



## 思科安全分析和日志记录

- 关于 Cisco Defense Orchestrator 中安全分析和日志记录 (SaaS) ， 第 2 页
- CDO 中的事件类型 ， 第 2 页
- 关于 ASA 的安全分析和日志记录 (SAL SaaS), on page 7
- 为 ASA 设备实施安全日志记录分析 (SaaS) ， 第 10 页
- 使用 CDO 宏将 ASA 系统日志事件发送到思科云, on page 12
- 使用命令行接口将 ASA 系统日志事件发送到思科云, on page 15
- ASA 设备的 NetFlow 安全事件日志记录 (NSEL), on page 21
- 已解析的 ASA 系统日志事件, on page 33
- 为云交付的防火墙管理中心托管设备实施 SAL (SaaS) ， 第 34 页
- SAL (SaaS) 集成的要求、准则和限制 ， 第 34 页
- 使用系统日志将云交付的防火墙管理中心托管事件发送到 SAL (SaaS) ， 第 35 页
- 使用直接连接将云交付的防火墙管理中心托管的时间日志发送到 SAL (SaaS) ， 第 37 页
- 启用或禁用威胁防御设备以使用直接连接将事件日志发送到 SAL (SaaS) ， 第 38 页
- 安全事件连接器 ， 第 39 页
- 安装安全事件连接器 ， 第 40 页
- 取消调配思科安全分析和日志记录 (SaaS) ， 第 59 页
- 删除安全事件连接器 ， 第 60 页
- 调配思科安全云分析门户, on page 61
- 在安全云分析中查看传感器运行状况和 CDO 集成状态 ， 第 62 页
- 用于全面网络分析和报告的思科安全云分析传感器部署, on page 62
- 从 CDO 查看 Cisco Secure Cloud Analytics 警报, on page 63
- 思科安全云分析和动态实体建模, on page 64
- 使用基于防火墙事件的警报, on page 65
- 修改警报优先级 ， 第 71 页
- 查看实时事件, on page 71
- 在事件日志记录页面上显示和隐藏列, on page 74
- 可自定义的事件过滤器, on page 77
- 安全分析和日志记录中的事件属性, on page 78
- 在事件日志记录页面中搜索和过滤事件 ， 第 110 页

- [下载后台搜索](#)，第 119 页
- [数据存储计划](#), on page 119
- [查找用于安全日志记录分析 \(SaaS\) 的设备 TCP、UDP 和 NSEL 端口](#), on page 121

## 关于 Cisco Defense Orchestrator 中安全分析和日志记录 (SaaS)

思科安全分析和日志记录 (SAL) 允许您从所有 ASA 设备捕获连接、入侵、文件、恶意软件和安全情报事件，以及从 Secure Firewall Threat Defense 捕获所有系统日志事件和 Netflow 安全事件日志记录 (NSEL) 事件并在 Cisco Defense Orchestrator (CDO) 中的一个位置进行查看。事件存储在思科云中，可从 CDO 中的事件日志记录 (**Event Logging**) 页面查看，您可以在其中过滤和查看事件，以便清楚地了解在网络中触发的安全规则。

通过额外许可，在捕获这些事件后，您可以从 CDO 交叉启动为您调配的安全云分析门户。安全云分析是一种软件即服务 (SaaS) 解决方案，通过对事件和网络流数据执行行为分析来跟踪网络状态。通过从源（包括防火墙事件和网络流数据）收集有关网络流量的信息，它会创建有关流量的观察结果，并根据其流量模式自动识别网络实体的角色。使用此信息与其他威胁情报来源（例如 Talos）相结合，安全云分析会生成警报，警告可能存在恶意行为。除警报外，安全云分析还提供网络和主机可视性以及所收集的情景信息，为您研究警报和查找恶意行为的来源提供更好的基础。

**术语说明：**在本文档中，当思科安全分析和日志记录与安全云分析门户（软件即服务产品）配合使用时，您会看到此集成称为思科安全分析和日志记录 (SaaS) 或 SAL (SaaS)。

## CDO 中的事件类型

过滤安全日志分析 (SaaS) 记录的 ASA 和 Secure Firewall Threat Defense 事件时，可以从 CDO 支持的 ASA 和 FTD 事件类型列表中进行选择。从 CDO 菜单中，导航到分析 (**Analytics**) > 事件日志记录 (**Event Logging**)，然后单击过滤器图标以选择事件。这些事件类型代表系统日志 ID 组。下表显示了包含在何种事件类型中的系统日志 ID。如果要了解有关特定系统日志 ID 的更多信息，可以在[思科 ASA 系列系统日志消息](#)或[Cisco Secure Firewall Threat Defense 系统日志消息](#)指南中进行搜索。

某些系统日志事件将具有附加属性“EventName”。您可以通过过滤“属性:值”对来过滤事件表，查找使用 EventName 属性的事件。请参阅[系统日志事件的 EventName 属性](#)。

某些系统日志事件将具有附加属性“EventGroup”和“EventGroupDefinition”。您将能够通过过滤“属性:值”对来过滤事件表，查找使用这些附加属性的事件。请参阅[某些系统日志消息的 EventGroup 和 EventGroupDefinition 属性](#)。

NetFlow 事件不同于系统日志事件。**NetFlow** 过滤器搜索生成 NSEL 记录的所有 NetFlow 事件 ID。这些 NetFlow 事件 ID 在《[思科 ASA NetFlow 实施指南](#)》中进行了定义。

下表介绍了 CDO 支持的事件类型，并列出了与这些事件类型对应的系统日志或 NetFlow 事件编号：

过滤器名称	说明	相应的系统日志事件或 NetFlow 事件
AAA	这些是系统在配置 AAA 的情况下，在认证、授权或用尽网络资源的尝试失败或无效时生成的事件。	109001-109035 113001-113027
僵尸网络	当用户尝试访问可能包含受恶意软件感染的主机（可能是僵尸网络）的恶意网络时，或者当系统检测到流向或来自动态过滤器阻止列表中的域或 IP 地址的流量时，系统会记录这些事件。	338001-338310
故障切换	当系统在发生故障切换时检测到有状态和无状态故障切换配置中的错误或辅助防火墙设备中的错误时，将记录这些事件。	101001-101005、102001、 103001-103007、 104001-104004、105001-105048 210001-210022 311001-311004 709001-709007
防火墙被拒绝	当防火墙系统出于各种原因拒绝网络数据包流量时，会生成这些事件，从安全策略导致的数据包丢弃到由于系统收到具有相同源 IP 和目的 IP 的数据包而导致的丢弃，这可能意味着对网络的攻击。  防火墙拒绝事件可能包含在 NetFlow 中，并且可能使用 NetFlow 事件 ID 和系统日志 ID 进行报告。	106001, 106007, 106012, 106013, 106015, 106016, 106017, 106020, 106021, 106022, 106023, 106025, 106027

过滤器名称	说明	相应的系统日志事件或 NetFlow 事件
防火墙流量	<p>这些是根据网络中的各种连接尝试、用户身份、时间戳、终止的会话等记录的事件。</p> <p>防火墙流量事件可能包含在 NetFlow 中，并且可能使用 NetFlow 事件 ID 和系统日志 ID 进行报告。</p>	<p>106001-106100, 108001-108007, 110002-110003</p> <p>201002-201013、 209003-209005、215001</p> <p>302002-302304、 302022-302027、 303002-303005、 313001-313008、 317001-317006、 324000-324301、337001-337009</p> <p>400001-400050, 401001-401005, 406001-406003, 407001-407003, 408001-408003, 415001-415020, 416001, 418001-418002, 419001-419003, 424001-424002, 431001-431002, 450001</p> <p>500001-500005、508001-508002</p> <p>607001-607003、 608001-608005、 609001-609002、616001</p> <p>703001-703003、726001</p>
IPSec VPN	<p>当 IPSec 安全关联中发生不匹配或系统在其接收的 IPSec 数据包中检测到错误时，这些事件会记录在 IPSec VPN 配置的防火墙中。</p>	<p>402001-402148、 602102-602305、702304-702307</p>
NAT	<p>当创建或删除 NAT 条目时，以及当 NAT 池中的所有地址都用尽并耗尽时，这些事件会记录在 NAT 配置的防火墙中。</p>	<p>201002-201013、 202001-202011、305005-305012</p>
SSL VPN	<p>当创建或终止 WebVPN 会话、用户访问错误和用户活动时，这些事件会记录在 SSL VPN 配置的防火墙中。</p>	<p>716001-716060、 722001-722053、 723001-723014、 724001-724004、725001-725015</p>
NetFlow	<p>当网络数据包进出接口时，这些事件记录在 IP 网络流量、时间戳、用户身份和传输的数据量周围。</p>	<p>0, 1, 2, 3, 5</p>

过滤器名称	说明	相应的系统日志事件或 NetFlow 事件
连接	<p>您可以在用户生成通过系统传递的流量时生成连接事件。启用访问规则连接日志记录以生成这些事件。还可启用安全情报策略和 SSL 解密规则日志记录，以生成连接事件。</p> <p>连接事件包含关于检测到的会话的数据。任何单个连接事件的可用信息都取决于多种因素，但通常包括：</p> <ul style="list-style-type: none"> <li>• 基本连接属性：时间戳、源和目标 IP 地址、入口和出口区域，处理连接的设备等。</li> <li>• 系统发现或推断的其他连接属性：应用、请求的 URL 或与连接关联的用户等。</li> <li>• 有关连接记录原因的元数据：哪个配置处理流量，连接是被允许还是被阻止，以及有关已加密和已解密连接的详细信息等。</li> </ul>	430002, 430003
入侵	<p>系统检查网络上传输的数据包是否存在可能影响主机及其数据的可用性、完整性和机密性的恶意活动。如果系统识别出潜在的入侵，会生成入侵事件；入侵事件是有关攻击源和攻击目标的日期、时间、攻击程序类型以及情境信息的记录。无论调用访问控制规则的日志记录配置如何，系统均会生成设为阻止或提醒的入侵规则的入侵事件。</p>	430001

过滤器名称	说明	相应的系统日志事件或 NetFlow 事件
文件	<p>文件事件表示系统基于文件策略在网络流量中检测到或者被阻止的文件。只有在应用文件策略的访问规则中启用文件日志记录，才能生成这些事件。</p> <p>无论调用访问控制规则采用何种日志记录配置，在系统生成文件事件时，都会记录相关连接的终止。</p>	430004
恶意软件	<p>作为整体访问控制配置的一部分，系统可在网络流量内检测恶意软件。适用于 Firepower 的 AMP 可以生成恶意软件事件，其中包含生成事件的处置，有关检测该恶意软件的方式、位置和时间的情境数据。只有在应用文件策略的访问规则中启用文件日志记录，才能生成这些事件。</p> <p>文件的处置可能发生变化，例如，从安全变为恶意软件或从恶意软件变为安全。如果适用于 Firepower 的 AMP 向 AMP 云查询文件，且云决定在查询一周内更改处置，系统即会生成追溯性恶意软件事件。</p>	430005
安全情报	<p>安全情报事件是由安全情报策略为该策略阻止或监控的每个连接生成的一种连接事件。所有安全情报事件都有一个由系统填充的“安全情报类别”字段。</p> <p>对于各事件，都有一个相应的“常规”连接事件。由于评估安全智能策略后才会评估许多其他安全策略（包括访问控制），所以当安全智能阻止连接时，所生成事件不含系统从后续评估中收集的信息（如用户身份）。</p>	430002, 430003

# 关于 ASA 的安全分析和日志记录 (SAL SaaS)

通过安全分析和日志记录 (SaaS)，您可以从 ASA 捕获所有系统日志事件和 Netflow 安全事件日志记录 (NSEL)，并在 Cisco Defense Orchestrator (CDO) 中的一个位置进行查看。

事件存储在思科云中，可从 CDO 中的“事件日志记录”页面查看，您可以在其中过滤和查看事件，以便清楚地了解在网络中触发的安全规则。日志记录和故障排除软件包为您提供这些功能。

使用日志记录分析和检测包（以前称为防火墙分析和日志记录包），系统可以将安全云分析动态实体建模应用于 FTD 事件，并使用行为建模分析生成安全云分析观察结果和警报。如果您获取全部网络分析和监控软件包，则系统会对 FTD 事件和网络流量应用动态实体建模，并生成观察结果和警报。您可以使用思科单点登录从 CDO 交叉启动为您调配的安全云分析门户。

## 如何在 CDO 事件查看器中显示 ASA 事件

在 ASA 上启用日志记录且网络流量与访问控制规则条件匹配时，会生成系统日志事件和 NSEL 事件。将事件存储在思科云中后，您可以在 CDO 中查看它们。

您可以安装多个安全事件连接器 (SEC)，并将任何设备上的规则生成的事件发送到任何 SEC，就像它是系统日志服务器一样。然后，SEC 将事件转发到思科云。请勿将相同的事件转发到您的所有 SEC。您将复制发送到思科云的事件，并不必要地提高每日采集速率。

## 如何通过安全事件连接器将系统日志和 NSEL 事件从 ASA 发送到思科云

使用基本日志记录和故障排除许可证，ASA 事件通过以下方式到达思科云：

1. 您使用用户名和密码将 ASA 载入 CDO。
2. 将 ASA 配置为将系统日志和 NSEL 事件作为系统日志服务器转发到任何一个 SEC，并在设备上启用日志记录。
3. SEC 将事件转发到存储事件的思科云。
4. CDO 根据您的过滤器在其事件查看器中显示来自思科云的事件。

使用日志记录分析和检测 或 全部网络分析和监控 许可证时，还会发生以下情况：

1. 思科安全云分析将分析应用到存储在思科云中的 ASA 系统日志事件。
2. 生成的观察结果和警报可从与您的 CDO 门户关联的安全云分析门户访问。
3. 在 CDO 门户中，您可以交叉启动 Secure Cloud Analytics 门户，以查看这些观察结果和警报。

## 解决方案中使用的组件

**安全设备连接器 (SDC)** - SDC 会将 CDO 连接到您的 ASA。ASA 的登录凭证被存储在 SDC 上。有关详细信息，请参阅[安全设备连接器](#)。

**安全事件连接器 (SEC)** - SEC 是一种可从 ASA 接收事件并将其转发到思科云的应用。进入思科云后，您可以在 CDO 的“事件日志记录” (Event Logging) 页面上查看事件，或使用“安全云分析”进

行分析。根据您的环境，SEC 安装在安全设备连接器（如果有）上；或在您的网络中维护的 CDO 连接器虚拟机上。有关详细信息，请参阅[安全事件连接器, on page 39](#)。

**自适应安全设备 (asa)** - ASA 在一台设备以及带附加模块的集成服务中提供高级状态防火墙和 VPN 集中器功能。ASA 包括许多高级功能，例如多安全情景（类似于虚拟化防火墙）、集群（将多个防火墙组合成一个防火墙）、透明（第 2 层）防火墙或路由（第 3 层）防火墙操作、高级检测引擎、IPsec VPN、SSL VPN 和无客户端 SSL VPN 支持以及许多其他功能。

安全云分析可将动态实体建模应用于 ASA 事件，并根据此信息生成检测。这提供了对从网络收集的遥测数据的更深入分析，使您能够识别趋势并检查网络流量中的异常行为。如果您拥有[日志记录分析和检测](#)或[全面的网络分析和监控](#)许可证，则可以使用此服务。

## 许可

要配置此解决方案，您需要以下账户和许可证：

- 思科防御协调器。您必须有 CDO 租户。
- 安全设备连接器。安全设备连接器没有单独的许可证。
- 安全事件连接器。安全事件连接器没有单独的许可证。
- 安全日志记录分析 (SaaS)。请参阅 [安全分析和日志记录许可证表格](#)。
- 自适应安全设备 (ASA)。基本许可证或更高版本。

## 安全分析和日志记录许可

要实施安全分析和日志记录 (SaaS)，您需要购买以下许可证之一：

许可证名称	提供的功能	可用许可证持续时间	功能前提条件
日志记录故障排除	<ul style="list-style-type: none"> <li>• 在 CDO 中以实时源和历史视图的形式查看 ASA 事件和事件详细信息</li> </ul>	<ul style="list-style-type: none"> <li>• 1 年</li> <li>• 3 年</li> <li>• 提高</li> </ul>	<ul style="list-style-type: none"> <li>• 首席数据官</li> <li>• 运行软件版本 9.6 或更高版本的本地 ASA 部署。</li> <li>• 部署一个或多个 SEC 以将 ASA 事件传递到思科云。</li> </ul>

许可证名称	提供的功能	可用许可证持续时间	功能前提条件
日志记录分析和检测 (以前称为 防火墙分析和监控)	<p>日志记录和故障排除功能，以及：</p> <ul style="list-style-type: none"> <li>对事件应用动态实体建模和行为分析。</li> <li>根据事件数据在 Secure Cloud Analytics 中打开警报，从 CDO 事件查看器交叉启动。</li> </ul>	<ul style="list-style-type: none"> <li>1 年</li> <li>3 年</li> <li>提高</li> </ul>	<ul style="list-style-type: none"> <li>首席数据官</li> <li>运行 9.6 或更高版本软件的本地 ASA 部署</li> <li>部署一个或多个 SEC 以将 ASA 事件传递到思科云。</li> <li>新调配的或现有的 Cisco Secure Cloud Analytics 门户。</li> </ul>
全面的网络分析和监控	<p>日志记录分析和检测，以及：</p> <ul style="list-style-type: none"> <li>将动态实体建模和行为分析应用于 ASA 事件、本地网络流量和基于云的网络流量</li> <li>基于 ASA 事件数据、思科安全云分析传感器收集的本地网络流量数据以及从 CDO 交叉启动传递到思科安全云分析的基于云的网络流量的组合，在思科安全云分析中打开警报事件查看器。</li> </ul>	<ul style="list-style-type: none"> <li>1 年</li> <li>3 年</li> <li>提高</li> </ul>	<ul style="list-style-type: none"> <li>首席数据官</li> <li>运行 9.6 或更高版本软件的本地 ASA 部署</li> <li>部署一个或多个 SEC 以将事件传递到思科云。</li> <li>部署至少一个 Cisco Secure Cloud Analytics 传感器版本 4.1 或更高版本，以将网络流量数据传递到云，或者将 Cisco Secure Cloud Analytics 与基于云的部署集成，以将网络流量数据传递到 Cisco Secure Cloud Analytics。</li> <li>新调配的或现有的 Cisco Secure Cloud Analytics 门户。</li> </ul>

### 数据计划

您需要购买一个数据计划，以反映思科云每天从注册的 ASA 接收的事件数量。这称为“每日注入速率”。您可以使用[日志记录量估算器](#)工具来估算您的每日注入速率，并且随着该速率的变化，您可以更新数据计划。

数据计划有 1 年、3 年或 5 年期限，每日增量为 1 GB。有关数据计划的信息，请参阅《[安全日志分析 \(SaaS\) 订购指南](#)》。



**Note** 如果您有安全分析和日志记录许可证和数据计划，则在以后获取不同的许可证，这不需要您获取不同的数据计划。如果您的网络流量吞吐量发生变化，并且您获得了不同的数据计划，则不需要您获得不同的安全分析和日志记录许可证。

### 30 天免费试用

您可以通过登录 CDO 并导航到[监控 \(Monitoring\) > 事件日志记录 \(Event Logging\)](#) 选项卡来申请 30 天无风险试用。完成 30 天试用后，您可以按照[安全日志分析 \(SaaS\) 订购指南](#)中的说明，从思科商务工作空间 (CCW) 订购所需的事件数据量，以继续使用服务。

### 下一步

转至为 [ASA 设备实施安全日志记录分析 \(SaaS\)](#)

## 为 ASA 设备实施安全日志记录分析 (SaaS)

### 准备工作

- 查看[关于 ASA 的安全分析和日志记录 \(SAL SaaS\)](#)，以了解：
  - 如何将事件发送到思科云
  - 应用解决方案
  - 您需要的许可证
  - 您需要的数据计划
- 您已联系托管服务提供商或 CDO 销售代表创建 CDO 租户。
- 查看[安全设备连接器](#)。使用 SDC 将 CDO 连接到 ASA 被视为“最佳实践”，但这不是必需的。
- 如果您选择在网络中部署 SDC，可以使用以下方法之一进行安装：
  - 使用[使用 CDO 的 VM 映像部署安全设备连接器](#)，以使用 CDO 准备的 VM 映像安装 SDC。这是部署 SDC 的首选且最简单的方法。
  - 使用[使用您自己的虚拟机映像部署安全设备连接器](#)。

- 您[安装安全事件连接器](#)，并且可以将任何 ASA 中的事件发送到载入到您的租户的任何 SEC。
- 您已为账户的用户[建立双因素身份验证](#)。

实施思科安全分析和日志记录 (SaaS) 以及通过安全事件连接器将事件发送到思科云的工作流程

1. 请务必查看上面的“开始之前”，确保您的环境配置正确。
2. 将 ASA 设备载入 CDO 用户名和密码。
3. 使用命令行接口将 ASA 系统日志事件发送到思科云。
4. 使用 CDO 宏为 ASA 设备配置 NSEL。
5. 确认事件显示在 CDO 中。从导航栏中，选择**监控 (Monitoring)** > **事件日志记录 (Event Logging)**。点击“实时” (Live) 选项卡以查看实时事件。
6. 如果您有防火墙分析和监控或全面网络分析和监控许可证，请继续下一部分使用 **Cisco Secure Cloud Analytics** 分析事件。

#### 使用 Cisco Secure Cloud Analytics 分析事件

如果您有防火墙分析和监控或全面网络分析和监控许可证，除上述步骤外还应执行以下操作：

1. [调配思科安全云分析门户，第 61 页。](#)
2. 如果您购买了全面网络分析和监控许可证，请将一个或多个安全云分析传感器部署到您的内部网络。请参阅[用于全面网络分析和报告的思科安全云分析传感器部署，第 62 页。](#)
3. 邀请用户创建与其思科单点登录凭证相关联的安全云分析用户账户。请参阅[从 CDO 查看 Cisco Secure Cloud Analytics 警报，第 63 页。](#)
4. 从 CDO 到 Secure Cloud Analytics 的交叉启动，以监控 FTD 事件生成的安全云分析警报。请参阅[从 CDO 查看 Cisco Secure Cloud Analytics 警报，第 63 页。](#)

#### 通过从 CDO 交叉启动查看 Cisco Secure Cloud Analytics 警报

使用防火墙分析和监控或全面网络分析和监控许可证，您可以从 CDO 交叉启动安全云分析，以查看 FTD 事件生成的警报。

有关详细信息，请参阅以下文章：

- [登录 CDO](#)
- [从 CDO 查看 Cisco Secure Cloud Analytics 警报，第 63 页](#)
- [思科安全云分析和动态实体建模](#)
- [使用基于防火墙事件的警报](#)

### 安全事件连接器问题故障排除

使用这些故障排除主题收集有关状态和日志记录的信息

- [安全事件连接器载入故障排除](#)
- [事件日志记录故障排除日志文件](#)
- [使用运行状况检查了解安全事件连接器的状态](#)

### 工作流程

[使用安全和分析日志记录事件进行故障排除](#)介绍了如何使用思科安全分析和日志记录生成的事件来确定用户无法访问网络资源的原因。

另请参阅[使用基于防火墙事件的警报](#)。

## 使用 CDO 宏将 ASA 系统日志事件发送到思科云

您可以使用[使用命令行接口将 ASA 系统日志事件发送到思科云](#)中描述的所有命令来创建一个 CDO 宏，并在同一批次的所有 ASA 上运行该宏，从而配置所有 ASA 将事件发送到思科云。

通过 CDO 的宏工具，您可以组合 CLI 命令列表，将命令语法的元素转换为参数，然后保存命令列表，以便可以多次使用。宏也可以一次在多台设备上运行。

使用经过验证的宏可提高设备之间的配置一致性，并防止使用命令行界面时可能发生的语法错误。

在进一步阅读之前，请查看这些主题，以便了解使用宏的机制。本文仅介绍汇编最终宏。

- [用于管理设备的 CLI 宏](#)
- [创建 CLI 宏](#)
- [运行 CLI 宏](#)
- [编辑 CLI 宏](#)
- [删除 CLI 宏](#)

## 创建 ASA 安全分析和日志记录 (SaaS) 宏

您将在以下过程中看到两种类型的格式：ASA CLI 命令和宏格式。编写 ASA CLI 命令遵循 [ASA 语法约定](#)。创建 CLI 宏中介绍了宏约定。 [从新命令创建 CLI 宏](#)

在开始之前，请在单独的窗口中打开 [Send ASA Syslog Events to the Cisco Cloud](#)，并与此程序同时阅读，以便在创建宏时阅读命令说明。[使用命令行接口将 ASA 系统日志事件发送到思科云, on page 15](#)



---

**Note** 如果 ASA 上已存在日志记录配置，则从 CDO 运行宏不会先清除所有现有的日志记录配置。相反，CDO 宏中定义的设置将合并到可能已经存在的任何设置中。

---

**步骤 1** 打开纯文本编辑器，并根据以下说明和选项创建要转换为宏的命令列表。CDO 将按照在宏中写入的顺序执行命令。某些命令会将值转换为 `{{parameters}}`，以便在运行宏时填写。

**步骤 2** 配置 ASA 将消息发送到 SEC，就像它是系统日志 服务器一样。

使用 `logging host` 命令将 SEC 指定为您向其发送消息的系统日志服务器。您可以将事件发送到您已载入到租户的任何一个 SEC。

`logging host` 命令指定要向其发送事件的 TCP 或 UDP 端口。要确定应该使用哪个端口，请参阅[查找用于安全日志记录分析 \(SaaS\) 的设备 TCP、UDP 和 NSEL 端口](#)。

```
interface_name SEC_IP_address logging host {tcp/port | udp/port}
```

根据您的用于向 SEC 发送系统日志事件的协议，将此命令转换为两个不同的宏之一：

```
logging host {{interface_name}} {{SEC_ip_address}} tcp/{{port_number}}
```

```
logging host {{interface_name}} {{SEC_ip_address}} udp/{{port_number}}
```

（可选）如果使用 TCP，可以将此命令添加到宏命令列表中。它不需要任何参数。

#### logging permit-hostdown

**步骤 3** 指定应将哪些系统日志消息发送到系统日志服务器。

使用 `logging trap` 命令指定应将哪些系统日志消息发送到系统日志服务器：

```
logging trap {severity_level | message_list}
```

如果要按严重性级别定义发送到 SEC 的事件，请将命令转换为以下宏：

```
logging trap {{severity_level}}
```

如果您只想将属于邮件列表的事件发送到 SEC，请将命令转换为以下宏：

```
日志记录陷阱 {{message_list_name}}
```

如果在上一步中选择了 `logging trap message_list` 命令，则需要在消息列表中定义系统日志。打开创建自定义事件列表，以便在创建宏时阅读命令说明。[创建自定义事件列表, on page 18](#)使用以下命令启动：

```
logging listname {level[level [classmessage_class] | messagestart_id [-end_id]}
```

并将其分解为以下变体：

```
日志记录列表 {{message_list_name}} 级别 {{security_level}}
```

```
logging list {{message_list_name}} level {{security_level}} class {{message_class}}
```

```
日志记录列表 {{message_list_name}} 消息 {{syslog_range_or_number}}
```

在最后一个变体中，消息参数 `{{syslog_range_or_number}}` 可以输入为单个系统日志 ID 106023 或范围 302013-302018。在任意数量的行中使用一个或多个命令变体来创建邮件列表。请记住，在单个宏中，具有相同名称的所有参数都将使用您输入的相同值。CDO 不会运行参数为空的宏。

**Important** 在宏中，`logging list` 命令必须位于 `logging trap` 命令之前。首先定义列表，然后 `logging trap` 命令可以使用它。请参阅下面的[示例宏](#)。

**步骤 4** (可选) 添加系统日志时间戳。如果要向 ASA 上发出系统日志消息的消息添加日期和时间, 请添加此命令。时间戳值显示在系统日志时间戳 (SyslogTimestamp) 字段中。将此命令添加到命令列表中, 它将不需要任何参数:

#### logging timestamp

**Note** 从版本 9.10(1) 开始, ASA 提供了在事件系统日志中根据 RFC 5424 启用时间戳的选项。当启用此选项时, 系统日志消息的所有时间戳将按照 RFC 5424 格式显示时间。以下是 RFC 5424 格式的输出示例:

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from
src interface :src IP/src port to dest IP/dest port
```

。

**步骤 5** (可选) 在非 **EMBLEM** 格式的系统日志消息中包括设备 ID。打开 Include the Device ID in Non-EMBLEM Format Syslog Messages, 以便您可以在创建宏时阅读命令说明。在非 **EMBLEM** 格式系统日志消息中包含设备 ID, on [page 20](#)这是您的宏所基于的 CLI 命令:

**logging device-id** { **cluster-id** | **context-name** | **hostname** | **ipaddress** *interface\_name* [**system**] | **stringtext**}

并将其分解为以下变体:

**logging device-id cluster-id**

**logging device-id context-name**

**logging device-id hostname**

logging device-id ipaddress {{interface\_name}} system

logging device-id string {{text\_16\_char\_or\_less}}

**步骤 6** 启用日志记录。将此命令按原样添加到宏。它没有任何参数:

**logging enable**

**步骤 7** 不要将写入内存添加到宏的最后一行。请改为添加 **show running-config logging** 命令, 以查看您输入的日志记录命令的结果, 然后再将其提交到 ASA 的启动配置。

**show running-config logging**

**步骤 8** 在确定已进行配置更改后, 您可以为 **write memory** 命令创建单独的宏, 或使用 CDO 的批量命令行接口功能向使用宏配置的所有设备发出该命令。[批量 CLI 接口](#)

**write memory**

**步骤 9** (可选) 对访问控制规则“允许”事件启用日志记录。将 ASA 系统日志事件发送到思科云程序中所述的此步骤, 但未包含在此宏中。[使用命令行接口将 ASA 系统日志事件发送到思科云, on page 15](#)它在 CDO GUI 中执行。

**步骤 10** 保存宏。

### Example

以下是组合成单个宏的命令列表示例:

```
logging host {{interface_name}} {{SEC_ip_address}} {{tcp_or_udp}}/{{port_number}}
```

