

态势感知

用户指南

用户指南

Agent插件

安装Agent

态势感知Agent插件是态势感知提供的本地插件，您需要在您的服务器操作系统上安装态势感知Agent插件，才能使用态势感知提供的安全防护服务。

阿里云公共镜像集成插件

态势感知Agent插件已集成于公共镜像中。如果您在购买ECS实例时，选择公共镜像并选择启用 **安全加固** 选项的话，态势感知Agent插件即默认通过镜像安装。



登录 云盾服态势感知控制台 > 资产列表，可以查看您所有服务器的保护状态，也就是态势感知Agent的在线/离线状态。

若您的服务器保护状态显示为离线，请按照以下方式，手动下载并安装态势感知Agent插件。

手动安装（支持非阿里云服务器）

注意：如果您已在服务器上安装了安全软件（如安全狗、云锁等），可能会导致态势感知Agent插件无法正常安装。建议您在安装态势感知Agent插件前，确认您的服务器上是否存在这类安全软件。如果存在，建议您暂时关闭或卸载该安全软件，然后再安装态势感知Agent插件。

前提条件

安装前，请确认您的服务器环境符合以下条件：

- 服务器在阿里云上，可以直接安装。
- 服务器不在阿里云上，与阿里云走Internet通信，应确保Internet连通。
- 服务器不在阿里云上，与阿里云通过专线连接走内网通信，则您需要在域名解析记录中添加以下DNS配置，指定态势感知服务端DNS：
100.100.25.3 jsrv.aegis.aliyun.com
100.100.25.4 update.aegis.aliyun.com

操作步骤

参照以下步骤，手动安装态势感知Agent插件：

登录 云盾态势感知控制台。

在左侧导航栏，单击 **设置**。

单击 **安装/卸载插件**，进入态势感知Agent页面。



根据您的服务器操作系统，选择安装步骤，获取并安装最新版本的态势感知Agent插件。

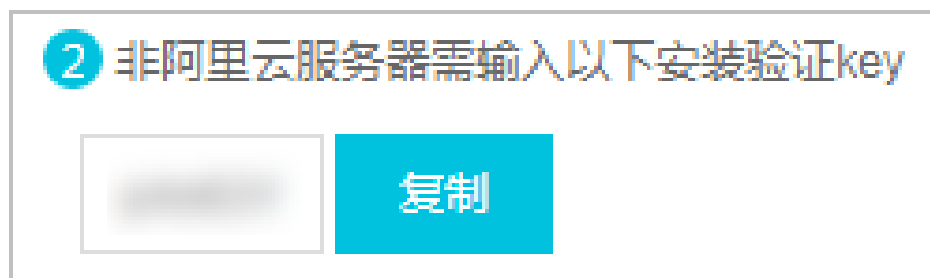
Windows系统

在态势感知Agent页面，单击 **点击下载**，下载最新版本态势感知Agent插件安装文件到本地计算机。

将安装文件上传至您的Windows服务器。例如，您可以通过FTP工具，将安装文件上传到服务器。

在您的Windows服务器上，以管理员权限运行态势感知Agent插件安装程序，完成安装。

注意：态势感知Agent插件安装过程中，您会收到提示，要求您输入安装验证Key。该安装验证Key用于关联您的阿里云账号，您可在云盾态势感知Agent页面找到您的安装验证Key。



Linux系统

根据您的实际情况，在态势感知Agent页面选择 **阿里云服务器** 或 **非阿里云服务器**。

以管理员身份登录您的Linux服务器。

根据您的操作系统类型，选择32位或64位的安装命令，并复制至您的Linux服务器上。

执行安装命令，完成态势感知Agent插件的下载及安装。

注意：该安装命令包含从阿里云站点下载最新版本的态势感知Agent插件，请确认您的服务器已连接公网。

态势感知Agent插件安装完成约五分钟后，您即可在云盾态势感知控制台上，查看您服务器的在线情况：

- 阿里云服务器将会从离线变成在线。
- 非阿里云服务器将会被添加至您的服务器列表中。

验证Agent安装

在您成功安装态势感知Agent后，建议您参照以下步骤进行验证：

检查您的服务器上态势感知Agent的AliYunDun和AliYunDunUpdate进程是否正常运行。关于态势感知Agent进程说明，请参考 [Agent说明](#)。

在您的服务器上，执行以下telnet命令，检查您的服务器是否能正常连通态势感知服务器。确保您的服务器能够连通至少一个jsrv和一个update服务域名。

- telnet jsrv.aegis.aliyun.com 80
- telnet jsrv2.aegis.aliyun.com 80
- telnet jsrv3.aegis.aliyun.com 80
- telnet update.aegis.aliyun.com 80
- telnet update2.aegis.aliyun.com 80
- telnet update3.aegis.aliyun.com 80

如果态势感知Agent安装验证失败，请参考 [Agent离线排查](#)。

注意事项

非阿里云服务器必须通过安装程序（Windows）或脚本命令（Linux）方式安装态势感知Agent插件。

如果您的非阿里云服务器通过以下方式安装态势感知Agent插件，则您需要删除态势感知Agent插件目录后，按照上述手动安装步骤重新安装态势感知Agent插件。

- 通过已安装态势感知Agent插件的镜像批量安装服务器。
- 从已安装态势感知Agent插件的服务器上直接复制态势感知Agent插件文件。

态势感知Agent插件文件目录

- Windows：C:\Program Files (x86)\Alibaba\Aegis
- Linux：/usr/local/aegis

金融云、VPC用户安装Agent

针对无法直接连通公网的云服务器（如阿里金融云上的服务器、或使用专有网络VPC的云服务器），您可通过以下步骤安装态势感知Agent。

安装步骤

注意：如果您已在服务器上安装了安全软件（如安全狗、云锁等），可能会导致态势感知Agent插件无法正常安装。建议您在安装态势感知Agent插件前确认您的服务器上是否存在这类安全软件。如果存在，建议您先关闭、或卸载该安全软件之后，再安装态势感知Agent插件。

登录 [云盾态势感知控制台](#)，单击 [设置](#)。

单击 **安装/卸载插件**，进入态势感知Agent页面。



根据您的服务器操作系统，选择安装步骤，获取并安装最新版本态势感知Agent插件。

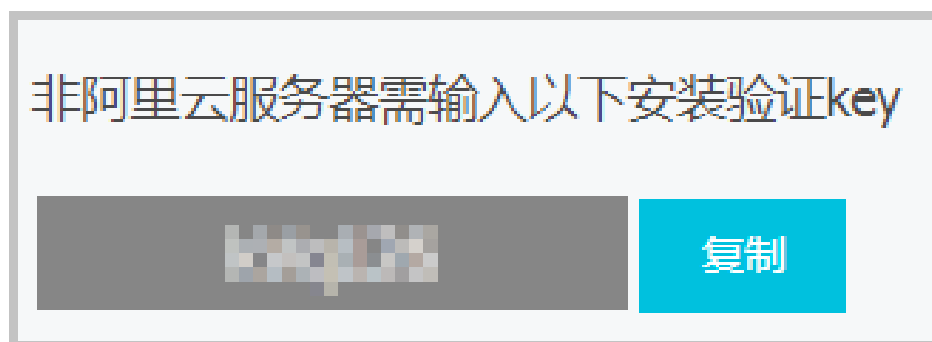
Windows 系统

在态势感知Agent页面，单击 **点击下载**，下载最新版本态势感知Agent插件安装文件到本地计算机。

将安装文件上传至您的Windows服务器。例如，通过FTP工具将安装文件上传到服务器。

在您的Windows服务器上，以管理员权限运行态势感知Agent插件安装程序，完成安装。

注意：态势感知Agent插件安装过程中可能会提示您输入安装验证Key。该安装验证Key用于关联您的阿里云账号，您可在云盾态势感知Agent页面找到您的安装验证 Key。



Linux系统

根据您的服务器的 Linux 系统版本，单击以下链接将态势感知Agent安装程序下载至本地计算机。

- **Linux 32 位系统**：态势感知Agent安装程序
- **Linux 64 位系统**：态势感知Agent安装程序

将态势感知Agent安装程序上传至您的Linux服务器。例如，通过FTP工具将安装文件上传到服务器。

以管理员身份登录您的Linux服务器。

定位到您已上传的态势感知Agent安装程序所在目录，根据您的服务器的Linux系统版本，执行以下命令安装态势感知Agent。

- **Linux 32 位系统**：chmod +x AliAqsInstall_32.sh &&
./AliAqsInstall_32.sh xxxxxx
- **Linux 64 位系统**：chmod +x AliAqsInstall_64.sh &&
./AliAqsInstall_64.sh xxxxxx

注意：此安装命令末尾处的xxxxxx为安装验证Key，执行安装命令时请根据您的云盾态势感知Agent页面中显示的六位安装验证Key替换xxxxxx部分。此安装验证Key与Windows系统安装步骤中的安装验证Key一致。该安装验证Key将用于关联您的阿里云账号，在云盾态势感知控制台登录您的阿里云账号，即可保护您的服务器安全。

4. 态势感知Agent插件安装完成约五分钟后，您即可在云盾态势感知控制台中查看您服务器的在线情况，您的服务器状态将会从离线变成在线。

验证Agent安装

在您成功安装态势感知Agent后，建议您参考以下步骤进行验证：

1. 检查您的服务器上态势感知Agent的AliYunDun和AliYunDunUpdate这两个进程是否正常运行。关于态势感知Agent进程说明，请参考 [Agent说明](#)。

在您的服务器上，执行以下telnet命令，检查您的服务器是否能正常连通态势感知服务器。

注意：确保以下两个服务器都能连通。

- telnet jsrv3.aegis.aliyun.com 80
- telnet update3.aegis.aliyun.com 80

如果态势感知Agent安装验证失败，请参考 [Agent离线排查](#)。

Agent说明

工作原理

态势感知Agent每隔五个小时会主动向态势感知服务器端上报一次在线数据信息。

如果态势感知Agent没有按时上报在线信息，态势感知服务器端则在12小时后判定该服务器不在线，并在态势感知控制台中将此服务器的保护状态更新为离线。

相关进程

态势感知Agent包含以下两个主要进程：

说明：态势感知Agent的进程在Linux系统的服务器上以root账号运行，在Windows系统的服务器上以system账号运行。

AliYunDun

此进程用于与态势感知服务器建立连接。

进程文件所在路径如下：

- **Windows 32位系统**：C:\Program Files\Alibaba\aeis\aeis_client
- **Windows 64位系统**：C:\Program Files (x86)\Alibaba\aeis\aeis_client
- **Linux 系统**：/usr/local/aeis/aeis_client

AliYunDunUpdate

此进程用于定期检测态势感知Agent是否需要升级。

进程文件所在路径如下：

- **Windows 32 位系统**：C:\Program Files\Alibaba\aeis\aeis_update
- **Windows 64 位系统**：C:\Program Files (x86)\Alibaba\aeis\aeis_update
- **Linux 系统**：/usr/local/aeis/aeis_update

Agent离线排查

如果您的态势感知Agent处于离线状态，请按照以下步骤进行排查：

登录您的服务器，查看态势感知Agent相关进程是否正常运行。

如果态势感知Agent相关进程无法运行，建议您重启服务器，或者参考 [安装Agent](#) 重新安装态势感知Agent。

Windows系统

在任务管理器中，查看相关进程是否正常运行。

映像名称	用户名
AliYunDun.exe	SYSTEM
AliYunDunUpdate.exe	SYSTEM

Linux系统

执行top命令，查看相关进程是否正常运行。

```
/usr/local/aegis/aegis_update/AliYunDunUpdate  
/usr/local/aegis/aegis_client/aegis_10_19/AliYunDun
```

对于首次安装态势感知Agent的服务器，如果其在安装Agent后，保护状态仍然为离线，请参考以下方法，重新启动态势感知Agent：

Linux 系统：执行killall AliYunDun && killall AliYunDunUpdate && /usr/local/aegis/aegis_client/aegis_10_xx/AliYunDun命令。

注意：您必须将命令中的xx替换为该目录下的最大的数字。

Windows 系统：在服务项中重新启动以下两个服务项，选中对应服务，右键选择重新启动即可。



检查您的服务器网络连接是否正常。

服务器有公网IP（如经典网络、EIP、云外机器）

- **Windows 系统**：在命令行中执行ping jsrv.aegis.aliyun.com -l 1000命令。
- **Linux 系统**：执行ping jsrv.aegis.aliyun.com -s 1000命令。

服务器无公网IP（如金融云、VPC专有网络）

- **Windows 系统**：在命令行中执行ping jsrv3.aegis.aliyun.com -l 1000命令。
- **Linux 系统**：执行ping jsrv3.aegis.aliyun.com -s 1000命令。

如果解析不通，请使用以下方法，检查您的服务器网络连接状况：

确认您的服务器的DNS服务正常运行。

如果DNS服务无法运行，请您重启您的服务器，或者检查服务器DNS服务是否有故障。

检查服务器是否设置了防火墙ACL规则或阿里云安全组规则。

如果有，请确认已将态势感知的服务端IP加入防火墙白名单（出、入方向均需添加）以允许网络访问。

注意： 请将下列IP段的80端口添加至白名单，最后一个IP段需要同时添加80和443端口至白名单。

- i. 140.205.140.0/24 80
- ii. 106.11.68.0/24 80
- iii. 110.173.196.0/24 80
- iv. 106.11.68.0/24 80
- v. 100.100.25.0/24 80 443

检查您的服务器公网带宽是否为零。

如果您的服务器公网带宽为零，请参考以下步骤进行解决：

在您服务器的hosts文件添加以下域名解析记录：

- a. 100.100.25.3 jsrv.aegis.aliyun.com
- b. 100.100.25.4 update.aegis.aliyun.com

修改hosts文件后，执行ping jsrv.aegis.aliyun.com命令。

注意： 如果返回的结果不是100.100.25.3，请您重启服务器或检查服务器DNS服务是否有故障。

如果仍然无法解析到正确的IP，您可以尝试修改态势感知Agent安装目录下conf目录中的network_config配置文件，将t_srv_domain、h_srv_domain对

应的值分别修改为100.100.25.3及100.100.25.4。修改完成后，重启态势感知Agent进程。

注意： 修改前请务必备份network_config配置文件。

此方法只适用于公网带宽为零，且态势感知Agent处于离线状态的服务器。

如果Ping命令执行解析成功，再次尝试通过Telnet命令连接解析出的域名IP的80端口（例如，执行telnet 140.205.140.205 80命令），查看是否连通。如果无法连通，请确认防火墙是否存在相关限制。

检查您的服务器CPU、内存是否长期维持较高占用率（如 95%、100%），此情况可能导致态势感知Agent进程无法正常工作。

检查服务器是否已安装第三方的防病毒产品（如安全狗、云锁等）。部分第三方防病毒软件可能会禁止态势感知Agent插件访问网络。

如果有，请暂时关闭该产品，并重新安装态势感知Agent。

卸载Agent

如果您决定不再使用云盾态势感知服务的安全防护功能，您可以选择以下方式来卸载态势感知Agent。

注意： 卸载态势感知Agent后，请耐心等待六个小时，然后该服务器在态势感知控制台上的保护状态才会变更为离线。

自动卸载态势感知Agent

您可以通过以下方式，在云盾态势感知控制台上，自动卸载态势感知Agent。

注意： 如果您在卸载Agent插件后需要重新安装它，请进行手工安装，并忽略期间的报错，重复操作3次以上。因为态势感知在卸载后会有一段24小时的保护期，期间重新安装时需要重复执行3次以上安装命令。

前提条件

请务必确保态势感知Agent在当前主机上处于在线状态，否则该主机无法接收到卸载指令。

操作步骤

参照以下步骤，自动卸载态势感知Agent插件：

登录 云盾态势感知控制台。

在左侧导航栏，单击 **设置**。

单击 **安装/卸载插件**，进入态势感知Agent页面。

单击页面右上方的 **卸载插件**。

在弹出的 **卸载提示** 对话框中，选择您决定卸载态势感知Agent的服务器，单击 **确认卸载**。

系统将自动卸载您选择的服务器上的态势感知Agent。

手动卸载态势感知Agent

您也可以参考以下步骤手动卸载您服务器上的态势感知Agent。

Linux系统服务器

登录您的Linux系统服务器。

执行以下命令下载态势感知Agent卸载脚本。

```
wget http://update.aegis.aliyun.com/download/uninstall.sh
```

