

# 多云安全治理服务 操作指南



腾讯云

## 【 版权声明 】

©2013–2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

## 【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

## 【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

## 【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

# 文档目录

## 操作指南

发起评估任务

查看评估任务进度

查看风险内容

开启“暴露面管理服务”联动

查看互联网暴露面

检索暴露路径

评估周期管理

# 操作指南

## 发起评估任务

最近更新时间：2024-11-11 17:01:52

在您完成云账号授权后，即可发起评估任务。

### 前提条件

已完成云账号授权，授权文档如下：

- [腾讯云账号授权](#)
- [阿里云账号授权](#)

### 操作步骤

1. 登录 [多云安全治理服务控制台](#)，在左侧菜单栏中，单击**总览**。
2. 在总览页面，单击**一键评估**或**重新评估**，即可发起安全评估任务。

- 首次发起安全评估任务时，页面显示如下：



- 若已发起过安全评估任务，页面显示如下：

安全评估



最新评估时间: 2024-10-31 16:33:59

评估完成, [查看详情](#)

最新评估中, 共发现   个风险

点击下方按钮即可一键启动无损安全评估

[重新评估](#)

最新评估情况:



紧急风险 !



全部风险



检测资产



成功策略   个

失败策略: 0 个

# 查看评估任务进度

最近更新时间：2024-11-11 17:01:52

发起评估任务后，您可以通过以下步骤查看评估任务的进度。

## 操作步骤

### 方案一

登录 [多云安全治理服务控制台](#)，在左侧菜单栏单击**总览**，查看最新任务的进度情况。

总览



### 方案二

1. 登录 [多云安全治理服务控制台](#)，在左侧菜单栏中，单击**扫描任务**。
2. 在扫描任务页面，支持通过评估状态、任务 ID、任务开始/结束时间来筛选目标任务。
3. 在选中目标任务后，您可以通过查看任务进度列来了解相关进度。

评估任务

请选择评估状态

请输入任务 ID Q

任务开始时间

任务结束时间 📅

🔄

[周期运行管理](#)

任务 ID	创建人	任务状态	任务进度	任务耗时	风险个数	资产个数	任务开始时间	任务结束时间	操作
xspm-a8	1000	评估完成	<div style="width: 100%; height: 10px; background-color: green;"></div> 100%	1小时 秒	0	0 个	2024-10-30 17:55:27	2024-10-30 19:38:06	<a href="#">查看详情</a>
xspm-e	1000	评估完成	<div style="width: 100%; height: 10px; background-color: green;"></div> 100%	6分钟17秒	0	0 个	2024-10-30 16:21:40	2024-10-30 16:27:57	<a href="#">查看详情</a>
xspm-l	100	评估完成	<div style="width: 100%; height: 10px; background-color: green;"></div> 100%	3分钟34秒	0	0 个	2024-10-11 10:56:19	2024-10-11 10:59:53	<a href="#">查看详情</a>
xspm-ssl	100	评估完成	<div style="width: 100%; height: 10px; background-color: green;"></div> 100%	4分钟24秒	0	0 个	2024-09-14 16:51:03	2024-09-14 16:55:27	<a href="#">查看详情</a>

共 4 条
10 条 / 页 ⏪ 1 / 1 页 ⏩

4. 在扫描任务页面，单击目标任务的[查看详情](#)，即可查看具体任务信息。

任务 ID: xspm-[redacted] ×

### 基本信息

任务状态: 评估完成  
创建人: 10[redacted] 🔒  
任务进度: 100 %  
任务策略: 🟢 93 个 🔴 0 个  
任务耗时: 1小时42分钟39秒  
任务开始时间: 2024-10-30 17:55:27  
任务结束时间: 2024-10-30 19:38:06

---

### 风险结果

🔴 [redacted]

### 资产结果

🔴 [redacted] ↑

---

### 任务目标

云账号	云厂商
[redacted]6	<span>🔴</span>

---

### 策略信息

请输入风险策略名 请选择策略状态 ▼

风险策略名	状态
阿里云 Elasticsearch Service未开https协议	<span>成功</span>
阿里云 Elasticsearch Service未开启数据备份	<span>成功</span>
阿里云 ACK集群未开启删除保护	<span>成功</span>

