审核日志

审核日志

使用审核日志，对系统所做的配置更改会记录到单独的日志文件中进行审核。

审核日志（标准）

启用审核日志时不选择详细审核日志选项，即会将系统配置为标准审核日志。

使用标准审核日志，对系统所做的配置更改会记录到单独的日志文件中进行审核。 显示在功能配置 GUI 中的“控制中心 - 网络服务”下的思科审核事件服务，会监控用户对系统所做的任何配置更改，或用户操作导致的任何配置更改。

您可以访问功能配置 GUI 中的**审核日志配置**窗口以配置审核日志的设置。

标准审核日志包含以下部分：

- 审核日志记录框架 - 框架包含使用警报库将审核事件写入审核日志的 API。 定义为 GenericAlarmCatalog.xml 的警报目录适用于这些警报。 不同的系统组件提供自己的日志记录。

  以下示例显示 Unified Communications Manager 组件可用于发送警报的 API：

```
User ID: CCMAdministratorClient IP Address: 172.19.240.207 Severity: 3
EventType: ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:
Successful Description: CallManager Service status is stopped
```

- 审核事件日志 - 审核事件代表需要进行记录的任何事件。 以下示例显示示例审核事件：

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService
EventStatus:Successful Description: Call Manager Service status is stopped
App ID:Cisco Tomcat Cluster ID:StandAloneCluster Node ID:sa-cm1-3
```

提示 请注意审核事件日志默认为集中式并启用。称为“系统日志审核”的警报监控将写入日志。默认情况下，将日志配置为轮换。 如果 AuditLogAlarmMonitor 无法写入审核事件，AuditLogAlarmMonitor 会将此失败记录为系统日志文件中的严重错误。 警告管理器会将此错误作为 SeverityMatchFound 警告的一部分报告。 即使事件记录失败，实际操作也会继续。 系统将从 Cisco Unified 实时监控工具中的“跟踪和日志中心”收集、查看和删除所有审核日志。

Cisco Unified 功能配置标准事件日志记录

Cisco Unified 功能配置记录以下事件：

- 激活、停用、启动或停止服务。
- 跟踪配置和警报配置更改。
- SNMP 配置更改。
- CDR 管理中的更改。 （仅限 Cisco Unified Communications Manager）
- 查看功能配置报告存档中的任何报告。 此日志在报告器节点上查看。 （仅限 Unified Communications Manager）

Cisco Unified 实时监控工具标准事件登录

Cisco Unified 实时监控工具使用审核事件警报记录以下事件：

- 警告配置
- 警告暂停
- 电子邮件配置
- 设置节点警告状态
- 警告添加
- 添加警告操作
- 清除警告
- 启用警告
- 删除警告操作
- 删除警告

Unified Communications Manager 标准事件日志记录

Cisco CDR 分析和报告 (CAR) 为这些事件创建审核日志：

- 加载程序计划

- 每日、每周和每月报告计划
- 邮件参数配置
- 拨号方案配置
- 网关配置
- 系统首选项配置
- 自动清除配置
- 持续时间、一天中的时间和语音质量的评级引擎配置
- QoS 配置
- 预生成报告配置的自动生成/警告。
- 通知限制配置

Cisco Unified CM 管理标准事件日志记录

以下事件是为 Cisco Unified Communications Manager 管理的各个组件而记录：

- 用户日志记录（用户登录和用户注销）
- 用户角色成员资格更新（添加用户、删除用户、更新用户角色）
- 角色更新（添加、删除或更新新角色）
- 设备更新（电话和网关）
- 服务器配置更新（更改警报或跟踪配置、服务参数、企业参数、IP 地址、主机名、以太网设置和 Unified Communications Manager 服务器添加或删除）

Cisco Unified Communications 自助门户标准事件日志记录

将为 Cisco Unified Communications 自助门户记录用户日志记录（用户登录和用户注销）事件。

