ALIBABA CLOUD

阿里云

Web应用防火墙

系统管理

文档版本：20210121

阿里云

法律声明

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。

1. 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。

2. 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
危险	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。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会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，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**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。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *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。	`switch {active|stand}`

目录

1.查看产品信息

产品信息页向您展示当前Web应用防火墙（WAF）实例的资源详情、WAF的防护规则更新通知、功能更新通知和WAF的回源IP段。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，选择**系统管理 > 产品信息**。
4. 在**产品信息**页面，查看以下信息：
   - WAF资源详情
     - 当前WAF版本及到期时间（支持执行**续费**和**升级**操作）
     - 支持接入防护的**一级域名数**
     - 支持接入防护的**总域名数**
     - 所有接入业务的最大**业务带宽**
     - 所有接入业务的最大**业务QPS**
     - 已购买的**独享资源包**数量

   - **规则更新通知**

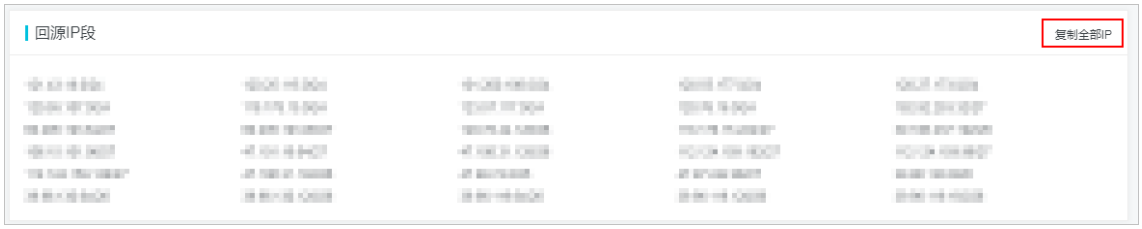
     展示WAF内置防护规则的最新更新记录。

   - **功能更新公告**

     展示WAF功能调整的最新记录，单击记录可查看详情。

- **回源IP段**

  展示WAF的所有回源IP地址，单击**复制全部IP**可直接复制。



2.功能与规格设置（按量付费模式）

使用按量付费模式开通Web应用防火墙后，您可以实时调整Web应用防火墙的功能与规格，享受更贴近业务现状的安全防护。功能与规格调整保存后实时生效，每日账单依据当天最高配置进行计算。

背景信息

调整Web应用防火墙的功能规格后，Web应用防火墙的计费会发生变化。关于按量付费Web应用防火墙服务的计费方式，请参见产品价格页。Web应用防火墙控制台也提供了基于当前配置的价格预估功能，具体请参见查询预估价估。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**系统管理 > 功能与规格设置**。
4. 定位到**功能与规格设置**区域，根据防护需要调整功能与规格设置，并单击**保存设置**。

下表描述了支持调整的功能与规格。

类型	名称	说明	相关操作
安全防护	Web攻击防护	支持以下两种规格： ○ **基础防护**：默认防护策略，支持预警和拦截模式，提供高中低3个规则组。 ○ **高级防护**：包括基础防护能力，并提供防扫描和大数据深度学习引擎防护能力。	设置规则防护引擎 设置大数据深度学习引擎（限**高级防护**） 设置扫描防护（限**高级防护**）
	缓解CC攻击	支持以下两种规格： ○ **基础防护**：默认防护策略，依据独家算法引擎，支持秒级拦截恶意CC攻击，并提供正常和攻击紧急两种拦截模式。 ○ **高级防护**：在基础防护的基础上，提供基于URL设定IP访问频率的功能，即自定义CC防护策略。	设置CC安全防护 设置自定义防护策略（限**高级防护**）
	精准访问控制（黑白名单）	支持以下两种规格： ○ **基础防护**：提供基于IP和URL的黑白名单功能，每个域名可设置10条规则。 ○ **高级防护**：提供基于IP、URL、Cookie、User-Agent、Referer、提交参数、X-Forwarded-For等各类常见HTTP头部的逻辑组合判断功能，每个域名可设置100条规则。	设置IP黑名单 设置自定义防护策略（限**高级防护**）
	数据风控	开启后可以配置防护规则，防止恶意短信注册、恶意登录、活动作弊等机器威胁。	设置数据风控
	网页防篡改、敏感信息防泄漏	开启后支持网站防篡改和防敏感信息泄露功能。	设置网站防篡改 设置防敏感信息泄露
高级特性	支持HTTPS相关业务	开启后可以设置网站一键HTTPS（仅需上传证书私钥，无需变更源站）和设置HTTP回源，降低网站负载损耗。	开启HTTPS高级设置
	日志服务	开启后为接入网站提供全量日志实时存储、分析、自定义报表和告警等一站式日志增值服务能力。	开启WAF日志服务
	支持非标准端口业务防护	开启后可以使用默认端口（HTTP 80、8080，HTTPS 443、8443）以外的非标端口接入Web应用防火墙。 **说明** 开启非标端口支持后，不支持关闭。	WAF支持的端口

