安全云脑

最佳实践

文档版本 01

发布日期 2023-06-20

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 数据转入转出操作指导

1.1 场景说明

安全云脑除默认支持的云服务日志接入外，还具备采集管理功能，使用该功能可对日志进行采集、解析、转出、可视化查询、威胁建模等。

在此过程中，需要安装Agent组件，打通安全云脑与ECS通道。还需要安装Logstash组件，用于数据接入、解析、转出等操作。

本场景将介绍以下两种接入操作指导：

- **使用默认解析方式快速接入数据**：使用安全云脑数据采集中默认的解析方式快速接入数据。
- **使用自定义解析方式接入数据**：根据您的需要通过自定义解析方式接入数据。

1.2 约束与限制

安全云脑采集管理功能有以下约束与限制：

- 数据采集的Agent目前仅支持运行在某些版本的EulerOS的Linux系统的主机上，具体请参见**支持的操作系统**。
- 安装Agent时，在控制台中查看信息时，仅支持使用IAM账号登录。

支持的操作系统

数据采集的Agent目前仅支持运行在Linux系统x86_64架构的ECS主机上。ECS主机支持以下操作系统类型：Huawei Cloud EulerOS 2.5、Huawei Cloud EulerOS 2.9、EulerOS 2.5、EulerOS 2.9、CentOS 7。

1.3 快速接入安全云脑

本部分介绍通过**UDP**的方式采集ECS中的日志，再使用采集管理中提供的**默认解析器配置**进行日志解析，并将解析完的数据接入到安全云脑管道。接入后，可在“安全分析”页面进行查询。

前提条件

已获取登录控制台的IAM账号和密码。

步骤一：购买 ECS

购买弹性云服务器详细操作请参见**购买ECS**。

⚠ 注意

数据采集的Agent目前仅支持运行在Linux系统x86_64架构的ECS主机上。ECS主机支持以下操作系统类型：Huawei Cloud EulerOS 2.5、Huawei Cloud EulerOS 2.9、EulerOS 2.5、EulerOS 2.9、CentOS 7.9。

购买时，需注意操作系统和版本的选择。

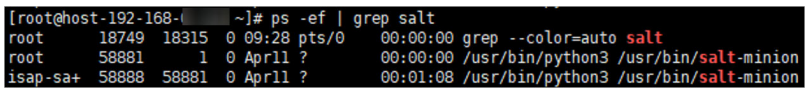
图 1-1 选择操作系统版本

步骤二：安装 Agent

Agent是维持安全云脑与ECS通信的客户端软件，具有命令下发，心跳数据上报的能力。

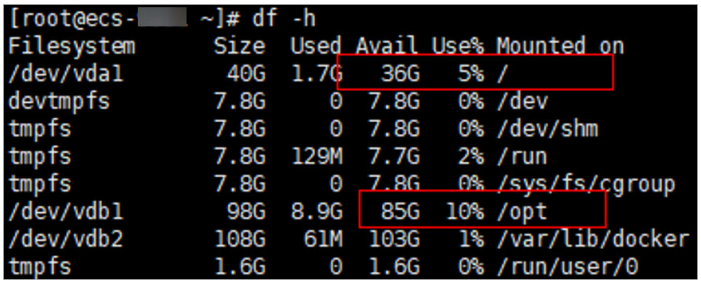
1. 安装Agent前预检查。
   a. 安装Agent前，执行**ps -ef | grep salt**命令，检查主机之前的salt-minion进程是否残留。
      - 如果有，请先关闭。
      - 如果没有，请继续执行**1.b**。

