log – lz

- log， 第 3 页
- log-adjacency-changes， 第 5 页
- log-adj-changes， 第 9 页
- log-adjacency-changes， 第 10 页
- logging asdm， 第 11 页
- logging asdm-buffer-size， 第 13 页
- logging buffered， 第 15 页
- logging buffer-size， 第 17 页
- logging class， 第 19 页
- logging console， 第 23 页
- logging debug-trace， 第 25 页
- logging debug-trace persistent， 第 27 页
- logging device-id， 第 29 页
- logging emblem， 第 31 页
- logging enable， 第 33 页
- logging facility， 第 35 页
- logging flash-bufferwrap， 第 37 页
- logging flash-maximum-allocation， 第 39 页
- logging flash-minimum-free， 第 41 页
- logging flow-export-syslogs， 第 43 页
- logging from-address， 第 45 页
- logging ftp-bufferwrap， 第 47 页
- logging ftp-server， 第 49 页
- logging hide username， 第 51 页
- logging history， 第 53 页
- logging host， 第 55 页
- logging list， 第 58 页
- logging mail， 第 62 页
- logging message， 第 64 页

- logging message standby， 第 66 页
- logging monitor， 第 67 页
- logging permit-hostdown， 第 69 页
- logging queue， 第 71 页
- logging rate-limit， 第 73 页
- logging recipient-address， 第 76 页
- logging savelog， 第 79 页
- logging standby， 第 81 页
- logging timestamp， 第 83 页
- logging trap， 第 85 页
- login， 第 87 页
- login-button， 第 89 页
- login-message， 第 91 页
- login-title， 第 93 页
- 徽标， 第 95 页
- logout， 第 97 页
- logout-message， 第 98 页
- lsp-full suppress， 第 100 页
- lsp-gen-interval， 第 104 页
- lsp-refresh-interval， 第 108 页

log

使用模块化策略框架时，通过在 match 或 class 配置模式下使用 **match** 命令，记录与 **log**命令或类映射匹配的数据包。此日志操作在检测策略映射（ **policy-maptypeinspect**命令）中可用于应用流量。要禁用此操作，请使用此命令的 no 形式。

log
nolog

Syntax Description

此命令没有任何参数或关键字。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
匹配和类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

检查策略图由一个或多个 **match**和 **class**命令组成。检查策略图可用的确切命令取决于应用程序。输入 **match** 或 **class** 命令标识应用流量（ **class** 命令是指现有的 **class-maptypeinspect**命令，后者包含 **match** 命令）后，可以输入 **log**命令记录与 **match** 命令或 **class** 命令。

在第 3/4 层策略映射（下简称 **policy-map** 命令）中使用 **inspect** 命令启用应用检测时，您可以启用包含此操作的检测策略映射，例如，请输入 **inspecthttphttp_policy_map** 命令，其中 http_policy_map 是检测策略映射的名称。

CR_Examples

以下示例在数据包与 http-traffic 类映射匹配时发送日志。

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# log
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。

命令	说明
class-maptypeinspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
policy-maptypeinspect	定义特殊的应用检查操作。
showrunning-configpolicy-map	显示所有当前的策略映射配置。

log-adjacency-changes

要使 IS-IS 在 NLSP IS-IS 邻接关系更改状态（打开或关闭）时发送系统日志消息，请在路由器 isis 配置模式下使用 **log-adjacency-changes** 命令。要关闭此功能，请使用此**no**命令的形式。

log-adjacency-changes [**all**]
no log-adjacency-changes [**all**]

Syntax Description

all	（可选）包括非 IIH 事件生成的更改。

Command Default

此命令默认禁用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
IPv6 路由器配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

此命令允许监控 IS-IS 邻接状态更改。这在监控大型网络时可能非常有用。使用系统错误消息工具记录消息。消息的形式如下：

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

CR_Examples

以下示例指示路由器记录邻接更改：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# log-adjacency-changes
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。

命令	说明
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定IS-IS实例全局使用的IS-IS报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertise-prefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。

命令	说明
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置LSP刷新间隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级。
routeprioorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。

命令	说明
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

log-adj-changes

要配置路由器在 OSPF 邻居启动或关闭时发送系统日志消息，请在 **log-adj-changes**路由器配置模式下使用该命令。要关闭此功能，请使用此**no**命令的形式。

log-adj-changes [**detail**]
no log-adj-changes [**detail**]

Syntax Description

detail	（可选）每次状态改变时都发送系统日志消息，而不仅仅是在邻居启动或关闭时发送。

Command Default

默认情况下会启用此命令。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
路由器配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

默认情况下，将启用**log-adj-changes** 命令；默认情况下，默认值为“禁用”。在这种情况下，除非使用 **no** 形式将其删除，否则它将显示在运行配置中。

CR_Examples

以下示例在 OSPF 邻居启动或关闭时禁用系统日志消息的发送：

```
ciscoasa(config)# router ospf 5
ciscoasa(config-router)# no log-adj-changes
```

Related Commands

命令	说明
routerospf	进入路由器配置模式。
showospf	显示关于OSPF路由过程的一般信息。

log-adjacency-changes

要配置路由器在 OSPFv3 邻居启动或关闭时发送系统日志消息，请在 **log-adjacency-changes**IPv6 路由器配置模式下使用该命令。要关闭此功能，请使用此**no**命令的形式。

log-adjacency-changes [**detail**]
no log-adjacency-changes [**detail**]

Syntax Description

detail	（可选）每次状态改变时都发送系统日志消息，而不仅仅是在邻居启动或关闭时发送。

Command Default

默认情况下会启用此命令。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
路由器配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

默认情况下，将启用**log-adjacency-changes** 命令；默认情况下，默认值为“禁用”。在这种情况下，除非使用 **no** 形式将其删除，否则它将显示在运行配置中。

CR_Examples

以下示例在 OSPFv3 邻居启动或关闭时禁用发送系统日志消息：

```
ciscoasa(config)# ipv6router ospf 5
ciscoasa(config-router)# no log-adjacency-changes
```

Related Commands

命令	说明
ipv6routerospf	进入路由器配置模式。
showipv6ospf	显示关于 OSPFv3 路由过程的一般信息。

logging asdm

要将系统日志消息发送到 ASDM 日志缓冲区，请在 **loggingasdm** 全局配置模式下使用该命令。要禁用记录到 ASDM 日志缓冲区的 **no**功能，请使用此命令的形式。

loggingasdm [*logging_list* | *level*]
no loggingasdm [*logging_list* | *level*]

Syntax Description

水平　设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为3，则ASA将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示：

- 或**0emergencies**— 系统不可用。
- 或**1alerts**——需要立即采取行动。
- 或**2critical**——危急情况。
- 或**3errors**——错误情况。
- 或**4warnings**——警告情况。
- 或**5notifications**——正常但重要的情况。
- **6**或**informational**—信息性消息。
- 或**7debugging**——调试消息。

注释
由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与Cisco技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

logging_list　指定标识要发送到 ASDM 日志缓冲区的消息的列表。有关创建列表的信息，请参阅 **logginglist** 命令。

Command Default

默认情况下，ASDM 日志记录处于禁用状态。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

在将任何消息发送到 ASDM 日志缓冲区之前，您必须使用 **loggingenable** 命令启用日志记录。

当ASDM日志缓冲区已满时，ASA会删除最旧的消息，以便在缓冲区中为新消息腾出空间。要控制 ASDM 日志缓冲区中保留的系统日志消息数量，请使用该 **loggingasdm-buffer-size**命令。

ASDM 日志缓冲区与该命令启用的日志缓冲区不 **loggingbuffered**同。

CR_Examples

以下示例显示如何启用日志记录，将严重性级别为 0、1 和 2 的日志缓冲区消息发送到 ASDM，以及如何将 ASDM 日志缓冲区大小设置为 200 消息：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging asdm 2
ciscoasa(config)# logging asdm-buffer-size 200
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

Related Commands

命令	说明
clearloggingasdm	清除 ASDM 日志缓冲区中包含的所有消息。
loggingasdm-buffer-size	指定 ASDM 日志缓冲区中保留的 ASDM 消息数
loggingenable	启用日志记录。
logginglist	创建可重复使用的消息选择标准列表。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示日志记录配置。

logging asdm-buffer-size

要指定ASDM日志缓冲区中保留的系统日志消息数，请在全局配置模式下使用**loggingasdm-buffer-size**命令。要将 ASDM 日志缓冲区大小重置为默认的 100 条消息，请使用此命令的 **no** 形式。

loggingasdm-buffer-size*num_of_msgs*
no loggingasdm-buffer-size*num_of_msgs*

Syntax Description

num_of_msgs	指定 ASA 在 ASDM 日志缓冲区中保留的系统日志消息数。

Command Default

默认 ASDM 系统日志缓冲区大小为 100 条消息。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

当ASDM日志缓冲区已满时，ASA会删除最旧的消息，以便在缓冲区中为新消息腾出空间。要控制是否启用记录到 ASDM 日志缓冲区的日志记录或控制保留在 ASDM 日志缓冲区中的系统日志消息的类型，请使用 **loggingasdm** 命令。

ASDM 日志缓冲区与该命令启用的日志缓冲区不 **loggingbuffered**同。

CR_Examples

以下示例显示如何启用日志记录，将严重性级别为 0、1 和 2 的消息发送到 ASDM 日志缓冲区，以及如何将 ASDM 日志缓冲区大小设置为 200 条消息：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging asdm 2
ciscoasa(config)# logging asdm-buffer-size 200
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
```

```
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: level critical, 48 messages logged
```

Related Commands

命令	说明
clearloggingasdm	清除 ASDM 日志缓冲区中包含的所有消息。
loggingasdm	启用到 ASDM 日志缓冲区的日志记录。
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示当前正在运行的日志配置。

logging buffered

要使 ASA 能够将系统日志消息发送到日志缓冲区，请在 **loggingbuffered** 全局配置模式下使用该命令。要禁用将日志记录到日志缓冲区，请使用此命令的 **no** 形式。

loggingbuffered [*logging_list* | *level*]
no loggingbuffered [*logging_list* | *level*]

Syntax Description

水平	设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为 3，则 ASA 将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示： • 或**0emergencies**— 系统不可用。 • 或**1alerts**——需要立即采取行动。 • 或**2critical**——危急情况。 • 或**3errors**——错误情况。 • 或**4warnings**——警告情况。 • 或**5notifications**——正常但重要的情况。 • **6**或**informational**—信息性消息。 • 或**7debugging**——调试消息。 **注释** 由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。
日志记录列表	指定标识要发送到日志缓冲区的消息的列表。有关创建列表的信息，请参阅**logginglist** 命令。

Command Default

默认值如下：

- 日志记录到缓冲区已禁用。
- 缓冲区大小为 4 KB。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

在任何消息发送到日志缓冲区之前，必须使用 **loggingenable** 命令启用日志记录。

新消息将附加到缓冲区的末端。当缓冲区填满时，ASA 会清除缓冲区并继续向其中添加消息。当日志缓冲区已满时，ASA 会删除最旧的消息，以便在缓冲区中为新消息腾出空间。您可以在缓冲区的内容每次“包装”时自动保存缓冲区内容，这意味着自上次保存以来的所有邮件都已替换为新邮件。有关详细信息，请参阅 **loggingflash-bufferwrap**和 **loggingftp-bufferwrap**命令。

您可以随时将缓冲区的内容保存到闪存。有关详细信息，请参阅 **loggingsavelog**命令。

您可以使用 **showlogging** 命令查看已发送到缓冲区的系统日志消息。

CR_Examples

以下示例为严重性级别为 0 且事件为 1 的缓冲区配置日志记录：

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

以下示例创建一个名为“notif-list”的列表，最大严重性级别为 7，并为将日志记录配置到缓冲区，以便为“notif-list”列表标识的系统日志消息配置日志记录：

