云盾-安骑士高级版
用户指南

中建三局信息科技有限公司

2024 年 5 月

法律声明

天工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. 您应当通过天工云网站或天工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。本文档的内容视为天工云的保密信息，您应当严格遵守保密义务；未经天工云事先书面同意，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. 未经天工云事先书面许可，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。天工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，并在天工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天工云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用天工云产品及服务的参考性指引，天工云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。天工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，但天工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，天工云不承担任何法律责任。在任何情况下，天工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（即使天工云已被告知该等损失的可能性）。

5. 天工云网站上所有内容，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，均由天工云和/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。非经天工云和/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、发行或公开发表天工云网站、产品程序或内容。此外，未经天工云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制天工云的名称（包括但不限于单独为或以组合形式包含“天工云”、“TianGongYun”等天工云和/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天工云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与天工云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.使用须知

在登录云盾控制台前，您需要确认本地PC符合以下配置。

本地PC需要满足如配置要求表中配置要求，才可以正常登录云盾控制台。

表 1. 配置要求表

内容	要求
浏览器	• Internet Explorer浏览器：11及以上版本 • Chrome浏览器（推荐）：42.0.0及以上版本 • Firefox浏览器：30及以上版本 • Safari浏览器：9.0.2版本及以上版本 • 国密浏览器：Chrome内核69及以上的主流国密浏览器
操作系统	• Windows XP版本 • Windows 7及以上版本 • Mac系统 • 龙蜥系统

2.快速入门

2.1. 用户权限说明

本文介绍了云盾涉及的用户角色。

所有云盾安全中心角色均为默认角色，无法自定义添加。在登录云盾安全中心前，您需要确认自己的账号已经分配云盾相关的角色，具体角色说明，请参见云盾默认角色。

表 1. 云盾默认角色

角色名称	角色说明
云安全中心系统管理员	负责云盾安全中心系统管理设置，具备天工云账号管理、云端同步、告警设置、及全局设置的权限。
云安全中心安全管理员	负责整个专有云平台的安全状态，管理云盾各功能模块的安全策略设置，包括态势感知、网络安全、应用安全、云主机安全、物理机安全、资产管理各目录下的所有功能节点权限。 说明 Web应用防火墙、云防火墙等功能的权限需要单独开通。
部门安全管理员	负责某个指定部门中各云产品资源的安全状态，管理针对该部门的云盾各功能模块的安全策略设置，包括态势感知、网络安全、应用安全、云主机安全、物理机安全、资产管理各目录下的所有功能节点权限。同时，部门管理员还可以设置该部门中安全事件告警的联系人及告警方式。 说明 Web应用防火墙、云防火墙等功能的权限需要单独开通。
云安全中心审计员	负责整个专有云平台安全审计工作，查看审计事件、原始日志并设置相关审计策略，具备安全审计目录下所有功能节点权限。

如果您没有相关账号和角色，请联系管理员创建用户及授予角色，具体步骤，请参见《Apsara Uni-manager运营控制台用户指南》中创建用户。

2.2. 登录Apsara Uni-manager运营控制台

本文主要向您介绍如何登录Apsara Uni-manager运营控制台。

前提条件

- 登录Apsara Uni-manager运营控制台前，确认您已从部署人员处获取Apsara Uni-manager运营控制台的服务域名地址。
- 推荐使用Chrome浏览器。

操作步骤

1. 在浏览器地址栏中，输入Apsara Uni-manager运营控制台的服务域名地址，按回车键。
2. 输入正确的用户名及密码。

   请向运营管理员获取登录控制台的用户名和密码。

> **说明** 首次登录Apsara Uni-manager运营控制台时，需要修改登录用户名的密码，请按照提示完成密码修改。为提高安全性，密码长度必须为10~32位，且至少包含以下两种类型：
>
> - 英文大写或小写字母（A~Z、a~z）
> - 阿拉伯数字（0~9）
> - 特殊符号（感叹号（!）、at（@）、井号（#）、美元符号（$）、百分号（%）等）

3. 单击**账号登录**。
4. 如果账号已激活MFA多因素认证，请根据以下两种情况进行操作：
   - 管理员强制开启MFA后的首次登录：
     a. 在绑定虚拟MFA设备页面中，按页面提示步骤绑定MFA设备。
     b. 按照步骤2重新输入账号和密码，单击**账号登录**。
     c. 输入6位MFA码后单击**认证**。
   - 您已开启并绑定MFA：

     输入6位MFA码后单击**认证**。

     > **说明** 绑定并开启MFA的操作请参见《Apsara Uni-manager运营控制台用户指南》中的《绑定并开启虚拟MFA设备》章节。

3.安骑士

3.1. 安全总览

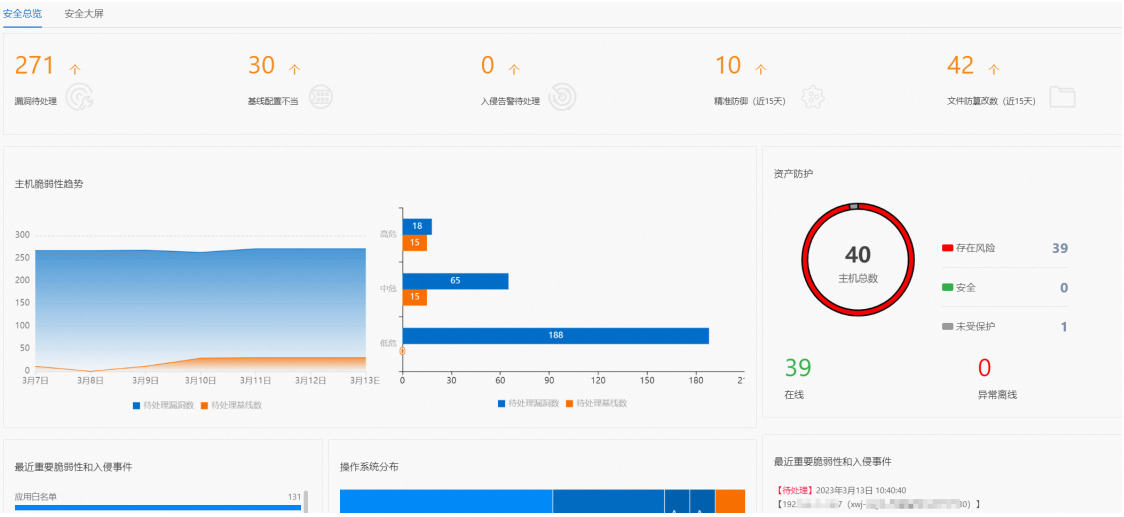
安全总览是对云主机整体的安全情况进行概要性展示，以便安全管理员快速了解和掌握当前安全情况。本文介绍如何查看主机安全总览。

安全总览

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**主机安全 > 安骑士**。在**安骑士**授权页面，选择**地域**并单击**角色授权访问**。

> **说明**
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，单击**安全总览**。
4. 单击**安全总览**页签，查看安全总览以及安全态势大屏。



安全总览整体展现云主机环境各类型的安全弱点（**漏洞待处理**、**基线配置不当**）和安全事件（**入侵告警待处理**、**精准防御**、**文件防篡改数**）的数量。

- **主机脆弱性趋势**：展示云主机待处理漏洞数、基线数及风险程度分布。
- **资产防护**：查看目前云主机中正在受到保护的主机数量和离线数量。
- **最近重要脆弱性和入侵事件**：展示最近重要的云主机安全弱点和安全事件，单击弱点、事件的链接可以查看具体详细情况。
- **操作系统分布**：按照操作系统类别，统计展示服务器资产。

安全大屏

安全大屏支持展示您的资产、漏洞、基线、告警等数据指标，您可根据业务需要自定义安全大屏需要展示的内容。

自定义安全态势大屏展示内容

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**主机安全 > 安骑士**。在**安骑士**授权页面，选择**地域**并单击**角色授权访问**。

> **说明**
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，单击**安全总览**。
4. 在**安全大屏**页签，单击**直接访问**。

5. 在安全态势大屏页面，单击右上角图标。
6. 配置安全大屏数据和内容后，单击**保存设置**。
   - 在**选择数据**页签，选中需要在大屏上实时展示的数据类型。用户可以选中**全部**或单个数据分类。
   - 在**内容配置**页签，配置需要在大屏上显示的**标题文案**、**标题装饰**。

自定义大屏场景

为满足不同业务领域展示不同场景数据的需要，安全态势大屏支持自定义场景，您可以根据业务的需要自定义多个不同的大屏场景。

1. 在**安全大屏**页签，单击**直接访问**。

2. 在安全态势大屏页面，单击右上角图标。
3. 配置安全大屏数据和内容后，单击**保存设置**。
   - 在**选择数据**页签，选中需要在大屏上实时展示的数据类型。用户可以选中**全部**或单个数据分类。
   - 在**内容配置**页签，配置需要在大屏上显示的**标题文案**、**标题装饰**。

   如果您需要展示其它场景，可在**场景列表**页面定位到需要展示的场景并单击**立即启用**。

> 说明
>
> 安全态势大屏自定义场景不限数量。

安全态势大屏页面介绍

漏洞

漏洞区域展示了您资产中漏洞的总数量、不同危险等级漏洞的环形占比图、需处理的漏洞类型和对应的数量、最近7天不同风险等级的漏洞的数据统计柱状图。**漏洞**区域包含以下信息：

- **总量**：您资产中漏洞的总数量。
- **需紧急修复**：您资产中需立即修复的漏洞数量。状态符号为红色。
- **可延后修复**：您资产中可稍后再进行修复的漏洞总数量。状态符号为橙色。
- **暂可不修复**：您资产中暂时无法进行修复的漏洞数量。状态符号为灰色。
- 最近7天不同风险等级的漏洞的数据统计柱状图。

资产

资产区域展示了云安全中心检测到的资产统计信息。**资产**区域包含以下信息：

- **总量**：您资产的总数量。
- **已失陷**：您资产中存在未处理的高危级别告警的服务器数量。状态符号为红色。
- **存在风险**：您资产中存在漏洞、基线和中低级别告警的服务器数量。状态符号为橙色。
- **安全**：您资产中不存在漏洞、基线风险和告警的服务器数量。状态符号为绿色。
- 存在安全风险情况最为严重的排名前五的资产及其状态。

基线

基线区域展示了您资产中基线检查风险项的总数量、不同等级的基线风险项及其对应的数量、最近7天不同风险等级的基线风险项的数据统计柱状图。当天统计数据为实时数据。**基线**区域包含以下信息：

- **总量**：您资产中基线风险项的总数量。
- **高危**：您资产中的高危基线风险项数量。状态符号为红色。建议立即进行排查和修复。
- **中危**：您资产中的中危基线风险项数量。状态符号为橙色。
- **低危**：您资产中的低危基线风险项数量。状态符号为灰色。
- 最近7天不同危险等级的基线风险项的数据统计柱状图。

安全态势

安全态势区域展示了最近7天、15天或30天安全评分的趋势图。当天统计数据为实时数据。

告警

告警区域展示了最近24小时内未处理的、排名前五的高风险告警列表，包括告警事件发生的时间、事件名称和服务器名称。

攻击来源TOP 5

攻击来源TOP 5区域展示了最近24小时内您服务器受到的攻击次数排名前五的攻击来源IP地址及其发起的攻击次数。

云平台最佳实践

云平台最佳实践区域展示了云平台配置检查功能实时检测出的项目信息。

以下是检测项、风险等级和影响资产的说明：

- **检测项**：云平台配置检查支持的检测项目详情。
- **风险等级**：检测项目的风险级别。以下是风险等级颜色和风险级别的对应关系：
  - 红色代表高风险。
  - 橙色代表中风险。
  - 灰色代表低风险。
  - 绿色代表正常。
- **影响资产**：检测项目对应风险影响的资产数量。

最高风险资产

最高风险资产区域展示了排名前五的高风险资产。

3.2. 资产中心

3.2.1. 资产管理

将服务器接入安骑士后，支持手动同步最新资产信息、查看服务器信息、对服务器进行分组管理等。本文介绍如何进行服务器管理。

同步最新资产

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**主机安全 > 安骑士**。在**安骑士**授权页面，选择**地域**并单击**角色授权访问**。

   > **说明**
   >
   > 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**资产中心 > 资产管理**。
4. 在**资产管理**页面，单击**同步最新资产**。

   安骑士会拉取最新的服务器资产信息，刷新服务器列表。

   > **说明**
   >
   > 同步最新资产信息需要1分钟时间，请耐心等待。

查看服务器信息

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**主机安全 > 安骑士**。在**安骑士**授权页面，选择**地域**并单击**角色授权访问**。

   > **说明**
   >
   > 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**资产中心 > 资产管理**。
4. 在**资产管理**页面，查看服务器信息。
   - 通过检索查看服务器的信息

     您可使用服务器列表上方提供的搜索组件，通过该服务器的**实例名称**、**公网IP**、**私网IP**等查找到该服务器，支持设置一个或者多个检索条件，筛选出满足筛选条件的服务器。

     在目标服务器的**风险状况**列，可查看到该服务器是否存在安全风险。

     单击目标服务器**操作**列的**修复**，进入该服务器的详情页面，查看服务器的详细信息。

功能页签	说明
基本信息	■ 风险状态：展示漏洞、告警等风险情况。 ■ 详细信息：展示了该服务器的基本信息，如服务器的ID、地域、分组、操作系统等。 ■ 云盘快照：展示云盘快照情况。 ■ 漏洞检测：展示漏洞检测类型，支持为该服务器开启或关闭不同类型的漏洞检测功能 ■ 资产指纹调查：展示资产指纹数据。 ■ 登录安全设置：展示该服务器已添加的常用登录地址、登录的IP、时间和账号，支持设置该服务器的相关告警。
漏洞信息	展示该服务器的漏洞检测结果。
安全告警处理	展示该服务器的安全告警信息。
云外暴露	展示云外暴露信息。
基线检查	展示该服务器的基线检查结果。
资产指纹调查	展示该服务器指纹的详细信息。

   - 查看同一分类的服务器的信息：安骑士提供了**安全风险**、**资产属性**的服务器分类方式，帮助您对服务器进行分类管理。

在服务器列表，还支持以下操作：

场景	操作步骤
对服务器进行分类	a. 选中目标服务器，在服务器列表下方选择**资产分类** > **更换分组**。 b. 在**更换分组**对话框，选择新的分组，单击**确定**。
指令下发	a. 选中目标服务器，在服务器列表下方单击**指令下发**。 b. 在**指令下发**对话框，选择下发指令，单击**确定**。
数据导出	选中目标服务器，在服务器列表下方，单击需要下载的数据。 支持导出资产基本信息、弱口令信息、资产漏洞信息、基线风险信息、基线检查全量信息和客户端日志。

多云资产添加

安骑士支持对第三方云服务器和IDC服务器进行防护和管理。下面介绍添加添加多云、IDC供应商操作步骤。

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**主机安全** > **安骑士**。在**安骑士**授权页面，选择**地域**并单击**角色授权访问**。

> 说明
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**资产中心** > **资产管理**。
4. 在服务器列表左侧**资产分类管理**区域，单击供应商。
5. 在供应商页面，单击创建供应商，并填写供应商信息。

   如果供应商没有region概念，可创建默认region用于管理机房信息。

   创建完成后，支持在**操作**列，**编辑**、**删除**、**添加region**等操作。

管理服务器的分组及标签

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**主机安全** > **安骑士**。在**安骑士**授权页面，选择**地域**并单击**角色授权访问**。

> 说明
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**资产中心** > **资产管理**。

4. 在**资产管理**页面左侧区域，管理服务器分组和标签。
   - 管理服务器分组：在使用网页防篡改、基线检查、漏洞扫描等功能，选择生效的服务器时，如果您提前对服务器进行了分组，即可按照服务器的分组进行快捷选择，免去一个个选择生效服务器繁琐步骤。

