

阿里云 应用发现服务

操作指南

文档版本：20190919

法律声明

阿里云提醒您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
	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。	 禁止： 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	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。	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。	单击 确定 。
<code>courier</code> 字体	命令。	执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。
<code>##</code>	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
<code>[]</code> 或者 <code>[a b]</code>	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
<code>{ }</code> 或者 <code>{a b}</code>	表示必选项，至多选择一个。	<code>swich {stand slave}</code>

目录

法律声明.....	I
通用约定.....	I
1 操作概述.....	1
2 准备工作.....	3
2.1 安装采集器.....	3
2.2 安装探针.....	6
2.3 新建项目.....	8
3 控制台指南.....	10
3.1 查看主机信息.....	10
3.2 查看进程信息.....	11
4 参考信息.....	15
4.1 采集周期说明.....	15

1 操作概述

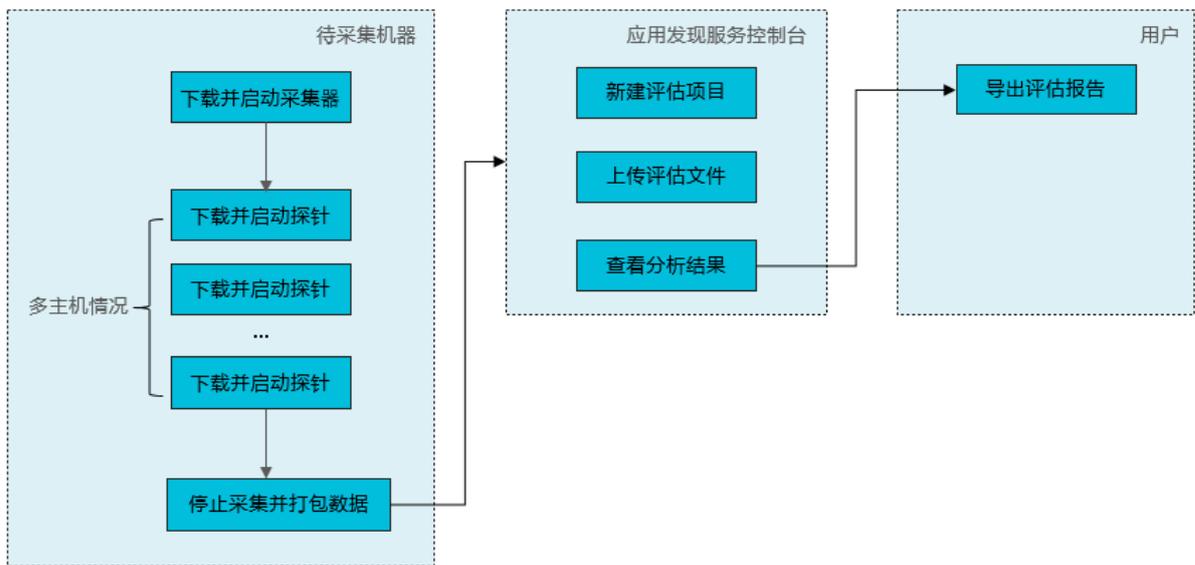
本文将介绍使用应用发现服务自动发现线下 IT 资产、识别主机与进程的网络关系的操作流程。

前提条件

确保主机的操作系统在支持列表中，参见[#unique_4](#)。

操作流程

具体流程如下图所示。



1. [#unique_5](#)

应用发现服务采集器安装在用户机房的中心主机上，其主要作用是接收来自各个探针的数据，并初步汇总。

2. [#unique_6](#)

应用发现服务探针安装在每台普通主机上，其主要作用是抓取主机、进程的元信息、依赖关系以及监控数据，并且将数据发送至采集器。

3. [停止采集并打包数据](#)

完成数据采集后，需将中心主机上采集器收集的数据编译成 ZIP 文件（即采集器离线文件 ZIP 包）并下载至本地。数据采集周期详细说明参见[#unique_8](#)。