```
ciscoasa(config)# logging list notif-list level 7
ciscoasa(config)# logging buffered notif-list
ciscoasa(config)#
```

Related Commands

命令	说明
clearloggingbuffer	清除包含的所有系统日志消息的日志缓冲区。
loggingbuffer-size	指定日志缓冲区大小。
loggingenable	启用日志记录。
logginglist	创建可重复使用的消息选择标准列表。
loggingsavelog	将日志缓冲区的内容保存到闪存。

logging buffer-size

要指定日志缓冲区的大小，请在全局配置模式下使用命令 **loggingbuffer-size**。要将日志缓冲区重置为其默认大小 4 KB 内存，请使用此命令的 **no** 形式。

loggingbuffer-size*bytes*
no loggingbuffer-size*bytes*

Syntax Description

bytes	设置用于日志缓冲区的内存量（以字节为单位）。例如，如果指定 8192，则 ASA 将 8 KB 的内存用于日志缓冲区。

Command Default

默认日志缓冲区大小为 4 KB 内存。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

要查看 ASA 是否使用的日志缓冲区大小不是默认缓冲区大小，请使用 **showrunning-configlogging** 命令。如果未显示 **loggingbuffer-size** 命令，则 ASA 使用 4 KB 的日志缓冲区。

有关 ASA 如何使用缓冲区的详细信息，请参阅 **loggingbuffered** 命令。

CR_Examples

以下示例启用日志记录缓冲区，并指定 ASA 将 16 KB 的内存用于日志缓冲区：

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

Related Commands

命令	说明
clearloggingbuffer	清除包含的所有系统日志消息的日志缓冲区。
loggingbuffered	启用将日志记录记录到日志缓冲区。

命令	说明
loggingenable	启用日志记录。
loggingflash-bufferwrap	当日志缓冲区已满时，将日志缓冲区写入到闪存。
loggingsavelog	将日志缓冲区的内容保存到闪存。

logging class

要为消息类配置每个日志记录目标的最大严重性级别，请在全局配置模式下使用**loggingclass**命令。要删除消息类别严重性级别配置，请使用此命令的 **no**形式。

logging class类目标级别 [目标级别 . . .]
no logging class *class*

Syntax Description

class	指定最大严重性级别按目标配置的消息类。有关 类 的有效值，请参阅“使用指南”部分。
destination	为 类指定日志记录目标。对于目标， 级别 确定发送到 目标 的最大严重性级别。有关 *destination*的有效值，请参阅下面的“使用指南”部分。
水平	设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为 3，则 ASA 将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示： • 或**0emergencies**— 系统不可用。 • 或**1alerts**——需要立即采取行动。 • 或**2critical**——危急情况。 • 或**3errors**——错误情况。 • 或**4warnings**——警告情况。 • 或**5notifications**——正常但重要的情况。 • **6**或**informational**—信息性消息。 • 或**7debugging**——调试消息。 **注释** 由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此， **请** 仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

Command Default

默认情况下，ASA 不会对日志记录目标和消息类应用严重性级别。相反，每个已启用的日志记录目标接收其严重性级别（由日志记录列表确定）或接收启用日志记录目标时指定的严重性级别的所有类的消息。

Command Modes

下表显示了您可以输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.2(1)	添加了此命令。
8.0(2)	**eigrp** 选项已添加到有效的类别值。
8.2(1)	**dap** 选项已添加到有效的类别值。
9.12(1)	已为有效类别值添加 **bfd, bgp, idb, ipv6, multicast, routing, object-group-search, pbr, sla** 选项

使用指南

类 别的有效值包括以下内容：

- —用**auth**户身份验证。
- —**bfd**BFD路由
- —**bgp**BGP路由
- —**bridge**透明防火墙。
- —**ca**PKI 证书颁发机构。
- —**config**命令界面。
- 动态访**dap**—问策略。
- —**eap**可扩展身份验证协议 (EAP)。记录以下类型的事件以支持网络准入控制：EAP 会话状态更改、EAP 状态查询事件以及 EAP 报头和数据包内容的十六进制转储。
- —**eapoudp**UDP 上的可扩展身份验证协议 (EAP)。记录 EAPoUDP 事件以支持网络准入控制，并生成 EAPoUDP 报头和数据包内容的完整记录。
- —**eigrp**EIGRP 路由。
- —电子**email**邮件代理。
- —故障**ha**转移。
- -界面**idb**
- —入**ids**侵检测系统。
- —**ip**IP 堆栈。

- IP地**ipaa**—址分配
- **ipv6**-IPv6 堆栈
- **multicast**—-多播路由
- **nac**—网络准入控制。记录以下类型的事件：初始化、例外列表匹配、ACS 事务、无客户端身份验证、默认 ACL 应用和重新验证。
- —网**np**络处理器。
- —**object-group-search**对象组搜索
- —**ospf**OSPF路由。
- —基于**pbr**策略的路由
- —**rip**RIP路由。
- —资**rm**源管理器。
- **routing**- 所有路由
- —用**session**户会话。
- **sla**-SLA 对象跟踪
- —**snmp**SNMP。
- -系**sys**统。
- —**vpn**IKE 和 IPsec。
- —**vpnc**VPN 客户端。
- —**vpnfo**VPN 故障转移。
- —**vpnlb**VPN负载均衡。

有效的日志记录目的地如下：

- **asdm**- 要了解此目标，请参阅 **loggingasdm** 命令。
- **buffered**- 要了解此目标，请参阅 **loggingbuffered** 命令。
- **console**- 要了解此目标，请参阅 **loggingconsole** 命令。
- **history**- 要了解此目标，请参阅 **logginghistory** 命令。
- **mail**- 要了解此目标，请参阅 **loggingmail** 命令。
- **monitor**- 要了解此目标，请参阅 **loggingmonitor** 命令。
- **trap**- 要了解此目标，请参阅 **loggingtrap** 命令。

CR_Examples

以下示例指定，对于故障转移相关消息，ASDM日志缓冲区的最大严重性级别为2，系统日志缓冲区的最大严重性级别为 7：

```
ciscoasa(config)# logging class ha asdm 2 buffered 7
```

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging console

要使 ASA 能够在控制台会话中显示系统日志消息，请在全局配置模式下使用 **loggingconsole**命令。要禁用控制台会话中系统日志消息的 **no**显示，请使用此命令的形式。

loggingconsole [*logging_list* | *level*]
nologgingconsole

注释 我们建议您不要使用此命令，因为它可能会导致许多系统日志消息因缓冲区溢出而被丢弃。有关更多信息，请参阅“使用指南”部分。

Syntax Description

水平 设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为3，则ASA将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示：

- 或**0emergencies**— 系统不可用。
- 或**1alerts**——需要立即采取行动。
- 或**2critical**——危急情况。
- 或**3errors**——错误情况。
- 或**4warnings**——警告情况。
- 或**5notifications**——正常但重要的情况。
- **6** 或**informational**—信息性消息。
- 或**7debugging**——调试消息。

  注释
  由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与Cisco技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

logging_list 指定标识要发送到控制台会话的消息的列表。有关创建列表的信息，请参阅 **logginglist** 命令。

Command Default

默认情况下，ASA 不在控制台会话中显示系统日志消息。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

在将任何消息发送到控制台之前，必须使用 **loggingenable** 命令启用日志记录。

⚠

注意 使用 **loggingconsole** 命令可能会显着降低系统性能。而是使用 logging buffered 命令启动日志记录，并使用 show logging 命令查看消息。要查看最新消息，请使用 clear logging **buffer** 命令清除缓冲区。

CR_Examples

以下示例显示如何使严重性级别为 0、1、2 和 3 的系统日志消息显示在控制台会话中：

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

Related Commands

命令	说明
loggingenable	启用日志记录。
logginglist	创建可重复使用的消息选择标准列表。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging debug-trace

要将调试消息作为在严重性级别 7 发出的系统日志消息 711001 重定向到日志，请在全局配置模式下使用 **loggingdebug-trace** 命令。要停止将调试消息发送到日志，请使用此命令的 **no** 形式。

loggingdebug-trace
nologgingdebug-trace

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，ASA 不在系统日志消息中包括调试输出。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

调试消息生成为严重性级别为 7 的消息。它们显示在系统日志消息编号为 711001 的日志中，但不会显示在任何监控会话中。

CR_Examples

以下示例显示如何启用日志记录、将日志消息发送到系统日志缓冲区、将调试输出重定向到日志，以及打开磁盘活动调试。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging debug-trace
ciscoasa(config)# debug disk filesystem
```

以下是可能在日志中显示的调试消息的输出示例：

```
%ASA-7-711001: IFS: Read: fd 3, bytes 4096
```

Related Commands

命令	说明
loggingenable	启用日志记录。

命令	说明
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging debug-trace persistent

要启用特定会话中的调试系统日志活动（即使在会话结束后），请在全局配置模式下使用 **loggingdebug-tracepersistent** 命令。要禁用特定持久调试配置，请使用此命令的 **no** 形式。这将从本地会话和持久调试中将其清除。

loggingdebug-tracepersistent
nologgingdebug-tracepersistent

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，当会话结束时，在该特定会话中启用的所有调试命令在配置中不再存在，因此不再登录到系统日志服务器。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
9.5(2)	添加了此命令。

使用指南

在启用 logging debug-trace persistent 命令时，从任何会话输入的调试命令将全局保存，并对所有会话均可见。此命令将保存到运行配置中，并在系统重新启动时保存。

CR_Examples

以下示例显示如何启用日志记录，将日志消息发送到系统日志缓冲区，将调试输出重定向到日志，以及打开磁盘活动的持久调试。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging debug-trace persistent
ciscoasa(config)# debug disk filesystem
```

以下是可能在日志中显示的调试消息的输出示例：

```
%ASA-7-711001: IFS: Read: fd 3, bytes 4096
```

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging device-id

要将 ASA 配置为在非 EMBLEM 格式的系统日志消息中包含设备 ID，请在 **loggingdevice-id** 全局配置模式下使用该命令。要禁用设备 ID，请使用此命 **no**令的形式。

loggingdevice-id {**cluster-id** | **context-name** | **hostnameipaddress***interface_name* [**system**] | **string***text*}
no logging device-id

Syntax Description

cluster-id	将集群中单个 ASA 单元的唯一名称指定为设备 ID。
hostname	将 ASA 的主机名指定为设备 ID。
ipaddress*interface_name*	在 *interface_name*中指定接口的设备 ID 或 IP 地址。如果使用 ipaddress 关键字，则发送到外部服务器的系统日志消息包括指定接口的 IP 地址，而不考虑 ASA 使用哪个接口将日志数据发送到外部服务器。
string 文本、	指定作为设备 ID 的 文本 中包含的字符，长度最多可以为 16 个字符。不能使用空格字符或以下任何字符： • &—与号 • '—单引号 • "—双引号 • < - 小于号 • >—大于号 • ？ - 问号
system	（可选）在集群环境中，规定设备 ID 成为接口上的系统 IP 地址。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。

版本	修改
9.0(1)	已添加 **cluster-id**和关 **system**键字。

使用指南

如果使用 ipaddress 关键字，则设备 ID 将成为指定的 ASA 接口 IP 地址，无论消息从哪个接口发送。此关键字为从设备发送的所有消息提供单一、一致的设备 ID。如果使用 **system** 关键字，则指定的 ASA 将使用系统 IP 地址而不是集群中设备的本地 IP 地址。 **cluster-id** 和 **system** 关键字仅适用于 ASA 5580 和 5585-X。

CR_Examples

以下示例显示如何配置名为“secappl-1”的主机：

```
ciscoasa(config)# logging device-id hostname
ciscoasa(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

主机名显示在系统日志消息的开头，如以下消息所示：

```
secappl-1 %ASA-5-111008: User 'enable_15' executed the 'logging buffer-size 4096' command.
```

要删除设备 ID，请使用不带参数命令的 **no** 形式； **no** 形式不适用于参数。

```
ciscoasa(config)# show running-config logging
logging buffered informational
logging device-id hostname
firepower(config)# no logging device-id
ciscoasa(config)# show running-config logging
logging buffered informational
```

