阿里云
DDoS防护

DDoS原生防护-基础版

文档版本：20200624

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. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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
	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。	 **禁止：** 重置操作将丢失用户配置数据。
	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。
	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。
	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。	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 新功能发布记录

本章节介绍了DDoS基础防护的产品功能和对应的文档动态。

2019年12月

功能名称	功能描述	发布时间	相关文档
新版控制台界面	发布新版控制台界面，主要变更如下： • 左侧导航栏标题由**DDoS基础防护**变更为**DDoS防护产品**。 • 左侧导航栏**基础防护** > **实例**页面变更为**资产中心**页面，且页面中的**DDoS攻击防护说明**内容更新。 • 左侧导航栏**防护包** > **安全报表**、**防护包** > **防护包列表**、**防护包** > **流量包管理**和**防护包** > **操作日志**页面变更为**DDoS原生防护** > **实例管理**页面。 • 左侧导航栏新增以下页面： - **DDoS高防** > **DDoS高防（新BGP）**：直达DDoS高防（新BGP）管理控制台。 - **DDoS高防** > **DDoS高防（国际）**：直达DDoS高防（国际）管理控制台。 - **行业解决方案** > **游戏盾**：直达游戏盾管理控制台。 - **DDoS防护选型**：访问帮助文档**基于防御场景选择DDoS防护解决方案。**	2019-12-18	快速入门
资产中心	原**基础防护** > **实例**页面变更为**资产中心**页面。 DDoS防护资产中心向您展示阿里云账号下已开通资产（包括ECS、SLB、EIP等）的DDoS防护状态，帮助您快速了解资产的DDoS安全风险，并支持为指定资产提升DDoS防护能力。	2019-12-18	资产中心

功能名称	功能描述	发布时间	相关文档
动态弹性防护	原固定弹性防护阈值变更为动态弹性防护，控制台不再显示**安全信誉**分值。 动态弹性防护方式下，阿里云根据当前DDoS防护机房的水位、可用资源和资产遭受的历史攻击，以及账号安全信誉等因素，在免费的基础防护能力以上，为您的资产动态分配额外的弹性防护能力。	2019-12-18	#unique_6

2 快速入门

2.1 快速入门

云盾DDoS防护默认开启，免费为您阿里云账号下的ECS、SLB和EIP实例提供不超过5Gbps流量的DDoS攻击防护能力。本快速入门将指导您查看阿里云账号下云资源的DDoS防护配置和数据，以及DDoS防护说明。您可以根据需要调整防护配置。

背景信息

使用DDoS防护时，请注意以下内容：

- 根据业务需求设置适当的清洗阈值。当IP遭受的DDoS攻击带宽超过清洗阈值时，阿里云会开始对攻击流量进行清洗，并尽可能保障您的业务可用。
- 关注实例的DDoS攻击防护能力。当攻击带宽不超过实例的DDoS基础防护阈值时，阿里云免费为您清洗攻击流量。IP所在地域不同，所提供的默认DDoS基础防护阈值不同。
- 根据实际需求开通DDoS高防。当攻击带宽超过DDoS基础防护阈值，被攻击IP将进入黑洞状态。建议您使用DDoS高防提升防护能力。关于DDoS高防的详细介绍，请参见什么是DDoS高防。

操作步骤

1. 登录云盾DDoS防护产品控制台。
2. 在**资产中心**页面上方选择资产所在地域。
3. 在**资产中心**页面查看**DDoS攻击防护说明**。DDoS攻击防护说明中提供以下内容链接：
   - 单击**默认基础防护阈值**，查看不同地域下资产的默认DDoS防护能力，即支持防御的DDoS攻击带宽。
   - 单击**黑洞**，查看阿里云黑洞策略。
   - 单击**高防IP**，前往DDoS高防控制台**实例列表**页面，您可以根据需要开通DDoS高防实例。

更多信息，请参见资产中心。

4. 根据需要调整流量清洗阈值。

   a) 在**资产中心**页面，单击对应页签，选择要操作的云产品类型：**ECS**、**SLB**、**EIP（含NAT）**、**其他**。

   - **ECS**：云服务器ECS实例公网IP
   - **SLB**：负载均衡SLB实例公网IP
   - **EIP（含NAT）**：弹性公网IP和NAT IP