4. [#unique_9](#)

在控制台新建项目并将采集器离线文件 ZIP 包上传到控制台后，将以加密形式存入阿里云 OSS 中，再由应用发现服务进行解析、处理。

5. 在控制台查看主机和进程的分析结果，快速了解硬件资产的各项状态：

- 查看主机详情，参见[#unique_10](#)。
- 查看进程详情，参见[#unique_11](#)。

若需进一步分析，可在控制台导出评估报告。

2 准备工作

2.1 安装采集器

使用应用发现服务自动发现线下 IT 资产、识别主机与进程的网络关系时，需要在局域网内的中心主机上安装采集器，用于收集整理探针采集的数据并形成日志文件。本文将介绍如何安装应用发现服务采集器。

前提条件

- 确保您的主机的操作系统在支持列表中，参见[#unique_4](#)。
- 已在待安装采集器的中心主机上安装 1.8 及以上版本的 [JDK](#)。

操作步骤

1. 登录[应用发现服务控制台](#)，然后在左上角选择地域。
2. 在概览页单击新手引导，然后在新手引导页面查看并保存 license。



3. 在概览页单击下载采集器。



4. 将安装包拷贝到待安装采集器的服务器上，并执行以下命令解压安装包。

```
unzip apds-collector.zip
```

5. 在解压文件中按需修改 `apds-collector.config` 文件中的参数。

- a) 以编辑模式进入 `apds-collector.config` 文件。

```
vi apds-collector.config
```

- b) 按 `i` 键开始编辑，按需修改各参数为真实配置。各参数含义如下：

表 2-1: 参数含义

参数	含义
<code>server.port</code>	RESTful api 的端口号
<code>agent.port</code>	连接探针的端口号
<code>logger.level</code>	日志等级
<code>file.rolling.interval</code>	离线文件中单个数据文件滚动的周期
<code>file.max.size.mb</code>	离线文件总大小上限，达到上限要开始滚动数据文件（删除旧的数据文件写新的数据文件），单位为：MB
<code>file.path</code>	生成采集器离线文件的路径
<code>file.zip.path</code>	压缩采集器离线文件的路径
<code>file.max.time.hour</code>	离线文件采集的最大时长，达到时长后会开始自动滚动（删除旧的数据文件写新的数据文件），单位为：小时
<code>encrypt</code>	是否数据加密
<code>license</code>	加密的密钥，若不加密可以不填。 <code>license</code> 在控制台查看，每个账户拥有唯一的 <code>license</code> 。
<code>agent.survival.time.hour</code>	探针上报的最大时长（以第一个探针上报开始算采集起始点），单位为：小时。达到时长后会自动通知所有探针停止采集上报。若要探针再次开采，采集器需调用 <code>clean</code> 和 <code>startAll</code> API
<code>loggingRoot</code>	日志根路径



说明:

所有配置参数均可缺省。

- c) 按 Esc 键结束编辑。
- d) 输入 `:wq!` 命令保存并退出 `apds-collector.config` 目录。

6. 执行以下命令启动采集器。

```
sh start.sh
```

结果验证

执行 `less apds-collector.log` 命令在 `apds-collector.log` 查看采集器运行日志，若出现以下日志则表示启动成功。

```
bind success, ip : *.*.*.*.**, port : ****
```

后续步骤

采集器安装完成后，您还需要进行以下操作：

- 安装探针，参见[#unique_6](#)。
- 在应用发现服务控制台新建项目，参见[#unique_9](#)。

采集器和探针管理

- 通过采集器安装包中的脚本文件来进行采集器和探针管理，各文件说明如下：

表 2-2: 文件说明

文件名	含义
<code>apds-collector.log</code>	记录采集器运行日志。
<code>stop.sh</code>	停止采集器。
<code>compress.sh</code>	压缩采集器离线文件。运行脚本后，所有探针将停止采集数据，采集器离线文件开始打包，完成后所有探针将恢复采集。还可以通过执行 <code>http://127.0.0.1:8082/compress</code> 来完成此操作。
<code>status.sh</code>	查看探针链接状态。还可以通过执行 <code>http://127.0.0.1:8082/status</code> 来完成此操作。
<code>stopAllAgentCollect.sh</code>	使所有探针停止采集数据。还可以通过执行 <code>http://127.0.0.1:8082/stopAll</code> 来完成此操作。