```
logging permit-hostdown
logging list {{message_list_name}} level {{security_level}}
logging list {{message_list_name}} message {{syslog_range_or_number_1}}
logging list {{message_list_name}} message {{syslog_range_or_number_2}}
logging trap {{message_list_name}}
logging device-id cluster-id
logging enable
show running-config logging
```



**Note** 有多个 logging list 命令可用于添加不同的特定系统日志 ID 或范围。  
{{syslog\_range\_or\_number\_X}} 参数需要数字或其他一些区分符，否则在填写宏时，它们的值将全部相同。另请记住，如果不是所有参数都指定了值，CDO 将不会运行宏，因此仅包含要执行的宏中的命令。我们希望所有系统日志 ID 都包含在同一个列表中，以便每行中的 event\_list\_name 保持不变。

### What to do next

#### 运行宏

创建并保存 ASA 安全分析和日志记录宏后，运行宏将 ASA 系统日志事件发送到思科云。

## 使用命令行接口将 ASA 系统日志事件发送到思科云

此程序介绍如何将 ASA 系统日志事件转发到安全事件连接器 (SEC)，然后启用日志记录。这些程序仅说明了完成该工作流程所需执行的操作。有关在 ASA 上配置日志记录的所有方式的更广泛讨论，请参阅《[ASDM1: 思科 ASA 系列常规操作 ASDM 配置指南](#)》或《[CLI 手册 1: 思科 ASA 系列常规操作 CLI 配置指南](#)》中的“监控”一章。

### 支持的 ASA 命令的限制

CDO 尚未支持以下系统日志命令或消息格式：

- 系统日志的 EMBLEM 格式
- 保护系统日志

## ASA 的 CDO 命令行界面

对于此程序中的所有任务，您将使用 ASA 的 CDO 的命令行界面。要打开命令行界面页面，请执行以下操作：

**步骤 1** 在导航栏中，点击清单 (Inventory)。

**步骤 2** 点击设备选项卡。

**步骤 3** 点击相应的设备类型选项卡，然后选择要为其启用日志记录的 ASA。

**步骤 4** 在右侧“设备操作”(Device Actions)窗格中, 点击**命令行接口 (Command Line Interface)**。

**步骤 5** 点击 **命令行接口 (Command Line Interface)**。现在, 您可以在提示符后输入如下所述的命令。

输入每个命令后, 您将点击“发送”。由于 CDO 的 CLI 接口是与 ASA 的直接连接, 因此该命令会立即写入设备的运行配置。要将更改写入 ASA 的启动配置, 还需要发出 `write memory` 命令。

## 将 ASA 系统日志事件转发到安全事件连接器

要将 ASA 系统日志事件转发到您已自行激活的安全事件连接器 (SEC) 之一, 然后启用日志记录, 您需要在以下程序中完成这些任务。

**步骤 1** 配置 ASA 以便将消息发送到 SEC, 就像它是系统日志服务器一样。

**步骤 2** 决定要发送到 SEC 的所有日志的严重性级别或系统日志事件列表。

**步骤 3** 启用日志记录。

**步骤 4** 保存对 ASA 的启动配置所做的更改。

## 使用 CLI 将 ASA 系统日志事件发送到思科云

**步骤 1** 配置 ASA 以便将消息发送到 SEC, 就像它是系统日志服务器一样

将系统日志事件从 ASA 发送到思科云时, 您可以将其作为外部系统日志服务器转发到 SEC, 然后 SEC 会将消息转发到思科云。

要将系统日志消息发送到 SEC, 请执行以下步骤:

- a. 将 ASA 配置为使用 TCP 或 UDP 将消息发送到 SEC, 就像它是系统日志服务器一样。SEC 可以使用 IPv4 或 IPv6 地址。您将向 TCP 或 UDP 端口发送事件。要确定应该使用哪个端口, 请参阅[查找用于安全日志记录分析 \(SaaS\) 的设备 TCP、UDP 和 NSEL 端口](#)。

以下是 `logging host` 命令语法的示例:

```
logging host interface_name SEC_IP_address [[ tcp/port ]] [[ udp/port ]]
```

示例:

```
> logging host mgmt 192.168.1.5 tcp/10125
> logging host mgmt 192.168.1.5 udp/10025
> logging host mgmt 2002::1:1 tcp/10125
> logging host mgmt 2002::1:1 udp/10025
```

- **interface\_name** 参数指定将消息发送到系统日志服务器的 ASA 接口。“最佳实践”是通过已用于与 SDC 通信的同一 ASA 接口将系统日志消息发送到 SDC。
- **SEC\_IP\_address** 参数应包含安装了 SEC 的虚拟机的 IP 地址。

- **tcp/port** 或 **udp/port** 关键字-参数对指定应使用 TCP 协议和相关端口或 UDP 协议和相关端口发送系统日志消息。可以将 ASA 配置为使用 UDP 或 TCP（但不同时使用两者）将数据发送到系统日志服务器。如果未指定协议，则默认协议为 UDP。

如果指定 TCP，则在系统日志服务器发生故障时 ASA 会发现此情况，作为安全防护措施，将会阻止通过 ASA 的新连接。要允许新连接而不考虑与 TCP 系统日志服务器的连接，请参阅步骤 b。如果指定 UDP，则无论系统日志服务器是否正常运行，ASA 都将继续允许新连接。有效的端口值

**Note** 如果要向 ASA 消息发送到两个单独的系统日志服务器，可以使用另一个系统日志服务器的相应接口、IP 地址、协议和端口运行第二个 logging host 命令。

- b. （可选）如果通过 TCP 向 SEC 发送事件，并且 SEC 已关闭或 ASA 上的日志队列已满，则会阻止新连接。备份系统日志服务器，且日志队列不再已满后，将再次允许新连接。要允许新连接而不考虑与 TCP 系统日志服务器的连接，请使用以下命令禁用该功能以在连接 TCP 的系统日志服务器关闭时阻止新连接：

#### logging permit-hostdown

示例：

```
> logging permit-hostdown
```

### 步骤 2 通过以下命令指定应将哪些系统日志消息发送到系统日志服务器：

**logging trap { severity\_level | message\_list }**

示例：

```
> logging trap 3
> logging trap asa_syslogs_to_cloud
```

可以指定严重性级别号（1 至 7）或名称。例如，如果将严重性级别设置为 3，则 ASA 会发送严重性级别为 3、2 和 1 的系统日志消息。

message\_list 参数将替换为自定义事件列表的名称（如果已创建）。指定自定义事件列表时，仅将该列表中的系统日志消息发送到安全事件连接器。在上面的示例中，asa\_syslogs\_to\_cloud 是事件列表的名称。

使用 message\_list 可以通过严格定义将哪些系统日志消息发送到思科云来节省资金。

请参阅[创建自定义事件列表](#)以创建 message\_list。有关数据注入和存储成本的详细信息，请参阅[数据存储计划](#)。

### 步骤 3 （可选）添加系统日志时间戳

使用 logging timestamp 命令将在 ASA 上发出的系统日志消息的日期和时间添加到消息中。时间戳值显示在系统日志时间戳 (SyslogTimestamp) 字段中。

示例：

```
> logging timestamp
```

**Note** 从版本 9.10(1) 开始，ASA 提供了在事件系统日志中根据 RFC 5424 启用时间戳的选项。当启用此选项时，系统日志消息的所有时间戳将按照 RFC 5424 格式显示时间。以下是 RFC 5424 格式的输出示例：

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from src interface :src IP/src port to dest IP/dest port.
```

### 步骤 4 （可选）在非 EMBLEM 格式的系统日志消息中包括设备 ID

设备 ID 是可插入到系统日志消息中的标识符，可帮助您轻松区分从特定 ASA 发送的所有系统日志消息。有关说明，请参阅[在非 EMBLEM 格式系统日志消息中包含设备 ID](#)。

#### 步骤 5（可选）对访问控制规则“允许”事件启用日志记录

当访问控制规则拒绝访问资源时，系统会自动记录该事件。如果您还想记录访问控制规则允许访问资源时生成的事件，则需要打开访问控制规则的日志记录并配置严重性类型。有关如何为单个网络访问控制规则打开日志记录的说明，请参阅[日志规则练习](#)。

**Note** 启用访问控制规则“允许”事件的日志记录将使用您购买的更多数据计划，因为它基于您的每日事件采集速率。

#### 步骤 6 启用日志记录

在命令提示符下，键入 `logging enable`。在 ASA 上，为整个设备启用日志记录，而不是为单个规则启用日志记录。

示例：

```
> logging enable
```

**Note** 目前，CDO 不支持启用安全日志记录。

#### 步骤 7 保存对启动配置所做的更改

在命令提示符下，键入 `write memory`。在 ASA 上，为整个设备启用日志记录，而不是为单个规则启用日志记录。

示例：

```
> write memory
```

---

#### 相关信息：

- [在 SDC 虚拟机上安装安全事件连接器, on page 40](#)
- [使用 CDO 映像安装 SEC](#)

## 创建自定义事件列表

使用以下方法之一将 ASA 系统日志事件发送到思科云时，创建自定义事件列表：

- [使用命令行接口将 ASA 系统日志事件发送到思科云](#)
- [使用 CDO 宏将 ASA 系统日志事件发送到思科云](#)

您可以根据以下三个条件创建事件列表（也称为 `message_list`）：

- 事件类
- 严重性
- 消息 ID

要创建将发送到特定日志记录目标（例如，系统日志服务器或安全事件连接器）的自定义事件列表，请执行以下步骤：

**步骤 1** 在清单 (**Inventory**) 页面中，点击设备 (**Devices**) 选项卡。

**步骤 2** 点击相应的选项卡，然后选择要将其系统日志消息包含在自定义事件列表中的 ASA。

**步骤 3** 在设备操作 (**Device Actions**) 窗格中，点击 >\_命令行接口 (>\_ **Command Line Interface**)。

**步骤 4** 使用此命令语法向 ASA 发出 **logging list** 命令：

```
logging list name { level level [ class message_class ] | message start_id [ -end_id ] }
```

*name* 参数指定列表的名称。**level level** 关键字/参数对指定严重性级别。**class message\_class** 关键字/参数对指定特定消息类。**message start\_id [-end\_id]** 关键字-参数对指定单个系统日志消息编号或编号范围。

**Note** 请勿使用严重性级别的名称作为系统日志消息列表的名称。禁止的名称包括 **emergencies**、**alert**、**critical**、**error**、**warning**、**notification**、**informational** 和 **debugging**。同样，请勿在事件列表名称的开头使用这些单词的前三个字符。例如，请勿使用以字符 “err” 开头的事件列表名称。

- 根据严重性将系统日志消息添加到事件列表。例如，如果将严重性级别设置为 3，则 ASA 会发送严重性级别为 3、2 和 1 的系统日志消息。

示例：

```
> logging list asa_syslogs_to_cloud level 3
```

- 根据其他条件将系统日志消息添加到事件列表：

输入与上一步中相同的命令，指定现有消息列表的名称和其他条件。为要添加到列表的每个条件输入新命令。例如，可以在列表中包含系统日志消息的条件指定如下：

- 日志消息 ID 属于范围 302013 至 302018。
- 所有系统日志消息都具有 **critical** 或更高的严重性级别（**emergency**、**alert** 或 **critical**）。
- 所有 HA 类系统日志消息都具有 **warning** 或更高的严重性级别（**emergency**、**alert**、**critical**、**error** 或 **warning**）。

示例：

```
> logging list asa_syslogs_to_cloud message 302013-302018
> logging list asa_syslogs_to_cloud level critical
> logging list asa_syslogs_to_cloud level warning class ha
```

**Note** 如果系统日志消息满足以下任何条件，则会将其记录。如果系统日志消息满足其中多个条件，则该消息仅记录一次。

**步骤 5** 保存对启动配置所做的更改

在命令提示符下，键入 **write memory**。

示例：

```
> write memory
```

## 在非 EMBLEM 格式系统日志消息中包含设备 ID

您可以将 ASA 配置为在非 EMBLEM 格式系统日志中包含设备 ID。只能为系统日志指定一种类型的设备 ID。以下程序引用此程序：

- 使用命令行接口将 ASA 系统日志事件发送到思科云
- 使用 CDO 宏将 ASA 系统日志事件发送到思科云

此设备标识符将反映在“事件日志记录” (Event Logging) 页面上显示的系统日志事件的“传感器 ID” (SensorID) 字段中。

**步骤 1** 选择要为其系统日志信息分配设备 ID 的 ASA。

**步骤 2** 在“设备操作” (Device Actions) 窗格中，点击>\_命令行接口 (>\_Command Line Interface)。

**步骤 3** 使用此命令语法向设备发出 logging device-id 命令。

```
logging device-id { cluster-id | context-name | hostname | ipaddress interface_name [system] | stringtext }
```

示例：

```
> logging device-id hostname
> logging device-id context-name
> logging device-id string Cambridge
```

**context-name** 关键字指示应用作设备 ID 的当前情景的名称（仅适用于多情景模式）。如果在多情景模式下为管理情景启用日志记录设备 ID，则源于系统执行空间中的消息使用设备 ID **system**，源于管理情景中的消息使用管理情景的名称作为设备 ID。

**Note** 在 ASA 集群中，始终使用所选接口的主设备 IP 地址。

**cluster-id** 关键字指定集群中单个 ASA 设备的启动配置中的唯一名称作为设备 ID。

**hostname** 关键字指定应用作设备 ID 的 ASA 的主机名。

**ipaddress interface\_name** 关键字/参数对指定应将指定为 *interface\_name* 的接口 IP 地址用作设备 ID。如果使用 **ipaddress** 关键字，则无论从哪个接口发送系统日志消息，设备 ID 都会成为指定的 ASA 接口 IP 地址。在集群环境中，**system** 关键字指示设备 ID 成为接口上的系统 IP 地址。此关键字为从设备发送的所有系统日志消息提供单个一致的设备 ID。

**string text** 关键字/参数对指定应将 *text* 字符串用作设备 ID。字符串可以包含多达 16 个字符。

不能使用空格或以下任何字符：

- &（与号）
- ‘（单引号）
- "（双引号）

- < (小于)
- > (大于)
- ? (问号)

#### 步骤 4 保存对启动配置所做的更改

在命令提示符下，键入 `write memory`。

示例：

```
> write memory
```

## ASA 设备的 NetFlow 安全事件日志记录 (NSEL)

来自 ASA 的基本系统日志消息缺少安全云分析用于确定 ASA 报告的事件是否表明存在威胁所需的许多数据。Netflow 安全事件日志记录 (NSEL) 为安全云分析提供该数据。

“流定义为通过网络设备传递的具有一些常见属性的单向数据包序列。这些收集的流将导出到外部设备，即 NetFlow 收集器。网络流具有高度的粒度；例如，流记录包括 IP 地址、数据包和字节计数、时间戳、服务类型 (ToS)、应用端口、输入和输出接口等详细信息。”<sup>1</sup>

Cisco ASA 支持 NetFlow 版本 9 服务。NSEL 的 ASA 和实施提供 IP 状态流跟踪方法，该方法仅导出那些表示流中重大事件的记录。在状态流跟踪中，跟踪的流将经历一系列状态更改。

本文档介绍使用 CDO 宏为您的 ASA 配置 NetFlow 的直接方法。《思科 ASA NetFlow 实施指南》提供了有关在 ASA 上配置 NetFlow 的极其详细的讨论，您可能会发现它是与此内容配套的宝贵资源。

#### 后续操作

转至[使用 CDO 宏为 ASA 设备配置 NSEL](#)。

#### 相关文章

- [使用 CDO 宏为 ASA 设备配置 NSEL](#)
- [从 ASA 删除 NetFlow 安全事件日志记录 \(NSEL\) 配置](#)
- [确定 ASA 全局策略的名称](#)

1. ("Cisco Systems NetFlow 服务导出版本 9." 互联网工程任务组，网络工作组，征求意见：3954，2004 年 10 月，B. Claise，Ed.<https://www.ietf.org/rfc/rfc3954.txt>)

## 使用 CDO 宏为 ASA 设备配置 NSEL

ASA 使用 Netflow 安全事件日志记录 (NSEL) 报告详细的连接事件数据。您可以将 Cisco Secure Cloud Analytics 应用于此连接事件数据，其中包括双向流统计信息。此程序介绍如何在 ASA 设备上配置 NSEL 并将这些 NSEL 事件发送到流收集器。在这种情况下，流收集器是安全事件连接器 (SEC)。

此过程引用此宏，配置 NSEL：

```

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate {{timeout_rate_in_mins}}
flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
flow-export active refresh-interval {{refresh_interval_in_mins}}
class-map {{flow_export_class_name}}
    match {{add_this_traffic_to_class_map}}
policy-map {{global_policy_map_name}}
    class {{flow_export_class_name}}
        flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
service-policy {{global_policy_map_name}} global
logging flow-export-syslogs disable
show run flow-export
show run policy-map {{global_policy_map_name}}
show run class-map {{flow_export_class_name}}

```

以下是 ConfigureNSEL 宏的示例，其中填写了所有默认值、类映射的通用名称以及添加到 global\_policy 的类映射。完成这些过程后，您的宏将如下所示：

```

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate 60
flow-export delay flow-create 55
flow-export active refresh-interval 1
class-map flow_export_class_map
    match any
policy-map global_policy
    class flow_export_class_map
        flow-export event-type all destination {{SEC_IPv4_address}}
logging flow-export-syslogs disable
show run flow-export
show run policy-map global_policy
show run class-map flow_export_class_map

```

## 准备工作

收集以下信息：

- 如果您以前从未使用过 CDO 宏，请阅读以下主题：
  - [命令行界面宏](#)
  - [编辑 CLI 宏](#)
  - [运行 CLI 宏](#)
- 从 ASA 接收数据的 SEC 的 IPv4 地址
- ASA 上用于将数据发送到 SEC 的接口
- 用于转发 NetFlow 事件的 UDP 端口号请参阅[查找用于安全日志记录分析 \(SaaS\) 的设备 TCP、UDP 和 NSEL 端口, on page 121](#)。
- [确定 ASA 全局策略的名称, on page 28](#)

## 工作流程

按照此工作流程使用 CDO 宏为 ASA 设备配置 NSEL。您需要执行以下每个步骤：

1. 打开配置 NSEL 宏, on page 23。
2. 定义 NSEL 消息的目的地及其发送到 SEC 的间隔, on page 23。
3. 创建定义将发送到 SEC 的 NSEL 事件的类映射, on page 24。
4. 为 NSEL 事件定义策略映射, on page 25。
5. 禁用冗余系统日志消息, on page 26。
6. 查看并发送宏, on page 27。

#### 后续操作

通过转至 [打开配置 NSEL 宏, on page 23](#) 开始上述工作流程。

## 打开配置 NSEL 宏

### Before you begin

这是较长工作流程的第一部分, 在开始之前请参阅 [使用 CDO 宏为 ASA 设备配置 NSEL, on page 21](#)。

**步骤 1** 在清单 (Inventory) 页面中, 点击设备 (Devices) 选项卡。

**步骤 2** 点击相应的设备类型选项卡, 然后选择要配置 NetFlow 安全事件日志记录 (NSEL) 的 ASA。

**步骤 3** 在设备操作 (Device Actions) 窗格中, 点击命令行接口 (Command Line Interface)。

**步骤 4** 点击宏星标  **Macros** 以显示可用宏的列表。

**步骤 5** 从宏列表中, 选择配置 NSEL (Configuring NSEL)。

**步骤 6** 在“宏” (Macro) 框下, 点击查看参数 (View Parameters)。

### What to do next

请继续 [定义 NSEL 消息的目的地及其发送到 SEC 的间隔, on page 23](#)。

## 定义 NSEL 消息的目的地及其发送到 SEC 的间隔

NSEL 消息可以发送到您已载入到租户的任何一个 SEC。这些说明引用了宏的这一部分:

```
flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
```

```
flow-export template timeout-rate {{timeout_rate_in_mins}}
```

```
flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
```

```
flow-export active refresh-interval {{refresh_interval_in_mins}}
```

### Before you begin

这是更大工作流程的一部分。在开始之前, 请参阅 [使用 CDO 宏为 ASA 设备配置 NSEL, on page 21](#)。

---

**步骤 1 flow-export destination** 命令定义将 NetFlow 数据包发送到的收集器。在这种情况下，您会将它们发送到 SEC。填写以下参数的字段：

- **{{interface}}** - 输入发送 NetFlow 事件的 ASA 上的接口的名称。
- **{{SEC\_IPv4\_address}}** - 输入 SEC 的 IPv4 地址。SEC 用作流收集器。
- **{{SEC\_NetFlow\_port}}** - 输入 SEC 上向其发送 NetFlow 数据包的 UDP 端口号。

**步骤 2 flow-export template timeout-rate** 指定将模板记录发送到所有已配置的输出目标的时间间隔。

- **{{timeout\_rate\_in\_mins}}** - 输入重新发送模板之前的分钟数。我们建议使用 **60 分钟** 的值。SEC 不处理模板。较大的数字会减少到 SEC 的流量。

**步骤 3 flow-export delay flow-create** 命令将流创建事件的发送延迟指定的秒数。此值与建议的活动超时值匹配，并减少从 ASA 导出的流事件数。在该速率下，NSEL 事件将在连接关闭时或在创建连接后的 55 秒内首次出现在 CDO 中，以较早者为准。如果未配置此命令，则不会延迟，并会在创建流后立即导出流创建事件。

- **{{delay\_flow\_create\_rate\_in\_secs}}** - 输入发送流创建事件之间的延迟秒数。我们建议使用 **55 秒** 的值。

**步骤 4 flow-export active refresh-interval** 命令定义从 ASA 发送长生存期流状态更新的频率。有效值为 1 到 60 分钟。在“流更新间隔” (Flow Update Interval) 字段中，将 **flow-export active refresh-interval** 配置为至少比 **flow-export delay flow-create** 间隔多 5 秒可防止流更新事件出现在流创建事件之前。

- **{{refresh\_interval\_in\_mins}}** - 我们建议使用 **1 分钟** 的值。有效值为 1 到 60 分钟。

---

### What to do next

请继续[创建定义将发送到 SEC 的 NSEL 事件的类映射](#), on page 24。

## 创建定义将发送到 SEC 的 NSEL 事件的类映射

宏中的以下命令将所有 NSEL 事件分组到一个类中，然后将该类导出到安全事件连接器 (SEC)。这些说明引用了宏的这一部分：

```
class {{flow_export_class_name}}  
匹配 {{add_this_traffic_to_class_map}}
```

### Before you begin

这是更大工作流程的一部分。在开始之前，请参阅[使用 CDO 宏为 ASA 设备配置 NSEL](#), on page 21。

---

**步骤 1 class-map** 命令命名用于标识将导出到 SEC 的 NSEL 流量的类映射。

- **{{flow-export-class-name}}**-输入类映射的名称。其中，名称最多可包含 40 个字符。名称“class-default”和任何以“\_internal”或“\_default”开头的名称均已保留。所有类型的类映射都使用同一命名空间，因此无法重复使用已被另一类型的类映射使用的名称。

**步骤 2** 标识将与您的类映射关联（匹配）的流量。为 **{{add\_this\_traffic\_to\_class\_map}}** 的值选择以下选项之一：

- 在 **{{add\_this\_traffic\_to\_class\_map}}** 字段中输入 **any**。这将监控 NSEL 流量的所有流量类型。我们建议使用值“any”。
- 在 **{{add\_this\_traffic\_to\_class\_map}}** 字段中输入 **access-list name-of-access-list**。这会将所有与您创建的访问列表关联的流量相关联。有关详细信息，请参阅《思科 ASA NetFlow 实施指南》中的[通过模块化策略框架配置流导出操作](#)。

---

### What to do next

请继续为 [NSEL 事件定义策略映射, on page 25](#)。

## 为 NSEL 事件定义策略映射

该任务会将 NetFlow 导出操作分配给您在上一个任务中创建的类，然后将该类分配给新的策略映射。这些说明引用了宏的这一部分：

```
policy-map {{global_policy_map_name}}
class {{flow_export_class_name}}
flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
```

### Before you begin

这是更大工作流程的一部分。在开始之前，请参阅[使用 CDO 宏为 ASA 设备配置 NSEL, on page 21](#)。

---

**步骤 1** **policy-map** 命令可创建策略映射。在下一个任务中，您可以将此策略映射与全局策略关联。

- **{{global\_policy\_map\_name}}** - 输入策略映射的名称。我们建议使用防火墙现有全局策略的名称（如有）。全局策略的默认名称为 **global\_policy**。请参阅[确定 ASA 全局策略的名称](#)。如果您根据《思科 ASA NetFlow 实施指南》中的[通过模块化策略框架配置流导出操作](#)来创建新的策略映射并全局应用，则其余检测策略将被停用。

**步骤 2** **class** 命令会继承您在 [创建定义将发送到 SEC 的 NSEL 事件的类映射, on page 24](#) 中创建的类映射的名称。

**步骤 3** **flow-export event-type {{event-type}} destination {{IPv4\_address}}** 命令可定义应将哪些事件类型发送到流收集器（在本例中为 SEC）。

- **{{event-type}}** - **event\_type** 关键字是过滤的受支持事件的名称。我们建议使用值“all”。
- **{{SEC\_IPv4\_address}}** - 这是 SEC 的 IPv4 地址。其值继承自您在 [定义 NSEL 消息的目的地及其发送到 SEC 的间隔, on page 23](#) 中输入的值。

**What to do next**

请继续[禁用冗余系统日志消息](#), on page 26。

**禁用冗余系统日志消息**

这些说明引用了宏的这一部分。您不需要修改命令。

```
logging flow-export-syslogs disable
```

启用 NetFlow 以导出流信息会使列出在下列表格中的系统日志消息冗余。出于性能考虑，建议您禁用冗余系统日志消息，因为相同的信息会通过 NetFlow 导出。



**Note** 当 NSEL 和系统日志消息均已启用时，不能保证两种日志记录类型之间的时间排序。

系统日志消息	说明	NSEL 事件 ID	NSEL 扩展事件 ID
106100	每当遇到访问控制规则 (ACL) 时生成。	1—已创建流（如果 ACL 允许流）。 3—流被拒绝（如果 ACL 拒绝流）。	0—如果 ACL 允许流。 1001—流被入口 ACL 拒绝。 1002—流被出口 ACL 拒绝。
106015	TCP 流被拒绝，因为第一个数据包不是 SYN 数据包。	3—流被拒绝。	1004—TCP 流被拒绝，因为第一个数据包不是 SYN 数据包。
106023	当通过访问组命令连接到接口的 ACL 拒绝流时。	3—流被拒绝。	1001—流被入口 ACL 拒绝。 1002—流被出口 ACL 拒绝。
302013、302015、 302017、302020	TCP、UDP、GRE 和 ICMP 连接创建。	1—已创建流。	0—忽略。
302014、302016、 302018、302021	TCP、UDP、GRE 和 ICMP 连接断开。	2—已删除流。	0—忽略。 > 2000—流已断开。
313001	发送到设备的 ICMP 数据包被拒绝。	3—流被拒绝。	1003—由于配置，已拒绝传入流。
313008	发送到设备的 ICMP v6 数据包被拒绝。	3—流被拒绝。	1003—由于配置，已拒绝传入流。
710003	尝试连接到设备接口被拒绝。	3—流被拒绝。	1003—由于配置，已拒绝传入流。

如果您不想禁用冗余系统日志消息，可以编辑此宏并仅从中删除此行：

**logging flow-export-syslogs disable**

您可以稍后按照[禁用和重新启用 NetFlow 相关系统日志消息](#)中的程序启用或禁用各个系统日志消息。

## 查看并发送宏

### Before you begin

这是更大工作流程的一部分。在开始之前，请参阅[使用 CDO 宏为 ASA 设备配置 NSEL, on page 21](#)。

**步骤 1** 填写宏的字段后，点击 **查看 (Review)** 以查看命令，然后再将其发送到 ASA。

**步骤 2** 如果您对命令的响应感到满意，请点击**发送 (Send)**。

**步骤 3** 在发送命令后，您可能会看到消息“某些命令可能对运行配置进行了更改” (Some commands may have made changes to the running config) 以及两个链接。

Some commands may have made changes to the running config [Write to Disk](#) [Dismiss](#)

- 点击**写入磁盘 (Write to Disk)** 会将此命令所做的更改以及运行配置中的任何其他更改保存到设备的启动配置中。
- 点击**消除 (Dismiss)** 关闭消息。

您已完成[使用 CDO 宏为 ASA 设备配置 NSEL, on page 21](#)中所述的工作流程。

## 从 ASA 删除 NetFlow 安全事件日志记录 (NSEL) 配置

此程序介绍如何删除 ASA 上的 NetFlow 安全事件日志记录 (NSEL) 配置，该配置将安全事件连接器 (SEC) 指定为 NSEL 流收集器。此程序与[使用 CDO 宏为 ASA 设备配置 NSEL](#)中所述的宏相反。

此过程引用此宏 **DELETE NSEL**：

```
policy-map {{flow_export_policy_name}}
no class {{flow_export_class_name}}
no class-map {{flow_export_class_name}}
no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}
no flow-export template timeout-rate {{timeout_rate_in_mins}}
no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
no flow-export active refresh-interval {{refresh_interval_in_mins}}
logging flow-export-syslogs enable
show run flow-export
show run policy-map {{flow_export_policy_name}}
show run class-map {{flow_export_class_name}}
```

### 打开 DELETE-NSEL 宏

**步骤 1** 在清单 (**Inventory**) 页面中，点击**设备 (Devices)** 选项卡。

**步骤 2** 点击相应的设备类型选项卡，然后选择要删除 NetFlow 安全事件日志记录 (NSEL) 配置的 ASA。

在宏中输入值以完成无命令

**步骤 3** 在设备操作 (**Device Actions**) 窗格中, 点击命令行接口 (**Command Line Interface**)。

**步骤 4** 点击宏星标  **Macros** 以显示可用宏的列表。

**步骤 5** 在宏列表中, 选择 **DELETE-NSEL**。

**步骤 6** 在“宏” (Macro) 框下, 点击**查看参数 (View Parameters)**。

## 在宏中输入值以完成无命令

ASA CLI 使用命令的“no”形式将其删除。填写宏中的字段以填写命令的“no”形式:

**步骤 1** `policy-map {{flow_export_policy_name}}`

- `{{flow_export_policy_name}}` - 输入策略映射名称的值。

**步骤 2** `no class {{flow_export_class_name}}`

- `{{flow_export_class_name}}` - 输入类映射名称的值。

**步骤 3** `no class-map {{flow_export_class_name}}`

- `{{flow_export_class_name}}` - 类映射名称的值继承自上述步骤。

**步骤 4** `no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}`

- `{{interface}}` - 输入发送 NetFlow 事件的 ASA 上的接口的名称。
- `{{IPv4_address}}`-输入 SEC 的 IPv4 地址。SEC 用作流收集器。
- `{{NetFlow_port}}`-输入 SEC 上向其发送 NetFlow 数据包的 UDP 端口号。