   说明：

ECS或SLB绑定的EIP均属于EIP类型。

- **其他**：代播实例IP段

b) 在实例列表中定位到要操作的实例，单击其**IP**。

如果实例过多，建议您使用**实例ID**、**实例名称**或**实例IP**搜索目标实例。

进入**实例详情**侧边页。该页面展示了当前实例在近7天内的流量和报文记录以及DDoS攻击事件记录。

c) 在**实例详情**页面，单击**清洗设置**，选择**手动设置**或选择**系统默认**的清洗阈值。

更多信息，请参见设置清洗阈值。

3 用户指南

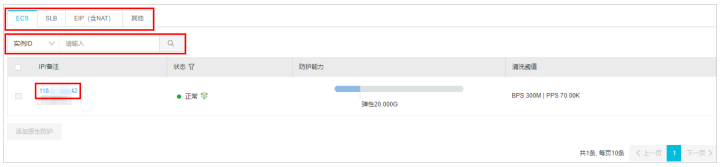
3.1 设置清洗阈值

云盾DDoS防护为您的阿里云资产（包括ECS、SLB、EIP等）免费提供DDoS基础防护能力，资产开通后默认启用DDoS防护。当IP遭受的DDoS攻击带宽超过清洗阈值时，DDoS防护对攻击流量进行清洗，并尽可能保障您的业务可用。本文介绍了为指定资产设置DDoS防护清洗阈值的操作方法。

操作步骤

1. 登录云盾DDoS防护产品控制台。
2. 在**资产中心**页面上方选择资产所在地域。
3. 单击对应页签，选择要操作的云产品类型：**ECS**、**SLB**、**EIP（含NAT）**、**其他**。
4. 在实例列表中定位到要操作的实例，单击其**IP**。

   如果实例过多，建议您使用**实例ID**、**实例名称**或**实例IP**搜索目标实例。



5. 在**实例详情**侧边页，单击**清洗设置**。

6. 在**清洗设置**侧边页，设置目标实例的清洗阈值，支持**系统默认**和**手动设置**。

   - 选择**系统默认**，系统会根据云服务器的流量负载动态调整清洗阈值。
   - 选择**手动设置**，可以手动选择流量和报文数量的清洗阈值。

   清洗阈值设置建议：

   - 清洗阈值需要略高于实际访问值。阈值设置过高，起不到防御效果；而设置过低，DDoS防护触发流量清洗可能会影响正常的访问。
   - 如果清洗影响了正常的请求，请适当调高清洗阈值。
   - 在网站做推广或者活动时，建议您适当调大清洗阈值。

预期结果

成功设置清洗阈值。当网站请求达到设置的清洗阈值时，DDoS防护将触发流量清洗。

3.2 取消流量清洗

云盾DDoS防护默认为阿里云服务器提供DDoS攻击防御能力。当服务器遭受流量攻击时，监控系统自动检测到攻击，并为服务器清洗异常流量。对于处于异常状态（清洗中）的IP资产，您可以手动取消流量清洗。

背景信息

清洗是指对进入服务器的数据流量进行实时监控，及时发现包括DDoS攻击在内的异常流量。在不影响正常业务的前提下，清洗掉异常流量，将可疑流量从原始网络路径中重定向到净化产品上进行恶意流量的识别和剥离，还原出的合法流量回注到原网络中转发给目标系统。

说明：
一个账号一天之内可以手动取消流量清洗三次。

操作步骤

1. 登录云盾DDoS防护产品控制台。

2. 在**资产中心**页面上方选择资产所在地域。
3. 单击对应页签，选择要操作的云产品类型：**ECS**、**SLB**、**EIP（含NAT）**、**其他**。
4. 在实例列表中定位到要操作的实例（**状态**为**清洗中**），单击其**IP**。
5. 在**实例详情**侧边页，定位到进行中的清洗事件（**事件**为**清洗**且**结束时间**为空），单击其操作列下的**取消清洗**。

> **说明：**
> 如果当前没有进行中的清洗事件，则**取消清洗**操作不会出现。

预期结果

成功取消流量清洗。

后续步骤

取消流量清洗后，建议您根据当前业务需要（例如活动或大促期间业务访问量增大）适当调高清洗阈值，避免再次触发流量清洗。更多信息，请参见设置清洗阈值。

说明:

最大清洗阈值和云产品实例的规格绑定。如果可配置的最大清洗阈值无法满足您的需求，建议您升级云产品规格。

3.3 查看黑洞时长

服务器遭受DDoS攻击触发黑洞后，其公网IP在一定时间内将无法被访问，只有等到黑洞时长过后才会恢复正常访问。不同地域资产的默认黑洞时长不同，且黑洞时长受资产遭受的攻击情况影响。您可以在DDoS防护控制台查看当前资产的黑洞时长。

背景信息

默认的黑洞时长是2.5小时，黑洞期间不支持解封。实际黑洞时长视攻击情况而定，从30分钟到24小时不等。黑洞时长主要受以下因素影响：

- 攻击是否持续。如果攻击一直持续，黑洞时间会延长。
- 攻击是否频繁。如果用户首次被攻击，黑洞时间会自动缩短；反之，频繁被攻击的用户被持续攻击的概率较大，因此黑洞时间会自动延长。

具体黑洞阈值和实际黑洞时长以云盾DDoS防护控制台显示为准，详见下文操作步骤。

说明:

- 针对个别黑洞过于频繁的用户，阿里云保留延长黑洞时长和降低黑洞阈值的权利。
- 黑洞是网络运营商为阿里云提供的服务，运营商有明确的黑洞解除时间限制。因此，一般情况下黑洞时长不小于30分钟，且您账号的黑洞时长将根据您账号的安全信誉等级自动调整。

