2017 可信云大会 可信云标准新一代 客户满意是未来
Cloud Computing Summit 2017.7.25-26

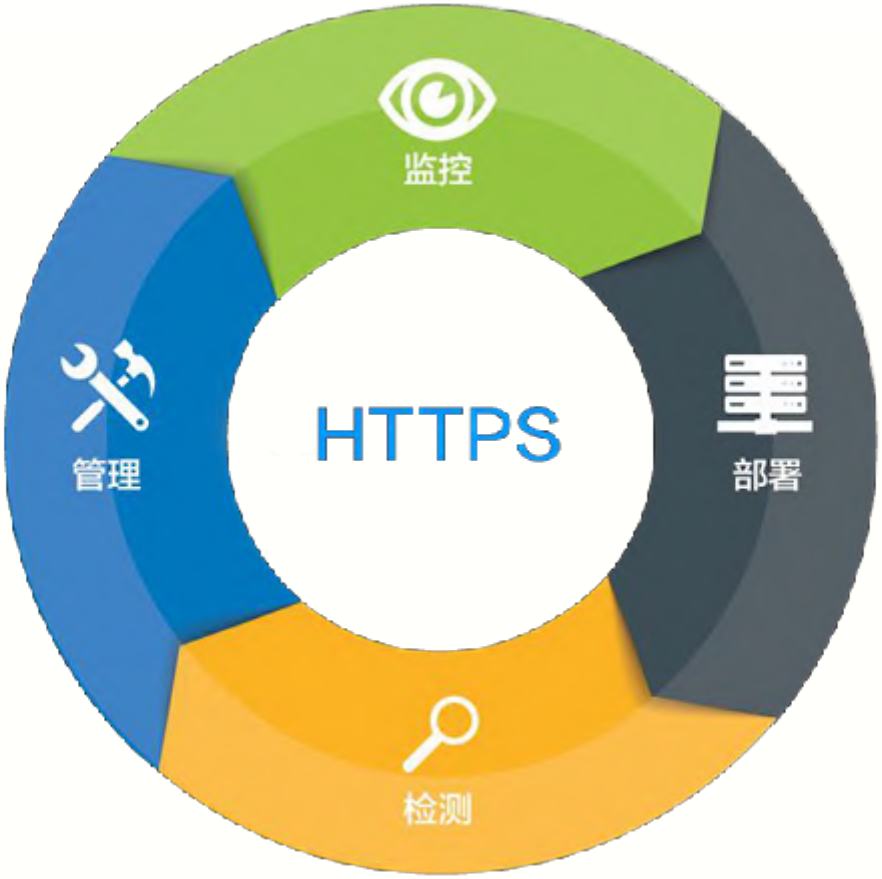
亞洲誠信 TRUSTAsia

现代化的HTTPS运维

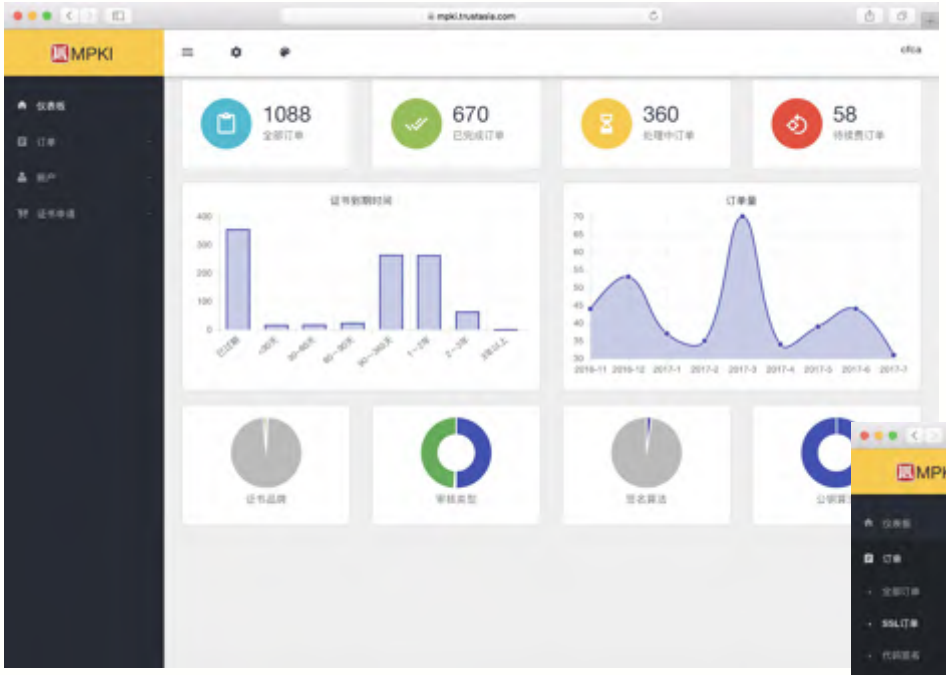
