日志记录

本章介绍如何记录系统消息并将其用于故障排除。

关于日志记录

系统日志记录是将来自设备的消息收集到运行系统日志后台守护程序的服务器的方法。将信息记录到中央系统日志服务器有助于汇聚日志和提醒。思科设备可以将其日志消息发送到 UNIX 样式的系统日志服务。系统日志服务接受消息并将其存储在文件中，或者根据简单配置文件打印消息。以这种形式记录日志可为日志提供受保护的长期存储。日志对常规故障排除及事件处理均有帮助。

ASA 系统日志提供有关对 ASA 进行监控和故障排除的信息。通过日志记录功能，可以执行以下操作：

- 指定应记录哪些系统日志消息。
- 禁用或更改系统日志消息的严重性级别。
- 指定系统日志消息应发送到的一个或多个位置，包括：
  - 内部缓冲区
  - 一个或多个系统日志服务器
  - ASDM
  - SNMP 管理站
  - 指定的电子邮件地址
  - 控制台
  - Telnet 和 SSH 会话。

- 以组形式（例如，按严重性级别或消息类）配置和管理系统日志消息。
- 指定是否对系统日志生成应用速率限制。
- 指出在内部日志缓冲区已满时如何处理其内容：覆盖缓冲区、将缓冲区内容发送到 FTP 服务器，或者将内容保存到内部闪存。
- 按位置、严重性级别、类或自定义消息列表过滤系统日志消息。

多情景模式下的日志记录

每个安全情景包含自己的日志记录配置并生成其自己的消息。如果登录到系统或管理情景，然后更改为其他情景，则只能在会话中查看与当前情景相关的消息。

请在管理情景中查看在系统执行空间中生成的系统日志消息（包括故障转移消息）以及在管理情景中生成的消息。无法在系统执行空间中配置日志记录或查看任何日志记录信息。

可以将ASA配置为在每个消息中包含情景名称，从而帮助区分发送到单个系统日志服务器的情景消息。此功能有助于确定哪些消息来自管理情景，哪些消息来自系统；源于系统执行空间的消息使用设备 ID **system**，源于管理情景的消息使用管理情景的名称作为设备 ID。

系统日志消息分析

以下是可从各种系统日志消息审阅中获取的信息类型的一些示例：

- ASA 安全策略允许的连接。这些消息帮助确定安全策略中仍存在的漏洞。
- ASA 安全策略拒绝的连接。这些消息显示将哪些类型的活动定向到受保护内部网络。
- 使用 ACE 拒绝率日志记录功能显示在 ASA 上发生的攻击。
- IDS 活动消息可以显示已发生的攻击。
- 用户身份验证和命令使用情况提供安全策略更改的审计线索。
- 带宽使用情况消息显示每个已建立和中断的连接，以及各连接使用的持续时间和流量。
- 协议使用情况消息显示每个连接使用的协议和端口号。
- 地址转换审计线索消息记录建立或中断的 NAT 或 PAT 连接，如果接收到从网络内部到外部环境的恶意活动报告，这些消息会有所帮助。

系统日志消息格式

系统日志消息的结构如下：

```
[<PRI>] [Timestamp] [Device-ID] : %ASA-Class-Level-Message_number: Message_text
```

字段说明如下：

<PRI>	优先级值。在启用日志记录 EMBLEM 后，此值将显示在系统日志消息中。日志记录 EMBLEM 与 UDP 兼容，但与 TCP 不兼容。
时间戳	系统将显示事件的日期和时间。在启用时间戳日志记录后，如果时间戳被配置为 RFC 5424 格式，则系统日志消息中的所有时间戳都会以 UTC 显示时间，如 RFC 5424 标准所示。
Device-ID	通过用户界面启用登录 device-id 选项时配置的设备标识符字符串。如果启用，则在 EMBLEM 格式化系统日志消息中不会显示设备 ID。
分类	系统日志消息类提供一个按类型将系统日志消息分类的方法，相当于设备的特性或功能。例如，vpnc 类表示 VPN 客户端。
ASA	由 ASA 所生成消息的系统日志消息设备代码。值始终为 `ASA`。
级别	0 到 7。级别反映系统日志消息所描述情况的严重性 - 数字越小，情况越严重。
Message_number	用于标识系统日志消息的唯一六位数编号。所有消息都记录在 Cisco Secure Firewall ASA 系列系统日志消息指南中。
Message_text	用于描述情况的文本字符串。系统日志消息的这一部分有时包含 IP 地址、端口号或用户名。

启用了日志记录 EMBLEM、日志记录时间戳 rfc5424 和设备 ID 的系统日志消息示例。

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

启用了日志记录时间戳 rfc5424 和设备 ID 的系统日志消息示例。

```
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
```

系统日志消息的结构如下：

```
[<PRI>] [Timestamp] [Device-ID] : %ASA-Level-Message_number: Message_text
```

字段说明如下：

<PRI>	优先级值。在启用日志记录 EMBLEM 后，此值将显示在系统日志消息中。日志记录 EMBLEM 与 UDP 兼容，但与 TCP 不兼容。
时间戳	系统将显示事件的日期和时间。在启用时间戳日志记录后，如果时间戳被配置为 RFC 5424 格式，则系统日志消息中的所有时间戳都会以 UTC 显示时间，如 RFC 5424 标准所示。
Device-ID	通过用户界面启用登录 device-id 选项时配置的设备标识符字符串。如果启用，则在 EMBLEM 格式化系统日志消息中不会显示设备 ID。
ASA	由 ASA 所生成消息的系统日志消息设备代码。值始终为 `ASA`。
级别	0 到 7。级别反映系统日志消息所描述情况的严重性 - 数字越小，情况越严重。
Message_number	用于标识系统日志消息的唯一六位数编号。

Message_text	用于描述情况的文本字符串。系统日志消息的这一部分有时包含 IP 地址、端口号或用户名。

设备生成的所有系统日志消息都记录在 Cisco Secure Firewall ASA 系列系统日志消息指南中。

启用了日志记录 EMBLEM、日志记录时间戳 rfc5424 和设备 ID 的系统日志消息示例。

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

启用了日志记录时间戳 rfc5424 和设备 ID 的系统日志消息示例。

```
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
```

严重性级别

下表列出系统日志消息严重性级别。可以为各严重性级别分配自定义颜色，更轻松地在 ASDM 日志查看器中对其进行区分。要配置系统日志消息颜色设置，请依次选择**工具 > 首选项 > 系统日志**选项卡，或者在日志查看器中点击工具栏上的**颜色设置**。

表 *1:* 系统日志消息严重级别

级别号	严重性级别	说明
0	**应急**	系统不可用。
1	**警报**	需要立即采取措施。
2	**严重**	严重情况。
3	**错误**	错误情况。
4	**警告**	警告情况。
5	**通知**	正常但重大的情况。
6	**信息性**	消息仅供参考。
7	**调试**	消息仅供调试。 调试问题时，仅临时记录此级别的日志。此日志级别可能会生成太多消息，从而影响系统性能。

注释 ASA 和 不会生成严重性级别为零 (emergencies) 的系统日志消息。

系统日志消息过滤

您可以过滤生成的系统日志消息，以便仅将某些系统日志消息发送到特定输出目标。例如，您可以将ASA配置为将所有系统日志消息发送至一个输出目标，而将这些系统日志消息中的一部分发送至其他输出目标。

