概览信息和控制台主要的功能模块。

您可在SSL证书控制台对证书进行以下管理和操作:

- ・购买SSL证书服务
- ・查看SSL证书状态
- ・管理证书:
  - #unique\_4到控制台统一进行管理
  - 申请签发证书或撤销申请
  - 将已签发的证书部署到云产品
  - 下载已签发的证书并安装到其他服务器
  - 删除/#unique\_8
- ・ 证书#unique\_9

📋 说明:

如果您在证书安装、验证、快速审核上有紧急需求,可在SSL证书控制台右侧安全服务区域选择需 要的安全服务并单击立即咨询购买相应的增值服务,会有专业人员为您解决相关问题。

Q 消息 <sup>99+</sup> 费用 工单 备案 企业	支持与服务 🔼 📜 简体中文
	关闭
	🔄 购买证书 🏠 上传证书
全部品牌 ∨ 证书域名 Q 🔡 🗮	公告
实例: ✓ Symantec. Symantec 免费版 SSL 绑定域名	<ul> <li>新版本控制台使用指南</li> <li>SSL证书安装指南(包含多种服务器)</li> <li>Symantec SSL数字证书升级重签提示</li> <li>苹果ATS - 证书选择及配置</li> </ul>
1年有效期 <u> </u>	常见问题
	<ul> <li>SSL证书续费和到期新购</li> <li>SSL证书退费申请</li> <li>Apache2 部署SSL证书</li> <li>Tomcat部署SSL证书</li> <li>订单提交很久了,为什么还是审核中</li> <li>各版本证书的区别</li> <li>浏览器或手机浏览器提示证书不可信</li> <li>域名验证推送到阿里云DNS失败</li> <li>皮全服务</li> <li>定取答用</li> <li>安实证的服务(仅限</li> <li>Symantec/GeoTrust品牌)。¥360元</li> <li>起</li> </ul>
	<b>需要技术辅助服务吗?</b> 帮您解决订单审核失败、验证失败相 关问题(仅适合OV/EV)。¥68元起

控制台布局模式

SSL证书控制台页面有两种布局模式,您可单击控制台上方切换布局按钮选择您需要的布局模式。

		📜 购买证书	土传证书
全部品牌     ∨     证书域名     Q     日     Ξ	公告		

#### 本文档所有操作指南以卡片式为例:

### ・卡片式

SSL证书		
全部 146 审核失败 即将过期 更多状态 >		
未签发证书		
实例: cas-c Geo <b>Trust</b>	实例: ca: Symantec.	实例: cas-cn 🧭 Symantec.
GeoTrust 绑定域名: 1年有效期	Syman( 绑定域名 1年有效明	Symantec 绑定域名:o 1年有效期
已付款 申请	待验证 申请 撤回	日付款 申请
实例: cas-xj WoSign	实例: cas-wWoSign	
绑定域名: 1年有效期	绑定域名:\ 到期时间:2017年4月12日	
已关闭	巳吊销	

#### ・列表式

SSL证书									
全部 146	审核失败	即将过期	更多状态 >						
未签发证书									
证书		状态		绑定域名		有效期限		到期时	间
GeoTru 实例: c		已付款		aliy		1年		2018年	11月29日
Syman 实例: c		待验证		ww		1年		2018年	11月29日
Syman 实例: c	81.12	已付款		ov2	ie	1年		2018年	11月29日
Syman 实例: c	1 m	已付款		ww		1年		2018年	11月29日
WoSigi 实例: c	-	已关闭				1年		2018年	11月29日
实例: c		已吊销		wha		1年		2017年	4月12日
已签发证书									
证书				状态	绑定域名		有效期限		到期时间
2301a 实例: -(上传)				已签发			10 年		2028年8月31日

#### 购买SSL证书服务

您可在SSL证书服务控制台右上角单击购买证书购买证书服务。详情参见选择并购买证书。

工単省室	企业 支持与服务 👾 2 简体中文 💮
	▲ 上传证书
ର 88 ≣	公告
< 1 2 3 >	<ul> <li>新版本控制台使用指南</li> <li>SSL证书安装指南(包含多种服务器)</li> <li>Symantec SSL数字证书升级重签提示</li> <li>苹果ATS - 证书选择及配置</li> </ul>
	常见问题

SSL证书服务提供多种类型的证书服务,详见功能特性。

#### 查看SSL证书状态

您可在SSL证书控制台查看您拥有的证书的状态。

管理控制台	💴 中国大陆 🖣					
未签发 6	审核失败 2	已签发 152	即将过期	更多状态 へ		
实例: cas-cn-	0pp113znb169	•	Geo <b>Trust</b>	已付款4	i5vk1fs	Symantec.
GeoTrust € 鄉定域名: 1年有效期	₹业版通配符 OV S	SSL		审核中 已过期 86 已吊销 1	} DV SSL	
已付款			申请	已付款		申请

证书有以下几种状态:

- ・ 未签发: 证书已完成付款购买, 需提交证书申请和完成审核后才可使用。
  - 已付款
  - 待验证
  - 已吊销
- · 已签发: 证书已完成付款购买、申请和通过审核后,可进行部署到云产品或下载/删除证书的操作。
  - 已过期:证书已到期,需要重新购买和申请证书才能继续防护您的网站安全。

管理证书

SSL证书审核通过后,您可以通过SSL证书服务控制台对您拥有的所有证书进行统一的管理,包括 查看证书的状态和有效期、上传您所拥有的其他证书到SSL控制台、删除、吊销证书等。 · 上传证书: 您可将您拥有的其他证书上传到控制台, 并对所有证书进行统一管理。

工単  备案	企业 支持与服务 🔄 2 简体中文 💮
	★ 购买证书
৭ 88 ≣	   公告
< 1 2 3 >	<ul> <li>新版本控制台使用指南</li> <li>SSL证书安装指南(包含多种服务器)</li> <li>Symantec SSL数字证书升级重签提示</li> <li>苹果ATS - 证书选择及配置</li> </ul>
	常见问题

· 申请/撤回申请签发证书: 对已完成购买的证书进行证书申请或撤回申请证书。

未签发证书	
实例: can ch-lippdirchit 10   6 GeoTrust	实例: cus-cm-1000msdc luo
GeoTrust 专业版 OV SSL 绑定域名: 1年有效期	Symantec 免费版 SSL 绑定域名:www.aliyun.com 1年有效期
已付款 申请	待验证 申请 撤回

Ê	说明:	
已签发	<b>发的证书无法撤回申请</b> 。	

· 部署到云产品: 将已签发的证书部署到云产品。

已签发证书	
实例: -(上传)	Alibaba
<b>2301a</b> 绑定域名:*.baidu.com 到期时间:2028年8月31日	
已签发	部署到云产品 > 下載   删除



目前支持部署到CDN和SLB(负载均衡)。

· 下载证书: 下载已签发的证书并安装到web务器。

实例: cas-9fdpbnej01bn	Co GeoTrust
cert-1539853379162	
绑定域名: <b>##30#10*10*10*</b> 到期时间:2019年10月18日 SLB	tificatiestests.com
已签发	部署到云产品 > 下載   吊销

·删除/吊销证书:对已签发并不再使用的证书执行删除或者吊销操作。

已签发证书	
实例: cas-ta-Octaber #017a	实例: -(上传)
<b>cert-15427990095446</b> 绑定域名:c <b>m21154121.certificateriasta.com</b> 到期时间:2019年11月21日	test-upload-cert-001 绑定域名: * * * * * * * * * * * * * * * * * * *



证书删除后无法恢复,请谨慎操作。



签发后30天内完成吊销可退全款,签发超过30天后再吊销无法退款。

# 2选择并购买证书

本文档介绍了如何 选择和购买 阿里云 SSL证书,包括选择 证书的品牌 、 类型 、购买数量、购买 年限等。

#### 操作步骤

- 1. 登录阿里云云盾证书购买服务页面。
- 2. 选择您需要的证书配置。

	盾证书服务	(包年)
	选择品牌	GeoTrust GlobalSign CFCA Symantec
		【动态】Digicert 于 2017年12月1日 ,完成对 Symantec 证书服务的并购。此后,所有新申请的 Symantec/GeoTrust 品牌证书,切换到 Digicert+Symantec 交叉认证 PKI 体系下签发。阿里云平台的Symantec/GeoTrust已签发的旧根,也会按计划更新到新交叉根下。 GeoTrust是全球第二大数字证书颁发机构,也是身份认证和信任服务的领导者
	证书类型	专业版OV SSL 通配符DV SSL
		OV SSL,提供加密功能,对申请者做严格的身份审核验证,提供可信身份证明
本配置	保护类型	通配符域名 1个域名 多个域名
1994		保护一个带通配符域名(该*号同级别的全部明细域名)。申请证书时,如申请*.example.com,那么该证书支持a.example.com, a1.example.com, a2.example.com以此类推,但是不支持b.a.example.com, b1.a.example.com以此类推。如需支持,需另外再申请一 张*.a.example.com证书。此外,当前云上不支持多域名通配证书,即一张证书包含多个通配符证书,如申请一张包含*.example.com, *.a.example.com, *.a1.example.com, *.example1.com这样包含4个通配符的证书时,下单4个OV专业版通配符订单及一个单域名OV后,需 通过提交工单合并上述所有订单,再补全签发该OV多域名通配符证书。当前只支持OV级多域名通配符证书合并成一个证书签发,不支持 DV、EV合并
	域名个数	1个 您如选择保护类型为"通配符"需提交一个级别的通配符域名,您选择保护类型为"单域名",需提交一个明细域名

