思科 Firepower 威胁防御系统日志消息

首次发布日期: 2018 年 6 月 1 日

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

关于本指南

以下主题介绍如何使用本指南。

有关 Firepower 威胁防御的系统日志消息

Firepower 威胁防御操作系统使用 ASA 操作系统的某些部分，其中包括系统日志实用程序。由于共享此实用程序，因此 Firepower 威胁防御系统日志的消息全都以“%ASA”开头。

下表列出消息类以及与每个类相关联的消息 ID 范围。消息 ID 的有效范围为 100000 到 999999。

注释 如果序列中跳过某个数字，则表示该消息将不再出现在 Firepower 威胁防御设备代码中。

有关如何配置系统日志和 SNMP 的信息，请参阅《Firepower 管理中心配置指南》。

大多数 ISAKMP 消息都具有公用前置对象集来帮助识别隧道。这些对象在适用时置于消息的描述性文本前面。如果在生成消息时对象未知，则不显示特定的 **heading = value** 组合。

对象将按如下方式前置：

组 = **groupname**, 用户名 = **user**, IP = **IP_address**,...

其中“组”标识隧道组，“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 L2L 对等设备的公用 IP 地址。

表 *1:* 系统日志消息类和关联的消息 *ID* 号

日志记录类	定义	系统日志消息 ID 号
auth	用户身份验证	109、113
—	访问列表	106

关于本指南

日志记录类	定义	系统日志消息 ID 号
—	应用防火墙	415
网桥	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	思科 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	电邮代理	719
—	环境监控	735
ha	故障切换	101、102、103、104、105、210、311、709、727
—	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
—	黑名单、白名单和灰名单	338
—	许可	444

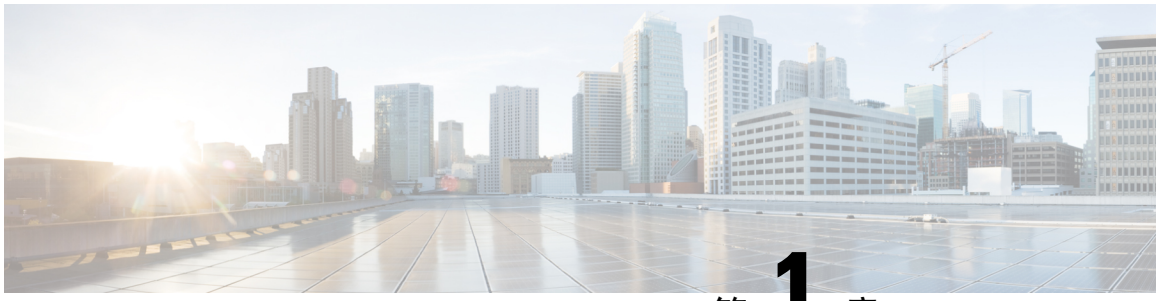
日志记录类	定义	系统日志消息 ID 号
mdm-proxy	MDM 代理	802
nac	网络接入控制	731、732
nacpolicy	NAC 策略	731
nacsettings	配置 NAC 设置，以应用 NAC 策略	732
—	网络无线接入点	713
np	网络处理器	319
—	NP SSL	725
ospf	OSPF 路由	318、409、503、613
—	密码加密	742
—	电话代理	337
rip	RIP 路由	107、312
rm	资源管理器	321
—	Smart Call Home	120
session	用户会话	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
—	ScanSafe	775
ssl	SSL 堆栈	725
svc	SSL VPN 客户端	722
sys	System	199、211、214、216、306、307、315、414、604、605，606、610、612、614、615、701、711、741
—	威胁检测	733
tre	事务规则引擎	780
—	UC-IME	339
标记交换	服务标记交换	779

日志记录类	定义	系统日志消息 ID 号
vm	VLAN Mapping	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 故障切换	720
vpnlb	VPN 负载均衡	718
—	VXLAN	778
webfo	WebVPN 故障切换	721
webvpn	WebVPN 和 AnyConnect 客户端	716
—	NAT 与 PAT	305

获取文档和提交服务请求

有关获取文档、使用思科缺陷搜索工具 (BST)、提交服务请求和收集其他信息的说明，请参阅思科产品文档更新。

要将新的和经过修订的思科技术内容直接接收到桌面，您可以订阅。RSS 源是一项免费服务。



第 1 章

系统日志消息 101001-199021

本章包含以下各节：

ID 介于 101001 到 109104 之间的消息

本部分包括 ID 介于 101001 到 109104 之间的消息。

101001

错误消息：`%ASA-1-101001: (Primary) Failover cable OK.`

说明：故障切换电缆存在且正常工作。主设备也可列为辅助设备的辅助设备。

建议的操作：无需执行任何操作。

101002

错误消息：`%ASA-1-101002: (Primary) Bad failover cable.`

说明：故障切换电缆存在，但无法正常工作。主设备也可列为辅助设备的辅助设备。

建议的操作：更换故障切换电缆。

101003、101004

错误消息：`%ASA-1-101003: (Primary) Failover cable not connected (this unit).`

错误消息：`%ASA-1-101004: (Primary) Failover cable not connected (other unit).`

说明：故障切换模式已启用，但故障切换电缆未连接到故障切换对的其中一台设备。主设备也可列为辅助设备的辅助设备。

建议的操作：将故障切换电缆连接到故障切换对的两台设备。

101005

错误消息：`%ASA-1-101005: (Primary) Error reading failover cable status.`

说明：故障切换电缆已连接，但主设备无法确定其状态。

建议的操作：更换电缆。

103001

错误消息：`%ASA-1-103001: (Primary) No response from other firewall (reason code = code).`

说明：主设备无法通过故障切换电缆与辅助设备进行通信。主设备也可列为辅助设备的辅助设备。下表列出了原因代码和说明，可用于确定发生故障切换的原因。

原因代码	说明
1	本地设备在发生 LAN 故障切换时，未在故障切换 LAN 接口上接收 Hello 数据包，或者在发生串行故障切换时未在串行故障切换电缆上接收 Hello 数据包，并宣告对等体已关闭。
2	接口没有通过以下四项故障切换测试之一：1) 链路打开、2) 监控网络流量、3) ARP，以及 4) 广播 Ping。
3	在串行电缆上发送命令后超过 15 秒没有接收到正确的确认消息。
4	故障切换 LAN 接口已关闭，且其他数据接口不响应其他接口测试。此外，本地设备宣告对等体已关闭。
5	在配置同步过程中备用对等体关闭。
6	复制未完成；故障切换设备未同步。

建议的操作：验证故障切换电缆是否已正确连接，以及两台设备的硬件、软件和配置是否相同。如果问题仍然存在，请联系思科 TAC。

103002

错误消息：`%ASA-1-103002: (Primary) Other firewall network interface interface_number OK.`

说明：主设备检测到辅助设备上的网络接口正常。主设备也可列为辅助设备的辅助设备。

建议的操作：无需执行任何操作。

103003

错误消息：`%ASA-1-103003: (Primary) Other firewall network interface interface_number failed.`

说明：主设备检测到辅助设备上的网络接口故障。主设备也可列为辅助设备的辅助设备。

建议的操作：检查辅助设备的网络连接和网络集线器连接。如有必要，更换发生故障的网络接口。

103004

错误消息：`%ASA-1-103004: (Primary) Other firewall reports this firewall failed.Reason: reason-string`

说明：主设备从辅助设备接收到指示主设备发生故障的消息。主设备也可列为辅助设备的辅助设备。原因可能是以下任意一项：

- 故障切换命令接口遗漏的轮询数据包超出阈值。
- LAN 故障切换接口发生故障。
- 对等体无法进入“备用就绪”状态。
- 无法完成配置复制。防火墙的配置可能不同步。
- 故障切换消息传输失败，未收到忙碌状态的确认消息。