     在服务器列表左侧**资产分类管理**区域的**服务器组**，在**服务器组**页面，管理服务器分组。
     - 新建服务器组：单击**添加分组**，输入**分组名称**，选择包含的服务器，单击**确定**。
     - 修改和更换服务器组：定位到目标分组，在**操作**列，单击**管理**。
     - 删除服务器：定位到目标分组，在**操作**列，单击**删除**。
   - 管理服务器标签：使用**标签**功能为服务器自定义标签标识其特殊属性，可方便您筛选具有相同属性的服务器。

     在服务器列表左侧**标签**区域，管理服务器标签。
     - 新建服务器标签：单击**管理**，输入服务器标签名称并设置标签包含的服务器，单击**确定**。
     - 删除服务器标签：定位到目标服务器标签，单击 × 图标，在**提示**对话框，的**确定**。

3.2.2. 主机指纹

本文介绍如何通过查看服务器端口监听信息、软件版本信息、进程信息、账号信息、计划任务、中间件信息。

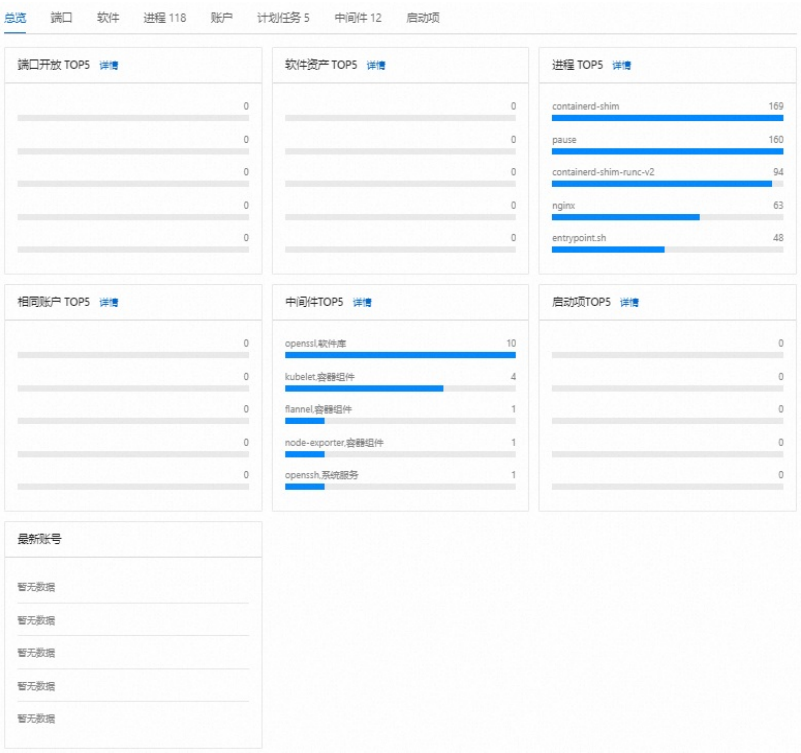
操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**主机安全 > 安骑士**。在**安骑士**授权页面，选择**地域**并单击**角色授权访问**。

   > **说明**
   >
   > 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**资产中心 > 主机指纹**。
4. 单击**配置管理**，在相应项目的下拉菜单中，选择主机指纹采集频率。
5. 在**主机指纹**页面，查看主机指纹信息。
   - **总览**

在总览页签，查看主机指纹信息。



- **监听端口**

> **说明**
>
> 监听端口的应用场景包括：清点一个端口被哪些服务器监听、清点一台服务器开通了哪些端口。

在**端口**页签，查看所有**监听端口号**、**网络协议**和服务器信息。

- 您可以通过搜索端口号、服务器进程名称、服务器名称或IP，快速查找端口。
- 在服务器信息列表中，查看服务器的**对应进程**、**IP**、**最新扫描时间**。

- **管理软件版本**

> **说明**
>
> 软件版本的应用场景包括：清点非法软件资产（非法安装）、清点版本过低软件资产、漏洞爆发时快速定位受影响资产范围。

在**软件**页签，查看所有使用中的**软件资产**和使用这些软件的**服务器数**。

- 您可以使用软件名、版本、软件安装目录、服务器名称或IP进行搜索。
- 单击软件名，查看其对应资产、软件版本等信息。
- 单击右上角图标，下载软件版本数据表到本地，方便后续盘点资产。

- **管理运行进程**

> **说明**
>
> 运行进程的应用场景包括：清点一个进程在哪些服务器中运行、清点一台服务器运行了哪些进程。

在**主机指纹**页面，单击**进程**页签，查看所有运行中进程和运行这些进程的主机数。

- 您可以使用**进程名**、**运行用户**、**启动参数**或**服务器名称或IP**进行搜索。
- 单击进程名，查看进程对应资产、路径、启动参数等详细信息。

- **管理账户信息**

> **说明**
>
> 账号信息应用场景包括：清点一个账号被哪些服务器创建、清点一台服务器创建了哪些账号。

在**主机指纹**页面，单击**账户**页签，查看所有已登录的系统账号和使用这些账号的主机数。

- 您可以使用账号名、root权限、服务器名称或IP进行搜索。
- 单击账号名，查看对应资产、root权限、用户组等详细信息。

- **管理计划任务**

在**主机指纹**页面，单击**计划任务**页签，查看所有任务的路径和运行这些任务的主机数。

- 您可以使用任务路径、服务器名称或IP进行搜索。
- 单击任务路径，查看对应资产、执行命令、任务周期等详细信息。

- **管理中间件**

在**主机指纹**页面，单击**中间件**页签，查看所有任务的中间件的指纹数。

- 您可以使用任务路径、服务器名称或IP进行搜索。
- 单击任务路径，查看对应资产、执行命令、任务周期等详细信息。

- **管理启动项**

在**主机指纹**页签，单击**启动项**页签，查看启动项和对应的指纹数。

3.3. 安全预防

3.3.1. 漏洞管理

3.3.1.1. 管理Linux软件漏洞

本文介绍如何管理Linux软件漏洞。

背景信息

比对CVE官方漏洞库，自动检测您服务器上安装的软件版本是否存在漏洞，并向您推送漏洞消息。针对检测到的漏洞，提供漏洞修复指令和验证功能。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在顶部菜单栏，单击**安全**，在**主机安全**区域，单击**安骑士**。

> **说明**
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**安全预防 > 漏洞管理**。
4. 在**Linux软件漏洞**页签的漏洞列表中，查看检测出的Linux漏洞。

> **说明**
>
> 通过漏洞搜索和筛选功能，能够快速定位到具体漏洞。

5. 单击漏洞名称，进入漏洞详情页，查看漏洞详细信息和影响资产。

> **说明**
>
> 通过搜索和筛选功能，能够快速展示影响资产。

   - **基本信息**：显示该漏洞的名称、漏洞影响分值、简介和解决方案等信息。
   - **影响资产**：展示涉及该漏洞的所有服务器。

6. 根据漏洞影响情况，选择相应的处理方式。

   表 1. 漏洞操作方式

操作	说明
生成修复命令	自动生成修复漏洞的指令，然后登录服务器运行该指令来修复漏洞。
一键修复	直接修复漏洞。
已重启并验证	如果修复漏洞需要重启服务器才能生效，必须等待漏洞修复状态变为**修复成功待重启**后，重启该服务器，然后单击**已重启并验证**完成修复。
忽略	可忽略该漏洞，系统将不再上报并告警此服务器上被忽略的漏洞。
验证	修复漏洞后，单击**验证**，一键验证该漏洞是否已修复成功。 如果未进行手动验证，漏洞修复成功后 48 小时内系统会自动去验证。

   对于影响资产，可以进行单个操作或多个批量操作。

   - **单个操作**：在**操作**列，对单个受影响的服务器进行处理。

- 批量操作：选中一个或多个需要处理的服务器，使用列表下方的批量操作按钮进行批量处理。

3.3.1.2. 管理Windows系统漏洞

本文介绍如何管理Windows系统漏洞。

背景信息

比对微软官方补丁更新，自动检测您服务器上的补丁是否已更新，并向您推送漏洞消息。针对重大漏洞更新，提供自动检测和修复功能。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在顶部菜单栏，单击**安全**，在**主机安全**区域，单击**安骑士**。

> **说明**
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**安全预防 > 漏洞管理**。
4. 在**Windows系统漏洞**页签的漏洞列表中，查看检测出的Windows系统漏洞。

> **说明**
>
> 通过漏洞搜索和筛选功能，能够快速定位到具体漏洞。

5. 单击漏洞名称，进入漏洞详情页，查看漏洞详细信息和影响资产。

> **说明**
>
> 通过搜索和筛选功能，能够快速展示影响资产。

   - **基本信息**：显示该漏洞的名称、漏洞影响分值、简介和解决方案等信息。
   - **影响资产**：展示涉及该漏洞的所有服务器。
6. 根据漏洞影响情况，选择相应的处理方式，如漏洞操作方式所示。

   表 1. 漏洞操作方式

操作	说明
立即修复	直接修复漏洞。系统会在云端缓存一份Windows官方补丁文件，您的Windows系统服务器会直接下载云端的补丁并完成自动更新。
忽略	可忽略该漏洞，系统将不再上报并告警此服务器上被忽略的漏洞。

验证	修复漏洞后，单击**验证**，一键验证该漏洞是否已修复成功。
已重启并验证	如果修复漏洞需要重启服务器才能生效，必须等待漏洞修复状态变为**修复成功待重启**后，重启该服务器，然后单击**已重启并验证**完成修复。

对于影响资产，可以进行单个操作或多个批量操作。

- 单个操作：在**操作**列，对单个受影响的服务器进行处理。
- 批量操作：选中一个或多个需要处理的服务器，使用列表下方的批量操作按钮进行批量处理。

3.3.1.3. 管理Web-CMS漏洞

本文介绍如何管理Web-CMS漏洞。

背景信息

Web-CMS 漏洞功能通过及时获取漏洞预警和相关补丁，并通过云端下发补丁更新，实现漏洞快速发现、快速修复的功能。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在顶部菜单栏，单击**安全**，在**主机安全**区域，单击**安骑士**。

> **说明**
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**安全预防 > 漏洞管理**。
4. 在**Web-CMS漏洞**页签，查看所有漏洞。

> **说明**
>
> 通过漏洞搜索和筛选功能，能够快速定位到具体漏洞。

5. 单击漏洞名称，进入漏洞详情页，查看漏洞详细信息和影响资产。

> **说明**
>
> 通过搜索和筛选功能，能够快速展示影响资产。

6. 根据漏洞影响情况，选择相应的处理方式，如漏洞操作方式所示。

表 1. 漏洞操作方式

操作	说明

立即修复	系统将替换服务器上存在漏洞的Web文件以修复Web-CMS漏洞。 说明 修复Web-CMS漏洞前，建议备份该漏洞相关的Web文件，Web文件的具体路径可参考漏洞处理说明栏中的路径。
忽略	可忽略该漏洞，系统将不再上报并告警此服务器上被忽略的漏洞。
验证	修复漏洞后，单击**验证**，一键验证该漏洞是否已修复成功。 如果未进行手动验证，漏洞修复成功后48小时内系统会自动去验证。
回滚	对于已修复完成的漏洞，单击**回滚**可进行漏洞回滚，还原修复前的Web文件。

对于影响资产，可以进行单个操作或多个批量操作。

- 单个操作：在**操作**列，对单个受影响的服务器进行处理。
- 批量操作：选中一个或多个需要处理的服务器，使用列表下方的批量操作按钮进行批量处理。

3.3.1.4. 管理应急漏洞

本文介绍如何管理应急漏洞。

背景信息

云盾安全中心自动检测服务器上的Redis未授权访问漏洞、STRUTS-052命令执行漏洞等漏洞，并推送漏洞消息。同时，支持漏洞的修复验证操作。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在顶部菜单栏，单击**安全**，在**主机安全**区域，单击**安骑士**。

   说明
   用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**安全预防 > 漏洞管理**。
4. 在**应急漏洞**页签，查看所有漏洞。

   通过漏洞搜索和筛选功能，快速定位到具体漏洞。
5. 单击漏洞名称，进入漏洞详情页，查看漏洞**详情**、**修复建议**、**受影响资产**。

   通过搜索和筛选功能，快速展示影响资产。
6. 根据漏洞影响情况，选择相应的处理方式，如漏洞操作方式所示。

   应急漏洞需要按照修复说明手动修复。

表 1. 漏洞操作方式

操作	说明
忽略	可忽略该漏洞，系统将不再上报并告警此服务器上被忽略的漏洞。
验证	手动修复漏洞后，单击**验证**，一键验证该漏洞是否已修复成功。 如果未进行手动验证，漏洞修复成功后48小时内系统会自动验证漏洞是否已修复。

对于影响资产，可以进行单个操作或多个批量操作。

- 单个操作：在**操作**列，对单个受影响的服务器进行处理。
- 批量操作：选中一个或多个需要处理的服务器，使用列表下方的批量操作按钮进行批量处理。

3.3.1.5. 设置漏洞管理策略

漏洞管理设置允许您开启或关闭不同类型漏洞的自动检测，有选择性地对指定服务器应用漏洞检测，对已失效漏洞设置自动删除周期，和配置漏洞白名单。

背景信息

漏洞白名单用于彻底忽略某些漏洞，您可以在漏洞列表下批量添加漏洞至白名单。添加成功后，系统将不再去检测漏洞白名单中的漏洞。使用漏洞管理设置可以维护漏洞白名单。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在顶部菜单栏，单击**安全**，在**主机安全**区域，单击**安骑士**。

> 说明
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**安全预防** > **漏洞管理**。
4. 单击右上角的**漏洞管理设置**，配置相关策略。

- 选择需要操作的漏洞类型，单击切换开关，开启或关闭该漏洞检测。
- 选择需要操作的漏洞类型，单击**管理**，配置应用该漏洞检测的服务器。
- 选择失效漏洞自动删除周期：7天、30天、90天。

> **说明**
>
> 对于检测出来的漏洞不做任何处理的话，默认该告警失效，并在指定周期后自动删除。

- 选中需要扫描的漏洞等级：
  - **高**：需尽快修复
  - **中**：可延后修复
  - **低**：暂可不修复
- 在漏洞白名单下选中相应漏洞，单击**移除**，重新启用对该漏洞的检测和告警。

3.3.2. 基线检查

3.3.2.1. 基线检查介绍

基线检查功能可自动检测服务器上的安全配置，并针对所发现的检测结果提供问题详情说明和基线加固建议。

功能描述

使用基线检查功能可自动检测服务器上的系统、账号、数据库、弱密码、合规性配置中存在的风险点，并提供加固建议。具体检测内容请参见基线检查内容。

基线检查默认每天0点到6点进行一次全面的自动检测。您可以自行添加和管理基线扫描策略，自定义需要检查的基线项目、检查周期、检测触发时间和应用该策略的服务器。具体请参见设置基线检查策略。

注意事项

以下检查项默认关闭，如果您需要检查该项目，请确认在不影响业务的情况下，在自定义基线扫描策略时选中这些检测项目。

- 部分弱密码检测项（例如，MySQL弱密码检测、PostgreSQL弱密码检测、SQLServer弱密码检测）

  > 说明 这些检测项会采用尝试登录方式进行检查，会占用一定的服务器资源以及生成较多的登录失败记录。

- 系统等保
- CIS标准检测项

基线检查内容

基线检查项分类	检查项
高危风险利用	• 高危风险利用-CouchDB未授权访问高危风险 • 高危风险利用-Docker未授权访问高危风险 • 高危风险利用-Elasticsearch未授权访问高危风险 • 高危风险利用-Memcached未授权访问高危风险 • 高危风险利用-Apache Tomcat AJP文件包含漏洞风险 • 严重威胁利用-ZooKeeper未授权访问高危风险
	天工云标准的安全基线检查 • 天工云标准-Aliyun Linux 2安全基线检查 • 天工云标准-CentOS Linux 6安全基线检查 • 天工云标准-CentOS Linux 7安全基线检查 • 天工云标准-Debian Linux 8安全基线检查 • 天工云标准-Redhat Linux 6安全基线检查 • 天工云标准-Redhat Linux 7安全基线检查 • 天工云标准-Ubuntu安全基线检查 • 天工云标准-Windows 2008 R2安全基线检查 • 天工云标准-Windows 2012 R2安全基线检查 • 天工云标准-Windows 2016/2019 R2安全基线检查

