ALIBABA CLOUD

阿里云

云安全中心（态势感知）

安全防范

文档版本：20220712

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

云安全中心提供漏洞修复功能，支持对常见漏洞类型进行扫描和修复，可以帮助您更全面地了解并修复您资产中的漏洞风险。本文介绍漏洞修复功能支持扫描和修复的漏洞类型、漏洞修复的优先级以及对操作系统的限制说明。

支持扫描和修复的漏洞类型

下表介绍云安全中心的不同版本对各类型漏洞的扫描、修复的支持情况。

> **说明** 下表中的标识说明如下：
>
> - ✓：表示支持。
> - ×：表示不支持。

漏洞类型	功能模块						
Linux软件漏洞	漏洞扫描	手动扫描	×	×	✓	✓	✓
		周期性自动扫描	✓（默认每2天）	✓（默认每2天）	✓（默认每天）	✓（默认每天）	✓（默认每天）
	漏洞修复						
Windows系统漏洞	漏洞扫描	手动扫描	×	×	✓	✓	✓
		周期性自动扫描	✓（默认每2天）	✓（默认每2天）	✓（默认每天）	✓（默认每天）	✓（默认每天）
	漏洞修复						
Web-CMS漏洞	漏洞扫描	手动扫描	×	×	✓	✓	✓
		周期性自动扫描	✓（默认每2天）	✓（默认每2天）	✓（默认每天）	✓（默认每天）	✓（默认每天）
	漏洞修复						

漏洞类型	功能模块						
应用漏洞	漏洞扫描	手动扫描	×	×	×	✓	✓
		周期性自动扫描	×	×	×	✓（每周，支持配置）	✓（每周，支持配置）
	漏洞修复						
应急漏洞	漏洞扫描	手动扫描	✓	✓	✓	✓	✓
		周期性自动扫描	×	×	✓（每周，支持配置）	✓（每周，支持配置）	✓（每周，支持配置）
	漏洞修复						

说明 云安全中心仅支持扫描应急漏洞和应用漏洞，不支持修复。您需要根据漏洞详情中提供的修复建议，登录服务器手动修复。

漏洞修复优先级

当您的资产被扫描出存在多个漏洞时，您可能无法确认优先修复哪个漏洞。针对此场景，云安全中心提供的阿里云漏洞脆弱性评分系统能评估修复漏洞的优先顺序，帮助您做出漏洞修复优先级决策。

阿里云漏洞脆弱性评分系统

通用漏洞评分系统（Common Vulnerability Scoring System，简称CVSS）在捕捉漏洞的范围和影响方面成效显著，该系统不仅能够评估某个漏洞被利用的可能性，还能很好地解释该漏洞一旦被利用会有什么后果。阿里云在CVSS的基础上，结合实际攻防场景下漏洞严重性级别开发了阿里云漏洞脆弱性评分系统。

阿里云漏洞脆弱性评分系统在使用CVSS确定漏洞修复优先级和严重性的基础上，根据云上实际攻防场景下漏洞严重性级别（严重、高、中和低），结合互联网实际披露的漏洞可利用程序状态，以及云安全中心入侵检测数据模型中的黑客利用漏洞的成熟度对漏洞进行评分，帮助企业提高资产高可利用风险漏洞的补救效率以及补救措施的有效性。

说明 漏洞的严重性级别由四个因素决定：

- 技术影响
- 利用成熟度（PoC、EXP、蠕虫或病毒武器化）
- 风险威胁（服务器权限失陷与否）
- 受影响数量级（互联网受影响IP量级决定漏洞被黑客关注程度）

漏洞修复紧急度得分计算模型

漏洞修复的紧急度得分是一个动态变化的数据。当漏洞被披露时，阿里云漏洞脆弱性评分系统会根据漏洞本身固有特性所可能造成的影响给该漏洞一个基本评分，即阿里云漏洞脆弱性评分。随着时间的推移，通过软件版本的更新对漏洞进行修复，存在漏洞的系统越来越少，漏洞的威胁也越来越小，漏洞修复紧急度得分也应该随之降低。另外漏洞修复紧急度得分还与资产的部署环境、资产的重要性有关。

综合以上影响漏洞修复紧急度得分的因素，阿里云漏洞修复紧急度得分计算模型如下：

漏洞修复紧急度得分=阿里云漏洞脆弱性评分*时间因子*实际环境因子*资产重要性因子

计算模型中的各参数的说明如下：

参数	参数项解释	附加说明
阿里云漏洞脆弱性评分	基于阿里云漏洞脆弱性评分系统指标。	阿里云漏洞脆弱性评分系统指标，用来评测漏洞的严重程度。
时间因子	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	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

漏洞修复优先级

您可根据漏洞修复紧急度得分按照漏洞修复的优先级顺序修复漏洞。

漏洞修复紧急度得分与修复优先级对照表如下：

优先级	描述	修复紧急度得分	修复建议
高	该评级是针对未经身份验证的远程攻击者可以轻松利用并导致系统受损（任意代码执行）而无需用户交互的漏洞。此类漏洞通常为蠕虫、勒索软件等利用的漏洞。	13.5分以上	该漏洞需尽快修复。
中	该评级适用于潜在可能危及资源的机密性、完整性或可用性的缺陷。此类漏洞通常为暂无法真实可利用，但官方或互联网上披露的评级较高漏洞，建议持续关注。	7.1~13.5分	该漏洞可延后修复。
低	该评级适用于能被成功利用可能性极低或者成功利用后无实际风险的漏洞。此类漏洞通常是程序源代码中的BUG缺陷，以及对合规场景和业务性能有影响的漏洞。	7分以下	该漏洞暂可不修复。

> 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。

限制说明

云安全中心针对服务器的操作系统版本，存在以下限制。

- 漏洞扫描和修复功能支持以下操作系统版本

操作系统类型	版本
CentOS	CentOS 7、CentOS 5（EOL之前的漏洞）、CentOS 6（EOL之前的漏洞）、CentOS 8（EOL之前的漏洞）
Redhat	Redhat 7、Redhat 8、Redhat 5（EOL之前的漏洞）、Redhat6（EOL之前的漏洞）
Ubuntu	Ubuntu 12（EOL之前的漏洞）、Ubuntu 14（EOL之前的漏洞）、Ubuntu 16（EOL之前的漏洞）、Ubuntu 18、Ubuntu 20、Ubuntu 21
Windows Server	Windows Server 2008（EOL之前的漏洞）、Windows Server 2012、Windows Server 2016、Windows Server 2019
Alibaba Cloud Linux	Alibaba Cloud Linux 2.1903、Alibaba Cloud Linux 3
Anolis OS	Anolis OS 8、Anolis OS 7.9

- 操作系统生命周期限制
  针对下表所示的已终止生命周期（EOL）的操作系统，云安全中心在EOL时间之后不再继续扫描和修复对应的漏洞补丁。

操作系统版本	官方终止生命周期（EOL）时间	云安全中心支持漏洞补丁情况
Windows Server 2003	2015年07月14日	云安全中心支持和修复2015年07月14日之前出现的漏洞补丁，不再支持检测和修复该日期之后出现的漏洞。
Windows Server 2008	2020年01月14日	云安全中心支持检测和修复2020年01月14日之前出现的漏洞补丁，不再支持检测和修复该日期之后出现的漏洞。
Windows Server 2008 R2	2020年01月14日	云安全中心支持检测和修复2020年01月14日之前出现的漏洞补丁，不再支持检测和修复该日期之后出现的漏洞。
Windows Server 2008 SP2	2020年01月14日	云安全中心支持检测和修复2020年01月14日之前出现的漏洞补丁，不再支持检测和修复该日期之后出现的漏洞。

操作系统版本	官方终止生命周期（EOL）时间	云安全中心支持漏洞补丁情况
Ubuntu 12.04 LTS	2017年04月28日	云安全中心支持检测和修复2017年04月28日之前出现的漏洞补丁，不再支持检测和修复该日期之后出现的漏洞。
Ubuntu 14.04 LTS	2019年04月	云安全中心支持检测和修复2019年04月之前出现的漏洞补丁，不再支持检测和修复该日期之后出现的漏洞。
Ubuntu 16.04 LTS	2021年05月	云安全中心支持检测和修复2021年05月之前出现的漏洞补丁，不再支持检测和修复该日期之后出现的漏洞。
CentOS 5	2017年03月31日	云安全中心支持检测和修复2017年03月31日之前出现的漏洞补丁，不再支持检测和修复该日期之后出现的漏洞。
CentOS 6	2020年11月30日	云安全中心支持检测和修复2020年11月30日之前出现的漏洞补丁，不再支持检测和修复该日期之后出现的漏洞。
CentOS 8	2021年12月31日	云安全中心支持检测和修复2021年12月31日之前出现的漏洞补丁，不再支持检测和修复该日期之后出现的漏洞。
Redhat 5	2017年03月31日	云安全中心支持检测和修复2017年03月31日之前出现的漏洞补丁，不再支持检测和修复该日期之后出现的漏洞。
Redhat 6	2020年11月30日	云安全中心支持检测和修复2020年11月30日之前出现的漏洞补丁，不再支持检测和修复该日期之后出现的漏洞。

相关文档

漏洞扫描周期说明

基线和漏洞有什么区别？

我有台服务器在资产中心无法开启漏洞检测怎么办？

1.2. 扫描漏洞

为了您的资产安全，建议您定期对资产进行漏洞扫描。云安全中心支持周期性自动扫描漏洞和手动扫描漏洞。本文介绍如何设置周期性自动扫描漏洞和执行手动扫描漏洞。

背景信息

云安全中心的不同版本对各类型漏洞的扫描、修复的支持情况如下表。

漏洞类型	功能模块						
Linux软件漏洞	漏洞扫描	手动扫描	×	×	✓	✓	✓
		周期性自动扫描	✓（默认每2天）	✓（默认每2天）	✓（默认每天）	✓（默认每天）	✓（默认每天）
	漏洞修复						
Windows系统漏洞	漏洞扫描	手动扫描	×	×	✓	✓	✓
		周期性自动扫描	✓（默认每2天）	✓（默认每2天）	✓（默认每天）	✓（默认每天）	✓（默认每天）
	漏洞修复						
Web-CMS漏洞	漏洞扫描	手动扫描	×	×	✓	✓	✓
		周期性自动扫描	✓（默认每2天）	✓（默认每2天）	✓（默认每天）	✓（默认每天）	✓（默认每天）
	漏洞修复						
应用漏洞	漏洞扫描	手动扫描	×	×	×	✓	✓
		周期性自动扫描	×	×	×	✓（每周，支持配置）	✓（每周，支持配置）
	漏洞修复						
应急漏洞	漏洞扫描	手动扫描	✓	✓	✓	✓	✓
		周期性自动扫描	×	×	✓（每周，支持配置）	✓（每周，支持配置）	✓（每周，支持配置）

漏洞类型	功能模块	
	漏洞修复	

操作步骤

1. 登录云安全中心控制台，在左侧导航栏，选择**安全防范 > 漏洞修复**。
2. 在**漏洞修复**页面，进行手动扫描漏洞或配置自动扫描漏洞。
   - 手动扫描漏洞
     如果您想立即了解服务器是否存在漏洞风险，您可以使用**一键扫描**功能，手动扫描服务器中的漏洞。
     a. 在**漏洞修复**页面，单击**一键扫描**。
     进行**一键扫描**前，您可单击右上角的**漏洞管理设置**，在**漏洞管理设置**面板上，单击漏洞检查项右侧的**管理**，查看要扫描的服务器是否已添加到扫描生效的服务器列表中。
     b. 在**漏洞扫描**对话框，选中要扫描的漏洞类型，并单击**确定**。

     > **说明** **一键扫描**会对云安全中心保护的所有资产进行检测，预计30分钟内完成扫描，请耐心等待，您可以手动刷新页面查看最新扫描数据。

   - 自动扫描漏洞
     您可以配置漏洞的自动扫描周期，定期对服务器上存在的漏洞进行自动扫描。
     a. 在**漏洞修复**页面右上角，单击**漏洞管理设置**。
     b. 在**漏洞管理设置**面板上，按业务需要进行配置。

配置项	说明
Linux软件漏洞	开启或关闭该类型漏洞扫描。开启后，单击右侧**管理**，添加或移除要扫描的服务器资产。
Windows系统漏洞	
Web-CMS漏洞	
应急漏洞	
应用漏洞	开启或关闭应用漏洞检测。

配置项	说明
YUM/APT源配置	开启或关闭优先使用阿里云源进行漏洞修复。 **说明** 在修复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。打开该开关后，云安全中心会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。建议您选择打开**YUM/APT源配置**开关。
应急漏洞扫描周期	设置应急漏洞扫描周期。 **说明** ■ 仅支持高级版、企业版和旗舰版用户设置**应急漏洞扫描周期**。应急漏洞默认扫描时间段为*00:00:00*至*07:00:00*。 ■ 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。
应用漏洞扫描周期	设置应用漏洞扫描周期。 **说明** 仅支持企业版和旗舰版用户设置**应用漏洞扫描周期**。应用漏洞默认扫描时间段为*00:00:00*至*07:00:00*。
失效漏洞自动删除	设置失效漏洞自动删除的时间。 **说明** 漏洞在被检测出之后，您未对该漏洞进行处理，之后的多次检测中再未检测出该漏洞，那么在达到您设置的失效漏洞自动删除时间时，该漏洞记录将自动从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。
漏洞扫描等级	设置漏洞扫描的等级。 **说明** 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。

配置项	说明
漏洞白名单配置	如果您不想扫描某个漏洞，可以将该漏洞添加到漏洞白名单，系统不会检测漏洞白名单中的漏洞。 ■ **新增白名单规则**：您可以单击右侧的**新增规则**，在**新增规则**面板上基于不同类型的漏洞公告自定义加白规则。 ■ **编辑白名单**：您可单击目标白名单右侧的**编辑**，对该白名单的**规则范围**和**备注**进行修改。 ■ **移除白名单**：您可单击目标白名单右侧的**移除**，将漏洞从白名单中移除。漏洞从白名单移除后，云安全中心将重新启用对该漏洞的检测和告警。

配置完成后，云安全中心将按照您的配置对您的服务器进行漏洞检测。漏洞扫描结束后，您可前往对应的漏洞页签下查看最新的扫描结果。

相关文档

漏洞扫描周期说明

基线和漏洞有什么区别？

我有台服务器在资产中心无法开启漏洞检测怎么办？

1.3. 查看和修复漏洞

为了您的资产安全，建议您及时查看和处理云安全中心扫描出的资产中存在的漏洞。本文介绍如何查看和修复资产中存在的漏洞。

支持扫描和修复的漏洞类型

下表介绍云安全中心的不同版本对各类型漏洞的扫描、修复的支持情况。

说明 下表中的标识说明如下：

- ✓：表示支持。
- ×：表示不支持。

漏洞类型	功能模块						
Linux软件漏洞	漏洞扫描	手动扫描	×	×	✓	✓	✓
		周期性自动扫描	✓（默认每2天）	✓（默认每2天）	✓（默认每天）	✓（默认每天）	✓（默认每天）
	漏洞修复						