**步骤 5** `no flow-export template timeout-rate {{timeout_rate_in_mins}}`

- `{{timeout_rate_in_mins}}`-输入流导出模板超时速率。

**步骤 6** `no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}`

- `{{delay_flow_create_rate_in_secs}}`-输入流导出延迟流创建速率。

**步骤 7** `no flow-export active refresh-interval {{refresh_interval_in_mins}}`

- `{{refresh_interval_in_mins}}`-输入流导出活动刷新间隔。

## 确定 ASA 全局策略的名称

要确定 ASA 的全局策略的名称, 请遵循以下程序:

**步骤 1** 在 **清单 (Inventory)** 页面中，选择要为其查找全局策略名称的设备。

**步骤 2** 在“设备操作” (Device Actions) 窗格中，选择 **>\_Command Reference**。

**步骤 3** 在命令行界面窗口中，在提示符后键入：

```
show running-config service-policy
```

在下面的示例输出中，`global_policy` 是全局策略的名称。

示例：

```
> show running-config service-policy
```

```
service-policy global_policy global
```

## NSEL 数据流故障排除

使用 **CDO 宏为 ASA 设备配置 NSEL** 后，请使用以下程序验证 NSEL 事件是否从 ASA 发送到思科云以及思科云是否正在接收这些事件。

请注意，一旦 ASA 被配置为将 NSEL 事件发送到安全事件连接器 (SEC)，然后再发送到思科云，数据不会立即流动。假设 ASA 上生成了与 NSEL 相关的流量，第一个 NSEL 数据包可能需要几分钟才能到达。



**Note** 此工作流程向您展示如何直接使用“`flow-export counters`”命令和“`capture`”命令对 NSEL 数据流进行故障排除。有关这些命令用法的更详细讨论，请参阅《[CLI 手册 1: 思科 ASA 系列常规操作 CLI 配置指南](#)》中的“数据包捕获”和《[思科 ASA NetFlow 实施指南](#)》中的“监控 NSEL”。

执行这些任务：

- 验证 NetFlow 数据包是否正在发送到 SEC
- 验证思科云是否正在接收 NetFlow 数据包

### 验证 NSEL 事件是否正在发送到 SEC

使用以下两个命令之一验证是否正在向 SEC 发送 NSEL 数据包：

- `flow-export counters`
- 捕获

使用“`flow-export counters`”命令检查正在发送的流导出数据包和 NSEL 错误

- 请确保您已将 ASA 配置为向 SEC 发送 NSEL 事件。请参阅[使用 CDO 宏为 ASA 设备配置 NSEL](#)。
- SEC IP 地址是 NSEL 事件的流收集器地址。如果您已将多个 SEC 载入租户，请确保使用正确的 IP 地址。

- 查找用于转发 NetFlow 事件的 UDP 端口号。请参阅[查找用于安全日志记录分析 \(SaaS\) 的设备 TCP、UDP 和 NSEL 端口](#)。
- 我们推荐的发送 NSEL 事件的接口是 ASA 上的管理接口；您的接口可能有所不同。

使用 CDO 中的命令行界面将这些命令发送到您为 NSEL 配置的 ASA。[批量命令行接口](#)

**步骤 1** 在导航窗格中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备选项卡**。

**步骤 3** 点击相应的设备选项卡，然后选择您配置的 ASA 将 NSEL 事件发送到 SEC。

**步骤 4** 在右侧**设备操作(Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

**步骤 5** 通过运行 `clear flow-export counters` 命令重置流导出计数器。这会将清除导出流计数器重置为零，以便您可以轻松判断是否有新事件传入。

示例：

```
> clear flow-export counters  
Done!
```

**步骤 6** 运行 `show flow-export counters` 命令以查看 NSEL 数据包的目的地、发送的数据包数量和任何错误：

示例：

```
>show flow-export counters  
目的地: management 209.165.200.225 10425  
统计信息:  
发送的数据包数 25000  
错误:  
block allocation errors 0  
invalid interface 0  
template send failure 0  
no route to collector 0  
source port allocation 0
```

在上面的输出中，目的行显示从其发送 NSEL 事件的 ASA 上的接口、SEC 的 IP 地址和 SEC 的端口 10425。它还显示发送的数据包 25000。

如果没有错误且正在发送数据包，请跳至下面的验证思科云是否已接收 NetFlow 数据包。[验证思科云是否正在接收 NetFlow 数据包, on page 32](#)

错误说明：

- **block allocation errors** - 如果收到块分配错误，则 ASA 未将内存分配给流导出器。
  - 恢复操作：致电 思科 Technical Assistance Center (TAC)。

- 接口无效 - 表示您正在尝试将 NSEL 事件发送到 SEC，但您为流导出定义的接口未配置为执行此操作。
  - 恢复操作：查看您在配置 NSEL 时选择的接口。我们建议使用管理接口，您的接口可能与此不同。
- 模板发送失败 - 未正确解析您必须定义的 NSEL 模板。
  - 恢复操作：联系 Defense Orchestrator 支持。[联系思科威胁防御支持](#)
- **no route to collector** - 表示没有从 ASA 到 SEC 的网络路由。
  - 恢复操作：
    - 确保配置 NSEL 时用于 SEC 的 IP 地址是正确的。
    - 确保 SEC 的状态为“活动”，并且最近已发送心跳。请参阅[SDC 无法接通](#)。
    - 确保安全设备连接器的状态为活动，并且最近发送了心跳。
- **source port allocation** - 可能表示您的 ASA 上的端口存在问题。

## 使用“capture”命令捕获从 ASA 发送到 SEC 的 NSEL 数据包

- 请确保您已将 ASA 配置为向 SEC 发送 NSEL 事件。请参阅[使用 CDO 宏为 ASA 设备配置 NSEL](#)。
- SEC IP 地址是 NSEL 事件的流收集器地址。如果您已将多个 SEC 载入租户，请确保使用正确的 IP 地址。
- 查找用于转发 NetFlow 事件的 UDP 端口号。请参阅[查找用于安全日志记录分析 \(SaaS\) 的设备 TCP、UDP 和 NSEL 端口](#)。
- 我们推荐的发送 NSEL 事件的接口是 ASA 上的管理接口；您的接口可能有所不同。

使用 CDO 中的命令行界面将这些命令发送到您为 NSEL 配置的 ASA。[CDO 命令行界面](#)

**步骤 1** 在导航窗格中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击相应的设备类型选项卡，然后选择您配置的 ASA 将 NSEL 事件发送到 SEC。

**步骤 4** 在右侧**设备操作(Device Actions)**窗格中，点击**命令行接口 (Command Line Interface)**。

**步骤 5** 在命令窗口中，运行以下 **capture** 命令：

```
>capture capture_name interface interface_name match udp any host IP_of_SEC eq NetFlow_port  
位置
```

- *capture\_name* 是数据包捕获的名称。
- *interface\_name* 是 NSEL 数据包离开 ASA 的接口的名称。

- *IP\_of\_SEC* 是 SEC VM 的 IP 地址。
- *NetFlow\_port* 是 NSEL 事件发送到的端口。

这将启动数据包捕获。

**步骤 6** 运行 **show capture** 命令以查看捕获的数据包：

```
> show capture capture_name
```

其中，*capture\_name* 是您在上一步中定义的数据包捕获的名称。

以下是显示捕获时间、发送数据包的 IP 地址、IP 地址以及数据包发送到的端口的输出示例。在本例中，192.168.25.4 是 SEC 的 IP 地址，端口 10425 是 SEC 上接收 NSEL 事件的端口。

6 个数据包被捕获

```
1: 14:23:51.706308 192.168.0.169.16431 > 192.168.25.4.10425: udp 476
2: 14:23:53.923017 192.168.0.169.16431 > 192.168.25.4.10425: udp 248
3: 14:24:07.411904 192.168.0.169.16431 > 192.168.25.4.10425: udp 1436
4: 14:24:07.411920 192.168.0.169.16431 > 192.168.25.4.10425: udp 1276
5: 14:24:21.021208 192.168.0.169.16431 > 192.168.25.4.10425: udp 112
6: 14:24:27.444755 192.168.0.169.16431 > 192.168.25.4.10425: udp 196
```

**步骤 7** 运行 **capture stop** 命令以手动停止数据包捕获：

```
> capture capture_name stop
```

其中，*capture\_name* 是您在上一步中定义的数据包捕获的名称。

## 验证思科云是否正在接收 NetFlow 数据包

### 准备工作

验证是否正在从 ASA 发送 NSEL 事件。

### 检查实时 NSEL 事件

检查实时事件和历史事件。

此程序将过滤思科云在过去一小时内收到的 NSEL 事件。

**步骤 1** 从 CDO 菜单中，选择 **分析 (Analytics) > 事件日志记录 (Event Logging)**。

**步骤 2** 点击**实时 (Live)** 选项卡。

**步骤 3** 固定打开事件过滤器。

**步骤 4** 在“ASA 事件” (ASA Events) 部分中，确保选中 NetFlow。

**步骤 5** 在传感器 ID 字段中，输入配置为发送 NSEL 事件的 ASA 的 IP 地址。

步骤 6 在过滤器的底部，确保选中“包括 NetFlow 事件”。

## 检查历史 NSEL 事件

此程序将过滤思科云在您指定的时间范围内收到的 NSEL 事件。

步骤 1 从 CDO 菜单中，选择 **分析 (Analytics) > 事件日志记录 (Event Logging)**。

步骤 2 点击 **历史 (Historical)** 选项卡。

步骤 3 固定打开事件过滤器。

步骤 4 在“ASA 事件” (ASA Events) 部分中，确保选中 NetFlow。

步骤 5 将开始时间设置得足够远，以检查 CDO 是否收到过 NSEL 事件。

步骤 6 在传感器 ID 字段中，输入配置为发送 NSEL 事件的 ASA 的 IP 地址。

步骤 7 在过滤器的底部，确保选中“包括 NetFlow 事件”。

## 已解析的 ASA 系统日志事件

解析的系统日志事件包含比其他系统日志事件更多的事件属性，并允许您搜索任何特定的解析字段。SEC 会将您指定的所有 ASA 事件转发到思科云，但仅解析下表中的系统日志消息。所有已解析的系统日志事件均显示为斜体，以帮助您识别事件类型。

有关系统日志的详细说明，请参阅 [思科 ASA 系列系统日志消息](#)。

系统日志 ID	系统日志类别	系统日志消息的用途
106015	防火墙	表示非 TCP 拒绝状态
106023	防火墙	ACL 拒绝了真实 IP 数据包。即便您没有为 ACL 启用 <b>log</b> 选项，也会显示此消息。
106100	访问列表/用户会话	数据包被 ACL 允许或拒绝。
113019	用户身份验证	关键 AnyConnect
302013、302015、302017、302020	用户会话	TCP、UDP、GRE 和 ICMP 连接创建的连接开始和结束系统日志。
302014、302016、302018、302021	用户会话	TCP、UDP、GRE 和 ICMP 连接创建的连接开始和结束系统日志。
302020 - 302021	用户会话	ICMP 会话建立和断开。

系统日志 ID	系统日志类别	系统日志消息的用途
305006	用户会话/NAT 和 PAT	NAT 连接失败
305011-305014	用户会话/NAT 和 PAT	NAT Build/Teardown 相关
313001、313008	IP 堆栈	表示拒绝与设备的连接。
414004	System	关键 AnyConnect
609001 - 609002	防火墙	网络状态容器时为连接到区域的主机 <b>ip-address</b> 而保留或移除的。
710002、710004 710005	用户会话	连接 box 失败
710003	用户会话	表示拒绝与设备的连接。
746012、746013	用户会话	关键 AnyConnect

#### 相关信息：

- [使用命令行接口将 ASA 系统日志事件发送到思科云](#)
- [在事件日志记录页面中搜索和过滤事件](#)

## 为云交付的防火墙管理中心托管设备实施 SAL (SaaS)

要部署此集成，您必须使用系统日志或直接连接在 SAL (SaaS) 中设置事件数据存储。

- [使用系统日志将云交付的防火墙管理中心托管事件发送到 SAL \(SaaS\)，第 35 页](#)
- [使用直接连接将云交付的防火墙管理中心托管的时间日志发送到 SAL \(SaaS\)，第 37 页](#)

## SAL (SaaS) 集成的要求、准则和限制

类型	说明
Cisco Secure Firewall Threat Defense	<ul style="list-style-type: none"> <li>• CDO 管理的独立威胁防御设备，版本 7.2 及更高版本。</li> <li>• 要使用系统日志发送事件，您必须有威胁防御 6.4 或更高版本。</li> <li>• 要直接发送事件，您必须有威胁防御 7.2 或更高版本。</li> <li>• 必须部署防火墙系统并成功生成事件。</li> </ul>

类型	说明
区域云	<ul style="list-style-type: none"> <li>• 确定要向其发送事件的区域云。</li> <li>• 无法在不同的区域云之间查看或移动事件。</li> <li>• 如果您使用直接连接将事件发送到云以与思科 SecureX 或思科 SecureX 威胁响应集成，则必须使用相同的云区域来进行此集成。</li> <li>• 如果直接发送事件，则在 CDO 中指定的区域云必须与 CDO 租户的区域相匹配。</li> </ul>
数据计划	<ul style="list-style-type: none"> <li>• 您必须购买一个数据计划，以反映思科云每天从威胁防御设备接收的事件数量。这称为每日注入速率。</li> <li>• 使用<a href="#">日志记录量估算器工具</a>来估算您的数据存储要求。</li> </ul>
帐户	当您购买此集成的许可证时，系统会为您提供一个 CDO 租户帐户来支持集成。

## 使用系统日志将云交付的防火墙管理中心托管事件发送到 SAL (SaaS)

本步骤提供了有关从 CDO 托管的设备发送安全事件（连接、安全情报、入侵、文件和恶意软件事件）的系统日志消息的配置信息。

### 开始之前

- 配置策略以生成安全事件，并验证您希望看到的事件显示在分析 (Analysis) 菜单下的适用表中。
- 收集与系统日志服务器 IP 地址，端口和协议（UDP 或 TCP）相关的信息。
- 确保您的设备可以访问系统日志服务器。

**步骤 1** 登录 CDO。

**步骤 2** 从 CDO 菜单中，点击 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)** 以打开 **服务 (Services)** 页面。

**步骤 3** 点击并选择云托管 **FMC (Cloud-Delivered FMC)**，然后点击 **配置 (Configuration)**。

**步骤 4** 为威胁防御设备配置系统日志设置：

- 点击 **设备 (Devices)** > **平台设置 (Platform Settings)** 并编辑与您的威胁防御设备关联的平台设置策略。
- 在左侧导航窗格中，点击 **系统日志 (Syslog)** 并配置系统日志设置，如下所示：

点击此 UI 元素...	要执行以下操作:
日志记录设置	启用日志记录, 制定 FTP 服务器设置, 以及闪存用法。
日志记录目标	启用向特定目标的记录日志, 并指定按邮件严重性级别、事件类别或自定义事件列表进行过滤。
邮件设置	指定用作以邮件形式发送的系统日志消息的源地址的邮件地址。
事件列表	定义包括事件类、严重性级别和事件 ID 的自定义事件列表。
速率限制	指定发送到所有配置的目标的邮件数量, 并定义要为其分配速率限制的邮件严重性级别。
系统日志设置	指定日志记录设施, 启用时间戳包含, 并启用其他设置以将服务器设置为一个系统日志目标。
系统日志服务器	为指定为日志记录目标的系统日志服务器指定 IP 地址、使用的协议、格式和安全区域。

c) 点击保存。

**步骤 5** 配置访问控制策略的常规日志记录设置（包括文件和恶意软件日志记录）：

- 点击策略 (Policies) > 访问控制 (Access Control), 然后编辑与威胁防御设备关联的访问控制策略。
- 点击更多 (More), 然后选择日志记录 (Logging)。配置访问控制策略的常规日志记录设置（包括文件和恶意软件日志记录），如下所示：

点击此 UI 元素...	要执行以下操作:
使用特定系统日志警报发送	从现有的预定义警报列表中选择一个系统日志警报, 或者通过指定名称、日志主机、端口、设施和严重程度来添加一个警报。
使用在设备上部署的 FTD 平台设置策略中配置的系统日志设置	通过在平台设置 (Platform Settings) 中配置系统日志配置并重新使用访问控制策略中的设置来统一系统日志配置。所选的严重性适用于所有连接和入侵事件。默认严重性为警报 (ALERT)。
发送 IPS 事件的系统日志消息	作为系统日志消息发送事件。除非覆盖, 否则将使用默认的系统日志设置。
发送文件和恶意软件事件的系统日志消息	作为系统日志消息发送文件和恶意软件事件。除非覆盖, 否则将使用默认的系统日志设置。

c) 点击保存。

**步骤 6** 为访问控制策略启用安全情报事件日志记录：

- a) 在同一访问控制策略中，点击 **安全情报** 选项卡。
- b) 点击 **日志记录 (Logging)** 并使用以下条件启用安全智能日志记录：
  - 按域名 - 点击 **DNS 策略 (DNS Policy)** 下拉列表旁边的日志记录。
  - 按 IP 地址 - 点击 **网络** 旁边的日志记录。
  - 按 URL - 点击 **URL** 旁边的日志记录。
- c) 点击 **保存 (Save)**。

**步骤 7** 为访问控制策略中的每个规则启用系统日志记录：

- a) 在同一访问控制策略中，点击 **规则** 选项卡。
- b) 点击要编辑的规则。
- c) 点击规则中的 **日志记录 (Logging)** 选项卡。
- d) 选中连接开始时的日志 (**Log at beginning of connection**) 和连接结束时的日志 (**Log at end of connection**) 复选框。
- e) 如果要记录文件事件，请选中 **日志文件 (Log Files)** 复选框。
- f) 选中 **系统日志服务器 (Syslog Server)** 复选框。
- g) 验证规则是在访问控制日志记录中使用默认系统日志配置 (**ng default syslog configuration in Access Control Logging**)。
- h) 点击 **保存**。
- i) 对策略中的每个规则重复步骤 7.a 至 7.h。

---

#### 下一步做什么

如果您已完成所有必要的更改，请将更改部署到托管设备。

## 使用直接连接将云交付的防火墙管理中心托管的时间日志发送到 SAL (SaaS)

配置云交付的防火墙管理中心以便直接向 SAL (SaaS) 发送事件。按照此程序在云交付的防火墙管理中心中启用思科云事件全局设置。必要时，您可以排除单个 FTD 设备向 SAL (SaaS) 发送事件日志。有关详细信息，请参阅[启用或禁用威胁防御设备以使用直接连接将事件日志发送到 SAL \(SaaS\)](#)，第 38 页。

#### 开始之前

- 将设备载入云交付的防火墙管理中心，将许可证分配给这些设备，然后将这些设备配置为直接将事件发送到 SAL (SaaS)。
- 通过编辑规则并选择在连接开始时记录 (**Log at Beginning of Connection**) 和在连接结束时记录 (**Log at End of Connection**) 选项来启用基于每个规则的连接日志记录。

步骤 1 登录 CDO。

步骤 2 在 CDO 菜单中，点击 **工具和服务 (Tools & Services) > 防火墙管理中心 (Firewall Management Center)**。

步骤 3 点击云交付的 **FMC (Cloud-Delivered FMC)**，然后在右侧的 **系统 (System)** 窗格中，点击 **思科云事件 (Cisco Cloud Events)**。

步骤 4 在配置思科云事件 (**Configure Cisco Cloud Events**) 构件中，执行以下操作：

1. 点击 **将事件发送到云 (Send Events to the Cisco Cloud)** 切换按钮以启用整体配置。
2. 选中 **将入侵事件发送到云 (Send Intrusion Events to the cloud)** 复选框以将入侵事件发送到云。
3. 选中 **将文件和恶意软件事件发送到云 (Send File and Malware Events to the cloud)** 复选框，将文件和恶意软件事件发送到云。
4. 选择一个选项以便将连接事件发送到云：
  - 点击 **无 (None)** 单选按钮可不将连接事件发送到云。
  - 点击 **安全事件 (Security Events)** 单选按钮，仅将安全情报事件发送到云。
  - 点击 **全部 (All)** 单选按钮，将所有连接事件发送到云。
5. 点击 **保存 (Save)**。

## 启用或禁用威胁防御设备以使用直接连接将事件日志发送到 SAL (SaaS)

启用或禁用云交付的防火墙管理中心管理的 FTD 设备，以将事件直接发送到 SAL (SaaS)。通过此设备级控制，您可以选择性地排除特定 FTD 设备向思科云发送事件日志，以减少流量或维护 SAL 和本地事件日志存储的组合。



### 注释

- 要启用或禁用从 FTD 设备向思科云发送事件，请在云交付的防火墙管理中心中启用思科云事件全局设置。有关启用思科云事件全局设置的详细信息，请参阅 [使用直接连接将云交付的防火墙管理中心托管的时间日志发送到 SAL \(SaaS\)](#)，第 37 页。

在云交付的防火墙管理中心中启用思科云事件全局设置时，默认情况下会为所有 FTD 设备启用将事件发送到思科云。

- FTD 7.4.1 或更高版本支持启用或禁用 FTD 设备向云发送事件日志的选项。

### 开始之前

- 将设备载入云交付的防火墙管理中心，将许可证分配给这些设备，然后将这些设备配置为直接将事件发送到 SAL (SaaS)。
- 通过编辑规则并选择在连接开始时记录 (**Log at Beginning of Connection**) 和在连接结束时记录 (**Log at End of Connection**) 选项来启用基于每个规则的连接日志记录。

步骤 1 登录 CDO。

步骤 2 在 CDO 菜单中，点击清单 (**Inventory**)。

步骤 3 点击设备 (**Devices**) 选项卡以找到设备。

步骤 4 点击 **FTD** 选项卡。

步骤 5 从清单列表中选择要编辑其配置的 FTD 设备。

步骤 6 在设备管理 (**Device Management**) 窗格中，点击云事件 (**Cloud Events**)。

步骤 7 点击将事件发送到云 (**Send Events to the Cisco Cloud**) 切换按钮以启用或禁用配置。

步骤 8 点击保存 (**Save**)。

## 安全事件连接器

安全事件连接器 (SEC) 是安全分析和日志记录 SaaS 解决方案的一个组件。它接收来自 ASA 和 FDM 管理设备的事件，并将其转发到思科云。CDO 在“事件日志记录” (Event Logging) 页面上显示事件，以便管理员可以在该页面或使用 Cisco Secure Cloud Analytics 进行分析。

SEC 安装在您的网络中部署的安全设备连接器上，安装在您的网络中部署的自己的 CDO 连接器虚拟机上，或安装在 AWS 虚拟私有云 (VPC) 上。

### 安全事件连接器 ID

与思科 Technical Assistance Center (TAC) 或其他 CDO 支持人员合作时，您可能需要 SEC 的 ID。该 ID 可在 CDO 的“安全连接器” (Secure Connectors) 页面上找到。要查找 SEC ID，请执行以下操作：

1. 从左侧 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。
2. 点击您要标识的 SEC。
3. SEC ID 是“详细信息” (Details) 窗格中“租户 ID” (Tenant ID) 上方列出的 ID。

### 相关信息：

- [关于 ASA 的安全分析和日志记录 \(SAL SaaS\)](#)
- [在 SDC 虚拟机上安装安全事件连接器，第 40 页](#)
- [使用 VM 映像安装 SEC](#)

- [使用 VM 映像安装 SEC](#)
- [使用 Terraform 模块在 AWS VPC 上安装安全事件连接器，第 58 页](#)
- [删除安全事件连接器](#)
- [取消调配思科安全分析和日志记录 \(SaaS\)](#)

## 安装安全事件连接器

安全事件连接器 (SEC) 可以安装在有或没有 SDC 的租户上。

您可以在与安全设备连接器相同的虚拟机上安装一个 SEC（如果有）；或者，您可以在网络中维护的 SEC 自己的 CDO 连接器虚拟机上安装 SEC。

请参阅以下介绍各种安装情况的主题：

- [使用 VM 映像安装 SEC，第 50 页](#)
- [使用 CDO 映像安装 SEC，第 43 页](#)
- [使用 Terraform 模块在 AWS VPC 上安装安全事件连接器，第 58 页](#)

## 在 SDC 虚拟机上安装安全事件连接器

安全事件连接器 (SEC) 从 ASA 和 FDM 管理设备接收事件，并将其转发到思科云。CDO 在“事件日志记录” (Event Logging) 页面上显示事件，以便管理员可以在该页面或使用思科安全云分析进行分析。

您可以在与安全设备连接器相同的虚拟机上安装一个 SEC（如果有）；或者，您可以在网络中维护的 SEC 自己的 CDO 连接器虚拟机上安装 SEC。

本文介绍如何在与 SDC 相同的虚拟机上安装 SEC。如果要安装更多 SEC，请参阅 [使用 CDO 映像安装 SEC，第 43 页](#) 或 [使用 VM 映像安装 SEC，第 50 页](#)。

### 开始之前

- 购买思科安全和分析日志记录、日志记录和故障排除许可证。或者，如果您想先注销思科安全和分析，请登录 CDO，然后在主导航栏上，选择 **分析 (Analytics) > 事件日志记录 (Event Logging)** 并点击 **请求试用 (Request Trial)**。您还可以购买 **日志记录分析和检测 (Logging Analytics and Detection)** 以及 **全面网络分析和监控 (Total Network Analytics and Monitoring)** 许可证，以将安全云分析应用于事件。
- 确保您的 SDC 已安装。如果需要安装 SDC，请执行以下程序之一：
  - [使用 CDO 的虚拟机映像部署安全设备连接器](#)
  - [使用您自己的虚拟机部署安全设备连接器](#)



---

**注释** 如果您在自己的虚拟机上安装了本地 SDC，则需要进行[您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置](#)才能允许事件到达它。

---

- 确保 SDC 与 CDO 通信：
    1. 从 CDO 菜单中，选择 **工具和服务 (Tools & Services) > 安全连接器 (Secure Connectors)**。
    2. 在安装 SEC 之前，请确保 SDC 的最后一次心跳不超过 10 分钟，并且 SDC 的状态为活动。
  - 系统要求 - 为运行 SDC 的虚拟机分配额外的 CPU 和内存：
    - CPU：分配额外 4 个 CPU 以容纳 SEC，使 CPU 总数达到 6 个。
    - 内存：为 SEC 分配额外 8 GB 内存，使内存总量达到 10 GB。
- 更新 VM 上的 CPU 和内存以适应 SEC 后，打开 VM 并确保“安全连接器”页面指示 SDC 处于“活动”状态。

---

**步骤 1** 登录 CDO。

**步骤 2** 从 CDO 菜单中，选择 **工具和服务 (Tools & Services) > 安全连接器 (Secure Connectors)**。

**步骤 3** 点击蓝色加号按钮，然后点击**安全事件连接器 (Secure Event Connector)**。

步骤 4 跳过向导的步骤 1，转至步骤 2。在向导的步骤 2 中，点击复制 **SEC 引导程序数据 (Copy SEC Bootstrap Data)** 的

### Deploy an On-Premises Secure Event Connector ✕

```
dRaU9pSmhNM1UxWTJVMFppMDNNakZrTFRSaFpUVXRPV013TkMweU5UZG10VE5oTWpnMU9HVW1MQ0pq
YkdsbGJuUmZhV1FpT21KaGNHa3RZMnhwW1c1ME1uMC5tTzh0bTZMz1N6cjI4b1ZGZERqYjJNRzVqUE
ZmYTZQYzVsRjRITT1teVVEVzh2Qk5FWW44c3V0Z3NTQ0o0TH15N0xzVGsydEx4N05nbS00STB6SmZ6
aWdQTKRiV1RsRW1tcjI5SkFVZ2NBWEhySkdzckctMREszUnJUM0hZU3JkZ21Hd1dG6b3FwWUdZnkJHRU
VacmI0YVFLSjFTdnJ5RjVFZ2FqajZFZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZX1MT09qcjRicEN0UnhYaEVMUFzV19qQW1PNXM3Tm02Sn1rMXR1QTFsYmE3VkxN0Up4bk9RS1pqaW
1rdDNsYnRRbDNrTHMxeWduaXdVU1RuWkQxM0c5T2FJWEXCQ093T3NESGdNeH16UU13ZWJVNUdGT2RS
NfN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YwDpbmCuZGV2LmxvY2toYXJ0Lm
1vIgpDRE9fVEV0QU5UPSJDRE9fY2lZy28tYW1hbGxpbyIKQ0RPX0JPT1RTVFJBUf9VUkw9Imh0dHBz
0i8vc3RhZ21uZy5kZXlYubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY2lZy28tYW1hbGxpby
IKT05MMWV9FVkvOVE1ORz0idHJ1ZSik
```

[Copy CDO Bootstrap Data](#)

**Step 2**

Read the [instructions](#) about deploying the Secure Event Connector on vSphere.  
Copy the bootstrap data below and paste it when prompted for "SEC bootstrap Data".

**⚠ The SEC bootstrap data is valid until 10/13/2021, 10:44:14 AM**

```
U1NFx0RFVklDRV9JRd0iZTBhZTJkNmMtMDdhYy00Y2JkLWEzNWQtOGYzZDJKMjQ1ZmU3IqpTU0VfRE
U0VfT1RQPSI5Y2IzNTI4ZWZlMzg0OTQ2NjViMDFkZmEyYjUyMGUxNSIKVEVOQU5UX05BTUU9IKNET1
9jaXNjby1hbWFSbG1vIg==
```

[Copy SEC Bootstrap Data](#) ←

**Step 3**

Verify the connection status of the new SEC by exiting this dialog and checking the "Last Heartbeat" information.

