ALIBABA CLOUD

阿里云

云安全中心（态势感知）

安全防范

文档版本：20201026

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.漏洞修复

1.1. 漏洞修复概述

云安全中心支持对主流漏洞类型进行检测并提供一键修复功能。您可在漏洞修复页面查看服务器当前存在的漏洞风险、手动执行一键扫描，帮助您更全面地了解您资产中的漏洞和风险情况。

背景信息

漏洞是指在操作系统实现或安全策略上存在的缺陷，例如操作系统软件或应用软件在逻辑设计上存在的缺陷或在编写时产生的错误。攻击者可以对这类缺陷或错误进行利用，从而能够在未获得授权的情况下访问和窃取您的系统数据或破坏系统。系统漏洞需要系统管理员及时处理并修复，否则将带来严重的安全隐患。

有关云安全中心各版本支持的漏洞修复功能的详细差异，请参见漏洞修复。

云安全中心支持检测以下类型的漏洞：

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

漏洞修复原理

您在云安全中心控制台一键修复漏洞时，漏洞补丁包会下载到专用目录，并在漏洞修复完成3天后自动清理。具体说明如下：

- Linux软件漏洞

  执行一键修复Linux软件漏洞后，Linux系统的YUM源包管理系统会负责安装包的自动下载、安装和清理，无需您进行手动操作。

- Windows系统漏洞

  执行一键修复Windows系统漏洞后，由云安全中心Agent负责安装包的自动下载、安装和清理，无需您进行手动操作。漏洞修复完成超过3天后，如果安装包未被及时清理掉，您可手动清理漏洞补丁包，详细操作步骤请参见如何清理云安全中心Agent目录中的Windows漏洞修复补丁包。

漏洞扫描支持的操作系统类型

操作系统类型	版本
CentOS	CentOS 5、CentOS 6、CentOS 7
Ubuntu	Ubuntu 14、Ubuntu 16、Ubuntu 18
Windows Server	Windows Server 2008、Windows Server 2012、Windows Server 2016、Windows Server 2019

漏洞统计信息

您可以登录云安全中心控制台，在漏洞修复页面查看以下统计信息：

- 存在漏洞的服务器

单击**存在漏洞的服务器**下的数值，可跳转到**资产中心 > 服务器**页面，查看存在漏洞问题的服务器资产的详情。

- **需紧急修复的漏洞（CVE）**

  单击**需紧急修复的漏洞（CVE）**下的数值，展开**需紧急修复的漏洞（CVE）**页面。您可以在**需紧急修复的漏洞（CVE）**页面查看和修复所有紧急程度为高的漏洞。

  

- **修复中漏洞**

  单击**修复中漏洞**下的数值，展开**修复中漏洞**页面。查看**修复中**漏洞的影响资产列表和各资产漏洞的修复进度。

  

- **今日已修复漏洞或累计已修复漏洞**

  单击**今日已修复漏洞或累计已修复漏洞**下的数值，展开**今日已修复漏洞或累计已修复漏洞**页面。查看**修复中**或**已修复**漏洞的影响资产列表和相关信息。

  

  支持执行以下操作：

  - **查看漏洞修复的关联进程**：单击影响资产列表中**关联进程**列的 图标，查看漏洞修复的关联进程，了解修复该漏洞可能会影响的进程或业务系统。
  - **查看阿里云漏洞库详细信息**：单击影响资产列表中**漏洞（cve）**栏的漏洞编号可跳转至阿里云漏洞库，查看该漏洞详细信息。

    资产存在多个漏洞时，**漏洞（cve）**栏显示漏洞个数。鼠标移动到显示的漏洞名称，可选择查看不同漏洞的详细信息。

    

  - **查看漏洞修复的详情**：单击影响资产列表中**操作**栏的**详情**，查看漏洞修复影响说明和风险提示。

    

  - **回滚**：云安全中心支持对已创建快照的资产执行回滚操作。单击影响资产列表中**操作**栏的**回滚**，选择待回滚快照，单击**确认**。

    > **说明** 仅Linux软件漏洞支持回滚功能。

- **最新系统漏洞发现时间**

  最近一次系统进行漏洞扫描的时间。

  > **说明** 如果您需要在云安全中心提供的系统自动扫描周期以外的时间，实时检测新购买的ECS服务器是否存在漏洞风险，可以执行**一键扫描**。更多信息请参见**一键扫描漏洞**。

1.2. 一键扫描漏洞

云安全中心支持周期性自动扫描漏洞和非周期性手动实时扫描漏洞。

背景信息

如果您需要在云安全中心提供的系统自动扫描周期以外的时间，实时检测新购买的ECS服务器是否存在漏洞风险，可以执行**一键扫描**，实时地手动扫描服务器中的漏洞。

各类型漏洞的自动检测周期（自动扫描周期）请参见漏洞扫描周期说明。

以下表格介绍云安全中心各版本对不同漏洞类型、基线和云平台配置扫描的支持情况。

> **说明** 以下是表格中使用的标识说明：
> - X：表示该版本不支持该项的扫描和检测。
> - √：表示该版本支持该项的扫描和检测。

检查项目		基础版	基础杀毒版	高级版	企业版
漏洞	Linux软件漏洞	X	√	√	√
	Windows系统漏洞	X	√	√	√
	Web-CMS漏洞	X	√	√	√
	应用漏洞	X	X	X	√
	应急漏洞	√	√	√	√
基线问题		X	X	√	√
云平台配置		X	X	√	√

操作步骤

您可参考以下步骤立即扫描服务器中是否存在漏洞。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 漏洞修复**。
3. 在**漏洞修复**页面，单击**最新系统漏洞发现时间**下方的**一键扫描**。
4. 在**一键检测**对话框，选择需要的检测类型，并单击**确定**。

   以下是一键扫描支持的检测类型描述：

   - **漏洞**：支持检测Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞、应用漏洞和应急漏洞。

     > **说明** 各版本支持扫描的漏洞类型请参见一键扫描支持的扫描项目列表。

   - **基线问题**：基线检查功能为云安全中心的增值服务，仅高级版和企业版用户可开通和使用该服务。一键扫描支持选择已有的基线检查策略或**创建新的策略**。仅企业版用户支持创建新的策略，高级版用户只支持使用默认策略扫描基线安全风险。创建基线检查策略的详细操作请参见设置基线检查策略。
   - **云平台配置**：支持检查云平台配置是否存在风险。

   一键扫描会对云安全中心保护的所有资产进行检测，可能需要1~5分钟时间完成检测。请您耐心等待。

   扫描结束后，您可前往对应页面查看最新的扫描结果。

   - 漏洞扫描结果的详细内容请参见漏洞统计信息。
   - 基线问题扫描结果的详细内容请参见查看和处理基线检查结果。

- 云平台配置扫描结果的详细内容请参见查看和处理云平台配置检查结果。

1.3. 漏洞修复优先级

云安全中心可展示漏洞的修复紧急度得分，帮助您判断一个漏洞是否应该优先修复。本文档介绍了如何确定漏洞修复的优先级。

背景信息

保护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，当被检测出多个漏洞时，您可能无法确定应该优先修复哪些漏洞。为解决这个问题，云安全中心制定了漏洞修复紧急度评分标准，为您有序地修复漏洞提供参考。

计算方法

漏洞修复紧急度得分 = 软件漏洞的CVSS影响分 * 时间因子 * 实际环境因子 * 资产重要性因子

其中参数解释如下：

参数项	参数项解释	附加说明
软件漏洞的CVSS影响分	来源于该漏洞的CVSS影响分。取值范围为0~10。	CVSS（即通用漏洞评分系统），用来评测漏洞的严重程度。
时间因子	弥补CVSS影响分的不足，综合了漏洞缓解措施受部署的时间延迟和漏洞利用方法的普及等因素后，形成的一条动态变化的时间曲线。取值范围为0~1。	在漏洞公开的前三天，由于曝光率的增加，该漏洞被利用的机率会急剧增加，时间因子将从0增加并达到短暂的峰值（小于1），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天之内逐渐增加并趋近于1。

参数项	参数项解释	附加说明

实际环境因子	您服务器的实际环境。云安全中心对该漏洞利用所需的条件和您服务器的状态进行综合考虑，得出一个环境风险因子。 实际环境因子对判断漏洞风险非常重要。	当前纳入参考的环境因素有：
		• 您的服务器已与公网连接：
		  ○ 如果漏洞属于一个可以远程利用的漏洞，则环境因子取值为1.5。
		  ○ 如果漏洞属于一个可利用的漏洞，则环境因子取值为1.2。
		  ○ 如果漏洞属于本地利用，则环境因子取值为1。
		  ○ 对某些需要云上难以复现的环境来利用的漏洞，通过环境因子大幅降权，云安全中心根据您服务器的实际情况动态调整权重。
		• 您的服务器只连接了内网，未连接公网：
		  ○ 如果漏洞属于一个可以远程利用的漏洞，则通过环境因子大幅降权，云安全中心根据您服务器的实际情况动态调整权重。
		  ○ 如果漏洞属于一个可利用的漏洞，则环境因子为1.2。
		  ○ 如果漏洞属于本地利用，则环境因子为1。
		  ○ 对某些需要云上难以复现的环境来利用的漏洞，通过环境因子大幅降权，云安全中心根据您服务器的实际情况动态调整权重。

资产重要性因子	当服务器数量很多时，系统为不同的服务器资产赋予不同使用场景下的重要性分值，并把该分值纳入漏洞修复紧急度得分的计算之中，为您有序修复漏洞提供有价值的参考。	资产重要性因子默认值为1。您可以在**资产中心**页面设置资产重要性为**重要资产**、**一般资产**或**测试资产**。以下是不同类型资产对应的资产重要因子： • **重要资产**：1.5 • **一般资产**：1 • **测试资产**：0.5

漏洞修复建议（推荐）

- **需尽快修复**：漏洞修复紧急度得分在13.5~15之间（通常是高危漏洞）。
- **可延后修复**：漏洞修复紧急度得分在7.1~13.5之间（通常是中危漏洞）。
- **暂可不修复**：漏洞修复紧急度得分在7以下（通常是低危漏洞）。

> 说明
> - 由于网络抖动等原因导致云安全中心无法获取该漏洞的环境因子时，漏洞修复建议会展示为暂可不修复。
> - 应急漏洞和Web-CMS漏洞均为阿里云安全工程师确认后的高危漏洞，建议您尽快修复这两类漏洞。

1.4. Linux软件漏洞

云安全中心支持检测并快速修复Linux软件漏洞。本文档介绍了如何查看Linux软件漏洞的相关信息和对Linux软件漏洞进行处理。

背景信息

云安全中心**基础版**和**基础杀毒版**只提供漏洞检测，不提供漏洞修复的服务；如需一键修复漏洞，请开通云安全中心**高级版**或**企业版**。基础版、基础杀毒版、高级版和企业版详细功能介绍请参见功能特性。

查看漏洞基本信息

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 漏洞修复**。
3. 在**Linux软件漏洞**页面的漏洞列表中，查看云安全中心检测到的Linux软件漏洞关联的漏洞公告，漏洞公告名称通常以*USN*、*RHSA*或*CVE*字符开头。
   - **查看漏洞公告信息**

     
   - **查看漏洞的修复紧急度和影响资产数量**

     漏洞的建议修复紧急度用不同颜色的图标表示，图标中的数字表示存在该漏洞的资产数量。 以下是图标颜色和漏洞修复紧急度的对应关系：
     - 红色图标：表示漏洞修复紧急度为**高**。
     - 橙色图标：表示漏洞修复紧急度为**中**。
     - 灰色图标：表示漏洞修复紧急度为**低**。

     

     > **说明** 建议您立即修复紧急程度为高的漏洞。
   - **将漏洞加入白名单**

     您可在**Linux软件漏洞**页面，选中需要加入白名单的漏洞并单击**加入白名单**，将一个或多个漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。

     

     加入白名单的漏洞将从**Linux软件漏洞**的漏洞列表中移除，并记录在**漏洞管理设置**页面的**漏洞白名单配置**列表中。

     如需恢复云安全中心对白名单中漏洞的检测和告警提示，可在**漏洞管理设置**页面移除该漏洞。

     

   - **批量修复漏洞**

     批量修复功能会自动识别您选择的漏洞公告对应的资产，并修复这些资产中您所选择的漏洞。您可在**Linux软件漏洞**页面，选择需要批量修复的漏洞并单击**批量修复**。在**批量修复**对话框中查看云安全中心为您识别出的需要修复漏洞的资产列表，选择**自动创建快照并修复**或**不建立快照备份直接修复**后，单击**立即修复**。

     

> **说明**
>
> - 批量修复功能仅支持选择当前页面的漏洞，不支持跨页选择漏洞。漏洞列表每页可以展示10、20或50条漏洞信息，即您最多可以选择50个漏洞进行批量修复。
> - 部分过期的操作系统（厂商已不维护更新，无可适配补丁来修复漏洞）和商业版本的操作系统，需要手动升级操作系统，才能修复漏洞。此类漏洞不支持批量修复。您执行批量修复操作后，云安全中心会自动为您忽略此类漏洞。以下操作系统中的漏洞不支持批量修复，需要手动升级操作系统进行修复：
>   - Red Hat 5、Red Hat 6、Red Hat 7、Red Hat 8
>   - CentOS 5
>   - Ubuntu 12
>   -
> - 系统在修复漏洞时，可能存在一定的失败风险，建议您在修复漏洞前选中**自动创建快照并修复**对系统进行快照备份。快照的更多信息请参见ECS服务的**快照概述**。
> - 创建快照将产生一定的费用，费用由快照产品收取（40 GB的系统盘，快照存储一天的费用大约是0.15元）。快照计费方式更多信息请参见**快照计费**。

- **搜索漏洞**

  您可在**Linux软件漏洞**页面，通过筛选漏洞危险等级（高、中、低）、漏洞处理状态（已处理、未处理）、资产分组、VPC名称或输入漏洞名称搜索到到相关的漏洞。

  

  > **说明** 漏洞名称支持模糊搜索。

- **导出漏洞**

  您可在**Linux软件漏洞**页面单击 图标，将云安全中心检测到的所有Linux软件漏洞统一导出并保存到本地。导出的文件为Excel格式。

  > **说明** 根据您资产中漏洞数据的大小，导出漏洞列表可能需要耗费一定时间，请耐心等待。

查看漏洞详情和处理漏洞

1. 登录**云安全中心控制台**。
2. 在左侧导航栏单击**安全防范 > 漏洞修复**。
3. 在Linux软件漏洞列表，定位到需要查看的漏洞。单击该漏洞的**漏洞公告**名称或操作栏的**修复**，可展开对应的**漏洞详情**页面。
4. 在**漏洞详情**页面，查看漏洞详情并处理漏洞。

   

   您可根据需要执行以下操作。

   - **查看漏洞详情**

     漏洞详情页面可展示该漏洞公告所有关联漏洞，及漏洞影响的所有资产信息，方便您对所有相关的漏洞进行分析和批量处理。您可以查看以下内容：

     - 在**漏洞详情**页签查看该漏洞公告关联的所有漏洞、漏洞的描述、漏洞紧急度。

- 单击**待处理漏洞**页签，查看漏洞影响的资产列表。

  您可查看该漏洞影响的所有资产和资产漏洞状态等信息，并可对漏洞执行验证、修复、加入白名单、忽略或回滚的操作。

  漏洞处理

  在漏洞影响资产列表中，单击**影响资产**下的资产名称，可跳转到**资产中心 > 漏洞信息**页面，为您展示该资产关联的所有漏洞信息。

  

- **查看阿里云漏洞库详细信息**

  在**漏洞详情**页面，单击**漏洞编号**可跳转至阿里云漏洞库。

  

  您可在阿里云漏洞库页面，查看该漏洞更加详细的信息，包括漏洞的描述、基本信息、修复建议等信息。

- **查看漏洞严重等级**

  漏洞紧急度用不同颜色的图标表示：

  - 红色图标：表示漏洞修复紧急度为**高**。
  - 橙色图标：表示漏洞修复紧急度为**中**。
  - 灰色图标：表示漏洞修复紧急度为**低**。
  -

  > **说明** 建议您立即修复紧急程度为高的漏洞。

- **查看漏洞修复的关联进程**

  在漏洞影响资产列表中，单击**关联进程**列的 图标，查看漏洞关联进程，帮助您了解修复该漏洞可能会影响的进程或业务系统。

  

- **查看漏洞详细状态**

  漏洞状态可分为已处理和未处理：

  - **已处理**
    - **修复成功**：漏洞已执行一键修复并修复成功。
    - **已忽略**：漏洞已执行**忽略**的操作，云安全中心将不再对该漏洞进行告警。

    > **说明** **已处理**的漏洞支持**回滚**操作，漏洞回滚后将重新变为**未处理**的状态。

  - **未处理**
    - **未修复**：漏洞待修复。
    - **修复中**：漏洞正在修复处理中。
    - **修复失败**：漏洞修复失败，可能因为漏洞文件已被修改或漏洞文件已不存在。
    - **修复成功待重启**：漏洞已修复，需要重启系统生效。
    - **验证中**：漏洞已修复，如果需要重启系统，完成重启后，执行验证。

- **处理受影响资产漏洞**

  您可在漏洞影响资产列表中，对受影响资产漏洞进行修复、验证、加入白名单、忽略或回滚的操作。

  

  以下内容介绍您可以执行的操作：

  - **修复漏洞**

    您需要分以下两种情况修复漏洞：

    - **修复按钮显示正常**

      单击修复，修复单个漏洞或批量修复多个关联漏洞。修复漏洞时支持自动创建快照并修复。您可以根据需要选择自动创建快照并修复或不建立快照备份直接修复。

      > **说明**
      >
      > - 系统在修复漏洞时，可能存在一定的失败风险，建议您在修复漏洞前选中**自动创建快照并修复**对系统进行快照备份。快照的更多信息请参见ECS服务的快照概述。
      > - 创建快照将产生一定的费用，费用由快照产品收取（40 GB的系统盘，快照存储一天的费用大约是0.15元）。快照计费方式更多信息请参见快照计费。

      

- **修复按钮显示为灰色**

  修复按钮显示为灰色有以下原因：

  - 部分过期的操作系统（厂商已不维护更新，无可适配补丁来修复漏洞）和商业版本的操作系统，需要手动升级操作系统，才能修复漏洞。

    > **说明** 目前，以下操作系统中的漏洞，需要升级操作系统进行修复。
    >
    > - Red Hat 5、Red Hat 6、Red Hat 7、Red Hat 8
    > - CentOS 5
    > - Ubuntu 12

  - 服务器磁盘空间过小、文件权限设置等问题都可能会导致Linux软件漏洞修复失败。您需要先手动处理服务器的这些问题，才能在云安全中心控制台上修复该服务器上的漏洞。以下是您需要手动处理的服务器异常情况：
    - 磁盘空间小于3 GB。