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging emblem

要对发送到系统日志服务器之外的目标的系统日志消息使用 EMBLEM 格式，请在全局配置模式下使用 **loggingemblem**命令。要禁用 EMBLEM 格式，请使用此命 **no**令的形式。

loggingemblem
nologgingemblem

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，ASA 不对系统日志消息使用 EMBLEM 格式。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	此命令已更改为独立于 **logginghost**命令。

使用指南

通过 **logging** 徽章命令，您可以为系统日志服务器以外的所有日志记录目标启用 EMBLEM 格式日志记录。如果还启用了 **loggingtimestamp** 关键字，则会发送带有时间戳的消息。

要为系统日志服务器启用 EMBLEM 格式日志记录，请将 **formatemblem** 选项与 **logginghost** 命令配合使用。

注释 徽章格式的时间戳字符串不包括年份。要在事件系统日志中显示年份，可以根据 RFC 5424 使用 **logging timestamp rfc5424** 命令启用时间戳。以下是 RFC 5424 格式的输出示例：

```
<166>2018-06-27T12：17：46Z asa：□ASA-6-110002：无法定位从源接口：源IP /源端口到目标IP /目标端口的协议出口接口
```

或者，您可以使用该 **logging device-id**命令。

CR_Examples

以下示例显示如何启用日志记录并使用 EMBLEM 格式以将日志记录发送到除系统日志服务器之外的所有日志记录目标：

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

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

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging enable

要为所有已配置的输出位置启用日志记录，请在全局配置模式下使用 **loggingenable** 命令。要禁用日志记录，请使用此命 **no**令的形式。

loggingenable
nologgingenable

Syntax Description

此命令没有任何参数或关键字。

Command Default

日志记录默认将禁用。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	此命令由该 **loggingon**命令改变而来。

使用指南

loggingenable 命令允许您启用或禁用将系统日志消息发送到任何受支持的日志记录目标。您可以使用 no logging enable 命令停止所有日志记录。

您可以使用以下命令启用到各个日志记录目标的日志记录：

- **loggingasdm**
- **loggingbuffered**
- **loggingconsole**
- **logginghistory**
- **loggingmail**
- **loggingmonitor**
- **loggingtrap**

CR_Examples

以下示例显示如何启用日志记录。 **showlogging** 命令的输出说明了必须如何单独启用每个可能的日志记录目标：

```
ciscoasa
(config)#
logging enable
ciscoasa
(config)#
show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

Related Commands

命令	说明
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging facility

要指定将消息发送到系统日志服务器的日志记录工具，请在全局配置模式下使用 **loggingfacility**命令。要将日志记录功能重置为默认值 20，请使用此命令的 **no**形式。

loggingfacility*facility*
nologgingfacility

Syntax Description

facility	指定日志记录设备；有效值为16到23。

Command Default

默认设备为 20 (LOCAL4)。

Command Modes

下表显示可输入 命令的模式，“语法说明”部分注明了例外情况。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

系统日志服务器根据消息中的设备编号生成文件消息。有八个可能的设施：16 (LOCAL0) 至 23 (LOCAL7)。

CR_Examples

以下示例显示如何指定 ASA 在系统日志消息中将日志记录设备指示为 16。 **showlogging** 命令的输出包括 ASA 正在使用的工具：

```
ciscoasa(config)# logging facility 16
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
```

Related Commands

命令	说明
loggingenable	启用日志记录。
logginghost	定义系统日志服务器。
loggingtrap	启用到系统日志服务器的日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging flash-bufferwrap

要使ASA可在每次日志缓冲区填满从未保存的消息时将日志缓冲区写入闪存，请在全局配置模式下使用 **loggingflash-bufferwrap**命令。要禁止将日志缓冲区写入闪存，请使用此命令的 **no**形式。

loggingflash-bufferwrap
nologgingflash-bufferwrap

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认值如下：

- 日志记录到缓冲区已禁用。
- 将日志缓冲区写入闪存已禁用。
- 缓冲区大小为 4 KB。
- 最低可用闪存为 3 MB。
- 为缓冲区日志记录分配的最大闪存为 1 MB。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

为了使ASA将日志缓冲区写入闪存，您必须启用日志记录到缓冲区；否则，日志缓冲区永远不会有数据写入闪存。您可以使用 **logging buffered** 命令，启用缓冲区的日志记录。但是，如果配置的日志记录缓冲区大小超过 2 MB，则内部日志缓冲区不会写入闪存。

在 ASA 将日志缓冲区内容写入闪存时，ASA 会继续将新的事件消息存储到日志缓冲区。

ASA 将创建其名称使用默认时间戳格式的日志文件，如下所示：

```
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）。

闪存的可用性会影响 ASA 使用 **loggingflash-bufferwrap** 命令保存系统日志消息的方式。有关详细信息，请参阅 **loggingflash-maximum-allocation**和 **loggingflash-minimum-free**命令。

CR_Examples

以下示例显示如何启用日志记录、启用日志缓冲区，以及使ASA可将日志缓冲区写入闪存：

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

Related Commands

命令	说明
clearloggingbuffer	清除包含的所有系统日志消息的日志缓冲区。
copy	将文件从一个位置复制到另一个位置，包括复制到TFTP或FTP服务器。
delete	从磁盘分区删除文件（如已保存的日志文件）。
loggingbuffered	启用将日志记录记录到日志缓冲区。
loggingbuffer-size	指定日志缓冲区大小。

logging flash-maximum-allocation

要指定 ASA 用于存储日志数据的最大闪存量，请在全局配置模式下使用 **loggingflash-maximum-allocation**命令。要将用于此目的的最大闪存量重置为其默认的 1 MB 闪存大小，请使用此命令的 **no** 形式。

loggingflash-maximum-allocation千字节
nologgingflash-maximum-allocation千字节

Syntax Description

千字节	ASA 可用于保存日志缓冲区数据的最大闪存量（以千字节为单位）。

Command Default

为日志数据分配的最大闪存默认为 1 MB。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

该命令确定有多少闪存可用于 **loggingsavelog** 和 **loggingflash-bufferwrap** 命令。

如果要由 **loggingsavelog** 或 **loggingflash-bufferwrap** 保存的日志文件导致日志文件的闪存使用量超过 **loggingflash-maximum-allocation** 命令指定的最大数量，则 ASA 将删除最早的日志文件，以便为新的日志文件释放足够的内存。如果没有要删除的文件，或者在删除所有旧文件后，可用内存对于新日志文件来说太小，则 ASA 无法保存新日志文件。

要查看 ASA 分配的最大闪存大小是否与默认大小不同，请使用 **showrunning-configlogging** 命令。如果未显示 **loggingflash-maximum-allocation** 命令，则 ASA 最多为已保存的日志缓冲区数据使用 1 MB 的空间。分配的内存同时用于 **loggingsavelog** 和 **loggingflash-bufferwrap** 命令。

有关 ASA 如何使用日志缓冲区的更多信息，请参阅 **loggingbuffered** 命令。

CR_Examples

以下示例显示如何启用日志记录、启用日志缓冲区、使 ASA 能够将日志缓冲区写入闪存，其中用于写入日志文件的最大闪存量设置为大约 1.2 MB 内存：

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

Related Commands

命令	说明
clearloggingbuffer	清除日志缓冲区中包含的所有系统日志消息。
loggingbuffered	启用将日志记录记录到日志缓冲区。
loggingenable	启用日志记录。
loggingflash-bufferwrap	当日志缓冲区已满时，将日志缓冲区写入到闪存。
loggingflash-minimum-free	指定必须可供ASA使用的最小闪存量，以允许将日志缓冲区写入闪存。

logging flash-minimum-free

要指定 ASA 保存新日志文件之前必须存在的最小可用闪存量，请在全局配置模式下使用 **loggingflash-minimum-free** 命令。要将所需的最小可用闪存量重置为其默认大小 3 MB，请使用此命令的 **no** 形式。

loggingflash-minimum-free千字节
nologgingflash-minimum-free千字节

Syntax Description

千字节	在ASA保存新的日志文件之前必须可用的最小闪存量（以千字节为单位）。

Command Default

默认的最小可用闪存为 3 MB。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

logging flash-minimum-free 命令指定 **loggingsavelog** 和 **loggingflash-bufferwrap** 命令始终必须保留的闪存量。

如果要保存的日志文 **loggingsavelog**件 **loggingflash-bufferwrap**会导致可用闪存量低于命令指定的限 **loggingflash-minimum-free**制，则 ASA 会删除最旧的日志文件，以确保在保存新日志文件后仍有足够的可用内存。如果没有要删除的文件，或者在删除所有旧文件后，可用内存仍然低于限制，则 ASA 将无法保存新的日志文件。

CR_Examples

以下示例显示如何启用日志记录、启用日志缓冲区、启用 ASA 以将日志缓冲区写入闪存，并指定可用闪存的最小值为 4000 KB：

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

Related Commands

命令	说明
clearloggingbuffer	清除包含的所有系统日志消息的日志缓冲区。
loggingbuffered	启用将日志记录记录到日志缓冲区。
loggingenable	启用日志记录。
loggingflash-bufferwrap	当日志缓冲区已满时，将日志缓冲区写入到闪存。
loggingflash-maximum-allocation	指定可用于写入日志缓冲区内容的最大闪存量。

logging flow-export-syslogs

要启用或禁用NetFlow捕获的所有系统日志消息，请在全局配置模式下使用**loggingflow-export-syslogs**命令。

loggingflow-export-syslogs { **enable** | **disable** }

Syntax Description

enable	启用Netflow捕获的所有系统日志消息。
disable	禁用Netflow捕获的所有系统日志消息。

Command Default

默认情况下，NetFlow 捕获的所有系统日志均已启用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
8.1(1)	添加了此命令。

使用指南

如果安全设备配置为导出 NetFlow 数据，为提高性能，我们建议您通过输入**loggingflow-export-syslogsdisable** 命令禁用冗余系统日志消息（NetFlow 也捕获的日志消息）。将禁用的系统日志消息如下：

系统日志消息	说明
106015	TCP 流被拒绝，因为第一个数据包不是 SYN 数据包。
106023	被通过命令附加到接口的入口 ACL 或出口 ACL 拒绝的 **access-group**流。
106100	ACL 允许或拒绝的流。
302013 and 302014	TCP 连接和删除。
302015 and 302016	UDP 连接和删除。
302017 and 302018	GRE 连接和删除。
302020 and 302021	ICMP 连接和删除。

系统日志消息	说明
313001	发送至安全设备的 ICMP 数据包被拒绝。
313008	发送至安全设备的 ICMPv6 数据包被拒绝。
710003	尝试连接安全设备被拒绝。

注释 虽然这是一个配置模式命令，但它并不存储在配置中。只有 **nologgingmessagexxxxxx**命令存储在配置中。

CR_Examples

以下示例显示如何禁用 NetFlow 捕获的冗余系统日志消息以及显示的样本输出：

```
ciscoasa(config)# logging flow-export-syslogs disable
ciscoasa(config)# show running-config logging
no logging message xxxxx1
no logging message xxxxx2
```

其中 *xxxxx1* 和 *xxxxx2* 是系统日志消息，由于已通过 NetFlow 捕获相同的信息，因此这些消息是冗余的。此命令类似于命令别名，并将转换为一批无日志记录消息 xxxxxx 命令。在禁用系统日志消息后，可以使用**loggingmessagexxxxxx**命令单独启用它们，其中 *xxxxxx* 是特定系统日志消息编号。