Cancel
OK

链接。

步骤 5 打开终端窗口并以“cdo”用户身份登录 SDC。

步骤 6 登录后，切换到“sdc”用户。当系统提示输入密码时，请输入“cdo”用户的密码。以下是这些命令的示例：

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdcsdc-vm ~]$
```

步骤 7 在提示符后，运行 **sec.sh setup** 脚本：

```
[sdcsdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

步骤 8 在提示符的末尾，粘贴您在步骤 4 中复制的引导程序数据，然后按 **Enter** 键。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjkhOuihIuyftyXtfcghvjbkbB=
```

载入 SEC 后，sec.sh 将运行脚本来检查 SEC 的运行状况。如果所有运行状况检查均为“绿色”，则运行状况检查会向事件日志发送示例事件。示例事件在事件日志中显示为名为“sec-health-check”的策略。

```
=====
Running SEC health check for tenant [REDACTED]
-----
SEC cloud URL [REDACTED] is: Reachable
-----
SEC Connector status: Active
-----
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
-----
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in
=====
```

如果您收到注册失败或 SEC 载入失败的消息，请转至[对安全事件连接器载入失败进行故障排除](#)。

**步骤 9** 确定运行 SDC 和 SEC 的虚拟机是否需要额外配置：

- 如果您在自己的虚拟机上安装了 SDC，请继续 [您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置](#)，第 55 页。
- 如果您使用 CDO 映像安装了 SDC，请继续执行“下一步”。

#### 下一步做什么

退回至 [为 ASA 设备实施安全日志记录分析 \(SaaS\)](#)，第 10 页。

#### 相关信息：

- [对安全设备连接器进行故障排除](#)
- [安全事件连接器故障排除](#)
- [安全事件连接器载入故障排除](#)
- [安全事件连接器注册失败故障排除](#)

## 使用 CDO 映像安装 SEC

安全事件连接器 (SEC) 将事件从 ASA 和 FTD 转发到思科云，以便您可以在“事件日志记录”页面中查看它们，并根据您的许可使用安全云分析进行调查。

您可以在租户上安装多个安全事件连接器 (SEC)，并将事件从您的 ASA 和 FDM 托管的设备定向到您安装的任何 SEC。拥有多个 SEC 可让您将 SEC 安装在不同的位置，并将事件发送到思科云的工作分发给他们。

安装 SEC 的过程分为两部分：

1. 使用 [CDO VM 映像安装 CDO 连接器，以便支持安全事件连接器](#)，第 44 页 您安装的每个 SEC 都需要一个 CDO 连接器。CDO 连接器不同于安全设备连接器 (SDC)。
2. 在 [CDO 连接器虚拟机上安装安全事件连接器](#)，第 56 页。



**注释** 如果要通过创建自己的 VM 来创建 CDO 连接器，请参阅[您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置](#)。

**后续操作：**

继续执行 [使用 CDO VM 映像安装 CDO 连接器，以便支持安全事件连接器](#)，第 44 页

## 使用 CDO VM 映像安装 CDO 连接器，以便支持安全事件连接器

**开始之前**

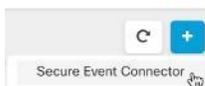
- 购买思科安全和分析日志记录、日志记录和故障排除许可证，您还可以购买日志记录分析和检测以及全面网络分析和监控许可证，以便将安全云分析应用于事件。  
如果愿意，您还可以登录 CDO，然后在主导航栏中选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)** 并点击 **请求试用 (Request Trial)**，以便申请获取试用版的安全分析和日志记录。
- CDO 需要进行严格的证书检查，并且不支持 CDO 连接器和互联网之间的 Web/内容代理检查。如果使用代理服务器，请禁用对 CDO 连接器和 CDO 之间的流量进行检查。
- 此进程中安装的 CDO 连接器必须在 TCP 端口 443 上具有对互联网的完全出站访问权限。
- 查看 [将 Cisco Defense Orchestrator 连接到 Secure Device Connector](#)，以便确保 CDO 连接器能够正确访问网络。
- CDO 支持使用 vSphere Web 客户端或 ESXi Web 客户端来安装其 CDO 连接器 VM OVF 映像。
- CDO 不支持使用 VM vSphere 桌面客户端来安装 CDO 连接器 VM OVF 映像。
- ESXi 5.1 虚拟机监控程序。
- 仅用于托管 CDO 连接器和 SEC 的 VM 的系统要求：
  - VMware ESXi 主机需要 4 个 vCPU。
  - VMware ESXi 主机至少需要 8GB 内存。
  - VMware ESXi 需要 64GB 磁盘空间来支持虚拟机，具体取决于您的调配选择。
- 在开始安装之前收集以下信息：
  - 要用于 CDO 连接器虚拟机的静态 IP 地址。
  - 您在安装过程中创建的 **root** 和 **cdo** 用户的密码。
  - 您的组织使用的 DNS 服务器的 IP 地址。

- SDC 地址所在网络的网关 IP 地址。
- 时间服务器的 FQDN 或 IP 地址。
- CDO 连接器虚拟机被配置为定期安装安全补丁，为此需要打开通出站端口 80。

**步骤 1** 登录到要为其创建 CDO 连接器的 CDO 租户。

**步骤 2** 从 CDO 菜单中，选择 **工具和服务 (Tools & Services) > 安全连接器 (Secure Connectors)**。

**步骤 3** 点击蓝色加号按钮，然后点击**安全事件连接器 (Secure Event Connector)**。



**步骤 4** 在步骤 1 中，点击下载 **CDO 连接器虚拟机映像 (Download the CDO Connector VM image)**。这是您在上一步安装 SEC 的特殊映像。始终下载 CDO 连接器虚拟机，以确保使用的是最新映像。



**步骤 5** 从 zip 文件中提取所有文件。它们看起来和下面有些相似：

- CDO-SDC-VM-ddd50fa.ovf
- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

**步骤 6** 使用 vSphere Web 客户端以管理员身份登录 VMware 服务器。

**注释** 请勿使用 VM vSphere 桌面客户端。

**步骤 7** 按照相关提示从 OVF 模板部署本地 CDO 连接器虚拟机。（您将需要 .ovf、.mf 和 .vdk 文件才能部署模板。）

**步骤 8** 在设置完成后，打开虚拟机电源。

**步骤 9** 打开新 CDO 连接器虚拟机的控制台。

**步骤 10** 以 **cdo** 用户的身份登录。默认密码为 **adm123**。

**步骤 11** 在提示符处键入 `sudo sdc-onboard setup`

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

**步骤 12** 出现提示时，输入 **cdo** 用户的默认密码：**adm123**。

**步骤 13** 按照提示为 **root** 用户创建一个新密码。

**步骤 14** 按照提示为 **cdo** 用户创建一个新密码。

**步骤 15** 按照提示输入 Cisco Defense Orchestrator 的域信息。

**步骤 16** 输入您要用于 CDO 连接器虚拟机的静态 IP 地址。

**步骤 17** 输入要在上面安装 CDO 连接器虚拟机的网络的网关 IP 地址。

**步骤 18** 输入 CDO 连接器的 NTP 服务器地址或 FQDN。

**步骤 19** 出现提示时，输入 Docker 网桥的信息，如果不适用，则可将其留空，然后按 <Enter>。

**步骤 20** 确认您的输入内容。

**步骤 21** 当系统提示“您想立即设置 SDC 吗？”(Would you like to setup the SDC now?) 时输入 **n**。

**步骤 22** 以 **cdo** 用户身份登录，以便创建与 CDO 连接器的 SSH 连接。

**步骤 23** 在提示符处键入 **sudo sdc-onboard bootstrap**

```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

**步骤 24** 在出现提示时，请输入 **cdo** 用户的密码。

**步骤 25** 在出现提示时，返回 CDO 并复制 CDO 引导程序数据，然后将其粘贴到 SSH 会话中。要复制 CDO 引导程序数据，请执行以下操作：

1. 登录 CDO。
2. 从 CDO 菜单中，选择 **工具和服务 (Tools & Services) > 安全连接器 (Secure Connectors)**。
3. 选择您开始载入的安全事件连接器。状态应显示为“正在载入” (Onboarding)。
4. 在“操作” (Actions) 窗格中，点击部署本地安全事件连接器 (**Deploy an On-Premises Secure Event Connector**)。

5. 复制对话框步骤 1 中的 CDO 引导程序数据。

Deploy an On-Premises Secure Event Connector
✕

i
SEC will be deployed on a new VM

**Step 1**

Download the [CDO Connector VM](#) and follow the [documentation](#) to deploy the CDO VM on vSphere. You will be prompted for "CDO Bootstrap Data". Copy the data below and paste it into the CDO Bootstrap Data input field in vSphere.

CDO Bootstrap Data

```

Q0RPX1RPS0V0PSJ1eUpOYkdjaU9pS1NVekxTm1Jc0luUjVjQ0k2SWtwWFZDSjkuZX1KM1pYSW1PaU
l3SWl3aWMyTnZjR1VpT2xzaWRISjFjM1FpTENKeVpXRmtJaXdpZDNKcGRHVWlMQ0poTTJVMVkyVTBa
aTAzTWpGa0xUUmhaVFV0T1dNd05DMH10VGRpT1R0aE1qZzFPR1VpWFN3aVlXMXlJam9pYzJGdGJDSX
NjBkp2YkdWek1qcGJJbEpQVEVWZ1UxV1FSVkpUUVVST1NVNG1YU3dpYVh0ek1qb2lhWFJrSWl3aVky
eDFjM1JsY2tsa0lqb2lNU0lZSW1sa0lqb2labVF3T0dReVpHVXRNMlZpT1MwMFpEYzRMV0kwW1dNdF
pUWXh0V0UyWmpjNFkyUm1JaXdpYzNWaWftVmpkRlI1Y0dVaU9pSjFjM1Z5SWl3aWFuUnBJam9pTURB
VacmI0YVFLSjFTdnJ5RjVfZ2FqajZFZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZXlMT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXRlQTFsYmE3VksxNOUp4bk9RS1pqaW
1rdDNsYnRRbDnrTHMxeWduaXdVU1RuWkQxM0c5T2FJWExCQ093T3NESGdNeHl6UU13ZWJVNUdGT2RS
NFN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YWdpbmcuZGV2LmxvY2toYXJ0Lm
1vIgpDRE9fVEVOQU5UPSJDRE9fY2lZy28tYW1hbGxpbyIKQ0RPX0JPT1RTVFJBUf9VUkw9Imh0dHBz
Ois8vc3RhZ2luZy5kZXUyubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY2lZy28tYW1hbGxpby
IKT05MWV9FVkvOVEl0Rz0idHJ1ZS1K
```

📄
Copy CDO Bootstrap Data
←

Cancel
OK

**步骤 26** 当系统提示您是否要更新这些设置时？(Would you like to update these settings?) 输入 **n**。

**步骤 27** 返回 CDO 中的“部署本地安全事件连接器对话框”(Deploy an On-Premises Secure Event Connector)，然后点击确定 (**OK**)。在“安全连接器”(Secure Connectors) 页面上，您会看到安全事件连接器处于黄色的正在载入状态。

### 下一步做什么

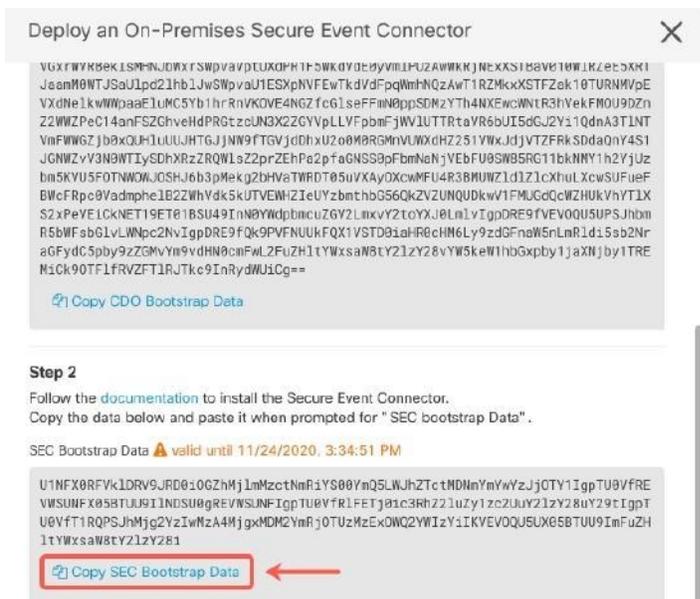
请继续在 [CDO 连接器虚拟机上安装安全事件连接器](#)，第 47 页。

## 在 CDO 连接器虚拟机上安装安全事件连接器

### 开始之前

您应该已安装 CDO 连接器虚拟机，如使用 [CDO VM 映像安装 CDO 连接器](#)，以便支持安全事件连接器，第 44 页中所述。

- 步骤 1 登录 CDO。
- 步骤 2 从 CDO 菜单中，选择 **工具和服务 (Tools & Services) > 安全连接器 (Secure Connectors)**。
- 步骤 3 选择您在上一步加载的 CDO 连接器。在“安全连接器” (Secure Connectors) 表中，它将被称为“安全事件连接器”，并且应仍处于“正在载入”状态。
- 步骤 4 点击右侧“操作” (Actions) 窗格中的 **部署现场安全事件连接器 (Deploy an On-Premises Secure Event Connector)**。
- 步骤 5 在向导的步骤 2 中，点击 **复制 SEC 引导程序数据 (Copy SEC bootstrap data)** 的链接。



- 步骤 6 创建与 CDO 连接器的 SSH 连接，并以 **cdo** 用户身份登录。
- 步骤 7 登录后，切换到 **sdc** 用户。当系统提示输入密码时，请输入“cdo”用户的密码。以下是这些命令的示例：

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

- 步骤 8 在提示符后，运行 **sec.sh** 安装脚本：

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

- 步骤 9 在提示符的末尾，粘贴您在步骤 4 中复制的引导程序数据，然后按 **Enter** 键。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFuIyIOHKNkjbKhhvgyRstwtterTyufGUihjPojp9UOoiUY8VHHGFREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

载入 SEC 后，**sec.sh** 将运行脚本来检查 SEC 的运行状况。如果所有运行状况检查均为“绿色”，则运行状况检查会向事件日志发送示例事件。示例事件在事件日志中显示为名为“sec-health-check”的策略。

```
=====
Running SEC health check for tenant [redacted]
-----
SEC cloud URL [redacted] is: Reachable
-----
SEC Connector status: Active
-----
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
-----
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
=====
```

如果您收到注册失败或 SEC 载入失败的消息，请转至[安全事件连接器载入故障排除](#)。

如果您收到成功消息，请返回 CDO 并点击[完成部署现场安全事件连接器 \(Done on the Deploy an ON-Premise Secure Event Connector\)](#) 对话框。

**步骤 10** 继续“下一步做什么。”

### 下一步做什么

退回至 [为 ASA 设备实施安全日志记录分析 \(SaaS\)](#)，第 10 页。

相关信息：

- [对安全设备连接器进行故障排除](#)
- [安全事件连接器故障排除](#)
- [安全事件连接器载入故障排除](#)

## 在 Ubuntu 虚拟机上部署安全事件连接器

### 开始之前

您应该已按照 [在 Ubuntu 虚拟机上部署安全设备连接器](#) 和 [安全事件连接器](#) 中的说明在 Ubuntu VM 上安装了安全设备连接器。

**步骤 1** 登录 CDO。

**步骤 2** 选择 [工具和服务 \(Tools & Services\)](#) > [安全连接器 \(Secure Connectors\)](#)。

**步骤 3** 在 [服务 \(Services\)](#) 页面上，选择 [安全连接器 \(Secure Connectors\)](#) 选项卡，点击 ，然后选择 [安全事件连接器 \(Secure Event Connector\)](#)。

**步骤 4** 将窗口中步骤 2 中的 SEC 引导程序数据复制到记事本。

**步骤 5** 执行以下命令：

```
[sdc@vm]:~$sudo su sdc
sdc@vm:/home/user$ cd /usr/local/cdo/toolkit
```

出现提示时，请输入您复制的 SEC 引导程序数据。

```
sdc@vm:~/toolkit$ ./sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
Successfully on-boarded SEC
```

安全事件连接器可能需要几分钟才能在 CDO 中变为“活动”状态。

## 使用 VM 映像安装 SEC

安全事件连接器 (SEC) 将事件从 ASA 和 FTD 转发到思科云，以便您可以在“事件日志记录”页面中查看它们，并根据您的许可使用安全云分析进行调查。

您可以在租户上安装多个安全事件连接器 (SEC)，并将事件从您的 ASA 和 FDM 托管的设备定向到您安装的任何 SEC。拥有多个 SEC 可让您在不同区域安装 SEC，并将事件发送到思科云的工作分发给他们。

使用您自己的 VM 映像安装多个 SEC 的过程分为三部分。您必须执行以下每个步骤：

1. [使用 VM 映像安装 CDO 连接器以支持 SEC，第 50 页](#)
2. [您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置，第 55 页](#)
3. [在 CDO 连接器虚拟机上安装安全事件连接器](#)



**注释** 将 CDO VM 映像用于 CDO 连接器是安装 CDO 连接器的最简单、最准确和首选的方法。如果要使用该方法，请参阅[使用 CDO 映像安装 SEC，第 43 页](#)。

后续操作：

请继续[使用 VM 映像安装 CDO 连接器以支持 SEC，第 50 页](#)

## 使用 VM 映像安装 CDO 连接器以支持 SEC

CDO 连接器 VM 是安装 SEC 的虚拟机。CDO 连接器仅用于为思科安全分析和日志记录 (SaaS) 客户提供 SEC 支持。

这是安装和配置安全事件连接器 (SEC) 所需完成的三个步骤中的第一步。完成此程序后，您需要完成以下程序：

- [您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置，第 55 页](#)
- [在 CDO 连接器虚拟机上安装安全事件连接器](#)

开始之前

- 购买思科安全和分析日志记录、日志记录和故障排除许可证，您还可以购买日志记录分析和检测以及全面网络分析和监控许可证，以将安全云分析应用于事件。

如果愿意，您还可以登录 CDO，然后在主导航栏中选择 **分析 (Analytics) > 事件日志记录 (Event Logging)** 并点击 **请求试用 (Request Trial)**，以便申请获取试用版的安全分析和日志记录。

- CDO 需要严格的证书检查，并且不支持 CDO 连接器和互联网之间的 Web/内容代理。
- CDO 连接器必须在 TCP 端口 443 上具有对互联网的完全出站访问权限。
- 查看 [使用安全设备连接器连接到思科防御协调器](#) 以确保对 CDO 连接器进行适当的网络访问。
- 安装了 vCenter Web 客户端或 ESXi Web 客户端的 VMware ESXi 主机。



---

**注释** 我们不支持使用 vSphere 桌面客户端进行安装。

---

- ESXi 5.1 虚拟机监控程序。
- Cent OS 7 访客操作系统。
- 仅托管 CDO 连接器和 SEC 的 VM 的系统要求：
  - CPU：分配 4 个 CPU 以容纳 SEC。
  - 内存：为 SEC 分配 8 GB 内存。
  - 磁盘空间：64 GB
- 执行此过程的用户应该能够轻松地在 Linux 环境中使用 **vi** 可视化编辑器编辑文件。
- 如果您在 CentOS 虚拟机上安装 CDO 连接器，我们建议您定期安装 Yum 安全补丁。根据您的 Yum 配置，要获取 Yum 更新，您可能需要在端口 80 和 443 上打开出站访问。您还需要配置 yum-cron 或 crontab 来安排更新。与您的安全运营团队合作，确定是否需要更改任何安全策略以允许您获取 Yum 更新。
- 在开始安装之前收集以下信息：
  - 要用于 CDO 连接器的静态 IP 地址。
  - 您在安装过程中创建的 **root** 和 **cdo** 用户的密码。
  - 您的组织使用的 DNS 服务器的 IP 地址。
  - CDO 连接器地址所在网络的网关 IP 地址。
  - 时间服务器的 FQDN 或 IP 地址。
- CDO 连接器虚拟机被配置为定期安装安全补丁，为此需要打开出站端口 80。
- **开始之前**：不要将本程序中的命令复制并粘贴到终端窗口中，而应键入这些命令。某些命令包括 “n-dash”，在剪切和粘贴过程中，这些命令可以作为 “m-dash” 应用，这可能会导致命令失败。

- 步骤 1** 在安全设备连接器页面中，点击蓝色加号按钮 ，然后点击安全事件连接器。
- 步骤 2** 使用提供的链接，复制“部署现场安全事件连接器” (Deploy an On-Premises Secure Event Connector) 窗口的步骤 2 中的 SEC 引导程序数据。
- 步骤 3** 安装 CentOS 7 虚拟机 ([http://isoredirect.centos.org/centos/7/isos/x86\\_64/CentOS-7-x86\\_64-Minimal-1804.iso](http://isoredirect.centos.org/centos/7/isos/x86_64/CentOS-7-x86_64-Minimal-1804.iso))，其内存、CPU 和磁盘空间至少应符合此程序的要求。
- 步骤 4** 安装后，配置基本网络，例如指定 CDO 连接器的 IP 地址、子网掩码和网关。
- 步骤 5** 配置 DNS（域名服务器）服务器。
- 步骤 6** 配置 NTP（网络时间协议）服务器。
- 步骤 7** 在 CentOS 上安装 SSH 服务器，以便与 CDO 连接器的 CLI 轻松交互。
- 步骤 8** 运行 yum 更新，然后安装软件包：**open-vm-tools**、**nettools** 和 **bind-utils**
- ```
[root@sdc-vm ~]# yum update -y
[root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```
- 步骤 9** 安装 AWS CLI 软件包 (<https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html>)
- 注释 请勿使用 --user 标志。
- 步骤 10** 安装 Docker CE 软件包 (<https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce>)
- 注释 使用“使用存储库安装”方法。
- 步骤 11** 启动 Docker 服务并使其在启动时启动：
- ```
[root@sdc-vm ~]# systemctl start docker
[root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to /usr/lib/systemd/system/docker.service.
```
- 步骤 12** 创建两个用户：**cdo** 和 **sdc**。cdo 用户将是您登录以运行管理功能的用户（因此您无需直接使用 root 用户），sdc 用户将是运行 CDO 连接器 docker 容器的用户。
- ```
[root@sdc-vm ~]# useradd cdo
[root@sdc-vm ~]# useradd sdc -d /usr/local/cdo
```
- 步骤 13** 配置 sdc 用户以使用 crontab：
- ```
[root@sdc-vm ~]# touch /etc/cron.allow
[root@sdc-vm ~]# echo "sdc" >> /etc/cron.allow
```
- 步骤 14** 为 cdo 用户设置密码。
- ```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```
- 步骤 15** 将 cdo 用户添加到“wheel”组，为其提供管理 (sudo) 权限。
- ```
[root@sdc-vm ~]# usermod -aG wheel cdo
[root@sdc-vm ~]#
```

**步骤 16** 安装 Docker 时，会创建一个用户组。根据 CentOS/Docker 的版本，它可能被称为 “docker” 或 “dockerroot”。检查 `/etc/group` 文件以查看创建的组，然后将 `sdc` 用户添加到此组。

```
[root@sdc-vm ~]# grep docker /etc/group
docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

**步骤 17** 如果 `/etc/docker/daemon.json` 文件不存在，请创建该文件，并使用以下内容填充。创建后，重新启动 Docker 后台守护程序。

**注释** 确保在 “组” 项中输入的组名称与 [步骤 16](#) 匹配。

```
[root@sdc-vm ~]# cat /etc/docker/daemon.json
{
  "live-restore": true,
  "group": "docker"
}
[root@sdc-vm ~]# systemctl restart docker
[root@sdc-vm ~]#
```

**步骤 18** 如果您当前使用的是 vSphere 控制台会话，请切换到 SSH 并以 `cdo` 用户身份登录。登录后，更改为 `sdc` 用户。当系统提示输入密码时，请输入 `cdo` 用户的密码。

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

**步骤 19** 将目录更改为 `/usr/local/cdo`。

**步骤 20** 创建一个名为 `bootstrapdata` 的新文件，并将部署向导步骤 1 中的引导程序数据粘贴到此文件中。保存文件。您可以使用 `vi` 或 `nano` 创建该文件。

## Deploy an On-Premises Secure Event Connector



**i** SEC will be deployed on a new VM

**Step 1**

Download the [CDO Connector VM](#) and follow the [documentation](#) to deploy the CDO VM on vSphere. You will be prompted for "CDO Bootstrap Data". Copy the data below and paste it into the CDO Bootstrap Data input field in vSphere.

CDO Bootstrap Data

```
Q0RPX1RPS0V0PSJ1eUp0YkdjaU9pS1NVekKxTm1Jc01uUjVjQ0k2SWtwWFZDSjkuZX1KM1pYSW1PaU
13SW13aWMYtnZjR1VpT2xzaWRISjFjM1FpTENKeVpXRmtJaXdpZDNKcGRHVW1MQ0poTTJVMVkyVTBa
aTAzTWpGa0xUUhmaVfV0T1dNd05DMH10VGRpT1R0aE1qZzFPR1VpWfN3aV1XMX1Jam9pYzJGdGJDSX
NjBkp2YkdWek1qcGJJbEpQVEVWZ1UxV1FSVkpUUVVST1NVNG1YU3dpYVh0ek1qb21hWFJrSW13aVky
eDFjM1JsY2tsa01qb21NU01zSW1sa01qb21abVF3T0dReVpHVXRNM1ZpT1MwMFpEYzRMV0kwW1dNdF
pUWXh0V0UyWmpjNFkyUm1JaXdpYzNWaWFtVmpkR1I1Y0dVaU9pSjFjM1Z5SW13aWfUUnBJam9pTURB
VacmI0YVFLSjFTdnJ5RjVfZ2FqajZfZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZX1MT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXR1QTFsYme3Vkn0Up4bk9RS1pqaW
1rdDNsYnRRBDNrTHMxeWduaXdVU1RuWkQxM0c5T2FJWExCQ093T3NESGdNeh16UU13ZWJVNUdGT2RS
NfN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YwDpbmCuZGV2LmxvY2toYXJ0Lm
1vIgpDRE9fVEV0QU5UPSJDRE9fY21zY28tYW1hbGxpbYIKQ0RPX0JPT1RTVFJBUf9VUkw9Imh0dHBz
0i8vc3RhZ21uZy5kZXlYubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY21zY28tYW1hbGxpbY
IKT05MwV9FVkvOVE10Rz0idHJ1ZSIK
```

Copy CDO Bootstrap Data



Cancel

OK

**步骤 21** 引导程序数据采用 base64 编码。对其进行解码并将其导出到名为 **extractedbootstrapdata** 的文件

```
[sdc@sdc-vm ~]$ base64 -d /usr/local/cdo/bootstrapdata > /usr/local/cdo/extractedbootstrapdata
[sdc@sdc-vm ~]$
```

运行 **cat** 命令以查看解码后的数据。命令和解码后的数据应如下所示：

```
[sdc@sdc-vm ~]$ cat /usr/local/cdo/extractedbootstrapdata
CDO_TOKEN=<token string>"
CDO_DOMAIN="www.defenseorchestrator.com"
CDO_TENANT="<tenant-name>"
<CDO_URL>/sdc/bootstrap/CDO_acm="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"

ONLY_EVENTING="true"
```

**步骤 22** 运行以下命令，将解码的引导程序数据部分导出到环境变量。

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > secenv && source secenv
[sdc@sdc-vm ~]$
```

**步骤 23** 从 CDO 下载引导程序捆绑包。

```
[sdc@sdc-vm ~]$ curl -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL" -o $CDO_TENANT.tar.gz
100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
[sdc@sdc-vm ~]$ ls -l /usr/local/cdo/*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/cdo/CDO_<tenant_name>
```

**步骤 24** 解压缩 CDO 连接器 tarball，并运行 bootstrap\_sec\_only.sh 文件以安装 CDO 连接器软件包。

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/cdo/tenant-name-SDC
<snipped - extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$ /usr/local/cdo/bootstrap/bootstrap_sec_only.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
toolkit.sh
common.sh
es_toolkit.sh
sec.sh
healthcheck.sh
troubleshoot.sh
no crontab for sdc
-bash-4.2$ crontab -l
*/5 * * * * /usr/local/cdo/toolkit/es_toolkit.sh upgradeEventing 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
0 2 * * * sleep 30 && /usr/local/cdo/toolkit/es_toolkit.sh es_maintenance 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

### 下一步做什么

请继续 [您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置](#)，第 55 页。

## 您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置

如果您在自己的 CentOS 7 虚拟机上安装了 CDO 连接器，则需要执行以下附加配置程序之一，以允许事件到达 SEC。

- 在 CentOS 7 虚拟机上禁用 `firewalld` 服务。这与思科提供的 SDC VM 的配置相匹配。
- 允许 `firewalld` 服务运行并添加防火墙规则以允许事件流量到达 SEC，第 56 页。这是一种允许入站事件流量的更精细的方法。

### 准备工作：

这是安装和配置 SEC 所需完成的三个步骤中的第二步。如果尚未完成这些配置，请完成 [使用 VM 映像安装 CDO 连接器以支持 SEC](#)，第 50 页。

完成此处所述的其中一项其他配置更改后，请完成在 [CDO 连接器虚拟机上安装安全事件连接器](#)

### 在 CentOS 7 虚拟机上禁用 `firewalld` 服务

1. 以“cdo”用户身份登录 SDC VM 的 CLI。

2. 停止 `firewalld` 服务，然后确保该服务在 VM 后续重新启动时保持禁用。如果系统提示，请输入 `cdo` 用户的密码：

```
[cdo@SDC-VM ~]$ sudo systemctl stop firewalld
cdo@SDC-VM ~]$ sudo systemctl disable firewalld
```

3. 重新启动 `Docker` 服务，以便将 `Docker` 特定条目重新插入本地防火墙：

```
[cdo@SDC-VM ~]$ sudo systemctl restart docker
```

4. 继续在 [CDO 连接器虚拟机上安装安全事件连接器](#)。

### 允许 `firewalld` 服务运行并添加防火墙规则以允许事件流量到达 `SEC`

1. 以“`cdo`”用户身份登录 SDC VM 的 CLI。
2. 添加本地防火墙规则，以便允许从配置的 TCP、UDP 或 NSEL 端口到 `SEC` 的传入流量。有关 `SEC` 使用的端口，请参阅[查找用于安全日志记录分析 \(SaaS\) 的设备 TCP、UDP 和 NSEL 端口](#)。如果系统提示，请输入 `cdo` 用户的密码。以下是命令的示例。您可能需要指定不同的端口值。

```
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10125/tcp
cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10025/udp
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10425/udp
```

3. 重新启动 `firewalld` 服务，以便让新的本地防火墙规则始终保持激活：

```
[cdo@SDC-VM ~]$ sudo systemctl restart firewalld
```

4. 继续在 [CDO 连接器虚拟机上安装安全事件连接器](#)。

## 在 CDO 连接器虚拟机上安装安全事件连接器

### 开始之前

这是安装和配置安全事件连接器 (SEC) 所需完成的三个步骤中的第三步。如果尚未完成，请先完成以下两项任务，然后再继续执行此程序：

- [使用 VM 映像安装 CDO 连接器以支持 SEC，第 50 页](#)
- [您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置，第 55 页](#)

**步骤 1** 登录 CDO。

**步骤 2** 从 CDO 菜单中，选择 **工具和服务 (Tools & Services) > 安全连接器 (Secure Connectors)**。

**步骤 3** 选择您使用上述必备条件中的程序安装的 CDO 连接器。在“安全连接器” (Secure Connectors) 表中，它将被称为“安全事件连接器” (Secure Event Connector)。

**步骤 4** 点击右侧“操作”窗格中的 **部署现场安全事件连接器**。

**步骤 5** 在向导的 **步骤 2** 中，点击复制 **SEC 引导程序数据 (Copy SEC Bootstrap Data)** 的链接。

Deploy an On-Premises Secure Event Connector
✕

```

dRaU9pSmhNM1UxWTJVMFppMDNNakZrTFRSaFpUVXRPV013TkMweU5UZG10VE5oTWpnMU9HVW1MQ0pq
YkdsbGJuUmZhV1FpT2lKaGNHa3RZMnhwW1c1MEluMC5tTzh0bTZMz1N6cjI4b1ZGZERqYjJNRzVqUE
ZmYTZYzVsRjRITT1teVVEVzh2Qk5FWW44c3V0Z3NTQ0o0TH15N0xzVGsydEx4N05nbS00STB6SmZ6
aWdQTKRiV1RsRW1tcjI5SkFVZ2NBWEhySkdzckMREszUnJUM0hZU3JkZ21Hd1dGb3FwWUdZnkJHRU
VacmI0YVFLSjFTdnJ5RjVFZ2FqajZFZkNVaERNMUE3Q3c1Q0p1Sn1JmNFZbGpNUzBXeVg3Nm9KeTQ2
ZX1MT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXR1QTFsYmE3VkxN0Up4bk9RS1pqaW
1rdDNsYnRRbDNrTHMxeWduaXdVU1RuWkQxM0c5T2FJWExCQ093T3NESGdNeH16UU13ZWJVNUdGT2RS
NfN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YwdbmZGV2LmXvY2toYXJ0Lm
1vIgpDRE9fVEV0QU5UPSJDRE9fY2lZy28tYW1hbGxpbYIKQ0RPX0JPT1RTVFJBU9VUkw9Imh0dHBz
O18vc3RhZ21uZy5kZXlyubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY2lZy28tYW1hbGxpbY
IKT05MMV9FvkVOVE10Rz0idHJ1ZSIK

```

[Copy CDO Bootstrap Data](#)

---

**Step 2**

Read the [instructions](#) about deploying the Secure Event Connector on vSphere.  
Copy the bootstrap data below and paste it when prompted for "SEC bootstrap Data".