证书的品牌、类型等配置信息详见本文档中SSL证书类型配置表。

3. 选择购买数量和购买年限。

### 📕 说明:

所有证书类型购买年限最长为2年。以下类型证书只能购买1年,证书申请审核通过后1年内证书 有效,超过1年需重新购买和申请证书:

- · GeoTrust通配符DV SSL
- · Symantec免费型DV SSL
- · Symantec通配符DV SSL

4. 完成支付后即可进行申请证书操作。

#### 证书到期续费

证书有效期为1-2年,到期前需续费购买。详见#unique\_13。

#### SSL证书类型配置表

证书根据不同的验证级别,分为以下三类:

- ・ 域名型SSL(DV SSL)
- ・企业型SSL (OV SSL)
- ・ 増强型SSL(EV SSL)

根据保护域名的数量需求,SSL 证书又分为:

- · 单域名版:只保护一个域名,例如 www.abc.com 或者 login.abc.com 之类的单个域名
- · 多域名版:一张证书可以保护多个域名,例如同时保护 www.abc.com, www.bcd.com, pay .efg.com 等
- ·通配符版:一张证书保护同一个主域名下同一级的所有子域名,不限个数,形如\*.abc.com。 注意,通配符版只有 DVSSL 和 OVSSL 具有, EVSSL 不具有通配符版本。

证书品牌	证书类型	保护域名的类型	说明
GeoTrust	专业版OV SSL	<ul> <li>・1个带通配符的域名</li> <li>・1个明细域名</li> <li>・多个明细域名</li> </ul>	提供加密功能,对申请者 的身份进行严格的审核验 证,可提供可信身份证 明。 多个域名例上限为300个。 如:buy1.example.com ,buy2.example.com ,next.buy.example2. com,上述3个明细子域名
			计算为3个域名。
	高级版EV SSL	<ul> <li>・1个域名</li> <li>・多个域名</li> </ul>	提供加密功能,对申请者 做最严格的身份审核验 证,提供最高度可信身份 证明,提供浏览器绿色地 址栏。
GlobalSign	专业版OV SSL	通配符域名	提供加密功能,对申请 者进行严格的身份审核验 证,提供可信身份证明。

证书品牌	证书类型	保护域名的类型	说明
CFCA	专业版OV SSL	<ul> <li>・ 通配符域名</li> <li>・ 1个域名</li> <li>・ 多个域名</li> </ul>	提供加密功能,对申请 者进行严格的身份审核验 证,提供可信身份证明。
	高级版EV SSL	<ul> <li>・1个域名</li> <li>・多个域名</li> </ul>	提供加密功能,对申请者 做最严格的身份审核验 证,提供最高度可信身份 证明,提供浏览器绿色地 址栏。
Symantec	专业版OV SSL	<ul> <li>・通配符域名</li> <li>・1个域名</li> <li>・多个域名</li> </ul>	提供加密功能,对申请 者进行严格的身份审核验 证,提供可信身份证明。
	通配符DV SSL	通配符域名	-
	增强型OV SSL	<ul> <li>・1个域名</li> <li>・多个域名</li> </ul>	提供站点加密功能,需要 核验组织注册信息,证书 中会显示组织名称。组织 信息验证通过后,3个工作 日内颁发证书。
	高级版EV SSL	<ul> <li>・1个域名</li> <li>・多个域名</li> </ul>	提供加密功能,对申请者 做最严格的身份审核验 证,提供最高度可信身份 证明,提供浏览器绿色地 址栏。
	增强型EV SSL	<ul> <li>・1个域名</li> <li>・多个域名</li> </ul>	增强型EV SSL提供站点 加密功能,浏览器绿色地 址栏显示组织信息强化信 任。组织信息验证通过后7 个工作日内颁发证书。
	免费型DV SSL	1个域名	免费新根证书,切入 DigiCert PKI体系,兼 容性操作系统版本IOS 5. 0+、Android 2.3.3+、 JRE 1.6.5+、WIN 7+。 最多保护一个明细子域 名,不支持通配符,一个 阿里云帐户最多签发20张 免费证书。

# 3申请和提交审核

证书完成购买后,您需先完成证书申请、验证和提交审核并通过审核后,才能开始使用证书。

#### 步骤一 填写证书申请信息

- 1. 登录阿里云SSL证书控制台。
- 2. 单击已购买并需要完成申请的证书模块右侧操作栏下的申请, 打开证书申请侧页面。

■ 购买证书 ▲ 上传证书	🕼 金站HTTPS			全部状态 874 、	/ 全部品牌	∨ 证书城名	Q ⊞ ≣
✓ 未签发							
征书	品牌/类型	状态	绑定域名	有效期限	已部署		操作
Symantec 增强型 OV SSL 实例:	<b>♂Symantec.</b> 增强型 OV SSL	已付款		1年			退款 证书申请

3. 在证书申请页面,完整填写证书的申请信息。

SSL证书					证书申请			×
证书购买后,需要完善证书信息并提交审核通过后才能使用。	查看详细使用说明 找需要人工服务描导				ij	泻申请	经正信息	
购买证书▶ 完善资料、提交审核	DV型&免费证书 域名所有权验证 OV&EV型证书	▶ 部署证书 / 下载证书			<ul> <li>证书绑定域名:</li> <li>小司欠急;</li> </ul>	Alizaba	0	
	● 组织机构检证			_	* 公司美型:	● 私善个体 ○ 商业企业 ○ 政府实体 ○	非营利组织	
近形台政 ◎ 日 田炭的近市 待 874 735 7	■清的证书 即将过期的证书 ● 第标 7 1 33	*失败的证书 8			* 公司电话:	1	0	
				_	* 公司机构号码:	1	0	
★ 別天正书 ▲ 上侍正书 ◎ 全站HTT	PS		全部状态 874 ~	全部品牌	• 新在地:	中国大陆/	~	
◇ 未签发					* 详细地址:	执服中住		
证书 品牌/类型	状态	御定城名	有效期限	已部署	* 自动改编码:	1		
Symante	巴付款		1年		* 申请人姓名:	5000		
0					* 申请人手机号:	10.000	0	
GeoTrus	何验证		1年		*申请人邮箱:		0	
·					* 由请人身份证			
Symante 家例: ca:	軍核失敗 🗿		1年		킁:			
0				_	* CSR生成方式:	CSR文件是您的公钥证书原始文件,包含了您的服务 原、需要得交给CA认证中心审核,建议您使用系统会建	發信息和您的单位信 的CSR、避免内容不正	
Symantes 京例: cas	待输证	abc.bigmr.me	1年			确而导致的审核失败		
				_		· ····	下一步取	C/M
GeoTrust GooTrust								

选择不同类型的证书需要填写的申请信息也不同。免费版SSL和普通版需要填写个人信息;专业版SSL需要填写个人信息和申请人公司详细信息。

参数名	说明
证书绑定域名	您可单击对话框后的问号图标查看域名添加提示,根据提示的限制来 填写域名信息。
	证书申请 ×
	填写申请     验证信息       * 证书绑定域名:     最多添加1个普通域名和0个通配符域名。查看       更多     更多
	<ul><li>说明:</li><li>不同类型的证书绑定域名的限制要求不同,请根据添加域名限制提示</li><li>输入需要绑定的域名。</li></ul>
公司名称	请按要求填写真实的信息。
公司类型	请按实际情况勾选公司的类型。
公司电话	请填写正确,签证中心人员会拨打该电话号码确认证书认证相关的信 息。
公司机构号码	请按要求填写真实的信息。
所在地	请按实际情况勾选公司所在地。
详细地址	请正确填写公司详细地址信息。
邮政编码	请正确填写邮政编码。
申请人姓名	请正确填写您的姓名。

参数名	说明
申请人手机号码	请填写正确,签证中心人员会拨打该电话号码确认证书认证相关的信 息。
申请人邮箱	请填写正确,证书提交审核后CA中心将会向您的邮箱发送验证邮件,请注意及时查收。
申请人身份证号码	请正确填写您的身份证号码。

- 4. 选择CSR生成方式。
  - · 系统生成:系统将自动帮您生成证书私钥,并且您可以在证书申请成功后直接在证书管理页 面下载您的证书和私钥。



CSR生成方式建议选择系统生成,否则将无法部署到云产品。

· 手动生成: 手动生成CSR文件并将文件内容复制到CSR文件内容对话框中。详 见#unique\_15。

▋ 说明:

手动生成CSR的证书不支持一键部署到云产品。

* CSR生成方式:	€ CSR文件是您的公钥证书原始文件,包含了您的服务器信息和您的单位信
	息,需要提交给CA认证中心审核。建议您使用系统创建的CSR,避免内容不正
	确而导致的审核失败
	○ 系统生成
[	● 手动填写
* CSR文件内容:	请填写要上传的CSR文件

说明:

- 您的CSR文件格式正确与否直接关系到您证书申请流程是否能顺利完成。
- 在制作CSR文件时请务必保存好您的私钥文件。私钥和数字证书一一对应,一旦丢失了私 钥您的数字证书也将不可使用。阿里云不负责保管您的私钥,如果您的私钥丢失,您需要 重新购买并替换您的数字证书。
- 5. 单击下一步,进入验证页面。

#### 步骤二 验证申请信息并提交审核

完成证书申请信息的填写后,您需要上传验证文件。

<del>آ</del>	书申请	×
	填写申请 验证信息	
1	您需要先下载文件模板,没有"下载模板"按钮则表示没有模板	
2	打印并填写完成后, 签署姓名	
3	选择要上传的扫描文件 (仅支持PNG/JPG格式,文件大小不超过500KB)	
	营业执照,上传文件	

