



用于 Cisco Secure Network Analytics 7.5.1 的 Cisco Security Analytics and Logging（本地部署）： 防火墙事件集成指南

上次修改日期: 2024 年 12 月 3 日

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



目录

第 1 章

简介 1

概述 1

概念和架构 1

支持的事件类型 2

第 2 章

部署 5

要求 5

Cisco Secure Network Analytics 许可 7

Cisco Secure Network Analytics 资源分配 7

通信端口 9

配置概述 10

Cisco Secure Network Analytics 部署和配置 11

Data Store 部署和配置 11

Cisco Secure Firewall Management Center 配置 12

在 Cisco Secure Firewall Management Center 中配置向导 12

配置 Cisco Secure Firewall Management Center 以便将事件数据发送到 Data Store 部署 13

配置 Cisco Secure Firewall Management Center 以便使用系统日志将数据平面事件日志发送至 Cisco Secure Network Analytics 16

停止在管理中心上存储低优先级连接事件 16

ASA 设备配置 17

从 ASA 设备发送系统日志事件的 CLI 命令 18

用于从 ASA 设备发送系统日志事件的 ASDM 配置 20

从 ASA 设备发送系统日志事件的 CSM 配置 21

第 3 章

后续步骤 25

后续步骤 25

在管理中心和使用存储在 Cisco Secure Network Analytics 设备上的连接事件上工作 25

使用交叉启动调查事件 26

附录 A:

故障排除 29

故障排除 29



第 1 章

简介

- [概述，第 1 页](#)

概述

本指南介绍如何配置 Cisco Security Analytics and Logging（本地部署）以存储防火墙事件数据，从而在更长的保留期内增加存储量。通过部署 Cisco Secure Network Analytics（前身为 Stealthwatch）设备并将其与防火墙部署集成，您可以将事件数据导出到 Cisco Secure Network Analytics 设备。

然后，您可以：

- 将事件存储在 Cisco Secure Firewall Management Center 上，并将事件存储在 Cisco Secure Network Analytics 部署上。
- 指定此远程数据源以便在管理中心查看这些事件。
- 使用事件查看器从 Cisco Secure Network Analytics 管理器（前身为 Stealthwatch 管理控制台）Web App UI 查看事件数据。
- 从管理中心 UI 交叉启动到事件查看器，以便查看有关交叉启动信息的其他情景。



注释 如果要将防火墙事件数据存储在思科云中而不是内部部署，请参阅 [Cisco Security Analytics and Logging \(SaaS\) 文档](#) 了解详细信息。

概念和架构

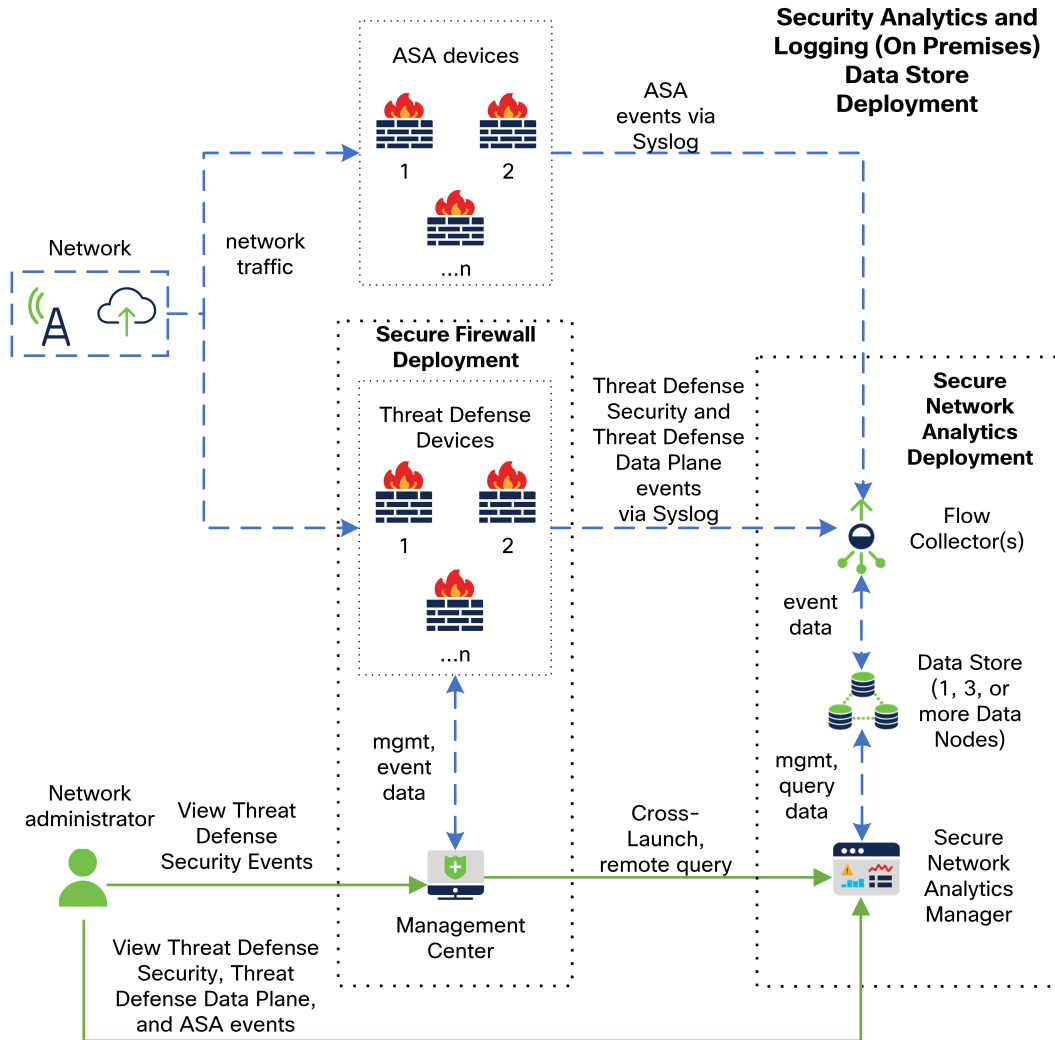
在 Security Analytics and Logging (OnPrem) 部署中，您可以使用 Cisco Secure Network Analytics 设备存储来自其他思科产品部署。在 Cisco Secure Firewall 部署中，您可以将安全事件和数据平面事件从管理中心托管的 Cisco Secure Firewall Threat Defense 设备导出到管理器，以便存储这些信息。