**⚠ The SEC bootstrap data is valid until 10/13/2021, 10:44:14 AM**

```

U1NFX0RFVklDRV9JRD0iZTBhZTJkNmMtMDdhYv00Y2JkLWEzNWQtOGYzZDZkMiq1ZmU3IqpTU0VfRE
U0VfT1RQPSI5Y2IzNTI4ZWZlMzg0TQ2NjViMDFkZmEyYjUyMGUxNSIKVEV0QU5UX05BTUU9IkNET1
9jaXNjby1hbWFSbG1vIg==

```

[Copy SEC Bootstrap Data](#) ←

---

**Step 3**

Verify the connection status of the new SEC by exiting this dialog and checking the "Last Heartbeat" information.

Cancel OK

**步骤 6** 使用 SSH 连接到安全连接器并以 **cdo** 用户身份登录。

**步骤 7** 登录后，切换到 **sdC** 用户。当系统提示输入密码时，请输入“cdo”用户的密码。以下是这些命令的示例：

```

[cdo@sdC-vm ~]$ sudo su sdC
[sudo] password for cdo: <type password for cdo user>
[sdc@sdC-vm ~]$

```

**步骤 8** 在提示符后，运行 **sec.sh** 安装脚本：

```

[sdc@sdC-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup

```

**步骤 9** 在提示符的末尾，粘贴您在步骤 4 中复制的引导程序数据，然后按 **Enter** 键。

```

Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFuIyIOHKNkJbKhvhgyRStwterTyufGUIhoJpojP9U0oiUY8VHGHFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkbB=

```

载入 SEC 后，sec.sh 将运行脚本来检查 SEC 的运行状况。如果所有运行状况检查均为“绿色”，则运行状况检查会向事件日志发送示例事件。示例事件在事件日志中显示为名为“sec-health-check”的策略。

```

=====
Running SEC health check for tenant ██████████
-----
SEC cloud URL ██████████ is: Reachable
-----
SEC Connector status: Active
-----
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
-----
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
=====

```

如果您收到注册失败或 SEC 载入失败的消息，请转至[安全事件连接器载入故障排除](#)。

如果您收到成功消息，请点击[部署现场安全事件连接器 \(Deploy an ON-Premise Secure Event Connector\)](#)对话框中的完成 (Done)。您已在虚拟机映像上安装 SEC。

**步骤 10** 继续执行“下一步操作”。

#### 下一步做什么

返回此程序以继续实施 SAL SaaS: [为 ASA 设备实施安全日志记录分析 \(SaaS\)](#)，第 10 页。

#### 相关信息：

- [对安全设备连接器进行故障排除](#)
- [安全事件连接器故障排除](#)
- [安全事件连接器载入故障排除](#)
- [SEC 注册失败故障排除](#)

## 使用 Terraform 模块在 AWS VPC 上安装安全事件连接器

### 开始之前

- 要执行此任务，您必须在 CDO 租户上启用 SAL。本部分假定您已拥有 SAL 许可证。如果还没有，请购买思科安全和分析日志记录、日志记录和故障排除许可证。
- 确保您已安装新的 SEC。要创建新的 SEC，请参阅[在 SDC 虚拟机上安装安全事件连接器](#)，第 40 页。
- 在安装 SEC 时，请确保记下 CDO 引导程序数据和 SEC 引导程序数据。

**步骤 1** 转到 Terraform 注册表中的[安全事件连接器 Terraform 模块](#)，然后按照说明将 SEC Terraform 模块添加到 Terraform 代码。

**步骤 2** 应用 Terraform 代码。

**步骤 3** 确保打印 instance\_id 和 sec\_fqdn 输出，因为稍后在程序中会用到它们。

**注释** 要对 SEC 进行故障排除，您必须使用 AWS 系统管理器会话管理器 (SSM) 来连接到 SEC 实例。请参阅 [AWS 系统管理器会话管理器](#) 文档，了解有关使用 SSM 连接到实例的更多信息。

出于安全原因，使用 SSH 连接到 SDC 实例的端口不会被公开。

**步骤 4** 要启用从 ASA 向 SEC 发送日志的功能，请使用 **步骤 3** 的输出来运行以下命令，以获取您创建的 SEC 的证书链并删除枝叶证书：

```
rm -f /tmp/cert_chain.pem && openssl s_client -showcerts -verify 5 -connect <FQDN>:10125 < /dev/null
| awk '/BEGIN CERTIFICATE/,/END CERTIFICATE/{ if(/BEGIN CERTIFICATE/){a++; out="/tmp/cert_chain.pem";
if(a > 1) print >>out}'
```

**步骤 5** 将 /tmp/cert\_chain.pem 的内容复制到剪贴板。

**步骤 6** 使用以下命令记录 SEC 的 IP 地址：

```
nslookup <FQDN>
```

**步骤 7** 登录 CDO 并开始添加新的信任点对象。有关详细信息，请参阅 [添加受信任 CA 证书对象](#)。在点击添加 (Add)，请确保取消选中其他选项 (Other Options) 中的在基本限制扩展中启用 CA 标志 (Enable CA flag in basic constraints extension) 复选框。

**步骤 8** 点击添加 (Add)，复制 CDO 生成的 CLI 命令在安装证书 (Install Certificate) 页面中，然后点击取消 (Cancel)。

**步骤 9** 在注册终端 (enrollment terminal) 下方，在文本剪贴板中添加 no ca-check。

**步骤 10** 通过 SSH 连接到 ASA 设备或使用 CDO 中的 ASA CLI 选项并执行以下命令：

```
DataCenterFW-1> en
Password: *****
DataCenterFW-1# conf t
DataCenterFW-1(config)# <paste your modified ASA CLIs here and press Enter>
DataCenterFW-1(config)# wr mem
Building configuration...
Cryptochecksum: 6634f35f 4c5137f1 ab0c5cdc 9784bdb6
```

### 下一步做什么

您可以使用 AWS SSM 来检查 SEC 是否正在接收数据包：

您现在应该会看到类似于以下内容的日志：

```
time="2023-05-10T17:13:46.135018214Z" level=info msg="[ip-10-100-5-19.ec2.internal][util.go:67
plugin.createTickers:func1] Events - Processed - 6/s, Dropped - 0/s, Queue size - 0"
```

## 取消调配思科安全分析和日志记录 (SaaS)

如果允许思科安全分析和日志记录 (SaaS) 付费许可证失效，则您有 90 天的宽限期。如果您在此宽限期内续订付费许可证，则服务不会发生中断。

否则，如果您允许 90 天的宽限期，系统将清除所有的客户数据。您无法再从“事件日志记录” (Event Logging) 页面查看 ASA 或 FTD 事件，也无法将动态实体建模行为分析应用于您的 ASA 或 FTD 事件和网络流数据。

## 删除安全事件连接器

**警告：**此程序会从安全设备连接器中删除安全事件连接器。这样做会阻止您使用安全日志分析(SaaS)。这一操作不可逆。如果您有任何问题或疑虑，请在执行此操作之前[联系 CDO 支持](#)。

从安全设备连接器中删除安全事件连接器的过程可分为两步：

1. 从 [CDO](#) 中删除 SEC。
2. 从 [SDC](#) 中删除 SEC 文件。

下一步：继续从 [CDO](#) 中删除 SEC

### 从 CDO 中删除 SEC

开始之前

请参阅[删除安全事件连接器](#)，第 60 页。

**步骤 1** 登录 CDO。

**步骤 2** 从 CDO 菜单中，选择 **工具和服务 (Tools & Services) > 安全连接器 (Secure Connectors)**。

**步骤 3** 选择设备类型为安全事件连接器 (**Secure Event Connector**) 的行。

**警告：**要小心。请勿选择您的安全设备连接器。

**步骤 4** 在“操作” (Actions) 窗格中，点击删除 (**Remove**)。

**步骤 5** 点击确定 (**OK**) 以确认您删除安全事件连接器的意图。

下一步做什么

请继续从 [SDC](#) 中删除 SEC 文件，第 60 页。

### 从 SDC 中删除 SEC 文件

这是从 SDC 中删除安全事件连接器程序的第二部分。开始前，请参阅[删除安全事件连接器](#)，第 60 页。

**步骤 1** 打开虚拟机监控程序并启动 SDC 的控制台会话。

**步骤 2** 切换到 SDC 用户。

```
[cdo@tenant toolkit]$sudo su sdc
```

**步骤 3** 在提示符后键入以下命令之一：

- 如果您仅管理自己的租户：

```
[sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove
```

- 如果您管理多个租户，请将 CDO\_ 添加到租户名称的开头。例如：

```
[sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove CDO_[tenant_name]
```

**步骤 4** 确认您打算删除 SEC 文件。

## 调配思科安全云分析门户

所需许可证： 日志记录分析和检测 或 全面网络分析和监控

如果您购买了日志记录分析和检测或全局网络分析和监控许可证，则在部署和配置安全事件连接器 (SEC) 后，必须将安全云分析门户与 CDO 门户关联，以查看安全云分析警报。购买许可证时，如果您有安全云分析门户，则可以提供安全云分析门户名称，并立即将其链接到您的 CDO 门户。

否则，您可以从 CDO UI 请求新的安全云分析门户。首次访问安全云分析警报时，系统会将您引导至请求安全云分析门户的页面。向请求此门户的用户授予门户中的管理员权限。

**步骤 1** 从 CDO 菜单中，选择 **分析 (Analytics) > 安全云分析 (Secure Cloud Analytics)** 以在新窗口中打开安全云分析 UI。

**步骤 2** 点击**开始免费试用 (Start Free Trial)** 以调配安全云分析门户并将其与您的 CDO 门户关联。

**Note** 请求门户后，调配可能需要几个小时。

在继续下一步之前，请确保您的门户已调配。

1. 从 CDO 菜单中，选择 **分析 (Analytics) > 安全云分析 (Secure Cloud Analytics)** 以在新窗口中打开安全云分析 UI。
2. 您有以下选择：
  - 如果您请求了安全云分析门户，并且系统指出它仍在调配门户，请稍后再尝试访问警报。
  - 如果已调配安全云分析门户，请输入您的用户名和密码，然后点击**登录 (Sign in)**。



**Note** 管理员用户可以邀请其他用户在安全云分析门户中创建账户。有关详细信息，请参阅[从 CDO 查看 Cisco Secure Cloud Analytics 警报, on page 63](#)。

### What to do next

- 如果您购买了日志记录分析和检测许可证，则配置已完成。如果要从安全云分析门户 UI 查看 CDO 集成状态或传感器运行状况，请参阅[在安全云分析中查看传感器运行状况和 CDO 集成状](#)

态, on page 62 了解更多信息。如果要使用安全云分析门户中的警报, 请参阅[从 CDO 查看 Cisco Secure Cloud Analytics 警报, on page 63](#)和[使用基于防火墙事件的警报](#)以了解详细信息。

- 如果您购买了[全面网络分析和监控](#)许可证, 请将一个或多个安全云分析传感器部署到您的内部网络, 以将网络流数据传递到云。如果要监控基于云的网络流数据, 请将基于云的部署配置为将流数据传递到安全云分析。有关详细信息, 请参阅[用于全面网络分析和报告的思科安全云分析传感器部署, on page 62](#)。

## 在安全云分析中查看传感器运行状况和 CDO 集成状态

### 传感器状态

所需许可证: 日志记录分析和检测 或 全面网络分析和监控

在思科安全云分析 Web UI 中, 您可以从“传感器列表”(Sensor List) 页面查看 CDO 集成状态和已配置的传感器。CDO 集成是只读连接事件传感器。Stelathwatch 云在主菜单中提供传感器的整体运行状况:

- 绿色云图标 (☁) - 已与所有传感器和 CDO (如果已配置) 建立连接
- 黄色云图标 (☁) - 已与某些传感器或 CDO (如果已配置) 建立连接, 但一个或多个传感器未正确配置
- 红色云图标 (☁) - 与所有已配置的传感器和 CDO (如果已配置) 的连接丢失

每个传感器或 CDO 集成, 绿色图标表示连接已建立, 红色图标表示连接丢失。

---

**步骤 1** 1. 在安全云分析门户 UI 中, 选择设置 (⚙) > 传感器 (Sensors)。

**步骤 2** 选择传感器列表 (Sensor List)。

---

## 用于全面网络分析和报告的思科安全云分析传感器部署

### 安全云分析传感器概述和部署

所需许可证: 全面网络分析和监控

如果您获得了[全面网络分析和监控](#)许可证, 则在调配安全云分析门户后, 您可以:

- 在本地网络中部署和配置安全云分析传感器, 以将网络流数据传递到云进行分析。
- 配置基于云的部署, 以将网络流日志数据传递到安全云分析进行分析。

网络边界的防火墙收集有关内部网络和外部网络之间流量的信息, 而安全云分析传感器收集有关内部网络流量的信息。



**Note** FDM 管理 Secure Firewall Threat Defense 设备可以配置为传递 NetFlow 数据。部署传感器时，请勿将其配置为从您还配置为将事件信息传递到 CDO 的任何 FDM 管理 Secure Firewall Threat Defense 设备传递 NetFlow 数据。

有关传感器部署说明和建议，请参阅《[安全云分析传感器安装指南](#)》。

有关基于云的部署配置说明和建议，请参阅《[安全云分析公共云监控指南](#)》。



**Note** 您还可以查看安全云分析门户 UI 中的说明，以配置传感器和基于云的部署。

有关安全云分析的详细信息，请参阅《[安全云分析免费试用指南](#)》。

#### 后续步骤

- 继续执行 [从 CDO 查看 Cisco Secure Cloud Analytics 警报, on page 63](#)。

## 从 CDO 查看 Cisco Secure Cloud Analytics 警报

所需许可证：日志记录分析和检测 或 全面网络分析和监控

虽然您可以在“事件日志记录”(Events logging)页面上查看防火墙事件，但无法从 CDO 门户 UI 中查看 Cisco Secure Cloud Analytics 警报。您可以使用“安全分析”(Security Analytics)菜单选项从 CDO 交叉启动安全云分析门户，并查看从防火墙事件数据（如果启用了**全面网络分析和监控 (Total Network Analytics and Monitoring)**，则从网络流数据）生成的警报。“安全分析”(Security Analytics)菜单选项会显示一个标记，其中包含处于打开的工作流程状态的安全云分析警报的数量（如果有一个或多个）。

如果您使用安全分析和日志记录许可证生成安全云分析警报，并且已调配新的安全云分析门户，请登录 CDO，然后使用 Cisco Security Cloud Sign On 来启动安全云分析。您还可以通过其 URL 直接访问安全云分析门户。

有关详细信息，请参阅 [Cisco Security Cloud Sign On](#)。

## 邀请用户加入您的安全云分析门户

请求安全云分析门户调配的初始用户在安全云分析门户中具有管理员权限。该用户可以通过邮件邀请其他用户加入门户。如果这些用户没有 Cisco Security Cloud Sign On 凭证，可以使用邀请邮件中的链接创建这些凭证。然后，用户可以在从 CDO 到 Secure Cloud Analytics 的交叉启动期间使用 Cisco Security Cloud Sign On 凭证登录。

要通过邮件邀请其他用户访问 Secure Cloud Analytics 门户，请执行以下操作：

- 
- 步骤 1 以管理员身份登录 Secure Cloud Analytics 门户。
  - 步骤 2 选择 Settings Account Management User Management。 > >
  - 步骤 3 输入邮件地址。
  - 步骤 4 点击邀请 (Invite)。
- 

## 从 CDO 交叉启动到 Cisco Secure Cloud Analytics

要从 CDO 查看安全警报，请执行以下操作：

- 
- 步骤 1 登录到 CDO 门户。
  - 步骤 2 从 CDO 菜单中，选择 分析 (Analytics) > 安全云分析 (Secure Cloud Analytics)。
  - 步骤 3 在 Cisco Secure Cloud Analytics 界面中，选择监控 (Monitor) > 警报 (Alerts)。
- 

## 思科安全云分析和动态实体建模

**所需许可证 (Required License):** 日志记录分析和检测 (Logging Analytics and Detection) 或全面网络分析和监控 (Total Network Analytics and Monitoring)

安全云分析是一种软件即服务 (SaaS) 解决方案，可用于监控您的本地和基于云的网络部署。通过从源（包括防火墙事件和网络流数据）收集有关网络流量的信息，它会创建有关流量的观察结果，并根据其流量模式自动识别网络实体的角色。使用此信息与其他威胁情报来源（例如 Talos）相结合，安全云分析会生成警报，警告可能存在恶意行为。除警报外，安全云分析还提供网络和主机可视性以及所收集的情景信息，为您研究警报和查找恶意行为的来源提供更好的基础。

### 动态实体建模

动态实体建模可通过对防火墙事件和网络流数据执行行为分析来跟踪网络状态。在 Cisco Secure Cloud Analytics 环境中，实体是指可以随时间推移进行跟踪的对象，例如网络上的主机或终端。动态实体建模根据实体传输的流量及其在网络上执行的活动，收集实体的相关信息。与日志记录分析和检测许可证集成的 Cisco Secure Cloud Analytics 可以从防火墙事件和其他流量信息中进行提取，以便确定实体通常传输的流量类型。如果您购买了全面网络分析和监控许可证，则 Cisco Secure Cloud Analytics 还可以在对实体流量进行建模时纳入 NetFlow 和其他流量信息。Cisco Secure Cloud Analytics 会随着时间的推移更新这些模型，因为实体会继续发送流量，并且可能会发送不同的流量，从而保持每个实体的最新模型。根据这些信息，Cisco Secure Cloud Analytics 可以识别：

- 实体的角色，即实体通常执行的操作的描述符。例如，如果实体发送通常与邮件服务器关联的流量，Cisco Secure Cloud Analytics 会为该实体分配邮件服务器角色。角色/实体关系可以是多对一，因为实体可以履行多种角色。

- 对实体的观察结果，即有关实体在网络上的行为的事实，例如与外部 IP 地址建立的心跳连接或与另一个实体建立的远程访问会话。如果与 CDO 集成，则可以从防火墙事件中获取这些事实。如果您还购买了全面的网络分析和监控许可证，则系统还可以从 NetFlow 获取事实，并从防火墙事件和 NetFlow 中生成观察结果。观察结果本身并不具有超出其所代表的事实的意义。一个典型的客户可能有数千个观察结果和若干个警报。

### 警报和分析

Cisco Secure Cloud Analytics 会根据角色、观察结果和其他威胁情报的组合生成警报，这些警报是可操作项目，代表系统标识的可能的恶意行为。请注意，一个警报可能代表多个观察结果。如果防火墙记录了与同一连接和实体相关的多个连接事件，则可能只会生成一个警报。

例如，新的内部设备观察结果本身并不构成可能的恶意行为。但是，随着时间的推移，如果实体传输的流量与域控制器一致，则系统会向该实体分配域控制器角色。如果实体随后使用异常端口与之前未建立连接的外部服务器建立了连接，并且传输了大量的数据，则系统将记录新的大型连接（外部）观察结果和异常域控制器观察结果。如果该外部服务器被识别为一个 Talos 监视列表，则所有这些信息的组合将导致 Cisco Secure Cloud Analytics 生成此实体行为的警报，从而提示您采取进一步措施来研究和补救恶意行为。

在 Cisco Secure Cloud Analytics Web 门户 UI 中打开警报时，您可以查看导致系统生成该警报的支持性观察结果。您还可以从这些观察结果中查看有关所涉实体的其他背景信息，包括它们传输的流量以及外部威胁情报（如果可用）。您还可以查看实体涉及的其他观察结果和警报，然后确定此行为是否与其他潜在恶意行为相关。

请注意，在 Cisco Secure Cloud Analytics 中查看和关闭警报时，无法允许或阻止来自 Cisco Secure Cloud Analytics UI 的流量。如果在主动模式下部署设备，则必须更新防火墙访问控制规则以允许或阻止流量；如果在被动模式下部署防火墙，则必须更新防火墙访问控制规则。

## 使用基于防火墙事件的警报

所需许可证：日志记录分析和检测 或 全面网络分析和监控

### 警报工作流程

警报的工作流程基于其状态。当系统生成警报时，其默认状态为“待处理”，并且未分配任何用户。当您查看警报总结时，默认情况下会显示所有待处理警报，因为这些都是最需要关注的。

注意：如果您拥有全面网络分析和监控许可证，则警报可以基于从 NetFlow 生成的观察结果、从防火墙事件生成的观察结果或来自两个数据源的观察结果。

查看警报总结时，可以分配和标记警报，以及将其状态更新为初始分类。您可以使用过滤器和搜索功能查找特定警报，也可以显示不同状态的警报或具有不同标记或负责人的警报。您可以将警报的状态设置为“已暂停”，在这种情况下，警报要等暂停期过后才会重新显示在待处理警报列表中。您也可以移除警报的“已暂停”状态，使其再次显示为待处理警报。查看警报时，您可以将其分配给您自己或系统中的其他用户。用户可以搜索分配给其用户名的所有警报。

在警报摘要中，您可以查看警报详细信息页面。此页面允许您查看有关生成此警报的支持性观察结果的其他背景信息，以及有关此警报中涉及的实体的其他背景信息。这些信息可帮助您查明实际问题，以便进一步研究网络上的问题，并且有可能解决恶意行为。

当您在 CDO 中的 Stealthwatch 云 web 门户 UI 和网络中进行研究时，可以进行备注，描述您对警报的发现。这有助于为您的研究创建记录，供您将来参考。

完成分析后，您可以将状态更新为“已关闭”，使其不再默认显示为待处理警报。如果情况发生变化，您还可以在将来重新打开已关闭的警报。

下面介绍有关如何调查给定警报的一般准则和建议。Stealthwatch 云会在记录警报时提供附加背景信息，因此，您可以使用此信息帮助指导调查工作。

这些步骤既不全面，也非包罗万象。它们仅提供一个总体框架来帮助您开始调查警报。

通常，查看警报时可以采取以下步骤：

1. [对待处理警报进行分类, on page 66](#)
2. [暂停警报以供以后分析, on page 67](#)
3. [更新警报以进行进一步调查, on page 67](#)
4. [查看警报并开始调查, on page 68](#)
5. [检查实体和用户, on page 69](#)
6. [使用安全云分析补救问题, on page 70](#)
7. [更新并关闭警报, on page 70](#)

## 对待处理警报进行分类

对待处理警报进行分类，特别是如果要调查多个待处理警报：

- 有关从 CDO 交叉启动和查看警报的详细信息，请参阅[从 CDO 查看 Cisco Secure Cloud Analytics 警报](#)。

询问以下问题：

- 您是否将此警报类型配置为高优先级？
- 您是否为受影响的子网设置了高灵敏度？
- 这是网络上新实体的异常行为吗？
- 实体的正常角色是什么，此警报中的行为与该角色的匹配度如何？
- 这是否是此实体正常行为的异常偏离？
- 如果用户参与其中，这是用户的预期行为还是异常行为？
- 受保护数据或敏感数据是否有被泄露的风险？
- 如果允许此行为继续下去，会对网络产生多严重的影响？

- 如果与外部实体有通信，这些实体过去是否与您网络上的其他实体建立了连接？

如果这是高优先级警报，请考虑将该实体与互联网隔离，或以其他方式关闭其连接，然后再继续调查。

## 暂停警报以供以后分析

当警报的优先级较低（与其他警报相比）时，可将其暂停。例如，如果您的组织将邮件服务器重新定位为 FTP 服务器，并且系统生成紧急配置文件警报（表明一个实体的当前流量匹配了它以前没有匹配的行为概要文件），您可以暂停此警报（因为这是预期行为），并在以后重新访问它。已暂停的警报不会与待处理警报一起显示；您必须专门过滤才能查看这些暂停的警报。

暂停警报：

---

**步骤 1** 点击关闭警报 (Close Alert)。

**步骤 2** 在暂停此警报窗格中，从下拉列表中选择暂停时段。

**步骤 3** 点击保存 (Save)。

---

### What to do next

当您准备好查看这些警报时，可以取消暂停该警报。这会将状态设置为“未处理”(Open)，并在其他“未处理”的警报旁边显示该警报。

取消暂停已暂停的警报：

- 从暂停的警报中，点击取消暂停警报 (Unsnooze Alert)。

## 更新警报以进行进一步调查

打开警报详细信息：

---

**步骤 1** 选择监控 (Monitor) > 警报 (Alerts)。

**步骤 2** 点击警报类型名称。

---

### What to do next

根据您的初始分类和优先级，分配警报并标记：

1. 从被分派人 (Assignee) 下拉列表中选择用户以分配警报，以使用户可以开始调查。
2. 从下拉列表中选择一个或多个标签，以将标签添加到警报，以便更好地对警报进行分类以供将来识别，并尝试在警报中建立长期模式。

3. 输入为此警报添加注释 (**Comment on this alert**)，然后点击注释 (**Comment**) 以根据需要留下注释，以跟踪您的初始发现，并协助分配到警报的人员。警报同时跟踪系统注释和用户注释。

## 查看警报并开始调查

如果您正在查看已分配的警报，请查看警报详细信息以了解 Stealthwatch 云生成警报的原因。查看支持性观察结果，了解这些观察结果对源实体的意义。

请注意，如果警报是基于防火墙事件生成的，则系统不会注意到您的防火墙部署是此警报的来源。

查看此源实体的所有支持性观察结果，以了解其一般行为和模式，并查看此活动是否可能影响着某个长期趋势：

### SUMMARY STEPS

1. 在观察结果控制面板上，点击观察结果类型旁边的箭头图标 (↕)，以查看该类型的所有已记录观察结果。
2. 点击**网络的所有观察结果 (All Observations for Network)** 旁边的箭头图标 (↕)，查看此警报的源实体的所有已记录观察结果。

### DETAILED STEPS

---

**步骤 1** 在观察结果控制面板上，点击观察结果类型旁边的箭头图标 (↕)，以查看该类型的所有已记录观察结果。

**步骤 2** 点击**网络的所有观察结果 (All Observations for Network)** 旁边的箭头图标 (↕)，查看此警报的源实体的所有已记录观察结果。

---

如果要对这些观察结果执行其他分析，请下载逗号分隔值文件中的支持观察结果：

- 在警报详细信息的支持观察结果窗格中，点击 **CSV**。

从观察结果，确定源实体行为是否指示恶意行为。如果源实体与多个外部实体建立了连接，请确定外部实体是否以某种方式相关，例如它们是否都具有相似的地理位置信息，或者它们的 IP 地址是否来自同一子网。

从源实体 IP 地址或主机名称查看有关源实体的其他背景信息，包括它可能涉及的其他警报和观察结果、有关设备本身的信息以及它传输的会话流量类型：

- 从 IP 地址或主机名下拉列表中选择**警报 (Alerts)**，以查看与该实体相关的所有警报。
- 从 IP 地址或主机名下拉列表中选择**观察结果 (Observations)**，以查看与实体相关的所有观察结果。
- 从 IP 地址或主机名下拉列表中选择**设备 (Device)**，以查看有关设备的信息。
- 从 IP 地址或主机名下拉列表中选择**会话流量 (Session Traffic)**，以查看与此实体相关的会话流量。
- 从 IP 地址或主机名下拉列表中选择**复制 (Copy)** 以复制 IP 地址或主机名。

请注意，Stealthwatch 云中的源实体始终位于您的网络内部。将此与防火墙事件中的发起方 IP 进行对比，后者指示发起连接的实体，并且可能位于您的网络内部或外部。

从观察结果中，检查有关其他外部实体的信息。检查地理位置信息，确定是否有任何地理位置数据或 Umbrella 数据标识恶意实体。查看这些实体生成的流量。检查 Talos、AbuseIPDB 或 Google 是否有关于这些实体的任何信息。查找多天的 IP 地址，并查看外部实体与您网络上的实体建立的其他类型的连接。如有必要，请找到这些内部实体，并确定是否有任何证据表明存在攻击活动或意外行为。