漏洞类型	功能模块						
Windows系统漏洞	漏洞扫描	手动扫描	×	×	✓	✓	✓
		周期性自动扫描	✓（默认每2天）	✓（默认每2天）	✓（默认每天）	✓（默认每天）	✓（默认每天）
	漏洞修复						
Web-CMS漏洞	漏洞扫描	手动扫描	×	×	✓	✓	✓
		周期性自动扫描	✓（默认每2天）	✓（默认每2天）	✓（默认每天）	✓（默认每天）	✓（默认每天）
	漏洞修复						
应用漏洞	漏洞扫描	手动扫描	×	×	×	✓	✓
		周期性自动扫描	×	×	×	✓（每周，支持配置）	✓（每周，支持配置）
	漏洞修复						
应急漏洞	漏洞扫描	手动扫描	✓	✓	✓	✓	✓
		周期性自动扫描	×	×	✓（每周，支持配置）	✓（每周，支持配置）	✓（每周，支持配置）
	漏洞修复						

说明 云安全中心仅支持扫描应急漏洞和应用漏洞，不支持修复。您需要根据漏洞详情中提供的修复建议，登录服务器手动修复。

查看漏洞信息

1. 登录云安全中心控制台，在左侧导航栏，选择**安全防范 > 漏洞修复**。

2. 在**漏洞修复**页面，查看资产中存在的漏洞。
   - 查看总览
     您可以在**漏洞修复**页面上方的漏洞信息统计区域查看漏洞的统计信息。

   - 需紧急修复的漏洞（CVE）（图示①）
     单击**需紧急修复的漏洞（CVE）**区域的数字展开**需紧急修复的漏洞（CVE）**面板，面板上为您展示了需要您紧急修复的各类型的漏洞。您可以在面板上查看和修复所有紧急程度为**高**的漏洞。
   - 存在漏洞的服务器（图示②）
     单击**存在漏洞的服务器**下的数字，可跳转到**资产中心 > 服务器**页签，查看存在漏洞问题的服务器资产的详情。
   - 修复中漏洞（图示③）
     单击**修复中漏洞**下的数字，展开**修复中漏洞**面板，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。
   - 今日已处理复漏洞（图示④）
     单击**今日已处理漏洞**下的数字，展开**今日已处理漏洞**面板，查看今日已修复的漏洞的影响资产列表和相关信息。
     - **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**列的**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**列的**回滚**，选择待回滚快照，单击**确定**。

       > **说明** Linux软件漏洞和Windows系统漏洞支持快照回滚功能。

   - 累计已处理漏洞（图示⑤）
     单击**累计已处理漏洞**下的数字，展开**累计已处理漏洞**面板，查看累计已修复的所有漏洞的影响资产列表和相关信息。
   - 已支持漏洞（图示⑥）
     单击**已支持漏洞**下方的数字展开**支持检测的漏洞列表**面板，可查看云安全中心已支持检测的漏洞的列表及查看漏洞的详细信息，包括漏洞的**漏洞编号**、**漏洞名称**、**检测方式**、**发布时间**。您也可以使用列表上方的搜索功能通过漏洞的编号或漏洞的名称搜索某个漏洞云安全中心是否已支持检测。单击目标漏洞的名称，可跳转阿里云漏洞库查看该漏洞的详细信息。

- 最新系统漏洞发现时间（图示⑦）
  下方为您显示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**。详细信息，请参见扫描漏洞。

- 按漏洞类型查看漏洞公告列表
  您可以在**漏洞修复**页面，单击**Linux软件漏洞**、**Windows系统漏洞**等页签，查看资产中存在的不同类型的漏洞的漏洞公告列表。

  > **说明** 在漏洞公告列表的**影响资产**列，漏洞的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。
  > - 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。

- 搜索漏洞
  您可使用漏洞公告列表上方的搜索组件，按漏洞修复的紧急程度、是否已处理、资产分组或输入漏洞名称等搜索目标漏洞。

  > **说明** 漏洞名称支持模糊搜索。

- 查看漏洞详情
  单击漏洞公告的名称，展开漏洞详情面板，在详情面板上，您可以查看漏洞详情及待处理漏洞列表。
- 导出漏洞
  您可单击漏洞公告列表右上方的图标，将云安全中心检测到漏洞导出并保存到本地。导出的文件为Excel格式。

修复漏洞

1. 登录云安全中心控制台，在左侧导航栏，选择**安全防范 > 漏洞修复**。
2. 在**漏洞修复**页面，修复资产中存在的漏洞。
   - 加入白名单
     如果某个漏洞您判断不需要修复，并且以后不再上报该漏洞，您可以将该漏洞加入白名单。
     在漏洞公告列表中，选中一个或多个要加入白名单的漏洞公告，单击列表下方的**加入白名单**，在对话框中单击**确定**。

     > **说明** 加入白名单后，所选漏洞记录将自动删除，并且以后不再提醒，如需取消白名单请到漏洞管理设置中删除该白名单规则。

1.4. Windows系统漏洞

云安全中心支持检测并快速修复Windows系统漏洞。本文介绍如何查看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

云安全中心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

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，选择**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**页签下，查看和管理云安全中心检测到的所有Windows系统漏洞信息。

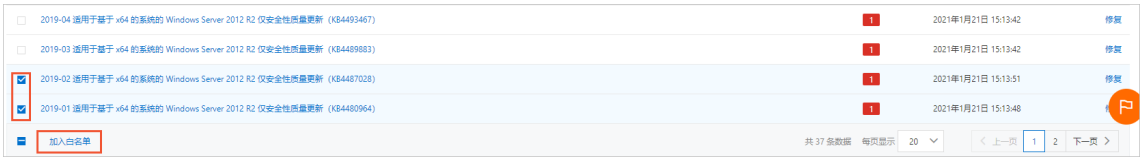
   您可以执行以下操作：

   - **查看漏洞公告信息**
     您可在**Windows系统漏洞**页签下的漏洞公告列表中，查看漏洞公告信息。

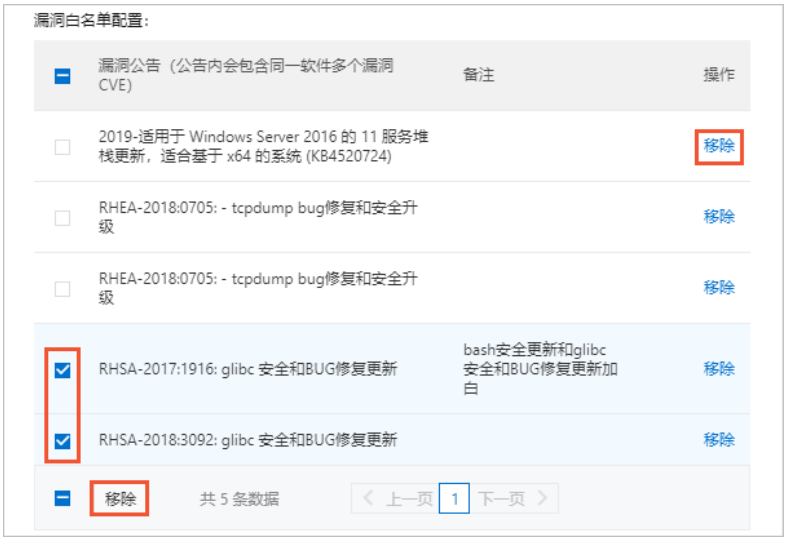
   - **查看漏洞的修复紧急程度建议**

     > 说明 建议立即修复高危漏洞（紧急程度为高）。

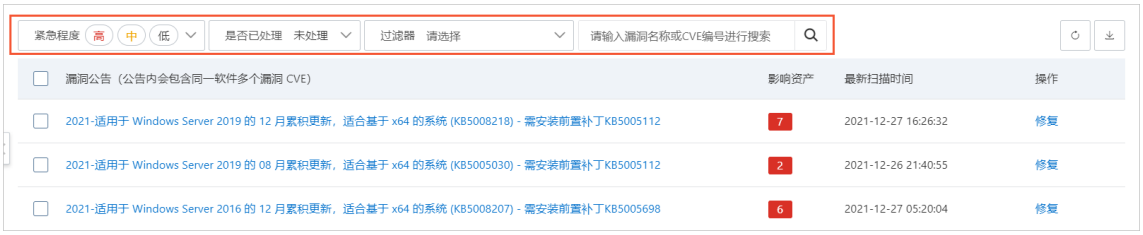
   - **将漏洞加入白名单**
     您可在**Windows系统漏洞**页签下，选中需要加入白名单的漏洞并单击**加入白名单**，将该漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。



   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。



- **搜索漏洞**
  您可在**Windows系统漏洞**页签下，使用以下功能中的一个或者多个组合筛选或搜索目标漏洞：



- **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系统漏洞导出并保存到本地。导出的文件为Excel格式。

  > 说明

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，选择**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**漏洞详情**面板。
   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**面板，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**
     - 在**漏洞详情**页签下，查看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**待处理漏洞**页签下，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。

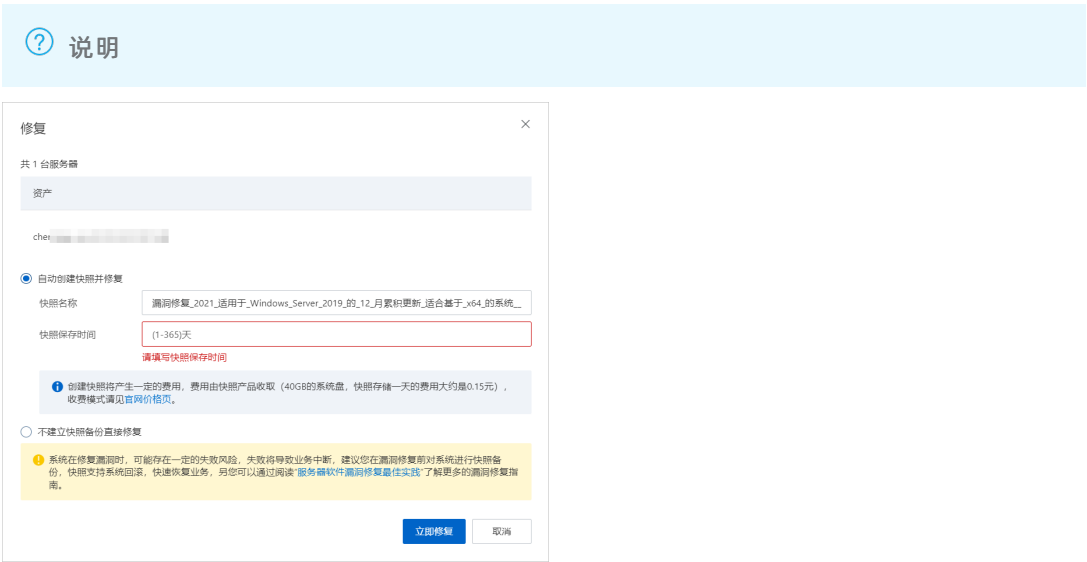
   - **查看漏洞详细状态**
     - **已处理**

- **未处理**
  -
  -
  -
  - 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：

  - 您需要分以下两种情况修复漏洞：
    - **修复**按钮显示正常



    - **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。
  -

- **将漏洞加入白名单**
  您可在**Windows系统漏洞**页签下，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。
-

- **搜索漏洞影响资产**
- **导出漏洞影响资产**

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

漏洞扫描周期说明

基线和漏洞有什么区别？

我有台服务器在资产中心无法开启漏洞检测怎么办？

1.5. 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）。本文介绍如何查看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**
>
> -
> - 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。

云安全中心支持检测的Web-CMS漏洞列表，请参见支持检测的Web-CMS漏洞。

查看漏洞基本信息

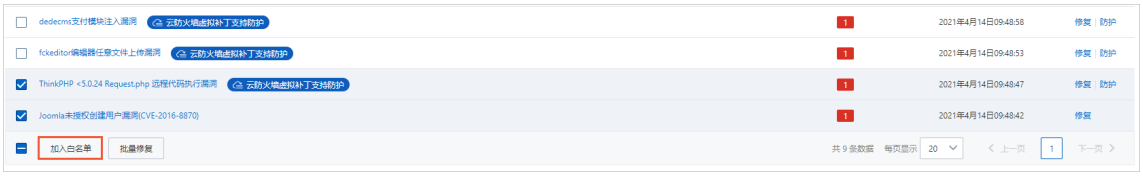
1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全防范 > 漏洞修复**。
3. 在**漏洞修复**页面，单击**Web-CMS漏洞**页签。
4. 在**Web-CMS漏洞**页面，查看云安全中心检测到的所有Web-CMS漏洞信息。
   您可以进行以下操作：
   - **查看漏洞信息**

- **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。

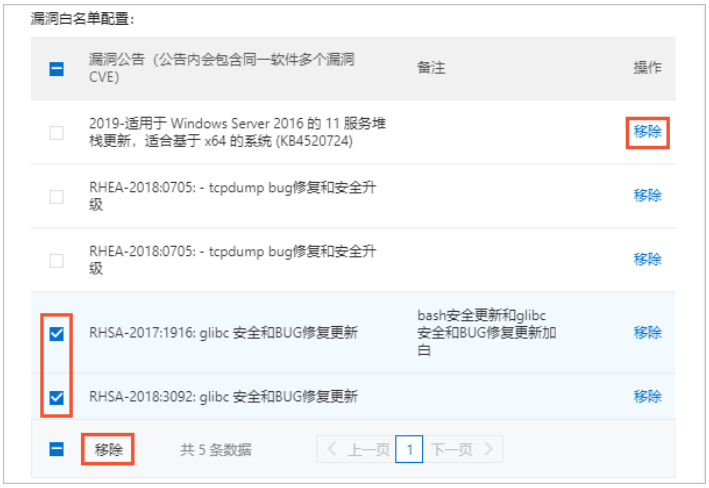
  > **说明** 建议尽快修复Web-CMS类型漏洞。

- **处理云防火墙可防护漏洞**
  云安全中心针对云防火墙可以防护的漏洞，提供**云防火墙虚拟补丁支持防护**标签，您可以单击该标签或该漏洞操作列的**防护**跳转至云防火墙控制台为该漏洞开启防护。具体操作，请参见漏洞防护。

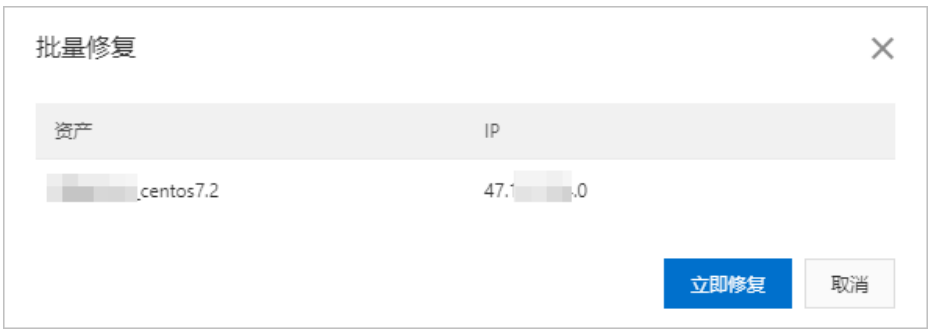
- **将漏洞加入白名单**
  您可在**Web-CMS漏洞**页面，选中需要加入白名单的漏洞并单击**加入白名单**，将该漏洞加入白名单中。加入白名单后，云安全中心将不再对白名单中的漏洞进行告警。