等保合规	CIS标准的安全基线检查 • CIS标准-Aliyun Linux 2安全基线检查 • CIS标准-CentOS Linux 6安全基线检查 • CIS标准-CentOS Linux 7安全基线检查 • CIS标准-Debian Linux 8安全基线检查 • CIS标准-Ubuntu 14安全基线检查 • CIS标准-Ubuntu 16/18安全基线检查 • CIS标准-Windows Server 2008 R2安全基线检查 • CIS标准-Windows Server 2012 R2安全基线检查 • CIS标准-Windows Server 2016/2019 R2安全基线检查
	等保三级合规基线检查 • 等保三级-Aliyun Linux 2合规基线检查 • 等保三级-CentOS Linux 6合规基线检查 • 等保三级-CentOS Linux 7合规基线检查 • 等保三级-Debian Linux 8合规基线检查 • 等保三级-Redhat Linux 6合规基线检查 • 等保三级-Redhat Linux 7合规基线检查 • 等保三级-SUSE 10合规基线检查 • 等保三级-SUSE 11合规基线检查 • 等保三级-SUSE 12合规基线检查 • 等保三级-Ubuntu 14合规基线检查 • 等保三级-Ubuntu 16/18合规基线检查 • 等保三级-Windows 2008 R2合规基线检查 • 等保三级-Windows 2012 R2合规基线检查 • 等保三级-Windows 2016/2019 R2合规基线检查

最佳安全实践	• 天工云标准-Aliyun Linux 2安全基线检查 • 天工云标准-Apache安全基线检查 • 天工云标准-CentOS Linux 6安全基线检查 • 天工云标准-CentOS Linux 7/8安全基线检查 • 天工云标准-Debian Linux 8安全基线检查 • 天工云标准-IIS 8安全基线检查 • 天工云标准-Memcached安全基线检查 • 天工云标准-MongoDB 3.x版本安全基线检查 • 天工云标准-Mysql安全基线检查 • 天工云标准-Nginx安全基线检查 • 天工云标准-Redhat Linux 6安全基线检查 • 天工云标准-Redhat Linux 7安全基线检查 • 天工云标准-Redis安全基线检查 • 天工云标准-Ubuntu安全基线检查 • 天工云标准-Windows 2008 R2安全基线检查 • 天工云标准-Windows 2012 R2安全基线检查 • 天工云标准-Windows 2016/2019 R2安全基线检查 • 天工云标准-Apache Tomcat 安全基线检查
弱口令	• 弱口令-MongoDB登录弱口令检测(支持2.x版本) • 弱口令-FTP登录弱口令检查 • 弱口令-Linux系统登录弱口令检查 • 弱口令-MongoDB登录弱口令检测 • 弱口令-SQL Server数据库登录弱口令检查 • 弱口令-Mysql数据库登录弱口令检查 • 弱口令-Mysql数据库登录弱口令检查(Windows版) • 弱口令-PostgreSQL数据库登录弱口令检查 • 弱口令-Redis数据库登录弱口令检查 • 弱口令-rsync服务登录弱口令检查 • 弱口令-svn服务登录弱口令检查

3.3.2.2. 设置基线检查策略

本文介绍如何如何新增、编辑、删除基线检查策略，并设置基线检查等级的范围。

背景信息

默认情况下，基线检查会使用**默认策略**检测资产的基线安全情况。您可以根据实际业务情况（例如需要满足等保二级），自定义基线检查策略。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在顶部菜单栏，单击**安全**，在**主机安全**区域，单击**安骑士**。

> **说明**
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**安全预防 > 基线检查**。
4. 单击控制台界面右上角**策略管理**，在**策略管理**页面，新增、修改或删除自定义基线检查策略，或修改默认策略。
   - 单击策略列表右上角的**添加策略**，自定义基线检查策略后单击**确定**。

配置项	说明
策略名称	输入用于识别该策略的名称。
检测周期	选择检测周期（每隔1天、3天、7天、30天检测一次）和检测触发时间（00:00~06:00、06:00~12:00、12:00~18:00、18:00~24:00）。
基线名称	选中需要检测的基线项目，在数据库、系统、弱密码检测、中间件下选中具体需要检测的内容。
生效服务器	选中需要应用该策略的分组资产。 **说明** 新购买的服务器默认归属在**分组资产 > 未分组**中，如需对新购资产自动应用该策略，请选中**未分组**。

   - 单击策略名称后的**编辑**或**删除**，对已有策略进行修改或删除。

     > **说明**
     >
     > 策略删除后不可恢复。

   - 单击策略模板列表中默认策略右侧操作栏的**编辑**，调整应用默认策略的资产分组。

     > **说明**
     >
     > 默认策略不支持删除，检测项不支持更改，仅支持修改应用默认策略的资产分组。

   - 在**策略管理**页面下方，您可以设置基线检查的等级范围（高、中、低）。
5. 单击**确定**。

3.3.2.3. 查看和处理基线检查结果

云盾控制台提供了检查后的基线详情说明、基线加固建议和风险处理功能。本文介绍如何在云盾控制台查看和处理基线项目的检查结果，具体包括查看基线项目影响的资产、基线项目详情等信息，以及如何对风险项进行处理。

查看检测结果总览数据

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**主机安全 > 安骑士**。在**安骑士**授权页面，选择地域并单击**角色授权访问**。

> **说明**
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**安全预防 > 基线检查**。
4. 在**基线检查**页面上方，查看云盾控制台根据不同基线检查策略，在您资产中检测到的基线检查结果汇总数据。

在**基线检查策略**下拉框中选择目标基线检查策略，查看以下信息。

- **服务器**：执行基线检查的服务器数量，即配置基线检查策略时，选中的分组服务器中服务器的总台数。
- **检查项**：配置基线检查策略时，选中的**基线名称**的数量。
- **通过率**：最近一次执行基线检查的基线合格率。

  通过率字体为绿色时，代表扫描的资产中基线配置合格率较高；字体为红色时，说明检查的资产中不合格的基线配置较多，可能存在安全隐患，建议前往基线检查详情页面查看并修复。

5. 在**基线检查策略**下拉框中选择**全部策略**。

   基线检查页面会展示所有基线检查项目的列表，包括**基线名称**、**基线检查项**、**风险项/影响服务器数**、**基线分类**及**最新检查时间**。

> **说明**
>
> 您也可在**基线检查策略**下拉框中选择某个基线检查策略，查看该策略对应的基线检查项目列表。

查看基线项目详情

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**主机安全 > 安骑士**。在**安骑士**授权页面，选择地域并单击**角色授权访问**。

> 说明
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**安全预防 > 基线检查**。
4. 在基线检查列表的**基线名称**列中，单击待查看的基线项目，展开该基线项目的详情页面。

   您可查看到该基线项目影响的资产及资产的**通过项**或**风险项**的数量。
5. 在基线详情页面对检测出的风险项进行处理。
   - 单击待查看资产右侧**操作**列下的**查看**，进入**风险项**页面，查看风险检查项详情。
   - 单击资产右侧**操作**列下的**验证**，对已处理风险项的资产进行验证。如果验证通过，资产的**风险项**数值会相应地减少，同时该风险项状态会更新为**已通过**。

查看风险项详情

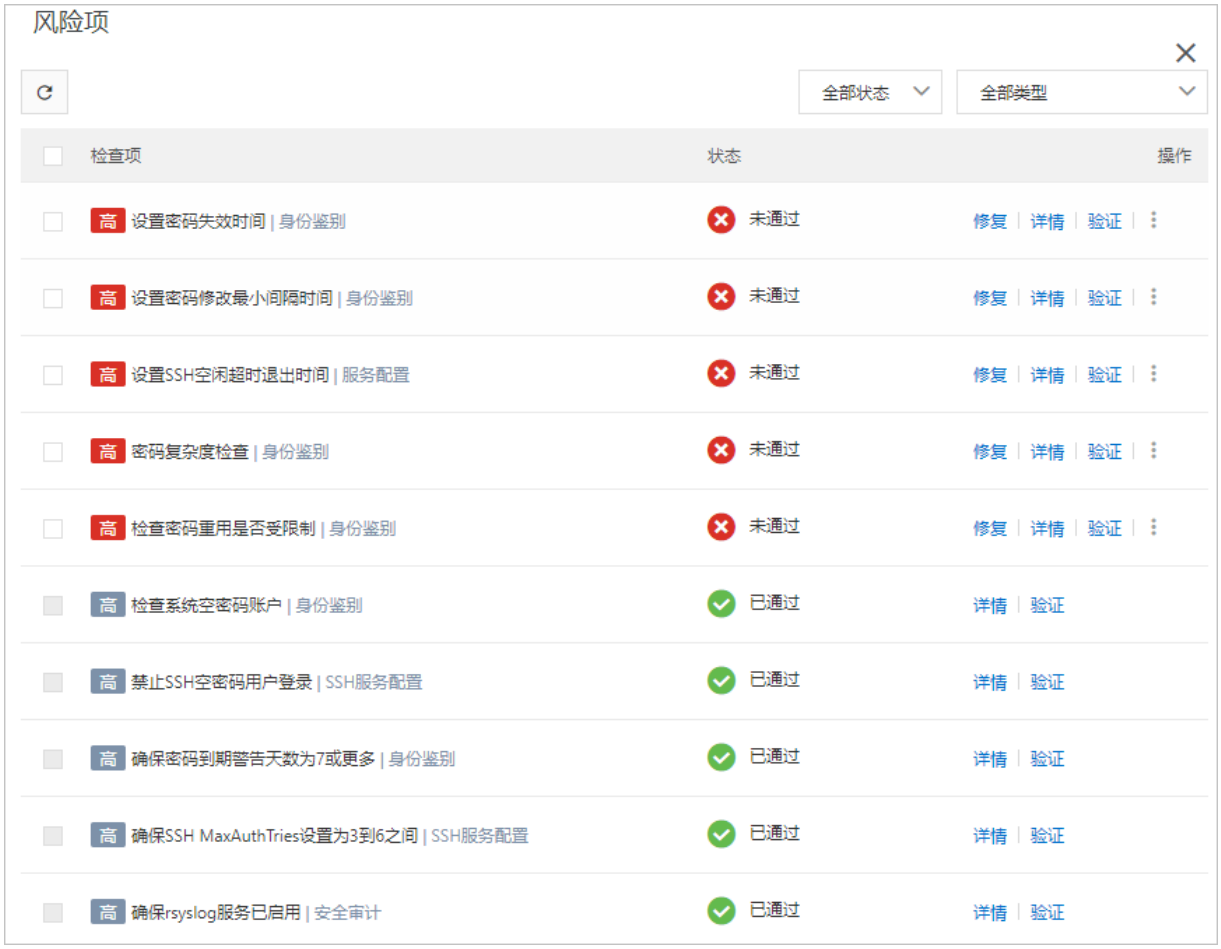
1. 在基线项目详情页面，单击待查看风险项资产右侧**操作**列下的**查看**，展开该资产的风险项页面。

   您可查看到该资产详细的基线配置检查项及检查项对应的检查结果（**已通过**/**未通过**）。
2. 单击待查看检查项右侧**操作**列下的**详情**，可查看该风险检查项的详细描述、检查提示和加固建议等。

> 说明
>
> 建议您根据加固建议及时修复**未通过**的基线检查项目，尤其是高危险等级的风险项。

处理风险检查项

在风险项列表中，根据需要对风险检查项进行相应的处理。



- **加入白名单**

  如果您不希望收到指定的基线检查项的告警，可对指定检查项执行加白名单操作。加入白名单后，该基线检查项将不再触发告警。

  > **说明**
  >
  > 选中多个检查项后，单击左下角的**加白名单**，可批量将多个检查项加入白名单。

- **修复**

  仅支持天工云标准基线检查项的批量修复，修复时可选择多台具有相同基线风险的服务器。

  > **重要**
  >
  > 基线修复存在一定的风险，请在修复前请确认已做好备份。

- **取消已忽略的基线检查配置项告警**

  如果需要云盾控制台对已忽略的基线检查配置项再次触发告警，可对已忽略的检查项执行取消加白。支持单个或批量取消忽略的操作。取消加白后，该基线检查配置项会再次触发告警。

- **验证已修复的基线检查配置项**

  基线检查风险项修复后，单击验证，手动验证该基线项目是否已修复成功。执行验证后，该项目状态将显示为验证中。

如果未进行手动验证，将会根据在扫描策略中设置的检测周期执行自动验证。

验证通过后，资产的基线检查配置项的状态更新为已通过。

3.3.3. 风险暴露检测

风险暴漏检测支持自动分析您的服务器在互联网上的暴露情况，帮助您快速定位资产和应用在互联网上的异常暴露情况并提供相应漏洞的修复建议。本文介绍如何使用安骑士风险暴露检测功能。

统计数据说明

计项	说明
暴露资产/公网IP数	暴露在互联网上的服务器总数量和IP地址总数量。
网关资产	暴露在互联网上的网关资产（负载均衡、NAT网关）总数量。单击相应数值打开网关资产面板，可查看网关资产的列表。
暴露端口	暴露在互联网上的端口总数量。单击相应数值打开暴露端口面板，可查看暴露端口的列表。
暴露组件	暴露在互联网上的您ECS服务器的系统组件（例如OpenSSL、OpenSSH）总数量。单击相应数值打开暴露组件面板，可查看暴露组件的列表。
可被利用漏洞	暴露在互联网上可被黑客利用的漏洞总数量及高危、中危、低危漏洞数量。单击表示高危、中危、低危漏洞数量的数字可跳转至漏洞修复页面。不同类型的漏洞使用不同颜色表示： • 高危：红色。此类漏洞会对您的资产安全较大的威胁，建议您重点关注并及时修复。 • 中危：橙色。此类漏洞对您的资产会产生一定的危害，建议您及时修复。 • 低危：灰色。此类漏洞对您的资产安全危害较小，您可以延后修复。

查看暴露详情

资产暴露

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**安全预防 > 风险暴露检测**。
4. 在**风险暴露检测**页面的**资产暴露**页签，查看目标资产暴露信息。
   - 筛选目标资产：支持从有无漏洞、资产分组、端口等维度筛选查看资产暴露情况。
   - 查看目标资产暴露详情：在**操作**列，单击**暴露详情**。在目标资产面板，查看资产暴露通信链路拓扑图、链路详情等。

- 导出资产暴露数据：单击资产暴露列表右上角

  图标，将暴露资产的详细信息统一导出并保存到本地。导出的文件为Excel格式。

应用暴露

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**安全预防** > **风险暴露检测**。
4. 在**风险暴露检测**页面的**应用暴露**页签，查看目标应用暴露信息。
   - 筛选目标应用：支持从有无漏洞、服务/中间件版本、服务/中间件名称等维度筛选查看应用暴露情况。
   - 查看目标应用暴露详情：在**操作**列，单击**详情**。在目标应用面板，查看应用暴露详情信息。
   - 导出应用暴露数据：单击应用暴露列表右上角

     图标，将暴露应用的详细信息统一导出并保存到本地。导出的文件为Excel格式。

3.3.4. 应用防护

应用防护功能基于RASP（Runtime Application Self-Protection）技术，通过在应用运行时检测攻击并进行应用保护，为应用提供安全防御。您无需修改应用代码，只需在实例中安装应用防护探针，即可为应用提供强大的安全防护能力，并抵御绝大部分未知漏洞所使用的攻击手法。

步骤一：接入应用防护

在使用应用防护功能前，您需要先新建应用，再根据应用的部署位置在应用防护功能中接入主机或容器。

新建应用

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**安全预防** > **应用防护**。
4. 在**应用防护**的**配置**页签，单击**新建应用**，在对话框中填写要新建的应用的名称和备注信息，单击**确定**。

   新建应用后，应用的防护策略为默认策略，默认的防护模式为监控。您可单击应用**操作**列的**防护策略**查看默认策略。
5. 在**提示**对话框，单击**取消**。

