网络检测与响应 NDR

用户指南

文档版本 01

发布日期 2025-08-27

华为云计算技术有限公司

商标声明


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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 通过 IAM 授予使用 NDR 的权限

1.1 创建用户并授权使用 NDR

如果您需要对您所拥有的NDR进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称IAM），通过IAM，您可以：

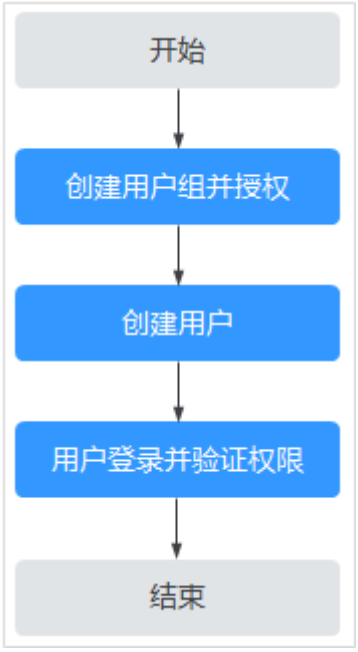
- 根据企业的业务组织，在您的账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用NDR资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将NDR资源委托给更专业、高效的其他账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用NDR服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**图1-1**所示。

示例流程

图 1-1 给用户授权服务权限流程



1. 创建用户组并授权。

   在IAM控制台创建用户组，在“操作”列下选择“授权”，并授予NDR服务的管理员权限“NDR FullAccess”。

2. 创建用户并加入用户组。

   在IAM控制台创建用户，在“操作”列下选择“授权”，并将其加入1中创建的用户组。

3. 用户登录并验证权限。

   新创建的用户登录控制台，切换至授权区域，验证权限：

   单击页面左上方的 ☰，选择“安全 > 网络响应与检测 NDR”，单击“开通服务”，如果操作成功，表示“NDR FullAccess”已生效。

1.2 自定义策略

如果系统预置的NDR权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参见**权限及授权项**。

目前支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

NDR 自定义策略样例

- 示例1：授权用户查询NDR拦截日志的权限

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ndr:system:listBlockLog"
            ]
        }
    ]
}
```

- 示例2：授权用户开通服务的权限

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ndr:system:createSubscription"
            ]
        }
    ]
}
```