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。

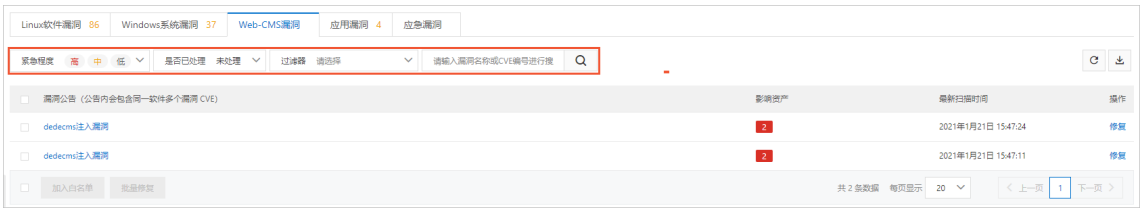


- **批量修复漏洞**
  批量修复功能会自动识别您选择的漏洞公告对应的资产，并修复这些资产中您所选择的漏洞。您可在**Web-CMS漏洞**页面，选择需要批量修复的漏洞并单击**批量修复**。在**批量修复**对话框中查看云安全中心为您识别出的需要修复漏洞的资产列表，单击**立即修复**。



> **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

- **导出漏洞**

  您可在**Web-CMS漏洞**页面，单击 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

处理漏洞

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**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**面板。
   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**

> **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。

- **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**。

> **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。
-

- **导出漏洞影响资产**

支持检测的Web-CMS漏洞

组件类型	检测项
	74CMS多处SQL注入漏洞
	74CMS越权漏洞
	74CMS SQL注入漏洞

组件类型	检测项
	74CMS V4.1.15一处任意文件删除
	74CMS最新版本任意文件读取漏洞
DedeCMS	DedeCMS变量覆盖漏洞
	DedeCMS任意文件上传漏洞
	DedeCMS重装漏洞
	DedeCMS注入漏洞
	DedeCMS上传漏洞
	DedeCMS密码重置漏洞
	DedeCMS Cookies泄漏导致前台任意用户登录漏洞
	DedeCMS SESSION变量覆盖导致SQL注入
	DedeCMS后台文件任意上传漏洞
	DedeCMS SQL注入漏洞
	DedeCMS模版SQL注入漏洞
	DedeCMS Cookies泄漏导致SQL漏洞
	DedeCMS支付模块注入漏洞
	DedeCMS V5.7注册用户任意文件删除漏洞
	DedeCMS V5.7 CSRF保护措施绕过漏洞
	DedeCMS select_soft_post.php普通用户权限支持上传任意文件漏洞
	DedeCMS V5.7 sp2任意文件上传漏洞 （CVE-2019-8362）
Discuz	Discuz代码执行漏洞
	Discuz MemCache+ssrf获取权限漏洞（GetShell）
	Discuz后台SQL注入漏洞
	Discuz越权漏洞导致任意附件下载
	Discuz任意文件删除漏洞
	Discuz AuthCode函数缺陷导致密文伪造漏洞
	Discuz!后台数据库备份功能命令执行漏洞

组件类型	检测项
ECShop	ECShop代码注入漏洞
	ECShop密码找回漏洞
	ECShop注入漏洞
	ECShop后门
	ECShop任意用户登录漏洞
	ECShop后台SQL注入
	ECShop SQL注入漏洞
	ECShop后台安装目录变量覆盖漏洞
	ECShop SQL注入漏洞导致代码执行
	ECShop二次注入漏洞
	ECShop后台获取权限漏洞（GetShell）
	ECShop 2.7.3后台文件打包下载漏洞
FCKEditor	FCKEditor编辑器任意文件上传漏洞
Joomla	Joomla畸形反序列化数据包注入导致远程代码执行
	Joomla未授权创建用户漏洞（CVE-2016-8870）
	Joomla 3.7.0 Core SQL注入
	Joomla SQL注入漏洞
PHPCMS	PHPCMS注入漏洞
	PHPCMS AuthKey泄漏漏洞
	PHPCMS V9宽字节注入
	PHPCMS前台注入导致任意文件读取漏洞
	PHPCMS某处逻辑问题导致获取权限漏洞（GetShell）
	PHPCMS AuthKey生成算法问题导致AuthKey泄露
	PHPCMS V9.6.2 SQL注入漏洞
	PHPCMS 2008 common.inc 远程代码执行漏洞
	PHPCMS 2008 template缓存写入远程代码执行漏洞
	phpMyAdmin反序列化注入漏洞

组件类型	检测项
phpMyAdmin	phpMyAdmin CVE-2016-6617 SQL注入漏洞
	phpMyAdmin <=4.8.1 checkPageValidity函数缺陷可导致获取权限漏洞（GetShell）
	phpMyAdmin 4.8.5
phpwind	phpwind V9任务中心GET型CSRF代码执行漏洞
	phpwind V9 MD5 padding漏洞导致获取权限漏洞（GetShell）
	phpwind后台SQL注入
	phpwind UBB标签属性XSS注入
ThinkPHP5	ThinkPHP 5.0.10-3.2.3缓存函数设计缺陷可导致获取权限中危漏洞（GetShell）
	ThinkPHP5远程代码执行高危漏洞
	ThinkPHP 5.1.X <=5.1.30.远程代码执行漏洞
	ThinkPHP<5.0.24 Request.php远程代码执行高危漏洞
WordPress	WordPress任意文件上传漏洞
	WordPress IP验证不当漏洞
	WordPress WP_Image_Editor_Imagick指令注入漏洞
	WordPress bbPress插件XSS漏洞
	WordPress-Mailpress远程代码执行
	WordPress后台插件更新模块任意目录遍历导致DOS漏洞
	WordPress后台插件任意用户登录SQL注入漏洞
	WordPress <4.7.1用户名枚举漏洞（CVE-2017-5487）
	WordPress SQL注入
	WordPress跨站脚本漏洞（XSS）
	WordPress内容注入漏洞
	WordPress Mail Sitename字段处理不当导致多处远程代码执行漏洞
	WordPress插件Catalogue SQL注入漏洞
	WordPress任意文件删除漏洞
	WordPress Author权限路径穿越等多个缺陷可导致获取权限漏洞（GetShell）

相关文档

漏洞扫描周期说明

基线和漏洞有什么区别？

我有台服务器在资产中心无法开启漏洞检测怎么办？

1.6. 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。本文介绍了如何查看应用漏洞的相关信息和处理应用漏洞。

版本限制

仅云安全中心的企业版和旗舰版支持该功能，其他版本不支持。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

限制说明

- 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**登录到您自己的服务器并手动修复应用漏洞。
- 应用漏洞支持**Web扫描器**和**软件成分分析**两种检测方式。两种检测方式支持的服务器限制说明如下：
  - **Web扫描器**：仅支持检测在云安全中心防护范围内（即已安装云安全中心Agent）可以访问公网的服务器，支持阿里云和非阿里云服务器。
  - **软件成分分析**：支持检测云安全中心防护范围内的阿里云和非阿里云服务器。

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，选择**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漏洞紧急程度（高、中、低）、漏洞处理状态（已处理、未处理）、扫描方式（Web扫描器、软件成分分析）、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。
-

> 说明

- 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。

- 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

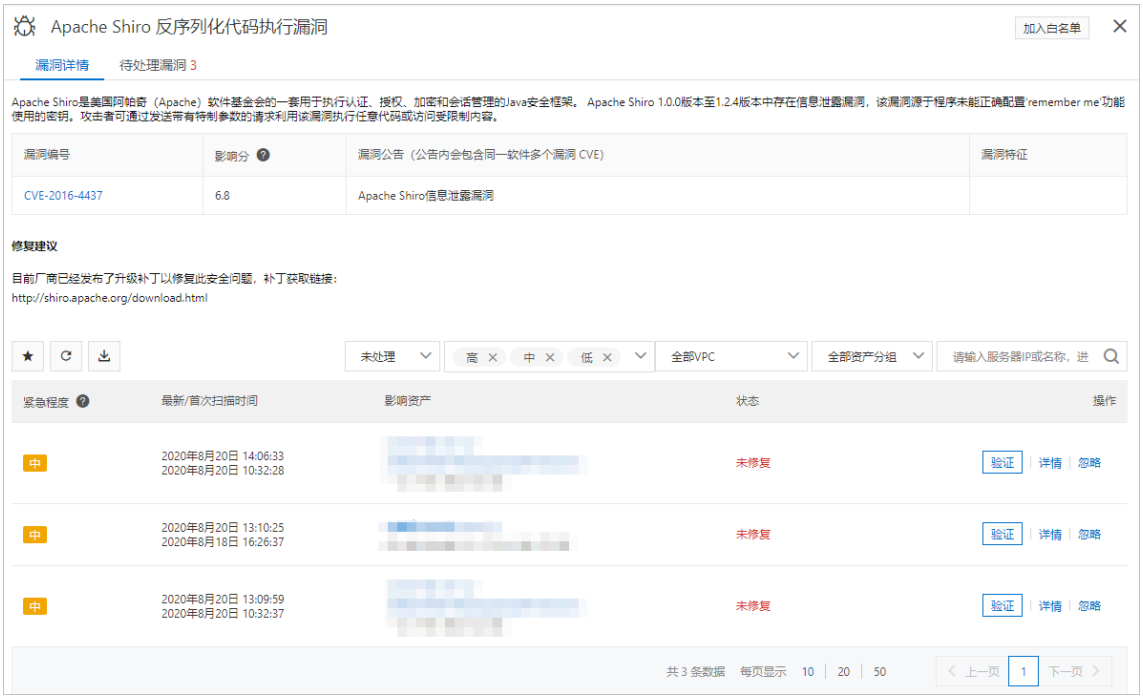
查看漏洞详情和处理漏洞

> 说明

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**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**面板。
5. 在**漏洞详情**面板，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。

- 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**
    -
    - 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

- **处理云防火墙可防护漏洞**
  云安全中心针对云防火墙可以防护的漏洞，提供**云防火墙虚拟补丁支持防护**标签，您可以单击该标签或该漏洞操作列的**防护**跳转至云防火墙控制台为该漏洞开启防护。具体操作，请参见漏洞防护。

支持检测的应用漏洞

应用漏洞类型	检测项
系统服务弱口令	OpenSSH服务
	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

应用漏洞类型	检测项
应用服务漏洞	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
	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

应用漏洞类型	检测项
	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

相关文档

漏洞扫描周期说明

基线和漏洞有什么区别？

我有台服务器在资产中心无法开启漏洞检测怎么办？

1.7. 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。本文介绍如何查看应急漏洞详情和处理应急漏洞。

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**。

版本限制

云安全中心所有版本用户都可使用该功能。各版本支持的功能详情，请参见功能特性。

支持的服务器类型

云安全中心仅支持检测阿里云ECS服务器上的应急漏洞，不支持检测非阿里云服务器和IDC服务器上的应急漏洞。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**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**
  应急漏洞支持以下检测方式：
  - **一键扫描所有漏洞**
    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。更多信息，请参见扫描漏洞。
  - **立即检测单个漏洞**
    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。执行立即检测后，可实时展示该应急漏洞的检测进度。
  - **周期性检测**（仅高级版、企业版和旗舰版支持）
    在**漏洞管理设置**面板，选择应急漏洞扫描周期。应急漏洞默认扫描时间段为*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。具体操作，请参见漏洞管理设置。

    > **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。

  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**。如果您从未执行过**一键扫描**或单击待检测应急漏洞右侧的**立即检测**，则您控制台上所有应急漏洞的**风险数**一栏会显示**未检测**。云安全中心会不定期发布互联网上爆发的高危应急漏洞，云安全中心对此类漏洞不会进行自动检测，建议您定期查看应急漏洞列表，设置周期性检测或手动执行此类漏洞的检测。

- **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。

- **导出漏洞**

  在**应急漏洞**页面，单击 图标，导出存在风险的应急漏洞列表。

  > **注意** 如果资产中未检测到存在风险的应急漏洞，您无法使用导出漏洞功能。

- **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。

状态	子状态	说明
已处理	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	即漏洞待修复。
	验证中	手动修复漏洞后，单击目标漏洞**操作**列的**验证**时，**未修复**状态会变成**验证中**，此操作用于验证漏洞是否修复成功。

- **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**

- **处理云防火墙可防护漏洞**
  云安全中心针对云防火墙可以防护的漏洞，提供**云防火墙虚拟补丁支持防护**标签，您可以单击该标签或该漏洞操作列的**防护**跳转至云防火墙控制台为该漏洞开启防护。具体操作，请参见漏洞防护。

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？

漏洞扫描周期说明

基线和漏洞有什么区别？

我有台服务器在资产中心无法开启漏洞检测怎么办？

1.8. 容器镜像漏洞

云安全中心支持容器镜像漏洞检测，可有效检测出高危系统漏洞、应用漏洞，为您提供安全可信的镜像。本文档介绍了如何查看容器镜像漏洞的相关信息。

背景信息

使用容器镜像漏洞功能前，您需要开通镜像安全扫描功能。
镜像安全扫描功能为云安全中心增值服务，需单独购买。仅支持高级版、企业版、旗舰版和仅采购增值服务用户购买镜像安全扫描功能。

执行容器镜像漏洞扫描

执行镜像安全扫描

查看容器镜像漏洞

查看镜像系统漏洞扫描结果

修复容器镜像漏洞

容器镜像漏洞不支持一键修复，您可以根据镜像系统漏洞扫描结果中提供的检测结果，手动在容器镜像中对漏洞进行修复。

> **说明** 建议您根据云安全中心提供的修复命令、影响说明或恶意文件路径等信息，及时处理容器中的相关漏洞。

容器镜像漏洞修复完成后，您需要在**镜像安全扫描**页面执行立即扫描，才能看到更新的漏洞状态，确认该漏洞是否已成功修复。

1.9. 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。

相关文档

漏洞扫描周期说明

基线和漏洞有什么区别？

我有台服务器在资产中心无法开启漏洞检测怎么办？

1.10. 排查漏洞修复失败的原因

本文档列举了在云安全中心控制台，使用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、Windows系统漏洞修复失败的可能原因

在您使用云安全中心修复Linux软件漏洞、Windows系统漏洞时，如果提示漏洞修复失败，请参考以下步骤进行排查和处理：

> **注意** 建议您针对以下表格中的说明，按照**从上到下**的顺序来排查漏洞修复失败的原因。

问题原因	具体说明	处理方案
网络连接不正常。	您服务器所在的网络连接如果不正常，漏洞将无法修复。	排查并首先处理网络问题。

问题原因	具体说明	处理方案
漏洞所在的服务器Agent已离线。	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。	建议您及时排查Agent离线的原因并进行相应处理。更多信息，请参见Agent离线排查。
漏洞所在的服务器磁盘空间已占满、或内存不足。	如果您服务器上的磁盘空间已满，云安全中心执行漏洞修复时，无法在您的服务器上下载相关补丁文件，从而导致漏洞修复失败。	处理步骤如下： 1. 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。 2. 确定目标服务器的存储空间够用后，重新在云安全中心控制台修复该漏洞。具体操作，请参见处理Linux漏洞、处理Windows漏洞。
对漏洞所在的服务器磁盘文件系统没有读写权限。	如果您没有磁盘文件系统的读写权限，会因为无法成功下载补丁安装包而导致漏洞修复失败。	处理步骤如下： 1. 更改磁盘文件系统的读写权限。 2. 确认权限修改成功后，在云安全中心控制台重新修复该漏洞。具体操作，请参见处理Linux漏洞、处理Windows漏洞。
（Linux漏洞）漏洞所在的服务器系统更新源配置存在问题。	由于系统更新源配置问题导致无法安装更新，或YUM软件列表未更新到最新版。	处理步骤如下： 1. 配置服务器系统更新源。您可以根据需要选择以下任一方式进行配置： ○ 在云安全中心控制台**漏洞管理设置**页面，**YUM/APT源配置**勾选**优先使用阿里云源进行漏洞修复**。 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源修复漏洞，帮助您有效提高漏洞修复的成功率。 参考以下内容将服务器系统的YUM/APT源配置到阿里云源： Ubuntu系统、CentOS系统、其他系统。 ○ 将YUM源列表升级到最新版。 2. 在云安全中心控制台重新修复该漏洞。具体操作，请参见处理Linux漏洞。
（Linux漏洞）RPM数据库损坏。	RPM数据库损坏可能会导致更新软件包安装失败，从而导致漏洞修复失败。	处理步骤如下： 1. 执行 `rm -f /var/lib/rpm/_db.*` 删除RPM锁文件。 2. 执行 `rpm -rebuilddb` 重建RPM数据库。 注意 该命令执行可能耗时较长。

