

解决方案实践

基于开源 Modsecurity 构建 WAF

文档版本 1.0
发布日期 2023-07-17



版权所有 © 华为技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

目录

1 方案概述	1
2 资源和成本规划	3
3 实施步骤	4
3.1 准备工作.....	4
3.2 快速部署.....	8
3.3 开始使用.....	13
3.4 快速卸载.....	15
4 附录	17
5 修订记录	18

1 方案概述

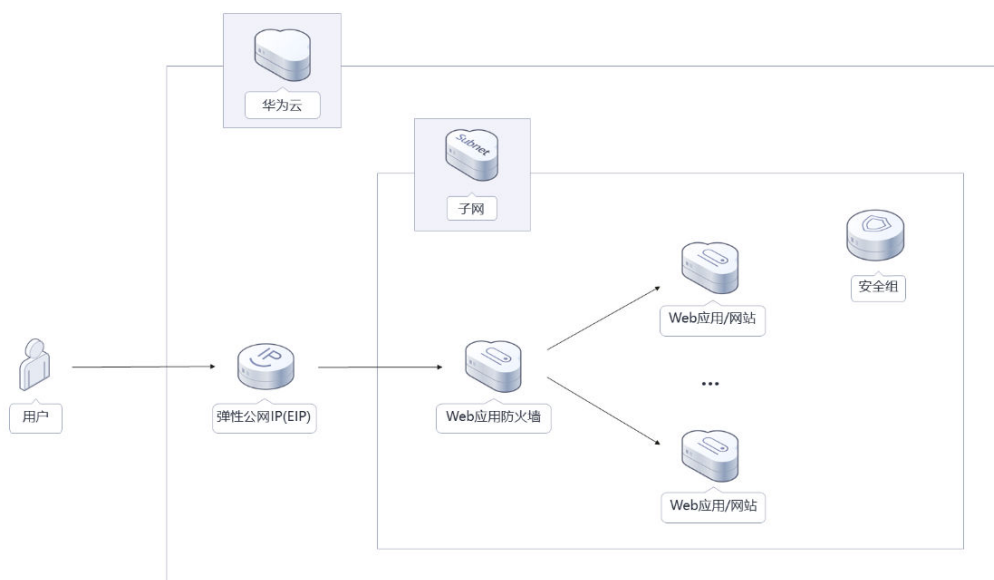
应用场景

该解决方案可以帮助您在华为云弹性云服务器上基于开源ModSecurity软件，一键部署实现Web应用防火墙（WAF）功能。配合Nginx的灵活与高效，有效的增强Web安全性。ModSecurity是一个开源的、跨平台的Web应用防火墙（WAF）。它可以通过检查Web服务接收到的数据，以及发送出去的数据来对网站进行安全防护。

方案架构

该解决方案在华为云弹性云服务器 ECS上基于开源ModSecurity软件，一键部署实现WAF功能。部署架构如下图所示：

图 1-1 方案架构



该解决方案会部署如下资源：

- 创建一台Linux弹性云服务器，用于搭建Web应用防火墙（WAF）和Nginx负载均衡环境。

- 在Linux弹性云服务器中安装配置Nginx，用于提供负载均衡能力。
- 在Linux弹性云服务器中安装配置ModSecurity，用于提供Web应用防火墙（WAF）能力。
- 创建弹性公网IP并绑定到服务器，用于提供访问公网和被公网访问能力。

方案优势

- 低成本
提供极致性价比的云服务器，基于开源的ModSecurity软件构建WAF。
- 一键部署
一键轻松部署，即可完成弹性云服务器的创建和Web应用防火墙（WAF）安装部署。
- 开源和定制化
该解决方案是开源的，用户可以免费用于商业用途，并且还可以在源码基础上进行定制化开发。

