安全云脑

最佳实践

文档版本 02

发布日期 2023-10-16

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。

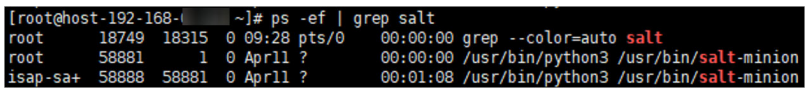
图 1-1 选择操作系统版本

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。

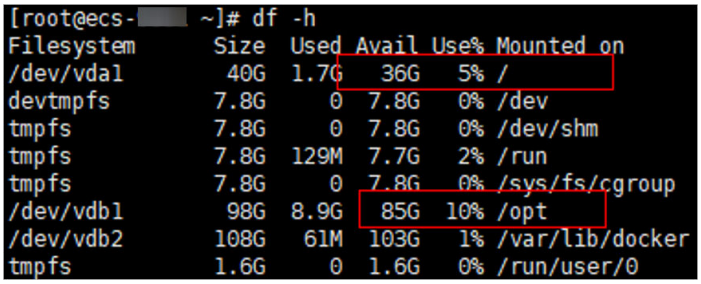
1. 安装Agent前预检查。
   a. 安装Agent前，执行**ps -ef | grep salt**命令，检查主机之前的salt-minion进程是否残留。
      - 如果有，请先关闭。
      - 如果没有，请继续执行**1.b**。

      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

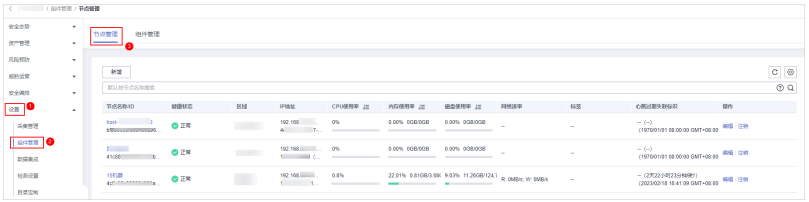
如果内存不足，请关闭一些高内存占用的应用程序或扩充内存容量后再进行安装。扩容操作详情请参见**变更服务器规格**。

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

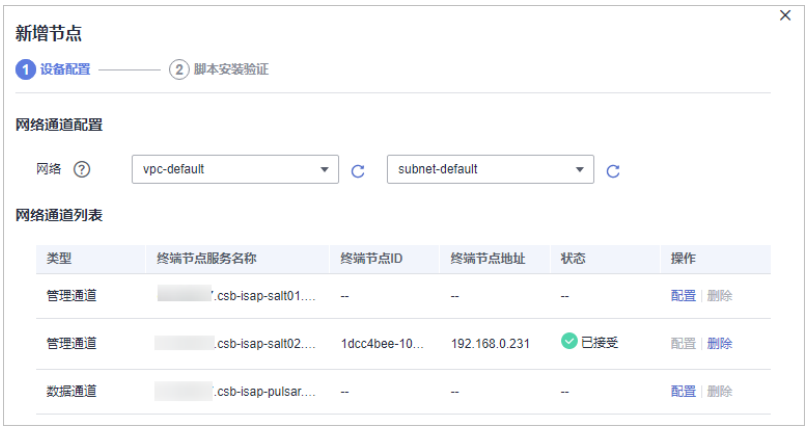
5. 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

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。

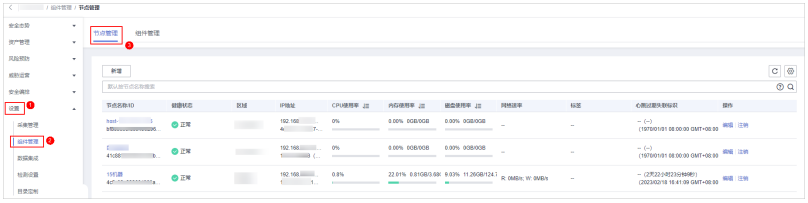
> **注意**
>
> 安装路径建议为“/opt/cloud”，本章节也以此路径为例进行介绍。如需安装在其他自定义路径中，请根据路径修改。

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

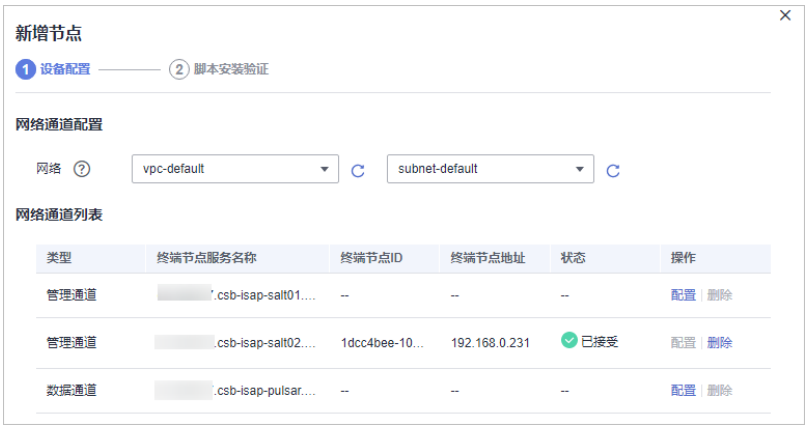
1. 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

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

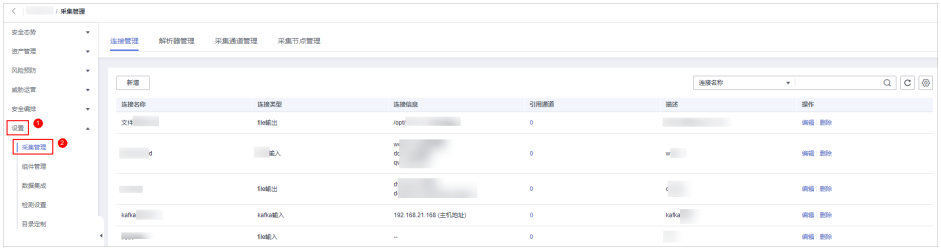
新增用于转入数据的存储管道，详细操作请参见**创建管道**。

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”。

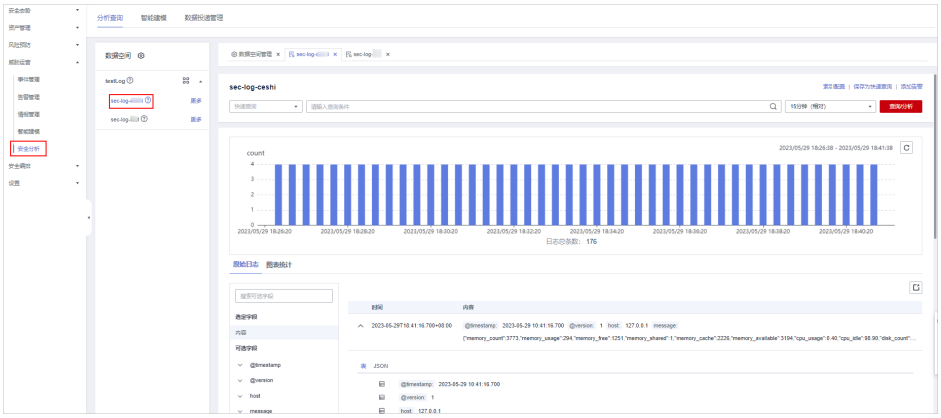
新增采集通道结束后，会对管道进行下发，刷新界面，当健康状态为“正常”，则下发完成。

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
```

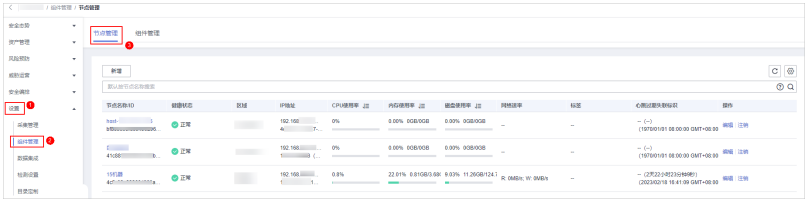
如果内存不足，请关闭一些高内存占用的应用程序或扩充内存容量后再进行安装。扩容操作详情请参见**变更服务器规格**。

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

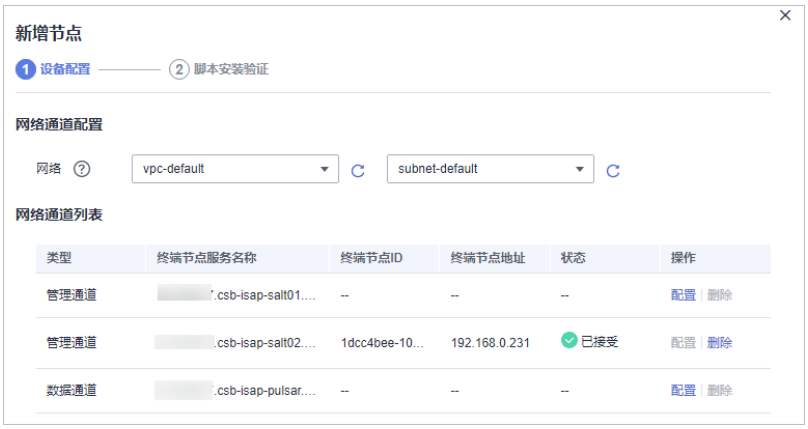
5. 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

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。

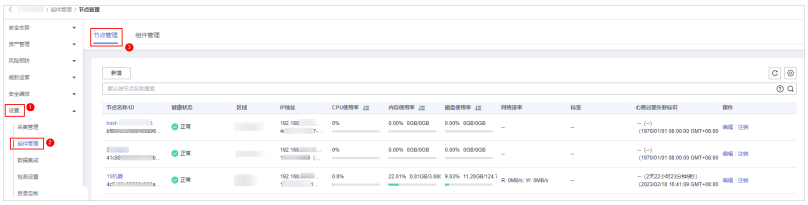
11. 粘贴复制的**8**复制的安装命令，以root权限执行，在ECS中安装Agent。
12. 根据界面提示，输入登录控制台的IAM账号和密码。
13. 若界面回显类似如下信息时，则表示Agent安装成功。