您可以按如下方式部署 Cisco Secure Network Analytics：

- Data Store - 部署 Cisco Secure Network Analytics 流量收集器（最多 5 个）以接收事件，部署包含 1、3 或更多（3 个一组）Cisco Secure Network Analytics 数据节点的 Cisco Secure Network Analytics Data Store 以存储事件，以及可从中查看和查询事件的管理器

Data Store

有关具有 管理器、数据节点和流量收集器的 Data Store 部署示例，请参阅下图：



在该部署中，威胁防御和 Cisco Secure Firewall ASA 设备会向流量收集器发送防火墙事件。流量收集器会将事件发送到 Data Store 进行存储。从管理中心 UI 中，用户可以交叉启动到管理器以查看有关存储事件的更多信息。他们还可以远程查询来自管理中心的事件。

支持的事件类型

- 威胁防御 安全事件
 - 连接事件

- 入侵
- 文件和恶意软件
- 威胁防御数据平面事件
- ASA 事件



第 2 章

部署

- 要求，第 5 页
- 配置概述，第 10 页
- Cisco Secure Network Analytics 部署和配置，第 11 页
- Cisco Secure Firewall Management Center配置，第 12 页
- ASA 设备配置，第 17 页

要求

以下列出了部署 Security Analytics and Logging (OnPrem) 以存储防火墙事件数据的设备要求。

防火墙设备

您必须部署以下防火墙设备：

解决方案组件	需要的版本	Security Analytics and Logging (OnPrem) 的许可	说明
Cisco Secure Firewall Management Center (硬件或虚拟)	v7.2+ 有关运行较早版本的管理中心，请参阅 https://cisco.com/go/sal-on-prem-docs 。	无	<ul style="list-style-type: none">• 您可以为每个管理中心部署一个管理器，也可以选择部署多个流量收集器和数据节点。
Cisco Secure Firewall 托管设备	v7.0+，使用向导 威胁防御 v6.5 或更高版本，使用系统日志 NGIPS v6.5，使用系统日志	无	<ul style="list-style-type: none">• 有关如何使用威胁防御 v6.5 的系统日志的说明，请参阅 从早期版本的威胁防御设备发送事件。
ASA 设备	v9.12+	none	

Cisco Secure Network Analytics 设备

您可以按如下方式部署 Cisco Secure Network Analytics:

- **Data Store** - 部署流量收集器以注入事件，部署 Data Store 来存储事件，以及部署 管理器 来查看和查询事件

表 1: **Data Store**

解决方案组件	需要的版本	Security Analytics and Logging (OnPrem) 的许可	说明
管理器	Cisco Secure Network Analytics v7.5.1	无	<ul style="list-style-type: none"> • 单节点 Data Store 和多遥测需要使用 Cisco Secure Network Analytics v7.5.1,
流量收集器	Cisco Secure Network Analytics v7.5.1	无	<ul style="list-style-type: none"> • 您最多可以部署 5 个为 Data Store 配置的流量收集器。 • 流量收集器可以从多个威胁防御设备接收事件，所有均由一个管理中心管理。 • 流量收集器可以从多个 ASA 设备接收 ASA 事件。 • 单节点 Data Store 和多遥测需要使用 Cisco Secure Network Analytics v7.5.1。
Data Store	Cisco Secure Network Analytics v7.5.1	无	<ul style="list-style-type: none"> • 您可以部署 1、3 或更多（以 3 个为一组）数据节点。 • 存储由流量收集器接收的防火墙事件。 • 单节点 Data Store 和多遥测需要使用 Cisco Secure Network Analytics v7.5.1。

除了这些组件之外，您还必须确保所有设备都可以使用 NTP 来同步时间。

如果要远程访问 Cisco Secure Firewall 或 Cisco Secure Network Analytics 设备的控制台，您可以启用通过 SSH 访问。

Cisco Secure Network Analytics 许可

在评估模式下，Security Analytics and Logging (OnPrem) 可以在没有许可证的情况下使用 90 天。若要在 90 天后继续使用 Security Analytics and Logging (OnPrem)，根据预期每天会从防火墙部署向 Cisco Secure Network Analytics 设备发送系统日志数据的 GB 数，您必须为智能许可获取日志记录和故障排除智能许可证。



注释 出于许可证计算的目的，数据量会以最接近的整数 GB 来报告（往下舍入）。例如，如果一天会发送 4.9 GB，则报告为 4 GB。

有关许可 Cisco Secure Network Analytics 设备的详细信息，请参阅《[Cisco Secure Network Analytics 智能软件许可指南](#)》。

Cisco Secure Network Analytics 资源分配

为 Security Analytics and Logging (OnPrem) 部署时，Cisco Secure Network Analytics 提供以下注入速率：

- 包含 3 个数据节点的虚拟版 (VE) Data Store 部署平均可注入大约 5 万个 EPS，短时间内可迅速达到 17.5 万个 EPS
- 包含 3 个数据节点的硬件 Data Store 部署平均可以注入大约 15 万个 EPS 并开启 Security Analytics and Logging (OnPrem) 和 `sal_to_flow_cache`

根据分配的硬盘驱动器存储，您可以将数据存储数周或数月。这些估计值受各种因素影响，包括网络负载、流量峰值和每个事件传输的信息。



注释 在较高的 EPS 注入速率下，Security Analytics and Logging (OnPrem) 可能会丢弃数据。此外，如果发送所有事件类型，而不是仅发送连接、入侵、文件和恶意软件事件，则 Security Analytics and Logging (OnPrem) 可能会随着您的整体 EPS 上升而丢弃数据。在这种情况下，查看日志文件。

Data Store 建议

为获得最佳性能，请在部署 管理器 VE、流量收集器 VE 和 Data Store VE 时分配以下资源：



注释 如果您使用的是单节点 Data Store，或者已在 Cisco Secure Network Analytics 中启用多遥测，则您的资源分配和存储容量可能与以下建议不同。有关详细信息，请参阅《《[Cisco Secure Network Analytics 设备安装指南（硬件或虚拟版）](#)和[系统配置指南 v7.5.1](#)》。