      处理建议：

      处理建议：扩容或清理磁盘后，再次在云安全中心控制台上尝试修复该漏洞。
    - APT-GET或APT/YUM进程正在运行中。

      处理建议：稍后或手动结束该服务器的APT-GET或APT/YUM进程，再次在云安全中心控制台上尝试修复该漏洞。
    - 执行APT、YUM或RPM命令时权限不足。

      处理建议：检查并合理管控文件权限，建议将文件权限设置为755，并确保文件所有者为root用户后，再次在云安全中心控制台上尝试修复该漏洞。

      > **说明** 将文件权限设置为755表示文件所有者对该文件具有读、写、执行权限，该文件所有者所在用户组及其他用户对该文件具有读和执行权限。

  您可以将鼠标移至**修复**按钮处，查看云安全中心为您提供的操作系统升级相关提示或服务器问题处理建议。

- **重启系统**

  Linux内核漏洞需要在漏洞修复完成后重启系统。您可以通过以下两种方式重启系统：

  - （推荐）在控制台漏洞详情页面单击**重启**。

    

    > **说明** 如果需要重启的服务器有其他漏洞在修复或验证中，则无法进行重启操作。单击**重启**后您将在控制台上看到重启失败的提示信息。您需要等待该服务器正在进行修复或验证的漏洞相应操作全部结束后，才能执行重启操作。

  - 在您的Linux服务器中使用命令行执行重启。

- **验证漏洞**

  单击**验证**，验证单个漏洞或批量验证多个关联漏洞，检测该漏洞是否已修复成功。

  单击**验证**后，该漏洞的**状态**转为**验证中**。需要等待数秒后漏洞验证才可完成。

- **将漏洞加入白名单**

  单击**漏洞详情**页面右上角**加入白名单**，将该漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。

  加入白名单的漏洞将从**Linux软件漏洞**的漏洞列表中移除，并记录在**漏洞管理设置**页面的**漏洞白名单配置**列表中。

  如需恢复云安全中心对白名单中漏洞的检测和告警提示，可在**漏洞管理设置**页面移除该漏洞。

- **忽略漏洞**

  定位到需要忽略的漏洞，单击其操作列 图标后选择**忽略**，在确认对话框中填写忽略操作说明并单击**确定**，云安全中心将不再提示该漏洞。

  您可以在**已处理**漏洞中查看已忽略的漏洞和忽略该漏洞时填写的操作说明。

  > **说明** 被忽略漏洞的状态将转为**已忽略**。如需云安全中心继续对该漏洞进行告警提示，可在**已处理**的漏洞列表中找到该漏洞并对其**取消忽略**。

- **回滚漏洞**

  定位到需要回滚的漏洞单击其操作列 图标，并单击**回滚**。在**回滚**对话框中选择待回滚快照，单击**确定**。

  回滚

- **搜索漏洞影响资产**

  在漏洞影响资产列表上方，通过筛选漏洞危险等级（高、中、低）、VPC名称、资产分组、漏洞处理状态（已处理、未处理）或输入服务器IP或名称定位到相关的漏洞影响的资产。

  > **说明** 服务器IP或名称支持模糊搜索。

- **导出漏洞影响的资产列表**

  在漏洞影响资产列表左上方，单击导出图标，将云安全中心检测到的该漏洞下的影响资产统一导出并保存到本地。导出的文件为Excel格式。

  > **说明** 根据受影响资产数量的大小，导出资产列表可能需要耗费一定时间，请耐心等待。

- **保存已筛选漏洞**

  在漏洞影响资产列表左上方，单击

  图标保存筛选出的所有漏洞为一个漏洞修复批次，方便您对该批次漏洞的状态进行持续跟踪。

  保存筛选

Linux软件漏洞详情页说明

漏洞详情页项目	描述
漏洞编号	该漏洞对应的CVE漏洞号。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。通过漏洞编号（如*CVE-2018-1123*），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。

影响分（CVSS分值）	CVSS分值遵循被广泛采纳的行业标准 - 通用漏洞评分系统（Common Vulnerability Scoring System），根据漏洞的多种属性通过公式计算得出。主要用于量化漏洞的严重程度。
	在CVSS v3.0评分体系中，不同分值代表的漏洞严重程度如下：
	• 0：无漏洞
	• 0.1~3.9：低危
	  ◦ 可导致本地拒绝服务的漏洞。
	  ◦ 其他危害较低的漏洞。
	• 4.0~6.9：中危
	  ◦ 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，可进一步利用的漏洞。
	• 7.0~8.9：高危
	  ◦ 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。
	• 9.0~10.0：严重
	  ◦ 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，导致数据泄漏的漏洞。
	  ◦ 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。

影响资产	存在该漏洞的服务器资产信息，包括资产的公网或私网IP地址等。

紧急度	漏洞的严重等级，包括：
	• 紧急度高：
	  高风险漏洞，建议尽快修复。
	• 紧急度中：
	  中危漏洞，您可根据业务需要尽快修复或延后修复。
	• 紧急度低：
	  低风险漏洞，您可根据业务需要尽快修复或暂不修复。
	漏洞修复优先级详情，请参见漏洞修复优先级。

漏洞详情页项目	描述

详情	您可单击漏洞详情页面右侧详情查看修复命令、漏洞命中原因等信息。
	• 修复命令：执行该命令可修复对应的Linux软件漏洞。
	• 影响说明：
	  ○ 软件：该软件在当前服务器系统中的版本信息。
	  ○ 命中：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）。
	  ○ 路径：该软件在服务器上的路径。
	• 风险重要提醒：关于漏洞的风险提醒、补充修复建议和参考文档。

1.5. Windows系统漏洞

云安全中心支持检测并快速修复Windows系统漏洞。本文档介绍了如何查看Windows系统漏洞的相关信息和对Windows系统漏洞进行处理。

背景信息

通过实时同步微软官网补丁源，对高危及有影响的漏洞进行有效的检测和告警，避免攻击者通过Windows系统漏洞对您的服务器进行攻击或威胁您服务器的数据安全。

> 说明 云安全中心基础版和基础杀毒版只提供漏洞检测，不提供漏洞修复的服务；如需一键修复漏洞，请开通云安全中心高级版或企业版。基础版、基础杀毒版、高级版和企业版详细功能介绍请参见功能特性。

查看漏洞基本信息

1. 登录云安全中心控制台。
2. 在左侧导航栏单击安全防范 > 漏洞修复。
3. 在漏洞修复页面单击Windows系统漏洞页签。
4. 在Windows系统漏洞页面，查看和管理云安全中心检测到的所有Windows系统漏洞信息。您可以执行以下操作：
   - 查看漏洞信息

     
   - 查看漏洞的修复紧急程度建议

     漏洞的建议修复紧急度用不同颜色的图标表示，图标中的数字表示存在该漏洞的资产数量。 以下是图标颜色和漏洞修复紧急度的对应关系：
     - 红色图标：表示漏洞修复紧急度为高。
     - 橙色图标：表示漏洞修复紧急度为中。
     - 灰色图标：表示漏洞修复紧急度为低。

     

     > 说明 建议立即修复高危漏洞（紧急程度为高）。
   - 将漏洞加入白名单

您可在**Windows系统漏洞**页面，选中需要加入白名单的漏洞并单击**加入白名单**，将该漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。

加入白名单的漏洞将从**Windows系统漏洞**的漏洞列表中移除，并记录在**漏洞管理设置**页面的**漏洞白名单配置**列表中。

如需恢复云安全中心对白名单中漏洞的检测和告警提示，可在**漏洞管理设置**页面移除该漏洞。

- **搜索漏洞**

  您可在**Windows系统漏洞**页面通过筛选漏洞危险等级（高、中、低）、漏洞处理状态（已处理、未处理）、资产分组、VPC名称或输入漏洞名称定位到相关的漏洞。

  

  > **说明** 漏洞名称支持模糊搜索。

- **导出漏洞**

  您可在**Windows系统漏洞**页面，单击 

图标，将云安全中心检测到的所有Windows系统漏洞统一导出并保存到本地。导出的文件为Excel格式。

  > **说明** 根据您资产中漏洞数据的大小，导出漏洞列表可能需要耗费一定时间，请耐心等待。

查看漏洞详情和处理漏洞

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 漏洞修复**。
3. 在**漏洞修复**页面单击**Windows系统漏洞**页签。
4. 在Windows系统漏洞列表，单击**漏洞公告**名称或**漏洞公告**对应**操作**栏的**修复**，可展开对应的**漏洞详情**页面。您可查看该漏洞的**漏洞详情**和**待处理漏洞**数量及待处理漏洞关联资产。

   

5. 在**漏洞详情**页面，查看漏洞详情并处理漏洞。您可以根据需要执行以下操作：
   - **查看漏洞详情**

     漏洞详情页面可展示该漏洞所有关联漏洞，即该漏洞影响的所有资产信息，方便您对所有相关的漏洞进行分析和批量处理。

     - 您可在**漏洞详情**页面查看该漏洞公告关联的所有漏洞简介。
     - 单击**待处理漏洞**页签，直接跳至**漏洞详情**下的漏洞影响资产列表。

       您可在漏洞影响资产列表，查看该漏洞影响的所有资产、漏洞的状态等信息，并可对漏洞执行验证、修复、加入白名单或忽略的操作。

       

   - **查看漏洞严重等级**

     Windows系统漏洞的修复紧急程度，参考微软官方对相应漏洞的评级。漏洞修复紧急程度用不同颜色的图标表示：

     - 红色：修复紧急程度为**高**，对应微软官方的漏洞等级为**危急**或**高危**。

- 橙色：修复紧急程度为**中**，对应微软官方的漏洞等级为**中**。
- 灰色：修复紧急程度为**低**，对应微软官方的漏洞等级为**低**。

> **说明** 建议您立即修复紧急程度为高的漏洞。

- **查看漏洞详细状态**
  - **已处理**
    - **修复成功**：漏洞已执行一键修复并修复成功。
    - **已忽略**：漏洞已执行**忽略**的操作，云安全中心将不再对该漏洞进行告警。
  - **未处理**
    - **未修复**：漏洞待修复。
    - **修复中**：漏洞正在修复处理中。
    - **修复失败**：漏洞修复失败，可能因为漏洞文件已被修改或漏洞文件已不存在。
    - **验证中**：执行验证操作后，漏洞状态将变为**验证中**。
- **处理受影响资产漏洞**

  您可在漏洞影响资产列表中，对受影响资产漏洞进行修复、验证、加入白名单或忽略的操作。

  

  您可以根据需要进行以下操作：

- **修复漏洞**

  您需要分以下两种情况修复漏洞：

  - **修复按钮显示正常**

    单击**修复**，修复单个漏洞或批量修复多个关联漏洞。修复漏洞时支持自动创建快照并修复。您可以根据需要选择**自动创建快照并修复**或**不建立快照备份直接修复**。

    > **说明**
    >
    > - 系统在修复漏洞时，可能存在一定的失败风险，建议您在修复漏洞前选中**自动创建快照并修复**对系统进行快照备份。快照的更多信息请参见ECS服务的**快照概述**。
    > - 创建快照将产生一定的费用，费用由快照产品收取（40 GB的系统盘，快照存储一天的费用大约是0.15元）。快照计费方式更多信息请参见**快照计费**。

    Windows系统漏洞修复

  - **修复按钮显示为灰色**

    服务器的磁盘空间过小、Windows Update服务正在运行中等原因都会导致Windows服务器上的漏洞修复失败。服务器出现此类情况时，云安全中心会将漏洞的修复按钮置为灰色。您需要先手动处理服务器的这些问题，才能在云安全中心控制台上修复该服务器上的漏洞。您可以将鼠标移至修复按钮处，查看服务器存在的问题和云安全中心提供的问题处理建议。以下是您需要手动处理的服务器异常情况：

    - Windows Update服务正在运行中。

      处理建议：稍后再操作或手动结束该服务器中的Wusa进程，然后再次在云安全中心控制台上尝试修复该漏洞。

    - 服务器Windows Update Service已被禁用。

      处理建议：进入该服务器的系统服务管理器，开启Windows Update Service后，再次在云安全中心控制台上尝试修复该漏洞。

    - 服务器磁盘空间小于500 MB。

      处理建议：扩容或清理磁盘后，再次在云安全中心控制台上尝试修复该漏洞。

- **验证漏洞**

  单击**验证**，验证单个漏洞或批量验证多个关联漏洞，检测该漏洞是否已修复成功。

  单击**验证**后，该漏洞的**状态**转为**验证中**。需要等待数秒后漏洞验证才可完成。

- **将漏洞加入白名单**

  单击**漏洞详情**页面右上角**加入白名单**，将该漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。

  加入白名单的漏洞将从**Windows系统漏洞**的漏洞列表中移除，并记录在**漏洞管理设置**页面的**漏洞白名单配置**列表中。

  如需恢复云安全中心对白名单中漏洞的检测和告警提示，可在**漏洞管理设置**页面**移除**该漏洞。

- **忽略漏洞**

  定位到需要忽略的漏洞，单击其操作列 图标后选择**忽略**，在确认对话框中填写忽略操作说明并单击**确定**，云安全中心将不再提示该漏洞。

  您可以在**已处理**漏洞中查看已忽略的漏洞和忽略该漏洞时填写的操作说明。

  

  > **说明** 被忽略漏洞的状态将转为**已忽略**。如需云安全中心继续对该漏洞进行告警提示，可在**已处理**的漏洞列表中找到该漏洞并对其取消忽略。

- **搜索漏洞影响资产**

  在漏洞影响资产列表上方，通过筛选漏洞危险等级（高、中、低）、VPC名称、资产分组、漏洞处理状态（已处理、未处理）或输入服务器IP或名称定位到相关的漏洞影响的资产。

  

  > **说明** 服务器IP或名称支持模糊查询。

- **导出漏洞影响资产**

  在漏洞影响资产列表左上方，单击导出图标，将云安全中心检测到的该漏洞下的影响资产统一导出并保存到本地。导出的文件为Excel格式。

  > **说明** 根据受影响资产数量的大小，导出资产列表可能需要耗费一定时间，请耐心等待。

- **保存已筛选漏洞**

  在漏洞影响资产列表左上方，单击

  

  图标保存筛选出的所有漏洞为一个漏洞修复批次，方便您对该批次漏洞的状态进行持续跟踪。

  

相关文档

云安全中心修复Windows实例漏洞时出现“0x80240017 104 （Patch Not Applicable）”报错

1.6. Web-CMS漏洞

云安全中心支持检测并快速修复Web-CMS漏洞。Web-CMS漏洞检测功能可监控网站目录并识别通用建站软件（通过漏洞文件比对方式检测建站软件中的漏洞）。本文档介绍了如何查看Web-CMS漏洞的相关信息和对Web-CMS漏洞进行处理。

背景信息

Web-CMS漏洞功能通过及时获取最新的漏洞预警和相关补丁，并通过云端下发补丁更新，实现快速发现和快速修复漏洞的功能。云安全中心Web-CMS漏洞功能可帮助您解决漏洞发现不及时、不会修复漏洞、无法批量进行补丁更新等诸多问题。

> 说明
>
> - 云安全中心基础版和基础杀毒版只提供漏洞检测，不提供漏洞修复的服务；如需一键修复漏洞，请开通云安全中心高级版或企业版。基础版、基础杀毒版、高级版和企业版详细功能介绍请参见功能特性。
> - 在云安全中心控制台修复Web-CMS漏洞后立即生效，无需再次验证。

查看漏洞基本信息

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 漏洞修复**。
3. 在**漏洞修复**页面单击**Web-CMS漏洞**页签。
4. 在**Web-CMS漏洞**页面，查看云安全中心检测到的所有Web-CMS漏洞信息。
   - **查看漏洞信息**

     
   - **查看漏洞的修复紧急度建议**

     Web-CMS类型漏洞已经过阿里云安全工程师确认会导致严重危害，因此所有检查出的Web-CMS漏洞修复紧急程度都为高，并用红色图标表示。

     

     > 说明 建议尽快修复Web-CMS类型漏洞。
   - **将漏洞加入白名单**

     您可在**Web-CMS漏洞**页面，选中需要加入白名单的漏洞并单击**加入白名单**，将该漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。

     

     加入白名单的漏洞将从**Web-CMS漏洞**的漏洞列表中移除，并记录在**漏洞管理设置**页面的**漏洞白名单配置**列表中。

     如需恢复云安全中心对白名单中漏洞的检测和告警提示，可在**漏洞管理设置**页面移除该漏洞。

     

   - **批量修复漏洞**

     批量修复功能会自动识别您选择的漏洞公告对应的资产，并修复这些资产中您所选择的漏洞。您可在**Web-CMS漏洞**页面，选择需要批量修复的漏洞并单击**批量修复**。在**批量修复**对话框中查看云安全中心为您识别出的需要修复漏洞的资产列表，单击**立即修复**。

     > 说明 批量修复功能仅支持选择当前页面的漏洞，不支持跨页选择漏洞。漏洞列表每页可以展示10、20或50条漏洞信息，即您最多可以选择50个漏洞进行批量修复。
   - **搜索漏洞**

     您可在**Web-CMS漏洞**页面，通过筛选漏洞危险等级（高、中、低）、漏洞处理状态（已处理、未处理）、资产分组或输入漏洞名称定位到相关的漏洞。

     

> **说明** 漏洞名称支持模糊搜索。

- **导出漏洞**

  您可在**Web-CMS漏洞**页面，单击**导出**图标，将云安全中心检测到的所有Web-CMS漏洞统一导出并保存到本地。导出的文件为Excel格式。

  > **说明** 根据您资产中漏洞数据的大小，导出漏洞列表可能需要耗费一定时间，请耐心等待。

处理漏洞

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 漏洞修复**。
3. 在**漏洞修复**页面单击**Web-CMS漏洞**页签。
4. 在漏洞列表中，单击**漏洞公告**名称或**漏洞公告**对应**操作**栏的**修复**，可展开对应的**漏洞详情**页面。 您可查看该漏洞的漏洞详情、待处理漏洞数量及关联资产信息。

   

5. 在**漏洞详情**页面，查看并处理漏洞。您可以根据需要执行以下操作：
   - **查看漏洞详情**

     漏洞详情页面可展示该漏洞所有关联漏洞，即该漏洞影响的所有资产信息，方便您对所有相关的漏洞进行分析和批量处理。

     - 在**漏洞详情**页签下，查看该漏洞公告简介和修复方案。
     - 单击**待处理漏洞**页签，查看漏洞影响资产列表。

       您可在漏洞影响资产列表，查看该漏洞影响的所有资产、漏洞的状态等信息，并可对漏洞执行验证、修复、加入白名单或忽略的操作。

     

     在**漏洞详情**页面的漏洞列表中，单击**影响资产**名称可跳转到**资产中心 > 漏洞信息**页面，为您展示该资产关联的所有Web-CMS漏洞信息。

     

   - **查看漏洞的修复紧急度建议**

     Web-CMS类型漏洞已经过阿里云安全工程师确认会导致严重危害，因此所有检查出的Web-CMS漏洞修复紧急程度都为高，并用红色图标表示。

     