具体而言，您可以根据以下条件将系统日志消息定向到输出目标：

- 系统日志消息 ID 号
- 系统日志消息严重性级别
- 系统日志消息类（相当于一个功能区）

通过创建一个在设置输出目标时可以指定的消息列表来自定义这些条件。或者，可以将ASA配置为将一个特定的消息类发送至每种类型的输出目标，而不管消息列表是什么。

系统日志消息类

可以通过两种方法使用系统日志消息类：

- 指定整个类别的系统日志消息的输出位置。
- 创建指定消息类的消息列表。

系统日志消息类提供一个按类型将系统日志消息分类的方法，相当于设备的特性或功能。例如，RIP 类表示 RIP 路由。

特定类中的所有系统日志消息共享其系统日志消息 ID 号中相同的前三位数字。例如，所有以数字 611 开头的系统日志消息 ID 都与 vpnc（VPN 客户端）类相关联。与 VPN 客户端功能相关联的系统日志消息范围从 611101 至 611323。

此外，大多数 ISAKMP 系统日志消息都具有公用预置对象集来帮助识别隧道。这些对象在适用时前置于系统日志消息的描述性文本。如果在生成系统日志消息时对象未知，则不显示特定的 heading = value 组合。

对象的前缀如下：

Group = *groupname*, Username = *user*, IP = *IP_address*

其中组是隧道组，用户名是来自本地数据库或 AAA 服务器的用户名，IP 地址是远程访问客户端或第 2 层对等体的公用 IP 地址。

下表列出消息类以及每个类中的消息 ID 范围。

表 *2:* 系统日志消息类和关联的消息 *ID* 号

类别	定义	系统日志消息 ID 号
auth	用户身份验证	109、113
-	访问列表	106

类别	定义	系统日志消息 ID 号
-	应用防火墙	415
—	僵尸网络流量筛选	338
bridge	透明防火墙	110、220
ca	PKI 证书颁发机构	717
citrix	Citrix Client	723
-	集群	747
-	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
-	环境监控	735
ha	故障转移	101、102、103、104、105、210、311、709
-	基于身份认证的防火墙	746
ids	入侵检测系统	400、733
-	IKEv2 工具包	750、751、752
ip	IP 堆栈	209、215、313、317、408
ipaa	IP 地址分配	735
ips	入侵保护系统	400、401、420
-	IPv6	325
-	许可	444
mdm-proxy	MDM 代理	802
nac	网络准入控制	731、732

类别	定义	系统日志消息 ID 号
nacpolicy	NAC 策略	731
nacsettings	配置 NAC 设置，以应用 NAC 策略	732
-	NAT 与 PAT	305
-	网络无线接入点	713
np	网络处理器	319
-	NP SSL	725
ospf	OSPF 路由	318、409、503、613
-	密码加密	742
-	电话代理	337
rip	RIP 路由	107、312
rm	资源管理器	321
-	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
snmp	SNMP	212
-	ScanSafe	775
ssl	SSL 堆栈	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
-	威胁检测	733
标记交换	服务标记交换	779
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

类别	定义	系统日志消息 ID 号
vpnc	VPN 客户端	611
vpnfo	VPN 故障转移	720
vpnlb	VPN 负载均衡	718
-	VXLAN	778
webfo	WebVPN 故障转移	721
webvpn	WebVPN 和 Secure Client	716

在日志查看器中对消息进行排序

您可以对 ASDM 日志查看器（即 Real-Time Log Viewer、Log Buffer Viewer 和 Latest ASDM Syslog Events Viewer）中的所有消息进行排序。要按多列对表进行排序，请点击要按其排序的第一列的标题，然后按住 **Ctrl** 键，同时点击要包含在排序顺序中的其他列的标题。要按时间顺序对消息进行排序，请同时选中日期和时间列；否则，消息仅按日期（无论时间）或仅按时间（无论日期）排序。

在 Real-Time Log Viewer 和 Latest ASDM Syslog Events Viewer 中对消息进行排序时，传入的新消息按照已排序的顺序显示，而不是显示在顶部。也就是说，它们会与其他消息混合。

自定义消息列表

灵活地创建自定义消息列表，以对将哪些系统日志消息发送至哪个输出目标实施控制。在自定义系统日志消息列表中，可以使用以下任意或所有条件指定系统日志消息组：

- 严重性级别
- 消息 ID
- 系统日志消息 ID 范围
- 消息类

例如，可以使用消息列表执行以下操作：

- 选择严重性级别为 1 和 2 的系统日志消息，然后将其发送到一个或多个邮件地址。
- 选择与消息类（例如 ha）关联的所有系统日志消息，然后将其保存到内部缓冲区。

消息列表可以包含多个消息选择条件。 但是，必须使用新命令条目来添加各消息选择条件。可以创建包含重叠消息选择条件的消息列表。如果消息列表中的两个条件选择同一消息，则消息仅记录一次。

集群

系统日志消息是在集群环境中用于记帐、监控和故障排除的一种实用工具。集群中的每台ASA设备（最多允许八台设备）都是独立生成系统日志消息；然后，某些**logging**命令支持您控制报头字段，其中包括时间戳和设备 ID。系统日志服务器使用设备 ID 标识系统日志生成器。您可以使用 **logging device-id** 命令来生成具有相同或不同设备ID的系统日志消息，以使消息看上去是来自集群中的相同或不同设备。

注释 要监控来自集群中的设备的系统日志消息，必须打开要监控的每台设备的 ASDM 会话。

日志记录准则

本节介绍您在配置日志记录之前应审阅的准则和限制。

IPv6 准则

- 支持 IPv6。可以使用 TCP 或 UDP 发送系统日志。
- 确保配置用于发送系统日志的接口已经启用，支持 IPv6，并且可以通过指定接口到达系统日志服务器。
- 不支持通过 IPv6 进行安全登录。

其他准则

- 系统日志服务器必须运行一个名为 syslogd 的服务器程序。Windows 提供了一个系统日志服务器，作为其操作系统的组成部分。
- 要查看由ASA生成的日志，必须指定日志记录输出目标。如果启用日志记录而未指定日志记录输出目标，则ASA会生成消息，但不会将其保存到可对其进行查看的位置。必须单独指定每个不同的日志记录输出目标。例如，要将多个系统日志服务器指定为输出目标，请对每个系统日志服务器在**系统日志服务器**窗格中指定单独的条目。
- 不支持在备用设备上通过 TCP 发送系统日志。
- 如果您使用 TCP 作为传输协议，系统会打开与系统日志服务器的 4 个连接，以确保消息不会丢失。如果您使用系统日志服务器从大量设备收集消息，并且合并的连接开销对该服务器来说太大，请改用 UDP。
- 不能将两个不同的列表或类分配给不同的系统日志服务器或相同位置。
- 您最多可以配置 16 个系统日志服务器。不过，在多情景模式下，限制为每个情景 4 个服务器。
- 应该可以通过ASA到达系统日志服务器。应将该设备配置为拒绝可以从其到达系统日志服务器的接口上的 ICMP 不可达消息，并将系统日志发送到同一服务器。请确保已对所有严重性级别

启用日志记录。要防止系统日志服务器崩溃，请抑制系统日志 313001、313004 和 313005 的生成。

- 用于系统日志的 UDP 连接数与硬件平台上的 CPU 数量和您配置的系统日志服务器数量直接相关。在任何时刻，UDP 系统日志连接的数量都等于 CPU 数量乘以已配置的系统日志服务器数量的积。这是预期行为。请注意，全局 UDP 连接空闲超时适用于这些会话，默认值为 2 分钟。如果您想更快关闭这些会话，可以调整该设置，但超时适用于所有 UDP 连接，而不仅是系统日志。
- 使用自定义消息列表仅与访问列表命中相匹配时，对于已将其日志记录严重性级别提高至调试（级别 7）的访问列表不会生成访问列表日志。对于 **logging list** 命令，默认日志记录严重性级别设置为 6。此默认行为是程序设计的。将访问列表配置的日志记录严重性级别显式更改为调试时，还必须更改日志记录配置本身。