Related Commands

命令	说明
flow-exportdestination	指定 NetFlow 收集器的 IP 地址或主机名，以及 NetFlow 收集器侦听的 UDP 端口。
flow-exporttemplatetimeout-rate	控制将模板信息发送到 NetFlow 收集器的间隔。
showflow-exportcounters	显示一组 NetFlow 运行时计数器。

logging from-address

要指定ASA发送的系统日志消息的发件人邮件地址，请在全局配置模式下使用**loggingfrom-address**命令。所有已发送的系统日志消息都似乎来自您指定的地址。要删除发件人电子邮件地址，请使用此命令的 **no**形式。

loggingfrom-address发件人电子邮件地址
no loggingfrom-address发件人电子邮件地址

Syntax Description

发件人电子邮件地址	源邮件地址，即系统日志消息显示为来自的邮件地址（例如，cdb@example.com）。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

使用 **loggingmail** 命令启用通过邮件发送系统日志消息。

使用此命令指定的地址无需对应于现有的邮件帐户。

CR_Examples

要启用日志记录并将 ASA 设置为通过邮件发送系统日志消息，请使用以下条件：

- 发送重要、警报或紧急消息。
- 使用 ciscosecurityappliance@example.com 作为发件人地址发送邮件。
- 将邮件发送到 admin@example.com。
- 使用 SMTP、主要服务器 pri-smtp-host 和辅助服务器 sec-smtp-host 发送邮件。

输入以下命令：

```
ciscoasa
```

```
(config)#
logging enable
ciscoasa
(config)#
logging mail critical
ciscoasa
(config)#
logging from-address ciscosecurityappliance@example.com
ciscoasa
(config)#
logging recipient-address admin@example.com
ciscoasa
(config)#
smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

命令	说明
loggingenable	启用日志记录。
loggingmail	启用 ASA 通过邮件发送系统日志消息，并确定通过邮件发送系统日志消息。
loggingrecipient-address	指定系统日志消息的发送目标邮件地址。
smtp-server	配置 SMTP 服务器。
showlogging	显示已启用的日志记录选项。

logging ftp-bufferwrap

要使 ASA 能够在每次缓冲区填满从未保存的消息时，将缓冲区中已满的从未保存的消息发送到 FTP 服务器，请在全局配置模式下使用 **loggingftp-bufferwrap**命令。要禁止将日志缓冲区发送到 FTP 服务器，请使用此命令的 **no**形式。

loggingftp-bufferwrap
no loggingftp-bufferwrap

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认值如下：

- 日志记录到缓冲区已禁用。
- 已禁用将日志缓冲区发送到 FTP 服务器。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

当启用 **loggingftp-bufferwrap**时，ASA 将日志缓冲区数据发送到您使用 **loggingftp-server** 命令指定的 FTP 服务器。在 ASA 向 FTP 服务器发送日志数据的同时，它会继续将所有新的事件消息存储到日志缓冲区。

为了使 ASA 能够将日志缓冲区内容发送到 FTP 服务器，您必须启用日志记录到缓冲区；否则，日志缓冲区永远不会有数据写入闪存。要启用缓冲区记录功能，请使用该 **loggingbuffered**命令。

ASA 将创建其名称使用默认时间戳格式的日志文件，如下所示：

```
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）。

CR_Examples

以下示例显示如何启用日志记录、启用日志缓冲区、指定 FTP 服务器以及使 ASA 可将日志缓冲区写入 FTP 服务器。此示例指定主机名为 logserver-352 的 FTP 服务器。可以使用用户名 logovernor 和密码 1luvMy10gs 访问该服务器。日志文件将存储在 /syslogs 目录中：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
ciscoasa(config)# logging ftp-bufferwrap
ciscoasa(config)#
```

Related Commands

命令	说明
clearloggingbuffer	清除包含的所有系统日志消息的日志缓冲区。
loggingbuffered	启用将日志记录记录到日志缓冲区。
loggingbuffer-size	指定日志缓冲区大小。
loggingenable	启用日志记录。
loggingftp-server	指定与 **loggingftp-bufferwrap** 命令配合使用的 FTP 服务器参数。

logging ftp-server

要指定启用 **loggingftp-bufferwrap** 时 ASA 向其发送日志缓冲区数据的 FTP 服务器的详细信息，请在全局配置模式下使用 **loggingftp-server** 命令。要删除有关 FTP 服务器的所有详细信息，请使用此命令的 **no** 形式。

loggingftp-server*ftp_serverpathusername* [*0* | *8*] *password*
no loggingftp-server*ftp_serverpathusername* [*0* | *8*] *password*

Syntax Description

0	（可选）指定将遵循未加密的（明文）用户密码。
8	（可选）指定将遵循加密的用户密码。
ftp-server	外部 FTP 服务器 IP 地址或主机名。 注释 如果指定主机名，请确保 DNS 在您的网络上正常运行。
password	指定用户名的密码，最长可以包含 64 个字符。
path	FTP 服务器上保存日志缓冲区数据的目录路径。此路径相对于 FTP 根目录。例如： `/security_appliances/syslogs/appliance107`
username	有效的登录 FTP 服务器的用户名。

Command Default

默认情况下，没有指定 FTP 服务器。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.3(1)	增加了对密码加密的支持。

使用指南

只能指定一个 FTP 服务器。如果已指定日志记录 FTP 服务器，使用 **loggingftp-server** 命令会将 FTP 服务器配置替换为您输入的新配置。

ASA 不会验证您指定的 FTP 服务器信息。如果任何详细信息配置错误，ASA 将无法将日志缓冲区数据发送到 FTP 服务器。

在 ASA 启动或升级期间，不支持单位数密码以及以数字开头后跟空格的密码。例如，0 为通过，1 为无效密码。

CR_Examples

以下示例显示如何启用日志记录、启用日志缓冲区、指定 FTP 服务器以及使 ASA 可将日志缓冲区写入 FTP 服务器。此示例指定主机名为 logserver 的 FTP 服务器。可使用用户名 user1 和密码 pass1 访问服务器。日志文件将存储在 /path1 目录中：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging ftp-server logserver /path1 user1 pass1
ciscoasa(config)# logging ftp-bufferwrap
```

以下示例显示如何输入加密的密码：

```
ciscoasa(config)# logging ftp-server logserver /path1 user1 8 JPAGWzIIFVlheXv2I9nglfytOzHU
```

以下示例显示如何输入未加密（明文）密码：

```
ciscoasa(config)# logging ftp-server logserver /path1 user1 0 pass1
```

Related Commands

命令	说明
clearloggingbuffer	清除包含的所有系统日志消息的日志缓冲区。
loggingbuffered	启用将日志记录记录到日志缓冲区。
loggingbuffer-size	指定日志缓冲区大小。
loggingenable	启用日志记录。
loggingftp-bufferwrap	当日志缓冲区已满时，将日志缓冲区发送到FTP服务器。

logging hide username

当用户名的有效性未知时，要在系统日志中隐藏用户名（例如，“*****”），请在全局配置模式下使用 **logginghideusername**命令。要查看这些用户名，请使用此命令的 **no** 形式。

logginghideusername
no logginghideusername

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认为隐藏用户名。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.3(3)	添加了此命令。

使用指南

logginghideusername命令允许您在系统日志中隐藏用户名，直到它们被验证为有效为止。

注释 此命令在版本 9.4(1) 中不可用。

CR_Examples

以下示例显示如何在系统日志中隐藏用户名，直到这些用户名被验证为有效：

```
ciscoasa(config)# logging hide username
ciscoasa# show logging
Syslog logging: enabled
...
Hide Username logging: enabled | disabled
...
```

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。

命令	说明
showrunning-configlogging	显示运行配置的日志相关部分。

logging history

要启用 SNMP 日志记录并指定要发送到 SNMP 服务器的消息，请在 **logging history** 全局配置模式下使用该命令。要禁用 SNMP 日志记录，请使用此命 **no**令的形式。

logginghistory [**rate-limit***number interval***level***level* | *logging_list* | *level*]
no logging history

Syntax Description

interval	指定日志记录间隔（以秒为单位）（在 **rate-limit**下），从而限制将日志转发到 SNMP 的速率。如果设置 **logging rate-limit** 命令，则该命令优先于本设置。
level	指定历史速率限制的日志记录级别。转发到SNMP的消息仅限于指定的系统日志级别。
水平	设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为3，则ASA将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示： • 或**0emergencies**— 系统不可用。 • 或**1alerts**——需要立即采取行动。 • 或**2critical**——危急情况。 • 或**3errors**——错误情况。 • 或**4warnings**——警告情况。 • 或**5notifications**——正常但重要的情况。 • **6**或**informational**—信息性消息。 • 或**7debugging**——调试消息。 注释 由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与Cisco技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。
logging_list	指定标识要发送到SNMP服务器的消息的列表。有关创建列表的信息，请参阅**logginglist**命令。
number	当使用 **rate-limit**时，请指定要在该 间隔 期间记录的消息 数 。
rate-limit	限制转发到 SNMP 的日志。指定 **rate-limit**（秒）以记录系统日志。

Command Default

默认情况下，ASA 不记录到 SNMP 服务器。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.20(1)	添加了 **rate-limit** 关键字，以对发送到SNMP的日志进行速率限制。

使用指南

logginghistory 命令允许您启用到 SNMP 服务器的日志记录，并设置 SNMP 消息级别或事件列表。

CR_Examples

以下示例显示如何启用 SNMP 日志记录并指定将严重性级别为 0、1、2 和 3 的消息发送到配置的 SNMP 服务器：

```
ciscoasa(config)# logging enable
ciscoasa(config)# snmp-server host infrastructure 10.2.3.7 trap community gam327
ciscoasa(config)# snmp-server enable traps syslog
ciscoasa(config)# logging history errors
ciscoasa(config)#
```

CR_Examples

以下示例将发送到 SNMP 的关键系统日志速率限制为 15 条消息/15 秒。

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

使用 **no logging history** 命令以缓解设备的内存泄漏。此命令不会影响到系统日志服务器的常规日志记录。

Related Commands

命令	说明
loggingenable	启用日志记录。
logginglist	创建可重复使用的消息选择标准列表。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。
snmp-server	指定 SNMP 服务器的详细信息。

logging host

要定义系统日志服务器，请在全局配置模式下使用 **logging host**命令。要删除 syslog 服务器定义，请使用此命 **no**令的形式。

logging host*interface_namesyslog_ip* [**tcp** [*/ port*] | **udp** [*/ port*]] [**format emblem** | **timestamp** [**legacy** | **rfc5424**]] [**secure** [**reference-identity***reference_identity_name*]]
no logging host*interface_namesyslog_ip* [**tcp** [*/ port*] | **udp** [*/ port*]] [**format emblem** | **timestamp** [**legacy** | **rfc5424**]] [**secure** [**reference-identity***reference_identity_name*]]

Syntax Description

format emblem	（可选）为系统日志服务器启用 EMBLEM 格式日志记录。EMBLEM 格式日志记录仅适用于 UDP 系统日志消息。
interface_name	指定系统日志服务器所在的接口。
port	指示 syslog 服务器侦听消息的端口。对于任一协议，有效的端口值都是 1025 – 65535。如果输入零作为端口号或使用无效字符或符号，将会发生错误。
secure	（可选）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。 注释 只能与支持 SSL/TLS 的系统日志服务器建立安全日志记录连接。如果无法建立 SSL/TLS 连接，所有新连接都将被拒绝。您可以输入 **loggingpermit-hostdown** 命令来更改此默认行为。
syslog_ip	指定系统日志服务器的 IP 地址（IPv4 或 IPv6）。
tcp	指定 ASA 应使用 TCP 向系统日志服务器发送消息。
udp	指定 ASA 应使用 UDP 向系统日志服务器发送消息。
reference_identity_name	指定引用标识对象的名称，该对象启用 RFC 6125 引用标识检查以提高安全性。根据此先前配置的引用身份对象对收到的服务器证书进行身份检查
timestamp [**legacy** | **rfc5424**]	（可选）启用时间戳格式，可以指定为传统格式或 RFC5424 格式（yyyy-MM-THH:mm:ssZ，其中字母 Z 表示 UTC 时区）。