     > **说明** 建议尽快修复Web-CMS类型漏洞。

   - **搜索漏洞**

     在漏洞影响资产列表上方，通过筛选漏洞危险等级（高、中、低）、VPC名称、资产分组、漏洞处理状态（已处理、未处理）或输入服务器IP或名称定位到相关的漏洞影响的资产。

     

     > **说明** 搜索服务器IP或名称支持模糊查询。

- **查看漏洞详细状态**
  - **已处理**
    - 修复成功：漏洞已执行一键修复并修复成功。
    - 已忽略：漏洞已执行**忽略**的操作，云安全中心将不再对该漏洞进行告警。
    - 漏洞已失效：云安全中心重新检测Web-CMS漏洞时未发现该漏洞，可能由于您已删除该漏洞文件。
  - **未处理**
    - 未修复：漏洞待修复。
    - 修复中：漏洞正在修复处理中。
    - 修复失败：漏洞修复失败，可能因为漏洞文件已被修改或漏洞文件已不存在。
    - 验证中：漏洞已修复后验证漏洞是否已修复成功。
- **处理受影响资产漏洞**

  您可在漏洞影响资产列表中，对受影响资产漏洞进行修复、验证、加入白名单或忽略的操作。

  处理漏洞

  - **修复漏洞**

    单击**修复**，修复单个或多个关联漏洞。在**修复**对话框中单击**立即修复**。

    修复漏洞

    > **说明** 建议在修复漏洞前，对业务系统做好安全备份措施，避免异常情况造成业务中断。

  - **验证漏洞**：如果您手动修复了Web-CMS漏洞，需要执行验证操作，验证结束后漏洞状态才会刷新。在云安全中心控制台上修复的Web-CMS漏洞会立即生效，无需再次验证。
  - **将漏洞加入白名单**

    单击**漏洞详情**页面右上角**加入白名单**，将该漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。

    加入白名单的漏洞将从**Web-CMS漏洞**的漏洞列表中移除，并记录在**漏洞管理设置**页面的**漏洞白名单配置**列表中。

    如需恢复云安全中心对白名单中漏洞的检测和告警提示，可在**漏洞管理设置**页面**移除**该漏洞。

  - **忽略漏洞**

    定位到需要忽略的漏洞，单击其操作列 图标后选择**忽略**，在确认对话框中填写忽略操作说明并单击**确定**，云安全中心将不再提示该漏洞。

    您可以在**已处理**漏洞中查看已忽略的漏洞和忽略该漏洞时填写的操作说明。

    > **说明** 被**忽略**漏洞的状态将转为**已忽略**。如需云安全中心继续对该漏洞进行告警提示，可在**已处理**的漏洞列表中找到该漏洞并对其**取消忽略**。

- **导出漏洞影响资产**

在漏洞影响资产列表左上方，单击导出图标，将云安全中心检测到的该漏洞下的影响资产统一导出并保存到本地。导出的文件为Excel格式。

> 说明 根据受影响资产数量的大小，导出资产列表可能需要耗费一定时间，请耐心等待。

- **保存已筛选漏洞**

  在漏洞影响资产列表左上方，单击

  

  图标保存筛选出的所有漏洞为一个漏洞修复批次，方便您对该批次漏洞的状态进行持续跟踪。

  

1.7. 应用漏洞

应用漏洞检测功能可以检测主流的应用漏洞类型。本文档介绍了如何查看应用漏洞的相关信息和处理应用漏洞。

限制说明

应用漏洞检测功能存在以下限制。

限制项目	限制信息
资产类型	只支持阿里云ECS服务器，不支持非阿里云服务器和IDC服务器。
版本类型	仅云安全中心企业版支持应用漏洞检测，基础版、基础杀毒版和高级版不支持该功能。

> 注意 云安全中心仅支持检测应用漏洞，不支持修复应用漏洞。您需要根据漏洞详情页面提供的修复建议手动修复应用漏洞。

查看漏洞基本信息

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 漏洞修复**。
3. 在**漏洞修复**页面单击**应用漏洞**页签。
4. 在**应用漏洞**页面，查看云安全中心检测到的所有应用漏洞。

   

   您可根据需要执行以下操作：

   - **搜索漏洞**

     您可在应用漏洞页面通过筛选扫描方式（Web扫描器、软件成分分析）、漏洞处理状态（已处理、未处理）、漏洞危险等级（高、中、低）、资产分组、VPC名称、搜索漏洞名称或输入服务器IP、名称定位到相关的漏洞。

     

   - **查看漏洞公告信息**

     

- **查看漏洞扫描方式**

  应用漏洞支持以下扫描方式：

  - **Web扫描器**：通过检测网络流量识别您系统中的安全漏洞，例如SSH弱口令、远程命令执行。
  - **软件成分分析**：通过采集客户端软件版本信息识别您系统中的安全漏洞，例如Apache Shiro授权问题漏洞、Kubernetes kubelet资源管理错误漏洞。

- **查看漏洞的修复紧急度和影响资产数量**

  漏洞的建议修复紧急度用不同颜色的图标表示，图标中的数字表示存在该漏洞的资产数量。 以下是图标颜色和漏洞修复紧急度的对应关系：

  - 红色图标：表示漏洞修复紧急度为**高**。
  - 橙色图标：表示漏洞修复紧急度为**中**。
  - 灰色图标：表示漏洞修复紧急度为**低**。

  

  > **说明** 建议您立即修复紧急程度为高的漏洞。

- **将漏洞加入白名单**

  您可在**应用漏洞**页面，选中需要加入白名单的漏洞并单击**加入白名单**，将一个或多个漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。

  加入白名单的漏洞将从**应用漏洞**的漏洞列表中移除，并记录在**漏洞管理设置**页面的**漏洞白名单配置**列表中。

  如需恢复云安全中心对白名单中漏洞的检测和告警提示，可在**漏洞管理设置**页面**移除**该漏洞。

  

- **导出漏洞**

  您可在**应用漏洞**页面单击 图标，将云安全中心检测到的所有应用漏洞软件统一导出并保存到本地。

  导出的文件为Excel格式。

  > **说明** 根据您资产中漏洞数据的大小，导出漏洞列表可能需要耗费一定时间，请耐心等待。

查看漏洞详情和处理漏洞

> **说明** 云安全中心仅支持检测应用漏洞，不支持修复应用漏洞。您需要根据**漏洞详情**页面提供的修复建议手动修复应用漏洞。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 漏洞修复**。
3. 在**漏洞修复**页面单击**应用漏洞**页签。
4. 定位到需要查看的漏洞，单击该漏洞的**漏洞公告**名称或操作列的**修复**，展开对应漏洞的**漏洞详情**页面。
5. 在**漏洞详情**页面，查看漏洞详情并处理漏洞。您可根据需要执行以下操作：

   - **查看漏洞详情**

     漏洞详情页面可展示该漏洞公告所有关联漏洞，及漏洞影响的所有资产信息，方便您对所有相关的漏洞进行分析和批量处理。您可以查看以下内容：

- 在漏洞详情页签查看该漏洞公告关联的所有漏洞、漏洞的描述、影响分和漏洞特征信息。
- 单击**待处理漏洞**页签，查看漏洞影响的资产列表。

  您可查看该漏洞影响的所有资产和资产漏洞状态等信息，并可对漏洞执行验证、加入白名单、忽略或取消忽略的操作。

  

  单击漏洞列表中**影响资产**列的目标资产名称，可跳转到**资产中心 > 漏洞信息 > 应用漏洞**页面，了解该资产中检测到的应用漏洞信息。

- **查看阿里云漏洞库详细信息**

  在**漏洞详情**页面，单击**漏洞编号**可跳转至阿里云漏洞库。您可在阿里云漏洞库页面，查看该漏洞更加详细的信息，包括漏洞的描述、基本信息、修复建议等信息。

- **查看漏洞详细状态**

  漏洞状态可分为已处理和未处理：

  - **已处理**
    - 修复成功：该应用漏洞已成功修复。
    - 已忽略：漏洞已执行**忽略**的操作，云安全中心将不再对该漏洞进行告警。
  - **未处理**
    - **未修复**：漏洞待修复。
    - 验证中：执行验证操作后，漏洞状态将变为验证中。

  > **说明** 应用漏洞列表默认为您展示所有**未处理**的应用漏洞。

- **验证漏洞**

  您根据**漏洞详情**页面的**修复建议**手动修复漏洞后，需要执行**验证**查看漏洞是否已被修复。您需要定位到需验证的漏洞，并单击其操作列下的**验证**。

  对漏洞进行验证后，漏洞的**状态**会变更为**验证中**。需要等待数秒才可完成漏洞验证。

  漏洞验证完成后有以下两种结果：

  - 验证成功：该漏洞的状态将变为**已修复**，您可以在**已处理**的漏洞列表中查看该漏洞。
  - 验证失败：该漏洞的状态将变为**未修复**，说明该漏洞未修复。建议您排查漏洞修复失败原因，及时处理该漏洞。

- **忽略漏洞**

  如果某漏洞无需关注，您可以忽略该漏洞。您可以定位到需忽略的漏洞，并单击其操作列下的**忽略**。忽略操作执行完成后，云安全中心将不再提示该漏洞。

  > **说明** 被忽略漏洞的状态将转为**已忽略**。如需云安全中心继续对该漏洞进行告警提示，可在**已处理**的漏洞列表中找到该漏洞并对其**取消忽略**。

支持检测的应用漏洞类型

应用漏洞类型	检测项
	OpenSSH服务

应用漏洞类型	检测项
系统服务弱口令	MySQL数据库服务
	MSSQL数据库服务
	MongoDB数据库服务
	FTP、VSFTP、ProFTPD服务
	Memcache缓存服务
	Redis缓存服务
	Subversion版本控制服务
	SMB文件共享服务
	SMTP邮件发送服务
	POP3邮件接收服务
	IMAP邮件管理服务
系统服务漏洞	OpenSSL心脏滴血
	SMB • Samba • 弱口令暴力破解
	RSYNC • 匿名访问导致敏感文件信息 • 认证密码暴力破解
	VNC密码暴力破解
	pcAnywhere密码暴力破解
	Redis密码暴力破解
	phpMyAdmin弱口令检测
	Tomcat控制台弱密码检测
	Apache Struts 2远程命令执行漏洞
	Apache Struts 2远程命令执行漏洞（S2-046）
	Apache Struts 2远程命令执行漏洞（S2-057）
	ActiveMQ CVE-2016-3088任意文件上传漏洞
	Confluence任意文件读取漏洞

应用漏洞类型	检测项
应用服务漏洞	CouchDB Query Server远程命令执行
	Discuz!后台管理员弱口令破解
	Docker未授权访问漏洞
	Drupal Drupalgeddon 2远程代码执行CVE-2018-7600
	ECshop登录接口代码执行漏洞
	Elasticsearch未授权访问
	Elasticsearch MvelRCE CVE-2014-31
	Elasticsearch Groovy RCE CVE-2015-1427
	泛微OA表达式注入
	Hadoop YARN ResourceManager未授权访问
	JavaServer Faces 2目录遍历漏洞
	JBoss EJBInvokerServlet Java反序列化漏洞
	Jenkins Manage匿名访问CVE-2018-1999001、CVE-2018-1999002
	Jenkins未授权访问
	Jenkins Script Security Plugin RCE
	Kurbernetes未授权访问漏洞
	MetInfo getPassword接口存在SQL注入漏洞
	MetInfo login接口存在SQL注入漏洞
	PHPCMS 9.6任意文件上传漏洞
	PHP-CGI远程代码执行
	Actuator unauth RCE
	ThinkPHP_RCE_20190111
	WebLogic UDDI Explorer SSRF漏洞
	WordPress xmlrpc.php存在SSRF漏洞
	Zabbix Web控制台暴力破解
	OpenSSL心脏滴血检测
	Apache Tomcat WEB-INF配置文件未授权访问

1.8. 应急漏洞

云安全中心支持对近期互联网上爆发的高危应急漏洞进行检测，帮助您及时确认您的资产是否有受到影响。本文档介绍了如何查看应急漏洞详情和对应急漏洞进行处理。

背景信息

应急漏洞功能具有以下特性：

- 支持自定义设置需要检测的漏洞危险等级。
- 支持应急漏洞按披露时间排序。
- 支持应急漏洞检测并展示检测进度。
- 支持应急漏洞告警，实时展示应急漏洞影响的资产信息和漏洞详情。
- 支持展示应急漏洞的修复紧急程度、并提供修复建议。
- 支持应急漏洞修复完成后进行验证，检测该漏洞是否已成功修复。

> 说明
> - 云安全中心基础版、基础杀毒版、高级版和企业版都支持应急漏洞功能。
> - 云安全中心只支持检测应急漏洞并提供修复建议，不支持一键修复应急漏洞。您需要根据应急漏洞详情页面的修复建议在受影响的服务器中手动修复应急漏洞。

限制说明

仅阿里云ECS服务器支持应急漏洞的检测，非阿里云服务器和IDC服务器不支持该功能。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 漏洞修复**。
3. 在**漏洞修复**页面单击**应急漏洞**页签。
4. 在**应急漏洞**页面，查看云安全中心检测到的最新应急漏洞情况和应急漏洞记录，并对应急漏洞进行检测，确认该漏洞是否对您的资产有影响。您可以进行以下操作：
   - **检测漏洞**

     在漏洞列表中，单击待检测漏洞右侧的**立即检测**，对应急漏洞立即执行检测。

     您也可以在**最新系统漏洞发现时间**下单击**一键扫描**，在**一键检测**对话框中选择**应急漏洞**，并单击**确定**。云安全中心会为您检测所有服务器上是否存在应急漏洞。一键扫描更多信息请参见一键扫描漏洞。

     如果有检测到风险，**风险数**会红色高亮显示，并展示存在该应急漏洞的资产数量。您可单击该应急漏洞名称前往漏洞详情页面，查看漏洞具体信息，并对该漏洞进行处理。

     

     > 说明 对于从未被检测过的漏洞，会在**风险数**一栏中提示**未检测**。

     执行立即检测后，可实时展示该应急漏洞的检测进度。

     

   - **搜索漏洞**

您可在**应急漏洞**页面，通过筛选漏洞检测方式（版本检测、网络扫描）、风险状态（存在风险、无风险）或输入漏洞名称定位到相关的漏洞。

以下是两种检测方式的说明：

- **版本检测**：通过采集软件版本信息对内网资产进行漏洞识别和分析。
- **网络扫描**：云安全中心提供Web扫描器为您检测公网资产中是否存在漏洞，您无需进行任何配置即可使用网络扫描检测漏洞。

- **查看受影响资产的漏洞详细状态**

状态	子状态	说明
已处理	修复成功	表示漏洞已成功修复。
	修复失败	表示漏洞修复失败，可能因为漏洞文件已被修改或漏洞文件已不存在。
	已忽略	漏洞已执行**忽略**的操作，云安全中心将不再对该漏洞进行告警。
	漏洞已失效	表示该漏洞在7天内未被再次扫描到。
	未处理	未修复

- **查看受影响资产的漏洞修复紧急度**

  漏洞修复紧急度是根据漏洞等级、公开时间、服务器真实环境等因素综合分析出来的修复建议说明，分为高、中、低三个等级。

  > **说明** 建议立即修复紧急度为高的漏洞。

- **处理应急漏洞**

  云安全中心只支持检测应急漏洞并提供修复建议，不支持一键修复应急漏洞。您需要根据应急漏洞详情页面的**修复建议**在受影响的服务器中手动修复**应急漏洞**。

  您可以执行以下操作：

  - **查看漏洞详情页面提示的漏洞修复建议**，在受影响的服务器中手动进行修复。
  - **验证**：漏洞修复完成后可验证漏洞是否已修复成功。
  - **忽略**：忽略漏洞后，云安全中心将不再提示该漏洞。

    > **说明** 被**忽略**漏洞的状态将转为**已忽略**。如需云安全中心继续对该漏洞进行告警提示，可在**已处理**的漏洞列表中找到该漏洞并对其**取消忽略**。

相关文档

为什么fastjson类的应急漏洞多次扫描时每次检测结果可能不一致？

1.9. 漏洞管理设置

您可通过漏洞管理设置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开启漏洞检测、设置漏洞扫描周期和扫描方式、对已失效漏洞设置自动删除周期或将漏洞从白名单中移除。本文介绍了相关配置的详细操作步骤。

背景信息

云安全中心支持在Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞、应用漏洞列表中批量添加漏洞至白名单。添加成功后，系统将不再检测漏洞白名单中的漏洞。您可根据实际情况在**漏洞管理设置**页面移除已添加到白名单中的漏洞。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 漏洞修复**。
3. 在**漏洞修复**页面右上角单击**漏洞管理设置**
4. 在**漏洞管理设置**页面，选择您需要的配置。

   您可以执行以下操作：

   - 单击漏洞类型右侧的切换开关，开启或关闭该漏洞检测。
   - 单击**管理**，添加开启该漏洞检测的服务器。

     

   - 设置**应急漏洞扫描周期**：默认扫描时间段为*00:00:00*至*07:00:00*，可设置每隔三天、一周、两周执行一次扫描任务，或者设置为停止扫描。

     > **说明** 如果您的服务器与公网隔离，遭受黑客攻击的可能性较小，或者有其他无需进行应急漏洞检测的场景，您可以将**应急漏洞扫描周期**设置为**停止扫描**。由于黑客可以通过多种方式攻击的您的服务器，建议您开启应急漏洞周期性扫描，以便云安全中心帮助您及时发现服务器上的应急漏洞。

   - 设置**应用漏洞扫描周期**。默认扫描时间段为*00:00:00*至*07:00:00*，可设置每隔三天、一周或两周执行一次扫描任务。
   - 选择**YUM/APT源配置**。在修复任意Linux软件漏洞时都需要配置正确的YUM或APT源。如果YUM或APT源配置不正确，会导致漏洞修复失败。云安全中心为您自动选择阿里云的**YUM/APT源配置**，帮助您有效地提高漏洞修复成功率。建议您选择**YUM/APT源配置**。
   - 选择**扫描方式**。您可以选择以下扫描方式：
     - **真实风险模式**：基于黑客视角，对系统中存在的漏洞进行自动化分析，为您扫描和展示真实可被利用的漏洞。选择该模式后，在**漏洞修复**页面仅展示紧急度得分大于等于13.5分的漏洞。如果您只需要展示修复紧急度较高的漏洞，建议您选择该模式。

       > **说明**
       > - 紧急度得分可以帮助您判断一个漏洞是否应该优先修复。紧急度得分大于等于13.5分通常是高危漏洞，即需尽快修复的漏洞。更多信息请参见漏洞修复优先级。
       > - **真实风险模式**和**全量规则扫描模式**下，完成漏洞扫描需要1~5分钟。

- **全量规则扫描模式**：覆盖合规类漏洞，扫描的漏洞类型更加全面。选择该模式后，在**漏洞修复**页面为您展示所有危险等级的漏洞信息。

- 设置失效漏洞自动删除周期：可设置7天、30天或90天。

  > **说明** 如果对检测出来的漏洞不做任何处理、或修复后再次检测时未发现该漏洞，在达到您设置的失效漏洞自动删除周期时，该漏洞记录将自动从**安全防范 > 漏洞修复**页面的漏洞列表中移除。后续当云安全中心再次检测出同类漏洞时，仍会产生告警。

