ALIBABA CLOUD

阿里云

云安全中心（安骑士）

常见问题

文档版本：20220531

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

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

目录

1.短信或邮件报网站后门

当您收到邮件或是短信提示您的服务器存在网站后门，说明您的服务器已经被黑客入侵，并上传了后门文件，黑客可以操作您的网站或数据库的数据。

您可以通过安骑士对该后门文件进行隔离，但具体的入侵原因还需要进一步排查，否则黑客还是会通过该漏洞进行入侵。

如需排查漏洞点，您可以进一步咨询安全专家服务应急响应。

2.基线检查验证失败如何处理？

安骑士基线检查验证已修复风险项失败可能由以下原因导致。

- **安骑士 Agent 版本过低**

  如果您服务器上的安骑士 Agent 版本过低，可能导致基线检查失败。如果您的安骑士 Agent 没有正常自动更新，建议您参考安装Agent手动安装最新版安骑士 Agent。

- **安骑士 Agent 离线**

  如果您服务器上的安骑士 Agent 显示为离线，安骑士基线检查将无法执行。建议您参考Agent离线排查进行排查，确保您服务器上的安骑士 Agent 在线。

3.安骑士检测范围说明

本文档介绍了安骑士的检测范围。

服务器安全（安骑士）服务通过安装在您云服务器上的Agent和云端安骑士防护中心的联动，为您提供服务器的资产清点、漏洞管理、基线管理和入侵检测的功能。

关于安骑士检测范围说明，请仔细阅读以下内容：

> **说明** 以下收集的服务器相关信息的内容如发生变动，阿里云将提前在阿里云官网的适当版面公告向您提示修改内容；如您不同意阿里云所做的修改，您有权停止使用阿里云安骑士服务。这种情况下，您可以查看如何卸载安骑士Agent删除您云服务器上的安骑士Agent。如您继续使用阿里云安骑士服务，则视为您接受阿里云所做的相关修改。

可疑文件信息

为提供恶意文件检测功能，系统在检测到可疑文件后，会上传该文件的相关信息（包括但不限于文件的路径、MD5值、创建时间等）到云端安骑士防护中心，以便进行最终核查。确认为恶意文件后，给您发送安全告警通知。

可疑进程信息

为提供恶意进程检测功能，系统在检测到可疑进程后，会上传该进程的相关信息（包括但不限于进程名、进程启动参数、进程对应文件的路径、进程启动时间等）到云端安骑士防护中心，以便进行最终核查。确认为恶意进程后，给您发送安全告警通知。

账户信息

为提供登录审计、疑似账号提醒、暴力破解拦截等功能，系统会定期分析和上传服务器的账号信息（包括但不限于用户名、用户权限等）和登录日志信息（包括但不限于登录名、登录IP等）。若发生异常登录事件，将会给您发送安全告警通知。

异常连接信息

为提供异常网络连接检测功能，系统在检测到可疑网络连接后，会上传该网络连接的相关信息（包括但不限于访问源IP、源端口、访问目的IP、目的端口等）到云端安骑士防护中心，以便进行最终核查。确认为异常连接后，给您发送安全告警通知。

服务器资产信息

为提供资产管理功能，系统将定期收集服务器的相关资产信息（包括但不限于安装的软件信息、监听的端口信息、运行的网站信息等）。

4.金融云、VPC用户安装Agent

针对无法直接连通公网的云服务器（如阿里金融云上的服务器、或使用专有网络VPC的云服务器），您可通过以下步骤安装安骑士Agent。

安装步骤

> **说明** 如果您已在服务器上安装了安全软件（如安全狗、云锁等），可能会导致安骑士Agent插件无法正常安装。建议您在安装安骑士Agent插件前确认您的服务器上是否存在这类安全软件，如果存在建议您先关闭、或卸载该安全软件之后，再安装安骑士Agent插件。

1. 登录云盾服务器安全（安骑士）管理控制台，单击**设置**。

2. 单击**安装/卸载**进入安装安骑士Agent页面。

3. 根据您的服务器操作系统选择安装步骤，安装最新版本的安骑士Agent插件。
   - **Windows系统**
     a. 在安装安骑士Agent页面，单击**点击下载**下载最新版本安骑士Agent插件安装文件到本地计算机。
     b. 将安装文件上传至您的Windows服务器，例如通过FTP工具将安装文件上传到服务器。
     c. 在您的Windows服务器上以管理员权限运行安骑士Agent插件安装程序。
     d. 非阿里云服务器输入安装验证Key。

        您可在云盾安装安骑士页面找到您的安装验证Key。

        > **说明**
        > - 安装验证Key将用于关联您的阿里云账号，在云盾安骑士管理控制台登录您的阿里云账号即可保护您的服务器安全。
        > - 每个安装验证Key有效期为1小时，超过该时间将无法正确安装安骑士Agent插件。安装插件前请及时刷新安装验证Key。

     e. 完成安装。

f. 单击**立即查看**打开资产列表，查看资产在线状态。

- **Linux系统**
  a. 根据您服务器的Linux系统版本，单击以下链接将安骑士Agent安装程序下载至本地计算机。
     - **Linux 32位系统：** 安骑士Agent安装程序
     - **Linux 64位系统：** 安骑士Agent安装程序
  b. 将安骑士Agent安装程序上传至您的Linux服务器，例如通过FTP工具将安装文件上传到服务器。
  c. 以管理员身份登录您的Linux服务器。
  d. 定位到您已上传的安骑士Agent安装程序所在目录，根据您的服务器的Linux系统版本，执行以下命令安装安骑士Agent。
     - **Linux 32 位系统：** `chmod +x AliAqsInstall_32.sh && ./AliAqsInstall_32.sh xxxxxx`
     - **Linux 64 位系统：** `chmod +x AliAqsInstall_64.sh && ./AliAqsInstall_64.sh xxxxxx`

> **说明** 此安装命令末尾处的 `xxxxxx` 为安装验证Key，执行安装命令时请用您云盾安装安骑士页面中显示的六位安装验证Key替换 `xxxxxx` 部分。此安装验证Key与Windows系统安装步骤中的安装验证Key一致。该安装验证Key将用于关联您的阿里云账号，在云盾安骑士管理控制台登录您的阿里云账号即可保护您的服务器安全。

4. 安骑士Agent插件安装完成约五分钟后，您即可在云盾安骑士管理控制台中查看您服务器的在线情况，您的服务器状态将会从离线变成在线。

验证Agent安装

在您成功安装安骑士Agent后，建议您参考以下步骤进行验证：

1. 检查您的服务器上安骑士Agent的*AliYunDun*和*AliYunDunUpdate*这两个进程是否正常运行。关于安骑士Agent进程说明，请参考什么是安骑士Agent插件？。
2. 在您的服务器上，执行以下telnet命令检查您的服务器是否能正常连通安骑士服务器。

> **说明** 确保以下两个服务器都能连通。
>
> - `telnet jsrv3.aegis.aliyun.com 80`
> - `telnet update3.aegis.aliyun.com 80`

如果安骑士Agent安装验证失败，请参考Agent 离线排查。

5.短信报肉鸡、杀软提示病毒文件或挖矿进程

Windows 系统用户展开任务管理器如果看到如下异常进程，表明存在用户机器被黑客入侵并被植入木马的风险。

异常特征如下：

- 进程名不合符英语语法习惯：如 eeosec.exe。
- 进程名全为数字：如 117466363.exe。
- 进程名具有一定意义上的随机性：如 lkdhpec.exe。
- 进程名具有明显的中文特征：如 SB360.exe、 caonima.exe。
- CPU状态呈现一条很平稳的直线，CPU使用率维持为较高的水位。
- Linux 系统 /usr/bin/dpkgd 目录中可能含有 ps、ss、lsof 、netstat 这几个文件。

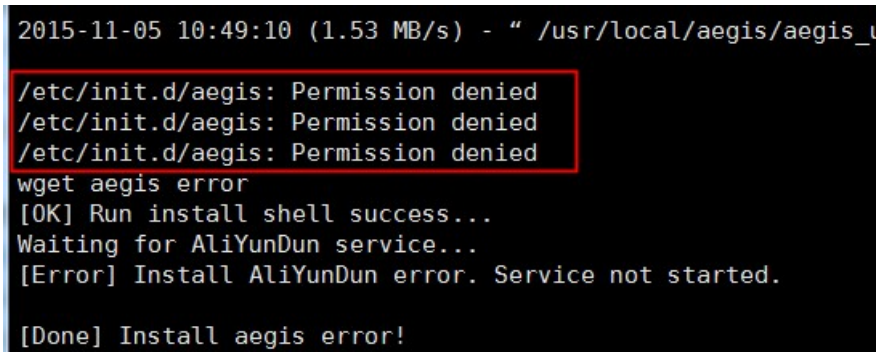
> **注意** 回滚快照并不会彻底解决问题，因为漏洞仍然存在，黑客仍然极有可能通过该漏洞重复入侵。

出现肉鸡、病毒文件或挖矿进程时，建议您使用安骑士的异常登录、网站后门等入侵检测功能，以及软件漏洞、一键查杀恶意进程或修复系统漏洞。

您还可以联系阿里安全管家服务事件处理进行服务器的全面安全检测，排查漏洞并删除木马。

6.安装Agent提示“Permission denied”错误

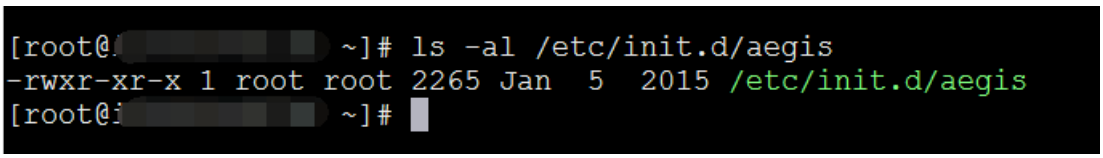
您在 ECS Linux 系统服务器中安装安骑士插件时，收到“Permission denied”的错误提示。



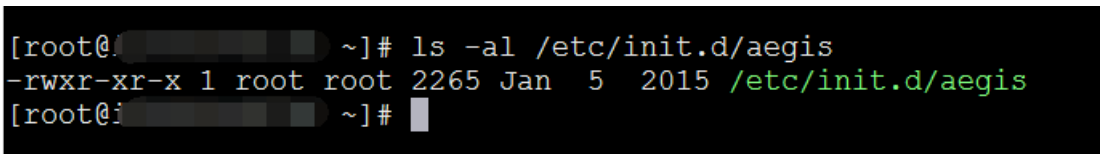
解决方法

您可以参考以下方法进行排查，并解决该问题。

1. 检查是否通过 root 账号进行安装，并且执行 `ls -al /etc/init.d/aegis` 命令查看对于 */etc/init.d/aegis* 目录是否有执行权限。