命令行界面标准事件日志记录

将记录通过命令行界面发出的所有命令（Unified Communications Manager 和 Cisco Unity Connection 都适用）。

Cisco Unity Connection 管理标准事件日志记录

Cisco Unity Connection 管理会记录以下事件：

- 用户日志记录（用户登录和用户注销）
- 所有配置更改，包括但不限于用户、联系人、呼叫管理对象、网络、系统设置和电话
- 任务管理（启用或禁用任务）

- 批量管理工具（批量创建，批量删除）
- 自定义键盘映射（映射更新）

Cisco Personal Communications Assistant (Cisco PCA) 标准事件日志记录

Cisco Personal Communications Assistant 客户端记录以下事件：

- 用户日志记录（用户登录和用户注销）
- 通过 Messaging Assistant 进行的所有配置更改

Cisco Unity Connection 功能配置标准事件日志记录

Cisco Unity Connection 功能配置记录以下事件：

- 用户登录（用户登录和用户注销）。
- 所有配置更改。
- 激活、停用、启动或停止服务。

使用具象状态传输 (REST) API 的 Cisco Unity Connection 客户端事件日志记录

使用具象状态传输 (REST) API 的 Cisco Unity Connection 客户端记录以下事件：

- 用户日志记录（用户 API 身份验证）。
- 使用 Cisco Unity Connection 预配置接口的 API 呼叫。

Cisco Unified IM and Presence 功能配置标准事件日志记录

Cisco Unified IM and Presence 功能配置记录以下事件：

- 激活、停用、启动或停止服务。
- 跟踪配置和警报配置更改。
- SNMP 配置更改
- 查看功能配置报告存档中的任何报告（可在报告器节点上查看此日志）

Cisco Unified IM and Presence 实时监控工具标准事件日志

Cisco Unified IM and Presence 实时监控工具使用审核事件警报记录以下事件：

- 警告配置
- 警告暂停
- 电子邮件配置
- 设置节点警告状态

- 警告添加
- 添加警告操作
- 清除警告
- 启用警告
- 删除警告操作
- 删除警告

Cisco IM and Presence 管理标准事件日志记录

以下事件是为 Cisco Unified Communications Manager IM and Presence 管理的各个组件而记录：

- 管理员日志记录（登录和注销管理、操作系统管理、灾难恢复系统和报告等 IM and Presence 接口）
- 用户角色成员资格更新（添加用户、删除用户、更新用户角色）
- 角色更新（添加、删除或更新新角色）
- 设备更新（电话和网关）
- 服务器配置更新（更改警报或跟踪配置、服务参数、企业参数、IP 地址、主机名、以太网设置和 IM and Presence 服务器添加或删除）

IM and Presence 应用程序标准事件日志记录

以下事件是为 IM and Presence 应用程序的各个组件而记录：

- IM 客户端上的最终用户日志记录（用户登录、用户注销和登录尝试失败）
- 用户进入和退出 IM 聊天室
- IM 聊天室的创建和销毁

命令行界面标准事件日志记录

所有通过命令行界面发出的命令都将被记录。

审核日志（详细）

详细审核日志是一项可选功能，用于记录未存储在标准（默认）审核日志中的附加配置修改。 除了在标准审核日志中存储的所有信息外，详细的审核日志还包括添加、更新和删除的配置项目（含修改的值）。 默认情况下禁用详细的审核日志，但您可以在**审核日志配置**窗口中启用它。

Audit Log Types

系统审核日志

系统审核日志跟踪活动（例如创建、修改或删除Linux OS用户，篡改日志，更改文件或目录权限）。由于收集的数据量较大，因此默认情况下禁用此类型的审核日志。 要启用此功能，必须使用CLI手动启用 utils auditd。 在启用系统审核日志功能后，您可以从实时监控工具的跟踪和日志中心收集、查看、下载或删除所选的日志。 系统审核日志采用 `vos-audit.log` 的格式。

有关如何启用此功能的详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面参考指南》。 有关如何从实时监控工具访问收集的目录的信息，请参阅《*Cisco Unified* 实时监控工具管理指南》。