约束与限制

- 部署该解决方案之前，您需注册华为云账户，完成实名认证，且账号不能处于欠费或冻结状态，请根据[表2-1](#)中预估价格。
- 已有虚拟私有云VPC、子网、安全组以及业务虚拟机。
- 使用中国大陆节点服务器部署的Web网站，您需要注册域名，并在开通网站前按照工信部要求办理网站备案，以确保您的网站可以通过域名正常访问。华为云支持一站式完成域名注册、实名认证、网站备案和网站解析等操作，详细操作请参考[流程指引](#)。
- 该解决方案安装Nginx默认监听80和443端口，如未开通请参考[添加安全组规则](#)添加加入方向规则，打开指定的TCP端口。

2 资源和成本规划

该解决方案主要部署如下资源，不同产品的花费仅供参考，实际以收费账单为准，具体请参考华为云[官网价格](#)：

表 2-1 资源和成本规划

华为云服务	计费说明	每月花费
弹性云服务器	按需计费：0.22/小时 <ul style="list-style-type: none">区域：华北-北京四计费模式：按需计费规格：X86计算 ECS s6.medium.2 1vCPUs 2GiB镜像：CentOS 7.6 64bit系统盘：高IO 100GB购买时长：1个月购买量：1	$0.22 * 24 * 30 = 158.40$ 元
弹性公网IP	按需计费（按带宽计费）：0.34元/5M/小时 <ul style="list-style-type: none">区域：华北-北京四计费模式：按带宽计费线路：动态BGP公网带宽：按带宽计费带宽大小：5Mbit/s购买时长：1个月购买量：1	$0.34 * 24 * 30 = 244.80$ 元
合计		403.20元

3 实施步骤

- 3.1 准备工作
- 3.2 快速部署
- 3.3 开始使用
- 3.4 快速卸载

3.1 准备工作

创建 rf_admin_trust 委托（可选）

步骤1 进入华为云官网，打开[控制台管理](#)界面，鼠标移动至个人账号处，打开“统一身份认证”菜单

图 3-1 控制台管理界面



图 3-2 统一身份认证菜单



步骤2 进入“委托”菜单，搜索“rf_admin_trust”委托

图 3-3 委托列表



- 如果委托存在，则不用执行接下来的创建委托的步骤
- 如果委托不存在时执行接下来的步骤创建委托

步骤3 单击步骤2界面中的“创建委托”按钮，在委托名称中输入“rf_admin_trust”，委托类型选择“云服务”，输入“RFS”，单击“下一步”

图 3-4 创建委托



步骤4 在搜索框中输入” Tenant Administrator” 权限，并勾选搜索结果

图 3-5 选择策略



步骤5 选择“所有资源”，并单击下一步完成配置

图 3-6 设置授权范围



步骤6 “委托”列表中出现“rf_admin_trust”委托则创建成功

图 3-7 委托列表



----结束

获取子网、安全组 ID

本章节主要帮助用户在快速部署该解决方案之前，获取部分依赖的资源，以供一键部署时使用。

步骤1 登录[华为云官网控制台](#)，单击[虚拟私有云VPC](#)，打开后端业务服务器所属VPC，单击该VPC下的[子网](#)，单击任一子网或后端业务服务器所属子网，获取网络ID。