- 设置**漏洞扫描等级**：可选择**高**、**中**、**低**。

  云安全中心只检测并展示您在**漏洞扫描等级**中已选择等级的漏洞。例如您选择了**高**和**中**后，云安全中心只检测漏洞修复紧急度为**高**和**中**的漏洞，您只能在**漏洞修复**页面查看修复紧急度为**高**和**中**的漏洞，无法查看修复紧急度为低的漏洞。

- 在**漏洞白名单配置**列表中可查看已加入白名单的漏洞。您需要将漏洞从白名单中移除时，仅需选择相应漏洞，并单击**移除**。从白名单移除后，云安全中心将重新启用对该漏洞的检测和告警。

1.10. 服务器软件漏洞修复建议

修复服务器软件漏洞时可参考本文提供的方法和建议，确保漏洞修复的有效性和可靠性。

> **说明** 本文提供的建议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流程

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备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修复流程：

修复前

- 修复人员应对目标服务器系统进行资产确认，并通过云安全中心对目标服务器系统上检测出的漏洞进行确认。
- 修复人员在确认目标服务器上的系统漏洞后，应确认哪些系统漏洞需要修复。并不是所有被发现的软件漏洞都需要在第一时间进行修复，应根据实际业务情况、服务器的使用情况、及漏洞修复可能造成的影响来判定漏洞是否需要修复。
- 修复人员在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漏洞修复测试报告。漏洞修复测试报告应包含漏洞修复情况、漏洞修复的时长、补丁本身的兼容性、漏洞修复可能造成的影响。
- 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服务器进行备份。例如，通过ECS的快照功能备份目标ECS实例。

修复中

- 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），防止出现误操作的情况。
- 修复人员按照待修复的系统漏洞列表，逐项进行升级、修复。

修复后

- 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。
- 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

为了确保在服务器软件漏洞修复过程中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，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。

- **使用仿真测试环境**

  通过使用仿真测试环境，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。

  仿真测试环境要求：

  - 仿真测试环境中系统环境（操作系统、数据库系统）与在线业务系统完全一致。
  - 仿真测试环境中应用系统与在线业务系统完全一致。
  - 测试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。当系统环境异常或数据丢失时，系统备份可以及时对系统进行恢复，确保业务稳定。建议使用云安全中心漏洞修复自动快照功能对业务系统进行快速、高效的备份。

  > 说明 仅Linux软件漏洞和Windows系统漏洞支持自动创建快照修复漏洞。

1.11. 排查漏洞修复失败的原因

本文档列举了使用云安全中心漏洞修复功能修复漏洞时失败的可能原因，您可以参考本文内容进行问题排查。

概述

服务器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。本文已覆盖常见的修复失败原因，如果您在按照本文档列出的原因进行排查后，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和排查。

适用范围

本文适用于排查以下类型漏洞修复失败的原因：

- Linux软件漏洞
- Windows系统漏洞
- Web-CMS漏洞

Linux软件漏洞和Windows系统漏洞修复失败的可能原因

在您使用云安全中心漏洞修复功能修复Linux软件漏洞或Windows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 建议您及时修复您服务器上的系统软件漏洞。更多信息请参见服务器软件漏洞修复建议。

1. 检查您的服务器Agent是否离线。Agent离线将导致漏洞修复失败。服务器的网络连接异常、CPU或内存占用率过高等问题都会导致服务器Agent离线。如果您服务器的Agent处于离线状态，建议您及时排查原因并进行相应处理。更多信息请参见Agent离线排查。

2. 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，会导致云安全中心漏洞修复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。

3. 检查您是否有磁盘文件系统读写执行权限。如果您没有磁盘文件的读写权限，漏洞修复会因为无法成功下载补丁安装包而失败。

   如果确认您没有磁盘文件系统读写权限，您需要更改磁盘文件系统的读写权限。确认权限修改成功后，重新修复该漏洞。

4. 根据您的服务器操作系统查看其它可能原因：

   - **Linux系统服务器**

     确认是否是由于系统更新源配置问题导致无法安装更新。建议您在**漏洞管理设置**页面，选中**YUM/APT源配置**。选中该配置后，在修复Linux软件漏洞时云安全中心会为您自动选择阿里云的YUM/APT修复漏洞，帮助您有效地提高漏洞修复成功率。

     参考以下内容将系统的ATP源配置到阿里云源：

     - Ubuntu系统
     - CentOS系统
     - 其他系统

     更多Linux软件漏洞相关问题请参见常见问题。

   - **Windows系统服务器**

     a. **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，您可以尝试重执行漏洞修复操作。

     b. **补丁安装包不匹配**

        云安全中心漏洞修复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，请您在云安全中心**漏洞修复**页面忽略该漏洞。

     c. **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，建议您在当前补丁安装完成后再重新执行漏洞修复操作。

     d. **检查其他设置**

        a. 检查Windows Update服务的Cryptographic Services服务是否正常运行。

        b. 检查Users用户是否对*C:\Windows*目录有读取和执行的权限。

        c. 运行Windows Update，查看是否正常工作。

        d. 重置Windows更新组件，更多信息请参见Windows 更新-其他资源。

        e. 排查更新失败原因，更多信息请参见Windows Update补丁更新失败排查。

Web-CMS漏洞修复失败可能原因

在您使用云安全中心漏洞修复功能修复Web-CMS漏洞时，如果提示漏洞修复失败，请参考以下可能原因：

1. 检查您的服务器Agent是否离线。Agent离线将导致漏洞修复失败。服务器的网络连接异常、CPU或内存占用率过高等问题都会导致服务器Agent离线。如果您服务器的Agent处于离线状态，建议您及时排查原因并进行相应处理。更多信息请参见Agent离线排查。
2. 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，导致云安全中心无法进行漏洞修复。

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

3. 确认云安全中心漏洞修复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云安全中心在进行安装匹配验证时发现该文件的MD5值不一致，云安全中心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，可通过云安全中心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（此时该漏洞状态显示为**已修复**），说明您已成功修复该漏洞。

4. 如果云安全中心漏洞修复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。

5. 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，会导致云安全中心漏洞修复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。

2.基线检查

2.1. 基线检查概述

基线检查功能针对服务器操作系统、数据库、软件和容器的配置进行安全检测，并提供检测结果说明和加固建议。基线检查功能可以帮您进行系统安全加固，降低入侵风险并满足安全合规要求。

应用场景

功能描述

云安全中心的基线检查功能支持检测操作系统和服务（数据库、服务器软件、容器等）的弱口令、账号权限、身份鉴别、密码策略、访问控制、安全审计和入侵防范等安全配置，并提供检测结果，针对存在的风险配置给出加固建议。具体检测内容请参见基线检查内容。

基线检查默认策略每隔一天在00:00~06:00进行一次全面的自动检测。策略管理支持自定义策略、自定义弱口令字典和设置基线检查等级（高、中、低）。更多信息请参见设置基线检查策略。

限制说明

基线检查功能为云安全中心的增值服务，仅高级版和企业版用户可开通和使用该服务。基础版、基础杀毒版用户都需先升级到高级版或企业版才可使用基线检查功能。有关升级的更多信息请参见升级与降配。

以下表格介绍不同版本支持的基线检查类型详情。

基线检查项类型	基础版	基础杀毒版	高级版	企业版
弱口令	X	X	√	√
高危风险利用	X	X	X	
最佳安全实践				
容器安全				
等保合规				

以下表格介绍高级版和企业版策略管理能力的不同点。

版本	基线分类支持	策略管理	自动修复
高级版	弱口令	不支持	不支持
企业版	• 高危风险利用 • 容器安全 • 最佳安全实践 • 等保合规 • 弱口令	支持	Linux系统的阿里云标准和等保标准基线相关检查项支持自动修复。

说明 企业版用户可以使用基线检查的所有功能。高级版用户无法添加基线检查策略，仅支持使用默认策略执行基线检查。

基线检查内容

基线分类	检查标准及检查内容	覆盖的系统和服务	修复紧急度说明
弱口令	使用非登录爆破方式检测是否存在弱口令。避免登录爆破方式锁定账户影响业务的正常运行。	• 操作系统 Linux、Windows • 数据库 MySQL、Redis、SQL Server、 MongoDB、PostgreSQL • 应用 Tomcat、FTP、Rsync、SVN	需紧急修复。特别是暴露公网的风险，避免系统被入侵或发生数据泄露事件。
高危风险利用	• 未授权访问基线 检测服务是否存在未授权访问风险，避免被入侵或者数据泄露。 • 其他高危配置风险基线 检测服务是否存在高危配置风险，避免存在远程文件读取、命令执行等漏洞风险。	Memcached、Elasticsearch、Docker、CouchDB、Zookeeper、Jenkins、Hadoop、Tomcat	
最佳安全实践	阿里云标准 基于阿里云最佳安全实践标准检测是否存在账号权限、身份鉴别、密码策略、访问控制、安全审计和入侵防范等安全配置风险。	• 操作系统 ◦ Centos 6、7、8 ◦ Redhat 6、7 ◦ Ubuntu 12、14、16 ◦ Debian 8 ◦ Aliyun Linux 2 ◦ Windows 2008、2012、2016、2019 R2 • 数据库 MySQL、Redis、MongoDB、SQL server、Oracle 11g • 应用 Tomcat、IIS、Nginx、Apache	重要安全加固项，建议修复。基于最佳安全实践的加固标准，降低配置弱点被攻击和配置变更风险。

基线分类	检查标准及检查内容	覆盖的系统和服务	修复紧急度说明
容器安全	阿里云标准 基于阿里云容器最佳安全实践的Kubernetes Master和Node节点配置风险检查。	• Docker • Kubernetes集群	
等保合规	• 等保二级、三级合规 基于服务器安全等保基线检查。对标权威测评机构安全计算环境测评标准和要求。 • CIS国际标准 基于CIS标准的操作系统安全基线检查。	• 等保合规 ○ Centos 6、7、8 ○ Redhat 6、7 ○ Ubuntu 12、14、16 ○ SUSE 10、11、12 ○ Debian 8 ○ Aliyun Linux 2 ○ Windows 2008、2012、2016、2019 R2 • CIS国际标准 ○ Centos 6、7 ○ Ubuntu 12、14、16 ○ Debian 8 ○ Aliyun Linux 2 ○ Windows 2008、2012、2016、2019 R2	基于业务是否有合规需要进行修复。

基线检查支持的检查项详情，请参见基线检查项目。

2.2. 基线检查项目

云安全中心提供默认的基线检查项目。通过对服务器进行基线检测，获取服务器在基线配置和应用上存在的风险和缺陷，为您提供风险告警和修复建议。本文为您列举基线检查支持的所有检查项。

基线分类	基线名称	基线描述	包含的检查项数量
	弱口令-MongoDB登录弱口令检测（支持MongoDB 2.X版本）	检查MongoDB服务是否存在弱口令用户，支持MongoDB 2.x版本。	1
	弱口令-SQL Server数据库登录弱口令检查	Microsoft SQL Server数据库登录账号弱口令检测基线。	1
	弱口令-MongoDB登录弱口令检测	检查MongoDB服务是否存在弱口令风险，支持3.x和4.x版本。	1
	弱口令-MySQL数据库登录弱口令检查	新版MySQL数据库登录账号弱口令检测基线，拥有更丰富的常见弱口令样本，更好的检测性能。	1
	弱口令-MySQL数据库登录弱口令检查（Windows版）	Windows版MySQL数据库登录账号弱口令检测基线。	1

基线分类	基线名称	基线描述	包含的检查项数量
弱口令	弱口令-PostgreSQL数据库登录弱口令检查	PostgreSQL数据库登录账号弱口令检测基线。	1
	弱口令-Redis数据库登录弱口令检查	Redis数据库登录弱口令检测基线。	1
	弱口令-rsync服务登录弱口令检查	rsync服务器登录弱口令检测基线。	1
	弱口令-SVN服务登录弱口令检查	SVN服务器登录弱口令检测基线。	1
	弱口令-Linux系统登录弱口令检查	新版Linux系统登录账号弱口令检测基线，拥有更丰富的常见弱口令样本，更好的检测性能。	1
	弱口令-Windows系统登录弱口令检查	新版Windows Server系统登录账号弱口令检测基线，拥有更丰富的常见弱口令样本，更好的检测性能。	1
	弱口令-Apache Tomcat控制台弱口令检查	Apache Tomcat控制台登录弱口令检查，支持Tomcat 7、8、9版本。	1
	弱口令-FTP登录弱口令检查	检查FTP服务是否存在登录弱口令和匿名登录。	1
高危风险利用	高危风险利用-CouchDB未授权访问高危风险	CouchDB未授权访问高危风险利用基线。	1
	高危风险利用-Docker未授权访问高危风险	Docker未授权访问高危风险基线。	1
	高危风险利用-Elasticsearch未授权访问高危风险	Elasticsearch未授权访问高危风险基线。	1
	高危风险利用-Hadoop未授权访问高危风险	Hadoop未授权访问高危风险基线。	1
	高危风险利用-Jenkins未授权访问高危风险	Jenkins未授权访问高危风险基线。	1
	高危风险利用-Memcached未授权访问高危风险	Memcached未授权访问高危风险基线。	1
	高危风险利用-Apache Tomcat AJP文件包含漏洞风险	Apache Tomcat AJP文件包含的漏洞风险检测。	1
	高危风险利用-ZooKeeper未授权访问高危风险	ZooKeeper未授权访问高危风险基线。	1
容器安全	阿里云标准-Docker安全基线检查	基于阿里云最佳安全实践的Docker基线标准。	13
	阿里云标准-Kubernetes-Master安全基线检查	基于阿里云最佳安全实践的K8s基线检测。	17

基线分类	基线名称	基线描述	包含的检查项数量
	阿里云标准-Kubernetes-Node安全基线检查	基于阿里云最佳安全实践的K8s基线检测。	7
最佳安全实践	阿里云标准-Alibaba Cloud Linux/Aliyun Linux 2安全基线检查	基于阿里云最佳安全实践的Alibaba Cloud Linux/Aliyun Linux 2基线标准。	14
	阿里云标准-Memcached安全基线检查	基于阿里云最佳安全实践的Memcached基线标准。	4
	阿里云标准-MongoDB安全基线检查（支持3.x版本）	基于阿里云最佳安全实践的MongoDB基线标准（支持3.x版本）。	11
	阿里云标准-MySQL安全基线检查	基于阿里云最佳安全实践的MySQL基线标准，支持版本：MySQL 5.1~MySQL 5.7。	12
	阿里云标准-Oracle 11g安全基线检查	基于阿里云最佳安全实践的Oracle 11g基线标准。	14
	阿里云标准-Redis安全基线检查	基于阿里云最佳安全实践的Redis基线标准。	6
	阿里云标准-SQL server安全基线检查	基于阿里云最佳安全实践的SQL Server 2012安全基线检查。	16
	阿里云标准-Debian Linux 8安全基线检查	基于阿里云最佳安全实践的Debian Linux 8基线标准。	15
	阿里云标准-CentOS Linux 6安全基线检查	基于阿里云最佳安全实践的CentOS Linux 6基线标准。	15
	阿里云标准-CentOS Linux 7/8安全基线检查	基于阿里云最佳安全实践的CentOS Linux 7、8基线标准。	15
	阿里云标准-Redhat Linux 6安全基线检查	基于阿里云最佳安全实践的Redhat Linux 6基线标准。	15
	阿里云标准-Redhat Linux 7安全基线检查	基于阿里云最佳安全实践的Redhat Linux 7基线标准。	15
	阿里云标准-Ubuntu安全基线检查	基于阿里云最佳安全实践的Ubuntu 14、Ubuntu 16、Ubuntu 18基线标准。	15
	阿里云标准-Apache安全基线检查	参考CIS标准和阿里云基线标准进行中间件层面基线检测。	16
	阿里云标准-Nginx安全基线检查	基于阿里云最佳安全实践的Nginx基线检测。	9

基线分类	基线名称	基线描述	包含的检查项数量
	阿里云标准-WebSphere Application Server安全基线检查	基于阿里云最佳安全实践的WebSphere Application Server安全基线检查。	12
	阿里云标准-WebLogic Server 12c安全基线检查	基于阿里云最佳安全实践的WebLogic Server 12c安全基线检查。	11
	阿里云标准-Windows 2008 R2安全基线检查	基于阿里云最佳安全实践的Windows 2008 R2基线标准。	12
	阿里云标准-Windows 2012 R2安全基线检查	基于阿里云最佳安全实践的Windows 2012 R2 基线检查。	12
	阿里云标准-Windows 2016/2019 R2安全基线检查	基于阿里云最佳安全实践的Windows 2016、2019 R2 基线检查。	11
	阿里云标准-IIS 8安全基线检查	基于阿里云最佳安全实践的Internet Information Services 8基线标准。	8
	CIS标准-Alibaba Cloud Linux/Aliyun Linux 2安全基线检查	符合CIS基线标准，适用于有专业安全水准要求的企业用户，从CIS基线提供的丰富的检查项规则中依据业务场景和安全需求对系统进行安全加固。具体支持的操作系统包括： • Alibaba Cloud Linux、Aliyun Linux 2 • CentOS Linux 6、7、8 • Debian Linux 8 • Ubuntu 14、16、18 • Windows Server 2008 R2、2012 R2、2016 R2、2019 R2	179
	CIS标准-CentOS Linux 6安全基线检查		197
	CIS标准-CentOS Linux 7安全基线检查		198
	CIS标准-CentOS Linux 8安全基线检查		171
	CIS标准-Debian Linux 8安全基线检查		156
	CIS标准-Ubuntu 14安全基线检查		178
	CIS标准-Ubuntu 16/18安全基线检查		177
	CIS标准-Windows Server 2008 R2安全基线检查		273
	CIS标准-Windows Server 2012 R2安全基线检查		274
	CIS标准-Windows Server 2016/2019 R2安全基线检查		274