      图 1-2 检查进程

   b. 安装Agent前，执行**df -h**命令，检查磁盘的根目录盘或者opt盘预留50G以上，CPU核数需要2核以上，内存需要4G以上。

      图 1-3 检查磁盘

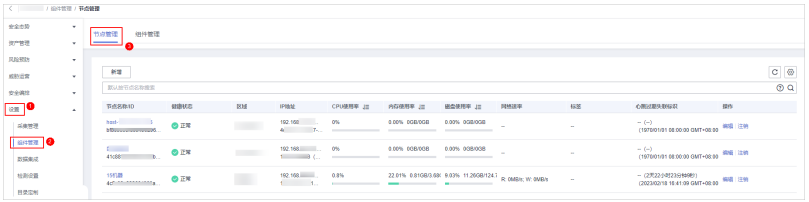
如果内存不足，请关闭一些高内存占用的应用程序或扩充内存容量后再进行安装。扩容操作详情请参见**变更服务器规格**。

2. 登录管理控制台。
3. 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。
4. 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 1-4 进入目标工作空间管理页面

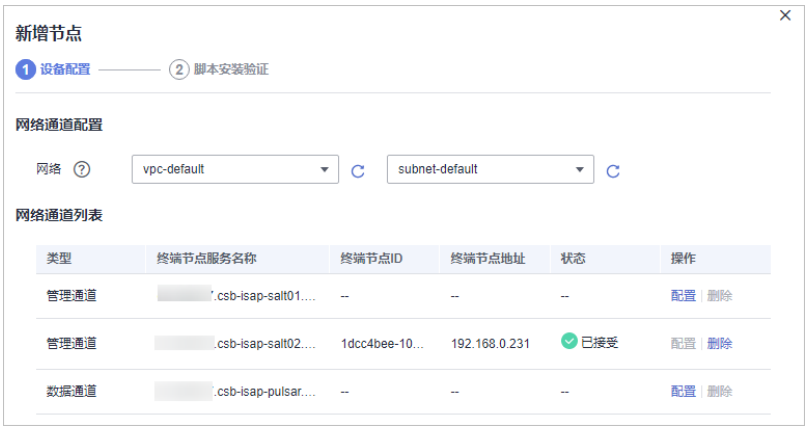
5. 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 1-5 进入节点管理页面



6. 在节点管理页面中，单击“新增”，页面右侧弹出新增节点页面。
7. 在新增节点页面中，配置设备。

图 1-6 新增节点



a. 在网络通道配置栏中，选择网络通道所属的虚拟私有云和子网。
b. 在网络通道列表中，单击通道“操作”列的“配置”，并在弹出的确认框中，单击“确认”。

8. 单击页面右下角“下一步”，进入脚本安装验证页面后，单击 复制安装Agent的命令。

9. 远程登录待安装Agent的ECS。
   - **华为云主机**
     - 您可以登录弹性云服务器控制台，在“弹性云服务器”列表中，单击“远程登录”登录主机，详细操作请参见**在云服务器控制台上登录主机**。
     - 若您的主机已经绑定了弹性IP，您也可以使用远程管理工具（例如：PuTTY、Xshell等）登录主机，并使用root账号在主机中安装Agent。
   - **非华为云主机**

     请使用远程管理工具（例如：PuTTY、Xshell等）连接您服务器的弹性IP，远程登录到您的服务器。
10. 执行**cd /opt/cloud**命令，进入安装目录。

> **注意**
>
> 安装路径建议为“/opt/cloud”，本章节也以此路径为例进行介绍。如需安装在其他自定义路径中，请根据路径修改。

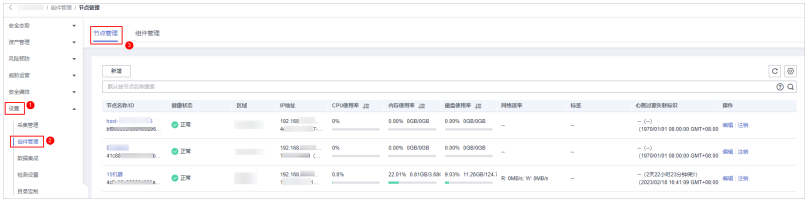
11. 粘贴复制的**8**复制的安装命令，以root权限执行，在ECS中安装Agent。
12. 根据界面提示，输入登录控制台的IAM账号和密码。
13. 若界面回显类似如下信息时，则表示Agent安装成功。

```
install isap-agent successfully
```