传统方式运维HTTPS面对的问题

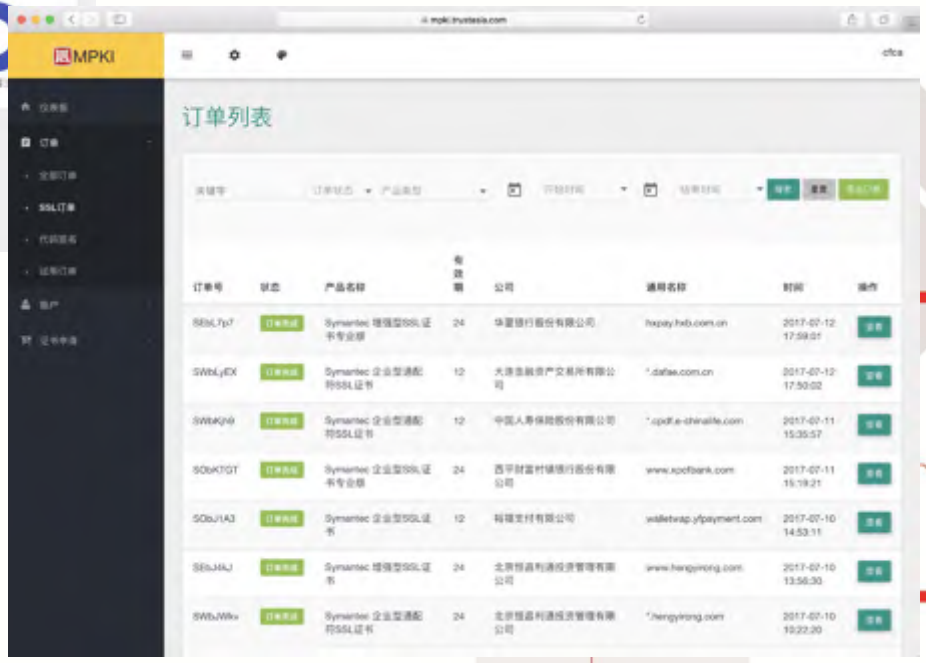
- 证书太多不知道每张证书什么时候到期
- 密钥对管理存在安全隐患
- 我的HTTPS是不是安全的
- 我的HTTPS客户端兼容性如何
- 我的HTTPS对服务器的性能消耗是不是合理的
- 我的HTTPS是否可以实现自动化运维