2. 查看您的服务器是否安装了云锁。您可以通过执行 `ps -ef | grep yunsuo_agent` 或 `ps aux | grep yunsuo` 命令进行检查。

   如果服务器上已安装了云锁，可能会对安骑士插件的安装进行拦截。建议您暂时关闭云锁后，再尝试安装。

   云锁的默认目录是 */usr/local/yunsuo_agent*。

7.如何在非阿里云服务器上使用安骑士？

在非阿里云的服务器上，您同样可以使用安骑士来进行安全防护。

1. 参考安装Agent，将安骑士 Agent 安装至您的非阿里云服务器上。

   > **说明** 安骑士 Agent 安装过程中会提示您输入安装验证 Key。该安装验证 Key 用于关联您的阿里云账号。您可以登录云盾服务器安全（安骑士）管理控制台，在云盾安装安骑士页面找到您的安装验证 Key。

2. 安装完成大约五分钟后，前往**资产列表**，可以看到该服务器 IP 被添加至资产列表中以及服务器的保护状态等信息。
3. 您可在安骑士管理控制台中，对该服务器的安全状态进行管理。同时，安骑士也会针对该服务器上的安全风险事件及漏洞，向您提示告警信息。

8.被暴力破解成功之后该怎么办？

如果您的服务器被暴力密码破解成功，攻击者很有可能已经入侵并登录您的服务器留下恶意程序，建议您采取以下步骤加固您的服务器安全。

1. 修改服务器用户密码。

   请尽快更换您服务器被暴力破解成功的用户密码，建议您使用复杂密码。

2. 使用安骑士基线检查功能进行风险检测。

   使用安骑士的基线检查功能全面检测您的服务器安全，并根据建议处理风险项。

   > **说明** 基线检查功能仅在安骑士企业版中提供。

3. 重置您的服务器，并加固服务器安全。

9.修改22端口后仍然出现密码暴力破解提示

您已将 Linux 服务器上的 SSH 服务的默认端口从 22 修改为其它端口，仍然收到安骑士异常事件功能提示的密码暴力破解告警信息。建议您参考本文介绍的问题解答。

问题解答

安骑士异常登录事件功能依据尝试登录 SSH 服务的频繁度来检测暴力破解攻击行为，与端口无关。因此，即使您已修改 SSH 服务的默认端口，当恶意攻击者尝试暴力破解您的 SSH 服务时，安骑士仍然能正常检测到攻击行为并为您提示告警信息。

如果您的服务器被暴力破解成功，建议您参考被暴力破解成功之后该怎么办对您的服务器安全进行加固。

10.如何在镜像中安装安骑士？

登录云盾服务器安全（安骑士）管理控制台，并前往**插件安装/卸载**页面，按照页面提示安装安骑士Agent。安装成功后，验证以下内容：

1. 在系统启动后，检查是否存在 "AliYunDun" 和 "AliYunDunUpdate" 两个进程（Windows 系统检查是否存在 "AliYunDun.exe" 和 "AliYunDunUpdate.exe"）。
2. 检查版本号是否正确。打开 "AliYunDunUpdate" 进程目录下的*cur_version.txt*文件，查看其内容是否是 `update_00_86(windows)` ， `update_00_87(linux)` 或为以上版本。
   - Linux 系统位于*/usr/local/aegis/aegis_update/*目录下。
   - Windows 系统一般位于*C:\Program Files (x86)\Alibaba\Aegis\aegis_update*目录下。
3. 通过 `telnet` 命令检查在镜像中是否可连通安骑士服务器。例如，以下两个结果表明可以连通。

```
telnet jsrv.aegis.aliyun.com 80
telnet update.aegis.aliyun.com 80
```

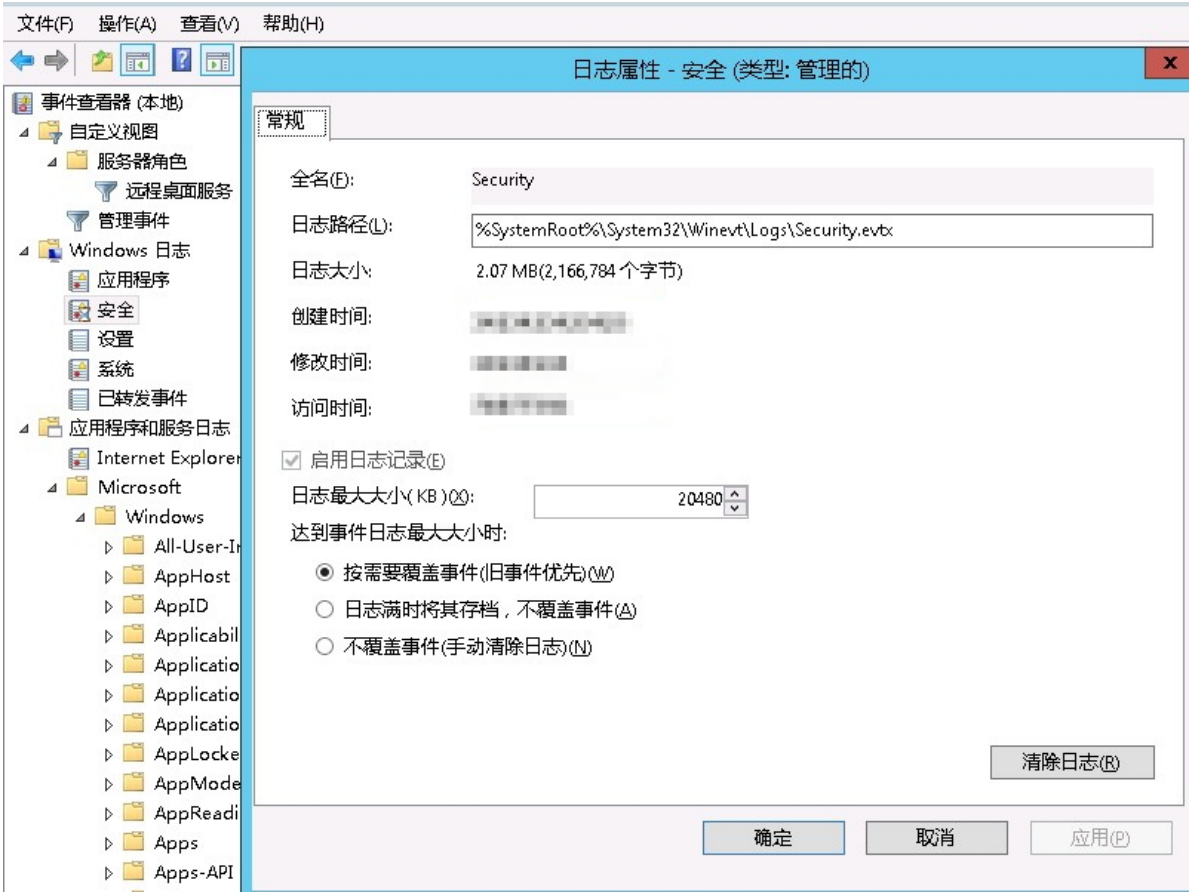
11.如何在Windows2012中查看登录失败的用户名？

由于Windows 2012 远程桌面服务开启了SSL安全层，安全日志无法记录登录失败的源IP和用户名。因此，安骑士的暴力破解拦截功能也无法获取对方用户名。但是您可以通过人工分析并获取登录失败的用户名。