依次执行以下命令，卸载态势感知Agent。

- chmod +x uninstall.sh
- ./uninstall.sh

Windows系统服务器

登录您的Windows系统服务器。

在您的服务器上下载 态势感知Agent卸载脚本。

注意：您也可以将态势感知Agent卸载脚本文件下载至本地计算机后，通过FTP文件传输工具，将脚本文件上传至您的服务器后执行卸载。

双击uninstall.bat文件执行脚本，卸载态势感知Agent。

资产列表

在态势感知控制台的资产列表页面，您可以查看态势感知已防护的服务器的安全状态。为了方便您对特定服务器资产进行安全管控，资产列表提供了资产分组和标签分类的功能。您可以将资产分组，以组别的维度查看安全事件；也可以通过资产标签来筛选查看具有相同属性的资产。

本文介绍了资产列表的操作方法，包括以下内容：

- 查看资产保护状态
- 暂停/开启保护
- 一键安全检查
- 管理分组
- 添加资产到指定组
- 添加/编辑标签
- 删除非阿里云机器

操作步骤

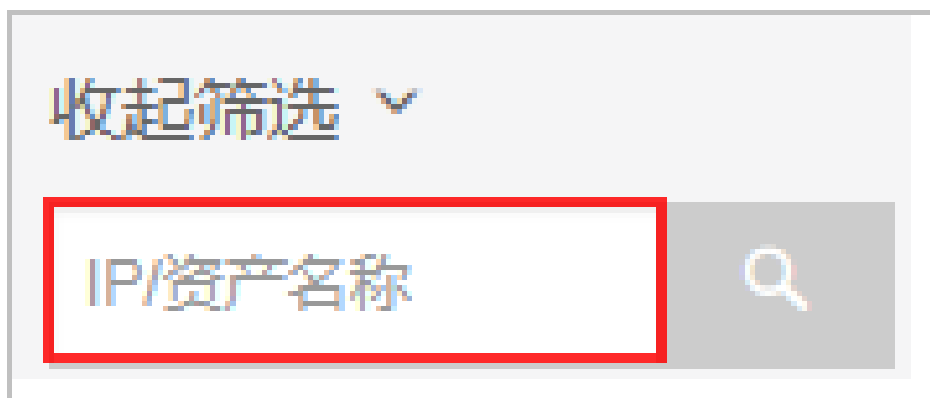
查看资产保护状态

参照以下步骤，查看您的资产保护状态：

登录 云盾态势感知控制台。

在左侧导航栏，单击 **资产列表**，查看态势感知已防护的服务器的保护状态。您也可以展开筛选栏，使用搜索和筛选功能快速定位到特定资产。

在左上角的搜索框中输入一个服务器的IP进行搜索，查看某台服务器的安全状态。



使用 **资产类型**、**标签**、**地域**、**安全状态**、**Agent**、**操作系统**、**所有分组** 筛选项，筛选出特定服务器。

说明：当筛选项中的子项太多，导致不便查找时，您可以使用筛选项右侧的排序按钮进行排序（**所有分组** 不支持此操作）。资产列表筛选项支持的排序方式包括A to Z/Z to A（筛选项名称字母组合升序、降序），1 to 9/9 to 1（筛选项下的资产数量升序、降序）。



单击上述筛选项下的任意子项，直接显示筛选结果。例如，单击 **地域** 下的 **华东1**，直接显示华东1下的服务器。

勾选一个筛选项下的多个子项，并单击该筛选项下的 **应用**，可筛选一个筛选项下的多个结果。例如，勾选 **地域** 下的 **华东1** 和 **华北1**，并单击 **地域** 下的 **应用**，可以显示华东1和华北1下的服务器。

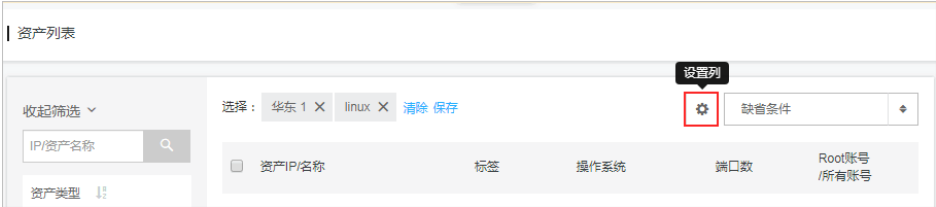


同时应用多个筛选项。例如，已限制 **地域** 为 **华东1** 以后，可以再限制 **操作系统** 为 **linux**，只显示华东1地域中的Linux系统的服务器。

说明：对于已应用的筛选项组合，您可以选择将其保存为常用筛选条件。单击 **保存**，为该筛选条件命名（例如华东1，Linux）后，就可以在页面右上角的条件框中直接选用该筛选条件。



单击 **资产列表** 页右上角的 **设置列** 按钮，可以设置需要显示的列内容。





暂停/开启保护

如果您在一段时间内不希望态势感知Agent占用您的ECS服务器的资源，您可以参照以下步骤，暂停对该服务器的安全防护：

在 **资产列表** 中，勾选一个或多个 **保护状态** 为 **在线** 的目标服务器。

单击 **资产列表** 下方的 **更多操作** > **暂停保护**。



暂停保护后，态势感知Agent插件停止工作，不再收集上报您服务器上的安全信息，也不再占用系统资源。您可以通过 **更多操作** > **开启保护**，对暂停保护的服务器重新开启保护。

一键安全检查

在 **资产列表** 使用 **一键安全检查** 功能，可以对指定服务器立即执行安全扫描，更新其漏洞信息、基线配置风险信息、及资产清点信息。您可以参照以下步骤，使用一键安全检查：

在 **资产列表** 中，勾选一个或多个目标服务器。

单击 **资产列表** 下方的 **一键安全检查**。

在 **安全检查** 对话框，勾选需要执行的检查项目。



单击 **确认**，执行检查。

一键安全检查结束后，最新的检查结果会自动更新到态势控制台。

管理分组

如果您的账号在 **资产列表** 下存在多台服务器资产，为方便您快速定位到多个对象，或对多个对象执行批量操作，建议您使用分组功能，为同类型的资产创建一个分组。参照以下步骤，创建和管理资产分组：

展开筛选栏后，在 **资产列表** 页左下角，单击 **所有分组** 右侧的 **管理**，打开 **资产分组管理** 对话框。

创建资产分组。



说明：未进行资产分组时，您所有的服务器资产都在 **未分组** 中。当您删除某个分组时，该分组中的资产也默认被移入 **未分组**。

- i. 单击 **添加一级分组**。
- ii. 输入组名称，并单击 **确认**。
- iii. 对于已创建的一级分组，单击其右侧的 **+** 可创建子分组。您也可以重命名或者删除该一级分组。
注意：最多可支持三级资产子分组。

资产分组排序。当同一级别具有多个分组时，单击一个分组右侧的 **↑** 和 **↓** 可调整该分组的显示位置。

删除分组。当您不再需要某个分组时，单击其右侧的 **×** 可删除该分组。

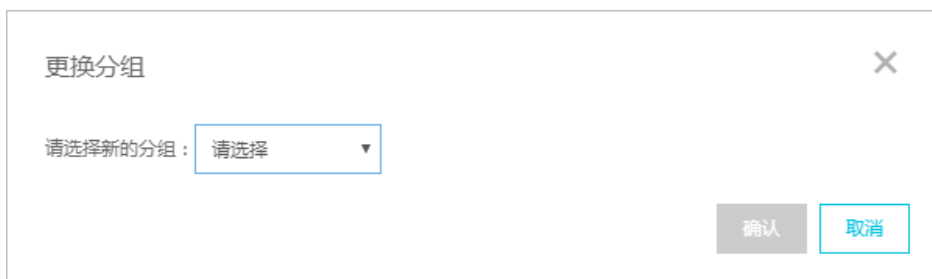
注意：删除分组（含子分组）后，该分组（和子分组）内的机器将被转移到 **未分组**。

添加资产到指定组

您可以将多个同类型资产添加到一个分组中，便于对这些资产执行批量操作，如在配置主机基线检查策略模板时，按组别配置生效服务器。在 **资产列表**，您也可以使用组别筛选特定资产。参照以下步骤，将资产添加到指定资产组中：

在 **资产列表** 页，勾选一个或多个服务器资产，单击资产列表下方的 **更换分组**。

选择一个新的资产分组，将选定的服务器资产划分到该分组。

该对话框用于更改资产分组。它包含一个标题“更换分组”、一个关闭按钮（X）、一个提示“请选择新的分组：”、一个下拉菜单（显示“请选择”）、以及“确认”和“取消”两个按钮。

更换分组

请选择新的分组：

请选择

确认

取消

注意：服务器资产与子分组不能归属在同一级资产分组。例如，资产分组A下已有子分组B，则您无法将服务器资产C放至资产分组A中。

单击 **确认**，完成更换分组。

添加/编辑标签

为您的资产添加标签，能够标识其特殊属性，也可用于在 **资产列表** 中筛选特定资产。参照以下步骤，为资产添加标签：

在 **资产列表** 页，选择一个服务器资产。

单击其 **标签** 列下的标签按钮，并单击 **添加**。

输入标签名或选择已有标签，支持添加多个标签。

单击 **确认**，完成添加。

勾选一个或多个已有标签的服务器资产，单击资产列表下方的 **编辑标签**，可以修改其标签。

删除非阿里云机器

如果您不希望态势感知继续防护您的非阿里云主机的安全，您可以从资产列表中移除该非阿里云主机。

说明：对于阿里云ECS服务器，即使您卸载了Agent插件，该服务器仍将以离线状态出现在资产列表中，不会被移除。

参照以下步骤，从资产列表中移除非阿里云机器：

在 **资产列表** 中，勾选一个或多个非阿里云服务器。

选择 **资产列表** 下方的 **更多操作 > 删除非阿里云机器**。



单击 **确定**，系统会在自动卸载安装在您服务器上的Agent插件，并将目标服务器中资产列表中移除。

安全告警

态势感知监测您服务器的安全状态，提供对常见网络入侵行为的检测和告警，帮助您了解和处理服务器安全隐患。

查看和处理告警

安全告警检测和记录以下网络入侵行为：

异常登录：检测服务器上的登录行为，通过设置并应用合法登录IP、时间及账号，对于例外的登录行为进行告警。支持手动添加和自动更新常用登录地，对指定资产的异地登录行为进行告警。

网站后门：使用自主查杀引擎检测常见后门文件，支持定期查杀和实时防护，并提供一键隔离功能。

- Web目录中文件发生变动会触发动态检测，每日凌晨扫描整个Web目录进行静态检测。
- 支持设置木马查杀区域。
- 对发现的木马文件，支持隔离、恢复和忽略等处理操作。

主机异常：查看在您服务器检测到的异常进程行为、敏感文件篡改、异常网络连接、异常事件和可疑文件等。

恶意进程（病毒云查杀）：采用云+端的查杀机制，客户端负责捕获进程启动信息，上报到云端控制中心进行病毒样本检测；若判断为恶意进程，客户端决定对恶意进程处置方式（停止进程、隔离文件）。

操作步骤

参照以下步骤，查看和处理您服务器上的网络入侵：

登录 态势感知控制台。

在左侧导航栏，选择 **安全告警**。

在事件列表中查看所有检测到的网络入侵。使用搜索和页签筛选功能可以快速定位到特定事件。例如，您可以使用服务器IP或名称、事件名称搜索相关事件。



对不同类型的事件，进行相应处理。

- 异常登录：确认该登录记录后，单击 **标记为已处理**。
- 网站后门：选择 **隔离** 或 **忽略** 该后门文件。被隔离文件可通过页面右上角的 **文件隔离箱** 进行查看。
注意：被成功隔离的文件在30天内可进行一键恢复，过期系统将自动清除。
- 异常网络连接、进程异常行为、敏感文件篡改：选择 **忽略本次**、**确认事件** 或 **标记为误报**，标记为误报的事件可以 **取消标记误报**。
- 恶意进程（云查杀）：选择 **木马在线处理**、**忽略本次**、**确认事件** 或 **标记为误报**，标记为误报的事件可以 **取消标记误报**。

安全告警设置

安全告警设置支持手动维护常用登录地和Web目录，也允许您设置安全告警等级范围和配置高级登录报警功能。

说明：高级登录报警只有在企业版服务中提供，允许您配置更精细的异常登录检测，例如限制合法登录的IP、时间、账号。

操作步骤

参照以下步骤，进行安全告警设置：

登录 态势感知控制台。

在左侧导航栏，选择 **安全告警**。

单击页面右上角 **安全告警设置**，进行配置：

添加常用登录地

a. 单击 **常用登录地** 下的 **添加**。

常用登录地		添加
深圳市	生效服务器：3台	编辑 删除
澳门特别行政区	生效服务器：0台	编辑 删除
共有 13 条,每页显示 5 条		« < 1 2 3 > »

b. 选择一个登录地点，然后选择添加该地点为常用登录地的服务器或服务器组。

添加常用登录地

请选择要添加的常用登录地：

请选择 ▼

请添加应用的服务器：

全部资产 分组资产

输入关键词进行搜索 🔍

☐ 全部

☐ [模糊资产名称]

取消 确定

c. 单击 **确定**，完成添加。

成功添加的常用登录地，您可以对其 **编辑** 和 **删除**。

- 单击一个常用登录地下的 **编辑**，修改该登录地的生效服务器。
- 单击一个常用登录地下的 **删除**，删除该常用登录地配置。

配置高级登录报警

说明：使用高级登录告警，您可以进一步指定合法的登录IP、时间段、和账号，态势感知会对指定外的登录情形进行告警。以下功能的操作类似 **常用登录地** 配置，您可以参考上文进行 **添加**、**编辑**、**删除** 操作。

- 单击 **合法登录IP** 下的切换开关，开启/关闭登录IP检查，开启后通过非指定IP登录会触发报警。

合法登录IP

非合法登录IP报警：☒

添加

	生效服务器：0台	编辑	删除
	生效服务器：1台	编辑	删除

共有 4 条,每页显示 5 条

«

<

1

>

»

- 单击 **合法登录时间** 下的切换开关，开启/关闭登录时间检查，开启后在非指定时间登录会触发报警。

合法登录时间

非合法登录时间报警：☒

添加

01:00 - 02:00	生效服务器：1台	编辑	删除
22:00 - 23:59	生效服务器：1台	编辑	删除

共有 2 条,每页显示 5 条

«

<

1

>

»

- 单击 **合法账号** 下的切换开关，开启/关闭登录账号检查，开启后使用非指定账号登录会触发报警。

合法账号

非合法账号登录报警：☒

添加

root	生效服务器：1台	编辑	删除
admin	生效服务器：1台	编辑	删除

共有 2 条,每页显示 5 条

«

<

1

>

»

定义Web目录

态势感知会自动检测您服务器资产中的Web目录，并进行动态检测和静态扫描；您也可以手动添加服务器中的其它Web目录进行检测扫描。

- a. 单击 **Web目录定义** 下的 **添加**。

Web目录定义（如下目录列表为自动识别，如缺少请手动添加）

添加

☐	木马文件路径	对应服务器	来源	操作
☐		1	系统自动识别	--
☐	/c	1	手动添加	编辑 删除

- b. 输入一个合法的Web路径，然后选择生效服务器，即将该路径添加为扫描路径的服务器。

注意：出于性能效率考虑，不支持直接添加root目录作为Web目录。

添加Web路径

×

请填写要添加的合法路径：

请添加应用的服务器：

全部资产

输入关键词进行搜索

47.104.6.205 (陌浅_游戏盾回源测试勿删)

取消

确定

- c. 单击 **确定**，完成添加。

设置安全告警等级范围

在 **安全告警设置** 栏最下方，勾选需要检测的安全事件的严重程度。

安全告警等级范围：☒ 紧急 ☒ 可疑 ☒ 提醒

等级范围包括以下：

- **提醒：**需要确认的安全事件，如创建新账号等。
- **可疑：**可能发生入侵行为的安全事件，如ECS异地登录等。
- **紧急：**存在黑客成功攻击的安全事件，如恶意进程运行，发生拒绝服务等。

主机漏洞管理

态势感知提供全面的漏洞检测和修复服务，分为主机漏洞管理和网络漏洞扫描。主机漏洞管理自动检测您服务器系统上的漏洞；网络漏洞扫描通过公网模拟攻击的方式，主动探测您服务器上的Web漏洞。