   您也可以单击**确定**，直接进行应用接入。具体操作，请参见接入主机和接入容器。
6. **可选**：如果不想使用默认策略，您可以参考以下步骤修改防护策略。

   i. 在**配置**页签下的应用列表，单击目标应用**操作**列的**防护策略**。

ii. 在**防护策略**面板，编辑应用的防护策略，单击**确定**。

配置项	说明
防护模式	选择应用的防护模式，可选项： ■ **监控**：只监控攻击行为，不影响应用运行。检测到攻击行为时，会产生**处理方式**为**监控**的告警。 ■ **防护**：监控并阻断攻击行为，同时也会对应用的一些高危操作进行监控。阻断攻击行为的同时，会产生**处理方式**为**阻断**的告警。 ■ **禁用**：关闭当前应用的应用防护功能，不检测也不阻断任何攻击行为。
检测超时时间	攻击检测的最大时间，输入范围为1～60,000毫秒，默认设置为300毫秒。若攻击检测超过设置的时间，即使未完成检测逻辑也会继续执行原始业务逻辑。如无特殊原因，建议使用默认值。
源IP判断方式	选择**默认**，系统会根据常规的源IP header值获取源IP。常规的源IP包括：X-Real-IP、True-Client-IP、X-Forwarded-For。 选择**取自定义header的值**，系统会优先根据自定义的header值获取源IP。如果自定义header值未命中，则默认规则生效。
检测类型	检测攻击的分类，建议使用默认配置（即全选）。具体检测类型说明，请参见检测攻击类型说明。

接入主机

1. 在**配置**页签下的应用列表，单击目标应用**操作**列的**接入管理**。
2. 在**接入管理**面板，按照**主机接入指南**页签的接入步骤，安装RASP探针，再重启应用。

   您也可以单击**一键推送**，为应用所在的服务器推送并安装RASP探针。

   重启应用时，您需要根据应用运行环境进行相关部署。下表以手动安装部署应用的JVM参数为例介绍重启应用时的运行环境部署。

   在配置参数时，您需要使用**主机接入指南**页签展示的应用ID替换 `{appId}` 。

运行环境	参数配置说明
Tomcat（Linux）	在{TOMCAT_HOME}/bin/setenv.sh文件中第一行添加以下配置。 `JAVA_OPTS="$JAVA_OPTS -javaagent:/usr/local/aegis/rasp/apps/{appId}/rasp.jar"` 如果您的Tomcat版本没有setenv.sh配置文件，请打开{TOMCAT_HOME}/bin/catalina.sh文件，并在JAVA_OPTS后添加上述配置。

Tomcat（Windows）	在{TOMCAT_HOME}/bin/catalina.bat文件中":setArgs"内容的下方添加以下配置。
	○ Windows 64位：
	`set JAVA_OPTS=%JAVA_OPTS% "-javaagent:C:\Program Files (x86)\Alibaba\Aegis\rasp\apps\{appId}\rasp.jar"`
	○ Windows 32位：
	`set JAVA_OPTS=%JAVA_OPTS% "-javaagent:C:\Program Files\Alibaba\Aegis\rasp\apps\{appId}\rasp.jar"`

Jetty	在{JETTY_HOME}/start.ini配置文件中添加以下配置。 `--exec -javaagent:/usr/local/aegis/rasp/apps/{appId}/rasp.jar`
Spring Boot	启动Spring Boot进程时，在启动命令后加上-javaagent参数。 `java -javaagent:/usr/local/aegis/rasp/apps/{appId}/rasp.jar` 例如，您在启动Spring Boot进程时修改前的命令为 `java -jar app.jar` ，需要安装RASP Agent时启动Spring Boot进程执行的命令为 `java -javaagent:/usr/local/aegis/rasp/apps/{appId}/rasp.jar -jar app.jar` 。

如果不需要应用防护功能防护您的应用，您可以单击**卸载指南**页签，按照页面提供的操作步骤卸载RASP探针。

接入容器

1. 在**配置**页签下的应用列表，单击目标应用**操作**列的**接入管理**。
2. 在**接入管理**面板，按照**容器接入指南**页签的接入步骤，安装RASP探针，再重启容器。

   您也可以单击一键**推送**，为应用所在的容器推送并安装RASP探针。

   重启容器时，您需要根据您容器的运行环境进行相关部署。下表以手动安装部署应用的JVM参数为例介绍重启容器时的运行环境部署。

   在配置参数时，您需要使用容器接入指南页签展示的 `Dmanager.key` 值替换 `{manager.key}` 。

运行环境	参数配置说明

SpringBoot	在镜像打包时安装RASP Agent，您需要在Dockerfile修改启动参数，将启动应用的命令由 `CMD ["java","-jar","/app.jar"]` 修改为 `CMD ["java","-javaagent:/rasp/rasp.jar","-Dmanager.key={manager.key}","-jar","/app.jar"]` 。

Tomcat	○ 在镜像打包时安装RASP Agent，您需要在Dockerfile中添加以下内容。
	`ENV JAVA_OPTS="-javaagent:/rasp/rasp.jar -Dmanager.key={manager.key}"`
	○ 在容器启动时安装RASP Agent，您需要在启动时添加以下参数。
	`docker --env JAVA_OPTS="-javaagent:/rasp/rasp.jar -Dmanager.key={manager.key}"`
	例如，您在启动容器时修改前的命令为 `docker -itd --name=test -P 镜像名` ，需要安装RASP Agent时启动容器执行的命令为 `docker -itd --env JAVA_OPTS="-javaagent:/rasp/rasp.jar -Dmanager.key={manager.key}" --name=test -P 镜像名` 。

Weblogic	○ 在镜像打包时安装RASP Agent，您需要在Dockerfile中添加以下内容。
	`ENV JAVA_OPTIONS="-javaagent:/rasp/rasp.jar -Dmanager.key={manager.key}"`
	○ 在容器启动时安装RASP Agent，您需要在启动时添加以下参数。
	`docker --env JAVA_OPTIONS="-javaagent:/rasp/rasp.jar -Dmanager.key={manager.key}"`
	例如，您在启动容器时修改前的命令为 `docker -itd --name=test -P 镜像名` ，需要安装RASP Agent时启动容器执行的命令为 `docker -itd --env JAVA_OPTIONS="-javaagent:/rasp/rasp.jar -Dmanager.key={manager.key}" --name=test -P 镜像名` 。

如果不需要应用防护功能防护您的容器，您可以单击**卸载指南**页签，按照页面提供的操作步骤卸载RASP探针。

步骤二：查看告警事件

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**安全预防 > 应用防护**。
4. 在**应用防护**的**告警**页签，查看告警事件的相关信息。

   告警页签下以环图的形式展示接入应用防护后应用产生的行为以及应用受到攻击的统计情况。页面下方列表则展示了每一攻击行为的详细数据，包括攻击行为的类型、URL、行为数据以及该行为的处理方式等。

   ○ 查看应用行为统计

应用行为统计区域展示经过应用防护检测的应用行为以及其对应的分类，包括正常行为和攻击行为。

- 查看攻击统计

  攻击统计区域展示应用防护检测到的具有实际威胁的攻击行为以及其对应的攻击类型。

- 查看攻击详情

  攻击详细列表展示每一个攻击行为的具体情况。您可以在列表中查看攻击行为产生的时间、具体类型、URL、具体数据和该行为的处理方式。您也可以单击目标告警**操作**列的**查看**，在**详情**面板查看目标攻击行为的详情，包括漏洞的详情、请求详情和服务器的详情。

配置白名单放行特定请求

您可以通过配置白名单放行来自指定源IP的请求。针对满足规则的请求，安骑士不会产生告警，也不会阻断对应的操作。

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**安全预防 > 应用防护**。
4. 在**应用防护**的**白名单**页签，单击**配置白名单**。

   在**配置白名单**面板，参考以下步骤配置白名单的规则并选择生效应用。

   i. 在**规则名称**文本框输入白名单规则名称。

   ii. 在**源IP**设置需加白的攻击源IP列表。

   支持配置IP和IP网段，最多可以设置100个IP或IP网段。

   > **重要**
   >
   > 0.0.0.0/0表示放行所有IP地址的访问，请谨慎配置。

   iii. 在**请求路径**中配置需加白的IP访问应用的路径。

   支持通过以下类型配置请求路径：

   - **前缀匹配**：放行来自指定IP地址且访问地址前缀满足此处设置条件的请求。配置示例：`http://39.104.XX.XX:8080/`。
   - **后缀匹配**：放行来自指定IP地址且访问地址后缀满足此处设置条件的请求。配置示例：`/Vulns/file/io/read`。

   > **说明**
   >
   > 系统匹配时会忽略请求路径的查询字符串（QueryString）参数部分。例如，如果请求路径为 `http://127.0.XX.XX:8088/Vulns/file/io/read?path=/etc/passwd`，系统进行匹配时会自动忽略问号（?）及其后面的部分，即忽略 `?path=/etc/passwd`。

   iv. 在**检测类型**区域选择需要放行的检测类型，单击**下一步**。

   v. 选择白名单生效的应用，单击**确定**。

配置完成后，该白名单规则会对生效的应用下所有在线状态的RASP实例生效。

检测攻击类型说明

下表介绍应用防护可检测的攻击类型及相关防护建议。

攻击类型	说明	防护建议
JNI注入	JNI注入是一种通用的RASP（Runtime Application Self-Protection）绕过手段。当攻击者拿到代码执行权限后，可以通过Java Native函数去调用外部的恶意动态链接库，从而绕过Java层的安全防护，并隐匿具体的恶意行为。	您的服务器可能存在代码执行漏洞，请检查漏洞的位置并限制执行代码的功能。
SQL注入	SQL注入手段通过把SQL命令插入到页面请求或Web表单的查询字符串中，以达到欺骗服务器执行指定SQL语句的目的。它可以通过在Web表单中输入SQL语句，得到存在安全漏洞的网站上的数据。	SQL注入是由拼接SQL语句引起的。请尽可能使用预编译来处理传入的参数，或通过白名单和黑名单来限制拼接参数。
XXE	指XML外部实体注入漏洞（XML External Entity Injection）。当XML文件在引用外部实体时，通过构造恶意内容，可以导致任意文件读取，命令执行和内网攻击等不良后果。	请检查应用程序在解析XML时是否需要加载外部实体。如果不需要，请在XML解析配置中禁用外部实体。
恶意DNS查询	恶意DNS查询存在多种利用方式。攻击者极有可能通过DNS协议来突破内网的网络限制，从而将敏感信息带出内网，也可能通过DNS协议去探测内网系统是否存在SSRF、JNDI注入等漏洞。	恶意DNS查询是由服务器向用户控制的参数发送请求所引起的。请检查参数并通过白名单进行限制。
恶意反射调用	RASP自保护模块，禁止攻击者通过反射的方式去修改运行时RASP的相关数据。	您的服务器可能存在代码执行漏洞。请检查漏洞的位置并限制执行代码的功能。
恶意外连	SSRF（Server-side request forgery）服务器端请求伪造漏洞指的是攻击者通过构造由服务端发起的请求，对网站内部系统进行攻击。	SSRF是由服务器向用户传入的参数发送请求所引起的。请检查参数并通过白名单进行限制。
恶意文件读写	Java提供RandomAccessFile，用于文件读写操作。当使用该Class进行文件读写的时候，如果未对文件路径、文件内容进行限制，攻击者可能读取到系统敏感文件，也可能上传木马文件。	请检查文件读取和上传是否正常。如果出现异常，请检查函数代码，并通过黑名单进行限制。

恶意文件上传	对于网站提供的文件上传功能，如果未对上传文件的类型进行限制，攻击者可能通过上传木马文件来获取服务器的更大权限，从而造成严重危害。	请限制上传文件的类型，禁止上传具有执行权限的文件，如JSP。
命令执行	命令执行漏洞是指服务器没有对执行的命令进行过滤，用户可以随意执行系统命令。	通常远程命令执行是由Web Shell或服务器的危险代码引起的。请检查命令执行的位置。如果是Web Shell，请及时删除。如果是服务器的正常功能，则可以通过白名单限制执行的命令。
目录遍历	网站自身的配置缺陷可能会使得网站目录被任意浏览，导致隐私信息泄露。攻击者可以利用该信息对网站进行攻击。	请检查目录遍历操作是否正常。如果异常，请检查函数的代码，并通过黑名单对相关命令（如“./”和“../”）进行限制。
内存马注入	内存马是一种新兴的木马技术，攻击者通过一些特殊的技术手段将木马注入到内存中，可以有效绕过WAF和主机防御的检测。	您的服务器可能存在代码执行漏洞。请检查漏洞的位置并限制执行代码的功能。
任意文件读取	对于网站提供的文件下载和读取功能，如果是直接通过绝对路径或目录穿越符对文件进行读取和下载，没有相关文件路径的限制，那么，攻击者就可以利用这种方式获取敏感信息，对服务器进行攻击。	请检查文件读取操作是否正常。如果异常，请检查函数的代码，并使用黑名单对传入参数（如“./”和“../”）进行限制。
数据库弱口令	当数据库使用强度较低的密码时，攻击者可能通过暴力破解获取正确的数据库密码，从而达到窃取数据库数据、获取系统权限等目的。	请使用更复杂的密码。
线程注入	线程注入是一种通用的RASP绕过手段。当攻击者拿到代码执行权限后，可以通过新建线程的方式使RASP丢失掉运行环境的上下文，从而影响RASP的防御能力。	您的服务器可能存在代码执行漏洞。请检查漏洞的位置并限制执行代码的功能。
恶意Attach	Attach API是Java提供的动态修改字节码技术，该功能可以实现动态修改运行时应用的字节码。很多攻击者通过该手法进行Agent型内存马的注入，具有较高的欺骗性。	您的服务器可能存在代码执行漏洞。请检查漏洞的位置并限制执行代码的功能。
JNDI注入	当应用进行JNDI查询的时候，若查询的URL可以由攻击者控制，则攻击者可以使服务器去查询恶意的链接使得服务器加载一些恶意class，实现任意代码执行。	• 若该漏洞源于第三方组件，请及时进行组件版本升级。 • 若为自写JNDI查询代码，请对查询的URL进行限制，禁止一些危险协议的查询。

危险协议使用	若服务端进行访问的URL用户端可控，而应用本身又未对该URL的协议进行限制，那么攻击者可能通过file、netdoc等危险协议对服务器上的敏感文件进行读取。	请对URL可以访问的协议进行限制。
反序列化攻击	Java反序列是指把字符序列恢复为Java对象的过程，在对象生成过程中，若该对象包含一些危险度较高的代码，则攻击者可能通过控制生成对象的成员变量在对象进行反序列化的时候实现一些恶意攻击。	• 及时升级存在漏洞的组件版本。 • 若官方还未提供漏洞修复的组件版本，请暂时关闭该功能。
任意文件删除	对于网站提供的文件删除功能，如果是直接通过绝对路径或目录穿越符对文件进行读取和下载，没有相关文件路径的限制，那么，攻击者就可以利用这种方式获取敏感信息，对服务器进行攻击。	请检查文件删除操作是否正常。如果异常，请检查函数的代码，并使用黑名单对传入参数（如“./”和“../”）进行限制。
表达式注入	表达式组件提供了十分丰富的功能，支持在运行时查询和处理数据等，但很多表达式组件也提供了函数调用等权限较高的功能，如果未对这些功能做限制，而攻击者又能够控制表达式执行的内容，那么攻击者将很有可能通过表达式执行任意代码。	请对进入表达式的内容进行严格限制，禁止大部分Java函数的调用。若是第三方组件漏洞导致，请及时升级组件版本。
引擎注入	Java提供较多的第三方引擎组件（如rhino、Nashorn等JS引擎，velocity、freemarker等模板引擎），这些引擎通常提供了函数调用等权限较高的功能，如果对这些功能未做限制，而攻击者又能够控制引擎执行的内容，那么攻击者将很有可能通过引擎执行任意代码。	请对进入引擎文件的内容进行严格限制，禁止大部分Java函数的调用。若是第三方组件漏洞导致，请及时升级组件版本。
恶意Beans绑定	Java存在一些框架支持对应用运行时Beans的参数绑定，如果未对绑定Beans的类型进行限制，攻击者就可以通过对一些敏感Beans值的修改，破坏应用的运行，甚至造成执行任意代码。	请对可以绑定的Beans的类型进行限制，禁止对类似于Class、Classloader类型的Beans值进行修改。若是第三方组件漏洞导致，请及时升级组件版本。
恶意类加载	现阶段，很多0day、WebShell的利用均依赖于恶意类的加载，一旦恶意类加载成功，攻击者便可以通过恶意类的初始化来取得代码执行权限，从而进行一系列的恶意操作。	• 若恶意类的加载是通过WebShell控制，请及时删除WebShell。 • 若恶意类的加载是框架导致，请及时升级框架版本。