类型	名称	说明	相关操作
	支持黑名单管理能力	开启后支持封禁指定IP地址或IP地址段的访问，以及封禁指定地理区域（中国内地省份和港澳台地区、海外国家）来源IP地址的访问。	设置IP黑名单
	提供业务分析报表	开启后提供指定时间段内的访问请求总数，各类攻击拦截总数，业务QPS、攻击拦截次数、带宽和响应码的变化趋势，访问量最高的源IP、来源地域和目标URL等统计信息。	查看安全报表
系统规格	**扩展域名包**	支持根据需求增加扩展域名包的数量。 一个Web应用防火墙实例默认支持接入10个域名（仅限在1个一级域名下）。每增加1个域名包，则可以多使用一个不同的一级域名，且支持多接入10个域名。最多可增加1000个扩展域名包。 **说明** 增加扩展域名包数量后，不支持减小。	扩展域名包
	独享IP	支持增加独享IP的数量。每30天内只允许做1次调整。最多可增加10个独享IP。 **说明** 增加独享IP数量后，不支持减少。	域名独享资源包

5. （可选）查询预估价格。 完成功能与规格设置后，如果您想了解当前配置下Web应用防火墙按量付费的预估日结费用，请参照以下步骤进行操作：
   i. 定位到**价格预估**区域，设置**我的QPS**，即被防护网站的QPS日峰值。
   ii. 在**价格预估**后，查看当前配置下Web应用防火墙实例的价格，单位：元/天。

注意 预估价格仅作为计费参考，实际价格以账单为准。

3.账单与套餐中心（按量2.0版本）

WAF按量计费模式已升级到2.0版本。升级后，您可以在按量计费WAF的控制台访问账单与套餐中心页面，查看WAF的实时账单金额、调整需要启用的功能、查看账单列表。

背景信息

开通WAF按量计费实例后，默认为您开启规则防护引擎（Web入侵防护）、基础精准条件（访问控制）功能。

如果您需要使用更多防护功能，需要通过修改套餐，开启对应的功能。更多信息，请参见修改按量计费套餐。

您可以通过账单与套餐中心进行以下操作：

- 查看实时账单。
- 查看账单列表。
- 修改已开通的功能和获取预估费用。
- 通过访问费用中心入口，查看账单明细。

> **说明** 如果您购买的是旧版按量计费套餐，请参见功能与规格设置（按量付费模式）。

适用版本

本功能仅适用于WAF按量计费2.0版本。

查看账单费用

1. 登录Web应用防火墙控制台。
2. 在左侧导航栏，选择**系统管理 > 账单与套餐中心**。
3. 在**账单与套餐中心**页面，查看**实时账单**。支持查看当天的功能费用和消耗的流量费用。

修改按量计费套餐

1. 登录Web应用防火墙控制台。
2. 在左侧导航栏，选择**系统管理 > 账单与套餐中心**。
3. 在**账单与套餐中心**页面，定位到**已开通功能**模块。
4. 单击右上角**修改套餐**。
5. 在**修改套餐**页面，设置WAF的功能和对应的规格。**修改套餐**页面提供了各个功能的描述和开启后的费用。您可以进行以下设置：
   - 通过选中所需要的功能项，为您的WAF实例启用该功能。
   - 通过取消选中所需要的功能项，为您的WAF实例关闭该功能。
   - 在**系统规格**模块中，增加或减少日志存储容量和大屏服务的使用数量。
   - 域名和独享IP根据实际的使用数量计费，无需您手动设置数量。

   > **说明** 修改套餐功能项和系统规格后，您的WAF套餐账单金额也会产生相应的变化。您可以通过**修改套餐**页面上方的费用估算模块，了解修改套餐后使用WAF服务的预估账单金额。