建议的操作：验证主设备的状态。

103005

错误消息：`%ASA-1-103005: (Primary) Other firewall reporting failure.Reason: SSM card failure`

说明：辅助设备已向主设备报告 SSM 卡故障。主设备也可列为辅助设备的辅助设备。

建议的操作：验证辅助设备的状态。

103006

错误消息：`%ASA-1-103006: (Primary|Secondary) Mate version ver_num is not compatible with ours ver_num`

说明：Firepower 威胁防御设备检测到对等体设备运行的版本不同于本地设备，且与 HA 无中断升级功能不兼容。

- *ver_num* - 版本号。

建议的操作：在两台设备上安装相同或兼容版本的映像。

103007

错误消息：`%ASA-1-103007: (Primary|Secondary) Mate version ver_num is not identical with ours ver_num`

说明：Firepower威胁防御设备检测到对等体设备运行的版本不完全相同，但支持无中断升级且与本地设备兼容。由于映像版本不完全相同，因此系统性能可能会降级，并且如果长期运行不完全相同的映像，Firepower 威胁防御设备可能会出现稳定性问题。

- **ver_num** - 版本号

建议的操作：尽快在两台设备上安装相同的映像版本。

103008

错误消息：`%ASA-1-103008: Mate hwdib index is not compatible`

说明：主用设备和备用设备上的接口数量不相同。

建议的操作：验证设备的接口数量是否相同。您可能需要安装更多接口模块，或使用不同的设备。物理接口匹配后，<asa>通过输入 **write standby** 命令</asa><ftd>暂停然后恢复 HA</ftd>，即可强制同步配置。

104001、104002

错误消息：`%ASA-1-104001: (Primary) Switching to ACTIVE (cause: string ).`

错误消息：`%ASA-1-104002: (Primary) Switching to STANDBY (cause: string ).`

说明：您已通过以下两种方式之一强制使故障切换对交换角色，在备用设备上输入 **failover active** 命令，或在主用设备上输入 **no failover active** 命令。主设备也可列为辅助设备的辅助设备。字符串变量的可能值如下所示：

- state check
- bad/incomplete config
- ifc [interface] check, mate is healthier
- the other side wants me to standby
- in failed state, cannot be active
- switch to failed state
- other unit set to active by CLI config command fail active

建议的操作：如果由于人工干预而显示此消息，则无需任何操作。否则，请使用辅助设备报告的原因来验证故障切换对两台设备的状态。

104003

错误消息：`%ASA-1-104003: (Primary) Switching to FAILED.`

说明：主设备发生故障。

建议的操作：检查主设备的消息是否指明了问题的性质（请参阅消息 104001）。主设备也可列为辅助设备的辅助设备。

104004

错误消息：`%ASA-1-104004: (Primary) Switching to OK.`

说明：之前发生故障的设备报告它再次运行。主设备也可列为辅助设备的辅助设备。

建议的操作：无需执行任何操作。

105001

错误消息： `%ASA-1-105001: (Primary) Disabling failover.`

说明： 说明：在 7.x 及更高版本中，此消息可能指示：由于模式不匹配（单个或多个）、许可证不匹配（加密或情景）或硬件差异（一台设备安装的是 IPS SSM，而其对等体安装的是 CSC SSM），系统已自动禁用故障切换。主设备也可列为辅助设备的辅助设备。

建议的操作： 无需执行任何操作。

105002

错误消息： `%ASA-1-105002: (Primary) Enabling failover.`

说明： 在之前禁用故障切换功能之后，您在控制台上使用了无参数的 **failover** 命令。主设备也可列为辅助设备的辅助设备。

建议的操作： 无需执行任何操作。

105003

错误消息： `%ASA-1-105003: (Primary) Monitoring on interface interface_name waiting`

说明： Firepower威胁防御设备正在测试该故障切换对的另一台设备的指定网络接口。主设备也可列为辅助设备的辅助设备。

建议的操作： 无需执行任何操作。Firepower 威胁防御设备经常在正常运行期间监控其网络接口。

105004

错误消息： `%ASA-1-105004: (Primary) Monitoring on interface interface_name normal`

说明： 指定网络接口的测试已成功。主设备也可列为辅助设备的辅助设备。

建议的操作： 无需执行任何操作。

105005

错误消息： `%ASA-1-105005: (Primary) Lost Failover communications with mate on interface interface_name.`

说明： 故障切换对的一台设备无法再与故障切换对的另一台设备进行通信。主设备也可列为辅助设备的辅助设备。

建议的操作： 验证连接到指定接口的网络是否正常运行。

105006、105007

错误消息： `%ASA-1-105006: (Primary) Link status Up on interface interface_name.`

错误消息： %ASA-1-105007: (Primary) Link status Down on interface interface_name.

说明： 系统报告了指定接口的链路状态监控结果。主设备也可列为辅助设备的辅助设备。

建议的操作： 如果链路状态为关闭，请验证连接到指定接口的网络是否正常运行。

105008

错误消息： %ASA-1-105008: (Primary) Testing interface interface_name.

说明： 已对指定网络接口进行测试。只有当Firepower威胁防御设备在预期间隔后无法从该接口的备用设备上接收消息时，才会执行此测试。主设备也可列为辅助设备的辅助设备。

建议的操作： 无需执行任何操作。

105009

错误消息： %ASA-1-105009: (Primary) Testing on interface interface_name {Passed|Failed}.

说明： 系统报告了上一次接口测试的结果（“通过”或“失败”）。主设备也可列为辅助设备的辅助设备。

建议的操作： 如果结果为“通过”，则无需执行任何操作。如果结果为“失败”，则应检查两台故障切换设备的网络电缆连接，网络本身是否正常运行，并验证备用设备的状态。

105010

错误消息： %ASA-3-105010: (Primary) Failover message block alloc failed.

说明： 数据块内存已耗尽。这是临时消息，Firepower威胁防御设备应恢复。主设备也可列为辅助设备的辅助设备。

建议的操作： 使用 show blocks 命令来监控当前的数据块内存。

105011

错误消息： %ASA-1-105011: (Primary) Failover cable communication failure

说明： 故障切换电缆无法实现主设备和辅助设备之间的通信。主设备也可列为辅助设备的辅助设备。

建议的操作： 确保电缆已正确连接。

105020

错误消息： %ASA-1-105020: (Primary) Incomplete/slow config replication

说明： 发生故障切换时，主用Firepower威胁防御设备在内存中检测到配置不完整。通常情况下，这种错误是由于复制服务中断而导致的。主设备也可列为辅助设备的辅助设备。

建议的操作：在 Firepower 威胁防御设备 检测到故障切换后，Firepower 威胁防御设备会自动重新启动并从闪存加载配置和/或与另一台 Firepower 威胁防御设备重新同步。如果故障切换情况持续发生，请检查故障切换的配置，并确保两台 Firepower 威胁防御设备彼此之间可以进行通信。

105021

错误消息：`%ASA-1-105021: (failover_unit ) Standby unit failed to sync due to a locked context_name config.Lock held by lock_owner_name`

说明：在配置同步期间，如果某个其他进程将配置锁定超过五分钟，则备用设备将自行重新加载，这会阻止故障切换进程应用新配置。系统正在同步配置时，如果管理员翻阅备用设备上正在运行的配置，可能会发生这种情况。另请参阅特权 EXEC 模式下的 **show running-config** 命令以及思科 *ASA 5500* 系列命令参考中全局配置模式下的 **pager lines num** 命令。