关于阿里云黑洞策略的更多信息，请参见#unique_9。

操作步骤

1. 登录云盾DDoS防护产品控制台。
2. 在**资产中心**页面上方选择资产所在地域。

3. 在资产列表上方查看**DDoS攻击防护说明**。

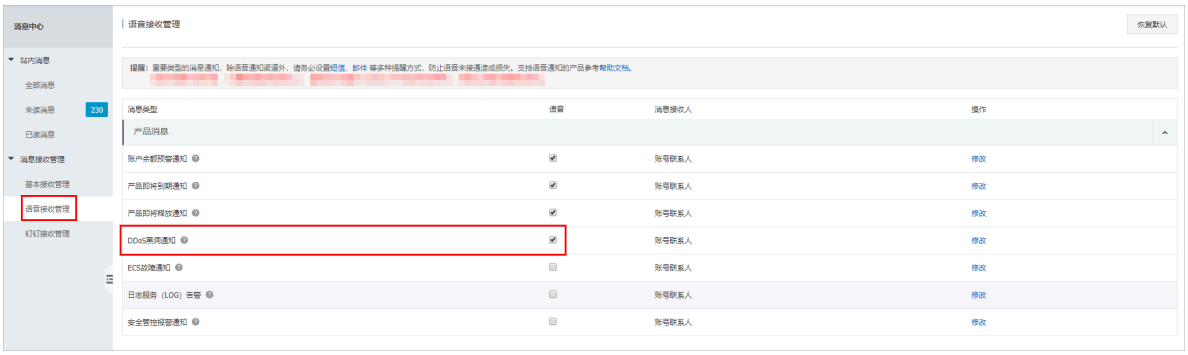
   DDoS攻击防护说明中的**当前黑洞解除时间**即当前地域下资产的黑洞时长

3.4 设置黑洞告警通知

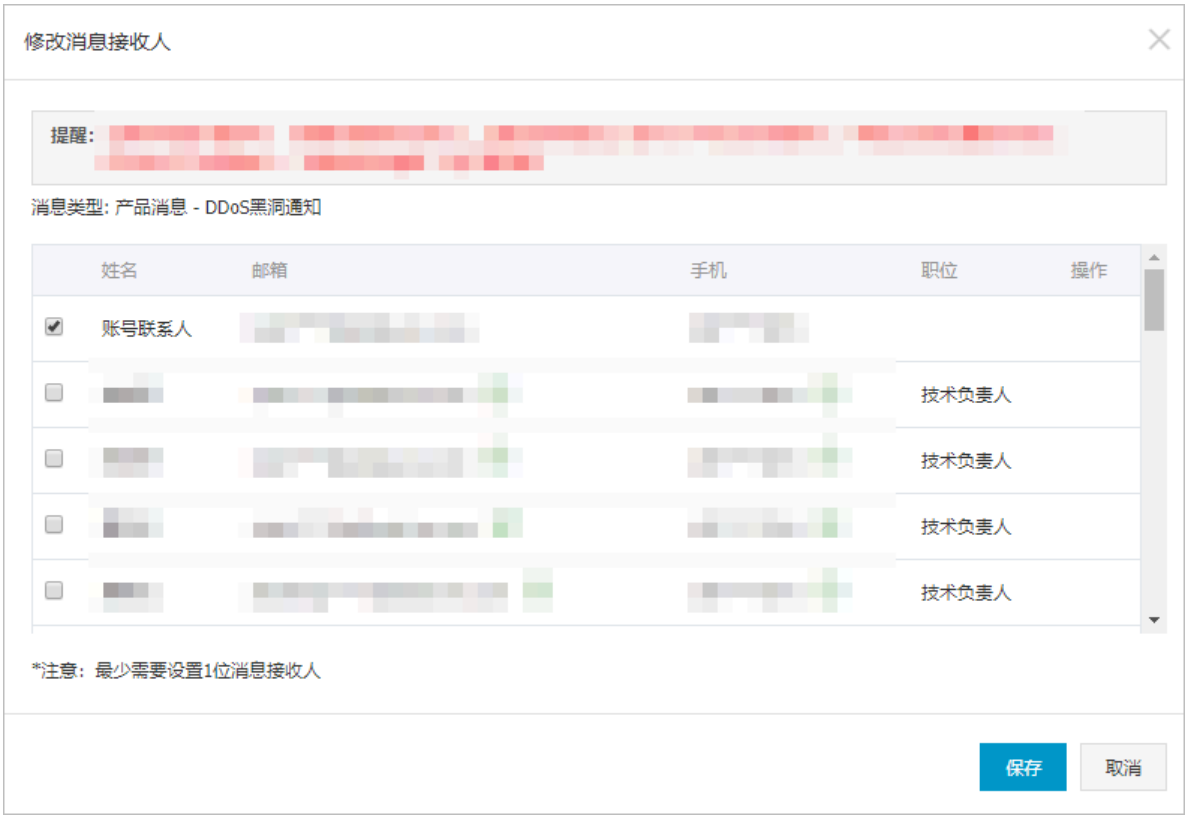
阿里云的DDoS黑洞通知提供告警通知功能。当您账号中的服务器遭受大量DDoS攻击触发黑洞时，您所设定的消息接收人将收到通知。