文件名	含义
<code>startAllAgentCollect.sh</code>	使所有探针开始采集数据。还可以通过执行 <code>http://127.0.0.1:8082/startAll</code> 来完成此操作。
<code>reset.sh</code>	清空本地采集器离线文件。还可以通过执行 <code>http://127.0.0.1:8082/clean</code> 来完成此操作。

- 通过采集器的 RESTful API 进行探针和采集器管理，具体 API 参考含义如下：

表 2-3: 采集器的 RESTful API 列表

RESTful API	说明
<code>http://127.0.0.1:8082/start?vpcId=xxx&clientIp=yyy</code>	指定某个探针开始采集上报数据，探针启动后默认是采集上报状态，也可以让其停止采集然后再次开启采集，如果探针重启后会默认变成采集上报状态。需指定探针的 <code>vpcId</code> 和 <code>clientIp</code> 。
<code>http://127.0.0.1:8082/stop?vpcId=xxx&clientIp=yyy</code>	指定某个探针停止采集上报数据。需指定探针的 <code>vpcId</code> 和 <code>clientIp</code> 。
<code>http://127.0.0.1:8082/status</code>	查看目前连接在线的所有探针的 <code>vpcId</code> 、 <code>clientIp</code> 和对应的探针状态。
<code>http://127.0.0.1:8082/compress</code>	开始对本地采集的数据文件打压缩包，上传到 web 的是压缩包。
<code>http://127.0.0.1:8082/clean</code>	清空本地的数据文件，此时 <code>agent.survival.time.hour</code> 重新开始计算。
<code>http://127.0.0.1:8082/startAll</code>	使所有探针开始采集上报数据。
<code>http://127.0.0.1:8082/stopAll</code>	使所有探针停止采集上报数据。
<code>http://127.0.0.1:8082/help</code>	API 帮助提示信息。

2.2 安装探针

在局域网中心主机上安装采集器后，需要在所有普通主机上分别安装探针以抓取主机、进程的元信息和监控数据，以及各应用组件间的依赖关系等数据。本文将介绍如何安装应用发现服务探针。

前提条件

- 确保您的主机的操作系统在支持列表中，参见[#unique_4](#)。
- 已在中心主机上安装采集器，参见[#unique_5](#)。

操作步骤

1. 登录[应用发现服务控制台](#)，然后在左上角选择地域。
2. 在概览页单击新手引导，然后在新手引导页面查看并保存 license。



3. 在概览页单击下载探针，然后根据您的主机规则选择下载探针的类型（Linux 32 位或 Linux 64 位）。



4. 将安装包拷贝到待安装探针的服务器上，并执行以下命令解压安装包。

```
unzip apds-agent.zip
```

5. 执行以下命令启动探针。

```
sh start.sh <ip> <port> <license>
```



说明：

<ip> 为安装采集器的主机 IP 地址；<port> 为采集器 agent.port；<license> 为真实 license。

例如：

```
//172.**.**.138 为安装采集器的主机 IP 地址  
//9528 为采集器 agent.port  
//7E1023431D**** 为 license  
sh start.sh 172.**.**.138 9528 7E1023431D****
```

预期结果

执行 `less apds-agent.log` 命令在 `apds-agent.log` 文件中查看探针运行日志，若出现以下日志则表示启动成功。

```
Start transport service successfully
```