1. 按照证书申请页面提示执行相应操作。申请不同类型的证书验证信息的要求不同。



- ・如需下载模板并填写和盖章,请根据验证页面的提示操作。
- ·如需上传照片,照片格式必须为PNG或JPEG格式,且图片大小不能超过500 KB。
- · 证书是有有效期限制的,您可在申请过程中保存您所填写的申请信息以供下次申请证书时使用。
- 2. 单击上传文件按要求上传资质文件。
- 3. 单击页面右下角提交审核,系统将提示您已成功提交到CA公司,请您保持电话畅通,并及时查 阅邮箱中来自CA公司的电子邮件。



阿里云将在收到您的提交审核信息后开始证书资质的验证。验证时间根据不同CA中心的要求而不同,请及时关注您的邮箱和电话,及时回复将能有效缩短您的数字证书的验证时间。

您可在SSL证书控制台页面未签发证书区域,看到您已提交申请的证书预计签发时间、证书类型、 绑定的域名和有效期等信息。

📕 说明:

申请信息如需修改,您可在证书签发前撤回申请并修改申请信息。证书签发后无法撤回申请。

#### 申请证书需要提交的资料

证书品牌	需要提交的资料
GeoTrust/Symantec/GlobalSign	企业营业执照
	银行开户许可(仅EV证书需要)
CFCA	企业营业执照
	经办人身份证
	律师证(仅EV证书需要)
	申请表、授权书、律师函(阿里云SSL证书控制 台提供模板)

#### 相关文档

#unique\_16

#unique\_17

#unique\_18

#unique\_19

# 4 已签发证书部署到阿里云云产品

证书签发完成后,可一键部署到阿里云云产品。

目前SSL证书支持部署到以下云产品,后续将支持更多云产品:

- ・ SLB(负载均衡)
- · CDN(内容分发网络)
- $\cdot$  SCDN
- · DCDN



证书完成签发后才可部署到云产品。

#### 操作步骤

- 1. 登录阿里云SSL证书控制台。
- 2. 在已签发证书区域单击目标证书的部署到云产品。

已签发证书		
实例: cas		𝗭 Symantec.
cert-		
绑定域名:dns2018 到期时间:2019年11月21日	ests.com	
已签发	部署到云产品 へ	下载 吊销
实例: -(上传)	CDN SLB	Alibaba

3. 在下拉列表中选择需要部署的云产品。

4. 在右侧打开的证书部署到CDN/SLB页面中勾选需要部署的区域。

ù	E书部署到SLB	×
该	证书适用于SLB服务中以下区域,请选择要部署的区域:	
-	ap-southeast-1	
	eu-central-1	
	ap-southeast-5	
	cn-qingdao	
	us-east-1	
	ap-south-1	
	cn-beijing	
	cn-shanghai	
	ap-northeast-1	

#### 可选择多个部署区域。

说明:

部署到SLB时需选择您购买的SLB所部署的区域。



📃 说明:

绑定的CDN域名要和证书域名匹配。

5. 单击确定完成云产品区域部署。

证书部署到云产品后您可以单击部署云产品的证书卡片,打开证书详情页面查看证书的详细信息和 部署的云产品信息。

证书域名 Q	证书详情	$\times$
	实例:-(上传)	
	证书名称:234	
	证书来源:用户上传	
	绑定域名:cd	
	颁发厂商:Alibaba	
< 1	有效期限:10年	
Qo	签发时间:2018年10月26日	
	到期时间:2028年10月23日	
	已部署的产品	
yole.com	SLB : ap-sc	
4	SLB : eu-ce	
	SLB : ap-sc	

# 5 上传已有证书

您可使用阿里云SSL证书服务上传您所拥有的其他证书,在SSL证书控制台对您的全部证书进行统 一管理。

SSL证书服务只支持上传PEM编码格式的证书文件,其他编码格式的证书需要转化成PEM编码文件 后才能上传。

PEM编码文件包括以下两种类型的扩展名:

- · .pem
- · .crt



上传的证书不支持下载。

操作步骤

- 1. 登录阿里云SSL证书控制台。
- 2. 单击证书页面右上角上传证书打开上传证书对话框。



 在上传证书对话框中按要求输入证书名称,并将您的证书文件(文件格式或后缀 为.pem或.crt)内容拷贝至证书文件对话框中,将证书私钥文件(文件格式或后缀为.key)内 容拷贝至证书私钥对话框中。

上传证书		$\times$
* 证书名称:	certicate	
	名称仅支持英文字母、数字、下划线、中线	
* 证书文件:	VLUCSM9QIX/Noms8NptcFYWQTeGIUJYVQRZaVDbMFeVET ul7619W8Dn/ysWZNMpO FXIhMIxJz9itZly0D+YIbmImEpeWxQrZKmDJDENP0O0wiJI ZbZIO4MaE1s5XVT53 zDI6LaALXAXwEmI08HEppbCuxG1eIEOqIULAfzdiu45WTav	
	Je2Rgn/iGf6wGgUnI=	
* 证书私钥:	USZOGYJSTORUONG SEC4K2I4PIKeQG8fsWoHTfp9WL9pgYrxg+OrmIUIYAOXC 0d9D5YrigYIDQLUbXAG nF+FrH8wDXUF+eiCnUhJzUCldZTdmePNOAsu7g9ceRdXr QTKIAkm+Gh6iH3+A8at yptuFfMYgGnBLtX4LeHfA4I=	
	确认取消	Í



请用文本工具(notepad或notepad ++)打开您的证书文件和私钥文件。

4. 单击确认完成证书上传。

您可以在已签发的证书中找到您刚上传的证书。上传的证书也可以部署到云产品。

已签发证书	
实例:-(上传)	Alibaba
<b>上传证书 修改</b> 绑定域名:key.test.com 到期时间:2028年4月30日	
已签发	部署到云产品 > 下載 删除

# 6 下载证书并安装到其他服务器

### 6.1 下载证书

SSL证书服务支持下载证书并将其安装到您的Web服务器。安装好证书后,您的Web服务器将能支持SSL通信,从而保证您Web服务器的通信安全。

已签发和已过期的证书支持下载;其他类型证书不可下载。

操作指南

- 1. 登录阿里云SSL证书控制台。
- 在SSL证书页面,点击已签发标签,定位到需要下载的证书并单击证书卡片右下角的下载打开证 书下载对话框。

₩ 105005					全部状态 864	✓ 2888# ✓ (2582 Q)	88 🚍
<ul> <li>* 未签发</li> <li>* 已签发</li> </ul>							
ē#	圓碑	秋志	修定域名	有效期限	日終着		操作
	Contract of Contra	日振波		1年 2020年7月23日到期	-	法律 聖皇 人 上部	£ 709
		已签发	1.0.0	1年 2020年7月18日到朝		洋橋 道政  部署 > 下田	8   7899

- 3. 定位到您需要安装证书的服务器类型并单击右侧操作栏的下载将证书压缩包下载到本地。
- 4. 将证书解压缩后安装到您的Web服务器上。

阿里云SSL证书支持安装到以下类型的Web服务器:

- Tomcat
- Apache
- Nginx
- · IIS
- ・其他类型服务器

### 6.2 Tomcat服务器安装SSL证书

### 6.2.1 安装PFX格式证书

您可以将下载的证书安装到Tomcat服务器上。Tomcat支持PFX格式和JKS两种格式的证书,您可 根据您Tomcat的版本择其中一种格式的证书安装到Tomcat上。

#### 背景信息

·本文教程以Tomcat 7为例。

・ Tomcat 9强制要求证书别名设置为tomcat。您需要使用以下keytool命令将protocol="

HTTP/1.1"转换成protocol="org.apache.coyote.http11.Http11NioProtocol"。

```
keytool -changealias -keystore domain name.pfx -alias alias -
destalias tomcat
```

- ·本文档证书名称以domain name为示例,如证书文件名称为domain name.pfx,证书密码文件名称为pfx-password.txt。
- ・申请证书时如果未选择系统自动创建CSR,证书下载压缩包中将不包含.txt文件。需要您选择其 他类型服务器下载.crt证书,并使用openssl命令生成pfx文件。

操作指南

- 1. 登录阿里云SSL证书控制台。
- 在SSL证书页面,点击已签发标签,定位到需要下载的证书并单击证书卡片右下角的下载打开证 书下载对话框。

未签发4	审核失败 1	已签发 152	即将过其
实例:- (上传	)		-
绑定域名: 到期时间:20	28年8月31日	and the second	
已签发		部署到云产品 > [	下载 删除

3. 在证书下载对话框中定位到Tomcat服务器,并单击右侧操作栏的下载将Tomcat版证书压缩包 下载到本地。 4. 解压Tomcat证书。

您将看到文件夹中有2个文件:

- ・证书文件(以.pfx为后缀或文件类型)
- ・密码文件(以.txt为后缀或文件类型)

新建文件夹			
名称	Ŧ	修改日期	类型
domain name.pfx		2018/12/18 17:45	Personal Inform 文本文档
		2010/12/10 17.43	又4—又19

🗐 说明:

每次下载证书都会产生新的密码,该密码仅匹配本次下载的证书。如果需要更新证书文件,同时也要更新匹配的密码。

- 5. 在Tomcat安装目录下新建cert目录,将下载的证书和密码文件拷贝到cert目录下。
- 6. 打开Tomcat > conf > server.xml文件,在server.xml文件中添加以下属性(其中port属性 请根据您的实际情况修改):

```
<!--
  <Connector port="8443"
protocol="HTTP/1.1"
 port="8443" SSLEnabled="true"
 maxThreads="150" scheme="https" secure="true"
 clientAuth="false" sslProtocol="TLS" />
-->
<Connector port="443"
   protocol="HTTP/1.1"
   SSLEnabled="true"
   scheme="https"
   secure="true"
   keystoreFile="domain name.pfx"
                                    #此处keystoreFile代表证书文件的路
径、请用您证书的文件名替换domain name。
   keystoreType="PKCS12"
   keystorePass="证书密码"
                            #请用您证书密码替换文件中的内容。
   clientAuth="false"
   SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
   ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256
_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_A
ES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WI
TH_AES_256_CBC_SHA256"/>
```