```
install isap-agent successfully
```

步骤三：新增节点

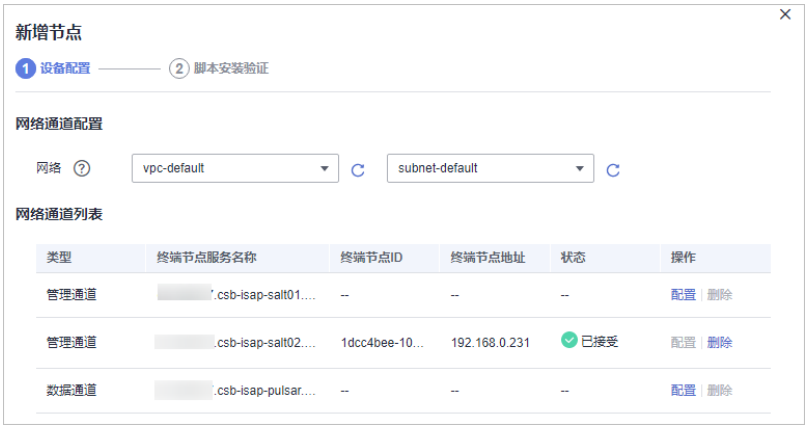
1. 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

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

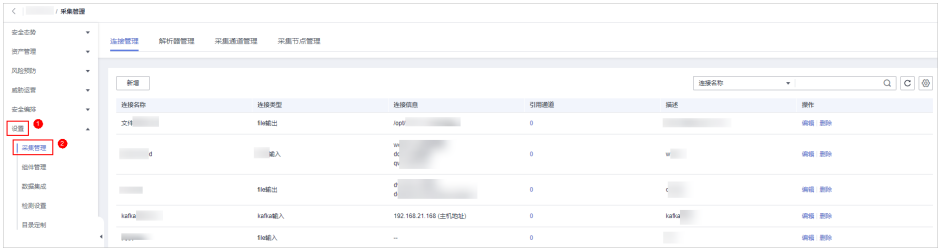
新增用于转入数据的存储管道，详细操作请参见**创建管道**。

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。

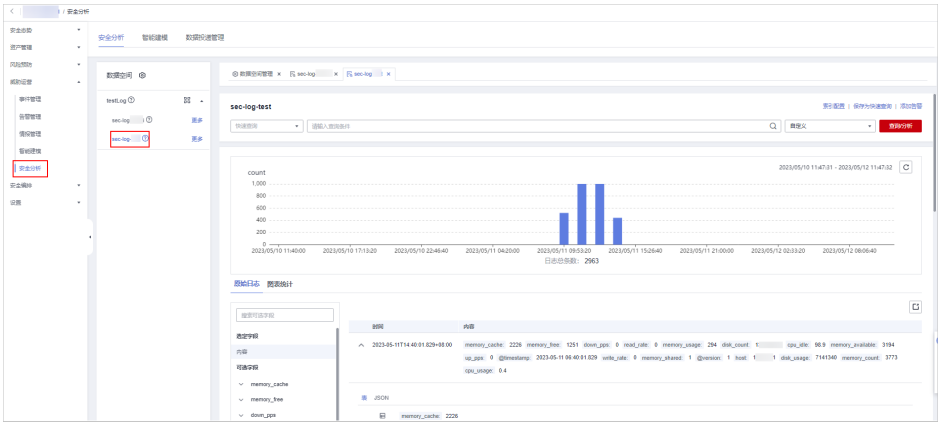
步骤九：安全查询分析

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



2 安全云脑护网/重保最佳实践

2.1 场景说明

安全云脑（SecMaster）是华为云原生的新一代安全运营中心，集华为云多年安全经验，基于云原生安全，提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力。支持在重大保障及防护演练前，信息全面的脆弱性盘点；在攻防演练期间，高强度7*24的安全保障，侧重于防攻击，保障业务可用性不因安全攻击受影响，侧重于防入侵，保障不因入侵失分被问责。能够更智能、更快速，帮助您实现一体化、自动化安全运营管理，满足您的安全需求。

本场景将介绍在护网、重保场景中安全云脑的使用。

2.2 业务信息梳理

操作场景

护网/重保前，需要对整体护网信息进行盘点，全面梳理可能针对云上业务系统的攻击路径，构建安全防护架构。

安全云脑纳管了网站、弹性云服务器、数据库、IP、VPC等资产，并关联对应的安全服务，护网、重保期间立志于从网络层、应用层、主机层、数据层等多方面构建整体网络防护架构，全面保障用户业务系统的安全稳定。

梳理网站资产

Web业务是企业最为重要和广泛使用的业务之一，也是最容易受到攻击的业务之一，因此，护网/重保前需要先进行Web资产的梳理。

针对网站域名，支持通过Web应用防火墙（Web Application Firewall，WAF）服务对网站业务流量进行全方位检测和防护，智能识别恶意请求特征和防御未知威胁，避免源站被黑客恶意攻击和入侵，防止核心资产遭窃取，为网站业务提供安全保障。

安全云脑的资产管理功能会自动将WAF中已录入的域名同步过来，可以在安全云脑中进行统一管理。护网/重保期间需要保证所有网站均已接入WAF并开启防护，以提高网站安全性。

您可以登录SecMaster控制台，进入目标工作空间的“资产管理 > 资产管理 > 网站”页面，查看网站防护状态，如图2-1所示。关于安全云脑中的网站防护状态说明如表2-1所示。

图 2-1 查看网站防护状态

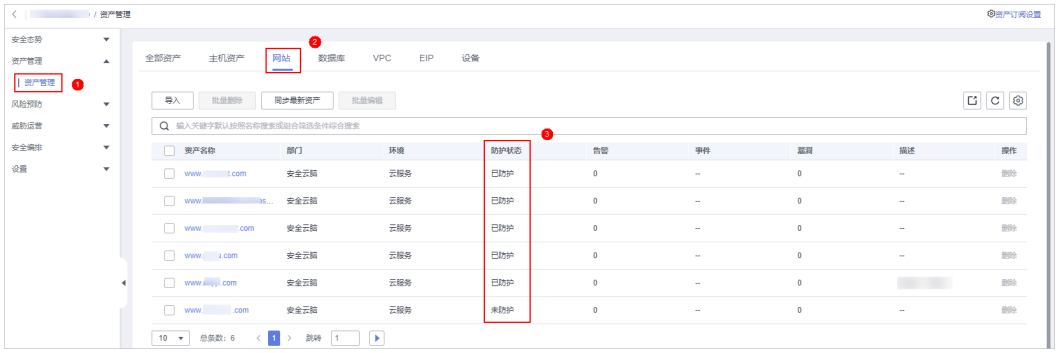


表 2-1 网站防护状态说明

网站防护状态	说明
未防护	网站域名未在WAF中开启防护。 为防止网站被各种恶意流量攻击，建议您在将网站接入WAF，才能对HTTP(S)请求进行检测，保障业务核心数据安全，详细操作请参见网站接入WAF。
已防护	已购买WAF，且已在WAF中接入网站域名并开启防护。
-	对应的安全防护产品(WAF)在该region不支持使用。

说明

如果网站资产未在安全云脑中显示，则可以通过设置资产订阅同步资产信息；如果需要导入云下资产，请参考导入资产进行处理。

梳理主机资产

安全云脑的资产管理功能会自动完成弹性云服务器（Elastic Cloud Server，ECS）资产的梳理，包括资产名称、镜像、IP等信息。

针对ECS主机资产，支持通过企业主机安全（Host Security Service，HSS）服务，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。

护网/重保期间需要保证所有ECS主机均接入HSS，尤其是绑定了EIP、以及Web业务所在ECS，以提高主机安全风险防御能力。

您可以登录SecMaster控制台，进入目标工作空间的“资产管理 > 资产管理 > 主机资产”页面，查看主机防护状态，如图2-2所示。关于主机资产防护状态说明请参见表2-2。

图 2-2 查看主机资产防护状态

表 2-2 主机资产防护状态说明

主机防护状态	说明
未防护	ECS主机未开启防护，被威胁入侵的风险较高，建议您尽快为主机开启防护。开启防护步骤如下： 1. **购买防护配额**。 2. **安装Agent**。 3. **开启主机防护**。 开启防护后，建议优化主机防护配置，如开启恶意软件云查、配置告警通知等，详细操作请参见**优化主机安全防护配置**。
已防护	主机已开启防护。企业主机安全会持续优化迭代Agent版本，请及时参考**升级Agent**将Agent升级为最新版。
-	对应的安全防护产品(HSS)在该region不支持使用。

说明

如果网站资产未在安全云脑中显示，则可以通过**设置资产订阅**同步资产信息；如果需要导入云下资产，请参考**导入资产**进行处理。

梳理数据库资产

梳理数据库资产的目的主要是在安全运营过程中，相关告警会自动关联数据库资产。

安全云脑的资产管理功能会自动完成云数据库（Relational Database Service，RDS）资产的梳理。针对数据库资产，支持通过数据库安全服务（Database Security Service，DBSS）服务来保障云上数据库的安全。

护网/重保期间需要保证所有RDS资产均已开启数据库安全审计，以保障云上数据库的安全。

您可以登录SecMaster控制台，进入目标工作空间的“资产管理 > 资产管理 > 数据库”页面，查看数据库防护状态，如**图2-3**所示。关于数据库防护状态说明请参见**表2-3**。

图 2-3 查看数据库防护状态

表 2-3 数据库防护状态说明

主机防护状态	说明
未防护	RDS资产未在DBSS中配置并开启防护。 为防止数据库被攻击，建议您开通并使用数据库安全审计，详细操作请参见**审计RDS关系型数据库（安装Agent）**或**审计RDS关系型数据库（免安装Agent）**。
已防护	RDS资产已在DBSS中配置并开启防护。
-	对应的安全防护产品(DBSS)在该region不支持使用。

说明

如果网站资产未在安全云脑中显示，则可以通过**设置资产订阅**同步资产信息；如果需要导入云下资产，请参考**导入资产**进行处理。

2.3 安全自查与整改

2.3.1 基线检查

2.3.1.1 配置基线整改

操作场景

安全云脑支持根据基线检查计划检查您的服务基线配置是否存在风险，提供了“安全上云合规检查1.0”、“等保2.0三级要求”、“护网检查”三大类别的检查规范。

护网/重保期间推荐使用“安全上云合规检查1.0”和“护网检查”两个规范。

检查之后分类呈现云服务配置检测结果，告警提示存在安全隐患的配置，并提供相应配置加固建议和帮助指导。

所有检查项检查完成之后进入详情页面，不合格检查项按照加固建议进行修复，特别是靶标，通过资产搜索，清零不合格检查项。同时，配置检查计划，每天定时扫描刷新结果。

另外，除了基线检查内置的检查项，护网/重保期间也可以针对自己的业务场景，通过安全模型自定义自己的检查机制，通过告警通知触发跟踪，具体详情请参见**安全运营策略调整**。

执行基线检查

步骤1 登录管理控制台。

步骤2 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。

步骤3 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 2-4 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“风险预防 > 基线检查”，并在基线检查页面右上角单击“立即检查”，立即执行扫描任务。

刷新页面，查看“最近检查时间”，即可确认是否为最新的扫描结果。

图 2-5 立即检查

步骤5 执行手动检查。

“安全上云合规检查1.0”和“护网检查”中的一些检查项目为手动检查项，需要用户自主排查对应检查项。

请根据检查项详情描述和检查过程检查之后，将结果反馈到安全云脑的基线检查页面中。

1. 在“检查规范”页签中，单击待反馈结果的手动检查项目所在行“操作”列的“反馈结果”。

图 2-6 手动检查

2. 在弹出提示框中，选择反馈结果，并单击“确定”。

图 2-7 反馈结果

说明

反馈结果有效期为7天，7天后请重新手动检查。

----结束

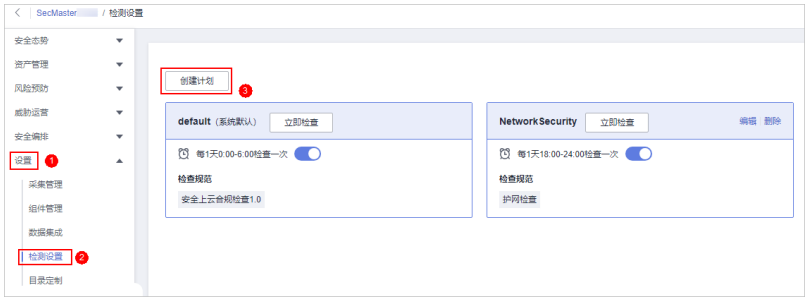
设置基线检查计划

检查计划是规范和时间组合形成的，也就是设置的定时扫描任务。通过配置检查计划自动的定期的对资产进行检查，保证检查结果的即时性。

护网/重保期间推荐对“护网检查规范”配置对应检查计划，配置策略周期为每天检查一次。