HTTPS全生命周期管理



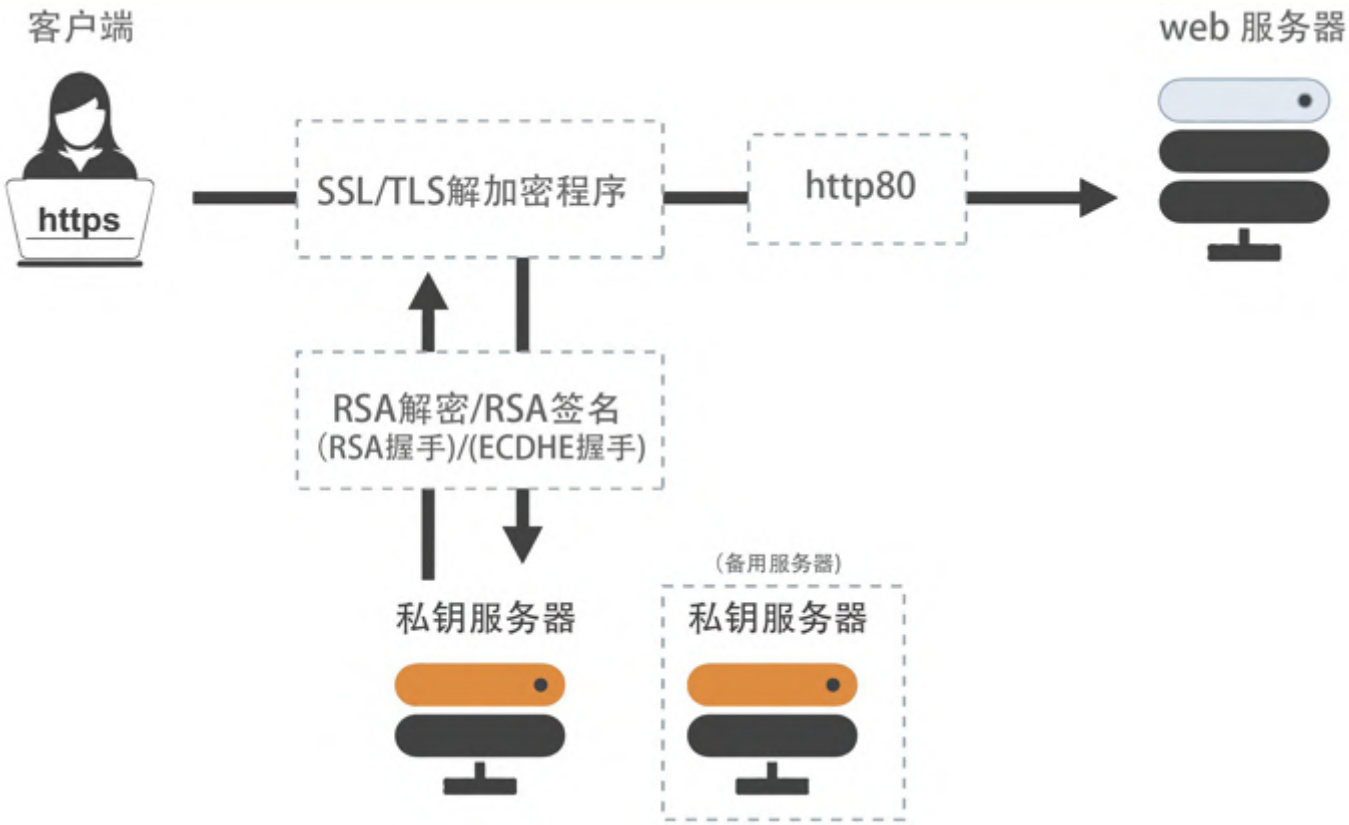
证书生命周期管理平台-MPKI





SSL证书管理
SSL证书申请
SSL证书吊销
SSL证书重颁发
SSL证书到期提醒
SSL证书更新

密钥安全管理（Keyless）



我的HTTPS是否安全？

- Web Server OpenSSL漏洞
- 不安全的SSL协议版本
- 不安全的SSL协议加密套件
- 证书链不完整
- 正向保密技术（PFS）
- 是否支持ATS
- 是否支持PCI DSS

我的HTTPS是否安全？

SSL漏洞

	是否影响	危险系数	说明
DROWN 漏洞	否	高	CVE-2016-0800
OpenSSL CCS 注入漏洞	否	高	CVE-2014-0224
心血漏洞(Heartbleed)	否	高	CVE-2014-0160
OpenSSL Padding Oracle 攻击	是	高	CVE-2016-2107
不安全的客户端重协商(MITM)	否	高	
FREAK漏洞	否	低	CVE-2015-0204
POODLE漏洞	否	低	CVE-2014-3566
CRIME漏洞	否	低	CVE-2012-4929