启用DDoS黑洞语音告警

1. 登录消息中心管理控制台。
2. 在左侧导航栏，单击**消息接收管理 > 语音接收管理**。
3. 定位到**DDoS黑洞通知**，勾选**语音**，启用语音告警功能。



4. 单击**DDoS黑洞通知**操作列下的**修改**，并在**修改消息接收人**对话框中添加、修改DDoS黑洞通知的消息接收人。



设置云盾安全信息通知的消息接收人

云盾安全信息通知支持以站内信、邮箱、短信的形式向您设置的消息接收人发送安全信息通知。

1. 登录消息中心管理控制台。
2. 在左侧导航栏，单击**消息接收管理 > 基本接收管理**。
3. 定位到**云盾安全信息通知**，单击**账号联系人**下的**修改**。

4. 在**修改消息接收人**对话框中，修改云盾安全信息通知的消息接收人。

说明:

您也可以单击**新增消息接收人**，添加消息接收人。

3.5 查看IP进入黑洞的时间和原因

当ECS或SLB实例的公网IP遭到大量DDoS攻击，且DDoS攻击的流量超出对应的黑洞阈值后，该公网IP将被黑洞，所有来自外部的流量都将被丢弃，导致相关的业务无法正常访问。您可以在云盾DDoS防护控制台查看账号下资产的黑洞事件信息，例如IP进入黑洞的时间及所遭受的攻击流量。

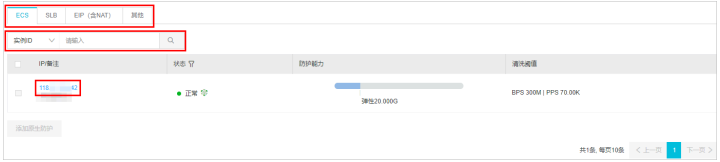
背景信息

不同地域下实例的黑洞阈值可能不同。关于黑洞的具体说明，请参见#unique_9。

操作步骤

1. 登录云盾DDoS防护产品控制台。
2. 在**资产中心**页面上方选择资产所在地域。
3. 单击对应页签，选择要操作的云产品类型：**ECS**、**SLB**、**EIP（含NAT）**、**其他**。
4. 在实例列表中定位到要操作的实例，单击其**IP**。

   如果实例过多，建议您使用**实例ID**、**实例名称**或**实例IP**搜索目标实例。



5. 在**实例详情**侧边页，通过事件列表查看历史黑洞事件（**事件**为**黑洞**）的信息，并在流量图中查看黑洞事件发生时的攻击流量。

   黑洞事件中记录了黑洞的**开始时间**和**结束时间**。

   > **说明：**
   > 如果当前资产中未发生过黑洞/清洗事件，则事件列表中将无记录展示。

6. （可选）单击目标事件操作列下的**证据下载**，您可以下载针对该攻击事件的抓包文件作为证据，用于向网监报案。

3.6 连接已被黑洞的服务器

本文介绍了在服务器进入黑洞时，通过阿里云同地域ECS服务器连接被黑洞服务器的方法。

背景信息

假如您的服务器遭受大流量攻击而进入黑洞，则所有来自外部的流量都会被丢弃，但是阿里云内部与该服务器同地域的云产品仍然能够正常连通该服务器。

因此，在您的服务器进入黑洞后，您可以使用阿里云内部的ECS云服务器连接该服务器。

操作步骤

1. 登录与被黑洞服务器同地域且可正常访问的ECS云服务器。

   说明:

   该ECS云服务器需要与被黑洞的服务器可连通，属于同一个专有网络VPC环境，且连接不被安全组的相关访问控制规则所阻断。更多信息，请参见#unique_18。

2. 在ECS云服务器中，通过工具或命令连接黑洞状态的服务器。

   通过ECS云服务器成功连接该服务器后，您可以将处于黑洞状态的服务器上的文件转移至已登录的ECS云服务器，您也可以通过这种方式变更该服务器上的配置文件等。

3.7 DDoS基础防护黑洞阈值

云盾DDoS基础防护各个地域默认初始黑洞触发阈值如下表所示（单位：bps）。

说明:

- 此黑洞默认阈值适用于阿里云ECS、SLB、EIP、WAF实例，且适用于IPv4和IPv6环境的防护，但部分地区暂不支持IPv6防护。在下表中的支持IPv6列，√表示该地区支持IPv6防护，防护阈值同时适用于IPv4和IPv6；×表示该地区暂不支持IPv6防护，防护阈值仅适用于IPv4。
- ECS、SLB、EIP实例的实际黑洞阈值还与您所购买的实例规格及带宽有关，具体以云盾DDoS防护产品控制台的**资产中心**页面显示为准。更多信息，请参见资产中心。
- WAF实例IP的黑洞阈值与SLB、EIP实例一致。