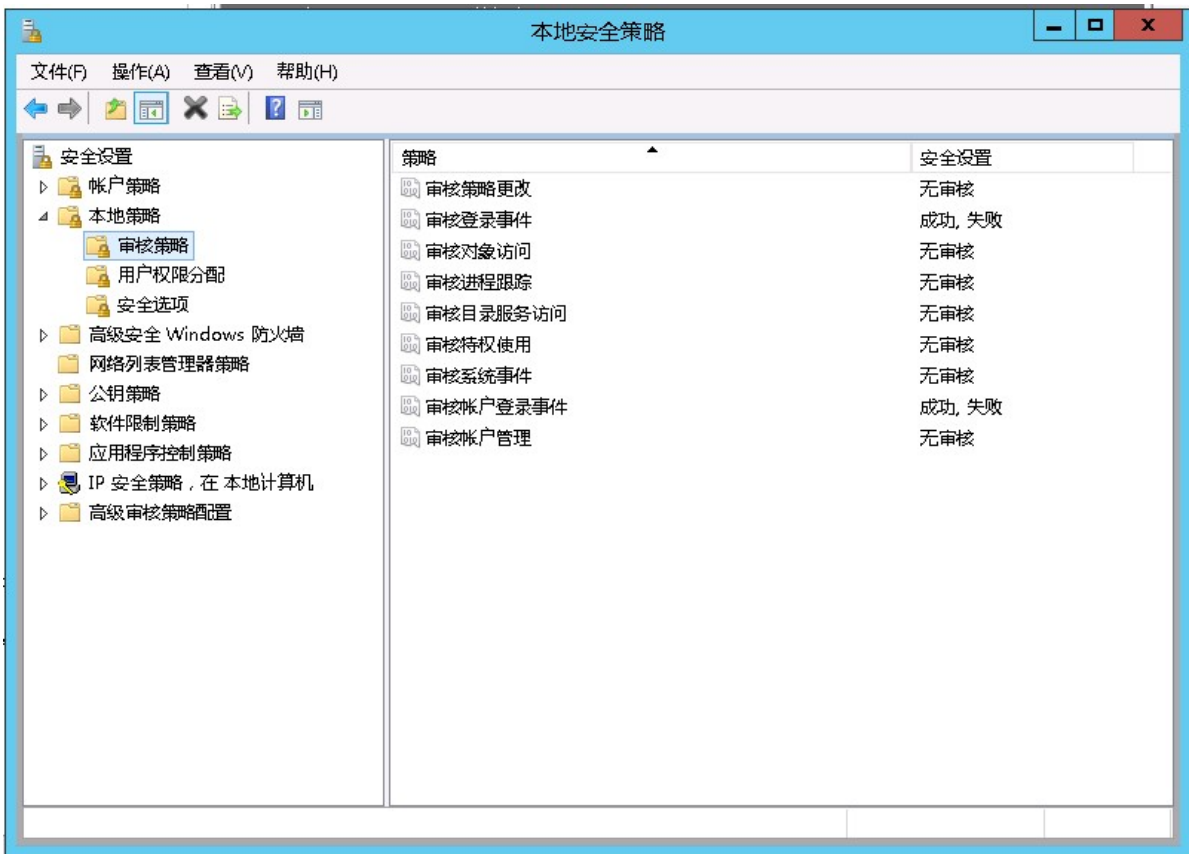
前提条件

人工分析获取登录失败用户名的前提条件是：Windows 2012已经打开审核登录事件日志。您可以通过：

- 在 **控制面板 > 系统和安全 > 管理工具 > 事件查看器** 中，查看日志功能是否启用并记录。



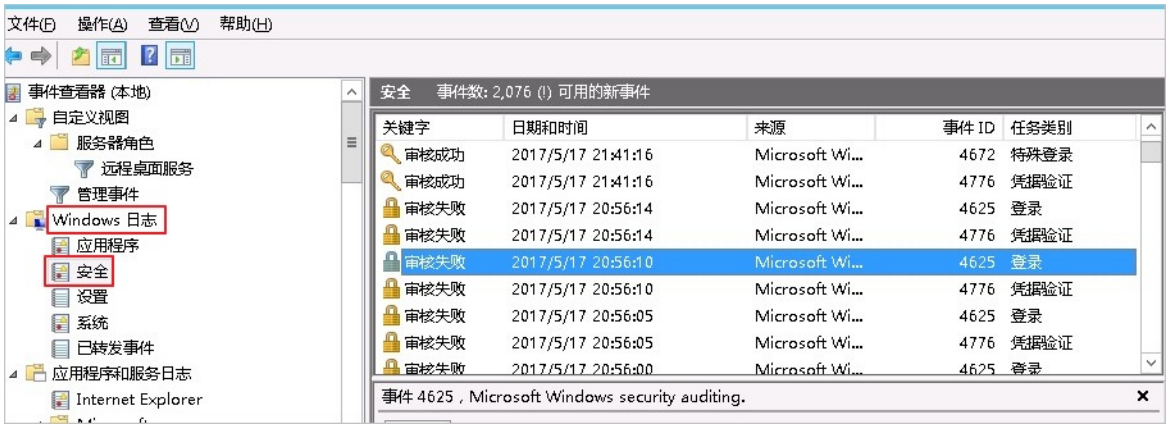
- 在 **控制面板 > 系统和安全 > 管理工具** 中，开启审核登录事件、审核账户登录事件。



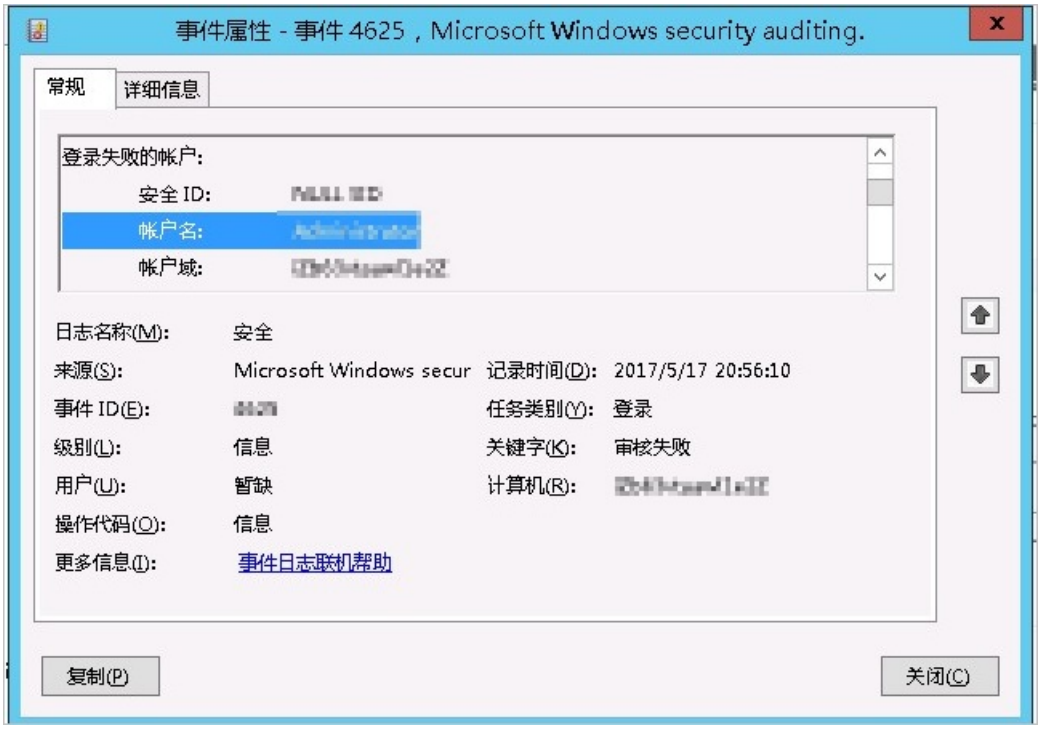
操作步骤

在安骑士控制台 **入侵检测 > 异常登录** 的记录中，**对方用户名**记录为**N/A**。参照以下步骤执行手动分析并获取登录失败的用户名。

1. 登录云盾服务器安全（安骑士）管理控制台，并前往**资产列表**。
2. 找到目标服务器，单击其**异常登录**菜单下的告警数字，进入**异常登录**页面。
3. 找到**爆破登录**告警记录，查看其**登录时间**（该记录的**对方用户名**为**N/A**）。
4. 登录Windows 2012服务器，打开 **控制面板 > 系统和安全 > 管理工具 > 事件查看器** ，并查找 **Windows日志 > 安全** 。
5. 查找安骑士提示爆破登录时刻的明细日志。根据关键字**审核失败**、任务类别**登录**定位到具体爆破登录事件。



6. 在**常规**页面中查看登录失败原因：未知用户名或密码错误。其中，**账户名**为登录失败的用户。


事件属性 - 事件 4625，Microsoft Windows security auditing.
常规
详细信息
登录失败的帐户:
安全 ID:
帐户名:
帐户域:
日志名称(M):
安全
来源(S):
Microsoft Windows secur
记录时间(D):
2017/5/17 20:56:10
事件 ID(E):
任务类别(Y):
登录
级别(L):
信息
关键字(K):
审核失败
用户(U):
暂缺
计算机(R):
操作代码(O):
信息
更多信息(I):
事件日志联机帮助
复制(P)
关闭(C)

12.SSH、RDP远程登录被拦截

如果发现您当前IP无法远程连接（SSH、RDP）云上服务器，可以在安全管控平台将登录IP加入到服务器白名单，可以防止其访问服务器时被拦截。

参照以下步骤，将登录IP添加到服务器白名单。

1. 登录云盾安全管控平台管理控制台。

   > **说明** 您可以将鼠标移至在阿里云管理控制台右上角的账户图标，单击**安全管控**打开云盾安全管控平台管理控制台。

2. 定位到**访问白名单**页面，单击**添加**，将要加入白名单的IP地址填写在**来源IP**输入框中，并配置允许该IP地址登录的服务器。从左侧**所有服务器**框中选择目标服务器（可多选），并单击右向箭头，将其添加到右侧**白名单配置生效的服务器**框中。

3. 配置完成后，单击**确认**。

13.在ECS中对安骑士服务端地址进行加白

如果您需要对您的ECS服务器做安全组或是iptables进行访问控制配置，请对下面的地址及端口进行加白设置，否则防火墙对上述地址进行拦截会导致您的安骑士离线，无法提供安全检测、上报、更新功能。

服务端地址如下：

- 106.11.68.0/24 80
- 110.75.102.0/24 80
- 140.205.140.0/24 80
- 42.156.166.0/24 80
- 10.143.23.0/24 80 443
- 100.100.25.0/24 80 443
- 110.173.196.0/24 80 443
- 110.75.114.0/24 80 443

使用方法

在您的ECS服务器上对上述地址段，配合后面的80端口进行加白设置。注意：后面4个IP地址段，不仅需要对80端口加白，还需要对其IP地址的443端口也要进行加白。（注：VPC环境下只用添加：10.143.23.0/24 80 443 、100.100.25.0/24 80 443 即可）。

14.服务器软件漏洞修复最佳实践

本文档介绍了修复服务器软件漏洞的最佳实践方法。

在安骑士的软件漏洞功能发现您服务器上的漏洞后，您可参考以下方法对您服务器上的漏洞进行修复，保证漏洞修复工作的有效性和可靠性。

> **说明** 本方法适用于服务器上的各类操作系统、网络设备、数据库、中间件的漏洞修复工作。

服务器软件漏洞修复方法

不同于普通PC上的漏洞修复，服务器上的软件漏洞修复应由具有一定专业知识的人员进行操作。漏洞修复工作的负责人应遵循以下的修复流程：

开始漏洞修复前

1. 修复人员应对目标服务器系统进行资产确认，并通过安骑士对目标服务器系统上的系统漏洞进行确认。关于安骑士对Linux软件漏洞的各项参数说明，请参考Linux软件漏洞各参数说明。
2. 修复人员在对目标服务器的系统漏洞确认后，确定需要修复的系统漏洞列表。并不是所有被发现的软件漏洞都需要第一时间进行修复，请根据实际业务情况、服务器的使用情况、及漏洞修复可能造成的影响判定漏洞是否需要进行修复。
3. 修复人员在模拟测试环境中部署待修复漏洞的相关补丁，从兼容性和安全性方面进行测试，并在测试完成后形成补丁漏洞修复测试报告。漏洞修复测试报告应包含补丁漏洞修复情况、漏洞修复的时长、补丁本身的兼容性、及漏洞修复可能造成的影响。
4. 为了防止出现不可预料的后果，在正式开始漏洞修复前，修复人员应使用备份恢复系统对待修复的业务服务器系统进行备份。例如，通过 ECS 的快照功能对目标 ECS 实例进行备份。

漏洞修复操作中

1. 在目标服务器部署修复漏洞的相关补丁及进行修复操作时，应至少有两名修复人员在场（一人负责操作，一人负责记录），尽量防止可能出现的误操作。
2. 修复人员按照待修复的系统漏洞列表，逐项进行升级、修复操作。

漏洞修复完成后

1. 修复人员对目标服务器系统上的漏洞修复进行验证，确保漏洞已修复且目标服务器没有出现任何异常情况。
2. 修复人员对整个漏洞修复过程进行记录，形成最终漏洞修复报告，并将相关文档进行归档。

服务器软件漏洞补丁修复风险规避措施

为了防止在服务器软件漏洞修复过程中出现异常情况、防止漏洞修复对目标服务器系统造成损害，保证目标服务器系统在漏洞修复过程中及漏洞修复后出现异常情况下能及时的恢复与运转，确保目标服务器系统的正常运行、并将异常情况发生的可能性降到最低点，在漏洞修复过程中应采取以下风险规避措施：