本文介绍了主机漏洞管理的功能及操作方法。关于网络漏洞扫描，请参考 [网络漏洞扫描](#)。

漏洞检测与修复

主机漏洞管理针对服务器系统漏洞提供检测和修复服务，可处理以下四类漏洞：

Web-CMS漏洞

通过云端最新漏洞补丁库，提供漏洞自动检测和一键修复功能。

- 自动扫描漏洞，上报检测结果，并推送告警信息。
- 通过一键替换通用Web文件（MD5值识别）实现漏洞修复。
- 对于手动修复的漏洞，支持验证是否修复成功。对于修复完成漏洞，支持回滚，用来还原修复前的Web文件。

Linux软件漏洞

比对CVE官方漏洞源，自动检测您服务器上安装的软件版本是否存在漏洞，并向您推送漏洞消息。针对检测到的漏洞，提供漏洞修复指令和验证功能。

Windows系统漏洞

比对微软官方补丁更新，自动检测您服务器上的补丁是否已更新，并向您推送漏洞消息。针对重大漏洞更新，提供自动检测和修复功能。

其他漏洞

自动检测服务器上的Redis未授权访问漏洞、STRUTS-052命令执行漏洞等漏洞，并向您推送漏洞消息。同时，支持漏洞的修复验证操作。

操作步骤

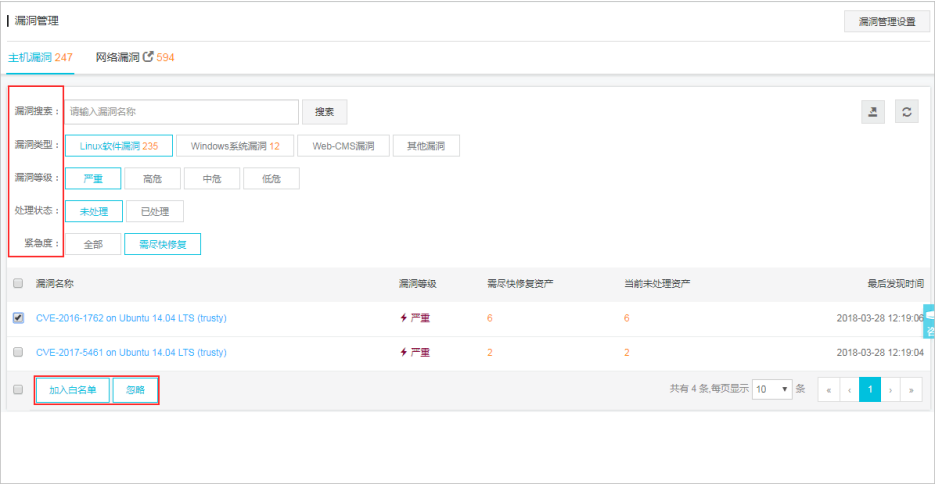
参照以下步骤，查看和修复服务器操作系统（Linux和Windows）和内容管理系统上存在的漏洞：

登录 [云盾态势感知控制台](#)。

在左侧导航栏，选择 **漏洞管理**。

在 **主机漏洞** 分页下，查看所有主机漏洞。使用漏洞搜索和分类页签功能，快速定位到具体漏洞。例如：

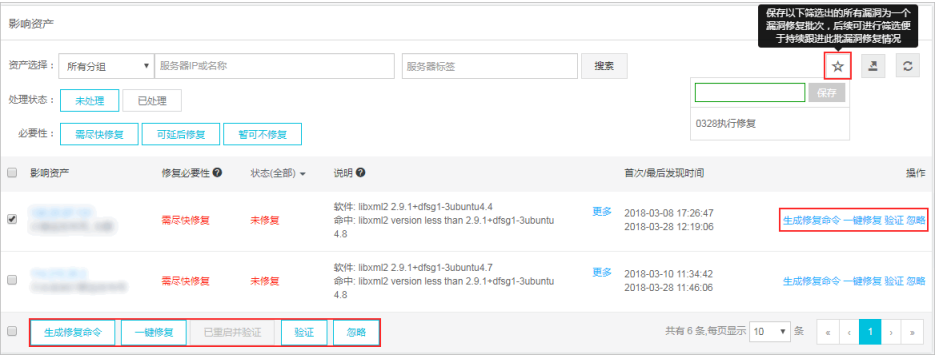
- 输入漏洞名称，搜索相关漏洞。
- 选择对应页签，可以快速定位到**未处理**，且**需尽快修复的**，**严重的Web-CMS漏洞**等。



如果您不希望收到特定漏洞的告警信息，您可以勾选该漏洞，单击漏洞列表下方的 **忽略**，忽略该漏洞告警；如果您想彻底忽略特定漏洞，即不希望态势感知去检测该漏洞，您可以勾选该漏洞，单击漏洞列表下方的 **加入白名单**，系统不会去检测白名单中的漏洞。

单击漏洞名称，进入漏洞详情页，查看漏洞详细信息和影响资产。

根据漏洞类型，选择相应处理方式：



说明：您可以使用 **操作** 列提供的操作，针对单个受影响服务器进行处理；也可以勾选一个或多个需要处理的服务器，使用列表下方的批量操作按钮进行批量处理。

说明：如果您想分批次来修复漏洞，您可以使用 **影响资产** 页面右上角提供的批次管理工具。输入一个批次名称，并单击 **保存**，将筛选出来的漏洞保存为一个漏洞修复批次；后续您可以直接使用批次记录来筛选目标服务器，持续跟进此批漏洞的修复情况。

Linux软件漏洞

- 单击 **一键修复** 直接修复该漏洞，或者单击 **生成修复命令** 自动生成修复漏洞的指令，然后登录您的服务器运行该指令来修复漏洞。
注意：如果漏洞修复需要重启服务器才能生效，您必须等待漏洞修复 **状态** 变为 **修复成功待重启** 后，重启该服务器，然后单击 **已重启并验证** 完成修复。
- 单击 **忽略**，可忽略该漏洞，系统将不再上报并告警此服务器上被忽略的漏洞。
- 修复漏洞后，单击 **验证**，一键验证该漏洞是否已修复成功。如果您未进行手动验证，漏洞修复成功后 48 小时内系统会自动去验证。

Windows系统漏洞

- 单击 **立即修复**，修复该漏洞。系统会在云端缓存一份Windows官方补丁文件，您的Windows系统服务器会直接下载云端的补丁并完成自动更新。
注意：如果漏洞补丁更新后需要重启服务器才能生效，您必须等待漏洞修复 **状态** 变为 **修复成功待重启** 后，重启该服务器，然后单击 **已重启并验证**。
- 单击 **忽略**，可忽略该漏洞，系统将不再上报并告警此服务器上被忽略的漏洞。
- 如果您在服务器上已更新了漏洞补丁，您可单击 **验证**，验证该漏洞是否已经修复。

Web-CMS漏洞

- 单击 **立即修复**，系统将替换您服务器上存在漏洞的Web文件以修复Web-CMS漏洞。
注意：修复Web-CMS漏洞前，建议您备份该漏洞相关的Web文件。您可参考漏洞处理说明栏中的路径，备份相关的Web文件。
- 单击 **忽略**，可忽略该漏洞，系统将不再上报并告警此服务器上已被忽略的漏洞。
- 漏洞修复后，单击 **验证**，可一键验证该漏洞是否已修复成功；如果您未进行手动验证，漏洞修复成功后 48 小时内系统会自动验证。
- 对于已修复完成的漏洞，单击 **回滚** 可进行漏洞回滚，还原修复前的Web文件。

其他漏洞

- 单击 **忽略**，忽略该漏洞，系统将不再上报并告警此服务器上已被忽略的漏洞。
- 按照修复说明手动修复该漏洞后，单击 **验证**，可一键验证该漏洞是否已经修复。如果您未进行手动验证，漏洞修复成功后 48 小时内系统会自动验证。

漏洞管理设置

漏洞管理设置允许您开启/关闭不同类型漏洞的自动检测，有选择性地对指定服务器应用漏洞检测，对已失效漏洞设置自动删除周期，和配置漏洞白名单。

漏洞白名单用于彻底忽略某些漏洞，您可以在漏洞列表下批量添加漏洞至白名单。添加成功后，系统将不再去检测漏洞白名单中的漏洞。使用漏洞管理设置可以维护漏洞白名单。

操作步骤

登录 云盾态势感知控制台。

在左侧导航栏，选择 **漏洞管理**。

在 **主机漏洞** 分页下，单击 **漏洞管理设置** 进行配置。您可以执行以下操作：

漏洞管理设置

Linux软件漏洞：共114台（已全部开启）[管理](#)

Windows漏洞：共114台（还有2台未开启）[管理](#)

Web-CMS漏洞：共114台（还有108台未开启）[管理](#)

其他漏洞：共114台（还有1台未开启）[管理](#)

扫描漏洞等级范围：☒ 严重 ☒ 高危 ☒ 中危 ☒ 低危

失效漏洞自动删除：

30天

漏洞白名单配置：

☐	漏洞名称	操作
☐	Microsoft.NET Framework安全更新	移除
☐	CVE-2017-7526 on Ubuntu 16.04 LTS (xenial) - medium.	移除
☐	移除	

共有 6 条,每页显示 10 条

<<<1>>>

- 选择需要操作的漏洞类型，单击其切换开关，开启/关闭该漏洞检测。
- 选择需要操作的漏洞类型，单击其 **管理**，配置应用该漏洞检测的服务器。
- 勾选需要扫描的漏洞等级：严重、高危、中危、低危。
- 选择失效漏洞自动删除周期：7天、30天、90天。
说明：对于检测出来的漏洞不做任何处理的话，默认该告警失效，并在指定周期后自动删除。
- 在漏洞白名单下勾选相应漏洞，单击 **移除**，重新启用对该漏洞的检测和告警。

网络漏洞扫描

态势感知提供全面的漏洞检测和修复服务，分为主机漏洞管理和网络漏洞扫描。主机漏洞管理自动检测您服务器系统上的漏洞；网络漏洞管理通过公网模拟攻击的方式，主动探测您服务器暴露在公网上的安全漏洞。

本文介绍了网络漏洞扫描的操作方法。关于主机漏洞管理请参考 [主机漏洞管理](#)。

网络漏洞扫描

网络漏洞扫描系统（AVDS）通过公网模拟黑客入侵攻击，对您的服务器进行Web漏洞扫描。在使用网络漏洞扫描前，您必须先添加和验证您的网络资产。

操作步骤

参照以下步骤，添加和验证资产并启动Web漏洞扫描：

登录 云盾态势感知控制台。

在左侧导航栏，选择 **漏洞管理**。

单击 **网络漏洞** 前往网络漏洞管理页面。

前往 **资产** 页，单击页面右上角的 **添加资产**，添加扫描对象。

添加资产域名，并单击 **下一步**。多条域名间以分号（;）分隔。

完成资产认证。您可以选择邮箱验证、文件验证（添加的是子域名）和CNAME验证（添加的是主域名）。

完成认证后，单击 **确定**。

验证审核成功的资产可自动进行资产发现。回到 **资产列表**，单击资产下的 **资产清单** 可查看所有自动发现的资产信息，包括资产子域名、对应的IP地址、端口、服务、操作系统、中间件等。

前往 **扫描** 页，单击 **新建扫描任务**，创建并配置扫描任务。配置参数如下：

新扫描任务

任务名称：

regular scan

扫描目标：

组

资产

全部

未分组 ×

扫描模式：

☐ 资产模式

☒ 标准模式

☐ 深度模式

扫描速度：

☐ 快速

☒ 常速

☐ 慢速

扫描频率：

☐ 单次任务

☒ 周期任务

扫描周期：

每周一次

开始时间：

2018-03-28

结束时间：

2018-03-28

扫描时间段：

00

:

00

至

02

:

00

取消

确定

任务名称：为任务命名，用于识别任务。

扫描目标：支持对单独资产和资产组进行扫描。

扫描模式：可以根据实际需求选择资产模式、标准模式、深度模式。

资产模式：仅用于资产识别，可自适应地分析您暴露在互联网上的资产信息，包括域名、子域名、IP、系统类型、端口服务指纹、WEB应用指纹等。

标准模式：仅启用经过严谨设计的扫描插件，几乎不存在侵入性的风险，但所发现的漏洞也会较深度模式少。

深度模式：启用所有扫描插件，会进行深度页面爬取，所检测的漏洞范围更全面，耗时较长，且部分插件具有渗透性。如果您的网站存在漏洞，可能会对网站造成影响，需谨慎启用。建议您在非业务环境，如上线前使用。如需业务环境使用，建议您尽量避开业务高峰期。

触发类型：设置为单次任务或者周期任务。

开始时间：设置任务启动时间。

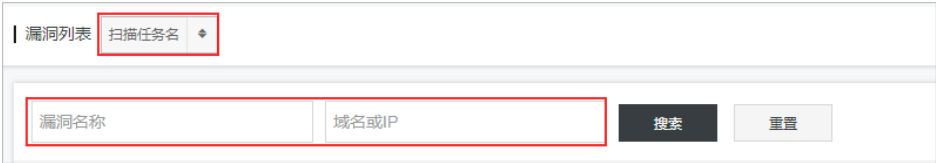
扫描周期：设置为周期任务时配置，选择每天一次、每周一次、每月一次。

扫描间隔：设置为周期任务时配置，选择每多少扫描周期（每天/每周/每月）进行一次扫描。

结束时间：设置为周期任务时配置，设置任务结束时间。

单击 **确定** 完成任务配置，并等待扫描任务完成。

前往 **漏洞** 页，在**漏洞列表**，选择扫描任务，查看扫描结果。您也可以通过 **漏洞名称**、**域名或IP**进行搜索。



单击漏洞名称，查看漏洞详细信息，在 **安全建议** 中提供了漏洞修复方法。

返回漏洞列表，在 **操作** 列，选择相应处理方式：

☐	漏洞名称	威胁程度(全部)	状态(全部)	影响资产	最后发现时间	操作
☐	信息泄露 - WEB目录开放浏览	中危	未修复	10.10.10.10	2018-02-07 06:53:11	修复 忽略 标记误报
☐	WEB程序未启用CSRF保护	中危	未修复	10.10.10.10	2018-02-07 05:55:13	修复 忽略 标记误报

- 参照 **安全建议** 完成修复操作后，单击 **修复**，修改该漏洞状态。
- 在确认不需要该告警通知时，单击 **忽略**，忽略该漏洞告警。
- 在确认您的系统不存在相应漏洞时，单击 **标记误报** 进行反馈。

漏洞扫描设置

网络漏洞扫描支持以下设置：

- 告警方式：选择告警通知等级和通知方式。
- 扫描全局开关：暂停所有扫描。

操作步骤

参照以下步骤，进行漏洞扫描设置：

登录 云盾态势感知控制台。

在左侧导航栏，选择 **漏洞管理**。

单击 **网络漏洞** 前往网络漏洞管理页面。

单击 **设置** 进入设置页面，您可以执行以下操作：

- 勾选漏洞告警通知等级：高危、中危、低危、提示。
- 勾选通知方式：短信、邮件、站内信。
- 在 **扫描全局开关** 下单击 **暂停所有扫描**，中断扫描。

主机基线检查

态势感知基线检查功能自动检测您服务器和云产品上存在的风险配置项，并为您提供修复建议。该功能分为主机基线检查和云产品基线检查。

主机基线检查自动检测您服务器上系统、账号、数据库、弱密码、合规性配置中存在的风险点，并针对所发现的问题项为您提供修复建议。本文介绍了使用主机基线检查来检测并修复您服务器上不安全配置的操作方法。关于云产品基线检查，请参考 [云产品基线检查](#)。

功能说明

主机基线检查功能在启用后，自动检测服务器上的系统、账号、数据库、弱密码、合格性配置中存在的风险点，并提供修复建议。具体检查内容，参见文末 [主机基线检查检测内容](#)。

主机基线检查的默认策略为每一天进行一次全面自动检测，在凌晨0到6点间完成。您可以自行添加和维护检测策略模板，自定义需要检查的项目、生效的服务器、检查周期、和触发时间。

注意：某些检测项（例如，MySQL弱密码检测、SQLServer弱密码检测），可能采用尝试登录的方式进行检查，从而会占用一定的服务器资源，生产较多的登录失败记录。这些检查项目默认是关闭。如果您需要这些功能，请确认上述风险后，自定义主机基线检查策略模板，并勾选这些项目。