  以下是来自 **show running-config logging** 命令的不含访问列表命中的样本输出，因为其日志记录严重性级别已更改为调试：

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging list test message 106100
logging buffered test
```

  以下是来自 **show running-config logging** 命令的包含访问列表命中的样本输出：

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging buffered debugging
```

  在此情况下，访问列表配置不更改，并会显示访问列表命中数，如下例所示：

```
ciscoasa(config)# access-list global line 1 extended
permit icmp any host 4.2.2.2 log debugging interval 1 (hitcnt=7) 0xf36b5386
ciscoasa(config)# access-list global line 2 extended
permit tcp host 10.1.1.2 any eq www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
ciscoasa(config)# access-list global line 3 extended
permit ip any any (hitcnt=543) 0x25f9e609
```

- 当 ASA 通过 TCP 发送系统日志时，在系统日志服务重新启动后，需要大约一分钟来启动连接。
- 从系统日志服务器收到的服务器证书的 Extended Key Usage 字段中必须包含“ServAuth”。此检查将仅针对非自签名证书进行，自签名证书在此字段中不提供任何值。

配置日志记录

本节介绍如何配置日志记录。

启用日志记录

要启用日志记录，请执行以下步骤：

过程

步骤 1 在 ASDM 中，依次选择以下其中一项：

- **Home** > **Latest ASDM Syslog Messages** > **Enable Logging**
- **Configuration** > **Device Management** > **Logging** > **Logging Setup**
- **Monitoring** > **Real-Time Log Viewer** > **Enable Logging**
- **Monitoring** > **Log Buffer** > **Enable Logging**

步骤 2 选中 **Enable logging** 复选框以开启日志记录。

配置输出目标

要优化系统日志消息使用情况以进行故障排除和性能监控，建议指定一个或多个应发送系统日志消息的位置，包括内部日志缓冲区、一个或多个外部系统日志服务器、ASDM、SNMP 管理站、控制台端口、指定的邮件地址或 Telnet 和 SSH 会话。

在启用了仅管理访问的接口上配置系统日志记录时，数据平面相关日志（会丢弃系统日志 ID 302015、302014、106023 和 304001），并且不会到达系统日志服务器。由于数据路径路由表没有管理接口路由，将会丢弃系统日志消息。因此，请确保您配置的接口已禁用仅管理访问

将系统日志消息发送至外部系统日志服务器

可以根据外部系统日志服务器上的可用磁盘空间将消息存档，并在保存日志记录数据后对其进行处理。例如，可以指定在记录特定类型的系统日志消息时要执行的操作，从日志提取数据并将记录保存到其他文件以进行报告，或者使用特定于站点的脚本跟踪统计信息。

要将系统日志消息发送到外部系统日志服务器，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **日志记录设置**。

步骤 2 选中 **Enable logging** 复选框以面向 ASA 启用日志记录。

步骤 3 选中 **Enable logging on the failover standby unit** 复选框以面向备用 ASA 启用日志记录（如果可用）。

步骤 4 选中 **Send debug messages as syslogs** 复选框以将所有调试跟踪输出重定向到系统日志。如果启用了此选项，则在控制台上不显示系统日志消息。因此，要查看调试消息，必须在控制台上启用日志记

录并将其配置为调试系统日志消息号和严重性级别的目标。要使用的系统日志消息编号是 **711001**。此系统日志消息的默认安全级别是调试。

步骤 5 选中 **Send syslogs in EMBLEM format** 复选框以启用 EMBLEM 格式，以便将其用于所有日志记录目标（系统日志服务器除外）。

步骤 6 指定在启用了日志记录缓冲区的情况下将系统日志消息保存到的内部日志缓冲区的大小。当缓冲区已满时，除非将日志保存到 FTP 服务器或内部闪存，否则会覆盖消息。默认缓冲区大小为 4096 字节。范围为 4096 到 1048576。

步骤 7 要在缓冲区内容被覆盖之前将其保存至 FTP 服务器，请选中 **Save Buffer To FTP Server** 复选框。要允许覆盖缓冲区内容，请取消选中此复选框。

步骤 8 点击 **Configure FTP Settings** 以确定 FTP 服务器并配置用于保存缓冲区内容的 FTP 参数。

步骤 9 选中 **Save Buffer To Flash** 复选框以在缓冲区内容被覆盖之前将其保存至内部闪存。

注释 此选项仅可用于路由模式或透明单模式。

步骤 10 点击 **Configure Flash Usage** 以指定要在内部闪存中应用于日志记录的最大空间以及要保留的最小可用空间（以KB为单位）。启用此选项将在存储消息的设备磁盘上创建一个名为“syslog”的目录。

注释 此选项仅可用于单一路由模式或透明模式。

步骤 11 指定要在 ASA 中查看的系统日志的队列大小。

配置 FTP 设置

要指定用于保存日志缓冲区内容的 FTP 服务器的配置，请执行以下步骤：

过程

步骤 1 选中 **Enable FTP client** 复选框以启用 FTP 客户端的配置。

步骤 2 指定 FTP 服务器的 IP 地址。

步骤 3 指定用于存储已保存日志缓冲区内容的 FTP 服务器的目录路径。

步骤 4 指定用于登录到 FTP 服务器的用户名。

步骤 5 指定与用于登录到 FTP 服务器的用户名相关联的密码。

步骤 6 确认密码，然后点击 **OK**。

配置日志记录闪存的使用

要指定将日志缓冲区内容保存到内部闪存的限制，请执行以下步骤：

过程

步骤 1 指定可用于日志记录的最大内部闪存量（以 KB 为单位）。

步骤 2 指定保留的内部闪存量（以 KB 为单位）。当内部闪存接近该限制时，不再保存新日志。

步骤 3 点击 **OK** 以关闭 **Configure Logging Flash Usage** 对话框。

启用安全日志记录

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **系统日志服务器**。

步骤 2 选择要为其启用安全日志记录的系统日志服务器，然后点击 **Edit**。

系统将显示 **Edit Syslog Server** 对话框。

步骤 3 点击 **TCP** 单选按钮。

安全日志记录不支持 UDP；如果尝试使用此协议，则会发生错误。

步骤 4 选中 **Enable secure syslog with SSL/TLS** 复选框，然后点击 **OK**。

步骤 5 （可选） 按名称指定一个 **Reference Identity** 对象，以对通过系统日志服务器收到的证书启用 RFC 6125 引用标识检查。

有关引用标识对象的详细信息，请参阅 配置引用标识。

将 EMBLEM 格式的系统日志消息生成到系统日志服务器

要将 EMBLEM 格式的系统日志消息生成到系统日志服务器，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **系统日志服务器**。

支持通过 IPv6 发送系统日志。

步骤 2 点击 **Add** 以添加新系统日志服务器。

系统将显示 **Add Syslog Server** 对话框。

注释 可以设置每个安全情景最多四个系统日志服务器（最多 16 个）。

步骤 3 指定当系统日志服务器繁忙时允许在 ASA 上排队的消息数。0 值表示无限数量的消息可以进入队列。

步骤 4 选中 **Allow user traffic to pass when TCP syslog server is down** 复选框，在任何系统日志服务器关闭的情况下允许所有流量。

当ASA配置为向连接TCP的系统日志服务器发送系统日志消息时，如果系统日志服务器发生故障，则作为安全保护，将阻止通过ASA的新连接。要允许新连接（即使系统日志服务器无法运行），请选中此复选框。

如果指定UDP，则无论系统日志服务器是否可运行，ASA都会继续允许新连接。这两个协议的有效端口值为 1025 至 65535。默认 UDP 端口为 514。默认 UDP 端口为 1470。

注释　不支持在备用 ASA 上通过 TCP 发送系统日志。

将 EMBLEM 格式的系统日志消息生成到其他输出目标

要将 EMBLEM 格式的系统日志消息生成到其他输出目标，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **日志记录设置**。