查看与源实体建立了连接的外部实体 IP 地址或主机名称的背景信息：

- 从 IP 地址或主机名下拉列表中选择 **IP 流量 (IP Traffic)**，以查看此实体的最近流量信息。
- 从 IP 地址或主机名下拉列表中选择 **会话流量 (Session Traffic)**，以查看此实体的最近会话流量信息。
- 从 IP 地址或主机名下拉列表中选择 **AbuseIPDB**，以查看有关 AbuseIPDB 网页实体的信息。
- 从 IP 地址或主机名下拉列表中选择 **思科 Umbrella (Cisco Umbrella)**，可在 Cisco Umbrella 网站上查看有关此实体的信息。
- 从 IP 地址或主机名下拉列表中选择 **Google 搜索 (Google Search)**，以在 Google 上搜索此 IP 地址。
- 从 IP 地址或主机名下拉列表中选择 **Talos 智能 (Talos Intelligence)**，以查看有关 Talos 网页的信息。
- 从 IP 地址或主机名下拉列表中选择 **将 IP 添加到监视列表 (Add IP to watchlist)**，以将此实体添加到监视列表。
- 从 IP 地址或主机名下拉列表中选择 **查找多天的 IP (Find IP on multiple days)**，以搜索此实体上个月的流量。
- 从 IP 地址或主机名下拉列表中选择 **复制 (Copy)** 以复制 IP 地址或主机名。

请注意，Stealthwatch 云中的连接实体始终位于您的网络外部。将此与防火墙事件中的响应方 IP 进行对比，后者指示响应连接请求的实体，并且可能位于您的网络的内部或外部。

就您的发现进行备注。

- 在警报详细信息中，输入对此警报的注释 (**Comment on this alert**)，然后点击注释 (**Comment**)。

## 检查实体和用户

在 Stealthwatch 云门户 UI 中查看警报后，您可以直接对源实体、可能与此警报相关的任何用户以及其他相关实体执行其他检查。

- 确定源实体在网络上的物理位置或云中的位置，并直接访问它。找到此实体的日志文件。如果它是网络上的物理实体，请访问设备以查看日志信息，并查看是否有任何信息表明是什么导致了此行为。如果它是虚拟实体或存储在云中，请访问日志并搜索与此实体相关的条目。检查日志，了解有关未经授权的登录、未经批准的配置更改等活动的更多信息。

- 检查实体。确定您能否识别实体本身上的恶意软件或漏洞。查看是否发生了一些恶意更改，包括设备是否发生了物理更改，例如插入了未经组织批准的 U 盘。
- 确定所涉及的用户来自您的网络内部还是外部。如果可能，询问他们当时在做什么。如果询问未果，请确定他们是否应该具有访问权限，以及是否发生了导致此行为的情况，例如，离职员工在离开公司之前将文件上传到外部服务器。

就您的发现进行备注：

- 在警报详细信息中，输入**对此警报的注释 (Comment on this alert)**，然后点击**注释 (Comment)**。

## 使用安全云分析补救问题

如果恶意行为导致生成警报，请修复恶意行为。例如：

- 如果恶意实体或用户尝试从网络外部进行登录，请更新防火墙规则和防火墙配置，防止该实体或用户访问您的网络。
- 如果实体尝试访问未经授权或恶意的域，请检查受影响的实体，以确定是否为恶意软件导致的原因。如果存在恶意 DNS 重定向，请确定网络上的其他实体是否受到影响，或是否是僵尸网络的一部分。如果用户有意这样做，请确定是否存在合法原因，例如测试防火墙设置。更新防火墙规则和防火墙配置，以防止进一步访问该域。
- 如果实体表现出与历史实体模型行为不同的行为，请确定是否有意更改行为。如果不是故意的，请检查网络上的其他授权用户是否应对更改负责。更新防火墙规则和防火墙配置，以解决涉及与网络外部实体的连接的意外行为。
- 如果发现漏洞或漏洞攻击，请更新或修补受影响的实体以消除漏洞，或更新防火墙配置以防止未经授权的访问。确定网络上的其他实体是否可能受到类似影响，并向这些实体应用相同的更新或补丁。如果漏洞或漏洞攻击当前没有修补程序，请联系相应的供应商告知他们。
- 如果发现恶意软件，请隔离实体并删除恶意软件。查看防火墙文件和恶意软件事件，以确定网络上的其他实体是否存在风险，更新实体以防止此恶意软件传播。使用有关此恶意软件或导致此恶意软件的实体的信息更新安全情报。更新您的防火墙访问控制以及文件和恶意软件规则，以防止此恶意软件将来感染您的网络。根据需要向供应商发出警报。
- 如果恶意行为导致数据泄露，请确定发送到未授权源的数据的性质。对于未经授权的数据泄露，请遵循组织协议进行操作。更新您的防火墙配置，以防止此来源未来的数据泄露尝试。

## 更新并关闭警报

根据您的调查结果添加其他标签：

---

**步骤 1** 在 Cisco Secure Cloud Analytics 门户 UI 中，选择**监控 (Monitor) > 警报 (Alerts)**。

**步骤 2** 从下拉列表中选择一个或多个标签。

---

添加描述调查结果的最终注释，以及所采取的任何补救步骤：

- 在警报的详细信息中，输入为此警报添加注释 (**Comment on this alert**)，然后点击注释 (**Comment**)。

关闭警报，然后将其标记为有用或无用：

1. 在警报的详细信息中，点击**关闭警报 (Close Alert)**。
2. 如果警报有用，请选择**是 (Yes)**；如果警报无用，请点击**否 (No)**。请注意，这并不一定意味着该警报是由恶意行为导致的，而只是表示它对您的组织有所帮助。
3. 点击**保存 (Save)**。

### What to do next

#### 重新打开已关闭的警报

如果您发现与已关闭警报相关的其他信息，或者想要添加与该警报相关的更多备注，则可以将其重新打开，并将状态更改为“待处理”。然后，您可以根据需要对警报进行更改，并在其他调查完成后再次将其关闭。

重新打开已关闭的警报：

- 在已关闭警报的详细信息中，点击**重新打开警报 (Reopen Alert)**。

## 修改警报优先级

**所需许可证 (Required License):** 日志记录分析和检测 (**Logging Analytics and Detection**) 或全面网络分析和监控 (**Total Network Analytics and Monitoring**)

警报类型具有默认优先级，这会影响系统对生成此类警报的敏感程度。根据思科情报和其他因素，警报的优先级默认为低或正常。根据您的网络环境，您可能希望重新确定警报类型的优先级，以强调您关注的某些警报。您可以将任何风险通告类型配置为低、正常或高优先级。

- 选择**监控 (Monitor) > 警报 (Alerts)**。
- 点击设置下拉图标 ()，然后选择警报类型和优先级。👇
- 点击警报类型旁边的编辑图标 ()，然后选择低、中或高以更改优先级。✎

## 查看实时事件

实时事件页面显示与您输入的**在事件日志记录页面中搜索和过滤事件**匹配的最近 500 个事件。如果“实时事件”页面最多显示 500 个事件，并且有更多事件传入，则 CDO 会显示最新的实时事件，并将最早的实时事件传输到“历史事件”页面，使实时事件总数保持为 500。执行该传输大约需要一分钟。如果未添加过滤条件，您将看到配置为记录事件的规则生成的所有最新实时 500 事件。

事件的时间戳以查看事件的 CDO 管理员的本地时间显示。

更改过滤条件（无论是正在播放还是已暂停的实时事件）会清除事件屏幕并重新启动收集过程。

要在 CDO 事件查看器中查看实时事件，请执行以下操作：

---

**步骤 1** 在导航窗格中，选择 **分析 (Analytics) > 事件日志记录 (Event Logging)**。

**步骤 2** 点击**实时 (Live)** 选项卡。

---

### What to do next

通过阅读了解如何播放和暂停事件。

相关信息：

- [播放/暂停实时事件, on page 72](#)
- [查看历史事件, on page 73](#)
- [自定义事件视图, on page 73](#)

## 播放/暂停实时事件

您可以在实时事件传入时“播放”或“暂停”。如果实时事件正在“播放”，则 CDO 将按接收顺序来显示与事件查看器中指定的过滤条件匹配的事件。如果事件已暂停，则在您重新开始播放实时事件之前，CDO 不会更新“实时事件” (Live events) 页面。当您重新开始播放事件时，CDO 会从您重新开始播放事件的位置开始在“实时” (Live) 页面中填充事件。它不会回填您遗漏的内容。

要查看 CDO 收到的所有事件（无论您已播放还是暂停），请点击“历史” (Historical) 选项卡。

### 自动暂停实时事件

在连续显示事件约 5 分钟后，CDO 会警告您即将暂停实时事件流。届时，您可以点击该链接以继续流传输其他 5 分钟的实时事件，或者允许流停止。在准备就绪后，您可以重新启动实时事件流。

### 接收和报告事件

在实时事件查看器中，安全事件连接器 (SEC) 接收事件和 CDO 发布事件之间可能会存在一点延迟。您可以在“实时” (Live) 页面上查看差距。事件的时间戳是 SEC 收到的时间。

Events

Search by event fields and values

Historical **Live**

Date/Time	Event Type
⚙️ Waiting for matching events after 1:38:40 PM.	
May 31, 2019 1:33:35 PM	Connection
May 31, 2019 1:33:36 PM	Connection
May 31, 2019 1:33:44 PM	Connection

## 查看历史事件

实时事件页面会显示与您输入的[在事件日志记录页面中搜索和过滤事件](#)匹配的 500 个最新事件。超出最近的 500 个事件将被传输到历史事件表。执行该传输大约需要一分钟。然后，您可以过滤已存储的所有事件，以便找到要查找的事件。

要查看历史事件，请执行以下操作：

**步骤 1** 在导航窗格中，选择 **分析 (Analytics) > 事件日志记录 (Event Logging)**。

**步骤 2** 点击**历史 (Historical)** 选项卡。默认情况下，当您打开历史事件表时，过滤器会被设置为显示最近一小时内收集的事件。

事件属性与 Firepower 设备管理器 (FDM) 或自适应安全设备管理器 (ASDM) 报告的属性基本相同。

- 有关 Firepower 威胁防御事件属性的详尽说明，请参阅[思科 FTD 系统日志消息](#)。
- 有关 ASA 事件属性的详尽说明，请参阅[思科 ASA 系列系统日志消息](#)。

## 自定义事件视图

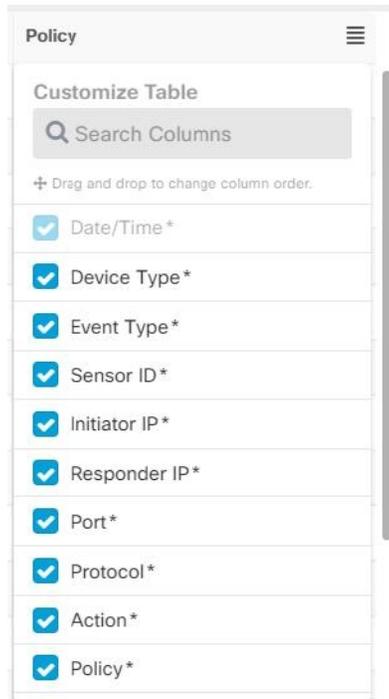
当您离开此页面并稍后返回时，系统会自动保存对“事件日志记录” (Event Logging) 页面所做的任何更改。



**Note** 实时和历史事件视图具有相同的配置。自定义事件视图时，这些更改将同时应用于实时和历史视图。

## 列

您可以修改实时事件和历史事件的事件视图，以仅包含适用于所需视图的列标题。点击列右侧的列过滤器图标 ，然后选择或取消选择所需的列：



默认情况下，事件表中提供带星号的列，但您可以随时将其删除。使用搜索栏手动搜索可能要包括的其他列的关键字。

## 订单

您可以对“事件”视图的列重新排序。点击列右侧的列过滤器图标  可展开所选列的列表，并手动将列拖放到所需的顺序，其中下拉菜单中列表顶部的列位于左侧-事件视图中的大多数列。

相关信息：

- [在事件日志记录页面中搜索和过滤事件](#)
- [安全分析和日志记录中的事件属性](#)

# 在事件日志记录页面上显示和隐藏列

事件日志记录页面显示从配置的 ASA 和 FDM 管理设备发送到思科云的 ASA 和 FTD 系统日志事件以及 ASA NetFlow 安全事件日志记录 (NSEL) 事件。

您可以通过对表使用显示/隐藏构件来显示或隐藏“事件日志记录”页面上的列：

**步骤 1** 从 CDO 导航栏中，选择 **分析 (Analytics) > 事件日志记录 (Event Logging)**。

**步骤 2** 滚动到表格的最右侧，然后点击**显示/隐藏列 (Show/Hide Columns)** 按钮 。

**步骤 3** 选中要查看的列，并取消选中要隐藏的列。

**步骤 4** 将鼠标悬停在“显示/隐藏列” (Show/Hide Columns) 下拉菜单中的列名称上，然后抓住灰色十字，重新排列列顺序。

登录到租户的其他用户将看到您选择显示的相同列，直到列再次显示或隐藏。

下表介绍了列标题：

列标题	说明
日期/时间	设备生成事件的时间。时间以计算机的本地时间显示。
设备类型	ASA（自适应安全设备） FTD（Firepower 威胁防御）

列标题	说明
事件类型	<p>此组合列可以包含以下任何内容：</p> <ul style="list-style-type: none"> <li>• <b>FTD 事件类型</b> <ul style="list-style-type: none"> <li>• 连接 - 显示访问控制规则中的连接事件。</li> <li>• 文件 - 显示访问控制规则中文件策略报告的事件。</li> <li>• 入侵 - 显示访问控制规则中入侵策略报告的事件。</li> <li>• 恶意软件 - 显示访问控制规则中的恶意软件策略报告的事件。</li> </ul> </li> <li>• <b>ASA 事件类型</b> - 这些事件类型表示系统日志或 NetFlow 事件组。有关哪个系统日志 ID 或哪个 NetFlow ID 包含在哪个组中的详细信息，请参阅 <a href="#">ASA 事件类型</a>。 <ul style="list-style-type: none"> <li>• 解析的事件 - 解析的系统日志事件包含比其他系统日志事件更多的事件属性，并且 CDO 能够更快地返回基于这些属性的搜索结果。解析的事件不是过滤类别；但是，解析的事件 ID 以斜体显示在“事件类型” (Event Types) 列中。不以斜体显示的事件 ID 不会被解析。</li> </ul> </li> <li>• <b>ASA NetFlow 事件 ID</b>：此处会显示 ASA 的所有 <a href="#">Netflow (NSEL) 事件</a>。</li> </ul>
传感器 ID (Sensor ID)	传感器 ID 是将事件发送到安全事件连接器的 IP 地址。这通常是 Firepower 威胁防御或 ASA 上的管理接口。
发起方 IP	这是网络流量源的 IP 地址。发起方地址字段的值对应于事件详细信息中发起方 IP 字段的值。您可以输入单个地址（例如 10.10.10.100）或以 CIDR 表示法定义的网络（例如 10.10.10.0/24）。
响应方 IP	这是流数据包的目的 IP 地址。“目的地地址” (Destination address) 字段的值对应于事件详细信息中 ResponderIP 字段中的值。您可以输入单个地址（例如 10.10.10.100）或以 CIDR 表示法定义的网络（例如 10.10.10.0/24）。

列标题	说明
Port	会话响应方使用的端口或 ICMP 代码。目标端口的值对应于事件详细信息中的 <b>ResponderPort</b> 值。
协议	它代表事件中的协议。
操作	<p>指定规则定义的安全操作。输入的值必须与要查找的内容完全匹配；但是，大小写无关紧要。为连接、文件、入侵、恶意软件、系统日志和 NetFlow 事件类型输入不同的值：</p> <ul style="list-style-type: none"> <li>对于连接事件类型，过滤器在 AC_RuleAction 属性中搜索匹配项。这些值可以是“允许”(Allow)、“阻止”(Block)、“信任”(Trust)。</li> <li>对于文件事件类型，过滤器在 FileAction 属性中搜索匹配项。这些值可以是“允许”、“阻止”、“信任”。</li> <li>对于入侵事件类型，过滤器在 InLineResult 属性中搜索匹配项。这些值可以是“已允许”(Allowed)、“已阻止”(Blocked)、“已信任”(Trusted)。</li> <li>对于恶意软件事件类型，过滤器会在 FileAction 属性中搜索匹配项。这些值可以是“云查找超时”(Cloud Lookup Timeout)。</li> <li>对于系统日志和 NetFlow 事件类型，过滤器在操作属性中搜索匹配项。</li> </ul>
策略	触发事件的策略的名称。ASA 和 FDM 管理设备的名称将有所不同。

相关信息：

[在事件日志记录页面中搜索和过滤事件, on page 110](#)

## 可自定义的事件过滤器

如果您是安全日志记录分析 (SaaS) 客户，则可以创建并保存您经常使用的自定义过滤器。

过滤器的元素会在您配置时保存到过滤器选项卡中。每当您返回“事件日志记录”(Event Logging) 页面时，这些搜索都可供使用。租户的其他 CDO 用户将无法使用它们。如果您管理多个租户，它们将无法在其他租户上使用。

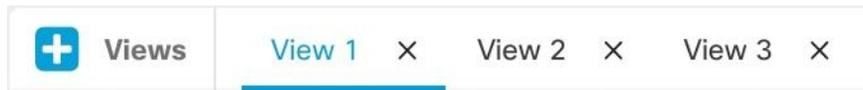


**Note** 请注意，在过滤器选项卡中操作时，如果修改任何过滤器条件，这些更改将自动保存到自定义过滤器选项卡。

**步骤 1** 从主菜单中选择分析 (Analytics) > 事件日志记录 (Event Logging)。

**步骤 2** 清除任何值的搜索字段。

**步骤 3** 在事件表上方，点击蓝色加号按钮以添加视图选项卡。过滤器视图被标记为“视图 1” (View 1)、“视图 2” (View 2)、“视图 3” (View 3) 等，直到您为其指定名称。



**步骤 4** 选择一个视图选项卡。

**步骤 5** 打开过滤器栏，然后在自定义过滤器中选择所需的过滤器属性。请参阅[在事件日志记录页面中搜索和过滤事件, on page 110](#)。请记住，自定义过滤器中仅保存过滤器属性。

**步骤 6** 自定义要在事件日志记录表中显示的列。有关显示和隐藏列的讨论，请参阅[在事件日志记录页面上显示和隐藏列, on page 74](#)。

**步骤 7** 双击带有“视图 X” (View X) 标签的过滤器选项卡并将其重命名。

**步骤 8** (可选) 现在您已创建自定义过滤器，您可以通过向“搜索” (Search) 字段添加搜索条件来微调“事件日志记录” (Event Logging) 页面上显示的结果，而无需更改自定义过滤器。请参阅[在事件日志记录页面中搜索和过滤事件, on page 110](#)。

## 安全分析和日志记录中的事件属性

### 事件属性说明

CDO 使用的事件属性说明与 Firepower Device Manager (FDM) 和自适应安全设备管理器 (ASDM) 报告的内容基本相同。

- 有关自适应安全设备 (ASA) 事件属性的完整说明，请参阅[思科 ASA 系列系统日志消息](#)。

某些 ASA 系统日志事件经过“解析”，其他事件具有其他属性，您可以在使用“属性:值”对过滤事件日志记录表的内容时使用这些属性。有关系统日志事件的其他重要属性，请参阅以下附加主题：

- [已解析的 ASA 系统日志事件](#)
- [某些系统日志消息的 EventGroup 和 EventGroupDefinition 属性](#)
- [系统日志事件的 EventName 属性](#)
- [系统日志事件中的时间属性](#)

## 某些系统日志消息的 EventGroup 和 EventGroupDefinition 属性

某些系统日志事件将具有附加属性“EventGroup”和“EventGroupDefinition”。您将能够通过过滤“属性:值”对来过滤事件表，查找使用这些附加属性的事件。例如，您可以通过在事件日志记录表的搜索字段中输入 `apfw:415*` 来过滤应用防火墙事件。

系统日志消息类和关联的消息 ID 号

事件组	EventGroupDefinition	系统日志消息 ID 号（前 3 数字）
aaa/auth	用户身份验证	109、113
acl/session	访问列表/用户会话	106
apfw	应用防火墙	415
bridge	透明防火墙	110、220
ca	PKI 证书颁发机构	717
citrix	Citrix Client	723
clst	集群	747
cmgr	卡管理	323
config	命令界面	111、112、208、308
csd	安全桌面	724
cts	Cisco TrustSec	776
dap	动态访问策略	734
eap, eapoudp	用于网络准入控制的 EAP 或 EAPoUDP	333、334
eigrp	EIGRP 路由	336
电子邮件	邮件代理	719
ipaa/envmon	环境监控	735
ha	故障转移	101、102、103、104、105、210、311、709
idfw	基于身份认证的防火墙	746
ids	入侵检测系统	733
ids/ips	入侵检测系统/入侵保护系统	400
ikev2	IKEv2 工具包	750、751、752
ip	IP 堆栈	209、215、313、317、408
ipaa	IP 地址分配	735

事件组	EventGroupDefinition	系统日志消息 ID 号（前 3 数字）
ips	入侵保护系统	401、420
ipv6	IPv6	325
l4tm	阻止列表、允许列表、灰名单	338
许可证	许可	444
mdm-proxy	MDM 代理	802
nac	网络准入控制	731、732
vpn/nap	IKE 和 IPsec/网络接入点	713
np	网络处理器	319
ospf	OSPF 路由	318、409、503、613
passwd	密码加密	742
pp	电话代理	337
rip	RIP 路由	107、312
rm	资源管理器	321
sch	Smart Call Home	120
session	用户会话	106、108、201、202、204、 302、303、304、305、314、 405、406、407、500、502、 607、608、609、616、620、 703、710
会话/natpat	用户会话/NAT 和 PAT	305
snmp	SNMP	212
ssafe	ScanSafe	775
ssl/np ssl	SSL 协议栈/NP SSL	725
svc	SSL VPN 客户端	722
sys	System	199、211、214、216、306、 307、315、414、604、605、 606、610、612、614、615、 701、711、741
tre	事务规则引擎	780
ucime	UC-IME	339
标记交换	服务标记交换	779
td	威胁检测	733

事件组	EventGroupDefinition	系统日志消息 ID 号（前 3 数字）
vm	VLAN 映射	730
vpdn	PPTP 和 L2TP 会话	213、403、603
vpn	IKE 和 IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN 客户端	611
vpnfo	VPN 故障转移	720
vpnlb	VPN 负载均衡	718
vxlan	VXLAN	778
webfo	WebVPN 故障转移	721
webvpn	WebVPN 和 AnyConnect 客户端	716
会话/natpat	用户会话/NAT 和 PAT	305

## 系统日志事件的 EventName 属性

某些系统日志事件将具有附加属性“EventName”。您将能够通过过滤“属性:值”对来过滤事件表，查找使用 EventName 属性的事件。例如，您可以通过在事件日志记录表的搜索字段中输入 **EventName:"Denied IP Packet"** 来过滤“被拒绝的 IP 数据包”的事件。

### 系统日志事件 ID 和事件名称表

- [AAA 系统日志事件 ID 和事件名称](#)
- [僵尸网络系统日志事件 ID 和事件名称](#)
- [故障切换系统日志事件 ID 和事件名称](#)
- [防火墙拒绝系统日志事件 ID 和事件名称](#)
- [防火墙流量系统日志事件 ID 和事件名称](#)
- [基于身份的防火墙系统日志事件 ID 和事件名称](#)
- [IPSec 系统日志事件 ID 和事件名称](#)
- [NAT 系统日志事件 ID 和事件名称](#)
- [SSL VPN 系统日志事件 ID 和事件名称](#)

### AAA 系统日志事件 ID 和事件名称

EventID	EventName
109001	AAA 开始

EventID	EventName
109002	AAA 失败
109003	AAA 服务器发生故障
109005	身份验证成功
109006	身份验证失败
109007	授权成功
109008	授权失败
109010	AAA 待处理
109011	AAA 会话已启动
109012	AAA 会话已结束
109013	AAA
109014	AAA 失败
109016	未找到 AAA ACL
109017	AAA 限制到达
109018	AAA ACL 空
109019	AAA ACL 错误
109020	AAA ACL 错误
109021	AAA 错误
109022	AAA HTTP 限制已达到
109023	需要 AAA 身份验证
109024	授权失败
109025	授权失败
109026	AAA 错误
109027	AAA 服务器错误
109028	AAA 绕行
109029	AAA ACL 错误
109030	AAA ACL 错误

EventID	EventName
109031	身份验证失败
109032	AAA ACL 错误
109033	身份验证失败
109034	身份验证失败
109035	AAA 限制到达
113001	AAA 会话限制范围
113003	AAA 已覆盖
113004	AAA 成功
113005	授权被拒绝
113006	AAA 用户已锁定
113007	AAA 用户已解锁
113008	AAA 成功
113009	AAA 已检索
113010	AAA 挑战已收到
113011	AAA 已检索
113012	身份验证成功
113013	AAA 错误
113014	AAA 错误
113015	身份验证已被拒绝
113016	AAA 已被拒绝
113017	AAA 已被拒绝
113018	AAA ACL 错误
113019	AAA 已断开
113020	AAA 错误
113021	AAA 日志记录失败
113022	AAA 失败

EventID	EventName
113023	AAA 已重新激活
113024	AAA 客户端证书
113025	AAA 认证失败
113026	AAA 错误
113027	AAA 错误

## 僵尸网络系统日志事件 ID 和事件名称

EventID	EventName
338001	僵尸网络源阻止列表
338002	僵尸网络目标阻止列表
338003	僵尸网络源阻止列表
338004	僵尸网络目标阻止列表
338101	僵尸网络源允许列表
338102	僵尸网络目标允许列表
338202	僵尸网络目的地（灰色）
338203	僵尸网络源灰色
338204	僵尸网络目标灰色
338301	僵尸网络 DNS 已拦截
338302	僵尸网络 DNS
338303	僵尸网络 DNS
338304	僵尸网络下载成功
338305	僵尸网络下载失败
338306	僵尸网络身份验证失败
338307	僵尸网络解密失败
338308	僵尸网络客户端
338309	僵尸网络客户端
338310	僵尸网络动态过滤器失败

## 故障切换系统日志事件 ID 和事件名称

EventID	EventName
101001	故障切换电缆 OK
101002	故障切换电缆 BAD
101003	故障切换电缆未连接
101004	故障切换电缆未连接
101005	故障切换电缆读取错误
102001	故障转移电源失败
103001	故障转移伙伴无响应
103002	故障转移配对接口 OK
103003	故障转移伙伴接口 BAD
103004	故障转移伙伴报告失败
103005	故障转移伙伴报告自身失败
103006	故障转移版本不兼容
103007	故障转移版本差异
104001	故障转移角色切换
104002	故障转移角色切换
104003	故障转移设备发生故障
104004	故障转移单元 OK
106100	允许/被 ACL 拒绝
210001	状态故障转移错误
210002	状态故障转移错误
210003	状态故障转移错误
210005	状态故障转移错误
210006	状态故障转移错误
210007	状态故障转移错误
210008	状态故障转移错误

EventID	EventName
210010	状态故障转移错误
210020	状态故障转移错误
210021	状态故障转移错误
210022	状态故障转移错误
311001	状态故障转移更新
311002	状态故障转移更新
311003	状态故障转移更新
311004	状态故障转移更新
418001	被拒绝的向管理发送的数据包
709001	故障转移复制错误
709002	故障转移复制错误
709003	故障转移复制开始
709004	故障转移复制完成
709005	故障转移接收复制开始
709006	故障转移接收复制完成
709007	故障转移复制失败
710003	被拒绝的访问设备

#### 防火墙拒绝系统日志事件 ID 和事件名称

EventID	EventName
106001	被安全策略拒绝
106002	出站拒绝
106006	被安全策略拒绝
106007	被拒绝的进站 UDP
106008	被安全策略拒绝
106010	被安全策略拒绝
106011	被拒绝的进站

EventID	EventName
106012	由于 IP 选项错误而被拒绝
106013	对 PAT IP 的 ping 操作丢弃
106014	被拒绝的进站 ICMP
106015	被安全策略拒绝
106016	被拒绝的 IP 欺骗
106017	由于着陆攻击而被拒绝
106018	被拒绝的出站 ICMP
106020	被拒绝的 IP 数据包
106021	被拒绝的 TCP
106022	被拒的绝欺骗数据包
106023	被拒绝的 IP 数据包
106025	被丢弃的数据包未能检测情景
106026	被丢弃的数据包未能检测情景
106027	被丢弃的数据包未能检测情景
106100	允许/被 ACL 拒绝
418001	被拒绝的向管理发送的数据包
710003	被拒绝的访问设备

#### 防火墙流量系统日志事件 ID 和事件名称

EventID	EventName
108001	检查 SMTP
108002	检查 SMTP
108003	检查 ESMTP 已丢弃
108004	检查 ESMTP
108005	检查 ESMTP
108006	检查 ESMTP 违规
108007	检查 ESMTP

EventID	EventName
110002	找不到路由器
110003	未能找到下一跳
209003	分段限制范围
209004	分段长度无效
209005	分段 IP 丢弃
302003	H245 连接开始
302004	H323 连接开始
302009	重新启动 TCP
302010	连接使用情况
302012	H225 CALL SIGNAL CONN
302013	内置 TCP
302014	拆解 TCP
302015	内置 UDP
302016	拆解 UDP
302017	内置 GRE
302018	拆解 GRE
302019	H323 失败
302020	内置 ICMP
302021	拆解 ICMP
302022	内置 TCP 末节
302023	拆解 TCP 末节
302024	内置 UDP 末节
302025	拆解 UDP 末节
302026	内置 ICMP 末节
302027	拆解 ICMP 末节
302033	连接 H323

EventID	EventName
302034	H323 连接失败
302035	内置 SCTP
302036	拆解 SCTP
303002	FTP 文件下载/上传
303003	检查 FTP 已丢弃
303004	检查 FTP 已丢弃
303005	检查 FTP 重置
313001	ICMP 已拒绝
313004	ICMP 丢弃
313005	ICMP 错误消息丢弃
313008	ICMP ipv6 已拒绝
324000	GTP 数据包丢弃
324001	GTP 数据包错误
324002	内存错误
324003	GTP 数据包丢弃
324004	不支持 GTP 版本
324005	GTP 隧道失败
324006	GTP 隧道失败
324007	GTP 隧道失败
337001	电话代理 SRTP 失败
337002	电话代理 SRTP 失败
337003	电话代理 SRTP 身份验证失败
337004	电话代理 SRTP 身份验证失败
337005	电话代理 SRTP 无媒体会话
337006	电话代理 TFTP 无法创建文件
337007	电话代理 TFTP 无法查找文件