后续步骤

采集数据结束后，需要在控制台新建项目并上传采集器离线文件，应用发现服务才能进行分析和识别。参见[#unique_9](#)。

您还可以参考以下信息来管理探针：

- 在同级目录的 `apds-agent.log` 文件查看运行日志。
- 若需停止探针，则运行 `stop.sh` 脚本。

2.3 新建项目

当数据采集结束后，需将中心主机上采集器收集的数据编译成 ZIP 文件（即采集器离线文件 ZIP 包）。在应用发现服务控制台新建项目并上传采集器离线文件 ZIP 包后，应用发现服务将对文件进行解析和处理。

前提条件

- 在中心主机上安装采集器，参见[#unique_5](#)。
- 在普通主机上安装探针，参见[#unique_6](#)。
- 在安装采集器的中心主机上执行 `sh compress.sh` 命令将采集器收集的数据编译成一个 ZIP 文件（即采集器离线文件 ZIP 包），并将 ZIP 文件下载至本地。



说明：

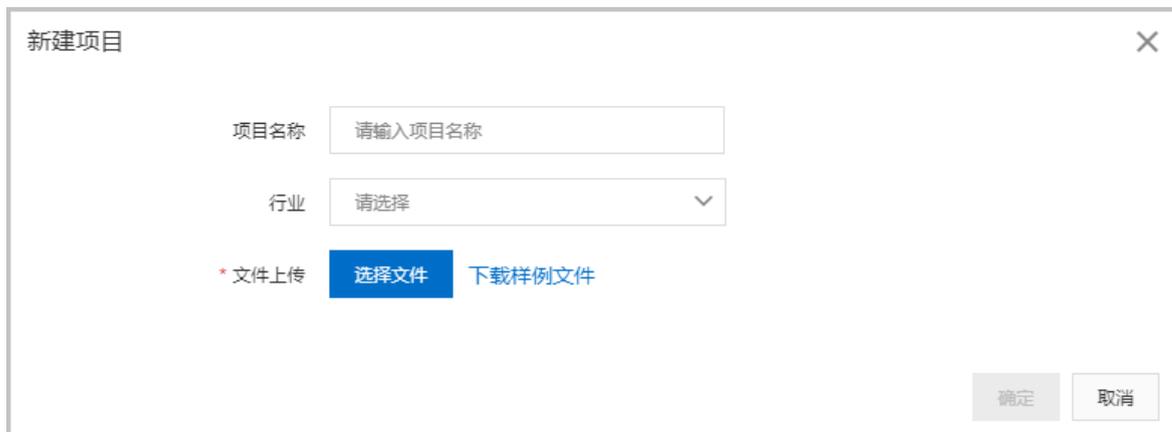
编译后的 ZIP 文件在配置 `apds-collector.config` 文件中 `file.zip.path` 的路径下。

操作步骤

1. 登录[应用发现服务控制台](#)。
2. 在概览页单击新建项目。



3. 在新建项目对话框中填写项目名称，选择行业，并单击选择文件上传采集器离线文件 ZIP 包，然后单击确认。



说明:

- 行业信息将用于数据分析，应用发现服务将针对所在行业为您推荐适用的云服务（待上线）。
- 采集器离线文件 ZIP 包需在安装采集器的中心主机上获取，参见[停止采集并打包数据](#)。若您没有采集器离线文件 ZIP 包，可以下载样例文件再新建项目，体验应用发现服务的自动识别分析功能。

预期结果

项目上传成功后，应用发现服务将检测分析项目中的主机数和进程数并展示在概览页面。



说明:

若采集器离线文件解析错误，请按照错误码说明来解决问题，参见[错误码说明](#)。

后续步骤

- 查看主机详情，参见[#unique_10](#)。
- 查看进程详情，参见[#unique_11](#)。

3 控制台指南

3.1 查看主机信息

成功创建项目后，应用发现服务将自动分析识别采集器离线文件中的数据。您可以查看主机信息了解该主机详情、主机上运行的进程，以及与其它主机之间的网络拓扑关系。

功能入口

1. 登录[应用发现服务控制台](#)。
2. 在控制台左上角选择地域。
3. 请选择一种方式进入主机页面。
 - 在概览页面我的项目区域通过关键字搜索目标项目，然后单击项目卡片的主机图标。
 - 在控制台左侧导航中选择发现 > 主机，在主机页面左上角选择对应的项目。