图 3-8 VPC 下的子网

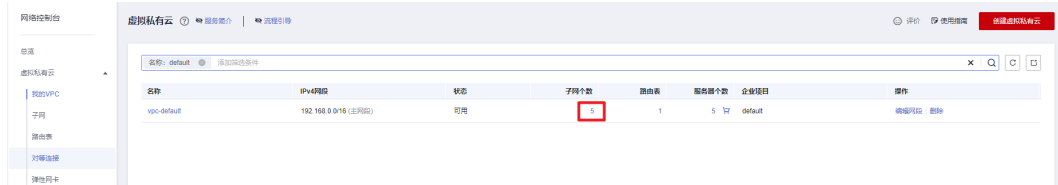


图 3-9 子网列表

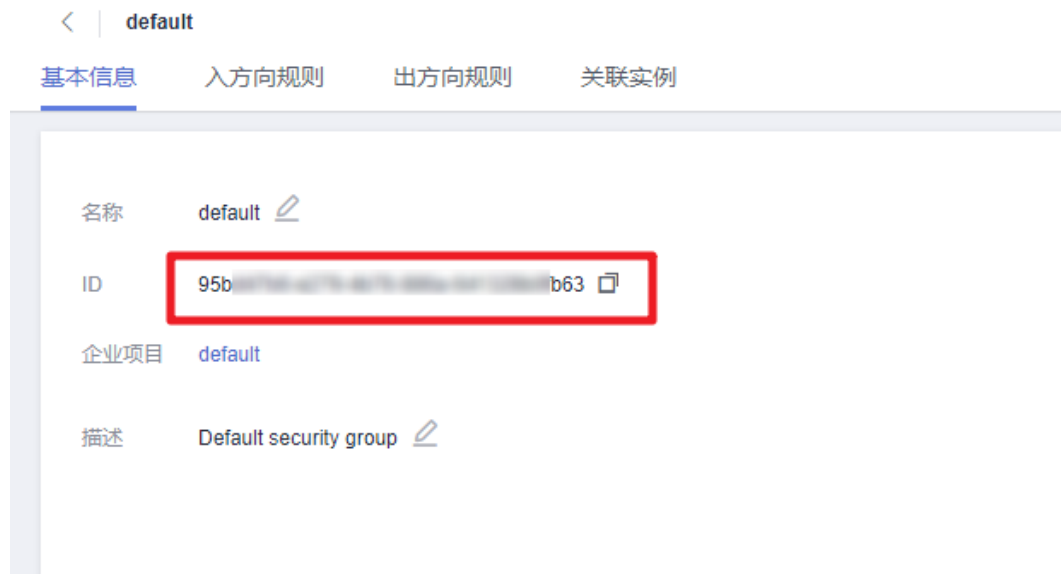


图 3-10 子网网络 ID



步骤2 在网络控制台查看**安全组**，打开业务虚拟机所配置的安全组，获取安全组ID。

图 3-11 安全组 ID



----结束

3.2 快速部署

本章节主要帮助用户快速部署该解决方案。

表 3-1 参数填写说明

参数名称	类型	是否必填	参数解释	默认值
subnet_id	String	必填	子网ID，该模板使用已有子网，请选择后端业务服务器相同虚拟私有云VPC下子网，查询并获取子网ID请参考 3.1准备工作步骤1 。	空
security_group_id	String	必填	安全组ID，该模板使用已有安全组，建议选择后端业务服务器相同安全组，查询并获取安全组ID请参考 3.1准备工作步骤2 。	空
ecs_name	String	必填	Web应用防火墙（WAF）云服务器名称，不支持重名。取值范围：1-54个字符组成，包括字母、数字、下划线（_）、连字符（-）和句点（.）。	waf_on_modsecurity_demo

参数名称	类型	是否必填	参数解释	默认值
ecs_flavor	String	必填	Web应用防火墙（WAF）云服务器规格，具体请参考官网 弹性云服务器规格清单 。	s6.medium.2 (1vCPUs 2GiB)
ecs_image	String	必填	Web应用防火墙（WAF）云服务器镜像，其他镜像请参考官网 镜像服务公共镜像 。	CentOS 7.6 64bit.
ecs_password	String	必填	Web应用防火墙（WAF）服务器初始化密码，创建完成后请参考 3.3开始使用步骤1 重置密码。取值范围：长度为8-26位，密码至少包含大写字母、小写字母、数字和特殊字符（\$!@%-_+=[]:./^,{}?）中的三种，密码不能包含用户名或用户名的逆序。管理员账户为root。	空
bandwidth_size	Number	必填	带宽大小，该模板计费方式为按带宽计费。取值范围：1-2,000Mbit/s。	5Mbit/s
ip_list	String	必填	用户后端业务服务器的私有IP地址及Web服务访问端口，格式为：IP1:端口1,IP2:端口2，所有符号均为英文半角符号。例如： 192.168.0.1:8080,192.168.0.2:8081,192.168.0.3:8083（在浏览器中访问该环境时，请选择后端端口对应的HTTP协议或者HTTPS协议访问）。	空
ssl_certificate	String	必填	用户已有SSL证书(公钥)文件名称，包含后缀名。该模板部署完成后，请在Web应用防火墙（WAF）云服务器指定目录下（/usr/local/nginx/ssl/）上传该证书文件。	空
ssl_certificate_key	String	必填	用户已有SSL证书(私钥)文件名称，包含后缀名。该模板部署完成后，请在Web应用防火墙（WAF）云服务器指定目录下（/usr/local/nginx/ssl/）上传该证书文件。	空