主机基线检查也支持白名单设置，允许您彻底忽略某些主机基线检查项目，态势感知不会检测主机基线检查白名单中的项目。加入白名单或忽略操作支持填写备注，以便后续查看。

操作步骤

参照以下步骤，查看并修复您服务器上的风险配置项：

登录 云盾态势感知控制台。

在左侧导航栏，单击 **基线检查**。

在 **主机基线** 分页下，查看您服务器上存在的配置风险项。您可以使用风险搜索和页签筛选功能，快速定位到具体风险。



如果您不希望收到特定风险的告警信息，您可以勾选该风险项，单击风险列表下方的 **忽略**，忽略该风险告警；如果您想彻底忽略特定风险，即不希望态势感知去检测该风险，您可以勾选该风险，单击风险列表下方的 **加入白名单**，系统不会去检测白名单中的风险。

选择一个风险项，单击其名称，进入风险详情页面，查看该风险的详细信息和受影响的资产。

参照 **风险详情 > 更多** 下的加固建议，在对应服务器上进行修复。



说明：您可以勾选一个或多个受影响资产，使用 **影响资产** 列表下方的批量操作按钮进行批量操作。

修复风险后，您可以单击 **操作** 列中的 **验证**，一键验证该风险是否已修复成功。如果您未进行手动验证，风险修复成功后 72 小时内态势感知会进行自动验证。

如果您不希望收到该风险项的告警，您可以单击 **操作** 列中的 **忽略**，忽略该风险，态势感知将不再上报并告警此服务器上的这个风险项。

如果您希望彻底忽略该风险项，不再对其进行检测，您可以单击页面右上角的 **加入白名单**，并添加备注信息。添加进白名单中的风险项可在 **主机基线检查设置** 中进行恢复。

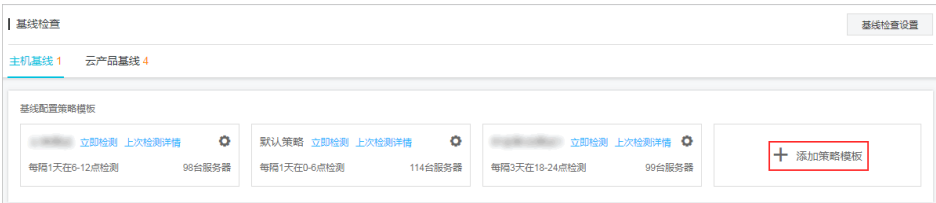
主机基线检查设置

如果您需要自定义扫描策略和检测项目，您可以参照以下步骤，新建一个扫描策略模板：

登录 云盾态势感知控制台。

在左侧导航栏，单击 **基线检查**。

单击 **添加策略模板**，新建一个扫描策略模板，完成以下配置：



- i. 输入一个用于识别该模板的名称。
- ii. 勾选需要检测的项目，在合规性检测、弱密码检测、系统、账号、数据库下勾选具体检测内容，详情参见文末 **主机基线检查检测内容**。
- iii. 选择检测周期（每1天/3天/7天/30天检测一次）和检测触发时间（0-6点、6-12点、12-18点、18-24点）。
- iv. 勾选应用上述设置的分组资产。
注意：新创建的服务器默认归属在 **分组资产 > 未分组**，如需对新创建资产自动应用该模板，请勾选 **未分组**。
- v. 单击 **提交**，完成创建。

已添加策略模板自动生效，按照配置的周期和触发时间自动执行扫描任务。您也可以在 **主机基线** 分页下，单击策略模板下的 **立即检测**，立即执行该扫描任务。

对于已添加的模板，您可以单击 **基线检查** 页面右上角的 **基线检查设置**；然后在 **扫描策略** 下，选择相应模板，单击 **编辑** 修改其内容，或单击 **删除** 移除该模板。

基线检查设置

扫描策略

添加

策略模板	检测周期	生效服务器	检测项目	操作
	每隔1天 在6~12点检测	98台	3项	编辑 删除
默认策略	每隔1天 在0~6点检测	114台	14项	编辑
	每隔3天 在18~24点检测	99台	4项	编辑 删除

失效风险自动删除：

30天
7天
30天
90天

基线白名单：?

☐ 风险名称	操作
☐ 密码策略合规检测	移除
☐ 系统共享配置检测	移除
☐ 移除	

共有 2 条,每页显示 10 条

<< < 1 > >>

提醒风险等级范围：

☒ 严重 ☒ 高危 ☒ 中危 ☐ 低危

主机基线检查设置也支持以下设置：

选择 **失效风险自动删除** 周期：7天、30天、90天。
说明：对检测出来的风险项不做任何处理的话，该风险项默认失效，并在指定的周期后被自动删除。

维护 **基线白名单**：单击一个风险项下的 **移除**，将其从白名单中移除，系统将重新对其进行检测和告警。

- 勾选 **提醒风险等级范围**：
- 严重：极不安全的配置，需要立刻修复。
 - 高危：高风险配置，如密码太弱等，极易被黑客利用。
 - 中危：中风险配置，如Web容器用root权限运行等，存在被恶意利用的风险。
 - 低危：低风险配置，如密码长度不足32位等，不太容易被黑客利用，但某些合规性检查中会

规定该内容。

主机基线检查检测内容

分类	检测项	说明
系统	系统自启动项检测 (Windows)	检测 Windows 系统服务器中的注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit中的键值是否包含可疑的可执行文件。
	系统共享配置检测 (Windows)	检测 Windows 系统服务器中的注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous中的键值，查看该键值控制是否允许远程操作注册表。
	组策略检测 (Windows)	检测 Windows 系统服务器中以下账号相关的安全策略： - 账号密码长度最小值 - 密码复杂度（数字、大小写字母、特殊字符组合） - 密码更新时必须与原密码不同 - 登录框是否显示上次登录账号 - 登录事件记录是否开启 - 登录过程中事件记录是否开启
	SSH 登录基线检测	检测 Linux 系统服务器中以下 SSH 登录安全策略配置： - 登录端口是否为默认 22 端口 - root 账号是否允许直接登录 - 是否使用不安全的 SSH V1 协议 - 是否使用不安全的 RSH 协议 - 是否运行基于主机身

		份验证的登录方式
弱密码检测	Linux 系统登录弱口令检测	检测 Linux 系统服务器的登录账号的密码是否为常见弱口令，及 SSH 登录的密码是否常见弱口令。
	SQLServer 登录弱口令检测	检测服务器上 SQLServer 登录账号的密码是否为常见弱口令。
	Windows 系统登录弱口令检测	检测 Windows 系统服务器中系统登录账号的密码是否为常见弱口令，及 RDP 登录的密码是否为常见弱口令。
	FTP 匿名登录检测	检测服务器上的 FTP 服务是否开启匿名登录。
	MySQL 弱口令检测	检测服务器上的 MySQL 服务的登录账号是否为常见弱口令。
	PostgreSQL 登录弱口令检测	检测服务器中 PostgreSQL 登录账号的密码是否为常见弱口令。
账号	风险账号扫描	检测服务器系统中可疑的隐藏账号、及克隆账号。
	密码策略合规检测	检测 Linux 系统服务器中的以下账号密码策略： - 账号密码最大使用期限 - 密码修改最小间隔时间 - 密码最小长度 - 密码到期开始通知时间
	空密码账号检测	检测服务器中密码为空的账号。
	Linux 账号完整性检测	检测 Linux 系统服务器中新增账号的完整性。
数据库	Redis 配置漏洞被利用和可疑文件检测	检测服务器上的 Redis 服务是否存在未授权访问漏洞被利用，并向系统关键文件写入异常数据的情况。
	Redis 配置漏洞检测	检测服务器上的 Redis 服务是否对公网开放。
CIS基线检测（参考链接）	Linux-Tomcat7基线检测	按照CIS-Tomcat7最新基线标准进行中间件层面基线检测。
	Linux-Centos7基线检测	按照CIS-Linux Centos7最新基线标准进行系统层面基线检测。

云产品基线检查

态势感知基线检查功能自动检测您服务器和云产品上存在的风险配置项，并为您提供修复建议。该功能分为主机基线检查和云产品基线检查。

本文介绍了云产品基线检查的操作方法。关于主机基线检查，请参考 [主机基线检查](#)。

功能说明

云产品基线检查支持下表中列述的检测项目。

类别	检查项
身份认证及权限	检查云平台主账号双因素认证配置。
网络访问控制	检查SLB高危端口暴露情况。
	检查安全组RDS白名单配置。
日志审计	检查云平台操作审计配置。
数据安全	检查RDS数据库安全策略。
基础安全防护	检查是否启用云盾WAF。
	检查是否启用云盾态势感知。

操作步骤

参照以下步骤，手动进行云产品基线检查：

登录 云盾态势感知控制台。

在左侧导航栏，单击 **基线检查**。

前往 **云产品基线** 分页，并单击 **立即检测**。



等待检测过程结束，查看有风险的项目，并参照 **指导方案** 进行修复。

参照以下步骤，启用云产品基线自动检查：

单击 **云产品基线** 分页上方的 **设置**。

勾选执行自动检查的工作日。

单击 **确认**，完成设置。

态势感知会在您勾选的工作日的22：00自动执行云产品基线检查，并刷新检查结果。

资产指纹

态势感知资产指纹功能定期收集并记录您服务器上的以下信息：运行进程、系统账号、开放端口、软件版本、和网站后台，帮助您全面了解资产的运行状态和进行回溯分析。本文介绍了使用资产指纹查看相关记录的操作方法。

功能说明

资产指纹功能包含以下五个模块：

运行进程：定期收集服务器的进程信息，用于清点进程。应用场景包括：清点一个进程被哪些服务器运行；清点一台服务器运行了哪些进程。

系统账号：定期收集服务器的账号信息，用于清点账号。应用场景包括：清点一个账号被哪些服务器创建；清点一台服务器创建了哪些账号。

开放端口：定期收集服务器的对外端口监听信息，用于清点端口。应用场景包括：清点一个端口被哪些服务器监听；清点一台服务器开通了哪些端口。

软件版本：定期收集服务器的软件版本信息，用于清点软件资产。应用场景包括：清点非法软件资产（非法安装）；清点版本过低软件资产；漏洞爆发时快速定位受影响资产范围。

网站后台：定期收集和记录网站后台的登录信息，并检测弱密码和撞库攻击，用于监控后台登录安全。应用场景包括：查看后台登录记录；查看后台登录账号是否存在弱密码；查看后台被撞库攻击次数。

同时，通过资产指纹设置功能，您可以选择运行进程、系统账号、开放端口、软件版本数据的收集刷新频率。

操作步骤

查看运行进程

参照以下步骤，查看服务器运行进程：

登录 云盾态势感知控制台。

在左侧导航栏，选择 **资产指纹 > 运行进程**。

在 **运行进程** 页面，查看所有运行中进程和运行这些进程的主机数。您可以使用进程名或运行用户进行搜索。

单击一个进程名，查看其详细信息。

进程：

返回运行进程

(((4)))4

搜索：

资产选择（全部）

服务器IP或名称

服务器标签

运行用户

启动参数

搜索

重置

对应资产	进程路径	启动参数	启动时间	运行用户	运行权限	PID	父进程	文件MD5	获取时间
资产名称	进程路径	启动参数	2017-12-08 11:47:26	root	root	467	systemd	文件MD5	2017-12-19 18:53:13
资产名称	进程路径	启动参数	2017-11-12 13:06:07	root	root	401	systemd	文件MD5	2018-03-25 09:20:51
资产名称	进程路径	启动参数	2017-12-29 15:57:56	root	root	365	systemd	文件MD5	2018-03-25 09:50:45

共有 3 条,每页显示 20 条

« < 1 > »

查看系统账号

参照以下步骤，查看服务器系统账号：

登录 云盾态势感知控制台。

在左侧导航栏，选择 **资产指纹 > 系统账号**。

在 **系统账号** 页面，查看所有已登录的系统账号和使用这些账号的主机数。您可以使用账号名进行搜索。

单击一个账号名，查看其详细信息。

账号：admin

返回账号信息

(((4)))4

搜索：

资产选择（全部）

服务器IP或名称

服务器标签

搜索

重置

ROOT权限：

是

否

对应资产	root权限	用户名	到期时间	上次登录	获取时间
资产名称	否	admin	never	时间：N/A 来源：N/A	2018-03-14 09:35:37

共有 1 条,每页显示 20 条

« < 1 > »

查看开放端口

参照以下步骤，查看服务器开放端口：

登录 云盾态势感知控制台。

在左侧导航栏，选择 **资产指纹** > **开放端口**。

在 **开放端口** 页面，查看所有已开放端口、端口对应的网络协议、和开放这些端口的主机数。您可以使用端口号或进程名进行搜索。

单击一个端口号，查看其详细信息。

端口：49164 返回开放端口 4

搜索：	资产选择（全部）	服务器IP或名称	服务器标签	服务器进程名称	搜索	重置
对应资产	对应进程	绑定IP	获取时间			
资产名称	N/A	IP地址	2018-01-08 00:11:36			
资产名称	SERVICES.EXE	IP地址	2018-03-25 11:48:17			

共有 2 条,每页显示 20 条

«<1>»

查看软件版本

参照以下步骤，查看服务器软件版本：

登录 云盾态势感知控制台。

在左侧导航栏，选择 **资产指纹** > **软件版本**。

在 **软件版本** 页面，查看所有使用中的软件和使用这些软件的主机数。您可以使用软件名、版本名、或软件安装目录进行搜索。

单击一个软件名，查看其版本等信息。

软件：acpi 返回软件版本 4

搜索：	资产选择（全部）	服务器IP或名称	服务器标签	软件版本	软件安装目录	搜索	重置
对应资产	软件版本	软件最后更新时间	软件安装目录	获取时间			
资产名称	1.7-1	2018-03-21 05:03:16	安装目录	2018-03-22 11:53:20			
资产名称	1.7-1	2018-03-22 07:02:47	安装目录	2018-03-22 11:53:24			

共有 2 条,每页显示 20 条

«<1>»

查看网站后台登录记录

参照以下步骤，查看网站后台登录记录：

登录 云盾态势感知控制台。

在左侧导航栏，选择 **资产指纹** > **网站后台**。

在 **网站后台** 页面，查看所有网站后台登录记录，以及登录弱密码检测结果、撞库攻击检测结果。

网站后台						
			((4)) 4		资产指纹设置	
名称	后台地址	是否存在弱口令	昨日被撞库攻击次数	历史被撞库攻击次数	最近发现时间	首次发现时间
401 Unauthorized	http://192.168.1.100:8080/401Unauthorized	否	0	0	2018-03-25 07:33:19	2018-03-13 05:12:01
phpMyAdmin	http://192.168.1.100:8080/phpMyAdmin	否	0	0	2017-11-17 05:22:31	2017-11-12 16:28:51
phpMyAdmin	http://192.168.1.100:8080/phpMyAdmin	否	0	0	2017-06-02 05:02:49	2016-06-13 05:02:12

资产指纹设置

参照以下步骤，设置资产数据的收集刷新频率：

登录 云盾态势感知控制台。

前往 **资产指纹** 下任意子功能页，并单击页面右上角 **资产指纹设置**。

完成以下配置：

- 选择 **监听端口数据自动刷新** 频率：不开启、1小时/3小时/12小时/1天/7天收集1次。
- 选择 **运行进程数据自动刷新** 频率：不开启、1小时/3小时/12小时/1天/7天收集1次。
- 选择 **账号信息数据自动刷新** 频率：不开启、1小时/3小时/12小时/1天/7天收集1次。
- 选择 **安装软件数据自动刷新** 频率：不开启、1小时/3小时/12小时/1天/7天收集1次。