问题原因	具体说明	处理方案
（Windows漏洞）该漏洞前置补丁缺失。	前置补丁缺失会导致漏洞修复失败。	处理步骤如下： 1. 及时安装前置补丁。 2. 安装成功后，重新在云安全中心控制台修复该漏洞。具体操作，请参见处理Windows漏洞。
（Windows漏洞）漏洞所在的服务器Windows Update或Windows Modules Installer服务已被禁用。	Windows Update或Windows Modules Installer服务被禁用时，您将无法下载漏洞补丁文件，从而导致系统无法更新。	处理步骤如下： 1. 启用Windows Update和Windows Modules Installer服务。 2. 在云安全中心控制台重新修复该漏洞。相关内容，请参见处理Windows漏洞。
（Windows漏洞）漏洞补丁包的下载和安装存在问题。	补丁安装包不存在、补丁安装包不匹配等问题会导致无法下载或安装漏洞补丁文件。	处理方法如下： • 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，您可以尝试重新下载补丁安装包后，再重新执行漏洞修复操作。 • 补丁安装包不匹配 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，您可以在云安全中心控制台**漏洞修复**页面忽略该漏洞。 • 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，建议您在当前补丁安装完成后再重新执行漏洞修复操作。
（Windows漏洞）服务器其他问题。	无	处理方法如下： • 重置Windows更新组件。具体操作，请参见Windows 更新-其他资源。 • 排查更新失败原因。具体操作，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：

> **说明** 建议您针对以下表格中的说明，按照**从上到下**的顺序来排查漏洞修复失败的原因。

问题原因	具体说明	处理方案
网络连接不正常。	您服务器所在的网络连接如果不正常，漏洞将无法修复。	排查并首先处理网络问题。
漏洞所在的服务器Agent已离线。	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。	建议您及时排查Agent离线的原因并进行相应处理。更多信息，请参见Agent离线排查。

问题原因	具体说明	处理方案
漏洞所在的服务器磁盘空间已占满、或内存不足。	如果您服务器上的磁盘空间已满，云安全中心执行漏洞修复时，无法在您的服务器上下载相关补丁文件，从而导致漏洞修复失败。	处理步骤如下： 1. 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。 2. 确定目标服务器的存储空间够用后，重新在云安全中心控制台修复该漏洞。具体操作，请参见处理Web-CMS漏洞。
漏洞所在的服务器安装了第三方安全软件。	如果您的服务器上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，可能会导致system账号对 `www` 目录及其子目录没有读写权限，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账号是否对 `www` 目录及其子目录有读写权限。如果没有，请手动为system账号添加读写权限。
漏洞文件已不存在。	如果漏洞文件已被删除，云安全中心会提示漏洞修复失败。	处理步骤如下： 1. 根据云安全中心控制台漏洞详情中提供的文件路径，在您的服务器中查看该文件是否已被删除。 2. 如果确认该漏洞文件已被删除，您可以忽略该漏洞告警。具体操作，请参见忽略漏洞。

相关文档

建议您及时修复系统漏洞。修复漏洞前，您需要了解相关准备工作和风险规避措施。更多信息，请参见服务器软件漏洞修复建议。

如果您对漏洞修复存在其他方面的疑问，请参考漏洞修复问题。

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。

什么是基线

基线指操作系统、数据库及中间件的安全实践及合规检查的配置红线，包括弱口令、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检查。云安全中心的安全基线支持弱口令、未授权访问、历史漏洞和配置红线的立体巡检，合规基线支持等保合规和CIS标准。安全基线与合规基线均已覆盖常用的30多个系统版本和10多个数据库及中间件，可以满足企业多种合规需求。

应用场景

功能介绍

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、企业版和旗舰版用户可开通和使用该服务。免费版、防病毒版用户都需先升级到高级版、企业版或旗舰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	免费版	防病毒版	高级版	企业版	旗舰版
弱口令			✓		
未授权访问					

基线检查项类型	免费版	防病毒版	高级版	企业版	旗舰版
最佳安全实践	×	×	×	✓	✓
容器安全					
等保合规					
自定义基线					

> **说明**
>
> - 高级版用户仅支持使用默认策略执行基线检查，不支持创建标准策略和自定义策略。关于基线检查策略的介绍，请参见基线检查策略。
> - 企业版、旗舰版用户可以使用基线检查的所有功能，支持添加标准策略、自定义策略以及对基线策略进行编辑、删除（默认策略不能删除）。另外，企业版、旗舰版中Linux系统的阿里云标准和等保标准基线相关检查项还支持自动修复。

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。 **说明** 弱口令检测是通过读取HASH值与弱口令字典计算的HASH值进行对比来检查是否存在弱口令。如果您不想读取HASH值，您可以从基线检查策略中移除弱口令基线。	• 操作系统 Linux、Windows • 数据库 MySQL、Redis、SQL Server、MongoDB、PostgreSQL、Oracle • 应用 Tomcat、FTP、Rsync、SVN、Activemq、RabbitMQ、OpenVpn、Jboss6/7、Jenkins、Openldap、VncServer、pptpd	需紧急修复。避免弱口令暴露在公网上导致系统被入侵或发生数据泄露事件。
未授权访问	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。	Memcached、Elasticsearch、Docker、CouchDB、Zookeeper、Jenkins、Hadoop、Tomcat、Redis、Jboss、ActiveMQ、RabbitMQ、openLDAP、rsync、Mongodb Postgresql	

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

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、8
		  ◦ Ubuntu 14、16、18、20
		  ◦ Debian 8、9、10
		  ◦ Aliyun Linux 2、3
		  ◦ Windows 2008R2、2012R2、2016、2019
		  ◦ Rocky Linux 8
		  ◦ Alma Linux 8
		  ◦ SUSE Linux 15
		  ◦ Anolis 8
		  ◦ 麒麟
		  ◦ UOS
		• 数据库
		MySQL、Redis、MongoDB、SQL server、Oracle 11g、CouchDB、Influxdb、 PostgreSql
		• 应用
		Tomcat、IIS、Nginx、Apache、Windows SMB、RabbitMQ、Activemq、ElasticSearch、Jenkins Hadoop、Jboss6/7、Tomcat
			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。

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	

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

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。
		• 操作系统
		  ◦ CentOS 6、7、8
		  ◦ Redhat 6、7、8
		  ◦ Ubuntu 14、16、18、20
		  ◦ SUSE 10、11、12、15
		  ◦ Debian 8、9、10
		  ◦ Aliyun Linux 2、3
		  ◦ Windows 2008R2、2012R2、2016、2019
		  ◦ Anolis 8
		  ◦ 麒麟
		  ◦ UOS
		• 数据库
		Redis、MongoDB、PostgreSql、Oracle、MySql、SQL Server、Informix
		• 应用
		Websphere Application Server、Jboss6/7、Nginx、Weblogic、Bind、IIS
			基于业务是否有合规需要进行修复。

CIS合规	基于CIS标准的操作系统安全基线检查。	• CentOS 6、7、8 • Ubuntu 14、16、18、20 • Debian 8、9、10 • Aliyun Linux 2 • Windows 2008R2、2012R2、2016、2019	基于业务是否有合规需要进行修复。
自定义基线	支持CentOS Linux 7自定义基线，可对基线检查策略中的检查项进行编辑，自定义安全加固项。	CentOS 7、CentOS6、Windows 2008R2、2012R2、2016、2019	用户自定义的安全加固项，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。

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，可以获取服务器在基线配置和应用上存在的风险和缺陷，同时云安全中心还会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	包含的检查项的数量
	Zabbix登录弱口令检查	Zabbix登录弱口令检测基线。	1

基线分类	基线名称	基线描述	包含的检查项的数量
弱口令	Samba登录弱口令检测	检查Samba数据库用户是否存在弱口令风险。	1
	ElasticSearch服务登录弱口令检查	ElasticSearch服务器登录弱口令检测基线。	1
	Activemq登录弱口令检查	Activemq登录弱口令检查。	1
	RabbitMQ登录弱口令检查	RabbitMQ登录弱口令检测基线。	1
	Linux系统OpenVpn弱口令检测	检测Linux系统OpenVPN账号常见弱口令。	1
	Jboss6/7登录弱口令检查	Jboss6/7登录弱口令检测基线。	1
	Jenkins登录弱口令检查	新版Jenkins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
	Proftpd登录弱口令检查	新版Proftpd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
	Influxdb数据库登录弱口令检查	新版Influxdb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
	Weblogic 12c登录弱口令检测	检查Weblogic 12c用户是否存在弱口令风险。	1
	Openldap登录弱口令检查	Openldap登录账号弱口令检测基线。	1
	VncServer弱口令检查	检测Vnc服务端登录账号常见弱口令。	1
	pptpd服务登录弱口令检查	pptp服务器登录弱口令检测基线。	1
	Oracle登录弱口令检测	检查Oracle数据库用户是否存在弱口令风险。	1
	SVN服务登录弱口令检查	SVN服务器登录弱口令检测基线	1
	Rsync服务登录弱口令检查	Rsync服务器登录弱口令检测基线	1
	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
	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
	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
	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
	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

基线分类	基线名称	基线描述	包含的检查项的数量
	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
	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
	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
	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
	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
	MongoDB登录弱口令检测（支持2.X版本）	检查MongoDB服务是否存在弱口令用户。	1
未授权访问	Influxdb未授权访问高危风险	Influxdb未授权访问高危风险基线。	1
	Redis未授权访问高危风险	Redis未授权访问高危风险基线。	1
	Jboss未授权访问高危风险	Jboss未授权访问高危风险基线。	1
	ActiveMQ未授权访问高危风险	ActiveMQ未授权访问高危风险基线。	1
	RabbitMQ未授权访问高危风险	RabbitMQ未授权访问高危风险基线。	1
	openLDAP未授权访问高危风险（Linux环境）	openLDAP未授权访问漏洞基线。	1
	Kubernetes-Apiserver未授权访问高危风险	Kubernetes-apiserver未授权访问高危风险基线。	1
	LDAP未授权访问高危风险（Windows环境）	LDAP未授权访问高危风险基线。	1
	Rsync未授权访问高危风险	Rsync未授权访问漏洞基线。	1
	Mongodb未授权访问高危风险	Mongodb未授权访问高危风险基线。	1
	PostgreSQL未授权访问高危风险基线	PostgreSQL未授权访问高危风险基线。	1
	Jenkins未授权访问高危风险	Jenkins未授权访问高危风险基线。	1
	Hadoop未授权访问高危风险	Hadoop未授权访问高危风险基线。	1

基线分类	基线名称	基线描述	包含的检查项的数量
	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
	ZooKeeper未授权访问高危风险	ZooKeeper未授权访问高危风险基线。	1
	Docker未授权访问高危风险	Docker未授权访问高危风险基线。	1
	Memcached未授权访问高危风险	Memcached未授权访问高危风险基线。	1
	Elasticsearch未授权访问高危风险	Elasticsearch未授权访问高危风险基线。	1
容器安全	CIS标准-Kubernetes (ACK) Node节点安全基线检查	CIS基线标准，适用于有专业安全水准的企业用户，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针对性的对系统进行安全加固。	52
	CIS标准-Kubernetes (ACK) Master节点安全基线检查	CIS基线标准，适用于有专业安全水准的企业用户，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针对性的对系统进行安全加固。	8
	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
	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。	18
	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。	17
	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。	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-Debian Linux 8/9/10安全基线检查	基于阿里云最佳安全实践的Debian Linux 8基线检查标准。	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 7/8安全基线检查	基于阿里云最佳安全实践的Redhat Linux 7/8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基线检查。	15

基线分类	基线名称	基线描述	包含的检查项的数量
最佳安全实践	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 安全基线检查	基于阿里云最佳安全实践的Windows 2016、Windows Server2019基线检查。	12
	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。	17
	阿里云标准-Memcached安全基线检查	基于阿里云最佳安全实践的Memcache基线标准。	5
	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。	9
	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：MySQL5.1~MySQL5.7。	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-PostgreSQL安全基线检查	基于阿里云最佳安全实践的PostgreSQL基线标准。	11
	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。	7
	阿里云标准-Anolis 8安全基线检查	基于阿里云最佳安全实践的Anolis 8基线标准。	15
	阿里云标准-Apache安全基线检查	参考CIS及阿里云基线标准进行中间件层面基线检测。	19
	平安普惠风险监控	平安普惠风险监控。	5
	平安普惠标准-CentOS Linux 7安全基线检查	基于平安标准定制的最佳安全实践CentOS Linux 7基线标准。	31
	阿里云标准-CouchDB安全基线检查	阿里云标准-CouchDB安全基线检查。	5
	阿里云标准-ElasticSearch安全基线检查	基于阿里云最佳安全实践的ElasticSearch基线标准。	3
	阿里云标准-Hadoop安全基线检查	基于阿里云最佳安全实践的Hadoop安全基线检查。	3
	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

基线分类	基线名称	基线描述	包含的检查项的数量
	阿里云标准-Influxdb安全基线检查	基于阿里云最佳安全实践的Influxdb基线标准。	5
	阿里云标准-Jboss6/7安全基线检查	基于阿里云最佳安全实践的Jboss6/7安全基线检查。	11
	阿里云标准-Kibana安全基线检查	基于阿里云最佳安全实践的Kibana基线标准。	4
	阿里云标准-麒麟安全基线检查	阿里云标准-麒麟安全基线检查。	15
	阿里云标准-Activemq安全基线检查	基于阿里云最佳安全实践的Activemq安全基线检查。	7
	阿里云标准-Jenkins安全基线检查	基于阿里云最佳安全实践的Jenkins基线标准。	6
	阿里云标准-RabbitMQ安全基线检查	基于阿里云最佳安全实践的RabbitMQ安全基线检查。	4
	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。	13
	阿里云标准-Windows SMB安全基线检查	基于阿里云最佳安全实践的Windows SMB基线标准。	2
	阿里云标准-SUSE Linux 15安全基线检查	基于阿里云最佳安全实践的SUSE Linux 15基线标准。	15
	阿里云标准-Apache Tomcat安全基线检查（Windows环境）	参考CIS及阿里云基线标准进行中间件层面基线检测。	8
	阿里云标准-Uos安全基线检查	基于阿里云最佳安全实践的uos基线标准。	15
	阿里云标准-Zabbix安全基线检查	基于阿里云最佳安全实践的Zabbix安全基线检查。	6
	阿里云标准-Apache Tomcat 安全基线检查	参考CIS及阿里云基线标准进行中间件层面基线检测。	13
	CIS标准-Alibaba Cloud Linux/Aliyun Linux 2安全基线检查	CIS基线标准，适用于有专业安全水准的企业用户，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针对性的对系统进行安全加固。	178
	CIS标准-CentOS Linux 6安全基线检查	CIS基线标准，适用于有专业安全水准的企业用户，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针对性的对系统进行安全加固。	196