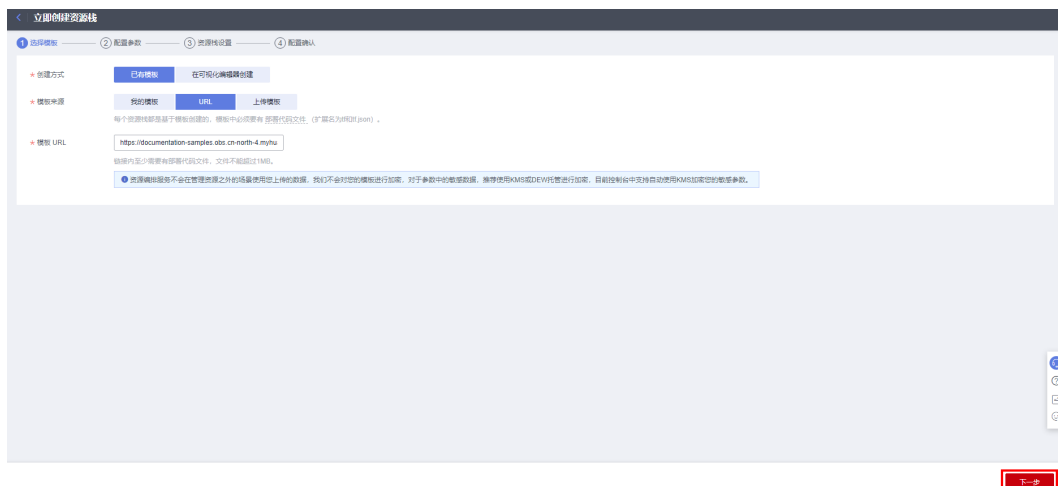
步骤1 登录[华为云解决方案实践](#)，选择“基于开源Modsecurity构建WAF”，数据中心下拉菜单可以选择需要部署的区域，单击“一键部署”，跳转至解决方案创建资源栈界面。