建议的操作：当备用设备首次启动且正在与主用设备建立故障切换连接时，请避免在备用设备上查看或修改配置。

105031

错误消息：`%ASA-1-105031: Failover LAN interface is up`

说明：LAN 故障切换接口链路已启动。

建议的操作：无需执行任何操作。

105032

错误消息：`%ASA-1-105032: LAN Failover interface is down`

说明：LAN 故障切换接口链路已关闭。

建议的操作：检查 LAN 故障切换接口的连接。确保速度或双工设置是正确的。

105033

错误消息：`%ASA-1-105033: LAN FO cmd Iface down and up again`

说明：故障切换的 LAN 接口已关闭。

建议的操作：验证故障切换链路，可能是出现了通信问题。

105034

错误消息：`%ASA-1-105034: Receive a LAN_FAILOVER_UP message from peer.`

说明：对等体刚刚启动并发送了初始联系消息。

建议的操作：无需执行任何操作。

105035

错误消息： `%ASA-1-105035: Receive a LAN failover interface down msg from peer.`

说明： 对等体 LAN 故障切换接口链路已关闭。如果该设备处于备用模式，则将切换到主用模式。

建议的操作： 检查对等体 LAN 故障切换接口的连接。

105036

错误消息： `%ASA-1-105036: dropped a LAN Failover command message.`

说明： Firepower 威胁防御设备丢弃了未确认的 LAN 故障切换命令消息，指示 LAN 故障切换接口存在连接问题。

建议的操作： 检查是否连接了 LAN 接口电缆。

105037

错误消息： `%ASA-1-105037: The primary and standby units are switching back and forth as the active unit.`

说明： 主设备和备用设备来回切换为主用设备，表示存在 LAN 故障切换连接问题或软件错误。

建议的操作： 确保连接了 LAN 接口电缆。

105038

错误消息： `%ASA-1-105038: (Primary) Interface count mismatch`

说明： 发生故障切换时，主用 Firepower 威胁防御设备在内存中检测到配置不完整。通常情况下，这种错误是由于复制服务中断而导致的。主设备也可列为辅助设备的辅助设备。

建议的操作： Firepower 威胁防御设备检测到故障切换之后，Firepower 威胁防御设备会自动重新启动并从闪存加载配置和/或与另一台 Firepower 威胁防御设备重新同步。如果故障切换情况持续发生，请检查故障切换的配置，并确保两台 Firepower 威胁防御设备彼此之间可以进行通信。

105039

错误消息： `%ASA-1-105039: (Primary) Unable to verify the Interface count with mate.Failover may be disabled in mate.`

说明： 故障切换最初验证主辅 Firepower 威胁防御设备上配置的接口数量是否相同。此消息指示主 Firepower 威胁防御设备无法验证辅助 Firepower 威胁防御设备上配置的接口数量。此消息指示主 Firepower 威胁防御设备无法通过故障切换接口与辅助 Firepower 威胁防御设备进行通信。主设备也可列为辅助设备的辅助设备。

建议的操作： 验证主辅 Firepower 威胁防御设备上的故障切换 LAN、接口配置和状态。确保辅助 Firepower 威胁防御设备正在运行 Firepower 威胁防御设备应用且故障切换已启用。

105040

错误消息： `%ASA-1-105040: (Primary) Mate failover version is not compatible.`

说明： 主辅 Firepower 威胁防御设备应运行相同版本的故障切换软件，才能充当故障切换对。此消息指示辅助 Firepower 威胁防御设备故障切换软件版本与主 Firepower 威胁防御设备不兼容。主 Firepower 威胁防御设备上禁用了故障切换。“主设备”还可能列为辅助 Firepower 威胁防御设备的“辅助设备”。

建议的操作： 在主辅 Firepower 威胁防御设备之间保持软件版本一致以启用故障切换。

105041

错误消息： `%ASA-1-105041: cmd failed during sync`

说明： nameif 命令复制失败，这是因为主用设备和备用设备上的接口数量不相同。

建议的操作： 验证设备的接口数量是否相同。您可能需要安装更多接口模块，或使用不同的设备。物理接口匹配后，<asa>通过输入 **write standby** 命令</asa><ftd>暂停然后恢复 HA</ftd>，即可强制同步配置。

105042

错误消息： `%ASA-1-105042: (Primary) Failover interface OK`

说明： LAN 故障切换接口链路已启动。

用于发送故障切换消息至辅助 Firepower 威胁防御设备的接口正在运行。“主设备”还可能列为辅助 Firepower 威胁防御设备的“辅助设备”。

建议的操作： 无需执行任何操作。

105043

错误消息： `%ASA-1-105043: (Primary) Failover interface failed`

说明： LAN 故障切换接口链路已关闭。

建议的操作： 检查 LAN 故障切换接口的连接。确保速度或双工设置是正确的。

105044

错误消息： `%ASA-1-105044: (Primary) Mate operational mode mode is not compatible with my mode mode.`

说明： 当故障切换对等体之间的操作模式（单个或多个）不匹配时，系统将禁用故障切换功能。

建议的操作： 将故障切换对等体配置为采用相同的操作模式，然后重新启用故障切换功能。

105045

错误消息： `%ASA-1-105045: (Primary) Mate license (number contexts) is not compatible with my license (number contexts).`

说明： 当故障切换对等体之间的功能许可证不匹配时，系统将禁用故障切换功能。

建议的操作： 将故障切换对等体配置为使用相同的功能许可证，然后重新启用故障切换功能。

105046

错误消息： `%ASA-1-105046 (Primary|Secondary) Mate has a different chassis`

说明： 两台故障切换设备采用不同类型的机箱。例如，其中一台设备采用三插槽机箱；另一台设备采用六插槽机箱。

建议的操作： 确保两台故障切换设备是相同的。

105047

错误消息： `%ASA-1-105047: Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2`

说明： 两台故障切换设备各自的插槽中有不同类型的卡。

建议的操作： 确保故障切换设备的卡配置是相同的。

105048

错误消息： `%ASA-1-105048: (unit ) Mate's service module (application ) is different from mine (application )`

说明： 故障切换进程检测到主用设备和备用设备中的服务模块上正在运行不同的应用。如果使用不同的服务模块，则两台故障切换设备不兼容。

- **unit** - 主设备或辅助设备
- **application** - 应用的名称，例如 InterScan Security Card

建议的操作： 确保两台设备拥有完全相同的服务模块，然后再尝试重新启用故障切换功能。

105050

错误消息： `%ASA-3-105050: ASAv ethernet interface mismatch`

说明： 备用设备上的以太网接口数量少于主用设备上的以太网接口数量。

建议的操作： 应将拥有相同接口数量的Firepower威胁防御设备彼此配对。验证设备的接口数量是否相同。您可能需要安装更多接口模块，或使用不同的设备。物理接口匹配后，<asa>通过输入 **write standby** 命令</asa><ftd>暂停然后恢复 HA</ftd>，即可强制同步配置。

106001

错误消息： `%ASA-2-106001: Inbound TCP connection denied from`*`IP_address/port`* `to` *`IP_address/port`* `flags tcp_flags on interface interface_name`

说明： 尝试连接到内部地址的操作被针对指定流量类型定义的安全策略拒绝。显示的IP地址是真实IP地址，而不是通过NAT显示的IP地址。可能的tcp_flags值与连接被拒绝时存在的TCP报头中的标志对应。例如，TCP数据包到达时Firepower威胁防御设备中不存在连接状态，于是该数据包会被丢弃。此数据包中的tcp_flags是FIN和ACK。

tcp_flags如下所示：

- ACK - 收到确认号
- FIN - 数据已发送
- PSH - 接收方已将数据传递到应用
- RST - 连接已重置
- SYN - 序列号已同步以启动连接
- URG - 紧急指针宣告有效

建议的操作： 无需执行任何操作。

106002

错误消息： `%ASA-2-106002:` *`protocol`* `Connection denied by outbound list acl_ID src inside_address dest outside_address`