基线分类	基线名称	基线描述	包含的检查项数量
	等保二级-Alibaba Cloud Linux/Aliyun Linux 2合规基线检查	Alibaba Cloud Linux/Aliyun Linux 2等保合规基线检查，支持中国等保2.0二级等保标准，对标权威测评机构安全计算环境测评标准和要求。	15
	等保二级-CentOS Linux 6合规基线检查	CentOS Linux 6等保合规基线检查，支持中国等保2.0二级等保标准，对标权威测评机构安全计算环境测评标准和要求。	15
	等保二级-CentOS Linux 7合规基线检查	CentOS Linux 7等保合规基线检查，支持中国等保2.0二级等保标准，对标权威测评机构安全计算环境测评标准和要求。	15
	等保二级-Debian Linux 8合规基线检查	Debian Linux 8等保合规基线检查，支持中国等保2.0二级等保标准，对标权威测评机构安全计算环境测评标准和要求。	15
	等保二级-Redhat Linux 7合规基线检查	Redhat Linux 7等保合规基线检查，满足中国等保2.0二级等保标准中，关于权威测评机构安全计算环境测评的标准和要求。	15
	等保二级-Ubuntu 14合规基线检查	Ubuntu 14等保合规基线检查，支持中国等保2.0二级等保标准，对标权威测评机构安全计算环境测评标准和要求。	15
	等保二级-Ubuntu16/18合规基线检查	Ubuntu16、18等保合规基线检查，支持中国等保2.0二级等保标准，对标权威测评机构安全计算环境测评标准和要求。	15
	等保二级-Windows 2008 R2合规基线检查	Windows 2008 R2等保合规基线检查，支持中国等保2.0二级等保标准，对标权威测评机构安全计算环境测评标准和要求。	12
	等保二级-Windows 2012 R2合规基线检查	Windows 2012 R2等保合规基线检查，支持中国等保2.0二级等保标准，对标权威测评机构安全计算环境测评标准和要求。	12
	等保二级-Windows 2016/2019 R2合规基线检查	Windows 2016/2019 R2等保合规基线检查，支持中国等保2.0二级等保标准，对标权威测评机构安全计算环境测评标准和要求。	12

基线分类 等保合规	基线名称	基线描述	包含的检查项数量
	等保三级-Alibaba Cloud Linux/Aliyun Linux 2合规基线检查	Alibaba Cloud Linux、Aliyun Linux 2等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19
	等保三级-BCLinux 7合规基线检查	BCLinux 7等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19
	等保三级-BCLinux 6合规基线检查	BCLinux 6等保合规基线检查，满足中国等保2.0三级等保标准中，关于权威测评机构安全计算环境测评的标准和要求。	19
	等保三级-CentOS Linux 6合规基线检查	CentOS Linux 6等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19
	等保三级-CentOS Linux 7合规基线检查	CentOS Linux 7等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19
	等保三级-CentOS Linux 8合规基线检查	CentOS Linux 8等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	21
	等保三级-Debian Linux 8合规基线检查	Debian Linux 8等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19
	等保三级-Redhat Linux 6合规基线检查	Redhat Linux 6等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19
	等保三级-Redhat Linux 7合规基线检查	Redhat Linux 7等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19
	等保三级-SUSE 10合规基线检查	SUSE 10等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19

基线分类	基线名称	基线描述	包含的检查项数量
	等保三级-SUSE 11合规基线检查	SUSE 11等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19
	等保三级-SUSE 12合规基线检查	SUSE 12等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19
	等保三级-Ubuntu 14合规基线检查	Ubuntu14等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19
	等保三级-Ubuntu 16/18合规基线检查	Ubuntu16、18等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19
	等保三级-Windows 2008 R2合规基线检查	Windows 2008 R2等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19
	等保三级-Windows 2012 R2合规基线检查	Windows 2012 R2等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19
	等保三级-Windows 2016/2019 R2合规基线检查	Windows 2016、2019 R2等保合规基线检查，支持中国等保2.0三级等保标准，对标权威测评机构安全计算环境测评标准和要求。	19

2.3. 设置基线检查策略

云安全中心支持根据基线检查策略检查您的服务器基线配置是否存在风险。本文档介绍了如何新增、编辑、删除基线检查策略，设置基线检查等级的范围以及如何自定义弱口令规则。

前提条件

您已购买云安全中心高级版或企业版，仅高级版和企业版支持基线检查功能。

> **说明** 基础版和基础杀毒版用户都需先升级到高级版或企业版才可使用基线检查功能。

背景信息

开通基线检查服务后，云安全中心将使用默认策略对所有资产进行检测。以下内容描述了默认策略的自动检测时间和检测对象：

- 默认策略自动检测时间：每隔一天检测一次，每次在00:00~06:00进行检测。

- 默认策略检测对象：您阿里云账号下的所有资产。

您也可自定义基线检查策略，补充默认策略无法检测的基线项目。

> **说明** 仅企业版支持自定义基线检查策略，高级版不支持自定义基线检查策略。高级版可使用默认策略和已存在的自定义的基线检查策略执行基线检查。

云安全中心基于阿里云威胁情报，为您提供了默认的内置弱口令检测规则。您也可以基于业务的需要，自定义基线弱口令规则。更多信息请参见自定义弱口令规则。

管理基线检查策略

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 基线检查**。
3. 在**基线检查**页面右上角单击**策略管理**。
4. 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。

     

     您可以参考以下表格中的参数说明，配置基线检查策略的参数。

参数	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	选择需要检测的基线项目，在高危风险利用、容器安全、等保合规、最佳安全实践、弱口令类型下选择具体需要检测的内容。 基线检查项目详情请参见基线检查内容。
生效服务器	选择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**所有分组 > 未分组**中，如需对新购资产自动应用该策略，请选择**未分组**。如果您需要添加新的分组或修改已有分组，详细操作步骤请参见管理资产分组。

   - 单击目标策略模板操作列的**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生效服务器。

     

   - 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）。

基线检查等级

自定义弱口令规则

云安全中心为您提供了默认的内置弱口令检测规则，您可以基于业务需要，自定义基线弱口令规则。以下步骤介绍如何自定义弱口令规则：

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 基线检查**。
3. 在**基线检查**页面右上角单击**策略管理**。
4. 在**自定义弱口令规则**区域，单击**下载模板**。

5. 在下载的模板中完成自定义弱口令设置后，单击**导入文件**。

> **说明** 上传的弱口令文件有以下限制：
>
> - 文件大小不能超过5 KB。
> - 文件中弱口令之间必须换行区分，每行中不可以有多个弱口令，否则将无法准确检测弱口令。
> - 文件中仅支持2,000条弱口令。

相关操作

完成基线检查策略制定后，您可根据已制定的策略检查您的服务器是否存在安全风险。具体内容请参见执行基线检查。

2.4. 执行基线检查

云安全中心高级版和企业版支持检查您服务器的基线配置是否存在风险。本文档介绍了如何执行基线检查。

前提条件

- 您已购买云安全中心高级版或企业版，仅高级版和企业版支持基线检查功能。

  > **说明** 基础版和基础杀毒版用户都需先升级到高级版或企业版才可使用基线检查功能。

- 您已配置自定义的基线检查策略。详细内容请参见设置基线检查策略。

  > **说明** 仅企业版支持自定义基线检查策略，高级版不支持自定义基线检查策略。如果您未配置自定义的基线检查策略，云安全中心将根据系统中默认的策略执行基线检查。默认策略中不包含所有的基线检查项，因此可能不会覆盖您实际需要检查的项目。

背景信息

基线检查的范围，请参见基线检查内容。

云安全中心基线检查功能支持周期性自动检查和即时手动检查：

- **周期性自动检查**：根据云安全中心为您提供的基线检查默认策略或您自定义的基线检查策略，定时自动执行基线检查。默认策略每隔1天在0点的时候自动执行基线检查。
- **即时手动检查**：如果您新增或修改了自定义的基线检查策略，您可以在**基线检查**页面选择该**基线检查策略**，立即执行基线检查，实时查看服务器中是否存在对应的基线风险。

即时手动检查

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 基线检查**。
3. 在**基线检查策略**列表中，选择需要执行即时手动检查的基线策略。

   

4. 单击**立即检查**。

   

   您可查看基线检查的实时检测进度和详细的检查结果。

   - 检查概览区域将显示实时检测进度。

     
   - 单击检查概览区域的**进度详情**，可展示当前已检测成功和失败的服务器数量、检测失败的原因。您可单击**查看解决方案**参考对应的解决方案来解决检测失败的问题。

     

     单击**刷新进度详情**更新检测进度。
   - 在基线检查结果列表中查看具体的基线检查风险项。

     基线检查完成后，**基线检查**页面的基线检查项目列表会展示最新的检查结果。

     

     > **说明** 风险项/影响服务器数不为0，表示有服务器未通过该基线检测，未通过检测的服务器存在风险隐患。

后续步骤

完成基线检查后，您需要在**基线检查**页面查看并对检查出的风险项进行处理。详细内容请参见查看和处理基线检查结果。

2.5. 查看和处理基线检查结果

本文介绍如何在阿里云云安全中心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。

前提条件

已完成基线检查。具体操作步骤请参见执行基线检查。

背景信息

开通基线检查服务后，云安全中心会使用系统内置的默认基线策略对所有资产进行基线检查。您也可自定义基线检查策略，检查基线策略中添加的资产是否存在相应的风险。基线检查策略的具体内容请参见设置基线检查策略。

> **说明** 仅企业版支持自定义基线检查策略，高级版不支持自定义基线检查策略。高级版可使用默认策略和已存在的自定义的基线检查策略执行基线检查。

查看检测结果总览数据

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 基线检查**。
3. 在**基线检查**页面上方，查看云安全中心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**列表中，选择目标基线检查策略，查看以下信息：

   - **检查服务器数**：云安全中心执行基线检查的服务器数量，即您在配置基线检查策略时，选中的分组中服务器的总台数。
   - **检查项**：是您在配置基线检查策略时，选中的**基线名称**的数量。
   - **高危弱口令风险**：当前基线检查策略检测出的高危弱口令风险项数量。单击**高危弱口令风险**下的数字，可以查看高危弱口令风险项的列表
   - **最近检查通过率**：最近一次执行基线检查的基线合格率。 以下是**最近检查通过率**字体颜色的含义：
     - 绿色：表示扫描的资产中基线配置合格率较高。
     - 红色：表示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。

   查看基线项目风险详情内容请参见查看风险项详情。

   修复基线检查配置风险项的具体操作请参见处理风险检查项。

查看基线检查项目列表

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 基线检查**。
3. 在**基线检查策略**列表中，选择**全部策略**。

   云安全中心控制台的**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**、**基线分类**、**最新检查时间**，以及**基线检查项**数量和**风险项/影响服务器数**等信息。

   > **说明** 您也可在**基线检查策略**列表中，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. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 基线检查**。
3. 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。
4. 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。具体内容请参见查看风险项详情。
   - 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**。
   - 单击资产右侧**操作**列下的**回滚**，选择待回滚快照，单击**确定**，对已处理风险项进行回滚。

> **说明** 如果由于风险检查项修复失败导致业务中断，云安全中心支持对已创建快照的资产执行回滚操作。执行回滚操作后，您的资产可恢复到相应快照的配置。

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。

   风险项列表

   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**或**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。详细内容请参见处理风险检查项。

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。

- **修复基线检查配置项**

  仅支持修复Linux系统的阿里云标准和等保标准基线相关检查项。单击检查项**操作**列下的**修复**，在**修复风险检查项**页面，选择修复设置，并单击**立即修复**。

  您可以根据以下说明修复该风险检查项：

  - **批量配置**：单击**批量配置后的查看详情**，在列出的存在相同问题的资产中，根据需求选择需要执行相同**修复方式**的资产。
  - **修复方式**：选择**修复方式**。

    > **说明** 不同类型的风险项对应的修复方式是不同的，请根据实际场景选择您需要的修复方式。

  - **风险保障**：选择是否自动创建快照，建议您选择**自动创建快照并修复**。

    > **说明** 系统在修复基线检查项时，可能存在修复失败的风险，影响业务正常运行，建议您在修复前对系统进行快照备份。快照支持回滚，可快速恢复到执行修复操作前的状态，使业务能正常运转。

  修复完成后，您可进行手动验证确认该风险项是否已成功修复。云安全中心也会根据您在扫描策略中设置的检测周期执行自动验证。

- **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。更多信息请参见加入白名单。

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

- **取消加白**

如果需要云安全中心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加白的操作。取消加白后，该基线检查配置项会再次触发告警。

取消加白

- **验证已修复的基线检查风险项**

  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**。

  验证中

  如果您未进行手动验证，云安全中心将会根据您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**。

2.6. 加入白名单

基线检查支持设置白名单。将基线检查风险项加入到白名单后，云安全中心不再对该风险项进行告警。如果您确认检测状态为未通过的基线风险项为正常业务结果，可通过加入白名单功能对该检查项产生的告警进行忽略。本文档介绍了如何将需要忽略告警的检查项加入白名单中。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**安全防范 > 基线检查**。
3. 在基线检查列表中，单击目标基线名称。

   查看基线项目详情

4. 在需要忽略告警的资产操作列单击**查看**，查看该资产中已检测出的基线风险项。
5. 在**风险项**页面单击目标检查项操作列的**加白名单**。

   加白名单

   如果需要将多个检查项加入白名单，您需要先选择状态为**未通过**并需要加入白名单的检查项，再单击检查项列表左下方的**加白名单**，将检查项批量加入白名单中。
6. 在**检查项忽略原因**对话框中填写加入白名单操作的备注信息。如果您需要忽略所有存在该风险项的服务器上的该检查项告警，请选中**请确认是否要批量处理**。

   检查项忽略原因

   此处填写的备注信息将展示在检查项列表中，以便后续回溯分析。

   > **说明** 定位到已加入白名单的检查项，将鼠标移动到该检查项的**已忽略**状态区域时，您可以查看该检查项加入白名单时填写的备注信息。

   查看已加白检测项备注信息

7. 单击**确定**。
   将检查项加入白名单后，该检查项默认展示在检查项列表的最后一页，并且该检查项状态将变为**已忽略**。

   加白名单结果

相关操作

- 查看已加入白名单的检查项信息。

在**风险项**页面状态类型下拉框中选择**已忽略**，可查看已加入白名单的检查项列表。

查看已加白的检测项

- 取消已加入白名单的检查项。

  如果您需要云安全中心继续对某个检查项进行告警，可以对该已加入白名单的检查项执行取消加入白名单的操作。

  在**风险项**页面，定位到需取消白名单的检查项，单击其操作列**取消加白**，或选择该检查项并单击检查项列表左下方的**取消加白**，可将该检查项移出白名单。

  取消加白

2.7. 提升登录口令安全最佳实践

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

背景信息

在服务器系统中使用弱口令可能会造成以下危害：

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

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

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

提升口令安全

您可以通过以下方法提升登录口令的安全性：

- **设置复杂密码**

  复杂密码应同时满足以下要求：

  - 密码长度大于等于8个字符。
  - 至少包含以下三种字符的组合：
    - 大写字母（A~Z）
    - 小写字母（a~z）
    - 数字（0~9）
    - 特殊字符（`~!@$%^&*()-_=+#|[{}];:'",<.>/?）
  - 密码不能为用户名或用户名的倒序。

- **不使用常见或公开的弱口令**

  以下是常见或公开的弱口令：

  - 已公开的常用弱口令。例如abcd1234、admin、root、admin@123等。
  - 数字或字母连排或混排，键盘字母连排。例如123456、abcdef、123abc、qwerty、1qaz2wsx等。
  - 短语密码。例如5201314、woaini1314等。

- 公司名称、 生日、姓名、身份证、手机号、邮箱名、用户ID、时间年份等。

- **定期修改密码**

  建议每隔90天更改一次密码。

修改常见的服务器弱口令

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

系统名称	修改登录口令操作步骤	说明
Linux系统	在Linux系统服务器中，执行passwd [<user>]命令修改用户登录口令。	其中 `<user>` 为登录用户名，如果不输入则修改的是当前用户的口令。执行完命令后请根据提示输入新口令。
Windows系统	本处以Windows 10为例说明修改用户登录口令的方法。 1. 登录Windows服务器后，在左下角单击 图标。 2. 单击 图标。 3. 在Windows设置页面，单击帐户。 4. 在左侧导航栏单击登录选项。 5. 根据页面提示更改服务器密码。	无。

系统名称	修改登录口令操作步骤	说明

MySQL数据库	1. 登录MySQL数据库。
	2. 执行以下命令查看数据库用户密码信息。
	`SELECT user, host, authentication_string FROM user;`
	说明 部分MySQL数据库版本可能不支持上述查询命令。如果您执行上述命令未获得用户密码信息，请您执行以下命令。
	`SELECT user, host, password FROM user;`
	3. 执行以下命令根据查询结果及弱密码告警信息修改具体用户的密码。
	`SET PASSWORD FOR '用户名'@'主机' = PASSWORD('新密码');`
	4. 执行刷新命令 `flush privileges;` 。
		无。

Redis数据库	1. 打开Redis数据库的配置文件*redis.conf*。 2. 执行以下命令修改或增加口令。 `requirepass <password>;` 3. 重启Redis服务。	其中 `<password>` 为登录口令。如果已存在登录口令，则将其修改为复杂口令；如果不存在登录口令，则添加新口令。
SQL Server数据库	• Linux系统登录 登录SQL Server数据库，执行以下命令修改登录口令。 `exec sp_password '<oldpassword>','<newpassword>','<user>'` • Windows认证登录 在SQL Server数据库客户端依次选择**安全性** > **登录名** ，选中用户后将弱口令修改为复杂口令。	其中 `<oldpassword>` 为旧口令， `<newpassword>` 为新口令， `<user>` 为用户名。

系统名称	修改登录口令操作步骤	说明
MongoDB数据库	1. 登录MongoDB数据库。 2. 执行 `use admin` 命令切换到admin用户。 3. 执行 `use <db_name>` 命令切换到需要修改登录口令的数据库。 4. 执行 `db.updateUser('<username>',{pwd:'<newpassword>'})` 命令修改数据库的登录名和口令。	• `db_name` 为需要修改登录口令的数据库名称。 • `username` 为待修改口令的用户名， `newpassword` 为新口令。 • 修改口令完成后，需等待15分钟才能检测修改后的口令是否为弱口令。
PostgreSQL数据库	1. 登录PostgreSQL数据库。 2. 执行以下命令修改弱口令。 `ALTER USER <user> WITH PASSWORD '<newpassword>';`	其中 `<user>` 为用户名， `<newpassword>` 为新口令。
Tomcat	1. 打开Tomcat根目录下的配置文件*conf/tomcat-user.xml*。 2. 修改user节点的password属性值为复杂口令。	无。
Rsync	1. 打开Rsync的配置文件*rsyncd.conf*。 2. 找到 `secrets file` 配置项，并在该配置项中找到 `rsyncd.secret` 文件的路径。 3. 将*rsyncd.secret*文件按 `用户名:口令` 的形式编辑，修改对应用户的口令为新的复杂口令。 4. 重启Rsync服务。	无。
SVN	1. 打开版本库目录。 2. 在配置文件*<path>/conf/svnserve.conf*中找到 `password-db` 。 3. 根据password-db配置找到口令配置文件路径，将该文件中的口令修改为指定的口令（默认为passwd文件）。 4. 重启SVN服务。	无。

