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-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。

EMBLEM 系统日志格式是基于 RFC 3164 和 RFC 5424 标准构建的思科特定约定。因此，在启用 EMBLEM 时，系统日志消息会在<PRI>字段中输入密码。

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。请注意<PRI>字段后的冒号（：）（ *<166>*）。

```
<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。时间戳前不能为冒号 (:)。

```
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。

级别号	严重性级别	说明
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。使用 **logging class** 命令。
- 创建指定消息类的消息列表。使用 **logging list** 命令。

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
-	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

类别	定义	系统日志消息 ID 号
-	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
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

类别	定义	系统日志消息 ID 号
-	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
tag-switching	服务标记交换	779
transactional-rule-engine-tre	事务规则引擎	780
UC-IMS	UC-IMS	339
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	778
webfo	WebVPN 故障转移	721
webvpn	WebVPN 和 Secure Client	716

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。

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。
- 系统日志服务器基于防火墙系统的syslog-ng进程运行。请勿使用外部配置文件，例如SecureWorks的 *scwx.conf* 文件。此类文件与设备不兼容。使用它们将导致解析错误，最终 syslog-ng 进程将失败。
- 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输入新命令。
- 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，限制为每种情景 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。

- 当 TCP 日志记录主机关闭时，其连接状态从“已 连接”*(Connected)* 更改为 “未连接”*(Not connected)*需要大约 6 分钟。日志记录依赖 TCP 检测通道状态；在此之前，日志记录通过通道发送日志。在此期间，当您执行 **show log**时，输出会将 TCP 日志记录主机显示为已连接。TCP 通道关闭后，TCP 日志记录主机状态将更新为 未连接。
- 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

启用日志记录。

logging enable

示例：

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

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 将 ASA 配置为向系统日志服务器发送消息。

可以将 ASA 配置为向 IPv4 或 IPv6 系统日志服务器发送消息。

logging host *interface_name syslog_ip* [**tcp**[*/port*] | **udp** [*/port*] [**format emblem**]]

示例：

```
ciscoasa(config)# logging host dmz1 192.168.1.5 udp/1026
ciscoasa(config)# logging host dmz1 2002::1:1 udp/2020
```

format emblem 关键字为系统日志服务器启用 EMBLEM 格式日志记录（仅限 UDP）。*interface_name* 参数指定访问系统日志服务器所通过的接口。*syslog_ip* 参数指定系统日志服务器的 IP 地址。**tcp**[*/port*] or**udp**[*/udp*] 关键字-参数对指定 ASA 应使用 TCP 或 UDP 将系统日志消息发送到系统日志服务器。

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。

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。要允许新连接而不考虑与 TCP 系统日志服务器的连接，请参阅第 3 步。

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。

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。

logging trap {*severity_level* | *message_list*}

示例：

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

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。可以指定标识要发送到系统日志服务器的系统日志消息的自定义消息列表。

步骤 3 （可选）禁用在 TCP 连接的系统日志服务器关闭时阻止新连接的功能。

logging permit-hostdown

示例：

```
ciscoasa(config)# logging permit-hostdown
```

如果将 ASA 配置为将系统日志消息发送至基于 TCP 的系统日志服务器，并且其中任何一个系统日志服务器关闭或日志队列已满，则会阻止到ASA的新连接。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。使用此命令，即使系统日志服务器无法运行，也可以允许新连接。

步骤 4 （可选）将日志记录设备设置为大多数 UNIX 系统期望的除 20 以外的值。

logging facility 编号

示例：

```
ciscoasa(config)# logging facility 21
```

启用安全日志记录

过程

通过在 logging host 命令中指定 **secure** 关键字启用安全日志记录。此外，还可以选择输入 **reference-identity**。

logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**[**reference-identity** *reference_identity_name*]]