6. 单击**确认修改**。

修改WAF套餐功能和规格后，您可以在**实时账单**模块，看到当前最新的预估账单金额。

相关文档

- 按量计费2.0版本计费方式
- 按量计费2.0版本常见问题

4.关闭WAF

如果您决定不再继续使用按量计费模式的WAF实例，您可以关闭WAF，确保不再产生任何费用。包年包月模式的WAF实例到期后，您也可以通过关闭WAF来释放该实例。

前提条件

只有在满足以下条件时，您才能够关闭或释放WAF实例。

- 包年包月模式： WAF实例已经到期。
- 按量付费模式： 近两日内仅有少量或没有请求到达WAF实例。

背景信息

如果您希望变更Web应用防火墙的计费方式，则必须先关闭当前WAF实例。

- 如果要将Web应用防火墙的计费方式从按量付费变更为包年包月，则必须先关闭当前按量付费模式的WAF实例。
- 如果要将Web应用防火墙的计费方式从包年包月变更为按量付费，则必须先释放已到期的包年包月模式的WAF实例。

> **说明** 关闭WAF实例前，请确认当前配置的网站域名DNS已解析回源站。关闭或释放WAF实例后，所有网站域名配置信息将被清空。如果仍有请求到达WAF实例，其将无法被正常转发，导致网站无法正常访问。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**海外地区**）。
3. 在**总览**页面右上角，单击**关闭WAF**。

   > **说明** 包年包月模式的WAF只有在实例到期后，才会出现该按钮。

4. 确认当前配置的网站域名解析已切换回到源站，单击**确定**，即可关闭WAF。

5.设置独享集群

为更好地支持个性化业务的应用防护需求，Web应用防火墙（WAF）提供独享版，即采用虚拟独享集群，支持基于业务特性的定制化接入和防护能力。

背景信息

为了特定的业务需求，网站业务可能使用非常规的设计方式实现。独享集群支持将具有定制化需求的业务系统接入WAF，为业务提供全面的应用层攻击防护。

购买WAF独享版后，您可以根据业务特性自定义独享集群的业务配置，具体包括：

- 集群所在地区：支持自主选择集群地区。
- 集群端口设置：支持更大范围的非标端口的接入防护，支持基于HTTP、HTTPS和HTTP 2.0协议的自定义回源端口配置。

  > **说明** 仅不支持22、53、9100、4431、4646、8301、6060、8600、56688、15001、4985、4986、4987这些特定的系统端口。

- SNI认证：支持上传默认SNI证书，允许暂不支持标准SNI协议的客户端设备正常访问网站。
- 防护响应页面：支持配置已上传至阿里云CDN的静态页面URL，WAF将使用该页面作为防护响应页面，提升网站用户体验。
- TLS安全策略： 支持自主选择TLS协议版本与加密套件。
- 长链接超时配置：支持自定义建立连接、请求、响应的超时时长。

创建独享集群

购买或升级至WAF独享版后，您可以选择使用虚拟独享防护集群和公共防护集群两种形式的防护资源对您的网站进行防护。使用独享集群前，需要根据您的业务特性创建独享集群。

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，选择**系统管理 > 独享集群设置**。
4. 在**独享集群设置**页面，根据业务特性设置集群配置。
   - 选择**集群地区**。

     > **说明** 独享集群创建完成后，**集群地区**无法变更。

   - 设置**服务器端口**范围：选择协议类型，单击**自定义**，填写服务器端口范围并单击**保存**。当您将网站域名配置接入独享集群时，可快速选择独享集群服务器端口范围中的端口。
   - 设置**防护响应页面URL**：填写已上传至阿里云CDN的静态页面URL，接入独享集群防护的网站业务将使用该页面作为WAF的防护响应页面。
   - 填写默认SNI**证书文件**和**私钥文件**内容：上传默认SNI证书。
   - HTTPS协议加密设置。
     - **TLS协议版本**：默认为**支持TLS1.0及以上版本，兼容性最高，安全性较低**。您可以根据安全需要选择仅支持TLS1.1或TLS1.2以上版本。