地区	支持IPv4	支持IPv6	1 核 CPU 规格 ECS 实例	2 核 CPU 规格 ECS 实例	4 核以上 CPU 规格 ECS 实例	SLB、EIP（含NAT网关公网IP）、WAF实例
华东1（杭州）	√	√	500 M	1 G	5 G	5 G
华东2（上海）	√	√	500 M	1 G	2 G	2 G
华北1（青岛）	√	×	500 M	1 G	5 G	5 G
华北2（北京）	√	√	500 M	1 G	2 G	2 G
华北3（张家口）	√	√	500 M	1 G	2 G	2 G
华北5（呼和浩特）	√	√	500 M	1 G	2 G	2 G
华南1（深圳）	√	√	500 M	1 G	2 G	2 G
华南2（河源）	√	√	500 M	1 G	2 G	2 G

地区	支持IPv4	支持IPv6	1 核 CPU 规格 ECS 实例	2 核 CPU 规格 ECS 实例	4 核以上 CPU 规格 ECS 实例	SLB、EIP（含NAT网关公网IP）、WAF实例
西南1（成都）	√	×	500 M	1 G	2 G	2 G
中国（香港）	√	√	500 M	500 M	500 M	500 M
新加坡	√	×	500 M	500 M	500 M	500 M
澳大利亚（悉尼）	√	×	500 M	500 M	500 M	500 M
马来西亚（吉隆坡）	√	×	500 M	500 M	500 M	500 M
印度尼西亚（雅加达）	√	×	500 M	500 M	500 M	500 M
日本（东京）	√	×	500 M	500 M	500 M	500 M
德国（法兰克福）	√	×	500 M	500 M	500 M	500 M
英国（伦敦）	√	×	500 M	500 M	500 M	500 M
美国（硅谷）	√	×	500 M	1 G	2 G	2 G
美国（弗吉尼亚）	√	×	500 M	500 M	500 M	500 M
印度（孟买）	√	×	500 M	1 G	1 G	1 G
阿联酋（迪拜）	√	×	500 M	500 M	500 M	500 M

默认的黑洞时长是2.5个小时，黑洞期间不支持解封。 实际黑洞时长视攻击情况而定，从30分钟到24小时不等。黑洞时长主要受以下因素影响：

- 攻击是否持续。如果攻击一直持续，黑洞时间会延长，黑洞时间从延长时刻开始重新计算。
- 攻击是否频繁。如果某用户是首次被攻击，黑洞时间会自动缩短；反之，频繁被攻击的用户被持续攻击的概率较大，黑洞时间会自动延长。

说明：

针对个别黑洞过于频繁的用户，阿里云保留延长黑洞时长和降低黑洞阈值的权利，具体黑洞阈值和黑洞时长以控制台显示为准。

3.8 云虚拟主机DDoS防护黑洞阈值

云独享虚拟主机默认黑洞触发阈值如下（单位：bps）。

说明:

对于共享虚拟主机，由于多台共享虚拟主机会共享同一个IP，因此其黑洞阈值无法确定，但必定低于同地域独享虚拟主机的黑洞阈值。而且，如果有一台共享虚拟主机遭受大量DDoS攻击并触发黑洞机制，那么与它共享IP的其他虚拟主机都将无法访问。如果您的业务对安全性和稳定性有一定要求，建议购买独享虚拟主机或者ECS云服务器。

地区	独享虚拟主机
华东 1（杭州）	5G
华北 1（青岛）	5G
华南 1（深圳）	2G
华北 2（北京）	2G
华东 2（上海）	2G
中国香港	500M
美国	500M
新加坡	500M

默认的黑洞时长是2.5小时，黑洞期间不支持解封。实际黑洞时长视攻击情况而定，从30分钟到24小时不等。黑洞时长主要受以下因素影响：

- 攻击是否持续。如果攻击一直持续，黑洞时间会延长，黑洞时间从延长时刻开始重新计算。
- 攻击是否频繁，如果某用户是首次被攻击，黑洞时间会自动缩短；反之，频繁被攻击的用户被持续攻击的概率较大，黑洞时间会自动延长。

说明:

针对个别黑洞过于频繁的用户，阿里云保留延长黑洞时长和降低黑洞阈值的权利，具体黑洞阈值和黑洞时长以控制台显示为准。

如果您想获得更高的增量DDoS防护能力，购买DDoS高防IP服务，获得每天最高300G的独享DDos防护服务。

3.9 云产品规格与清洗阈值

阿里云免费为您提供基础DDoS防护能力，帮助您缓解面向公网开放的云产品所遭受的DDoS攻击。当云产品公网IP的网络流量超过设置的清洗阈值时，DDoS基础防护服务将自动对该IP的流量进行清洗，尽可能地保障您的正常业务免受DDoS攻击影响。