# 查看风险内容

最近更新时间：2024-11-11 17:01:52

安全评估任务完成后，即可查看云账号下的风险内容。

## 操作步骤

1. 登录 [多云安全治理服务控制台](#)，在左侧菜单栏中，单击**风险治理指引**。
2. 在风险治理指引，您可以看到分层的风险列表，支持通过**检测模式**和**云账号信息**，对风险进行过滤。

### 风险治理指引

The screenshot displays the 'Risk Governance Guide' interface. At the top, there are two dropdown menus for 'Select Detection Mode' and 'Select Cloud Provider'. To the right, there are summary statistics for risk levels: 3 Severe, 654 High, 60 Medium, and 65 Low. A 'Patrol Time' indicator shows 2024-10-31 16:33:59. Below this, there are two main sections: 'Urgent Risk Disposition' and 'Exposed Risk'. Each section contains a table of risks with columns for Cloud Provider, Detection Description, Risk Level, Risk Description, and Action.

云厂商	检测描述	风险等级	风险说明	操作
腾讯云	检查主机安全事件	严重	发现 1 个主机安全事件	<a href="#">详情</a>
腾讯云	检查OSS Bucket是否可匿名读写路径	高危	发现 1 个OSS Bucket可匿名读写路径	<a href="#">详情</a>
腾讯云	检测OSS Bucket是否可匿名遍历路径	高危	发现 1 个OSS Bucket可匿名遍历路径	<a href="#">详情</a>

云厂商	检测描述	风险等级	风险说明	操作
腾讯云	检查云数据库RDS是否对公网暴露	高危	发现 1 个RDS实例对公网暴露	<a href="#">详情</a>
腾讯云	检查云服务器是否对公网暴露端口	中危	发现 1 个云服务器对公网暴露端口	<a href="#">详情</a>

参数名称	说明
检测模式	页面将展示归属已选择检测模式的所有风险。检测模式列表源自系统预制及您自定义

	义的检测模式。
云厂商-云账号	页面将展示归属已选择云账号的所有风险。云账号列表源自您授权的云账号。

3. 在风险治理指引页面，单击右上角的 ，选择**汇总导出**或**按云账号拆分导出**，单击**确定**即可导出 Excel 格式的风险报告。

**说明：**

- 汇总导出：将所有云账号的风险汇总成一份报告。
- 按云账号拆分导出：将各云账号的风险分别导出一份报告。

### 风险治理指引

请选择云厂商-云 严重 3 高危 651 中危 6 低危 0 巡检时间：2024-10-31 16:33:59 

#### 紧急风险处置

云厂商	检测描述	风险等级	风险说明	操作
	检查最近30天是否存在未处置的主机安全事件。	严重	发现 1 个主机安全事件	<a href="#">详情</a>

共 1 条

4. 在风险治理指引页面，单击目标风险的详情，可以了解风险的危害、修复建议和具体列表。

腾讯云数据库MySQL开放公网且绑定的安全组入站规则开放范围配置过大 中危



3 删除存在风险的规则（来源范围过大），或者更新来源，遵循放通IP最小化开放原则，只按业务所需对指定来源需要开放指定来源指定端口。

删除安全组规则



! 该安全组已关联1个实例，删除规则可能导致业务中断，请再次确认修改后的影响

来源	协议端口	策略	备注
3	ALL	允许	

确认 取消

4 如安全组不再使用，请及时删除安全组。

规则操作

已开启检测该规则

受影响资产列表

请输入资产名称  🔍 🔄 📄

资产名称/ID	风险状态	服务商/类型/地域	云账号	发现时间	操作
ram cdb	<span style="color: #ffc107;">!</span> 未修复	云数据库 华南地区(广州)	1000	2024-11-02 14:27:27	<a href="#">跳转到控制台</a> <a href="#">验证</a> <a href="#">标记忽略</a>
		云数据库 MySQL			

# 开启“暴露面管理服务”联动

最近更新时间：2024-11-11 17:01:52

多云安全治理服务可与 [暴露面管理服务](#) 开启联动。开启后，多云治理服务完成互联网暴露面梳理时，将相关资产通过接口发送至暴露面管理服务进行扫描，待扫描完成后，将读取结果数据，在多云治理服务的 [互联网暴露面](#) 页面进行关联展示。