- 示例3：授权用户安装插件和创建端口组的权限

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ndr:hosts:install",
                "ndr:portGroup:create"
            ]
        }
    ]
}
```

1.3 权限及授权项

如果您需要对您所拥有的NDR进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），如果账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用NDR的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。

- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

类别	权限	授权项
只读权限	以PCAP格式导出载荷内容文件	ndr:system:exportLogPacket
	查询当前特别关注	ndr:system:listLabelSpecialAttentionIp
	查询检测策略	ndr:detectionStrategies:list
	配额校验	ndr:system:listQuota
	查询拦截日志	ndr:system:listBlockLog
	查询IP组	ndr:ipGroup:list
	查询关联IP组列表	ndr:system:listAttackerSet
	查询威胁情报信息	ndr:system:listThreatIntelligence
	查询ips配置	ndr:system:getIpsConfig
	查询单个关联IP组详情	ndr:system:getAttackerSet
	查询主机插件状态	ndr:hosts:list
	查询攻击者信息标题	ndr:system:getAttackerProfileTitle
	查询安全分析报告响应总览数据	ndr:system:getReportResponse
	查询安全分析报告总体数据	ndr:system:getReportOverview
	获取攻击日志的报表信息	ndr:system:getStatisticsAttackTime
	查看拦截规则详情	ndr:blockRule:get
	下载拦截规则模板	ndr:blockRule:getTemplate
	获取所有的告警信息	ndr:system:listAlarm
	查询服务开通状态	ndr:system:getSubscription
	导出攻击日志	ndr:system:exportAttackLog
	导出拦截规则	ndr:blockRule:export
	查询租户流量	ndr:system:getStatisticsFlow
	查询攻击关系图	ndr:system:getAttackerProfileDiagram
	查询租户攻击信息	ndr:system:getStatisticsAttack
	查询EIP列表	ndr:eip:list
	获取Attack矩阵	ndr:system:getattckMatrix
	查询安全分析报告检测总览数据	ndr:system:getReportDetection

类别	权限	授权项
	查询流量日志	ndr:system:listflowLog
	查询安全事件	ndr:system:listEvent
	出入口的流量统计	ndr:system:getStatisticsFlowTime
	查询用户配置	ndr:system:getUserConfiguration
	查询攻击日志	ndr:system:listAttackLog
	查询IP配置设置	ndr:system:geAttackertLabel
	查询攻击者信息图表	ndr:system:listAttackerProfileChart
	导出流量日志	ndr:system:exportFlowLog
	查询拦截规则列表	ndr:blockRule:list
	查询攻击者时间线	ndr:system:getAttackerProfileTimeline
	查询攻击者列表	ndr:system:listAttackerProfileAttacker
	导出拦截日志	ndr:system:exportBlockLog
	查询端口组	ndr:portGroup:list
	任务规则描述列表	ndr:system:listipsRule
写权限	新增关联IP组设置	ndr:system:createAttackerSet
	删除检测策略	ndr:detectionStrategies:delete
	删除关联IP组中的成员	ndr:system:deleteAttackerSetMember
	修改用户配置	ndr:system:putUserConfiguration
	删除端口组	ndr:portGroup:delete
	创建IP组	ndr:ipGroup:create
	EIP批量取消关联规则	ndr:eip:disassociateRule
	修改安全事件	ndr:system:putEvent
	删除关联IP组	ndr:system:deleteAttackerSet
	删除IP组	ndr:ipGroup:delete
	规则批量关联EIP	ndr:blockRule:associateEip
	新增关联IP组中的成员	ndr:system:createAttackerSetMember
	修改告警信息	ndr:system:putAlarm
	批量启用关联IP	ndr:system:enableAttackerSetMember
	修改端口组	ndr:portGroup:put

类别	权限	授权项
	删除特别关注	ndr:system:deleteLabelSpecialAttentionIp
	批量禁用关联IP	ndr:system:disableAttackerSetMember
	导入拦截规则	ndr:blockRule:import
	EIP批量关联规则	ndr:eip:associateRule
	批量删除特别关注	ndr:system:batchDeleteLabelSpecialAttentionIp
	更新检测策略	ndr:detectionStrategies:pu
	批量启用EIP防护	ndr:eip:enableProtection
	开通服务	ndr:system:createSubscription
	修改IP组	ndr:ipGroup:put
	停用检测策略	ndr:detectionStrategies:disable
	批量删除关联IP组中的成员	ndr:system:batchDeleteAttackerSetMember
	安装插件	ndr:hosts:install
	启用检测策略	ndr:detectionStrategies:enable
	更新插件	ndr:hosts:upgrade
	规则批量取消关联EIP	ndr:blockRule:disassociateEip
	创建端口组	ndr:portGroup:create
	同步EIP	ndr:eip:synchronization
	手动执行资源同步	ndr:system:syncResource
	修改IP配置	ndr:system:putAttackerLabel
	删除拦截规则	ndr:blockRule:delete
	批量停用EIP防护	ndr:eip:disableProtection
	新增IP配置	ndr:system:createAttackerLabel
	修改检测策略	ndr:detectionStrategies:modify
	禁用基础防御规则	ndr:system:disableIpsRule
	变更配额	ndr:system:modifyQuota
	创建拦截规则	ndr:blockRule:create
	更改ips配置	ndr:system:updateIpsConfig
	卸载插件	ndr:hosts:uninstall

类别	权限	授权项
	取消开通服务	ndr:system:deleteSubscription
	创建检测策略	ndr:detectionStrategies:create
	启用基础防御规则	ndr:system:enableIpsRule
	编辑拦截规则	ndr:blockRule:put
	修改单个关联IP组	ndr:system:putAttackerSet

2 开通服务

在使用网络检测与响应服务之前，您需要先开通服务。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在“概览”页面，单击“开通服务”。

图 2-1 开通服务

步骤4 根据实际配置服务参数。

表 2-1 参数说明

参数	说明
带宽大小（Mbit/s）	选择需要的带宽。
委托（可选）	单击“创建委托”，查看使用NDR服务需要的权限内容，如果您同意授权这些权限，单击“同意授权并创建”，如果您不同意，单击“关闭”，后续可在IAM服务中授权。
基础版插件配额	基础版插件的数量。
专业版插件配额	专业版插件的数量。

步骤5 单击“立即开通”。

----结束

3 查看概览信息