Command Default

默认协议为 UDP。

formatemblem 选项的默认设置为 false。

secure 选项的默认设置为 false。

默认端口号如下：

- UDP—514

- TCP -1470

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0	添加了此命令。
8.0(2)	添加了 **secure** 关键字。
8.4(1)	可以启用和禁用连接阻止。
9.6.2	增加了 **reference-identity** 选项。
9.7(1)	现在，可以将IPv6地址用于系统日志服务器。如果您有直接连接的系统日志服务器，可以使用 ASA 和系统日志服务器上的 /31 子网创建点对点连接。

使用指南

logginghost*syslog_ip* format徽章命令允许您为每个系统日志服务器启用 EMBLEM 格式日志记录。EMBLEM 格式日志记录仅适用于 UDP 系统日志消息。如果为特定系统日志服务器启用 EMBLEM 格式日志记录，则消息会发送到该服务器。如果使用 **loggingtimestamp** 命令，则带有时间戳的消息也会发送。

您可以使用多个日志主机命令来指定所有接收系统日志消息的附加服务器。但是，只能指定服务器来接收 UDP 或 TCP 系统日志消息，而不是同时接收两者。

如果服务器证书中显示的身份与配置的身份不匹配**reference-identity**，则不会建立连接并记录错误。

当 已将 **logginghost** 命令配置为使用 TCP 向系统日志服务器发送消息时，连接阻止的默认设置为打开。如果配置了基于 TCP 的系统日志服务器，则可以使用 **loggingpermit-hostdown** 命令禁用连接阻止。

注释 在**logginghost**命令中使用 **tcp** 选项时，如果无法访问系统日志服务器，ASA 将丢弃穿过防火墙的连接。

您可以仅显示之前输入的 端口 和 协议 值，方法是使用 **showrunning-configlogging** 命令并在列表中查找该命令 - TCP 会列出为 6，UDP 会列出为 17。TCP 端口仅适用于系统日志服务器。该 端口 必须与系统日志服务器侦听的端口相同。

注释 如果尝试将 **logginghost** 命令和 **secure** 关键字与 UDP 配合使用，则会出现错误消息。

不支持在备用 ASA 上通过 TCP 发送系统日志。

在 9.18.2.4 版中，允许使用路由查找转发系统日志流量。这使得流量能够被转发，而不管日志主机 interface_name **ip_address 配置中指** 定的接口是什么。但是，在 9.18.3.60 及更高版本中，9.18.2.4 中引入的更改已被删除。因此，日志主机接口 **名称 ip_address** 中指定的配置优先于路由查找，并且系统日志流量从指定的接口转发。

CR_Examples

以下示例显示如何将严重性级别为 0、1、2 和 3 的系统日志消息发送到使用默认协议和端口号的内部接口上的系统日志服务器：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 10.2.2.3
ciscoasa(config)# logging trap errors
ciscoasa(config)#
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 2001:192:168:88::111
ciscoasa(config)# logging trap errors
ciscoasa(config)#
```

Related Commands

命令	说明
loggingenable	启用日志记录。
loggingtrap	启用到系统日志服务器的日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging list

要创建日志记录列表以便在其他命令中使用，以根据各种标准（日志记录级别、事件类别和消息ID）指定消息，请在 **logginglist** 全局配置模式下使用该命令。要删除列表，请使用此命 **no**令的形式。

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

Syntax Description

class*event_class*	（可选）设置系统日志消息的事件类别。对于指定的级别， 命令仅标识指定类的系统日志消息。请参阅“使用指南”部分以获取类别列表。
level级别	设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为 3，则 ASA 将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示： • 或**0emergencies**— 系统不可用。 • 或**1alerts**——需要立即采取行动。 • 或**2critical**——危急情况。 • 或**3errors**——错误情况。 • 或**4warnings**——警告情况。 • 或**5notifications**——正常但重要的情况。 • **6**或**informational**—信息性消息。 • 或**7debugging**——调试消息。 注释 由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此， 请 仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。
message*start_id* [*-end_id*]	已指定消息 ID 或 ID 范围。要查找消息的默认级别，请使用 **showlogging** 命令或参阅系统日志消息指南。
name	设置日志记录列表名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

可以使用列表的日志记录命令如下：

- **loggingasdm**
- **loggingbuffered**
- **loggingconsole**
- **logginghistory**
- **loggingmail**
- **loggingmonitor**
- **loggingtrap**

event_class 可能的值包括：

- —用**auth**户身份验证。
- —**bridge**透明防火墙。
- —**ca**PKI 证书颁发机构。
- —**config**命令界面。
- —**eap**可扩展身份验证协议 (EAP)。记录以下类型的事件以支持网络准入控制：EAP 会话状态更改、EAP 状态查询事件以及 EAP 报头和数据包内容的十六进制转储。
- —**eapoudp**UDP 上的可扩展身份验证协议 (EAP)。记录 EAPoUDP 事件以支持网络准入控制，并生成 EAPoUDP 报头和数据包内容的完整记录。
- —电子**email**邮件代理。
- —故障**ha**转移。
- —入**ids**侵检测系统。
- —**ip**IP 堆栈。

- —网**nac**络准入控制。记录以下类型的事件：初始化、例外列表匹配、ACS 事务、无客户端身份验证、默认 ACL 应用和重新验证。
- —网**np**络处理器。
- —**ospf**OSPF路由。
- —**rip**RIP路由。
- —用**session**户会话。
- —**snmp**SNMP。
- -系**sys**统。
- —**vpn**IKE 和 IPSec。
- —**vpnc**VPN 客户端。
- —**vpnfo**VPN 故障转移。
- —**vpnlb**VPN负载均衡。

CR_Examples

以下示例显示如何使用 logging list 命令：

```
ciscoasa(config)# logging list my-list 100100-100110
ciscoasa(config)# logging list my-list level critical
ciscoasa(config)# logging list my-list level warning class vpn
ciscoasa(config)# logging buffered my-list
```

前面的示例说明匹配指定条件的系统日志消息将被发送到日志记录缓冲区。此示例中指定的条件为：

- Syslog 消息 ID 在 100100 到 100110 范围内
- 所有具有严重或更高级别（紧急、警报或严重）的系统日志消息
- 所有具有警告级别或更高级别（紧急、警报、严重、错误或警告）的 VPN 类系统日志消息

如果系统日志消息满足其中任何一个条件，它就会被记录到缓冲区。

注释 在设计列表条件时，条件可以指定重叠的消息集。通常会记录与多组条件匹配的系统日志消息。

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。

命令	说明
showrunning-configlogging	显示运行配置的日志相关部分。

logging mail

要使ASA能够通过邮件发送系统日志消息以及确定通过邮件发送的消息，请在全局配置模式下使用**loggingmail**命令。要禁用系统日志消息的电子邮件发送，请使用此命令的 **no**形式。

loggingmail [*logging_list* | *level*]
no loggingmail [*logging_list* | *level*]

Syntax Description

水平　设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为3，则ASA将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示：

- 或**0emergencies**— 系统不可用。
- 或**1alerts**——需要立即采取行动。
- 或**2critical**——危急情况。
- 或**3errors**——错误情况。
- 或**4warnings**——警告情况。
- 或**5notifications**——正常但重要的情况。
- **6**或**informational**—信息性消息。
- 或**7debugging**——调试消息。

注释
由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与Cisco技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

logging_list　指定标识要发送给邮件收件人的邮件的列表。有关创建列表的信息，请参阅 **logginglist** 命令。

Command Default

默认情况下，电子邮件记录功能是禁用的。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

通过邮件发送的系统日志消息显示在所发送邮件的主题行中。

CR_Examples

要将 ASA 设置为通过邮件发送系统日志消息，请使用以下条件：

- 发送重要、警报或紧急消息。
- 使用 ciscosecurityappliance@example.com 作为发件人地址发送邮件。
- 将邮件发送到 admin@example.com。
- 使用 SMTP、主要服务器 pri-smtp-host 和辅助服务器 sec-smtp-host 发送邮件。

输入以下命令：

```
ciscoasa
(config)#
logging mail critical
ciscoasa
(config)#
logging from-address ciscosecurityappliance@example.com
ciscoasa
(config)#
logging recipient-address admin@example.com
ciscoasa
(config)#
smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

命令	说明
loggingenable	启用日志记录。
loggingfrom-address	指定邮件系统日志消息似乎来自的邮件地址。
logginglist	创建可重复使用的消息选择标准列表。
loggingrecipient-address	指定邮件系统日志消息的发送目标邮件地址。
smtp-server	配置 SMTP 服务器。

logging message

要启用系统日志消息的日志记录，或更改消息级别，请在全局配置模式下使用**loggingmessage**命令。要禁用消息日志记录或将其设置为默认级别，请使用此命令的 **no** 形式。

loggingmessage*syslog_id* [**level***level* | **standby**]
no loggingmessage*syslog_id* [**level***level* | **standby**]

Syntax Description

level级别 （可选）设置指定系统日志消息的严重性级别。您可以指定编号或名称，如下所示：

- 或**0emergencies**— 系统不可用。
- 或**1alerts**——需要立即采取行动。
- 或**2critical**——危急情况。
- 或**3errors**——错误情况。
- 或**4warnings**——警告情况。
- 或**5notifications**——正常但重要的情况。
- **6**或**informational**—信息性消息。
- 或**7debugging**——调试消息。

注释
由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此， **请** 仅将调试用于解决特定问题或在与Cisco技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

要查找消息的默认级别，请使用 **showlogging** 命令或参阅系统日志消息指南。

syslog_id 您希望启用或禁用或希望修改其严重性级别的系统日志消息的 ID。

standby （可选）带 **no**] 关键字指定命令的 **standby**] 形式，可阻止在备用设备上生成特定系统日志消息。

Command Default

默认情况下，系统会启用所有系统日志消息，并将所有消息的严重性级别设置为其默认级别。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。
9.4(1)	添加了 **standby** 关键字。

使用指南

您可以将 **loggingmessage** 命令用于以下目的：

- 指定消息是否启用或禁用。
- 在备用设备上禁用生成系统日志消息。
- 设置消息的严重性级别。

您可以使用 **showlogging**命令来确定当前分配给消息的级别以及是否已启用该消息。

要防止 ASA 生成特定系统日志消息，请在全局配置模式下使用 **loggingmessage** 命令的 **no** 形式（不带 **level** 关键字）。要让 ASA 生成特定系统日志消息，请使用 **loggingmessage** 命令（不带 **level** 关键字）。您可以并行使用这两个版本的 **loggingmessage** 命令。

CR_Examples

以下示例中的一系列命令显示了如何使用 **loggingmessage** 命令指定是否已启用消息以及消息的严重性级别：

```
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)
ciscoasa(config)# no logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)
ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)
ciscoasa(config)# no logging message 403503 standby
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled),standby logging (disabled)
ciscoasa(config)# no logging message 403503 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

Related Commands

命令	说明
clearconfigurelogging	清除所有日志记录配置或仅清除消息配置。
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging message standby

要解除阻止备用单元上之前阻止生成的特定系统日志消息，请在**loggingmessagestandby**全局配置模式下使用该命令。要阻止在备用单元上生成特定的系统日志消息，请使用此命令的 **no**形式。

loggingmessage*syslog_id***standby**
no loggingmessage*syslog_id***standby**

Syntax Description

syslog_id	要在备用设备上启用或禁用的系统日志消息的ID。

Command Default

默认情况下，所有系统日志消息都在备用设备上生成（仅当启用 logging standby 命令时）。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
9.4(1)	添加了此命令。

使用指南

您可以使用 **[no]loggingmessage***syslog_id***standby** 命令指定在备用设备上是启用还是禁用系统日志消息。

您可以使用 **showlogging**命令确定是否已启用系统日志消息。

CR_Examples

以下示例中的命令系列显示如何使用 **loggingmessage***syslog_id***standby** 命令指定是否已在备用设备上启用系统日志消息：