单击 **确认**，完成设置。

日志检索

使用日志检索

态势感知提供主机和Web日志检索功能，将散落在阿里云各系统中的日志集中管理，便于您在出现主机和Web问题时一站式搜索定位问题根源。

注意：您需要升级到态势感知（企业版）才能使用日志检索功能。目前，态势感知（企业版）支持180天以内的日志存储，并提供30天以内的日志查询。

功能特性

态势感知日志检索功能具备以下特性：

一站式日志检索平台，集中查询阿里云各产品日志，单一接口，便于问题溯源。

日志功能的SaaS化，无需进行额外安装部署，仅使用浏览器登录到态势感知控制台，即可查询服务器日志。

支持TB级数据检索，以及50个维度的数据逻辑（布尔表达式）组合，可以秒级展示日志全文检索结果。

支持丰富的主机和Web日志源。

支持日志投递，允许您将安全日志导入到阿里云日志服务做进一步分析。关于日志投递功能，请参考[日志投递](#)。

应用场景

日志检索帮助您实现以下需求：

安全事件分析：主机发生安全事件后，通过日志功能进行调查，评估资产受损范围和影响。

操作审计：对主机的操作日志进行审计，对高危操作和严重问题进行细粒度排查。

业务流量统计：对Web访问日志进行统计和分析，追踪来访者的环境和状态，对业务和服务响应进行筛选。

可供检索的日志

日志检索功能支持查询以下日志源：

类型	日志源	说明
主机日志	登录流水	系统登录成功的日志记录
	暴力破解	系统登录失败的日志记录
	进程快照	某一时刻主机上的进程运行信息
	端口监听快照	某一时刻主机上的监听端口信息
	账号快照	某一时刻主机上的账号登录信息
	进程启动日志	主机上进程启动的相关信息
	网络连接日志	主机对外主动连接的日志
Web日志	Web访问日志	云上业务的HTTP协议日志
	网络会话日志	云上业务的网络5元组日志（全端口）
	DNS日志	网络DNS解析日志

注意：各种日志源支持的字段信息，请查看 各日志源字段说明。

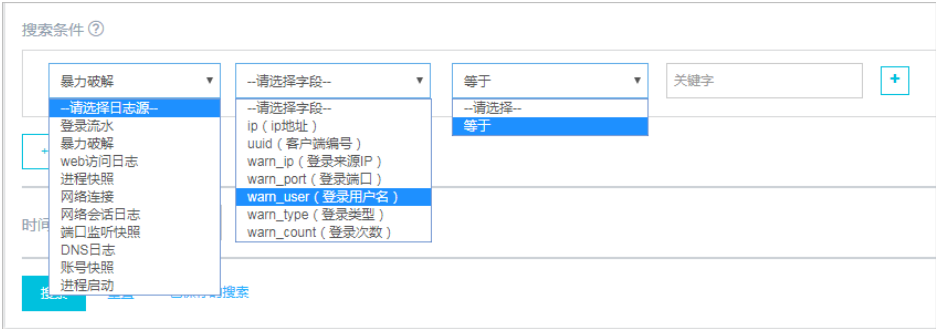
操作步骤

参照以下步骤，使用日志检索功能查询日志：

登录 态势感知控制台。

在左侧导航栏，选择 **更多功能 > 日志检索**。

选择日志源、需要检索的日志字段，输入您想要检索的关键词，并选择搜索时间范围（24小时，7天，或自定义最近30天内），然后单击 **搜索**。



搜索条件 ②

web访问日志

src_ip (源IP)

等于

1.1.1.1

-

or

web访问日志

src_ip (源IP)

等于

2.2.2.2

+ -

or

网络会话日志

src_ip (源IP)

等于

1.1.1.1

+ -

+ 增加一组

时间范围: 7天内

搜索

重置

已保存的搜索

说明：您可以单击搜索条件右侧的 +，在一个搜索条件（一个日志源）下增加多个逻辑判断（单击 - 可以删除某个选项）；也可以单击 **增加一组**，增加多个搜索条件（不同的日志源），进行逻辑检索。关于语法逻辑的用法，请参考 [语法逻辑说明](#)。

例如，如上图所示，您可以同时搜索源IP等于1.1.1.1或者2.2.2.2的Web访问日志，和源IP等于1.1.1.1的网络会话日志。

根据您的设置的搜索条件，展示精细化的日志记录。同时，您可以在搜索结果中修改字段，直接做进一步检索；也可以单击 **保存搜索逻辑**，保存当前搜索条件，以便后续在 **已保存的搜索** 中直接调用。



您可以根据细粒度的时间维度查看搜索结果，并将数据结果导出。



语法逻辑说明

日志检索支持多条件逻辑检索，您可以在一个搜索条件（一个日志源）下增加多个判断逻辑，也可以对多个搜索条件（不同的日志源）进行逻辑组合。本文介绍了日志检索支持的语法逻辑，也列举了部分用例，帮助您理解和使用。

支持的语法逻辑

日志检索支持下表中列举的语法逻辑：

逻辑名称	描述
and	双目运算符。形式为 query1 and query2，搜索结果展示 query1 和 query2 查询结果的交集。 注意： 如果多个单词间没有语法关键词，默认是 and 的关系。
or	双目运算符。形式为 query1 or query2，搜索结果展示 query1 和 query2 查询结果的并集。
not	双目运算符。形式为 query1 not query2，搜索结果展示符合 query1 并且不符合 query2 的结果，相当于 query1-query2。 注意： 如果只有 not query1，那么表示从全部日志中选取不包含 query1 的结果。
(,)	左右括号用于把一个或多个子 query 合并成一个 query，提高括号内 query 的优先级。
:	用于 key-value 对的查询。term1:term2 构成一个 key-value 对。 注意： 如果 key 或者 value 内有空格，需要用引号把整个 key 或者 value 包括起来。

"	把一个关键词转换成普通的查询字符。左右引号内部的任何一个 term 都会被查询，而不会当成语法关键词。或者在 key-value 查询中把左右引号内的所有 term 当成一个整体。
\	转义符。用于转义引号，转义后的引号表示符号本身，不会当成转义字符，例如，\"代表列举引号。
	管道运算符，表示前一个计算的基础上进行更多计算。例如 query1 timeslice 1h count。
timeslice	时间分片运算符，表示多长时间的数据作为一个整体进行计算，使用方式有 timeslice 1h，timeslice 1m，timeslice 1s，分别表示以 1 小时、1 分钟、1 秒钟作为一个整体。例如，query1 timeslice 1h count 表示查询 query 这个条件，并且返回以 1 小时为时间分片的总次数。
count	计数运算符，表示日志条数。
*	模糊查询关键字，用于替代 0 个或多个字符。例如，使用 que*，会返回 que 开头的所有命中词。
?	模糊查询关键字，用于替代一个字符。例如，使用 qu?ry，会返回以 qu 开头，以 ry 结尾，并且中间还有一个字符的所有命中词。
__topic__	查询某个 topic 下数据，新的语法下，可以在 query 中查询 0 个或多个 topic 的数据。例如 __topic__:mytopicname。
__tag__	查询某个 tag key 下某个 tag value。例如 __tag__:tagkey:tagvalue。
source	查询某个 IP 的数据，例如 source:127.0.0.1。

注意：

- 语法关键词不区分大小写。
- 语法关键字的优先级由高到底排序为：> " > () > and not > or。
- 日志检索保留以下关键字的使用权，如果您需要使用以下关键字，请使用引号包含起来：> = < sort asc desc group by avg sum min max limit。
- 当您同时配置了全文索引和键值索引时，如果两者的分词字符不一样，那么使用全文查询方式时数据无法查出。

查询示例

您可以参照以下查询示例，来熟悉语法逻辑的用法。

- 查询同时包含 a 和 b 的日志：a and b 或者 a b
- 查询包含 a 或者包含 b 的日志：a or b
- 查询包含 a 但是不包含 b 的日志：a not b
- 查询不包含 a 的日志：not a

- 查询包含 a 而且包含 b , 但是不包括 c 的日志 : a and b not c
- 查询包含 a 或者包含 b , 而且一定包含 c 的日志 : (a or b) and c
- 查询包含 a 或者包含 b , 但不包括 c 的日志 : (a or b) not c
- 查询包含 a 而且包含 b , 可能包含 c 的日志 : a and b or c
- 查询 FILE 字段包含 apsara 的日志 : FILE:apsara
- 查询 FILE 字段包含 apsara 和 shennong 的日志 : FILE:"apsara shennong" 或者 FILE:apsara FILE:shennong 或者 FILE:apsara and FILE:shennong
- 查询 FILE 字段包含 apsara 或者 shennong 的日志 : FILE:apsara or FILE:shennong
- 查询 file info 字段包含 apsara 的日志 : "file info":apsara
- 查询包含 and 的日志 : and
- 查询包括引号的日志 : \"
- 查询以 shen 开头的所有日志 : shen*
- 查询 FILE 字段下 , 以 shen 开头的所有日志 : FILE:shen*
- 查询以 shen 开头 , 以 ong 结尾 , 中间还有一个字符的日志 : shen?ong
- 查询包括以 shen 开头 , 并且包括以 aps 开头的日志 : shen* and aps*
- 查询以 shen 开头的日志的分布 , 时间片为 20 分钟 : shen*| timeslice 20m | count
- 查询 topic1 和 topic2 下的所有数据 : __topic__:topic1 or __topic__ : topic2
- 查询 tagkey1 下 tagvalue2 的所有数据 : __tag__ : tagkey1 : tagvalue2

各日志源字段说明

本文介绍了态势感知日志检索功能可以采集并供检索的原始日志类型和字段说明。

各日志源字段列表

日志检索功能支持您查询下表列述的日志源。您可以单击一个日志源查看其支持的字段信息。

类型	日志源	说明
主机日志	登录流水	系统登录成功的日志记录
	暴力破解	尝试暴力破解登录密码的日志记录
	进程快照	主机上进程运行的相关信息
	端口监听快照	主机上监听端口的相关信息
	账号快照	主机上账号登录的相关信息
	进程启动	主机上进程启动的相关信息
	网络连接	主机对外主动连接的日志
Web日志	Web访问日志	云上业务的HTTP协议日志

	网络会话日志	云上业务的网络5元组日志（全端口）
	DNS日志	网络DNS解析日志

登录流水

登录流水查询支持以下字段：

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
warn_ip	string	登录来源IP
warn_port	string	登录端口
warn_user	string	登录用户名
warn_type	string	登录类型
warn_count	string	登录次数
time	datetime	登录时间

暴力破解

暴力破解查询支持以下字段：

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
warn_ip	string	攻击来源IP
warn_port	string	破解端口
warn_user	string	破解用户名
warn_type	string	类型
warn_count	string	破解次数
time	datetime	破解时间

进程启动日志

进程启动日志查询支持以下字段：

字段	数据类型	说明
uuid	string	客户端编号

IP	string	IP地址
pid	string	进程ID
groupname	string	用户组
ppid	string	父进程ID
uid	string	用户ID
username	string	用户名
filename	string	文件名
pfilename	string	父进程文件名
cmdline	string	命令行
filepath	string	进程路径
pfilepath	string	父进程路径
time	datetime	启动时间

端口监听快照

端口监听快照查询支持以下字段：

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
src_port	string	监听端口
src_ip	string	监听IP
proc_path	string	进程路径
PID	string	进程ID
proc_name	string	进程名
proto	string	协议
time	datetime	数据获取时间

网络连接日志

网络连接日志查询支持以下字段：

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
src_ip	string	源IP

src_port	string	源端口
proc_path	string	进程路径
dst_port	string	目标端口
proc_name	string	进程名
dst_ip	string	目标IP
status	string	状态
proto	string	协议
time	datetime	连接时间

账号快照

账号快照查询支持以下字段：

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
perm	string	是否拥有root权限
home_dir	string	home目录
warn_time	string	密码到期提醒时间
groups	string	用户属于的组
login_ip	string	最后一次登录的ip地址
last_chg	string	密码最后修改时间
shell	string	linux的shell命令
domain	string	windows域
tty	string	登录的终端
account_expire	string	账号超期时间
passwd_expire	string	密码超期时间
last_logon	string	最后登录时间
user	string	用户
status	string	用户状态：0-禁用；-正常
time	datetime	数据获取时间

进程快照

进程快照查询支持以下字段：

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
path	string	进程路径
start_time	string	进程启动时间
uid	string	用户ID
cmdline	string	命令行
pname	string	父进程名
name	string	进程名
pid	string	进程ID
user	string	用户名
md5	string	进程文件MD5值，超过1MB不计算
time	datetime	数据获取时间

Web访问日志

Web访问日志查询支持以下字段：

字段	数据类型	说明
request_datetime	string	请求时间
host	string	主机名host
uri	string	请求URI
src_ip	string	访问源IP
dst_ip	string	目的IP
method	string	请求方法GET/POST
referer	string	来源Referer
user_agent	string	客户端user_agent
cookie	string	客户端cookie
post_data	string	POST请求内容
ret_code	string	返回响应码
jump_location	string	跳转到的URL
set_cookie	string	返回的set_cookie
src_port	string	访问源端口号
dst_port	string	目的端口号

x_forward_for	string	来源x_forward_for
rsp_content_type	string	请求内容类型
rqs_content_type	string	返回内容类型
content_length	string	返回数据长度
token	string	会话标识
ds	string	分区-天
hh	string	分区-小时

网络会话日志

网络会话日志查询支持以下字段：

字段	数据类型	说明
asset_type	string	资产类型：RDS/SLB/ECS等
session_time	datetime	访问时间
src_ip	string	源IP
src_port	string	源端口
dst_ip	string	目的IP
dst_port	string	目的端口
proto	string	协议类型：TCP/UDP
ds	string	分区-天
hh	string	分区-小时

DNS日志

DNS日志查询支持以下字段：

字段	数据类型	说明
query_datetime	datetime	请求时间
src_ip	string	源IP
src_port	string	源端口
dst_ip	string	目的IP
dst_port	string	目的端口
response_datetime	datetime	响应时间
qname	string	解析域名
qtype	string	请求记录类型

qid	string	请求的ID
rcode	string	返回码
answer_num	string	answer字段数量
answer	string	answer字段
authority_num	string	authority字段数量
authority	string	authority字段
additional_num	string	additional字段数量
additional	string	additional字段
in_out	string	方向
region	string	地区

日志投递

态势感知的日志功能允许您将安全日志投递到 阿里云日志服务（Log Service），便于您使用日志服务进行日志分析，或再次投递到MaxCompute（ODPS）、OSS中，进行自定义二次分析等。

支持的日志类型

日志投递功能支持将以下安全日志导入到阿里云日志服务：

- 进程启动日志（由态势感知Agent插件采集，实时数据，进程一启动日志就上报）
- 网络连接日志（由态势感知Agent插件采集，Windows为实时数据，Linux每10秒采集，增量上报）
- 登录流水（由态势感知Agent插件采集，实时的登录成功数据）
- 暴力破解（由态势感知Agent插件采集，准实时的登录失败日志）
- 进程快照（若在态势感知-资产指纹中开启了自动收集则会有数据，快照形式，某一时刻的运行进程信息）
- 账号快照（若在态势感知-资产指纹中开启了自动收集则会有数据，快照形式，某一时刻的账号信息）
- 端口快照（若在态势感知-资产指纹中开启了自动收集则会有数据，快照形式，某一时刻的监听端口信息）
- Web访问日志（由态势感知系统采集，非实时数据，延迟5个小时左右）
- 网络会话日志（由态势感知系统采集，非实时数据，延迟5个小时左右）
- DNS日志（由态势感知系统采集，非实时数据，延迟5个小时左右）

说明：各种日志源支持的字段信息，请查看 各日志源字段说明。

操作步骤

参照以下步骤，开启并配置日志投递功能：

登录 云盾态势感知控制台。

在左侧导航栏，选择 **更多功能** > **日志检索**。

单击页面右上角的 **日志投递**。

首次使用日志投递功能时，单击 **同意授权**，向日志服务授予访问态势感知的权限。

在 **日志投递** 对话框中，选择需要投递的日志类型，单击其投递开关来开启/关闭日志投递。

开启日志投递后，配置投递位置，分别选择投递区域、对应的Project名称、和Logstore名称。

说明：您需要提前在 日志服务控制台 完成Project和Logstore创建，并建立索引（全文索引），才能将安全日志投递到日志服务。关于Project和Logstore的创建方法，请参考 日志服务快速入门 中的 **创建项目** 和 **创建日志库** 部分。