## 前提条件

- 您已购买 [多云安全治理服务](#)。
- 您当前登录的腾讯云账号已购买 [暴露面管理服务](#)，或您当前登录的腾讯云账号未曾试用 [暴露面管理服务](#)。

## 操作步骤

1. 登录 [多云安全治理服务控制台](#)，在左侧菜单栏中，单击 [安全服务联动配置](#)。
2. 在安全服务联动配置页面中，分为以下两种情况：
  - 若您当前登录的腾讯云账号已购买 [暴露面管理服务](#)，单击 [开启联动开关](#)。

### 安全服务联动配置

#### 安全服务联动

#### 暴露面管理服务

**产品介绍** 暴露面管理服务是一个主动的风险管理服务，旨在根据企业的授权，通过一系列脆弱性发现、威胁监测等工具对企业资产的暴露面及潜在威胁进行挖掘与物理资产的可访问性、暴露面及可利用性，帮助企业降低漏洞利用风险，优化运营流程。

**联动说明** 开启产品联动后，多云安全治理服务的每个检测任务，将主动推送您账号下的资产信息下发给暴露面管理服务进行扫描，并在扫描完成后，同步扫描结果页面，获取到开放资产的探测结果。

**购买状态** 试用中：2024-11-06 23:59:59到期

**开启联动**

请您仔细阅读开通说明，确认无误后，单击 [确定](#) 即可开通。

## 开启暴露面管理服务联动



当您选择开启多云安全治理服务与暴露面管理服务的联动后，即默认您同意多云安全治理服务在每一次执行安全评估任务时，将获取到的本账号下所有资产IP、域名、端口下发至暴露面管理服务进行扫描。扫描完成后，相关资产的探测结果、漏洞信息等信息将通过本控制台进行关联展示。

 我已阅读并同意以上开通说明

确定

取消

- 若您当前登录的腾讯云账号未购买暴露面管理服务，并且也未曾有过试用，支持开启7天的免费试用，任意腾讯云主账号仅可试用一次。

## 安全服务联动

## 暴露面管理服务

**产品介绍** 暴露面管理服务是一个主动的风险管理服务，旨在根据企业的授权，通过一系列脆弱性发现、威胁监测等工具对企业资产的暴

**联动说明** 开启产品联动后，多云安全治理服务的每个检测任务，将主动推送您账号下的资产信息下发给暴露面管理服务进行扫描，并在

**购买状态** [开启试用](#) 或 联系您的专属售前工程师完成购买。

**开启联动**

单击[开启试用](#)后，请您仔细阅读《暴露面管理服务授权书》及开通说明，确认无误后，单击[确定](#)即可开通。

## 开通暴露面管理服务试用



当您选择开启多云安全治理服务与暴露面管理服务的联动后，即默认您同意多云安全治理服务在每一次执行安全评估任务时，将获取到的本账号下所有资产IP、域名、端口下发至暴露面管理服务进行扫描。扫描完成后，相关资产的探测结果、漏洞信息等信息将通过本控制台进行关联展示。

- 我已阅读并同意 [《暴露面管理服务授权书》](#)
- 我已阅读并同意以上开通说明

请先查看 [《暴露面管理服务授权书》](#) 后，才可以开启试用

确定

取消

# 查看互联网暴露面

最近更新时间：2025-01-06 14:09:12

多云安全治理服务将通过资产配置梳理的方式，对云上网络设备、云服务器、数据库等资源进行关联分析，绘制您云上的互联网暴露面状态。您可以通过以下步骤查看并治理互联网暴露面。

## 特殊说明

此功能为额外付费功能，当前限时免费提供给已购买多云安全治理服务的用户使用。本次限免截止时间暂定为2025年03月31日。付费使用时间待定，后续我们将发布相关公告并通过站内信、邮件等方式提前通知您。

## 数据统计

- 登录 [多云安全治理服务控制台](#)，在左侧菜单栏中，单击互联网暴露面。
- 在互联网暴露面-数据统计模块中，支持从开放状态、资产类型、改进方向等维度进行互联网暴露面的数据统计。