系统名称	修改登录口令操作步骤	说明
vsftpd服务器软件	• 本地用户 i. 打开配置文件*vsftpd.conf*。 ii. 增加或修改配置项 `anonymous_enable` 的值为**NO**。 `anonymous_enable` 的值为**NO**表示禁止匿名登录。 iii. 执行 `passwd <ftpuser>` 命令修改FTP用户的口令。 `<ftpuser>` 为ftp用户的用户名。 iv. 根据提示设置符合要求的新的复杂口令。 • 虚拟用户 i. 打开文件*/etc/vsftpd/login.txt*。 ii. 修改用户名对应的口令并保存。 该文件格式为：第1行是用户A的用户名，第2行是用户A的口令，第3行是用户B的用户名，第4行是用户B的口令，以此类推。 iii. 执行 `db_load -T -t hash -f /etc/vsftpd/login.txt /etc/vsftpd/login.db` 命令。 iv. 修改*/etc/pam.d/vsftpd*文件。 在存在 `auth pam_userdb.so` 和 `account pam_userdb.so` 的行后分别添加语句 `db=/etc/vsftpd/login`，修改完成后保存。具体位置见下图。 v. 重启vsftpd。	无。

3.云平台配置检查

3.1. 云平台配置检查概述

云安全中心支持云平台配置检查功能，检查您云产品的安全配置是否存在安全隐患。本文档介绍了云平台配置检查功能的特性和检查项信息。

背景信息

云安全中心云平台配置检查从身份认证及权限、网络访问控制、数据安全、日志审计、监控告警、基础安全防护六个维度为您提供云产品安全配置的检查，帮助您及时发现您的云产品配置风险并提供相应的修复方案。

> **说明** 云安全中心基础版和基础杀毒版的云平台配置检查功能不支持检测所有检查项，高级版和企业版支持检测所有检查项。基础版和基础杀毒版用户需要升级至高级版或企业版，才能使用云平台配置检查的所有检查项服务。各版本支持的检查项详情请参见云平台配置检查项列表。

您可以在云安全中心控制台的**云平台配置检查**页面，查看**已启用检查项数**。

已启用检查项

云平台配置检查项列表

下表罗列了云安全中心各版本（基础版、基础杀毒版、高级版和企业版）对云平台配置检查项的支持情况，其中用到的标识：

- X：表示不包含在服务范围中。
- √：表示包含在服务范围中。

支持的检查项	检查类型	说明	基础版或基础杀毒版	高级版或企业版
主账号安全-AK使用	身份认证及权限	检查主账号的AK账号权限。由于主账号对名下资源有完全控制权限，为了避免因访问密钥泄露所带来的损失，不建议您为主账号创建访问密钥并使用该密钥进行日常工作。 **注意** 该检测项存在延时，当天禁用AK之后再次验证，不会立刻通过，需在第二天后台数据更新之后才会通过。	X	√
CDN-实时日志推送	日志审计	检查阿里云CDN是否配置CDN实时日志推送服务。阿里云CDN提供将采集到的实时日志实时推送至日志服务，并进行日志分析。通过日志的实时分析，您可以快速发现和定位问题。	X	√
云平台-操作审计配置检查	日志审计	检测是否有开启云平台操作审计功能。未开启操作审计，将无法对管理员在云平台的操作行为进行记录、也不符合合规要求。	X	√

支持的检查项	检查类型	说明	基础版或基础杀毒版	高级版或企业版
PolarDB-备份设置	数据安全	检查云数据库PolarDB是否开启了自动备份功能。数据库定期备份有利于提升数据库安全，在出现数据库异常时可以根据历史备份信息进行恢复。云数据库PolarDB提供了自动备份策略，建议您保持开启，确保每天备份一次。	X	√
PolarDB-SQL洞察	日志审计	检查云数据库PolarDB是否开通SQL洞察功能。云数据库PolarDB提供SQL洞察功能，可以为您的数据库提供安全审计、性能诊断等增值服务，建议开启。	X	√
OSS-授权策略	身份认证及权限	检查OSS的授权策略。OSS有三种权限控制方式，包括ACL、RAM Policy、Bucket Policy，其中在配置Bucket Policy的时候，不建议对匿名账号授予读写或完全控制权限。	X	√
SLB-访问日志配置	日志审计	检查是否开启负载均衡SLB的访问日志功能。负载均衡SLB提供七层的访问日志功能，可以收集所有发送到负载均衡的请求的详细信息，包括请求时间、客户端IP地址、延迟、请求路径和服务器响应等，建议开启。	X	√
容器镜像服务-仓库权限设置	数据安全	检查容器镜像服务的仓库是否设置为私有。容器镜像服务的仓库分为公有仓库和私有仓库，公有仓库允许所有互联网用户匿名下载。如果镜像内部有敏感信息，建议设置为私有；如果没有，可以忽略该条告警。	X	√
容器镜像服务-安全扫描	基础安全防护	检查容器镜像服务是否开通安全扫描功能。针对基于Linux的基础镜像，容器镜像服务已经提供了镜像安全扫描的功能。安全扫描可以发现基础镜像的系统漏洞、风险，建议扫描所有镜像。如果有最新基础镜像，建议采用最新的基础镜像完成安全扫描。	X	√
ECS-安全组策略	网络访问控制	检测ECS访问策略。建议安全组最小粒度开放访问策略，仅对必须全网开放的服务才开启0.0.0.0/0，例如80、443、22、3389端口。	X	√
OSS-Bucket服务端加密	数据安全	检测OSS Bucket是否开启数据加密功能。OSS提供服务器端加密功能，对持久化在OSS上的数据进行加密保护，建议您对敏感类型数据开启。	X	√
OSS-Bucket防盗链配置	网络访问控制	检测OSS-Bucket是否开启防盗链功能。OSS防盗链功能通过检查Referer，进行白名单限制，可以用于防止他人盗用OSS数据，建议您开启。	X	√
OSS敏感文件泄露	数据安全	检测OSS敏感文件是否有设置访问权限。	X	√

支持的检查项	检查类型	说明	基础版或基础杀毒版	高级版或企业版
RDS-跨地域备份	数据安全	检测RDS数据实例是否开启跨地域备份功能。RDS为MySQL提供跨地域备份功能，可以自动将本地备份文件复制到另一个地域的OSS上，跨地域的数据备份能够有效的实现异地容灾。建议您开启跨地域备份。	X	√
Redis-备份设置	数据安全	检测Redis数据库实例是否开启了数据备份功能。	X	√
Redis-SSL开启	日志审计	检查云数据库Redis是否开启SSL加密功能。Redis 2.8标准版、集群版实例和Redis 4.0集群版实例支持SSL加密。启用SSL（Secure Socket Layer）加密，可以提高您的Redis数据传输的安全性。	X	√
Redis-审计日志配置	日志审计	检查云数据库Redis是否开启日志审计功能。云数据库Redis提供日志审计功能，该功能可以记录所有的Redis请求记录并保存在日志服务中，建议开启。	X	√
MongoDB-日志审计	日志审计	检测MongoDB数据库是否开启审计日志功能。云数据库MongoDB审计日志记录了您对数据库执行的所有操作。通过审计日志记录，您可以对数据库进行故障分析、行为分析、安全审计等操作，有效帮助您获取数据的执行情况。建议您开启MongoDB数据库审计日志功能。	X	√
MongoDB-SSL开启	数据安全	检测MongoDB数据库是否开启SSL加密。为提高MongoDB数据库数据链路的安全性，建议您启用SSL加密。	X	√
MongoDB-备份设置	数据安全	检测云数据库MongoDB是否开启自动备份功能。数据库定期备份有利于提升数据库安全，在出现数据库异常时可以根据历史备份信息进行恢复。云数据库MongoDB提供了自动备份策略，建议您保持开启，确保每天备份一次。	X	√
云监控-主机插件状态	监控告警	检测ECS主机运行状态。云监控可以针对阿里云资源和互联网应用进行监控，为了监控ECS主机运行状态，并在出现主机异常指标时可以告警通知，建议在ECS主机安装云监控主机插件。	X	√
VPC-DNAT管理端口开放	网络访问控制	检测端口是否有开启公网访问。 建议VPC NAT网关创建DNAT规则时内部管理端口不要开启公网访问。例如：不要对所有端口或者22、80、443、1433、3306、3389、8080等重要端口开启公网访问。	X	√

支持的检查项	检查类型	说明	基础版或基础杀毒版	高级版或企业版
云平台-主账号双因素认证	主账号身份认证及权限	检查是否开启主账号双因素认证配置。在只使用单一密码认证的情况下，黑客可能通过暴力破解等手段获取您的云平台管理密码。建议对云平台管理员账号开启密码加手机短信双重身份认证，防止密码泄露带来的安全隐患。	√	√
RAM-子账号多因素认证	子账号身份认证及权限	检查子账号是否启用了多因素认证（Multi-Factor Authentication，简称MFA）。	√	√
云盾-主机安全防护状态	基础安全防护	检测安骑士Agent插件安装情况。云安全防御体系中，需要部署安骑士解决主机安全防护问题。未部署安骑士将导致云主机缺乏入侵检测及防御的能力，系统无法及时发现各种黑客入侵行为，例如：上传的Webshell、木马等恶意文件、异地登录、账号暴力破解攻击等。	√	√
云盾-高防回源配置检查	网络访问控制	检测DDoS高防服务是否有配置仅允许WAF回源IP地址访问。使用DDoS高防服务或Web应用防火墙后，需要对后端服务器真实IP地址进行隐藏，避免攻击者绕过高防或WAF直接攻击云主机。	√	√
云盾-WAF回源配置	网络访问控制	检测WAF（Web应用防火墙）服务是否配置仅允许WAF回源IP地址访问。使用DDoS高防服务或Web应用防火墙后，需要对后端服务器真实IP地址进行隐藏，避免攻击者绕过高防或WAF直接攻击云主机。	√	√
云安全中心-AK泄露检测配置	监控告警	检测是否已开启云安全中心AK&账密泄露检测功能。	√	√
ECS-密钥对登录	身份认证及权限	检测ECS中的Linux主机是否绑定了阿里云SSH密钥对。SSH密钥登录与SSH密码登录方式相比，更加安全便捷。推荐使用阿里云SSH密钥对方式。	√	√
ECS-存储加密	数据安全	检测ECS主机磁盘是否开启了加密功能。	√	√
ECS-自动快照策略	数据安全	检测ECS磁盘是否开启自动快照功能。自动快照可以提升ECS主机的数据安全，实现容灾备份。	√	√
SLB-白名单配置	网络访问控制	检测SLB负载均衡实例访问控制配置，http或https服务是否启用了访问控制，并且是否有开放0.0.0.0/0。	√	√
SLB-高危端口暴露	网络访问控制	检测SLB是否开转发非必要的公共服务端口。	√	√
SLB-健康状态	监控告警	检测SLB后端服务器是否可用。	√	√
SLB-证书过期	监控告警	检测SLB的可用证书是否已过期。	√	√

支持的检查项	检查类型	说明	基础版或基础杀毒版	高级版或企业版
OSS-Bucket权限设置	数据安全	检测OSS Bucket权限是否设置成了私有。	√	√
OSS-日志记录配置	数据安全	检测OSS是否有开启日志记录功能。	√	√
OSS-跨区域复制配置	数据安全	检测OSS是否有开启跨区域复制功能。	√	√
RDS-白名单配置	网络访问控制	检测RDS的访问控制策略是否有0.0.0.0/0（任意IP）或为空的配置。不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。	√	√
RDS-数据库安全策略	数据安全	检测RDS数据库是否开启了SQL审计功能、SSL加密传输功能和透明数据库加密功能。	√	√
RDS-开启数据库备份	数据安全	检测RDS数据库实例是否开启了数据备份功能。	√	√
Redis-白名单配置	网络访问控制	检测Redis的访问控制策略是否有0.0.0.0/0（任意IP）或为空的配置。不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。	√	√
分析型数据库PostgreSQL版-白名单配置	网络访问控制	检测PostgreSQL的访问控制策略是否有0.0.0.0/0（任意IP）或为空的配置。不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。	√	√
SSL证书-有效期检查	数据安全	检测SSL证书是否超出有效期。如果证书过期，您将无法继续使用SSL证书服务。	√	√
PolarDB-白名单配置	网络访问控制	检测云数据库PolarDB的访问控制策略是否开放公网访问且有 `0.0.0.0/.0` （任意IP）的配置，不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。	√	√
操作审计-日志配置	日志审计	检测对象存储服务（OSS）或者日志服务中的操作日志。 云安全体系要求云平台开启操作审计功能，操作日志需保存在对象存储服务（OSS）或者日志服务中，并合理设置日志的访问权限，以实现高危操作可追溯。	√	√
MongoDB-白名单配置	网络访问控制	检测MongoDB的访问控制策略是否有 `0.0.0.0/.0` （任意IP）或为空的配置。不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。	√	√

相关文档

执行云平台配置检查

查看和处理云平台配置检查结果

3.2. 执行云平台配置检查

云安全中心的云平台配置检查功能支持检查您云产品中是否存在配置上的风险。本文介绍了如何在云安全中心对云平台配置执行即时手动检查，及设置检查周期进行周期性自动检查。

背景信息

云安全中心支持手动立即检查和周期性自动检查云平台配置是否存在风险。

- **手动检查**：在**云平台配置**页面，执行**立即检查**，即时手动检查您云产品的配置是否存在风险。
- **周期性自动检查**：云安全中心默认每隔1天在 `00:00~06:00` 自动检查云平台配置是否存在风险。您也可根据需要设置自定义的检查周期，定期检查云平台配置，帮助您及时发现并处理您的云产品配置风险。

手动检查

您需要立即执行云平台配置检查时，可以执行以下步骤进行手动检查。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 云平台配置检查**。
3. 在**云平台配置检查**页面，单击检查项列表上方的**立即检查**，对云产品配置进行全量检查，确定是否存在风险项以及影响的资产数量。

   > **说明** 全量检查时，需要完成全部检查项的检查后才可以进行其他操作，请耐心等待。

   完成检查后，检查项列表中按检查结果的严重等级由高风险到低风险进行排序。

自动检查

云安全中心默认每隔1天在 `00:00~06:00` 自动检查云平台配置是否存在风险。如果该检查时间不满足您的业务需求，您可以执行以下步骤设置自动检查的周期和时间。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 云平台配置检查**。
3. 在**云平台配置检查**页面右上角单击**检查设置**。
4. 在**检查设置**对话框中设置云平台配置检查的**检查周期**和**检查时间**。

配置项

   - **检查周期**：可选星期一至星期日，支持多选。
   - **检查时间**：可选择 `24:00~06:00` 、 `06:00~12:00` 、 `12:00~18:00` 、 `18:00~24:00` 这4个时间段中的任意一个。
5. 单击**确定**。
   在选定时间段内，云安全中心会对所有检查项自动执行一次检查。

后续步骤

云平台配置检查完成后，可在**云平台配置检查**页面，查看并处理检查结果。详细内容请参见查看和处理云平台配置检查结果。

3.3. 查看和处理云平台配置检查结果

本文介绍了如何在云安全中心查看并处理云平台配置检查结果，具体包括检查项、检查项详情描述、可能产生的影响和处理建议。您可以在云平台配置检查页面集中处理检查出来的风险配置项。

前提条件

已执行云平台配置检查。更多信息请参见执行云平台配置检查。

查看云平台配置检查结果

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 云平台配置检查**。
3. 在**云平台配置检查**页面，查看云平台配置检查项结果及其详情。

   云平台配置检查

   - **查看最近一次检查结果的统计**

     您可在云平台配置检查项列表上方，查看到有风险的检查项数量（**风险项**包括总数量和不同等级风险的检查项数量）、有风险的资产数量（**风险数**）、未启用检查项数量、已启用检查项数量统计及最新检查时间。

     单击**未启用检查项**或**已启用检查项**下的数字，可以查看未启用或已启用的云平台配置检查项列表。

   - **查看检查项**

     您可查看云平台配置检查项列表信息，包括检查结果风险等级、影响资产类型及数量、检查项类型和最新检查时间等。检测出风险的云平台配置检查项按照对您资产的危害程度分为以下风险等级：

     - **高风险**：红色图标，表示当前不合规的检查项对您资产的危害较大，建议您尽快处理高风险的检查项。
     - **中风险**：橙色图标，表示当前不合规的检查项对您资产的危害一般，您可以延后处理该检查项。
     - **低风险**：灰色图标，表示当前不合规的检查项对您资产的影响较小，您可以暂时不处理该检查项。
     - **正常**：绿色图标，表示该检查项未检测出风险。

   - **查看检查结果详情**

     单击**基线检查项**名称，跳转到检查项的详情页面，查看对应的检查详情描述、可能产生的影响和处理建议。

     查看检测详情

处理云平台配置检查结果

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 云平台配置检查**。
3. 在**云平台配置检查**页面，处理云平台配置检查结果。

   处理检查结果

   - **修复**

     单击风险检查项操作栏**修复**，跳转到检查项的详情页面。您也可单击**基线检查项**名称，跳转到检查项的详情页面。

     如果在检查项详情的**威胁影响**中有受影响的资产信息，单击受影响的资产操作栏的**修复**，根据修复页面的指导，修改风险检查项的配置。

     修复

> **说明** 在云平台配置检查页面，云安全中心为部分云平台配置检查项提供直接修复功能，即在检查项列表的操作栏提供修复按钮。
>
> - 如果风险检查项存在受影响的资产，单击该风险检查项修复，进入检查项详情页，按照上述操作修复云平台配置。
> - 如果风险检查项没有受影响的资产，单击该风险检查项的修复，直接进入修复页面，根据修复指导，修改风险检查项的配置。

- **验证**

  如果您对部分配置项进行了修改，在云平台配置检查项列表，定位到该配置检查项，单击操作栏的**验证**，检验新的配置是否存在安全风险。

  

  如果您需要同时验证多个检查项，可以选中这些检查项并单击检查项列表下方的**验证**，在**确认**对话框中单击**确定**。

- **加白名单**

  如果您判断检测出的某个风险项不存在安全风险，可在云平台配置检查项列表，定位到该配置检查项，单击**加白名单**将该检查项状态调整为**已忽略**。**已忽略**的检查项将不会包含在**风险项**总数中。

  在检查项列表中，您也可对**已忽略**的检查项**取消加白**。

  

  > **说明** **加白名单**只对本次检测结果进行忽略，后续如果再次检测该出该风险，云安全中心仍会展示该检测结果的告警。

导出检查结果

在云平台配置检查项列表上方，单击导出按钮，导出检查结果Excel文件到本地。

> **说明** 云安全中心仅企业版支持导出云平台配置检查的检查结果，基础版、基础杀毒版和高级版不支持。基础版、基础杀毒版和高级版用户需先升级到企业版，才可使用导出功能。

4.等保合规检查

等保合规检查（全称为等级保护合规检查）为您提供了全面覆盖通信网络、区域边界、计算环境和管理中心的网络安全检查。您可以使用该功能检查系统是否符合等保合规要求，及时发现和处理安全风险。本文介绍如何查看等保合规检查报告。

