基于 FortiWeb 部署高可用 WAF

解决方案

部署手册

刘春华

韩旭明

版本：v1.0.0

最后更新时间: 2021 年 3 月

亚马逊云科技

背景

本部署指南详细描述了如何在云上使用 Amazon CloudFormation 模板部署Fortinet FortiWeb WAF（Web application firewall），构建 WAF 高可用方案。

概览

该方案是基于 FortiWeb WAF 在云上实现自动化部署高。用户可以利用预先定义好的 CloudFormation 模板文件，结合 EC2，VPC，负载均衡等组件快速完成部署。

在使用方面，用户可以依赖 FortiWeb WAF 开箱即用的内置规则来进行防护。而无需投入很大精力从零开始设置复杂的 WAF 规则，同时客户也能基于现有 WAF 规则为基础进行扩展，快速创建自定义规则。

借助于该解决方案，可以阻止影响 Web 应用可用性、危害安全性或消耗过多资源的常见 Web 攻击行为。

可防止哪些攻击？

SQL 注入

攻击者将恶意 SQL 代码插入 Web 请求中，以从数据库中提取数据。此解决方案旨在阻止包含潜在恶意 SQL 代码的 Web 请求。

跨站点脚本攻击

跨站脚本攻击，也称为 XSS。攻击者利用网站中的漏洞将恶意客户端脚本文件

注入合法用户的 Web 浏览器中。检查传入请求中的参数，识别和阻止 XSS 攻击。

HTTP 泛洪

降低 Web 服务器和其他后端资源被 HTTP 泛洪等分布式拒绝服务（DDoS）攻击的风险。

恶意爬虫

对于可公开访问的 Web 应用程序，如果您在网页文件的目录中放置 robots.txt，以定义允许哪些爬虫访问您的网站。好的爬虫会根据 robots.txt 中定义的规则进行访问。但是，某些自动客户端（例如内容抓取工具或不良爬虫）会刻意隐藏自己，以绕过 robots.txt 的限制。而这些恶意爬虫将会被 WAF 识别并阻止。

使用场景

场景 1：基础网站安全通用保护

- 通过对 HTTP/HTTPS 请求进行检测，识别并阻断 SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等常见针对基础网站的攻击。

场景 2：针对指定网页和站点的特殊防护

- 针对 Web 网站中某些页面，这些页面具有敏感信息、特殊访问权限要求，或者其他的请求限制，需要进行特别的安全保护。可以通过 WAF 内容路由等方式，设置针对指定网页的特殊防护策略。针对特殊请求或响应的方法、字段、内容，设置 WAF 特定的防护策略，实现指定页面的高级防护功能。

场景 3：针对恶意爬虫的高级网站内容保护

- 网络爬虫是一种按照一定的规则，自动抓取 Web 网站信息的程序或脚本。但是网络中存在大量的恶意爬虫，恶意盗取目标网站内容，甚至进行复制站点等恶意行为。本解决方案可基于 User-agent，IP 地址，客户端事件以及人工智能的人机识别技术精准识别爬虫，并对恶意爬虫访问进行阻断。

场景 4：针对盗链的高级网站内容保护

盗链是指其他网站不依赖于自身提供 Web 内容，而是直接嵌入其它网

站的页面或元素，向最终用户展示从其他网站盗链的内容，骗取用户的浏览量和点击率。本解决方案通过检查来源请求的 Referer 字段，判断来源页面或访问者身份，从而决定来源请求的安全性。

场景 5：针对网站页面被篡改的高级防护

- 通配置网页防篡改规则，可以检测恶意攻击者在网站服务器注入的恶意代码，保护网站访问者安全。同时也可以防止页面被篡改，保护网站不被添加恶意代码或不良内容。

场景 6：针对电商类网站的高级业务安全保护

- 电商类或带有交易和消费属性的网站容易受到攻击，尤其是举办类似定时抢购秒杀活动时，业务接口可能在短时间承担大量的恶意请求。本解决方案可以灵活设置攻击防护的限速策略，保证业务服务不会因大量的并发访问而崩溃。

场景 7：针对应用层 DDoS 攻击的防护

- CC（ChallengeCollapsar，挑战黑洞）攻击是 DDoS 攻击的一种类型，使用代理服务器向受害服务器发送大量貌似合法的请求。该方案基于HTTP 访问请求频率/TCP 连接频率/人机识别等综合智能分析手段能有效地拦截 CC 攻击。

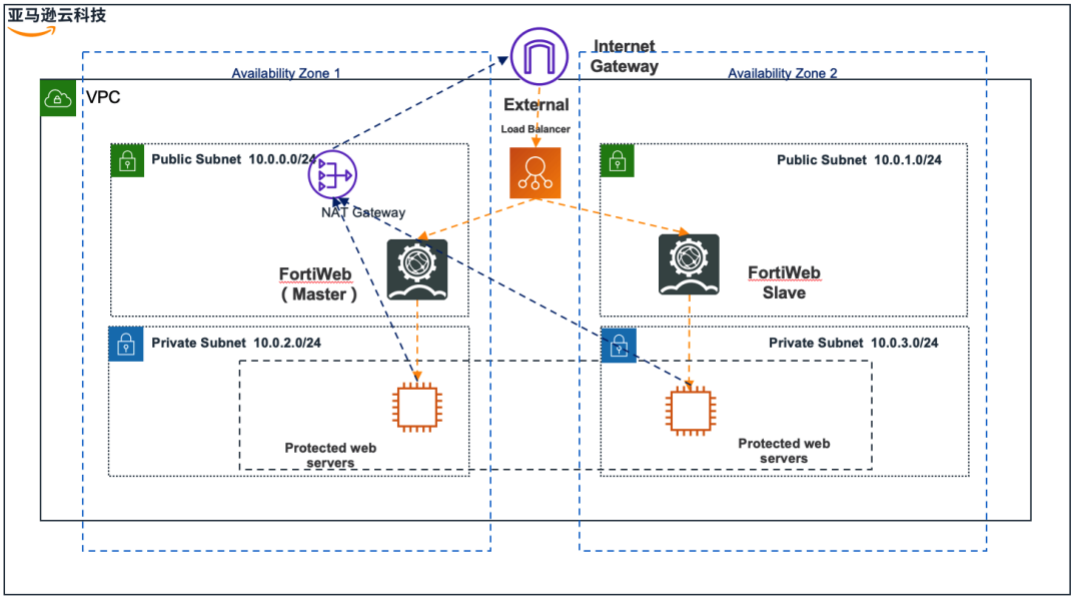
场景 8：针对暴力破解和撞库攻击的防护

- 针对暴力破解及撞库，该方案可以针对登录行为进行持续监控，如果检测到多次登录错误后会将账号进行锁定，或者是某 IP 频繁进行登录操作会将 IP 封禁。同时会检测攻击者使用的口令是否为威胁情报库中所收集过的被公开泄露的口令，如果命中，则直接判定为撞库攻击并进行阻断。

系统架构

架构图

此解决方案可在由西云数据运营的亚马逊云科技（宁夏）区域或由光环新网运营的亚马逊云科技（北京）区域中部署。



架构描述

1. 公有子网及私有子网：创建两种不同的子网，公有子网和私有子网。建议被 FortiWeb 保护的 Web 服务器部署在私有子网中。

2. ALB 及 NLB： FortiWeb 服务器前端的负载均衡可以是 Application Load Balancer 类型 ,也可以是 Network Load Balancer 类型。有关 Network Load Balancer 的详细信息，请参阅 Network Load Balancer 用戶指南。有关 ClassicLoad Balancer 的更多信息，请参阅 Classic Load Balancer 用戶指南。

3. 高可用架构：为了满足高可用性及冗余性的需求，在不同的可用区创建 FortiWeb Master 节点及 FortiWeb Slave 节点，形成 Active-Active-High volume 的部署模式。如果 FortiWeb Master 节点出现故障，那么 FortiWebSlave 节点会自动升级为 Master 节点，从而确保系统功能高可用。