〕 说明:

其中port属性根据实际情况修改(https默认端口为443)。如果使用其他端口号,则您需要使用https://yourdomain:port的方式来访问您的网站。

#### 7. 保存server.xml文件配置。

8. (可选步骤) 配置web.xml文件开启HTTP强制跳转HTTPS。

```
#在</welcome-file-list>后添加以下内容:
<login-config>
    <!-- Authorization setting for SSL -->
    <auth-method>CLIENT-CERT</auth-method>
    <realm-name>Client Cert Users-only Area</realm-name>
</login-config>
<security-constraint>
    <!-- Authorization setting for SSL -->
    <web-resource-collection >
        <web-resource-name >SSL</web-resource-name>
        <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <user-data-constraint>
        <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
</security-constraint>
```

#### 9. 重启Tomcat。

#### 后续操作

证书安装完成后,可通过登录证书绑定域名的方式验证证书是否安装成功。

https://domain name:port #domain name替换成证书绑定的域名

如果网页地址栏出现绿色小锁标志,表示证书安装成功。

验证证书是否安装成功时,如果网站无法通过https正常访问,需确认您安装证书的服务器443端口 是否已开启或被其他工具拦截。

#### 相关文档

- ・在Tomcat服务器上安装SSL证书
- #unique\_32
- **#unique\_33**
- **#unique\_34**
- #unique\_35
- #unique\_36
- #unique\_37

### 6.2.2 安装JKS格式证书

您可以将下载的证书安装到Tomcat服务器上。Tomcat支持PFX格式和JKS两种格式的证书,您可 根据选您Tomcat的版本择其中一种格式的证书安装到Tomcat上。

背景信息

- ·本文档证书名称以domain name为示例,如证书文件名称为domain name.pfx,证书密码文件名称为pfx-password.txt。
- ・申请证书时如果未选择系统自动创建CSR,证书下载压缩包中将不包含.txt文件。需要您选择其 他类型服务器下载.crt证书,并使用openssl命令生成pfx文件。

操作指南

- 1. 登录阿里云SSL证书控制台。
- 在SSL证书页面,点击已签发标签,定位到需要下载的证书并单击证书卡片右下角的下载打开证 书下载对话框。

未签发4	审核失败 1	已签发 152	即将过其
实例: - (上传)	)		-
绑定域名: 到期时间:20	28年8月31日	and the Pa	
已签发		部署到云产品 >	下载删除

- 3. 在证书下载对话框中定位到Tomcat服务器,并单击右侧操作栏的下载将Tomcat版证书压缩包 下载到本地。
- 4. 解压Tomcat证书。您将看到文件中有一个证书文件(以.pfx为后缀或文件类型)和一个密码文件(以.txt为后缀或文件类型)。

新建文件夹			
名称	•	修改日期	类型
🔯 domain name.pfx		2018/12/18 17:45	Personal Inform
pfx-password.txt		2018/12/18 17:45	文本文档



每次下载证书都会产生新的密码,该密码仅匹配本次下载的证书。如果需要更新证书文件,同时也要更新匹配的密码文件。

5. 输入以下JAVA JDK命令将PFX格式的证书转换成JKS格式。

```
keytool -importkeystore -srckeystore domain name.pfx -destkeystore
domain name.jks -srcstoretype PKCS12 -deststoretype JKS
```



Windows系统中, 需在%JAVA\_HOME%/jdk/bin目录下执行该命令。

6. 回车后输入PFX证书密码和JKS证书密码。



JKS证书密码等同于PFX证书密码。两个密码不同的时候会导致Tomcat重启失败。

- 7. 在Tomcat安装目录下新建cert目录,将证书和密码文件拷贝到cert目录下。
- 8. 打开Tomcat安装目录 > conf文件夹 > server.xml文件, 在server.xml文件中找到 <

Connector port="8443"标签并进行修改。

```
<!--

<Connector port="8443"

protocol="HTTP/1.1"

port="8443" SSLEnabled="true"

maxThreads="150" scheme="https" secure="true"

clientAuth="false" sslProtocol="TLS" />

-->
```

参考以下完整配置(其中port属性请根据您的实际情况修改):

```
<Connector port="443"
    protocol="HTTP/1.1"
    SSLEnabled="true"
    scheme="https"
    secure="true"
    keystoreFile="cert/domain name.jks" #此处keystoreFile代表证书文件
的路径,请用您证书的文件名替换domain name。
    keystoreType="PKCS12"
    keystorePass="证书密码" #请用您证书密码文件中的密码替换"证书密码"。
    clientAuth="false"
    SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
    ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256
_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_A
ES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WI
TH_AES_256_CBC_SHA256"/>
```

- 9. 保存server.xml文件配置。
- 10. (可选步骤) 配置web.xml文件开启HTTP强制跳转HTTPS。

```
#在</welcome-file-list>后添加以下内容:
<login-config>
```

```
<!-- Authorization setting for SSL -->
<auth-method>CLIENT-CERT</auth-method>
<realm-name>Client Cert Users-only Area</realm-name>
</login-config>
<security-constraint>
<i!-- Authorization setting for SSL -->
<web-resource-collection >
<web-resource-name >SSL</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

#### 11.重启Tomcat。

#### 后续操作

证书安装完成后,可通过登录证书绑定域名的方式验证证书是否安装成功。

https://domain name:port #domain name替换成证书绑定的域名

如果网页地址栏出现绿色小锁标志,表示证书安装成功。

验证证书是否安装成功时,如果网站无法通过https正常访问,需确认您安装证书的服务器443端口 是否已开启或被其他工具拦截。

### 6.3 在Apache服务器上安装SSL证书

您可以将从阿里云SSL证书控制台下载的证书安装到您的Apache服务器上,使Apache服务器支持HTTPS安全访问。

#### 前提条件

- · 已安装OpenSSL。
- ·本文档证书名称以domain name为示例,如证书文件名称为domain name\_public.crt,证书链文件名称为domain name\_chain.crt,证书秘钥文件名称为domain name.key。
- ·申请证书时如果未选择系统自动创建CSR,证书下载压缩包中将不包含.key文件。

### 📕 说明:

.crt扩展名的证书文件采用Base64-encoded的PEM格式文本文件,可根据需要修改成.pem等 扩展名。

#### 操作指南

1. 登录阿里云SSL证书控制台。

 在SSL证书页面,点击已签发标签,定位到需要下载的证书并单击证书卡片右下角的下载打开证 书下载对话框。

未签发 <mark>4</mark>	审核失败 1	已签发 152	即将过其
实例: - (上传)			-
绑定域名: 到期时间: 20	28年8月31日	and the first	
已签发		部署到云产品 > 下	载删除

- 3. 在证书下载对话框中定位到 Apache服务器 ,并单击右侧操作栏的下载将Apache版证书压缩包 下载到本地。
- 4. 解压Apache证书。

您将看到文件夹中有3个文件:

- ・证书文件(以.crt为后缀或文件类型)
- · 证书链文件(以.crt为后缀或文件类型)
- ·秘钥文件(以.key为后缀或文件类型)

新建文件夹			
名称	<u>^</u>	修改日期	类型
🗋 domain name.key		2018/12/18 15:39	KEY 文件
🗔 domain name_chain.crt		2018/12/18 15:39	安全证书
aomain name_public.crt		2018/12/18 15:39	安全证书

5. 在Apache安装目录中新建cert目录,并将下载的Apache证书、证书链文件和秘钥文件拷贝 到cert目录中。

# 🗐 说明:

如果申请证书时选择了手动创建CSR文件,请将手动生成创建的秘钥文件拷贝到cert目录中并 命名为domain name.key。

6. 在Apache安装目录下,打开Apache/conf/httpd.conf,在httpd.conf文件中找到以下参

数并进行配置。

```
#LoadModule ssl_module modules/mod_ssl.so #删除行首的配置语句注释符
号 "#" 加载mod_ssl.so模块启用SSL服务, Apache默认是不启用该模块的。如果找不到该
配置, 请重新编译mod_ssl模块。
#Include conf/extra/httpd-ssl.conf #删除行首的配置语句注释符号 "#"。
```

- 7. 保存httpd.conf文件并退出。
- 8. 打开Apache/conf/extra/httpd-ssl.conf,在httpd-ssl.conf文件中找到以下参数并

进行配置。证书路径建议使用绝对路径。

**1** 说明:

根据操作系统的不同, http-ssl.conf文件也可能存放在conf.d/ssl.conf目录中。