JSTL任意文件包含	JSP标准标签库（JSTL）是一个JSP标签集合，它封装了JSP应用的通用核心功能。当用户可控参数被直接拼接到JSTL标签中而未对该参数进行任何限制的情况下，攻击者可以构造特殊的攻击脚本造成任意文件读取、SSRF的攻击。	尽可能不要将用户可控参数直接拼接到JSTL标签上，如果必须这样做，请对该参数的内容进行严格的白名单控制。

3.4. 入侵防御

3.4.1. 病毒查杀

安骑士的病毒查杀设置功能提供自定义配置病毒查杀和网站后门查杀管理的服务。

病毒查杀

病毒查杀能够帮助您自动隔离常见网络病毒，包括主流木马病毒、勒索软件、挖矿病毒、DDoS木马等。所有支持自动隔离的病毒都经过了云盾安全专家的测试和验证，确保零误杀。

未开启自动隔离时，云盾安骑士以安全告警的形式向您展示在服务器上检测出的病毒，您需要在控制台手动处理。建议您开启病毒自动隔离，加固主机安全防线。

1. 登录Apsara Uni-manager运营控制台。
2. 在顶部菜单栏，单击**安全**，在**主机安全**区域，单击**安骑士**。

> 说明
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**入侵防御** > **病毒防御**。
4. 在**病毒查杀**页签下，单击**开始病毒扫描**。
5. 在弹出的对话框中，选中您要扫描的资产。
6. 单击**开始扫描**。
7. 在**病毒防御**页面，单击**实时防护**页签开关，开启病毒查拦截功能。

   开启病毒拦截后，安骑士将对检测出的主流病毒类型进行自动隔离，您可在安全告警处理页面**精准防御**类型告警列表中，查看被病毒查杀功能自动隔离掉的病毒。

网站后门查杀

1. 登录Apsara Uni-manager运营控制台。
2. 在顶部菜单栏，单击**安全**，在**主机安全**区域，单击**安骑士**。

> 说明
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**入侵防御** > **病毒防御**。

4. 配置对网站服务器网页目录进行检测和识别网站后门的检测范围。
   i. 在**网站后门查杀**区域，单击**管理**。
   ii. 选择哪些服务器需要进行网站后门查杀。
   iii. 单击**确定**，完成配置。

3.4.2. 网页防篡改

3.4.2.1. 概述

防篡改可实时监控网站目录并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容。

背景信息

网络攻击者通常会利用被攻击网站中存在的漏洞，通过在网页中植入非法暗链对网页内容进行篡改等方式，进行非法牟利或者恶意商业攻击等活动。网页被恶意篡改会影响用户正常访问网页内容，还可能会导致严重的经济损失、品牌损失甚至是政治风险。

网页防篡改支持将Linux和Windows服务器进程加入白名单，可实现网站防护文件实时更新。

防护原理

云盾Agent通过自动化采集获取被保护的服务器中写防护目录下文件的进程列表，实时识别异常进程和异常文件变动，并对异常文件的进程进行阻断。

您可以在云盾主机安全防篡改页面的告警列表中，查看被云盾检测出的异常文件变动告警、异常进程和该进程尝试写文件的次数。如果您确定该异常文件相关的进程是正常的业务结果，可以将该进程添加到白名单中。防篡改功能不再对加入到白名单中的进程进行拦截。对于新闻、教育类网站需要频繁修改网站内容的场景，可有效避免需要频繁开启和关闭防篡改功能的问题。

防篡改支持的系统内核版本

OS	支持的OS版本	支持的内核（Kernel）版本
Windows	Windows Server 2008及以上版本	所有版本
CentOS	6.5、6.6、6.7、6.8、6.9、6.10、7.0、7.1、7.2、7.3、7.4、7.5、7.6	• 2.6.32-x • 3.10.0-x

Ubuntu	14、16、18	• 3.13.0-32-generic • 3.13.0-86-generic • 4.4.0-62-generic • 4.4.0-63-generic • 4.4.0-93-generic • 4.4.0-151-generic • 4.4.0-117-generic • 4.15.0-23-generic • 4.15.0-42-generic • 4.15.0-45-generic • 4.15.0-52-generic

> 说明
>
> - 目前，防篡改支持的服务器kernel版本有限，不在支持范围内的服务器将无法使用防篡改进程白名单功能。请确认您的服务器kernel版本是否在上述支持列表覆盖范围内。如果不在支持范围内，需要手动升级kernel到支持列表里的版本，才能使用进程加白名单的功能。
> - 升级服务器kernel前请使用快照备份您的资产数据。

3.4.2.2. 创建网页防篡改保护

主机安全支持对主机开启网页防篡改防护，全面保护您网站的安全。

限制条件

- 每台服务器最多可添加10个防护目录。
- Windows系统单个防护目录大小不超过20 GB；单个防护目录下的文件夹不超过2000个；防护目录文件夹层级不超过20个；单文件大小不超过3 MB。
- Linux系统单个防护目录大小不超过20 GB；单个防护目录下的文件夹不超过3000个；防护目录文件夹层级不超过20个；单文件大小不超过3 MB。
- 建议您开启防护前检查文件夹目录层级、文件夹个数和防护目录大小是否超过限制。
- 建议您排除LOG、PNG、JPG、MP4、AVI、MP3等无需进行防护的文件类型，多个文件类型之间用半角分号（;）隔开。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在顶部菜单栏，单击**安全**，在**主机安全**区域，单击**安骑士**。

> 说明
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**入侵防御 > 防篡改**。

4. 在防篡改页面单击创建网页防篡改。
5. 在创建网页防篡改对话框中选中目标服务器。

6. 单击下一步，进入添加防护目录页签。
7. 在添加防护目录页签中，完成以下配置。

选择防护模式。可选白名单模式或黑名单模式。白名单模式下，会对添加的防护目录和文件类型进行保护；黑名单模式下，会防护目录下所有未排除的子目录、文件类型和指定文件。默认开启白名单模式。

- 白名单模式配置：

配置项	描述
防护目录	手动输入该服务器下需要开启防篡改保护的目录地址。 说明 Linux服务器和Windows服务器防护目录地址的格式可能会有区别，请根据页面提示输入正确的格式。
防护文件类型	单击下拉列表，选择该目录中需要防护的文件类型，例如：JS、HTML、XML、JPG等。
本地备份目录	展示防护目录的默认备份存储路径。 云盾安全中心为您指定的默认备份目录为/usr/local/aegis/bak（Linux服务器）和C:\Program Files (x86)\Alibaba\Aegis\bak（Windows服务器），您可手动修改默认的备份路径。

- **黑名单防护模式：**

配置项	描述
防护目录	手动输入该服务器下需要开启防篡改保护的目录地址。
排除子目录	手动输入无需开启网页防篡改的子目录地址。 单击**添加子目录**，支持添加多个子目录。 添加排除子目录后，云盾安全中心将不会对该子目录中的文件进行防护。
排除文件类型	选择无需进行网页防篡改检测的文件格式。 可选值包含log、txt、ldb。 选择排除文件类型后，云盾安全中心将不会对该防护目录下该类型的文件进行防护。
排除指定文件	手动输入无需开启网页防篡改的文件目录地址。 单击**添加文件**，支持添加多个文件。 输入指定文件后，云盾安全中心将不会对该指定文件进行防护。

本地备份目录	展示防护目录的默认备份存储路径。 云盾安全中心为您指定的默认备份目录为/usr/local/aegis/bak（Linux服务器）和C:\Program Files (x86)\Alibaba\Aegis\bak（Windows服务器），您可手动修改默认的备份路径。

8. 单击**开启防护**，完成添加服务器和目录的操作。

   添加服务器完成后，该服务器将显示在**网页防篡改**页面的防护服务器列表中。

   > **说明**
   >
   > 添加服务器后，服务器的网页防篡改防护是**默认关闭**状态的。您需要在**网页防篡改**页面**开启**目标服务器的防护状态。

9. 在**防篡改**页面，单击**防护管理**页签，打开目标服务器**防护状态**开关，为该服务器开启防护服务。

   > **说明**
   >
   > 添加服务器后，服务器的网页防篡改防护是**默认关闭**状态的。您需要在**网页防篡改**列表中开启目标服务器的防护状态。

   启动成功后服务状态将会显示为**正在运行**。

   > **说明**
   >
   > 当防护服务状态为**异常**时，在目标服务器服务状态栏单击**异常**，显示异常状态的详细原因并单击**重试**。

后续操作

为服务器开启网页防篡改保护后，您可在**安全告警处理**页面，筛选网页防篡改类型，查看云盾安全中心为您检测到的网页篡改事件和告警信息。

> 说明
>
> 配置完成防护目录后网页防篡改未立即生效，并且此时仍然可以对该防护目录写入文件。这种情况下，您需在**防护管理**列表中对该目录所在的服务器关闭**防护状态**开关，然后重新打开**防护状态**开关。

防护异常状态处理

服务状态	说明	建议
启动中	网页防篡改防护状态正在开启。	首次开启防护时，目标主机的服务状态将会显示为**启动中**。请耐心等待数秒。
正在运行	防护状态已成功开启，并正常运行中。	无。
异常	防护开启异常。	在目标主机服务状态栏单击**异常**，查看发生异常的原因并重试。
未启动	防护状态为未开启。	需将防护状态设置为**开**。

3.4.2.3. 查看防护状态

本文介绍了如何查看您资产的网页防篡改防护状态。

背景信息

网页防篡改功能可实时监控网站目录文件的变化并对异常的文件变动事件进行拦截。您可以在云盾控制台**主机安全 > 入侵防护 > 防篡改**页面查看到安骑士为您检测到的网页防篡改防护状态和信息，包括：

- 网页防篡改统计数据总览

您可以在统计数据总览模块中查看当天以及最近15天内发生变动的文件总数、已被防护的服务器数量和目录数量。

- 防篡改防护文件类型分布数据

防护文件类型包括TXT、PNG、MSI、ZIP等文件类型。您也可以手动添加需要防护的其他文件类型。

> 说明 目前防护文件类型不受限制，所有文件类型都支持网页防篡改防护。

- 文件变动数Top 5

  该模块展示了最近15天内检测到的变动次数排名前5的文件名称和文件所在路径。

- 网页防篡改告警详情列表。

该列表展示了网页防篡改功能为您资产拦截到的所有异常文件变动及其详细信息，包括告警等级、告警名称、受影响资产、异常变动文件的路径、防御状态等信息。

> **说明**
>
> - 如果告警尝试次数（进程写文件次数）超过100次，建议您及时关注并处理该告警。
> - 目前告警等级只有**中危**等级。
> - 防御状态只有**已防御**一种状态，表示网页防篡改功能在检测到异常文件变动事件时，已及时为您拦截执行该异常变动的进程。

3.4.3. 应用白名单

应用白名单可防止服务器上有未经过认证或授权的程序运行，为您提供可信的资产运行环境。本文介绍如何使用应用白名单功能。

创建应用白名单策略

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**入侵防御 > 应用白名单**。
4. 在**应用白名单**页面的**策略管理**页签，单击**创建策略**。
5. 在**创建应用白名单策略**面板，配置应用白名单策略，单击**创建策略**。

配置项	描述
策略名称	输入策略名称。
策略模式	选择告警模式或观察模式。
策略内容	设置策略内容。你可以单击对应策略内容旁边的**设置**，在对应面板设置策略内容。
选择资产	选择策略生效的资产。

在应用白名单策略列表，还支持以下操作：

- 编辑策略：定位到目标策略，在**操作**列，单击**编辑策略**。
- 启用或停用策略：选中目标策略， 在策略列表下方，单击**启用/停用**。
- 删除策略：选中目标策略， 在策略列表下方，单击**删除**。

查看应用白名单策略的服务器

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**入侵防御 > 应用白名单**。
4. 在**应用白名单**页面的**生效服务器**页签，查看策略生效的服务器。

   支持通过策略启用、停用、策略模式以及资产状态筛选目标服务器。同时支持服务器组、防护中等分组查看生效服务器。

   在生效服务器列表，支持以下操作：

   - 查看生效服务器策略详情：定位到目标服务器，在**操作**列，单击**查看详情**。
   - 启用或停用策略：选中目标服务器，在服务器列表下，单击**启用/停用**。
   - 解绑策略：选中目标服务器，在服务器列表下，选择**更多操作 > 解绑操作**。

创建采集任务

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**入侵防御 > 应用白名单**。
4. 在**应用白名单**页面的**知识库**页签，单击**进程采集**。
5. 在**进程采集**页签，单击**创建采集任务**。
6. 在**创建进程采集任务**面板，配置输入名称并选择观察截止时间和资产，单击**确定**。

   支持在采集任务列表，重新扫描资产以及查看任务详情。

自定义进程组

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**入侵防御 > 应用白名单**。
4. 在**应用白名单**页面的**知识库**页签，单击**自定义进程组**子页签。
5. 在**自定义进程组**页签，单击**创建自定义进程组**。
6. 在**创建自定义进程组**对话框，输入进程组名称，单击**创建**。

   创建完成后，您还可以修改进程组名称、删除进程组或为进程组添加MD5值。

3.4.4. 攻击分析

本文介绍了攻击分析的统计信息，包括攻击次数、攻击类型分布、攻击来源TOP 5、被攻击资产TOP 5和攻击详情列表。

背景信息

安骑士检测到基础攻击后会自动进行拦截和处理，并在**攻击分析**页面展示攻击相关的数据，针对这些攻击无需做任何处理。如果涉及风险较高的攻击事件，可对指定攻击来源的地址进行进一步分析或排查。建议根据自身业务需求，考虑从防火墙和业务安全方面构建更精细化的纵深防护体系。

在**攻击分析**页面，您可以设置时间范围查看以下攻击分析结果。您可以快速查看当天、最近7天或最近15天内的攻击分析结果，也可以选择**自定义时间**，查看最近任意时间范围的攻击分析结果。

资产受到的攻击详情，具体包括以下内容：

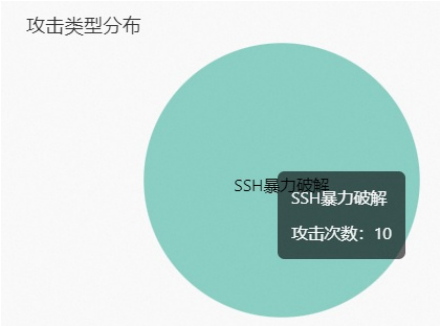
- 攻击次数：指定时间范围内资产被攻击的总次数。
- 攻击类型分布：攻击类型和对应的攻击次数。
- 攻击来源TOP 5：攻击次数排名前5位的攻击来源IP地址。
- 被攻击资产TOP 5：被攻击次数排名前5位的资产信息。
- 攻击详情列表：所有攻击事件的详细信息，包含攻击发生的时间、攻击源IP地址、被攻击的资产信息、攻击类型和攻击状态。

