ALIBABA CLOUD

Alibaba Cloud

云防火墙

云防火墙控制台概览

文档版本：20220420

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.概览 ---- 05
2.流量拓扑可视化 ---- 08
3.授权云防火墙访问云资源 ---- 10
4.升级和续费 ---- 17

1.概览

云防火墙概览页面从待处理事件、资产防护、安全防护、安全策略、流量趋势、场景数据、近期更新等角度，向您展示云防火墙的整体防护能力和统计信息，帮助您了解网络资产的安全状况。

访问概览页面

您可以在云防火墙控制台，单击左侧导航栏的**概览**，打开**概览**页面。

概览页面的右上角展示了当前云防火墙实例的版本和剩余有效天数，并支持以下操作：

- 对当前实例进行**带宽升级**、**升级**、**续费**以及设置**自动续费**。更多信息，请参见升级和续费。
- 单击**更多**，查看实例的详细信息，包含**公网流量处理能力**、**近期流量峰值**、**公网IP防护授权数**、**VPC防护授权数**、**日志审计存储量**和**多账号授权数**。

待处理事件

该区域展示了近期云防火墙在您已开启防护的资产中发现的**已失陷主机**、**待防护漏洞数**、**对外开放端口**、**异常外联**的数量。

您可以在该区域执行以下操作：

- 设置查询时间：单击右上角的时间下拉列表，选择要查询的时间范围（**最近1天**、**最近7天**）。
- 处理异常事件：将光标放置在某个异常事件区域，并单击**立即处理**，页面将会跳转到对应的异常事件列表（例如，单击上图中**异常外联**下的**立即处理**，将会跳转到**主动外联活动**页面），方便您处理异常事件。

  关于处理不同异常事件的具体方法，请参见以下内容：

  - 失陷感知
  - 漏洞防护
  - 互联网访问活动
  - 主动外联活动

资产保护

该区域展示了您的资产保护情况，包含已开启或未开启**互联网边界防火墙**、**VPC边界防火墙**、**主机边界防火墙**防护的公网IP资产的数量。

在该区域右上方，单击**按月自动续费**，云防火墙将会为您的网络资产持续防护。

对于没有开启防护的资产，您可以在云防火墙控制台的**防火墙开关**页面，开启对应的防火墙。更多信息，请参见开启或关闭互联网边界防火墙、开启或关闭VPC边界防火墙。

安全防护

该区域展示了近期，云防火墙为您的资产触发的安全防护的次数，包含**防护总次数**、**入侵攻击拦截数**、**访问控制拦截数**、**漏洞攻击拦截数**。

您可以在该区域执行以下操作：

- 设置查询时间：单击右上角的时间下拉列表，选择要查询的时间范围（**最近1天**、**最近7天**）。
- 查看详情：单击**展开**，可以查看不同防护模块的数据详情。

  关于不同防护模块的更多信息，请参见以下内容：

  - 入侵防御
  - 访问控制策略总览
  - 漏洞防护

安全策略

该区域展示了访问控制策略的相关数据，包含**待下发智能策略数**、**总ACL策略数**（及近7日的变化量）。

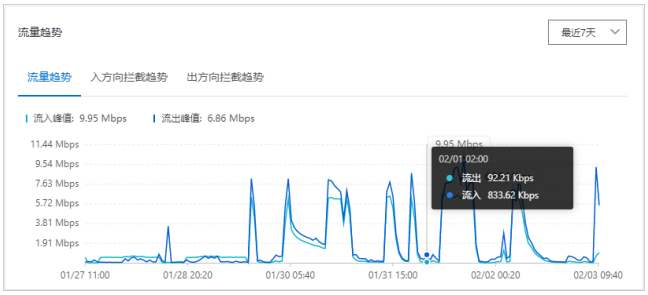
单击待下发智能策略的数量，页面将会跳转到**访问控制**页面的**智能策略推荐**面板，方便您查看和下发云防火墙为您推荐的智能策略。具体操作，请参见AI智能策略。

单击总ACL策略数的数量，页面将会跳转到**访问控制**页面，方便您查看或操作每条策略。

在该区域右上方，单击**观看ACL配置教程**，可观看**如何配置互联网边界防火墙访问控制策略**视频。

流量趋势

该区域展示了近期，已开启防护的资产上的整体流量趋势和云防火墙在入方向、出方向拦截的会话数量的变化趋势。



您可以在该区域执行以下操作：

- 设置查询时间：单击右上角的时间下拉列表，选择要查询的时间范围（**最近1天**、**最近7天**）。
- 切换要查看的趋势图：单击不同页签（**流量趋势**、**入方向拦截趋势**、**出方向拦截趋势**），可以查看对应的趋势图。