状态	资产类型					改进方向			总计
	负载均衡	弹性公网 IP	WAF	数据库公网连接...	其他	高危端口 ⓘ	非标端口 ⓘ	待接入 WAF ⓘ	
开放	2	6	0	0	137	64	129	18	145
白名单	2	1	0	0	56	56	57	0	59
关闭	4	0	0	0	4	1	5	0	8
总计	8	7	0	0	197	121	191	18	212

统计维度	说明
开放状态	<ul style="list-style-type: none"><li>开放：完全对互联网开放。</li><li>白名单：仅对白名单地址段开放。</li><li>关闭：无法访问。</li></ul>
资产类型	分为负载均衡、弹性公网 IP、WAF、数据库公网连接地址、其他。
改进方向	<ul style="list-style-type: none"><li>高危端口：根据高风险服务及对应的惯例端口号设定。</li><li>非标端口：未接入 WAF 或非 80，443 的端口将被视为非标端口。</li><li>待接入 WAF：未接入 WAF 的80/443端口。</li></ul>

3. 在数据统计模块中，您可以通过筛选云账号，来了解不同云账号的数据统计结果。

互联网暴露面

数据统计

请选择云厂商-云账号  请选择项目或资源组

	资产类型					改进方向			总计
	负载均衡	弹性公网 IP	WAF	数据库公网连...	其他	高危端口 ⓘ	非标端口 ⓘ	待接入 WAF ⓘ	
阿里云	2	6	0	0	137	64	129	18	145
腾讯云	2	1	0	0	56	56	57	0	59
关闭	4	0	0	0	4	1	5	0	8
总计	8	7	0	0	197	121	191	18	212

## 数据查询

在 [互联网暴露面-数据查询模块](#) 中，您可以查看到面向互联网暴露的端口列表，支持通过云账号、暴露资产类型、域名、IP、端口、开放状态、风险类型等多种筛选方式。

数据查询

请选择云厂商-云账号  请选择项目或资源组  请选择暴露资产类型  请输入域名  请输入 ip  请输入端口范围  请选择状态  请选择风险类型

云账号信息	域名	IP 地址	实例名	资源信息	端口范围	开放状态	探测结果	操作
多...	-	123.1	sh	云服务器	22	开放	1	暴露路径
多...	-	1.1 30	-	弹性公网IP ei...	22	开放	0	暴露路径
多...	testcd	.com	testcd	内容分发网络 CDN cd...	8080	开放	0	暴露路径

参数名称	说明
云厂商-云账号	云账号列表源自您授权的云账号。
暴露资产类型	对互联网暴露端口的云产品类型。

域名	暴露资产的域名信息。
IP	暴露资产的 IP 信息。
端口范围	暴露资产的端口信息。
状态	<ul style="list-style-type: none"> <li>● 开放：完全对互联网开放。</li> <li>● 白名单：仅对白名单地址段开放。</li> <li>● 关闭：无法访问。</li> </ul>
改进方向	<ul style="list-style-type: none"> <li>● 高危端口：根据高风险服务及对应的惯例端口号设定。</li> <li>● 非标端口：未接入 WAF 或非 80, 443 的端口将被视为非标端口。</li> <li>● 待接入WAF：未接入 WAF 的80/443端口。</li> </ul>

## 查看“暴露面管理服务”探测结果

1. 若您开启了“暴露面管理服务”的联动，支持在 [互联网暴露面-数据查询模块](#) 查看探测结果。

**数据查询**

云账号信息	域名	IP 地址	实例名	资源信息	端口范围	开放状态	探测结果	操作
	-	12.30	sh-	云服务器 ins-	22	开放	1	<a href="#">暴露路径</a>

2. 单击探测结果的数字，即可查看端口服务、漏洞信息、弱口令、网站后台等。

**探测结果** ✕

[端口服务](#)
[漏洞信息](#)
[弱口令](#)
[网站后台](#)

端口	服务	组件	banner	是否高危	创建时间	更新时间
22	ssh	-	-	否	2024-10-08 17:16:57	2024-10-31 10:59:10