功能介绍

在主机页面，展示了当前项目下每台主机的主机名、系统规格、主机 IP、CPU 占用率、内存占用率以及关联的主机数量等信息。

主机名	系统规格	主机IP	CPU	Memory	关联主机	操作
...	2 vCPU 4 GiB	...	最小: 1.21% 最大: 3.17% 平均: 1.72%	最小: 33.43% 最大: 33.48% 平均: 33.45%	已接入: 1 未接入: 22	查看详情
...	2 vCPU 4 GiB	...	最小: 1.41% 最大: 3.36% 平均: 1.98%	最小: 34.03% 最大: 34.11% 平均: 34.08%	已接入: 1 未接入: 12	查看详情
...	2 vCPU 4 GiB	...	最小: 0.20% 最大: 1.27% 平均: 0.30%	最小: 4.29% 最大: 4.30% 平均: 4.30%	已接入: 0 未接入: 3	查看详情
...	4 vCPU 8 GiB	...	最小: 0.68% 最大: 2.05% 平均: 1.07%	最小: 30.55% 最大: 30.60% 平均: 30.57%	已接入: 0 未接入: 21	查看详情

- 在页面右上角单击导出，即可导出主机详情的 csv 文件。
- 在目标主机关联主机列单击关联主机的数量，可查看关联主机的主机名和 IP 等信息。
- 在目标主机操作列单击查看详情即可查看主机的基本信息、入口连接、出口连接和在主机上运行的进程信息等。

表 3-1:

主机详情		说明
基本信息	主机名	主机实例名

主机详情		说明
	IP	主机的 IP 地址
	主机规格	主机的 CPU 大小
入口连接		调用该主机的所有主机及其端口
出口连接		该主机调用的所有主机及其端口
进程		该主机上运行的进程信息

3.2 查看进程信息

成功创建项目后，应用发现服务将自动分析识别采集器离线文件中的数据。您可以查看进程信息了解该进程详情、所属主机、命令行、进程的上下游组件以及资源占用情况。

功能入口

1. 登录[应用发现服务控制台](#)。
2. 在控制台左上角选择地域。
3. 任选一种方式进入主机页面。
 - 在概览页面我的项目区域搜索目标项目资源卡片，然后单击资源卡片的进程图标。
 - 在控制台左侧导航中选择发现 > 进程，在进程页面左上角选择对应的项目。