图 3-12 解决方案实施库



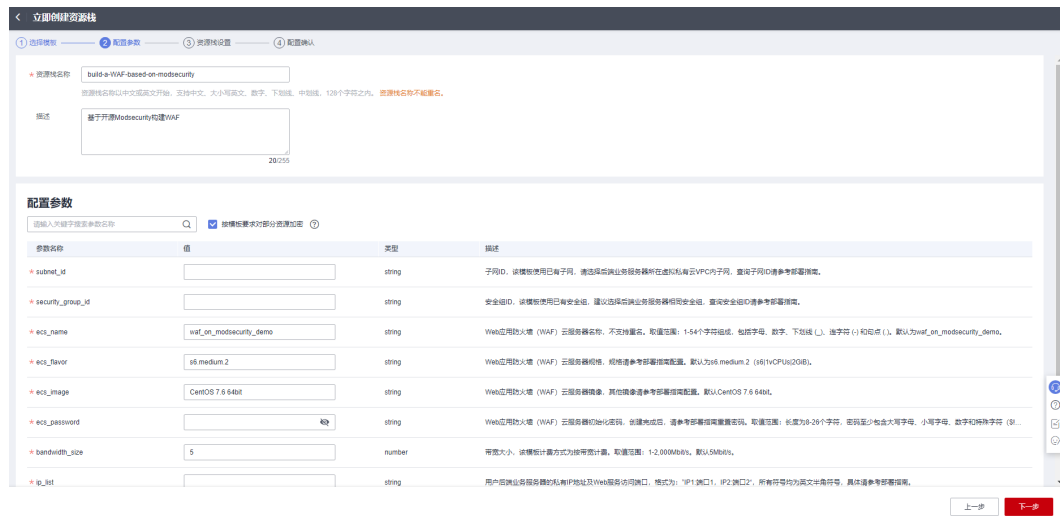
步骤2 在选择模板界面中，单击“下一步”。

图 3-13 选择模板



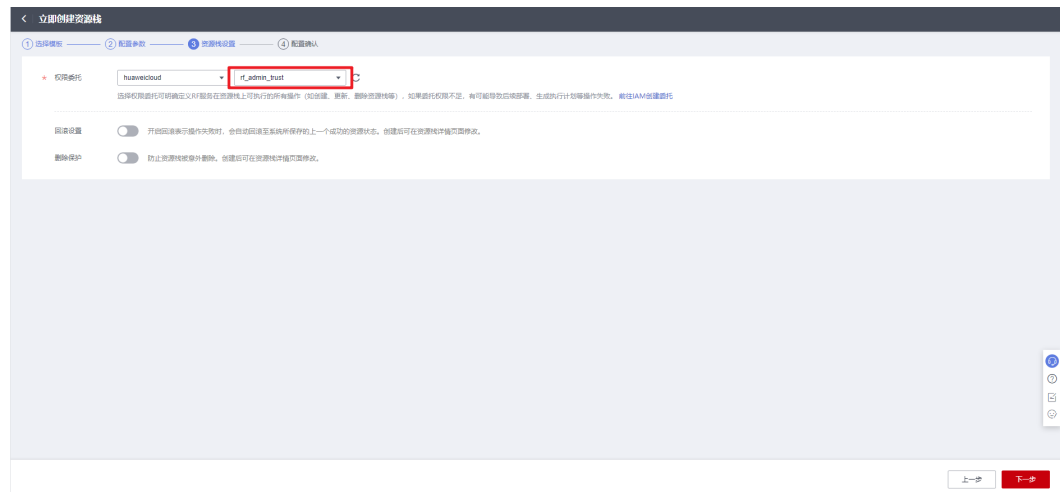
步骤3 在配置参数界面中，参考表3-1完成自定义参数填写，单击“下一步”。

图 3-14 配置参数



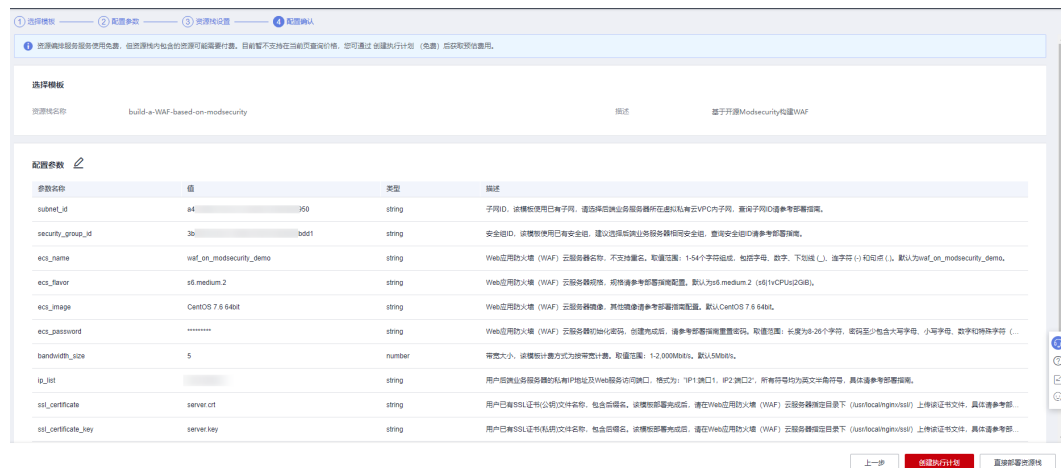
步骤4 (可选) 在资源设置界面中，在权限委托下拉框中选择“rf_admin_trust”委托，单击“下一步”。