- **制定漏洞修复方案**

  漏洞修复负责人应对修复对象（目标服务器）运行的操作系统和应用系统进行调研，并制定合理的漏洞修复方案。漏洞修复方案应通过可行性论证，并得到实际环境的测试验证支持。漏洞修复实施工作应严格按照漏洞修复方案所确定的内容和步骤进行，确保每一个操作步骤都对目标业务服务器系统没有损害。

- **使用模拟测试环境**

  通过使用模拟测试环境，对漏洞补丁修复方案进行验证，证明制定的漏洞补丁修复方案对待修复的在线业务系统没有损害。

> **说明** 模拟测试环境要求系统环境（操作系统、数据库系统）与在线业务系统完全一致，应用系统也与在线业务系统的版本一致，数据建议采用在线业务系统最近一次的全备份数据。

- **进行系统备份**

  对整个业务系统进行完全备份，包括系统、应用软件和数据。备份完成后，应对系统备份的数据进行有效性恢复验证。通过系统备份，当发生系统环境异常或数据丢失时，可以及时对系统进行恢复，确保业务稳定。建议使用 ECS 的快照功能对业务系统进行快速、高效的备份。

15.软件漏洞功能收费说明

阿里云安全采用“责任共担”模型。

- 虚拟化层及以下的安全由阿里云负责，包括虚拟化层到物理环境的整个环节中的安全。
- 操作系统及以上的安全则需要用户自主负责，包括操作系统本身、操作系统上安装的软件、运行的业务等。

> **说明** 操作系统可以使用镜像市场的镜像和自主上传的镜像。

安全责任共担模型举例

例如，作为地产开发商，建筑的地基、楼道的消防等属于开发商平台负责；但房子里面的装修，家具均由用户自主负责。

操作系统则可以类比为房子的基础（墙面和地面），用户可以自由粉刷和装修。

软件漏洞的范畴

- **Linux系统软件漏洞**

  安装在Linux系统服务器上的软件所存在的漏洞，如 SSH、Mysql、Vim 等软件存在的漏洞。

- **Windows系统漏洞**

  微软官方发布的Windows漏洞更新补丁。

- **Web应用漏洞**

  服务器上运行的网站或其他 Web 业务系统存在的漏洞。

软件漏洞功能收费说明

- **节省时间**

  通过软件漏洞功能，实现 “漏洞影响面定位 > 漏洞修复（**一键修复**或**生成修复命令**） > 修复完毕后验证” 的闭环，大大减少处理漏洞的时间。

- **漏洞运营**

  软件漏洞功能发现的每一个漏洞均由阿里云后端的安全运营工程师进行核对和校验，有很高的运营成本。

- **漏洞情报**

  软件漏洞功能共享了整个阿里巴巴集团的漏洞情报来源，漏洞数量全面，漏洞速度获取快。

相关文档

- 软件漏洞
- 系统软件漏洞FAQ
- 如何手动检测系统软件漏洞

16.Linux软件漏洞修复命令为空

当您在安骑士漏洞管理中，选择某Linux软件漏洞，单击生成修复命令时，生成的漏洞修复命令为空。您可以参照本文介绍的解决方案。

解决方案

您可以通过以下方案进行排查，解决该问题：

- 检查安骑士 Agent 版本是否过低。

  如果您服务器上的安骑士 Agent 版本过低，可能不支持漏洞扫描功能。如果您的安骑士 Agent 没有正常自动更新，建议您参考安装Agent 手动安装最新版安骑士 Agent。

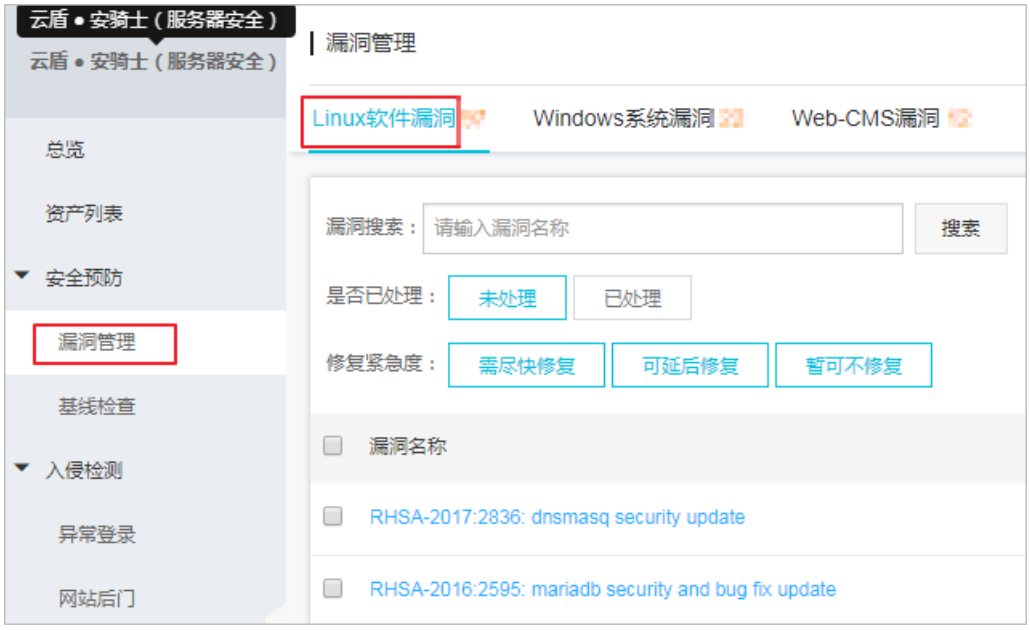
- 检查安骑士 Agent 是否离线。

  如果您服务器上的安骑士 Agent 显示为离线，您将无法通过漏洞管理功能生成修复命令。建议您参考Agent 离线排查进行排查，确保您服务器上的安骑士 Agent 在线。

17.Linux软件漏洞各参数说明

您通过本文档可以了解Linux软件漏洞各项参数的含义及相关说明，帮助您对安骑士发现的Linux软件漏洞有更深的认知。

您可以登录云盾服务器安全（安骑士）管理控制台，前往**安全预防 > 漏洞管理**页面，在**Linux软件漏洞**页签下查看到安骑士在您的服务器上检测到的Linux软件漏洞。



漏洞分类

安骑士漏洞检测覆盖的漏洞目前分为三大类：Linux软件漏洞、Windows系统漏洞、和Web-CMS应用漏洞。

在**Linux软件漏洞**页面单击需要查看的漏洞，进入该漏洞的详情页面。

漏洞名称

该Linux软件漏洞的名称，一般以 CVE 及 RHSA 开头。例如，RHSA-2016:2972: vim security update。

CVSS分值

CVSS 分值是依据行业公开标准，通用漏洞评分系统（Common Vulnerability Scoring System），对该漏洞判定的一个分值，主要用于评测漏洞的严重程度，可以帮助您确定所需反应的紧急度和重要度。

CVEID

该漏洞对应的 CVE 漏洞号，通过 CVEID，如 CVE-2016-1248。Common Vulnerabilities & Exposures（CVE）是已被广泛认同的信息安全漏洞或者已经暴露的弱点的公共名称。您可以快速地在任何其它 CVE 兼容的数据库中找到相应漏洞修复的信息，帮助您解决安全问题。

漏洞等级

漏洞等级分为严重、高危、中危和低危。

- **严重**等级的漏洞包括：
  - 可直接获取服务器系统权限的漏洞
  - 可直接获取重要的敏感信息导致数据泄漏
  - 可直接导致敏感信息越权访问的漏洞
  - 可造成大范围影响的其他漏洞
- **高危**等级的漏洞包括：
  - 可间接获取服务器和应用系统的普通权限的漏洞
  - 可导致任意文件读取、下载、写入、或删除的漏洞
  - 可导致敏感信息泄漏的漏洞

- 可直接导致业务中断、或远程拒绝服务的漏洞

- **中危**等级的漏洞包括：
  - 需要进行交互才能影响用户的漏洞
  - 可导致普通越权操作的漏洞
  - 通过本地修改配置或获取信息之后，可进一步的利用漏洞
- **低危**等级漏洞包括：
  - 可导致本地拒绝服务的漏洞
  - 其他危害较低的漏洞

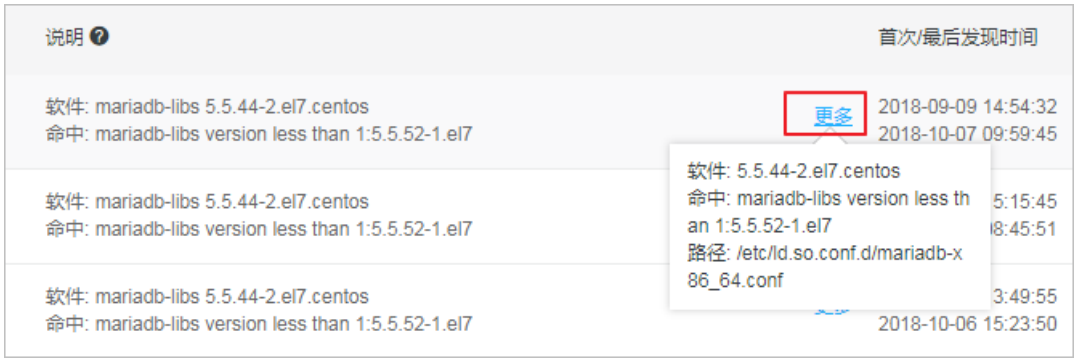
本例中的漏洞为高危等级漏洞，通过此漏洞可以间接获取服务器和应用系统的用户权限。

说明

漏洞说明包含软件及命中两个说明内容。

- **软件**：显示安骑士收集到的当前服务器系统中的软件版本信息。
- **命中**：显示该漏洞的匹配命中原因，一般是由于当前软件版本不满足或者小于某个版本（以小于某个版本为主），因此存在该漏洞。

单击**说明**内容右侧的**更多**，可查看详细说明信息。例如：



- **软件**：`5.5.44-2.el7.centos`

  安骑士检查到的您服务器上的软件版本，即当前检测到服务器上的mariadb-libs的版本是 5.5.44-2.el7.centos。

- **命中**：`mariadb-libs version less than 1:5.5.52-1.el7`

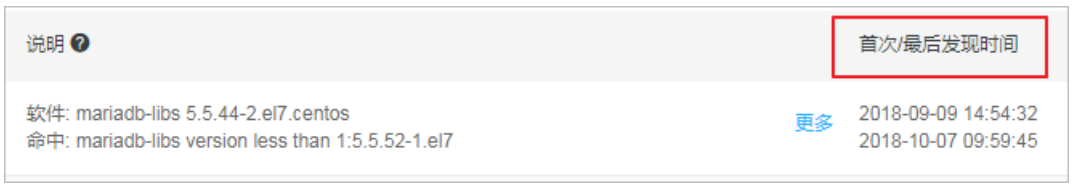
  该软件漏洞的匹配命中原因，即当前 mariadb-libs 软件版本小于1:5.5.52-1.el7。