步骤三：新增节点

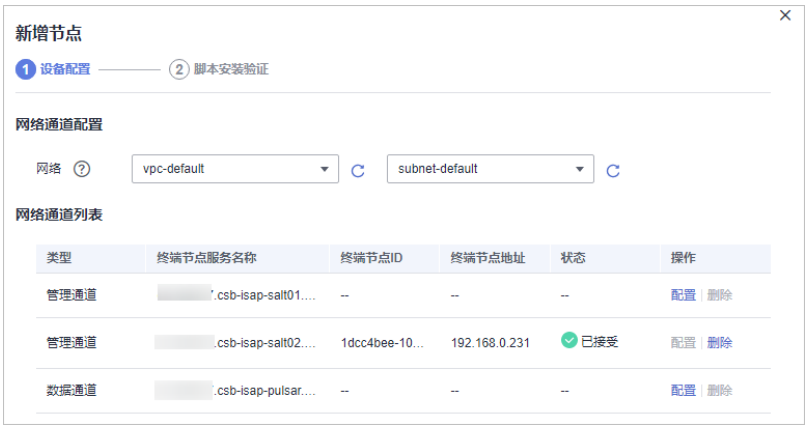
1. 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 1-7 进入节点管理页面



2. 在节点管理页面中，单击“新增”，页面右侧弹出新增节点页面。
3. 在新增节点页面中，配置设备。

图 1-8 新增节点



a. 在网络通道配置栏中，选择网络通道所属的虚拟私有云和子网。

b. 在网络通道列表中，单击通道“操作”列的“配置”，并在弹出的确认框中，单击“确认”。

4. 单击页面右下角“下一步”，进入“脚本安装验证”页面。
5. 确认已安装后，单击页面右下角“确认”。

步骤四：配置组件

Logstash是一个开源数据收集引擎，具有实时流水线功能，Logstash可以动态采集来自不同来源的数据，将其转换并输出到不同目的。

1. 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，选择“组件管理”页签，进入组件管理页面。

图 1-9 进入组件管理页面

2. 在组件管理页面中，单击待查看组件右上角“编辑配置”，右侧将弹出该组件的配置管理页面。
3. 在节点配置栏中，单击节点列表左上角“添加”，并在弹出的“添加节点”框中选择节点后，单击“确认”。
4. 单击页面右下角“保存并应用”。

步骤五：（可选）新增管道

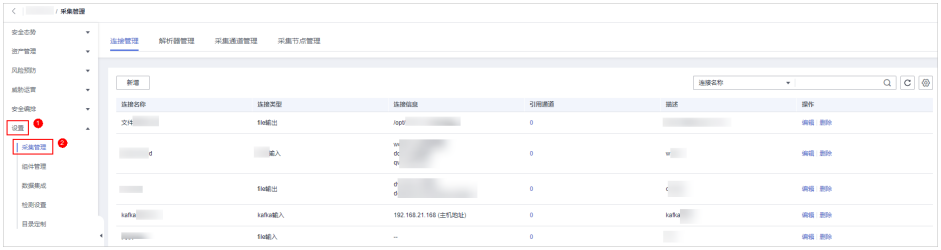
新增用于转入数据的存储管道，详细操作请参见**创建管道**。

步骤六：新增数据连接（来源、目的）

新增数据连接，包含数据来源、以及数据解析后转出位置。

1. 在左侧导航栏选择“设置 > 采集管理”，默认进入连接管理页面。

图 1-10 进入采集管理页面



2. 新增数据连接来源。
   a. 在“连接管理”页面中，单击“新增”，进入选择数据连接页面。
   b. 在“来源”页签中，选择数据源类型的来源“用户数据协议 Udp”，并配置UDP参数信息。