我的HTTPS客户端兼容性如何？

证书兼容性测试

	ECC	RSA
Android 2.3 (Gingerbread)	✓	✓
Android 3.2 (Honeycomb)	✓	✓
Android 4.0 (Ice Cream Sandwich)	✓	✓
Android 4.1 (Jelly Bean)	✓	✓
Android 4.2 (Jelly Bean)	✓	✓
Android 4.3 (Jelly Bean)	✓	✓
Android 4.4 (KitKat)	✓	✓
Android 5.0 (Lollipop)	✓	✓
Android 5.1 (Lollipop)	✓	✓
Android 6.0 (Marshmallow)	✓	✓
Android 7.0 (Android Nougat)	✓	✓
Android 7.1 (Android Nougat)	✓	✓
iOS 7	✓	✓
iOS 8	✓	✓
iOS 9	✓	✓
iOS 10	✓	✓
OS X Mavericks	✓	✓

我的HTTPS客户端兼容性如何？

客户端握手模拟

Android2.3.7 No SNI[2]	RSA2048(SHA256)	TLSv1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DHE 1024bits FS
Android4.0.4	RSA2048(SHA256)	TLSv1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECHDE secp256r1 FS
Android4.1.1	RSA2048(SHA256)	TLSv1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECHDE secp256r1 FS
Android4.2.2	RSA2048(SHA256)	TLSv1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECHDE secp256r1 FS
Android4.3	RSA2048(SHA256)	TLSv1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECHDE secp256r1 FS
Android4.4.2	RSA2048(SHA256)	TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECHDE secp256r1 FS
Android5.0.0	RSA2048(SHA256)	TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECHDE secp256r1 FS
Android6.0	RSA2048(SHA256)	TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECHDE secp256r1 FS
Android7.0	RSA2048(SHA256)	TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECHDE secp256r1 FS
BaiduJan2015	RSA2048(SHA256)	TLSv1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECHDE secp256r1 FS
BaiduSpiderJuly2017	RSA2048(SHA256)	TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECHDE secp256r1 FS
Baidu站长工具HTTPS认证	RSA2048(SHA256)	TLSv1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECHDE secp256r1 FS
BingPreviewJan2015	RSA2048(SHA256)	TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECHDE secp256r1 FS
Chrome49/XPSP3	RSA2048(SHA256)	TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECHDE secp256r1 FS

HTTPS如何进行性能和安全优化

协议详情

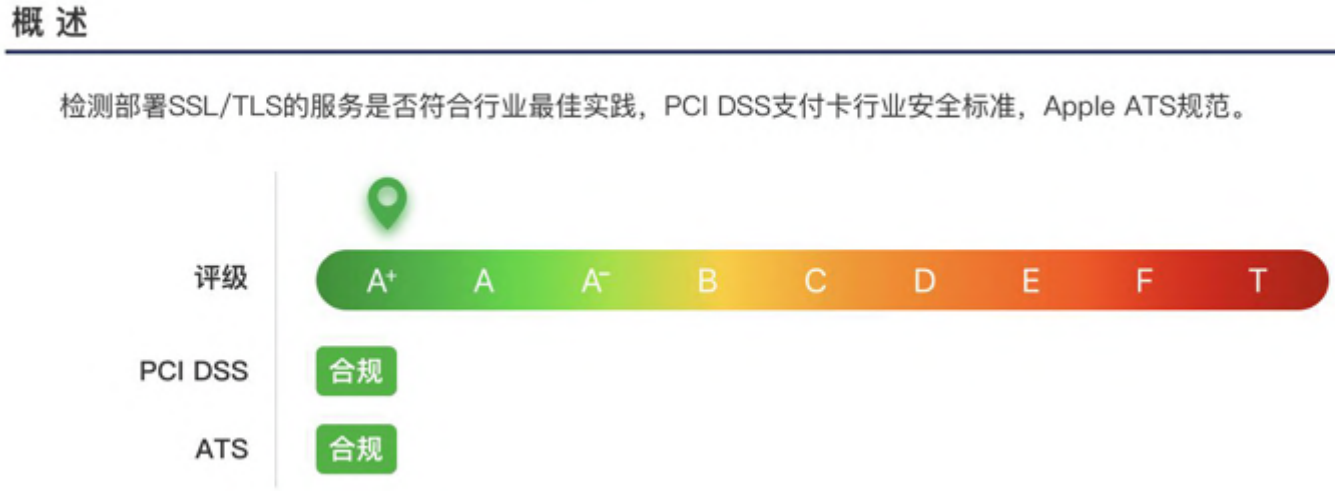
预防降级攻击	支持	
支持RC4套件	不支持	
正向保密	支持	
公钥固定（HPKP）	不支持	
公钥固定仅报告	不支持	
HSTS（HTTP严格传输安全）	支持	max-age=0
NPN	支持	h2,http/1.1
ALPN	支持	h2,http/1.1
OCSP装订	不支持	
TLS心跳（扩展）	支持	
支持的EC椭圆曲线	支持	secp256r1