说明： 由于 **outbound deny** 命令，指定的连接失败。**protocol** 变量可以是ICMP、TCP或UDP。

建议的操作： 使用 **show outbound** 命令检查出站列表。

106006

错误消息： `%ASA-2-106006: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port on interface interface_name.`

说明： 入站UDP数据包被针对指定流量类型定义的安全策略拒绝。

建议的操作： 无需执行任何操作。

106007

错误消息： `%ASA-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}.`

说明： 包含DNS查询或响应的UDP数据包被拒绝。

建议的操作： 如果内部端口号为53，则内部主机可能设置为缓存名称服务器。添加 **access-list** 命令语句，以允许UDP端口53上的流量和内部主机的转换条目。如果外部端口号为53，则DNS服务器可能会由于速度过慢而无法响应，并且该查询由另一台服务器应答。

106010

错误消息： `%ASA-3-106010: Deny inbound protocol src [interface_name : source_address/source_port ] [([idfw_user | FQDN_string ], sg_info )] dst [interface_name : dest_address /dest_port ][([idfw_user | FQDN_string ], sg_info )]`

说明： 您的安全策略拒绝了入站连接。

建议的操作： 如果应允许流量，请修改安全策略。如果该消息定期显示，请与远程对等体管理员联系。

106011

错误消息： `%ASA-3-106011: Deny inbound (No xlate) string`

说明： 如果有内部用户通过 Web 浏览器访问互联网，则在正常流量状况下，系统会显示此消息。每次重置连接时，如果在Firepower威胁防御设备收到连接重置消息后连接末端的主机发送数据包，系统将显示此消息。通常可以忽略此消息。

建议的操作： 通过输入 **no logging message 106011** 命令，可防止此消息登录系统日志服务器。

106012

错误消息： `%ASA-6-106012: Deny IP from IP_address to IP_address , IP options hex.`

说明： 系统显示带有 IP 选项的 IP 数据包。由于 IP 选项被视为存在安全风险，因此该数据包已被丢弃。

建议的操作： 联系远程主机系统管理员以确定问题。检查本地站点是采用松散源路由还是严格源路由。

106013

错误消息： `%ASA-2-106013: Dropping echo request from IP_address to PAT address IP_address`

说明： Firepower 威胁防御设备丢弃了入站 ICMP 回应请求数据包，其目的地址与 PAT 全局地址对应。入站数据包被丢弃，因为它无法指定哪台 PAT 主机应接收该数据包。

建议的操作： 无需执行任何操作。

106014

错误消息： `%ASA-3-106014: Deny inbound icmp src interface_name : IP_address [([idfw_user | FQDN_string ], sg_info )] dst interface_name : IP_address [([idfw_user | FQDN_string ], sg_info )] (type dec , code dec )`

说明： Firepower 威胁防御设备拒绝了任何入站 ICMP 数据包访问。默认情况下，除非明确允许，否则系统将拒绝所有 ICMP 数据包访问。

建议的操作： 无需执行任何操作。

106015

错误消息： `%ASA-6-106015: Deny TCP (no connection) from IP_address /port to IP_address /port flags tcp_flags on interface interface_name.`

说明： Firepower 威胁防御设备丢弃了在 Firepower 威胁防御连接表中没有关联连接的 TCP 数据包。Firepower 威胁防御设备在该数据包内查找 SYN 标志，该标志表示建立新连接的请求。如果未设置 SYN 标志，并且没有现有连接，则 Firepower 威胁防御设备会丢弃该数据包。

建议的操作： 除非 Firepower 威胁防御设备收到大量这种无效的 TCP 数据包，否则不需要执行任何操作。如果收到大量无效的 TCP 数据包，请跟踪数据包的来源并确定发送这些数据包的原因。

106016

错误消息： `%ASA-2-106016: Deny IP spoof from (IP_address ) to IP_address on interface interface_name.`

说明： 数据包到达 Firepower 威胁防御接口，该接口的目的 IP 地址为 0.0.0.0，目的 MAC 地址为 Firepower 威胁防御接口的 MAC 地址。此外，当 Firepower 威胁防御设备丢弃源地址无效的数据包时，系统会生成此消息，这些无效的源地址可能包括以下某个无效地址或其他一些无效地址：

- 环回网络 (127.0.0.0)
- 广播（受限、网络定向、子网定向和所有子网定向）
- 目的主机 (land.c)

要进一步增强欺骗数据包检测，请使用 **icmp** 命令配置 Firepower 威胁防御设备，以丢弃所包含源地址属于内部网络的数据包，这是因为 **access-list** 命令已被弃用，且不再保证能够正常工作。

建议的操作： 确定是否有外部用户尝试攻击受保护的网络。检查客户端是否配置错误。

106017

错误消息： `%ASA-2-106017: Deny IP due to Land Attack from IP_address to IP_address`

说明： Firepower 威胁防御设备收到 IP 源地址和 IP 目的地址相同且目的端口和源端口相同的数据包。此消息指示出现了旨在攻击系统的欺骗数据包。此攻击称为“着陆攻击”。

建议的操作： 如果此消息仍然存在，则表示正在发生攻击。数据包提供的信息不足以确定攻击的来源。

106018

错误消息： `%ASA-2-106018: ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address`

说明： 包含指定 ICMP 的从本地主机 (inside_address) 到外部主机 (outside_address) 的传出 ICMP 数据包被出站 ACL 列表拒绝。

建议的操作： 无需执行任何操作。

106020

错误消息： `%ASA-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address`

说明： Firepower 威胁防御设备丢弃了采用泪滴签名的 IP 数据包，该泪滴签名包含小偏移量或片段重叠。这是一个规避 Firepower 威胁防御设备或入侵检测系统的恶意事件。

建议的操作： 请与远程对等体管理员联系，或根据您的安全策略上报此问题。

106021

错误消息： `%ASA-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name`

说明： 正在发生攻击。有人试图伪造入站连接上的 IP 地址。单播 RPF（也称为“反向路由查找”）检测到没有用路由表示源地址的数据包，并认为它属于对 Firepower 威胁防御设备所进行的攻击。

使用 ip verify reverse-path 命令启用单播 RPF 时，系统会显示此消息。此功能适用于向接口输入的数据包；如果在外部配置，则 Firepower 威胁防御设备会检查从外部到达的数据包。

Firepower 威胁防御设备根据源地址查找路由。如果未找到条目且未定义路由，则系统会显示此消息并断开连接。

如果有路由，则 Firepower 威胁防御设备会检查其对应的接口。如果数据包到达另一个接口，则要么是欺骗数据包，要么存在有多条路径可通往目的地的非对称路由环境。Firepower 威胁防御设备不支持非对称路由。

如果在内部接口配置 Firepower 威胁防御设备，它会检查静态路由命令语句或 RIP，并且如果找不到源地址，则说明有内部用户在伪造其地址。

建议的操作： 即便正在发生攻击，如果启用此功能，则无需执行任何用户操作。Firepower 威胁防御设备会击退该攻击。

106022

错误消息： `%ASA-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name`

说明： 匹配连接的数据包到达的接口与连接开始的接口不同。此外，未配置 ip verify reverse-path 命令。

例如，如果用户在内部接口上启动连接，但 Firepower 威胁防御设备检测到该连接到达了外围接口，则 Firepower 威胁防御设备有多条路径可到达目的地。这称为非对称路由，不受 Firepower 威胁防御设备支持。

攻击者也可能试图将来自一个连接的数据包附加到另一个连接，作为入侵 Firepower 威胁防御设备的一种手段。在任一情况下，Firepower 威胁防御设备都会显示此消息并丢弃连接。