图 1-11 数据源来源

表 1-1 数据源来源

参数名称	参数说明
名称	自定义数据连接来源的名称。
描述	自定义数据连接来源的描述信息。
端口	设置需要采集的端口。
codec	设置编码格式，可设置为json或plain。
可选参数	自定义其他可选参数信息。

   c. 设置完成后，单击页面右下角“确认”。
3. 新增数据源连接目的。
   a. 在采集管理页面选择“连接管理”页签，进入连接管理页面后，单击“新增”，进入选择数据连接页面。

b. 选择“目的”页签中，选择数据源类型的目的“云脑管道 Pipe”，并配置管道信息。

图 1-12 数据源接入目的地

表 1-2 数据源接入的目的地

参数名称	参数说明
名称	自定义数据源目的名称。
描述	自定义数据源目的描述信息。
类型	此处选择“租户”。
管道	选择**步骤五：（可选）新增管道**创建的管道名称。
域账户	输入IAM域账号。
用户名	输入IAM用户名。
密码	输入IAM账号密码。
可选参数	自定义其他可选参数信息。

c. 设置完成后，单击页面右下角“确认”。

步骤七：新增采集通道

新增采集通道的目的在于将输入-解析-输出连接形成管道，并将管道下发至采集节点（安装Agent和Logstash的节点），完成此步骤后，整个数据接入转出真正开始运行。

1. 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

图 1-13 进入采集通道管理页面

2. 新增分组。
   a. 在采集通道管理页面中，单击“分组列表”右侧的。
   b. 输入分组名称，并单击，完成新增。
3. 在采集通道管理页面的分组列表右侧，单击“新增”，进入新增采集通道页面。
4. 在“基础配置”页面中，配置基础信息。

表 1-3 基础配置参数说明

参数名称		参数说明
基础信息	名称	自定义采集通道名称。
	通道分组	选择2新增的分组。
	（可选）描述	输入采集通道描述信息。
来源配置	源名称	选择**步骤六：新增数据连接（来源、目的）**新增的来源。
目的	目的名称	选择**步骤六：新增数据连接（来源、目的）**新增的目的。

5. 基础配置完成后，单击页面右下角“下一步”，进入“解析器配置”页面。
6. 在“解析器配置”页面中，选择“快速接入”。
   快速接入即会将原始日志全部放入message字段。
7. 解析器配置完成后，单击页面右下角“下一步”，进入“运行节点选择”页面。
8. 在“运行节点选择”页面中，单击“新增”，并在弹出的添加节点框中选择节点（安装了Agent和Logstash的节点）后，单击“确认”。
9. 运行节点选择完成后，单击页面右下角“下一步”，进入“通道详情预览”页面。
10. 在“通道详情预览”页面确认配置无误后，单击“确定”。

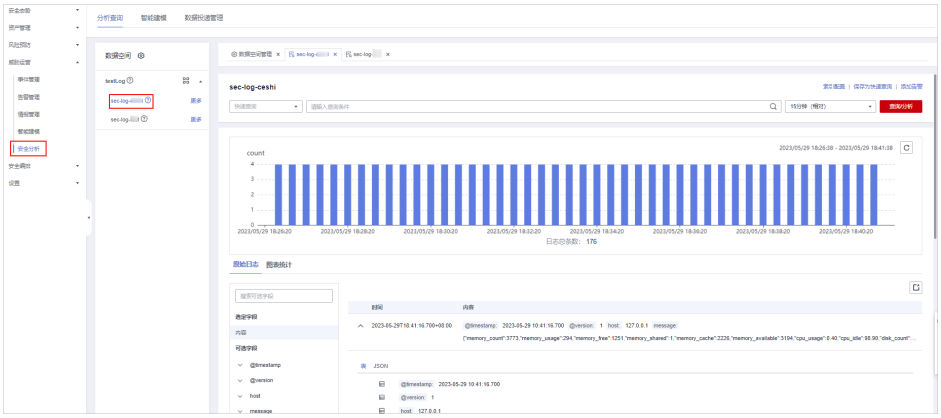
新增采集通道结束后，会对管道进行下发，刷新界面，当健康状态为“正常”，则下发完成。