功能介绍

进程页面从聚合、拓扑、明细三个方面展示了进程信息。

- 在聚合页签中，将当前项目下名称相同的进程聚合为一类，展示了各类进程的进程名、进程数量、规格和关联进程等信息。

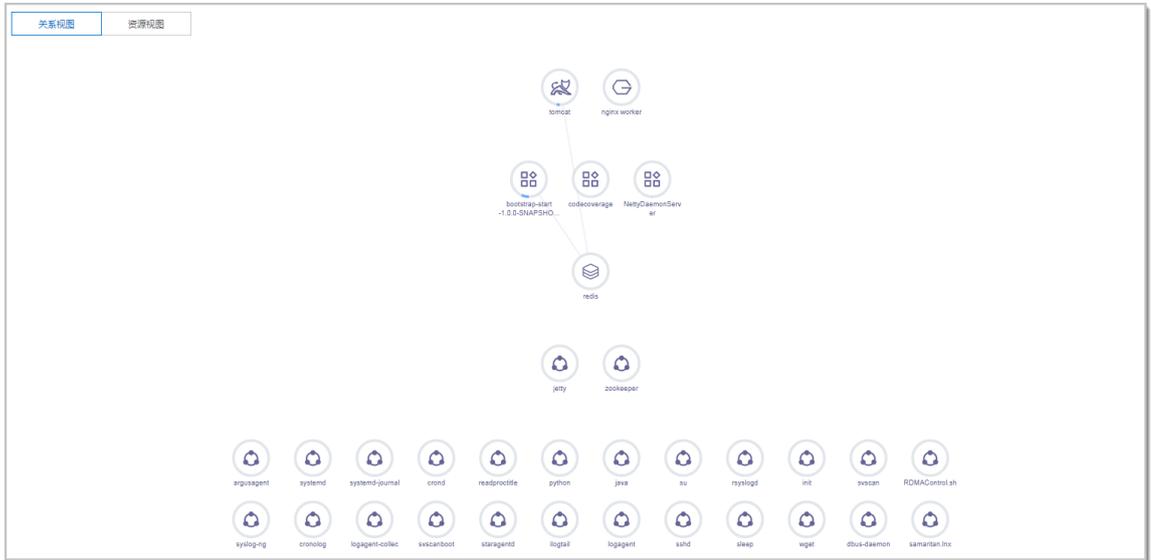
图 3-1: 聚合

进程名	进程数量	规格	关联进程	操作
nginx worker	9	24 vCPU 8 GiB Linux	未接入: 4	查看详情
crond	4	24 vCPU 8 GiB Linux		查看详情
/usr/local/ilogtail/ilogtail	2	24 vCPU 8 GiB Linux		查看详情
logagent-collector	2	24 vCPU 8 GiB Linux		查看详情
/bin/sh	2	24 vCPU 8 GiB Linux		查看详情
/opt/taobao/install/cronolog/...	2	24 vCPU 8 GiB Linux		查看详情
ilogtail	2	4 vCPU 8 GiB		查看详情
sshd:	2	24 vCPU 8 GiB Linux	未接入: 1	查看详情
su	2	4 vCPU 8 GiB Linux		查看详情
logagent-collec	2	4 vCPU 8 GiB		查看详情
supervising	1	24 vCPU 8 GiB Linux		查看详情
/home/staragent/plugins/log...	1	24 vCPU 8 GiB Linux		查看详情

- 单击目标进程关联进程栏的已接入或未接入，即可查看该类进程已被识别的关联进程信息或未被识别的关联进程所在主机 IP 信息。
- 单击目标进程操作栏的查看详情，即可查看该类所有进程的进程 ID、主机名、启动时间和命令行等信息。

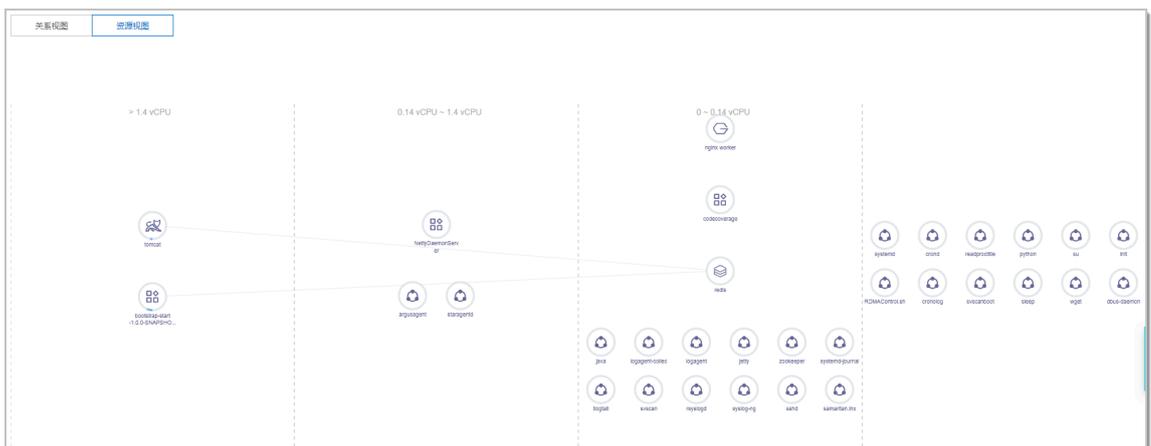
- 在拓扑页签中可自由切换关系视图和资源视图，直观地展示了进程的上下游组件以及资源占用情况。
- 关系视图页面展示了进程的上下游组件及其依赖关系。