背景信息

- 2019年12月1日起，*网络安全等级保护基本要求（GB/T 22239-2019信息安全技术）*等系列标准正式实施，落实网络安全等级保护制度是每个企业和单位的基本义务和责任。阿里云在确保云平台自身满足基本要求的基础上，提供了等保合规检查功能，帮助您更快速、高效和持续地落实网络安全等级保护制度，提升云上业务系统的安全防护能力。
- 云安全中心的基础版、基础杀毒版、高级版和企业版均支持等保合规检查。
- 您访问**等保合规检查报告**页面时，云安全中心会自动执行等保合规检查并为您提供最新的等保合规检查报告。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 等保合规检查**。
3. （可选）在**等保合规检查报告**页面上方*阿里云公共云等保合规白皮书2.0*提示信息右侧单击**申请下载**，申请下载云安全中心为您提供的等保2.0解决方案材料包。在**等保2.0解决方案材料包**页面，请根据提示填写您的信息并提交。您的申请审核通过后（预计2~4个工作日），您的邮箱将会收到等保2.0解决方案材料包。

   > **说明** 等保2.0解决方案材料包含以下内容：
   > - 阿里云安全架构师免费专业指导
   > - 等保2.0解决方案PPT
   > - 安全产品的销售许可证
   > - 阿里云平台等保备案证明
   > - 等保测评报告
   > - 阿里云公共云等保合规白皮书2.0（介绍阿里云如何助力云服务客户构建基于网络安全等级保护的安全合规体系）

4. 在**等保合规检查报告**页面，查看检查结果的统计数据。

   

   您可以执行以下操作。

   - **查看检测项总数和不合规项数**

     在**检测项总数**和**待处理不合规项数**查看等保合规支持的检测项总数量和不合规项的数量。单击**待处理不合规项数**可直接查看不合规的检查项列表。

   - **查看等级保护最佳实践**

     阿里云为您提供了等保合规2.0安全解决方案，可以帮助您顺利通过等保合规2.0的等保测评。您可以单击**点击查看等级保护最佳实践**，了解等保合规2.0安全解决方案的更多信息。

   - **等保问题在线咨询**

     单击**在线咨询**右侧的**咨询**，跳转到聊天窗口咨询等保相关问题。咨询时间为工作日09：00~17：00，请您在此时间内进行咨询。

- **主机配置检查**

  单击**前往合规检查功能，进行深度检查**，前往基线检查页面，查看并处理您资产中的基线问题。更多信息请参见查看和处理基线检查结果。

- **搜索指定检测项**

  在搜索框设置检查项分类和是否合规，或输入检测项目名称，查看符合条件的检测项。

5. 处理不合规的检查项目。 根据**改进建议**下的说明，处理不合规的检查项目。

> **说明** 云安全中心等保合规检查检测您的系统是否具备等保合规检查要求的安全能力，例如访问控制、日志审计等。您在确保具备等保合规检查的能力，并处理完发现的问题后，才可以通过等保测评。等保更多信息请参见等保合规2.0安全解决方案。

5.镜像安全扫描

云安全中心提供的镜像安全扫描功能可以检测镜像系统漏洞、镜像应用漏洞和镜像恶意样本，为您展示资产中存在的容器安全威胁，大幅降低使用容器的安全风险。本文介绍如何查看您资产中的镜像系统漏洞、镜像应用漏洞和镜像恶意样本。

前提条件

- 已购买容器镜像服务企业版实例。相关内容请参见创建企业版实例。
- 已购买云安全中心企业版。基础版、基础杀毒版和高级版用户需要升级到企业版才能使用镜像安全扫描功能。相关内容请参见升级与降配。

背景信息

镜像安全扫描公测中，云安全中心企业版用户无需开通和申请，即可免费使用镜像安全扫描功能。

云安全中心支持使用以下方式执行镜像安全扫描：

- 立即执行镜像安全扫描：如果您需要立即执行镜像安全扫描，您可以在**镜像安全扫描**页面单击**一键扫描**。
- 镜像漏洞扫描配置：如果您需要周期性执行镜像安全扫描，您可以配置周期性扫描的间隔时间和具体扫描时间。云安全中心会根据您的配置，周期性地执行镜像安全扫描。详细信息请参见镜像漏洞扫描配置。

云安全中心支持的安全镜像特性如下：

镜像安全项目	检测	修复	备注
镜像系统漏洞	仅检测	不支持修复	建议您根据云安全中心提供的修复命令和影响说明及时处理镜像系统漏洞。
镜像应用漏洞	仅检测	不支持修复	建议您根据云安全中心提供的修复命令和影响说明及时处理镜像应用漏洞。
镜像恶意样本	仅检测	不支持修复	建议您根据云安全中心提供的恶意文件路径等信息及时处理恶意文件样本。

支持的地域

目前，仅支持部署在华东1（杭州）、华东2（上海）、华北2（北京）、华南1（深圳）、新加坡地域的容器镜像服务企业版实例使用镜像安全扫描功能。

接入私有镜像仓库

镜像安全扫描目前仅支持接入仓库类型为harbor的私有镜像仓库。您可以参考以下步骤接入您的私有镜像仓库。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范** > **镜像安全扫描**。
3. 在**镜像安全扫描**页面单击**接入**。
4. 在**接入私有镜像仓**对话框中配置接入私有仓库的参数。

   您可以参考以下表格中的参数说明配置接入私有镜像仓库的参数。

参数	说明
私有仓库类型	选择私有仓库类型。目前仅支持选择habor。
版本	选择私有镜像仓库的版本。支持选择以下版本： ○ V1：镜像仓库为1.X.X选择该版本。 ○ V2：镜像仓库为2.X.X以上选择该版本。
通信类型	选择云安全中心和私有镜像仓库的通信协议。可选择http或https。
网络类型	选择私有镜像仓库的网络类型，可选择公网或VPC。
区域	选择私有镜像仓库所在区域。
域名	输入私有镜像仓库的域名。
IP	输入私有镜像仓库的IP地址。
用户名	输入访问私有镜像仓库时使用的用户名。
密码	输入访问私有镜像仓库的密码。

5. 单击**确定**。
6. （可选）立即扫描您的私有镜像仓库中是否存在安全漏洞和恶意样本。
   i. 单击**立即扫描**。
   ii. 在**一键扫描**对话框中选择**habor**。
   iii. 单击**确定**。

   该步骤执行完成后，云安全中心将开始扫描您的私有镜像仓库，扫描预计需要1分钟时间，您可以在1分钟后手动刷新页面查看扫描结果。

查看镜像漏洞和恶意样本

您可以在**镜像安全扫描**页面，查看扫描出的**镜像系统漏洞**、**镜像应用漏洞**和**镜像恶意样本**。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 镜像安全扫描**。
3. （可选）在**镜像安全扫描**页面单击**一键扫描**。如果您需要查看最新的镜像安全扫描结果，可以执行该步骤。扫描预计需要1分钟时间，扫描完成后您需要手动刷新当前页面查看最新数据。
4. 在**镜像系统漏洞**页签下查看扫描出的镜像系统漏洞。您可以执行以下操作：
   - **查看漏洞公告信息**

     您可以查看漏洞名称、漏洞特征、受影响镜像数和最新扫描时间。
   - **查看漏洞修复紧急度**

     漏洞的建议修复紧急度用不同颜色的图标表示，图标中的数字表示存在该漏洞的资产数量。 以下是图标颜色和漏洞修复紧急度的对应关系：
     - 红色图标：表示漏洞修复紧急度为**高**。
     - 橙色图标：表示漏洞修复紧急度为**中**。
     - 灰色图标：表示漏洞修复紧急度为**低**。

> **说明** 建议您立即修复紧急程度为高的漏洞。

- **搜索漏洞**

  您可在**镜像系统漏洞**页签，通过筛选漏洞危险等级（高、中、低），搜索实例ID、仓库名称、命名空间、摘要和漏洞名称定位到相关的漏洞。

  > **说明** 仓库名和漏洞名称都支持模糊搜索。

- **查看漏洞详情**

  单击需要查看的镜像系统漏洞操作列的**查看**，展开漏洞详情页面。在漏洞详情页面，您可根据需要进行以下操作：

  - **查看阿里云漏洞库详细信息**

    单击漏洞编号可跳转至阿里云漏洞库。

    

    您可在阿里云漏洞库页面，查看该漏洞更加详细的信息，包括漏洞的描述、基本信息、修复建议等信息。

  - **查看镜像系统漏洞的修复命令和影响说明**

    单击**详情**跳转到修复命令和影响说明页面，查看该镜像系统漏洞的修复命令和影响说明。

    

    - **修复命令**：执行该命令可修复对应的漏洞。
    - **影响说明**：
      - **软件**：该镜像的版本信息。
      - **命中**：该漏洞的匹配命中原因，一般是由于当前镜像版本不满足或者小于某个版本（以小于某个版本为主）。
      - **路径**：该镜像在服务器上的路径。
      - **镜像层**：存在漏洞的镜像层。
    - **风险重要提醒**：关于漏洞的风险提醒、补充修复建议和参考文档。

    > **说明** 云安全中心不支持一键修复镜像系统漏洞，您可以根据修复命令和影响说明中提供的检测结果手动对镜像中存在的漏洞进行排查和修复。镜像系统漏洞修复完成后，您需要在**镜像安全扫描**页面，单击**一键扫描**，才能在**镜像系统漏洞**列表中看到漏洞状态的更新。

5. 单击**镜像应用漏洞**页签。
6. 在**镜像应用漏洞**页签下查看扫描出的镜像应用漏洞。您可以执行以下操作：

   - **查看漏洞公告信息**

     您可以查看漏洞名称、漏洞特征、受影响的镜像数和最新扫描时间。

   - **查看漏洞修复紧急度**

     漏洞的建议修复紧急度用不同颜色的图标表示，图标中的数字表示存在该漏洞的资产数量。 以下是图标颜色和漏洞修复紧急度的对应关系：

     - 红色图标：表示漏洞修复紧急度为高。

- 橙色图标：表示漏洞修复紧急度为**中**。
- 灰色图标：表示漏洞修复紧急度为**低**。

> **说明** 建议您立即修复紧急程度为高的漏洞。

- **搜索漏洞**

  您可在**镜像应用漏洞**页面，通过筛选漏洞危险等级（高、中、低），搜索实例ID、仓库名称、命名空间、摘要和漏洞名称定位到相关的漏洞。

  > **说明** 仓库名和漏洞名称都支持模糊搜索。

- **查看漏洞详情**

  单击需要查看的镜像应用漏洞操作列的查看，展开漏洞详情页面。在漏洞详情页面，您可根据需要进行以下操作：

  - **查看阿里云漏洞库详细信息**

    单击漏洞编号可跳转至阿里云漏洞库。

    您可在阿里云漏洞库页面，查看该漏洞更加详细的信息，包括漏洞的描述、基本信息、修复建议等信息。

  - **查看镜像应用漏洞的修复命令和影响说明**

    单击**详情**跳转到修复命令和影响说明页面，查看该镜像应用漏洞的修复命令和影响说明。

    - **修复命令**：执行该命令可修复对应的漏洞。
    - **影响说明**：
      - **软件**：该镜像的版本信息。
      - **命中**：该漏洞的匹配命中原因，一般是由于当前镜像版本不满足或者小于某个版本（以小于某个版本为主）。
      - **路径**：该镜像在服务器上的路径。
      - **镜像层**：存在漏洞的镜像层。
    - **风险重要提醒**：关于漏洞的风险提醒、补充修复建议和参考文档。
    -

7. 单击**镜像恶意样本**页签。
8. 在**镜像恶意样本**页签下，您可以进行以下操作。

- **搜索镜像恶意样本**

  在镜像恶意样本列表右上角选择恶意样本的危险程度：**紧急**、**可疑**或**提醒**，根据实例ID、仓库名称、命名空间、概要、恶意样本名称等信息，搜索满足条件的镜像恶意样本。

- **查看镜像恶意样本列表**

  在镜像恶意样本列表中，您可以查看所有镜像恶意样本的名称、受影响的镜像数、首次或最新扫描时间和处理状态。

- **查看镜像恶意样本详情**

  在需要查看的**镜像恶意样本**操作列单击**详情**，可查看该镜像恶意样本的详情。

> **说明** 镜像恶意样本可能会通过将可读可写的内存属性改为可读可执行、修改网络代理设置等方式入侵您的服务器系统，造成较大的危害，建议您及时处理镜像恶意样本。

立即执行镜像安全扫描

需要立即执行镜像安全扫描时，您可以在**镜像安全扫描**页面单击**立即扫描**后，在**一键扫描**对话框中选择需要扫描的镜像类型，并单击**确定**。目前支持选择以下类型的镜像仓库：

- **acr**：选择该类型后，云安全中心将检测您在容器镜像服务控制台创建的企业版实例是否存在安全漏洞和恶意样本。
- **harbor**：选择该类型后，云安全中心将检测您已接入的私有镜像仓库是否存在安全漏洞和恶意样本。

扫描预计需要1分钟时间，您可以在1分钟后手动刷新页面查看扫描结果。

镜像漏洞扫描配置

在**镜像安全扫描**页面单击右上角**设置**，在**镜像漏洞扫描配置**对话框中选择镜像漏洞扫描的周期并单击**确定**。您可以根据需要选择扫描周期和扫描时间段。

- 扫描周期可选择：**每隔3天**、**每隔一周**、**每隔两周**或**停止扫描**。
- 扫描时间段可选择：**00:00~24:00**、**00:00~06:00**、**06:00~12:00**、**12:00~18:00**或**18:00~24:00**。

> **说明** 云安全中心会根据您选择的扫描时间间隔，在选择的扫描时间段内的任意时刻执行镜像安全扫描操作。如果您选择了扫描时间段**00:00~24:00**，则云安全中心可能会在一天内的任何时间点为您执行镜像安全扫描。

镜像漏洞扫描配置

相关文档

容器安全

查看容器安全状态

容器K8s威胁检测

使用运行时刻安全监控

6.安全组配置检查

安全组规则设置不当可能会引起严重的安全事故。安全组配置检查功能为您检查ECS服务器安全组中存在高危风险的规则，并提供修复建议，帮助您更安全高效地使用安全组功能。本文介绍如何在云安全中心控制台使用安全组配置检查功能。

背景信息

云安全中心基础版、基础杀毒版、高级版和企业版用户均支持安全组配置检查功能。

安全组是一种虚拟防火墙，仅适用于阿里云ECS服务器。安全组配置检查功能支持对普通安全组和企业级安全组进行安全检查。安全组相关信息请参见安全组概述。

安全组配置检查功能由云防火墙提供，您可前往云防火墙控制台体验更多网络安全功能。安全组配置检查支持的检查项详情请参见安全组配置检查项列表。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 安全组检查**。
3. （可选）在**安全组配置检查**页面单击**获取最新检查结果**。安全组检查预计需要1~5分钟，请您耐心等待。

   

   > **说明** 此处获取的最新检查结果只是针对安全规则的静态分析得出，可能无法覆盖全部的端口风险情况。您可以在云防火墙**互联网访问活动**页面查看端口相关的全部检查结果，了解端口的实际暴露情况。

4. （可选）在**云资源访问授权**页面单击**同意授权**。为了安全组检查功能的正常使用，您需要赋予当前账号AliyunCloudFirewallAccessingECSRole和AliyunCloudFirewallDefautlRole这两个角色。如果您已进行过授权操作，请跳过该步骤。
5. 在**检查结果详情**区域，查看检测出安全风险的规则详细信息。

   

   您可以查看规则**风险等级**、**检查项名称**、**风险安全组/服务器数**和**检查项状态**信息。

   > **说明** 检查项默认为开启状态。如果需要关闭某个检查项，您可以单击该检查项的**检查项状态**列下的  图标，关闭该检查项。检查项关闭后，云防火墙将不会对该检查项中的安全风险进行检查。

6. 修复高危安全组规则。
   i. 定位到指定规则，单击其操作列下的**修复详情**。您也可以单击**风险安全组数**下的数字跳转至**安全组修复详情**页面。
   ii. 在**安全组修复详情**页面，定位到需要修复的安全组，单击其操作列下的**去安全组修复**。

   

   安全组规则设置不当可能会引起严重的安全事故。**安全组修复详情**页面针对风险安全组提供了**修复建议**，您需要根据**修复建议**尽快修改存在风险的安全组规则。
   如果您是云防火墙高级版及以上版本用户，您将跳转到**安全组列表**页面。您需要根据**修复建议**手动修复高危安全组规则。更多信息请参见修改安全组规则。如果您是云防火墙免费版用户，您需要执行子步骤c中的内容。

iii. （可选）在**推荐使用云防火墙智能修复**对话框，单击**立即升级**或**去安全组手动修复**。可选择的修复方式说明如下：

- **立即升级**：购买云防火墙高级版本，使用云防火墙提供的**安全组配置检查**功能修复安全组高危规则。云防火墙可统一管理安全组和公网IP访问控制策略，及时缩小安全风险暴露面，提高安全管理效率。推荐您使用该方式。
- **去安全组手动修复**：跳转到**安全组列表**页面，手动修复高危安全组规则。更多信息请参见修改安全组规则。

安全组配置检查项列表

检查项名称	安全风险	修复建议
Linux远程运维端口暴露	22端口允许任意IP访问，关联的Linux服务器可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器22端口的访问。如果业务需要访问服务器22端口，建议您限制可访问该端口的公网IP，或使用堡垒机进行远程运维。更多信息请参见什么是堡垒机。
Windows远程运维端口暴露	3389端口允许任意IP访问，关联的Windows服务器可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器3389端口的访问。如果业务需要访问服务器3389端口，建议您限制可访问该端口的公网IP，或使用堡垒机进行远程运维。更多信息请参见什么是堡垒机。
DB2远程运维端口暴露	50000端口允许任意IP访问，关联的DB2数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器50000端口的访问。
ECS加入的安全组数量过多	ECS实例加入了3个及以上安全组，会增加运维难度，提高错误配置风险。	建议一台ECS实例加入的安全组数量小于等于2个。更多信息请参见安全组概述。
Elasticsearch远程运维端口暴露	9200、9300端口允许任意IP访问，关联的Elasticsearch可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器9200、9300端口的访问。
Hadoop YARN远程运维端口暴露	8088端口允许任意IP访问，关联的Hadoop YRAN可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器8088端口的访问。
Hadoop远程运维端口暴露	50070、50030端口允许任意IP访问，关联的Hadoop可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器50070、50030端口的访问。
MongoDB远程运维端口暴露	27017端口允许任意IP访问，关联的Mongo DB数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器27017端口的访问。
MySQL远程运维端口暴露	3306端口允许任意IP访问，关联的MySQL数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器3306端口的访问。
Oracle远程运维端口暴露	1521端口允许任意IP访问，关联的Oracle数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器1521端口的访问。
PostgreSQL远程运维端口暴露	5432端口允许任意IP访问，关联的PostgreSQL数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器5432端口的访问。