表 2: 管理器 VE

Resource	信息提示
CPU	8
RAM	64 GB
硬盘驱动器存储	480 GB

表 3: 流量收集器 VE

Resource	信息提示
CPU	8
RAM	70 GB
硬盘驱动器存储	480 GB

表 4: 数据节点 VE（作为 Data Store 的一部分）

Resource	信息提示
CPU	每个数据节点 12 个
RAM	每个数据节点 32 GB
硬盘驱动器存储	每个数据节点 VE 5 TB，或 3 个数据节点总共 15 TB

硬件规格

有关硬件规格，请参阅[设备规格表](#)。

预计保留（3 个数据节点）

根据您为 Data Store VE 分配的存储空间，或者如果您有硬件部署，您可以在 Data Store 部署中大致按以下时间范围来存储数据：

平均 EPS	平均每日事件数	虚拟	硬件
1,000	8650 万	1,500 天	3,000 天
5,000	4.3 亿	300 天	600 天

平均 EPS	平均每日事件数	虚拟	硬件
10,000	8.65 亿	150 天	300 天
2 万	17.3 亿	75 天	150 天
25,000	21.6 亿	60 天	120 天
50000	43.2 亿	30 天	60 天
75,000	64.8 亿	不支持	40 天
100,000	86.4 亿	不支持	30 天

当 Data Store 达到最大存储容量时，它会首先删除最早的数据，以便为传入数据腾出空间。要增加存储容量，请使用《[Cisco Secure Network Analytics 系统配置指南](#)》添加更多数据节点。



注释 我们已在此估计的注入和存储期间使用这些资源配置对这些虚拟设备进行了测试。如果您没有为虚拟设备分配足够的 CPU 或 RAM，您可能会发现由于资源配置不足而导致的意外错误。如果将数据节点存储分配增加到 5 TB 以上，则可能会发现由于资源配置不足而导致的意外错误。

通信端口

下表列出了必须为 Security Analytics and Logging (OnPrem) 部署的 Data Store 集成打开的通信端口。此外，请参阅《[x2xx 系列硬件设备安装指南](#)》或《[虚拟版设备安装指南](#)》，了解部署 Cisco Secure Network Analytics 必须打开的端口。

表 5: Data Store

从（客户端）	到（服务器）	端口	协议或用途
管理中心、威胁防御设备、管理器、流量收集器和 Data Store	外部互联网（NTP 服务器）	123/UDP	NTP 时间同步，全部同步到同一台 NTP 服务器
用户工作站	管理中心 和 管理器	443/TCP	使用 Web 浏览器通过 HTTPS 登录设备的 Web 界面
由管理中心管理的威胁防御设备	流量收集器	8514/UDP	系统日志从威胁防御设备导出，注入到流量收集器
ASA 设备	流量收集器	8514/UDP	系统日志从 ASA 设备导出，注入到流量收集器

从（客户端）	到（服务器）	端口	协议或用途
管理中心	管理器	443/TCP	从管理中心远程查询到管理器

配置概述

下面介绍了配置部署以存储事件数据的高级步骤。

在开始部署之前，请查看这些任务：

组件和任务	步骤
部署 Data Store	<ul style="list-style-type: none"> 将管理器、流量收集器以及 3 个或更多（以 3 个为一组）数据节点部署到您的网络。对每个设备执行初始配置，然后初始化 Data Store。有关更多信息，请参阅《x2xx 系列硬件设备安装指南》或《虚拟版设备安装指南》以及《Cisco Secure Network Analytics 系统配置指南》。
配置管理中心以便将事件发送到 Security Analytics and Logging (OnPrem)	<p>您有以下选择：</p> <ul style="list-style-type: none"> 按照Cisco Secure Firewall Management Center配置，第 12 页部分配置管理中心，以便将事件发送到 Cisco Secure Network Analytics 设备。 按照配置 Cisco Secure Firewall Management Center 以便使用系统日志将数据平面事件日志发送至 Cisco Secure Network Analytics部分配置数据平面事件日志记录。 按照停止在管理中心上存储低优先级连接事件部分减少管理中心上的日志记录负载。
配置 ASA 设备以便将事件发送到 Security Analytics and Logging (OnPrem)	<ul style="list-style-type: none"> 按照ASA 设备配置，第 17 页部分配置 ASA 设备，以便将事件发送到 Cisco Secure Network Analytics 设备。
查看后续步骤	<p>查看后续步骤：</p> <ul style="list-style-type: none"> 有关详细信息，请查看 Cisco Secure Firewall 在线帮助。请参阅在管理中心和使用存储在 Cisco Secure Network Analytics 设备上的连接事件上工作。。 有关如何使用 Cisco Secure Network Analytics 的详细信息，请查看管理器在线帮助。转到调查 (Investigate) > Security Analytics and Logging (OnPrem)。

Cisco Secure Network Analytics 部署和配置

要为 Security Analytics and Logging (OnPrem) 部署和配置 Cisco Secure Network Analytics，请执行以下操作：

1. 按照 Cisco Secure Network Analytics 部署的说明进行操作：

- [Data Store 部署和配置](#)，第 11 页

Data Store 部署和配置



重要事项 确保启用流量收集器，以便在设备首次设置期间注入和存储防火墙日志。此设置会将流量收集器配置为与 Security Analytics and Logging (OnPrem) 一起使用。配置设备后，您可以使用“流量收集器高级设置” (Flow Collector Advanced Settings) 来更新注入设置。有关详细信息，请参阅[使用流量收集器高级设置进行 Security Analytics and Logging \(本地部署\) 配置](#)部分。

开始之前

- 确保您已在网络中部署了管理器、流量收集器和数据节点，确保威胁防御设备的管理 IP 地址可访问流量收集器管理 IP 地址，并且管理器管理 IP 地址可通过管理中心的管理 IP 地址进行访问。记下管理 IP 地址，以便进一步配置。
- 确保您注册了 Cisco Secure Network Analytics 产品实例。注册后，管理器 VE 许可证会被自动添加到您的帐户中。有关详细信息，请参阅《[Cisco Secure Network Analytics 智能软件许可指南](#)》。

过程

步骤 1 按照《[x2xx 系列硬件设备安装指南](#)》中的说明部署 Cisco Secure Network Analytics 硬件设备，或按照《[虚拟版设备安装指南](#)》中的说明部署 Cisco Secure Network Analytics 虚拟设备。

步骤 2 按照《[Cisco Secure Network Analytics 系统配置指南](#)》配置设备。在流量收集器上配置首次设置时，请确保选择以下选项：