基线分类	基线名称	基线描述	包含的检查项的数量
CIS合规	CIS标准-CentOS Linux 7安全基线检查	CIS基线标准，适用于有专业安全水准的企业用户，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针对性的对系统进行安全加固。	197
	CIS标准-CentOS Linux 8安全基线检查	CIS基线标准，适用于有专业安全水准的企业用户，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针对性的对系统进行安全加固。	164
	CIS标准-Debian Linux 8安全基线检查	CIS基线标准，适用于有专业安全水准的企业用户，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针对性的对系统进行安全加固。	155
	CIS标准-Ubuntu 14安全基线检查	CIS基线标准，适用于有专业安全水准的企业用户，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针对性的对系统进行安全加固。	177
	CIS标准-Ubuntu 16/18/20安全基线检查	CIS基线标准，适用于有专业安全水准的企业用户，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针对性的对系统进行安全加固。	176
	CIS标准-Windows Server 2008 R2安全基线检查	CIS基线标准，适用于有专业安全水准的企业用户，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针对性的对系统进行安全加固。	274
	CIS标准-Windows Server 2012 R2安全基线检查	CIS基线标准，适用于有专业安全水准的企业用户，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针对性的对系统进行安全加固。	275
	CIS标准-Windows Server 2016/2019 R2安全基线检查	CIS基线标准，适用于有专业安全水准的企业用户，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针对性的对系统进行安全加固。	275
	等保三级-SUSE 15合规基线检查	SUSE 15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。	18
	等保三级-Alibaba Cloud Linux 3合规基线检查	Alibaba Cloud Linux 3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-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-Bind合规基线检查	Bind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。	4
	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

基线分类	基线名称	基线描述	包含的检查项的数量
	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。	19
	等保三级-IIS合规基线检查	Oracle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。	5
	等保三级-Informix合规基线检查	Informix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。	6
	等保三级-Jboss6/7合规基线检查	Jboss6/7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。	5
	等保三级-MongoDB合规基线检查	MongoDB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。	6
	等保三级-SQL Server合规基线检查	SQL Server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。	4
	等保三级-MySQL合规基线检查	MySQL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。	5
	等保三级-Nginx合规基线检查	Nginx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。	3
	等保三级-Oracle合规基线检查	Oracle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。	12
	等保三级-PostgreSQL合规基线检查	PostgreSQL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。	4
	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-Redis合规基线检查	Redis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。	4
	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
	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-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

等保合规基线分类	基线名称	基线描述	包含的检查项的数量
	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 16/18/20合规基线检查	Ubuntu16/18/20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-Websphere Application Server合规基线检查	Websphere Application Server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。	7
	等保三级-Weblogic合规基线检查	Weblogic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。	5
	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 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
	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。	12
	等保二级-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。	19
	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

基线分类	基线名称	基线描述	包含的检查项的数量
	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 合规基线检查	Windows 2016 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
	等保三级-Debian Linux 8/9/10合规基线检查	Debian Linux 8/9/10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
	等保三级-麒麟合规基线检查	麒麟等保合规基线检查，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-Uos合规基线检查	Uos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-Anolis 8合规基线检查	Anolis 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
自定义基线	阿里云标准-Ubuntu自定义安全基线检查	基于阿里云最佳安全实践的Ubuntu 14/16/18/20自定义基线标准。	62
	Windows自定义基线	全量Windows自定义基线模版，可通过模版选择检查项及配置检查项参数，满足自定义基线需要。	63
	CentOS Linux 6自定义基线	全量CentOS Linux 6自定义基线模版，可通过模版选择检查项及配置检查项参数，满足自定义基线需要。	47
	CentOS Linux 7/8自定义基线	全量CentOS Linux 7自定义基线模版，可通过模版选择检查项及配置检查项参数，满足自定义基线需要。	53

2.3. 设置基线检查策略

云安全中心支持配置基线检查策略，通过执行基线检查策略来检查您资产的基线配置是否存在风险。本文介绍了如何配置基线检查策略。

前提条件

您已购买云安全中心高级版、企业版或旗舰版，仅高级版、企业版和旗舰版支持基线检查功能。

> **说明** 免费版和防病毒版用户都需先升级到高级版、企业版或旗舰版才可使用基线检查功能。

背景信息

开通 检查服务后，云安全中心将使用**默认策略**对您阿里云账号下的所有资产每隔一天检查一次，每次在00:00~06:00进行检查。您可以单击**默认策略**右侧的**编辑**，进入**基线检查策略**面板，在**基线名称**列表中查看**默认策略**中包含的基线。弱口令

如果**默认策略**不能满足您的业务场景对基线检查的需求，您也可以通过**添加标准策略**和**添加自定义策略**，补充**默认策略**无法检查的基线项目。

> **说明** 仅企业版、旗舰版支持**添加标准策略**和**添加自定义策略**，高级版不支持。高级版仅可使用**默认策略**执行基线检查。

下表为您介绍默认策略、标准策略、自定义策略支持的基线检查类型、包含的基线数量以及它们支持的版本和使用场景。

策略类型	支持的版本	支持的基线类型	包含的基线数量	是否支持编辑	使用场景
默认策略	高级版、企业版、旗舰版	• 未授权访问 • 容器安全 • 最佳安全实践 • 弱口令 **说明** 高级版仅支持弱口令检查。	70以上	不支持	默认策略为云安全中心默认执行的基线检查策略，用于检查您的资产在未授权访问、容器安全、最佳安全实践以及弱口令这四类基线配置上是否存在风险。
标准策略	企业版、旗舰版	• 未授权访问 • 容器安全 • 等保合规 • 最佳安全实践 • 弱口令	120以上	支持编辑策略配置项	标准策略相比默认策略增加了等保合规基线检查类型，其他基线类型也增加了更多的基线，且支持编辑策略的配置项。您可为资产自行配置符合业务场景需要的基线检查策略。具体操作，请参见添加标准策略。
自定义策略	企业版、旗舰版	操作系统自定义基线	50以上	支持编辑策略配置项，且支持编辑部分基线的参数	自定义策略用于检查您的资产在操作系统自定义基线的配置上否存在风险。您可为资产自行配置基线检查策略，并可按照业务需求修改基线的参数，使得基线检查策略更加符合您的业务场景。具体操作，请参见添加自定义策略。

云安全中心基于阿里云威胁情报，为您提供了默认的内置 检查规则。您也可以基于业务需要，自定义基线弱口令规则。具体操作，请参见自定义弱口令规则。

添加标准策略

标准策略相比默认策略增加了等保合规基线检查类型，标准策略中的其他基线类型也增加了更多的基线检测项，并且标准策略支持编辑策略的配置项。您可通过添加标准策略，进一步完善对您资产基线配置的检查。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**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，单击**添加标准策略**。
5. 在**基线检查策略**面板上，进行如下配置。

参数	说明
策略名称	输入用于识别该策略的名称。
检查周期	选择检查周期。
检查开始时间	选择检查开始时间。
基线名称	选择需要检查的基线。基线详情，请参见基线检查内容。
生效资产	选择需要应用该策略的资产分组。 **说明** 新购买的资产默认归属在**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，请参见管理服务器的分组、重要性及标签。

6. 单击下方**确认**，完成基线检查策略的添加。

   云安全中心将按照创建的策略对您资产的基线配置进行检查。

自定义弱口令规则

您可在云安全中心默认提供的弱口令规则的基础上，根据您的业务场景，自定义更符合您需求的弱口令规则，进一步完善对弱口令的检查。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**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，配置弱口令规则。

   支持通过弱口令模板上传弱口令规则和自定义弱口令字典两种方式自定义弱口令规则。

   - 通过弱口令模板上传弱口令规则
     a. 单击**下载模板**。
     b. 在下载的模板中完成自定义弱口令设置。
     c. 单击**导入文件**，上传弱口令模板，完成弱口令配置。
     云安全中心将按照您上传的弱口令规则来检查您资产的口令是否存在风险。

     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，否则将无法准确检查弱口令。
     - 文件中仅支持2,000条弱口令。

   - 自定义弱口令字典
     a. 单击**自定义弱口令字典**。

b. 在**自定义弱口令字典**面板上进行如下配置。

配置项	说明
域名	填写您的资产的域名。
公司名称	填写您公司的名称。
关键字	填写您要加入到弱口令字典当中的口令。
弱口令字典	无需配置。此为云安全中心基于阿里云威胁情报，默认内置弱口令规则字典。

c. 单击下方**生成字典并导入**，完成弱口令字典配置。
云安全中心将按照您自定义的弱口令字典来检查您资产的口令是否存在风险。

添加自定义策略

您可通过添加自定义策略，检查您的资产在操作系统自定义基线的配置上否存在风险。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**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**面板上，单击**添加自定义策略**。
5. 在**基线检查策略**面板上，配置自定义策略。

参数	说明
策略名称	输入用于识别该策略的名称。
检查周期	选择检查周期。
检查开始时间	选择检查开始时间。
基线名称	选择需要检查的基线。基线详情，请参见基线检查内容。 **说明** 部分自定义基线的参数支持自定义配置，您可根据业务需要进行配置。
生效资产	选择需要应用该策略的资产分组。 **说明** - 一个资产分组仅可设置一个自定义策略。已存在自定义策略的资产分组，在新建自定义策略选择生效资产的资产分组时为置灰状态不支持选择。 - 新购买的资产默认归属在**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，请参见管理服务器的分组、重要性及标签。

6. 单击下方**确认**，完成自定义策略的添加。

云安全中心将按照创建的策略对您资产的基线配置进行检查。

管理策略

策略创建后，您可以根据业务场景需要设置**基线检查等级**，**编辑**或者**删除**某个策略。

- 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**）。
- 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，基线也不支持更改，仅支持修改应用默认策略的生效资产。

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资产是否存在安全风险。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、企业版或旗舰版，仅高级版、企业版和旗舰版支持基线检查功能。

> **说明** 免费版和防病毒版用户都需先升级到高级版、企业版或旗舰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

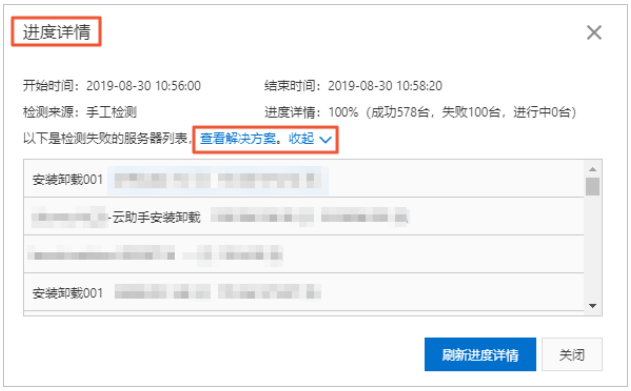
1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全防范 > 基线检查**。
3. 在**基线检查策略**列表中，选择需要执行即时手动检查的基线策略。

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

基线检查任务完成后，您可以在基线检查页面查看和处理资产中存在基线风险问题。本文介绍如何查看基线检查结果，以及处理资产中存在的基线风险问题。

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**默认策略**对所有资产进行基线检查。您也可按照业务场景需要自定义基线检查策略，检查您的资产是否存在相应的基线风险。自定义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、旗舰版支持**添加标准策略**和**添加自定义策略**，高级版不支持。高级版仅可使用**默认策略**执行基线检查。

前提条件

已完成基线检查。具体操作，请参见执行基线检查。

查看基线检查结果

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全防范 > 基线检查**。
3. 在**基线检查**页面，查看基线检查结果。

   基线检查结果页面分为总览区域和基线检查结果列表两个区域。

   - 总览区域

     在总览区域，您可以单击**基线检查策略**菜单，在菜单中查看所有的基线检查策略。选中某个策略后，在右侧可以查看该基线检查策略的**检查服务器数**、**检查项**、**高危弱口令风险**、**最新检查通过率**，单击**进度详情**可查看该基线检查策略执行的进度详情信息。

     以下是总览区域相关功能的介绍。

功能	说明
基线检查策略	在基线检查策略菜单中，可以查看已有的基线检查策略。
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	您在配置基线检查策略时，选中的**基线名称**的数量。

功能	说明
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。 注意 **高危弱口令风险**为风险等级较高的基线风险问题，建议您优先处理。
最新检查通过率	最近一次执行基线检查的基线合格率。以下是**最新检查通过率**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。

- 基线检查结果列表区域
  在基线检查结果列表区域，您可以查看详细的基线检查结果。
  a. 在基线检查结果列表中，单击基线名称，展开该基线的详情面板。
  在基线详情面板上，查看受该基线影响的资产及资产基线检查的**通过项**、**风险项**等信息。
  b. 在基线详情面板上，单击某个受影响的资产的**操作**列的**查看**，展开**风险项**面板。
  在**风险项**面板上，可查看该资产上存在的所有基线风险问题。
  c. 在**风险项**面板上，单击某个资产**操作**列的**详情**，可查看云安全中心提供的关于该风险项的**描述**、**检查提示**和**加固建议**等信息。
  d. （可选）在基线检查结果列表右上方，单击 图标，在**基线导出任务选项**对话框中选择导出方式，可以导出基线检查结果。
  针对基线中包含的弱口令信息的导出，云安全中心提供了以下导出方式：
  ■ **弱口令明文导出**：即对于基线检查结果中的弱口令信息直接明文导出。
  ■ **弱口令脱敏导出**：即对于基线检查结果中的弱口令信息脱敏后再导出。

处理基线检查结果

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全防范 > 基线检查**。
3. 在基线检查结果列表中，单击待处理的基线检查结果的基线名称。
4. 在右侧面板上，单击服务器**操作**列的**查看**。
5. 在**风险项**面板上，处理该服务器上存在的基线风险问题。
   - **修复**
     云安全中心仅支持修复Linux系统的阿里云标准和等保标准基线相关检查项。如果检查项为Linux系统的阿里云标准和等保标准基线相关检查项，您可以在云安全中心直接修复基线风险问题；如果检查项不是Linux系统的阿里云标准和等保标准基线相关检查项，则需要您登录存在该基线风险问题的服务器，在服务器上修改基线问题对应的服务器的配置，修改完成后，在云安全中心进行**验证**。

- 在云安全中心直接修复基线风险问题
  a. 在**风险项**面板上，单击目标检查项**操作**列的**修复**。
  b. 在**修复风险资产**对话框，进行如下配置。
  配置项说明如下：