4. 数据流向：因特网用戶如果要访问需受到保护并位于私有子网 Web 服务

器。

i. 第一步，请求首先会经过 Internet 网关 (IGW-Internet Gateway)。

ii. 第二步，请求经负载均衡(可以是 ALB 类型，也可以是 NLB 类型)进行分发。

iii. 第三步，请求会分发到 FortieWeb 服务器。FortiWeb 服务器根据内置 WAF 规则针对请求进行检测。如果发现请求是恶意的，可以选择针对请求进行日志记录或者是阻断。

iv. 第四步，经过检测后的正常安全请求会发送到 位于私有子网中的 Web 服务器。

5. 位于私有网络受保护的 Web 服务器如果需要访问互联网，例如更新软件等操作。该种请求会经过 NAT Gateway 进行流量的转发。

机型选择

该方案支持如下 EC2 实例类型：

m5.large

m5.xlarge

m5.2xlarge

m4.large

m4.xlarge

m4.2xlarge

m3.medium

m3.large

m3.xlarge

m3.2xlarge

c5.large

c5.xlarge

c5.2xlarge

c4.large

c4.xlarge

c4.2xlarge

c3.large

c3.xlarge

c3.2xlarge

根据需要防护的带宽进行机型选择

影响选择 FortiWeb EC2 实例类型的因素有许多。建议根据所需保护的 Web 服务器资源带宽进行评估。

- 如果需保护资源的 HTTP 带宽为 25Mpbs，建议选用 c5.large 机型
- 如果需保护资源的 HTTP 带宽为 100Mpbs，建议选用 c5.xlarge 机型
- 如果需保护资源的 HTTP 带宽为 500Mpbs，建议选用 m5.2xlarge 机型
- 如果需保护资源的 HTTP 带宽为 1000Mpbs，建议选用 m5.4xlarge 机型

部署说明

前提

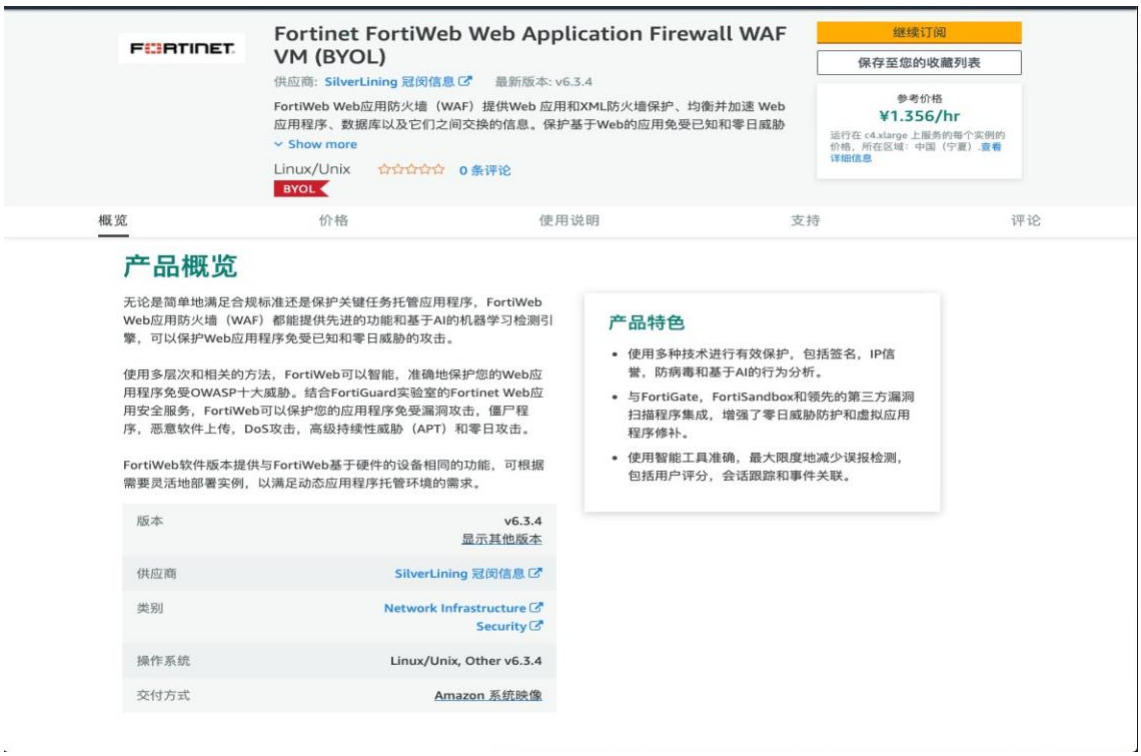
该方案部署前，需要准备如下文件和资源。

在 Marketplace 中订阅 Fortinet FortiWeb WAF

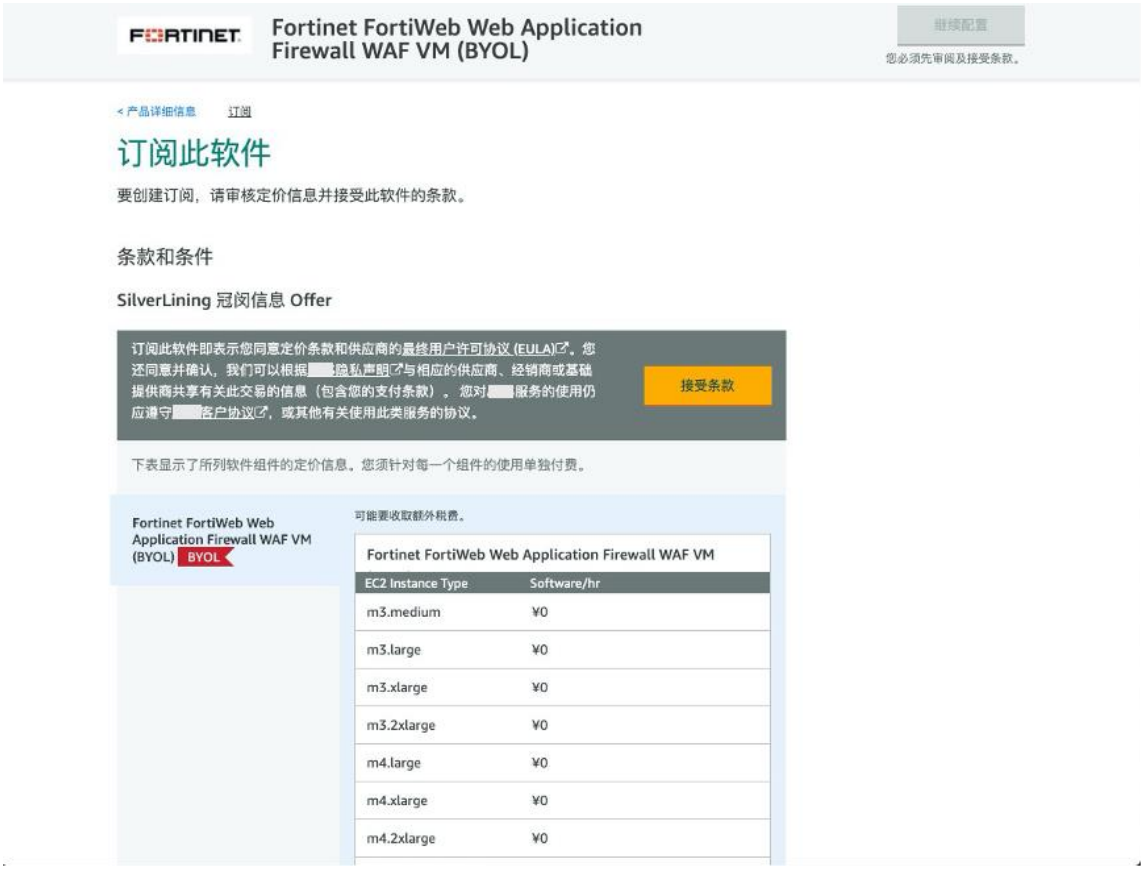
为了使用 FortiWeb,需要首先在 Maketplace 进行订阅。 首先请点击该链接:

https://awsmarketplace.amazonaws.cn/marketplace/pp/prodview-fcc3nuw2vz7moz?qid=1591167253836&sr=0-1&ref_=srh_res_product_title