单击 **确定**，完成配置。

设置

使用态势感知的设置功能，您可以执行以下操作：

- 安装/卸载态势感知Agent插件
- 启用/关闭安全日报
- 配置告警通知策略

本文介绍了具体的操作方法。

操作步骤

参照以下步骤，进行态势感知功能设置：

登录 云盾态势感知控制台。

在左侧导航栏，单击 **设置**，进入设置页。

安装/卸载态势感知插件

说明：态势感知Agent插件是态势感知提供的本地安全插件，您需要在您的服务器操作系统上安装态势感知Agent插件，才能使用态势感知提供的安全防护服务。

前往 [安装/卸载插件](#) 分页。

查看目标服务器是否处于 **离线** 状态。您可以输入服务器IP或名称进行搜索，快速定位到目标服务器。

对于处于 **离线** 状态的服务器，根据页面提示，获取并安装最新版本的态势感知Agent插件。具体步骤请参考 [安装Agent](#)。

如果您决定不再使用云盾态势感知服务的安全防护功能，您可以单击页面右上角的 **卸载插件** 进行自动卸载。具体步骤请参考 [卸载Agent](#)。

开启安全日报

说明：开启安全日报后，态势感知会以邮件形式，向您指定的收件人发送每日安全统计信息。

前往 [安全日报](#) 分页。

输入一个 **日报名称**，并开启 **发送日报**。

单击 **添加收件人**，输入收件人姓名和邮箱，并单击 **确认**。

说明：对于添加成功的收件人，您可以单击 **删除** 将其从收件人列表中移除。

完成上述操作后，态势感知会按照 **邮件模板** 的样式，向收件人发送每日安全统计信息。如果你不需要接收安全日报邮件，您可以在 [安全日报](#) 分页，关闭 **发送日报** 功能。

配置告警设置

说明：使用告警设置，您可以调整态势感知告警功能的告警策略。

注意：默认情况下，告警信息接收人为您的账号联系人，您也可以前往 [消息中心](#) > [基本接收管理](#) > [安全消息](#) > [云盾安全信息通知](#)，新增更多消息接收人。

前往 [告警设置](#) 分页。

针对 安全告警、漏洞管理、基线配置，分别勾选需要进行告警的安全事件等级、通知方式和通知时间。

即将下线功能

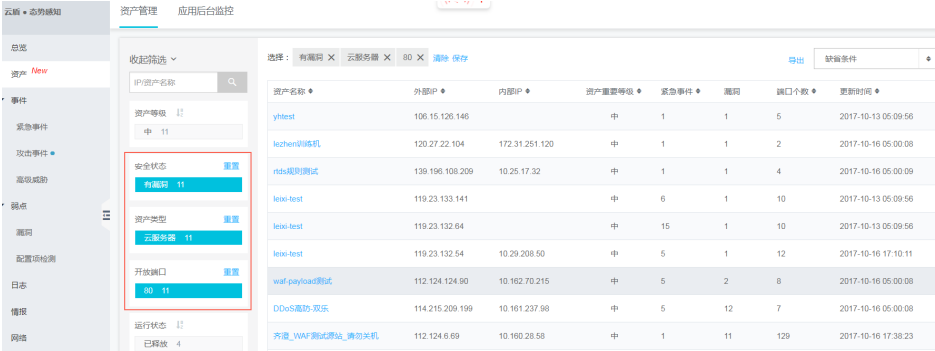
资产

操作指南

地址

<https://yundun.console.aliyun.com/?spm=5176.7946181.209102.4.7pkLDx&p=sas#/asset/manage>

筛选



保存搜索条件

资产管理应用后台监控

收起筛选

IP/资产名称

资产等级

安全状态

资产类型

开放端口

中 11

重置

有漏洞 11

重置

云服务器 11

重置

80 11

重置

选择

有漏洞

云服务器

80

清除

保存

资产名称	外部IP	内部IP
yhtest	106.15.126.146	
lezhen训练机	120.27.22.104	172.31.251.120
rtDs规则测试	139.196.108.209	10.25.17.32
leixi-test	119.23.133.141	
leixi-test	119.23.132.64	
leixi-test	119.23.132.54	10.29.208.50
waf-payload测试	112.124.124.90	10.162.70.215
DDoS高防-双乐	114.215.209.199	10.161.237.98

保存搜索条件

测试保存最多十个字啊

确定取消

资产重要等级编辑

资产名称	外部IP	内部IP	资产重要等级	紧急事件	漏洞	端口个数	更
dsy-yxdtest2	118.190.206.131	172.31.251.125	中	--	0	4	20
iZxmy0vvri3jsaZ	116.62.38.164	10.26.22.165	高		0	6	20
iZxmxzwa9hvsikZ	39.106.33.154	172.17.252.125	中		0	6	20
...	...	...	低		0	0	20

导出搜索结果

资产管理应用后台监控

收起筛选

IP资产名称

资产等级

安全状态

资产类型

开放端口

中 11

有漏洞 11

云服务器 11

80 11

选择：有漏洞 X 云服务器 X 80 X 清除 保存

导出

测试保存最多十个字符

资产名称	外部IP	内部IP	资产重要等级	紧急事件	漏洞	端口个数	更新时间
yhtest	106.15.126.146		中	1	1	5	2017-10-13 05:09:56
lezhen训练机	120.27.22.104	172.31.251.120	中	1	1	2	2017-10-16 05:00:08
rlds规则测试	139.196.108.209	10.25.17.32	中	1	1	4	2017-10-16 05:00:09
leixi-test	119.23.133.141		中	6	1	10	2017-10-13 05:09:56
leixi-test	119.23.132.64		中	15	1	10	2017-10-13 05:09:56
leixi-test	119.23.132.54	10.29.208.50	中	5	1	12	2017-10-16 17:10:11
waf-payload测试	112.124.124.90	10.162.70.215	中	5	2	8	2017-10-16 05:00:08

查看详情

点击资产名称即可进入资产详情页面。

资产详情

资产详情页面有3部分构成，分别是资产基础信息，资产安全事件统计图表和资产主要属性数据。基础属性信息中，可以编辑资产重要等级和备注信息。

基本信息

资产名称DDoS漏洞-双乐

资产类型ECS

更新时间2017-10-17 10:37:22

运行状态运行中

展开

统计

全部90天30天7天

漏洞等级分布

事件类型分布

紧急事件趋势

紧急事件

事件名称	事件类型	发现时间	描述
DDoS	DDoS	2016-03-28 14:52:40	遭受峰值流量为403M的DDoS攻击，持续时间32分钟

紧急事件

事件名称	事件类型	发现时间	描述
DDoS	DDoS	2016-03-28 14:52:40	遭受峰值流量为403M的DDoS攻击，持续时间32分钟
DDoS	DDoS	2016-03-23 00:08:32	遭受峰值流量为12.99G的DDoS攻击，持续时间41分钟
DDoS	DDoS	2016-03-23 00:08:32	遭受峰值流量为3.94G的DDoS攻击，持续时间1小时11分钟
DDoS	DDoS	2016-03-20 11:31:17	遭受峰值流量为14.61G的DDoS攻击，持续时间36分钟
DDoS	DDoS	2016-03-20 11:31:17	遭受峰值流量为5.41G的DDoS攻击，持续时间1小时6分钟

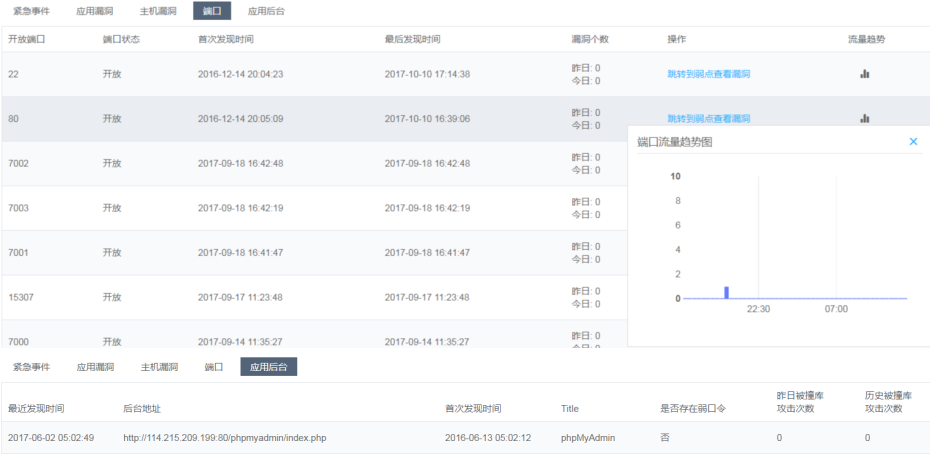
紧急事件

最后检测时间	首次检测时间	应用	漏洞名称	漏洞地址	漏洞等级	修复方案	漏洞状态
2016-03-02 09:22:58	2016-02-13 07:08:39	114.215.209.199	discuz代码执行漏洞	/var/www/html/can/source5.3/data/package/com.uc.1.0/api/uc.php	高危	修复成功	修复成功
2016-03-02 09:17:10	2016-02-13 07:02:52	114.215.209.199	discuz代码执行漏洞	/var/www/html/can/source5.3/api/uc.php	高危	修复成功	修复成功
2016-03-02 09:08:02	2016-02-13 06:53:43	114.215.209.199	discuz代码执行漏洞	/var/www/html/can/source5.2/data/package/com.uc.1.0/api/uc.php	高危	修复成功	修复成功
2016-03-02 09:02:14	2016-02-13 06:47:56	114.215.209.199	discuz代码执行漏洞	/var/www/html/can/source5.2/api/uc.php	高危	修复成功	修复成功

属性-紧急事件

属性-应用漏洞\主机漏洞

属性-端口



属性-应用后台

资产介绍

功能说明

从资产视角出发，展现客户资产的相关数据，让客户快速掌握资产的安全情况。

实现原理

- 通过用户授权扫描的资产信息，结合态势感知的安全管理能力，综合反映当前资产的安全态势相关数据

使用场景

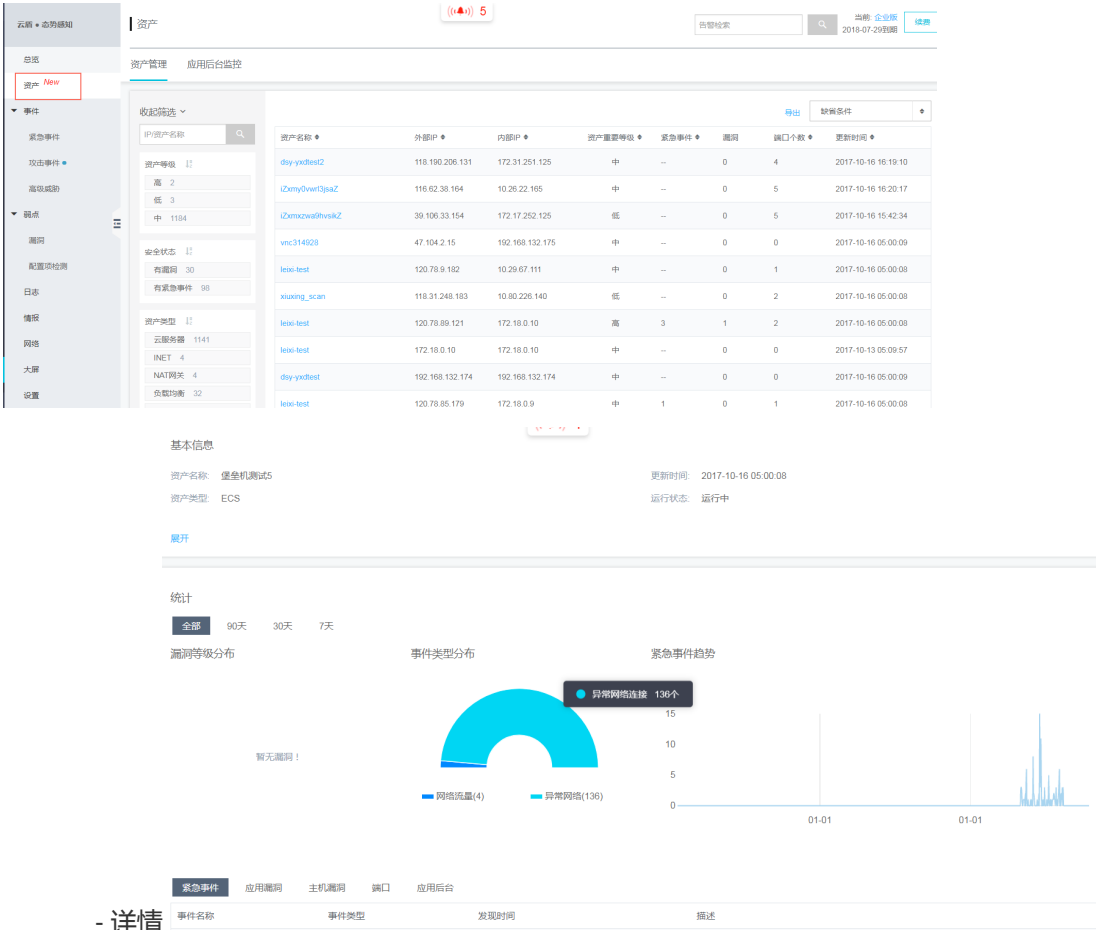
- 按资产查看安全状态

支持的资产类型

- ECS
- SLB
- RDS
- NAT网关
- INET

功能截图

- 列表



情报

情报功能介绍

功能说明

- 提供企业客户相关的情报内容，包括数据泄露情报，用户名密码泄露情报，暗网相关情报，QQ群攻击预谋情报
- （注意：本功能只针对专业版以上客户开放，基础版客户无此功能）

实现原理

- 通过态势感知团队搭建在网络空间中的威胁情报采集系统，可对Github等第三方代码托管网站，进行实时监控，捕获并判定被公开的源代码中（多为企业员工私自上传并不小心公开的源代码），是否含有ECS，RDS，Redis，MySQL等客户资产的登录名和密码等信息

使用场景

- 因为企业制度不规范，管理困难，导致企业员工有权限（或无意识）的将公司源码，上传至Github等代码托管平台，导致企业的数据库连接地址和密码，服务器登陆密码，在代码中直接外泄。
- 态势感知情报采集系统，可以通过网络爬虫，抓取这些代码托管网站，对企业相关的情报进行实时监控和通知，避免了企业因为管理问题导致的数据外泄。

支持的情报类型

1. AK信息检测
2. ECS用户名密码
3. RDS用户名密码
4. MySQL用户名密码
5. redis用户名密码
6. MongoDB用户名密码
7. SSH远程连接服务器的密码和IP

情报功能截图

筛选

最近 90 天

AK 类型: IP

安全状态

已备注 1

未备注 14

误报 1

情报来源

Github 15

黑产QQ群 0

情报类型

AK授权码泄露 1

用户账号泄露 14

情报信息

情报: AK授权码泄露

泄露用户名: default

情报来源: Github

泄露类型:

受影响资产: 云平台

备注: 大萨达大

误报: 否 (标记为误报)

代码片段

防护建议

1、禁止员工将公司源代码托管至Github等代码平台，防止源代码或数据库密码等泄露；
2、如果发现阿里云AK信息泄露，立即进入AK控制台，禁用并重置AK（或直接删除）；
3、如是RDS、ECS等密码泄露请尽快修改相关资产密码，并尽快删除Github托管代码；
4、前往日志检索平台，搜索对应的服务器访问日志（如检索日志源web访问日志，选择URI字段，包含有AK应用文件的文件路径），确认数据是否泄漏。

列表

发现时间

情报

受影响资产

泄露类型

泄露用户名

情报来源

备注

操作

	AK授权码泄露	云平台	--	default	Github	大萨达大	详情
2017-08-21 10:44:16	用户账号泄露	120.55.88.43	SSH	root	Github	--	详情
2017-08-21 10:44:16	用户账号泄露	120.55.88.43	FTP	V334Yx9d	Github	--	详情
2017-08-12 11:33:33	用户账号泄露	120.26.134.154	MongoDB	cms_dev	Github	--	详情
2017-08-12 11:33:33	用户账号泄露	123.56.113.131	MySQL	welical	Github	--	详情
2017-08-12 11:33:33	用户账号泄露	114.215.139.157	MySQL	root	Github	--	详情
2017-08-12 11:33:33	用户账号泄露	114.55.248.130	MySQL	tuerbao	Github	--	详情
2017-08-12 11:33:33	用户账号泄露	120.24.42.115	MySQL	root	Github	--	详情
2017-08-12 11:33:33	用户账号泄露	139.129.205.152	MySQL	admin	Github	--	详情
2017-08-12 11:33:33	用户账号泄露	apccofanewsprivate.mysql.rds.aliyuncs.com	RDS	searchadmin	Github	--	详情