步骤1 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面后，选择待创建计划所在的区域，并单击“创建计划”。

图 2-8 进入检测设置页面



步骤2 在右侧弹出新建检查计划页面，配置检查计划。

表 2-4 新建检查计划

参数名称		参数说明
基本信息	计划名称	自定义检查计划的名称。
	检查时间	选择检测周期和检查触发时间，建议设置为每隔1天00:00~06:00进行检查。

参数名称	参数说明
选择检查规划	选择需要检测的基线检查项目。 **说明** 同一个检查规范只能属于一个检查计划，如需检查多个检查规范，请设置多个检查计划。

步骤3 单击“确定”。

检查计划创建完成后，安全云脑会在指定的时间执行云服务基线扫描，扫描结果可以在“风险预防 > 基线检查”中查看。

----结束

2.3.1.2 清理关键风险项

操作场景

执行基线检查后，需要对不合格检查项按照加固建议进行修复。

安全套件覆盖

安全套件主要包含WAF和HSS服务。执行基线检查后，可以单击对应基线检查项目的“查看详情”，根据加固建议开启相关防护，因客观原因无法开启防护的情况，请单击“忽略”，来进行忽略某个检查项。

比如，检查项“WAF防护策略配置检查”，详情页会列出具体未开启防护的域名，需要根据提示去相关服务开启防护。

图 2-9 WAF 防护策略配置检查

敏感信息排查

敏感信息是对象存储服务（Object Storage Service，OBS）、ES、云数据库（Relational Database Service，RDS）中的数据，结合数据安全中心（Data Security Center，DSC）服务，进行敏感信息排查。

执行基线检查后，可以单击对应基线检查项目的“查看详情”，在详情页会列出来所有涉及的存储资产，需要根据加固建议对有敏感信息的数据进行整改。需要注意的是整改数据是**高危操作**，需要根据业务场景需求判断之后进行处置。

图 2-10 OBS 中敏感信息检查

例如，OBS桶的拥有者可以通过桶ACL授予指定账号或用户组特定的访问权限。所以，所有OBS桶尽量都控制好对应的访问权限，不要对匿名用户赋予桶访问权限或者ACL访问权限。同样，OBS服务端加密也是为了保证数据安全性的配置，在数据存储时使用服务端加密将数据加密成密文后存储。

图 2-11 OBS 桶的 ACL 权限检查

账号加固

账号加固主要针对云上凭证权限和主机密码的排查。通过凭证、口令等权限的控制，保证护网/重保期间账号的安全性。

执行基线检查后，请根据扫描结果的加固建议进行修复。需要注意的是所有权限账号的修改都要首先进行排查，在不影响业务正常运行的情况下进行修改。

图 2-12 主机弱密码检查

主机加固

主机加固是针对项目主机、网络、集群等相关方面的加固检查。

- 主机是针对业务开放的端口进行扫描，对高危端口进行告警。

图 2-13 主机高危端口暴露检查

- 集群只针对CCE集群，针对集群有安全漏洞风险的版本，建议进行升级。
- 网络针对包含不同VPC之前的互联和出口网关设备，建议是不同VPC之间没有进行任何的交互。如果因客观原因无法满足的，请单击“忽略”检查项。

图 2-14 CCE 集群 Kubernetes 版本检查

访问控制

访问控制主要针对安全组入方向规则进行检查，默认是针对全开放的规则和未最小化掩码开放的规则为不合格。

需要根据业务场景，保证最小化开放访问控制策略的原则进行安全组的配置。

图 2-15 安全组入方向规则控制检查

Sudo 漏洞

针对主机系统漏洞、Sudo漏洞检查是通过比对漏洞库检查主机是否存在对应风险的。

需要对扫描出不合格的主机进行修复。在HSS服务中对对应漏洞进行修复处置即可。

图 2-16 检查主机是否存在 Sudo 漏洞

2.3.2 漏洞管理

2.3.2.1 漏洞整改

操作场景

漏洞是攻击者入侵企业系统的主要手段之一，攻击者可以利用漏洞获取系统权限、窃取敏感信息或者破坏系统功能。完成漏洞整改可以有效地提高系统的安全性，预防潜在的攻击。

安全云脑提供漏洞修复帮助用户针对配置隐患和系统漏洞进行排查。安全云脑的漏洞管理分为Linux漏洞、Windows漏洞、Web-CMS漏洞、应用漏洞进行管理。

- Linux漏洞：内含常见Linux系统以及组件的各类漏洞，如内核漏洞、组件漏洞等。
- Windows漏洞：内含Windows系统最新漏洞以及补丁。
- Web-CMS漏洞：内含常见web-cms框架漏洞信息，如phpmyadmin等。
- 应用漏洞：内含常见应用类型漏洞，如fastjson、log4j2等。

前提条件

请确保修复漏洞时，您的业务处于低峰期或特定的变更时间窗。

修复漏洞操作步骤

步骤1 登录管理控制台。

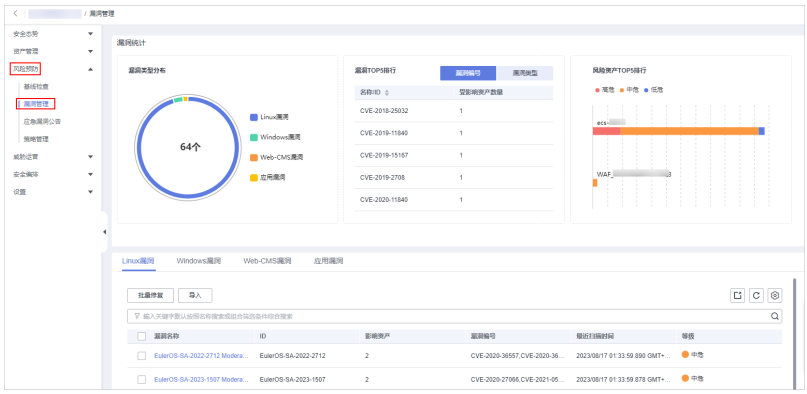
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 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 2-17 进入目标工作空间管理页面

步骤4 在安全云脑管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

图 2-18 进入漏洞管理页面



步骤5 筛选“等级”为“高危”、“是否已处理”为“未处理”的Linux漏洞、Windows漏洞和应用漏洞，优先进行修复。

须知

在进行漏洞修复前，需提前和您的业务相关人员确认漏洞修复是否会对业务造成影响。

图 2-19 筛选漏洞

步骤6 修复漏洞。

- 修复Linux、Windows漏洞

  单击目标漏洞名称，在右侧弹出漏洞信息页面中，选择“受影响资产”页签，并在资产列表中，单击待处理资产所在行“操作”列的“修复”，系统提示修复操作触发成功。

  如需批量修复，可以勾选所有需要修复的资产，然后在列表左上角，单击“批量修复”。

⚠ 注意

执行主机漏洞修复可能存在漏洞修复失败导致业务中断，或者中间件及上层应用出现不兼容等风险，并且无法进行回滚。为了防止出现不可预料的严重后果，建议您通过云服务器备份（CSBS）为ECS创建备份，详细操作请参见**创建云服务器备份**。然后，使用空闲主机搭建环境充分测试，确认不影响业务正常运行后，再对主机执行漏洞修复。

- 修复Web-CMS漏洞、应用漏洞
  a. 单击目标漏洞名称，在右侧弹出漏洞信息页面中，选择“受影响资产”页签，查看受影响资产信息。
  b. 登录漏洞影响的主机，手动修复漏洞。
     漏洞修复有可能影响业务的稳定性，为了防止在修复漏洞过程影响当前业务，建议参考以下两种方案，选择其中一种执行漏洞修复：
     - **方案一：创建新的虚拟机执行漏洞修复**
       1) 为需要修复漏洞的ECS主机创建镜像，详细操作请参见**通过云服务器创建整机镜像**。
       2) 使用该镜像创建新的ECS主机，详细操作请参见**通过镜像创建云服务器**。
       3) 在新启动的主机上执行漏洞修复并验证修复结果。
       4) 确认修复完成之后将业务切换到新主机。
       5) 确定切换完成并且业务运行稳定无故障后，可以释放旧的主机。如果业务切换后出现问题且无法修复，可以将业务立即切换回原来的主机以恢复功能。
     - **方案二：在当前主机执行修复**
       1) 为需要修复漏洞的ECS主机创建备份，详细操作请参见**创建云服务器备份**。
       2) 在当前主机上直接进行漏洞修复。
       3) 如果漏洞修复后出现业务功能问题且无法及时修复，立即使用备份恢复功能将主机恢复到修复前的状态，详细操作请参见**使用备份恢复服务器**。

     说明

     - 方案一适用于第一次对主机漏洞执行修复，且不确定漏洞修复的影响。新创建的ECS主机建议采用按需计费的方式创建，待业务切换完成后可以根据需要转换为包周期计费模式。如果漏洞修复不成功可以随时释放以节省开销。
     - 方案二适用于已经有同类主机执行过修复，漏洞修复方案已经比较成熟可靠的场景。

----结束

2.3.2.2 热门漏洞检查

安全云脑聚合了2022-2023发生的最新漏洞，结合多年的华为云经验，对其中的关键性漏洞/红队常利用漏洞进行扫描和检查，如：**Aache Log4j2 远程代码执行漏洞、Fastjson 1.2.8 反序列化漏洞、Apache Kafka远程代码执行漏洞**等。

在护网/重保期间建议尽可能全部修复高危漏洞，也可以针对自己的业务场景进行专项漏洞的修复。目前，安全云脑支持对应漏洞一键修复、以及批量修复。如下为热门漏洞检查项如**表2-5**所示，漏洞详情请如**表2-6**所示。

表 2-5 热门漏洞检查项

漏洞名称	影响版本	修复建议
Apache Log4j2 远程代码执行漏洞（CVE-2021-44228）	Apache Log4j 2.x <= 2.14.1	安全云脑支持一键修复，若修复升级失败请进入官方下载。 下载链接：https://github.com/apache/logging-log4j2