建议的操作： 检查路由是否不对称。

106023

错误消息： `%ASA-4-106023: Deny protocol src [interface_name :source_address /source_port ] [([idfw_user |FQDN_string ], sg_info )] dst interface_name :dest_address /dest_port [([idfw_user |FQDN_string ], sg_info )] [type {string }, code {code }] by access_group acl_ID [0x8ed66b60, 0xf8852875]`

说明： ACL 拒绝了真实 IP 数据包。即便您没有为 ACL 启用 **log** 选项，也会显示此消息。IP 地址是真实 IP 地址，而不是通过 NAT 显示的值。如果找到匹配的 IP 地址，则系统会为 IP 地址提供用户身份信息和 FQDN 信息。Firepower 威胁防御设备记录身份信息（域/用户）或 FQDN（如果用户名不可用）。如果身份信息或FQDN可用，Firepower威胁防御设备将为源地址和目的地址记录此类信息。

建议的操作： 如果消息始终来自同一源地址，则表示可能有人正在尝试执行足迹或端口扫描。请与远程主机管理员联系。

106024

错误消息： `%ASA-2-106024: Access rules memory exhausted`

说明： 访问列表编译进程已耗尽内存。自上次成功编译访问列表后添加的所有配置信息都已从 Firepower 威胁防御设备中删除，并且将继续使用最近编译的访问列表组。

建议的操作： 将访问列表、AAA、ICMP、SSH、Telnet 和其他规则类型作为访问列表规则类型进行存储和编译。删除其中一些规则类型，以便添加其他规则类型。

106025、106026

错误消息： `%ASA-6-106025: Failed to determine the security context for the packet:sourceVlan:source_address dest_address source_port dest_port protocol`

错误消息： `%ASA-6-106026: Failed to determine the security context for the packet:sourceVlan:source_address dest_address source_port dest_port protocol`

说明： 无法确定多情景模式中数据包的安全情景。在路由器和透明模式下丢弃 IP 数据包可能会生成这两条消息。

建议的操作： 无需执行任何操作。

106027

错误消息： `%ASA-4-106027:acl_ID: Deny src [source address] dst [destination address] by access-group “access-list name"`

说明： ACL 拒绝了非 IP 数据包。即使您没有为扩展 ACL 启用日志选项，系统也会显示此消息。

建议的操作： 如果消息始终来自同一源地址，则表示可能有人尝试跟踪足迹或执行端口扫描。请与远程主机管理员联系。

106100

错误消息： `%ASA-6-106100: access-list acl_ID {permitted | denied | est-allowed} protocol interface_name /source_address (source_port ) (idfw_user , sg_info ) interface_name /dest_address (dest_port ) (idfw_user , sg_info ) hit-cnt number ({first hit | number -second interval}) hash codes`

说明： 系统列出间隔期间的初始出现次数或总出现次数。此消息提供的信息比消息 106023 多，后者只记录被拒绝的数据包，并且不包括命中计数或可配置级别。

当访问列表行有 *log* 参数时，由于非同步数据包到达 Firepower 威胁防御设备并接受访问列表的评估，因此预计可能会触发此消息 ID。例如，如果在 Firepower 威胁防御设备上收到 ACK 数据包（连接表中不存在该数据包的 TCP 连接），则 Firepower 威胁防御设备可能生成消息 106100，指示允许接收该数据包；但由于没有匹配的连接，系统稍后会正确丢弃该数据包。

下表介绍消息值：

- permitted | denied | est-allowed - 这些值指定 ACL 是允许还是拒绝该数据包。如果值为 est-allowed，则 ACL 会拒绝该数据包，但对于已建立的会话则允许接收该数据包（例如，允许内部用户访问互联网，并且接受通常被 ACL 拒绝的响应数据包）。
- *protocol* - TCP、UDP、ICMP 或 IP 协议号。
- *interface_name* - 已记录流的源或目的地的接口名称。支持 VLAN 接口。
- *Source_address* - 已记录流的源 IP 地址。IP 地址是真实 IP 地址，而不是通过 NAT 显示的值。
- *dest_address* - 已记录流的目的 IP 地址。IP 地址是真实 IP 地址，而不是通过 NAT 显示的值。
- *Source_port* - 已记录流的源端口（TCP 或 UDP）。对于 ICMP，源端口之后的数字表示消息类型。
- *idfw_user* - 表示用户身份的用户名，包括当 Firepower 威胁防御设备可以找到 IP 地址的用户名时添加到现有系统日志的域名。
- *sg_info* - 当 Firepower 威胁防御设备可以找到 IP 地址的安全组标记时添加到系统日志的安全组标记。安全组名称将与安全组标记（如果可用）一起显示。
- *dest_port* - 已记录流的目的端口（TCP 或 UDP）。对于 ICMP，目的端口之后的数字表示 ICMP 消息代码，适用于某些消息类型。对于类型 8，该数字始终为 0。如需 ICMP 消息类型列表，请访问以下 URL：http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml。
- hit-cnt *number* - 此 ACL 条目在配置的时间间隔内允许或拒绝该流的次数。当 Firepower 威胁防御设备为该流生成第一条消息时，值为 1。
- first hit - 系统为该流生成的第一条消息。
- *number* -second interval - 累计命中计数的间隔。使用 **access-list** 命令和 **interval** 选项设置此间隔。
- hash codes - 始终为对象组 ACE 和组成常规 ACE 打印两个散列代码。具体的值取决于该数据包所命中的 ACE。要显示这些散列代码，请输入 **show-access list** 命令。

建议的操作： 无需执行任何操作。

106101

错误消息： `%ASA-1-106101 Number of cached deny-flows for ACL log has reached limit (number ).`

说明：如果您为 ACL **deny** 语句配置了 **log** 选项（**access-list** *id* **deny** 命令），且有流量与该 ACL 语句匹配，则 Firepower 威胁防御设备会缓存流量信息。此消息指示在 Firepower 威胁防御设备上缓存的匹配流量的数量超出了用户配置的限值（使用 **access-list deny-flow-max** 命令）。在受到 DoS 攻击后，系统可能会生成此消息。

- *number* - 使用 **access-list deny-flow-max** 命令配置的限值

建议的操作：无需执行任何操作。

106102

错误消息：`%ASA-6-106102: access-list acl_ID {permitted|denied} protocol for user username interface_name /source_address source_port interface_name /dest_address dest_port hit-cnt number {first hit|number -second interval} hash codes`

说明：通过 VPN 过滤器应用的访问列表允许或拒绝数据包。此消息是与消息 106100 等效的 VPN/AAA 过滤器消息。

建议的操作：无需执行任何操作。

106103

错误消息：`%ASA-4-106103: access-list acl_ID denied protocol for user username interface_name /source_address source_port interface_name /dest_address dest_port hit-cnt number first hit hash codes`

说明：通过 VPN 过滤器应用的访问列表拒绝了某个数据包。此消息是与消息 106023 等效的 VPN/AAA 过滤器消息。

建议的操作：无需执行任何操作。

107001

错误消息：`%ASA-1-107001: RIP auth failed from IP_address : version=number, type=string, mode=string, sequence=number on interface interface_name`

说明：Firepower 威胁防御设备收到包含身份验证错误的 RIP 应答消息。由于路由器或 Firepower 威胁防御设备上的配置错误，或者有人尝试攻击 Firepower 威胁防御设备的路由表却未能成功，系统可能会显示此消息。

建议的操作：此消息指示可能发生了攻击，应予以监控。如果您不熟悉此消息中列出的源 IP 地址，请更改受信任实体之间的 RIP 身份验证密钥。攻击者可能在尝试确定现有密钥。

109011

错误消息： `%ASA-2-109011: Authen Session Start: user 'user ', sid number`

说明：在主机和 Firepower 威胁防御设备之间启动了身份验证会话，但尚未完成。

建议的操作：无需执行任何操作。

109012

错误消息： `%ASA-5-109012: Authen Session End: user 'user', sid number, elapsed number seconds`