EventID	EventName
337008	电话代理呼叫失败
337009	电话代理无法创建电话条目
400000	IPS IP 选项 - 错误选项列表
400001	IPS IP 选项 - 记录数据包路由
400002	IPS IP 选项 - 时间戳
400003	IPS IP 选项 - 安全
400004	IPS IP 选项 - 松散源路由
400005	IPS IP 选项 - SATNET ID
400006	IPS IP 选项 - 严格源路由
400007	IPS IP 分段攻击
400008	IPS IP 不可能的数据包
400009	IPS IP 分段重叠
400010	IPS ICMP 回应应答
400011	IPS ICMP 主机不可达
400012	IPS ICMP 源抑制
400013	IPS ICMP 重定向
400014	IPS ICMP 回应请求
400015	数据报的 IPS ICMP 超时
400017	IPS ICMP 时间戳请求
400018	IPS ICMP 时间戳应答
400019	IPS ICMP 信息请求
400020	IPS ICMP 信息应答
400021	IPS ICMP 地址掩码请求
400022	IPS ICMP 地址掩码应答
400023	IPS 分段的 ICMP 流量
400024	IPS 大 ICMP 流量

EventID	EventName
400025	死亡之 IPS Ping 攻击
400026	IPS TCP NULL 标志
400027	IPS TCP SYN+FIN 标志
400028	仅 IPS TCP FIN 标志
400029	指定了不正确的 IPS FTP 地址
400030	指定了不正确的 IPS FTP 端口
400031	IPS UDP 炸弹攻击
400032	IPS UDP Snork 攻击
400033	IPS UDP Chargen DoS 攻击
400034	IPS DNS HINFO 请求
400035	IPS DNS 区域传输
400036	来自高端口的 IPS DNS 区域传输
400037	所有记录的 IPS DNS 请求
400038	IPS RPC 端口注册
400039	IPS RPC 端口取消注册
400040	IPS RPC 转储
400041	IPS 通过代理发送的 RPC 请求
400042	IPS YP 服务器端口映射请求
400043	IPS YP 绑定端口映射请求
400044	IPS YP 密码端口映射请求
400045	IPS YP 更新端口映射请求
400046	IPS YP 传输端口映射请求
400047	IPS 装载端口映射请求
400048	IPS 远程执行端口映射请求
400049	IPS 远程执行尝试
400050	IPS Statd 缓冲区溢出

EventID	EventName
406001	检查 FTP 已丢弃
406002	检查 FTP 已丢弃
407001	主机限制到达
407002	初期限制已到达
407003	既定限制已到达
415001	检查 Http 信头字段计数
415002	检查 Http 信头字段长度
415003	检查 Http 正文长度
415004	检查 Http 内容类型
415005	检查 Http URL 长度
415006	检查 Http URL 匹配
415007	检查 Http 正文匹配
415008	检查 Http 信头匹配
415009	检查 Http 方法匹配
415010	检查传输编码匹配
415011	检查 Http 协议违规
415012	检查 Http 内容类型
415013	检查 Http 格式错误
415014	检查 Http MIME 类型
415015	检查 Http Transfer-encoding
415016	检查 Http 未应答
415017	检查 Http 参数匹配
415018	检查 Http 信头长度
415019	检查 Http 状态已匹配
415020	检查 Http non-ASCII
416001	检查 SNMP 已丢弃

EventID	EventName
419001	已丢弃的数据包
419002	重复 TCP SYN
419003	数据包已修改
424001	被拒绝的数据包
424002	已丢弃的数据包
431001	已丢弃的 RTP
431002	已丢弃的 RTCP
500001	检查 ActiveX
500002	检查 Java
500003	检查 TCP 信头
500004	检查 TCP 信头
500005	检查连接已终止
508001	检查 DCERPC 已丢弃
508002	检查 DCERPC 已丢弃
509001	已阻止 No Forward Cmd
607001	检查 SIP
607002	检查 SIP
607003	检查 SIP
608001	检查 Skinny
608002	检查 Skinny 已丢弃
608003	检查 Skinny 已丢弃
608004	检查 Skinny 已丢弃
608005	检查 Skinny 已丢弃
609001	内置本地主机
609002	拆解本地主机
703001	H225 不支持的版本

EventID	EventName
703002	H225 连接
726001	检查即时消息

## 基于身份的防火墙系统日志事件 ID 和事件名称

EventID	EventName
746001	导入已开始
746002	导入完成
746003	导入失败
746004	超出用户组限制
746005	AD 代理关闭
746006	AD 代理不同步
746007	Netbios 响应失败
746008	Netbios 已启动
746009	Netbios 已停止
746010	导入用户失败
746011	超出用户限制
746012	用户 IP 添加
746013	用户 IP 删除
746014	FQDN 过时
746015	FQDN 已解析
746016	DNS 查找失败
746017	导入用户已颁发
746018	导入用户已完成
746019	更新 AD 代理失败

## IPSec 系统日志事件 ID 和事件名称

EventID	EventName
402114	收到无效的 SPI

EventID	EventName
402115	收到意外的协议
402116	数据包与身份不匹配
402117	收到的非 IPSEC 数据包
402118	无效的分段偏移量
402119	防重放检查失败
402120	身份验证失败
402121	数据包已丢弃
426101	cLACP 端口捆绑包
426102	cLACP 端口备用
426103	已将 cLACP 端口从备用端口移至捆绑包
426104	cLACP 非捆绑端口
602103	路径 MTU 已更新
602104	路径 MTU 已超出
602303	新 SA 已创建
602304	SA 已删除
702305	SA 到期 - 序列滚动
702307	SA 到期 - 数据滚动

## NAT 系统日志事件 ID 和事件名称

EventID	EventName
201002	超出主机的最大连接数
201003	已超出初期限制
201004	已超出 UDP 连接限制
201005	FTP 连接失败
201006	RCMD 连接失败
201008	不允许新建连接
201009	超出连接限制
201010	已超出初期连接限制
201011	已超出连接限制
201012	已超出每个客户端的初期连接限制

EventID	EventName
201013	已超出每个客户端连接限制
202001	全局 NAT 已耗尽
202005	初期连接错误
202011	超出连接限制
305005	未找到 NAT 组
305006	转换已失败
305007	连接已断开
305008	NAT 分配问题
305009	NAT 已创建
305010	NAT 拆解
305011	PAT 已创建
305012	PAT 拆解
305013	连接已被拒绝

## SSL VPN 系统日志事件 ID 和事件名称

EventID	EventName
716001	WebVPN 会话已启动
716002	WebVPN 会话已终止
716003	WebVPN 用户 URL 访问
716004	WebVPN 用户 URL 访问被拒绝
716005	WebVPN ACL 错误
716006	WebVPN 用户已禁用
716007	WebVPN 无法创建
716008	WebVPN 调试
716009	WebVPN ACL 错误
716010	WebVPN 用户接入网络
716011	WebVPN 用户访问
716012	WebVPN 用户目录访问
716013	WebVPN 用户文件访问
716014	WebVPN 用户文件访问

EventID	EventName
716015	WebVPN 用户文件访问
716016	WebVPN 用户文件访问
716017	WebVPN 用户文件访问
716018	WebVPN 用户文件访问
716019	WebVPN 用户文件访问
716020	WebVPN 用户文件访问
716021	WebVPN 用户访问文件被拒绝
716022	WebVPN 无法连接代理
716023	WebVPN 会话限制已到达
716024	WebVPN 用户访问错误
716025	WebVPN 用户访问错误
716026	WebVPN 用户访问错误
716027	WebVPN 用户访问错误
716028	WebVPN 用户访问错误
716029	WebVPN 用户访问错误
716030	WebVPN 用户访问错误
716031	WebVPN 用户访问错误
716032	WebVPN 用户访问错误
716033	WebVPN 用户访问错误
716034	WebVPN 用户访问错误
716035	WebVPN 用户访问错误
716036	WebVPN 用户登录成功
716037	WebVPN 用户登录失败
716038	WebVPN 用户身份验证成功
716039	WebVPN 用户身份验证被拒绝
716040	WebVPN 用户日志记录被拒绝
716041	WebVPN ACL 命中计数
716042	WebVPN ACL 命中
716043	WebVPN 端口转发

EventID	EventName
716044	WebVPN 错误参数
716045	WebVPN 参数无效
716046	WebVPN 连接已终止
716047	WebVPN ACL 使用情况
716048	WebVPN 内存问题
716049	WebVPN 空 SVC ACL
716050	WebVPN ACL 错误
716051	WebVPN ACL 错误
716052	WebVPN 会话已终止
716053	WebVPN SSO 服务器已添加
716054	WebVPN SSO 服务器已删除
716055	WebVPN 身份验证成功
716056	WebVPN 身份验证失败
716057	WebVPN 会话已终止
716058	WebVPN 会话已丢失
716059	WebVPN 会话已恢复
716060	WebVPN 会话已终止
722001	WebVPN SVC 连接请求错误
722002	WebVPN SVC 连接请求错误
722003	WebVPN SVC 连接请求错误
722004	WebVPN SVC 连接请求错误
722005	WebVPN SVC 连接更新问题
722006	WebVPN SVC 地址无效
722007	WebVPN SVC 消息
722008	WebVPN SVC 消息
722009	WebVPN SVC 消息
722010	WebVPN SVC 消息
722011	WebVPN SVC 消息
722012	WebVPN SVC 消息

EventID	EventName
722013	WebVPN SVC 消息
722014	WebVPN SVC 消息
722015	WebVPN SVC 无效帧
722016	WebVPN SVC 无效帧
722017	WebVPN SVC 无效帧
722018	WebVPN SVC 无效帧
722019	WebVPN SVC 数据不足
722020	WebVPN SVC 无地址
722021	WebVPN 内存问题
722022	WebVPN SVC 连接已建立
722023	WebVPN SVC 连接已终止
722024	WebVPN 压缩已启用
722025	WebVPN 压缩已禁用
722026	WebVPN 压缩重置
722027	WebVPN 解压重置
722028	WebVPN 连接已关闭
722029	WebVPN SVC 会话已终止
722030	WebVPN SVC 会话已终止
722031	WebVPN SVC 会话已终止
722032	WebVPN SVC 连接替换
722033	WebVPN SVC 连接已建立
722034	WebVPN SVC 新连接
722035	WebVPN 收到大数据包
722036	WebVPN 传输大型数据包
722037	WebVPN SVC 连接已关闭
722038	WebVPN SVC 会话已终止
722039	WebVPN SVC 无效 ACL
722040	WebVPN SVC 无效 ACL
722041	WebVPN SVC IPv6 不可用

EventID	EventName
722042	WebVPN 无效协议
722043	WebVPN DTLS 已禁用
722044	WebVPN 无法请求地址
722045	WebVPN 连接已终止
722046	WebVPN 会话已终止
722047	WebVPN 隧道已终止
722048	WebVPN 隧道已终止
722049	WebVPN 会话已终止
722050	WebVPN 会话已终止
722051	分配的 WebVPN 地址
722053	WebVPN 未知客户端
723001	WebVPN Citrix 连接开启
723002	WebVPN Citrix 连接关闭
723003	WebVPN Citrix 无内存问题
723004	WebVPN Citrix 不良流量控制
723005	WebVPN Citrix 无信道
723006	WebVPN Citrix SOCKS 错误
723007	WebVPN Citrix 连接列表已损坏
723008	WebVPN Citrix 无效 SOCKS
723009	WebVPN Citrix 无效连接
723010	WebVPN Citrix 无效连接
723011	WebVPN citrix 不良 SOCKS
723012	WebVPN Citrix 不良 SOCKS
723013	WebVPN Citrix 无效连接
723014	WebVPN Citrix 连接到服务器
724001	不允许使用 WebVPN 会话
724002	WebVPN 会话已终止
724003	WebVPN CSD
724004	WebVPN CSD
725001	SSL 握手已开始



Date/Time	Device Type	Event Type	Sensor ID	Initiator IP	Responder IP	Port	Protocol	Action	Policy
Jun 12, 2020, 7:27:02 AM	ASA	302013	admin	192.168.25.4	192.168.0.68	443	TCP	Built	
<b>Action</b>	Built	<b>EventType</b>	302013	<b>Protocol</b>	TCP				
<b>ConnectionID</b>	1169028	<b>IngressInterface</b>	management	<b>ResponderIP</b>	192.168.0.68				
<b>DeviceType</b>	ASA	<b>InitiatorIP</b>	192.168.25.4	<b>ResponderPort</b>	443				
<b>Direction</b>	inbound	<b>InitiatorPort</b>	36540	<b>SensorID</b>	admin				
<b>EgressInterface</b>	identity	<b>MappedInitiatorIP</b>	192.168.25.4	<b>Severity</b>	Informational				
<b>EventGroup</b>	session	<b>MappedInitiatorPort</b>	36540	<b>SyslogTimestamp</b>	2020-06-12 11:15:26 +0000 UTC				
<b>EventGroupDefinition</b>	User Session	<b>MappedResponderIP</b>	192.168.0.68	<b>timestamp</b>	Jun 12, 2020, 7:27:02 AM				
<b>EventName</b>	Built TCP	<b>MappedResponderPort</b>	443						
<b>Message</b>	ASA-6-302013: Built inbound TCP connection 1169028 for management:192.168.25.4/36540 (192.168.25.4/36540) to identity:192.168.0.68/443 (192.168.0.68/443)								

Date/Time	Device Type	Event Type	Sensor ID	Initiator IP	Responder IP	Port	Protocol	Action	Policy
Jun 12, 2020, 7:27:13 AM	ASA	5	192.168.0.169	192.168.25.4	192.168.0.169	443	TCP	Update	
<b>Action</b>	Update	<b>InitiatorBytes</b>	0	<b>Protocol</b>	TCP				
<b>ConnectionID</b>	482168	<b>InitiatorIP</b>	192.168.25.4	<b>ResponderBytes</b>	3581				
<b>DeviceType</b>	ASA	<b>InitiatorPackets</b>	0	<b>ResponderIP</b>	192.168.0.169				
<b>EgressInterface</b>	65535	<b>InitiatorPort</b>	38068	<b>ResponderPackets</b>	33				
<b>EventType</b>	5	<b>LastPacketSecond</b>	Jun 12, 2020, 7:27:07 AM	<b>ResponderPort</b>	443				
<b>FirewallExtendedEvent</b>	2034	<b>MappedInitiatorIP</b>	192.168.25.4	<b>SensorID</b>	192.168.0.169				
<b>FirstPacketSecond</b>	Jun 12, 2020, 7:27:07 AM	<b>MappedInitiatorPort</b>	38068	<b>Severity</b>	Informational				
<b>ICMPCode</b>	0	<b>MappedResponderIP</b>	192.168.0.169	<b>timestamp</b>	Jun 12, 2020, 7:27:13 AM				
<b>ICMPType</b>	0	<b>MappedResponderPort</b>	443						
<b>IngressInterface</b>	9	<b>NetFlowTimestamp</b>	1591961232						

数字	编号	说明
1	日期/时间	安全事件连接器 (SEC) 处理事件的时间。这可能与防火墙检查该流量的时间有所不同。与时间戳相同的值。
2	EventSecond	等于 LastPacketSecond。
3	FirstPacketSecond	连接打开的时间。防火墙会在此时检查数据包。  FirstPacketSecond 的值通过从 LastPacketSecond 中减去 ConnectionDuration 来计算得出。  对于在连接开始时记录的连接事件，FirstPacketSecond、LastPacketSecond 和 EventSecond 的值均相同。
4	LastPacketSecond	连接被关闭的时间。对于在连接结束时记录的连接事件，LastPacketSecond 和 EventSecond 将相等。
5	timestamp	安全事件连接器 (SEC) 处理事件的时间。这可能与防火墙检查该流量的时间有所不同。与日期/时间相同的值。

数字	编号	说明
6	系统日志时间戳	如果使用“日志记录时间戳”，则表示系统日志的发起时间。如果系统日志中没有此信息，则会反映 SEC 收到事件的时间。
7	NetflowTimeStamp	ASA 完成收集足够的流记录/事件以填充 NetFlow 数据包，然后将其发送到流收集器的时间。

## 思科安全云分析和动态实体建模

**所需许可证 (Required License):** 日志记录分析和检测 (Logging Analytics and Detection) 或全面网络分析和监控 (Total Network Analytics and Monitoring)

安全云分析是一种软件即服务 (SaaS) 解决方案，可用于监控您的本地和基于云的网络部署。通过从源（包括防火墙事件和网络流数据）收集有关网络流量的信息，它会创建有关流量的观察结果，并根据其流量模式自动识别网络实体的角色。使用此信息与其他威胁情报来源（例如 Talos）相结合，安全云分析会生成警报，警告可能存在恶意行为。除警报外，安全云分析还提供网络和主机可视性以及所收集的情景信息，为您研究警报和查找恶意行为的来源提供更好的基础。

### 动态实体建模

动态实体建模可通过对防火墙事件和网络流数据执行行为分析来跟踪网络状态。在 Cisco Secure Cloud Analytics 环境中，实体是指可以随时间推移进行跟踪的对象，例如网络上的主机或终端。动态实体建模根据实体传输的流量及其在网络上执行的活动，收集实体的相关信息。与日志记录分析和检测许可证集成的 Cisco Secure Cloud Analytics 可以从防火墙事件和其他流量信息中进行提取，以便确定实体通常传输的流量类型。如果您购买了全面网络分析和监控许可证，则 Cisco Secure Cloud Analytics 还可以在对实体流量进行建模时纳入 NetFlow 和其他流量信息。Cisco Secure Cloud Analytics 会随着时间的推移更新这些模型，因为实体会继续发送流量，并且可能会发送不同的流量，从而保持每个实体的最新模型。根据这些信息，Cisco Secure Cloud Analytics 可以识别：

- 实体的角色，即实体通常执行的操作的描述符。例如，如果实体发送通常与邮件服务器关联的流量，Cisco Secure Cloud Analytics 会为该实体分配邮件服务器角色。角色/实体关系可以是多对一，因为实体可以履行多种角色。
- 对实体的观察结果，即有关实体在网络上的行为的事实，例如与外部 IP 地址建立的心跳连接或与另一个实体建立的远程访问会话。如果与 CDO 集成，则可以从防火墙事件中获取这些事实。如果您还购买了全面的网络分析和监控许可证，则系统还可以从 NetFlow 获取事实，并从防火墙事件和 NetFlow 中生成观察结果。观察结果本身并不具有超出其所代表的事实的意义。一个典型的客户可能有数千个观察结果和若干个警报。

## 警报和分析

Cisco Secure Cloud Analytics 会根据角色、观察结果和其他威胁情报的组合生成警报，这些警报是可操作项目，代表系统标识的可能的恶意行为。请注意，一个警报可能代表多个观察结果。如果防火墙记录了与同一连接和实体相关的多个连接事件，则可能只会生成一个警报。

例如，新的内部设备观察结果本身并不构成可能的恶意行为。但是，随着时间的推移，如果实体传输的流量与域控制器一致，则系统会向该实体分配域控制器角色。如果实体随后使用异常端口与之前未建立连接的外部服务器建立了连接，并且传输了大量的数据，则系统将记录新的大型连接（外部）观察结果和异常域控制器观察结果。如果该外部服务器被识别为一个 Talos 监视列表，则所有这些信息的组合将导致 Cisco Secure Cloud Analytics 生成此实体行为的警报，从而提示您采取进一步措施来研究和补救恶意行为。

在 Cisco Secure Cloud Analytics Web 门户 UI 中打开警报时，您可以查看导致系统生成该警报的支持性观察结果。您还可以从这些观察结果中查看有关所涉实体的其他背景信息，包括它们传输的流量以及外部威胁情报（如果可用）。您还可以查看实体涉及的其他观察结果和警报，然后确定此行为是否与其他潜在恶意行为相关。

请注意，在 Cisco Secure Cloud Analytics 中查看和关闭警报时，无法允许或阻止来自 Cisco Secure Cloud Analytics UI 的流量。如果在主动模式下部署设备，则必须更新防火墙访问控制规则以允许或阻止流量；如果在被动模式下部署防火墙，则必须更新防火墙访问控制规则。

# 使用基于防火墙事件的警报

所需许可证：日志记录分析和检测 或 全面网络分析和监控

## 警报工作流程

警报的工作流程基于其状态。当系统生成警报时，其默认状态为“待处理”，并且未分配任何用户。当您查看警报总结时，默认情况下会显示所有待处理警报，因为这些是最需要关注的。

注意：如果您拥有全面网络分析和监控许可证，则警报可以基于从 NetFlow 生成的观察结果、从防火墙事件生成的观察结果或来自两个数据源的观察结果。

查看警报总结时，可以分配和标记警报，以及将其状态更新为初始分类。您可以使用过滤器和搜索功能查找特定警报，也可以显示不同状态的警报或具有不同标记或负责人的警报。您可以将警报的状态设置为“已暂停”，在这种情况下，警报要等暂停期过后才会重新显示在待处理警报列表中。您也可以移除警报的“已暂停”状态，使其再次显示为待处理警报。查看警报时，您可以将其分配给您自己或系统中的其他用户。用户可以搜索分配给其用户名的所有警报。

在警报摘要中，您可以查看警报详细信息页面。此页面允许您查看有关生成此警报的支持性观察结果的其他背景信息，以及有关此警报中涉及的实体的其他背景信息。这些信息可帮助您查明实际问题，以便进一步研究网络上的问题，并且有可能解决恶意行为。

当您在 CDO 中的 Stealthwatch 云 web 门户 UI 和网络中进行研究时，可以进行备注，描述您对警报的发现。这有助于为您的研究创建记录，供您将来参考。

完成分析后，您可以将状态更新为“已关闭”，使其不再默认显示为待处理警报。如果情况发生变化，您还可以在将来重新打开已关闭的警报。

下面介绍有关如何调查给定警报的一般准则和建议。Stealthwatch 云会在记录警报时提供附加背景信息，因此，您可以使用此信息帮助指导调查工作。

这些步骤既不全面，也非包罗万象。它们仅提供一个总体框架来帮助您开始调查警报。

通常，查看警报时可以采取以下步骤：

1. [对待处理警报进行分类, on page 66](#)
2. [暂停警报以供以后分析, on page 67](#)
3. [更新警报以进行进一步调查, on page 67](#)
4. [查看警报并开始调查, on page 68](#)
5. [检查实体和用户, on page 69](#)
6. [使用安全云分析补救问题, on page 70](#)
7. [更新并关闭警报, on page 70](#)

## 对待处理警报进行分类

对待处理警报进行分类，特别是如果要调查多个待处理警报：

- 有关从 CDO 交叉启动和查看警报的详细信息，请参阅[从 CDO 查看 Cisco Secure Cloud Analytics 警报](#)。

询问以下问题：

- 您是否将此警报类型配置为高优先级？
- 您是否为受影响的子网设置了高灵敏度？
- 这是网络上新实体的异常行为吗？
- 实体的正常角色是什么，此警报中的行为与该角色的匹配度如何？
- 这是否是此实体正常行为的异常偏离？
- 如果用户参与其中，这是用户的预期行为还是异常行为？
- 受保护数据或敏感数据是否有被泄露的风险？
- 如果允许此行为继续下去，会对网络产生多严重的影响？
- 如果与外部实体有通信，这些实体过去是否与您网络上的其他实体建立了连接？

如果这是高优先级警报，请考虑将该实体与互联网隔离，或以其他方式关闭其连接，然后再继续调查。

## 暂停警报以供以后分析

当警报的优先级较低（与其他警报相比）时，可将其暂停。例如，如果您的组织将邮件服务器重新定位为 FTP 服务器，并且系统生成紧急配置文件警报（表明一个实体的当前流量匹配了它以前没有

匹配的行为概要文件），您可以暂停此警报（因为这是预期行为），并在以后重新访问它。已暂停的警报不会与待处理警报一起显示；您必须专门过滤才能查看这些暂停的警报。

暂停警报：

---

**步骤 1** 点击关闭警报 (**Close Alert**)。

**步骤 2** 在暂停此警报窗格中，从下拉列表中选择暂停时段。

**步骤 3** 点击保存 (**Save**)。

---

### What to do next

当您准备好查看这些警报时，可以取消暂停该警报。这会将状态设置为“未处理”(Open)，并在其他“未处理”的警报旁边显示该警报。

取消暂停已暂停的警报：

- 从暂停的警报中，点击取消暂停警报 (**Unsnooze Alert**)。

## 更新警报以进行进一步调查

打开警报详细信息：

---

**步骤 1** 选择监控 (**Monitor**) > 警报 (**Alerts**)。

**步骤 2** 点击警报类型名称。

---

### What to do next

根据您的初始分类和优先级，分配警报并标记：

1. 从被分派人 (**Assignee**) 下拉列表中选择用户以分配警报，以使用户可以开始调查。
2. 从下拉列表中选择一个或多个**标签**，以将标签添加到警报，以便更好地对警报进行分类以供将来识别，并尝试在警报中建立长期模式。
3. 输入为此警报添加注释 (**Comment on this alert**)，然后点击注释 (**Comment**) 以根据需要留下注释，以跟踪您的初始发现，并协助分配到警报的人员。警报同时跟踪系统注释和用户注释。

## 查看警报并开始调查

如果您正在查看已分配的警报，请查看警报详细信息以了解 Stealthwatch 云生成警报的原因。查看支持性观察结果，了解这些观察结果对源实体的意义。

请注意，如果警报是基于防火墙事件生成的，则系统不会注意到您的防火墙部署是此警报的来源。

查看此源实体的所有支持性观察结果，以了解其一般行为和模式，并查看此活动是否可能影响着某个长期趋势：

## SUMMARY STEPS

1. 在观察结果控制面板上，点击观察结果类型旁边的箭头图标 (↕)，以查看该类型的所有已记录观察结果。
2. 点击**网络的所有观察结果 (All Observations for Network)** 旁边的箭头图标 (↕)，查看此警报的源实体的所有已记录观察结果。

## DETAILED STEPS

**步骤 1** 在观察结果控制面板上，点击观察结果类型旁边的箭头图标 (↕)，以查看该类型的所有已记录观察结果。

**步骤 2** 点击**网络的所有观察结果 (All Observations for Network)** 旁边的箭头图标 (↕)，查看此警报的源实体的所有已记录观察结果。

如果要对这些观察结果执行其他分析，请下载逗号分隔值文件中的支持观察结果：

- 在警报详细信息的支持观察结果窗格中，点击 **CSV**。

从观察结果，确定源实体行为是否指示恶意行为。如果源实体与多个外部实体建立了连接，请确定外部实体是否以某种方式相关，例如它们是否都具有相似的地理位置信息，或者它们的 IP 地址是否来自同一子网。

从源实体 IP 地址或主机名称查看有关源实体的其他背景信息，包括它可能涉及的其他警报和观察结果、有关设备本身的信息以及它传输的会话流量类型：

- 从 IP 地址或主机名下拉列表中选择**警报 (Alerts)**，以查看与该实体相关的所有警报。
- 从 IP 地址或主机名下拉列表中选择**观察结果 (Observations)**，以查看与实体相关的所有观察结果。
- 从 IP 地址或主机名下拉列表中选择**设备 (Device)**，以查看有关设备的信息。
- 从 IP 地址或主机名下拉列表中选择**会话流量 (Session Traffic)**，以查看与此实体相关的会话流量。
- 从 IP 地址或主机名下拉列表中选择**复制 (Copy)** 以复制 IP 地址或主机名。

请注意，Stealthwatch 云中的源实体始终位于您的网络内部。将此与防火墙事件中的发起方 IP 进行对比，后者指示发起连接的实体，并且可能位于您的网络内部或外部。

从观察结果中，检查有关其他外部实体的信息。检查地理位置信息，确定是否有任何地理位置数据或 Umbrella 数据标识恶意实体。查看这些实体生成的流量。检查 Talos、AbuseIPDB 或 Google 是否有关于这些实体的任何信息。查找多天的 IP 地址，并查看外部实体与您网络上的实体建立的其他类型的连接。如有必要，请找到这些内部实体，并确定是否有任何证据表明存在攻击活动或意外行为。

查看与源实体建立了连接的外部实体 IP 地址或主机名称的背景信息：

- 从 IP 地址或主机名下拉列表中选择 **IP 流量 (IP Traffic)**，以查看此实体的最近流量信息。
- 从 IP 地址或主机名下拉列表中选择 **会话流量 (Session Traffic)**，以查看此实体的最近会话流量信息。
- 从 IP 地址或主机名下拉列表中选择 **AbuseIPDB**，以查看有关 AbuseIPDB 网页实体的信息。
- 从 IP 地址或主机名下拉列表中选择 **思科 Umbrella (Cisco Umbrella)**，可在 Cisco Umbrella 网站上查看有关此实体的信息。
- 从 IP 地址或主机名下拉列表中选择 **Google 搜索 (Google Search)**，以在 Google 上搜索此 IP 地址。
- 从 IP 地址或主机名下拉列表中选择 **Talos 智能 (Talos Intelligence)**，以查看有关 Talos 网页的信息。
- 从 IP 地址或主机名下拉列表中选择 **将 IP 添加到监视列表 (Add IP to watchlist)**，以将此实体添加到监视列表。
- 从 IP 地址或主机名下拉列表中选择 **查找多天的 IP (Find IP on multiple days)**，以搜索此实体上个月的流量。
- 从 IP 地址或主机名下拉列表中选择 **复制 (Copy)** 以复制 IP 地址或主机名。

请注意，Stealthwatch 云中的连接实体始终位于您的网络外部。将此与防火墙事件中的响应方 IP 进行对比，后者指示响应连接请求的实体，并且可能位于您的网络的内部或外部。