- 当系统要求您将流量收集器部署为 Data Store 的一部分时，选择是 (Yes)。如果选择“否” (No)，则您必须部署新的虚拟设备或对您的设备进行 RFD。
- 在选择遥测类型屏幕上选择防火墙日志 (Firewall Logs)。然后输入 UDP 端口，默认情况下使用 8514。点击是 (Yes) 以确认设置。

Cisco Secure Firewall Management Center配置

为 Security Analytics and Logging (OnPrem) 配置 Cisco Secure Firewall Management Center 时，可以使用以下选项将事件发送到 Cisco Secure Network Analytics:

- 在 [Cisco Secure Firewall Management Center 中配置向导](#) 以便直接向 Cisco Secure Network Analytics 部署发送事件。
- 配置 [Cisco Secure Firewall Management Center](#) 以便使用系统日志将数据平面事件日志发送至 [Cisco Secure Network Analytics](#)。

在 Cisco Secure Firewall Management Center 中配置向导

下面介绍用于为所有 Cisco Secure Firewall Management Center 用户部署 Security Analytics and Logging (OnPrem) 以发送和存储防火墙事件的向导。

- **Data Store:** 部署流量收集器以接收事件、部署 Data Store 以存储事件，以及部署管理器 以便从中查看和查询事件。有关配置 Data Store 部署的详细信息，请参阅 [配置 Cisco Secure Firewall Management Center](#) 以便将事件数据发送到 Data Store 部署。

Cisco Secure Firewall 集成的前提条件

- Cisco Secure Firewall 系统必须按预期工作并生成要发送的事件。
- 将 Cisco Secure Network Analytics 和 Security Analytics and Logging (OnPrem) 产品设置为准备接收防火墙事件数据。
- 您必须具有以下 Cisco Secure Firewall 用户角色之一：
 - 管理
 - 分析师
 - 安全分析师
- 如果您当前使用系统日志将事件从支持直接发送事件的设备版本发送到 Cisco Secure Network Analytics，请禁用这些设备的系统日志（或为这些设备分配不包含系统日志配置的访问控制策略），以避免在远程卷上复制事件。
- 您具有以下详细信息：
 - 管理器 的主机名或 IP 地址。
 - （如果您使用流量收集器汇聚多个 Cisco Secure Network Analytics 设备以扩展存储容量）流量收集器的 IP 地址。（不能将主机名用于此设置。）
 - Cisco Secure Network Analytics 设备上具有管理员权限的帐户的凭证。

这些凭证不存储在管理中心；它们仅用于在管理器上为管理中心建立只读分析师 API 帐户。此集成无需专用帐户；您可以使用自己的管理员凭证。

您可能会在注册过程中从管理器注销；请完成所有正在进行的工作，然后再开始此向导。

- 如果您不想使用“首次使用时信任” (trust on first use) 选项，请从管理器获取 SSL 证书。

配置 Cisco Secure Firewall Management Center 以便将事件数据发送到 Data Store 部署

开始之前

- 确保您满足在 [Cisco Secure Firewall Management Center 中配置向导](#) 中提到的所有要求。
- 托管设备版本为 7.0 或更高版本。