其中：

- **logging host** *interface_name syslog_ip* 指定系统日志服务器所在的接口以及系统日志服务器的 IP 地址。
- [**tcp**/*port* | **udp**/*port*] 指定系统日志服务器为获取系统日志消息所侦听的端口（TCP 或 UDP）。**tcp** 关键字指定 ASA 应使用 TCP 将系统日志消息发送到系统日志服务器。**udp** 关键字指定 ASA 应使用 UDP 将系统日志消息发送到系统日志服务器。
- **format emblem** 关键字为系统日志服务器启用 EMBLEM 格式日志记录。
- **secure** 关键字指定与远程日志记录主机的连接应仅对 TCP 使用 SSL/TLS。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。
- [**reference-identity** *reference_identity_name*] 基于先前配置的引用标识对象启用对证书的 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。

示例：

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure  reference-identity
syslogServer
```

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

使用端口 514 通过 UDP 将 EMBLEM 格式的系统日志消息发送到系统日志服务器。

logging host *interface_name ip_address*{**tcp** [*/port*] | **udp** [*/ port*]] [**format emblem**]

示例：

```
ciscoasa(config)# logging host interface_1 127.0.0.1 udp format emblem
ciscoasa(config)# logging host interface_1 2001::1 udp format emblem
```

您可以配置 IPv4 或 IPv6 系统日志服务器。

format emblem 关键字为系统日志服务器启用 EMBLEM 格式日志记录（仅限 UDP）。*interface_name* 参数指定访问系统日志服务器所通过的接口。*ip_address* 参数指定系统日志服务器的 IP 地址。**tcp**[*/port*] or**udp**[*/udp*] 关键字和参数对指定 ASA 应使用 TCP 或 UDP 将系统日志消息发送到系统日志服务器。

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。

可以使用多个 **logging host** 命令指定将全部接收系统日志消息的其他服务器。如果配置两个或多个系统日志服务器，请确保对于所有日志记录服务器将日志记录严重性级别限于警告。

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 3 步（共 将系统日志消息发送至外部系统日志服务器，第 10 页 步）。

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

将 EMBLEM 格式的系统日志消息发送到系统日志服务器之外的输出目标，例如 Telnet 或 SSH 会话。

logging emblem

示例：

```
ciscoasa(config)# logging emblem
```

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 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。

logging buffered {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging buffered critical
ciscoasa(config)# logging buffered level 2
ciscoasa(config)# logging buffered notif-list
```

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。要清空内部日志缓冲区，请输入 **clear logging buffer** 命令。

步骤 2 更改内部日志缓冲区的大小。默认缓冲区大小为 4 KB。

logging buffer-size 字节

示例：

```
ciscoasa(config)# logging buffer-size 16384
```

注释
当更改日志记录缓冲区大小时，缓冲区中的现有日志将被清除，并使用新配置的大小创建新的缓冲区。

步骤 3 选择以下其中一个选项：

- 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。

  logging flash-bufferwrap

  示例：

  ```
  ciscoasa(config)# logging flash-bufferwrap
  ```

注释
如果缓冲区大小超过 2 MB，该命令将停止在闪存中写入数据，且不会发出任何警告。

- 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 FTP 服务器。

  logging ftp-bufferwrap

  示例：

  ```
  ciscoasa(config)# logging ftp-bufferwrap
  ```

  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）。

- 标识要存储日志缓冲区内容的 FTP 服务器。

  logging ftp-server *server pathusername password*

  示例：

  ```
  ciscoasa(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
  ```

  server 参数指定外部 FTP 服务器的 IP 地址。*path* 参数指定要在其上保存日志缓冲区数据的 FTP 服务器上的目录路径。此路径相对于 FTP 根目录。*username* 参数指定可日志记录到 FTP 服务器中的用户名。*password* 参数指示所指定用户名的 密码。

- 将当前日志缓冲区内容保存到内部闪存。

  logging savelog [*savefile*]