该任务指导用户查看高危级别网络攻击概况，主要展示最近一小时高危级别攻击次数和最近一小时高危级别攻击类型分布信息。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，单击“概览”，进入概览页面。

步骤4 单击下拉框，选择需要查看的范围，查看最近一小时高危级别攻击次数及类型分布。

- 全部：查看所有攻击。
- Internet流量：查看来自互联网的攻击。
- 内部流量：查看来自内部的攻击。

图 3-1 概览

----结束

4 查看流量访问详情

4.1 查看 Internet 访问详情

Internet访问指的是来自互联网的访问。通过“流量分析”页面，您可以查看特定时间内所有公网IP的Internet访问流量详情。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，单击“流量分析”，进入流量分析页面。

步骤4 单击“Internet访问”页签。

步骤5 选择时间，即可查看在指定时间段的流量详情。

图 4-1 Internet 访问

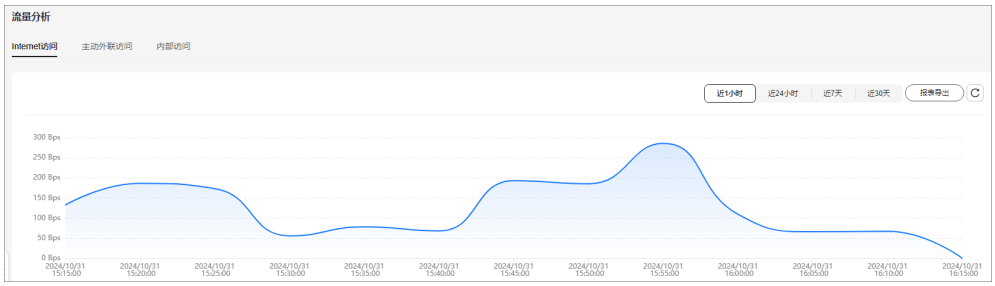


表 4-1 Internet 访问

信息	说明
Internet访问流量	指定时间段内通过Internet访问的流量详情。

说明

单击“报表导出”，可以导出当前报表。

----结束

4.2 查看主动外联访问详情

主动外联访问指的是用户云内资产对互联网的访问。通过“流量分析”页面，您可以查看特定时间内所有公网IP的主动外联访问流量详情。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，单击“流量分析”，进入流量分析页面。

步骤4 单击“主动外联访问”页签。

步骤5 选择时间，即可查看在指定时间段的流量详情。

图 4-2 主动外联访问

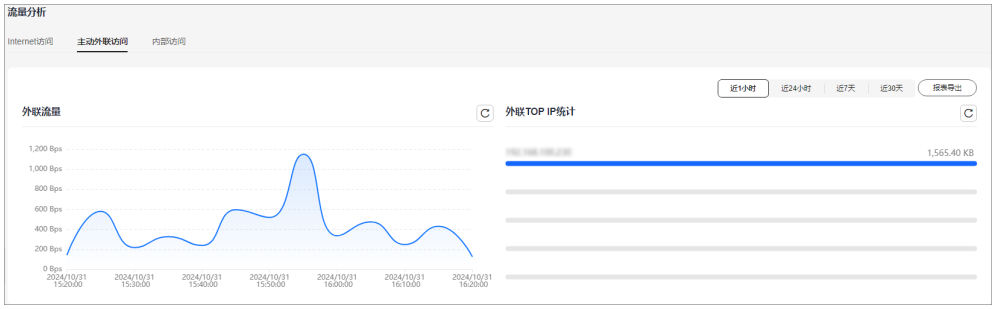


表 4-2 流量分析

信息	说明
外联流量	指定时间段内主动外联访问的流量详情。
外联TOP IP统计	指定时间段内外联访问的主要IP排行。

说明

单击“报表导出”，可以导出当前报表。

----结束

4.3 查看内部访问详情

内部访问指的是云内的访问。通过“流量分析”页面，您可以查看特定时间内所有公网IP的云内访问流量详情。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，单击“流量分析”，进入流量分析页面。

步骤4 单击“内部访问”页签。

步骤5 选择时间，即可查看在指定时间段的流量详情。

图 4-3 内部访问

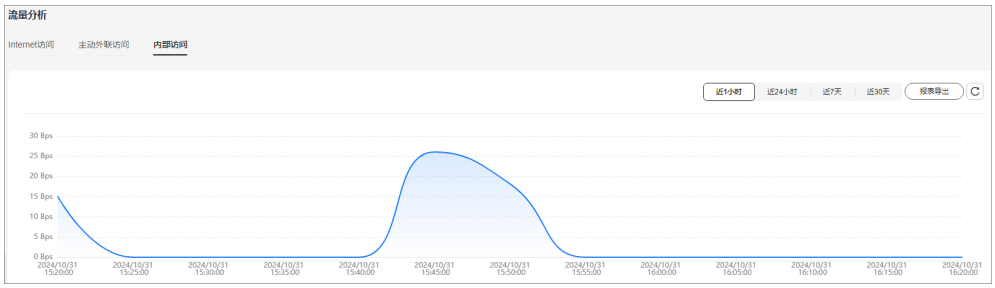


表 4-3 流量分析

信息	说明
内部流量	指定时间段，内部访问的流量详情。

说明

单击“报表导出”，可以导出当前报表。

----结束

5 查看安全分析信息

通过安全分析页面，可以查看产生告警和阻断的次数和趋势、TOP5的攻击源信息和地理分布等安全信息。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

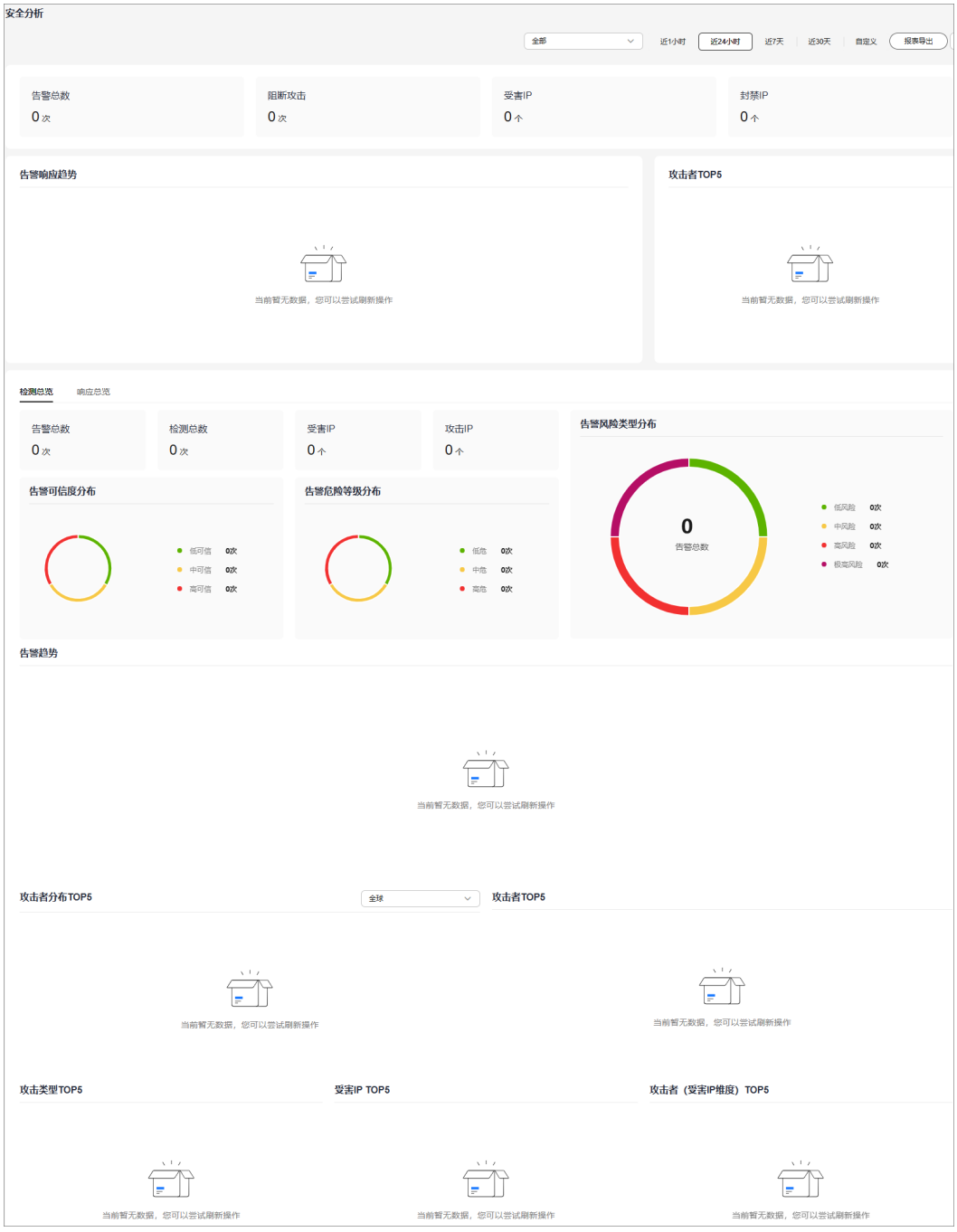
步骤3 在左侧导航树中，单击“安全分析”，进入安全分析页面。

说明

受害IP仅包含云内受害资产的IP地址。

步骤4 在“检测总览”页签，可以查看NDR检测出的安全详情。

图 5-1 检测总览



步骤5 单击“响应总览”，可以查看NDR响应的安全详情。

图 5-2 响应总览

说明

单击“报表导出”，可以导出当前报表。

----结束

6 查看攻击趋势

6.1 查看 Internet 访问的攻击趋势

Internet访问指的是来自互联网的访问。您可以通过“攻击趋势”查看Internet访问场景下，特定时间内所有公网IP的网络攻击趋势、攻击类型分布和TOP攻击类型排行。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“威胁检测 > 攻击趋势”，进入攻击趋势页面。

步骤4 单击“Internet访问”页签。

步骤5 选择时间，即可查看选定时间段的攻击趋势。

图 6-1 Internet 访问

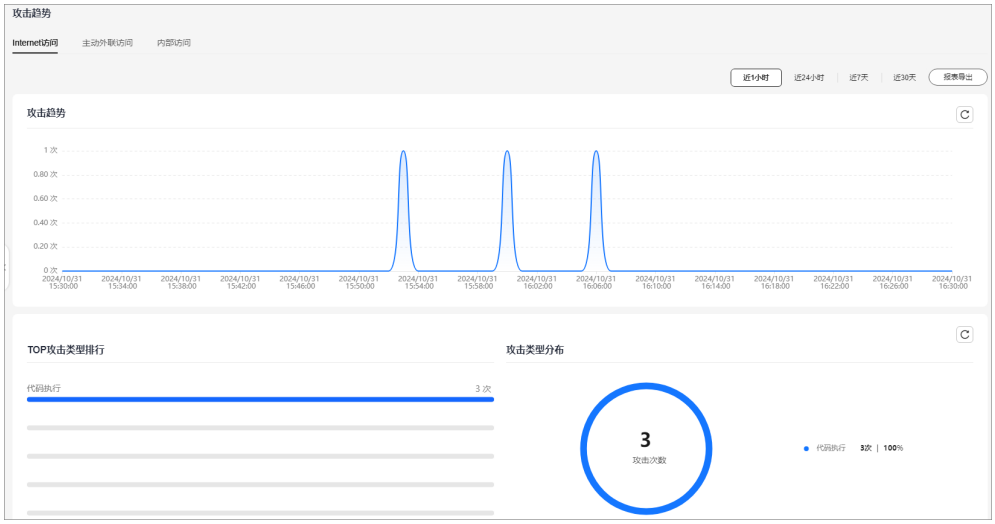


表 6-1 Internet 访问

类别	说明
攻击趋势	Internet访问场景下的攻击趋势。
TOP攻击类型排行	Internet访问场景下的主要攻击类型排行，例如：目录遍历、信息泄露、缓冲区溢出等多种攻击。
攻击类型分布	Internet访问场景下攻击类型的分布详情。

说明

单击“报表导出”，可以导出当前报表。

----结束

6.2 查看主动外联访问的攻击趋势

主动外联访问指的是用户云内资产对互联网的访问。您可以通过“攻击趋势”查看主动外联访问场景下，特定时间内所有公网IP的网络攻击趋势和外联TOP IP信息。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击 ☰，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“威胁检测 > 攻击趋势”，进入攻击趋势页面。

步骤4 单击“主动外联访问”页签。

步骤5 选择时间，即可查看选定时间段的攻击趋势。

图 6-2 主动外联访问

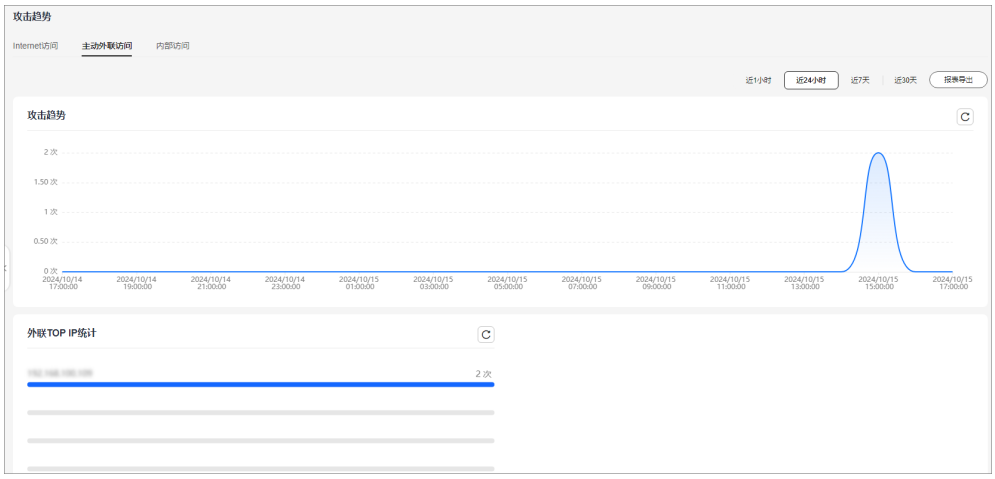


表 6-2 攻击趋势

信息	说明
攻击趋势	主动外联访问场景下的攻击趋势。
外联TOP IP统计	外联的主要IP类型排行。

说明

单击“报表导出”，可以导出当前报表。

----结束

6.3 查看内部访问的攻击趋势

内部访问指的是云内的访问。您可以通过“攻击趋势”查看内部访问场景下，特定时间内所有公网IP的攻击趋势、TOP攻击类型排行和攻击类型分布。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“威胁检测 > 攻击趋势”，进入攻击趋势页面。

步骤4 单击“内部访问”页签。

步骤5 选择时间，即可查看选定时间段的攻击趋势。

图 6-3 内部访问

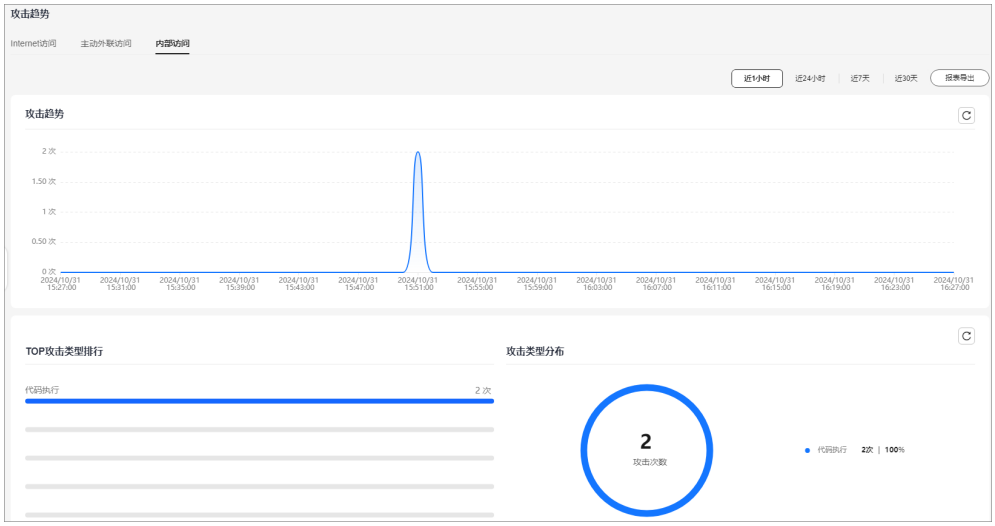


表 6-3 攻击趋势

信息	说明
攻击趋势	内部访问场景下的攻击趋势。
TOP攻击类型排行	内部访问场景下的主要攻击类型排行，例如：目录遍历、信息泄露、缓冲区溢出等多种攻击。
攻击类型分布	内部访问场景下攻击类型的分布详情。

说明

单击“报表导出”，可以导出当前报表。

----结束

7 查看 ATT&CK 矩阵

NDR支持对发现的攻击进行ATT&CK模型分类展示，您可以快速查看指定时间段内使用某一类ATT&CK技术攻击的所有日志。

操作步骤

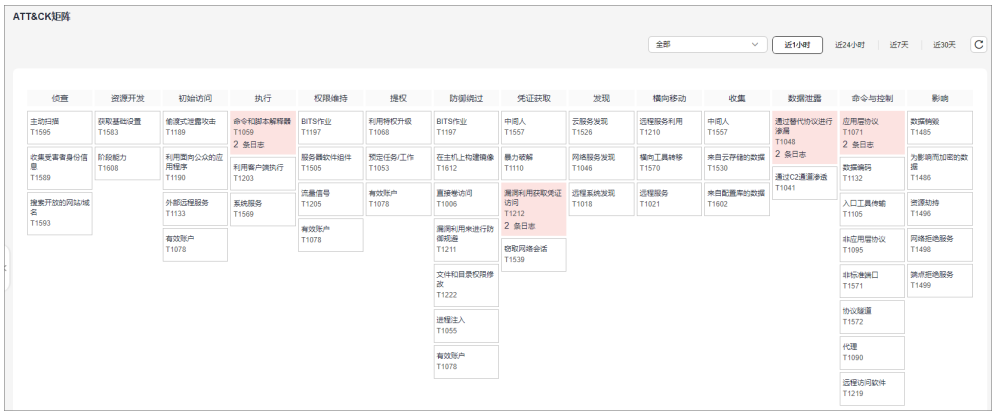
步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击 ☰，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“威胁检测 > ATT&CK矩阵”，进入“ATT&CK矩阵”页面。

步骤4 选择需要查看的时间范围，查看该时间段内攻击事件的ATT&CK技术类型。

图 7-1 ATT&CK 矩阵



步骤5 单击需要查看的ATT&CK类型，即可查看到该ATT&CK攻击分类下的所有日志。

----结束

8 查看日志

8.1 查看攻击事件日志

NDR将识别出的网络攻击记录在攻击事件日志，您可以通过查看攻击事件日志，定位攻击源、被攻击目标等信息。

操作步骤

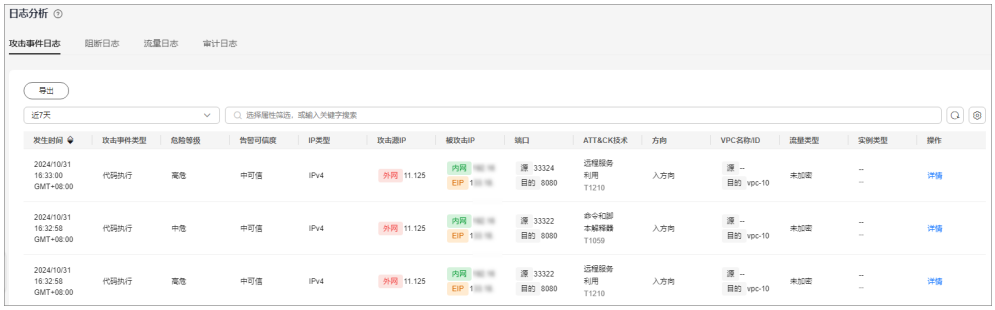
步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“威胁检测 > 日志分析”，进入日志页面。

步骤4 单击“攻击事件日志”页签，进入攻击事件日志列表。

图 8-1 攻击事件日志



- 在搜索框中，可筛选需要查看的日志，仅支持精确搜索。
- 单击“导出”，可导出日志，最大支持10000条。
- 单击，可选择日志显示内容，当前支持的日志信息如表8-1所示。

表 8-1 攻击事件分析

类别	说明
发生时间	攻击日志发生的时间，支持重新排序。
攻击事件类型	攻击事件的类型。
危险等级	该攻击日志的危险级别，支持筛选。
告警可信度	该攻击日志的告警可信的程度，支持筛选。
规则ID	基础防御规则的ID。
命中规则名称	基础防御规则的名称。
IP类型	支持IPv4和IPv6。
攻击源IP	作为攻击源头的IP信息。
被攻击IP	作为被攻击方的IP信息。
端口	攻击源端口和被攻击端口。
ATT&CK技术	检测出来网络攻击使用的技术，例如“通过替代协议进行渗漏”。
方向	流量的方向： – 入方向：外部IP指向云内资产IP的流量。 – 出方向：云内资产IP指向外部IP的流量。 – 内部流量：云内资产IP之间的流量。 – POD-DMZ流量：云内不同网络区域之间的流量。 – 未知：未能识别出来的流量。
传输协议	该攻击日志的传输层协议。
应用协议	该攻击日志的应用层协议。
VPC名称/ID	该日志所属的VPC名称和ID。
流量类型	加密流量和非加密流量。