```
ciscoasa(config)# no logging message 403503 standby
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled), standby logging disabled
```

Related Commands

命令	说明
clearconfigurelogging	清除所有日志记录配置或仅系统日志消息配置。
loggingenable	启用日志记录。
showrunning-configlogging	显示运行配置的日志相关部分。

logging monitor

要使 ASA 显示 SSH 和 Telnet 会话中的系统日志消息，请在全局配置模式下使用 **loggingmonitor**命令。要禁用 SSH 和 Telnet 会话中的系统日志消息显示，请使用此命令的 **no**形式。

loggingmonitor [*logging_list* | *level*]
nologgingmonitor

Syntax Description

水平　设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为3，则ASA将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示：

- 或**0emergencies**— 系统不可用。
- 或**1alerts**——需要立即采取行动。
- 或**2critical**——危急情况。
- 或**3errors**——错误情况。
- 或**4warnings**——警告情况。
- 或**5notifications**——正常但重要的情况。
- **6**或**informational**—信息性消息。
- 或**7debugging**——调试消息。

注释
由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与Cisco技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

logging_list　指定标识要发送到 SSH 或 Telnet 会话的消息的列表。有关创建列表的信息，请参阅**logginglist**命令。

Command Default

默认情况下，ASA 不在 SSH 和 Telnet 会话中显示系统日志消息。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

loggingmonitor 命令为当前情景中的所有会话启用系统日志消息；在每个会话中， **terminal** 命令可以控制系统日志消息是否显示在该会话中。

CR_Examples

以下示例显示如何在控制台会话中启用系统日志消息的显示。使用 **errors** 关键字表示严重性级别为 0、1、2 和 3 的消息应显示在 SSH 和 Telnet 会话中。 **terminal** 命令使该消息显示在当前会话中：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging monitor errors
ciscoasa(config)# terminal monitor
ciscoasa(config)#
```

Related Commands

命令	说明
loggingenable	启用日志记录。
logginglist	创建可重复使用的消息选择标准列表。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。
terminal	设置终端线路参数。

logging permit-hostdown

要使基于 TCP 的系统日志服务器的状态与新用户会话无关，请在全局配置模式下使用 **loggingpermit-hostdown**命令。要使 ASA 在基于 TCP 的系统日志服务器不可用时拒绝新用户会话，请使用此命令的 **no** 形式。

loggingpermit-hostdown
nologgingpermit-hostdown

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，如果您已启用到使用 TCP 连接的系统日志服务器的日志记录，则当系统日志服务器因任何原因不可用时，ASA 不允许新的网络访问会话。 **loggingpermit-hostdown** 命令的默认设置为 false。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

如果使用 TCP 作为日志记录传输协议用于将消息发送到系统日志服务器，并且在 ASA 无法访问系统日志服务器时，ASA 将拒绝新的网络访问会话，作为一项安全措施。您可以使用 **loggingpermit-hostdown** 命令删除此限制。

CR_Examples

以下示例使基于 TCP 的系统日志服务器的状态与 ASA 是否允许新会话无关。当 **loggingpermit-hostdown**命令在其输出中包括 **showrunning-configlogging** 命令时，基于 TCP 的系统日志服务器的状态与新的网络访问会话无关。

```
ciscoasa(config)# logging permit-hostdown
ciscoasa(config)# show running-config logging
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
ciscoasa(config)#
```

Related Commands

命令	说明
loggingenable	启用日志记录。
logginghost	定义系统日志服务器。
loggingtrap	启用到系统日志服务器的日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging queue

如要指定ASA在根据日志记录配置进行处理之前可在其队列中保留的系统日志消息数，请在全局配置模式下使用 **loggingqueue**命令。要将日志记录队列大小重置为默认值 512 条消息，请使用此命令的 **no** 形式。

loggingqueue*queue_size*
nologgingqueue*queue_size*

Syntax Description

queue_size	在处理系统日志消息之前，用于存储系统日志消息的队列中允许的系统日志消息数量。有效值为 0 到 8192 条消息，具体取决于平台类型。如果日志队列设置为零，则队列将是最大可配置大小（8192 条消息），具体取决于平台。在 ASA-5505 上，最大队列大小为 1024。在 ASA-5510 上，此值为 2048；在所有其他平台上，此值为 8192。

Command Default

默认队列大小为 512 条消息。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

当流量太大以致于队列已满时，ASA 可能会丢弃消息。在 ASA 5505 上，最大队列大小为 1024。在 ASA-5510 上为 2048。在所有其他平台上，它是 8192。

⚠

注意 在低端平台上增加日志记录队列大小可能会减少其他功能（例如 ASDM、WebVPN、DHCP 服务器等）的可用 DMA 内存量。如果系统耗尽 DMA 内存，这些功能会停止运行。使用 **showmemorydetail** 命令检查 MEMPOOL_DMA 池中的可用 DMA 内存量。

CR_Examples

以下示例显示如何显示 logging queue 和 show logging queue 命令的输出：

```
ciscoasa(config)# logging queue 0
ciscoasa(config)# show logging queue
```

```
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

在本例中，logging queue 命令设置为 0，表示队列设置为最大值 8192。ASA 以日志记录配置指定的方式处理队列中的系统日志消息，例如将系统日志消息发送至邮件收件人、将其保存至闪存等。

此 show logging queue 命令示例的输出显示有 5 条消息已排队，3513 条消息是自 ASA 最后一次启动后队列中一次的最大消息数，且已丢弃 1 条消息。即使队列设置为可容纳无限消息，该消息仍会被丢弃，因为没有块内存可用于将消息添加到队列。

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging rate-limit

要限制生成系统日志消息的速率，请在特权 EXEC 模式下使用 **logging rate-limit** 命令。要禁用速率限制，请在特权 EXEC 模式下使用此命令的 **no** 形式。

logging rate-limit {**unlimited** | **dynamic** {**block***value* [**message limit**值] } | {*num* [*interval*] } | **message** {*syslog_id* | **level***severity_level* } }
[**no**] **logging rate-limit** {**unlimited** | **dynamic** {**block***value* [**message limit**值] } | {*num* [*interval*] } | **message** {*syslog_id* | **level***severity_level* } }

Syntax Description

block值	用作速率限制阈值的块的百分比。
dynamic	当大小为 256 的块使用率超过指定的阈值时，限制记录率。当块使用率恢复正常值时禁用速率限制。
间隔	（可选）用于测量消息生成速率的时间间隔（以秒为单位）。间隔 值的有效范围为 0 到 2147483647。
level*severity_level*	将所设置的速率限制应用于属于特定严重性级别的所有系统日志消息。处于指定严重性级别的所有系统日志消息都将单独进行速率限制。 严重性_级别 的有效范围为 1 到 7。
message	抑制此系统日志消息的报告。
message limit值	动态速率限制允许的消息数量。
num	在指定时间间隔内可以生成的系统日志消息的数量。 *num* 值的有效范围为 0 到 2147483647。
syslog_id	要抑制的系统日志消息的 ID。值的有效范围为 100000 - 999999。
unlimited	禁用速率限制，这意味着日志记录速率没有限制。

Command Default

interval 的默认设置为 1。

message limit值 的默认设置为 10。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权 EXEC	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(4)	添加了此命令。
9.18(1)	添加了用于速率限制的动态选项。

使用指南

系统日志消息严重性级别如下：

- 0 - 系统不可用
- 1——需要立即采取行动
- 2—危急情况
- 3—错误情况
- 4—警告情况
- 5 - 正常但重大的情况
- 6—信息消息
- 7—调试消息

注释 由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，**请**仅将调试用于解决特定问题或在与Cisco技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

CR_Examples

要限制系统日志消息生成速率，可以输入特定消息 ID。以下示例显示如何使用特定消息 ID 和时间间隔来限制系统日志消息生成的速率：

```
ciscoasa(config)# logging rate-limit 100 600 message 302020
```

在指定的 600 秒间隔内达到速率限制 100 后，此示例禁止将系统日志消息 302020 发送到主机。

要限制系统日志消息生成速率，可以输入特定严重性级别。以下示例显示如何使用特定严重性级别和时间间隔来限制系统日志消息生成的速率。

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

此示例将严重性级别为 6 下的所有系统日志消息在 600 秒的指定时间间隔内抑制到指定的速率限制 1000。每条严重性级别为 6 的系统日志消息的速率限制为 1000。

要在大小为 256 的块使用率较高时启用消息的动态速率限制，请使用 **dynamic** 关键字。您可以指定空闲 256 个块的百分比作为触发动态速率限制的阈值。您还可以使用 **message limit** 关键字来允许进行动态速率限制的消息数。其默认值为10。

```
asa(config)# logging rate-limit ?

configure mode commands/options:
  <1-2147483647>  Specify logging rate-limit number
  dynamic         Specify dynamic option for rate-limit
  unlimited       Specify unlimited option for rate-limit

asa(config)# logging rate-limit dynamic ?

configure mode commands/options:
  block  Dynamic rate-limit for block usage

asa(config)# logging rate-limit dynamic block ?

configure mode commands/options:
  <1-100>  Specify 256 blocks free percentage to trigger dynamic rate-limit
asa(config)# logging rate-limit dynamic block 50 ?

configure mode commands/options:
  messagelimit  Specify the number of messages allowed for dynamic rate-limit

asa(config)# logging rate-limit dynamic block 50 messagelimit ?

configure mode commands/options:
  <1-100>  Specify logging rate-limit interval
```

Related Commands

命令	说明
clearrunning-configloggingrate-limit	将日志记录速率限制设置重置为其默认值。
showlogging	显示当前位于内部缓冲区或日志记录配置设置中的消息。
showrunning-configloggingrate-limit	显示当前日志记录速率限制设置。

logging recipient-address

要指定 ASA 发送的系统日志消息的接收邮件地址，请在全局配置模式下使用 **loggingrecipient-address** 命令。要删除接收电子邮件地址，请使用此命令的 **no**形式。

loggingrecipient-address*address* [**level***level*]
nologgingrecipient-address*address* [**level***level*]

Syntax Description

地址	通过电子邮件发送系统日志消息时指定收件人电子邮件地址。
level	表示严重性级别如下。
水平	设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为 3，则 ASA 将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示： • 或**0emergencies**— 系统不可用。 • 或**1alerts**——需要立即采取行动。 • 或**2critical**——危急情况。 • 或**3errors**——错误情况。 • 或**4warnings**——警告情况。 • 或**5notifications**——正常但重要的情况。 • 或**6informational**——信息性消息。 • 或**7debugging**——调试消息。 注释 由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此， 请 仅将调试用于解决特定问题或在与Cisco技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。 注释 我们不建议在 **loggingrecipient-address** 命令中使用大于 3 的严重性级别。较高的严重性级别可能会因缓冲区溢出而导致系统日志消息被丢弃。 由 **loggingrecipient-address** 命令指定的消息严重性级别会覆盖由 **loggingmail** 命令指定的消息严重性级别。例如，如果 **loggingrecipient-address** 命令指定的严重性级别为 7，但 **loggingmail** 命令指定的严重性级别为 3，则 ASA 将所有消息都发送给收件人，包括严重性级别为 4、5、6 和 7 的消息。

Command Default

默认值设置为 errors logging level。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

您最多可以配置 5 个收件人地址。如果需要，每个收件人地址可以具有不同于 **loggingmail** 命令指定的邮件级别。使用 **loggingmail** 命令启用通过邮件发送系统日志消息。

使用此命令可将更紧急的邮件发送给更多的收件人。

CR_Examples

要将 ASA 设置为通过邮件发送系统日志消息，请使用以下条件：

- 发送重要、警报或紧急消息。
- 使用 ciscosecurityappliance@example.com 作为发件人地址发送邮件。
- 将邮件发送到 admin@example.com。
- 使用 SMTP、主要服务器 pri-smtp-host 和辅助服务器 sec-smtp-host 发送邮件。

输入以下命令：

```
ciscoasa
(config)#
logging mail critical
ciscoasa
(config)#
logging from-address ciscosecurityappliance@example.com
ciscoasa
(config)#
logging recipient-address admin@example.com
ciscoasa
(config)#
smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