图 3-15 资源栈设置



步骤5 在配置确认界面中，单击“创建执行计划”。

图 3-16 配置确认



步骤6 在弹出的创建执行计划框中，自定义填写执行计划名称，单击“确定”。

图 3-17 创建执行计划



步骤7 单击“部署”，并且在弹出的执行计划确认框中单击“执行”。

图 3-18 执行计划

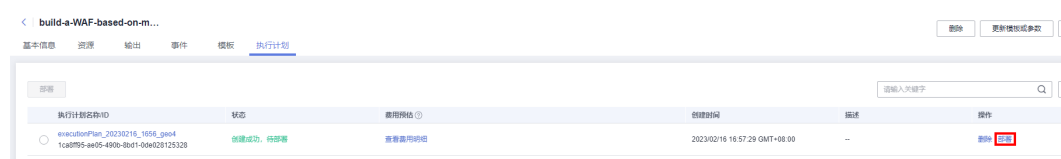
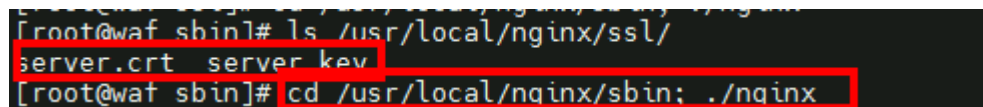


图 3-22 重置密码



步骤2 使用远程连接工具，登录Web应用防火墙（WAF）云服务器，上传已有SSL证书（公钥、私钥）文件至指定目录：/usr/local/nginx/ssl/，上传请参考[上传文件到云服务器方式概览](#)，执行“cd /usr/local/nginx/sbin; ./nginx”命令，启动Nginx服务。