Fastjson 1.2.8 反序列化漏洞(CVE-2022-25845)	FastJson <= 1.2.80	安全云脑支持一键修复，若修复升级失败请进入官方下载。 下载链接：https://github.com/alibaba/fastjson2/releases
Apache Kafka远程代码执行漏洞(CVE-2023-25194)	Apache Kafka 2.3.0 - 3.3.2	安全云脑支持一键修复，若修复升级失败请进入官方下载。 下载链接：https://kafka.apache.org/downloads
Apache RocketMQ命令注入漏洞(CVE-2023-33246)	Apache RocketMQ 5.x < 5.1.1 Apache RocketMQ 4.x < 4.9.6	安全云脑支持一键修复，若修复升级失败请进入官方下载。 下载地址：https://rocketmq.apache.org/download

漏洞名称	影响版本	修复建议
Atlasssian Confluence OGNL注入漏洞 (CVE-2022-26134)	Atlassian Confluence Server and Data Center >= 1.3.0 Atlassian Confluence Server and Data Center < 7.4.17 Atlassian Confluence Server and Data Center < 7.13.7 Atlassian Confluence Server and Data Center < 7.14.3 Atlassian Confluence Server and Data Center < 7.15.2 Atlassian Confluence Server and Data Center < 7.16.4 Atlassian Confluence Server and Data Center < 7.17.4 Atlassian Confluence Server and Data Center < 7.18.1	安全云脑支持一键修复，若修复升级失败请进入官方下载。
F5 BIG-IP 命令执行漏洞 (CVE-2022-1388)	16.1.0<=F5 BIG-IP<=16.1.2 15.1.0<=F5 BIG-IP<=15.1.5 14.1.0<=F5 BIG-IP<=14.1.4 13.1.0<=F5 BIG-IP<=13.1.4 12.1.0<=F5 BIG-IP<=12.1.6 11.6.1<=F5 BIG-IP<=11.6.5	安全云脑支持一键修复，若修复升级失败请进入官方下载。 下载链接：https://support.f5.com/csp/article/K23605346
Apache CouchDBi 权限提升漏洞 (CVE-2022-24706)	Apache CouchDB <3.2.2	安全云脑支持一键修复，若修复升级失败请进入官方下载。 下载链接：https://couchdb.apache.org/

漏洞名称	影响版本	修复建议
Atlassian Bitbucker Data Center 远程代码执行漏洞 (CVE-2022-26133)	Atlassian Bitbucket Data Center >= 5.14.x Atlassian Bitbucket Data Center 6.x Atlassian Bitbucket Data Center < 7.6.14 Atlassian Bitbucket Data Center < 7.16.x Atlassian Bitbucket Data Center < 7.17.6 Atlassian Bitbucket Data Center < 7.18.4 Atlassian Bitbucket Data Center < 7.19.4 Atlassian Bitbucket Data Center 7.20.0	安全云脑支持一键修复，若修复升级失败用户请尽快更新至安全版本：7.6.14、7.17.6、7.18.4、7.19.4、7.20.1、7.21.0。
Weblogic 远程代码执行漏洞(CVE-2023-21839)	WebLogic_Server = 12.2.1.3.0 WebLogic_Server = 12.2.1.4.0 WebLogic_Server = 14.1.1.0.0	安全云脑支持一键修复，若修复升级失败请进入官方下载。 下载链接：https://support.oracle.com/rs?type =doc&id=2917213.2
Apache HTTP Server HTTP 请求走私漏洞 (CVE-2023-25690)	Apache HTTP Server <= 2.4.55	安全云脑支持一键修复，若修复升级失败请进入官方下载 下载链接：https://httpd.apache.org/download.cgi
Apache Dubbo 反序列化漏洞(CVE-2023-23638)	2.7.0 <= Apache Dubbo <= 2.7.21 3.0.0 <= Apache Dubbo <= 3.0.13 3.1.0 <= Apache Dubbo <= 3.1.5	安全云脑支持一键修复，若修复升级失败请进入官方下载。 下载链接：https://mvnrepository.com/artifact/org.apache.dubbo/dubbo
Spring Framework 身份认证绕过漏洞 (CVE-2023-20860)	Spring Framework 6.0.0 - 6.0.6 Spring Framework 5.3.0 - 5.3.25	安全云脑支持一键修复，若修复升级失败请进入官方下载。 下载链接：https://github.com/spring-projects/spring-framework/releases

漏洞名称	影响版本	修复建议
Microsoft Outlook 特权提升漏洞 (CVE-2023-23397)	Microsoft Outlook 2016 (64-bit edition) Microsoft Outlook 2013 Service Pack 1 (32-bit editions) Microsoft Outlook 2013 RT Service Pack 1 Microsoft Outlook 2013 Service Pack 1 (64-bit editions) Microsoft Office 2019 for 32-bit editions Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft Office 2019 for 64-bit editions Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft Office LTSC 2021 for 64-bit editions Microsoft Outlook 2016 (32-bit edition) Microsoft Office LTSC 2021 for 32-bit editions	安全云脑支持一键修复，若修复升级失败请进入官方下载。 下载链接：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397
MinIO 信息泄露 (CVE-2023-28432)	RELEASE.2019-12-17T23-16-33Z <= MinIO < RELEASE.2023-03-20T20-16-18Z	安全云脑以支持一键修复，若修复升级失败请进入官方下载。 下载链接：https://github.com/minio/minio/tags
Grafana JWT 泄露漏洞 (CVE-2023-1387)	9.1.0 <= Grafana < 9.2.17 9.3.0 <= Grafana < 9.3.13 9.4.0 <= Grafana < 9.5.0	安全云脑支持一键修复，若修复升级失败请进入官方下载。 下载链接：https://grafana.com/get/?plcmt=top-nav&cta=downloads

漏洞名称	影响版本	修复建议
Foxit PDF Reader/Editor exportXFAData 远程代码执行漏洞 (CVE-2023-27363)	Foxit PDF Reader <= 12.1.1.15289 Foxit PDF Editor 12.x <= 12.1.1.15289 Foxit PDF Editor 11.x <= 11.2.5.53785 Foxit PDF Editor <= 10.1.11.37866	安全云脑支持一键修复，若修复升级失败请进入官方下载。 下载链接：https://www.foxit.com/downloads/
Apache RocketMQ 命令注入漏洞 (CVE-2023-33246)	Apache RocketMQ 5.x < 5.1.1 Apache RocketMQ 4.x < 4.9.6	安全云脑支持一键修复，若修复升级失败请进入官方下载。 下载链接：https://rocketmq.apache.org/download/