说明： 身份验证缓存已超时。用户在下次连接时必须重新进行身份验证。您可以使用 timeout uauth 命令更改此计时器的持续时间。

建议的操作： 无需执行任何操作。

109013

错误消息： `%ASA-3-109013: User must authenticate before using this service`

说明： 用户必须先进行身份验证，然后才能使用该服务。

建议的操作： 先使用 FTP、Telnet 或 HTTP 进行身份验证，然后再使用该服务。

109016

错误消息： `%ASA-3-109016: Can't find authorization ACL acl_ID for user 'user '`

说明： 在 AAA 服务器上为此用户指定的名称在 Firepower 威胁防御设备上不存在。如果在配置 Firepower 威胁防御设备之前配置 AAA 服务器，则会发生此错误。AAA 服务器上的供应商特定属性 (VSA) 可能是以下值之一：

- acl=acl_ID
- shell:acl=acl_ID
- ACS:CiscoSecured-Defined-ACL=acl_ID

建议的操作： 将 ACL 添加到 Firepower 威胁防御设备，确保使用在 AAA 服务器上指定的相同名称。

109018

错误消息： `%ASA-3-109018: Downloaded ACL acl_ID is empty`

说明： 下载的授权没有 ACE。这种情况可能是由于属性字符串 *ip:inacl#* 拼写错误或忽略 access-list 命令而导致的。

```
junk:junk# 1=permit tcp any any eq junk ip:inacl#1=”
```

建议的操作： 更正 AAA 服务器上存在此指示错误的 ACL 组件。

109019

错误消息： `%ASA-3-109019: Downloaded ACL acl_ID has parsing error; ACE string`

说明： 在解析已下载授权的属性字符串 ip:inacl#NNN= 中的序列号 NNN 期间发生错误。原因包括：缺少 =；# 和 = 之间包含非数值、非空格字符；NNN 大于 999999999。

```
ip:inacl# 1 permit tcp any any
```

```
ip:inacl# 1junk2=permit tcp any any
ip:inacl# 1000000000=permit tcp any any
```

建议的操作：更正 AAA 服务器上存在此指示错误的 ACL 元素。

109020

错误消息：`%ASA-3-109020: Downloaded ACL has config error; ACE`

说明：已下载授权的其中一个组件存在配置错误。消息中包含该元素的整个文本。出现此消息通常是由于 access-list 命令语句无效而导致的。

建议的操作：更正 AAA 服务器上存在此指示错误的 ACL 组件。

109026

错误消息：`%ASA-3-109026: [aaa protocol ] Invalid reply digest received; shared server key may be mismatched.`

说明：无法验证来自 AAA 服务器的响应。配置的服务器密钥可能不正确。在处理 RADIUS 或 TACACS+ 服务器的事务期间可能会生成此消息。

验证使用 **aaa-server** 命令配置的服务器密钥是否正确。

109027

错误消息：`%ASA-4-109027: [aaa protocol] Unable to decipher response message Server = server_IP_address , User = user`

说明：无法验证来自 AAA 服务器的响应。配置的服务器密钥可能不正确。在处理 RADIUS 或 TACACS+ 服务器的事务期间可能会显示此消息。server_IP_address 是相关 AAA 服务器的 IP 地址。用户是与连接关联的用户名。

建议的操作：验证使用 **aaa-server** 命令配置的服务器密钥是否正确。

109029

错误消息：`%ASA-5-109029: Parsing downloaded ACL: string`

说明：解析在用户身份验证期间从 RADIUS 服务器下载的访问列表时发生语法错误。

- *string* - 一条错误消息，详细说明了阻止访问列表正确解析的语法错误

建议的操作：使用此消息中显示的信息来识别并更正 RADIUS 服务器配置内访问列表定义中的语法错误。

109030

错误消息：`%ASA-4-109030: Autodetect ACL convert wildcard did not convert ACL access_list source |dest netmask netmask .`

说明：用于自动检测通配符网络掩码的机制不会转换已在RADIUS服务器上配置的动态ACL。发生此问题的原因是此机制无法确定网络掩码是通配符还是普通网络掩码。

- **access_list -** 无法转换的访问列表
- **source -** 源 IP 地址
- **dest -** 目的 IP 地址
- **netmask -** 以点分十进制记法表示的目的或源地址的子网掩码

建议的操作：检查 RADIUS 服务器上通配符配置的访问列表网络掩码。如果网络掩码应该是通配符，并且该服务器上的所有访问列表网络掩码均为通配符，则对AAA服务器使用**acl-netmask-convert**的通配符设置。否则，请将网络掩码改为普通网络掩码或不包含黑洞（即网络掩码显示连续二进制数 1 的位置）的通配符网络掩码。例如，00000000.00000000.00011111.11111111 或十六进制 0.0.31.255）。如果网络掩码应该是普通网络掩码，并且该服务器上的所有访问列表网络掩码均为普通网络掩码，则对 AAA 服务器使用 **acl-netmask-convert** 的普通网络掩码设置。

109032

错误消息：`%ASA-3-109032: Unable to install ACL access_list , downloaded for user username ; Error in ACE: ace .`

说明：Firepower威胁防御设备从RADIUS服务器接收访问控制列表以应用于用户连接，但列表中的条目包含语法错误。使用包含错误的列表可能会导致违反安全策略，因此Firepower威胁防御设备无法对用户进行身份验证。

- *access_list* - 分配给动态访问列表的名称，它将显示在 **show access-list** 命令的输出中
- *username* - 其连接将受此访问列表约束的用户的名称
- *ace* - 检测到错误时正在进行处理的访问列表条目

建议的操作：更正 RADIUS 服务器配置中的访问列表定义。

109033

错误消息：`%ASA-4-109033: Authentication failed for admin user user from src_IP .Interactive challenge processing is not supported for protocol connections`

说明：在对管理连接进行身份验证期间触发了 AAA 质询处理，但是 Firepower 威胁防御设备无法启动与客户端应用的交互式质询处理。发生这种情况时，系统将拒绝尝试进行身份验证的操作并拒绝连接。

- *user* - 要进行身份验证的用户的名称
- *src_IP* - 客户端主机的 IP 地址
- *protocol* - 客户端连接协议（SSH v1 或管理 HTTP）

建议的操作：重新配置AAA，使这些连接类型不发生质询处理。这通常意味着要避免通过RADIUS向 RSA SecurID 服务器或任何基于令牌的 AAA 服务器验证这些连接类型。

109034

错误消息： `%ASA-4-109034: Authentication failed for network user user from src_IP/port to dst_IP/port .Interactive challenge processing is not supported for protocol connections`

说明：在对网络连接进行身份验证期间触发了 AAA 质询处理，但是 Firepower 威胁防御设备无法启动与客户端应用的交互式质询处理。发生这种情况时，系统将拒绝尝试进行身份验证的操作并拒绝连接。

- *user* - 要进行身份验证的用户的名称
- *src_IP/port* - 客户端主机的 IP 地址和端口
- *dst_IP/port* - 客户端尝试连接的服务器的 IP 地址和端口
- *protocol* - 客户端连接协议（例如 FTP）

建议的操作：重新配置 AAA，使这些连接类型不发生质询处理。这通常意味着要避免通过 RADIUS 向 RSA SecurID 服务器或任何基于令牌的 AAA 服务器验证这些连接类型。

109035

错误消息： `%ASA-3-109035: Exceeded maximum number (<max_num>) of DAP attribute instances for user <user>`