攻击次数

支持在**攻击次数**区域查看指定时间范围内资产被攻击的总次数曲线图和攻击次数峰谷值。鼠标悬浮在曲线图上可展示攻击发生的日期、时间和次数值。

攻击类型分布

支持在**攻击类型分布**区域，查看攻击类型名称和该类型攻击发生的总次数。



攻击来源TOP 5

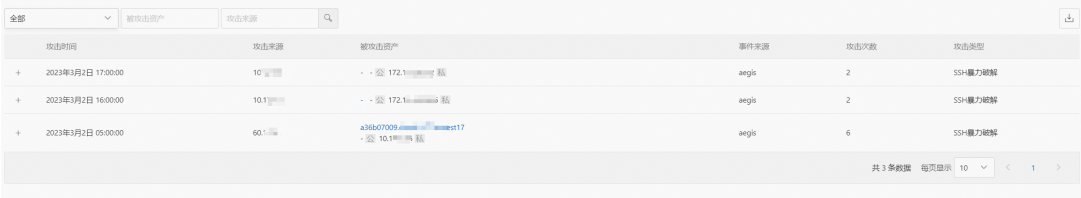
支持在**攻击来源TOP 5**区域，查看攻击次数排名前五的攻击来源IP地址及其对应的攻击次数。

被攻击资产TOP 5

支持在**被攻击资产TOP 5**区域，查看您资产中被攻击次数排名前5的资产公网IP地址及其被攻击次数。

攻击详情列表

支持在攻击详情列表中查看您资产受到的攻击详细信息，包含攻击发生的时间、攻击源IP地址、被攻击的资产信息、攻击类型、攻击方法和攻击状态。



在攻击详情列表，还支持以下操作：

- 搜索查看攻击事件

  支持通过攻击详情列表上方搜索条件，筛选指定的攻击类型、被攻击资产、攻击来源，搜索目标的攻击事件并查看其详细信息。

- 查看被攻击资产信息

  鼠标移动到**被攻击资产**名称处可查看该资产的基本信息。

- 导出攻击事件列表

单击攻击事件列表左上方的

图标，将安骑士检测出的攻击事件统一导出并保存到本地。导出的文件为Excel格式。

3.4.5. 安全告警

3.4.5.1. 安全告警概述

主机安全支持敏感文件篡改、进程异常行为、网站后门、异常登录、恶意进程等安全告警类型，通过全面的安全告警类型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。

云盾安全中心可对您已开启的告警防御能力提供总览数据，帮助您快速了解已开启和未开启的防御项目。您可在**安全告警**页面，查看安全告警的统计和防御项目的信息。

安全告警类型列表

防御项目包含的内容如下所示：

告警名称	告警说明
异常登录	检测服务器上的异常登录行为。通过设置合法登录IP、时间及账号，对于例外的登录行为进行告警。支持手动添加和自动更新常用登录地，对指定资产的异地登录行为进行告警。 可检测以下子项： • ECS非合法IP登录 • ECS在非常用地登录 • ECS登录后执行异常指令序列（SSH） • ECS被暴力破解成功（SSH）
应用白名单	通过在白名单策略中设置需要重点防御的服务器应用，检测服务器中是否存在可疑或恶意进程，并对不在白名单中的进程进行告警提示。
网站后门	使用自主查杀引擎检测常见后门文件，支持定期查杀和实时防护，并提供一键隔离功能： • Web目录中文件发生变动会触发动态检测，每日凌晨扫描整个Web目录进行静态检测。 • 支持针对网站后门检测的资产范围配置。 • 对发现的木马文件支持隔离、恢复和忽略。
异常网络连接	检测网络显示断开或不正常的网络连接状态。
精准防御	对主流勒索病毒、DDoS木马、挖矿和木马程序、恶意程序、后门程序和蠕虫病毒等类型进行防御。
异常账号	检测非合法的登录账号。
持久化后门	检测服务器上存在的可疑计划任务，对攻击者持久入侵用户服务器的威胁行为进行告警。

进程异常行为	检测资产中是否存在超出正常执行流程的行为。
恶意软件	检测模型发现您的服务器上正在执行恶意的软件。
敏感文件篡改	检测是否存在对服务器中的敏感文件进行恶意修改，包含Linux共享库文件预加载配置文件的可疑篡改等行为。
恶意脚本	检测资产的系统功能是否受到恶意脚本的攻击或篡改，对可能的恶意脚本攻击行为进行告警提示。恶意脚本分为有文件脚本和无文件脚本。攻击者在拿到服务器权限后，使用脚本作为载体来达到进一步攻击利用的目的。利用方式包括植入挖矿程序、添加系统后门、添加系统账户等操作。恶意脚本的语言主要包括Bash、Python、Perl、PowerShell、BAT、VBS。
漏洞利用	检测模型发现您的服务器上运行了漏洞利用程序，漏洞利用程序用于攻击或尝试攻击操作系统、应用程序的已知漏洞，用于实现提权、逃逸、任意代码执行等目的。

3.4.5.2. 查看和处理安全告警

您可以在安骑士查看和处理已检测出的告警事件。

背景信息

云盾检测出安全告警事件后，会展示相关告警信息。如果告警事件未被处理，会展示在**安全告警**页面的**待处理**告警列表中。告警事件处理完成后，将从**待处理**告警状态转化为**已处理**。

> **说明**
>
> 在**安全告警**页面为您一直保留**待处理**告警和**已处理**告警记录。默认展示**待处理**告警记录。

查看告警事件

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**入侵防御** > **安全告警**。
4. 在安全告警列表中，查看或搜索所有检测到的入侵和威胁告警及其详细信息。

处理告警事件

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**入侵防御** > **安全告警**。
4. 在**安全告警**页面，定位到目标告警事件，单击**操作**栏的**处理**，对不同告警事件执行相应的处理后单击**立即处理**。

> **说明**
>
> 如果告警事件包含多个关联异常，单击**处理**，会打开该告警事件的详情页面，您可对不同的异常事件分别进行处理。

- **忽略**：忽略本次告警，该告警状态将变为**已处理**，后续不会再对该事件进行告警。
- **加白名单**：如果告警为误报，您可以将本次告警加入白名单。告警加入白名单后该告警状态将变为**已处理**，后续安骑士不会再对该事件进行告警。您可以在**已处理**列表中定位到该事件对其进行**取消白名单**的操作。

  > **说明**
  >
  > 告警误报是指系统对正常程序进行告警。常见的告警误报有**对外异常TCP发包可疑进程**，提示您服务器上有进程在对其他设备发起了疑似扫描行为。

- **同时处理相同告警**：对多个告警事件进行批量处理。批量处理告警事件前，请详细了解告警事件的信息。

5. **可选**：如果您已确认一个或多个告警事件需要忽略或为误报，可在**安全告警**页面，选中一个或多个告警事件，直接进行**忽略本次**或**加白名单**处理。

导出告警事件

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**入侵防御** > **安全告警**。
4. 单击**安全告警**页面危险等级栏 图标，导出报表。

   报表导出完成后，安全告警页面右上角会提示**导出完成**。
5. 在**安全告警处理**页面右上角**导出完成**对话框中，单击**下载**。
   安全告警事件文件会下载到本地。

3.4.5.3. 查看告警自动化关联分析

安骑士支持告警自动化关联分析。您可在安全告警列表页面单击单个告警事件名称进入告警自动关联分析页面，查看和处理告警事件所有关联的异常情况并进行攻击自动溯源，帮助您对告警事件进行全方位分析和便捷处理。

背景信息

- 告警自动关联分析功能可对相关的异常事件进行实时自动化关联，挖掘出潜藏的入侵威胁。
- 告警自动化关联以告警发生的时间顺序聚合成关联的告警，帮助您更便捷地分析和处理告警事件，提升您系统的应急响应机制。
- 告警自动化关联分析聚合后的告警以 图标标识。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**入侵防御 > 安全告警**。
4. 在安全告警列表中，单击目标**告警名称**打开告警事件详情面板。
5. 在告警事件详情面板，查看告警事件的详细信息、关联的异常事件和对告警的异常事件进行处理。
   - 查看告警详细信息

     您可查看受该告警事件影响的资产信息、告警首次发生或最新发生时间、关联异常事件的详情。
   - 查看受影响资产

     鼠标悬停在**受影响资产**名称上，会弹出对应资产的详情页面，方便您集中查看该资产的全部告警信息、漏洞信息、基线检查漏洞和资产指纹等信息。
   - 查看和处理**关联异常**

     您可在**关联异常**区域查看该告警事件关联的所有异常情况的详细信息和建议方案。
     - 单击各关联异常区域右侧的**备注**，可为该关联异常事件添加备注信息。
     - 单击备注信息右侧的 × 图标，即可删除备注信息。

3.4.5.4. 文件隔离箱

安骑士可对检测到的威胁文件进行隔离处理，被成功隔离的文件会添加到安全告警处理页面的文件隔离箱中。被成功隔离的文件可在30天内进行一键恢复，且隔离30天后系统将自动清除被隔离文件。本文介绍了如何查看隔离文件和解除文件隔离。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**入侵防御 > 安全告警**。
4. 在**安全告警**页面单击右上角**文件隔离箱**。

   您可在**文件隔离箱**进行以下操作：
   - 在文件隔离箱列表中可以查看被隔离的文件主机地址、文件路径、状态和修改时间等信息。
   - 单击文件隔离箱页面右侧**操作**栏的**恢复**，可以将指定的被隔离文件从文件隔离箱中移除。恢复的文件将重新回到安全告警列表中。

3.4.5.5. 安全告警设置

安骑士的安全告警设置支持手动维护常用登录地和Web目录，并支持高级登录报警功能。

背景信息

安骑士提供高级登录报警功能，支持配置更精细的异常登录检测，例如设置合法登录的IP、时间、账号。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，在**主机安全**区域，单击**安骑士**。
3. 在左侧导航栏，选择**入侵防御 > 安全告警**。
4. 单击页面右上角**安全告警设置**。

   选择相应的功能页签，完成以下配置：

   - **添加常用登录地**

     a. 单击**常用登录地**右侧的**管理**按钮。

     b. 选中要添加的常用登录地点，然后选择添加应用的服务器。

     c. 单击**确定**，完成添加。

     安骑士支持**编辑**和**删除**已成功添加的常用登录地。

     - 单击目标常用登录地右侧的**编辑**，修改该登录地的生效服务器。
     - 单击目标常用登录地右侧的**删除**，删除该常用登录地配置。

   - **配置高级登录报警**

     > **说明**
     >
     > 配置高级登录告警，可进一步指定常用的登录IP、时间段和账号。配置完成后，安骑士会对指定外的登录情形进行告警。以下功能的操作类似**常用登录地**配置，可参考上文进行添加、编辑、删除。

     - 单击**常用登录IP**右侧的切换开关，打开或关闭登录IP检查，开启后通过非指定IP登录会触发报警。
     - 单击**常用登录时间**右侧的切换开关，打开或关闭登录时间检查，开启后在非指定时间登录会触发报警。
     - 单击**常用账号**右侧的切换开关，打开或关闭登录账号检查，开启后使用非指定账号登录会触发报警。

   - **自定义Web目录**

     安骑士会自动检测您服务器资产中的Web目录，并进行动态检测和静态扫描；您也可以手动添加服务器中的其它Web目录进行检测扫描。

     a. 单击**Web目录定义**右侧的**管理**。

     b. 输入一个合法的Web路径，然后选中生效服务器，该路径将被添加到扫描路径的服务器。

     > **说明**
     >
     > 出于性能效率考虑，不支持直接添加root目录作为Web目录。

     c. 单击**确定**，完成添加。

3.5. 日志检索

3.5.1. 日志检索介绍

云主机安全提供主机日志检索功能，将散落在专有云各系统中的日志集中管理，便于您在出现主机问题时一站式搜索定位问题根源。

支持180天以内的日志存储，并提供30天以内的日志查询。

功能特性

日志检索功能具备以下特性：

- **一站式日志检索平台**，集中查询专有云各产品日志，单一接口，便于问题溯源。
- **日志功能的SaaS化**，无需进行额外安装部署，即可查询所有云环境中的服务器日志。
- 支持TB级数据检索，以及50个维度的数据逻辑（布尔表达式）组合，可以秒级展示日志全文检索结果。
- 支持丰富的主机日志源。
- 支持日志投递，允许您将安全日志导入到日志服务做进一步分析。

应用场景

日志检索帮助您实现以下需求：

- **安全事件分析**：主机发生安全事件后，通过日志功能进行调查，评估资产受损范围和影响。
- **操作审计**：对主机的操作日志进行审计，对高危操作和严重问题进行细粒度排查。

可检索日志类型

表 1. 日志源

日志源	说明
登录流水	系统登录成功的日志记录。
进程快照	某一时刻主机上的进程运行信息。
端口监听快照	某一时刻主机上的监听端口信息。
账号快照	某一时刻主机上的账号登录信息。
进程启动日志	主机上进程启动的相关信息。
网络连接日志	主机对外主动连接的日志。

3.5.2. 查询日志

本文介绍如何搜索和查看主机日志。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**主机安全 > 安骑士**。在**安骑士**授权页面，选择**地域**并单击**角色授权访问**。

> 说明
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，单击**日志检索**。
4. 设置搜索条件。

搜索项	说明
请选择日志源	支持的日志源，具体内容请参见日志源。
请选择字段	各日志源支持的字段，具体内容请参见日志源。
关键字	需要搜索的字段具体关键字。
语法逻辑	等于。
+	在一个搜索条件（一个日志源）下增加多个逻辑判断。
增加一组	增加多个搜索条件（不同的日志源）。

5. 单击**搜索**，查看搜索结果。
   - **重置**：如果不需要原来设置的搜索条件，单击**重置**，搜索条件回到初始状态。
   - **保存搜索逻辑**：如果以后需要重用这个搜索条件，单击**保存搜索逻辑**进行保存。
   - **已保存的搜索**：如果需要执行以前保存的搜索条件，单击**已保存的搜索**，选择已有的搜索条件执行。

3.5.3. 各日志源字段说明

本文介绍了日志检索功能可以采集并供检索的原始日志类型和字段说明。

日志检索功能支持您查询下表列述的日志源。您可以单击一个日志源查看其支持的字段信息。

日志源	说明
登录流水	系统登录成功的日志记录。
进程快照	某一时刻主机上的进程运行信息。
端口监听快照	某一时刻主机上的监听端口信息。
账号快照	某一时刻主机上的账号登录信息。
进程启动日志	主机上进程启动的相关信息。

网络连接日志	主机对外主动连接的日志。

登录流水

登录流水查询支持下表描述的字段。

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
warn_ip	string	登录来源IP
warn_port	string	登录端口
warn_user	string	登录用户名
warn_type	string	登录类型
warn_count	string	登录次数

进程启动日志

进程启动日志查询支持下表描述的字段。

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
pid	string	进程ID
groupname	string	用户组
ppid	string	父进程ID
uid	string	用户ID
username	string	用户名
filename	string	文件名
pfilename	string	父进程文件名
cmdline	string	命令行
filepath	string	进程路径
pfilepath	string	父进程路径

端口监听快照

端口监听快照查询支持下表描述的字段。

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
src_port	string	监听端口
src_ip	string	监听IP
proc_path	string	进程路径
pid	string	进程ID
proc_name	string	进程名
proto	string	协议

账号快照

账号快照查询支持下表描述的字段。

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
perm	string	是否拥有root权限
home_dir	string	home目录
warn_time	string	密码到期提醒时间
groups	string	用户属于的组
login_ip	string	最后一次登录的IP地址
last_chg	string	密码最后修改时间
shell	string	Linux的shell命令
domain	string	Windows域
tty	string	登录的终端
account_expire	string	账号超期时间
passwd_expire	string	密码超期时间
last_logon	string	最后登录时间

user	string	用户
status	string	用户状态： • 0表示禁用 • 1表示正常

进程快照

进程快照查询支持下表描述的字段。

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
path	string	进程路径
start_time	string	进程启动时间
uid	string	用户ID
cmdline	string	命令行
pname	string	父进程名
name	string	进程名
pid	string	进程ID
user	string	用户名
md5	string	进程文件MD5值，超过1 MB不计算

网络连接日志

网络连接日志查询支持下表描述的字段。

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
src_ip	string	源IP
src_port	string	源端口
proc_path	string	进程路径
dst_port	string	目标端口

proc_name	string	进程名
dst_ip	string	目标IP
status	string	状态

3.5.4. 语法逻辑说明

日志检索支持多条件逻辑检索，您可以在一个搜索条件（一个日志源）下增加多个判断逻辑，也可以对多个搜索条件（不同的日志源）进行逻辑组合。本文介绍了日志检索支持的语法逻辑，也列举了部分用例，帮助您理解和使用。