  示例：

  ```
  ciscoasa(config)# logging savelog latest-logfile.txt
  ```

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 指定可用于保存日志文件的最大内部闪存量。

logging flash-maximum-allocation *kbytes*

示例：

```
ciscoasa(config)# logging flash-maximum-allocation 1200
```

默认情况下，ASA 可以为日志数据使用最多 50 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。flash-maximum-allocation 值的最大限制为 2 GB。

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 2 指定必须可供 ASA 用于保存日志文件的最小内部闪存量。

logging flash-minimum-free *kbytes*

示例：

```
ciscoasa(config)# logging flash-minimum-free 4000
```

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 指定应将哪些系统日志消息发送到邮件地址。

logging mail {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging mail high-priority
```

通过邮件发送时，系统日志消息显示在邮件的主题行中。因此，建议将此选项配置为通知管理员具有高严重性级别（例如 critical、alert 和 emergency）的系统日志消息。

步骤 2 指定在将系统日志消息发送到邮件地址时要使用的源邮件地址。

logging from-address *email_address*

示例：

```
ciscoasa(config)# logging from-address xxx-001@example.com
```

步骤 3 指定在将系统日志消息发送到邮件地址时要使用的收件人邮件地址。

logging recipient-address *e-mail_address*[*severity_level*]

示例：

```
ciscoasa(config)# logging recipient-address admin@example.com
```

步骤 4 指定在将系统日志消息发送到邮件地址时要使用的 SMTP 服务器。您可以提供主服务器和辅助服务器地址，以确保日志消息服务永不中断。或者，您也可以将接口与服务器关联，以识别要用于日志记录的路由表。如果未提供接口，ASA 将引用管理路由表，如果没有适当的路由条目，则会查看数据路由表。

smtp-server [*primary-interface*] *primary-smpt-server-ip-address* [[*backup-interface*]*backup-smpt-server-ip-address*]

示例：

```
ciscoasa(config)# smtp-server 10.1.1.24 10.1.1.34
ciscoasa(config)# smtp-server 10.1.1.24
ciscoasa(config)# smtp-server management 10.1.1.24 outside 10.1.1.34
ciscoasa(config)# smtp-server management 10.1.1.24
```

将系统日志消息发送到 ASDM

要将系统日志消息发送到 ASDM，请执行以下步骤：

过程

步骤 1 指定应将哪些系统日志消息发送到 ASDM。

logging asdm {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging asdm 2
```

ASA 为等待发送到ASDM的系统日志消息预留一个缓冲区，并在消息出现时将其保存在缓冲区中。ASDM 日志缓冲区是不同于内部日志缓冲区的缓冲区。当 ASDM 日志缓冲区已满时，ASA 将删除最早的系统日志消息以在缓冲区中为新系统日志消息腾出空间。删除最早的系统日志消息来为新系统日志消息腾出空间是ASDM中的默认设置。要控制ASDM日志缓冲区中保留的系统日志消息数，可以更改缓冲区的大小。

步骤 2 指定要在 ASDM 日志缓冲区中保留的系统日志消息数。

logging asdm-buffer-size *num_of_msgs*

示例：

```
ciscoasa(config)# logging asdm-buffer-size 200
```

输入 **clear logging asdm** 命令以清空 ASDM 日志缓冲区的当前内容。

配置日志记录队列

要配置日志记录队列，请执行以下步骤：

过程

指定 ASA 将系统日志消息发送到已配置的输出目标之前可以在其队列中保留的系统日志消息数。

logging queue *message_count*

示例：

```
ciscoasa(config)# logging queue 300
```

ASA 在内存中具有固定的块数，这些块可以分配用于在系统日志消息等待发送到已配置的输出目标时将其缓冲存储。所需的块数取决于系统日志消息队列的长度和所指定系统日志服务器的数量。默认队列大小为 512 条系统日志消息。队列大小仅受块内存可用性的限制。有效值为 0 至 8192 条消息，具体视平台而定。如果日志记录队列设置为 0，则队列的最大可配置大小为 8192 条消息。