- **路径**：`/etc/virc`

  安骑士检查到的该软件在您服务器上的路径，即 mariadb-libs 所在路径为 /etc/ld.so.conf.d/mariadb-x86_64.conf。

首次/最后发现时间

该Linux软件漏洞第一次被发现的时间，及最近一次进行安骑士漏洞检测发现的时间。



操作

您可对检测到的Linux漏洞执行以下操作：

- 生成修复命令：生成可执行的漏洞修复命令。
- 一键修复：一键修复Linux漏洞。
- 验证：对漏洞进行验证。
- 忽略：忽略该漏洞。

18.漏洞修复后手动验证没有反应

本文介绍了漏洞修复后手动验证没有反应的解决方案。

问题描述

您在服务器上手动执行安骑士生成的系统软件漏洞修复命令，将相关的系统软件成功升级到新的版本，并且该版本已符合安骑士控制台漏洞管理页面的描述要求。

然而，您在安骑士管理控制台的漏洞处理页面，选择相应的漏洞，单击**验证**，该漏洞的状态没有正常更新为已修复。

解决方案

您可以通过以下方案进行排查，解决该问题：

- 检查安骑士 Agent 版本是否过低。

  如果您服务器上的安骑士 Agent 版本过低，可能不支持漏洞扫描功能。如果您的安骑士 Agent 没有正常自动更新，建议您参考安装Agent 手动安装最新版安骑士 Agent。

- 检查安骑士 Agent 是否离线。

  如果您服务器上的安骑士 Agent 显示为离线，您将无法通过漏洞管理的验证功能对您的服务器进行验证。建议您参考Agent 离线排查进行排查，确保您服务器上的安骑士 Agent 在线。

19.Linux软件漏洞FAQ

本文档列举了Linux软件漏洞功能相关的常见问题，您可以在问题列表中选择您想要了解的问题，并单击该问题查看相关解答。

> **说明** 本文档仅适用于以下操作系统：CentOS、Ubuntu、及 Debian。

如何获取当前软件版本漏洞信息？

一般情况下，系统软件漏洞（CVE 漏洞）是通过软件包版本匹配的方式获取您的服务器当前的软件漏洞信息。

在安骑士中查看当前软件漏洞信息

您可以登录云盾服务器安全（安骑士）管理控制台，在**弱点 > 漏洞管理**中的**系统软件漏洞**页面，查看到安骑士在您的服务器上检测到的系统软件漏洞信息。关于安骑士对系统软件漏洞的各项参数说明，请参见系统软件漏洞各参数说明。

在您的服务器上查看当前软件版本信息

您也可以在您的服务器上直接查看当前的软件版本信息：

- **CentOS 系统**

  通过 `rpm -qa | grep xxx` 命令查看软件版本信息，其中 `xxx` 为软件包名。例如，执行 `rpm -qa | grep bind-libs` 命令查看服务器上的 bind-libs 软件版本信息。

- **Ubuntu 和 Debian 系统**

  通过 `dpkg-query -W -f '${Package} -- ${Source}\n' | grep xxx` 命令查看软件版本信息，其中 `xxx` 为软件包名。例如，执行 `dpkg-query -W | grep bind-libs` 命令查看服务器上的bind-libs软件版本信息。

  > **说明** 如果显示无法找到该软件包，您可以使用 `dpkg-query -W` 查看服务器上所安装的软件列表进行查看。

您通过以上命令获取您服务器上的软件版本信息后，可将得到软件版本信息与安骑士系统软件漏洞中检测到的相关漏洞的说明信息进行对比，根据漏洞说明参数中的 “软件”和“命中”信息，确认是否满足漏洞版本信息。

> **说明** 如果升级后老版本软件包还有残留信息，这些老版本信息可能仍会被安骑士检测收集，并作为漏洞上报。如果确认是由于这种情况产生的漏洞告警，建议您选择忽略该漏洞，或者您可以使用 `yum remove` 或者 `apt-get remove` 命令删除老版本的软件包（删除前，请务必确认已经没有在使用该老版本软件的业务或应用）。

如何将 Ubuntu 14.04 系统的 3.1* 内核升级至 4.4 内核？

注意 系统内核升级有一定风险，强烈建议您参考服务器软件漏洞修复最佳实践中的方法进行升级。

1. 执行 `uname -av` 命令，确认当前服务器的系统内核版本是否为3.1*。

```
root@iZbp14z5cm1cfm8uzf76owZ:~# uname  -av
Linux iZbp14z5cm1cfm8uzf76owZ 3.13.0-65-generic #106-Ubuntu SMP Fri Oct 2 22:08:27 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
root@iZbp14z5cm1cfm8uzf76owZ:~#
```

2. 执行以下命令，查看是否已有最新的内核 Kernel 更新包。

```
apt list | grep linux-image-4.4.0-94-generic
apt list | grep linux-image-extra-4.4.0-94-generic
```

3. 如果没有相关更新，您可执行 `apt-get update` 命令获取到最新的更新包。
4. 执行以下命令，进行内核升级。

```
apt-get update && apt-get install linux-image-4.4.0-94-generic
apt-get update && apt-get install linux-image-extra-4.4.0-94-generic
```

5. 更新包安装完成后，重启服务器完成内核加载。
6. 服务器重启后，执行以下命令验证内核升级是否成功。
   - 执行 `uname -av` 命令查看当前调用内核。

```
root@iZbp14z5cm1cfm8uzf76owZ:~# uname -av
Linux iZbp14z5cm1cfm8uzf76owZ 4.4.0-94-generic #117~14.04.1-Ubuntu SMP Wed Aug 30 06:50:25 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
root@iZbp14z5cm1cfm8uzf76owZ:~#
```

   - 执行 `dpkg -l | grep linux-image` 命令查看当前内核包情况。

```
root@iZbp14z5cm1cfm8uzf76owZ:~# uname -av
Linux iZbp14z5cm1cfm8uzf76owZ 4.4.0-94-generic #117~14.04.1-Ubuntu SMP Wed Aug 30 06:50:25 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
root@iZbp14z5cm1cfm8uzf76owZ:~# dpkg -l | grep linux-image
ii  linux-image-3.13.0-32-generic      3.13.0-32.57                amd64        Linux kernel image for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-3.13.0-65-generic      3.13.0-65.106               amd64        Linux kernel image for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-4.4.0-94-generic       4.4.0-94.117~14.04.1        amd64        Linux kernel image for version 4.4.0 on 64 bit x86 SMP
ii  linux-image-extra-3.13.0-32-generic 3.13.0-32.57               amd64        Linux kernel extra modules for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-extra-3.13.0-65-generic 3.13.0-65.106              amd64        Linux kernel extra modules for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-extra-4.4.0-94-generic  4.4.0-94.117~14.04.1       amd64        Linux kernel extra modules for version 4.4.0 on 64 bit x86 SMP
ii  linux-image-generic                 3.13.0.65.71                amd64        Generic Linux kernel image
```

内核漏洞升级修复后，安骑士仍然提示存在漏洞？

由于内核升级比较特殊，一般都会有老版本信息残留的问题。确认该漏洞告警是由于老版本信息残留造成后，您可以选择忽略该漏洞告警，或者删除老版本的残留信息。

1. 确认内核升级完成后，通过执行 `uname -av` 命令和 `cat /proc/version` 命令查看当前内核版本，确保当前使用的内核版本已符合漏洞说明命中条件中的要求。
2. 执行 `cat /etc/grub.conf` 命令查看配置文件，确认当前已经调用最新的内核版本。
3. 由于系统软件漏洞检测功能主要是通过针对版本进行匹配检测，如果系统中依然存在老版本的内核 rpm 安装包，仍将会被安骑士检测到并进行漏洞告警。您需要确认当前系统中已经没有老版本 rpm 安装包残留，如果有，您可以对老版本安装包进行卸载。
4. 卸载老版本安装包前，请务必确认当前系统已经使用新内核。强烈建议您在卸载老版本内核安装包前，为您的系统创建快照以便于发生异常情况后的恢复。

说明 如果由于某些原因不想卸载老版本内核，在您确认系统已经调用新内核后，可以在云盾服务器安全（安骑士）管理控制台的**系统软件漏洞**页面对该漏洞进行忽略（在该漏洞的漏洞处理页面，单击操作栏中的**忽略**），暂时忽略该系统漏洞告警提醒。

安骑士管理控制台中某些漏洞提示无更新？

- 您在对某些漏洞进行更新修复时，收到以下提示：

```
Package xxx already installed and latest version
Nothing to do
```

或

```
No Packages marked for Update
```

这种情况是由于官方更新源暂时还未提供更新，请您等待官方更新源的更新。目前已知未更新的软件包包括：

  - Gnutls
  - Libnl
  - Mariadb

- 您已经更新到了最新的软件包，但仍然无法满足安骑士管理控制台中报告的软件版本条件。

  请检查您的操作系统版本官方是否已经停止支持。例如，截止到 2017 年 9 月 1 日，官方已经停止对 CentOS 6.2-6.6/7.1 等版本的支持。这种情况下，建议您在安骑士管理控制台中忽略该漏洞（该漏洞对您服务器的风险可能依然存在），或者升级您的服务器操作系统。

如何手动检测服务器上的Linux软件漏洞？

如果您需要手动验证您服务器上的系统软件漏洞，您可以参考如何手动检测Linux软件漏洞中的操作步骤检测您服务器上的系统软件漏洞。

建议您使用安骑士的系统软件漏洞功能定期自动检测您服务器上的系统软件漏洞及时发现漏洞。

参考链接

- Frequently Asked Questions about CentOS in general
- Ubuntu security notices

20.如何手动检测系统软件漏洞？

如果您需要手动查看您服务器上存在的系统软件漏洞，请参考以下操作步骤。

注意 本文档仅适用于以下操作系统：CentOS、Ubuntu、及 Debian。

说明 安骑士系统软件漏洞功能可定期自动检测您服务器上的系统软件漏洞并对发现的漏洞进行告警提示，帮助您及时发现漏洞。同时，安骑士系统软件漏洞功能还可为您生成相应的漏洞修复命令，帮助您轻松修复检测到的系统软件漏洞。关于系统软件漏洞功能的更多说明，请参见软件漏洞。