日志检索支持下表中列举的语法逻辑。 表 1. 语法逻辑说明

逻辑名称	描述
and	双目运算符。 形式为 `query 1 and query 2` ，搜索结果展示 `query 1` 和 `query 2` 查询结果的交集。 说明 如果多个单词间没有语法关键词，默认是and的关系。
or	双目运算符。 形式为 `query 1 or query 2` ，搜索结果展示 `query 1` 和 `query 2` 查询结果的并集。
not	双目运算符。 形式为 `query 1 not query 2` ，搜索结果展示符合 `query 1` 并且不符合 `query 2` 的结果，相当于 `query 1 - query 2` 。 说明 如果只有 `not query 1` ，那么表示从全部日志中选取不包含 `query 1` 的结果。

3.6. 主机设置

3.6.1. 安装客户端

用户需要监控安骑士资产的安全，需要先在服务器上安装云安全中心客户端。本文介绍了如何通过安骑士设置选项，安装云安全中心客户端。

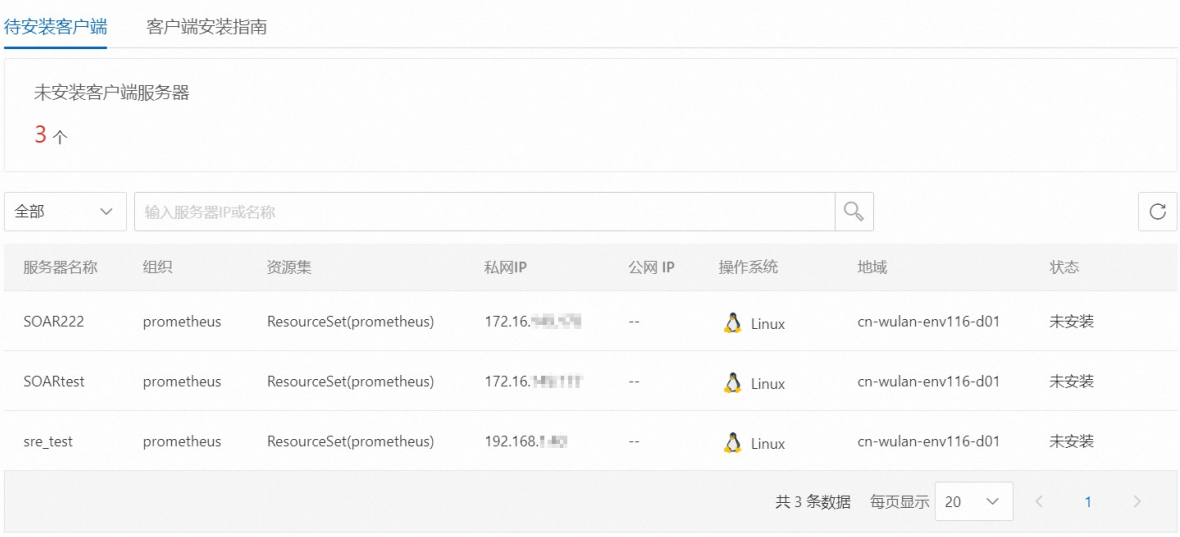
操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**主机安全 > 安骑士**。在**安骑士**授权页面，选择地域并单击**角色授权访问**。

> **说明**
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**主机设置 > 安装客户端**。
4. **可选：**单击**待安装客户端**页签，查看未安装客户端的服务器数量及其列表信息。

   您可以通过选择服务器操作系统类型、输入服务器IP或名称进行搜索，从而快速定位到目标服务器。



5. 单击**客户端安装指南**页签，安装客户端。
   - 命令行安装
     - **云内部署**
       a. 在**命令行安装**页签，定位到用户的服务器操作系统，单击对应的**复制命令**。

       > **说明**
       >
       > 如果没有找到对应的服务器操作系统安装命令，用户可以单击**新增安装命令**，选择**组织**、**资源集**、**客户端类型**后，单击**复制命令**。

       b. 在您的服务器执行该命令。

       c. 单击**验证安装结果**页签，根据服务器操作系统，复制验证命令，进行验证。

- **云外部署**

  > **重要**
  >
  > 安装客户端前请确认授权点数充足，且目标服务器到安骑士服务端域名解析正确。用户可以单击查看域名解析、查看授权信息，查看对应信息。

  a. 单击**供货商管理**，在**资产管理**页面，单击**供应商**。

  b. 单击**创建供应商**，填写**供应商名称**后，单击**确定**。

  c. 回到**客户端安装**页面，在**客户端安装指南**页签，单击**命令行安装**。

  d. 在**云外部署**区域，找到新增的供货商，单击新增安装命令，完成**组织**、**资源集**、**客户端类型**、**生效时间**、**区域(region)**、**机房(AZone)**、**绑定分组**的配置。

  e. 单击对应的**复制命令**，在您的服务器执行该命令。

  f. 单击**验证安装结果**页签，根据服务器操作系统，复制验证命令，进行验证。

- **镜像安装**

  > **重要**
  >
  > 安装客户端前请确认授权点数充足，且目标服务器到安骑士服务端域名解析正确。用户可以单击查看域名解析、查看授权信息，查看对应信息。

  a. 在**镜像安装**页签，根据控制台提示，安装客户端。

b. 单击**验证安装结果**页签，根据服务器操作系统，复制验证命令，进行验证。

3.6.2. 管理防护模式

本文介绍了如何管理云主机的防护模式，使服务器更高效、更安全。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**主机安全 > 安骑士**。在**安骑士**授权页面，选择**地域**并单击**角色授权访问**。

> **说明**
>
> 用户可以在控制台顶部菜单栏，选择组织、资源集、region，支持选择到二级组织及用户的资源集。

3. 在左侧导航栏，选择**主机设置 > 防护模式**。
4. 在**防护模式**页面，管理防护模式。
   - **防护模式管理**：支持管理高级防护模式、重大活动保护模式。为服务器选择适合的防护模式，更高效、更安全。
   - **自保护管理**：主动拦截恶意的卸载行为，保障主机防护机制的稳定运转。重要业务请使用支持自保护的操作系统，以免客户端被恶意破坏后服务器失去保护，造成安全隐患；关闭自保护需要半小时。

4.云盾系统配置

4.1. 登录Apsara Uni-manager运营控制台

本文主要向您介绍如何登录Apsara Uni-manager运营控制台。

前提条件

- 登录Apsara Uni-manager运营控制台前，确认您已从部署人员处获取Apsara Uni-manager运营控制台的服务域名地址。
- 推荐使用Chrome浏览器。

操作步骤

1. 在浏览器地址栏中，输入Apsara Uni-manager运营控制台的服务域名地址，按回车键。
2. 输入正确的用户名及密码。

   请向运营管理员获取登录控制台的用户名和密码。

   > 说明 首次登录Apsara Uni-manager运营控制台时，需要修改登录用户名的密码，请按照提示完成密码修改。为提高安全性，密码长度必须为10~32位，且至少包含以下两种类型：
   >
   > - 英文大写或小写字母（A~Z、a~z）
   > - 阿拉伯数字（0~9）
   > - 特殊符号（感叹号（!）、at（@）、井号（#）、美元符号（$）、百分号（%）等）

3. 单击**账号登录**。
4. 如果账号已激活MFA多因素认证，请根据以下两种情况进行操作：
   - 管理员强制开启MFA后的首次登录：
     a. 在绑定虚拟MFA设备页面中，按页面提示步骤绑定MFA设备。
     b. 按照步骤2重新输入账号和密码，单击**账号登录**。
     c. 输入6位MFA码后单击**认证**。
   - 您已开启并绑定MFA：

     输入6位MFA码后单击**认证**。

     > 说明 绑定并开启MFA的操作请参见《Apsara Uni-manager运营控制台用户指南》中的《绑定并开启虚拟MFA设备》章节。

4.2. 系统监控

通过监控总览，用户可以监控接入的云产品，及时发现异常产品，便于产品运维。本文介绍如何查看监控总览。

1. 登录Apsara Uni-manager运营控制台。

2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 系统配置**。在**系统配置**授权页面，选择**地域**并单击**角色授权访问**。
3. 在左侧导航栏，单击**系统监控**。
4. 在系统监控页面，查看监控总览和云产品监控数据。
   - 在**监控总览**页签，查看监控总览信息。

     - **监控数据总览：支持查看监控产品总数、异常产品总数、监控项总数、异常项总数等数据。**
     - **云产品监控数据：支持查看所有已接入的云产品的监控项数量、异常数、产品状态数据。**
   - 在云产品页签，查看各产品监控数据。
     - **支持监控的云产品包括：安骑士、基础服务、SOAR安全编排自动化响应、第三方产品对接平台、加密服务、威胁情报、智能分析平台、升级中心、可信计算、网络检测响应、SOC云安全管理中、密钥管理服务心、密码服务平台、密钥管理服务(底座版)、容器安全等。**

- 支持监控的内容：接入云产品的所有服务。以安骑士为例，介绍云产品监控的具体内容。

  单击**安骑士**页签，查看使用安骑士的所有服务。

  - 用户可以通过服务列表上的搜索框，根据服务状态和服务名称，搜索对应服务。
  - 在服务卡片区域，查看服务状态、CPU使用率、memo使用率、负载数、tcp连接数、进程数、nginx次数等数据。

- 单击服务卡片区域，查看服务监控详情。

监控项	说明
基础监控	用户可以设置监控时间、监控视角。 ■ 监控时间：支持监控3小时、6小时、12小时、1天、2天、自定义时间段。 用户可以单击图标，手动刷新监控数据，也可以打开自动刷新开关，自动刷新监控数据。 ■ 监控视角：支持集群视角、单机视角。
中间件	
健康检查	基于TCP、HTTP等探测方式，检查应用中所有主机的健康状态，以集群视角进行展示。

4.3. 规则运营

4.3.1. 云防火墙IPS规则运营

云防火墙内置IPS规则，用户可以根据自身的业务需求和网络环境自定义IPS规则，监控云防火墙运营状态。本文介绍如何添加和管理云防火墙的IPS规则。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 系统配置**。在**系统配置**授权页面，选择**地域**并单击**角色授权访问**。
3. 在左侧导航栏，单击**规则运营**。

4. 在云防火墙IPS规则运营页签，单击**添加自定义规则**。完成如下配置后，单击**确定**。

配置项	说明
规则名称	设置自定义IPS规则的名称，建议使用可识别规则用途的名称，便于后续管理。
规则引擎	在下拉栏中选择规则引擎，可选**基础规则**和**虚拟补丁**。
攻击类型	在下拉栏中选择该规则的攻击类型。
等级	在下拉栏中选择威胁等级，可选**低危**、**中危**或**高危**。
CVE	设置该规则的CVE编号。 **说明** 通用漏洞披露CVE（Common Vulnerabilities and Exposures）列出了已公开披露的各种计算机安全缺陷。CVE编号由CVE编号管理机构（CNA）分配。
攻击应用	设置攻击应用名称。
规则模式	在下拉栏中选择IPS检测的规则模式，可选**包模式**和**流模式**。
方向	在下拉栏中选择IPS检测的流量方向，可选**双向**、**入向**和**出向**。
规则内容	设置规则内容，规则采用Snort语法。 **说明** 添加规则内容时请确认正确性，不正确的规则内容可能会影响您的业务。
规则描述	设置规则描述信息，建议使用规则用途、影响等信息，便于后续管理。
备注	设置规则备注信息，建议使用规则用途、影响等信息，便于后续管理。

添加自定义规则后，用户可以在规则列表，执行如下操作：

- 查看规则详情

  您可以通过IPS规则列表上的筛选按钮，筛选需要查看的IPS规则。

  定位到某一规则，单击**操作**列中的**详情**，您可以查看该规则的具体信息。

- 启用规则

  如果需要启用某个规则，则定位到该规则，单击**启用状态**列中的切换开关，将**禁用**切换为**启用**。

- 禁用规则

  如果某个规则不适应于您的业务环境，您可以禁用该规则。

  定位到该规则，单击**启用状态**列中的切换开关，将**启用**切换为**禁用**。

4.3.2. Aliguard规则运营

Aliguard规则运营支持用户可以根据实际网络环境自定义DDos清洗策略、修改牵引阈值。本文介绍如何自定义DDoS的清洗策略和牵引阈值。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 系统配置**。在**系统配置**授权页面，选择**地域**并单击**角色授权访问**。
3. 在左侧导航栏，单击**规则运营**。
4. 在**Aliguard规则运营**页签，单击**清洗策略**，自定义清洗策略的阈值。
   i. 定位到需要调整的规则，单击**操作**列的**调整阈值**。
   ii. 在**调整阈值**对话框，输入阈值后，单击**确定**。
5. 在**Aliguard规则运营**页签，单击**牵引阈值**，自定义牵引阈值。
   i. 定位到需要调整的策略，单击**操作**列的**调整阈值**。
   ii. 在**调整阈值**对话框，输入阈值后，单击**确定**。
   iii. **可选：**单击**开启DDoS自动牵引清洗**，在**开启自动牵引**对话框，单击**确定**。

   > **说明**
   >
   > 开启DDoS自动牵引清洗开关默认关闭。

   - 自动牵引开关开启：根据用户自定义的DDos阈值触发清洗事件。受攻击IP会被自动牵引到DDoS集群进行流量清洗。
   - 自动牵引开关关闭：根据用户自定义的DDos阈值产生DDos告警事件，用户可以根据业务需要，在DDos控制台手动开始清洗和结束清洗。

4.3.3. 安骑士规则运营

您可以在安骑士规则运营中查看漏洞情况、基线列表、主机异常列表。本文介绍如何查看安骑士规则的运营情况。

操作步骤

1. 登录Apsara Uni-manager运营控制台。

2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 系统配置**。在**系统配置**授权页面，选择地域并单击**角色授权访问**。
3. 在左侧导航栏，单击**规则运营**。
4. 在**安骑士规则运营**页签，查看安骑士规则运营情况。

项目	说明
总览（图示①）	支持查看**漏洞检测规则总数**、**基线检查项总数**、**主机异常检测规则总数**、**引擎信息**。
漏洞（图示②）	在**漏洞**页签，查看检测到的所有漏洞及总数。 ○ 在搜索框选择漏洞类型、输入CVE编号、系统名称，可搜索对应漏洞。 ○ 在漏洞列表，查看检测到的漏洞的**漏洞名称**、**CVE编号**、**漏洞类型**、**系统**、**更新时间**、**状态**。
基线（图示②）	在**基线**页签，查看检测到的基线类型、基线检查项数据。 ○ 在搜索框选择基线类型、风险等级、检查项类别、检查项名称，可搜索对应基线。 ○ 在基线列表，查看**基线类型**、**检查项类别**、**检查项名称**、**风险等级**、**更新时间**、**状态**。
主机异常（图示②）	在**主机异常**页签，查看规则告警子类型数、WebShell&恶意病毒（进程）信息。 ○ 在搜索框选择规则父类、风险等级、规则告警子类名称，可搜索对应主机异常事件。 ○ 在主机异常列表，查看**子类名称**、**规则父类**、**风险等级**、**更新时间**、**来源**、**状态**。

4.3.4. WAF规则运营

通过WAF规则运营，用户可以根据自身的业务需求和网络环境自定义WAF运营规则规则，监控WAF运营状态。本文介绍如何添加和管理WAF运营规则。

操作步骤

> **重要**
>
> 该运营规则为全局自定义规则，会对所有租户生效，请谨慎操作。

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 系统配置**。在**系统配置**授权页面，选择**地域**并单击**角色授权访问**。
3. 在左侧导航栏，单击**规则运营**。
4. 在**WAF规则运营**页签，单击**添加自定义规则**。完成如下配置后，单击**确定**。