步骤八：安全查询分析

由于将日志输出至安全云脑管道，因此可在安全云脑中查询。

1. 在左侧导航栏选择“威胁运营 > 安全分析”，默认进入“安全分析”页面。
2. 选择**步骤五：（可选）新增管道**的安全云脑管道，即可在安全云脑界面查看日志解析后的数据。

图 1-14 安全查询分析



1.4 自定义接入安全云脑

通过UDP的方式采集ECS中的日志，将字符串解析成json格式（自定义解析），并将解析完的数据转出至安全云脑管道。接入后，可在“安全分析”页面进行查询，同时可基于解析后的日志进行威胁建模等。

前提条件

已获取登录控制台的IAM账号和密码。

步骤一：购买 ECS

购买弹性云服务器详细操作请参见**购买ECS**。

注意

数据采集的Agent目前仅支持运行在Linux系统x86_64架构的ECS主机上。ECS主机支持以下操作系统类型：Huawei Cloud EulerOS 2.5、Huawei Cloud EulerOS 2.9、EulerOS 2.5、EulerOS 2.9、CentOS 7.9。

购买时，需注意操作系统和版本的选择。

图 1-15 选择操作系统版本

步骤二：安装 Agent

Agent是维持安全云脑与ECS通信的客户端软件，具有命令下发，心跳数据上报的能力。

1. 安装Agent前预检查。
   a. 安装Agent前，执行**ps -ef | grep salt**命令，检查主机之前的salt-minion进程是否残留。

- 如果有，请先关闭。
- 如果没有，请继续执行**1.b**。

图 1-16 检查进程

```
[root@host-192-168-     ~]# ps -ef | grep salt
root      18749  18315  0 09:28 pts/0    00:00:00 grep --color=auto salt
root      58881      1  0 Aprll ?        00:00:00 /usr/bin/python3 /usr/bin/salt-minion
isap-sa+  58888  58881  0 Aprll ?        00:01:08 /usr/bin/python3 /usr/bin/salt-minion
```

b. 安装Agent前，执行**df -h**命令，检查磁盘的根目录盘或者opt盘预留50G以上，CPU核数需要2核以上，内存需要4G以上。

图 1-17 检查磁盘

```
[root@ecs-      ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda1        40G  1.7G   36G   5% /
devtmpfs        7.8G     0  7.8G   0% /dev
tmpfs           7.8G     0  7.8G   0% /dev/shm
tmpfs           7.8G  129M  7.7G   2% /run
tmpfs           7.8G     0  7.8G   0% /sys/fs/cgroup
/dev/vdb1        98G  8.9G   85G  10% /opt
/dev/vdb2       108G   61M  103G   1% /var/lib/docker
tmpfs           1.6G     0  1.6G   0% /run/user/0
```

如果内存不足，请关闭一些高内存占用的应用程序或扩充内存容量后再进行安装。扩容操作详情请参见**变更服务器规格**。

2. 登录管理控制台。
3. 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。
4. 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