图 3-2: 关系视图



- 资源视图页面中根据实际的资源占用来对进程进行分层，直观地展示了进程的占用消耗情况。

图 3-3: 资源视图



在拓扑图中单击任一进程，可查看该进程的进程 ID、主机名、启动时间和命令行等信息。

- 在明细页面，展示了当前项目下的所有进程名、类型、所属主机、命令行、PID、CPU、Memory 和关联进程等信息。

图 3-4: 明细

进程名	类型	主机名	命令行	PID	CPU	内存	关联进程	操作
codecoverage	APP	...	/opt/taobao/install...	13753	最小: 0.00% 最大: 0.20% 平均: 0.06%	最小: 1.30% 最大: 1.31% 平均: 1.30%	已接入: 0 未接入: 1	查看详情
NettyDaemonServer	APP	...	/opt/taobao/java/b...	114168	最小: 0.00% 最大: 0.70% 平均: 0.14%	最小: 2.85% 最大: 2.91% 平均: 2.85%	已接入: 1 未接入: 1	查看详情
jetty	APP	...	/opt/taobao/install...	122137	最小: 0.00% 最大: 0.40% 平均: 0.08%	最小: 1.35% 最大: 1.35% 平均: 1.35%		查看详情
nginx worker	WEB	...	nginx: worker proces...	31951	最小: 0.00% 最大: 0.40% 平均: 0.02%	最小: 0.17% 最大: 0.17% 平均: 0.17%		查看详情
redis	CACHE/redis-server *:637...	19672	最小: 0.00% 最大: 0.20% 平均: 0.06%	最小: 0.03% 最大: 0.03% 平均: 0.03%		查看详情
nginx worker	WEB	...	nginx: worker proces...	31953	最小: 0.00% 最大: 0.20% 平均: 0.02%	最小: 0.18% 最大: 0.18% 平均: 0.18%		查看详情
nginx worker	WEB	...	nginx: worker proces...	31949	最小: 0.00% 最大: 0.40% 平均: 0.02%	最小: 0.17% 最大: 0.18% 平均: 0.18%		查看详情
tomcat	WEB	...	/opt/taobao/install...	30678	最小: 4.20% 最大: 29.29% 平均: 7.48%	最小: 49.52% 最大: 50.11% 平均: 49.85%	已接入: 2 未接入: 19	查看详情

- 在页面右上角单击导出，即可导出进程详情的 csv 文件。
- 在选择类型右侧单击进程类型，可筛选该类型的进程。
- 在目标主机关联进程列单击关联进程的数量，可查看关联进程的信息。
- 在目标进程操作列单击查看详情，即可查看进程的基本信息、入口连接、出口连接、所属主机等信息。

表 3-2: 进程详情说明

进程详情		说明
基本信息	进程名	该进程的名称
	进程 ID	该进程的 ID
	命令行	该进程的命令行详情
	进程父 ID	父进程的 ID
入口连接		调用该进程的所有进程及其端口
出口连接		该进程调用的所有进程及其端口
主机		该进程所属主机名

4 参考信息

4.1 采集周期说明

采集器离线文件的数据准确性由数据的采集周期决定。本文将帮助您了解不同场景下使用应用发现服务的数据采集周期。

发现和识别线下 IT 资产的采集周期

若只需使用应用发现服务自动发现和识别线下 IT 资产，则确保所有探针在线并有同时上传数据的时间点即可。应用发现服务解析数据时，会将探针数量最多的时间点作为本次解析的时间点。

发现和识别主机与进程的网络关系的采集周期

若需使用应用发现服务发现和识别主机与进程的网络关系，则需确保所有探针在线并同时上传数据 30 分钟。发现和识别主机与进程的网络关系的采集周期中包含对线下 IT 资产的采集。