场景数据

该区域展示了近期，云防火墙在已开启防护的资产上检测到的暴力破解、扫描、挖矿行为、数据库防护风险信息。

您可以在该区域执行以下操作：

- 设置查询时间：单击右上角的时间下拉列表，选择要查询的时间范围（**最近1天**、**最近7天**）。
- 切换要查看的场景数据：单击不同页签（**暴力破解**、**扫描**、**挖矿行为**、**数据库防护**），可以查看对应的数据。不同数据的具体说明如下：
  - **暴力破解**：展示了暴力破解的攻击统计数据和攻击应用、攻击资产的排行图。攻击统计数据包含**攻击次数**、**拦截次数**、**攻击应用**数量、**攻击资产**数量。
  - **扫描**：展示了扫描风险统计数据和扫描应用、被扫描资产排行图。攻击统计数据包含**攻击次数**、**拦截次数**、**攻击应用**数量、**攻击资产**数量。
  - **挖矿行为**：展示了挖矿病毒的攻击统计数据和攻击应用、攻击资产的排行图。攻击统计数据包含**攻击次数**、**拦截次数**、**攻击应用**数量、**攻击资产**数量。
  - **数据库防护**：展示了数据库防护的攻击统计数据和攻击应用、攻击资产的排行图。攻击统计数据包含**攻击次数**、**拦截次数**、**攻击应用**数量、**攻击资产**数量。

近期更新

该区域展示了近期，云防火墙的**虚拟补丁**、**规则更新**和**功能更新**的更新记录。

您可以单击不同页签（**虚拟补丁**、**规则更新**、**功能更新**），查看对应的更新记录。

2.流量拓扑可视化

流量拓扑可视化功能展示了云防火墙防护的云资产的流量拓扑图。目前拓扑图支持展示云资产的互联网边界流量和VPC边界流量。

版本支持说明

仅企业版和旗舰版云防火墙支持该功能。

访问流量可视化拓扑页面

登录云防火墙控制台，通过**概览**页访问**流量拓扑可视化**页签。

总览

该区域展示了**公网IP**、**VPC**、**流量**和**入侵防护状态**。

您可以在该区域查看以下信息：

- **公网IP**：
  - **总IP数**：表示当前阿里云账号下所有公网资产IP的总数量。
  - **未保护IP数**：表示未开启防火墙开关的IP的总数量。

    单击**立即保护**，可跳转至**防火墙开关**页面的**互联网边界防火墙**页签，您可以对未开启防护的云资产开启防火墙开关。
- **VPC**：
  - **总VPC数**：表示当前阿里云账号下所有通过高速通道连接的VPC和云企业网中的VPC的个数。
  - **未保护VPC数**：表示未在云防火墙开启防护的VPC个数。

    单击**立即保护**，可跳转至**防火墙开关**页面的**VPC边界防火墙**页签，您可以对未开启防护的VPC开启防火墙开关。
- **流量**：
  - **近7天流量峰值**：表示距离当前时间7天内，云防火墙防护的流量的峰值。
  - **出流量峰值**：表示距离当前时间7天内，云防火墙防护的出方向流量的峰值。
  - **入流量峰值**：表示距离当前时间7天内，云防火墙防护的入方向流量的峰值。
- **入侵防御状态**：

  此处展示的入侵防御状态是同步自**防护配置**页面中威胁引擎运行模式的状态。相关内容，请参见威胁引擎运行模式。

> **注意** 云防火墙服务开通后，威胁引擎默认启用**拦截模式**。具体开启哪种程度的拦截模式，云防火墙会根据您流量的实际情况进行判断和默认选择。只有开启**拦截模式**后，威胁情报、基础防御和虚拟补丁模块才会开启相应的威胁拦截。如未开启**拦截模式**，入侵防御模块将只会对各类威胁和恶意流量进行监控。

- **攻击**：
  - **已拦截攻击数**：表示云防火墙已拦截的恶意攻击的次数。
  - **总攻击数**：表示云防火墙防护的云资产受到恶意攻击的总次数。
- **ACL**：展示了已创建的访问控制策略的数量。