```
SSLProtocol all -SSLv2 -SSLv3 # 添加SSL协议支持协议, 去掉不安全的协议。
SSLCipherSuite HIGH:!RC4:!MD5:!aNULL:!eNULL:!DH:!EDH:!EXP:+
MEDIUM # 使用此加密套件。
SSLHonorCipherOrder on
SSLCertificateFile cert/domain name_public.crt # 将domain
name_public.crt替换成您证书文件名。
SSLCertificateKeyFile cert/domain name.key # 将domain name.key替换
成您证书的秘钥文件名。
SSLCertificateChainFile cert/domain name_chain.crt # 将domain
name_chain.crt替换成您证书的秘钥文件名;证书链开头如果有#字符,请删除。
```

9. 保存 httpd-ssl.conf 文件配置并退出。

10.重启Apache服务器使SSL配置生效。

a. 在Apache bin目录下执行以下命令停止Apache服务。

apachectl -k stop

b. 在Apache bin目录下执行以下命令开启Apache服务。

apachectl -k start

11. (可选步骤) 设置Apache http自动跳转https。

在 httpd.conf 文件中, 在<VirtualHost \*:80> </VirtualHost>中间, 添加以下重定 向代码。

RewriteEngine on RewriteCond %{SERVER\_PORT} !^443\$ RewriteRule ^(.\*)\$ https://%{SERVER\_NAME}\$1 [L,R]

#### 后续操作

证书安装完成后,可通过登录证书绑定域名的方式验证证书是否安装成功。

https://domain name #domain name替换成证书绑定的域名

如果网页地址栏出现绿色小锁标志,表示证书安装成功。

验证证书是否安装成功时,如果网站无法通过https正常访问,需确认您安装证书的服务器443端口 是否已开启或被其他工具拦截。

#### 相关文档

- ・ 在Tomcat服务器上安装SSL证书
- #unique\_32
- #unique\_33
- #unique\_34
- #unique\_35
- #unique\_36
- #unique\_37

### 6.4 在Nginx/Tengine服务器上安装证书

您可以从阿里云SSL证书服务控制台下载证书安装到您的Nginx/Tengine服务器上。

#### 背景信息

本文档以CentOS 7、Nginx 1.15.6为例。

本文档证书名称以domain name为示例,如证书文件名称为domain name.pem,证书密钥文件 名称为domain name.key。

下载的Nginx证书压缩文件解压后包含:

- · .pem: 证书文件。PEM文件的扩展名为CRT格式。
- · .key: 证书的密钥文件。申请证书时如果未选择自动创建CRS,则下载的证书文件压缩包中不 会包含.key文件,需要您将自己手动常见的私钥文件拷贝到cert目录下。



.pem扩展名的证书文件采用Base64-encoded的PEM格式文本文件,您可根据需要修改成其他扩展名。

#### 证书的格式详见主流数字证书都有哪些格式。

#### 操作指南

- 1. 登录阿里云SSL证书控制台。
- 在SSL证书页面,点击已签发标签,定位到需要下载的证书并单击证书卡片右下角的下载打开证 书下载对话框。

未签发 4	审核失败 1	已签发 152	即将过其
实例: - (上传)	)		-
绑定域名: 到期时间:20	28年8月31日	and the first	
已签发		部署到云产品 > 🗍	「载 删除

- 3. 在证书下载对话框中定位到Nginx/Tengine服务器,并单击右侧操作栏的下载将Nginx版证书 压缩包下载到本地。
- 4. 解压Nginx证书。

您将看到文件夹中有2个文件:

- · 证书文件(以.pem为后缀或文件类型)
- ·密钥文件(以.key为后缀或文件类型)

新建文件夹			
名称	-	修改日期	类型
domain name.key		2018/12/18 17:11	KEY 文件
domain name.pem		2018/12/18 17:11	PEM 文件

5. 在Nginx安装目录下创建cert目录,并将下载的证书文件和密钥文件拷贝到cert目录中。



如果您在申请证书时选择手动创建CSR文件,请将对应的密钥文件放到cert目录中,并命名为domain name.key。

6. 打开Nginx安装目录 > conf文件夹 > nginx.conf文件,在nginx.conf文件中找到以下属性:

```
# HTTPS server
server {
    listen 443;
    server_name localhost;
    ssl_or;
    ssl_certificate cert.pem;
    ssl_certificate_key cert.key;
    ssl_session_timeout 5m;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+
EXP;
    ssl_prefer_server_ciphers on;
    location / {
```

修改nginx.conf文件如下:

```
# 以下属性中以ssl开头的属性代表与证书配置有关,其他属性请根据自己的需要进行配置。
server {
listen 443;
server_name localhost; # localhost修改为您证书绑定的域名。
         #设置为on启用SSL功能。
ssl on;
root html;
index index.html index.htm;
ssl_certificate cert/domain name.pem;
                                    #将domain name.pem替换成您证书
的文件名。
                                        #将domain name.key替换成您
ssl_certificate_key cert/domain name.key;
证书的密钥文件名。
ssl_session_timeout 5m;
ssl ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!
aNULL:!MD5:!ADH:!RC4; #使用此加密套件。
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
                                    #使用该协议进行配置。
ssl_prefer_server_ciphers on;
location / {
root html;
            #站点目录。
index index.html index.htm;
}
}
```

- 7. 保存nginx.conf文件后退出。
- 8. 重启Nginx服务器。

```
〕 说明:
```

如果您有配置多个虚拟主机Include conf/vhost,参考虚拟主机配置SSL证书进行配置。

9. (可选步骤)设置http请求自动跳转https。

在需要跳转的http站点下添加以下rewrite语句,实现http访问自动跳转到https页面

```
server {
  listen 80;
  server_name localhost;
  rewrite ^(.*)$ https://$host$1 permanent;
```

```
location / {
index index.html index.htm;
}
```

#### 虚拟主机配置SSL证书

1. 打开虚拟主机配置文件vhost.conf或\*.conf,复制以下内容粘贴到下方位置、将端口改

为443(https默认端口)并增加证书相关配置。