Openfire 身份认证绕过 (CVE-2023-32315)	3.10.0 <= Openfire < 4.6.8 4.7.0 <= Openfire < 4.7.5	安全云脑支持一键修复，若修复升级失败请进入官方下载。 Openfire >= 4.6.8 Openfire >= 4.7.5
nginxWebUI 远程命令执行漏洞	nginxWebUI <= 3.4.6	安全云脑支持一键修复，若修复升级失败请进入官方下载。 nginxWebUI >= 3.4.7
Nacos 反序列化漏洞	1.4.0 <= Nacos < 1.4.6 2.0.0 <= Nacos < 2.2.3	安全云脑支持一键修复，若修复升级失败请进入官方下载。 下载链接：https://github.com/alibaba/nacos/releases
Linux DirtyPipe 权限提升漏洞(CVE-2022-0847)	Linux kernel>=5.8	安全云脑支持一键修复，若修复升级失败请进入官方下载。 安全版本： Linux 内核 >= 5.16.11、Linux 内核 >= 5.15.25、Linux 内核 >= 5.10.102

表 2-6 热门漏洞详情

漏洞名称	披露时间	漏洞描述
Apache Log4j2 远程代码执行漏洞（CVE-2021-44228）	2021年12月10日	Apache Log4j是一个基于Java的日志记录组件。Apache Log4j2是Log4j的升级版本，通过重写Log4j引入了丰富的功能特性。该日志组件被广泛应用于业务系统开发，用以记录程序输入输出日志信息。 在特定的版本中由于其启用了lookup功能，从而导致产生远程代码执行漏洞。
Fastjson 1.2.8 反序列化漏洞(CVE-2022-25845)	2022年06月16日	Fastjson是开源的JSON解析库，它可以解析JSON格式的字符串，支持将Java Bean序列化为JSON字符串，也可以从JSON字符串反序列化到JavaBean。在Fastjson 1.2.80及以下版本中存在反序列化漏洞，攻击者可以在特定依赖下利用此漏洞绕过默认autoType关闭限制，从而反序列化有安全风险的类。
Apache Kafka远程代码执行漏洞(CVE-2023-25194)	2023年02月07日	Kafka是由Apache软件基金会开发的一个开源流处理平台，由Scala和Java编写。该项目的目标是为处理实时数据提供一个统一、高吞吐、低延迟的平台。其持久化层本质上是一个“按照分布式事务日志架构的大规模发布/订阅消息队列”，这使它作为企业级基础设施来处理流式数据非常有价值。此漏洞允许服务器连接到攻击者的LDAP服务器并反序列化LDAP响应，攻击者可以使用它在Kafka连接服务器上执行java反序列化小工具链。当类路径中有小工具时，攻击者可以造成不可信数据的无限制反序列化（或）RCE漏洞。此漏洞利用的前提是需要访问Kafka Connect worker，并能够使用任意Kafka客户端SASL JAAS配置和基于SASL的安全协议在其上创建/修改连接器。自Apache Kafka 2.3.0以来，这在Kafka Connect集群上是可能的。通过Kafka Connect REST API配置连接器时，经过身份验证的操作员可以将连接器的任何 Kafka 客户端的 `sasl.jaas.config` 属性设置为“com.sun.security.auth.module.JndiLoginModule”，它可以是通过“producer.override.sasl.jaas.config”、“consumer.override.sasl.jaas.config”或“admin.override.sasl.jaas.config”属性完成。

漏洞名称	披露时间	漏洞描述
Apache RocketMQ命令注入漏洞 (CVE-2023-33246)	2023年05月24日	Apache RocketMQ是一个分布式消息中间件，它支持多种消息模式，如发布/订阅、点对点、广播等，以及多种消息类型，如有序消息、延迟消息、批量消息等。它具有高吞吐量、低延迟、高可靠性、高可扩展性等特点，适用于互联网、大数据、移动互联网、物联网等领域的实时数据处理。Apache RocketMQ 在 5.1.1 和 4.9.6 版本之前存在命令注入漏洞。Apache RocketMQ中的多个组件缺乏权限验证，攻击者可以通过使用更新配置功能，以RocketMQ运行的系统用户执行命令。此外，攻击者还可以通过伪造RocketMQ协议内容达到相同的利用效果。
Atlasssian Confluence OGNL注入漏洞 (CVE-2022-26134)	2022年06月03日	Atlassian Confluence是专业wiki程序。它可以作为一个知识管理的工具，通过它能够实现团队成员之间的协作和知识共享。2022年6月3日，Atlassian官方发布官方公告，披露存在CVE-2022-26134 Confluence远程代码执行漏洞在野攻击漏洞事件。漏洞利用无需身份认证，可直接前台远程执行任意代码。
F5 BIG-IP 命令执行漏洞 (CVE-2022-1388)	2022年06月07日	F5 BIG-IP iControl REST存在命令执行漏洞(CVE-2022-1388)。该漏洞允许远程未经身份验证的攻击者绕过iControl REST服务身份验证访问内部敏感服务进而执行任意命令。攻击者可在应用处通过利用拼接、管道符、通配符等绕过手段来执行任意命令，写入后门，从而入侵服务器，获取服务器权限，直接导致服务器沦陷。
Apache CouchDBi权限提升漏洞 (CVE-2022-24706)	2022年04月29日	Apache CouchDB是一个开源的面向文档的数据库管理系统，可以通过RESTful JavaScript Object Notation (JSON) API访问。 在 3.2.2 版本之前的Apache CouchDB中，可以在不进行身份验证的情况下访问不正确的默认安装并获得管理员权限： 1. CouchDB打开一个随机网络端口，绑定到所有可用的接口以预期集群操作或runtime introspection，称为 "epmd "的实用程序向网络公布了这个随机端口。epmd本身在一个固定的端口上监听。 2. CouchDB包装之前为单节点和集群安装选择了一个默认的"cookie"值，该cookie用于验证Erlang节点之间的任何通信。

漏洞名称	披露时间	漏洞描述
Atlassian Bitbucker Data Center 远程代码执行漏洞 (CVE-2022-26133)	2022年04月27日	Atlassian发布安全公告，修复了一个存在于Atlassian Bitbucket Data Center中的代码执行漏洞。该漏洞是由于Atlassian Bitbucket Data Center 中的 Hazelcast接口功能未对用户数据进行有效过滤，导致存在反序列化漏洞而引起的。攻击者利用该漏洞可以构造恶意数据远程执行任意代码。只有当Atlassian Bitbucket Data Center以Cluster模式安装时，才可能受该漏洞影响。
Weblogic 远程代码执行漏洞 (CVE-2023-21839)	2023年01月18日	WebLogic是商业市场上主要的Java应用服务器软件之一，是世界上第一个成功商业化的J2EE应用服务器，目前已推出到14c版。而此产品也延伸出WebLogic Portal, WebLogic Integration等企业用的中间件，以及OEPE开发工具。WebLogic存在远程代码执行漏洞，未经授权的攻击者利用此漏洞通告T3、I IOP协议构造恶意请求发送给WebLogic服务器，成功利用此漏洞后攻击者可以接管WebLogic服务器，并执行任意命令。
Apache HTTP Server HTTP 请求走私漏洞 (CVE-2023-25690)	2023年03月08日	Apache HTTP Server是Apache一个开放源码的网页服务器软件，可以在大多数电脑操作系统中运行。由于其跨平台和安全性，被广泛使用，是最流行的Web服务器软件之一。它快速、可靠并且可通过简单的API扩展，将Perl / Python等解释器编译到服务器中。当启用mod_proxy以及某种形式的RewriteRule或ProxyPassMatch时，配置会受到影响，其中非特定模式与用户提供的请求目标 (URL) 数据的某些部分匹配，然后使用重新插入代理请求目标变量替换。
Apache Dubbo 反序列化漏洞 (CVE-2023-23638)	2023年03月08日	Apache Dubbo是一款易用、高性能的WEB和RPC框架，同时为构建企业级微服务提供服务发现、流量治理、可观测、认证鉴权等能力、工具与最佳实践。dubbo泛型调用存在反序列化漏洞，可导致恶意代码执行。