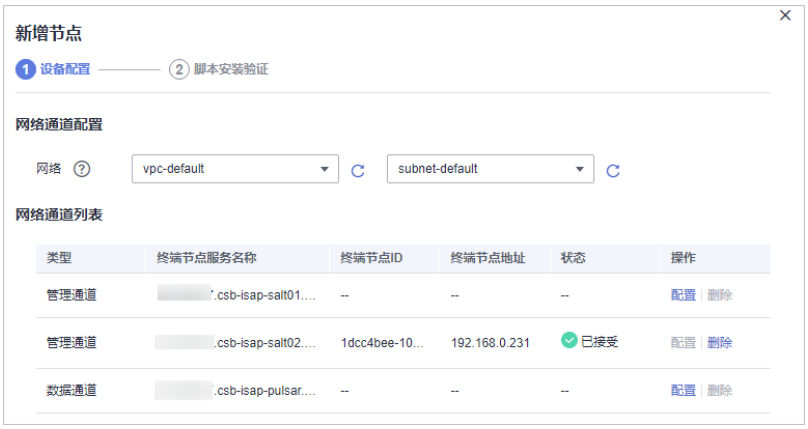
图 1-18 进入目标工作空间管理页面

5. 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 1-19 进入节点管理页面

6. 在节点管理页面中，单击“新增”，页面右侧弹出新增节点页面。
7. 在新增节点页面中，配置设备。

图 1-20 新增节点



a. 在网络通道配置栏中，选择网络通道所属的虚拟私有云和子网。

b. 在网络通道列表中，单击通道“操作”列的“配置”，并在弹出的确认框中，单击“确认”。

8. 单击页面右下角“下一步”，进入脚本安装验证页面后，单击 复制安装Agent的命令。

9. 远程登录待安装Agent的ECS。

   - **华为云主机**

     - 您可以登录弹性云服务器控制台，在“弹性云服务器”列表中，单击“远程登录”登录主机，详细操作请参见**在云服务器控制台上登录主机**。

     - 若您的主机已经绑定了弹性IP，您也可以使用远程管理工具（例如：PuTTY、Xshell等）登录主机，并使用root账号在主机中安装Agent。

   - **非华为云主机**

     请使用远程管理工具（例如：PuTTY、Xshell等）连接您服务器的弹性IP，远程登录到您的服务器。

10. 执行**cd /opt/cloud**命令，进入安装目录。

注意

安装路径建议为“/opt/cloud”，本章节也以此路径为例进行介绍。如需安装在其他自定义路径中，请根据路径修改。

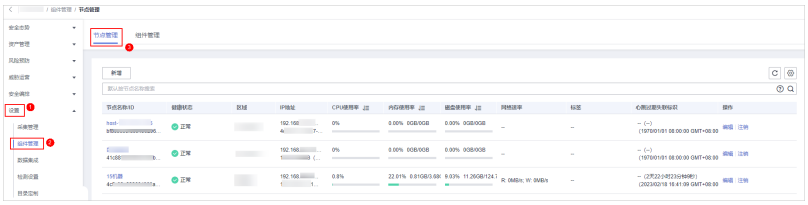
11. 粘贴复制的**8**复制的安装命令，以root权限执行，在ECS中安装Agent。
12. 根据界面提示，输入登录控制台的IAM账号和密码。
13. 若界面回显类似如下信息时，则表示Agent安装成功。

```
install isap-agent successfully
```

步骤三：新增节点

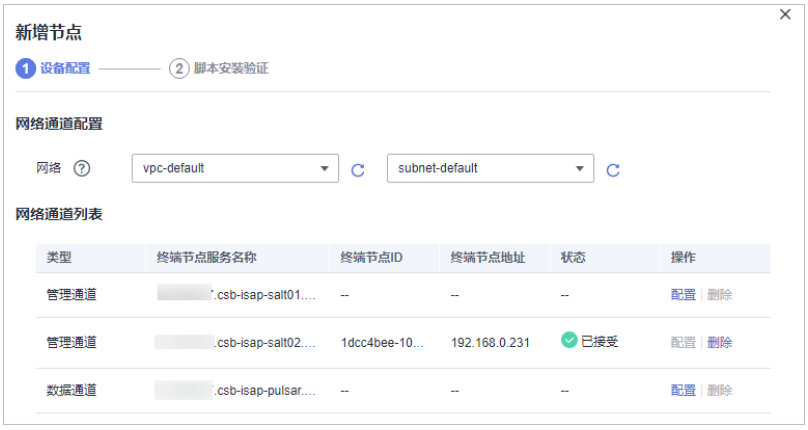
1. 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 1-21 进入节点管理页面