步骤 2 选中 **Send syslogs in EMBLEM format** 复选框。

添加或编辑系统日志服务器设置

要添加或编辑系统日志服务器设置，请执行以下步骤：

过程

步骤 1 从下拉列表中选择用于与系统日志服务器进行通信的接口。

步骤 2 输入用于与系统日志服务器进行通信的 IP 地址。

选择系统日志服务器用于与 ASA 或 ASASM 通信的协议（TCP 或 UDP）。可以将 ASA 和 ASASM 配置为使用 UDP 或 TCP 向系统日志服务器发送数据。如果未指定协议，则默认协议为 UDP。

警告　如果指定TCP，则在ASA发现日志服务器发生故障，出于安全原因，将会阻止通过ASA的新连接。要在系统日志服务器发生故障时允许新连接，请参阅第4步（共将EMBLEM格式的系统日志消息生成到系统日志服务器，第 13 页 步）。

步骤 3 输入系统日志服务器用于与 ASA 或 ASASM 通信的端口号。

步骤 4 选中 **Log messages in Cisco EMBLEM format (UDP only)** 复选框以指定是否记录思科 EMBLEM 格式的消息（仅在选择 UDP 作为协议的情况下才可用）。

步骤 5 选中 **Enable secure logging using SSL/TLS (TCP only)** 复选框以指定通过使用 SSL/TLS over TCP，与系统日志服务器的连接是安全的，并且系统日志消息内容已加密。您可以选择提及引用身份，以根据之前配置的引用身份对象验证证书。有关详细信息，请参阅启用安全日志记录，第 13 页。

步骤 6 点击 **OK** 以完成配置。

将系统日志消息发送至内部日志缓冲区

您需要指定应将哪些系统日志记录消息发送到充当临时存储位置的内部日志缓冲区。新消息附加到列表的末尾。当缓冲区已满时（也就是说，当缓冲区换行时），除非ASA配置为将完整缓冲区保存到其他位置，否则在生成新消息时会覆盖旧消息。

要将系统日志消息发送到内部日志缓冲区，请执行以下步骤：

过程

步骤 1 选择以下其中一个选项以指定应将哪些系统日志记录消息发送到内部日志缓冲区：

- **Home** > **Latest ASDM Syslog Messages** > **Configure ASDM Syslog Filters**
- **Configuration** > **Device Management** > **Logging** > **Logging Filters**

步骤 2 依次选择**监控** > **日志记录** > **日志缓冲区** > **视图**。然后，选择**日志缓冲区**窗格中的**文件** > **清除内部日志缓冲区**以清空内部日志缓冲区。

步骤 3 依次选择**配置** > **设备管理** > **日志记录** > **日志记录设置**，以更改内部日志缓冲区的大小。默认缓冲区大小为 4KB。

ASA 继续将新消息保存到内部日志缓冲区，并将完整日志缓冲区内容保存到内部闪存。将缓冲区内容保存到其他位置时， ASA 会创建具有使用以下时间戳格式的名称的日志文件：

```
LOG-YYYY-MM-DD-HHMMSS.TXT
```

其中 *YYYY* 是年，*MM* 是月，*DD* 是月日期，*HHMMSS* 是时间（以小时、分钟和秒为单位）。

步骤 4 要将新消息保存到其他位置，请选择以下其中一个选项：

- 选中 **Flash** 复选框以将新消息发送至内部闪存，然后点击 **Configure Flash Usage**。系统将显示 **Configure Logging Flash Usage** 对话框。
  1. 指定要用于日志记录的最大闪存量（以 KB 为单位）。
  2. 指定日志记录在闪存中将保留的最小可用空间量（以 KB 为单位）。
  3. 点击 **OK** 以关闭此对话框。
- 选中 **FTP Server** 复选框以将新消息发送到 FTP 服务器，然后点击 **Configure FTP Settings**。系统将显示 **Configure FTP Settings** 对话框。
  1. 选中 **Enable FTP Client** 复选框。
  2. 在提供的字段中输入以下信息：FTP 服务器 IP 地址、路径、用户名和密码。
  3. 确认密码，然后点击 **OK** 以关闭此对话框。

将内部日志缓冲区保存到闪存

要将内部日志缓冲区保存到闪存，请执行以下步骤：

过程

步骤 1 依次选择**文件** > **将内部日志缓存区保存到闪存**。

系统将显示 **Enter Log File Name** 对话框。

步骤 2 选择第一个选项以使用默认用户名 LOG-YYYY-MM-DD-hhmmss.txt 保存日志缓冲区。

步骤 3 选择第二个选项以指定日志缓冲区的文件名。

步骤 4 输入日志缓冲区的文件名，然后点击 **OK**。

更改可用于日志的内部闪存量

要更改可用于日志的内部闪存量，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **日志记录设置**。

步骤 2 选中 **Enable Logging** 复选框。

步骤 3 选中 **Logging to Internal Buffer** 区域中的 **Save Buffer to Flash** 复选框。

步骤 4 点击**配置闪存使用量 (Configure Flash Usage)**。

系统将显示 **Configure Logging Flash Usage** 对话框。

步骤 5 输入允许用于日志记录的最大内部闪存量（以 KB 为单位）。

默认情况下，ASA 可以为日志数据使用最多 1 MB 的内部闪存。可供 ASA 用于保存日志数据的最小内部闪存量为 3 MB。如果保存到内部闪存的日志文件会导致可用内部闪存量低于配置的最小限制，则ASA会删除最早的日志文件，以确保保存新日志文件后最小内存量保持可用。如果没有要删除的文件，或者如果在删除所有旧文件后可用内存仍然低于限制，则 ASA 将无法保存新日志文件。

步骤 6 输入在闪存中要保留用于日志记录的最小可用空间量（以 KB 为单位）。

步骤 7 点击**确定 (OK)** 以关闭**配置日志记录闪存使用量 (Configure Logging Flash Usage)** 对话框。

使用 ASDM Java 控制台查看和复制已记录的条目

使用 ASDM Java 控制台以文本格式查看并复制已记录的条目，这可能有助于对 ASDM 错误进行疑难解答。

要访问 ASDM Java 控制台，请执行以下步骤：

过程

步骤 1 依次选择**工具** > **ASDM Java 控制台**。

步骤 2 在控制台中输入 **m** 以显示虚拟机内存统计信息。

步骤 3 在控制台中输入 **g** 以执行垃圾回收。

步骤 4 打开 Windows 任务管理器并双击 **asdm_launcher.exe** 文件以监控内存使用情况。

注释 允许的最大内存分配为 256 MB。

将系统日志消息发送给邮件消息

如要将系统日志消息发送到邮件地址，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **邮件设置**。

步骤 2 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。

步骤 3 点击 **Add** 以输入指定的系统日志消息的新邮件地址收件人。

步骤 4 从下拉列表中选择发送给收件人的系统日志消息的严重性级别。用于目标邮件地址的系统日志消息严重性过滤器会导致发送指定严重性级别和更高严重性级别的消息。在 **Logging Filters** 窗格中指定的全局过滤器还会应用于每个邮件收件人。

步骤 5 点击 **Edit** 以修改发送给此收件人的系统日志消息的现有严重性级别。

步骤 6 点击 **OK** 以关闭 **Add E-mail Recipient** 对话框。

添加或编辑电子邮件收件人

要添加或编辑邮件收件人和严重性级别，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **邮件设置**。

步骤 2 点击 **Add** 或 **Edit** 以显示 **Add/Edit E-Mail Recipient** 对话框。

步骤 3 输入目标邮件地址，然后从下拉列表中选择系统日志严重性级别。严重性级别定义如下：

- Emergency（级别 0，系统不可用）

  注释 不建议使用严重性级别 0。

- Alert（级别 1，需要立即采取措施）

- Critical（级别 2，严重情况）
- Error（级别 3，错误情况）
- Warning（级别 4，警告情况）
- Notification（级别 5，正常但重大的情况）
- Informational（级别 6，消息仅供参考）
- Debugging（级别 7，消息仅供调试）