```
server {
listen 80;
server_name localhost ;
location / {
index index.html index.htm;
}
server {
listen 443;
server_name localhost;
ssl on;
root html;
index index.html index.htm;
ssl_certificate cert/domain name.pem; #将domain name.pem替换成您证书
的文件名。
ssl_certificate_key cert/domain name.key;
                                            #将domain name.key替换成您
证书的密钥文件名。
ssl_session_timeout 5m;
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!
aNULL: !MD5: !ADH: !RC4;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_prefer_server_ciphers on;
location / {
index index.html index.htm;
}
```

- 2. 保存nginx.conf文件后退出。
- 3. 重启Nginx服务器。

安装证书相关文档:

- ・在Tomcat服务器上安装SSL证书
- #unique\_41
- #unique\_32
- #unique\_33
- #unique\_35
- #unique\_36
- #unique\_37

### 6.5 在IIS服务器上安装证书

您可将下载的阿里云SSL证书安装到IIS服务器上,使您的IIS服务器支持HTTPS安全访问。

前提条件

申请证书时需要选择系统自动创建CSR。

申请证书时如果选择手动创建CSR,则不会生成证书文件。您需要选择其他服务器下载.crt证书文件后,使用openssl命令将.crt文件的证书转换成.pfx格式。

操作指南

- 1. 登录阿里云SSL证书控制台。
- 在SSL证书页面,点击已签发标签,定位到需要下载的证书并单击证书卡片右下角的下载打开证 书下载对话框。

A NAMER THE REPORT					全部状态 864	~ 全部政務	<ul> <li>         ·   ·        ·        ·</li></ul>	Q 89
> 未签发								
> 已签发								
证书	品牌	状态	病定域名	有效期限	已終發			操作
	Contraction (1997)	已整发		1年 2020年7月23日到期			洋橋(東朝	5 - TEL RM
10000		Bate	Coloring and Color	1年			洋橋(遺歌) 部項	

- 3. 在证书下载对话框中定位到IIS服务器,并单击右侧操作栏的下载将IIS版证书压缩包下载到本 地。
- 4. 解压IIS证书。您将看到文件中有一个证书文件(以.pfx为后缀或文件类型)和一个秘钥文件(以.txt为后缀或文件类型)。

服务器证书文件 ▶ 1570059_key.test.co	m_IIS PFX				
新建文件夹					
名称	-	修改日期	类型	大小	
31570059_key.test.com.pfx		2018/12/3 21:19	Personal Inform		3 KB
pfx-password.txt		2018/12/3 21:19	文本文档		1 KB



每次下载证书都会产生新的密码,该密码仅匹配本次下载的证书。如果需要更新证书文件,同时也要更新匹配的密码文件。

- 5. 在控制台操作对话框中导入您下载的IIS证书文件。
  - a. 单击开始 > 运行 > MMC打开控制台。



b. 单击文件 > 添加/删除管理单元打开添加/删除管理单元对话框。

4	控制	台1	- [控制台根	[节点]				
	文作	<b>#(F)</b>	操作(A)	查看(V)	收藏夹(O)	窗口(W)	帮助(H)	
		新建	≹(N)			C	trl+N	
		打开	F(O)			C	trl+0	
		保存	<b>₹(</b> S)			C	Ctrl+S	
		另存为(A)						
		添加	1/删除管理	单元(M)		C	trl+M	
	选项(P)							
	1 C:\windows\system32\comexp							
	2 C:\windows\system32\services							
		3 C:\windows\system32\devmgmt						
		4 C:\windows\system32\compmgmt						
		退出	1(X)					

c. 在可用的管理单元中单击证书 > 添加 > 计算机账户 > 本地计算机(运行此控制台的计算机)
 > 完成。

添加或删除管理单元		X
您可以在计算机上为此控制台选择可用的管理单元并配置所选 展项。	的一组管理单元。对于可扩展的管理单元,	您可以配置要启用哪些扩
可用的管理单元(S):	所选管理单元(E):	
管理单元 供应商 🔺	■ 控制台根节点	编辑扩展(X)
帰打印管理 Microsoft の 服务 Microsoft		删除(R)
☆高级安全 Windows Microsoft		
1 10 Nicrosoft		
│ ▲ 计算机管理     Microsoft		 
All All All All All All All All All Al		1 19 (D)
■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	<b>-</b>	
■		
││		
◎ 性能监视器 Microsoft		
₩世世 Microsoft		
Jut Land Land Land Land Land Land Land Land		
● 组件服务 Microsoft 「		
描述:		
证书管理单元允许您浏览自己的、一个服务的或一台计算机的	〕证书存储内容。	
		确定 取消
		10/13

d. 在控制台左侧导航栏单击控制台根节点下的证书打开证书树形列表。



e. 单击个人 > 证书 > > 所有任务 > 导入打开证书导入向导对话框。

😼 控制台1 - [控制台根节点]		
💫 文件(F) 操作(A) 査看(V)	收藏夹(O) 窗口(W) 帮助(H)	
<ul> <li></li></ul>	名称 家 证书(本地计算机)	
▶ <sup>□</sup> 中级 ▶ <sup>□</sup> 中级 ▶ <sup>□</sup> 受信	□(w) 高级操作(A) >	
<ul> <li>▷ □ 不信     <li>帮助(H)</li> <li>▷ □ 第三方根证书颁发机构     <li>▷ □ 受信任人     </li> </li></li></ul>		
<ul> <li>▷ <sup>(1)</sup> Homegroup Machine</li> <li>▷ <sup>(2)</sup> 证书注册申请</li> <li>▷ <sup>(2)</sup> 智能卡受信任的根</li> </ul>	C	
> 🗎 受信任的设备		

### f. 单击浏览导入下载的PFX格式证书文件。

说明:

(北日) 向日	1010		
市民、始立体		E书文件 🕨 1570059_key.test.com_IIS PFX	▼ 🍫 搜索 1570059_key.te.
<b>安守入的文件</b> 指定要导入的文件。	组织 ▼ 新建文件夹		
	★ 收藏夹 ▲ 名称	《修改日期	类型 大小
又仟名(F):	— 🔰 下载 🔂 1570059_ke	y.test.com.pfx 2018/12/3 21:19	Personal Inform 3 K
	■ 桌面 pfx-passwor	d.txt 2018/12/3 21:19	文本文档 1 K
注意: 用下列格式可以在一个文件中存储一个以上证书:	😓 最近访问的位置		
个人信息交换— PKCS #12 (.PFX,.P12)			
加密消息语法标准- PKCS #7 证书(.P7B)			
Microsoft 序列化证书存储(.SST)			
	▲ 图片		
	→ 音乐		
了解 <u>证书文件格式</u> 的详细信息			
	🥾 计算机		
< 上一步(B) 【T	一步 文件名(N): 1570059_ke	y.test.com.pfx 👻	所有文件(*.*)
2			打开(O) ▼ 取消

在导入证书文件时,文件名右侧文件类型下拉菜单中请选择所有文件类型。

#### g. 输入证书秘钥文件里的密码。

您可在下载的IIS证书文件中打开pfx-password .txt文件查看证书密码。

证书导入向导	X
<b>密码</b> 为了保证安全,已用密码保护私钥。	
为私钥键入密码。 密码(P):	
启用强私钥保护。如果启用这个选项,每次应用程序使用私钥时,您都会得到 提示(E)。	
标志此密钥为可导出的密钥。这将允许您在稍后备份或传输密钥(M)。	
☑包括所有扩展属性(A)。	
了解 <u>保护私钥</u> 的更多信息	
< 上一步(B) 下一步(N) >	

h. 勾选根据证书类型, 自动选择证书存储并单击下一步完成证书的导入。

<b>证书存储</b> 证书存储是保存证书的系统区域。
₩indows 可以自动选择证书存储,或者您可以为证书指定一个位置。
◎ 根据证书类型,自动选择证书存储(U)
◎ 将所有的证书放入下列存储(P)
证书存储: 个人
了解 <u>证书存储</u> 的更多信息
< 上一步(B) 下一步(N) > 取消

- 6. 分配服务器证书。
  - a. 打开IIS8.0 管理器面板,定位到待部署证书的站点,单击绑定。
  - b. 在网站绑定对话框中单击添加 > 选择https类型 > 端口选择443 > 导入的IIS证书名称 > 确定。

📋 说明:

SSL 缺省端口为 443 端口,请不要修改。如果您使用其他端口如:8443,则访问网站时必须输入https://www.domain.com:8443)。

安装证书相关文档:

- · 在Tomcat服务器上安装SSL证书
- #unique\_41
- #unique\_32
- #unique\_33
- #unique\_34
- #unique\_36
- #unique\_37

### 6.6 在GlassFish服务器上安装证书

本文档介绍如何在Glassfish服务器上安装SSL证书。

操作步骤

本文档证书名称以cer01为示例,如证书文件名称为cer01.pem,证书秘钥文件名称为cer01.key。

1. 登录阿里云SSL证书控制台。

 在SSL证书页面,点击已签发标签,定位到需要下载的证书并单击证书卡片右下角的下载打开证 书下载对话框。

未签发4	审核失败 1	已签发 152	即将过其
实例: - (上传	)		-
绑定域名: 到期时间:20	28年8月31日	and the re-	
已签发		部署到云产品 > 📑	载删除

- 在证书下载对话框中定位到其他服务器类型,并单击右侧操作栏的下载将证书压缩包下载到本 地。
- 4. 解压证书。您将看到文件中有一个证书文件(以.pem为后缀或文件类型)和一个秘钥文件(以.txt为后缀或文件类型)。

	All certificates	other PEM				
新建文件夹						
名称	A	修改日期	类型			
cer01.key		2018/12/3 21:19	KEY 文件			
cer01.pem		2018/12/3 21:19	PEM 文件			

5. 输入以下两行命令将证书和秘钥文件转换成JKS格式。

openssl pkcs12 -export -in cer01.pem -inkey cer01.key -out temp.p12 -passout pass:changeit -name slas #请用您的证书名称替换命令行中cer01.pem、用您的证书秘钥替换cer01.key。转换证书 格式时设置的密码必须和您Glassfish服务器中自带的证书密码一致,该证书默认密码是 changeit。