实例类型	主机的实例类型。
攻击结果	本次攻击的结果。

----结束

查看攻击事件日志详情

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击 ☰，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“威胁检测 > 日志分析”，进入日志页面。

步骤4 单击“攻击事件日志”页签，进入攻击事件日志列表。

步骤5 在需要查看的攻击事件日志所在行的“操作”列，单击“详情”，即可查看日志的详细信息，日志参数如表8-2所示。

表 8-2 详情参数

类别	参数	说明
基本信息	发生时间	攻击日志发生的时间，支持重新排序。
	攻击事件类型	攻击事件的类型。
	危险等级	该攻击日志的危险级别，支持筛选。 ● 高危 ● 中危 ● 低危
	告警可信度	该攻击日志的告警可信的程度，支持筛选。 ● 高可信 ● 中可信 ● 低可信
	规则ID	本次攻击命中的规则ID。
	命中规则名称	本次攻击命中的规则全称。
	IP类型	IP的类型。
	攻击源IP	作为攻击源头的IP信息。
	被攻击IP	作为被攻击方的IP信息。
	方向	流量的方向。 ● 入方向：外部IP指向云内资产IP的流量。 ● 出方向：云内资产IP指向外部IP的流量。 ● 内部流量：云内资产IP之间的流量。 ● POD-DMZ流量：云内不同网络区域之间的流量。 ● 未知：未能识别出来的流量。
	传输协议	攻击事件使用的传输层协议。
	应用协议	攻击事件使用的应用层协议。
	建议动作	NDR服务对该攻击事件的操作。 ● 阻断：阻断访问。 ● 放行：允许访问。
	流量类型	加密流量和非加密流量。
	攻击结果	本次攻击的结果。

类别	参数	说明
	攻击源标签	攻击源的资源标签。
	被攻击标签	被攻击对象的资源标签。
	攻击源端口	作为攻击源头的端口信息。
	被攻击端口	作为被攻击方的端口信息。
	CVE漏洞披露	该攻击所属的现有CVE漏洞披露信息。
	高频率爆破扫描类型	本次攻击的爆破扫描类型。 ● 一对多：一个攻击源IP攻击了多个目的IP。 ● 多对一：多个攻击源IP攻击了一个目的IP。 ● 一对一：一个攻击源IP攻击了一个目的IP。
	ATT&CK技术	使用的ATT&CK技术名称。
	ATT&CK矩阵	ATT&CK技术ID。
	源VPC名称	攻击源VPC的名称。
	源VPC ID	攻击源VPC的ID。
	目的VPC名称	被攻击的VPC名称。
	目的VPC ID	被攻击的VPC ID。
	实例ID	主机的实例ID。
	实例类型	主机的实例类型。
	响应码	HTTP响应码。
	代理	代理信息。
	爆破扫描攻击IP数	一分钟内高频率爆破攻击的攻击源IP数。
	爆破扫描被攻击IP数	一分钟内被高频率爆破攻击的IP数。
	爆破扫描被攻击端口数	一分钟内被高频率爆破攻击的端口数。
	攻击次数	一分钟内高频率爆破攻击的次数。
攻击payload	五元组信息	攻击事件的五元组信息，包括“攻击源IP”、“攻击源端口”、“被攻击IP”、“被攻击端口”、“传输协议”等。
	载荷内容	经Base64编码显示后的攻击访问的请求体内容。
威胁情报	攻击IP地理位置信息	攻击源IP所属的地理位置信息，包括“攻击源IP”、“国家”等信息。

----结束

下载 PCAP 报文

步骤1 在目标攻击事件日志所在行，单击“详情”，进入攻击事件日志详情页面。

步骤2 单击“攻击payload”页签。

步骤3 在“pcap原始文件”后单击“导出”。

----结束

8.2 查看阻断日志

NDR将阻断的访问请求记录在阻断日志，您可以通过查看阻断日志，获取所有被阻断访问的源IP、传输协议等信息。

操作步骤

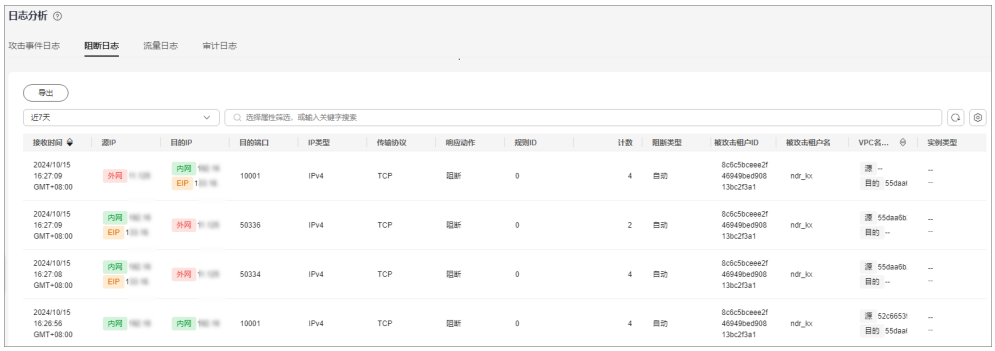
步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“威胁检测 > 日志分析”，进入日志页面。

步骤4 单击“阻断日志”页签，进入阻断日志列表。

图 8-2 阻断日志



- 在搜索框中，可筛选需要查看的日志，仅支持精确搜索。
- 单击“导出”，可导出日志，最大支持10000条。
- 单击，可选择日志显示内容，当前支持的日志信息如表8-3所示。

表 8-3 阻断日志

类别	说明
接收时间	阻断日志发生的时间，支持重新排序。

类别	说明
源IP	阻断日志源头IP信息。
目的IP	阻断日志目的IP信息。
目的端口	阻断日志目的端口信息。
IP类型	支持IPv4和IPv6。
传输协议	阻断日志的传输层协议。
响应动作	NDR服务对该攻击事件的操作，阻断/放行，支持筛选。
规则ID	触发阻断的阻断规则ID。
计数	三元组1秒内告警的次数。
阻断类型	• 自动：触发系统预置规则的阻断。 • 手动：触发用户所创建规则的阻断。
被攻击租户ID	被攻击租户的ID。
被攻击租户名	被攻击租户的名称。
VPC名称/ID	该日志所属的VPC名称和ID。
实例类型	主机的实例类型。

----结束

8.3 查看流量日志

NDR会对出入方向的流量进行全量检测，每一分钟生成一条流量日志。您可以通过查看流量日志，获取被检测流量的源IP、源端口、目的IP、目的端口等信息。

操作步骤

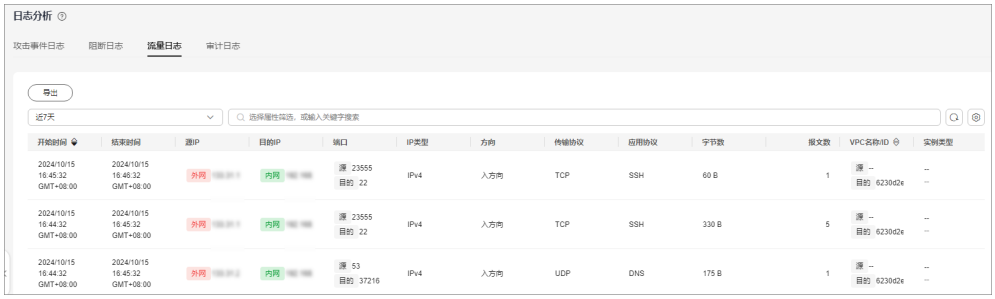
步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击 ☰，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“威胁检测 > 日志分析”，进入日志页面。

步骤4 单击“流量日志”页签，进入流量日志列表。

图 8-3 流量日志



- 在搜索框中，可筛选需要查看的日志，仅支持精确搜索。
- 单击“导出”，可导出日志，最大支持10000条。
- 单击  ，可选择日志显示内容，当前支持的日志信息如表8-4所示。

表 8-4 流量日志

类别	说明
开始时间	统计流量的开始时间，支持重新排序。
结束时间	统计流量的结束时间。
源IP	流量流出的IP信息。
目的IP	流量流入的IP信息。
端口	攻击源和被攻击的端口。
IP类型	支持IPv4和IPv6。
方向	流量的方向： ● 入方向：外部IP指向云内资产IP的流量。 ● 出方向：云内资产IP指向外部IP的流量。 ● 内部流量：云内资产IP之间的流量。 ● POD-DMZ流量：云内不同网络区域之间的流量。 ● 未知：未能识别出来的流量。
传输协议	被检测流量使用的传输层协议。
应用协议	被检测流量使用的应用层协议。
字节数	一分钟内的字节数，单位MB。
报文数	一分钟内的报文数。
VPC名称/ID	源VPC和目的VPC的名称及ID。
实例类型	实例的类型。

----结束

8.4 查看审计日志

当访问请求命中NDR内置的防御规则，系统将该信息记录到审计日志。您可以通过查看被审计日志，获取该访问请求命中的规则详情、流量方向、传输协议、应用协议等信息。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“威胁检测 > 日志分析”，进入日志页面。

步骤4 单击“审计日志”页签，进入审计日志列表。

图 8-4 审计日志

- 在搜索框中，可筛选需要查看的日志，仅支持精确搜索。
- 单击“导出”，可导出日志，最大支持10000条。
- 单击，可选择日志显示内容，当前支持的日志信息如表8-5所示。

表 8-5 审计日志参数

类别	说明
发生时间	审计日志发生的时间，支持重新排序。
危险等级	该审计日志的危险级别，支持筛选。 – 高危 – 中危 – 低危
告警可信度	该日志的告警可信的程度，支持筛选。 – 高可信 – 中可信 – 低可信
规则ID	流量检测和攻击拦截使用的系统内置规则ID。

类别	说明
命中规则名称	流量检测和攻击拦截使用的规则全称。
IP类型	支持IPv4和IPv6。
攻击源IP	作为攻击源头的IP信息。
被攻击IP	作为被攻击方的IP信息。
方向	流量的方向。 – 入方向：外部IP指向云内资产IP的流量。 – 出方向：云内资产IP指向外部IP的流量。 – 内部流量：云内资产IP之间的流量。 – POD-DMZ流量：云内不同网络区域之间的流量。 – 未知：未能识别出来的流量。
传输协议	被审计流量使用的传输层协议。
应用协议	被审计流量使用的应用层协议。
VPC名称/ID	该日志所属的VPC名称和ID。
流量类型	加密流量和非加密流量。
实例类型	主机的实例类型。
攻击结果	本次攻击的结果。

----结束

9 管理攻击者画像

9.1 查看攻击者画像

NDR支持对攻击者提供画像和溯源，可帮助用户查看攻击者地理分布、攻击源IP具体信息等。

操作步骤

步骤1 登录控制台。

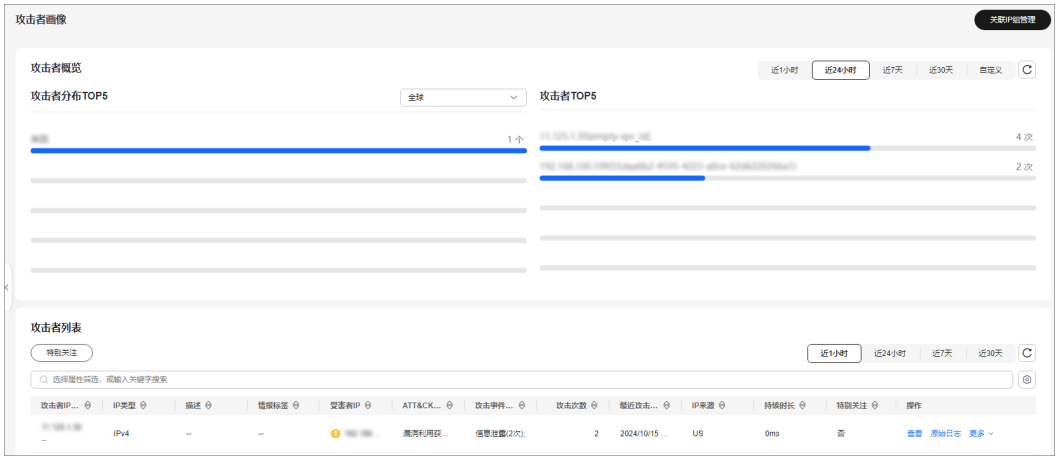
步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“威胁检测 > 攻击者画像”，进入“攻击者画像”页面。

步骤4 选择需要查看的时间范围，查看该时间段内攻击事件的攻击者概览信息。

- 攻击者分布TOP5：可以查看TOP5攻击者的地理分布图。
- 攻击者TOP5：可以查看TOP5攻击者的攻击IP。

图 9-1 攻击者概览



步骤5 在“攻击者列表”区域，可以查看指定时间范围的攻击者信息，具体参数如表9-1所示。