进入 Marketplace 中的 FortiWeb 页面。点击该页面右上角 【继续订阅】按钮。



点击【接受条款】按钮。

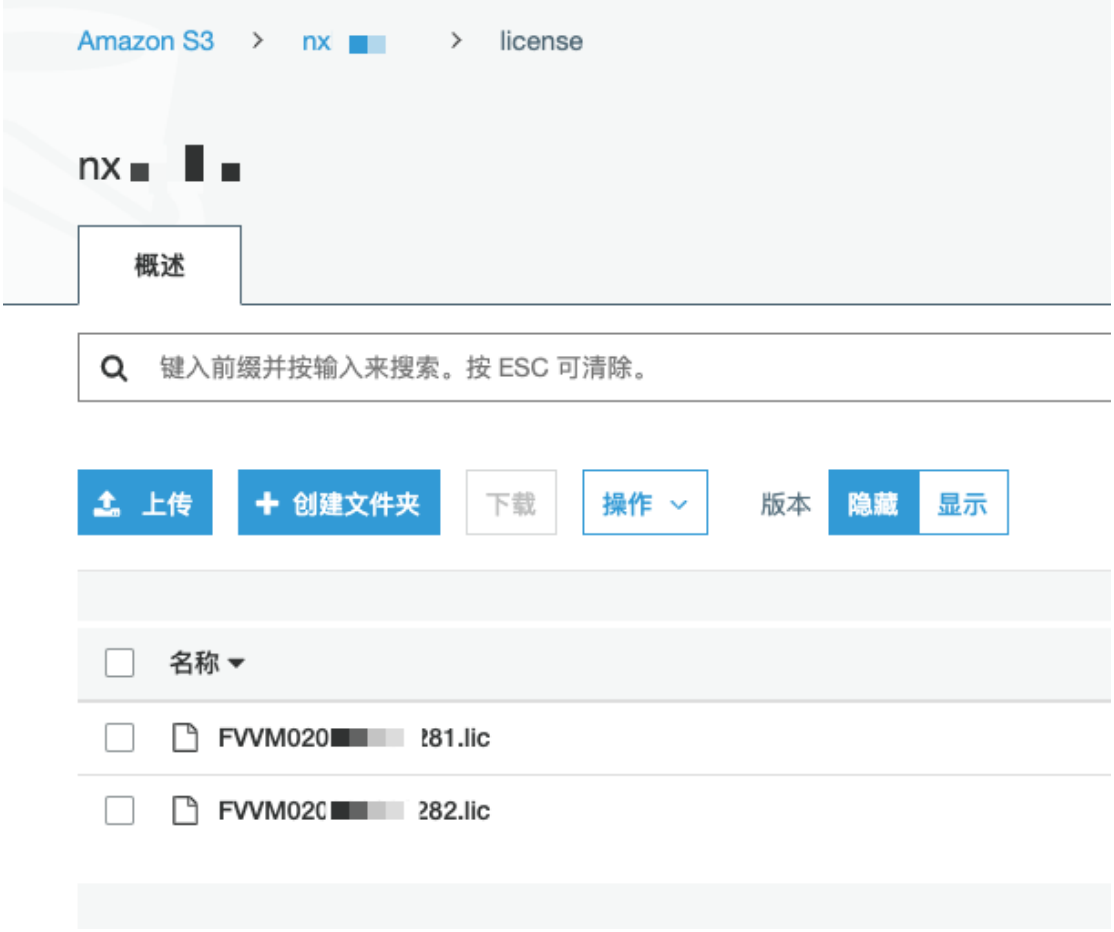


系统正在处理。

订阅成功后，产品名称表格中的生效日期列会显示订阅的生效日期。

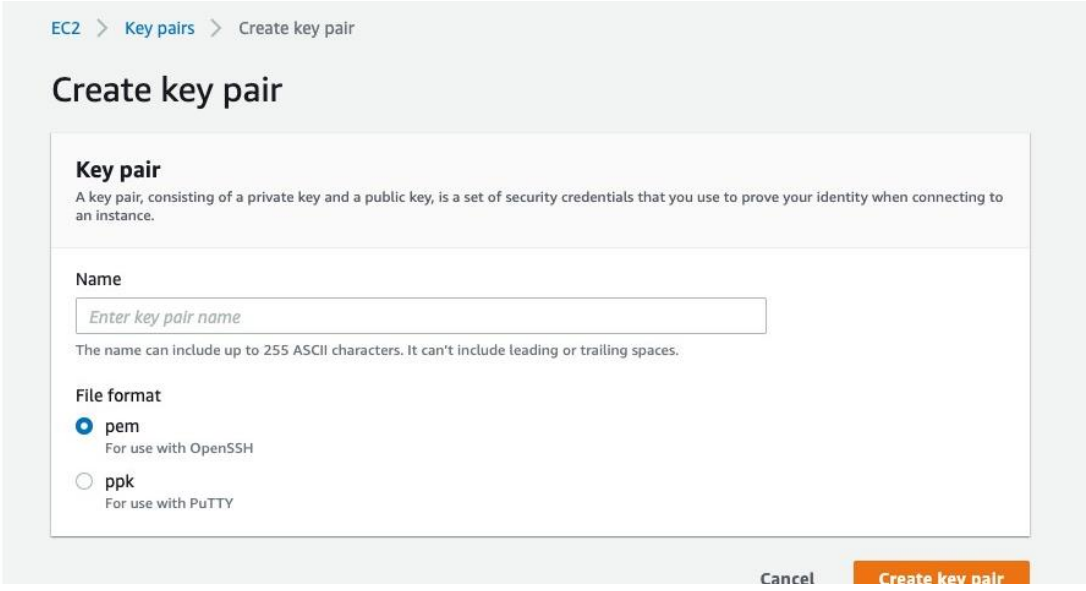
FortiWeb License 文件

该方案部署前，需要提前准备好同计划部署 FortiWeb 服务器数量相等的 License 文件。另外这些 License 文件需要提前上传到您所拥有 S3 存储桶中，并设置好相应的 Prefix。例如：如果把 License 文件存放在 S3 存储桶 nxbuckets，Prefix（逻辑上可以认为是目录）为 license 的路径中。参考截图如下：



EC2 密钥对（Key Pairs）

该方案需要提前准备好 EC2 密钥对。在方案部署完成后，可使用该密钥对以远程 SSH 的方式登录到 FortiWeb 服务器。创建密钥对截图如下：



快速部署

以下的步骤主要针对在运行在由西云数据运营的亚马逊云科技（宁夏）区域或由光环新网运营的亚马逊云科技（北京）区域中部署基于 Fortinet FortiWeb 构建高可用 WAF 解决方案。本解决方案通知支持 ALB 及 NLB 负载均衡方式。

如果您想使用 ALB（Application Load Balancer）进行流量的转发，可以使用以下链接快速启动一个 CloudFormation 堆栈来部署和管理整个方案：

如果您想使用 NLB（Network Load Balancer）进行流量的转发，可以使用以下链接快速启动一个 CloudFormation 堆栈来部署和管理整个方案：

1. 启动堆栈

打开Amazon Web Services管理控制台（如果您还没登录，系统会首先先跳转到登录页面，登录后进入模板启动页面）。可以使用控制台右上方的区域选择链接在其他的区域部署。

2. 配置启动参数

配置图例如下：

下表展示的是每一项参数的含义，这些参数随时可以更新。

参数类型	参数项	参数说明	缺省值

Common configuration	AvailabilityZones	选择 FortiWeb 服务器要部署的可用区，如果部署大于 2 台，请选择至少两个可用区。如果只部署 1 台，也需要选择至少两个可用区。	
Common configuration	Resource nameprefix	该方案所建资源名称的前缀	fwbha
Common configuration	S3 bucket name which store FortiWeb license file	存放 FortiWeb License 文件的存储桶（您自己拥有的 S3 存储桶）名称	
Common configuration	S3 key prefix which store FortiWeb license file	License 文件在存储桶存放的前缀（Prefix)名 称，可以理解为目录名称。请注意最后需要加"/" 字符。	
Common configuration	Key pair name	选择已经存在的密钥对，用于 SSH 登录 FortiWeb 服务器，	

Network configuration	VPC CIDR	新建 VPC 的 CIDR	10.0.0.0/16
Network configuration	VPC Public Subnet1	公有子网 1，用于部署 FortiWeb	10.0.0.0/24
Network configuration	VPC Public Subnet2	公有子网 2，用于部署 FortiWeb	10.0.1.0/24
Network configuration	VPC Private Subnet1	私有子网 1，用于部署被保护的 Web 服务器	10.0.3.0/24
Network configuration	VPC Private Subnet2	私有子网 2，用于部署被保护的 Web 服务器	10.0.4.0/24
FortiWeb configuration	FortiWeb Image Type	本方案只支持 BYOL 模式	BYOL

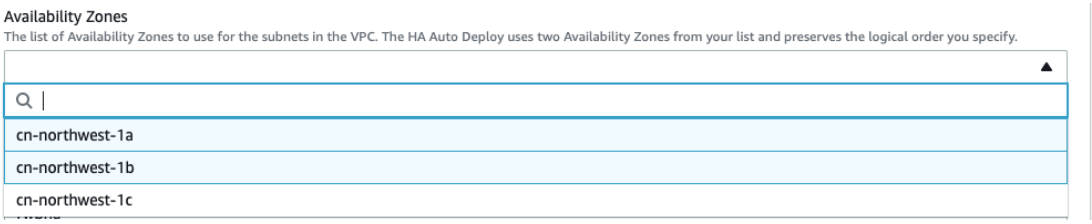
FortiWeb configuration	FortiWeb Image Version	FortiWeb 最新版本	LATEST
FortiWeb configuration	FortiWeb Instance type	请根据受保护的 HTTP 服务器带宽选择机型	C5.Large
FortiWeb configuration	FortiWeb Instance Count	部署 FortiWeb 服务器数量。请确保在 S3 桶中 License 文件数量大于或等于该数值	2
FortiWeb configuration	FortiWeb Admin password	用于登录 FortiWeb 系统的密码。请注意：密码需要包含大小写，字母，数字 和 @!%*#?& 这些特殊字符	
FortiWeb configuration	FortiWeb Admin Port	FortiWeb 后台管服务端口	8443
FortiWeb configuration	FortiWeb Http Port	FortiWeb 所保护 web server 的 Http 协议端口	80