关于流量清洗的详细说明，请参见流量清洗、黑洞与阈值。

其中，各云产品所支持设置的最大清洗阈值取决于各云产品实例的规格。在您创建或变更云服务器ECS、负载均衡SLB、NAT网关实例时，系统将自动计算当前实例规格所对应的最大清洗阈值。

说明：
各云产品实例的实际黑洞阈值将综合最大清洗阈值、安全信誉等因素进行计算。

- 关于云服务器ECS实例的最大清洗阈值的具体计算方式，请参见云服务器ECS DDoS基础防护。
- 关于负载均衡SLB实例的最大清洗阈值的具体计算方式，请参见负载均衡SLB DDoS基础防护。
- 关于NAT网关实例的最大清洗阈值的具体计算方式，请参见NAT网关 DDoS基础防护。

说明：
弹性公网IP（EIP）的最大清洗阈值的计算方式与NAT网关相同。

3.10 云服务器压力测试指引

云盾DDoS基础防护服务默认为云服务器提供DDoS攻击防御能力。默认情况下，当云服务器的网络流量超过每秒180M流量、每秒30,000个报文数、每秒480个HTTP请求中的任何一项（根据实际实例规格可能有所不同），云盾将自动启动DDoS防御服务对流量进行清洗。

因此，您在对云服务器进行压力测试前，需要在云盾DDoS基础防护管理控制台调整目标云服务器实例的DDoS防护阈值。具体操作方式，参考设置清洗阈值。

说明：
强烈建议您每分钟的压力测试增长速度不要超过100倍，否则仍可能触发流量清洗。

3.11 通过设置白名单解决因误判IP被拦截问题

若您发现部分正常业务或者 IP 无法访问，有可能是因为攻击误判导致 IP 被拦截,。

背景信息

例如，您的网络环境为 NAT 环境（即局域网内相关主机共享公网 IP 上网），由于局域网内部分主机因中病毒或被入侵后对外攻击某 ECS 服务器，被云盾识别后，会对相应的 NAT 共享公网 IP 进行拦截，从而导致无法访问。

您可以通过设置白名单放行因误判导致的 IP 被拦截问题。

操作步骤

1. 登录云盾安全管控平台管理控制台。

   说明:
   您也可以在登录阿里云控制台后，将鼠标移至右上角的账户图标打开用户菜单，并单击**安全管控**，进入云盾安全管控平台管理控制台。

2. 定位到**白名单管理** > **访问白名单**页面，单击**添加**。
3. 选择对象类型，输入源IP（非当前云账户名下的IP），在左侧列表中选择当前云账号名下的对象IP（例如ECS云服务器公网IP），单击右箭头按钮，将选中的IP加入右侧待添加列表，单击**确定**。即将所输入的访问源IP加入所添加的对象IP的访问白名单，所有来自该源IP对于您云账户名下的目标IP的访问都将不受任何安全管控限制。

   说明:

如果您想要放行所有对该对象IP的访问，在**源IP**框中输入0.0.0.0即可放行所有IP对该目标IP的访问。

来自访问白名单中的源IP对目标主机资产的访问将不受任何安全管控限制，即使访问可能是有风险的也不会进行任何安全管控限制。因此，请务必谨慎添加访问白名单。

说明:

IP添加至访问白名单后，将在10分钟内正式生效。

关于访问白名单的更多操作说明，参考访问白名单。

3.12 资产中心

DDoS防护资产中心向您展示阿里云账号下已开通资产（包括ECS、SLB、EIP等）的DDoS防护状态，帮助您快速了解资产的DDoS安全风险，并支持为指定资产提升DDoS防护能力。

操作步骤

1. 登录云盾DDoS防护产品控制台。

2. 在**资产中心**页面上方选择资产所在地域。
3. 单击对应页签，选择要操作的云产品类型：**ECS**、**SLB**、**EIP（含NAT）**、**其他**。
4. 在资产列表查看资产的DDoS防护状态。

   资产中心页面展示了当前地域下所有资产的DDoS防护信息，具体包括**状态**、**防护能力**、**清洗阈值**。

   - **状态**表示实例的DDoS安全状态，分为**正常**、**清洗中**、**黑洞中**。
     - 如果实例状态为清洗中，您可以手动取消流量清洗。更多信息，请参见取消流量清洗。
     - 如果实例状态为黑洞中，您可以查看黑洞事件记录。更多信息，请参见查看IP进入黑洞的时间和原因。
   - **防护能力**表示实例的DDoS攻击防护能力，即可以防御的最大攻击带宽。如果攻击带宽超过了当前实例的防护能力，则实例将会进入黑洞。您可以参照步骤5为指定实例提升DDoS防护能力。
   - **清洗阈值**表示触发流量清洗的最小访问带宽，体现在流量（Mbps）和报文数量（PPS）。更多信息，请参见设置清洗阈值。
5. 为指定资产提升DDoS防护能力。
   - 添加DDoS原生防护