- 详情

如何操作

操作指南

- 情报功能，是纯自动化服务，每天都会监控互联网上的企业相关情报，并通过消息推送的方式把告警信息上报到控制台中

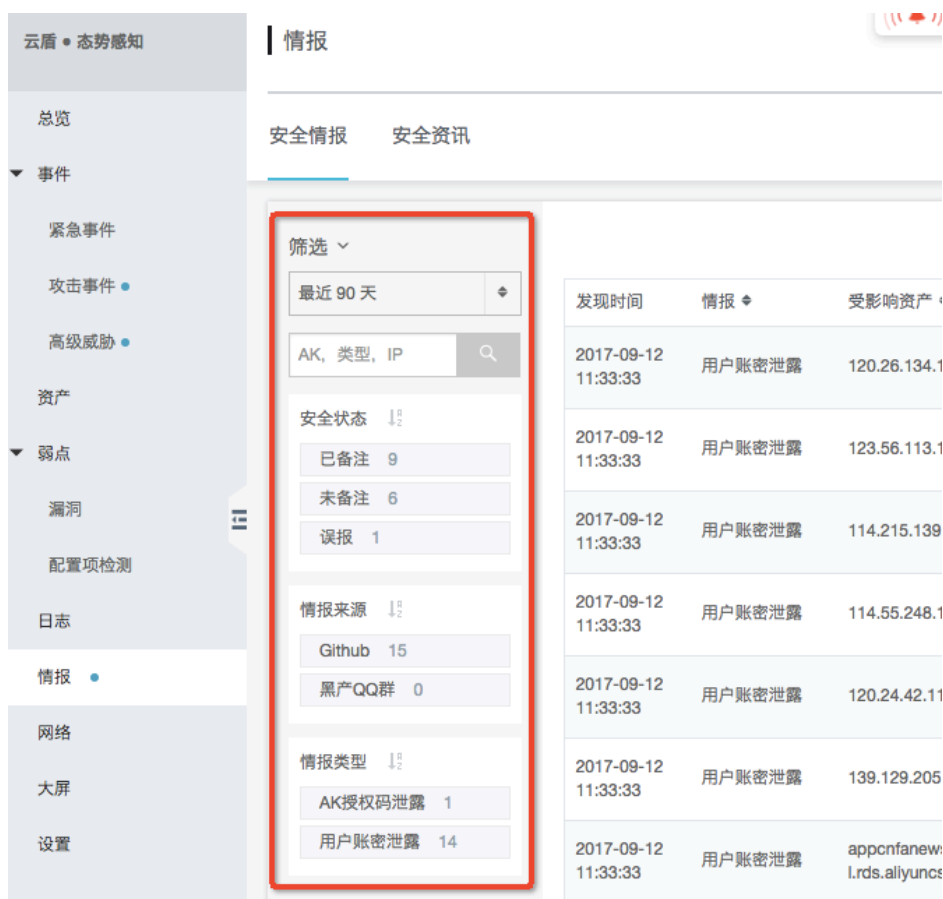
控制台地址：

- <https://yundun.console.aliyun.com/?spm=5176.7946181.209102.4.7pkLDx&p=sas#/info/sec>

操作



- 可筛选和检索情报信息（可输入资产IP,泄露类型，AK等）：



免费开通，付费升级

简介

- 云盾态势感知是一个SaaS化产品，即开即用，无需任何配置，开通后即可享受实时的安全态势监控，和40余种安全事件告警项。

如何免费使用

- 在阿里云控制台，前往：《云盾》-《态势感知》，点击免费开启服务，即可使用态势感知（基础版）



云盾·态势感知

态势感知：收集企业20种原始日志和网络空间威胁情报，利用机器学习还原已发生的攻击，并预测未发生的攻击。
您尚未购买“云盾·态势感知”：

版本对比

基础版	专业版	企业版
即开即用的态势感知平台，具备基础安全检测能力，适合中小站长。	功能完整的态势感知平台，具备全面的持续安全监控能力，适合专业用户	长时间日志保存，满足合规要求，适合企业用户
• 7种基础威胁检测 • SQL注入、XSS应用漏洞扫描 • 1个告警通知人	获得基础版所有功能，以及 • 几十种高级威胁检测 • 上千种应用漏洞扫描 • 资产风险管理 • 安全态势日报 • 10个告警通知人 • 保存7天原始日志 (详情)	获得专业版所有功能，以及 • 10块可视化大屏 (详情) • 保存180天原始日志
开通使用	立即购买	立即购买

如何升级至更高版本

- 在管理控制台，点击右上角的升级按钮，付费成功后，即可升级至专业版，企业版
- 功能特性，版本对比

态势感知试用指南

如何开通试用？

- 如您已经获得试用机会，在态势感知控制台任意页面中会有弹窗提醒，您只需点击“开通试用”即可



，截图如下：

试用指南

《态势感知》能帮您监控和管理云上业务的安全事件，并实时告警，提升您对安全事件的响应速度和效率，如下是态势感知的一些介绍和文档。

- 1、态势感知介绍和应用场景：https://help.aliyun.com/knowledge_detail/42302.html
- 5、态势感知功能特性：https://help.aliyun.com/knowledge_detail/42306.html
- 3、态势感知配置告警人：https://help.aliyun.com/document_detail/58032.html
- 4、态势感知-日志检索教程：https://help.aliyun.com/document_detail/54090.html
- 2、态势感知常见问题：https://help.aliyun.com/knowledge_list/42320.html

使用手册

下面我们从“洞察”、“洞悉”、“洞彻”三个方面，对云盾态势感知的安全分析能力、应用管理能力以及威胁发展趋势预测能力进行了评估与分析。

洞察——态势感知安全分析能力解析

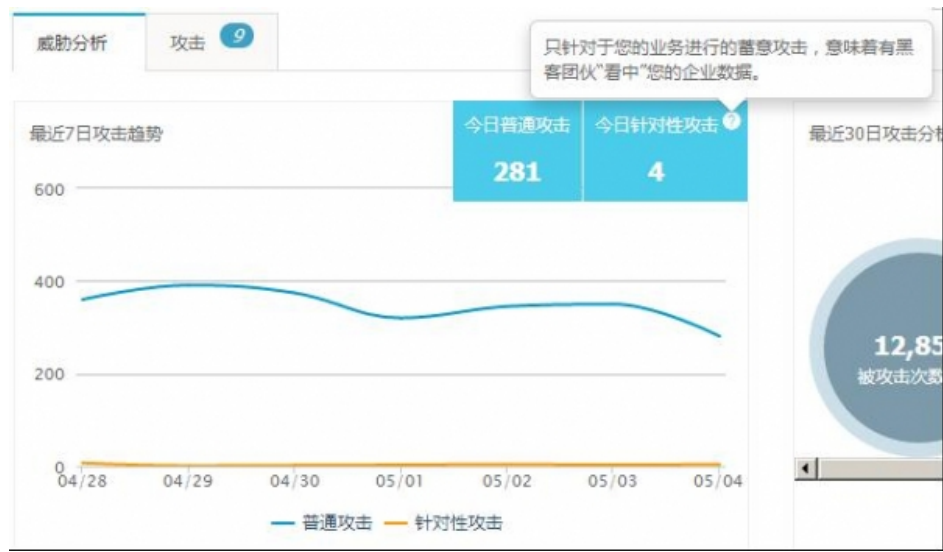
企业如果可以对自身的安全况态实时进行洞察、对网络威胁动态清晰掌握，自然可以查敌先机，先于对手做好防御工作，甚至主动出击将黑客擒拿归案，使其接受法律的制裁。那么如何可以对自身应用做到洞察秋毫呢，下面我们从态势感知的“感胁”、“弱点”、以及“紧急事件”几个部分，来具体做分析：

威胁分析

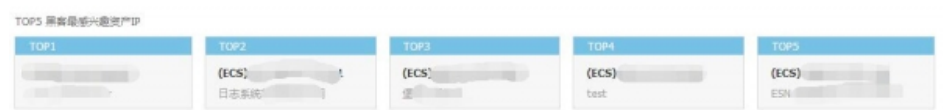
从海量的正常应用中识别网络威胁是安全分析平台很重要的能力。



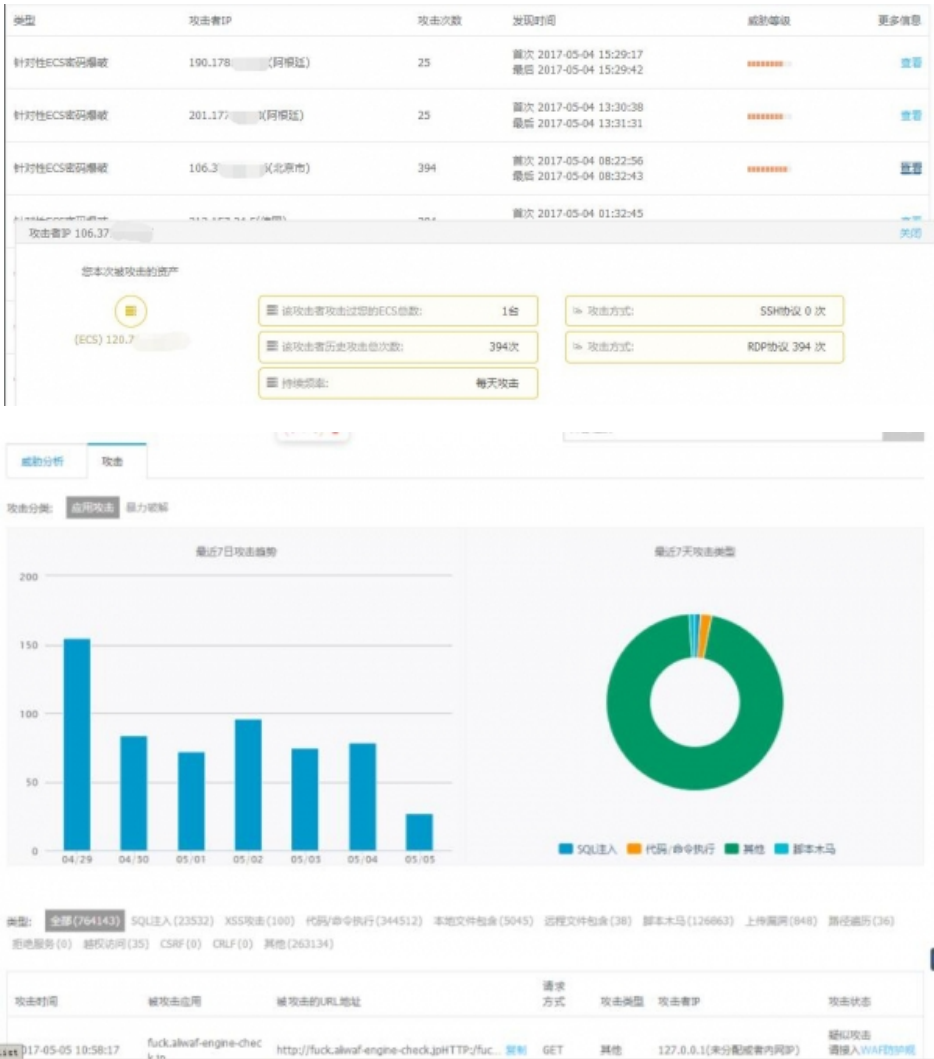
态势感知的威胁分析功能可以对Web攻击、密码爆破、撞库、扫描器等网络威胁和异常登录、非常用IP连接、批量账号登录等异常网络行为进行统计。当态势感知对此类攻击查觉之后，会向用户提供有针对性的解决方案，便于用户及时对威胁进行处理。



在威胁分析中，不但可以对常见的普通攻击进行统计，还可以将只针对于某特点用户或业务的攻击进行记录。和撒大网一样的普通攻击相比，针对性攻击往往意味着黑客已经对企业数据进行了“重点关注”。



在这方面，威胁分析可以将黑客最感兴趣的资产IP统计出来，以便于用户更加具有针对性的去进行防护。当黑客的攻击行为，不在隐匿在黑暗之中，可以被用户极时的感知，并有针对性的进行处理，黑客对企业的威胁必然也将随之下降。



威胁分析不但可以有效的将用户从海量日志分析中解放出来，直观的对攻击者的IP、攻击时间、次数、频率以及攻击方式进行记录，协助用户对攻击者进行溯源，以便从根源上解决问题之外，更重要的是，这些模型全部运行在云盾的实时检测引擎中，以前做这样的分析，需要写大段脚本并用离线的方式做大量计算，现在云盾的实时引擎可在5分钟内对黑客历史的数据进行遍历，以最快的方式分析出最新的网络威胁，真正的为用户提供了—双可以及时对威胁进行洞察的双眼。

弱点检测

企业信息系统中难免会存在一些旧有，或新出现的系统漏洞。这些弱点问题如果不能及时处理，也会对系统安全造成威胁。态势感知的弱点检测功能，可以有效的弥补这一短板。

弱点功能，不光覆盖了常见的SQL注入，XSS等awasp定义的各类漏洞，还能对互联网最新曝光的漏洞进行快速扫描外。在漏洞的发现上，做到快速和准确。

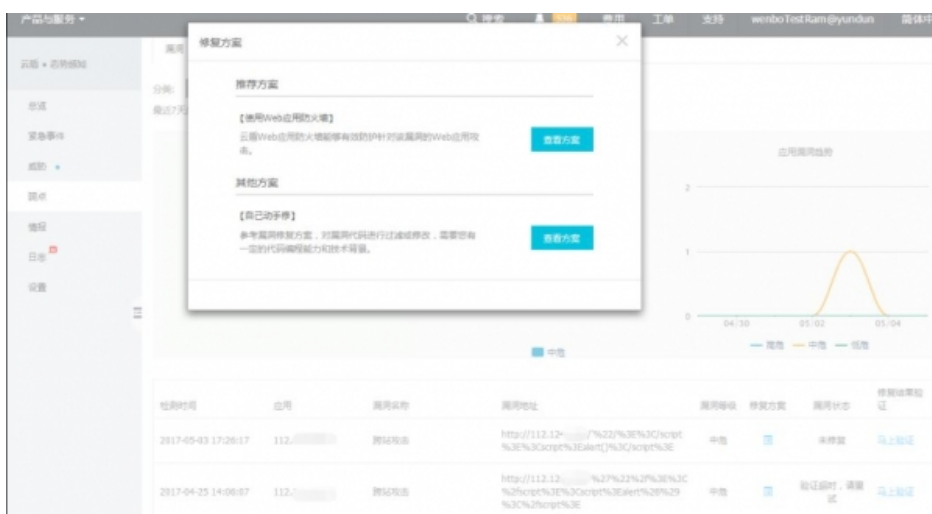
此外，弱点检测功能可以通过对资产的依赖关系，通过针对漏洞的攻击识别和攻击效果（例如有没有攻击成功、WAF是否防御、漏洞是否能直达核心服务器、是否能拖走数据库等），对当前漏洞的风险进行动态评估，并对补丁的下发，补丁是否需要重启服务器等信息做补全，方便客户做应急响应和业务决策。

比如前些天爆发的全球性勒索软件事件主因是这个漏洞：“MS17-010 远程命令执行漏洞”。用户可前往《云盾》-《态势感知》-《弱点》查看是否存受影响：

就是这个漏洞，没有就安心周末吧！

检测时间	应用	漏洞名称	漏洞地址	漏洞等级	修复方案	漏洞状态	修复结果验证
2017-05-13 21:06:56	445	MS17-010 远程命令执行漏洞	http://445	高危		未修复	马上验证

当监测到漏洞出现之后，态势感知会及时向用户告警，并提供相应解决方案，协助用户及时将漏洞进行弥补。



紧急事件

紧急事件就是客户最需要紧急处理的事件！不处理就会产生资损或业务中断。

态势感知的紧急事件功能，可以针对页面篡改、肉鸡行业、暴力破解成功、后门、DDoS、非法登陆、异常网络连接等多种网络威胁行为进行感知，并及时向用户进行告警。并可对受影响资产信息以及威胁事件进行详细描述，以便于用户有针对性的去解决问题。

紧急事件中，大部分告警都来自于网络，主机，应用，三种不同维度的大数据分析的结果。这里面的核心能力是在于，这三种数据的数据结构完全不同，属于异构数据，态势感知的紧急事件功能，利用云计算的大数据处理能力，能够在几分钟内快速的处理上TB的数量，并能对各维度的威胁和异常点进行关联，最后产出能引起资损的紧急事件。