过程

步骤 1 在管理中心中，转到集成 (**Integration**) > **Security Analytics & Logging**。

步骤 2 在 **Data Store** 构件中，点击开始 (**Start**)。

步骤 3 输入管理器的主机名或 IP 地址和端口。

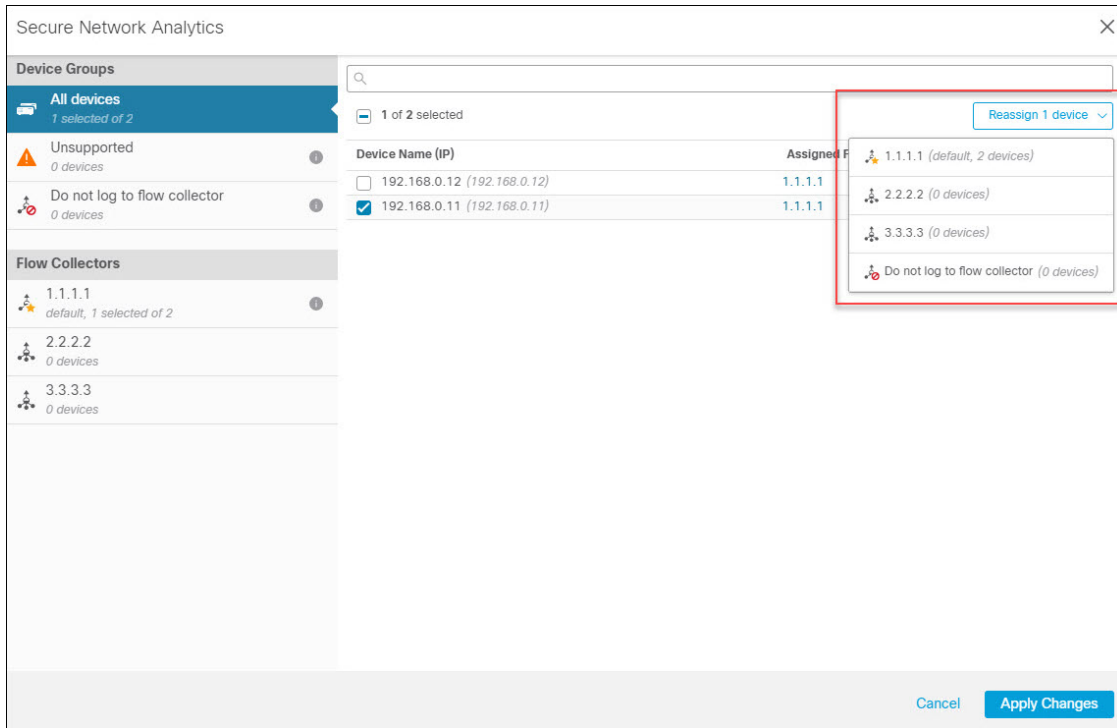
步骤 4 输入流量收集器的主机名或 IP 地址和端口。

要添加更多流量收集器，请点击 **+添加其他流量收集器 (+Add another flow collector)**。

步骤 5 (可选) 如果配置了多个流量收集器，请将托管设备与不同的流量收集器相关联。

默认情况下，所有托管设备都会被分配给默认流量收集器。

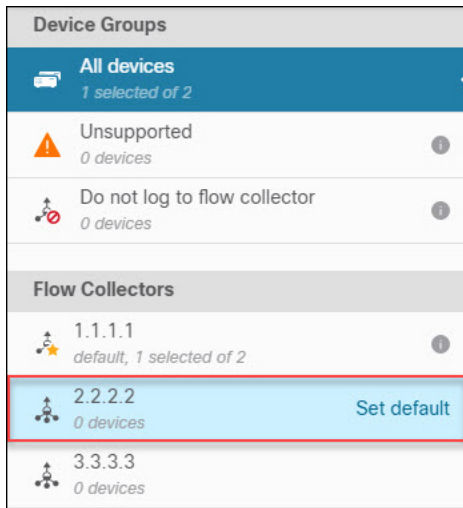
1. 点击分配设备 (**Assign Devices**)。
2. 选择要重新分配的托管设备。
3. 从重新分配设备下拉列表中选择流量收集器。



如果您不希望托管设备将事件数据发送到任何流量收集器，请选择该设备，然后从重新分配设备的下拉列表中选择不记录到流量收集器 (**Do not log to flow collector**)。

注释

您可以通过将鼠标悬停在预期的流量收集器上并点击**设置默认值 (Set default)** 来更改默认流量收集器。



4. 点击 **Apply Changes** (应用更改)。

步骤 6 点击下一步 (**Next**)。

步骤 7 确认发现的设置。

1. 验证交叉启动 URL 和端口，并在必要时进行修改。
2. 如果您不想使用“首次使用时信任” (trust on first use) 选项，请从管理器上传 SSL 证书。

注释

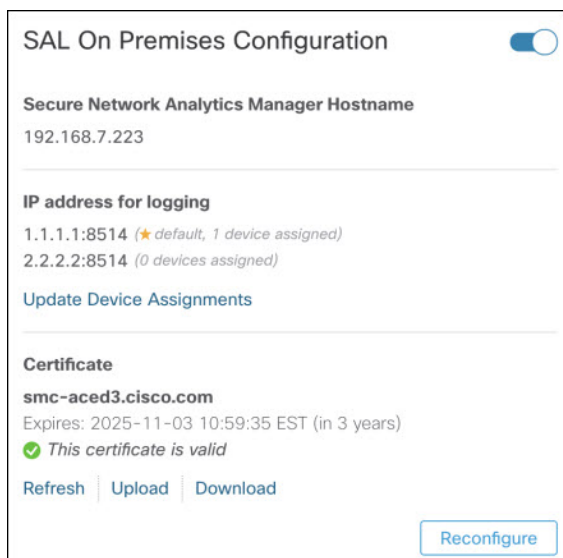
有关如何获取和上传 SSL 证书的详细信息，请参阅 [Cisco Secure Network Analytics: 托管设备的 SSL/TLS 证书](#)。

3. 点击下一步。

步骤 8 输入凭证登录管理器，以便为查询建立安全通信，然后点击**完成 (Complete)**。

这些凭证不存储在管理中心；它们仅用于在管理器上为管理中心建立只读分析师 API 帐户。此操作无需专用帐户；您可以使用自己的管理员凭证。

保存配置后，您可以通过点击 **Security Analytics & Logging** 页面上的**更新设备分配 (Update Device Assignments)** 来更新设备分配。



下一步做什么

- 启用使用 [配置 Cisco Secure Firewall Management Center](#) 以便使用系统日志将数据平面事件日志发送至 [Cisco Secure Network Analytics](#)，第 16 页 发送数据平面事件日志。
- 在确认事件已成功存储在 [Cisco Secure Network Analytics](#) 设备上之后等待一段时间，直到您确定管理中心上存储的所有事件也可远程使用。然后，请参阅[停止在管理中心上存储低优先级连接事件](#)。



注释 如果需要更改其中任何配置，请再次运行向导。如果禁用配置或再次运行向导，则会保留除帐户凭证之外的所有设置。

配置 Cisco Secure Firewall Management Center 以便使用系统日志将数据平面事件日志发送至 Cisco Secure Network Analytics

下面介绍如何在设备平台设置策略的 UI 选项中配置 管理中心，以便使用系统日志将数据平面事件日志发送至 Cisco Secure Network Analytics。



注释 Security Analytics and Logging (OnPrem) Data Store 部署支持数据平面事件。

开始之前

确保使用 管理中心 中的 在 Cisco Secure Firewall Management Center 中配置向导来启用将数据平面事件日志记录发送到 Cisco Secure Network Analytics。

过程

步骤 1 启用日志记录。

- 转到系统日志 (Syslog) > 日志记录设置 (Logging Setup) > 基本日志记录设置 (Basic Logging Settings)。
- 选中 **Enable Logging** 复选框。

步骤 2 配置日志记录陷阱。

- 转到系统日志 (Syslog) > 日志记录目标 (Logging Destinations)。
- 点击 + 添加日志记录目标 (+ Add Logging Destination)。
- 对于日志记录目标 (Logging Destination)，请选择系统日志服务器 (Syslog Servers)。
- 对于事件类 (Event Class)，选择按严重性过滤 (Filter on Severity)。
- 选择任何严重性。

步骤 3 配置日志记录设备。

- 转到系统日志 (Syslog) > 系统日志设置 (Syslog Settings) > 设备 (Facility)。
- 对于设备 (Facility)，请选择默认值 = LOCAL4(20) (default = LOCAL4[20])。

停止在 管理中心 上存储低优先级连接事件

绝大多数连接事件与已确定的威胁无关。您可以选择不 在 管理中心 上存储如此大量的事件。

未存储在 管理中心 上的事件不会计入 管理中心 设备的最大流速，如数据表<https://www.cisco.com/c/en/us/products/collateral/security/%20firesight-management-center/datasheet-c78-736775.html> 中所述。

以下连接事件被视为高优先级，并始终存储在 管理中心 上，即使您禁用连接事件的存储也是如此：

- 安全事件

- 与入侵事件关联的连接事件
- 与文件事件关联的连接事件
- 与恶意软件事件关联的连接事件

如果不在管理中心上存储低优先级连接事件，则可以为其他事件类型分配更多存储空间，从而延长调查威胁的时间窗口。此设置不会影响统计信息收集。

此设置适用于此管理中心托管的所有设备中的事件。

开始之前



注意 此程序将立即永久删除管理中心上当前存储的所有连接事件。

在执行此程序之前，请确保您的 Cisco Secure Network Analytics 设备已存在要保留的所有低优先级连接事件。通常，我们建议您在确认管理中心已成功将事件发送到 Cisco Secure Network Analytics 后的某个时间启用此选项。