图 9-2 攻击者列表

表 9-1 攻击者参数

参数	说明
攻击者IP/名称	攻击源IP地址和自定义名称。
IP类型	攻击源IP的类型。
描述	描述信息。
情报标签	根据IP历史数据设置的标记信息，比如矿池、僵尸网络、VPN等。
受害者IP	被攻击的IP地址，只涉及南北向流量。
ATT&CK技术	攻击者使用的网络攻击技术。
攻击事件类型	攻击类型。
攻击次数	网络攻击的次数。
最近攻击时间	最近一次攻击的时间。
IP来源	攻击者IP的地理来源。
持续时长	攻击的持续时间。
特别关注	该攻击者是否被设置为“特别关注”。设置方法请参考**添加特别关注**。

----结束

9.2 添加特别关注

攻击者画像功能支持将检测出的攻击者IP添加到特别关注列表，添加为特别关注的IP可以通过快速筛选进行查看。

方法一：添加已有 IP 为特别关注

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击 ☰，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“威胁检测 > 攻击者画像”，进入“攻击者画像”页面。

步骤4 在目标IP所在行，选择“更多 > 添加关注”。

图 9-3 添加关注

----结束

方法二：添加指定 IP 为特别关注

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击 ☰，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“威胁检测 > 攻击者画像”，进入“攻击者画像”页面。

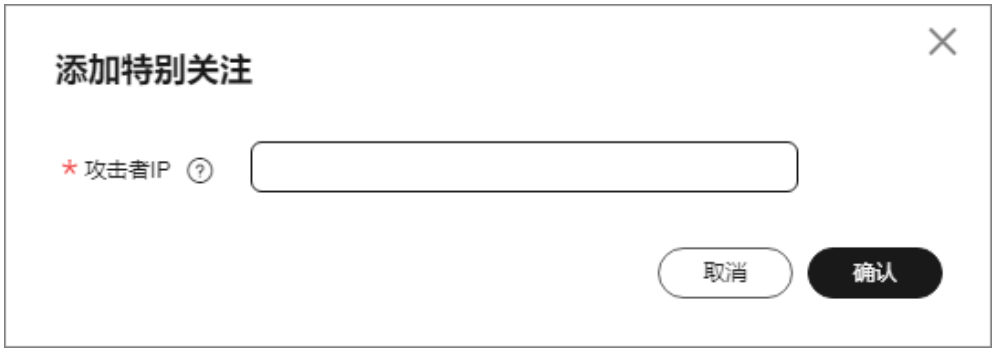
步骤4 在“攻击者列表”区域，单击“特别关注”。

步骤5 在“特别关注管理”页面，单击“添加”。

图 9-4 特别关注管理

步骤6 添加需要特别关注的攻击者IP。

图 9-5 添加 IP



步骤7 单击“确认”。

----结束

相关操作

- **编辑特别关注信息**：在特别关注的攻击者IP所在行，单击“设置IP名称/描述”，修改名称或描述后，单击“确认”。

- **删除单个特别关注**：在特别关注的攻击者IP所在行，单击“删除”，在弹出的窗口中单击“确定”。
- **批量删除特别关注**：勾选多个特别关注，单击“批量删除”，在弹出的窗口中单击“确定”。
- **将攻击者添加到白名单**：在攻击者IP所在行，选择“更多 > 加入白名单”，输入白名单名称后单击“确认”。
- **将攻击者添加到阻断规则**：在攻击者IP所在行，选择“更多 > 加入阻断规则”，填入参数后单击“确认”。

9.3 设置关联 IP

创建一个关联IP组，并将攻击者IP手动添加到关联IP组中，可以帮助用户快速分析关联IP的攻击信息。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击 ☰，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“威胁检测 > 攻击者画像”，进入“攻击者画像”页面。

步骤4 单击页面右上角的“关联IP组管理”，进入“关联IP组”页面。

图 9-6 关联 IP 组

步骤5 单击“新建”，填写关联IP组信息。

图 9-7 新建关联 IP 组

表 9-2 参数说明

参数	说明
名称	名称由中文、字母、数字、下划线、中划线组成，长度不超过20个字符。
描述	描述信息。

步骤6 单击“确认”。

添加关联IP

步骤7 在创建的关联IP组所在行，单击“查看”，进入“关联IP列表”。

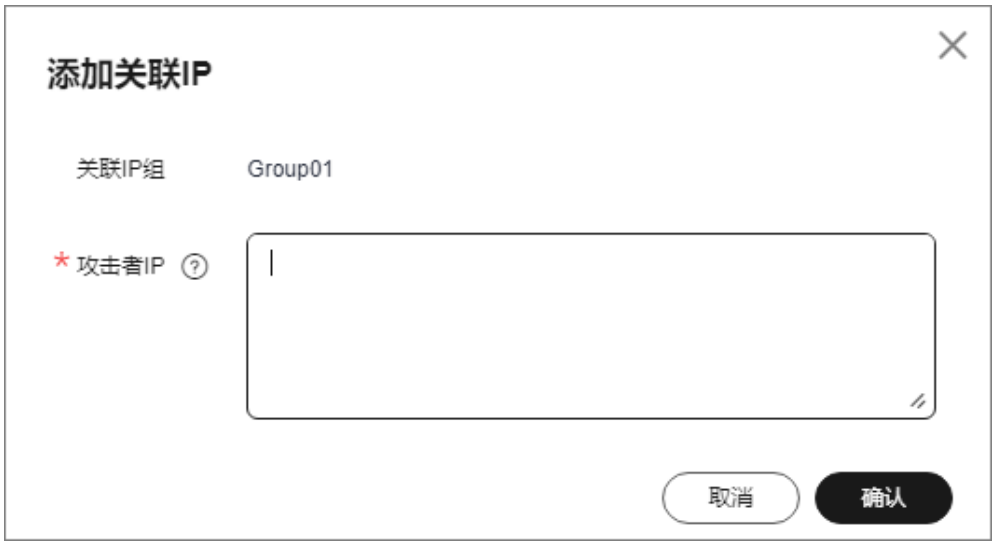
图 9-8 关联 IP 组

步骤8 在“关联IP列表”页面，单击“新建”。

步骤9 根据需要，添加攻击者IP。

攻击者IP：多个IP以英文逗号隔开。

图 9-9 添加 IP



步骤10 单击“确认”，完成添加。

图 9-10 添加结果

----结束

10 配置基础防御规则

合理配置防护策略能预防大规模威胁入侵，有效保护资产。您可以通过配置基础防护规则，提升系统安全性。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击 ☰，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“入侵响应 > 防护策略配置”，进入配置页面。

步骤4 在“基础防御”所在行，单击“查看规则”，进入“基础防御规则”页面。

图 10-1 防护策略配置

步骤5 根据实际调整基础防御规则。

- 启用规则：在需要启用的规则所在行，单击“启用”。
- 禁用规则：在需要禁用的规则所在行，单击“禁用”。
- 批量启用：勾选需要启用的规则，单击“批量启用规则”，在弹窗中单击“确认”。
- 批量禁用：勾选需要禁用的规则，单击“批量禁用规则”，在弹窗中单击“确认”。

图 10-2 基础防御规则

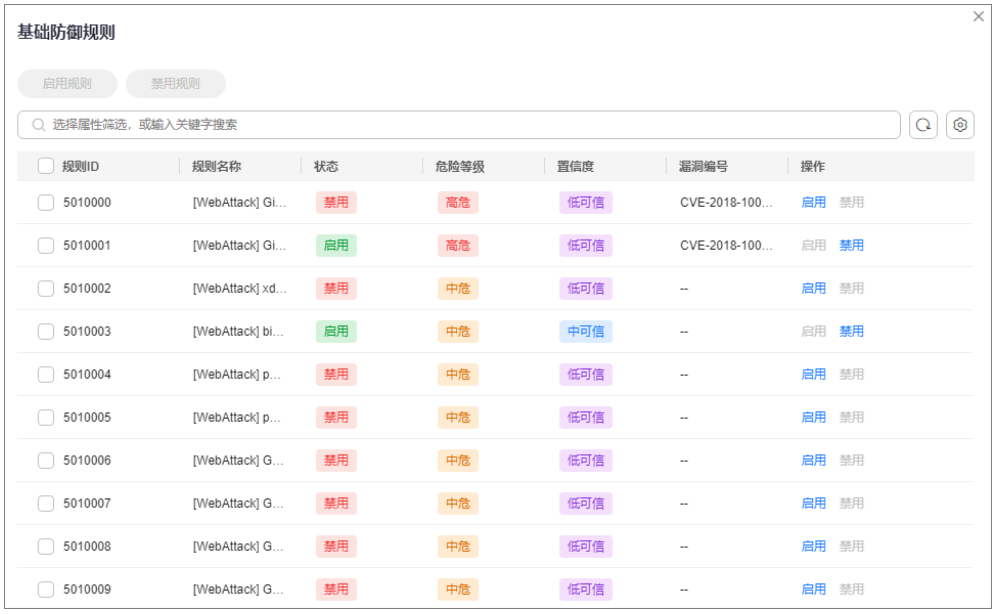


表 10-1 参数说明

类别	说明
规则ID	防御规则的ID。
规则名称	防御规则的名称。
状态	规则的状态。 ● 启用 ● 禁用
危险等级	防御规则对应的网络攻击的危险等级。 ● 高危 ● 中危 ● 低危
置信度	规则的检测可信度。 ● 高可信 ● 中可信 ● 低可信
漏洞编号	规则对应的漏洞编号。

----结束

11 配置阻断规则

操作场景

NDR提供精准阻断的功能，如果您需要精准阻断攻击源的访问或精准防护指定主机，都可以通过阻断规则的配置来实现。主要场景和配置建议如下：

- 攻击源IP未知但确定了防护对象范围：源IP设置为“**ANY**”，目的IP设置为“**IP/IP地址组**”、端口设置为“**端口**”或“**端口组**”。
- 已知攻击源IP但不确定防护对象范围：源IP设置为“**IP**”，目的IP和目的端口都设置为“**ANY**”。
- 已知攻击源IP且确定了防护对象范围：源IP设置为“**IP**”，目的IP设置为“**IP**”或“IP地址组”、端口设置为“**端口**”或“**端口组**”。

前提条件

- 如果您需要对多个攻击源IP/目的IP配置不同的阻断规则，可提前将这些IP配置为IP地址组，具体方法请参考**创建IP地址组**。
- 如果您需要对目的IP的多个端口配置不同的规则，可提前将这些端口配置为端口组，具体方法请参考**创建端口组**。

约束限制

- NDR阻断规则只能阻断TCP协议。
- NDR阻断采用旁路阻断技术（TCP Reset），无法达到100%阻断率，通常作为出现攻击时的应急响应处置措施；如果希望达到100%的阻断率或者作为长时间的访问控制策略，建议使用虚拟私有云（VPC）的安全组或CFW的访问控制策略功能。

操作步骤

步骤1 登录NDR服务控制台。

步骤2 在左侧导航树中，选择“入侵响应 > 阻断规则”，进入配置页面。

步骤3 单击“新建”，根据实际需要设置阻断规则，如**图11-1**所示。

图 11-1 新建阻断规则

表 11-1 阻断规则

类别	说明
名称	阻断规则的名称，只能由3～255个中文字符、英文字母、数字、下划线、中划线组成。
IP类型	仅支持IPv4。
源IP	• IP地址组：已知攻击源IP的情况下选择该项。创建方法参考**创建IP地址组**。 • IP地址：已知攻击源IP的情况下选择该项。 • ANY：无法获取攻击源IP的情况下选择该项。“源IP”和“目的IP”不能同时为“ANY”。

类别	说明
目的IP	• IP地址组：需要防护的目的IP地址组，创建方法参考**创建IP地址组**。 • IP地址：需要防护的目的IP地址。 • ANY：不设定防护IP时选择该项。“目的IP”和“源IP”不能同时为“ANY”。
目的端口	• 端口组：需要防护的目的端口组，创建方法参考**创建端口组**。 • 端口：需要防护的目的端口。 • ANY：选择该项时，防护目的IP的所有端口。
动作	• 封禁：符合阻断规则的访问将会被拦截，同时产生告警，可通过**攻击事件日志**或**阻断日志**查看拦截记录。 • 告警：符合阻断规则的访问只触发告警，不会被拦截。
过期时间	规则过期时间，不填则永久生效。
描述	规则的描述信息，不超过512个字符。

步骤4 单击“确认”，保存规则。

步骤5 在刚创建的规则所在行的“操作”列，单击“启用”。

步骤6 勾选需要关联该规则的服务器后，单击列表上方的“启用”，在弹出的对话框中单击“确定”。

当阻断规则“状态”为“已启用”，表示该规则启用成功。

----结束

相关操作

禁用阻断规则

步骤1 在需要禁用的阻断规则所在行，单击“更多 > 禁用”。

步骤2 勾选需要解除该规则的服务器，单击列表上方的“禁用”，在弹出的窗口中，单击“确定”。

----结束

编辑阻断规则

步骤1 在需要编辑的阻断规则所在行，单击“编辑”。

步骤2 根据实际修改配置后，单击“确认”。

----结束

删除阻断规则

步骤1 在需要删除的阻断规则所在行，单击“更多 > 删除”。

步骤2 在弹出的窗口中，单击“确定”。

----结束

12 查看防护对象

NDR支持查看防护的弹性公网IP及其绑定的实例信息，以便及时调整防护策略。

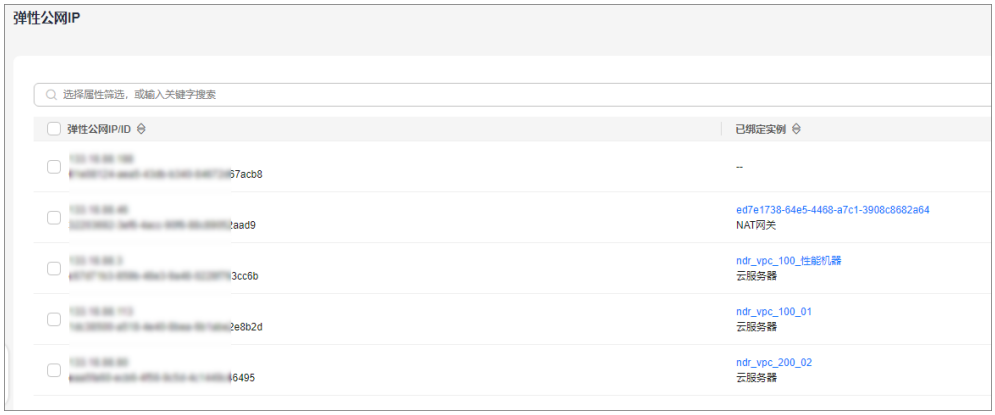