- **加密套件**：
  - 选择，支持基于域名维度自定义TLS版本和加密套件。TLS支持单独自定义，加密套件支持强加密、弱加密以及单个算法的自定义。
  - 选择**强加密套件，兼容性较低，安全性较高**，仅支持以下强加密套件：
    - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
  - 选择**全部加密套件，兼容性较高，安全性较低**，则除上述强加密套件外还支持以下弱加密套件：
    - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
    - TLS_RSA_WITH_AES_128_GCM_SHA256
    - TLS_RSA_WITH_AES_256_GCM_SHA384
    - TLS_RSA_WITH_AES_128_CBC_SHA256
    - TLS_RSA_WITH_AES_256_CBC_SHA256
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_AES_256_CBC_SHA
    - SSL_RSA_WITH_3DES_EDE_CBC_SHA

- 设置长连接超时时长。
  - **链接超时时长**：设置建立链接的超时时长，可设置5~3600秒间的值。
  - **读链接超时时长**：设置读取类链接的超时时长，可设置120~3600秒间的值。
  - **写链接超时时长**：设置写入类链接的超时时长，可设置120~3600秒间的值。

5. 单击**立即创建**。
   系统将根据所设定的集群配置为您创建独享集群，创建集群大约需要20分钟。独享集群创建完成后，您可以在**独享集群设置**页面查看和修改独享集群的相关设置。

后续步骤

独享集群创建完成后，您就可以将具有定制化需求的业务接入独享集群进行防护。具体分为以下场景：

- 您可以在新添加网站域名配置时，将业务接入独享集群进行防护。更多信息，请参见网站接入。
- 对于已添加的网站域名配置，您可以在**网站接入**页面将该域名配置记录的**防护资源**修改为**独享集群**，将业务接入独享集群进行防护。

  您也可以使用该方法将已接入独享集群的域名配置切换至公共集群。

  > **注意** 由于独享集群和公共集群的自定义端口范围存在差异，切换时请务必确认网站域名的自定义端口配置的兼容性。

6.独享集群最佳实践

Web应用防火墙（WAF）独享集群在WAF公共集群防护能力的基础上，为您提供与实际业务特性相结合的定制化服务，包括非标端口接入、SNI认证、自定义防护响应页面、HTTPS协议加密设置、长链接超时设置。若您的业务系统包含上述非常规设计/需求，您可以依据业务体系配置独享集群，并将网站业务接入独享集群进行防护。

独享集群vs公共集群

对比项	WAF公共集群	WAF独享集群
集群地区	公共集群在全球共部署14个防护节点，分布在以下地区：北京、上海、杭州、深圳、中国香港、新加坡、马来西亚、美东、美西、澳洲、德国、印度、印尼、迪拜。 业务接入公共集群防护时，根据源站IP自动匹配最佳地区的防护资源。	独享集群包括主、备集群。使用独享集群时，您可以从支持的地区中指定独享集群主集群的地区，备集群地区不可选择。 **说明** 主集群地区一经设置，不可更改。 业务接入独享集群防护时，默认使用独享集群主集群地区的防护资源；备集群则提供备用服务，在主集群出故障时承担业务，或在攻击来临时进行防御。
集群端口	若您的业务使用特殊端口，则在WAF添加网站配置时，您需要自定义端口。公共集群支持有限的非标端口，具体请参见非标端口支持。	独享集群比公共集群支持范围更广的非标端口，理论上仅不支持22、53、9100、4431、4646、8301、6060、8600、56688、15001、4985、4986、4987等特定的系统端口。 使用独享集群自定义端口时，您必须先在独享集群设置中开启服务器端口，然后在添加网站到独享集群防护时，选择应用已开启的端口。 **说明** 独享集群最多支持开启50个自定义端口，默认只开启了80和443端口。
SNI认证	业务接入WAF公共集群后，若客户端不兼容SNI，则可能导致HTTPS业务访问异常，具体请参见SNI兼容性导致HTTPS访问异常。	配置独享集群时，您可以上传默认SNI证书。这样，在业务接入独享集群后，即使暂不支持标准SNI协议的客户端设备也能正常访问网站。
防护响应页面	WAF公共集群使用默认的防护响应页面，例如异常访问被拦截时返回默认的拦截提示页面。	若您希望防护响应页面与您的网站设计风格保持一致，您可以使用独享集群自定义防护响应页面。 您可以将设计好的静态页面上传至阿里云CDN，并配置静态页面URL作为WAF的防护响应页面，提升网站用户体验。