过程

步骤 1 有两种方法可以停止在管理中心上存储低优先级连接事件：

两种方法的效果相同。

- 完成向 Security Analytics and Logging (OnPrem) 发送事件的向导后，请转至系统 (System) > 日志记录 (Logging) > Security Analytics and Logging，启用在 FMC 上存储更少事件 (Store Fewer Events on FMC) 的选项。
- 转到系统 (System) > 配置 (Configuration) > 数据库 (Database)，找到连接数据库 (Connection Database) 部分，然后将最大连接事件数 (Maximum Connection Events) 设置为零 (0)。

将此值设置为 0 以外的任何值，都会将所有低优先级连接事件计入最大流速。此设置不会影响连接摘要。

步骤 2 保存更改。

下一步做什么

在系统 (System) > 配置 (Configuration) > 数据库 (Database) 页面上提高所有其他事件类型的存储限制。

ASA 设备配置

ASA 系统日志提供有关对 ASA 设备进行监控和故障排除的信息。有关 ASA 事件类型的列表，请参阅[思科 ASA 系列系统日志消息](#)。



注释 Security Analytics and Logging (OnPrem) Data Store 部署支持 ASA 事件存储。

要让 ASA 将系统日志事件发送到 Security Analytics and Logging (OnPrem)，您必须在 ASA 设备上配置日志记录：

- 启用日志记录
- 将输出目标配置为 Cisco Secure Network Analytics 流量收集器



注释 Security Analytics and Logging (OnPrem) 不支持安全日志记录。

从 ASA 设备发送系统日志事件的 CLI 命令

使用以下配置命令将安全事件的系统日志消息从 ASA 设备发送到 Security Analytics and Logging (OnPrem)。

开始之前

- 查看要求和前提条件部分。
- 确认您的 ASA 设备可以访问流量收集器。
- 从管理器上的“集中管理”获取流量收集器 IP 地址和端口号。

过程

步骤 1 启用日志记录：

logging enable

示例：

```
ciscoasa(config)# logging enable
```

步骤 2 指定应将哪些系统日志消息发送到系统日志服务器（流量收集器）：

logging trap {severity_level | message_list}

示例：

您可以指定要发送到流量收集器的系统日志消息的严重性级别编号（1 至 7）或名称：

```
ciscoasa(config)# logging trap errors
```

示例:

此外，您可以指定标识要发送到流量收集器的系统日志消息的自定义消息列表：

```
ciscoasa(config)# logging list specific_event_list message 106100
ciscoasa(config)# logging list specific_event_list message 302013-302018
ciscoasa(config)# logging trap specific_event_list
```

步骤 3 将 ASA 配置为向流量收集器发送消息：

logging host *interface_name syslog_ip [protocol/port]*

示例:

```
ciscoasa(config)# logging host management 209.165.201.3 17/8514
```

注释

1. 对于系统日志 IP 和端口，请指定流量收集器 IP 和相应的系统日志端口号（有关说明，请参阅开始之前部分）。
2. 指定 *17* 以表示 UDP 协议。

步骤 4 （可选）配置系统日志消息中的时间戳格式：

logging timestamp *{rfc5424}*

示例:

```
ciscoasa(config)# logging timestamp
ciscoasa(config)# logging timestamp rfc5424
```

RFC5424 规定的时间戳格式为 *yyyy-MM-TTH:mm:ssZ*，其中字母 *Z* 表示 UTC 时区。

注释

仅 ASA 9.10(1) 支持 RFC5424。

步骤 5 （可选）配置 ASA 以显示带有设备 ID 的系统日志消息：

logging device-id *{cluster-id | context-name | hostname | ipaddress interface_name [system] | string text}*

示例:

```
ciscoasa(config)# logging device-id context-name
```

系统日志服务器使用设备 ID 标识系统日志生成器。只能为系统日志指定一种类型的设备 ID。

用于从 ASA 设备发送系统日志事件的 ASDM 配置

使用以下程序将 ASDM 配置为将安全事件的 ASA 系统日志消息发送至 Security Analytics and Logging (OnPrem)。

开始之前

- 查看要求和前提条件部分。
- 确认您的 ASA 设备可以访问流量收集器。
- 从管理器上的“集中管理”获取流量收集器 IP 地址和端口号。

过程

步骤 1 登录 ASDM。

步骤 2 启用日志记录。

- a) 点击**配置 (Configuration)** > **设备管理 (Device Management)** > **日志记录 (Logging)** > **日志记录设置 (Logging Setup)**。
- b) 选中 **Enable logging** 复选框以开启日志记录。
- c) (可选) 选中以 **EMBLEM 发送系统日志 (Send syslogs in EMBLEM)** 复选框以启用 EMBLEM 日志记录格式。

步骤 3 配置系统日志服务器（流量收集器）的日志过滤设置。

- a) 依次选择**配置 (Configuration)** > **设备管理 (Device Management)** > **日志记录 (Logging)** > **日志记录过滤器 (Logging Filters)**。
- b) 从表中选择系统日志服务器 (**Syslog Servers**)，然后点击**编辑 (Edit)**。
- c) 在**编辑日志记录过滤器 (Edit Logging Filters)** 对话框中，选择下列日志记录过滤器设置之一：

要根据严重性级别过滤系统日志消息，请点击**按严重性过滤 (Filter on severity)**，然后选择严重性级别。

注释

ASA 生成的系统日志信息的严重性级别最高可达指定级别。

或

要根据消息 ID 过滤系统日志消息，请点击**使用事件列表 (Use event list)**。您可以选择使用所需系统日志消息 ID 创建的事件列表，或点击**新建 (New)** 使用系统日志消息 ID 或 ID 范围创建一个列表。

- d) 保存设置。

步骤 4 使用流量收集器地址和端口来配置外部系统日志服务器。

- a) 依次选择**配置 (Configuration)** > **设备管理 (Device Management)** > **日志记录 (Logging)** > **系统日志服务器 (Syslog Server)**。
- b) 点击**添加 (Add)** 以添加新系统日志服务器。
- c) 在**添加系统日志服务器 (Add Syslog Server)** 对话框中，指定以下内容：