```
keytool -importkeystore -srckeystore temp.p12 -srcstoretype PKCS12 -
srcstorepass changeit -deststoretype JKS -destkeystore ./glassfish5
/glassfish/domains/domain1/config/keystore.jks -deststorepass
changeit -alias s1as
#转换证书格式时设置的密码必须和您Glassfish服务器中自带的证书密码一致,该证书默认
密码是changeit。
```

6. 重启domain。

./glassfish5/bin/asadmin restart-domain

7. 检查您阿里云证书绑定的域名是否生效。

wget https://127.0.0.1:8181

# 7吊销证书

阿里云SSL证书服务支持对证书进行吊销处理。

当您无需再使用证书时,或者处于安全因素考虑,可随时申请吊销证书。

证书签发后的30天内完成吊销可全额退款,签发超过30天或30天内无法完成吊销,不退款。

📋 说明:

上传的证书无法吊销。

证书吊销后可删除。吊销和删除的区别详见#unique\_45

操作步骤

注意:

证书提交吊销后将无法查看或下载,请谨慎操作。

- 1. 登录阿里云SSL证书控制台。
- 2. 定位到已签发页面。
- 3. 选择需要吊销的证书并单击吊销。

■ 別天证书					全部状态 863	∨ 全部品牌	✓ 证书域名 (	ર 89 ≣
> 未签发								
∨ 已签发								
证书	品牌	状态	绑定城名	有效期限	已部署			操作
and a second sec		已签发	1.000	1年 2020年7月23日到期			洋情  部署 ~	下载用销
	(product)	已签发		1 年 2020年7月18日到期			洋情 退款  部署 >	下载 吊销

- 4. 填写吊销申请并单击下一步提交申请。
- 5. 验证并提交审核。

审核通过后证书吊销成功。吊销DV证书当天完成审核,吊销OV/EV证书审核时间为3-5个工作 日。

# 8 全站HTTPS

### 8.1 全站HTTPS介绍

SSL证书支持全站HTTPS服务,帮助您解决SSL证书安装部署、证书到期更新、证书私钥安全存储 及TLS加速等问题。

将服务器域名的DNS记录解析到该服务的CNAME域名上,即可将您原来的站点服务器设置为全站 HTTPS服务。

功能优势

- · 使用全站HTTPS服务,无需再关注证书时间到期之前,重新申请并部署证书的问题。
- · 使用全站HTTPS服务,无需再关注证书时间到期后,网站无法提供服务的问题。
- 使用全站HTTPS服务,无需再关注各种加密套件的选择和配置问题。全站HTTPS服务的安全配 置支持苹果的ATS、腾讯公司的微信小程序和支付宝小程序及支付接口回调的要求。当仅配置证 书开启HTTPS服务时,如果使用错误或低级别的安全套件会使网站出现数据泄露的信息安全问题。
- ・使用全站HTTPS服务,提高保障数据传输和网上通信的安全性。您可以查看全站HTTPS服务站 点在SSL Labs的检测结果是A+。

私钥安全性

一般站点服务器的证书和密钥全部部署安装在Web服务器所属主机上。用户访问时,Web服务器会 直接处理用户的应用层请求,如果Web服务器存在漏洞(例如:缓冲区溢出等),则有可能导致密 钥泄漏,并占用Web服务器的CPU资源。

全站HTTPS服务采用的是阿里云自主研发的证书安全服务,将证书私钥文件加密保存 在KeyManager服务节点中。KeyManger是基于HSM使用信封加密的方式加密存储业务方密 钥,确保密钥的安全性。如果Web服务器出现漏洞,通知Web服务器将TLS/SSL的卸载转发 给KeyServer服务,KeyServer服务会按需到KeyManager服务获取私钥文件,并加密保存私钥 文件至内存中,而不会在硬盘中保存私钥文件。所以即便服务器被攻破了,也仍然无法获取到私 钥。

# **道** 说明:

Web服务器和KeyServer及KeyServer与KeyManager之间有严格的身份校验规则,同时使用TLS加密隧道进行数据交流。

#### TLS/SSL加速

TLS/SSL加速,即通过特定的算法优化内存中的私钥缓存数据。Tengine和KeyServer之间,KeyServer和KeyManager之间均采用保活连接,减少TCP握手和TLS握手的开销。同时KeyServer服务器上安装了英特尔公司的QAT双加速卡,通过冗余来保证高可用和容灾(每个Web服务器配置多个KeyServer集群,每个KeyServer配置多个KeyManager集群)。

### 8.2 开启全站HTTPS服务

本文档介绍如何开启全站HTTPS服务功能。

开启全站HTTPS服务流程如下:



您可以参考以下步骤添加站点:

1. 登录阿里云SSL证书控制台。

#### 2. 您可以参考以下三种方法进入添加站点页面。

- ・通过全站HTTPS
  - a. 在SSL证书控制台,单击全站HTTPS,进入全站HTTPS页面。

SSL证书				
证书购买后,需要完善说 购买证书	正书信息并提交审核通过后才前 ▶ 完善资料、提交审核	能使用。 <u>查看详细使用说明</u> DV型&免费证书 OV&EV型证书	我需要人工服务指导 域名所有权验证 组织机构验证	▶ 部署订
证书总数 ② 863	已签发的证书 735	<sup>待申请的证书</sup> 75	即将过期的证书 ②	审核失败的证书 30
📜 购买证书	▲ 上传证书 ② 全	站HTTPS		

b. 单击添加站点。

1	全站HTTPS り 返回证书列表					
	透知站点					
	城名	CName	接入状态	证书状态	证书到期时间	操作

· 通过已签发证书的部署操作

在SSL证书控制台已签发证书列表,单击证书右侧操作下的部署,并选择全站HTTPS。

	〒 购买证书 ▲ 上传证书	② 全站HTTPS				全部状态 863 🗸 全部品牌	. × 278823 Q 80 ≣
	> 未签发						
C	~ 已签发						
	证书	品牌	状态	绑定域名	有效期限	已部署	提作
	64	-	已签发		1年 2020年7月23日到期		详摘 部署 人 下載 用機
	and the second second		已签发	100000	1年 2020年7月18日到期		
	an internet		已签发	3257	1 年 2020年7月18日到期		安全加速 详情   退款 全站加速
		-	已签发	Contraction of the Contraction o	1 年 2020年7月18日到期		全站HTTPS 详情丨退款

- ・通过已签发证书的下载操作
  - a. 在SSL证书控制台已签发证书列表,单击证书右侧操作下的下载。
  - b. 在证书下载页面, 单击全站HTTPS服务模块的免费试用。

	★ 約天道市 出日後道市	() 全站HTTPS				全部状态 863 🗸 全	部品牌 >	证15%名 Q	证书下载	>
	> 未签发								请根据您的股务器供型选择证"	5下载:
Ľ	~ 已然发								服务器类型	操作
	证书	品牌	状态	御定城名	有效期限	日部署			Torncat	帮助   下蚊
	- 2+0	<b>H</b> arana and A	已签发		1年 2020年7月16日到期			洋橋 部署~「下	Apache	報助 下銀
		-	已签发		1年 2020年7月16日初期			洋橋(部署> 下	Nginx	帮助 下戲
									lis	聯動一下戰
	And South Contraction	÷	已推发	the second se	1年 2020年7月11日到期			洋橋(部署~)下	并也	下號
		8 mile	已签发		1年 2020年7月4日到期			洋橋 部器~ 下	全始HTTPS服务 不用安装证书,不用纠结部	种安全寄件的选择,不用
			已过期	1000000	1年 2019年7月15日到期	负疑均衡		详情(下蚊)用	担心私明泄露,全站HTTPS HTTPS问题。	服务基础也能决网站

#### 3. 在添加站点页面, 添加站点域名。

在站点域名页签,阅读使用条款并勾选我已仔细阅读并同意该服务条款,然后输入待添加站点域 名。

添加站点						
站点域名 站点IP SSL选项 配置证书						
使用条款 <ol> <li>该服务提供SSL证书的生命周期管理及TLS硬件加速服务,您不需要在自己的站点部署SSL证书,只需要将域名的DNS记录CNAME到该服务提供的域名;</li> <li>该服务目前不具备安全防护能力,如您的站点用了阿里云的WAF和高防,不推荐您使用该服务;</li> <li>使用该服务的站点必须经过备案,如您的站点遭受到攻击或者违反法律规定,阿里云有权利对您</li> </ol>						
站点停止使用该服务; 4、该服务目前处于公测阶段,您可以免费试用 3 个月。试用结束后,如果您没有购买服务,我们将 不再为您提供服务,将导致您的网站不可访问或者访问出错。请您留意我们的通知,及时购买服务; 5、公测期间,每个用户限制添加3个域名;						
<ul> <li>6、对于该服务,阿里云有最终解释权;</li> <li>✓ 我已仔细阅读并同意该服务条款</li> <li>● 域名:</li> </ul>						
ş.com						

4. 单击右下角的下一步,进入站点IP页签。

#### 5. 在站点IP页, 配置网站源站地址。

支持IPv4和域名两种源站地址类型。系统会自动检测您源站的域名解析情况,给出默认选择。 您可以根据实际情况调整。

说明: 最多可以填写三个IPv4地址	止,系统会采用RR策略I	可源。			
添加站点					×
站点域名	站点IP	SSL选项	$\rightarrow$	配置证书	
请填写源站地址信息, 并,	点"下一步"				
源站地址: IPv4	✓ 请输入IP				
	多个IP地址(属 不要使用其他	多3个)用半角逗号分开, 产品的CNAME域名的IP	系统用轮询 地址	(RR) 策略回源	, 请

6. 单击下一步,进行步骤二:设置SSL选项。

#### 步骤二:设置SSL选项

您可以参考以下步骤进行安全配置:

1. 在SSL选项页签, 单击对应功能按钮, 开启/关闭功能。

SSL选项分为以下两种安全配置:

- 强制HTTPS访问:开启该功能,来自客户端(浏览器)的每一个HTTP协议的URL地址请求,都将被301重定向等效的HTTPS协议的URL地址,同时支持HSTS。即浏览器端的每个HTTP请求都会被跳转成HTTPS请求。
- · TLS/SSL卸载:开启该功能,来自客户端(浏览器)的每一个HTTP协议的请求,都将被重 定向到等效HTTPS协议的URL地址。即阿里云服务器使用HTTPS协议访问您的源站。

添加	加站点						$\times$
	站点域名		站点IP	SSL选项		配置证书	
	强制HTTPS访	问 🕐					
	开启该功能,浏 □= <sup>http</sup> 浏览器 <mark>http</mark>	览器端的每 )	个HTTP请求都会被跳掉  301   ● 阿里云	<sup>专成HTTPS</sup> 请求。	L L L L L L L L L L L L L L L L L L L		
ſ	TLS/SSL卸载	0					
	开启该功能,阿	里云服务器	使用HTTP协议访问您的	的源站。	1 = - =		
	山三 http 浏览器	o/https	──→ ● ht 阿里云	tp>	源站		

2. 单击下一步,进入步骤三:配置证书页签。

#### 步骤三:配置证书

如果添加的站点域名在SSL证书系统申请过证书且有效期大于90天,您可以选择已有证书。您也可 以根据需要重新申请证书。 1. 在配置证书页签,选择或申请证书文件。

添	加站点							$\times$
	站点域名		站点IP		SSL选项		配置证书	
	选择现有证书							
	请选择			$\sim$				
	通配符域名证书	ŝ						
	你的域名独享一张 Common Name	征书	m					