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

指定应将哪些系统日志消息发送到控制台端口。

logging console { *severity_level* | *message_list*}

示例：

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

将系统日志消息发送到 SNMP 服务器

要启用到 SNMP 服务器的日志记录，请执行以下步骤。

过程

启用 SNMP 日志记录并指定要将哪些消息发送到 SNMP 服务器。

logging history [**rate-limit** *number interval* | **level** *level* | *logging_list* | *level*]

如果使用 **logging rate-limit** 命令来设置全局速率限制，则该命令优先于此命令中的 **rate-limit** 关键字。

示例：

```
ciscoasa(config)# logging history errors


ciscoasa(config)# logging history rate-limit 15 15 level critical
```

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 指定应将哪些系统日志消息发送到 Telnet 或 SSH 会话。

logging monitor {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging monitor 6
```

步骤 2 启用仅到当前会话的日志记录。

terminal monitor

示例：

```
ciscoasa(config)# terminal monitor
```

如果注销然后再次登录，则需要重新输入此命令。输入 **terminal no monitor** 命令以禁用到当前会话的日志记录。

配置系统日志消息

在系统日志显示或隐藏无效用户名

在系统日志消息中可显示或隐藏登录尝试未成功的无效用户名。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。

过程

步骤 1 显示无效用户名：

no logging hide username

步骤 2 隐藏无效用户名：

logging hide username

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

指定系统日志消息应包含其生成日期和时间。

logging timestamp

示例：

```
ciscoasa(config)# logging timestamp
LOG-2008-10-24-081856.TXT
```

要从系统日志消息中删除日期和时间，请输入 **no logging timestamp** 命令。

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

阻止 ASA 生成特定系统日志消息。

no logging message *syslog_id*

示例：

```
ciscoasa(config)# no logging message 113019
```

要重新启用已禁用的系统日志消息，请输入 **logging message** *syslog_id* 命令（例如，**logging message 113019**）。要重新启用所有已禁用系统日志消息的日志记录，请输入 **clear configure logging disabled** 命令。

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

指定系统日志消息的严重性级别。

logging message *syslog_id* **level** *severity_level*

示例：

```
ciscoasa(config)# logging message 113019 level 5
```

要将系统日志消息的严重性级别重置为其设置，请输入 **no logging message***syslog_id***level***severity_level* 命令（例如 **no logging message 113019 level 5**）。要将所有已修改的系统日志消息的严重性级别重置为其设置，请输入 **clear configure logging level** 命令。

在备用设备上阻止系统日志消息

过程

使用以下命令阻止在备用单元上正在生成的特定系统日志消息。

no logging message *syslog-id* **standby**

示例：

```
ciscoasa(config)# no logging message 403503 standby
```

取消阻止特定的系统日志消息，以确保在发生故障转移的情况下，故障转移备用ASA的系统日志消息保持同步。使用 **logging standby** 命令取消阻止以前阻止在备用设备上生成的特定系统日志消息。

注释
当主用和备用 ASA 同时记录的稳定状态期间，共享日志记录目标（例如系统日志服务器、SNMP 服务器和 FTP 服务器）上的流量翻倍。但是，在发生故障转移时，在切换阶段，备用 ASA 会生成更多事件，包括主用设备的切换入侵和连接事件。

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

将 ASA 配置为在非 EMBLEM 格式系统日志消息中包含设备 ID。只能为系统日志指定一种类型的设备 ID。

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

示例：

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

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。

注释
在 ASA 集群中，始终使用所选接口的控制单元 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）

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。

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 指定用于选择要保存在内部日志缓冲区中的消息的条件。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。

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

示例：

```
ciscoasa(config)# logging list list-notif level 3
```

姓名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。

注释
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。

步骤 2 （可选）向列表中添加更多消息选择条件。

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

示例：