应用程序审核日志

应用程序审核日志监控和记录用户所做的或用户操作导致的任何系统配置更改。

注释 应用程序审核日志 (Linux auditd) 只能通过CLI启用或禁用。 除了通过实时监控工具收集 vos-audit.log 之外，您无法更改此类审核日志的任何设置。

数据库审核日志

数据库审核日志跟踪与访问 Informix 数据库（例如登录）相关的所有活动。

审核日志配置任务流程

完成以下任务以配置审核日志记录。

过程

	命令或操作	目的
步骤1	设置审核日志记录，第 7 页	在“审核日志配置”窗口中设置您的审核日志配置。 您可以配置是否要使用远程审核日志记录以及是否需要详细的审核日志记录选项。
步骤2	配置远程审核日志传输协议，第 7 页	可选。 如果配置了远程审核日志记录，请配置传输协议。 在正常操作模式下，系统默认值为 UDP，但您也可以配置 TCP 或 TLS
步骤3	针对警告通知配置电子邮件服务器，第 8 页	可选。 在 RTMT 中，针对电子邮件警告设置电子邮件服务器。
步骤4	启用电子邮件警告，第 8 页	可选。 设置以下电子邮件警告之一：

	命令或操作	目的
		• 如果使用 TCP 配置远程审核日志记录，请设置 **TCPRemoteSyslogDeliveryFailed** 警告的电子邮件通知。 • 如果使用 TLS 配置远程审核日志记录，请设置 **TLSRemoteSyslogDeliveryFailed** 警告的电子邮件通知。
步骤 5	为平台日志配置远程审核日志记录，第 9 页	为平台审核日志和远程服务器日志设置远程审核日志记录。 对于这些类型的审核日志，必须配置 FileBeat 客户端和外部 logstash 服务器。

设置审核日志记录

开始之前

对于远程审核日志记录，您必须已设置远程系统日志服务器并在每个群集节点和远程系统日志服务器之间配置 IPSec，包括到两者之间任何网关的连接。 有关 IPSec 配置，请参阅《*Cisco IOS* 安全配置指南》。

过程

步骤 1 在 Cisco Unified 功能配置中，选择**工具** > **审核日志配置**。

步骤 2 从**服务器**下拉菜单中选择群集中的任何服务器，然后单击**前往**。

步骤 3 要记录所有群集节点，选中**应用到所有节点**复选框。

步骤 4 在**服务器名称**字段中，输入远程系统日志服务器的 IP 地址或完全限定域名。

步骤 5 可选。 要记录配置更新（包括修改的项目和修改的值），选中**详细审核日志记录**复选框。

步骤 6 在**审核日志配置**窗口完成其余字段的设置。 有关这些字段及其说明的帮助，请参阅联机帮助。

步骤 7 单击**保存**。

下一步做什么

配置远程审核日志传输协议，第 7 页

配置远程审核日志传输协议

此程序可用于更改远程审核日志的传输协议。 系统默认值为 UDP，但您可以重新配置为 TCP 或 TLS。

过程

步骤 1 登录到命令行界面。

步骤 2 运行 **utils remotesyslog show protocol** 命令以确认配置了哪个协议。

步骤 3 如果您需要更改此节点上的协议，请执行以下操作：

- 要配置 TCP，运行 **utils remotesyslog set protocol tcp** 命令。
- 要配置 UDP，运行 **utils remotesyslog set protocol udp** 命令。
- 要配置 TLS，运行 **utils remotesyslog set protocol tls** 命令。

  要设置 TLS 连接，必须将安全证书从系统日志服务器上传到 Unified Communications Manager 和 IM and Presence Service 上的 tomcat 信任存储区。

  注释 在 Common Criteria 模式下，将实施严格的主机名验证。 因此，需要使用与证书匹配的完全限定域名 (FQDN) 配置服务器。

步骤 4 如果更改了协议，请重新启动节点。

步骤 5 对每个 Unified Communications Manager 和 IM and Presence Service 群集节点重复此程序。

下一步做什么

针对警告通知配置电子邮件服务器， 第 8 页

针对警告通知配置电子邮件服务器

此程序用于针对警告通知设置您的电子邮件服务器。

过程

步骤 1 在实时监控工具的系统窗口中，单击**警告中心**。

步骤 2 选择**系统** > **工具** > **警告** > **配置电子邮件服务器**。

步骤 3 在**邮件服务器配置**弹出窗口中，输入邮件服务器的详细信息。

步骤 4 单击**确定**。

下一步做什么