Spring Framework 身份认证绕过漏洞 (CVE-2023-20860)	2023年03月22日	Spring框架是Java平台的一个开源的全栈（full-stack）应用程序框架和控制反转容器实现，一般被直接称为Spring。该框架的一些核心功能理论上可用于任何Java应用，但Spring还为基于Java企业版平台构建的Web应用提供了大量的拓展支持。Spring没有直接实现任何的编程模型，但它已经在Java社区中广为流行，基本上完全代替了企业级JavaBeans（EJB）模型。Spring Security使用 "**" 作为匹配模式，同时配置 mvcRequestMatcher 会导致 Spring Security 和 Spring MVC 之间的模式不匹配，并可能存在身份认证绕过。

漏洞名称	披露时间	漏洞描述
Microsoft Outlook 特权提升漏洞 (CVE-2023-23397)	2023年03月15日	Microsoft Office Outlook是对Windows自带的Outlook express的功能进行了扩充。Outlook的功能很多，可以用它来收发电子邮件、管理联系人信息、记日记、安排日程、分配任务。Microsoft Outlook存在特权提升漏洞。攻击者可以通过发送特殊设计的电子邮件，该电子邮件在Outlook客户端进行检索和处理时会自动触发该漏洞利用，导致受害者会连接外部攻击者控制的UNC，从而将受害者的 Net-NTLMv2 hash 值泄露给攻击者。
MinIO 信息泄露 (CVE-2023-28432)	2023年03月22日	MinIO是在 GNU Affero 通用公共许可证 v3.0 下发布的高性能对象存储。它与 Amazon S3 云存储服务 API 兼容。使用 MinIO 为机器学习、分析和应用数据工作负载构建高性能基础架构。MinIO 在 RELEASE.2019-12-17T23-16-33Z 至 RELEASE.2023-03-20T20-16-18Z 版本之前存在信息泄露，未经身份验证的攻击者向 MinIO 发送特制的 HTTP 请求可以获取 MINIO_SECRET_KEY、MINIO_ROOT_PASSWORD 等所有的环境变量。
Grafana JWT 泄露漏洞 (CVE-2023-1387)	2023年04月26日	Grafana是一个跨平台、开源的数据可视化网络应用程序平台。使用者组态连接的数据源之后，Grafana 可以在网络浏览器里显示数据图表和警告。 Grafana 是一个用于监控和可观察性的开源平台。从 9.1 分支开始，Grafan a 引入了在 URL 查询参数 auth_token 中搜索 JWT 并将其用作身份验证令牌的功能。通过启用“url_login”配置选项（默认情况下禁用），可以将 JWT 发送到数据源。
Foxit PDF Reader/Editor exportXFAData 远程代码执行漏洞 (CVE-2023-27363)	2023年05月15日	Foxit PDF Reader 是一个流行的 PDF 阅读软件，与 Adobe 的 PDF 软件相比，具有更快的速度和更小的体积。该软件存在一个远程代码执行（RCE）漏洞，由于在 exportXFAData 方法中暴露了一个可以写入任意文件的 JavaScript 接口，导致攻击者可以在受害者的系统中执行任意代码。

漏洞名称	披露时间	漏洞描述
Apache RocketMQ 命令注入漏洞 (CVE-2023-33246)	2023年05月24日	Apache RocketMQ是一个分布式消息中间件，它支持多种消息模式，如发布/订阅、点对点、广播等，以及多种消息类型，如有序消息、延迟消息、批量消息等。它具有高吞吐量、低延迟、高可靠性、高可扩展性等特点，适用于互联网、大数据、移动互联网、物联网等领域的实时数据处理。Apache RocketMQ 在 5.1.1 和 4.9.6 版本之前存在命令注入漏洞。Apache RocketMQ 中的多个组件缺乏权限验证，攻击者可以通过使用更新配置功能，以 RocketMQ 运行的系统用户执行命令。此外，攻击者还可以通过伪造 RocketMQ 协议内容达到相同的利用效果。
Openfire 身份认证绕过 (CVE-2023-32315)	2023年06月25日	Openfire是一个基于 XMPP 协议的实时协作服务器，它是一个开源的项目，使用 Apache 许可证授权。它可以支持多种平台，提供强大的安全性和性能。X MPP 是一种开放的即时通讯协议，也叫做Jabber。openfire可以用来搭建聊天室，群组，视频会议等应用。Openfire还提供了多种插件和扩展，以增强其功能和兼容性。Openfire 在 3.10.0-4.6.7 和 4.7.0-4.7.4 版本中存在身份认证绕过漏洞，这允许未经身份验证的用户在已配置的 Openfire 环境中使用未经身份验证的 Openf ire 安装环境，以访问 Openfire 管理控制台中为管理用户保留的受限页面。
nginxWebUI 远程命令执行漏洞	2023年06月28日	nginxWebUI是一款图形化管理 nginx 配置的工具，可以使用网页来快速 置 nginx 的各项功能，包括 http 协议转发、tcp协议转发、反向代理、负载均衡、静态html服务器、ssl证书自动申请、续签、配置等。配置好后可一键生成 nginx.conf 文件，同时可控制 nginx 使用此文件进行启动与重载，完成对 ng inx 的图形化控制闭环。nginxWebUI 存在未授权远程命令执行漏洞，攻击者可以直接在服务器上执行任意命令，甚至接管服务器。
Nacos 反序列化漏洞	2023年06月06日	Nacos是一款开源的分布式服务发现和配置管理平台，用于帮助用户实现动态服务发现、服务配置管理、服务元数据及流量管理等功能。Nacos 在 1.4.0-1. 4.5 和 2.0.0-2.2.2 版本中存在不安全的反序列化漏洞。Nacos 对部分 Jraft 请求处理时，使用 hessian 进行反序列化未限制而造成的 RCE 漏洞。

漏洞名称	披露时间	漏洞描述
Linux DirtyPipe 权限提升漏洞 (CVE-2022-0847)	2022年03月08日	CVE-2022-0847是存在于Linux内核 5.8 及之后版本中的本地提权漏洞。攻击者通过利用此漏洞，可覆盖重写任意可读文件中的数据，从而可将普通权限的用户提升到特权root。CVE-2022-0847的漏洞原理类似于CVE-2016-5195 脏牛漏洞（Dirty Cow），但它更容易被利用。

2.4 安全运营策略调整

2.4.1 接入数据

操作场景

日志作为安全运营提供重要数据支撑，护网/重保期间推荐使用一键接入功能接入全部日志，并开启自动转告警功能，将攻击日志转换格式到“告警管理”中进行跟踪监控。另外，安全设备及安全服务告警过多，可以关闭自动转告警，通过安全模型来识别攻击和入侵。

操作步骤

步骤1 登录管理控制台。

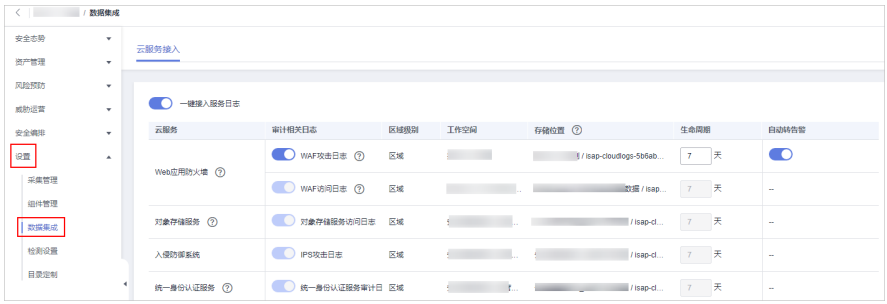
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 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 2-20 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 数据集成”，进入数据集成页面。

图 2-21 数据集成页面



步骤5 在待接入云产品的“审计相关日志”列，单击，开启接入的云服务日志。

如需接入当前region所有云产品日志，可直接单击“一键接入服务日志”前的按钮，一键接入当前region所有云服务日志。

步骤6 设置生命周期。

步骤7 设置是否自动转告警。

在待设置云产品的“自动转告警”列，单击，开启接入的云服务日志满足告警条件时，自动转为告警，并且在“告警管理”页面中进行展示。

说明

- 如果此处未开启自动转告警，在对应日志满足告警条件时，将不会转为告警，也不会在“告警管理”页面中进行展示。
- 在安全云脑的“漏洞管理”页面可以接入主机漏洞扫描结果，如果数据集成操作时接入了主机漏洞扫描结果，但是未开启自动转告警，则在“漏洞管理”将不会展示主机相关的漏洞扫描情况。

因此，建议您开启自动转告警设置。

步骤8 单击“保存”，并在弹出的配置保存框中，单击“确定”。

----结束

2.4.2 启用安全模型

操作场景

在智能建模页面安全云脑内置了基于应用、网络、主机多维度的安全分析模型，自动化的完成数据汇聚、分析和报警。

护网/重保期间建议使用以下内置的模板创建告警模型并启用模型：

应用-WAF关键攻击告警、网络-高危端口对外暴露、应用-源ip进行url遍历、应用-疑似存在源码泄露风险、网络-外部恶意IP扫描、网络-检测黑客工具攻击、网络-登录爆破告警、网络-僵尸网络、应用-疑似存在Shiro漏洞、应用-疑似存在log4j2漏洞、网络-疑似存在DDoS攻击、应用-疑似存在 Java框架通用代码执行漏洞、网络-命令注入告警、主机-暴力破解成功、主机-异常shell、主机-异地登录、网络-恶意软件 [蠕虫、病毒、木马]、主机-进程和端口信息隐匿、主机-异常文件权限修改、主机-异常文件属性修改、主机-恶意文件下载 (挖矿)、主机-rootkit事件、主机-恶意文件执行、主机-反弹shell、主机-恶意程序、主机-虚拟机横向连接、网络-后门、主机-恶意定时任务写入。