互联网边界防火墙

该区域展示了当前阿里云账号下所有的公网资产与互联网之间的流量拓扑图。

您在该区域可以进行以下操作：

- 单击云资产图标，会展示该云资产的公网IP。在页面左侧可查看**未保护IP**和**已保护IP**。
- 单击指定的IP，在页面左侧面板中会展示该IP入方向和出方向流量的详情。

  入向页签中会展示**IP**、**开放活动端口**、**是否推荐智能策略**、**ACL访问控制**等信息。

  出向页签中会展示**外联域名**、**外联IP**、**是否推荐智能策略**、**ACL访问控制**等信息。

VPC边界防火墙

该区域分为**所有VPC**页签和**互联VPC**页签：

- **所有VPC**：该页签展示了当前阿里云账号下所有通过高速通道连接的VPC和云企业网中的VPC， 图标表示VPC已开启防护， 图标表示VPC未开启防护。将光标放置在VPC上，会展示该VPC的具体信息。
- **互联VPC**：该页签展示了通过高速通道连接的VPC和云企业网中VPC的详细信息。表示通过高速通道连接的VPC，表示云企业网中的VPC。单击**展开**，您可以查看VPC间的流量拓扑图。

  在页面左侧，展示了云企业网和高速通道中存在互联关系的VPC总数和所有存在互联关系的VPC，您可单击VPC的名称，查看具体的流量拓扑图。

3.授权云防火墙访问云资源

首次登录云防火墙控制台时，您必须完成允许云防火墙访问相关云资源的授权，才能正常使用云防火墙提供的服务。本文介绍了通过云防火墙服务关联角色AliyunServiceRoleForCloudFW，进行云资源访问授权的相关内容，以及如何删除AliyunServiceRoleForCloudFW。

前提条件

您使用的是阿里云主账号或拥有创建和删除服务关联角色权限的RAM用户账号。

关于如何为RAM用户授予操作服务关联角色的权限，请参见相关问题。

背景信息

为了向您提供对云上网络流量的访问控制、监控分析等功能，云防火墙需要访问您的<授权对象>云服务器ECS、专有网络VPC、负载均衡、日志服务、堡垒机、云企业网、云安全中心、云数据库RDS等云服务资源，您可通过系统自动创建的云防火墙服务关联角色AliyunServiceRoleForCloudFW进行访问授权。服务关联角色无需您手动创建或做任何修改。相关内容，请参见服务关联角色。

操作步骤

1. 登录云防火墙控制台。
2. 在**云防火墙服务关联角色**对话框，单击**确定**。

   > **说明** 如果您已经创建过AliyunServiceRoleForCloudFW，则该对话框不会出现，您可以直接在控制台使用云防火墙。

   完成后，阿里云将自动为您创建云防火墙服务关联角色AliyunServiceRoleForCloudFW。

   您可以在RAM控制台的**角色**页面，查看阿里云为云防火墙自动创建的服务关联角色。只有创建服务关联角色AliyunServiceRoleForCloudFW后，您的云防火墙实例才能访问<授权对象>云服务器ECS、专有网络VPC、负载均衡、日志服务、堡垒机、云企业网、云安全中心、云数据库RDS等关联云服务的资源。

AliyunServiceRoleForCloudFW权限说明

AliyunServiceRoleForCloudFW默认拥有AliyunServiceRolePolicyForCloudFW系统权限策略的授权。AliyunServiceRolePolicyForCloudFW中定义的权限如下所示。