注释　用于过滤目标邮件地址的消息的严重性级别是在 **Add/Edit E-Mail Recipient** 对话框中指定的更高的严重性级别，并且是为 **Logging Filters** 窗格中所有邮件收件人设置的全局过滤器。

步骤 4 点击 **OK** 以关闭 **Add/Edit E-Mail Recipient** 对话框。

在 **E-mail Recipients** 窗格中将显示已添加或已修改的条目。

步骤 5 点击 **Apply** 以保存对运行配置所做的更改。

配置远程 SMTP 服务器

要配置为响应特定事件而将邮件提醒和通知发送到的远程 SMTP 服务器，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备设置** > **日志记录** > **SMTP**。

步骤 2 输入主 SMTP 服务器的 IP 地址。

步骤 3 （可选）输入备用 SMTP 服务器的 IP 地址，然后点击 **Apply** 以保存对运行配置所做的更改。

将系统日志消息发送到控制台端口

要将系统日志消息发送到控制台端口，请执行以下步骤：

过程

步骤 1 选择以下选项之一：

- **Home** > **Latest ASDM Syslog Messages** > **Configure ASDM Syslog Filters**
- **Configuration** > **Device Management** > **Logging** > **Logging Filters**

步骤 2 在 **Logging Destination** 列中选择控制台，然后点击 **Edit**。

系统将显示 **Edit Logging Filters** 对话框。

步骤 3 选择来自所有事件类的系统日志或来自特定事件类的系统日志，以指定应将哪些系统日志消息发送到控制台端口。

将系统日志消息发送到 Telnet 或 SSH 会话

要将系统日志消息发送到 Telnet 或 SSH 会话，请执行以下步骤：

过程

步骤 1 选择以下选项之一：

- **Home** > **Latest ASDM Syslog Messages** > **Configure ASDM Syslog Filters**
- **Configuration** > **Device Management** > **Logging** > **Logging Filters**

步骤 2 在 **Logging Destination** 列中选择 **Telnet** 和 **SSH Sessions**，然后点击 **Edit**。

系统将显示 **Edit Logging Filters** 对话框。

步骤 3 选择来自所有事件类的系统日志或来自特定事件类的系统日志，以指定应将哪些系统日志消息发送到 Telnet 或 SSH 会话。

步骤 4 依次选择**配置** > **设备管理** > **日志记录** > **日志记录设置**，以便仅为当前会话启用日志记录。

步骤 5 选中 **Enable logging** 复选框，然后点击 **Apply**。

配置系统日志消息

配置系统日志消息传递

要配置系统日志消息传递，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **系统日志设置**。

步骤 2 为系统日志服务器选择要用作文件消息基础的系统日志设备。默认为大多数 UNIX 系统期望的 LOCAL(4)20。但是，由于网络设备共享八台可用设备，您可能需要为系统日志更改这个值。

步骤 3 选中 **Include timestamp in syslogs** 复选框在发送的各系统日志消息中添加日期和时间。

使用时间戳格式下拉列表选择传统（mm：dd：yyyy hh：mm：ss）或RFC 5424（yyyy：dd：mmTHH：mm：ssZ）格式。

步骤 4 取消选中 **Hide username if its validity cannot be determined** 复选框以显示系统日志消息中用于不成功的登录尝试的无效用户名。在默认情况下，如果用户名无效或者有效性未知时，用户名会被隐藏。例如当用户意外键入密码而不是用户名时，在生成的系统日志消息中隐藏“用户名”会更为安全。您可能希望利用显示的无效用户名对登录问题进行故障排除。

步骤 5 选择要在 **Syslog ID** 表中显示的信息。可用选项如下：

- 选择 **Show all syslog IDs** 以指定 **Syslog ID** 表应显示整个系统日志消息 ID 列表。
- 选择 **Show disabled syslog IDs** 以指定 **Syslog ID** 表应仅显示已显式禁用的系统日志消息 ID。
- 选择 **Show syslog IDs with changed logging** 以指定 **Syslog ID** 表应仅显示严重性级别默认值已更改的系统日志消息 ID。
- 选择 **Show syslog IDs that are disabled or with a changed logging level** 以指定 **Syslog ID** 表应仅显示严重性级别已修改的系统日志消息 ID 和已显式禁用的系统日志消息 ID。

步骤 6 **Syslog ID Setup Table** 根据 Syslog ID Setup Table 中的设置显示系统日志消息列表。选择要修改的单条消息或消息 ID 范围。可以禁用所选消息 ID 或修改其严重性级别。要选择列表中的多个消息 ID，请点击范围中的第一个 ID，然后按住 Shift 键并点击范围中的最后一个 ID。

步骤 7 点击 **Advanced** 以将系统日志消息配置为包含设备 ID。

编辑系统日志 ID 设置

要更改系统日志消息设置，请执行以下步骤：

注释 **Syslog ID** 字段仅用于显示。此区域中显示的值由在位于 **Syslog Setup** 窗格中的 **Syslog ID** 表内的条目确定。

过程

步骤 1 选中 **Disable Message(s)** 复选框以禁用 **Syslog ID** 列表中显示的系统日志消息 ID 的消息。

步骤 2 选择要为 **Syslog ID** 列表中显示的系统日志消息 ID 发送的消息的日志记录严重性级别。严重性级别定义如下：

- Emergency（级别 0，系统不可用）

  注释 不建议使用严重性级别 0。

- Alert（级别 1，需要立即采取措施）
- Critical（级别 2，严重情况）
- Error（级别 3，错误情况）
- Warning（级别 4，警告情况）

- Notification（级别 5，正常但重大的情况）
- Informational（级别 6，消息仅供参考）
- Debugging（级别 7，消息仅供调试）

步骤 3 点击 **OK** 以关闭 **Edit Syslog ID Settings** 对话框。

在非 EMBLEM 格式化系统日志消息中包含设备 ID

要在非 EMBLEM 格式化系统日志消息中包含设备 ID，请执行以下步骤：

过程

步骤 1 选中 **Enable syslog device ID** 复选框以指定应在所有非 EMBLEM 格式化系统日志消息中包含的设备 ID。

步骤 2 要指定使用哪一项作为设备 ID，请选择以下其中一个选项：

- ASA 的主机名
- 接口 IP 地址

  从下拉列表中选择与所选 IP 地址对应的接口名称。

  如果正在使用集群，请选中 **In an ASA cluster, always use master's IP address for the selected interface** 复选框。
- 字符串

  指定用户定义的字母数字字符串。
- ASA 集群名称

步骤 3 点击 **OK** 以关闭 **Advanced Syslog Configuration** 对话框。

在系统日志消息中包含日期和时间

要在系统日志消息中包含日期和时间，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **系统日志设置**。

步骤 2 选中 **Syslog ID Setup** 区域中的 **Include timestamp in syslogs** 复选框。

步骤 3 点击 **Apply** 保存更改。

禁用系统日志消息

要禁用指定的系统日志消息，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **系统日志设置**。

步骤 2 选择要从表中禁用的系统日志，然后点击 **Edit**。

系统将显示 **Edit Syslog ID Settings** 对话框。

步骤 3 选中 **Disable messages** 复选框，然后点击 **OK**。

更改系统日志消息的严重性级别

要更改系统日志消息的严重性级别，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **系统日志设置**。

步骤 2 从表中选择要更改其严重性级别的系统日志，然后点击 **Edit**。

系统将显示 **Edit Syslog ID Settings** 对话框。

步骤 3 从 **Logging Level** 下拉列表中选择期望严重性级别，然后点击 **OK**。

在备用设备上阻止系统日志消息

要阻止在备用设备上生成特定系统日志消息，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **系统日志设置**。