通过模型汇聚分析筛选告警，降低误报率，提升值班人员分析处理效率。同时，也可以结合用户场景编辑模型进行模型调整，适配不同用户场景，降噪告警。

操作步骤

创建告警模型

步骤1 登录管理控制台。

步骤2 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。

步骤3 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。

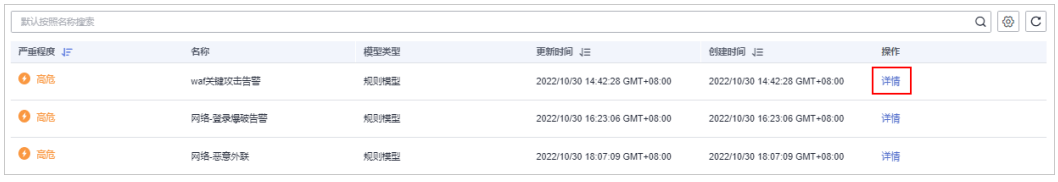
图 2-22 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 智能建模”，进入智能建模页面后，选择“模型模板”页签，进入模型模板页面。

图 2-23 模型模板页面

步骤5 在模型模板列表中，单击目标模型模板所在行“操作”列的“详情”，右侧弹出模板详情页面。

图 2-24 模型模板详情



步骤6 在模型模板详情页面，单击右下角“创建模型”，进入新建告警模型页面。

步骤7 在新增告警模型页面中，配置告警模型基础信息。

- 管道名称：选择该告警模型的执行管道，建议启用的模型对应管道信息请参见**表 2-7**。
- 其他参数建议保持默认值即可。

图 2-25 基础配置

步骤8 设置完成后，单击页面右下角“下一步”，进入设置模型逻辑页面。

步骤9 设置模型逻辑，建议保持默认即可。

如需进行配置，详细操作请参见**新建告警模型**。

步骤10 设置完成后，单击页面右下角“下一步”，进入模型详情预览页面。

步骤11 预览确认无误后，单击页面右下角“确定”。

步骤12 重复**步骤5**-**步骤11**为其他模板创建告警模型。

启用告警模型

步骤13 在左侧导航栏选择“威胁运营 > 智能建模”，进入智能建模的可用模型页面。

图 2-26 可用模型页面

步骤14 在模型列表中，勾选所有需要启动的模型，然后单击列表左上角的“启用”。

当模型状态更新为启用，则表示启动模型成功。

----结束

执行管道

表 2-7 选择执行管道

告警模板	需要选择的执行管道
应用-WAF关键攻击告警	sec-waf-attack
网络-高危端口对外暴露	sec-nip-attack
应用-源ip进行url遍历	sec-waf-access
应用-疑似存在源码泄露风险	sec-waf-access
网络-外部恶意IP扫描	sec-cfw-block
网络-检测黑客工具攻击	sec-nip-attack
网络-登录爆破告警	sec-nip-attack
网络-僵尸网络	sec-nip-attack
应用-疑似存在Shiro漏洞	sec-waf-attack
应用-疑似存在log4j2漏洞	sec-waf-attack
网络-疑似存在DDoS攻击	sec-cfw-block
应用-疑似存在 Java框架通用代码执行漏洞	sec-waf-attack
网络-命令注入告警	sec-nip-attack
主机-暴力破解成功	sec-hss-alarm
主机-异常shell	sec-hss-alarm
主机-异地登录	sec-hss-alarm
网络-恶意软件 [蠕虫、病毒、木马]	sec-nip-attack
主机-进程和端口信息隐匿	sec-hss-log
主机-异常文件权限修改	sec-hss-log
主机-异常文件属性修改	sec-hss-log
主机-恶意文件下载 (挖矿)	sec-hss-log
主机-rootkit事件	sec-hss-alarm
主机-恶意文件执行	sec-hss-log
主机-反弹shell	sec-hss-alarm
主机-恶意程序	sec-hss-alarm
主机-虚拟机横向连接	sec-hss-log
网络-后门	sec-nip-attack

告警模板	需要选择的执行管道
主机-恶意定时任务写入	sec-hss-log

2.4.3 启用流程和剧本

操作场景

数据采集后，针对云上安全事件提供了安全编排剧本，实现安全事件的高效、自动化响应处置。

安全云脑内置的流程默认已启用，无需再进行手动启用；内置的剧本已激活初始版本（V1），仅需启用对应剧本即可。

操作步骤

步骤1 登录管理控制台。

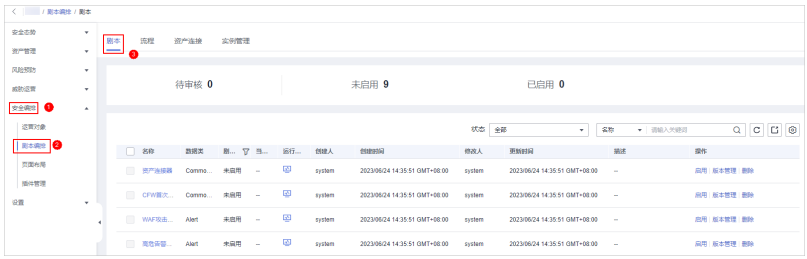
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 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 2-27 进入目标工作空间管理页面

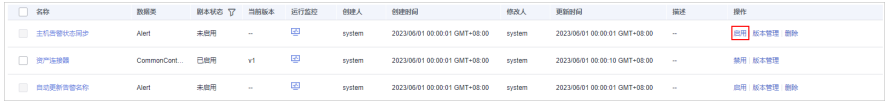
步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 2-28 进入剧本管理页面



步骤5 在剧本页面中，单击“告警指标提取”、“主机告警状态同步”、“重复告警自动关闭”剧本所在行“操作”列的“启用”。

图 2-29 启用剧本



步骤6 在弹出启用确认信息框中，选择启用的剧本版本v1，并单击“确认”。

----结束

2.5 安全监控与应急响应

2.5.1 值班监控

操作场景

安全云脑提供了4+1个大屏，一个是综合态势感知大屏，其他四个大屏是值班响应大屏、资产大屏、威胁态势大屏和脆弱性大屏。

护网及重保期间，安全值班人员需要重点关注**值班响应大屏**的数据信息，需要将值班响应大屏上的告警全部清零。

操作步骤

步骤1 登录管理控制台。

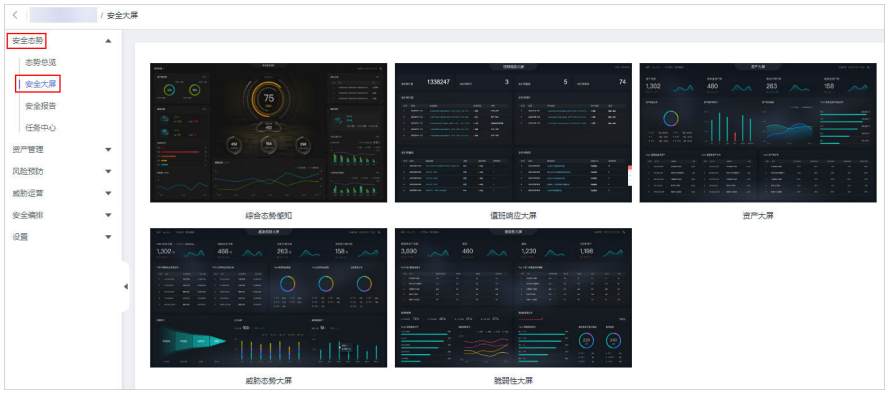
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 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 2-30 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全态势 > 安全大屏”，进入安全大屏页面。

图 2-31 进入安全大屏页面



步骤5 单击“值班响应大屏”图片，进入值班响应大屏信息页面后，在“未处理告警”模块中，单击告警名称，页面跳转到“告警管理”页面。

图 2-32 值班响应大屏

步骤6 处理告警。

不同的告警结合不同的信息进行分析，可以通过告警关联信息，告警payload，告警详情分析。也可以结合云脑的其他日志进行安全分析，比如WAF的告警可以结合WAF的日志进一步判断有没有入侵成功。

例如，某个单个源IP对域名进行多次攻击，虽然已经被WAF阻断，但是由于攻击次数较多，存在绕过WAF的风险，将多次攻击的行为冒泡出来，安全研判人员可以到waf_access日志，也就是Web的访问请求日志中，查询该IP有没有成功的访问请求(响应码为200)，来分析是否已经绕过了安全设备。通过分析如果看到该攻击ip请求成功的都是非敏感url，不存在攻击成功或绕过WAF检测的风险，直接关闭告警。如果是有风险url访问成功，则需要进行危险IP封堵。

封堵操作如下：

1. 在左侧导航栏选择“风险预防 > 策略管理”，进入策略管理页面后，选择“应急策略”页签，进入应急策略管理页面。
2. 在应急策略管理页面中，单击“新增”，右侧弹出新增应急策略页面。
3. 在新增策略页面中，配置策略信息。

表 2-8 新增应急策略

参数名称	参数说明
阻断对象	输入需要阻断的单个（或多个）IP地址或IP地址段，如有多个IP地址或地址段，请使用英文逗号隔开。 填写示例： – 单个IP地址：192.168.0.0 – IP地址段：192.168.0.0/12
标签	自定义应急策略的标签。
操作连接	选择该策略的操作连接。

参数名称	参数说明
阻断老化	确认是否老化该条阻断。建议设置老化时间为护网/重保周期时间，护网/重保结束之后封堵失效。 – 如果选择是，请设置策略老化时间，如设置为180天，即该策略在设置后的180天内有效，180天后将不再继续阻断设置的IP地址或IP地址段。 – 如果选择否，则该策略将一直有效，阻断设置的IP地址或IP地址段。
原因描述	自定义该策略的描述信息。

4. 单击“确定”

----结束

2.5.2 典型告警处理指导

操作场景

本章节介绍典型告警处理指导。

侦察阶段典型告警

恶意攻击者在对网站进行入侵时通常会进行大量的信息搜集，安全云脑可以通过模型：**网络-高危端口对外暴露、应用-源ip进行url遍历、应用-疑似存在源码泄露风险、网络-外部恶意IP扫描**等模型对即将来到的恶意攻击进行提前预判。

图 2-33 网络-高危端口对外暴露

图 2-34 应用-源 ip 进行 url 遍历

处理方案:

记录所有的访问请求和响应，及时发现攻击行为，针对攻击源IP进行限制或者阻断，可以通过配置黑名单策略进行封锁。

尝试攻击典型告警

- **描述**:

  黑客进行尝试攻击利用web应用程序的漏洞或缺陷进行攻击，可能会造成信息泄露、网站瘫痪、恶意软件传播、网站篡改等。

  安全云脑现有模型：**应用-WAF关键攻击告警、网络-检测黑客工具攻击、网络-登录爆破告警、应用-疑似存在Shiro漏洞、应用-疑似存在log4j2漏洞、网络-疑似存在DOS攻击、应用-疑似存在 Java框架通用代码执行漏洞、应用-疑似存在fastjson漏洞**等，可以针对于现在主流Web攻击漏洞进行检测。

图 2-35 应用-疑似存在 log4j2 漏洞

图 2-36 应用-WAF 关键攻击告警

- **处理方案**:

  需要联系业务责任人，排查Web服务器是否存在相关漏洞，确认是否攻击成功。若存在漏洞，应及时修改漏洞并加固安全；若攻击成功，可结合威胁情报对攻击IP进行拦截。

入侵成功典型告警

- **描述**:

  命令注入、暴力破解成功、异常shell、异地登录、恶意软件(蠕虫、病毒、木马)、高危命令执行等等，往往是入侵成功的标志。

  安全云脑现有模型：**网络-命令注入告警、主机-暴力破解成功、主机-异常shell、主机-异地登录、网络-恶意软件 [蠕虫、病毒、木马]、主机-进程和端口信息隐**

匿、主机-异常文件属性修改等多个模型，可以成功快速识别恶意行为，帮助我们对事件进行快速定位，快速相应。

图 2-37 主机-暴力破解成功

图 2-38 网络-恶意软件 [蠕虫、病毒、木马]


网络-恶意软件 [蠕虫、病毒、木马]
ID -- | 管道
中危 | 启用 | 规则模型 | 恶意软件

描述

【场景说明】
恶意软件（Malware），也称作恶意代码，是指那些旨在破坏计算机系统、窃取用户敏感信息、盗取账户密码或者其他恶意活动的软件程序。常见的恶意软件类型包括病毒、蠕虫、木马、间谍软件、广告软件等。
病毒（Virus）：病毒是一种能够自我复制并感染其他文件或程序的恶意软件。病毒通常会将自己附加到其他程序或文件上，以便在用户运行程序或打开文件时感染系统。病毒需要用户主动运行感染文件或程序才能生效，因此它们通常会通过电子邮件、下载的软件、可移动存储设备等途径传播。
蠕虫（Worm）：蠕虫是一种自我复制的恶意软件，与病毒不同的是，蠕虫可以在不需要用户干预的情况下自动传播。蠕虫通常会利用网络漏洞或弱密码等方式感染其他计算机，并在感染其他计算机后继续传播。蠕虫通常会占用大量网络带宽，导致网络拥塞或瘫痪。
木马（Trojan）：木马是一种隐藏在有用程序或文件中的恶意软件。它通常被设计成伪装成合法的程序，例如游戏、音乐、视频或其他应用程序，以欺骗用户下载或运行它，并在用户不知情的情况下执行恶意操作。木马通常是黑客攻击的初始入口，它可以为黑客提供远程访问目标计算机的权限，以进行各种攻击，如窃取敏感数据、安装其他恶意软件、控制计算机、进行勒索等。

【模型原理】
分析NIP攻击日志，将匹配到恶意软件(蠕虫、病毒、木马)签名的日志过滤冒泡出来。

【处置建议】
（1）断开网络连接。首先应该立即断开与互联网的连接，防止恶意软件进一步传播或者窃取您的敏感信息。
（2）运行杀毒软件。如果您已经安装了杀毒软件，可以立即运行杀毒软件进行扫描和清除恶意软件。
（3）使用系统还原。如果您的计算机系统支持系统还原功能，可以尝试使用系统还原将系统还原到之前的某个时间点，从而消除恶意软件的影响。
（4）手动清除恶意软件。如果杀毒软件无法清除恶意软件，可以尝试手动删除恶意软件。但是需要注意，手动清除可能会对系统造成不可逆的损害，因此建议在执行前备份重要数据和文件，以免造成数据丢失。
（5）重装操作系统。如果以上方法都无法清除恶意软件，最后的选择是重装操作系统。这是一种比较彻底的方式，可以消除系统中所有的恶意软件，并且可以重新建立一个干净的系统环境。

【使用约束】
依托nip攻击日志(sec-nip-attack)，需在安全云脑数据集成页面打开nip攻击日志接入开关。

防御绕过典型告警

- **描述**：

  当攻击者通过操作系统或应用程序中的安全漏洞获得系统的root权限后，攻击者会在侵入的主机中安装rootkit，常见的方式是通过加载特殊的驱动（windows）、安装内核模块（Linux）来修改系统内核，进而达到隐藏、操纵、收集数据等目的。在ATT&CK网站，Rootkit被列入Defense Evasion大类，即规避防御，其最终目的还是为了规避一些安全服务/软件的检测。

  安全云脑现有模型：**主机-恶意文件执行**、**主机-rootkit事件**，可以精准发现相关事件，快速进行告警减少失分。

图 2-39 主机-rootkit 事件

- **处理方案**：

  检测出恶意程序安装，建议您立即确认该程序安装是否正常业务引起。若非正常业务引起，建议您立即登录系统终止该恶意程序安装行为，利用主机安全告警信息全面排查系统风险，避免系统遭受进一步破坏。

权限维持典型告警

- **描述**：

  攻击者入侵成功后会进行权限维持获得持久权限，通常采用反弹shell、上传木马等方式进行权限维持。

  安全云脑现有模型：**主机-反弹shell**、**主机-恶意程序**、**网络-检测异常连接行为**，曾多次发现异常权限转发、控制行为，帮助我们及时处理相关问题，避免导致数据泄露、系统崩溃、网络瘫痪等严重后果。

图 2-40 主机-恶意程序

- **处理方案**：

  联系所属主机的责任人，登录到主机上停止恶意程序并删除恶意文件，同时进一步排查是否存在可疑进程，是否开放了可疑端口，是否有可疑连接等，并进一步检查自启动项，避免遗留，此外可以结合其他方式进行综合判断。

横向移动典型告警

- **描述**：

  攻击者在已经控制的一台计算机时，会通过横向移动或传播的方式，试图攻击其他计算机或系统，以获取更多的敏感信息或控制权，横向连接是一种常见的网络攻击手段。

  安全云脑现有模型：**主机-虚拟机横向连接**，可以快速识别失陷主机，精准定位受害情况，减少损失。

图 2-41 主机-虚拟机横向连接

- **处理方案**：

  建议通过堡垒机等审计记录查看该命令是程序执行还是人为操作，若为人为操作，需联系对应操作人确定，若为非正常业务人员操作，需尽快确定该行为是否为异常恶意行为，是否危害到对应虚拟机，及时采取措施，保护计算机和系统的安全。

持久化控制典型告警

- **描述**：

  黑客入侵成功后会在系统中留下的一个漏洞或隐藏的入口如修改计划任务等操作，攻击者可以利用这个漏洞或入口来绕过系统的安全防护措施，快速连接并获得系统的控制权。

  安全云脑现有模型：**网络-后门、主机-恶意定时任务写入**，可以防止黑客持久化控制进行长期的数据窃取、恶意软件传播、权限维持、挖矿等行为操作。

图 2-42 网络-后门

- **处理方案**：
  a. 断开网络连接。首先应该立即断开与互联网的连接，防止后门进一步传播或者窃取您的敏感信息。
  b. 使用杀毒软件进行扫描。您可以使用杀毒软件进行扫描和清除后门，确保系统的安全性。如果您没有安装杀毒软件，可以通过其他计算机下载杀毒软件并将其拷贝到感染的计算机上运行。
  c. 更新操作系统和软件。更新可以修复已知的漏洞和安全问题，提高系统的安全性。
  d. 查找和删除可疑文件。您可以查找和删除可疑文件，例如未知的程序或脚本文件，这些文件可能是后门的入口。

2.5.3 风险控制

操作场景

支持通过应急策略功能进行风险控制。

安全云脑的应急策略功能可以联动CFW/WAF/VPC安全组对源IP进行封堵和解封。当安全监控发现某个源IP正在攻击时，可以通过该功能进行全策略封堵。

操作步骤

步骤1 登录管理控制台。

步骤2 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。

步骤3 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 2-43 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“风险预防 > 策略管理”，进入策略管理页面后，选择“应急策略”页签，进入应急策略管理页面。

图 2-44 进入应急策略管理页面

步骤5 在应急策略管理页面中，单击“新增”，右侧弹出新增应急策略页面。

步骤6 在新增策略页面中，配置策略信息。

表 2-9 新增应急策略

参数名称	参数说明
阻断对象	输入需要阻断的单个（或多个）IP地址或IP地址段，如有多个IP地址或地址段，请使用英文逗号隔开。 填写示例： ● 单个IP地址：192.168.0.0 ● IP地址段：192.168.0.0/12
标签	自定义应急策略的标签。
操作连接	选择该策略的操作连接。
阻断老化	确认是否老化该条阻断。 ● 如果选择是，请设置策略老化时间，如设置为180天，即该策略在设置后的180天内有效，180天后将不再继续阻断设置的IP地址或IP地址段。 ● 如果选择否，则该策略将一直有效，阻断设置的IP地址或IP地址段。
原因描述	自定义该策略的描述信息。

步骤7 单击“确定”。

----结束

A 修订记录

发布日期	修改记录
2023-10-16	第二次正式发布。 新增**安全云脑护网/重保最佳实践**。
2023-06-20	第一次正式发布。