启用电子邮件警告， 第 8 页

启用电子邮件警告

如果您配置了采用 TCP 或 TLS 进行远程审核日志记录，此程序可用于设置电子邮件警告，让系统在出现传输失败时通知您。

过程

步骤 1 在实时监控工具**系统**区域中，单击**警告中心**。

步骤 2 在**警告中心**窗口中，

- 如果您配置的是采用 TCP 进行远程审核日志记录，选择 **TCPRemoteSyslogDeliveryFailed**
- 如果您配置的是采用 TLS 进行远程审核日志记录，选择 **TLSRemoteSyslogDeliveryFailed**

步骤 3 选择**系统** > **工具** > **警告** > **配置警告操作**。

步骤 4 在**警告操作**弹出窗口中，选择**默认**并单击**编辑**。

步骤 5 在**警告操作**弹出窗口中，**添加**收件人。

步骤 6 在弹出窗口中，输入您要向其发送电子邮件警告的地址，然后单击**确定**。

步骤 7 在**警告操作**弹出窗口中，确保地址显示在**收件人**之下并且已选中**启用**复选框。

步骤 8 单击**确定**。

为平台日志配置远程审核日志记录

完成这些任务，为平台审核日志、远程支持日志和批量管理 csv 文件添加远程审核日志支持。 对于这些类型的日志，将使用 FileBeat 客户端和 logstash 服务器。

开始之前

确保您已设置外部 logstash 服务器。

过程

	命令或操作	目的
步骤 1	配置 Logstash 服务器信息， 第 9 页	使用外部 logstash 服务器详细信息（例如 IP 地址、端口和文件类型）配置 FileBeat 客户端。
步骤 2	配置 FileBeat 客户端， 第 10 页	为远程审核日志记录启用 FileBeat 客户端。

配置 Logstash 服务器信息

此程序可用于使用外部 logstash 服务器信息（例如 IP 地址、端口号和可下载文件类型）配置 FileBeat 客户端。

开始之前

确保您已设置外部 logstash 服务器。

过程

步骤 1 登录到命令行界面。

步骤 2 运行 **utils FileBeat configure** 命令。

步骤 3 按照提示配置 logstash 服务器详细信息。

配置 FileBeat 客户端

此程序可用于启用或禁用FileBeat客户端以上传平台审核日志、远程支持日志和批量管理csv文件。

过程

步骤 1 登录到命令行界面。

步骤 2 运行 **utils FileBeat status** 命令以确认 FileBeat 客户端是否已启用。

步骤 3 运行以下命令之一：

- 要启用客户端，运行 **utils FileBeat enable** 命令。
- 要禁用客户端，运行 **utils FileBeat disable** 命令。

注释 TCP 是默认的传输协议。

步骤 4 可选。 如果要将 TLS 用作传输协议，请执行以下操作：

- 要启用 TLS 作为传输协议，运行 **utils FileBeat tls enable** 命令。
- 要禁用 TLS 作为传输协议，运行 **utils FileBeat tls disable** 命令。

注释 要使用 TLS，必须将安全证书从 logstash 服务器上传到 Unified Communications Manager 和 IM and Presence Service 上的 tomcat 信任存储区。

步骤 5 对于每个节点重复上述过程。

不要在所有节点上同时运行任何这些命令。

审核日志配置设置

开始之前

请注意，只有拥有审核角色的用户才可更改审核日志设置。 默认情况下，对于Unified Communications Manager，在全新安装和升级后，CCMAdministrator拥有审核角色。 CCMAdministrator可以在Cisco Unified Communications Manager管理的“用户组配置”窗口中将具有审核权限的任何用户分配给“标准审核用户”组分配。 如果想要这样做，您可以从“标准审核用户”组中删除CCMAdministrator。

对于 IM and Presence Service，在全新安装和升级后，管理员拥有审核角色，并且可以将拥有审核权限的任何用户分配给“标准审核用户”组。

对于 Cisco Unity Connection，在安装过程中创建的应用程序管理帐户具有审核管理员角色，并可以分配其他管理用户到该角色。 您也可以从此帐户删除审核管理员角色。