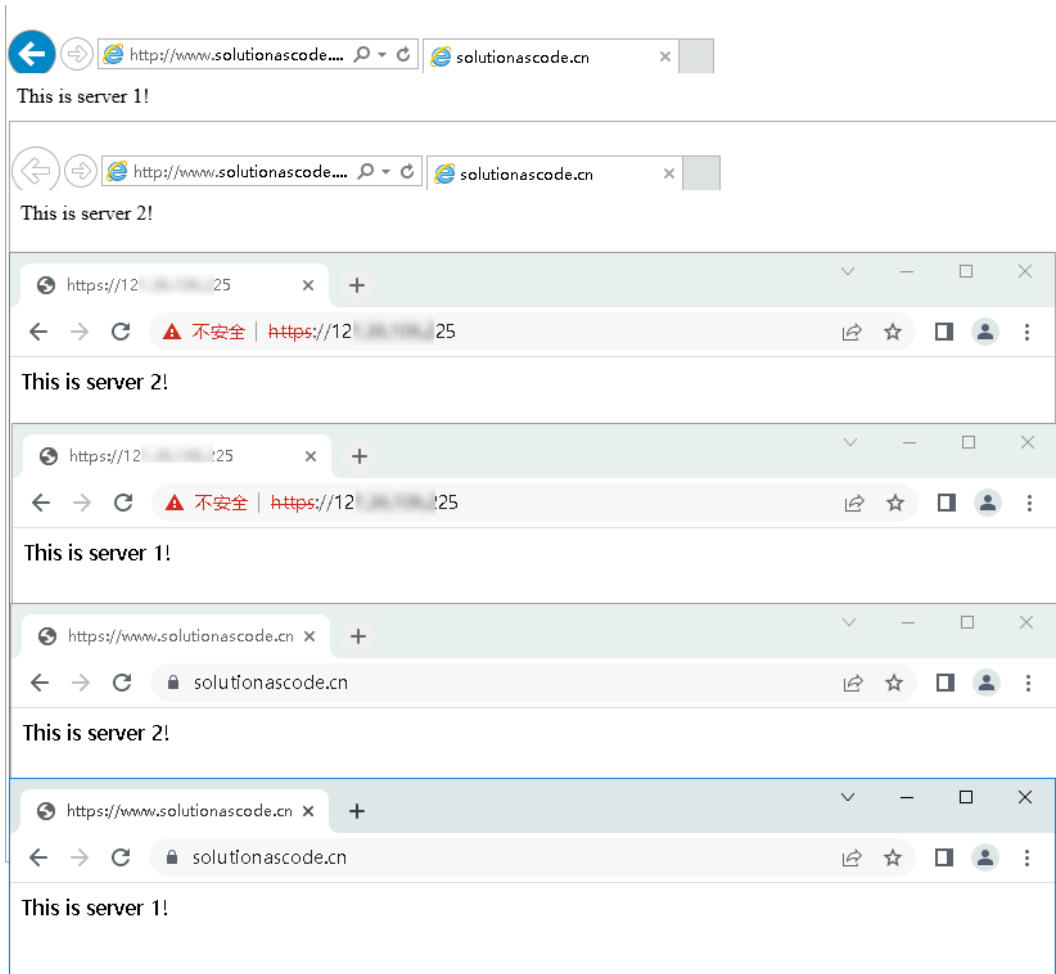
图 3-23 SSL 证书，启动 Nginx 服务



步骤3 配置域名解析。网站解析将域名与[3.2快速部署步骤9](#)中弹性公网IP地址相关联，实现通过在浏览器中直接输入域名访问网站。具体解析流程参考[快速添加域名解析](#)。

步骤4 在浏览器中多次使用HTTP协议或HTTPS协议访问弹性公网IP或者域名，可以轮询访问后端业务服务器。如http://EIP、http://域名、https://EIP，https://域名或直接输入域名。

图 3-24 访问 VIP 挂载的 EIP



步骤5 在浏览器中输入“https://弹性公网IP/?param=%22%3E%3Cscript%3Ealert(1);%3C/script%3E”即可验证Web应用防火墙（WAF）是否生效。

图 3-25 访问 Web 应用防火墙（WAF）

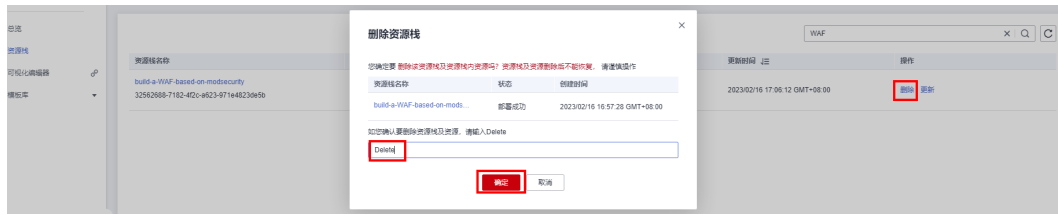


----结束

3.4 快速卸载

步骤1 登录[资源编排服务 RFS](#)，进入“[资源栈](#)”，选择创建的资源栈名称，单击“删除”。在弹出的删除资源栈确认框中，输入"Delete"，单击“确定”，即可卸载解决方案。

图 3-26 一键卸载



---结束

4 附录

名词解释

基本概念、云服务简介、专有名词解释

- 弹性云服务器ECS：是一种可随时自助获取、可弹性伸缩的云服务器，可帮助您打造可靠、安全、灵活、高效的应用环境，确保服务持久稳定运行，提升运维效率。
- 弹性公网EIP：提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟VIP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。
- Nginx：Nginx是十分轻量级的HTTP服务器,Nginx，是一个高性能的HTTP和反向代理服务器，同时也是一个IMAP/POP3/SMTP 代理服务器。具体请参考官网<http://nginx.org/en/>。
- ModSecurity是一个开源的、跨平台的Web应用防火墙（WAF）。它可以通过检查Web服务接收到的数据，以及发送出去的数据来对网站进行安全防护。具体请参考官网<http://www.modsecurity.cn/practice/>。

5 修订记录

发布日期	修订记录
2022-07-30	第一次正式发布。
2023-07-17	修订实施步骤。