操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“入侵响应 > 弹性公网IP”，进入“弹性公网IP”页面。

图 12-1 弹性公网 IP



说明

NDR默认1小时刷新一次弹性公网IP，如果数据未同步，请单击“资产同步”进行刷新。

----结束

13 创建地址组

13.1 创建 IP 地址组

操作场景

如果您需要对多个攻击源IP/目的IP配置不同的阻断规则，可提前将这些IP配置为IP地址组，在创建新的阻断规则时选择IP地址组即可，避免反复输入IP地址。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“入侵响应 > 地址组管理”。

步骤4 在“IP组”页签单击“新建IP组”。

步骤5 根据实际添加IP地址组，如图13-1所示。

图 13-1 新建 IP 组

表 13-1 新建 IP 组

类别	说明
名称	IP地址组的名称。只能由3～255个中文字符、英文字母、数字、下划线、中划线组成。
IP类型	支持IPv4和IPv6，请根据实际选择。
类型	选择IP地址输入模式。 • 非网段 • 网段
IP地址	• 类型为非网段时：输入IP地址，例如“192.168.1.1”，多个IP以英文逗号隔开。 • 类型为网段时：输入网段地址，例如“192.168.1.1/22”，多个网段以英文逗号隔开。

类别	说明
描述	可选参数，IP组的描述信息，不超过512个字符。

----结束

相关操作

说明

已关联阻断规则的IP地址组不可编辑和删除。

修改IP地址组

步骤1 在需要修改的IP地址组所在行的“操作”列，单击“编辑”。

步骤2 根据实际修改IP地址组的信息后，单击“确认”。

----结束

删除IP地址组

步骤1 在需要删除的IP地址组所在行的“操作”列，单击“删除”。

步骤2 在弹出的窗口中，单击“确定”。

----结束

13.2 创建端口组

操作场景

如果您需要对目的IP的多个端口配置不同的规则，可提前将这些端口配置为端口组，在创建新的阻断规则时选端口组即可，避免反复输入端口。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“入侵响应 > 地址组管理”。

步骤4 在“端口组”页签单击“新建端口组”。

步骤5 根据实际添加端口组，参数说明如表13-2所示。

图 13-2 新建端口组

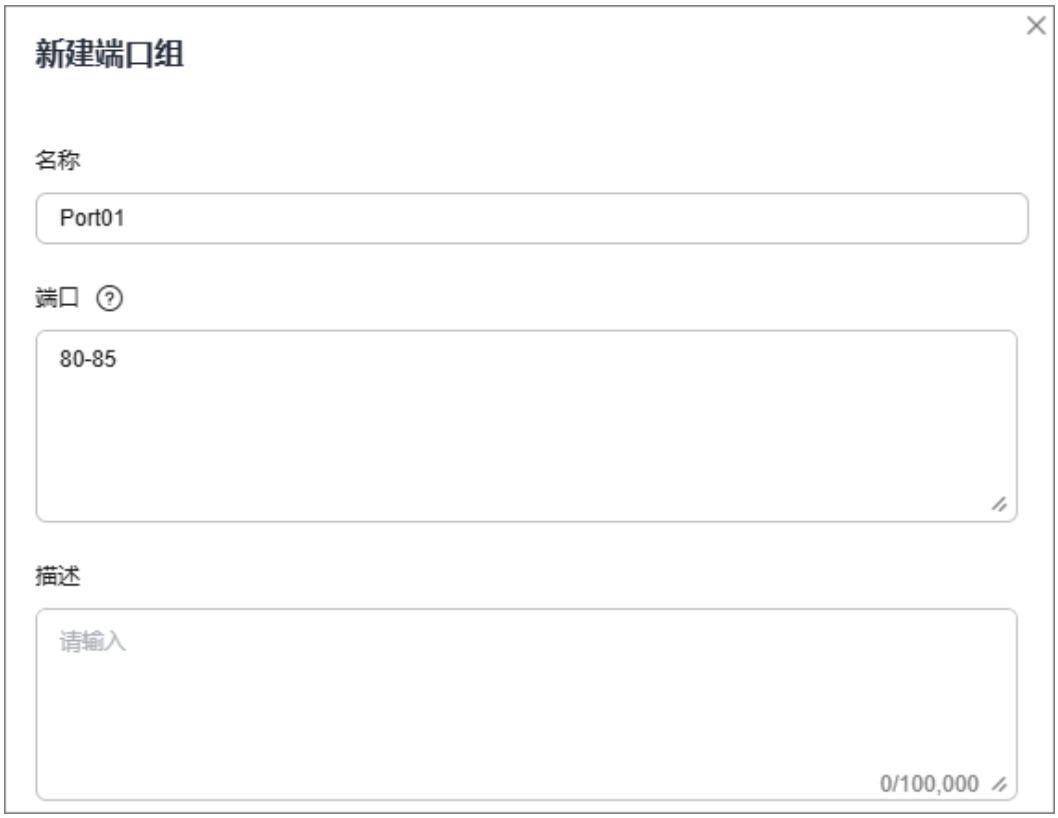


表 13-2 新建端口组

类别	说明
名称	端口组的名称。只能由3～255个中文字符、英文字母、数字、下划线、中划线组成。
端口	端口号，端口范围0～65535。多个端口以英文逗号隔开，支持输入端口范围，如“80-85”。
描述	可选参数，IP组的描述信息，不超过512个字符。

----结束

相关操作

说明

已关联阻断规则的端口组不可编辑和删除。

修改端口组

步骤1 在需要修改的端口组所在行的“操作”列，单击“编辑”。

步骤2 根据实际修改端口组的信息后，单击“确认”。

----结束

删除端口组

步骤1 在需要删除的端口组所在行的“操作”列，单击“删除”。

步骤2 在弹出的窗口中，单击“确定”。

----结束

14 管理检测策略

14.1 配置检测策略

NDR支持对指定VPC内的ECS主机配置检测策略，开启检测策略后，检测到的攻击将会记录到攻击事件日志。

操作步骤

步骤1 登录控制台。

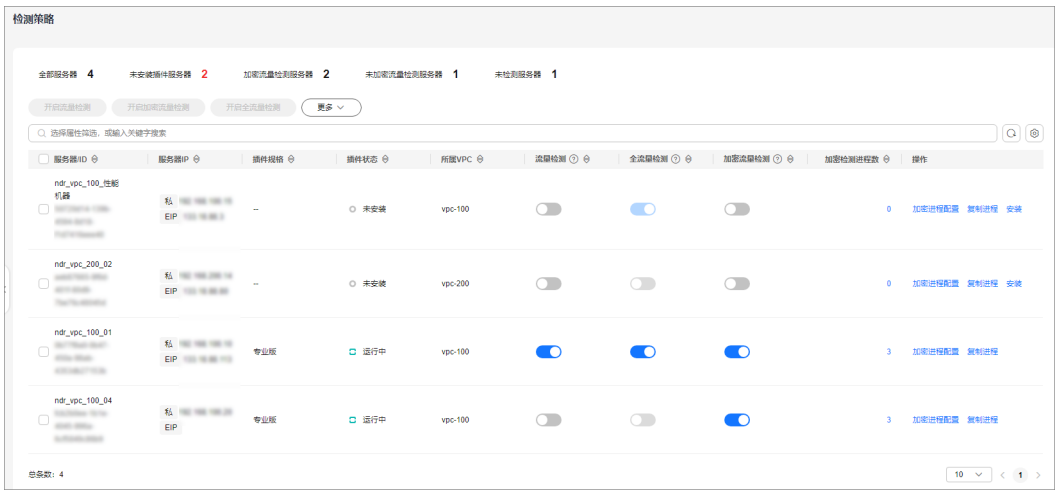
步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“检测管理 > 检测策略”，进入“检测策略”页面。

说明

如果您未创建委托，请先创建委托，授予NDR访问其他云服务资源。

图 14-1 检测策略



步骤4 勾选目标服务器后，单击需要开启的流量检测策略。

表 14-1 检测策略

流量检测策略	说明
开启流量检测	检测网络流量和未加密流量的攻击特征。
开启加密流量检测	检测加密流量的攻击特征。
开启全流量检测	检测全部流量。如果流量过大会导致服务器资源消耗增加。关闭后只检查以下高危端口的流量： ● Web服务：80、8080、8081、3128、9080。 ● 数据库服务：3306、1433、1521、5000、5432、5236、6379、11211、27017。 ● 其他常用协议：21、22、23、25、110、139、587、873、993、3389。

步骤5 在弹窗中单击“确定”。

----结束

相关操作

- 关闭流量检测：勾选目标服务器，选择“更多 > 关闭流量检测”。
- 关闭加密流量检测：勾选目标服务器，选择“更多 > 关闭加密流量检测”。
- 关闭全流量检测：勾选目标服务器，选择“更多 > 关闭全流量检测”。
- 复制进程：在目标服务器所在行单击“复制进程”，勾选需要复制的进程，单击“确认”。

14.2 配置加密进程

NDR支持开启内置进程加密，也支持用户对指定进程进行加密。

用户将服务器运行中的进程配置为加密进程后，NDR将对加密后的进程进行加密流量检测，进一步提高系统的安全性。针对无需检测加密流量的进程，可以通过配置黑名单目录，NDR将不再对该目录下的进程进行加密流量检测。

加密系统默认进程

步骤1 登录控制台。

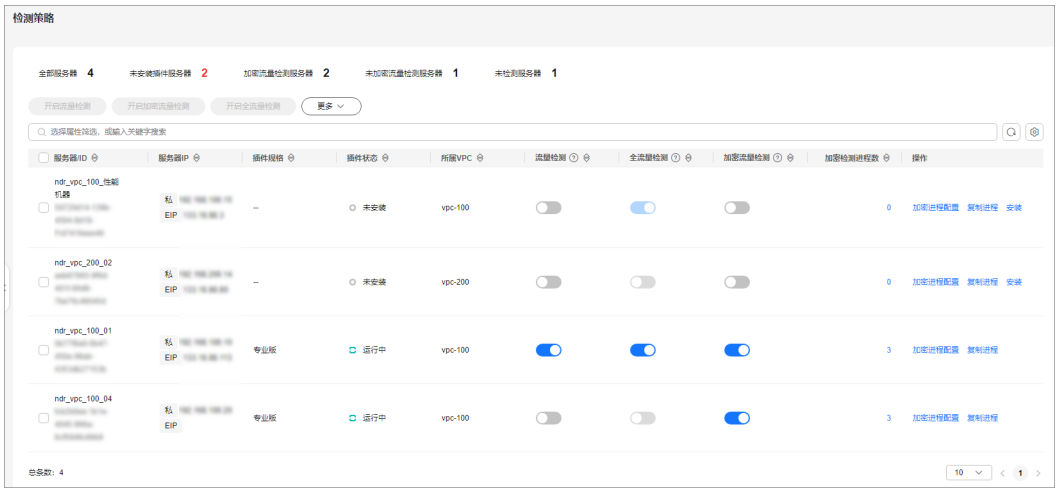
步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“检测管理 > 检测策略”，进入“检测策略”页面。

说明

如果您未创建委托，请先创建委托，授予NDR访问其他云服务资源。

图 14-2 检测策略



步骤4 在目标服务器所在行，单击“加密进程配置”。

步骤5 在“系统内置”页签，打开“默认进程检测”的开关。

图 14-3 默认进程检测

步骤6 在弹窗中，单击“确定”。

----结束

加密自定义进程

步骤1 登录控制台。

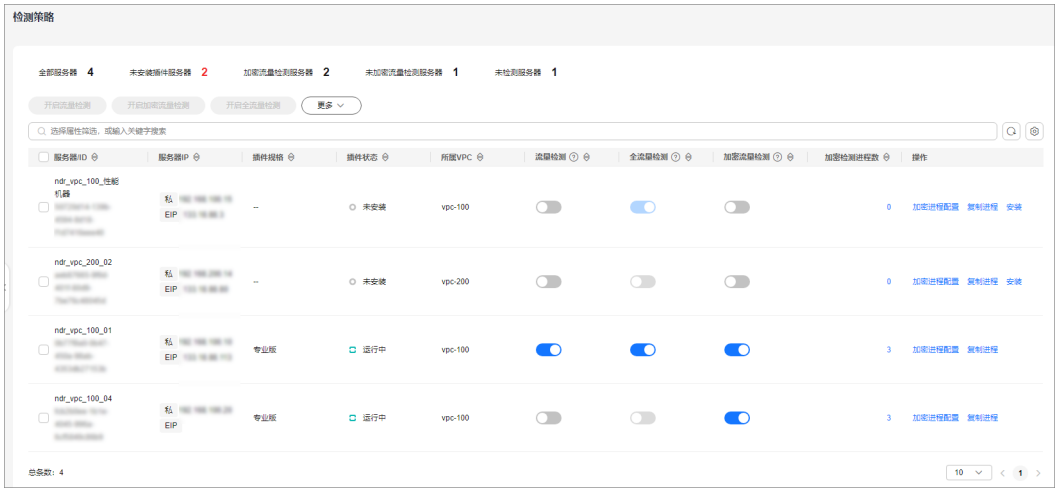
步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“检测管理 > 检测策略”，进入“检测策略”页面。

说明

如果您未创建委托，请先创建委托，授予NDR访问其他云服务资源。

图 14-4 检测策略



步骤4 在目标服务器所在行，单击“加密进程配置”。

步骤5 在“用户添加”页签，根据实际选择进程添加方式。

- 添加系统运行中的进程：单击“添加进程”，勾选需要的进程后，单击“确认”。
- 添加自定义进程：单击“创建自定义进程”，设置进程类型和进程名称后，单击“确认”。

表 14-2 自定义进程参数说明

参数	说明
进程类型	当前支持二进制和Java，根据实际选择。
进程	输入进程的名称。

图 14-5 自定义进程

----结束

配置黑名单目录

针对无需检测加密流量的进程，可以配置黑名单目录。配置完成后，NDR将不再对该目录下的进程进行检测。

步骤1 登录控制台。

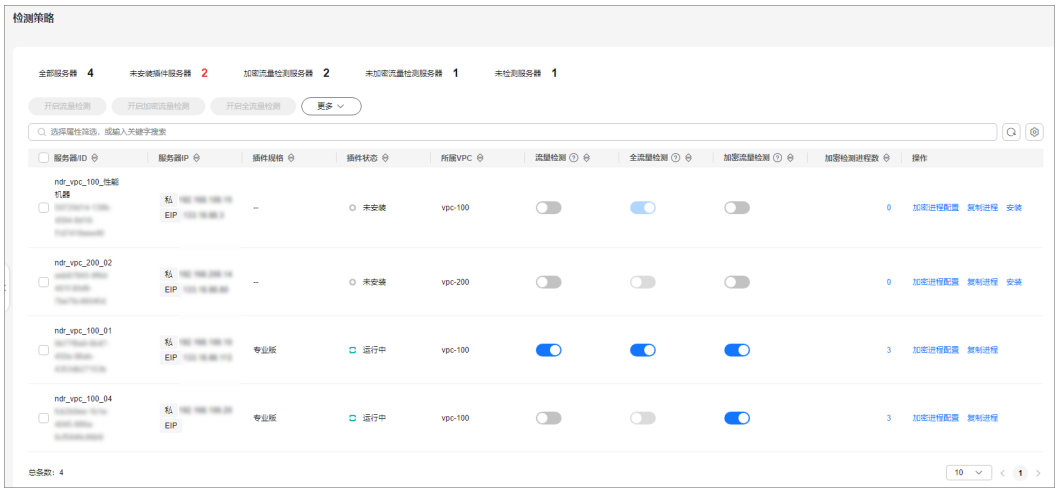
步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“检测管理 > 检测策略”，进入“检测策略”页面。

说明

如果您未创建委托，请先创建委托，授予NDR访问其他云服务资源。

图 14-6 检测策略



步骤4 在目标服务器所在行，单击“加密进程配置”。

步骤5 在“黑名单目录”页签，单击“创建黑名单目录”，配置黑名单目录信息。

表 14-3 黑名单目录参数说明

参数	说明
进程类型	当前支持二进制和Java，根据实际选择。
目录	设置无需检测加密流量的目录。 • 所有绝对路径都以根目录“/”开始。 • 路径中的每个目录和文件名之间用斜杠“/”分隔。 • 控制拉黑范围，不允许直接填写“/”，至少是二级目录。 • 仅支持“/文件夹/文件夹”，不支持“/abc/.. /abc/*/def”。
描述	输入进程的描述。

图 14-7 创建黑名单目录

步骤6 配置完成后，单击“确认”。

----结束

15 管理主机插件

15.1 安装插件

NDR支持为主机安装插件包，安装插件包后，可以对主机进行加密流量检测。

注意事项

- HSS服务升级Agent期间，主机插件功能不可用。
- 主机安装插件会占用一定主机资源，CPU约占用5%。

前提条件

- 目标版本的插件包配额充足，若配额不足，请参考**修改插件包配额**增加配额。
- 目标主机已绑定弹性公网IP，具体操作请参考《 弹性云服务器 ECS 用户指南 》。
- 目标主机已安装HSS服务的Agent并开启防护，具体操作请参考《 企业主机安全 HSS 用户指南 》。

操作步骤

步骤1 登录控制台。

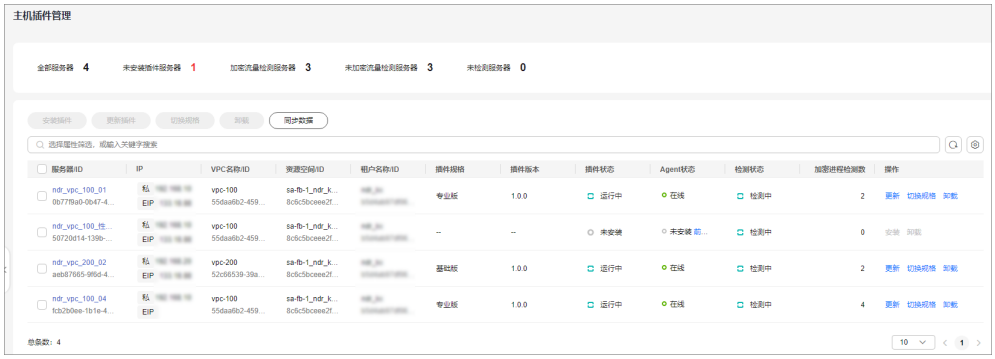
步骤2 选择“区域”，在页面左上角单击 ☰，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“检测管理 > 主机插件管理”，进入“主机插件管理”页面。

说明

如果您未创建委托，请先创建委托，授予NDR访问其他云服务资源。