共 1 条 10 条 / 页

## 查看暴露路径

1. 在 [互联网暴露面-数据查询模块](#) 中，每一条暴露面数据，均支持查看暴露路径。

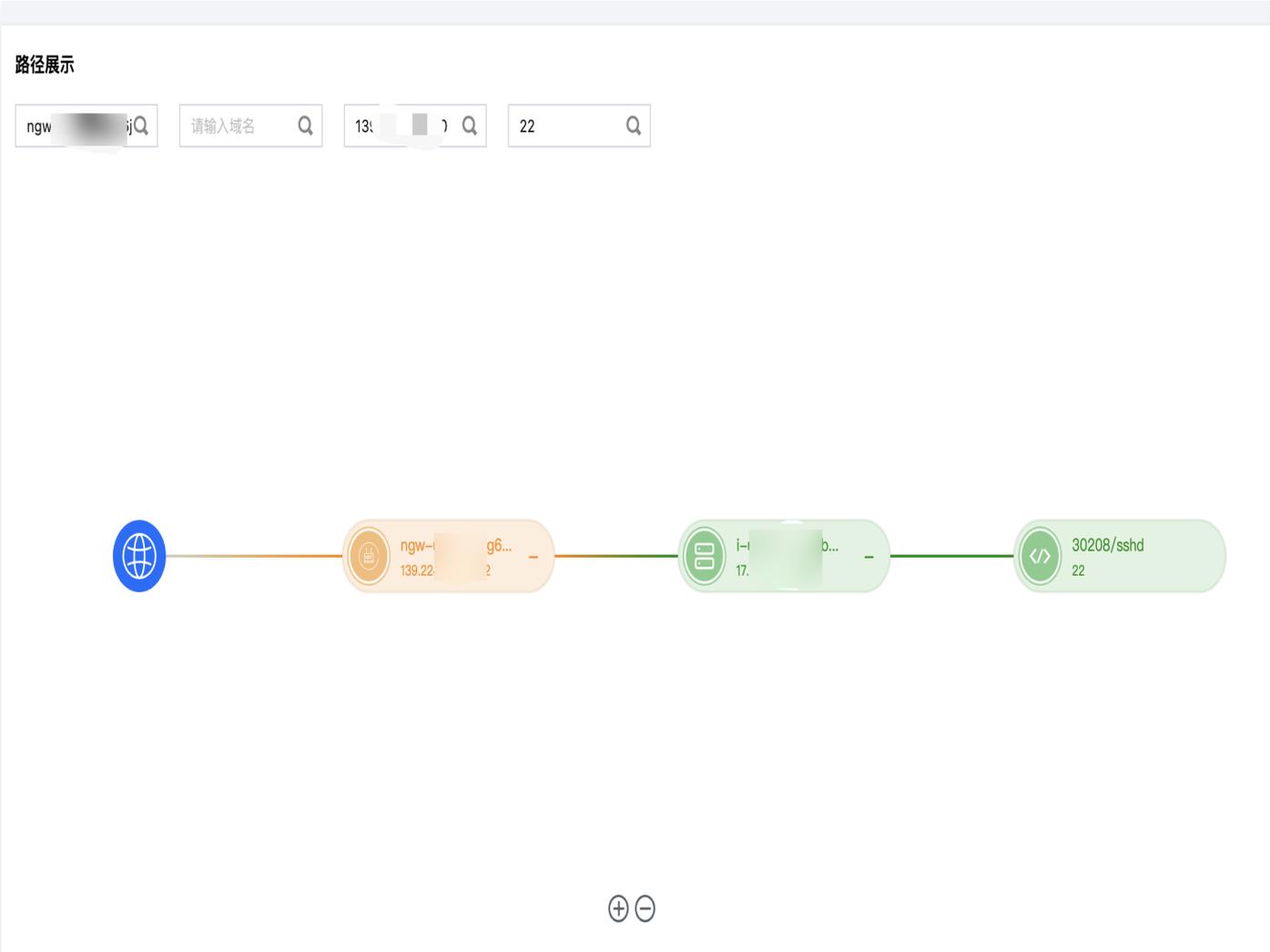
数据查询

请选择云厂商-云账	请选择项目或资源	请选择暴露资产类	请输入域名	请输入 ip	请输入端口范围	请选择状态	请选择风险类型
-----------	----------	----------	-------	--------	---------	-------	---------

云账号信息	域名	IP 地址	实例名	资源信息	端口范围	开放状态	探测结果	操作
安	-	12. . . 0	sha	云服务器 ins- . . . 4	22	开放	1	暴露路径