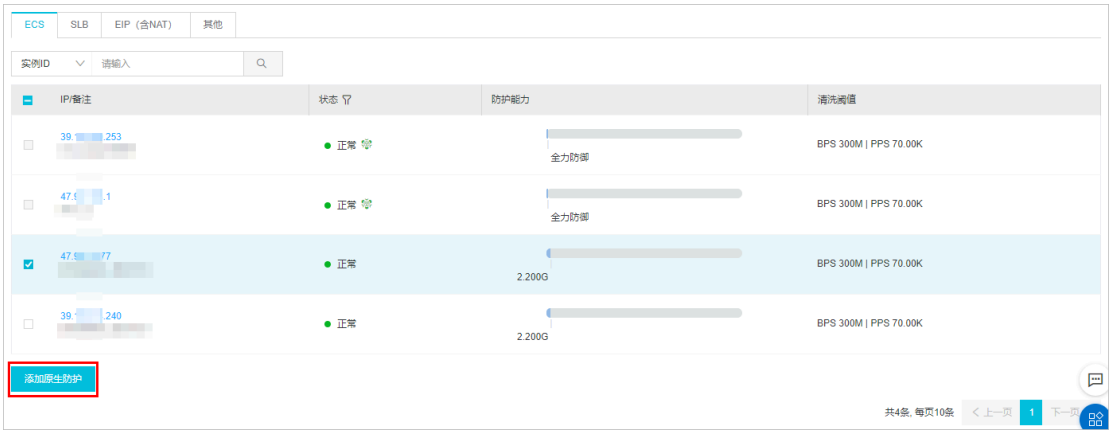
     如果您在当前地域下已开通付费版原生防护实例，则您可以参照以下步骤为指定资产开启原生防护。

     DDoS原生防护（企业版）为您提供账号级、全资产、全业务的DDoS防护，缓解企业在云上面临的DDoS攻击风险，降低DDoS可能导致的业务中断风险。针对企业提供费用可控、无需改变

业务架构、无延迟增加、支持大型业务的防护。更多信息，请参见什么是DDoS原生防护（防护包）。

为不同类型资产（ECS、SLB、EIP）开启原生防护的操作基本类似，以下以ECS为例介绍为资产开启原生防护的操作步骤，其它类型资产可作参考。

a. 在ECS实例列表中勾选要操作的实例，并单击列表下方的**添加原生防护**。



b. 在**DDoS原生防护列表**中，选择要应用的原生防护实例，单击其操作列下的**添加**。

c. 在**确认**对话框中，单击**确定**。

成功为指定资产开启DDoS原生防护。

- 开通DDoS高防服务

如果您的业务面临高风险的DDoS攻击，例如发生频率高、攻击流量大、业务影响严重等，建议您为资产开通DDoS高防服务。

DDoS高防服务采用中国大陆地域独有的T级八线BGP带宽资源，可以帮助您防御超大流量DDoS攻击。更多信息，请参见#unique_10。

您可以在左侧导航栏**DDoS高防**目录下单击**DDoS高防（新BGP）**或者**DDoS高防（国际）**，直达对应的产品控制台。

- DDoS高防（新BGP）适用于部署在中国大陆地域的业务。
- DDoS高防（国际）适用于部署在中国大陆地域以外的业务。

如果您的业务面临高风险的DDoS攻击，例如发生频率高、攻击流量大、业务影响严重等，建议您为资产开通DDoS高防服务。

DDoS高防服务采用中国大陆地域独有的T级八线BGP带宽资源，可以帮助您防御超大流量DDoS攻击。更多信息，请参见#unique_10。

4 原生防护相关协议

4.1 安全信誉防护联盟

为了给您带来更好的安全防护体验，并且提升安全防护能力，阿里云开展安全信誉防护联盟计划。免费加入该计划后，您将可以根据安全信誉评估结果，获得阿里云提供的动态的DDoS攻击防护能力。

目前，安全信誉防护联盟全量开放，默认所有阿里云用户自动加入安全信誉防护联盟。阿里云根据当前DDoS防护机房的水位、可用资源和资产遭受的历史攻击，以及账号安全信誉等因素，在免费的DDoS基础防护能力以外，为您的资产动态分配额外的弹性防护能力。

服务条款

1 您理解并确认，您不应利用基于加入联盟计划而将阿里云提供给您的安全防护能力从事如下行为：

1.1 为他人提供有偿或无偿安全防护的业务；

1.2 进行任何非法业务、进行任何不符合阿里云在阿里云官网（www.aliyun.com）公布的使用目的或流程的行为、或进行任何经阿里云自身判断不符合安全防护能力使用目的行为；