配置项	说明
修复方式	配置基线风险问题的修复方式。 **说明** 不同类型的风险项对应的修复方式不同，请根据实际场景配置修复方式。
批量处理	选择是否要批量处理存在相同基线风险问题的其他资产。
风险保障	选择是否通过创建快照的方式，备份系统数据。 **注意** 云安全中心在修复基线风险问题时，可能存在修复失败的风险，影响到您业务正常运行。建议您在修复前对系统进行备份，以便在修复失败影响您业务正常运行时，可快速恢复到执行修复操作前的状态，使业务能正常运转。 ■ 自动创建快照并修复：您需要设置**快照名称**、**快照保存时间**，然后单击**立即修复**。 **说明** 创建快照将产生费用。您可以单击页面上的**查看计费说明**，了解具体的快照计费信息。 ■ 不建立快照备份直接修复：如果您确定不创建快照直接修复基线问题，单击**立即修复**即可。

  c. 单击**立即修复**。
- 登录对应服务器修复基线风险问题
  在风险项面板上，单击目标检查项**操作**列的**详情**，可查看云安全中心提供的关于该检查项的**描述**、**检查提示**和**加固建议**等信息。请根据云安全中心提供的**加固建议**，登录存在该基线问题的服务器，在服务器上修改基线风险问题对应的服务器的配置。

- **加白名单**
  如果您确认检查项的**状态**为**未通过**的基线风险项为正常业务结果，可通过**加白名单**功能对该检查项产生的告警进行忽略。加入白名单后，后续基线检查时会忽略该检查项。更多信息，请参见加入白名单。

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

6. 验证基线风险问题修复结果。

   在**风险项**面板上，单击目标检查项**操作**列的**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**。

   说明 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。

相关操作

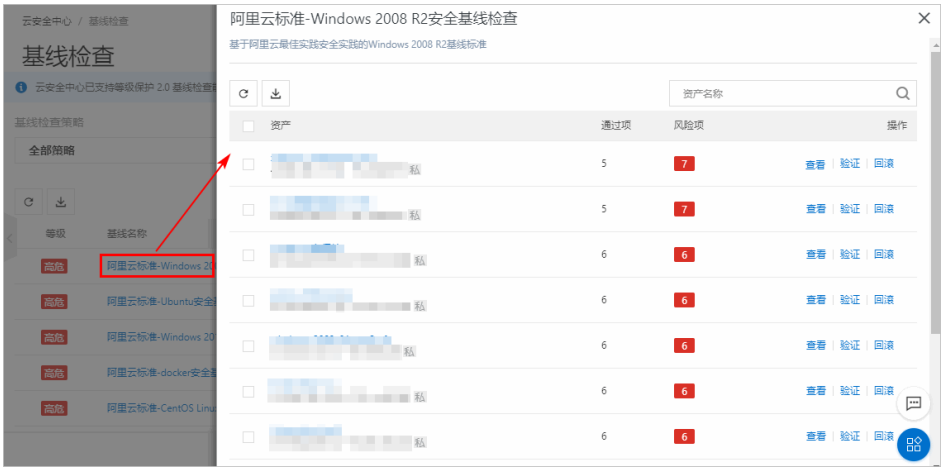
- **回滚**
  如果您在修复阿里云ECS服务器上存在的基线风险问题前，对该服务器使用快照进行了备份，在服务器上的基线风险问题修复失败导致业务中断时，您可在基线详情面板上，单击该服务器**操作**列的**回滚**，在**快照**对话框中，选中基线修复前备份的快照，单击下方**确定**。执行**回滚**操作后，该服务器的配置可恢复到基线风险问题修复前创建的快照的配置。
- **取消加白**
  如果需要云安全中心对已忽略的基线检查配置项再次触发告警，可对已忽略的检查项执行**取消加白**。取消加白后，该基线检查配置项会再次触发告警。
  在**风险项**面板上，定位到需取消白名单的检查项，单击其**操作**列**取消加白**，在**取消忽略操作**对话框中，单击**确定**，可将该检查项移出白名单。您也可以选中多个需要取消白名单的检查项，单击下方**取消加白**，将多个检查项批量移除白名单。

2.6. 加入白名单

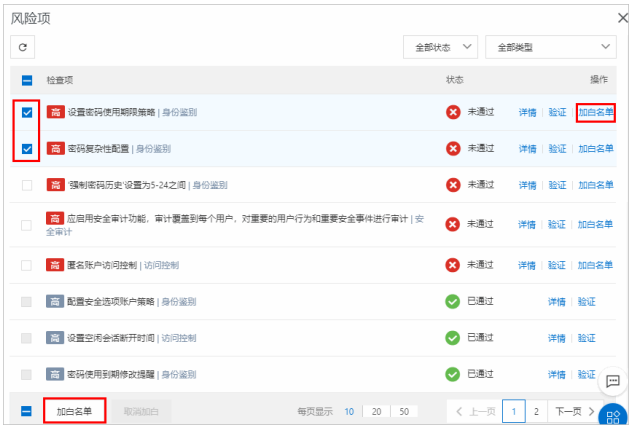
基线检查支持设置白名单。将基线检查风险项加入到白名单后，云安全中心不再对该风险项进行告警。如果您确认检测状态为未通过的基线风险项为正常业务结果，可通过加入白名单功能对该检查项产生的告警进行忽略。本文介绍了如何将需要忽略告警的检查项加入白名单中。

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。



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**面板上，单击目标检查项**操作**列的**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**。

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。

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**。

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。

- 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**，在**取消忽略操作**对话框中单击**确定**，可将该检查项移出白名单。

3.云平台配置检查

3.1. 云平台配置检查概述

云安全中心提供的云平台配置检查功能，可帮助您检查您云产品的安全配置是否存在安全隐患。本文介绍了云平台配置检查功能的版本限制信息和支持的检查项。

版本限制说明

云安全中心高级版、企业版和旗舰版的云平台配置检查功能支持检测所有检查项。免费版和防病毒版用户需要升级至高级版、企业版或旗舰版，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。

云平台配置检查项列表

下表罗列了云安全中心各版本对云平台配置的检查项的支持情况。

> **说明** 下表中使用的标识说明如下：
> - ×：表示不包含在服务范围中。
> - √：表示包含在服务范围中。
>
> 下表中的风险等级为阿里云云安全中心定义的风险等级。

最佳安全实践的类型	检查项名称	检查项所在章节	风险等级	说明	免费版、防病毒版	高级版、企业版、旗舰版
阿里云RAM最佳安全实践	RAM-云产品管理员授权	权限管理	中危	云产品权限授权应精细到具体操作，Action和Resourc不应该都为*。为RAM用户、用户组、角色授权时，应遵循最小授权原则，不要过度授权。	×	√
	RAM-超级管理员授权	权限管理	高危	检查超级管理员是否被授权引用，AdministratorAccess策略有管理所有云资源的权限，属于超级管理员，不应该被授权引用。为RAM用户、用户组、角色授权时，应遵循最小授权原则，不要过度授权。	×	√
	RAM-子账号双因素认证	RAM安全设置	高危	检查开启了控制台登录的RAM用户是否启用多因素认证（Multi-Factor Authentication，简称：MFA）。 **注意** 开启控制台登录的RAM用户，需要启用MFA，且在控制台登录管理启用必须开启多因素认证。	√	√

最佳安全实践的类型	检查项名称	检查项所在章节	风险等级	说明	免费版、防病毒版	高级版、企业版、旗舰版
	主账号安全-AK使用	主账号安全	高危	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 该检测项存在天延时，禁用AK之后再次验证，不会立刻通过，而是第二天后台数据更新之后才会通过，这点与其他检测项不同。	×	✓
	主账号安全-双因素认证	主账号安全	高危	检查用户登录阿里云控制台的主账号，是否启用了双因素认证（Multi-Factor Authentication，简称：MFA）。	✓	✓
阿里云OSS最佳安全实践	OSS-Bucket版本控制	容灾备份	中危	版本控制是针对存储空间（Bucket）级别的数据保护功能。开启版本控制后，针对数据的覆盖和删除操作将会以历史版本的形式保存下来。您在错误覆盖或者删除对象（Object）后，能够将Bucket中存储的Object恢复至任意时刻的历史版本。	×	✓
	OSS-授权策略	访问控制	高危	OSS有三种权限控制方式：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。	×	✓
	OSS-Bucket防盗链配置	访问控制	低危	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。	×	✓
	OSS-Bucket服务端加密	数据安全	低危	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。	×	✓
	OSS-跨区域复制配置	容灾备份	低危	跨区域复制（Bucket Cross-Region Replication）是跨不同OSS数据中心（地域）的Bucket自动、异步复制Object，它会将Object的创建、更新和删除等操作从源存储空间复制到不同区域的目标存储空间。该功能能够很好的提供Bucket跨区域容灾或满足用户数据复制的需求。目标Bucket中的对象是源Bucket中对象的精确副本，它们具有相同的对象名、元数据以及内容，例如创建时间、拥有者、用户定义的元数据、Object ACL、对象内容等。	✓	✓

最佳安全实践的类型	检查项名称	检查项所在章节	风险等级	说明	免费版、防病毒版	高级版、企业版、旗舰版
	OSS-日志记录配置	日志审计	中危	用户在访问OSS的过程中，会产生大量的访问日志。日志存储功能，可将OSS的访问日志，以小时为单位，按照固定的命名规则，生成一个Object写入您指定的Bucket（目标Bucket，Target Bucket）。您可以使用阿里云DataLakeAnalytics或搭建Spark集群等方式对这些日志文件进行分析。同时，您可以配置目标Bucket的生命周期管理规则，将这些日志文件转成归档存储，长期归档保存。	✓	✓
	OSS-Bucket权限设置	访问控制	高危	检查OSS所有Bucket是否允许公共读写或公共读，如果是则不合规。	✓	✓
阿里云SLB最佳安全实践	SLB-证书过期	监控告警	中危	检查SLB的可用证书是否过期，影响业务正常使用。	✓	✓
	SLB-白名单配置检查	访问控制	高危	检查SLB负载均衡实例访问控制配置，建议非HTTP或HTTPS服务启用访问控制，并且不能开放0.0.0.0/0。	✓	✓
	SLB-健康状态	监控告警	低危	检测负载均衡SLB服务的后端服务器（ECS实例）业务可用性。	✓	✓
	SLB-高危端口暴露	访问控制	高危	应依据最小服务原则设定SLB转发策略，只转发必要的公共服务端口（如：80、443等）至公网，其他端口不应进行转发，如被SLB发布到公网会增加系统遭受外部黑客攻击的风险。	✓	✓
阿里云PostgreSQL最佳安全实践	分析型数据库PostgreSQL版-白名单配置	访问控制	高危	检查分析型数据库PostgreSQL版的访问控制策略是否有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。	✓	✓
阿里云Redis最佳安全实践	Redis-SSL开启	数据安全	中危	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。	×	✓
	Redis-备份设置	容灾备份	中危	建议Redis数据库实例开启数据备份功能，数据备份应当每天备份一次。	×	✓

践 最佳安全实践的类型	检查项名称	检查项所在章节	风险等级	说明	免费版、防病毒版	高级版、企业版、旗舰版
	Redis-白名单配置	访问控制	高危	0.0.0.0/0和空代表不设IP访问的限制，您的Redis数据库将会面临爆破等安全风险。建议根据您的服务使用情况仅开放对应的外网IP或IP段。	✓	✓
阿里云RDS最佳安全实践	RDS-跨地域备份	容灾备份	低危	RDS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。	×	✓
	RDS-开启数据库备份	容灾备份	中危	建议RDS数据库实例开启数据备份功能，数据备份应当每天备份一次。	✓	✓
	RDS-白名单配置	访问控制	高危	数据库服务（RDS）端口不应直接对公网所有地址开放，应设定严格的访问控制策略，只允许特定的IP（如Web应用服务器）可以访问数据库服务。	✓	✓
	RDS-数据库安全策略	数据安全	中危	检查RDS的各个实例是否启用数据加密传输（SSL）、数据加密存储（TED）和SQL审计服务。	✓	✓
阿里云PolarDB最佳安全实践	PolarDB-SQL洞察	日志审计	中危	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。	×	✓
	PolarDB-备份设置	数据安全	中危	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。	×	✓
	PolarDB-白名单配置	访问控制	高危	检查云数据库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。	✓	✓
	云效-Codeup代码安全	数据安全	高危	云效Codeup代码安全提供了数据安全评分和安全风险事件提醒功能，及时检测企业代码资产的安全状态，实现安全预防、风险检测、主动防御的全方位保护。	✓	✓

最佳安全实践的类型	检查项名称	检查项所在章节	风险等级	说明	免费版、防病毒版	高级版、企业版、旗舰版
阿里云最佳安全实践	云盾-WAF回源配置	数据安全	高危	检查使用WAF服务后，需要隐藏后端服务器真实IP地址，避免攻击者直接访问真实IP绕过WAF。通过设置白名单的方式可以实现，当真实IP为弹性计算服务（ECS）IP时，在弹性计算服务（ECS）安全组进行设置，当真实IP为负载均衡服务（SLB）IP时，在负载均衡服务（SLB）上设置白名单访问控制策略，设置内容为：仅允许WAF回源IP地址访问。	✓	✓
	操作审计-日志配置	数据安全	中危	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（SLS）中，并合理设置日志的访问权限，以实现高危操作可追溯。 • 未开通操作审计时系统对管理员在云平台的操作行为不进行记录，当发生恶意操作时将无审计数据可查，难以定责。 • 未开通操作审计会不满足合规要求，例如：等级保护、ISO/IEC27001、PCI-DSS。	✓	✓
	云盾-高防回源配置	数据安全	高危	使用DDoS高防服务或Web应用防火墙（WAF）后，需要将后端服务器真实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。未使用负载均衡服务（SLB）情况下，在云主机（ECS）安全组中设置白名单访问控制策略实现地址隐藏；已使用负载均衡服务（SLB）的情况下，在负载均衡服务（SLB）上设置白名单访问控制策略实现地址隐藏；白名单设置内容为：仅允许DDoS、WAF回源IP地址访问真实IP。	✓	✓
	容器镜像服务-仓库权限设置	数据安全	高危	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，设置为公有仓库会造成镜像内部敏感信息泄漏。	×	✓
	SSL证书-有效期检查	数据安全	高危	检查SSL证书是否15天内将超出有效期或已过期，证书到期前需及时续费，否则您将无法继续使用SSL证书服务。	✓	✓
	CDN-实时日志推送	数据安全	中危	阿里云CDN提供将采集到的实时日志实时推送至日志服务SLS，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。	×	✓

最佳安全实践的类型	检查项名称	检查项所在章节	风险等级	说明	免费版、防病毒版	高级版、企业版、旗舰版
阿里云ECS最佳安全实践	ECS-安全组策略	访问控制	高危	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，例如网站的80、443端口。	×	✓
	ECS-自动快照策略	数据安全	中危	检查ECS磁盘是否开启自动快照功能。自动快照可以增加ECS主机的数据安全水位，实现容灾备份。创建快照将产生一定的费用，费用由快照产品收取，收费模式请见官网价格页。	✓	✓
	ECS-存储加密	数据安全	低危	检查ECS主机磁盘是否开启加密，开启云盘加密，可以满足您的业务更高的安全需求或法规合规要求。	✓	✓
	云监控-主机插件状态	监控告警	中危	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。	×	✓
	ECS-密钥对登录	身份认证	高危	检测ECS产品的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。	✓	✓
	云盾-主机安全防护	安全防护	高危	检查ECS主机的安骑士是否持续在线，云安全防御体系中，部署客户端提供主机漏洞、基线检测能力，主机入侵检测及防御的能力。	✓	✓
阿里云MongoDB最佳安全实践	MongoDB-SSL开启	数据安全	中危	为提高MongoDB数据库数据链路的安全性，建议您启用SSL加密。	×	✓
	MongoDB-日志审计	日志审计	中危	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。	×	✓
	MongoDB-备份设置	数据安全	中危	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。	×	✓