就您的发现进行备注。

- 在警报详细信息中，输入 **对此警报的注释 (Comment on this alert)**，然后点击 **注释 (Comment)**。

## 检查实体和用户

在 Stealthwatch 云门户 UI 中查看警报后，您可以直接对源实体、可能与此警报相关的任何用户以及其他相关实体执行其他检查。

- 确定源实体在网络上的物理位置或云中的位置，并直接访问它。找到此实体的日志文件。如果它是网络上的物理实体，请访问设备以查看日志信息，并查看是否有任何信息表明是什么导致了此行为。如果它是虚拟实体或存储在云中，请访问日志并搜索与此实体相关的条目。检查日志，了解有关未经授权的登录、未经批准的配置更改等活动的更多信息。
- 检查实体。确定您能否识别实体本身上的恶意软件或漏洞。查看是否发生了一些恶意更改，包括设备是否发生了物理更改，例如插入了未经组织批准的 U 盘。
- 确定所涉及的用户来自您的网络内部还是外部。如果可能，询问他们当时在做什么。如果询问未果，请确定他们是否应该具有访问权限，以及是否发生了导致此行为的情况，例如，离职员工在离开公司之前将文件上传到外部服务器。

就您的发现进行备注：

- 在警报详细信息中，输入 **对此警报的注释 (Comment on this alert)**，然后点击 **注释 (Comment)**。

## 更新并关闭警报

根据您的调查结果添加其他标签：

**步骤 1** 在 Cisco Secure Cloud Analytics 门户 UI 中，选择**监控 (Monitor) > 警报 (Alerts)**。

**步骤 2** 从下拉列表中选择一个或多个标签。

添加描述调查结果的最终注释，以及所采取的任何补救步骤：

- 在警报的详细信息中，输入为此警报添加注释 (**Comment on this alert**)，然后点击注释 (**Comment**)。

关闭警报，然后将其标记为有用或无用：

1. 在警报的详细信息中，点击**关闭警报 (Close Alert)**。
2. 如果警报有用，请选择**是 (Yes)**；如果警报无用，请点击**否 (No)**。请注意，这并不一定意味着该警报是由恶意行为导致的，而只是表示它对您的组织有所帮助。
3. 点击**保存 (Save)**。

### What to do next

#### 重新打开已关闭的警报

如果您发现与已关闭警报相关的其他信息，或者想要添加与该警报相关的更多备注，则可以将其重新打开，并将状态更改为“待处理”。然后，您可以根据需要对警报进行更改，并在其他调查完成后再次将其关闭。

重新打开已关闭的警报：

- 在已关闭警报的详细信息中，点击**重新打开警报 (Reopen Alert)**。

## 修改警报优先级

**所需许可证 (Required License)：** 日志记录分析和检测 (**Logging Analytics and Detection**) 或全面网络分析和监控 (**Total Network Analytics and Monitoring**)

警报类型具有默认优先级，这会影​​响系统对生成此类警报的敏感程度。根据思科情报和其他因素，警报的优先级默认为低或正常。根据您的网络环境，您可能希望重新确定警报类型的优先级，以强调您关注的某些警报。您可以将任何风险通告类型配置为低、正常或高优先级。

- 选择**监控 (Monitor) > 警报 (Alerts)**。
- 点击设置下拉图标 (⌵)，然后选择警报类型和优先级。👉
- 点击警报类型旁边的编辑图标 (✎)，然后选择低、中或高以更改优先级。👉

## 在事件日志记录页面中搜索和过滤事件

搜索和过滤特定事件的历史和实时事件表的方式与在 CDO 中搜索和过滤其他信息时的方式相同。当您添加过滤条件时，CDO 就会开始限制其在“事件” (Events) 页面上显示的内容。您还可以在搜索字段中输入搜索条件，以便查找具有特定值的事件。如果结合使用过滤和搜索机制，搜索会尝试在过滤事件后从显示的结果中查找您输入的值。

以下是执行搜索事件日志的选项：

- [在事件日志记录页面中搜索事件，第 117 页](#)
- [在后台搜索历史事件，第 117 页](#)

过滤实时事件的方式与过滤历史事件的方式相同，但不能按时间过滤实时事件。

了解这些过滤方法：

- [过滤实时或历史事件，第 110 页](#)
- [仅过滤 NetFlow 事件，第 112 页](#)
- [过滤 ASA 或 FDM 管理设备系统日志事件，但不过滤 ASA NetFlow 事件，第 112 页](#)
- [组合过滤器元素，第 112 页](#)

## 过滤实时或历史事件

此程序介绍了如何使用事件过滤查看“事件日志记录” (Event Logging) 页面中的事件子集。如果您发现自己重复使用某些过滤条件，则可以创建自定义过滤器并保存。有关详细信息，请参阅[可自定义的事件过滤器](#)。

**步骤 1** 在导航栏中，选择 **分析 (Analytics) > 事件日志记录 (Event Logging)**

**步骤 2** 点击“历史” (Historical) 或“实时” (Live) 选项卡。

**步骤 3** 点击过滤器按钮 。点击固定图标  可固定打开过滤列。

**步骤 4** 点击没有已保存过滤器元素的视图选项卡。



**步骤 5** 选择要作为过滤条件的事件详细信息：

- **FTD 事件**
  - 连接 - 显示访问控制规则中的连接事件。
  - 文件 - 显示访问控制规则中文件策略报告的事件。
  - 入侵 - 显示访问控制规则中入侵策略报告的事件。

- 恶意软件 - 显示访问控制规则中的恶意软件策略报告的事件。
- **ASA 事件 (ASA Events)** - 这些事件类型表示系统日志或 NetFlow 事件组。  
有关事件的详细信息，请参阅 [CDO 中的事件类型](#)。
  - 解析的事件 - 已解析的 [ASA 系统日志事件](#) 包含比其他系统日志事件更多的事件属性，并且 CDO 能够根据这些属性更快地返回搜索结果。解析的事件不是过滤类别；但是，解析的事件 ID 以斜体显示在“事件类型”列中。不以斜体显示的事件 ID 不会被解析。
- **时间范围 (Time Range)** - 点击开始或结束时间字段以选择要显示的时间段的开始和结束时间。时间戳以计算机的本地时间显示。
- **操作 (Action)** - 指定规则定义的安全操作。输入的值必须与要查找的内容完全匹配；但是，大小写无关紧要。为连接、文件、入侵、恶意软件、系统日志和 NetFlow 事件类型输入不同的值：
  - 对于连接事件类型，过滤器在 `AC_RuleAction` 属性中搜索匹配项。这些值可以是“允许” (Allow)、“阻止” (Block)、“信任” (Trust)。
  - 对于文件事件类型，过滤器在 `FileAction` 属性中搜索匹配项。这些值可以是“允许”、“阻止”、“信任”。
  - 对于入侵事件类型，过滤器在 `InLineResult` 属性中搜索匹配项。这些值可以是“已允许” (Allowed)、“已阻止” (Blocked)、“已信任” (Trusted)。
  - 对于恶意软件事件类型，过滤器会在 `FileAction` 属性中搜索匹配项。这些值可以是“云查找超时” (Cloud Lookup Timeout)。
  - 对于系统日志和 NetFlow 事件类型，过滤器在操作属性中搜索匹配项。
- **传感器 ID (Sensor ID)** - 传感器 ID 是将事件发送到安全事件连接器的管理 IP 地址。  
对于 FDM 管理设备，传感器 ID 通常是设备管理接口的 IP 地址。
- **IP 地址**
  - **发起方 (Initiator)** - 这是网络流量源的 IP 地址。发起方地址字段的值对应于事件详细信息中发起方 IP 字段的值。您可以输入单个地址（例如 10.10.10.100）或以 CIDR 表示法定义的网络（例如 10.10.10.0/24）。
  - **响应方 (Responder)** - 这是流数据包的目的 IP 地址。“目的地址” (Destination address) 字段的值对应于事件详细信息中 ResponderIP 字段中的值。您可以输入单个地址（例如 10.10.10.100）或以 CIDR 表示法定义的网络（例如 10.10.10.0/24）。
- **端口**
  - **发起方 (Initiator)** - 会话发起方使用的端口或 ICMP 类型。源端口的值对应于事件详细信息中的发起方端口的值。（添加范围 - 起始端口和结束端口之间的空格或发起方和响应方）
  - **响应方 (Responder)** - 会话响应方使用的端口或 ICMP 代码。目标端口的值对应于事件详细信息中的 ResponderPort 值。

- **NetFlow - ASA 设备的 NetFlow 安全事件日志记录 (NSEL)** 事件不同于系统日志事件。NetFlow 过滤器搜索生成 NSEL 记录的所有 NetFlow 事件 ID。这些“NetFlow 事件 ID”在《思科 ASA NetFlow 实施指南》中进行了定义。

**步骤 6**（可选）点击查看选项卡，将过滤器另存为自定义过滤器。

---

## 仅过滤 NetFlow 事件

此程序仅查找 ASA NetFlow 事件：

**步骤 1** 从 CDO 菜单栏中，选择 **分析 (Analytics) > 事件日志记录 (Event Logging)**。

**步骤 2** 点击过滤器图标  并将过滤器固定为打开状态。

**步骤 3** 检查 **Netflow ASA 事件过滤器**。

**步骤 4** 清除所有其他 ASA 事件过滤器。

事件日志记录表中仅显示 ASA NetFlow 事件。

---

## 过滤 ASA 或 FDM 管理设备系统日志事件，但不过滤 ASA NetFlow 事件

此过程仅查找系统日志事件：

**步骤 1** 从 CDO 菜单栏中，选择 **分析 (Analytics) > 事件日志记录 (Event Logging)**。

**步骤 2** 点击过滤器图标  并将过滤器固定为打开状态。

**步骤 3** 滚动到过滤器栏的底部，并确保取消选中包括 **NetFlow 事件 (Include NetFlow Events)** 过滤器。

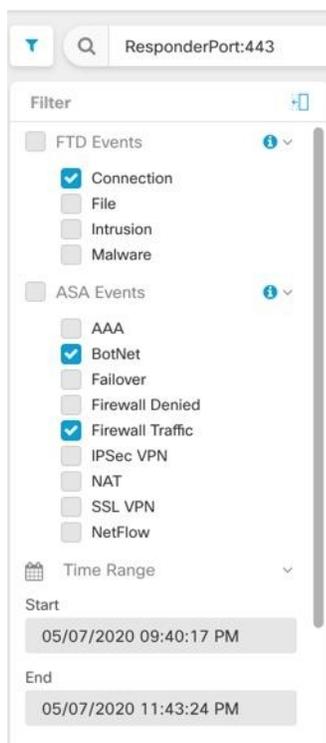
**步骤 4** 向上滚动到 ASA 事件过滤器树，并确保 **取消选中 NetFlow** 框。

**步骤 5** 选择 ASA 其余部分或 FTD 过滤条件。

---

## 组合过滤器元素

过滤事件通常遵循 CDO 中的标准过滤规则：过滤类别为“AND-ed”，类别中的值“OR-ed”。您还可以将过滤器与您自己的搜索条件配合使用。对于事件过滤器；但是，设备事件过滤器也是“OR-ed”。例如，如果在过滤器中选择了这些值：



使用此过滤器时，CDO 将显示 威胁防御 设备连接事件或 ASA 僵尸网络或防火墙流量事件，以及时间范围内两个时间之间发生的事件，并且还包含响应器端口 443 的事件。您可以按时间范围内的历史事件进行过滤。实时事件页面会始终显示最新事件。

#### 搜索特定属性：值对

您可以通过在搜索字段中输入事件属性和值来搜索实时或历史事件。执行此操作的最简单方法是在“事件日志记录” (Event Logging) 表中点击要搜索的属性，然后 CDO 会在“搜索” (Search) 字段中输入该属性。在滚动鼠标时，您可以点击的事件会显示为蓝色。以下为输出示例：

### Event Logging

Date/Time	Device Type	Event Type	Sensor ID / Hostname	Initiator IP																								
May 3, 2023, 7:23:40 PM	ASA	3																										
<table border="0"> <tr> <td>Action</td> <td>Deny</td> <td>IngressACLID</td> </tr> <tr> <td>ConnectorID</td> <td>08c0a888-b619-4f1a-a655-d4 bd005dd8c8</td> <td>IngressInterface</td> </tr> <tr> <td>DeviceType</td> <td>ASA</td> <td>InitiatorIP</td> </tr> <tr> <td>EgressInterface</td> <td>4</td> <td>InitiatorPort</td> </tr> <tr> <td>EventType</td> <td>3</td> <td>LastPacketSecond</td> </tr> <tr> <td>FirewallExtendedEvent</td> <td>1001</td> <td>MappedInitiatorIP</td> </tr> <tr> <td>ICMPCode</td> <td>0</td> <td>MappedInitiatorPort</td> </tr> <tr> <td>ICMPType</td> <td>0</td> <td>MappedResponderIP</td> </tr> </table>					Action	Deny	IngressACLID	ConnectorID	08c0a888-b619-4f1a-a655-d4 bd005dd8c8	IngressInterface	DeviceType	ASA	InitiatorIP	EgressInterface	4	InitiatorPort	EventType	3	LastPacketSecond	FirewallExtendedEvent	1001	MappedInitiatorIP	ICMPCode	0	MappedInitiatorPort	ICMPType	0	MappedResponderIP
Action	Deny	IngressACLID																										
ConnectorID	08c0a888-b619-4f1a-a655-d4 bd005dd8c8	IngressInterface																										
DeviceType	ASA	InitiatorIP																										
EgressInterface	4	InitiatorPort																										
EventType	3	LastPacketSecond																										
FirewallExtendedEvent	1001	MappedInitiatorIP																										
ICMPCode	0	MappedInitiatorPort																										
ICMPType	0	MappedResponderIP																										

在本示例中，通过滚动“InitiatorIP”值 10.10.11.11 并点击它即可开始搜索。发起方 IP 及其值已被添加到搜索字符串中。接下来，滚动并点击事件类型 3，然后将其添加到搜索字符串中，并且 CDO 添加了 AND。因此，此搜索的结果将是 10.10.11.11 和 3 种事件类型发起的事件列表。

请注意上面示例中值 3 旁边的放大镜。如果将鼠标悬停在放大镜上，您还可以选择 AND、OR、AND NOT 和 OR NOT 运算符来匹配要添加到搜索中的值。

在下面的示例中，选择的是“OR”。此搜索的结果将是 10.10.11.11 或 106023 种事件类型发起的事件列表。请注意，如果搜索字段为空，并且您右键点击表中的值，则只有 NOT 可用，因为没有其他值。

The screenshot shows the 'Event Logging' interface. At the top, there are tabs for 'Historical' and 'Live', and a search bar containing 'InitiatorIP: "10.10.11.11" AND EventType: "3"'. Below the search bar is a 'Time Range' filter set to 'After 05/03/2023 07:23:40 PM'. A 'Views' section shows 'View 1' selected. The main table displays event details for May 3, 2023, 7:23:40 PM on an ASA device. A dropdown menu is open over the 'Event Type' field, showing options: AND, OR, NOT, AND NOT, and OR NOT. The 'AND' option is highlighted in blue. The table columns are Date/Time, Device Type, Event Type, Sensor ID / Hostname, and Initiator IP. The table rows include Action (Deny), ConnectorID (08c0a888-b619-41bd005dd8c8), DeviceType (ASA), EgressInterface (4), EventType (3), FirewallExtendedEvent (1001), ICMPCode (0), and ICMPType (0).

Date/Time	Device Type	Event Type	Sensor ID / Hostname	Initiator IP
May 3, 2023, 7:23:40 PM	ASA	3		
Action	Deny		IngressACLID	
ConnectorID	08c0a888-b619-41bd005dd8c8		IngressInterface	
DeviceType	ASA		InitiatorIP	
EgressInterface	4		InitiatorPort	
EventType	3		LastPacketSecond	
FirewallExtendedEvent	1001		MappedInitiatorIP	
ICMPCode	0		MappedInitiatorPort	
ICMPType	0		MappedResponderIP	

只要滚动鼠标指针并将其突出显示为蓝色，您就可以将该值添加到搜索字符串中。

### AND、OR、NOT、AND NOT 和 OR NOT 过滤器运算符

以下是在搜索字符串中使用的“AND”、“OR”、“NOT”、“AND NOT”和“OR NOT”的行为：

和

在过滤器字符串中使用 AND 运算符可以查找包含所有属性的事件。AND 运算符不能位于搜索字符串的开头。

例如，下面的搜索字符串将搜索包含 TCP 协议、源自发起方 IP 地址 10.10.10.43 且从发起方端口 59614 发送的事件。正常情况下，每增加一个 AND 语句，符合条件的事件数量就会越来越少。

```
Protocol: "tcp" AND InitiatorIP: "10.10.10.43" AND InitiatorPort: "59614"
```

或

在过滤器字符串中使用 OR 运算符可以查找包含任何属性的事件。OR 运算符不能位于搜索字符串的开头。

例如，下面的搜索字符串将在事件查看器中显示事件，这些事件包括 TCP 协议、源自发起方 IP 地址 10.10.10.43 或从发起方端口 59614 发送的事件。正常情况下，每增加一个 OR 语句，符合条件的事件数量就会越来越多。

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR InitiatorPort: "59614"
```

不

仅在搜索字符串的开头使用此选项，以便排除具有某些属性的事件。例如，此搜索字符串将从结果中排除任何具有 InitiatorIP 192.168.25.3 的事件。

```
NOT InitiatorIP: "192.168.25.3"
```

### AND NOT

在过滤器字符串中使用 AND NOT 运算符可以排除包含某些属性的事件。AND NOT 不能用于搜索字符串的开头。

例如，此过滤器字符串将显示发起方 IP 为 192.168.25.3 的事件，但不会显示响应方 IP 地址为 10.10.10.1 的事件。

```
InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

您还可以组合使用 NOT 和 AND NOT，从而排除多个属性。例如，此过滤器字符串将排除具有 InitiatorIP 192.168.25.3 的事件以及具有 ResponderIP 10.10.10.1 的事件

```
NOT InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

### OR NOT

使用 OR NOT 运算符可包含排除了某些元素的搜索结果。OR NOT 运算符不能用于搜索字符串的开头。

例如，此搜索字符串将查找协议为 TCP 或发起方 IP 为 10.10.10.43 的事件，或者非发起方端口 59614 的事件。

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR NOT InitiatorPort: "59614"
```

您也可以这样考虑：搜索 (Protocol: "tcp") OR (InitiatorIP: "10.10.10.43") OR (NOT InitiatorPort: "59614")。

### 通配符搜索

使用星号 (\*) 表示属性值字段中的 **attribute:value** 搜索可在事件中查找结果。例如，此过滤器字符串，

```
URL: *feedback*
```

将在事件的 URL 属性字段中查找包含字符串 **feedback** 的字符串。

相关信息：

- [在事件日志记录页面上显示和隐藏列](#)
- [安全分析和日志记录中的事件属性](#)

## 在后台搜索历史事件

通过CDO，您可以定义搜索条件，并根据任何已定义的搜索条件来搜索事件日志。通过使用后台搜索功能，您还可以在后台执行事件日志搜索，并在后台搜索完成后查看搜索结果。

根据您的配置的订用警报和服务集成，当后台搜索完成后，您会收到通知。

您可以直接从“后台搜索”页面查看、下载或删除搜索结果。您还可以安排对一次性事件进行后台搜索，或安排周期性安排。导航至“通知设置”(Notification Settings)页面以查看或修改订用选项。

## 在事件日志记录页面中搜索事件

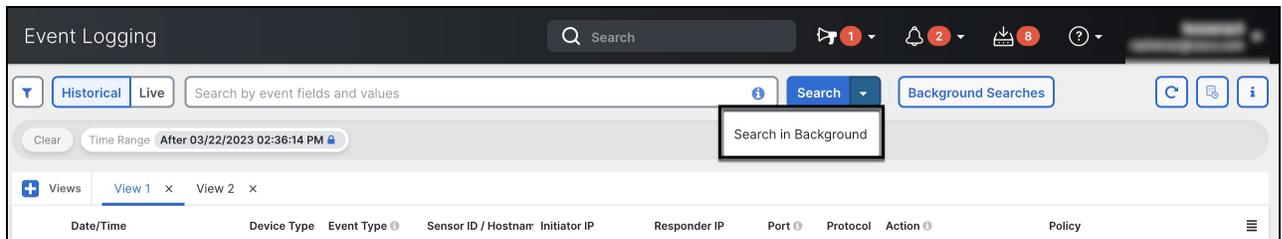
使用搜索和后台搜索功能查看“事件日志记录”(Event Logging)页面中记录的所有事件。请注意，只能对历史事件执行后台搜索。

**步骤 1** 在导航栏中，选择 **分析 (Analytics) > 事件日志记录 (Event Logging)**。

**步骤 2** 点击 **历史 (Historical)** 或 **实时 (Live)** 选项卡。

**步骤 3** 导航至搜索栏，键入搜索表达式，然后输入 **搜索 (Search)** 按钮以执行搜索。您可以使用绝对时间范围或相对时间范围来缩小或扩大搜索范围。

或者，从搜索下拉列表中选择在后台搜索，以便在离开搜索页面时在后台执行搜索。当搜索结果准备就绪时，您会收到通知。



如果点击**搜索 (Search)**按钮，结果将直接显示在事件日志记录视图中。选择任何特定搜索结果后，搜索条件会显示在搜索栏中，以便于参考。

如果您选择在后台执行搜索，搜索操作会加入队列，并在搜索完成后通知您。您可以在后台执行多个搜索查询。

**步骤 4** 点击“背景搜索”按钮以查看“背景搜索”页面。

Background Searches ✕

[Start a Background Search](#) [View Notification Settings](#)

Search Name	File Size	User	Status	Run Time	Actions
<input type="checkbox"/> Search_1679428080471	3.74 KB	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 3:48:03 PM Completed in 2 seconds	<a href="#">View</a> <a href="#">Download</a> <a href="#">...</a>
<input type="checkbox"/> Search_1679428045727	3.74 KB	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 3:47:27 PM Completed in 2 seconds	<a href="#">View</a> <a href="#">Download</a> <a href="#">...</a>
<input type="checkbox"/> Search_1679427993327	2.25 KB	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 3:46:35 PM Completed in 2 seconds	<a href="#">View</a> <a href="#">Download</a> <a href="#">...</a>
<input type="checkbox"/> Search_167942230313	662 Bytes	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 1:58:39 PM Completed in 3 seconds	<a href="#">View</a> <a href="#">Download</a> <a href="#">...</a>
<input type="checkbox"/> Search_1679408015574	662 Bytes	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 10:13:44 AM Completed in 3 seconds	<a href="#">View</a> <a href="#">Download</a> <a href="#">...</a>

[Close](#)

“后台搜索”页面显示搜索结果列表。您可以选择查看、下载或删除搜索结果。您还可以导航至“通知设置”页面以查看或修改订阅选项。选择开始后台搜索 (**Start a Background Search**) 按钮可从此页面启动搜索。

### 下一步做什么

如果需要重复查询，您可以将任何后台搜索转换为计划后台搜索。有关详细信息，请参阅[在事件查看器中计划后台搜索，第 118 页](#)。

## 在事件查看器中计划后台搜索

在事件查看器页面的后台计划定期查询。只能为历史事件安排搜索。您可以随时修改或取消预定搜索。您还可以将现有查询修改为周期性搜索。



**注释** 您可以选择获取有关已开始、已完成或已失败的搜索的警报。

只能为历史事件安排后台搜索。使用以下步骤创建计划的后台搜索：

- 步骤 1** 在导航栏中，选择分析 (**Analytics**) > 事件日志记录 (**Event Logging**)。
- 步骤 2** 点击**历史 (Historical)** 开关将其选中。您只能为历史事件安排后台搜索。
- 步骤 3** 在搜索栏中，键入要搜索的搜索表达式。点击**搜索 (Search)** 下拉按钮，然后选择在后台搜索 (**Search in background**)。
- 步骤 4** (可选) 重命名搜索。
- 步骤 5** 默认情况下，**立即搜索 (Search Now)** 复选框处于选中状态。如果已选中，将在保存时开始搜索；如果取消选中，则后台查询仅作为未来搜索运行。
- 步骤 6** 检查设置定期计划 (**Setup recurring schedule**) 并配置以下设置：
  - **搜索最近日志 (Search Logs for the Last)** - 要搜索多长时间以前的日志。
  - **频率 (Frequency)** - 您希望进行预定搜索的频率。

**步骤 7** 确认窗口底部的计划搜索条件。选择**计划并立即搜索 (Schedule and Search Now)**。或者，如果您没有选择立即开始搜索，则该按钮显示为**计划搜索 (Schedule Search)**

### 下一步做什么

计划后台搜索的结果最多可查看 7 天，然后 CDO 会自动将其删除。

## 下载后台搜索

搜索结果和计划查询会在 CDO 自动删除之前存储 7 天。下载对历史事件执行的后台搜索的 CSV 副本。

**步骤 1** 在导航窗格中，转到**分析 (Analytics) > 事件日志记录 (Event Logging)**。

**步骤 2** 点击**后台搜索 (Background Searches) > 操作 (Actions) > 下载 (Download)**。

**步骤 3** 找到您的搜索内容。计划的搜索存储在**查询 (Queries)** 选项卡下。

**步骤 4** 点击 **Download**。CSV 文件会自动下载到本地驱动器上的默认存储位置。

## 数据存储计划

您需要购买反映思科云每天从您载入的 ASA 和 FDM 托管设备接收的事件数量的数据存储计划。这称为“每日注入速率”。数据计划有整数 GB/天和 1 年、3 年或 5 年期限。确定注入速率的最佳方法是在购买之前参加安全日志分析 (SaaS) 的免费试用。这将为您提供对事件数量的一个很好的估计。

客户自动获得 90 天的滚动数据存储。这意味着最近 90 天的事件存储在思科云中，第 91 天将被删除。

客户可以升级到超过默认 90 天的额外事件保留，或通过更改订单对现有订用添加额外的每日量 (GB/天)，并且只需按比例对剩余的订用期限计费。

有关数据计划的所有详细信息，请参阅《[安全日志分析 \(SaaS\) 订购指南](#)》。



**Note** 如果您拥有安全分析和日志记录许可证和数据计划，然后在之后获得了不同的安全分析和日志记录许可证，则无需获得不同的数据计划。如果您的网络流量吞吐量发生变化，并且您获得了不同的数据计划，则不需要您获得不同的安全分析和日志记录许可证。

### 我的配额会统计哪些数据？

发送到安全事件连接器的所有事件都在安全日志分析 (SaaS) 云中累积，并根据您的数据分配进行计数。

过滤您在事件查看器中看到的内容并不会减少安全日志分析 (SaaS) 云中存储的事件数量，而是会减少您可以在事件查看器中看到的事件数量。

您的事件在安全日志分析 (SaaS) 云中存储 90 天；之后，它们将被清除。

我们的存储配额很快用尽，我们该怎么办？

以下是解决该问题的两种方法：

- 请求更多存储空间。<https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html>您可能低估了您的需求。
- 减少记录事件的规则数量。您可以从 SSL 策略规则、安全情报规则、访问控制规则以及入侵策略以及文件和恶意软件策略中记录事件。检查您正在记录的内容。您是否需要记录尽可能多的规则和策略的事件？

## 延长事件存储持续时间并增加事件存储容量

安全分析和日志记录客户在购买任何这些许可证时都会收到 90 天的事件存储。[许可，第 8 页](#)

- 日志记录故障排除
- 日志记录分析和检测
- 全面的网络分析和监控

您可以选择在首次购买许可证时或在许可证有效期内的任何时间将许可证升级为具有 1 年、2 年或 3 年的滚动事件存储。

首次购买安全分析和日志记录许可证时，系统会询问您是否要升级存储容量。如果您回答“是”，系统会在您购买的 PID 列表中添加一个额外的产品标识符 (PID)。

如果您在许可期限中间决定扩展滚动事件存储或增加事件云存储量，您可以：

---

**步骤 1** 在[思科商务工作空间](#)上登录您的账户。

**步骤 2** 选择您的 Cisco Defense Orchestrator PID。

**步骤 3** 按照提示升级存储容量的长度或容量。

增加的成本将根据现有许可证的剩余期限按比例分配。有关详细说明，请参阅《[安全日志分析\(SaaS\) 订购指南](#)》。

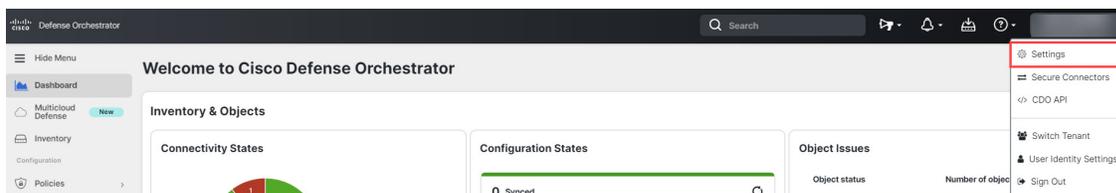
---

## 查看安全分析和日志记录数据计划的使用情况

要查看每月的日志记录限制、已使用的存储量以及使用期何时重置为零，请执行以下操作：

---

**步骤 1** 点击租户，选择设置 (Settings)。



**步骤 2** 点击日志记录设置 (Logging Settings)。

**步骤 3** 您还可以点击查看历史使用情况 (View Historical Usage)，查看最近 12 个月的存储使用情况。

## 查找用于安全日志记录分析 (SaaS) 的设备 TCP、UDP 和 NSEL 端口

安全日志分析 (SaaS) 允许您将事件从您的 ASA 或 FDM 管理设备发送到安全事件连接器 (SEC) 上的某些 UDP、TCP 或 NSEL 端口。然后，SEC 会将这些事件转发到思科云。

如果这些端口尚未被占用，SEC 会将其用于接收事件，而安全日志分析 (SaaS) 文档会建议您在配置功能时使用这些端口。

- TCP: 10125
- UDP: 10025
- NSEL: 10425

如果这些端口已被占用，则在配置安全日志记录分析 (SaaS) 之前，请查看 SEC 设备详细信息，以确定其实际用于接收事件的端口。

要查找 SEC 使用的端口号，请执行以下操作：

**步骤 1** 从 CDO 菜单中，选择 **工具和服务 (Tools & Services) > 安全连接器 (Secure Connectors)**。

**步骤 2** 在“安全连接器” (Secure Connectors) 页面中，选择要向其发送事件的 SEC。

**步骤 3** 在“详细信息” (Details) 窗格中，您将看到应向其发送事件的 TCP、UDP 和 NetFlow (NSEL) 端口。

## Boston-SEC

### Details

<b>ID</b>	54b039f6-8944-46a4-ac07
<b>Tenant ID</b>	0a2cddb4-5e63-4491-9fda
<b>Version</b>	202004270848
<b>IP Address</b>	192.168.25.4
<b>TCP Port</b>	10125
<b>UDP Port</b>	10025
<b>NetFlow Port</b>	10425

## 当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。