```
ciscoasa(config)# logging list list-notif message 104024-105999
ciscoasa(config)# logging list list-notif level critical
ciscoasa(config)# logging list list-notif level warning class ha
```

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，可以将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 104024 至 105999。
- 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）。

注释
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。

配置日志记录过滤器

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

覆盖指定的输出目标命令中的配置。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。

logging class *message_class* {**buffered** | **console** | **history** | **mail** | **monitor** | **trap**} [*severity_level*]

示例：

```
ciscoasa(config)# logging class ha buffered alerts
```

buffered、**history**、**mail**、**monitor** 和 **trap** 关键字指定应将此类中的系统日志消息发送到的输出目标。**history** 关键字启用 SNMP 日志记录。**monitor** 关键字启用 Telnet 和 SSH 日志记录。**trap** 关键字启用系统日志服务器日志记录。每个命令行条目选择一个目标。要指定类应转至多个目标，请为每个输出目标输入一个新命令。

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

在指定时间段内将指定的严重性级别（1 至 7）应用于消息集或单条消息（不是目标）。

logging rate-limit {**unlimited** | {*num* [*interval*]}} **message** *syslog_id* | **level** *severity_level*

示例：

```
ciscoasa(config)# logging rate-limit 1000 600 level 6
```

速率限制会影响发送到所有已配置的目标的消息量。要将日志记录速率限制重置为默认值，请输入 **clear running-config logging rate-limit** 命令。要重置日志记录速率限制，请输入 **clear configure logging rate-limit** 命令。

监控日志

请参阅以下命令来监控日志记录状态。

- **show logging**

  此命令显示系统日志消息，包括严重性级别。

注释

- 可供查看的最大系统日志消息数为 1000，这是默认设置。可供查看的最大系统日志消息数为 2000。
- 即使在执行 **clear logging counters all** 命令后，输出中仍会显示 **show logging** 的主机发送计数器。

- **show logging message**

  此命令显示严重性级别已修改的系统日志消息和已禁用的系统日志消息的列表。

- **show logging message** *message_ID*

  此命令显示特定系统日志消息的严重性级别。

- **show logging queue**

  此命令显示日志记录队列和队列统计信息。

- **show running-config logging rate-limit**

此命令显示当前日志记录速率限制设置。

- **配置** > **防火墙** > **访问规则**

  此窗格允许您根据搜索条件（规则十六进制ID）将日志记录的实时查看器过滤为特定日志。要查看结果，请选择规则并点击**显示日志 (Show Log)**。

日志记录示例

以下示例显示所显示的有关 **show logging** 命令的日志记录信息。

```
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address “10.1.1.1”
    Mail logging: disabled
    ASDM logging: disabled
```

```
ciscoasa (config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: enabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 330272 messages logged
    Trap logging: level debugging, facility 20, 325464 messages logged
        Logging to inside 2001:164:5:1::123
    Permit-hostdown logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

以下示例显示如何同时控制是否启用了系统日志消息以及指定的系统日志消息的严重性级别：

```
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)

ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503
```

```
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (disabled)

ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)
```

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。
速率限制	7.0(4)	限制生成系统日志消息的速率。 引入了以下命令：**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。 引入了以下命令：**logging list**。
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。 修改了以下命令：**logging host**。
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。 修改了以下命令：**logging class**。
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。 修改了以下命令：**logging class**。 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。 引入了以下命令：**clear logging queue bufferwrap**。
密码加密	8.3(1)	添加了对密码加密的支持。 修改了以下命令：**logging ftp server**。
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。

功能名称	平台版本	说明
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，请继续使用 **logging permit-hostdown**命令。 引入了以下系统日志消息：414005、414006、414007 和 414008。 修改了以下命令：**show logging**。
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。
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。 修改了以下命令：**logging device-id**。
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。 引入了以下命令：**logging message** *syslog-id* **standby**。
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。 添加或修改了以下命令：**[no] crypto ca reference-identity**、**logging host**。
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。 修改了以下命令：**logging host**
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。 修改了以下命令：**logging class**。
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**

功能名称	平台版本	说明
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。 新增/修改的命令：**logging history rate-limit**

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。