HTTPS如何进行性能和安全优化

- 优先使用ECC证书（ECC+RSA）
- 优先使用AES、ECDHE算法
- 启用HTTP/2
- 启用OCSP装订
- 启用HSTS（减少一次302跳转）
- 启用TLS Session

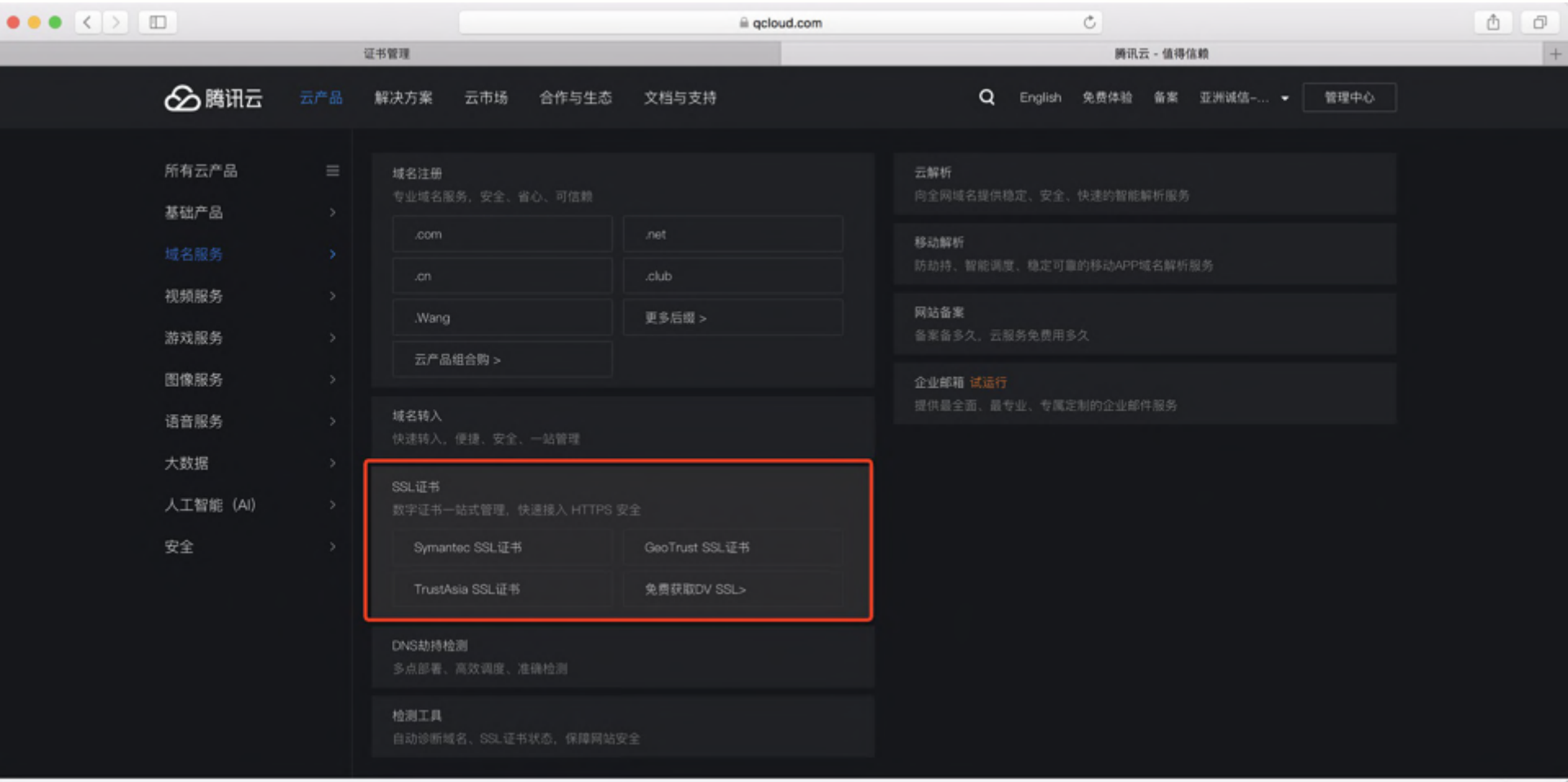
SSL/TLS安全评估系统

MySSL.com

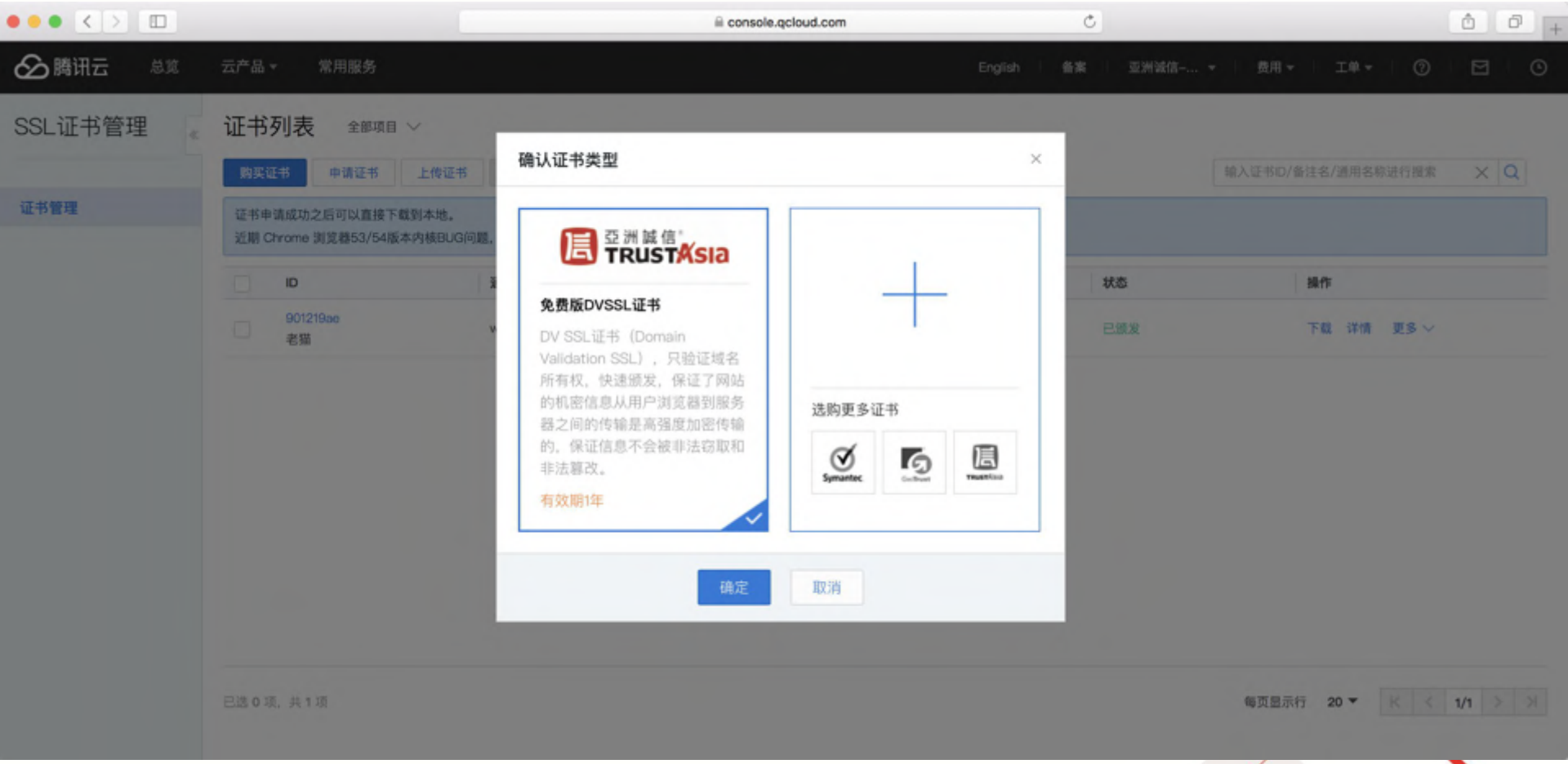


应用于HTTPS安全最佳实践的检测系统

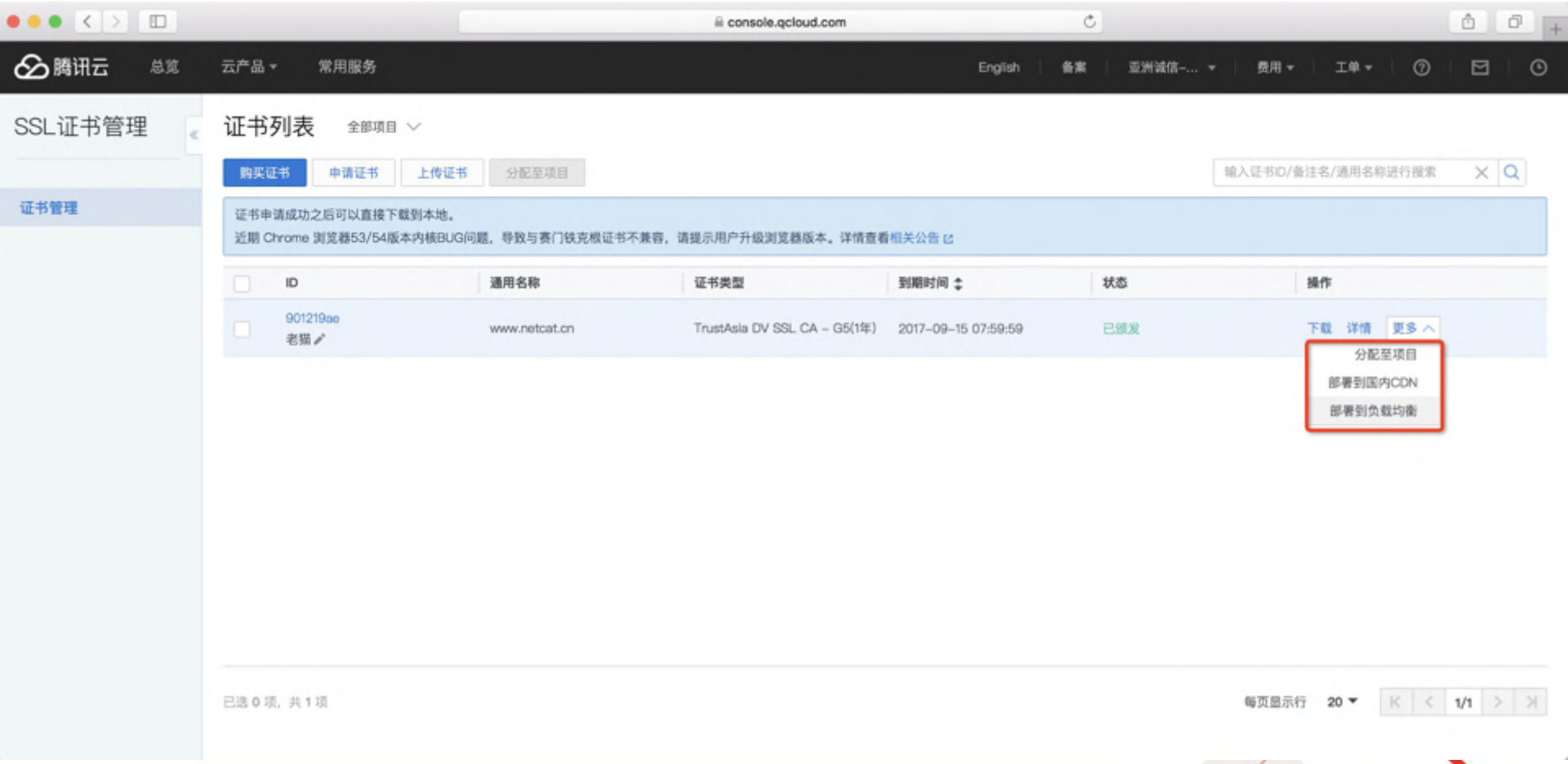
如何实现自动化运维


qcloud.com
证书管理
腾讯云 - 值得信赖
腾讯云
云产品
解决方案
云市场
合作与生态
文档与支持
English
免费体验
备案
管理中心
所有云产品
基础产品
域名服务
视频服务
游戏服务