- **接口** - 用于与系统日志服务器通信的接口。

- **IP 地址** - 从管理器上的“集中管理”获取的流量收集器 IP。
- **协议** - 选择 UDP。
- **端口** - 相应的流量收集器系统日志端口（默认为 8514）。
- （可选）选中思科 **EMBLEM** 格式的日志消息 (**Log messages in Cisco EMBLEM format**) 复选框以启用 EMBLEM 日志记录格式。

步骤 5 点击保存 (**Save**) 将更改应用于配置。

从 ASA 设备发送系统日志事件的 CSM 配置

使用以下程序将思科安全管理器 (CSM) 配置为将安全事件的 ASA 系统日志消息发送到 Security Analytics and Logging (OnPrem)。

开始之前

- 查看要求和前提条件部分。
- 确认您的 ASA 设备可以访问流量收集器。
- 从管理器上的“集中管理”获取流量收集器 IP 地址和端口号。
- 此集成不支持安全日志记录。

过程

步骤 1 登录思科安全管理器的配置管理器 (**Configuration Manager**) 窗口。

步骤 2 启用系统日志日志记录。

a) 要访问“系统日志日志记录设置” (Syslog Logging Setup) 页面，请执行以下操作之一：

- （设备视图）从策略选择器中依次选择平台 (**Platform**) > 日志记录 (**Logging**) > 系统日志 (**Syslog**) > 日志记录设置 (**Logging Setup**)。
- （策略视图）从策略类型选择器中依次选择路由器平台 (**Router Platform**) > 日志记录 (**Logging**) > 系统日志 (**Syslog**) > 日志记录设置 (**Logging Setup**)。选择现有策略或创建新策略。

b) 在“系统日志日志记录设置” (Syslog Logging Setup) 页面中，选中启用日志记录 (**Enable Logging**) 复选框以打开系统日志日志记录。

c) （可选）选中以 **EMBLEM** 发送系统日志 (**Send syslogs in EMBLEM**) 复选框以启用 EMBLEM 日志记录格式。

d) 点击保存 (**Save**)。

步骤 3 配置系统日志服务器（流量收集器）的日志过滤设置。

- a) 从策略选择器中依次选择平台 (**Platform**) > 日志记录 (**Logging**) > 系统日志 (**Syslog**) > 日志记录过滤器 (**Logging Filters**)。
- b) 从表中选择日志记录目标 (**Logging Destination**) 列下的系统日志服务器 (**Syslog Servers**)，然后点击编辑 (**Edit**)。如果未找到系统日志服务器对象，请点击添加行 (**Add Row**)。
- c) 在添加/编辑日志记录过滤器 (**Add/Edit Logging Filters**) 对话框中，选择下列日志记录过滤器设置之一：
 - 要根据严重性级别过滤系统日志消息，请点击按严重性过滤 (**Filter on severity**)，然后选择严重性级别。
注释
ASA 生成的系统日志信息的严重性级别最高可达指定级别。
 - 要根据消息 ID 过滤系统日志消息，请点击使用事件列表 (**Use event list**)，然后从下拉列表中选择所需的事件列表。
注释
如果未定义任何事件列表，则下拉列表将为空。必须至少定义一个事件列表（平台 (**Platform**) > 日志记录 (**Logging**) > 系统日志 (**Syslog**) > 事件列表 (**Event Lists**)）。
- d) 保存设置。

步骤 4 （可选）配置日志记录参数：

- a) （设备视图）依次选择平台 (**Platform**) > 日志记录 (**Logging**) > 系统日志 (**Syslog**) > 服务器设置 (**Server Setup**)。
- b) 要在系统日志信息中配置时间戳格式，请选中在每个系统日志信息上启用时间戳 (**Enable Timestamp on Each Syslog Message**) 复选框，然后选中启用时间戳格式 (**rfc5424**) (**Enable Timestamp Format[rfc5424]**) 复选框。
注释
仅 ASA 9.10(1) 支持 RFC5424。
- c) （可选）配置 ASA 以显示带有设备 ID 的系统日志消息：
 - 接口 - 点击此单选按钮并选择 ASA 设备的接口。
 - 用户定义的 ID - 点击此单选按钮并输入所需的名称，该名称将添加到 ASA 设备的所有系统日志消息中。
 - 主机名 - 点击此单选按钮，以显示带有设备主机名的系统日志消息。

注释

系统日志服务器使用设备 ID 标识系统日志生成器。只能为系统日志指定一种类型的设备 ID。

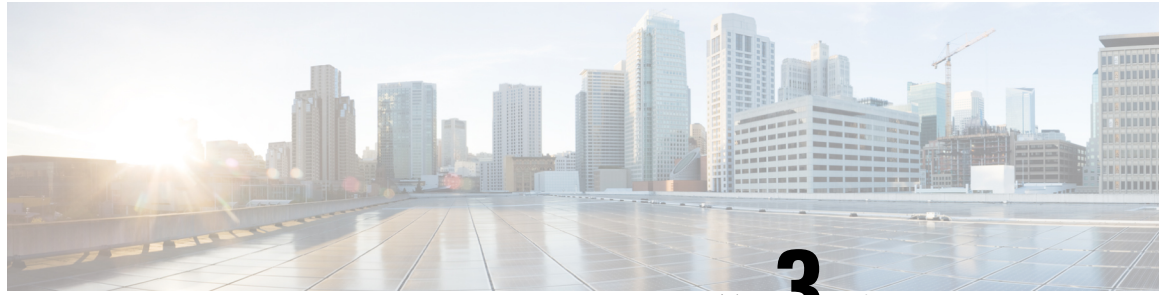
- d) 点击保存 (**Save**)。

步骤 5 配置系统日志消息要发送到的外部日志记录服务器。

- a) 要访问“系统日志服务器” (**Syslog Servers**) 页面，请执行以下操作之一：
 - （设备视图）从策略选择器中依次选择平台 (**Platform**) > 日志记录 (**Logging**) > 系统日志服务器 (**Syslog Servers**)。
 - （策略视图）从策略类型选择器中依次选择路由器平台 (**Router Platform**) > 日志记录 (**Logging**) > 系统日志服务器 (**Syslog Servers**)。选择现有策略或创建新策略。