标准审核日志配置角色能够删除审核日志以及读取/更新 Cisco Unified 实时监控工具、IM and Presence 实时监控工具、跟踪收集工具、实时监控工具 (RTMT) 警告配置、功能配置用户界面中的“控制中心 - 网络服务”、RTMT 配置文件保存、功能配置用户界面中的审核配置以及称为审核跟踪的资源。

标准审核日志配置角色能够删除审核日志以及读取/更新 Cisco Unified RTMT、跟踪收集工具、RTMT 警告配置、Cisco Unified 功能配置中的“控制中心 - 网络服务”、RTMT 配置文件保存、Cisco Unified 功能配置中的审核配置以及称为审核跟踪的资源。

Cisco Unity Connection 中的审核管理员角色能够查看、下载和删除 Cisco Unified RTMT 中的审核日志。

有关 Unified Communications Manager 中角色、用户和用户组的信息，请参阅《*Cisco Unified Communications Manager* 管理指南》。

有关 Cisco Unity Connection 中角色和用户的信息，请参阅《*Cisco Unity Connection* 的用户移动、添加和更改指南》。

有关 IM and Presence 中角色、用户和用户组的信息，请参阅《*Unified Communications Manager* 上 *IM and Presence Service* 的配置和管理》。

下表介绍了您可以在 Cisco Unified 功能配置的“审核日志配置”窗口中配置的设置。

表 *1:* 审核日志配置设置

字段	说明
选择服务器	
服务器	选择要在其中配置审核日志的服务器（节点），然后单击**前往**。
应用到所有节点	如果要将此审核日志应用到群集中的所有节点，请选中**应用到所有节点**复选框。
应用程序审核日志设置	

字段	说明
启用审核日志	选中此复选框时，即会为应用程序审核日志创建审核日志。 对于 Unified Communications Manager，应用程序审核日志支持对 Unified Communications Manager 用户界面的配置更新，例如 Cisco Unified Communications Manager 管理、Cisco Unified RTMT、Cisco Unified Communications Manager CDR 分析和报告以及 Cisco Unified 功能配置。 对于 IM and Presence Service，应用程序审核日志支持对 IM and Presence 用户界面的配置更新，例如 Cisco Unified Communications Manager IM and Presence 管理、Cisco Unified IM and Presence 实时监控工具和 Cisco Unified IM and Presence 功能配置。 对于 Cisco Unity Connection，应用程序审核日志支持对 Cisco Unity Connection 用户界面的配置更新，包括 Cisco Unity Connection 管理、Cisco Unity Connection 功能配置、Cisco Personal Communications Assistant 以及使用 Connection REST API 的客户端。 此设置默认显示为启用。 **注释** 网络服务审核事件服务必须正在运行。
启用清除	日志分区监控(LPM)查看“启用清除”选项以确定其是否需要清除审核日志。选中此复选框时，LPM将在公共分区磁盘使用超出上限时清除RTMT中的所有审核日志文件；不过，您可以通过取消选中该复选框禁用清除。 如果清除已禁用，则审核日志数量继续增加，直到磁盘已满。此操作可导致系统中断。当取消选中“启用清除”复选框时，会显示一条消息说明禁用清除的风险。 请注意，此选项适用于活动分区中的审核日志。 如果审核日志位于非活动分区，则审核日志在磁盘使用超出上限时将被清除。 您可以通过选择RTMT中的**跟踪和日志中心**>**审核日志**来访问审核日志。 **注释** 网络服务 Cisco 日志分区监控工具必须正在运行。
启用日志轮换	系统会读取此选项以确定其需要轮换审核日志文件还是需要继续创建新文件。 最大文件数不得超过 5000。选中“启用轮换”复选框时，系统在达到最大文件数量后将开始覆盖最旧的审核日志文件。 **提示** 日志轮换被禁用时（未选中），审核日志将忽略“最大文件数”设置。
详细审核日志	选中此复选框后，系统将启用详细审核日志。详细审核日志提供的项目与常规审核日志相同，但也包括配置更改。例如，审核日志包含已添加、更新和删除的项目，包括已修改值。

字段	说明