1. 在您的服务器上执行以下命令，收集您服务器上所有已安装的系统软件包列表：
   - **CentOS 系统**：`yum list installed`
   - **Ubuntu 及 Debian 系统**：`dpkg -l`
2. 根据您的服务器系统，从Open Vulnerability and Assessment Language网站下载所对应的漏洞定义。
3. 在对应的操作系统漏洞定义中，查看您服务器上已安装的软件版本是否受到漏洞影响。
4. 通过以下方法对受到漏洞影响的软件包进行更新修复：
   - 尝试使用包管理器对受到漏洞影响的软件包进行更新。
   - 如果使用包管理器更新失败，您还可以前往该软件的官方网站直接下载最新的二进制安装文件或者源码包进行编译安装。

21.漏洞修复失败可能原因

本文档列举了通过安骑士漏洞管理功能进行漏洞修复失败的可能原因，您可以参考以下原因进行排查。

> **说明** 由于可能导致漏洞修复失败的原因多种多样，例如服务器环境问题、修复补丁本身的兼容性问题、网络环境问题等原因都可能导致在您服务器上的漏洞修复失败。本文无法为您列出所有可能的情况，建议您在按照本文档列出的原因进行排查后，如果问题依然存在，请您尝试使用搜索引擎查找与此漏洞相关的更多信息进行针对性的分析、排查。

Web-CMS漏洞修复失败可能原因

在您使用安骑士漏洞管理功能修复Web-CMS漏洞时，如果提示漏洞修复失败，请参考以下可能原因：

- 确认您的目标服务器上是否安装了安全狗或者其他类似安全防护软件，并且使用这类软件进行过目录权限优化或者相应的设置。目录权限优化设置可能会导致 system 账号对 www 目录及其子目录没有写权限，从而导致安骑士无法进行漏洞修复。

  请您确认您目标服务器上的 system 账号对 www 目录及其子目录具有读写权限。如果没有，请手动为 system 账号添加相应权限。

- 确认安骑士漏洞管理提示漏洞修复失败的相关文件是否被手动修改过或者之前通过手动方式升级更新过官方补丁。漏洞的相关文件变更可能会导致安骑士在进行安装匹配验证时发现该文件的 md5 值不一致，安骑士为了防止误改动您的文件，不会擅自修改该文件，从而停止漏洞修复并返回失败。

  如果您确认已在服务器上手动修复该漏洞，可通过安骑士的漏洞验证功能进行验证（提示文件已修改）。执行验证 24 小时后，如果该漏洞没有重新告警（显示未修复），说明您已成功修复该漏洞。

- 如果安骑士漏洞管理提示该漏洞文件已不存在，请您在服务器上根据漏洞说明中的文件路径查看该文件是否已经被删除。

  如果确认该漏洞文件已被删除，您可以忽略该漏洞告警。

- 检查您的服务器上的存储空间。如果服务器上的磁盘空间已满，会导致安骑士漏洞管理无法在您的服务器上下载相关补丁文件，导致漏洞修复失败。

  如果确认是磁盘空间不够的情况，请您增大服务器的存储空间或者清理服务器上已不需要的文件。确定目标服务器的存储空间够用后，重新修复该漏洞。

系统软件漏洞修复失败可能原因

在您使用安骑士漏洞管理功能修复系统软件漏洞时，如果提示漏洞修复失败，请参考以下可能原因：

> **说明** 建议您参考系统软件漏洞修复最佳实践方法对您服务器上的系统软件漏洞进行修复。

- 检查您的服务器上的存储空间，如果服务器上的磁盘空间已满，会导致安骑士漏洞管理无法在您的服务器上下载相关补丁文件，导致漏洞修复失败。

  如果确认是磁盘空间不够的情况，请您增大服务器的存储空间或者清理服务器上已不需要的文件。确定目标服务器的存储空间够用后，重新修复该漏洞。

- 根据您的服务器操作系统查看其它可能原因：

- **Windows 系统服务器**
  - **补丁安装包不存在**

    您的服务器可能未正确下载补丁安装文件，您可以尝试重新执行漏洞修复操作。
  - **补丁安装包不匹配**

    安骑士漏洞管理发现当前补丁安装包与您的服务器系统不匹配，建议您在进一步确认该补丁安装包的详细信息后，如果该补丁确实与您的服务器系统不匹配，请您在安骑士漏洞管理中忽略该漏洞。
  - **另外一个补丁正在安装**

    由于服务器不能同时运行两个补丁安装程序，建议您等当前补丁安装完成后尝试重新执行漏洞修复操作。
  - **检查其他设置**
    - 检查 Windows Update 服务的Cryptographic Services服务是否正常运行。
    - 检查 Users 用户是否有对 *C:\Windows* 目录的读取和执行权限。
    - 运行 Windows Update，查看其是否正常工作。
    - 重置Windows更新组件
    - 参考Windows Update补丁更新失败排查进行排查。
- **Linux 系统服务器**

  您可以在系统软件漏洞FAQ中查看相关问题与解答。

22.漏洞管理回滚操作失败可能原因

本文档列举了通过安骑士漏洞管理功能进行回滚操作的可能原因，您可以参考以下原因进行排查。

如果您通过安骑士漏洞管理功能对某个漏洞进行回滚操作时，提示回滚失败，您可参考以下可能原因：

- 确认您的服务器的安骑士 Agent 处于在线状态。

  如果您的服务器显示离线，请参考Agent 离线排查进行排查。

- 确认您服务器上该漏洞的相关文件是否已被手动修改或者删除。

  > **说明** 如果在漏洞修复后相关文件已被手动修改或者删除，安骑士为了防止误改动您的文件，不会对该漏洞的相关文件进行回滚。

23.基线检查风险项修复建议

当安骑士基线检查功能检测到并提示您服务器上存在的风险项时，您可以参考本文档中的风险项修复建议为您的服务器进行安全加固。

SSH 登录配置项设置

修改登录端口为非默认22端口

1. 在您的 Linux 系统服务器上，执行 `vim /etc/ssh/sshd_config` ，修改该配置文件。
2. 定位到 `#Port 22` 这一行，删除前面的 # 号，然后修改 22 为您更换后的端口号。

   例如，将该行修改为 Port 50000。
3. 修改完成后，按 ECS 键进入命令模式并输入 **:wq** 保存修改。
4. 执行 `service sshd restart` 或者 `/etc/init.d/sshd restart` 命令，重启 sshd 服务即可。

修改 PermitRootLogin 禁止 root 账号通过 SSH 远程登录

1. 在您的 Linux 系统服务器上，执行 `vim /etc/ssh/sshd_config` ，修改该配置文件。
2. 定位到 `PermitRootLogin yes` 这一行，修改为 `PermitRootLogin no` 。
3. 修改完成后，按 ECS 键进入命令模式并输入 wq 保存修改。
4. 执行 `service sshd restart` 或者 `/etc/init.d/sshd restart` 命令，重启 sshd 服务即可。

进程权限配置不当

该检测项主要检查 webserver 和数据库服务是否以 root 或 system 权限（Linux 系统）、administrator 或 system 权限（Windows 系统）运行。如果安骑士基线检查检测到对应的风险项，您可参考以下步骤对相应的 webserver 或数据库进行降权处理。

Windows 系统

1. 在您的 Windows 系统服务器上，打开任务管理器，查看 websever 或数据库进程所对应的用户名是否为 administrator 或 system，如果是则需要降权处理。
2. 创建一个一般权限的账号。
3. 赋予该账号 webserver 或数据库运行目录的读写权限。
4. 登录该账号，启动 webserver 或数据库应用。

Linux 系统

Linux 系统服务器对于Nginx、Apache、MySQL 等应用通过源码编译方式即可修复该风险项。

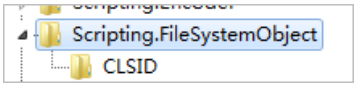
对于Memcache、MongoDB、Redis 等应用，您可以参考 Windows 系统中的操作步骤进行降权处理。

> **说明** 在 Linux 系统服务器上，您可以通过执行 `ps -aux` 命令查看相应进程的第一列（进程权限）是否为 root。

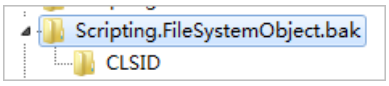
注册表加固

当安骑士基线检查功能检测到您的服务器上存在的注册表风险项时，建议您对检测出的有风险的注册表项名进行更改，修复该风险项。

例如，将注册表项名 Scripting.FileSystemObject，

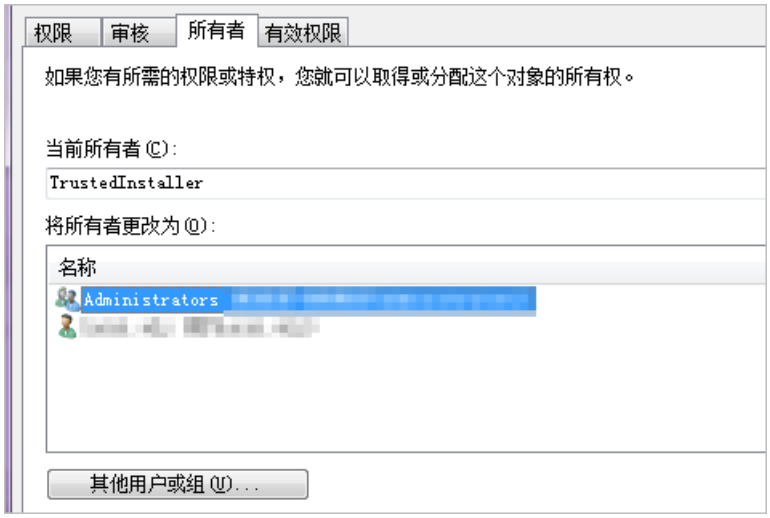


更改为 Scripting.FileSystemObject.bak。



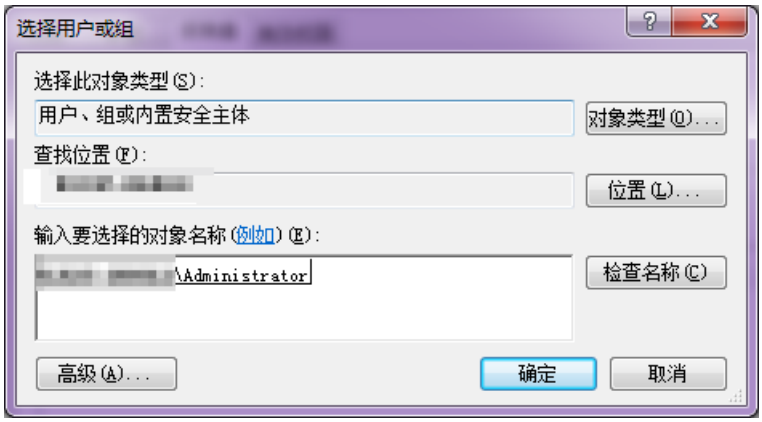
如果您在注册表项名更改过程中收到没有相关权限的提示，您可以通过对该注册表项及其子项的安全进行变更获得相关权限。