步骤 2 在表中选择系统日志 ID，然后点击 **Edit**。

系统将显示 **Edit Syslog ID Settings** 对话框。

步骤 3 选中 **Disable messages on standby unit** 复选框以阻止在备用设备上生成系统日志消息。

步骤 4 点击 **OK** 以关闭此对话框。

在非 EMBLEM 格式系统日志消息中包含设备 ID

要在非 EMBLEM 格式系统日志消息中包含设备 ID，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **系统日志设置** > **高级** > **高级日志记录配置**。

步骤 2 选中 **Enable syslog device ID** 复选框。

步骤 3 点击**设备 ID (Device ID)** 区域中的**主机名 (Hostname)**、**接口 IP 地址 (Interface IP Address)** 或**字符串 (String)** 单选按钮。

- 如果选择 **Interface IP Address** 选项，请确保在下拉列表中选择正确的接口。
- 如果选择 **String** 选项，请在 **User-Defined ID** 字段中输入设备 ID。字符串可以包含多达 16 个字符。

注释 如果启用，则在 EMBLEM 格式化系统日志消息和 SNMP 陷阱中不会显示设备 ID。

步骤 4 点击 **OK** 以关闭 **Advanced Syslog Configuration** 对话框。

创建自定义事件列表

可以使用以下三个条件来定义事件列表：

- 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，SNMP 服务器）的自定义事件列表，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **事件列表**。

步骤 2 点击**添加 (Add)** 以显示**添加事件列表 (Add Event List)** 对话框。

步骤 3 输入事件列表的名称。不允许使用空格。

步骤 4 点击**添加 (Add)** 以显示 **添加类和严重性过滤器 (Add Class and Severity Filter)** 对话框。

步骤 5 从下拉列表中选择事件类。可用事件类根据使用的设备模式进行更改。

步骤 6 从下拉列表中选择严重性级别。严重性级别包括：

- Emergency（级别 0，系统不可用）

  注释 不建议使用严重性级别 0。

- Alert（级别 1，需要立即采取措施）
- Critical（级别 2，严重情况）
- Error（级别 3，错误情况）
- Warning（级别 4，警告情况）
- Notification（级别 5，正常但重大的情况）
- Informational（级别 6，消息仅供参考）
- Debugging（级别 7，消息仅供调试）

步骤 7 点击**确定 (OK)** 以关闭**添加事件列表 (Add Event List)** 对话框。

步骤 8 点击**添加 (Add)** 以显示**添加系统日志消息 ID 过滤器 (Add Syslog Message ID Filter)** 对话框。

步骤 9 输入要在过滤器中包含的系统日志消息 ID 或 ID 范围（例如 101001 至 199012）。

步骤 10 点击**确定 (OK)** 以关闭**添加事件列表 (Add Event List)** 对话框。

列表中将显示相关事件。

配置日志记录过滤器

将消息过滤器应用于日志记录目标

要将消息过滤器应用于日志记录目标，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **日志记录筛选器**。

步骤 2 选择要对其应用过滤器的日志记录目标的名称。可用的日志记录目标如下：

- ASDM
- 控制台端口
- 邮件
- 内部缓冲区
- SNMP 服务器
- 系统日志服务器
- Telnet 或 SSH 会话

此选择中包含第二列 Syslogs From All Event Classes 和第三列 Syslogs From Specific Event Classes。第二列列出要用于过滤日志记录目标的消息的严重性或事件类，或者是否为所有事件类禁用了日志记录。第三列列出要用于过滤该日志记录目标的消息的事件类。

步骤 3 点击 **Edit** 以显示 **Edit Logging Filters** 对话框。要应用、编辑或禁用过滤器，请参阅应用日志记录过滤器，第 25 页。

应用日志记录过滤器

要应用过滤器，请执行以下步骤：

过程

步骤 1 选择 **Filter on severity** 选项以根据系统日志消息的严重性级别将其过滤。

步骤 2 选择 **Use event list** 选项以根据事件列表过滤系统日志消息。

步骤 3 选择 **Disable logging from all event classes** 选项以禁用到所选目标的所有日志记录。

步骤 4 点击 **New** 以添加新事件列表。要添加新事件列表，请参阅创建自定义事件列表，第 23 页。

步骤 5 从下拉列表中选择事件类。可用事件类根据使用的设备模式进行更改。

步骤 6 从下拉列表中选择日志记录消息的级别。严重性级别包括：

- Emergency（级别 0，系统不可用）

  注释 不建议使用严重性级别 0。

- Alert（级别 1，需要立即采取措施）
- Critical（级别 2，严重情况）
- Error（级别 3，错误情况）
- Warning（级别 4，警告情况）
- Notification（级别 5，正常但重大的情况）
- Informational（级别 6，消息仅供参考）
- Debugging（级别 7，消息仅供调试）

步骤 7 点击 **Add** 以添加事件类和严重性级别，然后点击 **OK**。

顶部将显示为过滤器所选的日志记录目标。

添加或编辑系统日志消息 ID 过滤器

要添加或编辑系统日志消息 ID 过滤器，请参阅编辑系统日志 ID 设置，第 20 页。

添加或编辑消息类和严重性过滤器

要添加或编辑用于过滤消息的消息类和严重性级别，请执行以下步骤：

过程

步骤 1 从下拉列表中选择事件类。可用事件类根据使用的设备模式进行更改。

步骤 2 从下拉列表中选择日志记录消息的级别。严重性级别包括：

- Emergency（级别 0，系统不可用）

  注释 不建议使用严重性级别 0。

- Alert（级别 1，需要立即采取措施）
- Critical（级别 2，严重情况）
- Error（级别 3，错误情况）
- Warning（级别 4，警告情况）
- Notification（级别 5，正常但重大的情况）
- Informational（级别 6，消息仅供参考）
- Debugging（级别 7，消息仅供调试）

步骤 3 进行选择完成后，点击 **OK**。

将类中的所有系统日志消息发送到指定输出目标

要将类中的所有系统日志消息发送到指定输出目标，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **日志记录筛选器**。

步骤 2 要覆盖指定输出目标中的配置，请选择要更改的输出目标，然后点击 **Edit**。

系统将显示 **Edit Logging Filters** 对话框。

步骤 3 修改 **Syslogs from All Event Classes** 或 **Syslogs from Specific Event Classes** 区域中的设置，然后点击 **OK** 以关闭此对话框。

例如，如果指定严重性级别为 7 的消息应该转至内部日志缓冲区，并且严重性级别为 3 的 ha 类消息应该转至内部日志缓冲区，则后者配置优先。

要指定类应转至多个目标，请为每个输出目标选择不同的过滤选项。

限制系统日志消息生成速率

要限制系统日志消息生成速率，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **日志记录** > **速率限制**。

步骤 2 选择要向其指定速率限制的日志记录级别（消息严重性级别）。严重性级别定义如下：

- Emergency（级别 0，系统不可用）
- Alert（级别 1，需要立即采取措施）
- Critical（级别 2，严重情况）
- Error（级别 3，错误情况）
- Warning（级别 4，警告情况）
- Notification（级别 5，正常但重大的情况）
- Informational（级别 6，消息仅供参考）
- Debugging（级别 7，消息仅供调试）

步骤 3 **No of Messages** 字段显示发送的消息数。**Interval (Seconds)** 字段显示用于限制可发送的此日志记录级别的消息数的间隔（以秒为单位）。从表中选择日志记录级别，然后点击 **Edit** 以显示 **Edit Rate Limit for Syslog Logging Level** 对话框。