- b) 点击**添加 (Add)** 以添加新系统日志服务器。
- c) 在**添加/编辑系统日志服务器 (Add/Edit Syslog Server)** 对话框中，指定以下内容：
- **接口** - 用于与系统日志服务器通信的接口。
 - **IP 地址** - 从管理器上的“集中管理”获取的流量收集器 IP。
 - **协议** - 选择 UDP。
 - **端口** - 相应的流量收集器系统日志端口（默认为 8514）。
 - （可选）选中思科 **EMBLEM** 格式的日志消息 (**Log messages in Cisco EMBLEM format**) 复选框以启用 EMBLEM 日志记录格式。
- d) 点击**确定 (OK)** 以保存配置并关闭对话框。表中会显示您定义的系统日志服务器。

步骤 6 提交并部署配置更改。



第 3 章

后续步骤

- [后续步骤](#)，第 25 页
- [在管理中心和使用存储在 Cisco Secure Network Analytics 设备上的连接事件上工作](#)，第 25 页
- [使用交叉启动调查事件](#)，第 26 页

后续步骤

在将防火墙设备配置为将事件数据作为 Security Analytics and Logging (OnPrem) 的一部分发送到 Cisco Secure Network Analytics 设备后，您可以执行以下步骤：

- 查看 [管理中心 在线帮助](#)。
- 查看 [管理器 在线帮助](#)，了解关于 Cisco Secure Network Analytics 的更多信息。转到 [调查 \(Investigate\) > Security Analytics and Logging \(OnPrem\)](#)。

在管理中心和使用存储在 Cisco Secure Network Analytics 设备上的连接事件上工作

如果您的设备正在使用 Security Analytics and Logging (OnPrem) 向 Cisco Secure Network Analytics 设备发送连接事件，您可以在管理中心的事件查看器和情景管理器中查看和使用这些远程存储的事件，并在生成报告时包括这些事件。您还可以从管理中心中的事件交叉启动，以查看 Cisco Secure Network Analytics 设备上的相关数据。

默认情况下，系统会根据您指定的时间范围自动选择适当的数据源。如果要覆盖数据源，请使用此程序。



重要事项 当您更改数据源时，您的选择会在依赖于事件数据源的所有相关分析功能（包括报告）中保持不变，直到您对其进行更改（即使在您注销后）。您的选择不适用于其他管理中心用户。

所选数据源仅用于低优先级连接事件。所有其他事件类型（入侵，文件和恶意软件事件；与这些事件关联的连接事件；以及安全智能事件）都会显示，无论数据源如何。

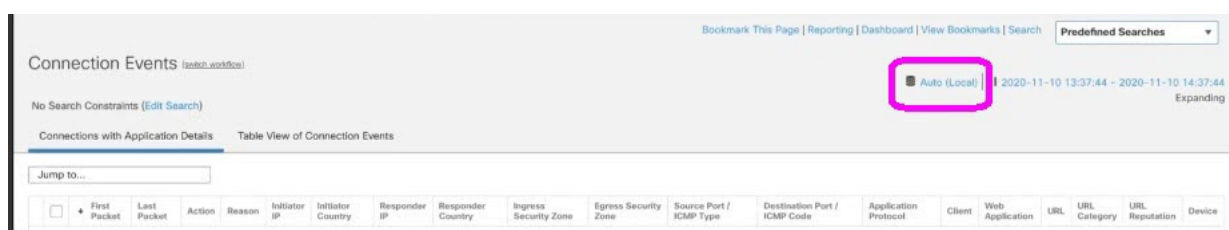
开始之前

您已使用向导 Security Analytics and Logging (OnPrem) 发送连接事件。

过程

步骤 1 在管理中心 Web 界面中，导航至显示连接事件数据的页面，例如 **分析 > 连接 > 事件**。

步骤 2 点击此处显示的数据源并选择一个选项：



注意

如果选择 **本地**，则系统仅显示管理中心上的可用数据，即使本地数据在所选的时间范围内不可用。您不会收到此情况的通知。

步骤 3 （可选）要直接在 Cisco Secure Network Analytics 设备中查看相关数据，请右键单击（在统一事件查看器中，点击）IP 地址或域等值，然后选择交叉启动选项。

使用交叉启动调查事件

在管理中心中查看事件时，您可以右键单击某些事件数据（例如，IP 地址），然后在管理器中查看相关数据。

过程

步骤 1 导航到管理中心中显示事件的以下其中一个页面：

- 控制面板（**概述 > 控制面板**），或
- 事件查看器页面（“分析” (Analysis) 菜单下包括事件表的任何菜单选项）。

步骤 2 右键单击感兴趣的事件字段，然后选择 Security Analytics and Logging (OnPrem) 交叉启动资源。管理器将在单独的浏览器窗口中打开。如果您尚未登录，系统可能会提示您输入用户名和密码。处理查询可能需要一些时间，这取决于要查询的数据量、管理器的速度 and 需求等。

步骤 3 登录到 管理器。



附录 A

故障排除

- [故障排除](#)，第 29 页

故障排除

Security Analytics and Logging (OnPrem) 一般故障排除

在管理器上，以下日志文件包含与 Security Analytics and Logging (OnPrem) 相关故障排除信息：

- `/lancope/var/logs/sal_preinstall.log` - 特定于应用安装过程的信息

在流量收集器上，以下日志文件包含与 Security Analytics and Logging (OnPrem) Data Store 部署相关的故障排除信息：

- `/lancope/var/sw/today/logs/sw.log` - 遥测日志记录的特定信息
- `/lancope/var/logs/containers/svc-db-ingest.log` - 特定于事件注入和数据库的信息

使用流量收集器高级设置的 Security Analytics and Logging (OnPrem) 配置（仅 Data Store）

如果您在首次设置时将流量收集器配置为不存储防火墙日志，则可以使用“流量收集器高级设置”页面来更新注入设置。以访问高级设置：

1. 登录到流量收集器（以前称为设备管理（管理员）界面）。
2. 点击支持 (Support) > 高级设置 (Advanced Settings)。
3. 在 `enable_sal` 字段中，输入 1 以启用防火墙事件日志注入。
4. 如果要更改防火墙日志的端口，请在 `sal_syslog_port` 字段中输入新值（默认端口为 8514）。
5. 点击应用 (Apply)，然后点击确定 (OK)。

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。