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
```

```
                "ecs:DescribeInstances",
                "ecs:DescribeTags",
                "ecs:JoinSecurityGroup",
                "ecs:LeaveSecurityGroup",
                "ecs:AuthorizeSecurityGroupEgress",
                "ecs:DescribeRegions",
                "ecs:DescribeVpcs",
                "ecs:RevokeSecurityGroupEgress",
                "ecs:ModifySecurityGroupAttribute",
                "ecs:DeleteSecurityGroup",
                "ecs:RevokeSecurityGroup",
                "ecs:DescribeSecurityGroupAttribute",
                "ecs:CreateSecurityGroup",
                "ecs:AuthorizeSecurityGroup",
                "ecs:DescribeSecurityGroups",
                "ecs:DescribeSecurityGroupReferences",
                "ecs:ModifySecurityGroupPolicy",
                "ecs:ModifySecurityGroupRule",
                "ecs:ModifySecurityGroupEgressRule",
                "ecs:CreateNetworkInterface",
                "ecs:DeleteNetworkInterface",
                "ecs:DescribeNetworkInterfaces",
                "ecs:CreateNetworkInterfacePermission",
                "ecs:DescribeNetworkInterfacePermissions",
                "ecs:DeleteNetworkInterfacePermission",
                "ecs:AttachNetworkInterface",
                "ecs:DetachNetworkInterface"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:DescribeVpcs",
                "vpc:DescribeNatGateways",
                "vpc:DescribeSnatTableEntries",
                "vpc:DescribeForwardTableEntries",
                "vpc:DescribeBandwidthPackages",
                "vpc:GetNatGatewayAttribute",
                "vpc:ModifyNatGatewayAttribute",
                "vpc:DescribeEipAddresses",
                "vpc:DescribeRouterInterfaces",
                "vpc:DescribeRouteTableList",
                "vpc:DescribeRouteTables",
                "vpc:DescribeVSwitches",
                "vpc:CreateRouteEntry",
                "vpc:DeleteRouteEntry",
                "vpc:CreateVpc",
                "vpc:DeleteVpc",
                "vpc:CreateVSwitch",
                "vpc:DeleteVSwitch",
                "vpc:DescribeZones",
                "vpc:CreateVirtualBorderRouter",
                "vpc:ConnectRouterInterface",
                "vpc:ModifyRouterInterfaceAttribute"
```

```
                "vpc:ModifyRouterInterfaceAttribute",
                "vpc:DeleteRouterInterface",
                "vpc:CreateRouterInterface",
                "vpc:DeleteVirtualBorderRouter",
                "vpc:DeactivateRouterInterface",
                "vpc:DescribeVirtualBorderRouters",
                "vpc:DescribePhysicalConnections",
                "vpc:ModifyVirtualBorderRouterAttribute",
                "vpc:DescribeVpcAttribute",
                "vpc:DescribeVSwitchAttributes",
                "vpc:DescribeHaVips",
                "vpc:DescribeVpnConnections",
                "vpc:DescribeVpnRouteEntries",
                "vpc:DescribeVpnPbrRouteEntries",
                "vpc:DescribeVpnGateways",
                "vpc:DescribeSslVpnServers",
                "vpc:AssociateEipAddress",
                "vpc:UnassociateEipAddress",
                "vpc:CreateRouteTable",
                "vpc:DeleteRouteTable",
                "vpc:AssociateRouteTable",
                "vpc:UnassociateRouteTable",
                "vpc:CreateSnatEntry",
                "vpc:DeleteSnatEntry",
                "vpc:DescribeSnatTableEntries",
                "vpc:DescribeRouteEntryList",
                "vpc:DescribeIpv6Addresses"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "slb:DescribeRegions",
                "slb:DescribeLoadBalancers",
                "slb:DescribeLoadBalancerAttribute",
                "slb:DescribeLoadBalancerUDPListenerAttribute",
                "slb:DescribeLoadBalancerTCPListenerAttribute",
                "slb:DescribeLoadBalancerHTTPListenerAttribute",
                "slb:DescribeLoadBalancerHTTPSListenerAttribute",
                "slb:DescribeHealthStatus",
                "slb:DescribeAccessControlListAttribute"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "log:PostLogStoreLogs",
                "log:GetProject",
                "log:ListProject",
                "log:GetLogStore",
                "log:ListLogStores",
                "log:CreateLogStore",
                "log:CreateProject",
```

```
                "log:CreateLogstore",
                "log:GetIndex",
                "log:CreateIndex",
                "log:UpdateIndex",
                "log:CreateDashboard",
                "log:ClearLogStoreStorage",
                "log:UpdateLogStore",
                "log:UpdateDashboard",
                "log:CreateSavedSearch",
                "log:UpdateSavedSearch",
                "log:DeleteLogStore",
                "log:DeleteSavedSearch",
                "log:GetSavedSearch",
                "log:ListSavedSearch",
                "log:DeleteDashboard",
                "log:GetDashboard",
                "log:ListDashboard"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "yundun-bastionhost:DescribeInstance",
                "yundun-bastionhost:DescribeRegions",
                "yundun-bastionhost:DescribeInstances",
                "yundun-bastionhost:DescribeInstanceBastionhost",
                "yundun-bastionhost:DescribeInstanceAttribute"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "cen:DescribeCens",
                "cen:DescribeCenAttachedChildInstances",
                "cen:DescribeCenAttachedChildInstanceAttribute",
                "cen:AttachCenChildInstance",
                "cen:DetachCenChildInstance",
                "cen:PublishRouteEntries",
                "cen:WithdrawPublishedRouteEntries",
                "cen:DescribePublishedRouteEntries",
                "cen:DescribeCenRegionDomainRouteEntries",
                "cen:ModifyCenAttribute",
                "cen:CreateCenRouteMap",
                "cen:DeleteCenRouteMap",
                "cen:ModifyCenRouteMap",
                "cen:DescribeCenRouteMaps",
                "cen:DescribeCenChildInstanceRouteEntries",
                "cen:CreateCenChildInstanceRouteEntryToCen",
                "cen:DeleteCenChildInstanceRouteEntryToCen",
                "cen:ListTransitRouters",
                "cen:CreateTransitRouter",
                "cen:DeleteTransitRouter",
                "cen:ListTransitRouterAttachments",
```