步骤 4 要继续，请参阅指定或更改各个系统日志消息的速率限制，第 27 页。

指定或更改各个系统日志消息的速率限制

要指定或更改单独系统日志消息的速率限制，请执行以下步骤：

过程

步骤 1 要指定特定系统日志消息的速率限制，请点击 **Add** 以显示 **Add Rate Limit for Syslog Message** 对话框。

步骤 2 要继续，请参阅添加或编辑系统日志消息的速率限制，第 28 页。

步骤 3 要更改特定系统日志消息的速率限制，请点击 **Edit** 以显示 **Edit Rate Limit for Syslog Message** 对话框。

步骤 4 要继续，请参阅编辑系统日志严重性级别的速率限制，第 28 页。

添加或编辑系统日志消息的速率限制

要添加或更改特定系统日志消息的速率限制，请执行以下步骤：

过程

步骤 1 要向特定系统日志消息中添加速率限制，请点击 **Add** 以显示 **Add Rate Limit for Syslog Message** 对话框。要更改系统日志消息的速率限制，请点击 **Edit** 以显示 **Edit Rate Limit for Syslog Message** 对话框。

步骤 2 输入要限制的系统日志消息的消息 ID。

步骤 3 输入在指定时间间隔内可以发送的最大消息数。

步骤 4 输入用于限制指定消息的速率的时间量（以秒为单位），然后点击 **OK**。

注释 要允许无限数量的消息，请将 **Number of Messages** 和 **Time Interval** 字段均留空。

编辑系统日志严重性级别的速率限制

要更改指定系统日志严重性级别的速率限制，请执行以下步骤：

过程

步骤 1 输入可以发送的处于此严重性级别的最大消息数。

步骤 2 输入用于限制处于此严重性级别的消息的速率的时间量（以秒为单位），然后点击 **OK**。

系统将显示所选消息严重性级别。

注释 要允许无限数量的消息，请将 **Number of Messages** 和 **Time Interval** 字段均留空。

分配或更改动态日志记录的速率限制

您可以根据使用的资源（块大小）分配日志记录的速率限制。通过指定阈值（百分比），可以限制系统日志消息的生成速率。您可以进一步定义当块大小使用量超过阈值时允许生成的消息数。

过程

步骤 1 依次选择 **配置** > **设备管理** > **日志记录** > **速率限制**。

步骤 2 在 **动态日志记录的速率限制**下，指定以下内容：

- Block - 指定用作触发动态速率限制的阈值的可用块百分比。
- **消息限制** - 指定动态速率限制允许的消息数。默认值为 10。

步骤 3 点击**应用 (Apply)**。

步骤 4 要修改已保存的值，请输入新值，然后点击 **应用 (Apply)**。

步骤 5 要禁用动态日志记录速率限制，请将字段留空。

监控日志

请参阅以下命令来监控日志记录状态。

- **Monitoring** > **Logging** > **Log Buffer** > **View**

  通过此窗格可查看日志缓冲区。

- **Monitoring** > **Logging** > **Real-Time Log Viewer** > **View**

  通过此窗格可查看实时日志。

- **工具** > **命令行界面**

  您可以在此窗格中发出各种非交互式命令并查看结果。

通过日志查看器过滤系统日志消息

可以根据与“实时日志查看器”和“日志缓冲区查看器”中的任何列对应的一个或多个值筛选系统日志消息。

要通过其中一个日志查看器过滤系统日志消息，请执行以下步骤：

过程

步骤 1 选择以下选项之一：

- **Monitoring** > **Logging** > **Real-Time Log Viewer** > **View**
- **监控** > **日志记录** > **日志缓冲区** > **视图**

步骤 2 在 **Real-Time Log Viewer** 或 **Log Buffer Viewer** 对话框中，点击工具栏上的 **Build Filter**。

步骤 3 在 **Build Filter** 对话框中，指定要应用于系统日志消息的过滤条件。

a) 在 **Date and Time** 区域中选择以下三个选项之一：real-time、特定时间或时间范围。如果选择特定时间，请通过输入数字并从下拉列表中选择小时或分钟来指示时间。如果选择时间范围，请点击 **Start Time** 字段中的下拉箭头以显示日历。从下拉列表中选择开始日期和开始时间，然后点

击 **OK**。点击 **End Time** 字段中的下拉箭头以显示日历。从下拉列表中选择结束日期和结束时间，然后点击 **OK**。

b) 在 **Severity** 字段中输入有效的严重性级别。或者，点击 **Severity** 字段右侧的 **Edit** 图标。点击列表中要按其过滤的严重性级别。要包含严重性级别 1 至 7，请点击 **All**。点击 **OK** 以在 **Build Filter** 对话框中显示这些设置。点击 **Severity** 字段右侧的 **Info** 图标以获取有关要使用的正确输入格式的其他信息。

c) 在 **Syslog ID** 字段中输入有效的系统日志 ID。或者，点击 **Syslog ID** 字段右侧的 **Edit** 图标。从下拉列表中选择要按其过滤的条件，然后点击 **Add**。点击 **OK** 以在 **Build Filter** 对话框中显示这些设置。点击 **Syslog ID** 字段右侧的 **Info** 图标以获取有关要使用的正确输入格式的其他信息。

d) 在 **Source IP Address** 字段中输入有效的源 IP 地址，或者点击 **Source IP Address** 字段右侧的 **Edit** 图标。选择单个 IP 地址或指定的 IP 地址范围，然后点击 **Add**。选中 **Do not include (exclude) this address or range** 复选框以排除特定 IP 地址或 IP 地址范围，点击 **OK** 以在 **Build Filter** 对话框中显示这些设置。点击 **Source IP Address** 字段右侧的 **Info** 图标以获取有关要使用的正确输入格式的其他信息。

e) 在 **Source Port** 字段中输入有效的源端口，或者点击 **Source Port** 字段右侧的 **Edit** 图标。从下拉列表中选择要按其过滤的条件，然后点击 **Add**。点击 **OK** 以在 **Build Filter** 对话框中显示这些设置。点击 **Source Port** 字段右侧的 **Info** 图标以获取有关要使用的正确输入格式的其他信息。

f) 在 **Destination IP Address** 字段中输入有效的目标 IP 地址，或者点击 **Destination IP Address** 字段右侧的 **Edit** 图标。选择单个 IP 地址或指定的 IP 地址范围，然后点击 **Add**。选中 **Do not include (exclude) this address or range** 复选框以排除特定 IP 地址或 IP 地址范围。点击 **OK** 以在 **Build Filter** 对话框中显示这些设置。点击 **Destination IP Address** 字段右侧的 **Info** 图标以获取有关要使用的正确输入格式的其他信息。

g) 在 **Destination Port** 字段中输入有效的目标端口，或者点击 **Destination Port** 字段右侧的 **Edit** 图标。从下拉列表中选择要按其过滤的条件，然后点击 **Add**。点击 **OK** 以在 **Build Filter** 对话框中显示这些设置。点击 **Destination Port** 字段右侧的 **Info** 图标以获取有关要使用的正确输入格式的其他信息。

h) 为 **Description** 字段输入过滤文本。文本可能是由一个或多个字符组成的任意字符串，包括正则表达式。但是，分号是无效字符，并且此设置区分大小写。多个条目须以逗号分隔。

i) 点击 **OK** 以将刚指定的过滤器设置添加到日志查看器中的 **Filter By** 下拉列表。过滤器字符串遵循特定格式。前缀 FILTER: 指定在 **Filter By** 下拉列表中显示的所有自定义过滤器。仍然可以在此字段中键入随机文本。