当用户接到紧急事件告警后，可以通过查看报告了解威胁的具体情况，并且可以根据态势感知提供的解决方案，对事件妥善进行处理。

洞悉——态势感知应用管理能力分析

三分防，七分管。一款出色的防护软件，不但要对威胁及时察觉，还应协助用户对正常应用进行分析和管理。帮助用户了解网络系统中有哪些应用最受用户关注，哪些访问是恶意在进行灌水，访问流量的高峰会在何时出现，系统的业务稳定性如何进行保障。

目前，阿里云云盾的态势感知则是基于阿里云的实时计算能力，即在大规模云计算环境中，对那些能够引发网络安全态势发生变化的要素，进行全面、快速和准确地捕获和分析，最终分析判断出未来可能产生的安全事件的威胁风险，并提供一个体系化的安全解决方案。下面，我们就从访问分析、资产探测、业务稳定这三方面，再对态势感知应用管理能力分析能力进行一下了解。

访问分析

在态势感知的访问分析功能模块中，可以对来访IP进行分别进行统计，并且将正常访问IP与恶意访问IP进行区分。使用户可以了解什么服务器部署的什么应用最受用户关注，有哪些应用的访问数量过高，是否需要将其中的业务在其它服务器上进行负载均衡。



在对正常访问进行统计的同时，访问分析还可以对恶意访问IP进行统计，查看进行访问的网络连接中，是否有恶意灌水的情况出现。从而更加精准的协助用户对业务访问情况进行判断。从而保障用户网络业务稳定高效的进行运营。

来访IP	识别类型	发生时间	UserAgent	目标应用	访问页面个数	最高每秒访问次数	本次访问是否有Web攻击
1.160.182	恶意IP	2017-05-08 04:50:50		5.211	2	1	否
18.6	恶意IP	2017-05-08 00:16:21		5.211	2	1	否
214.241	恶意IP	2017-05-08 00:16:37		55.211	2	1	否
8.234.206	恶意IP	2017-05-08 22:18:56		55.211	2	1	否
3.85.90 (北京市)	恶意IP	2017-05-08 00:17:20		5.211	2	3	否

资产探测

当用户在云计算系统中的应用增长至一定规模之后，对这些资产的运营管理问题将逐渐开始显现：哪些应用开放了什么样的端口？对应着什么样的域名？是否存在未进行修补的漏洞？态势感知的资产探测功能可能有效的协助用户进行这方面的管理。

安全总览	网络流量	访问分析	资产探测	可视化大屏	
服务器IP	OS版本	使用软件	开放端口个数	组件	操作
(ECS) 10.20.0.10 数据库审计	CentOS release 6.8 (Final)	--	昨日: 0 今日: 0	--	查看详情
(ECS) 101.20.0.10 iZ2reShwdrnseeb1d1ygstyZ	Ubuntu 14.04.4 LTS	--	昨日: 1 今日: 1	--	查看详情
(ECS) 101.20.0.10 iZ25pdqthc8Z	Microsoft Windows Server 2012 Standard Edition (build 9200), 64-bit_X64	--	昨日: 2 今日: 1	--	查看详情
(SLB) 101.20.0.10	--	--	昨日: 2 今日: 2	--	查看详情
(ECS) 101.37.0.10 baolei_test_win	Microsoft Windows Server 2008 R2 Enterprise Edition Service Pack 1 (build 7601), 64-bit	--	昨日: 1 今日: 1	--	查看详情
(ECS) 106.14.0.10 测试上海测试服务器	CentOS Linux release 7.2.1511 (Core)	--	昨日: 1 今日: 1	--	查看详情
(ECS) 106.14.0.10 态势感知中心测试服务器	CentOS Linux release 7.3.1611 (Core)	MySQL, Python	昨日: 2 今日: 2	--	查看详情
(ECS) 112.12.0.10 测试支付系统测试	Microsoft Windows Server 2003 R2, Standard Edition Service Pack 2 (build 3790)_X86	w3wp	昨日: 2 今日: 2	--	查看详情

在资产探测模块中，可以直观的对服务器IP、操作系统版本、使用软件、开放端口个数进行了解，并可以在查看详情中进一步对开放的端口号、是否存在弱点漏洞进行查看。从而便于用户对当前网络资产进行更加有效的监管。在减少漏洞的同时，对企业网络业务进行统一规划。

网络业务的稳定运营，需要对全网的网络状况有一个全局的掌握。网络的业务响应时延，是评价业务状态的一个最直观的技术指标。

在态势感知可视化大屏的“业务稳定性监控”中，可以对全国各地网络业务的响应时延，进行实时的查看。并将国内重点城市、响应最快与最慢的地区电信服务商以图文的形式提供了出来，极大方便了用户对于网络运营状态的全局掌控。



洞彻——态势感知威胁发展趋势预测

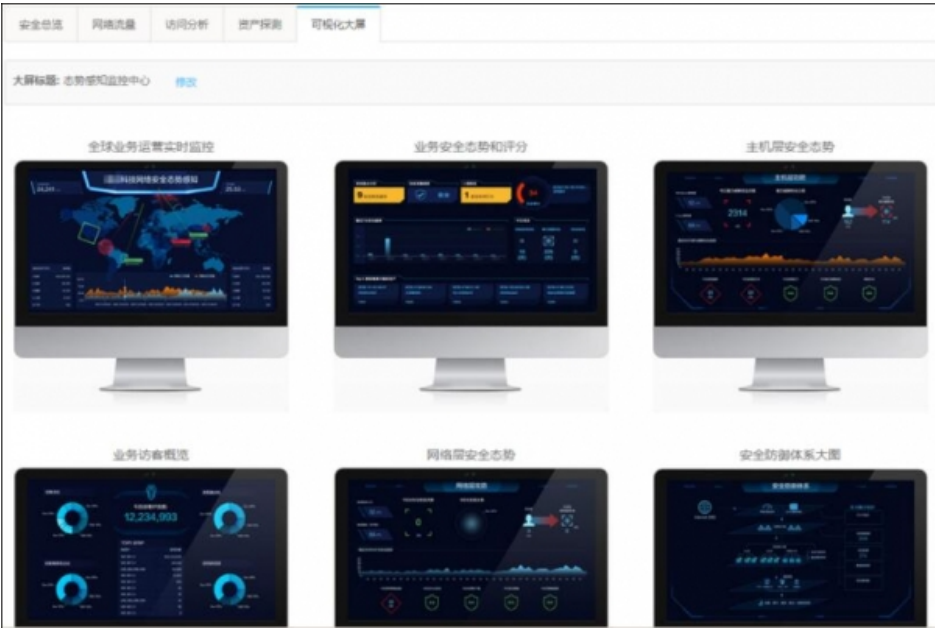
对风险进行预判，将威胁消灭在萌芽之中，这确实可以称得上是安全防护的最高境界。但是安全的风险需要如何进行预判？威胁信息又应当如何进行采集、分析？在海量的日志和频发的威胁告警中如何对有效信息进行判定？有很多SIEM（安全信息与事件管理）工具也在进行着日志审计类的工作，但其效果往往是亡羊补牢，对于当前主流的“0 day”等新发网络威胁，基本上无能为力。防患于未然对于网络安全而言，更多的是一种美好的梦想。

企业要想追求网络业务的良性发展，就必须对业务发展和威胁趋势进行准确判断。

对于小微企业和个人用户而言，一个安全事件告警就可以满足用户的防护需求。而有一定服务器规模的用户，还需要有对紧急事件和威胁分析能力、漏洞扫描以及系统脆弱点进行监控的能力。但是对于一些上规模的企业而言，就需要具备实时可视化的业务与威胁感知能力。下面我们就来看一下，云盾态势感知是如何通过10块可视化大屏界面与高效全面的情报分析能力，来协助用户实时对业务和威胁进行感知的。

可视化大屏

态势感知为用户提供了10块可视化的实时监控大屏，通过可视化的方式，实时的对业务运营状态、安全态势、业务访问状况等多种信息进行分析，并以图形化的方式实时的展现到客户面前。从而协助用户对企业业务进行管理，对威胁状态进行预判，保障企业网络应用业务的稳定运营。



情报分析

态势感知系统，并不是一个简单的图形化管理界面，在它的背后是由阿里云的大数据安全分析平台进行支撑。态势感知系统通过对资产、自然、情报三大类二十余种数据的采集，对资产等级划分、漏洞/隐患分析，对攻击和异常行为的感知、对业务风险的评估，以及对入侵过程的回溯、恶意行为的回溯乃至对黑客身份的定位等多种严密的分析形式，有效的协助企业解决因黑客攻击导致企业数据泄露问题的出现。



安全威胁处置

态势感知的分析系统会自动化的实时进行百亿级日志分析。依靠机器学习和建模算法，黑客攻击的下一步行动点，都可以被预测，并让防御提前发生。并且态势感知具有对每个安全事件，在攻击前后一定时间内的原始日志数据分析检索能力，可以通过威胁模型自动化分析和还原黑客攻击全过程，对入侵原因进行回溯，帮助找到“幕后的人”。

全量日志的准实时逻辑检索引擎



全量日志的采集和TB级大数据量的处理，一直是运维团队日常比较繁重的工作，现在态势感知利用了云的资源优势，和大数据处理能力，帮客户自动采集了云上全业务的网络流量HTTP请求日志（in，out方向），session五元组日志（全端口网络连接五元组），并能对15分钟前的全量日志进行逻辑检索，支持布尔表达式，如包含，不包含，等于，不等于，大于，小于，等逻辑。方便客户，对安全事件，或网络异常，进行日志查询和关联分析，更快更准更便捷的精准定位问题原因

功能截图

监控大屏

通过可视化大屏，对云上整体安全进行实时监控和告警



总览

云盾的态势感知从网络底层的协议解析，一直到主机层，应用层的异常行为分析，真正为用户提供可视化、透明化的数据分析能力。

通过网络行为层面检测到异常，云盾的态势感知形成了从“异常发现-实时分析-追溯取证”的整个安全解决方案闭环，并辅以直观的可视化的分析，让安全一目了然



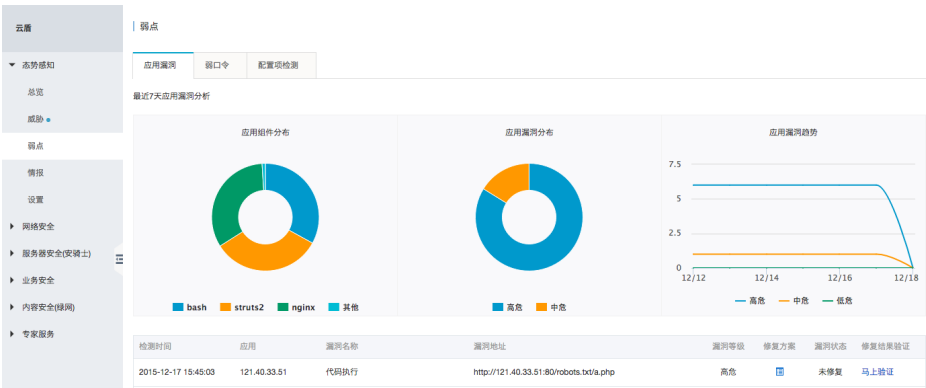
对云平台各安全状况进行统一展示，包含网络流量，主机拓扑，系统弱点等维度，并对网络DDoS攻击进行实时监控，对需要处理的紧急事件就行实时监控。

威胁



对攻击进行大数据分析，产出攻击特征，按攻击行为进行整合并对黑客的渗透攻击全面响应。

弱点



对系统自身存在的脆弱点和漏洞等问题进行检测，产出应用漏洞，弱口令，配置项隐患等检测项，让客户能把黑客入侵的几率降到最低

情报

同时，产品还具备“能监控、能记录”的特点。利用网络回溯分析系统，能够把用户所有产生的数据都保存下来，进行历史纪录，如有问题就可以追溯分析，实现实时监测和智能化取证。



包含了人员情报，应急响应情报，漏洞情报，行业新闻等外部的安全威胁，对可能对企业造成资产损失的安全事件进行实时监控，避免因外部问题造成安全事件。

功能点列表

分类	功能名	描述
总览	总览	当前云上业务的总体概览
	网络流量	云上业务的网络出入口流量曲线图
	安全可视化	可视化大屏
	资产探测	全部资产系统软件版本，OS版本检测
	访问分析	用户访问行为分析
紧急事件	页面篡改	页面内容被黑客篡改或黄赌毒页面
	页面篡改-篡改途径追溯	黑客恶意行为是由于何种漏洞导致入侵的
	肉鸡行为	ECS向外发起DDoS攻击或者暴力破解攻击
	肉鸡行为-进程定位	定位到是由哪个进程或者EXE程序发起的恶意新闻给
	暴力破解成功	通过登陆密码的拆解，最后爆破成功，登陆到ECS
	后门-webshell	典型的webshell后门
	后门-一句话shell检测	在正常文件中植入一句话可执行代码，可被长期控制
	后门-一句话shell入侵原因	分析发现被植入shell的原因，以及漏洞定位
	后门-shell恶意行为回放	黑客利用一句话shell执行了何种命令
	后门-独立多功能后门	带有独立控制台的大型shell
	后门-独立多功能后门入侵原因	发现被植入shell的原因
	后门-黑客溯源	通过威胁情报数据，溯源到黑客的身份和基本信息
	DDoS攻击检测	DDoS攻击识别
	DDoS-流量攻击分析	DDoS攻击中的流量攻击成分分析
	黑客非法登陆	服务器被恶意IP库中的IP进行了登陆和非法操作
	黑客非法登陆-详情信息	恶意IP的基本信息，如恶意行为判定和IP定级
	异常网络连接	主机中发生的异常网络请求，如请求恶意url源下载了恶意病毒等
	异常网络连接-连接病毒源分析	恶意病毒的威胁情报数据，如连接状况，存活周期等
	异常下载	服务器中有被异常下载的文件，如数据库数据，网站备份文件等
	异常下载-详情分析	详细分析被下载的备份文件大小，文件名，下载者信息等
威胁	攻击识别	web攻击识别
	定点web攻击	从攻击数据中探测到更有针对性的web攻击，如黑客定点攻击，批量扫描等
	针对性ECS密码爆破	从攻击数据中探测到更有针对性的密码爆破攻击，如黑客定点攻击，批量扫描等
	撞库攻击	探测黑客对login页面或最终用户的登陆库进行社工库撞库攻击
	登陆后台身份识别	对客户CRM或者后台库进行登陆识别，查找出被黑客登陆CRM的告警
	非常用IP连接数据库	对连接客户数据库的IP进行识别，告警异常行为
	扫描器攻击	来自扫描引擎的漏洞攻击
	跳板机识别	对异常的内网连接进行告警，避免内网被入侵后进一步的渗透
	发现代理服务	排查是否有非法开设的代理服务，进行告警，避免被黑客利用
	发现挖矿程序	ECS被利用为挖矿程序
	pingback被恶意利用	漏洞恶意利用
	WEBSHELL探测	webshell攻击行文检测
弱点	应用漏洞扫描	漏洞扫描
	主机漏洞	主机漏洞，系统漏洞等
	弱口令-ECS登陆弱口令	ECS的登陆弱口令，RDP和SSH协议
	弱口令-应用后台登陆弱口令	对后台CRM或CMS后台进行弱口令检测
	配置检测	对服务器配置或者如php.ini文件进行配置隐患检测
	配置检测-服务器配置文件检测	对服务器的配置或者防火墙，端口开放策略进行检测

*随着产品版本更新和功能迭代，列表可能和实际功能有偏差，请以控制台的实际功能为准

如何设置告警通知和日报邮件

如何设置告警通知和日报邮件

- 1. 进入《态势感知》-《设置》页面
- 2. 点击《安全日报》和《告警设置》即可进行告警配置



安全日报配置

- 安全日报可将当天24小时内的安全事件汇总，并进行邮件的发送，方便安全管理员总结一天的工作进展
- 一般邮件于凌晨1:00-6:00发出，汇总了昨天24小时的安全态势



配置步骤

- 配置安全日报的标题
- 配置安全日报的收件人
- 完成

安全告警通知项

- 前往《态势感知》-《设置》-《告警设置》页面
- 选择对应的告警项目，选择短信或者邮件的方式告警
- 告警频率
 - 对于紧急事件，告警短信发送为实时，但为了不打搅客户，同一事件一小时只会短信一次
 - 对于攻击事件，告警短信和邮件发送每天只会发送一次
- 告警人的设置，请前往《告警联系人》页面