命令	说明
loggingenable	启用日志记录。
loggingfrom-address	指定系统日志消息出现的邮件地址。

命令	说明
loggingmail	启用ASA通过邮件发送系统日志消息，并确定通过邮件发送系统日志消息。
smtp-server	配置 SMTP 服务器。
showlogging	显示已启用的日志记录选项。

logging savelog

要将日志缓冲区保存到闪存，请在 **loggingsavelog** 特权 EXEC 模式下使用该命令。

loggingsavelog [*savefile*]

Syntax Description

savefile （可选）已保存的闪存文件名。如果您未指定文件名，ASA 将使用默认时间戳格式保存日志文件，如下所示：

```
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）。

Command Default

默认值如下：

- 缓冲区大小为 4 KB。
- 最低可用闪存为 3 MB。
- 为缓冲区日志记录分配的最大闪存为 1 MB。
- “语法说明”部分介绍了默认日志文件名。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权 EXEC	• 是	• 支持	• 支持	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

在您将日志缓冲区保存到闪存之前，您必须启用日志记录到缓冲区；否则日志缓冲区始终不会将数据保存到闪存。要启用缓冲区记录功能，请使用该 **loggingbuffered**命令。

注释 该 **loggingsavelog**命令不会清除缓冲区。要清除缓冲区，请使用 **clearloggingbuffer**命令。

CR_Examples

以下示例启用日志记录和日志缓冲区，退出全局配置模式，并使用文件名 latest-logfile.txt 将日志缓冲区保存到闪存：

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

Related Commands

命令	说明
clearloggingbuffer	清除包含的所有系统日志消息的日志缓冲区。
copy	将文件从一个位置复制到另一个位置，包括复制到 TFTP 或 FTP 服务器。
delete	从磁盘分区删除文件（如已保存的日志文件）。
loggingbuffered	启用将日志记录记录到日志缓冲区。
loggingenable	启用日志记录。

logging standby

要使故障转移备用 ASA 能够将系统日志消息发送到日志记录目标，请在全局配置模式下使用 **loggingstandby** 命令。要禁用 syslog 消息传递和 SNMP 日志记录，请使用此命令的 **no**形式。

loggingstandby
nologgingstandby

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，logging standalone 命令是禁用的。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

您可以启用该 **loggingstandby**命令，以确保发生故障转移时故障转移备用 ASA 的系统日志消息保持同步。

注释 使用该 **loggingstandby**命令会导致共享日志记录目标（例如 syslog 服务器、SNMP 服务器和 FTP 服务器）的流量增加一倍。

CR_Examples

以下示例使 ASA 能够将系统日志消息发送到故障转移备用 ASA。 **showlogging** 命令的输出表示此功能已启用：

```
ciscoasa(config)# logging standby
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: enabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
```

```
Trap logging: disabled
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

命令	说明
failover	启用故障转移功能。
loggingenable	启用日志记录。
logginghost	定义系统日志服务器。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging timestamp

要指定系统日志消息应包含消息的生成日期和时间，请在全局配置模式下使用 **loggingtimestamp**命令。要从系统日志消息中删除日期和时间，请使用此命令的 **no**形式。

loggingtimestamp [**rfc5424**]
nologgingtimestamp

Syntax Description

rfc5424 （可选）所有系统日志消息的时间戳都将按照 RFC 5424 格式显示时间：

```
YYYY
-MM
-DD
THH:MM:SS
Z
```

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）。

Command Default

默认情况下，ASA 不在系统日志消息中包含日期和时间。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.10(1)	**TheoptiontoenabletimestampasperRFC5424formatwasadded**

使用指南

logging timestamp 命令使 ASA 在所有系统日志消息中包含时间戳。在版本 9.10(1) 之前，系统日志的时间戳符合 RFC 3164，其中时间戳以“MM DD YYYY HH:MM:SS”格式显示。

此格式在 SIEM 中不是首选格式，因此 9.10(1) 中引入了 RFC 5424 选项。

将 RFC 5424 选项与 logging timestamp 命令配合使用，以按照 RFC 5424 启用系统日志支持时区。

CR_Examples

以下示例启用在所有系统日志消息中包含时间戳信息：

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

以下示例启用在所有系统日志消息中包含 RFC 5424 格式的时间戳信息：

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

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging trap

要指定 ASA 将哪些系统日志消息发送到系统日志服务器，请在全局配置模式下使用 **loggingtrap**命令。要从配置中删除此命令，请使用此命 **no**令的形式。

loggingtrap [*logging_list* | *level*]
nologgingtrap

Syntax Description

水平	设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为3，则ASA将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示： • 或**0emergencies**— 系统不可用。 • 或**1alerts**——需要立即采取行动。 • 或**2critical**——危急情况。 • 或**3errors**——错误情况。 • 或**4warnings**——警告情况。 • 或**5notifications**——正常但重要的情况。 • 或**6informational**——信息性消息。 • 或**7debugging**——调试消息。 注释 由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此， 请仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。
日志记录列表	指定要发送到 syslog 服务器的消息的列表。有关创建列表的信息，请参阅 **logginglist** 命令。

Command Default

未定义默认系统日志消息陷阱。

Command Modes

下表展示可输入命令的模式。

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

如果使用 TCP 作为日志记录传输协议，并且在 ASA 无法访问系统日志服务器、系统日志服务器配置错误或磁盘已满时，作为一项安全措施，ASA 将拒绝新的网络访问会话。

如果系统日志服务器发生故障，基于 UDP 的日志记录不会阻止 ASA 传递流量。

CR_Examples

以下示例显示如何将严重性级别为 0、1、2 和 3 的系统日志消息发送到位于内部接口上并使用默认协议和端口号的系统日志服务器。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 10.2.2.3
ciscoasa(config)# logging trap errors
ciscoasa(config)#
```

Related Commands

命令	说明
loggingenable	启用日志记录。
logginghost	定义系统日志服务器。
logginglist	创建可重复使用的消息选择标准列表。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

login

要使用本地用户数据库登录到特权 EXEC 模式（请参阅 username 命令）或更改用户名，请在用户 EXEC 模式下使用 **login** 命令。

login

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
用户 EXEC	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

在用户 EXEC 模式下，您可以使用 **login** 命令以本地数据库中的任何用户名身份登录特权 EXEC 模式。当您启用了 enable 身份验证（请参阅**aaaauthenticationconsole** 命令）时， **login** 命令类似于 **enable** 命令。与 enable authentication 不同， **login** 命令只能使用本地用户名数据库，并且使用此命令需要始终进行身份验证。您还可以从任何 CLI 模式下使用 **login** 命令更改用户。

如要允许用户在登录后访问特权 EXEC 模式（以及所有命令），请将用户权限级别设置为 2（默认）到 15。如果配置本地命令授权，则用户只能输入分配给该权限级别或更低级别的命令。请参阅 以 **aaaauthorizationcommand** 了解更多信息。

⚠

注意 如果您将可以访问 CLI 但您不希望其进入特权 EXEC 模式的用户添加到本地数据库中，则应该配置命令授权。在无命令授权的情况下，如果用户的权限级别为 2 或更高（2 是默认值），则用户可以在 CLI 使用自己的密码访问特权 EXEC 模式（以及所有命令）。或者，您可以使用 RADIUS 或 TACACS+ 身份验证，或者您可以将所有本地用户设置为级别 1，以便您可以控制谁可以使用系统启用密码访问特权 EXEC 模式。

CR_Examples

以下示例显示了您输入 **login** 命令后的提示符：

```
ciscoasa> login
Username:
```

Related Commands

命令	说明
aaaauthorizationcommand	启用 CLI 访问的命令授权。
aaaauthenticationconsole	需要进行控制台、Telnet、HTTP、SSH 或 **enable** 命令访问的身份验证。
logout	注销 CLI。
username	将用户添加到本地数据库。

login-button

要自定义 WebVPN 用户连接到安全设备时显示的 WebVPN 页面登录框的登录按钮，请使用 webvpn 自定义配置模式下的 **login-button** 命令。要从配置中删除命令并导致值被继承，请使用命 **no**令的形式。

login-button { **text** | **style** } *value*

[**no**] **login-button** { **text** | **style** } *value*

Syntax Description

style	指示您正在更改样式。
text	指示您正在更改文本。
value	要显示的实际文本（最多 256 个字符）或层叠样式表 (CSS) 参数（最多 256 个字符）。

Command Default

登录按钮的默认文本为“Login”。

默认登录按钮样式为：

border: 1px secure;background- Color:white;font-height:bold; font-size：80%

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Webvpn 自定义配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

该 **style**选项表示为任何有效的层叠样式表 (CSS) 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的更多信息，请查阅万维网联盟 (W3C) 网站 www.w3.org 上的 CSS 规范。CSS 2.1 规范的附录 F 包含 CSS 参数的便捷列表，且在 www.w3.org/TR/CSS21/propidx.html 上提供。

以下是对 WebVPN 页面进行最常见更改（页面颜色）的一些技巧：

- 您可以使用逗号分隔的 RGB 值、HTML 颜色值或颜色的名称（如果已在 HTML 中标识）。
- RGB 格式是 0,0,0，每种颜色（红色、绿色、蓝色）的范围是从 0 到 255 的十进制数字；逗号分隔的条目表示每种颜色与其他颜色相结合的强度级别。

- HTML 格式是 #000000，十六进制格式的六位数；第一和第二个数字代表红色，第三和第四个数字代表绿色，第五和第六个数字代表蓝色。

注释 要轻松定制 WebVPN 页面，我们建议您使用 ASDM，它具有配置样式元素的便捷功能，包括色样和预览功能。

CR_Examples

以下示例使用文本“OK”自定义登录按钮：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-button text OK
```

Related Commands

命令	说明
login-title	自定义 WebVPN 页面登录框的标题。
group-prompt	自定义WebVPN页面登录框的群组提示。
password-prompt	自定义WebVPN页面登录框的密码提示。
username-prompt	自定义WebVPN页面登录框的用户名提示。

login-message

要自定义 WebVPN 用户连接到安全设备时显示的 WebVPN 页面的登录消息，请使用 webvpn 自定义配置模式下的 **login-message** 命令。要从配置中删除命令并导致值被继承，请使用命 **no**令的形式。

login-message { **text** | **style** } *value*

[**no**] **login-message** { **text** | **style** } *value*

Syntax Description

text	指示您正在更改文本。
style	指示您正在更改样式。
value	要显示的实际文本（最多 256 个字符）或层叠样式表 (CSS) 参数（最多 256 个字符）。

Command Default

默认登录消息是“请输入您的用户名和密码”。

默认登录消息样式为背景颜色：#CCCCCC;颜色：黑色。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
WebVPN 自定义配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

该 **style**选项表示为任何有效的层叠样式表 (CSS) 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的更多信息，请查阅万维网联盟 (W3C) 网站 www.w3.org 上的 CSS 规范。CSS 2.1 规范的附录 F 包含 CSS 参数的便捷列表，且在 www.w3.org/TR/CSS21/propidx.html 上提供。

以下是对 WebVPN 页面进行最常见更改（页面颜色）的一些技巧：

- 您可以使用逗号分隔的 RGB 值、HTML 颜色值或颜色的名称（如果已在 HTML 中标识）。
- RGB 格式是 0,0,0，每种颜色（红色、绿色、蓝色）的范围是从 0 到 255 的十进制数字；逗号分隔的条目表示每种颜色与其他颜色相结合的强度级别。
- HTML 格式是 #000000，十六进制格式的六位数；第一和第二个数字代表红色，第三和第四个数字代表绿色，第五和第六个数字代表蓝色。