```
                "cen:CreateTransitRouterVpcAttachment",
                "cen:DeleteTransitRouterVpcAttachment",
                "cen:UpdateTransitRouterVpcAttachmentAttribute",
                "cen:UpdateTransitRouterPeerAttachmentAttribute",
                "cen:CreateTransitRouterVbrAttachment",
                "cen:DeleteTransitRouterVbrAttachment",
                "cen:ListTransitRouterPeerAttachments",
                "cen:ListTransitRouterVpcAttachments",
                "cen:ListTransitRouterVbrAttachments",
                "cen:ListTransitRouterAvailableResource",
                "cen:CreateTransitRouterRouteTable",
                "cen:UpdateTransitRouterRouteTable",
                "cen:DeleteTransitRouterRouteTable",
                "cen:ListTransitRouterRouteTables",
                "cen:CreateTransitRouterRouteEntry",
                "cen:DeleteTransitRouterRouteEntry",
                "cen:ListTransitRouterRouteEntries",
                "cen:ListTransitRouterRouteTableAssociations",
                "cen:AssociateTransitRouterAttachmentWithRouteTable",
                "cen:DissociateTransitRouterAttachmentFromRouteTable",
                "cen:ListTransitRouterRouteTablePropagations",
                "cen:EnableTransitRouterRouteTablePropagation",
                "cen:DisableTransitRouterRouteTablePropagation",
                "cen:ModifyCenUserQuota"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "netana:DescribeNetworkQuotas",
                "netana:DescribeNetworkQuotaRequestResult",
                "netana:CreateNetworkQuotaRequest"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "yundun-sas:DescribeVulList",
                "yundun-sas:DescribeVulDetails"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "ram:CreateServiceLinkedRole",
```

```
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "cen.aliyuncs.com"
                }
            }
        },
        {
            "Action": [
                "resourcemanager:ListAccounts"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "ram:DeleteServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "cloudfw.aliyuncs.com"
                }
            }
        }
    ]
}
```

关于权限策略语法的详细说明，请参见权限策略基本元素。

删除服务关联角色

如果不再需要使用云防火墙，您可以删除云防火墙服务关联角色AliyunServiceRoleForCloudFW。只有当云防火墙实例已经过期并自动释放后，您才可以删除服务关联角色。具体操作，请参见删除RAM角色。

相关问题

为什么我的RAM用户无法自动创建云防火墙服务关联角色AliyunServiceRoleForCloudFW?

您需要拥有指定的权限，才能自动创建或删除AliyunServiceRoleForCloudFW。因此，在RAM用户无法自动创建AliyunServiceRoleForCloudFW时，您需为RAM用户添加以下权限策略。详细操作步骤指导，请参见为RAM用户授权。

```
{
    "Statement": [
        {
            "Action": [
                "ram:CreateServiceLinkedRole"
            ],
            "Resource": "acs:ram:*:主账号ID:role/*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "cloudfw.aliyuncs.com"
                    ]
                }
            }
        }
    ],
    "Version": "1"
}
```

4.升级和续费

云防火墙分为高级版、企业版和旗舰版三个版本，您可升级到对应版本使用符合您需要的云防火墙功能。

您可在云防火墙管理控制台**概览**页面右上角，单击**升级**或**续费**并进行对应的操作。

不同版本对应的功能请参见功能特性。

升级与续费操作请参见服务续费与升级。

> **说明** 云防火墙当前服务到期前请及时续费，否则会影响对您网络的安全防护。