2. 在节点管理页面中，单击“新增”，页面右侧弹出新增节点页面。
3. 在新增节点页面中，配置设备。

图 1-22 新增节点



   a. 在网络通道配置栏中，选择网络通道所属的虚拟私有云和子网。
   b. 在网络通道列表中，单击通道“操作”列的“配置”，并在弹出的确认框中，单击“确认”。
4. 单击页面右下角“下一步”，进入“脚本安装验证”页面。
5. 确认已安装后，单击页面右下角“确认”。

步骤四：配置组件

Logstash是一个开源数据收集引擎，具有实时流水线功能，Logstash可以动态采集来自不同来源的数据，将其转换并输出到不同目的。

1. 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，选择“组件管理”页签，进入组件管理页面。

图 1-23 进入组件管理页面

2. 在组件管理页面中，单击待查看组件右上角“编辑配置”，右侧将弹出该组件的配置管理页面。

3. 在节点配置栏中，单击节点列表左上角“添加”，并在弹出的“添加节点”框中选择节点后，单击“确认”。
4. 单击页面右下角“保存并应用”。

步骤五：（可选）新增管道

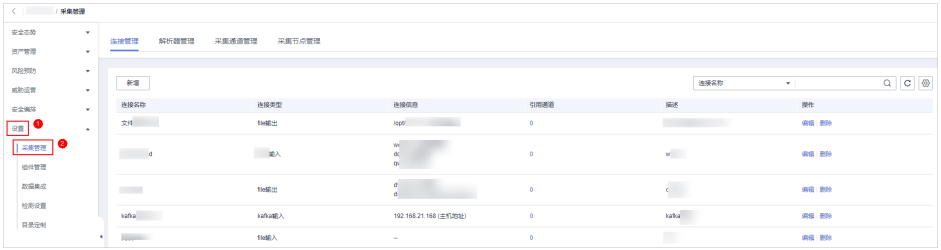
新增用于转入数据的存储管道，详细操作请参见**创建管道**。

步骤六：新增数据连接（来源、目的）

新增数据连接，包含数据来源、以及数据解析后转出位置。

1. 在左侧导航栏选择“设置 > 采集管理”，默认进入连接管理页面。

图 1-24 进入采集管理页面



2. 新增数据连接来源。
   a. 在“连接管理”页面中，单击“新增”，进入选择数据连接页面。
   b. 在“来源”页签中，选择数据源类型的来源“用户数据协议 Udp”，并配置UDP参数信息。

图 1-25 数据源来源

表 1-4 数据源来源

参数名称	参数说明
名称	自定义数据连接来源的名称。
描述	自定义数据连接来源的描述信息。

参数名称	参数说明
端口	设置需要采集的端口。
codec	设置编码格式，可设置为json或plain。
可选参数	自定义其他可选参数信息。

c. 设置完成后，单击页面右下角“确认”。

3. 新增数据源连接目的。

a. 在采集管理页面选择“连接管理”页签，进入连接管理页面后，单击“新增”，进入选择数据连接页面。

b. 选择“目的”页签中，选择数据源类型的目的“云脑管道 Pipe”，并配置管道信息。

图 1-26 数据源接入目的地

表 1-5 数据源接入的目的地

参数名称	参数说明
名称	自定义数据源目的名称。
描述	自定义数据源目的描述信息。
类型	此处选择“租户”。
管道	选择**步骤五：（可选）新增管道**创建的管道。
域账户	输入IAM域账号。
用户名	输入IAM用户名。
密码	输入IAM账号密码。
可选参数	自定义其他可选参数信息。

c. 设置完成后，单击页面右下角“确认”。

步骤七：配置解析器

1. 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 1-27 进入解析器管理页面

2. 在解析器管理页面中，单击“新增”，并在新增解析器页面中，进行参数配置新增采集通道。
   - 名称：设置解析器名称。
   - （可选）描述：输入解析器描述信息。
   - 规则列表：设置解析器解析规则。单击“添加”，并选择规则：
     - 条件控制：选择“if条件”，判断日志是否存在。
     - 解析规则：选择“json解析”，将原始字段(message)移除。