图像服务
语音服务
大数据
人工智能（AI）
安全
域名注册
专业域名服务，安全、省心、可信赖
.com
.net
.cn
.club
.Wang
更多后缀 >
云产品组合购 >
域名转入
快速转入，便捷、安全、一站管理
SSL证书
数字证书一站式管理，快速接入 HTTPS 安全
Symantec SSL证书
GeoTrust SSL证书
TrustAsia SSL证书
免费获取DV SSL>
DNS劫持检测
多点部署，高效调度，准确检测
检测工具
自动诊断域名、SSL证书状态，保障网站安全
云解析
向全网域名提供稳定、安全、快速的智能解析服务
移动解析
防劫持、智能调度，稳定可靠的移动APP域名解析服务
网站备案
备案备多久，云服务免费用多久
企业邮箱 试运行
提供最全面、最专业、专属定制的企业邮件服务

如何实现自动化运维


console.qcloud.com
腾讯云
总览
云产品
常用服务
English
备案
费用
工单
SSL证书管理
证书列表
全部项目
购买证书
申请证书
上传证书
证书管理
证书申请成功之后可以直接下载到本地。
ID
状态
操作
901219ae
老猫
已颁发
下载
详情
更多
确认证书类型
亚洲诚信 TRUSTAsia
免费版DVSSL证书
DV SSL证书（Domain Validation SSL），只验证域名所有权，快速颁发，保证了网站的机密信息从用户浏览器到服务器之间的传输是高强度加密传输的，保证信息不会被非法窃取和非法篡改。
有效期1年
选购更多证书
Symantec
确定
取消
每页显示行 20
1/1

如何实现自动化运维


console.qcloud.com
腾讯云
总览
云产品
常用服务
English
备案
亚洲诚信-...
费用
工单
SSL证书管理
证书管理
证书列表
全部项目
购买证书
申请证书
上传证书
分配至项目
输入证书ID/备注名/通用名称进行搜索
证书申请成功之后可以直接下载到本地。
近期 Chrome 浏览器53/54版本内核BUG问题，导致与赛门铁克根证书不兼容，请提示用户升级浏览器版本。详情查看相关公告
ID
通用名称
证书类型
到期时间
状态
操作
901219ae
老猫
www.netcat.cn
TrustAsia DV SSL CA – G5(1年)
2017-09-15 07:59:59
已颁发
下载
详情
更多
分配至项目
部署到国内CDN
部署到负载均衡
已选 0 项，共 1 项
每页显示行
20
1/1

已实现HTTPS自动化云服务商

腾讯云

又拍云

西部数码 www.west.cn

百度云

阿里云 aliyun.com

七牛云 QINIU

网易云 163yun.com

UCLOUD

华为云服务 HUAWEI

亞洲誠信 TRUSTAsia

B06展台

THANKS