检查项名称	安全风险	修复建议
Redis远程运维端口暴露	6379端口允许任意IP访问，关联的Redis数据库可能被暴力破解入侵。	建议您在ECS管理控制台的安全组列表页面配置拒绝公网IP对服务器6379端口的访问。
SQL Server远程运维端口暴露	1433端口允许任意IP访问，关联的SQL Sever数据库可能被暴力破解入侵。	建议您在ECS管理控制台的安全组列表页面配置拒绝公网IP对服务器1433端口的访问。
Spark远程运维端口暴露	6066端口允许任意IP访问，关联的Spark可能被暴力破解入侵。	建议您在ECS管理控制台的安全组列表页面配置拒绝公网IP对服务器6066端口的访问。
Splunk远程运维端口暴露	8089、8090端口允许任意IP访问，关联的Splunk可能被暴力破解入侵。	建议您在ECS管理控制台的安全组列表页面配置拒绝公网IP对服务器8089、8090端口的访问。
访问源过度开放	检查到安全组配置为入方向允许任意IP访问任意端口，关联服务器被入侵风险极大。	建议仅开放业务所需端口，并限制访问源IP范围。

7.常见问题

本文汇总了使用漏洞修复、基线检查和云平台配置检查功能时的常见问题。

- **Linux软件漏洞问题**
  - 如何手动检测服务器上的Linux软件漏洞？
  - 如何获取当前软件版本及漏洞信息？
  - 如何将Ubuntu 14.04系统的3.1*内核升级至4.4内核？
  - 漏洞修复完成后我是否还需要重启系统？
  - 内核漏洞升级修复后，云安全中心仍然提示存在漏洞如何处理？
  - 云安全中心控制台中某些漏洞提示无更新如何处理？
  - Linux软件漏洞各参数说明
- **漏洞修复问题**
  - 漏洞如何修复？
  - 漏洞已经修复了，但云安全中仍提示存在漏洞怎么办？
  - 我对漏洞进行修复，但是提示“权限获取失败，请检查权限后重试”怎么办？
  - 我的服务器Agent客户端已离线或关闭，为什么漏洞还在控制台中显示？
  - 如何清理云安全中心Agent目录中的Windows漏洞修复补丁包？
  - 云安全中心是否支持Elasticsearch漏洞检测？
  - 如何处理连接阿里云官方Yum源超时？
  - 修复漏洞时，提示token校验失败，应该如何处理？
  - 云安全中心无法验证系统漏洞修复时，应该如何处理？
  - 为什么漏洞修复后手动验证没有反应？
  - 为什么进行漏洞回滚操作会失败？
- **漏洞扫描问题**
  - 我有台服务器在资产中心无法开启漏洞检测怎么办？
  - 为什么fastjson类的应急漏洞多次扫描时每次检测结果可能不一致？
  - 漏洞扫描周期说明
  - 漏洞扫描会扫描系统层面和应用层面的漏洞吗？
  - 漏洞实时扫描是如何实现的？
- **基线检查问题**
  - 基线检查验证失败如何处理？
  - 基线和漏洞有什么区别？

如何手动检测服务器上的Linux软件漏洞？

如果您需要手动检测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。

建议您使用云安全中心的Linux软件漏洞功能定期自动检测服务器上的软件漏洞，以便及时发现漏洞。

如何获取当前软件版本及漏洞信息？

云安全中心通过匹配您服务器上的系统软件版本和存在漏洞（CVE 漏洞）的软件版本，判断您的服务器是否存在软件漏洞。因此，您可以通过以下方式查看当前软件版本的漏洞信息：

- **在云安全中心中查看当前软件版本及漏洞信息**

您可以在云安全中心控制台**安全防范 > 漏洞修复**页面，查看云安全中心在您的服务器上检测到的系统软件版本及漏洞信息。关于云安全中心对系统软件漏洞的各项参数说明，请参见Linux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**

  您也可以在服务器上直接查看当前软件版本信息：

  - **CentOS系统**

    执行 `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**

    执行 `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，您可以执行 `dpkg-query -W` 查看服务器上安装的所有软件列表。

通过以上命令获取您服务器上的软件版本信息后，您可以将得到的软件版本信息与云安全中心系统软件漏洞中检测到的相关漏洞的说明信息进行对比。漏洞说明参数中的**软件**和**命中**分别指当前软件版本和漏洞的匹配命中规则。

> **说明** 如果升级后旧版本软件包还有残留信息，这些旧版本信息可能仍会被云安全中心检测收集，并作为漏洞上报。如果确认是由于这种情况触发的漏洞告警，建议您选择忽略该漏洞。您也可以执行 `yum remove` 或者 `apt-get remove` 命令删除旧版本的软件包。删除前，请务必确认所有业务和应用都不再使用该旧版本软件。

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建议 中的方法进行升级。

参考以下方法将Ubuntu 14.04系统的3.1*内核升级至4.4内核。

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*。
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。

  

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

  

漏洞修复完成后我是否还需要重启系统？

在云安全中心控制台完成Linux内核漏洞修复后，还需要对服务器系统进行重启，漏洞修复才能生效。

满足以下任一条件您可以判定漏洞修复后需要重启系统：

- 您的服务器是Linux系统服务器，并且修复的漏洞为Linux内核漏洞。
- 在云安全中心控制台**安全防范 > 漏洞修复**的**Linux软件漏洞**页面，该漏洞的漏洞公告信息中有需要重启的标签。

  

内核漏洞升级修复后，云安全中心仍然提示存在漏洞如何处理？

由于内核升级比较特殊，可能会存在旧版本内核信息残留的问题。如果确认该漏洞告警是由于旧版本信息残留造成的，您可以选择忽略该漏洞告警，或者在服务器中手动删除旧版本的残留信息。可参考以下步骤进行处理：

1. 确认内核升级完成后，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Linux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旧版本的内核rpm安装包，仍将会被云安全中心检测到并进行漏洞告警。您需要确认当前系统中已经没有旧版本rpm安装包残留。如果有，您可以在服务器中对旧版本安装包进行卸载。

   > **说明** 卸载旧版本安装包前，请务必确认当前系统已经使用新内核。强烈建议您在卸载旧版本内核安装包前，为您的系统创建快照，以便卸载旧版本发生异常情况时对系统进行恢复。

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，可以参考如下步骤忽略该系统漏洞告警提醒。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全防范 > 漏洞修复**。
3. 在**Linux软件漏洞**页面定位到该漏洞，单击漏洞名称进入**漏洞详情**页面。
4. 在操作列下单击  图标下的**忽略**。

云安全中心控制台中某些漏洞提示无更新如何处理？

您可以根据以下情况采取不同的处理方式：

- 您在对某些漏洞进行更新修复时，可能收到以下提示：

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

  或者

```
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，但仍然无法满足云安全中心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是否在官方的支持范围中。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，建议您在云安全中心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。

Linux软件漏洞各参数说明

您可以在云安全中心控制台**安全防范 > 漏洞修复**的**Linux软件漏洞**页签下，查看到云安全中心在您的资产中检测到的Linux软件漏洞。您可以单击需要查看的漏洞名称，进入该漏洞的详情页面。以下内容介绍详情页面展示的Linux软件漏洞相关参数。

- **漏洞公告**

  Linux软件漏洞公告的名称，一般以CVE 、RHSA或USN开头。例如，RHSA-2016:2972: vim security update。

  漏洞公告

- **影响分**

  漏洞影响分（即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，可以帮助您确定漏洞修复的紧急度和重要度。

- **漏洞编号**

  漏洞编号是漏洞对应的CVE漏洞号（即CVEID），例如CVE-2016-XXXX。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。

- **漏洞紧急程度**

  漏洞紧急程度即漏洞修复的优先级，分为高、中、低3个等级。

  漏洞等级

  > **说明** 上图示例中的漏洞为中等级漏洞，此漏洞可以延后修复。

  - 高等级的漏洞包括：
    - 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的漏洞。
    - 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。

- **中**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。
- **低**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，可进一步利用的漏洞。
  - 可导致本地拒绝服务的漏洞。
  - 其他危害较低的漏洞。

- **影响说明**

  漏洞的影响说明提供了该漏洞当前软件版本、漏洞程序命中原因和漏洞程序所在路径信息。

  在某个漏洞的详情页面，单击具体漏洞操作列的**详情**，可查看当前漏洞的影响说明等信息。

  

  影响说明包含以下信息。

  - **软件**：云安全中心检测到服务器中出现漏洞的软件的版本信息。上图示例中，检测到服务器上的mariadb-libs当前版本是 5.5.52-1.el7。
  - **命中**：该软件漏洞的命中原因，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），导致存在该漏洞。上图示例中，该软件漏洞命中的原因为mariadb-libs软件版本低于1:5.5.56-2.el7。
  - **路径**：云安全中心检查到的漏洞程序在您服务器上的路径。上图示例中，mariadb-libs所在路径为 */etc/ld.so.conf.d/mariadb-x86_64.con*。

- **操作**

  您可对检测到的Linux漏洞执行以下操作：

  - 修复：修复该漏洞。
  - 验证：验证漏洞是否已修复成功。
  - 忽略：忽略该漏洞。

  更多详细信息请参见Linux软件漏洞。

漏洞如何修复？

云安全中心支持在控制台修复Linux软件漏洞、Windows系统漏洞和Web-CMS漏洞，应用漏洞和应急漏洞只支持检测，不支持修复。

您可以在云安全中心控制台**漏洞修复**页面，定位到需要修复的Linux软件漏洞、Windows系统漏洞或Web-CMS漏洞，单击其操作列的**修复**，Linux软件漏洞和Windows系统漏洞您可以选择创建快照进行修复。修复完成后，需要重启的漏洞会显示**待重启**，请您根据提示重启服务器后再验证漏洞。

对于应用漏洞和应急漏洞您需要根据漏洞详情页面的修复建议，手动修复漏洞。修复完成后，在漏洞修复页面，验证该漏洞。

漏洞已经修复了，但云安全中仍提示存在漏洞怎么办？

出现该情况是因为部分漏洞（即Linux内核漏洞）修复后需要重启服务器。请在漏洞详情页面，单击**重启**。重启完成后，单击**验证**，显示修复成功则代表该漏洞已修复成功。

我对漏洞进行修复，但是提示“权限获取失败，请检查权限后重试”怎么办？

出现该情况是因为当前登录的账户对所需操作的文件没有权限。建议您单击漏洞名称，查看漏洞详情，查看漏洞需要修复的文件其所属用户是否为root。如果不是root，请前往您的服务器中将该文件的所属用户改为root。文件所属用户修改完成后，再在云安全中心控制台执行修复操作。

我的服务器Agent客户端已离线或关闭，为什么漏洞还在控制台中显示？

服务器Agent客户端离线或关闭时，服务器上的漏洞在7天后才会自动失效，漏洞记录无法直接清除。

如何清理云安全中心Agent目录中的Windows漏洞修复补丁包？

执行一键修复Windows系统漏洞后，由云安全中心Agent负责安装包的自动下载、安装和清理，无需您进行手动操作。漏洞修复完成超过3天后，如果安装包未被及时清理掉，您可参考以下步骤手动清理漏洞补丁包：

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**设置**。
3. （可选）关闭客户端自保护模式。

   如果您未开启过客户端自保护模式，请跳过当前步骤，直接执行下一步骤。

   客户端自保护模式会对您服务器Agent目录下的所有进程文件提供默认保护。自保护模式开启情况下，您在Windows服务器上对Agent目录下的任何进程文件进行删除或下载操作都会被云安全中心拒绝。有关客户端自保护的详细内容请参见客户端自保护。
4. 使用管理员权限登录您的Windows服务器。
5. 找到漏洞补丁包并手动删除。

   补丁包所在的路径为*C:\Program Files (x86)\Alibaba\Aegis\globalcfg\hotfix*。

云安全中心是否支持Elasticsearch漏洞检测？

支持。

您可以在云安全中心控制台**安全防范 > 漏洞修复**页面的**应用漏洞**，查看是否检测出Elasticsearch漏洞。Elasticsearch的漏洞详情及修复方案，请参见Elasticsearch服务安全加固。

> **说明** 应用漏洞为企业版功能，基础版、基础杀毒版和高级版不支持。基础版、基础杀毒版和高级版用户需先升级到企业版，才可使用应用漏洞功能。

如何处理连接阿里云官方Yum源超时？

当连接阿里云官方Yum源超时时，会出现类似如下的报错信息：

```
[Errno 12] Timeout on http://mirrors.aliyun.com/centos/6/os/x86_64/repodata/repomd.xml: (28, 'connect(
) timed out!')
```

这种情况下，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，通过售后服务进行排查。

修复漏洞时，提示token校验失败，应该如何处理？

当您在云安全中心控制台执行某项操作，收到token校验失效的提示时，您可以刷新当前页面，重新登录云安全中心控制台。

> 说明 您可按Ctrl+F5，强制刷新当前浏览器页面。

云安全中心无法验证系统漏洞修复时，应该如何处理？

当云安全中心无法验证系统漏洞修复时，请按照以下步骤进行排查：

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执行过验证操作。

   > 说明 升级内核需重启才能生效。

4. 确认选择修复的版本不低于云安全中心建议的版本。

如果以上方案未能解决问题，建议您升级操作系统。

为什么漏洞修复后手动验证没有反应？

您在服务器上手动执行云安全中心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，并且该版本已符合云安全中心控制台**漏洞修复**页面的描述要求。然而，当您在云安全中心管理控制台的漏洞详情页面，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。

您可以使用以下方法进行排查，解决该问题：

- 检查漏洞扫描等级

  执行如下步骤，检查漏洞扫描等级。

  i. 登录云安全中心控制台。
  ii. 在左侧导航栏单击**安全防范 > 漏洞修复**。
  iii. 在**漏洞修复**页面单击右上角**漏洞管理设置**。
  iv. 在**漏洞管理设置**页面，查看**漏洞扫描等级**选中的等级。

  如果对应的扫描等级没有选中，则相应等级的漏洞数据不会自动更新。您可以根据需要选择对应的扫描等级。

- 云安全中心Agent版本过低

  如果您服务器上的云安全中心Agent版本过低，则可能不支持漏洞扫描功能。如果您的云安全中心Agent没有正常自动更新，建议您手动安装最新版云安全中心Agent。更多信息请参见安装Agent。

- 云安全中心Agent离线

  如果您服务器上的云安全中心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。建议您排查Agent离线原因，确保您服务器上的云安全中心Agent在线。更多信息请参见Agent 离线排查。

为什么进行漏洞回滚操作会失败？

当通过云安全中心漏洞管理功能对某个漏洞进行回滚操作时，提示回滚失败，您可以参考以下步骤排查问题：

1. 确认您的服务器的云安全中心Agent是否处于在线状态。如果您的服务器显示离线，请排查Agent离线原因。更多信息请参见Agent 离线排查。
2. 确认您服务器上该漏洞的相关文件是否已被手工修改或者删除。

> **说明** 如果在漏洞修复后相关文件已被手动修改或者删除，云安全中心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。

我有台服务器在资产中心无法开启漏洞检测怎么办？

您可以在**漏洞修复 > 漏洞管理设置**页面配置进行漏洞检测的服务器。如下图所示，还有四台服务器未开启Linux软件漏洞检测，即云安全中心无法扫描这四台服务器上的Linux软件漏洞。如果您需要开启这些服务器的漏洞检测，请单击对应漏洞右侧的**管理**，开启这些服务器的漏洞检测。

为什么fastjson类的应急漏洞多次扫描时每次检测结果可能不一致？

云安全中心检测fastjson类的应急漏洞时，如果fastjson的Jar包不在运行中，可能无法检测到相应漏洞。所以进行多次扫描时可能会出现不一样的检测结果。建议您定期进行fastjson类应急漏洞的扫描。

漏洞扫描周期说明

云安全中心支持漏洞扫描和修复，覆盖Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞、应急漏洞、应用漏洞等类型。以下表格展示了各类型漏洞默认的扫描周期。

漏洞类型	基础版	基础杀毒版	高级版	企业版
Linux软件漏洞	每隔一天自动扫描一次	每隔一天自动扫描一次	每天自动扫描一次	每天自动扫描一次
Windows系统漏洞	每隔一天自动扫描一次	每隔一天自动扫描一次	每天自动扫描一次	每天自动扫描一次
Web-CMS漏洞	每隔一天自动扫描一次	每隔一天自动扫描一次	每天自动扫描一次	每天自动扫描一次
应用漏洞	不支持扫描	不支持扫描	不支持扫描	每周自动扫描一次（支持修改自动扫描周期）
应急漏洞	仅支持手动扫描	仅支持手动扫描	仅支持手动扫描	仅支持手动扫描
容器镜像漏洞	不支持扫描	不支持扫描	不支持扫描	仅支持开通了容器镜像服务的用户进行手动扫描

如果需要开启或关闭某种类型漏洞的扫描能力，或修改应用漏洞的扫描周期，可使用**漏洞管理设置**功能。更多信息请参见漏洞管理设置。如果您需要立即扫描您的资产中是否存在漏洞，可使用云安全中心提供的一键扫描功能。更多信息请参见一键扫描漏洞。

漏洞扫描完成后，您可在云安全中心控制台**安全防范 > 漏洞修复**页面查看漏洞检测的结果并进行相应处理。

漏洞扫描会扫描系统层面和应用层面的漏洞吗？

是的，漏洞扫描会扫描系统漏洞（服务器上系统层级漏洞）和Web漏洞（应用层漏洞）。

漏洞实时扫描是如何实现的？

漏洞扫描每天会收集用户资产中新增的URL，然后在凌晨对这些新增的URL进行扫描。同时，还会扫描之前被曝出的漏洞，验证这些漏洞有没有被修复。实时主要指实时获取URL，等到凌晨再进行扫描。

基线检查验证失败如何处理？

云安全中心基线检查验证已修复风险项失败可能由以下原因导致：

- Agent版本过低

  如果您服务器上的云安全中心Agent版本过低，可能导致基线检查失败。如果您的云安全中心Agent没有正常自动更新，建议您手动安装最新版Agent。安装Agent的详细操作请参见安装Agent。

- Agent离线

  如果您服务器上的云安全中心Agent显示为离线，云安全中心基线检查将无法执行。建议您对Agent离线进行排查，确保您服务器上的云安全中心Agent在线。Agent离线排查的详细内容请参见Agent离线排查。

基线和漏洞有什么区别？

基线一般指配置和管理系统的详细描述，或者说是最低的安全要求，包括服务和应用程序设置、操作系统组件的配置、权限和权利分配、管理规则等。云安全中心的基线检查功能支持检测操作系统和服务（数据库、服务器软件、容器等）的弱口令、账号权限、身份鉴别、密码策略、访问控制、安全审计和入侵防范等安全配置，并提供检测结果，针对存在的风险配置给出加固建议。具体的检测项，请参见基线检查内容。

漏洞是指在操作系统实现或安全策略上存在的缺陷，例如操作系统软件或应用软件在逻辑设计上存在的缺陷或在编写时产生的错误。攻击者可以对这类缺陷或错误进行利用，从而能够在未获得授权的情况下访问和窃取您的系统数据或破坏系统。系统漏洞需要系统管理员及时处理并修复，否则将带来严重的安全隐患。

基线检查功能为云安全中心的增值服务，仅**高级版**和**企业版**用户可开通和使用该服务。基础版、基础杀毒版用户都需先升级到高级版或企业版才可使用基线检查功能。有关升级的更多信息请参见升级与降配。