2. 单击暴露路径，将打开新标签页展示暴露路径。



- 数据展示
- [互联网节点状态](#)
  - [路径节点信息](#)
  - [服务器列表](#)
  - [服务器进程](#)
  - [服务器漏洞](#)
  - [服务器高危基线](#)

# 检索暴露路径

最近更新时间：2025-01-06 14:09:12

支持对暴露路径任意节点（网络设备、云服务器、云数据库等）的检索能力，输入节点的信息，如实例 ID、域名、IP、端口后，将以树状图的形式展示包含相应资产节点的所有路径。

## 特殊说明

此功能为额外付费功能，当前限时免费提供给已购买多云安全治理服务的用户使用。本次限免截止时间暂定为2025年03月31日。付费使用时间待定，后续我们将发布相关公告并通过站内信、邮件等方式提前通知您。

## 检索路径

1. 登录 [多云安全治理服务控制台](#)，在左侧菜单栏中，单击**暴露路径**。
2. 在暴露路径-路径展示模块中，支持实例 ID、域名、IP、端口的检索，根据信息展示路径。

路径展示

ngw-...bj Q 请输入域名 Q 13: ... ) Q 22 Q



数据展示

- [互联网节点状态](#)
- 路径节点信息
- 服务器列表
- 服务器进程
- 服务器漏洞
- 服务器高危基线

检索字段说明

参数名称	说明	
实例 ID	待检索资源的实例 ID。	实例 ID、域名、IP 必须填写其中之一。
域名	待检索资源的域名。	
IP	待检索资源的 IP。	
端口	待检索资源的端口号。非必填项。	

节点状态说明：节点颜色代表了节点的不同状态。

节点位置	节点说明	节点颜色代表的状态
------	------	-----------

树状图的根节点	互联网 (Internet)	-
第二层节点	互联网节点	<ul style="list-style-type: none"> <li>● 绿色代表对公网开放。</li> <li>● 橙色代表有白名单的对公网开放。</li> <li>● 灰色代表无法访问。</li> </ul>
其余节点	路径节点	<ul style="list-style-type: none"> <li>● 绿色代表节点正常。</li> <li>● 灰色代表节点异常，无法访问。</li> </ul>

3. 鼠标置于节点上，支持查看节点的信息。



## 查看列表信息

在 [暴露路径-数据展示模块](#) 中，可查看暴露路径涉及的互联网节点、路径节点、服务器列表、服务器进程、服务器漏洞、服务器高危基线。

数据展示

[互联网节点状态](#) [路径节点信息](#) [服务器列表](#) [服务器进程](#) [服务器漏洞](#) [服务器高危基线](#)

云账号信息	域名	IP 地址	实例名	资源信息	端口	开放状态
	-	139.2: [redacted]	default_n-[redacted]	NAT网关 ngw-ufj[redacted]	22	<a href="#">白名单</a>

共 1 条 10 条/页

表格名	说明
互联网节点状态	树状图中互联网节点列表，展示详细的数据信息。
路径节点信息	树状图中路径节点列表，展示详细的数据信息。
服务器列表	若树状图中包含云服务器，将展示云服务器的列表，并展示云服务器主机安全终端的状态。数据源自腾讯云主机安全、阿里云云安全中心。
服务器进程	若树状图中包含云服务器，将展示云服务器上主机安全终端采集的进程数据。数据源自腾讯云主机安全、阿里云云安全中心。
服务器漏洞	若树状图中包含云服务器，将展示云服务器上主机安全终端采集的漏洞列表。数据源自腾讯云主机安全、阿里云云安全中心。
服务器高危基线	若树状图中包含云服务器，将展示云服务器上主机安全终端采集的高危基线列表。数据源自腾讯云主机安全、阿里云云安全中心。

# 评估周期管理

最近更新时间：2024-11-11 17:01:52

多云安全治理服务，支持周期运行评估任务，目前支持设置每日在指定时间运行。

## 操作步骤

1. 登录 [多云安全治理服务控制台](#)，在左侧菜单栏中，单击**扫描任务**。
2. 在扫描任务页面，单击**周期运行管理**。



3. 在周期运行管理窗口中，开启每日运行，选择运行时间，单击**确定**。