最佳安全实践的类型	检查项名称	检查项所在章节	风险等级	说明	免费版、防病毒版	高级版、企业版、旗舰版
	MongoDB-白名单配置	访问控制	高危	检查云数据库Mongodb实例是否开启白名单限制，白名单不允许拥有（0.0.0.0/0）的设置。	✓	✓

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

云平台配置检查功能支持手动检查和自动检查。本文介绍如何在云安全中心对云平台配置手动执行立即检查，以及设置检查周期进行自动检查。

背景信息

使用云平台配置检查功能，手动执行立即检查或设置自定义周期自动检查，可帮助您快速掌握您的云产品的安全状态并及时处理云产品上存在的安全风险。

手动检查

如果您想立即了解您的云产品配置的是否存在安全风险，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，选择**安全防范 > 云平台配置检查**。
3. 在**云平台配置检查**页面，单击**立即扫描**，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** 对云产品配置进行全量检查需要一段时间，请耐心等待。

自动检查

您也可以手动设置自动检查的周期和时间，云安全中心会在您设置的时间执行云平台配置检查。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**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**面板，配置云平台配置检查的检查周期、时间以及选择要检查的安全风险检测项。
5. 单击**确定**。

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

您可以在云平台配置检查页面集中处理检查出来的云平台配置风险。本文介绍如何查看和处理您的云产品配置中存在的安全风险。

背景信息

有关云安全中心支持检查的云平台配置项，请参见云平台配置检查项列表。

前提条件

已执行云平台配置检查。具体操作，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，选择**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。

   您可以执行以下操作：

   - 查看总览

     在**云平台配置检查**页面上方的总览区域，您可以查看云平台配置检查的**通过率**。将鼠标悬停在**通过率**下方的红色、橙色、蓝色或绿色的线段上，均可查看您的云产品配置检查结果中存在的**高危**、**中危**、**低危**以及**通过**的检查项的数量。
   - 查看目标风险项
     - 您可以在左侧**全部检查项**列表中单击目标最佳实践检查项菜单，然后在右侧的风险项列表中，查看与该检查项相关的风险项列表。
     - 您还可以通过列表上方提供的风险项的筛选组件，通过风险项的等级、状态等维度，筛选出您想要查看的目标风险项。

       > **说明** 不同的风险等级使用不同颜色的线段表示。
       >
       > - **高危**：红色。表示该风险项对您资产的危害较大，建议您尽快处理。
       > - **中危**：橙色。表示该风险项对您资产的危害一般，您可以延后处理。
       > - **低危**：灰色。表示该风险项对您资产的影响较小，您可以延后处理。
   - 查看目标风险项的详情

     单击目标风险项的检查项名称或风险项**操作**列的**详情**按钮，展开检查项的详情面板，查看该检查项的**检查项说明**、**处置方案**、**帮助资源**等详细信息。

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，选择**安全防范 > 云平台配置检查**。
3. 在**云平台配置检查**页面，处理检查出的风险项。

   您可以根据需要进行以下操作：

   - 修复

     您可以在风险项详情面板的**威胁影响**区域，单击存在风险的云产品的实例ID，跳转至对应的云产品实例管理控制台。然后根据风险项详情面板上提供的**处置方案**及**帮助资源**信息，修复该云产品配置中存在的安全风险。
   - 验证
     - 如果您已按照风险项详情面板上提供的修复建议，修改了**威胁影响**区域的受影响实例列表中某个云产品实例的配置，可在受影响实例列表中，单击该实例**操作**列的**验证**，检验新的配置是否存在安全风险。您修改后的云产品实例的配置在经过验证之后，通过了检查，则该实例会从**威胁影响**区域的受影响实例列表中移除。

- 如果您已对该存在该风险项的所有的云产品实例的配置项进行了修改，可在**云平台配置检查**页面的检查结果列表中，单击该风险项**操作**列的**验证**，检验新的配置是否存在安全风险。您修改后的云产品的配置在经过验证之后，通过了检查，则该风险项的状态会变为**已通过**。
- 如果您需要同时验证多个风险项，可以选中这些风险项并单击列表下方的**验证**，在**确认**对话框中单击**确定**。

- 加白名单
  如果您判断检查出的某个风险项不存在安全风险，可在**云平台配置检查**页面的检查结果列表中，定位到该风险项，单击其**操作**列的**加白名单**，将该风险项状态调整为**已加白**。**已加白**的风险项将不会包含在风险项总数中。

  > **说明** 将风险项加入白名单后，后续云平台配置检查中，将不会再上报与该风险项对应的检查项相关的风险。请您谨慎操作。

  您也可以在**云平台配置检查**页面的检查结果列表中，对已加白的风险项进行**取消加白**的操作。

4.镜像安全扫描

4.1. 镜像安全扫描概述

镜像安全扫描功能支持对镜像中存在的高中危系统漏洞、应用漏洞、恶意样本、配置风险和敏感数据进行检测，并提供漏洞修复方案，为您提供一站式漏洞管理能力。

版本限制说明

镜像安全扫描功能为云安全中心增值服务，需单独购买。仅支持高级版、企业版、旗舰版和仅采购增值服务用户购买镜像安全扫描功能。

> **说明** 免费版用户可升级至高级版、企业版、旗舰版或仅采购增值服务购买镜像安全扫描功能。防病毒版用户可升级至高级版、企业版或旗舰版购买镜像安全扫描功能。

支持的地域

目前，仅部署在华东1（杭州）、华东2（上海）、华北2（北京）、华南1（深圳）、中国香港、新加坡地域的容器镜像服务支持使用镜像安全扫描功能。

支持扫描的安全镜像特性

镜像安全检查项	检测	修复	备注
镜像系统漏洞	支持检测	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	支持检测	不支持	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。
镜像基线检查	支持检测	不支持	建议您根据云安全中心提供的基线检查详细信息及时处理镜像基线风险。
镜像恶意样本	支持检测	不支持	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。

支持的操作系统

操作系统类型	支持扫描的操作系统版本	支持修复的操作系统版本
Red Hat	• Red Hat 5 • Red Hat 6 • Red Hat 7	无
CentOS	• CentOS 5 • CentOS 6 • CentOS 7	• CentOS 7 • CentOS 8

操作系统类型	支持扫描的操作系统版本	支持修复的操作系统版本
Ubuntu	• Ubuntu 12.04 • Ubuntu 14.04 • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 18.10	• Ubuntu 14 • Ubuntu 16 • Ubuntu 18
Debian	• Debian 6 • Debian 7 • Debian 8 • Debian 9 • Debian 10	• Debian 9 • Debian 10
Alpine	• Alpine 2.3 • Alpine 2.4 • Alpine 2.5 • Alpine 2.6 • Alpine 2.7 • Alpine 3.1 • Alpine 3.2 • Alpine 3.3 • Alpine 3.4 • Alpine 3.5 • Alpine 3.6 • Alpine 3.7 • Alpine 3.8 • Alpine 3.9 • Alpine 3.10 • Alpine 3.11 • Alpine 3.12	Alpine 3.9
Amazon Linux	• Amazon Linux 2 • Amazon Linux AMI	无
Oracle Linux	• Oracle Linux 5 • Oracle Linux 6 • Oracle Linux 7 • Oracle Linux 8	无

操作系统类型	支持扫描的操作系统版本	支持修复的操作系统版本
SUSE Linux Enterprise Server	• SUSE Linux Enterprise Server 5 • SUSE Linux Enterprise Server 6 • SUSE Linux Enterprise Server 7 • SUSE Linux Enterprise Server 8 • SUSE Linux Enterprise Server 9 • SUSE Linux Enterprise Server 10 • SUSE Linux Enterprise Server 10 SP4 • SUSE Linux Enterprise Server 11 SP3 • SUSE Linux Enterprise Server 12 SP2 • SUSE Linux Enterprise Server 12 SP5	无
Fedora Linux	• Fedora Linux 2X • Fedora Linux 3X	无
openSUSE	• openSUSE 10.0 • openSUSE Leap 15.2 • openSUSE Leap 42.3	无

相关文档

容器安全概述

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

4.2. 开通服务

使用镜像安全扫描功能需先开通并购买该功能。本文介绍如何开通并购买镜像安全扫描功能。

背景信息

镜像安全扫描功能为云安全中心增值服务，需单独购买。仅支持高级版、企业版、旗舰版和仅采购增值服务用户购买镜像安全扫描功能。

镜像安全扫描功能按照扫描镜像次数计费，计费价格请参见云安全中心购买页。

> **说明** 免费版用户可升级至高级版、企业版、旗舰版或仅采购增值服务购买镜像安全扫描功能。防病毒版用户可升级至高级版、企业版或旗舰版购买镜像安全扫描功能。

免费版用户开通服务

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全防范 > 镜像安全扫描**。
3. 单击**立即购买**。
4. 单击**购买高级版**、**购买企业版**或**购买旗舰版**。

   旗舰版除支持**企业版**的所有功能外，还支持**容器网络拓扑**、**容器K8s威胁检测**和**运行时威胁检测**能力。

如果您对容器安全有较高的要求，建议您选择**购买旗舰版**。各版本的功能差异详情，请参见功能特性。

5. 在**购买高级版**、**购买企业版**或**购买旗舰版**页面，设置**容器镜像安全扫描**数量和其余配置。

容器镜像安全扫描数量建议设置为您在购买时间内需要进行容器漏洞检测的镜像数量。云安全中心是以摘要（Digest）值唯一标识一个镜像，镜像的摘要值不变时，只在第一次扫描时消耗一个镜像安全扫描次数。摘要值变化后，执行扫描操作会重新消耗镜像安全扫描次数。例如，您需要对10个镜像进行检测，在您购买云安全中心服务的期限内，预计镜像更新总次数为20次，则**容器镜像安全扫描**数量需要设置为30（即10+20）。
以下是购买页面相关参考链接：

- 计费详情，请参见计费方式。
- 如何配置购买页面其余参数，请参见购买云安全中心。

> **说明** 如果您仅需使用云安全中心提供的镜像安全扫描服务，您可以将版本选择为仅采购增值服务，并购买足够的**容器镜像安全扫描**数量。

6. 单击**立即购买**并完成支付。

非基础版用户开通服务

防病毒版用户需要升级至高级版、企业版或旗舰版，并购买镜像安全扫描次数来开通镜像安全扫描服务。高级版、企业版或旗舰版用户需要购买镜像安全扫描次数来开通镜像安全扫描服务。具体操作，请参见升级与降配。

4.3. 接入镜像仓库

对容器镜像进行安全扫描之前，您需要将镜像仓库接入到云安全中心。本文介绍如何将镜像仓库接入云安全中心。

背景信息

云安全中心支持接入的容器镜像仓包括：阿里云容器镜像服务ACR和第三方镜像服务（harbor、quay）。

前提条件

已开通镜像安全扫描功能。具体操作，请参见开通服务。

接入阿里云容器服务镜像仓库

阿里云容器镜像服务ACR包括企业版和个人版。目前云安全中心支持同步ACR企业版和个人版的镜像数据，但仅支持对企业版镜像进行镜像安全扫描。您只需为企业版实例添加专有网络，即可将企业版镜像仓库接入到云安全中心。相关操作，请参见配置专有网络的访问控制。

接入第三方镜像仓库（私有镜像仓库）

如果您的第三方镜像服务是通过线下IDC+云上VPC的混合云方式来部署的，您需要先配置流量的转发规则，再完成接入镜像仓库。具体操作，请参见混合云场景代理配置说明。

如果您的容器镜像仓库设置了访问控制策略，请确认已将镜像仓库对应的地域加入到访问控制白名单中。

地域	公网IP	私网IP
华东1（杭州）	121.41.35.192、121.41.39.7、121.41.39.39、121.41.39.153、121.41.38.32	100.104.177.0/26
华东2（上海）	47.103.62.83、47.103.60.134、47.103.58.177、47.103.54.252、47.103.49.93	100.104.7.192/26

地域	公网IP	私网IP
华北1（青岛）	47.104.111.68	100.104.87.192/26
华北2（北京）	123.57.55.56、123.57.55.21、123.57.55.18、123.57.55.7、123.57.55.6	100.104.20.128/26
华北3（张家口）	39.99.229.195	100.104.187.64/26
华北5（呼和浩特）	39.104.147.68	100.104.36.0/26
华南1（深圳）	47.106.245.198、47.107.237.185、47.107.237.182、47.107.237.170、47.107.237.152	100.104.9.192/26
中国香港（香港）	47.106.245.198、47.107.237.185、47.107.237.182、47.107.237.170、47.107.237.152	100.104.111.128/26
亚太东北1（东京）	47.74.24.20	100.104.69.0/26
亚太东南1（新加坡）	47.74.238.176、47.74.238.61、47.74.237.201、47.74.237.166、47.74.237.91	100.104.41.128/26
美国西部1（硅谷）	47.254.39.224	100.104.145.64/26
美国东部1（弗吉尼亚）	47.252.4.238	100.104.36.0/26
德国（法兰克福）	47.254.158.71	172.16.0.0/20
英国（伦敦）	8.208.14.12	172.16.0.0/20
印度尼西亚（雅加达）	149.129.238.99	100.104.193.128/26

1. 登录云安全中心控制台，在左侧导航栏，选择**安全防范 > 镜像安全扫描**。
2. 在**镜像安全扫描**页面的**三方镜像仓接入**区域，单击**接入**。
3. 在**接入镜像仓**面板，配置接入私有仓库的参数，然后单击**确定**。

配置项	说明
私有仓库类型	选择私有仓库类型。目前支持选择harbor、quay类型的仓库。 **说明** 请按照您容器镜像存储的镜像仓，选择对应的私有仓库类型即可。
版本	选择第三方镜像仓库的版本。 ○ **V1**：镜像仓库版本为1.X.X时，选择该版本。 ○ **V2**：镜像仓库版本为2.X.X及以上时，选择该版本。
通信类型	选择云安全中心与第三方镜像仓库的通信协议。
网络类型	选择第三方镜像仓库的网络类型。
RegionId	选择第三方镜像仓库所在区域。

配置项	说明
IP	输入第三方镜像仓库的IP地址。 **说明** 第三方镜像仓库部署在混合云环境中时，IP必须填写。
域名	输入第三方镜像仓库的域名。
限速	选择每小时可接入的镜像仓库个数。默认为**10**。 **注意** 如果每小时内接入的镜像过多，可能会影响您的正常业务的运行，建议您谨慎选择**无限制**。
用户名	输入访问第三方镜像仓库时使用的用户名。
密码	输入访问第三方镜像仓库的密码。

接入第三方镜像仓库后，您可以在**镜像安全扫描**页面的**扫描设置**面板中查看已接入的镜像仓库信息。

混合云场景代理配置说明

如果您的第三方镜像服务是通过线下IDC+云上VPC的混合云方式来部署的，您需要先配置流量的转发规则，再完成接入镜像仓库。操作流程如下：

1. 指定一台ECS服务器，将其访问流量转发到第三方镜像服务所在的IDC服务器上。

   示例：将执行转发任务的ECS服务器中A端口的流量，转发至第三方镜像服务所在的IDC服务器192.168.XX.XX的B端口。

   - CentOS 7命令：
     - 使用firewallcmd：

       ```
       firewall-cmd --permanent --add-forward-port=port=<A端口>:proto=tcp:toaddr=<192.168.XX.XX>:toport=<B端口>
       ```