下表显示所使用的格式的示例。

构建过滤器示例	过滤器字符串格式
Source IP = 192.168.1.1 或 0.0.0.0 Source Port = 67	FILTER: srcIP=192.168.1.1,0.0.0.0;srcPort=67;
Severity = Informational Destination IP = 1.1.1.1 至 1.1.1.10	FILTER: sev=6;dstIP=1.1.1.1-1.1.1.10;
系统日志 ID 不在范围 725001 至 725003 内	FILTER: sysID=!725001-725003;

构建过滤器示例	过滤器字符串格式
Source IP = 1.1.1.1 Description = Built outbound	FILTER: srcIP=1.1.1.1;descr=Built outbound

步骤 4 选择 **Filter By** 下拉列表中的设置之一以过滤系统日志消息，然后点击工具栏上的 **Filter**。此设置还适用于所有将来的系统日志消息。点击工具栏上的 **Show All** 以清除所有过滤器。

注释 无法使用 **Build Filter** 对话框保存已指定的过滤器。这些过滤器仅对其创建期间的 ASDM 会话有效。

编辑过滤设置

要使用 **Build Filter** 对话框编辑所创建的过滤器设置，请执行以下步骤：

过程

选择以下选项之一：

- 通过在 **Filter By** 下拉列表中输入更改，直接修改过滤器。
- 在 **Filter By** 下拉列表中选择过滤器，然后点击 **Build Filter** 以显示 **Build Filter** 对话框。点击 **Clear Filter** 以删除当前的过滤器设置并输入新的过滤器设置。否则，请更改显示的设置，然后点击 **OK**。

  注释 这些过滤器设置仅适用于 **Build Filter** 对话框中定义的过滤器。

- 点击工具栏上的 **Show All** 以停止过滤并显示所有系统日志消息。

使用日志查看器发出特定命令

可以使用任一日志查看器发出以下命令：**ping**、**traceroute**、**whois** 和 **dns lookup**。

要运行其中任何命令，请执行以下步骤：

过程

步骤 1 选择以下选项之一：

- **Monitoring** > **Logging** > **Real-Time Log Viewer** > **View**
- 监控 > 日志记录 > 日志缓冲区 > 视图

步骤 2 从 **Real-Time Log Viewer** 或 **Log Buffer** 窗格中点击 **Tools**，然后选择要执行的命令。或者，可以右键点击所列的特定系统日志消息以显示情景菜单，然后选择要执行的命令。

系统将显示 **Entering command** 对话框，其中所选命令会自动显示在下拉列表中。

步骤 3 在 **Address** 字段中输入所选系统日志消息的源 IP 地址或目标 IP 地址，然后点击 **Go**。

在提供的区域中将显示命令输出。

步骤 4 点击 **Clear** 以删除输出，然后从下拉列表中选择要执行的其他命令。如有必要，请重复第 3 步。完成后点击 **Close**。

日志记录功能历史记录

表 3: 日志记录功能历史记录

功能名称	平台版本	说明
日志记录	7.0(1)	通过各种输出目标提供 ASA 网络日志记录信息，并包括查看和保存日志文件的选项。 引入了以下屏幕：Configuration > Device Management > Logging > Logging Setup。
速率限制	7.0(4)	限制生成系统日志消息的速率。 修改了以下屏幕：Configuration > Device Management > Logging > Rate Limit。
日志记录列表	7.2(1)	创建要在其他命令中用于按各种条件（日志记录级别、事件类和消息 ID）指定消息的日志记录列表。 修改了以下屏幕：Configuration > Device Management > Logging > Event Lists。
安全日志记录	8.0(2)	指定与远程日志记录主机的连接应使用 SSL/TLS。仅在所选的协议为 TCP 的情况下此选项才有效。 修改了以下屏幕：Configuration > Device Management > Logging > Syslog Server。
日志记录类	8.0(4) 至 8.1(1)	添加了对日志记录消息的 ipaa 事件类的支持。 修改了以下屏幕：Configuration > Device Management > Logging > Logging Filters。
日志记录类和已保存的日志记录缓冲区	8.2(1)	添加了对日志记录消息的 dap 事件类的支持。 添加了对清除已保存的日志记录缓冲区（ASDM、内部、FTP 和闪存）的支持。 修改了以下屏幕：Configuration > Device Management > Logging > Logging Setup。

功能名称	平台版本	说明
密码加密	8.3(1)	添加了对密码加密的支持。
日志查看器	8.3(1)	向日志查看器中添加了源 IP 地址和目标 IP 地址。
增强型日志记录和连接阻止	8.3(2)	当您将系统日志服务器配置为使用 TCP 且系统日志服务器不可用时，ASA 将阻止生成系统日志消息的新连接，直到该服务器重新变为可用状态（例如 VPN、防火墙和直接转发代理连接）。此外，此功能已增强，也能在 ASA 上的日志记录队列已满时阻止新连接；连接将在日志记录队列被清除后恢复。 为符合通用标准 EAL4+ 而添加了此功能。除非要求，否则建议在无法发送或接收系统日志消息时允许连接。要允许连接，请继续选中“配置 > 设备管理 > 日志记录 > 系统日志服务器”窗格上的**允许用户流量在 TCP 系统日志服务器停机时通过**复选框。 引入了以下系统日志消息：414005、414006、414007 和 414008。 未修改任何 ASDM 屏幕。
系统日志消息过滤和排序	8.4(1)	已为下列各项添加了支持： • 根据与各列对应的多个文本字符串过滤系统日志消息 • 创建自定义过滤器 • 对消息进行列排序。有关详细信息，请参阅 ASDM 配置指南。 此功能与所有 ASA 版本互操作。 修改了以下屏幕： Monitoring > Logging > Real-Time Log Viewer > View。 Monitoring > Logging > Log Buffer Viewer > View。
集群	9.0(1)	添加了对集群环境下在 ASA 5580 和 5585-X 上生成系统日志消息的支持。 修改了以下屏幕：Configuration > Logging > Syslog Setup > Advanced > Advanced Syslog Configuration。
在备用设备上阻止系统日志	9.4(1)	添加了对于在故障转移配置中的备用设备上阻止生成特定系统日志消息的支持。 修改了以下菜单项：配置 > 设备管理 > 日志记录 > 系统日志设置。
安全系统日志服务器连接的参考身份	9.6(2)	TLS 客户端处理现在支持针对 RFC 6125 第 6 节中定义的服务器身份验证的规则。身份验证将在对到系统日志服务器的 TLS 连接进行 PKI 验证期间进行。如果提供的标识无法与配置的引用标识相匹配，则不会建立连接。 修改了以下页面：**ASDM Configuration > Remote Access VPN > Advanced**, and **Configuration > Device Management > Logging > Syslog Servers -> Add or Edit**。

功能名称	平台版本	说明
系统日志服务器支持 IPv6 地址	9.7(1)	现在，您可以使用 IPv6 地址来配置系统日志服务器，从而通过 TCP 和 UDP 记录、发送和接收系统日志。 修改了以下屏幕：**Configuration** > **Device Management** > **Logging** > **Syslog Servers** > **Add Syslog Server**
日志记录类	9.12(1)	添加了对 BFD、BGP、接口、IPv6、组播、对象组搜索、PBR、路由、SLA 类日志记录消息的支持。 我们修改了以下屏幕：**配置 (Configuration)** > **设备管理 (Device Management)** > **日志记录 (Logging)** > **日志记录过滤器 (Logging Filters)**。
系统日志的环回接口支持	9.18(2)	您现在可以添加环回接口并用于系统日志： 新增/修改的命令： **interface loopback**、**logging host** 新增/修改的屏幕： **配置** > **设备设置** > **接口设置** > **接口** > **添回环接口** 7.19 中添加了 ASDM 支持。
SNMP 系统日志的速率限制	9.20(1)	如果未设置系统范围的速率限制，那么您现在可以为发送到 SNMP 服务器的系统日志单独配置速率限制。

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。