服务器名称	输入您要用于接受系统日志消息的远程系统日志服务器的名称或IP地址。如果未指定服务器名称，Cisco Unified IM and Presence 功能配置不会发送系统日志消息。 请勿指定 Unified Communications Manager 节点作为目标，因为 Unified Communications Manager 节点不接受来自另一个节点的系统日志消息。 这仅适用于 IM and Presence Service。
远程系统日志审核事件级别	选择远程系统日志服务器所需的系统日志消息严重性。具有所选或更高严重性级别的所有系统日志消息都将被发送到远程系统日志。 这仅适用于 IM and Presence Service。
文件最大数	输入想要在日志中包括的最大文件数。 默认设置指定为250。最大数量指定 5000。
文件最大大小	输入审核日志的文件最大大小。 文件大小值必须介于 1MB 到 10MB 之间。 您必须指定一个介于 1 到 10 之间的数字。
接近日志轮换覆盖的预警阈值 (%)	当审核日志接近被覆盖的程度时，系统会警告您。 使用此字段设置当您处于该值时系统将向您发送警告的阈值。 例如，如果您使用 250 个 2 MB 文件、预警阈值为 80% 的默认设置，则系统会在累积的审核日志到200 个文件 (80%) 时给您发送警报。 如果想要保留审核历史记录，您可以在系统覆盖日志之前使用 RTMT 检索它们。 在您收集文件后，RTMT 会提供一个选项以将其删除。 输入介于 1 到 99% 之间的值。 默认值为 80%。 在设置此字段时，您还必须选中**启用日志轮换**选项。 **注释** 分配给审核日志的总磁盘空间为最大文件数乘以文件最大大小。 如果磁盘上的审核日志大小超过分配的总磁盘空间百分比，系统会在警告中心发出警报。
数据库审核日志过滤器设置	
启用审核日志	选中此复选框时，将为 Unified Communications Manager 和 Cisco Unity Connection 数据库创建审核日志。 将此设置结合“调试审核级别”设置使用，可让您为数据库的某些方面创建日志。

字段	说明
调试审核级别	此设置可让您选择要在日志中审核的数据库方面。从下拉列表框中选择以下选项之一。 请注意每个审核日志过滤器级别都是累积的。 • **方案** - 跟踪对审核日志数据库设置的更改（例如，数据库表中的列和行）。 • **管理任务** - 跟踪对 Unified Communications Manager 系统的所有管理更改（例如，为了维护系统而作的任何更改）以及所有**方案**更改。 **提示** 大多数管理员会将“管理任务”设置保留为禁用。 对于要审核的用户，请使用数据库更新级别。 • **数据库更新** - 跟踪对数据库的所有更改以及所有**方案**更改和所有**管理任务**更改。 • **数据库读取** - 跟踪对系统的每次读取，以及所有方案更改、管理任务更改和数据库更新更改。 **提示** 仅在您想要快速查看 Unified Communications Manager、IM and Presence Service 或 Cisco Unity Connection 系统时，选择数据库读取级别。 此级别使用大量的系统资源，只能短时使用。
启用审核日志轮换	系统会读取此选项以确定其需要轮换数据库审核日志文件还是需要继续创建新文件。选中“审核启用轮换”复选框时，系统在达到最大文件数量后将开始覆盖最旧的审核日志文件。 此设置复选框未选中时，审核日志将忽略最大文件数设置。
文件最大数	输入想要在日志中包括的最大文件数。确保为“最大文件数”设置输入的值大于为“日志轮换时删除的文件数”设置输入的值。 您可以输入介于 4（最小）到 40（最大）之间的数字。
日志轮换时删除的文件数	输入当发生数据库审核日志轮换时，系统可以删除的最大文件数。 您可以在此字段中输入的最小值为 1。最大值比您为“最大文件数”输入的值小 2。例如，如果您在“最大文件数”字段输入 40，则可以在“日志轮换时删除的文件数”字段中输入的最大数字为 38。
设置为默认值	**设为默认值**按钮指定默认值。建议将审核日志设置为默认模式，除非需要将其设置为不同的级别以进行详细故障诊断。 **设为默认值**选项将最大限度地减少日志文件使用的磁盘空间。

注意 启用后，数据库日志记录可能会在短时间内生成大量数据，特别是调试审核级别设置为**数据库更新**或**数据库读取**时。这可能会对繁忙使用期间的性能造成显著影响。一般情况下，我们建议您保持禁止数据库日志记录。如果您需要启用日志记录以跟踪数据库中的更改，我们建议您使用**数据库更新**级别仅在短时间内使用。同样，管理日志记录对Web用户界面的整体性能也有影响，特别是在轮询数据库条目时（例如，从数据库中轮询 250 台设备）。

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。