1. 选中该注册表项，单击右键，选择**权限**。
2. 单击**高级**，选择**所有者**页签。



例如，该图例中的注册表项所有者为 TrustedInstaller，因此当前管理员权限无法对此注册表项进行修改。

3. 将所有者变更为 Administrators 组。如果这个栏目中为空，单击**其他用户或组**，添加 Administrator 即可。



4. 将该注册表项的所有者变更为 Administrators 后，即可进行注册表项的更名操作。

24.系统漏洞修复FAQ

连接阿里云官方Yum源超时

当出现类似如下的报错时，

```
 [Errno 12] Timeout on http://mirrors.aliyun.com/centos/6/os/x86_64/repodata/repomd.xml: (2
8, 'connect() timed out!')
```

请检查您本机的DNS设置是否正常，并稍作等待。如果一段时间后仍无法解决，请提交工单让售后进行排查。

25.主机访问控制&安全运维功能下线说明

因安骑士产品功能调整，原有的主机访问控制与安全运维功能已下线。

主机访问控制

原功能说明

主机访问控制为主机提供类似安全组或iptable防火墙的功能，实现对于主机端口的访问控制。

如果您需要查看已设置的访问控制规则或将已设置的规则进行迁移，单击此处进入原功能控制台。

主机访问控制功能关闭及规则清除计划

您通过主机访问控制功能设置的访问控制规则将按照以下计划进行清除。

> **说明** 访问控制规则的清除过程不会影响您业务的正常运行。

- 如果您在云盾服务器安全（安骑士）管理控制台中已经不存在主机访问控制功能目录，说明您当前使用的安骑士版本已没有该功能的使用权限，我们将在2018年3月20日将您主机访问控制功能中的规则进行清除。请确认您所需设置的主机访问控制规则已通过其它功能（如ECS安全组或iptables等）进行配置。
- 如果您在云盾服务器安全（安骑士）管理控制台中仍然可以使用主机访问控制功能，请尽快完成主机访问控制规则的迁移工作，我们将在2018年3月20日停止规则编辑功能，在3月30日您主机访问控制功能中的规则进行清除并将主机访问控制功能从云盾服务器安全（安骑士）管理控制台中移除。

主机访问控制规则迁移建议

- **安全组**

  您可以使用ECS的安全组功能配置端口访问控制规则，将已在主机访问控制功能中配置的规则迁移到安全组中。

  > **说明** 如果所配置的主机访问控制规则已经不再需要或相关的访问控制规则已经在安全组中配置完成，您无需迁移安骑士主机访问控制功能中配置的规则。

- 对于在主机访问控制功能中已配置的入方向或出方向的端口黑白名单规则，您需要创建安全组并将需要配置访问控制策略的ECS实例加入该安全组，在安全组中添加相应的安全组规则。

  例如，如果您在主机访问控制功能中配置了以下规则。

  您可以通过在安全组中添加以下安全组规则，对ECS实例实现同样效果的端口访问控制。

> **说明** 对于主机访问控制功能中设置的非80端口的HTTP协议的端口访问控制策略，在安全组中可以通过设置自定义TCP协议类型的规则对所需端口进行访问控制。

- 对于在主机访问控制功能中所设置的全局黑白名单，您需要在ECS实例所在的安全组中添加协议类型为全部，授权对象为黑白名单IP的安全组规则。

  例如，添加以下安全组规则可以对安全组中的所有ECS实例实现类似全局黑名单的访问控制效果。

  > **说明** 您需要在安全组中分别添加出方向和入方向的两条规则，实现类似全局黑名单的访问控制效果。

  关于安全组的详细功能说明，请查看安全组。

- iptables

  如果安全组功能无法完全满足您的主机访问控制规则需求，或者您通过安骑士防护的主机是非阿里云云服务器主机（ECS实例），您可以使用Linux系统自带的iptables防火墙功能配置访问控制规则，将已在主机访问控制功能中配置的规则迁移到iptables中。

  > **说明** 使用iptables防火墙所配置的访问控制规则仅针对本机生效，因此您需要在每台主机中配置相应的iptables访问控制规则。

  例如，您可以在Linux系统主机中添加以下iptables规则实现主机的访问控制。 `iptables -A INPUT -p tcp --dport 80 -j ACCEPT # HTTP`

  > **说明** 对于Windows系统的主机，您可以通过系统自带的Windows防火墙的高级配置功能实现主机的访问控制。

  对于主机访问控制功能中配置的HTTP访问控制策略，建议您使用云盾Web应用防火墙实现更强大的Web应用访问控制。

安全运维

原功能说明

安全运维通过长连接命令通道，提供对主机进行批量运维的功能。通过安骑士的安全运维功能将自定义的bat、shell脚本批量下发到指定的主机，并查看执行结果。

安全运维功能关闭计划

安全运维功能将统一在2018年3月20日从云盾服务器安全（安骑士）管理控制台中移除。

您可以通过在 ECS 实例中安装云助手客户端，实现主机日常运维功能。关于云助手的详细功能说明，请查看云助手。

26.安骑士控制台提示“token校验失败”

在云盾服务器安全（安骑士）管理控制台中，执行某些操作时，提示“token校验失效”。

问题描述

例如，在云盾服务器安全（安骑士）管理控制台的**漏洞管理**页面，选择某个漏洞，单击**一键修复**时，提示**token校验失效**。

问题原因

由于用户长时间没有在控制台进行任何操作，之前验证的token失效，需重新登录控制台。

解决方法

刷新当前页面，重新登录云盾服务器安全（安骑士）管理控制台。

> **说明** 您可按Ctrl+F5，强制刷新当前浏览器页面。

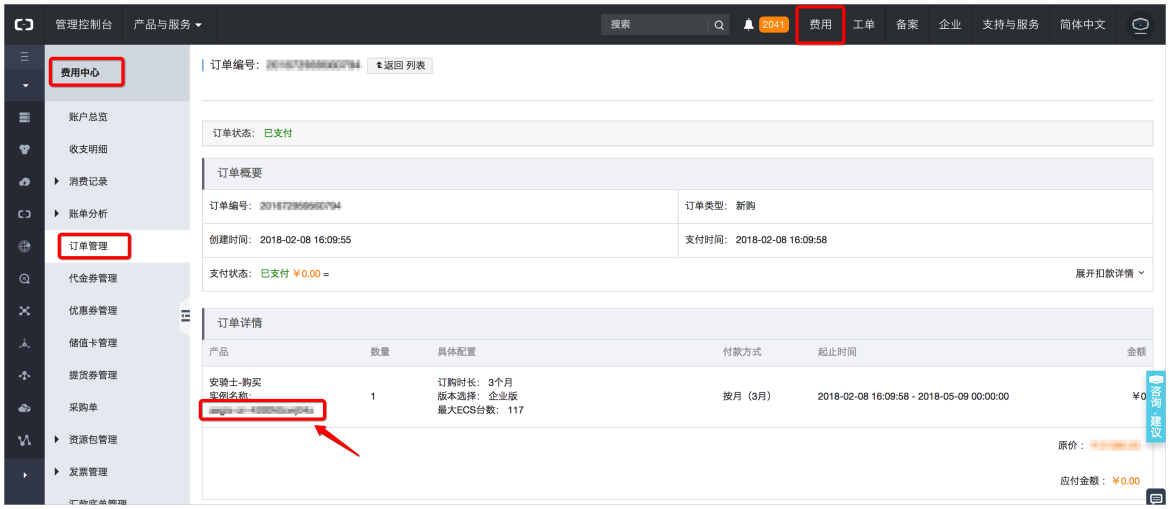
27.如何降低产品配置？

使用场景

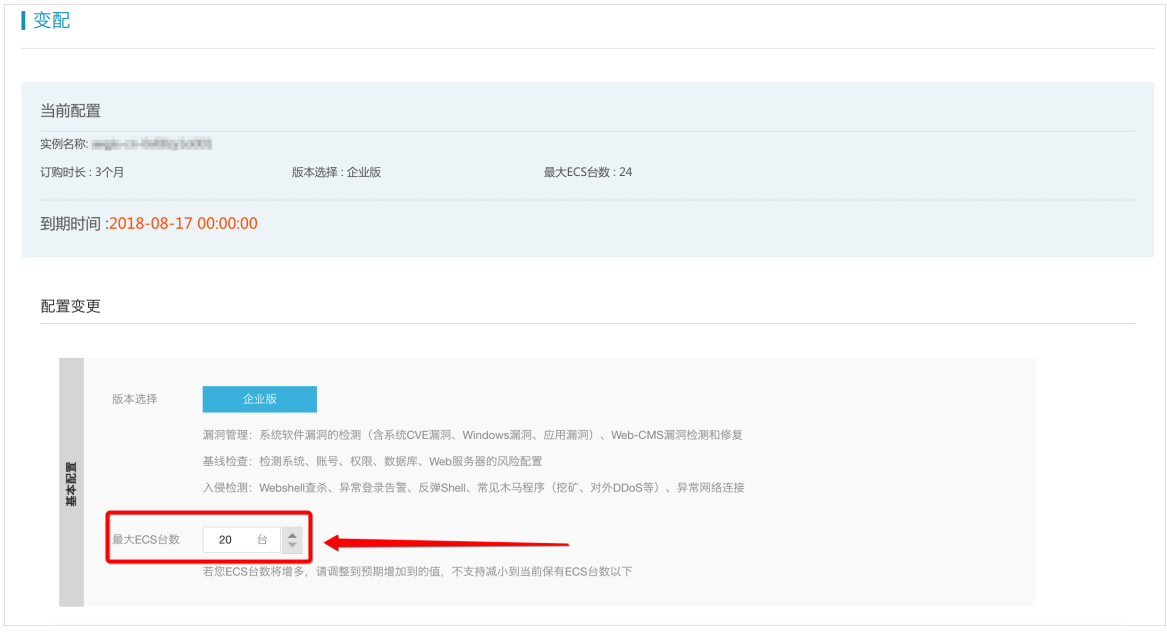
在续费的时候，当前的ECS台数已经小于了原购买时的台数，不用续那么多了。

操作步骤

1. 前往**费用中心**，找到原购买的订单，并进入订单详情，找到**实例名称**，并复制。



2. 前往地址（最后的XXX部分，需要替换成步骤1复制出来的内容）： https://common-buy.aliyun.com/?commodityCode=vipaegis&orderType=UPGRADE&instanceId=XXXXXXXX
3. 将最大ECS台数调整为当前保有的ECS数 。