FortiWeb configuration	FortiWeb Https Port	FortiWeb 所保护 web server 的 Https 协议端口	443
FortiWeb HA configuration	FortiWeb HA Mode	FortiWeb HA 模式，高可用请选择 active-active-high-volume 模式	active-active-high-volume
FortiWeb HA configuration	FortiWeb HA Group Name	FortiWeb HA Group 名称	FWHA Group
FortiWeb HA configuration	FortiWeb HA GroupID	FortiWeb HA Group ID 编号	30
FortiWeb HA configuration	FortiWeb HA Override	FortiWeb HA Override 模式	disable

具体配置截图如下

Availability Zones: 请选择 FortiWeb 服务器所在的 可用区，请选择两个可用区。（注:如果计划只部署 1 台 FortiWeb 服务器，也需要选择两个可用区。）

假设选择宁夏区域，建议选择 cn-northwest-1a 及 cn-northwest-1b，如下图



Resource name prefix: 该参数是资源名称前缀的自定义标识符，最多 10 个字符，只包含大写字母、小写字母和数字。最大长度是 10。示例：

S3 bucket name which store FortiWeb license file: 存储 FortiWeb license 文件的 S3 存储桶的名称

S3 key prefix which store FortiWeb license file : 存储 FortiWeb license 文件的 S3 文件前缀，注意: 请确保输入值以“/”字符为结尾。

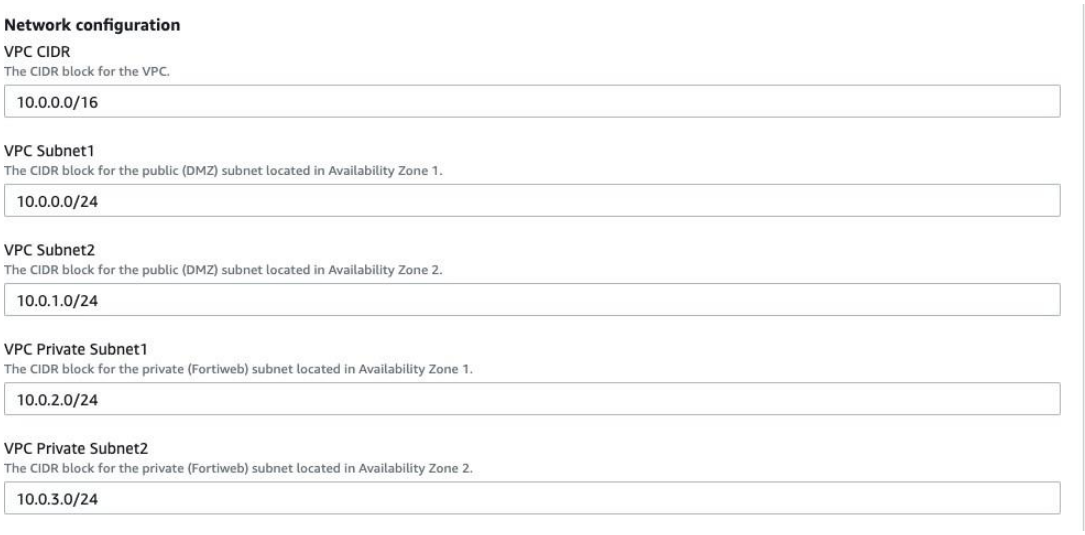
示例：

Network configuration:

按照常用的部署架构，FortiWeb 位于公有子网，而被保护的 Web Server 则需部署在私有子网中。示例：按照高可用架构，需要在两个可用区创建 4 个子网

（两个公有子网，两个私有子网）

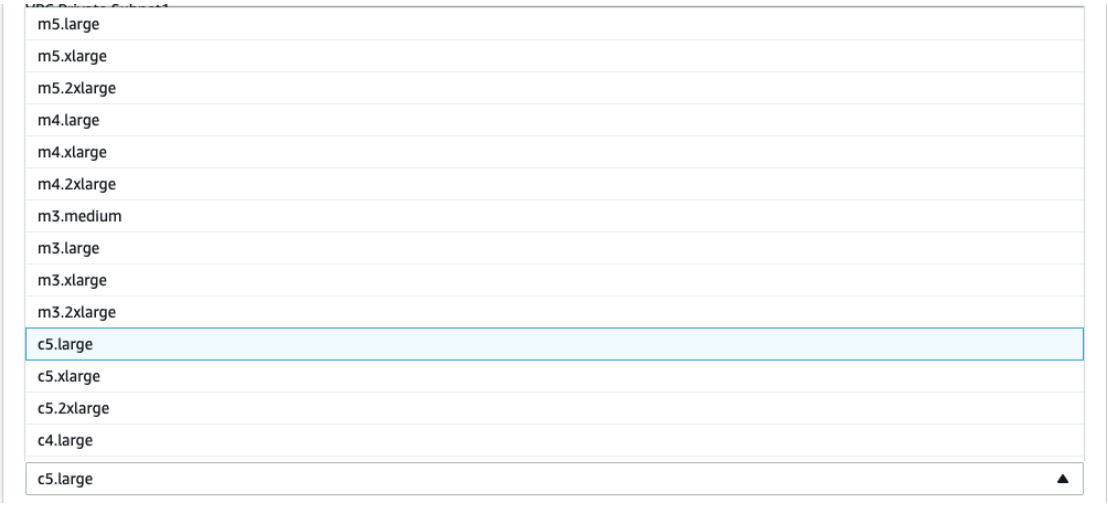
FortiWeb configuration



FortiWeb Image Type: 由于中国区的 Market Place 只支持 BYOL 的License 模式，所以请确保默认值。

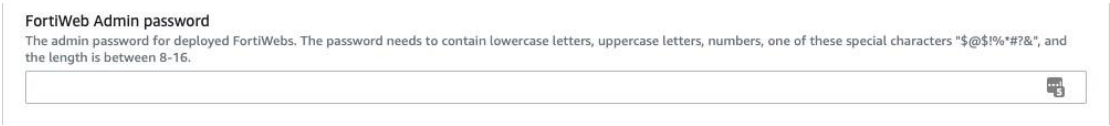
FortiWeb Image version: 请选择默认值 LATEST

FortiWeb Instance type: FortiWeb 现在支持的实例类型 19 种，请根据实际情况选择合适的机型。

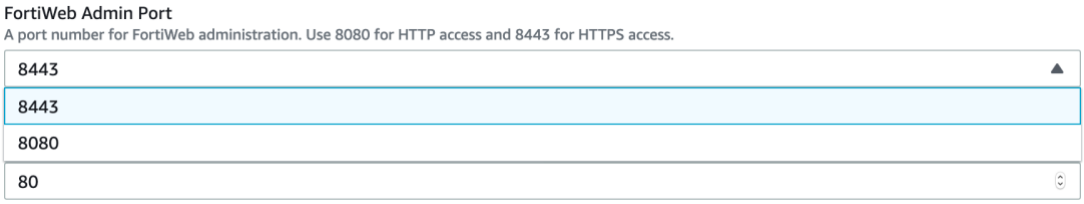


FortiWeb Instance Count:需要部署的 FortiWeb 的数量。缺省值为 2，以实现高可用。

FortiWeb Admin password：用于部署 FortiWeb 的 admin 用户的管理密码密码需要包含小写字母、大写字母、数字、特殊字符“$@$!%*#?”，长度在 8-16 个字符之间。

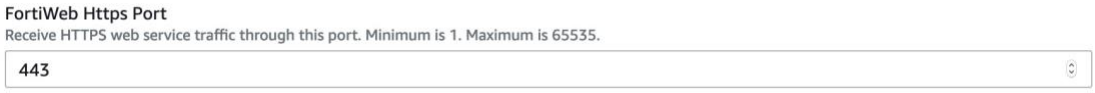


FortiWeb Admin Port,可以选择 8443， 8080， 80 等， 默认选择 8443:

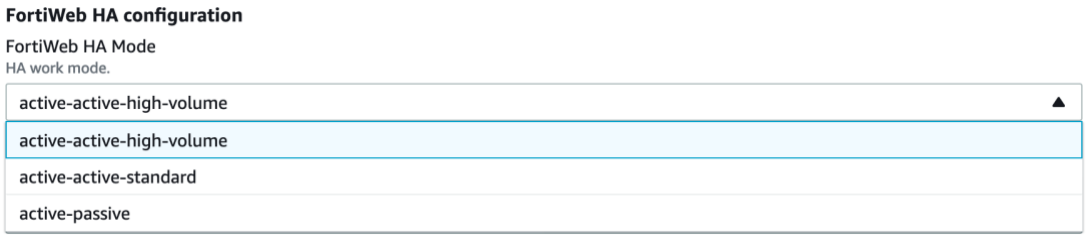


FortiWeb Http Port:

FortiWeb Https Port:



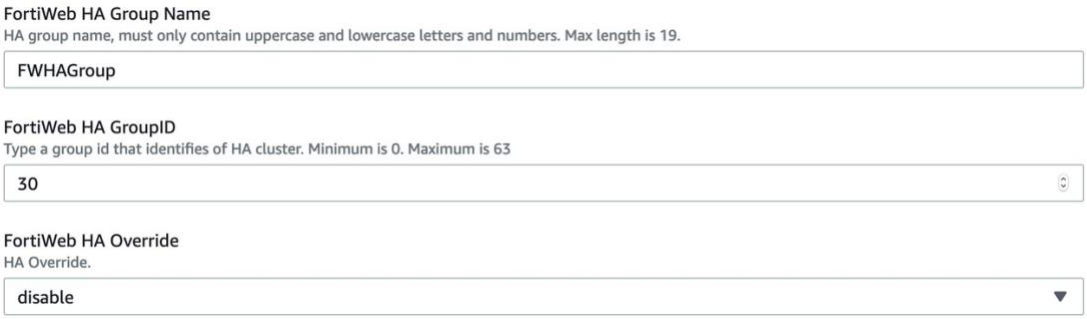
FortiWeb HA configuration：



FortiWeb HA Mode，本场景选择 active-active-high-volume 模式

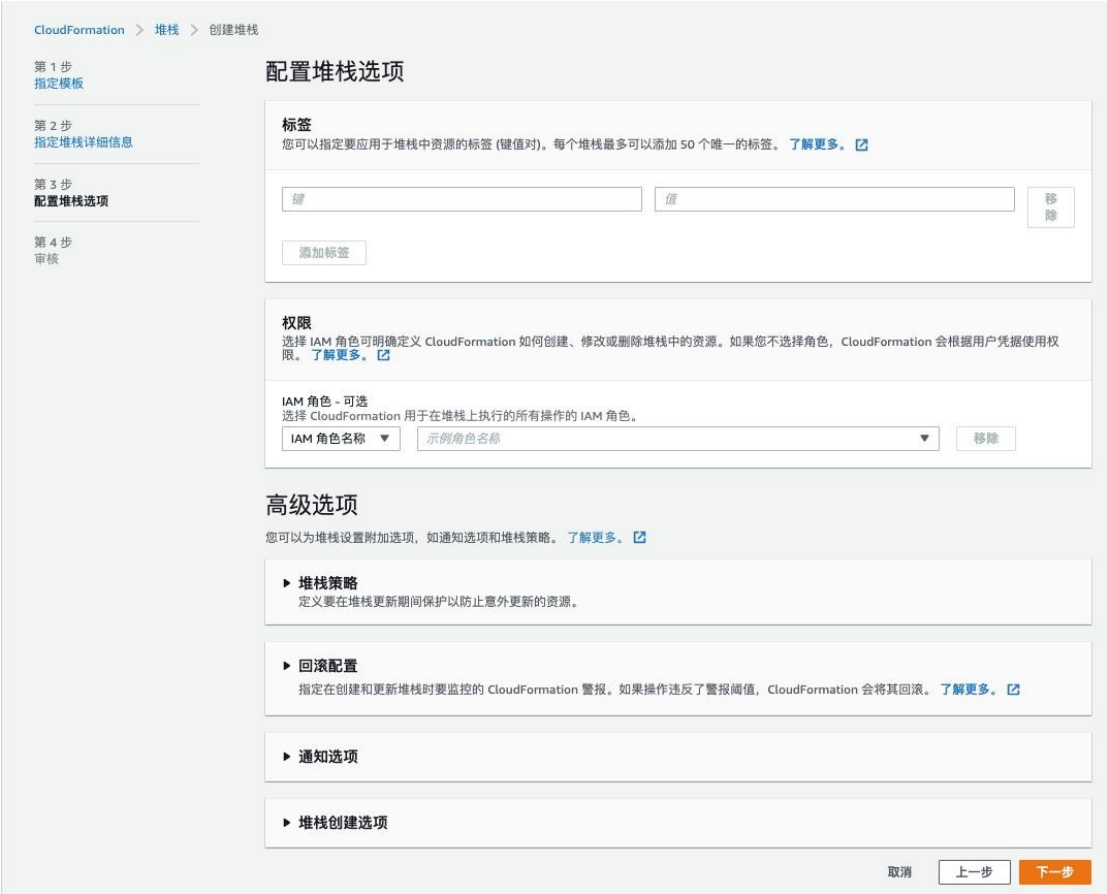
其他 HA 相关配置请保持默认值，无需更改。

参数设置完成后，点击下一步，并在下一步的配置堆栈选项保留默认，直接点击下一步。



2.高级选项

保持缺省值



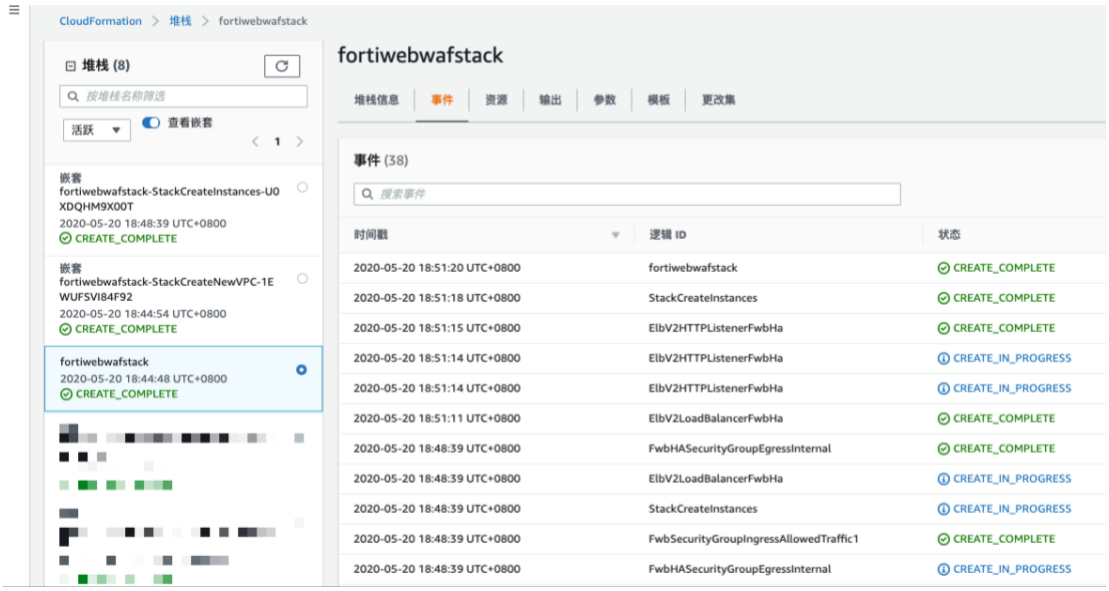
3. 审核环节

下一步的审核环节，审核前几个步骤配置的内容(可以保持默认值)，并勾选最后的两个确认复选框，之后点击“创建堆栈”

4. 等待堆栈创建成功

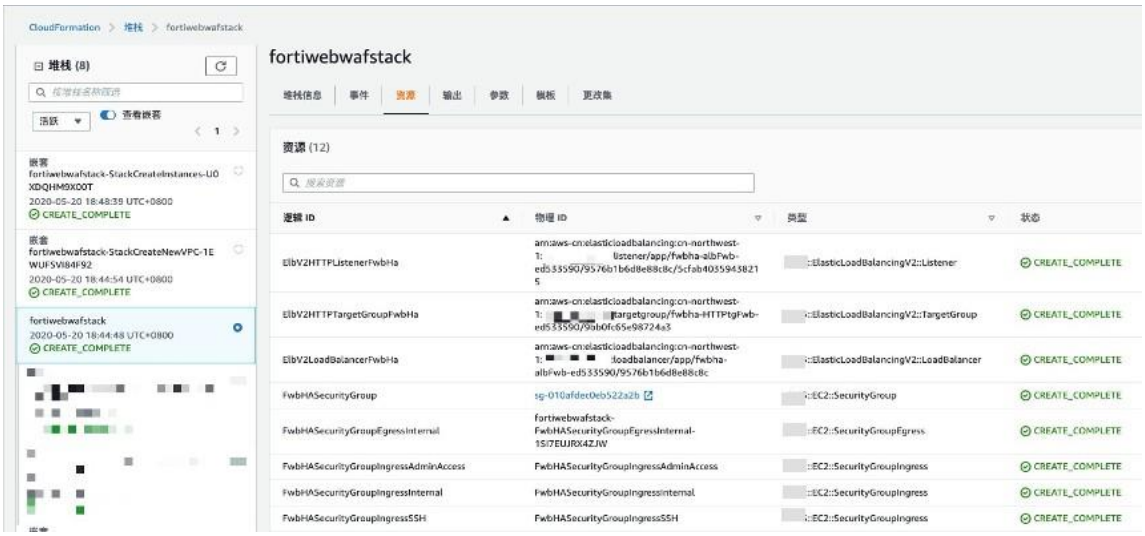
您可以在 Amazon CloudFormation 控制台的【状态】列中查看堆栈的状态，并点击右上方的刷新按钮更新状态。