     - 使用iptables：

       a. 开启端口转发。

       ```
       # echo "1" > /proc/sys/net/ipv4/ip_forward
       ```

       b. 设置端口转发。

       ```
       # iptables -t nat -A PREROUTING -p tcp --dport <A端口> -j DNAT --to-destination <192.168.XX.XX>:<B端口>
       ```

   - Windows命令：

     ```
     netsh interface portproxy add v4tov4 listenport=<端口A> listenaddress=* connectaddress=<192.168.XX.XX> connectport=<端口B> protocol=tcp
     ```

2. 将第三方镜像仓库接入到云安全中心。

   接入第三方镜像仓库时，配置项**IP**必须填写您已配置了转发规则的ECS的地址。详细操作说明，请参见接入第三方镜像仓库（私有镜像仓库）。

镜像接入错误码

code	message	解决方案
FailedToVerifyUsernameOrPwd	用户名或密码验证失败	检查用户名、密码是否正确
RegistryVersionError	镜像仓版本错误	检查镜像仓的版本是否选择正确
UserDoesNotHaveAdminRole	用户没有admin权限	前往harbor私服给用户添加管理员权限
NetworkConnectError	网络超时，请检查网络	检查网络是否联通、80或443端口是否开放

后续步骤

将镜像仓库接入到云安全中心后，您可以在**资产中心**查看受到云安全中心防护的镜像信息。具体操作，请参见查看容器安全状态。

您还需要执行镜像安全扫描操作，才能通过云安全中心检测您的镜像是否存在风险。具体操作，请参见执行镜像安全扫描。

4.4. 执行镜像安全扫描

云安全中心的镜像安全扫描功能，可以帮助您检测您的镜像中是否存在镜像漏洞和恶意样本，为您创造安全的镜像运行环境。本文介绍如何进行镜像安全扫描。

前提条件

- 已购买容器镜像服务企业版实例或已接入私有镜像仓库。相关内容，请参见创建企业版实例和接入镜像仓库。
- 已购买或升级至云安全中心企业版、旗舰版。具体操作，请参见购买云安全中心和升级与降配。各版本支持的功能详情，请参见功能特性。
- 已购买足够的**容器镜像安全扫描**镜像个数。

背景信息

镜像上的基础系统软件、中间件、Web应用、数据库服务等，可能会存在挖矿木马、后门程序等安全漏洞，危害您的资产安全。云安全中心支持立即执行镜像安全扫描和配置镜像漏洞扫描周期定期扫描两种镜像漏洞扫描方式。具体操作，请参见立即执行镜像安全扫描、配置镜像漏洞扫描周期（定期扫描）。

> **注意** 如果您镜像变更过（即镜像摘要发生变化），执行镜像安全扫描时会消耗您购买的**容器镜像安全扫描**次数。执行镜像安全扫描前，请确保您有足够的**容器镜像安全扫描**次数。

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，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。

镜像漏洞扫描预计需要1分钟时间，您可以在1分钟后手动刷新页面，在下方的镜像漏洞列表中查看扫描结果。

配置镜像漏洞扫描周期（定期扫描）

如果需要定期自动扫描您的资产中是否存在镜像漏洞或恶意样本，您可以参照以下步骤配置镜像漏洞扫描周期。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全防范 > 镜像安全扫描**。
3. 在**镜像安全扫描**页面的右上角，单击**扫描设置**。
4. 在**扫描设置**面板，配置相关参数。

   您可以参考以下表格中的参数说明，设置扫描相关参数。

配置项	说明
已消耗授权数/总授权	显示您已使用和已购买的容器镜像安全扫描次数。如果您的镜像安全扫描次数即将耗尽，您可以单击**扩容**按需求购买镜像安全扫描次数。
扫描周期	选择执行镜像安全扫描的周期。
扫描范围	设置需要扫描的镜像范围。具体操作如下： i. 单击**扫描范围**右侧的**管理**。 ii. 在**镜像管理**对话框中，选择需要扫描的镜像仓库。 iii. 单击**设置**。
扫描时间范围	选择镜像漏洞扫描的时间范围。 **注意** 扫描时间范围以镜像的更新时间为准。若无更新时间，则以创建时间为准，时间范围决定镜像是否会被扫描。比如扫描时间范围选择为**最近7天**，那么云安全中心会扫描最近7天以内更新的镜像。镜像更新时间超过7天，则不会被扫描。
漏洞保留时长	设置漏洞扫描结果的保留时长，超过保留时长后漏洞扫描结果会自动删除。

   云安全中心将按照您的漏洞扫描配置，对您的镜像进行安全扫描。

管理镜像仓

您可单击**镜像仓**页签，查看支持扫描的容器镜像服务企业版实例（镜像库类型为ACR）和已接入的私有镜像仓库（镜像库类型为Harbor）列表。

> **说明** 云安全中心会自动同步您账号下的容器镜像服务企业版实例至镜像仓库列表中，不支持在镜像仓库列表中移除容器镜像服务企业版实例。

- 如果您想扫描不在镜像仓库列表中的私有镜像仓库，您可以单击**接入镜像仓**接入您的私有镜像仓库。**接入私有镜像仓**相关参数配置，请参见接入镜像仓库。
- 如果镜像仓库列表中的某个私有镜像仓库无需扫描，您可以单击私有镜像仓库**操作**列的**移除**，并在提示信息对话框中单击**确定**，将其移除。

  > **说明** 镜像仓库列表中的两个默认镜像仓（镜像仓类型为acr、defaultAcr）不支持删除。

- 如果是harbor镜像仓，您可以单击**操作**列的**编辑**，对镜像扫描的**限速**进行设置，以提供镜像安全扫描的效率。限速默认为**10**。例如该harbor镜像仓中有200个镜像，使用默认限速，扫描完成需要20小时。如果将限速改为200，则扫描完成仅需1小时。

配置镜像基线扫描

您可以配置镜像漏洞扫描的同时，对您镜像的基线配置进行检查。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全防范 > 镜像安全扫描**。
3. 在**镜像安全扫描**页面的右上角，单击**扫描设置**。
4. 在**扫描配置**面板上，单击**基线配置管理**页签。
5. 单击**配置范围**右侧的**管理**。
6. 在**基线检查范围**面板上，选择您要检查的基线。

> 注意 下方的Access Key泄露检查、密码泄露检查两个配置项中包含的基线，与基线检查范围面板上的Access Key泄漏和密码泄漏这两个基线相同。如果您在基线检查范围面板上已经选择了Access Key泄漏和密码泄漏这两个基线，下方的Access Key泄露检查和密码泄露检查的配置状态开关会自动打开，您无需再重复设置。您也可以通过Access Key泄露检查、密码泄露检查后面的开关快捷开启或关闭这两个基线。

7. 单击下方**确定**。
   配置完成后，云安全中心在执行镜像安全扫描的同时，会对您镜像的基线配置进行检查。

后续步骤

执行完镜像安全扫描后，您可以查看镜像安全扫描结果。更多信息，请参见查看镜像安全扫描结果。

4.5. 查看镜像安全扫描结果

云安全中心提供的镜像安全扫描功能，可以检测您的镜像资产中存在的系统漏洞、应用漏洞、基线风险和恶意样本，并进行分类展示，帮助您全面了解您的镜像资产中存在的安全风险。本文介绍如何查看您镜像资产存在的安全风险。

前提条件

已执行镜像安全扫描。具体操作，请参见执行镜像安全扫描。

背景信息

镜像安全扫描功能仅支持检测镜像系统漏洞、镜像应用漏洞、基线风险和镜像恶意样本，不支持修复。建议您根据云安全中心提供的修复命令、影响说明或恶意文件路径等信息，及时处理容器中存在的安全风险。

查看镜像系统漏洞扫描结果

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全防范 > 镜像安全扫描**。
3. 在**镜像安全扫描**页面，单击**镜像系统漏洞**页签。
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：

   - 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**

> **说明**

- 您可在**镜像系统漏洞**页签，通过筛选漏洞危险等级（高、中、低），或者搜索实例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：

  - 单击漏洞编号可跳转至阿里云漏洞库。

  - **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。

    - ：执行该命令可修复对应的漏洞。
    - ：
      - ：该镜像的版本信息。
      - ：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）。
      - ：该镜像在服务器上的路径。
      - **镜像层**：存在漏洞的镜像层。
    -

    > **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。

- **导出扫描结果列表**

  您可以单击列表右上方的图标，一键导出镜像系统漏洞扫描结果列表。

查看镜像应用漏洞扫描结果

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全防范 > 镜像安全扫描**。
3. 在**镜像安全扫描**页面，单击**镜像应用漏洞**页签。
4. 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**

     > 说明

   - **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：
     - 单击漏洞编号可跳转至阿里云漏洞库。
     - **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。
       - ：执行该命令可修复对应的漏洞。
       - ：
         - ：该镜像的版本信息。
         - ：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）。
         - ：该镜像在服务器上的路径。
         - **镜像层**：存在漏洞的镜像层。
       -
   - **导出扫描结果列表**
     您可以单击列表右上方的图标，一键导出镜像应用漏洞扫描结果列表。

查看镜像基线检查扫描结果

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全防范 > 镜像安全扫描**。
3. 在**镜像安全扫描**页面，单击**镜像基线检查**页签。
4. 在**镜像基线检查**页签下，查看扫描出来的镜像基线检查结果列表。

   你可以执行以下操作：

   - **搜索基线检查结果**

您可以使用列表上方提供的搜索组件，通过基线检查结果的危险程度（**高危**、**中危**、**低危**）、基线的名称、基线的分类搜索满足条件的基线检查结果。

- **查看镜像基线检查结果**
  您可以在镜像基线检查结果列表中，查看单个或者所有镜像基线检查结果的**基线名称/分类**、**受影响镜像**、**最新扫描时间**、**首次扫描时间**以及基线的修复**状态**等信息。
- **查看镜像基线检查结果详情**
  您可以在镜像基线检查结果列表中，单击**操作**列的**详情**，展开该基线检查结果的详情面板，您可以查看受该基线影响的镜像资产的地址、版本及镜像上存在的基线风险的数量等信息。单击对应镜像资产**操作**列的**详情**，展开**风险项**面板，可查看该镜像资产中存在的风险检查项详情。
- **导出扫描结果列表**
  您可以单击列表右上方的图标，一键导出镜像基线检查结果列表。

查看镜像恶意样本扫描结果

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全防范 > 镜像安全扫描**。
3. 在**镜像安全扫描**页面，单击**镜像恶意样本**页签。
4. 在**镜像恶意样本**页签下，查看扫描出的镜像恶意样本列表。

> 注意 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。

您可以执行以下操作：

- **搜索镜像恶意样本**
  在镜像恶意样本列表左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。
- **导出扫描结果列表**
  您可以单击列表右上方的图标，一键导出样本扫描结果列表。

5.安全防范常见问题

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。

如何手动检测服务器上的Linux软件漏洞？

如果您需要通过命令行的方式在您服务器上手动检测系统软件漏洞，您可以参见如何手动检测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*。

   ```
   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
```

漏洞修复完成后我是否还需要重启系统？

- Windows服务器：
  在云安全中心控制台完成Windows系统漏洞的修复后，您还需要对Windows服务器系统进行重启，漏洞修复才能生效。
  所有Windows漏洞修复完成后，都需要执行重启的操作。
- Linux服务器：
  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清理。

> **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

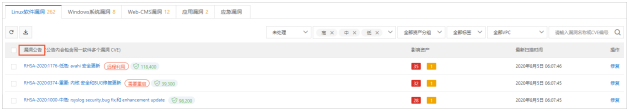
  ```
  No Packages marked for Update
  ```

  这种情况是由于该软件的官网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。



- **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。

> **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查看和修复漏洞。

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。

批量进行漏洞修复时，漏洞修复按照什么顺序执行？

Linux软件漏洞和Web-CMS漏洞按照控制台中漏洞列表的顺序执行批量修复。修复部分Windows系统漏洞时会需要先安装前置补丁，批量修复Windows系统漏洞时优先修复此类漏洞，其余漏洞按照控制台中漏洞列表顺序执行修复。

修复漏洞时创建快照失败是什么原因？我该怎么办？

修复漏洞时创建快照失败可能是以下原因造成的：

- 您当前执行修复操作的账号是RAM账号：如果您当前使用的是RAM账号，并且该账号不具备创建快照的权限，控制台会提示您创建快照失败。建议您使用阿里云账号进行操作。RAM账号更多信息，请参见RAM用户概览。
- 该服务器为非阿里云服务器：非阿里云服务器不支持创建快照修复漏洞。

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，已检测出的漏洞记录会一直保留在云安全中心控制台上。

客户端离线或关闭，系统漏洞的告警3天自动失效，应用漏洞的告警30天自动失效，应急漏洞的告警90天自动失效。漏洞失效后，您无法对漏洞执行任何操作，包括修复漏洞或清除漏洞记录。

除非您的云安全中心服务过期后7天您仍未续费，您的云安全中心数据才会被释放并彻底删除。此时，您在云安全中心控制台上看不到任何数据。

如何清理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。

> **说明** 应用漏洞为企业版和旗舰版功能，免费版、防病毒版和高级版不支持。免费版、防病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，请检查您服务器的DNS解析是否正常，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。

需要重启才能验证的漏洞，云安全中心能自动验证吗？

不会。

修复成功但需要重启才能验证的漏洞其状态为**修复成功待重启**。云安全中心会每天执行漏洞扫描，该类漏洞修复后，云安全中心将检测不到该类漏洞。从第一次检测不到该类漏洞起，控制台会将该类漏洞的信息保存三天（确保非网络或其他原因没有检测到该漏洞），三天后控制台会清除该类漏洞信息。

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。

应急漏洞检测会不会对我的业务系统产生影响？

应急漏洞检测是通过初步检测漏洞原理确认是否存在漏洞。云安全中心会发送1~2个TCP网络请求报文至您的所有ECS或SLB等IP地址，但不会执行任何实际上的黑客行为。云安全中心应急漏洞检测功能上线前都经过了大规模百万IP数量级的测试，具有很高的稳定性和可靠性。但是测试无法完全覆盖未知风险，可能会存在未知风险。例如会存在由于某些网站业务逻辑脆弱（1~2个TCP请求会导致服务器宕机）对业务系统造成风险。

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？

Fastjson漏洞的检测依赖JAR包运行态是否加载，Webserver对于JAR包的加载分为动态加载和静态加载。动态加载模式下，Fastjson漏洞只有在JAR包运行时才能被检测出来，所以每个时段检测结果会存在差异。建议您针对Fastjson漏洞进行多次检测，提升检测结果的准确度。

漏洞扫描周期说明

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

漏洞类型	免费版	防病毒版	高级版	企业版	旗舰版
Linux软件漏洞	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	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	每天自动扫描一次	每天自动扫描一次	每天自动扫描一次	每天自动扫描一次

漏洞类型	免费版	防病毒版	高级版	企业版	旗舰版
Web-CMS漏洞	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	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）	每周自动扫描一次（支持修改自动扫描周期）
应急漏洞	不扫描	不扫描	不扫描（支持设置扫描周期进行周期性扫描）	不扫描（支持设置扫描周期进行周期性扫描）	不扫描（支持设置扫描周期进行周期性扫描）

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、应急漏洞的扫描周期，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）。

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、企业版和旗舰版用户可使用该服务。免费版、防病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。