图 15-1 主机插件管理



步骤4 根据实际选择安装方法。

- 批量安装：勾选需要安装的主机，单击列表上方“安装插件”。
- 单个安装：在目标主机所在行，单击“安装”。

步骤5 选择需要安装的“插件规格”和“插件版本”。

图 15-2 安装插件

表 15-1 参数说明

参数	说明
插件规格	• 基础版：支持东西向和南北向流量检测。 • 专业版：支持东西向和南北向流量检测，同时支持加密流量的检测。
插件版本	根据需要选择插件的版本。

说明

如果主机未安装HSS服务的Agent，请在主机所在行单击“前往HSS”进行安装。

步骤6 单击“确认”。

----结束

15.2 更新插件

已安装插件包的主机，如需更新插件包版本，可参考此章节操作。

前提条件

主机已安装插件。具体操作请参考**安装插件**。

操作步骤

步骤1 登录控制台。

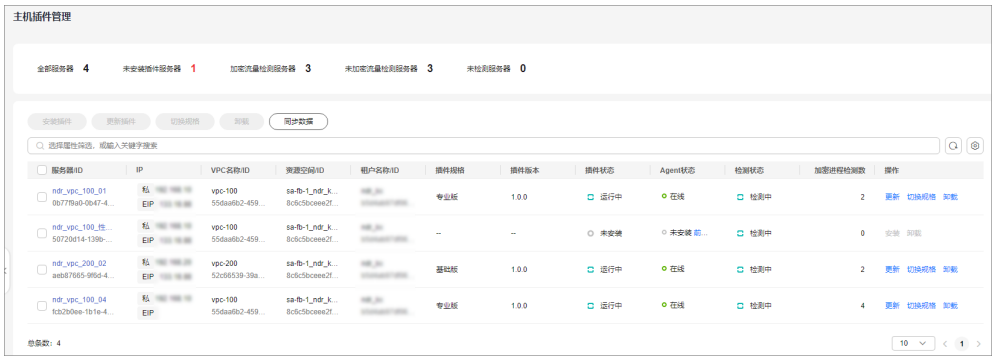
步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“检测管理 > 主机插件管理”，进入“主机插件管理”页面。

说明

如果您未创建委托，请先创建委托，授予NDR访问其他云服务资源。

图 15-3 主机插件管理

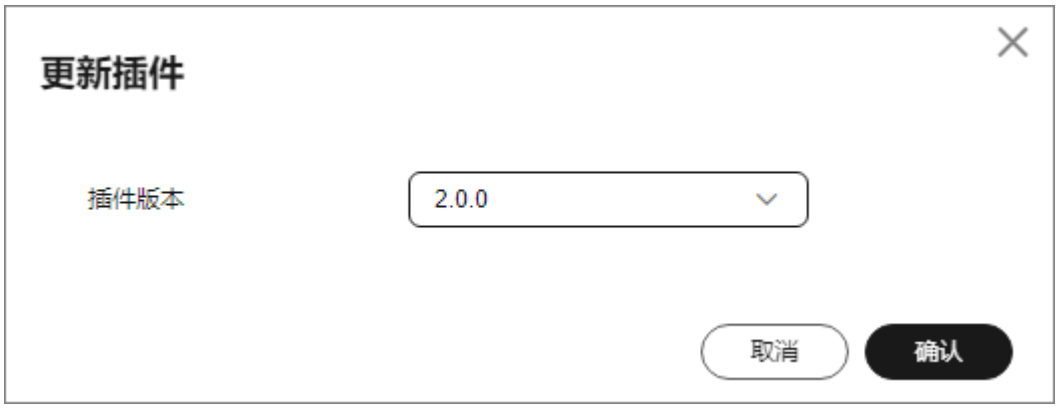


步骤4 根据实际选择更新方法。

- 批量更新：勾选需要更新的主机，单击列表上方“更新插件”。
- 单个更新：在目标主机所在行，单击“更新”。

步骤5 选择需要更新的版本，单击“确认”。

图 15-4 更新插件



----结束

15.3 变更规格

NDR插件规格包含基础版和专业版，支持切换规格。

前提条件

- 主机已安装插件。具体操作请参考**安装插件**。
- 目标版本插件存在剩余配额。如果配额不足，请参考**修改插件包配额**增加配额。

操作步骤

步骤1 登录控制台。

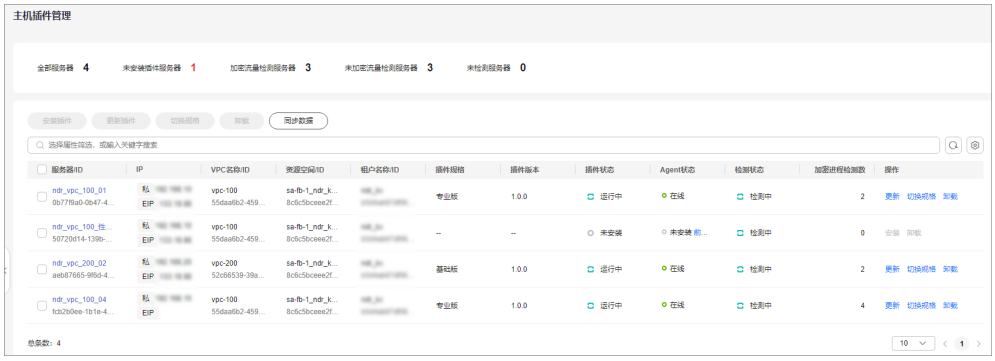
步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“检测管理 > 主机插件管理”，进入“主机插件管理”页面。

说明

如果您未创建委托，请先创建委托，授予NDR访问其他云服务资源。

图 15-5 主机插件管理



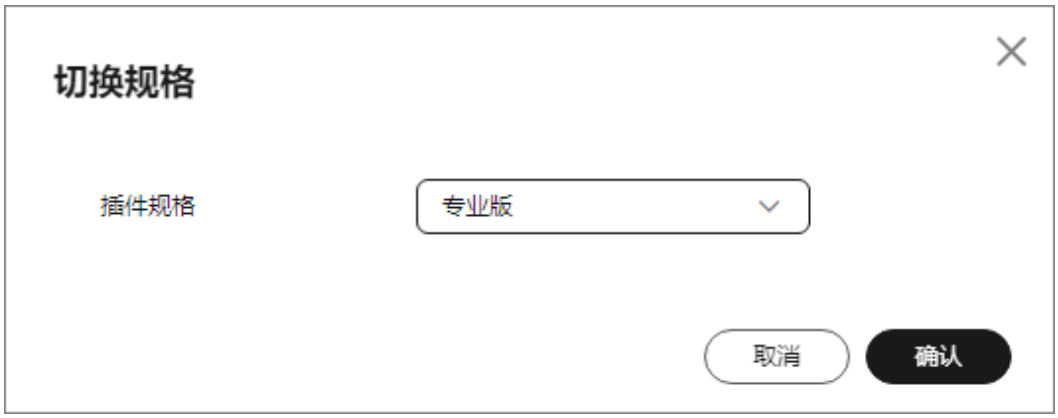
步骤4 根据实际选择变更方法。

- 批量变更：勾选需要变更规格的主机，单击列表上方“切换规格”。

- 单个变更：在目标主机所在行，单击“切换规格”。

步骤5 选择需要切换的规格，单击“确认”。

图 15-6 切换规格



----结束

15.4 卸载插件

NDR支持为安装了插件包的主机进行卸载操作，卸载插件包后，主机将无法进行加密流量检测，请谨慎操作。

前提条件

主机已安装插件包。具体操作请参考**安装插件**。

操作步骤

步骤1 登录控制台。

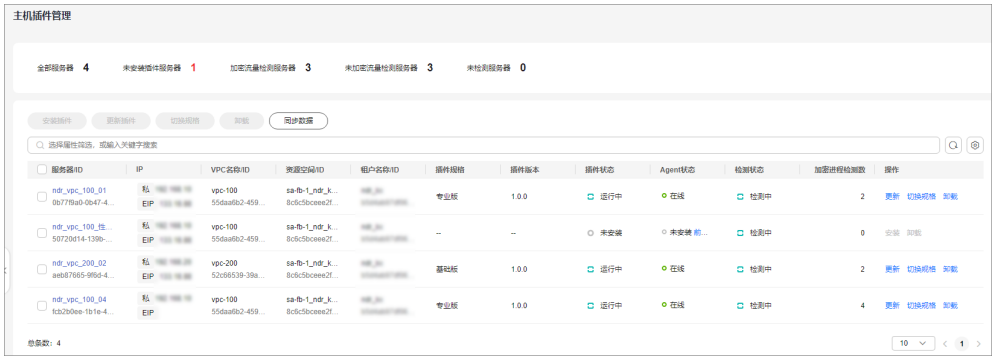
步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“检测管理 > 主机插件管理”，进入“主机插件管理”页面。

说明

如果您未创建委托，请先创建委托，授予NDR访问其他云服务资源。

图 15-7 主机插件管理



步骤4 根据实际选择卸载方法。

- 批量卸载：勾选需要卸载的主机，单击列表上方“卸载”。
- 单个卸载：在目标主机所在行，单击“卸载”。

步骤5 在弹出的窗口中，单击“确定”。

图 15-8 卸载插件

----结束

15.5 同步数据

NDR默认每小时同步一次主机数据，如果数据同步不及时，您可参考本章节手动刷新数据。

前提条件

主机已安装插件包。具体操作请参考**安装插件**。

操作步骤

步骤1 登录控制台。

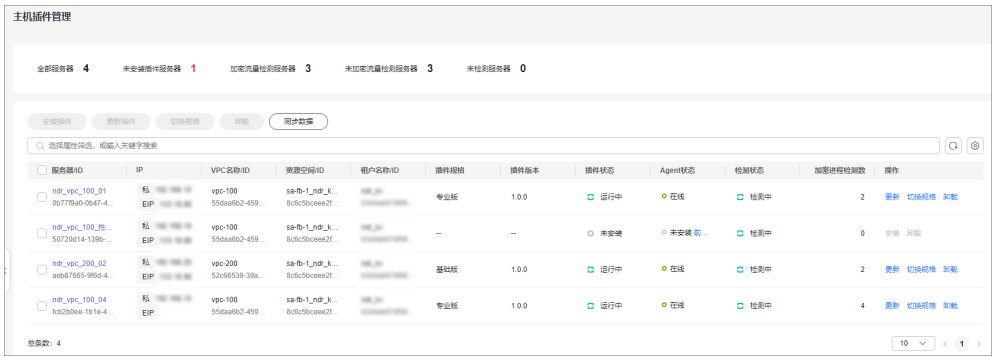
步骤2 选择“区域”，在页面左上角单击，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“检测管理 > 主机插件管理”，进入“主机插件管理”页面。

说明

如果您未创建委托，请先创建委托，授予NDR访问其他云服务资源。

图 15-9 主机插件管理



步骤4 在主机列表上方，单击“同步数据”。

当数据同步完成后，界面会提示“数据已同步”。

图 15-10 数据同步完成

----结束

15.6 修改插件包配额

如果当前插件包配额不满足使用需求，可以通过修改插件包配额增加插件包。

操作步骤

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击 ☰，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，单击“概览”，进入概览页面。

步骤4 在“产品信息”区域，在需要增加配额的插件版本下方，单击“变更”。

图 15-11 变更配额

步骤5 根据需要修改配额，确认配置无误后，勾选“我已知晓变更可能存在的风险及带来的费用变化，同意进行变更”，单击“确认”。

图 15-12 确认配额

等待申请任务实施成功后，规格变更成功。

----结束

16 配置告警通知

设置告警通知后，NDR可将触发的告警信息通过您设置的接收通知方式（例如邮件或短信）发送给您，您可以及时监测防护状态，迅速获得异常情况。

该任务介绍如何配置IPS检测到攻击时触发告警。

攻击告警

步骤1 登录控制台。

步骤2 选择“区域”，在页面左上角单击 ☰，选择“安全 > 网络检测与响应 NDR”。

步骤3 在左侧导航树中，选择“系统管理 > 告警通知”，进入“告警通知”页面。

步骤4 在“攻击告警”所在行的“操作”列，单击“编辑”，设置通知项参数，参数说明如**表 攻击告警参数说明**所示。

表 16-1 攻击告警参数说明

参数名称	参数说明
通知项说明	IPS攻击事件告警。
通知等级	选择触发通知的危险等级。 可选择“提示”、“次要”、“重要”，支持多选。 例如：选择“提示”和“次要”，那么当IPS检测到危险等级为低危和中危的入侵时，NDR将以短信或邮件的方式通知您及时处理。
通知时间	选择通知的时间段。
触发条件	设置触发条件。 **说明** 在设置时间间隔内，当攻击次数大于或等于您设置的阈值时系统才会发送告警通知。
通知群组	单击下拉列表选择已创建的主题，用于配置接收告警通知的终端。

步骤5 单击“确认”，完成通知项设置。

步骤6 确认信息无误后，在“攻击告警”所在行的“生效状态”列，单击  ，开启攻击告警通知。

----结束

17 查询审计日志

17.1 云审计服务支持的 NDR 操作列表

云审计服务（Cloud Trace Service，CTS）记录了NDR相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见《云审计服务 CTS 用户指南》。

云审计服务支持的NDR操作列表如**表17-1**所示。

表 17-1 CTS 支持的 NDR 操作列表

操作名称	事件名称
开通服务	createSubscription
同步EIP列表	syncEips
退订服务	deleteSubscription
安装插件	installPlugin
卸载插件	uninstallPlugin
更新插件	upgradePlugin
手动执行资源同步	syncResource
变更配额	changeQuota
批量更新攻击事件	batchUpdateAttackEvents
更新单个攻击事件	updateAttackEvent
创建检测策略	createDetectionStrategy
复制检测策略	copyDetectionStrategy
更新检测策略	updateDetectionStrategy
删除检测策略	deleteDetectionStrategy
启用检测策略	enableDetectionStrategy

操作名称	事件名称
停用检测策略	disableDetectionStrategy
批量停用默认检测进程	batchDisableDefaultProcess
删除检测策略默认进程	deleteStrategyDefaultProcess
批量修改主机流量检测状态	batchModifyHostFlowDetectionState
添加检测进程	addHostDetectionProcess
批量删除主机检测进程	deleteHostDetectionProcess
复制单个组件的加密进程配置到其他主机	copyHostDetectionPolicy
添加黑名单目录	addHostBlackDirectory
删除黑名单目录	deleteHostBlackDirectory
查询阻断规则列表	listBlockRule
创建阻断规则	createBlockRule
编辑阻断规则	updateBlockRule
删除阻断规则	deleteBlockRule
创建IP组	createAddressGroup
创建端口组	createPortGroup
删除IP组	deleteAddressGroup
修改IP组	updateAddressGroup
修改端口组	updatePortGroup