说明：如果从 RADIUS 服务器接收的 DAP 属性数量超出验证指定用户的连接时允许的最大数量，系统将生成此日志。

建议的操作：修改 DAP 属性配置以将 DAP 属性数量减少到低于日志中指定的最大允许数量，以便指定的用户可以进行连接。

109036

错误消息： `%ASA-6-109036: Exceeded 1000 attribute values for the attribute name attribute for user username .`

说明：LDAP 响应消息的一个属性有超过 1000 个值。

- *attribute_name* - LDAP 属性名称
- *username* - 登录时使用的用户名

建议的操作：无需执行任何操作。

109037

错误消息： `%ASA-3-109037: Exceeded 5000 attribute values for the attribute name attribute for user username .`

说明：Firepower 威胁防御设备支持从 AAA 服务器接收同一属性的多个值。如果 AAA 服务器发送的响应消息中所包含同一属性的值超过 5000 个，则 Firepower 威胁防御设备会将此响应消息视为格式错误并拒绝身份验证。只有在使用专门测试工具的实验室环境中，才能看到这种情况。实际的生产网络中不太可能会发生这种情况。

- *attribute_name* - LDAP 属性名称
- *username* - 登录时使用的用户名

建议的操作：使用协议嗅探器（例如 WireShark）捕获 Firepower 威胁防御设备和 AAA 服务器之间的身份验证流量，然后将跟踪文件转发到思科 TAC 进行分析。

109038

错误消息：`%ASA-3-109038: Attribute internal-attribute-name value string-from-server from AAA server could not be parsed as a type internal-attribute-name string representation of the attribute name`

说明：AAA 子系统尝试将来自 AAA 服务器的属性解析为内部表示形式时失败。

- *string-from-server* - 从 AAA 服务器收到的字符串，截断为 40 个字符。
- *type* - 指定属性的类型

建议的操作：验证 AAA 服务器上是否正确生成了该属性。有关其他信息，请使用 **debug ldap** 和 **debug radius** 命令。

109039

错误消息：`%ASA-5-109039: AAA Authentication:Dropping an unsupported IPv6/IP46/IP64 packet from lifc :laddr to fifc :faddr`

说明：包含 IPv6 地址或通过 NAT 转换为 IPv6 地址的 IPv4 地址的数据包需要 AAA 身份验证或授权。AAA 身份验证和授权不支持 IPv6 地址。系统丢弃此数据包。

- *lifc* - 入口接口
- *laddr* - 源 IP 地址
- *fifc* - 出口接口
- *faddr* - NAT 转换后的目的 IP 地址（如有）

建议的操作：无需执行任何操作。

109100

错误消息： `%ASA-6-109100: Received CoA update from coa-source-ip for user username , with session ID: audit-session-id , changing authorization attributes`

说明：Firepower 威胁防御设备已成功为会话 ID 为 *audit-session-id* 的用户 *username* 处理来自 *coa-source-ip* 的 CoA 策略更新请求。Firepower 威胁防御设备收到授权策略更新的更改，对其进行验证并应用后，将生成此系统日志消息。在非错误情况下，这是在接收和处理授权更改时生成的唯一系统日志消息。

- *coa-source-ip* - 发起授权请求更改的 IP 地址
- *username* - 会话正被更改的用户
- *audit-session-id* - 正在修改的会话的全局 ID

建议的操作：无需执行任何操作。

109101

错误消息： `%ASA-6-109101: Received CoA disconnect request from coa-source-ip for user username , with audit-session-id: audit-session-id`

说明： Firepower 威胁防御设备已收到针对活动 VPN 会话的格式正确的断开连接请求，并已成功终止连接。

- *coa-source-ip* - 发起授权请求更改的 IP 地址
- *username* - 会话正被更改的用户
- *audit-session-id* - 正在修改的会话的全局 ID

建议的操作： 无需执行任何操作。

109102

错误消息： `%ASA-4-109102: Received CoA action-type from coa-source-ip , but cannot find named session audit-session-id`

说明： Firepower 威胁防御设备已收到授权请求的有效更改，但该请求中指定的会话 ID 与 Firepower 威胁防御设备上的任何活动会话均不匹配。这可能是尝试在用户已关闭的会话上发出授权更改以更改授权服务器所导致的。

- *action-type* - 请求授权更改操作（更新或断开连接）
- *coa-source-ip* - 发起授权请求更改的 IP 地址
- *audit-session-id* - 正在修改的会话的全局 ID

建议的操作： 无需执行任何操作。

109103

错误消息： `%ASA-3-109103: CoA action-type from coa-source-ip failed for user username , with session ID: audit-session-id .`

说明： Firepower 威胁防御设备收到格式正确的授权更改请求，但无法成功处理该请求。

- *action-type* - 请求授权更改操作（更新或断开连接）
- *coa-source-ip* - 发起授权请求更改的 IP 地址
- *username* - 会话正被更改的用户
- *audit-session-id* - 正在修改的会话的全局 ID

建议的操作： 调查相关的 VPN 子系统日志，以确定无法应用更新属性的原因或无法终止会话的原因。

109104

错误消息： `%ASA-3-109104: CoA action-type from coa-source-ip failed for user username , session ID: audit-session-id .Action not supported.`

说明：Firepower 威胁防御设备收到格式正确的授权更改请求，但由于 Firepower 威胁防御设备不支持指示的操作，因此未处理该请求。

- *action-type* - 请求授权更改操作（更新或断开连接）
- *coa-source-ip* - 发起授权请求更改的 IP 地址
- *username* - 会话正被更改的用户
- *audit-session-id* - 正在修改的会话的全局 ID

建议的操作：无需执行任何操作。

109105

错误消息：`%ASA-3-109105: Failed to determine the egress interface for locally generated traffic destined to <protocol> <IP>:<port>.`

说明：当接口是 BVI 时，如果没有任何路由，则 Firepower 威胁防御设备有必要记录系统日志。显然，如果存在默认路由并且它没有将数据包路由到正确的接口，则无法对其进行跟踪。对于Firepower 威胁防御，系统会在数据接口之后先查找管理路由。因此，如果默认路由将数据包路由到不同的目的地，则很难进行跟踪。

建议的操作：强烈建议为正确的目的地添加默认路由或添加静态路由。

ID 介于 110002 到 113042 之间的消息

本部分包括 ID 介于 110002 到 113042 之间的消息。

110002

错误消息：`%ASA-6-110002: Failed to locate egress interface for protocol from src interface :src IP/src port to dest IP/dest port`

说明：当 Firepower 威胁防御设备尝试找到用于发送数据包的接口时发生错误。

- *protocol* - 数据包的协议
- *src interface* - 发送数据包的接口
- *src IP* - 数据包的源 IP 地址
- *src port* - 源端口号
- *dest IP* - 数据包的目的 IP 地址
- *dest port* - 目的端口号

建议的操作：复制错误消息、配置以及导致错误的事件的任何详细信息，并联系思科 TAC。

110003

错误消息：`%ASA-6-110003: Routing failed to locate next-hop for protocol from src interface :src IP/src port to dest interface :dest IP/dest port`

说明：当 Firepower 威胁防御设备尝试在接口路由表中查找下一跳时发生错误。

- *protocol* - 数据包的协议
- *src interface* - 发送数据包的接口
- *src IP* - 数据包的源 IP 地址
- *src port* - 源端口号
- *dest IP* - 数据包的目的 IP 地址
- *dest port* - 目的端口号

建议的操作：复制错误消息、配置以及导致错误的事件的任何详细信息，并联系思科 TAC。调试过程中，使用 **show asp table routing** 命令查看路由表的详细信息。

110004

错误消息：`%ASA-6-110004: Egress interface changed from old_active_ifc to new_active_ifc on ip_protocol connection conn_id for outside_zone /parent_outside_ifc :outside_addr /outside_port (mapped_addr /mapped_port ) to inside_zone /parent_inside_ifc :inside_addr /inside_port (mapped_addr /mapped_port )`