最终如图显示三个堆栈创建完成，主堆栈创建完成，确认没有出现创建失败的情况即完成 CloudFormation 堆栈的创建。



5. 查看堆栈资源

选中堆栈后点击【资源】标签，可以看到这个堆栈启动的所有资源。



验证环境

查看 EC2 已经被成功创建，进入 EC2 控制台页面，查看已经成功创建好的 EC2 实例。

此时可以在 VPC， EC2 等服务的控制台（Console）界面上检查创建的资源。

如 VPC 和子网：

四个子网：两个公有子网和两个私有子网

第一步：创建Nginx 服务器：

创建两台 Nginx 服务器作为要保护的目标 Web 服务器，本文以已经安装完成的镜像启动 Nginx，在 ec2 的 console 上选择 AMI，点击“启动”按钮：

在启动 Nginx 服务器时，可以通过 user data 配置安装配置 Nginx 服务并启动。

```
#!/bin/bash
sudo yum update -y
sudo amazon-linux-extras install -y nginx1sudo
systemctl enable nginx
sudo systemctl start nginx
```

注意根据本文档的架构，建议在私有子网中启动 Nginx 服务器，选择子网的时候需要注意，确保在创建实例时选择 private subnet1 或 private subnet2 子网。示例如下：

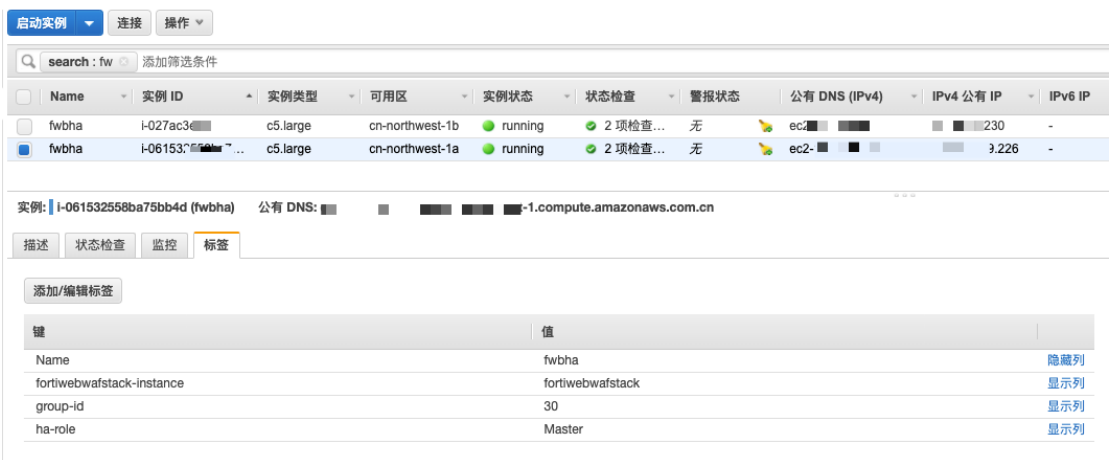
针对 web 服务器，选择堆栈中已经建立的安全组，该安全组开放 80 端口提供 web 服务，开放 22 端口用于 SSH 方式远程登录：

在私有网络创建好 Nginx 服务器后，请记录下该 Nginx 的私有网络 IP 地址。

第二步：配置FortiWeb选项

选择 FortiWeb 的 Master 节点

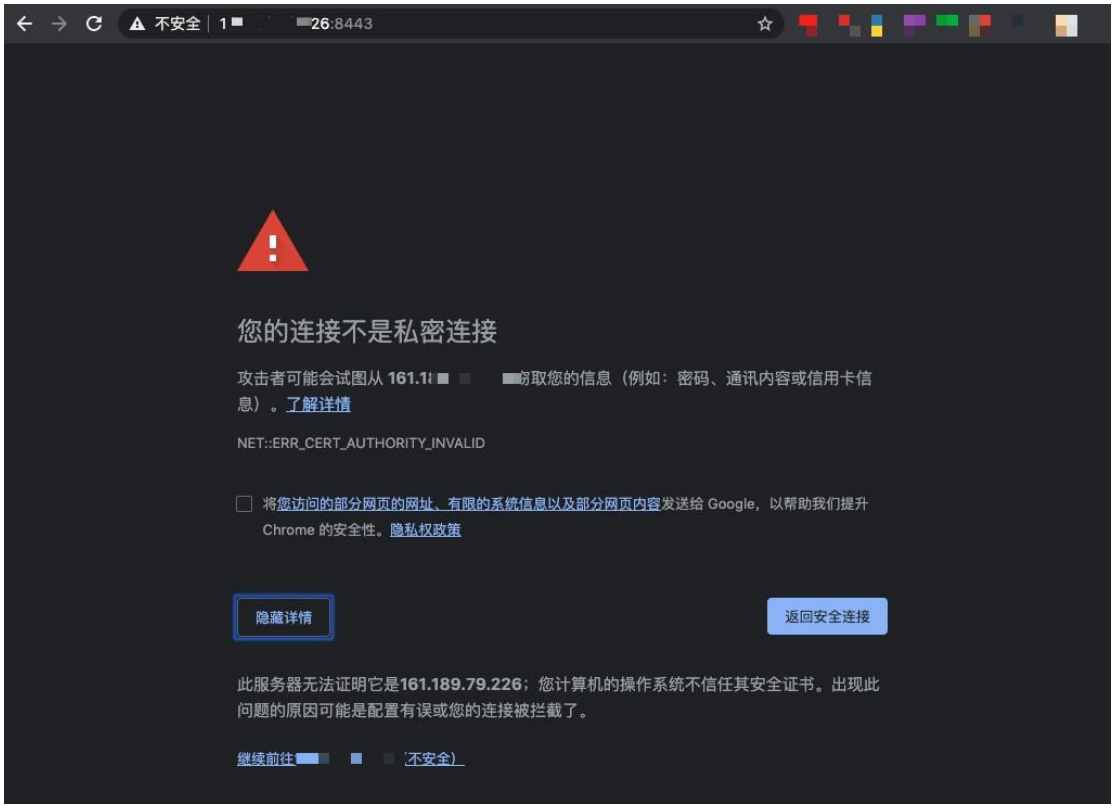
首先进入 EC2 管理界面，选择其中一台 EC2,点击 【标签】。



CloudFormation 堆栈时选择的 FortiWeb 的端口（例如 https://52.82.4.168:8443）。由于是自签发的数字证书，请忽略浏览器警告，继续访问。

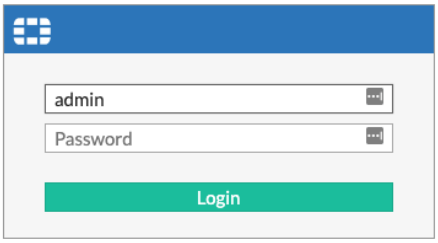
能在 Master 的节点上运行。另外点击 “描述”标签页。记录下该 EC2 的公网IP地址（如下图红框所示）。