删除端口组	deletePortGroup
启用阻断规则	enableBlockRule
禁用阻断规则	disableBlockRule
关闭一键bypass	disableBypass
启用一键bypass	enableBypass

17.2 查询审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录。

- **在CTS新版事件列表查看审计事件**
- **在CTS旧版事件列表查看审计事件**

操作视频

约束与限制

- 管理类追踪器未开启组织功能之前，单账号跟踪的事件可以通过云审计控制台查询。管理类追踪器开启组织功能之后，多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。组织追踪器的详细介绍请参见**组织追踪器概述**。
- 用户通过云审计控制台只能查询最近7天的操作记录，过期自动删除，不支持人工删除。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务（OBS）或云日志服务（LTS），才可在OBS桶或LTS日志组里面查看历史事件信息。否则，您将无法追溯7天以前的操作记录。
- 用户对云服务资源做出创建、修改、删除等操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。
- CTS新版事件列表不显示数据类审计事件，您需要在旧版事件列表查看数据类审计事件。

在 CTS 新版事件列表查看审计事件

步骤1 登录**CTS控制台**。

步骤2 登录控制台，单击左上角 ☰，选择“管理与部署 > 云审计服务 CTS”，进入云审计服务页面。

步骤3 单击左侧导航栏的“事件列表”，进入事件列表信息页面。

步骤4 在列表上方，可以通过筛选时间范围，查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

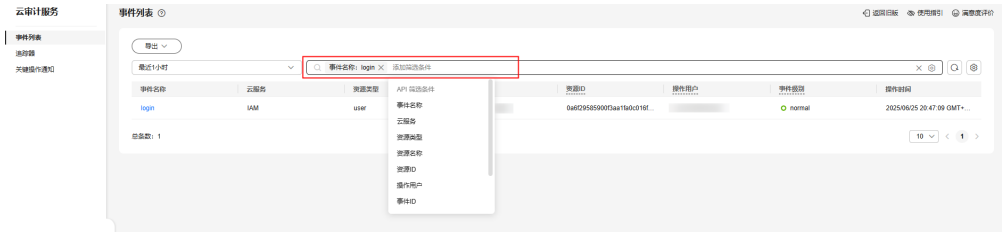
步骤5 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件。

表 17-2 事件筛选参数说明

参数名称	说明
事件名称	操作事件的名称。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 各个云服务支持审计的操作事件的名称请参见**支持审计的服务及详细操作列表**《云审计服务用户指南》的“支持审计的服务及操作列表”章节。 示例：updateAlarm

参数名称	说明
云服务	云服务的名称缩写。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 示例：IAM
资源名称	操作事件涉及的云资源名称。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。 示例：ecs-name
资源ID	操作事件涉及的云资源ID。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 当该资源类型无资源ID或资源创建失败时，该字段为空。 示例：*{虚拟机ID}*
事件ID	操作事件日志上报到CTS后，查看事件中的trace_id参数值。 输入的值需全字符匹配，不支持模糊匹配模式。 示例：01d18a1b-56ee-11f0-ac81-******1e229
资源类型	操作事件涉及的资源类型。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 各个云服务的资源类型请参见**支持审计的服务及详细操作列表**《云审计服务用户指南》的“支持审计的服务及操作列表”章节。 示例：user
操作用户	触发事件的操作用户。 下拉选项中选择一个或多个操作用户。 查看事件中的trace_type的值为“SystemAction”时，表示本次操作由服务内部触发，该条事件对应的操作用户可能为空。 IAM身份与操作用户对应关系，以及操作用户名称的格式说明，请参见**IAM身份与操作用户对应关系**。
事件级别	下拉选项包含“normal”、“warning”、“incident”，只可选择其中一项。 • normal代表操作成功。 • warning代表操作失败。 • incident代表比操作失败更严重的情况，如引起其他故障等。
企业项目ID	资源所在的企业项目ID。 查看企业项目ID的方式：在EPS服务控制台的“项目管理”页面，可以查看企业项目ID。 示例：b305ea24-c930-4922-b4b9-******1eb2

参数名称	说明
访问密钥ID	访问密钥ID，包含临时访问凭证和永久访问密钥。 查看访问密钥ID的方式：在控制台右上方，用户名下拉选项中，选择“我的凭证 > 访问密钥”，可以查看访问密钥ID。 示例：HSTAB47V9V******TLN9



步骤6 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。

- 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
- 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
- 单击按钮，可以获取到事件操作记录的最新信息。
- 单击按钮，可以自定义事件列表的展示信息。启用表格内容折行开关，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。

步骤7 （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

----结束

在 CTS 旧版事件列表查看审计事件

步骤1 登录CTS控制台。

步骤2 登录控制台，单击左上角，选择“管理与部署 > 云审计服务 CTS”，进入云审计服务页面。

步骤3 单击左侧导航栏的“事件列表”，进入事件列表信息页面。

步骤4 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。

步骤5 在页面右上方，可以通过筛选时间范围，查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

步骤6 事件列表支持通过筛选来查询对应的操作事件，如图17-1所示。

图 17-1 筛选框

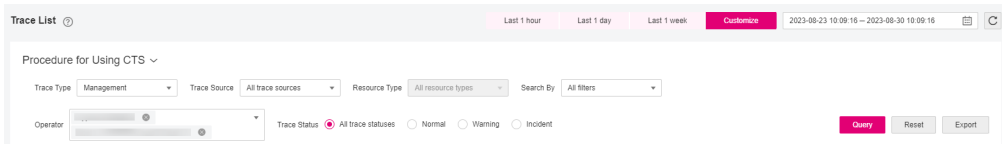


表 17-3 事件筛选参数说明

参数名称	说明
事件类型	事件类型分为“管理事件”和“数据事件”。 ● 管理类事件，即用户对云服务资源新建、修改、删除等操作事件。 ● 数据类事件，即OBS服务上报的OBS桶中的数据的操作事件，例如上传数据、下载数据等。
云服务	在下拉选项中，选择触发操作事件的云服务名称。
资源类型	在下来选项中，选择操作事件涉及的资源类型。 各个云服务的资源类型请参见**支持审计的服务及详细操作列表**《云审计服务用户指南》的“支持审计的服务及操作列表”章节。
筛选类型	筛选类型分为“资源ID”、“事件名称”和“资源名称”。 ● 资源ID：操作事件涉及的云资源ID。 当该资源类型无资源ID，或资源创建失败时，该字段为空。 ● 事件名称：操作事件的名称。 各个云服务支持审计的操作事件的名称请参见**支持审计的服务及详细操作列表**《云审计服务用户指南》的“支持审计的服务及操作列表”章节。 ● 资源名称：操作事件涉及的云资源名称。 当事件所涉及的云资源无资源名称，或对应的API接口操作不涉及资源名称参数时，该字段为空。
操作用户	触发事件的操作用户。 下拉选项中选择一个或多个操作用户。 查看事件中的trace_type的值为“SystemAction”时，表示本次操作由服务内部触发，该条事件对应的操作用户可能为空。 IAM身份与操作用户对应关系，以及操作用户名称的格式说明，请参见**IAM身份与操作用户对应关系**。
事件级别	可选项包含“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。 ● Normal代表操作成功。 ● Warning代表操作失败。 ● Incident代表比操作失败更严重的情况，如引起其他故障等。

步骤7 选择完查询条件后，单击“查询”。

步骤8 在事件列表页面，您还可以导出操作记录文件和刷新列表。

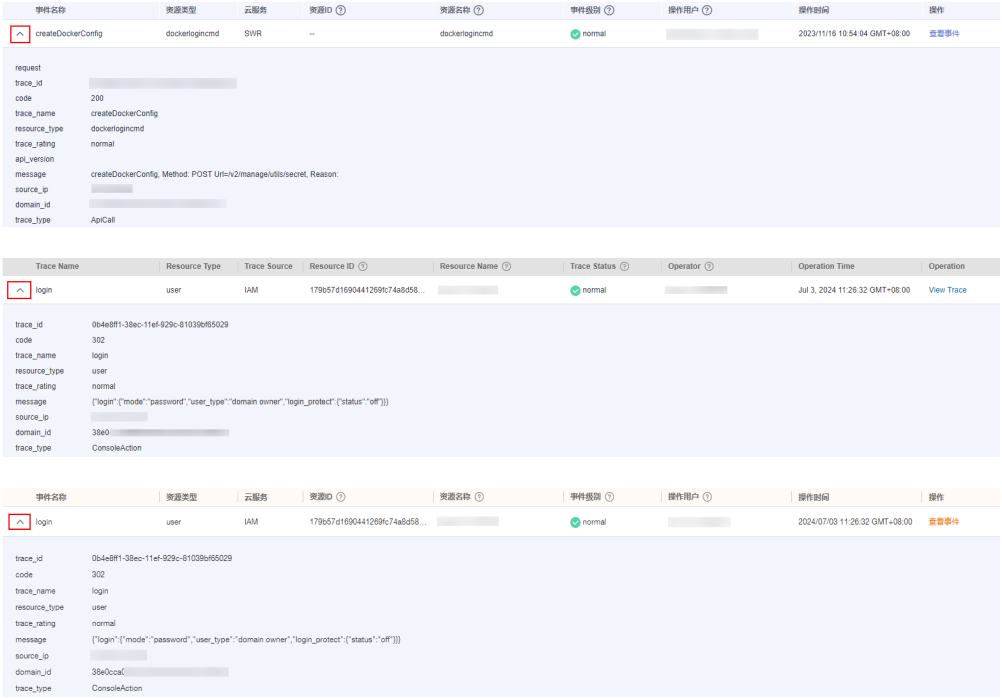
- 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
- 单击按钮，可以获取到事件操作记录的最新信息。

步骤9 在事件的“是否篡改”列中，您可以查看该事件是否被篡改：

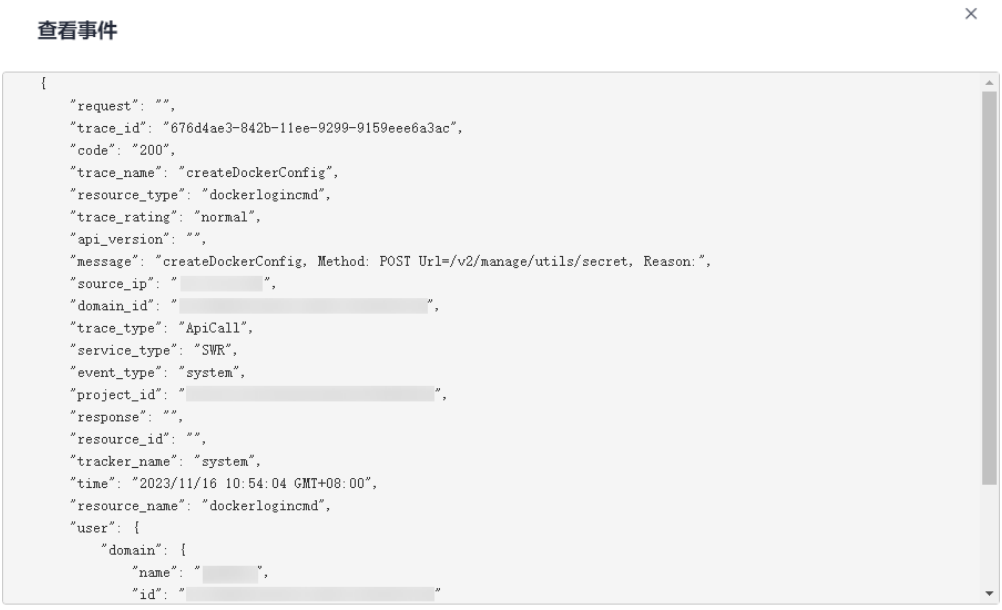
- 上报的审计日志没有被篡改，显示“否”；

- 上报的审计日志被篡改，显示“是”。

步骤10 在需要查看的事件左侧，单击 展开该记录的详细信息。



步骤11 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。



步骤12 （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

----结束