1.3 进行上传、下载或传播如下信息的行为或为他人上传、下载或传播该等信息提供便利：

1.3.1 违反国家规定的政治宣传和/或新闻；

1.3.2 涉及国家秘密和/或安全；

1.3.3 封建迷信和/或淫秽、色情和/或教唆犯罪；

1.3.4 博彩有奖、赌博游戏、“私服”、“外挂”等非法互联网出版活动；

1.3.5 违反国家民族和宗教政策；

1.3.6 妨碍互联网运行安全；

1.3.7 侵害他人合法权益和/或其他有损于社会秩序、社会治安、公共道德的活动；

1.3.8 其他违反法律法规、部门规章或国家政策的内容。

1.4 修改、翻译、改编、出租、转许可、在信息网络上传播或转让阿里云提供的软件/服务，也不得逆向工程、反编译或试图以其他方式发现阿里云提供的软件的源代码；

1.5 进行任何破坏或试图破坏网络安全的行为（包括但不限于钓鱼，黑客，网络诈骗，网站或空间中含有或涉嫌散播：病毒、木马、恶意代码，及通过虚拟服务器对其他网站、服务器进行涉嫌攻击行为如扫描、嗅探、ARP欺骗、DDoS等）；

1.6 不进行任何改变或试图改变阿里云提供的系统配置或破坏系统安全的行为；

1.7 不利用阿里云提供的服务/能力从事损害阿里云、阿里云的关联公司或阿里巴巴集团内包括但不限于阿里巴巴、淘宝、支付宝、阿里妈妈、阿里金融等（以下统称为阿里巴巴公司）各公司、网站合法权益之行为，前述损害阿里巴巴公司、网站合法权益的行为包括但不限于违反阿里巴巴公司公布的任何服务协议/条款、管理规范、交易规则等规范内容、破坏或试图破坏阿里巴巴公司公平交易环境或正常交易秩序等；

1.8 不从事其他违法、违规或违反本《安全信息防护联盟规则》的行为；

1.9 您理解阿里云同意您加入计划的前提，是基于您做出的前述承诺，如您违反您的前述承诺，阿里云有权终止向您提供基于本联盟而提供的服务/能力，同时有权经通知您，终止您的联盟会员身份。

2 您理解并确认，阿里云有权根据自身的业务计划或联盟运营情况等因素，随时终止本联盟计划而不负任何责任，在计划终止前，阿里云将提前通知您。计划终止时，您基于加入联盟计划而获得的能力/服务将一并终止。

3 您理解并确认，您已阅读《联盟计划下安全防护的工作机制》以及本《安全信誉联盟规则》并知悉您加入该计划后将会产生的结果，您加入该计划是出于您的自愿以及经过独立审慎的判断，因此，您对自己加入本联盟的行为及其产生的结果负责。

4 阿里云和您都应对您是否加入该联盟计划的情况进行保密，除非该信息已进入共有领域或阿里云依据双方的另行约定、法律法规的规定、以及相关权力机关的要求、命令、判决披露。同时您需对您安全信誉分及在此基础上生成的黑洞触发阈值及相关安全信誉信息保密，以防止该信息泄露后，引起黑客针对性攻击等不利后果的发生。

5 阿里云可能会定期或不定期的对于联盟计划下的安全防护机制进行优化或变更，阿里云将经提前通知您后向您提供最新版本的服务/或依据最新的工作体制向您提供服务/能力，如您不同意经优化后的安全防护机制，你可申请退出联盟计划并终止使用阿里云向您提供的服务。

6 您理解并确认，您加入联盟计划所获得的安全防护能力，是联盟成员共享资源池，阿里云将尽力提供给您根据您的信誉评分而获得的安全防护带宽，但在联盟会员遭遇集体性的攻击或其他等恶意攻击事件，共享资源池的带宽资源耗尽时，阿里云将会降低给您的安全防护带宽但（应不低于原机房默认阈值）。

7 免责与责任限制：您加入联盟后，获得的阿里云提供的安全防护是阿里云采取的一种技术措施，您理解并确认，阿里云按照《安全信誉防护联盟计划》执行上述技术措施，即视为提供了无瑕疵的安全防护，在阿里云无故意或重大过失的情况下，阿里云不对安全防护的结果承担责任。

8 如因您的网站遭遇计算机病毒、网络入侵和攻击破坏（包括但不限于DDoS）等危害网络安全事项或行为（以下统称该等行为），如果超过服务说明中防护范围，将会造成网站或服务在一定时间内不可被最终用户访问（以下统称“服务不可用”）。您理解并确认，该类服务不可用为阿里云履行安全防护服务的正常履行行为，并将不视为阿里云对相关服务的违约；如该行为给阿里云带来危害，或

影响阿里云与国际互联网或者阿里云与特定网络、服务器及阿里云内部的通畅联系，阿里云将保留暂停或终止按照联盟工作机制向您提供安全防护服务的权利（但阿里云暂停或终止时，将及时通知您），而无须承担任何义务和责任。

9 阿里云官网上公布的相关规则、规范和流程是本规则的完整组成部分，阿里云有权利随时对上述规则、规范和流程予以修改，并有权利在通知您后要求您符合最新修订的内容。