注释 要轻松定制 WebVPN 页面，我们建议您使用 ASDM，它具有配置样式元素的便捷功能，包括色样和预览功能。

CR_Examples

在以下示例中，登录消息文本设置为“username and password”：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-message text username and password
```

Related Commands

命令	说明
login-title	自定义 WebVPN 页面上登录框的标题。EXTENSI
username-prompt	自定义WebVPN页面登录的用户名提示。
password-prompt	自定义WebVPN页面登录的密码提示。
group-prompt	定制WebVPN页面登录的群组提示。

login-title

要自定义向 WebVPN 用户显示的 WebVPN 页面上的登录框的标题，请使用 webvpn 自定义配置模式下的 **login-title** 命令。要从配置中删除命令并导致值被继承，请使用命 **no**令的形式。

login-title { **text** | **style** } *value*

[**no**] **login-title** { **text** | **style** } *value*

Syntax Description

text	指示您正在更改文本。
style	指定您正在更改 HTML 样式。
value	要显示的实际文本（最多 256 个字符）或层叠样式表 (CSS) 参数（最多 256 个字符）。

Command Default

默认登录文本为“Login”。

登录标题的默认 HTML 样式为背景颜色: #666666;颜色：白色。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Webvpn 自定义配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

该 **style**选项表示为任何有效的层叠样式表 (CSS) 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的更多信息，请查阅万维网联盟 (W3C) 网站 www.w3.org 上的 CSS 规范。CSS 2.1 规范的附录 F 包含 CSS 参数的便捷列表，且在 www.w3.org/TR/CSS21/propidx.html 上提供。

以下是对 WebVPN 页面进行最常见更改（页面颜色）的一些技巧：

- 您可以使用逗号分隔的 RGB 值、HTML 颜色值或颜色的名称（如果已在 HTML 中标识）。
- RGB 格式是 0,0,0，每种颜色（红色、绿色、蓝色）的范围是从 0 到 255 的十进制数字；逗号分隔的条目表示每种颜色与其他颜色相结合的强度级别。
- HTML 格式是 #000000，十六进制格式的六位数；第一和第二个数字代表红色，第三和第四个数字代表绿色，第五和第六个数字代表蓝色。

注释 要轻松定制 WebVPN 页面，我们建议您使用 ASDM，它具有配置样式元素的便捷功能，包括色样和预览功能。

CR_Examples

以下示例配置登录标题样式：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-title style background-color: rgb(51,51,255);color:
rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
bold
```

Related Commands

命令	说明
login-message	自定义 WebVPN 登录页面的登录消息。
username-prompt	自定义 WebVPN 登录页面的用户名提示。
password-prompt	自定义 WebVPN 登录页面的密码提示。
group-prompt	自定义 WebVPN 登录页面的组提示。

徽标

要自定义 WebVPN 用户连接到安全设备时显示的 WebVPN 页面上的徽标，请使用 webvpn 自定义模式下的 **logo** 命令。要从配置中删除徽标并重置默认值（思科徽标），请使用此命令的 **no**形式。

logo {**none** | **file** {路径值} }

[**no**] **logo** {**{none** | **file** {路径值} }

Syntax Description

file	表示您提供的文件中包含徽标。
none	表示无徽标。设置一个空值，从而不允许使用徽标。防止继承徽标。
path	文件名的路径。可能的路径为 disk0:、disk1: 或 flash:
value	指定徽标的文件名。最大长度为 255 个字符，无空格。文件类型必须为 JPG、PNG 或 GIF，并且必须小于 100 KB。

Command Default

默认徽标是思科徽标。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Webvpn 自定义配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

如果指定的文件名不存在，将显示错误消息。如果删除徽标文件，但配置仍指向该文件，则不会显示任何徽标。

文件名不能包含空格。

CR_Examples

在下面的示例中，cisco_logo.gif 文件包含一个自定义徽标：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

Related Commands

命令	说明
title	自定义 WebVPN 页面的标题。
page style	定制使用层叠样式表 (CSS) 参数的 WebVPN 页面。

logout

要退出 CLI，请在用户 EXEC 模式下使用 **logout**命令。

logout

Syntax Description

此命令没有任何参数或关键字。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
用户 EXEC	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

logout命令允许您注销 ASA。您可以使用 **exit**或**quit** 命令返回到非特权模式。

CR_Examples

以下示例显示如何注销 ASA：

```
ciscoasa> logout
```

Related Commands

命令	说明
login	启动登录提示。
exit	退出访问模式。
quit	退出配置模式或特权模式。

logout-message

要自定义 WebVPN 用户从 WebVPN 服务注销时向其显示的 WebVPN 注销屏幕的注销消息，请在 webvpn 自定义配置模式下使用 **logout-message**命令。要从配置中删除命令并导致值被继承，请使用命 **no**令的形式。

logout-message { **text** | **style** } 数值

[**no**] **logout-message** { **text** | **style** } 数值

Syntax Description

style	指示您正在更改样式。
text	指示您正在更改文本。
value	要显示的实际文本（最多 256 个字符）或层叠样式表 (CSS) 参数（最多 256 个字符）。

Command Default

默认的注销消息文本为“Goodbye”。

默认注销消息样式为背景颜色：#999999;颜色：黑色。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
WebVPN 自定义配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

该 **style**选项表示为任何有效的层叠样式表 (CSS) 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的更多信息，请查阅万维网联盟 (W3C) 网站 www.w3.org 上的 CSS 规范。CSS 2.1 规范的附录 F 包含 CSS 参数的便捷列表，且在 www.w3.org/TR/CSS21/propidx.html 上提供。

以下是对 WebVPN 页面进行最常见更改（页面颜色）的一些技巧：

- 您可以使用逗号分隔的 RGB 值、HTML 颜色值或颜色的名称（如果已在 HTML 中标识）。
- RGB 格式是 0,0,0，每种颜色（红色、绿色、蓝色）的范围是从 0 到 255 的十进制数字；逗号分隔的条目表示每种颜色与其他颜色相结合的强度级别。

- HTML 格式是 #000000，十六进制格式的六位数；第一和第二个数字代表红色，第三和第四个数字代表绿色，第五和第六个数字代表蓝色。

注释 要轻松定制 WebVPN 页面，我们建议您使用 ASDM，它具有配置样式元素的便捷功能，包括色样和预览功能。

CR_Examples

以下示例配置注销消息样式：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# logout-message style background-color: rgb(51,51,255);color:
 rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
bold
```

Related Commands

命令	说明
logout-title	自定义 WebVPN 页面的注销标题。
group-prompt	自定义WebVPN页面登录框的群组提示。
password-prompt	自定义WebVPN页面登录框的密码提示。
username-prompt	自定义WebVPN页面登录框的用户名提示。

lsp-full suppress

要控制在链路状态协议数据单元 (PDU) 变满时抑制哪些路由，请在路由器 isis 配置模式下使用 **lsp-fullsuppress** 命令。要停止抑制已重新分发的路由，请指定此命令的 **no** 形式。

lsp-fullsuppress {**external** [**interlevel**] | **interlevel** [**external**] | **none**}
nolsp-fullsuppress

Syntax Description

external	抑制此 ASA 上的任何重新分配路由。
级别间	抑制来自其他级别的任何路由。例如，如果 Level-2 LSP 已满，则将抑制来自 Level 1 的路由。
无	不抑制任何路由。

Command Default

抑制重新分发的路由。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
路由器配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

此命令允许监控 IS-IS 邻接状态更改。这在监控大型网络时可能非常有用。使用系统错误消息工具记录消息。消息的形式如下：

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

CR_Examples

以下示例显示如何指定在 LSP 已满时，将从 LSP 抑制重新分发的路由和来自其他级别的路由：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-full suppress interlevel external
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定IS-IS实例全局使用的IS-IS报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertise-prefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。

命令	说明
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置LSP刷新间隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
pnrotocolshutdow	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。

命令	说明
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

lsp-gen-interval

要自定义 LSP 生成的 IS-IS 限制，请在路由器 isis 配置模式下使用 **lsp-gen-interval** 命令。要恢复默认值，请使用此命 **no**令的形式。

lsp-gen-interval [**level-1** | **level-2**] *lsp-max-wait* [*lsp-initial-waitlsp-second-wait*
nolsp-gen-interval

Syntax Description

level-1	（可选）仅适用于 1 级区域。
level-2	（可选）仅适用于 2 级区域。
lsp-max-wait	指示生成 LSP 的两次连续出现之间的最大间隔。范围为 1 到 120 秒。
lsp-initial-wait	（可选）表示初始 LSP 生成延迟。范围为 1 到 120,000 毫秒。
lsp-second-wait	（可选）指示第一次和第二次 LSP 生成之间的保持时间。范围为 1 到 120,000 毫秒。

Command Default

lsp-max-wait： 5 秒

lsp-initial-wait： 50 毫秒

lsp-second-wait： 5000 毫秒

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
路由器配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

以下描述可帮助确定是否更改此命令的默认值：

- *lsp-initial-* wait 参数表示生成第一个 LSP 之前的初始等待时间。
- 第三个参数指示在生成第一个和第二个 LSP 之间等待的时长。
- 每个后续的等待间隔都是前一个的两倍，直到等待间隔达到指定的 *lsp-max-wait* 间隔 为止，因此，在初始间隔和第二个间隔之后，该值会导致 LSP 生成节流或减慢。一旦达到此间隔，等待间隔就会以此间隔继续，直到网络稳定下来。

- 网络稳定下来并且在两倍 *lsp-max-wait* 间隔内没有触发器后，将恢复快速行为（初始等待时间）。

CR_Examples

以下示例为 LSP 生成限制配置间隔：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-gen-interval 2 50 100
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定IS-IS实例全局使用的IS-IS报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertise-prefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。

命令	说明
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置LSP刷新间隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的NET。

命令	说明
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

lsp-refresh-interval

如要设置 LSP 刷新间隔，请在路由器 isis 配置模式下使用 **lsp-refresh-interval** 命令。要恢复默认刷新间隔，请使用此命 **no**令的形式。

lsp-refresh-interval 秒
no lsp-refresh-interval

Syntax Description

秒 LSP 的刷新间隔。范围为 1 到 65535 秒。

Command Default

默认值为 900 秒（15 分钟）。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
路由器配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

刷新间隔确定该软件在 LSP 中定期发送其始发的路由拓扑信息的速率。这样做是为了防止数据库信息过时。

注释 在 LSP 的有效期到期前，必须定期刷新 LSP。为 **lsp-refresh-interval** 命令设置的值应小于为 **max-lsp-lifetime** 命令设置的值；否则 LSP 将在刷新前超时。如果设置的 LSP 有效期比 LSP 刷新间隔低很多，该软件将缩短 LSP 刷新间隔以防止 LSP 超时。

CR_Examples

以下示例将 IS-IS LSP 刷新间隔配置为 1080 秒：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-refresh-interval 1080
```

Related Commands

命令	说明
advertise passive-only	配置 ASA 以通告被动接口。

命令	说明
area-password	配置 IS-IS 区域身份验证密码。
authentication key	全局启用 IS-IS 身份验证。
authentication mode	指定IS-IS实例全局使用的IS-IS报文认证方式。
authentication send-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clear isis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hello padding	将 IS-IS hello 配置为完整 MTU 大小。
hostname dynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isis adjacency-filter	过滤 IS-IS 邻接关系的建立。
isis advertise-prefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isis authentication key	启用接口的身份验证。
isis authentication mode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isis authentication send-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isis circuit-type	配置用于 IS-IS 的邻接类型。
isis csnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isis hello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isis hello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isis hello padding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isis lsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。

命令	说明
isis metric	配置 IS-IS 度量的值。
isis password	配置接口的认证密码。EXTEN
isis priority	配置接口上指定 ASA 的优先级。
isis protocol shutdown	禁用每个接口的 IS-IS 协议。
isis retransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isis retransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isis tag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-full suppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置LSP刷新间隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocol shutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistribute isis	将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级。
route priority high	为 IS-IS IP 前缀分配高优先级。
router isis	启用 IS-IS 路由。

命令	说明
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
show clns	显示 CLNS 特定信息。
show isis	显示 IS-IS 信息。
show route isis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

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。