在浏览器输入：https://[FortiWeb 阶段的 ip 或域名]:8443 这个端口是在启动

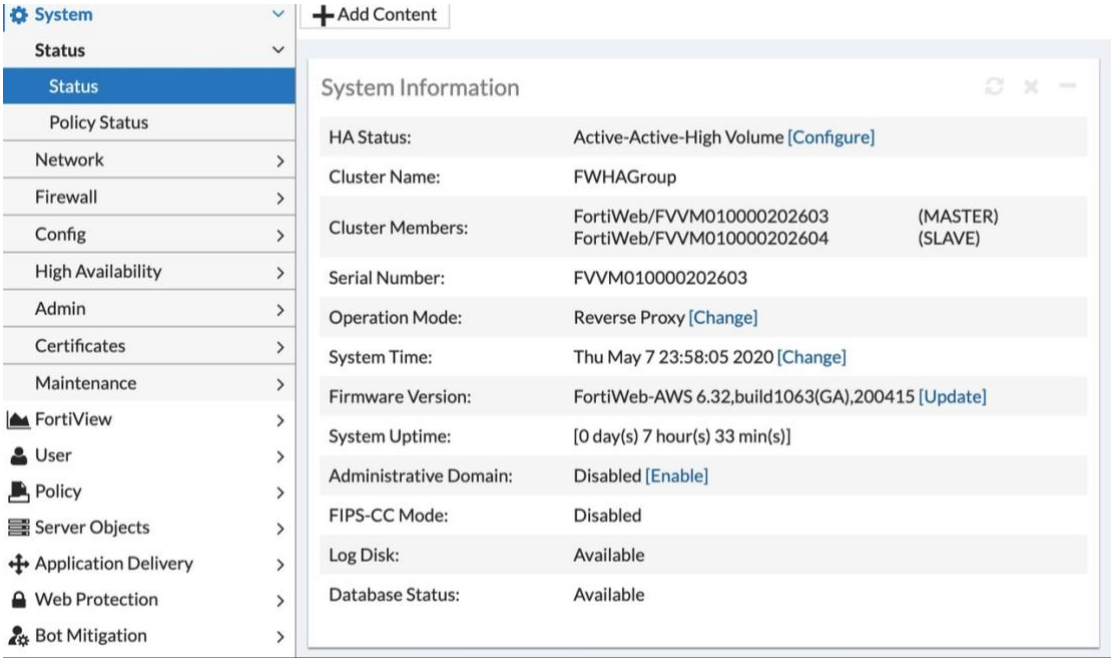


之后浏览器弹出输入用户名和密码的输入窗口。输入之后登录进入 FortiWeb 的管理界面。

请注意，Fotiweb 的缺省用户为 admin,密码为在 创建堆栈时里输入框为“FortiWebAdminPassword”所输入的字符串。

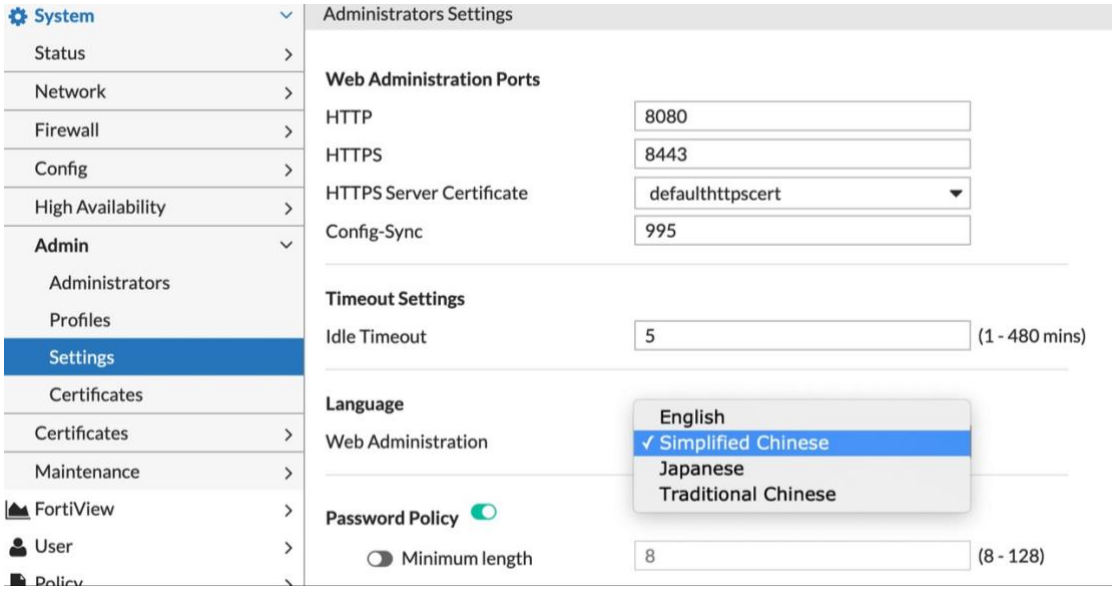


登录后，请注意当前的 HA Status 已经是 Active-Active-High Volume 模式



在如图所示的界面修改系统显示语言为简体中文。

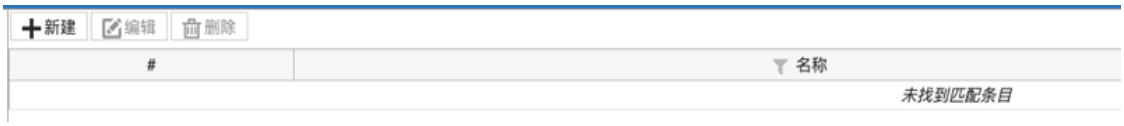
【Admin】->【Setting】-> 【Language】 选择 Simplified Chinese。



下面我们将配置对相应的 web 服务器进行防护，以及应用不同场景的策略配置

首先从左边的菜单选择：服务器对象→服务器→虚拟服务器，在编辑虚拟服务器的界面，输入名称，如 virtualserver1，之后点击“确认”。

点击 【新建】按钮

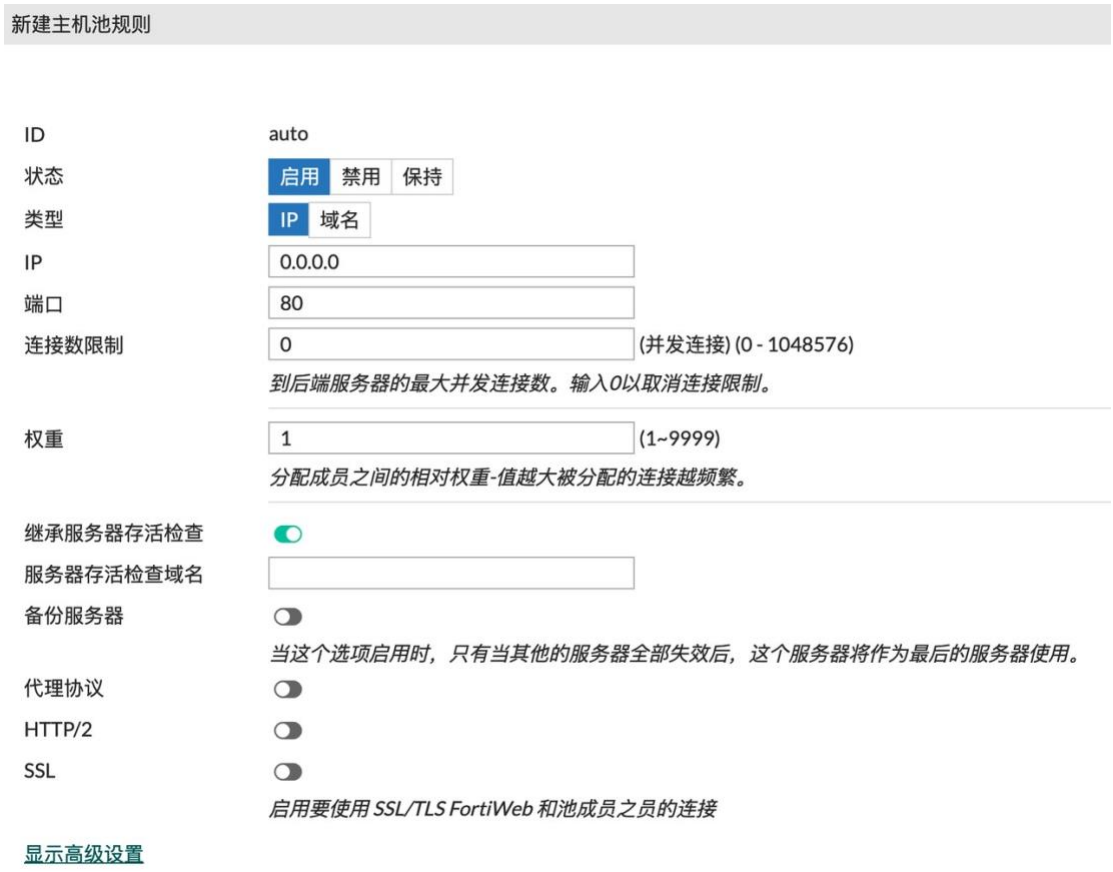


完成后，点击下面“+新建”，弹出编辑界面，在“接口”一栏选择“port1”，点击“确认”保存。

虚拟服务器配置之后的状态为：

下面配置主机池，在左边菜单依次选择服务器→对象服务器→主机池，该池是被保护的主机集合。进入新建主机池的界面，输入主机池名称后，在单服务器/负载均衡处，选择负载均衡（针对需要对多台主机需要保护的情况）或 单服务器（包含单台 Web 服务器），点击“确认”。