对比项	WAF公共集群	WAF独享集群
HTTPS协议加密设置	公共集群不支持该项配置。	在独享集群配置中，您可以根据业务安全需求选择合适的TLS协议版本和加密套件。
长链接超时限制	公共集群不支持该项配置。	在独享集群配置中，您可以根据业务需求设置长链接限制时长，减少网络连接问题占用资源。

业务接入WAF独享集群

前提条件

要使用WAF独享集群，您必须首先购买WAF独享版或升级现有WAF版本到独享版。更多信息，请参见开通Web应用防火墙、续费与升级（包年包月）。

操作步骤

开通WAF独享版后，您可以参照以下步骤接入网站业务到WAF独享集群进行防护。假设您的业务端口是90（不在公共集群支持的非标端口范围内）。

1. 配置独享集群。
   i. 登录Web应用防火墙控制台。
   ii. 在顶部导航栏，选择Web应用防火墙实例的资源组和地域（**中国大陆**、**海外地区**）。

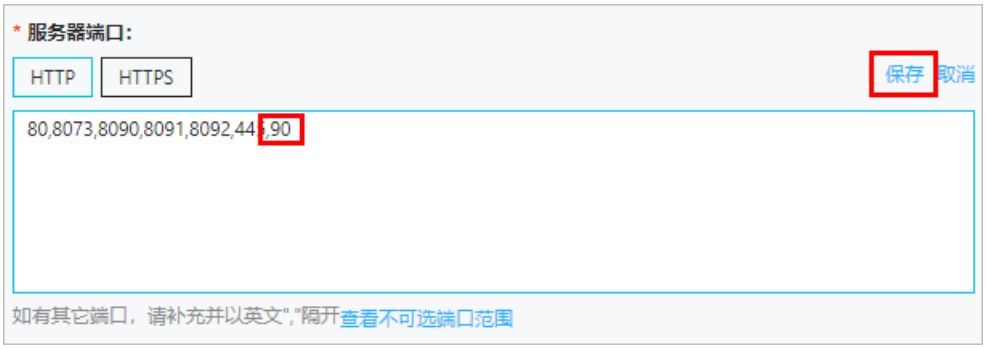
   iii. 在左侧导航栏，单击**系统管理 > 独享集群设置**。

iv. 在**独享集群设置**页面，根据您的业务特性配置独享集群。

本示例中，您需要在**服务器端口**中添加**HTTP**协议的**90**端口。操作步骤如下。

a. 在**服务器端口**下，单击**自定义**。

b. 在**HTTP**协议下添加90端口，并单击**保存**。



c. 确认90端口已开启。

更多信息，请参见设置独享集群。

v. 单击**保存设置**。

系统将根据所设定的集群配置为您配置独享集群。

2. 将具有定制化需求的业务（例如端口是90的业务）接入独享集群进行防护。

- 已添加网站配置

a. 在左侧导航栏，单击**资产中心 > 网站接入**。

b. 定位到要接入独享集群防护的网站，将其**防护资源**设置为**独享集群**。

> **说明**
>
> - 只有**独享版**Web应用防火墙实例才支持**防护资源**配置。
> - 在切换独享集群防护时，请确认网站配置的业务端口包含在独享集群设置中。例如当前网站配置的业务端口是HTTP协议80端口，则请确认独享集群设置下的服务器端口中包含HTTP协议80端口。

c. （可选）根据需要编辑网站配置（例如服务器端口修改为HTTP协议90端口）。更多信息，请参见网站接入。

- 新添加网站配置

a. 在左侧导航栏，单击**资产中心 > 网站接入**。

b. 在**网站接入**页面，单击**添加域名**，并选择**手动添加其他网站**。

c. 在**填写网站信息**任务中，将**防护资源**设置为**独享集群**，并填写实际业务信息（例如服务器端口选择HTTP协议90端口）。

> **说明** 选择**独享集群**防护后，则**服务器端口**只能从独享集群设置中已开启的服务器端口范围内选择，具体请参见配置独享集群。

更多信息，请参见手动添加网站。

d. 单击**下一步**，并根据页面提示修改域名的DNS解析，将实际业务切换到WAF进行防护。

更多信息，请参见修改域名DNS。

3. 业务接入WAF独享集群防护后，若业务特性发生变化且涉及到独享集群配置，请参见步骤1（更新集群配置）、步骤2（编辑网站配置）进行调整。