	仅保护		□, 小保护 ¥	/	年			
Ĩ	新申请一张证书	ŝ						
	你的域名独享一號 Common Name	铤书						
				免费申请	]			
								日本を
								が我们
						确	<b>认</b> 取	消

2. 单击确认,完成站点配置。

站点配置完后,会在全站HTTPS页的站点列表中呈现,然后进行步骤四:添加DNS解析记录。 步骤四:添加DNS解析记录

将已添加站点的DNS记录解析到该服务的CNAME域名。

1. 在全站HTTPS页的站点列表中,查看已添加站点的证书状态。

当证书状态是正常后,单击右侧操作栏下检测。

全站HT	TPS 5 返回证书列表					
添加	防点点					
城名		CName	接入状态	证书状态	证书到期时间	操作
-	The second second		异常 ⑦	正常	2020年7月16日	修改 证书 检测 删除
-	C. Conference	(help due (help	异常 ③	正常	2020年7月17日	修改 证书 检测 删除

2. 在接入检测页面,按照窗口给出的提示信息到您的DNS管理系统添加一条CNAME解析记录,完成您站点的接入配置。

添加解析记录请参考#unique\_49。

接入检	测		×
站点	接入状态进行检测		
Ø	系统资源准备完毕		
Ø	SSL证书准备完毕		
()	未发现域名解析记录,请	按照以下信息添加DNS记录,如配置请忽略。	
	记录类型	CNAME	
	主机记录	0	
	记录值	om	

#### 当站点接入状态是正常时,您的网站已经接入生效了,即开启了全站HTTPS服务。

全站HTTPS €	返回证书列表					
添加站点						
城名	CName		接入状态	证书状态	证书到期时间	操作
	Average Stationed	in a desired and the second	<b>#</b> # (0)	正常	2020年7月16日	修改 证书 检测 删除
	1000 CT0000		异常 ⑦	正常	2020年7月17日	修改 证书 检测 删除
-		a particular a provincia de la composición de la composi	异常 ③	升级中 ③	2020年7月17日	修改 检测 删除
			异常 ⑦	正常	2020年7月17日	修改 证书 检测 删除
-	La compañía	and the second sec	正常	正常	2020年7月18日	修改 证书

▋ 说明:

· 仅当站点的接入状态是异常,即未接入到全站HTTPS服务的站点才可以删除。

·已添加的站点支持修改源站地址、强制HTTPS访问功能、TLS/SSL卸载功能和证书配置。

#### 后续操作

请参见#unique\_50

### 8.3 修改DNS解析记录

修改域名的DNS解析记录,需要到您的域名DNS服务商系统中进行修改。本文档以阿里云DNS控制 台为例,介绍如何修改DNS解析记录。

当您完成全站HTTPS服务的添加站点及配置证书,且站点的接入状态和证书状态都正常后,控制 台会显示您站点专用的CName地址。可以使用该CNAME地址更新站点域名的CNAME解析记录 值,将网站的Web请求转发至全站HTTPS服务,完成该服务的接入。

操作步骤

您可以参考以下步骤修改DNS解析记录:

- 1. 登录云解析DNS控制台。
- 2. 在左侧导航栏,单击域名解析。选择待操作的域名,单击右侧操作列下的解析设置。
- 3. 选择待操作的域名,单击右侧操作栏下的解析设置。

云解析ONS / 域名解析				
域名解析				云解析DNS"免费版"与"付费版"的功能对比I
<ul> <li>公告: com/.net/.cn/.xin/.topl.xyz/.wp/.club/.shop/.wangi.ren等線名注册成功能必须进行域名实名认证, 否则会造成解析不生效, 实名认证率接通过后的1-2个工作</li> </ul>	日解析可恢复使用。宣誓详细			
全部域名         洪水量抗计         版本系質管理         更多服务				
形量自动动物 透加增多				✓ 総合快速提案 Q, 数量操作
城名	记录数	DNS服务器	付费版本	拥作
	0	③ 未使用阿里云解析	免费版	解析设置   升级   更多▼
S mox.	9	◎ 正常	免费版	解析设置   升级   更多 🕶
● 開除 更快分類				共2条 < 1 > 10 販页 ∨

4. 选择待操作的主机记录, 单击右侧操作栏下的修改。

关于域名的主机记录,以域名 abc.com为例:

- ·www:用于精确匹配www开头的域名,如www.abc.com。
- ・ @: 用于匹配根域名abc.com。
- ・\*: 用于匹配泛域名,包括根域名和所有子域名,如blog.abc.com、www.abc.com、abc
   .com等。

解析	解析设置									
⊘ ≚	前分配的DNS服务器是:	alatin en de	desare .							
模糊搜	索请用"关键字?"	搜索	新手引导						添加记录	导入/导出
	记录类型 💲	主机记录 💲	解析线路(isp) 🍦	记录值	MX优先级	TTL	状态	操作		
	А	www	默认	100000		10 分钟	正常	修改	停删除	备注
	А	@	默认	0.00.00.00		10 分钟	正常	修改 署	停删除	备注

#### 5. 在修改记录对话框中, 完成以下操作:

记录类型:	CNAME- 将域名指向另外一个域名	
主机记录:	WWW	
解析线路:	默认 - 必填!未匹配到智能解析线路时,	返回【默认】线路 \vee 🕐
* 记录值:	and the strength and the state of the state	

- ・记录类型:修改为CNAME。
- ·记录值:修改为已复制的WAF CNAME地址。
- ・其他设置保持不变。TTL值一般建议设置为10分钟。TTL值越大,则DNS记录的同步和更新 越慢。

关于修改解析记录:

- ・ 对于同一个主机记录,CNAME解析记录值只能填写一个,您需要将其修改为WAF CNAME 地址。
- 不同DNS解析记录类型间存在冲突。例如,对于同一个主机记录,CNAME记录与A记录、 MX记录、TXT记录等其他记录互相冲突。在无法直接修改记录类型的情况下,您可以先删 除存在冲突的其他记录,再添加一条新的CNAME记录。

📃 说明:

关于DNS解析记录互斥的详细说明,请参考解析记录冲突的规则。

- 6. 单击确定,完成DNS配置,等待DNS解析记录生效。
- 7. (可选)验证DNS配置。您可以Ping网站域名或使用17ce

📃 说明:

由于DNS解析记录生效需要一定时间,如果验证失败,您可以等待10分钟后重新检查。

#### 8. 查看DNS解析状态。

- a. 返回SSL证书控制台,进入全站HTTPS服务页面。
- b. 单击站点域名右侧操作栏中的检测。

接入检	测		×
站点	夏接入状态进行检测		
Ø	系统资源准备完毕		
Ø	SSL证书准备完毕		
0	未发现域名解析记录, i	请按照以下信息添加DNS记录,如配置请忽略。	
	记录类型	CNAME	
	主机记录	0	
	记录值	om	

# 8.4 阿里云企业邮箱接入全站HTTPS最佳实践

本文档介绍阿里云企业邮箱接入全站HTTPS服务的最佳实践。

背景信息

您需要已开通企业邮箱服务,并且设置了自己的企业邮箱域名。设置企业邮箱域名相关内容参见企 业邮箱。

操作步骤

1. 登录阿里云企业邮箱控制台。在左侧导航栏,单击邮箱列表。

■ (-) 阿里云	华东1(杭州) 🗸	Q 搜索	
企业邮箱	邮箱列表		
邮箱列表	全部邮箱 急需续费邮箱		
操作记录	城名: 到期日期: 芭 至	<b>討 搜索</b> 导出列表	
	□ 业务内容	产品名称	到期日期
		企业邮箱标准版-无限容量	2019年8月16日
	设置自动续费 取消自动续费 续费 转至其他账号		

2. 单击业务内容下的邮箱域名, 查看基本信息选项 , 获取邮箱访问地址。

基本信息	更换域名	设置解析	重置密码	重置安全问题	分配账号	
		邮箱域名:	m	更换域名		
		解析状态:	解析已生效 杜	检查域名解析 设置解	析	
	Ť	管理员账号:			習码 重置安全问	题
	邮箱	首访问地址:	-	ym 登录		
	已则	购买用户数:	50 扩容			
	企业	2网盘容量:	20G			
		产品名称:	企业邮箱标准	版-无限容量 升级		

- 3. 登录阿里云SSL证书控制台。
- 4. 单击全站HTTPS,进入全站HTTPS页面。

	SSL证书
	证书购买后,需要完善证书信息并提交审核通过后才能使用。查看详细使用说明   我需要人工服务指导       DV型&免费证书     域名所有权验证       购买证书     完善资料、提交审核       OV&EV型证书     组织机构验证
	证书总数 ②已签发的证书待申请的证书即将过期的证书 ③审核失败的证书86373575130
	▲ 上传证书 ② 全站HTTPS
5.	单击添加站点。

全站HTTPS 5 返回证书列表					
满加动动					
域名	CName	接入状态	证书状态	证书到期时间	操作

#### 6. 在添加站点页面,输入站点域名。

在站点域名页签,阅读使用条款并勾选我已仔细阅读并同意该服务条款,然后输入步骤3获取 的邮箱访问地址。

添加站点
站点域名 站点IP SSL选项 配置证书
使用条款 <ol> <li>该服务提供SSL证书的生命周期管理及TLS硬件加速服务,您不需要在自己的站点部署SSL证书,只需要将域名的DNS记录CNAME到该服务提供的域名;</li> <li>该服务目前不具备安全防护能力,如您的站点用了阿里云的WAF和高防,不推荐您使用该服务;</li> <li>使用该服务的站点必须经过备案,如您的站点遭受到攻击或者违反法律规定,阿里云有权利对您站点停止使用该服务;</li> <li>该服务目前处于公测阶段,您可以免费试用3个月。试用结束后,如果您没有购买服务,我们将不再为您提供服务,将导致您的网站不可访问或者访问出错。请您留意我们的通知,及时购买服务;</li> <li>公测期间,每个用户限制添加3个域名;</li> </ol>
<ul> <li>6、对于该服务,阿里云有最终解释权;</li> <li>✓ 我已仔细阅读并同意该服务条款</li> <li>• 域名:</li> </ul>

7. 单击右下角的下一步,在站点IP页,手动输入您的源站地址 。

支持IPv4和域名两种源站地址类型。此时源站地址类型选择域名。

添加站点				×
站点域名	站点IP	SSL选巧	,	配置证书
请填写源站地址信息	,并点"下一步"			
源站地址: 域	名 > mail.mxhic	hina.com		
	只支持一个域:	名回源		
				■ 联系 我们
			上一步	下一步 取消

8. 单击下一步,进入SSL选项,建议全部开启。

SSL选项分为以下两种安全配置:

- ·强制HTTPS访问:开启该功能,来自客户端(浏览器)的每一个HTTP协议的URL地址请求,都将被301重定向等效的HTTPS协议的URL地址,同时支持HSTS。即浏览器端的每个HTTP请求都会被跳转成HTTPS请求。
- ・TLS/SSL卸载: 开启该功能,来自客户端(浏览器)的每一个HTTP协议的请求,都将被重 定向到等效HTTPS协议的URL地址。即阿里云服务器使用HTTPS协议访问源站。

添加	站点							×
	站点域名		站点IP		SSL选项		配置证书	
3	强制HTTPS访问	?						
3	开启该功能,浏览 http- 浏览器 https-	器端的每个	HTTP请求都会被 → -301 ● → 阿里云	皮跳转成HTT 	PS请求。	○ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □		
	TLS/SSL卸载 ?	)						
9	开启该功能,阿里 回言 別览器	云服务器使 https	明HTTP协议访问 → ● の 回里云	]您的源站。 http——		源站		

9. 单击下一步,配置证书并完成服务接入,具体请参考开启全站HTTPS服务。