之后，选择“+新建”，进入主机池规则编辑界面，此处根据需要配置，本文档只需要编辑要被保护的主机的 IP。点击“确认”。



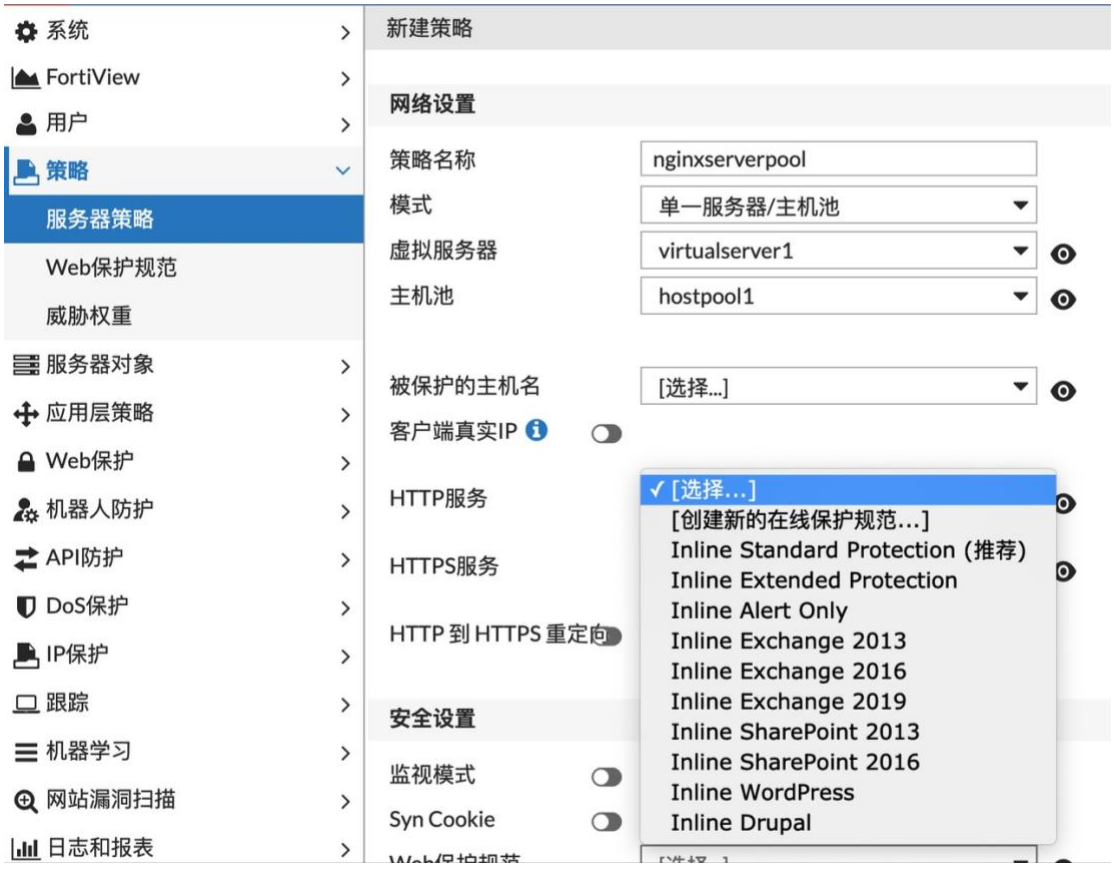
之后依次添加多台 Nginx 实例的私有 IP 地址，配置如下图所示

.

选择 web 保护规范，缺省情况下请选择 “Inline Standard Protection” - Recommended 规范。请注意，该规范是 FortiWeb 自带的开箱即用的规则，您也可以在此基础上进行扩展。

在左边菜单依次选择：策略→服务器策略，点击“+新建”，进入策略创建界面。输入策略名称，选择模式为“单一服务器/主机池”，选择虚拟服务器（前文创 建）和主机池（前文已经创建），在“安全设置”部分，“web 保护规范”处选择需要使用的保护策略，选择对 http 服务进行保护。根据不同场景，选择不同的保护策略。本文以基本的标准保护为例。选择“Inline Standard Protection”。因为

该规范已经内置开箱即用的 WAF 规则。



至此 FortiWeb 配置完成。

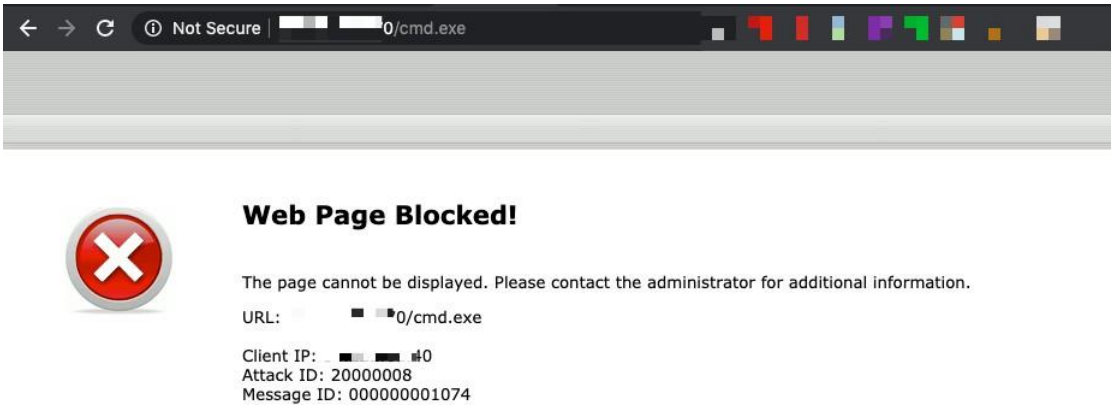
第三步：验证正常web请求

测试访问，在浏览器输入 Application Load Balancer 的域名。

如果显示 Nginx 的首页，这说明用户请求已经经过 ALB 的转发，经过 FortiWeb 检查后并成功转发给受保护的 Nginx web 服务器。

第四步：验证危险web 请求

由于 “Inline Standard Protection” - Recommended Web 保护规范已经内置 WAF 规则。例如在正常的请求 URL 中加入 cmd.exe 参数后，该保护规范认为此请求是危险请求，会进行阻止。



一键导入 WAF 防护场景

在 FortiWeb 安装成功后，其实还有很多的 WAF 安全规则需要配置。您可能会问，能否有不同场景的业务规则可以直接导入使用？本解决方案已经预先定义了以下六种使用场景，便于方便使用。

场景编号	WAF 使用场景	场景规则 ID
1	基础网站安全通用防护	GeneralWebSiteProtect
2	针对恶意爬虫的高级网站内容防护	AntiCrawler
3	针对盗链的高级网站防护	ProtectHotlinking
4	针对电商网站的高级业务安全防护	ProtectECommerce
5	针对应用层 DDoS 攻击的防护	ProtectDDoS

场景目录如下：

```
├── source
│   └── lambda
│       ├── cfnresponse.py                    [Python - Lambda 返回值]
│       └── index.py                          [Python - Lambda 创建 EC2,注入 Userdata并创建 Fortiweb active-active 集群]
│       └── policy                                [FortiWeb 场景规则]
│           ├── AntiCrawler                       [反爬虫场景]
│           │   ├── AntiCrawler.txt               [反爬虫场景规则]
│           │   └── ReadMe.txt                    [反爬虫场景使用文档]
│           ├── GeneralWebSiteProtect             [通用网站保护场景]
│           │   ├── GeneralWebSiteProtect.txt     [通用网站保护场景规则]
│           │   └── ReadMe.txt                    [通用网站保护场景使用文档]
│           ├── ProtectDDoS                       [DDoS保护场景]
│           │   ├── ProtectDDoS.txt               [DDoS场景规则]
│           │   └── ReadMe.txt                    [DDoS护场景使用文档]
│           ├── ProtectDatabaseBruteForce         [数据库撞库场景]
│           │   ├── ProtectDatabaseBruteForce.txt [数据库撞库场景规则]
│           │   └── ReadMe.txt                    [数据库撞库场景使用文档]
│           ├── ProtectECommerce                  [电子商务类网站保护场景]
│           │   ├── ProtectECommerce.txt          [电子商务类网站保护场景规则]
│           │   └── Readme.txt                    [电子商务类网站保护场景使用文档]
│           └── ProtectHotlinking                 [网页防盗链场景]
│               ├── ProtectHotlinking.txt        [网页防盗链场景规则]
│               └── ReadMe.txt                   [网页防盗链场景使用文档]
```

代码请从GitHub Repository下载: https://github.com/aws-samples/aws-deployment-with-fortiweb-waf。

如何导入

场景规则导入需要使用 SSH 远程登录到 FortiWeb 服务器并导入。请下载 /source/policy/ 目录下的文件，根据需要选择场景。

例如选择反爬虫的场景 进入 /source/policy/AntiCrawler 目录， FortiWeb 服务器的 IP 地址是 161.189.x.x, 该 EC2 的密钥对是 zhy.pem请执行如下的命令。

```
ssh -i ~/zhy.pem admin@161.189.x.x > /dev/null 2>&1 <
```