配置项	说明
模式	设置规则的处置模式和运行状态。 ○ 处置模式支持**拦截**、**放行**、**观察**、**检测模块控制**。 ○ 运行状态支持**启用**或**禁用**。
备注	填写规则的备注信息。
威胁等级	设置规则检测的威胁等级。可选项：**无威胁**、**低危**、**中危**、**高危**。
匹配条件	设置规则的**匹配字段**、**逻辑符**和**匹配内容**。
是否记录日志	设置记录日志的场景。可选项：**命中时记录**、命中时不记录。
攻击类型	选择规则检测的攻击类型。不支持多选。
阻断状态码	选择规则检测的阻断状态码。不支持多选。
过期时间	设置规则的过期时间。不设置时间表示规则永不过期。

添加运营规则后，用户可以在规则列表，执行如下操作：

- 通过规则列表上的筛选按钮，筛选需要查看的WAF运营规则。
- 定位到某一规则，单击**操作**列中的**编辑**，您可以修改规则信息。

4.4. 告警设置

告警设置支持设置告警联系人和告警规则。当监控数据满足报警规则时，系统自动发送告警信息给报警联系人，支持钉钉消息和邮件。本文介绍如何添加和管理告警联系人。

设置告警联系人

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 系统配置**。在**系统配置**授权页面，选择**地域**并单击**角色授权访问**。

3. 在左侧导航栏，单击**告警设置**。
4. 在**告警设置**页签，单击**添加联系人**。填写联系人姓名、钉钉机器人Token、邮箱信息后，单击**确定**。

   添加后的联系人可以在联系人列表查看，支持**编辑**、**批量删除**。

设置告警规则

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 系统配置**。在**系统配置**授权页面，选择**地域**并单击**角色授权访问**。
3. 在左侧导航栏，单击**告警设置**。
4. 在**安骑士**页签，选择要发送告警的类型、等级、通知方式、告警周期后，单击**保存**。

4.5. 升级中心

4.5.1. 升级中心概述

升级中心通过自动和手动方式，对专有云云盾的特征库和版本进行升级等操作，确保专有云及时获取最新的安全保障。

升级时，用户可以按照如下步骤，进行升级：

1. 配置升级包导入方式。

   升级中心支持**在线自动导入**、**离线手动导入**。

   - 专有云环境和公网互通，可以选择**在线自动导入**升级包方式。
   - 专有云环境和公网不通，可以选择**离线手动导入**升级包方式。选择该种方式时，需要下载升级包。具体操作，请参见升级包下载。
2. 升级特征库、版本。具体操作，请参见升级特征库或版本。

4.5.2. 升级特征库或版本

升级中心支持通过离线手动导入、在线自动导入升级包的方式，升级特征库或版本。本文介绍如何进行升级操作。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 系统配置**。在**系统配置**授权页面，选择**地域**并单击**角色授权访问**。
3. 在左侧导航栏，单击**升级中心**。
4. 在**升级配置**页签，配置升级包导入方式。

   - **离线手动导入**

     如果专有云环境无法与公网连通，可以通过离线手动导入升级包的方式更新特征库和版本。

     a. 选择升级包导入方式为**离线手动导入**，单击**生成升级标识符**，下载升级包。具体操作，请参见升级包下载。

b. 单击上传导入升级包，将已下载的升级包拖动到上传虚拟框内，或单击图标，上传升级包。

> 说明
>
> 上传升级包前，请先单击**手动导入离线升级包**对话框的网站链接，并信任此证书。

升级包导入成功后，用户可在特征库和版本升级页面查看升级包，执行升级操作。

- **在线自动导入**

  如果专有云环境无法与公网连通，可以通过在线自动导入升级包的方式更新特征库和版本。

  a. 选择升级包导入方式为**在线自动导入**，完成如下配置。

配置项	说明
天工云账号ID	输入天工云账号ID。
Access Key	输入Access Key。
Access Secret	输入Access Secret。
自动升级时间段	选择自动升级的时间段。支持选择： ■ 0~6时 ■ 0~8时 ■ 0~24时 ■ 22~6时

  b. 单击**连通性测试**。

  c. 无问题后，用户可以选择开启**自动更新**开关。

  启用**自动更新**后，系统能定期下载升级包。

5. 升级特征库或版本。

- **升级特征库**
  - 一键批量升级：在**特征库升级**页签，单击**一键升级**。
  - 单个云盾产品升级：在**特征库升级**页签，定位到需要升级的产品，单击**操作**列的**立即升级**。

  升级完成后，云盾产品对应的状态为**升级成功**。用户可以执行如下操作：

  - 如果升级失败，用户可以单击**操作**列的**升级记录**，定位到升级失败的特征库版本，单击操作列的**重试**。

- 如果升级成功，用户可以执行如下操作：
  - 在**特征库升级**页签，单击**操作**列的**版本详情**，查看该产品已升级的特征库版本，**重新升级**特征库中的单个规则库。
  - 在**特征库升级记录**面板，单击特征库版**操作**列的**详情**，查看特征库升级包详细信息。单击规则库名称**操作**列的**重新升级**，升级单个规格库。
  - 在**特征库升级**页签，单击**操作**列的**升级记录**，查看该产品已升级的特征库版本。
- **升级版本**
  - 一键批量升级：在**版本升级**页签，单击**一键升级**。
  - 单个云盾产品升级：在**版本升级**页签，定位到需要升级的产品，单击**操作**列的**立即升级**。

  升级完成后，云盾产品对应的状态为**升级成功**。
  - 如果升级失败，用户可以单击**操作**列的**升级记录**，定位到当前版本中，升级失败的特征库版本，单击操作列的**重试**。
  - 如果升级成功，用户可以执行如下操作：

    单击**操作**列的**升级记录**，查看该版本已升级成功的特征库版本，支持**重新升级**和**回滚**。

4.5.3. 升级包下载

当您需要升级混合云云盾产品或版本时，您可以在云安全中心下载混合云云盾产品对应的升级包，然后上传至云盾控制台，完成混合云云盾的升级。本文介绍混合云云盾的升级模式以及不同升级模式下如何下载升级包。

升级模式介绍

云安全中心提供了两种升级模式：普通模式和高级模式。两种升级模式的介绍如下表。

升级模式	描述	具体操作
普通模式	普通模式下，系统会根据您输入的云盾版本标识符，计算出本次更新所需的升级包，并将这些升级包封装成一个组合升级包供您版本升级使用。 选择普通模式，您无需关注本次升级需要下载哪些升级包，系统会自动为您计算并组合本次升级所需的产品升级包和版本升级包。推荐您使用普通模式快捷地升级混合云云盾。	普通模式
高级模式	高级模式下，您可以选择云盾版本号，获取该版本已发布的最新升级包。您可以根据您的业务需求，有选择地下载升级包升级混合云云盾。 **说明** 高级模式下，您需要明确各升级包之间的依赖关系和升级顺序。	高级模式

普通模式

1. 登录云安全中心控制台云安全中心控制台。

2. 在左侧导航栏，选择**安全运营 > 升级包下载**。
3. 在**升级包下载**页面的**升级模式**区域，单击**普通模式**。
4. 在**云盾版本标识符**的输入框中，输入要升级版本的混合云云盾的版本标识符，然后单击右侧的**获取规则包**，获取混合云云盾升级包。

> **说明**
> - 您可以单击输入框下方的**获取方式说明**，了解如何获取云盾版本标识符。
> - 云盾V3.12、V3.13、V3.14版本不支持版本标识符，可在版本标识符输入框中输入V3.12、V3.13或V3.14，以获取相应的升级包。

5. 在**升级包下载**区域的升级包列表中，在目标升级包**操作**列单击**下载**。
升级包下载完成后，将升级包上传至云盾控制台，在云盾控制台上继续进行升级相关的操作，完成混合云云盾升级。

高级模式

1. 登录云安全中心控制台云安全中心控制台。
2. 在左侧导航栏，选择**安全运营 > 升级包下载**。
3. 在**升级包下载**页面的**升级模式**区域，单击**高级模式**。
4. 在**云盾版本标识符**区域的左侧的下拉菜单中，选择混合云云盾的版本；在右侧的下拉菜单中，选择您要下载的升级包版本。
5. 在**升级包下载**区域的升级包列表中，在目标升级包**操作**列单击**下载**。
升级包下载完成后，将升级包上传至云盾控制台，在云盾控制台上继续进行升级相关的操作，完成混合云云盾升级。

4.6. 全局设置

4.6.1. 主机安全规则设置

通过配置全局暴破检测规则，防御主机被暴力破解、批量异常登录，可疑账户登录等情况。本文介绍如何设置主机安全规则。

> **重要**
> 本规则修改后，会影响全局主机类资产的暴力破解检测规则，包括租户侧主机、平台侧物理机等。同时还会影响态势感知的攻击分析结果，请谨慎操作。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 系统配置**。在**系统配置**授权页面，选择**地域**并单击**角色授权访问**。
3. 在左侧导航栏，单击**全局设置**。
4. 在**主机安全规则设置**页签，配置全局爆破检测规则后，单击**保存并应用**。

配置项	说明
主机暴力破解	设置主机暴力破解的时间范围（可选项：5分钟内、10分钟内、30分钟内、60分钟内）、登录失败次数。表示一定时间内，登录失败次数超过设置的阈值时，判断源IP正进行点对点暴力破解。
批量异常登录	设置批量异常登录的时间范围（可选项：5分钟内、10分钟内、30分钟内、60分钟内）、固定账号登录的服务器数量。表示一定时间内，使用固定账号登录超过服务器的次数超过设置的阈值时，判断源IP正进行批量异常登录。
可疑账户登录	如远程登录账户在可疑账户清单内，则对此登录行为进行可疑账户登录告警。 单击管理可疑账户清单，在可疑账户管理面板，手动输入可疑账号，或基于模板上传可疑账号清单，上传文件请确保大小限制在5 KB以下。由于Windows系统机制，输入Windows账户时请全部使用小写字母。

4.6.2. 白名单设置

在使用态势感知的安全阻断功能或者主机安全的异常登录功能时，如果存在安全误报，则可以通过白名单功能消除误报。本文介绍如何配置全局登录白名单和暴力破解白名单。

> **说明**
>
> 为了防止安全隐患，请确保白名单中的IP为可信的地址。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 系统配置**。在**系统配置**授权页面，选择**地域**并单击**角色授权访问**。
3. 在左侧导航栏，单击**全局设置**。
4. 在**白名单设置**页签，单击**添加**，完成如下配置后，单击**确定**。

配置项	说明
类型	○ **全局登录白名单**：符合此类型的白名单，安骑士将不会上报暴力破解事件和异常登录事件。 ○ **暴力破解白名单**：符合该类型的白名单，安骑士将不会上报暴力破解事件。
源IP	访问来源的IP或者IP段。
目的IP	访问目的的IP或者IP段。类型选择为**暴力破解白名单**时，需配置该项。

白名单添加成功后，支持删除不需要的白名单。

4.6.3. 拦截策略设置

通过安全阻断功能，能够防御Web攻击和暴力破解。本文介绍如何启用应用攻击阻断和暴力破解阻断功能。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 系统配置**。在**系统配置**授权页面，选择**地域**并单击**角色授权访问**。
3. 在左侧导航栏，单击**全局设置**。
4. 在**全局设置**页签，单击拦截类型操作列的开关，启用或圈闭拦截策略。

   关闭后，相应的拦截功能将被禁用，仅提供预警功能。

4.6.4. 物理主机防护设置

添加物理机安骑士账号后，您可使用该账号进行物理机安骑士和平台WAF产品配置和管理。本文介绍如何添加物理主机。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 系统配置**。在**系统配置**授权页面，选择**地域**并单击**角色授权访问**。
3. 在左侧导航栏，单击**全局设置**。
4. 在**物理主机防护配置**页签，单击**添加**。完成如下配置后，单击**确定**。

配置项	说明
用户名	设置要添加的物理机安骑士账号。如果用户尚未创建该账号，请按照控制台提示，创建账号。
所属部门名称	所属部门为平台部门，无需设置。
所属部门UID或Primay Key	设置要添加的物理机安骑士账号所属部门或Primay Key。

4.7. CFW运行监控

通过CFW运行监控，用户可以监控云防火墙运行情况，提前发现异常流量，及时处理异常情况。本文介绍如何进行系统巡检、服务监控。

操作步骤

1. 登录Apsara Uni-manager运营控制台。

2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 系统配置**。在**系统配置**授权页面，选择**地域**并单击**角色授权访问**。
3. 在左侧导航栏，单击**CFW运行监控**。
4. 在**系统巡检**区域，单击**一键巡检**。

   完成巡检后，用户可以执行如下操作：

   - 单击**互联网云防火墙(ICFW)**、**VPC云防火墙(CCFW)**或**流量安全监控(Beaver)**操作列的**详情**，查看各检查项的实际状态。
   - 单击**互联网云防火墙(ICFW)**、**VPC云防火墙(CCFW)**或**流量安全监控(Beaver)**操作列的**立即巡检**，可对单个系统进行巡检。
5. 在**服务监控**区域，设置**云防火墙ICFW**或**云防火墙CCFW**的监控配置。

   - **云防火墙ICFW**

     a. 单击**引流配置 - 业务网段**区域的**添加**，完成如下配置后，单击**确定**。

配置项	说明
设备集群ID	选择要添加的引流网段的设备集群ID。
引流方式	选择要引流的方式，可选项：ISW、XGW。
引流网段	输入要引流的网段。
类型	设置引流网段的类型，可选项：业务网段、测试网段。
业务描述	填写业务相关描述。

     完成配置后，可在**服务自检状态**区域、**接口状态**区域，查看引流网段的自动刷新频率、各设备集群的服务自检结果。

     > **说明**
     >
     > 在各区域单击**自动刷新**下拉框，可设置引流网段的自动刷新频率。用户也可以单击图标，手动刷新。

b. 在连通性健康检查区域，单击添加。完成如下配置后，单击确定。

配置项	说明
设备集群ID	选择要添加的引流网段的设备集群ID。
测试IP地址	输入要填写的IP地址。
类型	设置连通性健康检查的类型，可选项：业务、测试、系统。
探测频率	设置探测频率，单位为秒（s），且需要在1~60之间取整数。
探测阈值	设置探测阈值，单位为次，且需要在1~30之间取整数。
动作	设置动作，可选项：自动bypass、告警。

完成配置后，可测试IP地址的连通性。

c. 配置防火墙只对互联网入方向生效的全局默认策略模式为block all（拦截所有）、permit all（允许所有）。

- 云防火墙CCFW

  单击云防火墙ICFW页签，查看防火墙任务流、实例状态自检、设备状态自检、接口状态、连通性健康检查的详细信息。

4.8. 账号管理

4.8.1. 专有云账号管理

本文介绍如何查看、修改系统绑定的专有云账号信息。

> ⚠ 重要
>
> 云盾中的资产均与账号绑定，请谨慎修改。

操作步骤

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击安全，选择全局平台安全 > 系统配置。在系统配置授权页面，选择地域并单击角色授权访问。
3. 在左侧导航栏，单击账号管理。
4. 在专有云账号页签，修改天工云账号信息。
   i. 定位到要修改的天工云账号，单击操作列的修改。

ii. 在**账号修改**对话框中，修改天工云账号名、Access Key、Access Secret信息，单击**确定**。

修改完成后，用户可以单击**操作**列的详情，查看天工云账号详情。

4.8.2. 公有云账号管理

通过在专有云中添加公有云账号，您可以在专有云中管理该公有云账号下已购买的高防IP和WAF，实现混合云功能。本文介绍如何添加公有云账号。

操作步骤

如果专有云中需要使用混合云功能，需要根据本文添加天工云公有云账号。

1. 登录Apsara Uni-manager运营控制台。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 系统配置**。在**系统配置**授权页面，选择**地域**并单击**角色授权访问**。
3. 在左侧导航栏，单击**账号管理**。
4. 在**公有云账号**页签，单击**添加**。
   i. 定位到要修改的天工云账号，单击**修改**。完成如下配置后，单击确定。

配置项	说明
Access Key	设置要添加的公有云Access Key。
Access Secret	设置要添加的公有云Access Secret。
公有云产品	选择使用的公有云产品，支持高防IP和Web应用防护，可单选一个产品或全选。

添加完成后，用户可以在账号列表查看已添加的公有云账号，支持**修改**和**删除**账号。