图 1-28 规则列表

3. 设置完成后，单击页面右下角“确定”。

步骤八：新增采集通道

新增采集通道的目的在于将输入-解析-输出连接形成管道，并将管道下发至采集节点（安装Agent和Logstash的节点），完成此步骤后，整个数据接入转出真正开始运行。

1. 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

图 1-29 进入采集通道管理页面

2. 新增分组。
   a. 在采集通道管理页面中，单击“分组列表”右侧的。
   b. 输入分组名称，并单击，完成新增。
3. 在采集通道管理页面的分组列表右侧，单击“新增”，进入新增采集通道页面。
4. 在“基础配置”页面中，配置基础信息。

表 1-6 基础配置参数说明

参数名称		参数说明
基础信息	名称	自定义采集通道名称。
	通道分组	选择2新增的分组。
	（可选）描述	输入采集通道描述信息。
来源配置	源名称	选择**步骤六：新增数据连接（来源、目的）**新增的来源。
目的配置	目的名称	选择**步骤六：新增数据连接（来源、目的）**新增的目的地名称。

5. 基础配置完成后，单击页面右下角“下一步”，进入“解析器配置”页面。
6. 在“解析器配置”页面中，选择**步骤七：配置解析器**配置的解析器。
7. 解析器配置完成后，单击页面右下角“下一步”，进入“运行节点选择”页面。
8. 在“运行节点选择”页面中，单击“新增”，并在弹出的添加节点框中选择节点（安装了Agent和Logstash的节点）后，单击“确认”。
9. 运行节点选择完成后，单击页面右下角“下一步”，进入“通道详情预览”页面。
10. 在“通道详情预览”页面确认配置无误后，单击“确定”。

新增采集通道结束后，会对管道进行下发，刷新界面，当健康状态为“正常”，则下发完成。

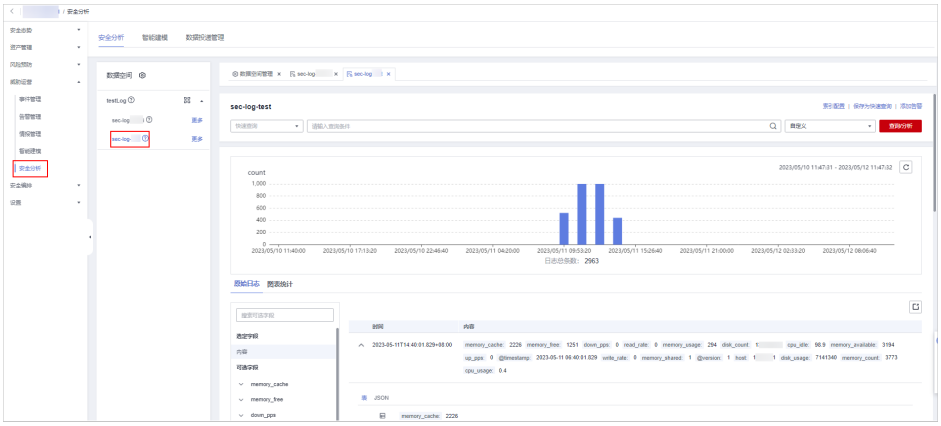
步骤九：安全查询分析

由于将日志输出至安全云脑管道，因此可在安全云脑中查询。

1. 在左侧导航栏选择“威胁运营 > 安全分析”，默认进入“安全分析”页面。

2. 选择**步骤五：（可选）新增管道**的安全云脑管道，即可在安全云脑界面查看日志解析后的数据。

图 1-30 安全查询分析



A 修订记录

发布日期	修改记录
2023-06-20	第一次正式发布。