特殊说明

- 降级配置不会有费用返还，请谨慎操作。
- 若有非阿里云服务器安装了安骑士，也会算在保有的ECS之内，您可以登录安骑士控制台删除非阿里云主机。

28.排查安骑士无法验证系统漏洞修复的问题

本文介绍在安骑士无法验证系统漏洞修复时如何进行排查。

详细信息

1. 查看漏洞的版本信息。
2. 确认系统是否使用阿里云的官方源。
3. 确认系统升级后是否有执行验证操作。

   > **说明** 升级内核需重启生效。

4. 确认选择修复的版本不低于安骑士建议的版本。
5. 如未解决，请升级操作系统。

适用于

- 安骑士

29.联通沃云购买企业版失败

尊敬的用户：

联通沃云暂不支持安骑士企业版购买，如有需求，请联系联通沃云官方，感谢您的支持！

30.查看安骑士Aegis的日志

本文主要介绍如何查看安骑士Aegis的日志。

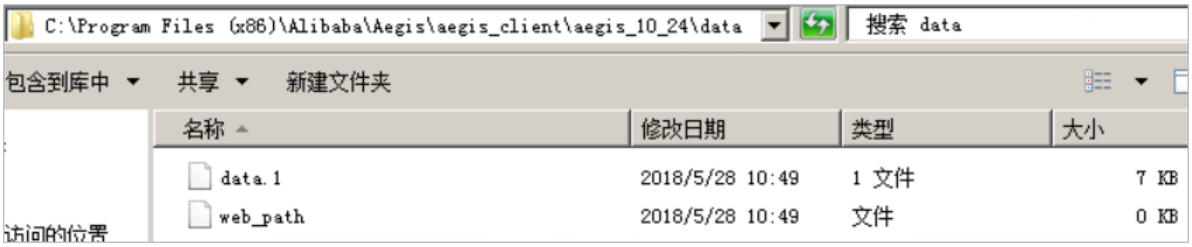
详细信息

安骑士的默认安装路径下包含一个data目录，该目录下的data.x即是日志文件。

- Linux的默认安装路径如下。 */usr/local/aegis/aegis_client/aegis_xx_xx* 查看data目录，系统返回类似如下。

```
root@[redacted]:~# ls /usr/local/aegis/aegis_client/aegis_10_41/data/
data.1  web_path
```

- Windows的默认安装路径如下。 *C:\Program Files (x86)\Alibaba\Aegis\aegis_client\aegis_xx_xx* 查看data目录，系统返回类似如下。



适用于

- 安骑士

31.Wget缓冲区溢出漏洞检测命中规则说明

2017年10月26日，GNU Wget官方发布Wget缓冲区溢出的漏洞公告。当使用存在漏洞的Wget版本下载特殊HTTP链接时，可能会受到恶意HTTP响应攻击，从而导致拒绝服务和恶意代码执行。 相关漏洞编号为CVE-2017-13089、CVE-2017-13090。

云盾安骑士的漏洞管理功能支持检测并修复该漏洞。

受影响版本说明

GNU官方公布的受影响版本为1.19.2之前的所有版本，即通过官方途径下载编译的Wget必须使用1.19.2之后的版本避免受该漏洞影响。然而，对于部分Linux软件源（如CentOS源）中的Wget工具，由于已通过补丁的方式对部分老版本中的该漏洞进行了修复，因此无需升级至1.19.2以上的版本。

根据阿里云安全专家反复测试验证，对于通过Linux软件源方式安装的Wget仅需高于1.14-15.el7_4.1版本即不会受到该漏洞影响。因此，在安骑士漏洞管理检测功能中，对于通过该途径安装的Wget工具使用以下命中规则进行漏洞检测：`wget version less than 1.14-15.el7_4.1` 。

32.漏洞修复优先级排序参考

漏洞修复中的难点

保护您的云上资产安全最重要的环节包括对漏洞修复进行优先级评定。如果您拥有的资产数量较多，您会在控制台看到多个漏洞，您将需要考虑优先修复哪些漏洞。为了解决这个问题，我们提供了一套新颖的评价标准来为您有序地修复漏洞提供参考。

漏洞修复建议分数判定级别说明

- **修复紧急度高**

  漏洞修复建议参考分在13.5-15之间。

- **修复紧急度中**

  漏洞修复建议参考分在7.1-13.5之间。

- **修复紧急度低**

  漏洞修复建议参考分在7以下。

Linux软件漏洞和Windows系统漏洞修复建议参考分计算方法

最终风险得分 = 漏洞的CVSS得分 * 时间因子 * 用户实际环境因子 * 资产重要性因子

> **说明** 应急漏洞和WebCMS漏洞均为经工程师反复确认的高危漏洞，所以统一建议您尽快修复。以下计算方式均只针对Linux软件漏洞和Windows系统/应用漏洞。

- 在计算漏洞修复建议得分的过程中，新发现一个漏洞到控制台提供修复建议大约有1天的延迟。
- 漏洞刚被公布时，官方可能没有给出CVSS基础分，这一部分漏洞的修复建议将会延迟到官方给出CVSS分后一天才能为您显示。
- 由于您的Agent离线等其他网络异常问题也可能导致环境因子无法计算，此时您需要等待网络环境恢复正常后一天才能看到修复建议。

软件漏洞的CVSS基础分

这个因子来源于该漏洞的CVSS V2和V3基础分。

影响漏洞带来风险的时间因素

时间因子是为了弥补CVSS分的不足，综合了漏洞缓解措施被部署的时间延迟，和漏洞利用方法的普及因素的一条动态变化曲线。

在漏洞公开的前三天，由于曝光率的增加，该漏洞被利用的几率会急剧增加，时间因子将会达到短暂的峰值，随后急剧下降。 随着时间的推移，对漏洞成熟的利用手段将越来越多，漏洞实际利用难度在下降，时间因子将在100天之内逐渐趋近于1。

您的实际环境

您的实际环境对判断漏洞真实至关重要，我们对该漏洞利用所需的条件和您服务器的情况进行综合考虑，得出一个风险乘数。

当前纳入参考的环境因素有：

- 您的服务器是否有对公网的流量。

如果是，且漏洞属于一个可以远程利用的漏洞，我们对环境因子进行1.5倍的加权；如果漏洞属于一个可邻网利用的漏洞，我们对环境因子进行1.2倍的加权；如果这个漏洞属于本地利用，我们不做加权；同时我们对某些需要云上难以复现的环境来利用的漏洞做环境因子大幅降权。

- 您的机器是否只有内网的流量。

  如果是，且漏洞属于一个可以远程利用的漏洞，我们对环境因子进行大幅降权（设0）；如果漏洞属于一个可邻网利用的漏洞，我们对环境因子进行1.2倍的加权；如果这个漏洞属于本地利用，我们不做加权；同时我们对某些需要云上难以复现的环境来利用的漏洞做环境因子大幅降权。

您的资产重要性

当您资产数量很多时，可以为不同的服务器/资产赋予您使用场景下的重要性分值，我们将把您自定义的分值纳入漏洞修复建议分的计算当中，为您有序修复漏洞提供有价值的参考。

> **说明** 资产重要性因子当前为 1。

特殊情况下的修复建议

- 当一个漏洞刚被扫描出来时，由于需要参照您的环境对参考分值进行加权，我们需要48小时的时间来评估修复建议，在这段时间内，漏洞的修复建议将按照漏洞本身的严重等级来给出：
  - **严重**漏洞： 建议立即修复
  - **高危**漏洞：可延后修复
  - **中危**漏洞：可延后修复
  - **低危**漏洞：暂可不修复
- 当由于网络抖动等原因我们无法获取该漏洞的环境因子时，该漏洞修复建议将统一为**暂可不修复**。

相关文档

- 软件漏洞
- 系统软件漏洞FAQ
- 系统软件漏洞各参数说明
- 如何手动检测系统软件漏洞

33.漏洞扫描周期说明

安骑士支持漏洞检测和修复，覆盖Linux软件漏洞、Windows漏洞、Web-CMS漏洞。

漏洞检测周期

检测周期：**每隔一天**自动检测一次。

其他漏洞如软件配置型漏洞、系统组件型漏洞都支持自动检测。

查看漏洞检测结果

您可通过安骑士控制台**漏洞管理**页面查看漏洞检测的结果并进行相应处理。详细内容参见漏洞管理功能说明。

34.安骑士是否支持自编译应用程序漏洞的检测？

安骑士不支持检测自编译应用程序的漏洞。

35.安骑士常见问题概览

本文档介绍了阿里云安骑士各类常见问题和对应的解决方案。

用户公告相关信息

- 新功能发布动态

购买、续费相关问题

- 如何降低产品配置
- 联通沃云购买企业版失败

安装、卸载相关问题

- 安装Agent提示“Permission denied”错误
- 金融云、VPC用户安装Agent
- 如何在非阿里云服务器上使用安骑士
- 如何在镜像中安装安骑士

异常登录相关问题

- 被暴力破解成功之后该怎么办
- 如何在Windows2012中查看登录失败的用户名
- 修改22端口后仍然出现密码暴力破解提示

漏洞相关问题

- 短信或邮件报网站后门
- 漏洞修复失败可能原因
- Linux软件漏洞FAQ
- Wget缓冲区溢出漏洞检测命中规则说明
- 系统漏洞修复常见问题FAQ
- Linux软件漏洞各参数说明
- Linux软件漏洞修复命令为空
- 如何手动检测系统软件漏洞
- 漏洞扫描周期说明
- 服务器软件漏洞修复最佳实践
- 漏洞修复后手动验证没有反应
- 软件漏洞功能收费说明
- 漏洞修复优先级排序
- 安骑士无法验证系统漏洞修复
- 安骑士是否支持自编译应用程序漏洞的检测？

基线相关问题

- 基线检查风险项修复建议
- 基线检查验证失败如何处理

日志问相关题

- 如何查看安骑士Aegis的日志

服务器相关问题

- 在ECS中对安骑士服务端地址进行加白
- 云服务器ECS感染木马病毒后的解决方法

安骑士其他使用问题

- 安骑士检测范围说明
- 安骑士控制台提示“token校验失败”

其他

说明 如果您的问题不在常见问题列表中，希望有专业的安全工程师为您提供服务的话，可以了解一下云市场第三方安全合作伙伴提供的漏洞修复或木马清除的服务。您可以在安骑士控制台右下角查看该服务信息，也可以直接在云市场中购买。

服务类型：

按主机数计费服务（单主机199元起）

挖矿病毒清除服务（599元）