说明：出口接口上的流量已更改。

建议的操作：无需执行任何操作。

111001

错误消息：`%ASA-5-111001: Begin configuration: IP_address writing to device`

说明：您已输入 **write** 命令，将您的配置存储在设备（软盘、闪存、TFTP、故障切换备用设备或控制台终端）上。**IP_address** 指示是在控制台端口还是通过 Telnet 连接进行登录。

建议的操作：无需执行任何操作。

111002

错误消息：`%ASA-5-111002: Begin configuration: IP_address reading from device`

说明：您已输入 **read** 命令，以从某设备（软盘、闪存、TFTP、故障切换备用设备或控制台终端）读取您的配置。**IP_address** 指示是在控制台端口还是通过 Telnet 连接进行登录。

建议的操作：无需执行任何操作。

111003

错误消息：`%ASA-5-111003: IP_address Erase configuration`

说明：您通过在控制台中输入 **write erase** 命令清除了闪存内容。**IP_address** 值指示是在控制台端口还是通过 Telnet 连接进行登录。

建议的操作：清除配置后，重新配置 Firepower 威胁防御设备并保存新配置。或者，您也可以从之前保存在软盘上或网络其他位置的 TFTP 服务器上的配置恢复信息。

111004

错误消息： `%ASA-5-111004: IP_address end configuration: {FAILED|OK}`

说明： 您输入了 **config floppy/memory/ network** 命令或 **write floppy/memory/network/standby** 命令。**IP_address** 值指示是在控制台端口还是通过 Telnet 连接进行登录。

建议的操作： 如果消息以 OK 结尾，则无需执行任何操作。如果消息指示发生了故障，请尝试解决问题。例如，如果向软盘写入数据，请确保软盘没有实施写保护；如果向 TFTP 服务器写入数据，请确保该服务器已启动。

111005

错误消息： `%ASA-5-111005: IP_address end configuration: OK`

说明： 您已退出配置模式。**IP_address** 值指示是在控制台端口还是通过 Telnet 连接进行登录。

建议的操作： 无需执行任何操作。

111007

错误消息： `%ASA-5-111007: Begin configuration: IP_address reading from device.`

说明： 您输入了 **reload** 或 **configure** 命令以读取配置。设备文本可以是软盘、内存、网络、备用设备或终端。**IP_address** 值指示是在控制台端口还是通过 Telnet 连接进行登录。

建议的操作： 无需执行任何操作。

111008

错误消息： `%ASA-5-111008: User user executed the command string`

说明： 用户输入了除 **show** 命令以外的任何命令。

建议的操作： 无需执行任何操作。

111009

错误消息： `%ASA-7-111009:User user executed cmd:string`

说明： 用户输入了不修改配置的命令。只有使用 **show** 命令时才会显示此消息。

建议的操作： 无需执行任何操作。

111010

错误消息： `%ASA-5-111010: User username , running application-name from IP ip addr , executed cmd`

说明： 用户进行了配置更改。

- *username* - 进行配置更改的用户
- *application-name* - 该用户运行的应用
- *ip addr* - 管理站的 IP 地址
- *cmd* - 用户已执行的命令

建议的操作：无需执行任何操作。

111111

错误消息：`% ASA-1-111111 error_message`

说明：发生了系统或基础设施错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

112001

错误消息：`%ASA-2-112001: (string :dec ) Clear complete.`

说明：清除模块配置的请求已完成。已标识源文件和行号。

建议的操作：无需执行任何操作。

113001

错误消息：`%ASA-3-113001: Unable to open AAA session.Session limit [limit ] reached.`

说明：由于 AAA 资源不可用，因此无法在 IPsec 隧道或 WebVPN 连接上执行 AAA 操作。**limit** 值指示并发 AAA 事务的最大数量。

建议的操作：尽可能减少对 AAA 资源的需求。

113003

错误消息：`%ASA-6-113003: AAA group policy for user user is being set to policy_name .`

说明：使用用户特定的策略*policy_name*覆盖与该隧道组关联的组策略。此*policy_name*在配置LOCAL身份验证时使用 **username** 命令指定，或者在配置 RADIUS 身份验证时在 RADIUS CLASS 属性中返回。

建议的操作：无需执行任何操作。

113004

错误消息：`%ASA-6-113004: AAA user aaa_type Successful: server = server_IP_address , User = user`

说明：IPsec 或 WebVPN 连接上的 AAA 操作已成功完成。AAA 类型是身份验证、授权或记账。**server_IP_address** 是相关 AAA 服务器的 IP 地址。**用户**是与连接关联的用户名。

建议的操作：无需执行任何操作。

113005

错误消息：`%ASA-6-113005: AAA user authentication Rejected: reason = AAA failure: server = ip_addr : user = *****: user IP = ip_addr`

说明：连接上的 AAA 身份验证失败。用户名在无效或未知时隐藏，但在有效或配置了 **no logging hide username** 命令时显示。

建议的操作：重试身份验证。

113005

错误消息：`%ASA-6-113005: AAA user authentication Rejected: reason = AAA failure: server = ip_addr : user = *****: user IP = ip_addr`

说明：连接上的 AAA 身份验证失败。用户名在无效或未知时隐藏，但在有效或配置了 **no logging hide username** 命令时显示。

建议的操作：重试身份验证。

113006

错误消息：`%ASA-6-113006: User user locked out on exceeding number successive failed authentication attempts`

说明：本地配置的用户被锁定。如果此用户连续尝试身份验证达到已配置的失败次数阈值，就会发生这种情况，并且这还表示此用户将来尝试进行的所有身份验证操作都将被拒绝，直到管理员使用 **clear aaa local user lockout** 命令解锁该用户。**user** 是现已锁定的用户，**number** 是使用 **aaa local authentication attempts max-fail** 命令配置的连续失败次数阈值。

建议的操作：尝试使用 **clear_aaa_local_user_lockout** 命令解锁用户或调整允许的最大连续身份验证失败次数。

113007

错误消息：`%ASA-6-113007: User user unlocked by administrator`

说明：超出使用 **aaa local authentication attempts max-fail** 命令设置的最大连续身份验证失败次数后被锁定的本地配置用户已由指示的管理员解锁。

建议的操作：无需执行任何操作。

113008

错误消息：`%ASA-6-113008: AAA transaction status ACCEPT: user = user`

说明：与 IPsec 或 WebVPN 连接关联的用户的 AAA 事务已成功完成。user 是与连接关联的用户名。

建议的操作：无需执行任何操作。

113009

错误消息：`%ASA-6-113009: AAA retrieved default group policy policy for user user`

说明：系统对 IPsec 或 WebVPN 连接进行了身份验证或授权。系统已检索使用 **tunnel-group** 或 **webvpn** 命令指定的组策略的属性。

建议的操作：无需执行任何操作。

113010

错误消息：`%ASA-6-113010: AAA challenge received for user user from server server_IP_address`

说明：SecurID 服务器对 IPsec 连接进行了身份验证。系统将提示用户提供详细信息，然后再进行身份验证。

- **user** - 与连接关联的用户名
- **server _IP_address** - 相关 AAA 服务器的 IP 地址

建议的操作：无需执行任何操作。

113011

错误消息：`%ASA-6-113011: AAA retrieved user specific group policy policy for user user`

说明：系统对 IPsec 或 WebVPN 连接进行了身份验证或授权。系统已检索使用 **tunnel-group** 或 **webvpn** 命令指定的组策略的属性。

建议的操作：无需执行任何操作。

113012

错误消息：`%ASA-6-113012: AAA user authentication Successful: local database: user = user`

说明：与 IPsec 或 WebVPN 连接关联的用户已成功通过本地用户数据库的身份验证。

- **user** - 与连接关联的用户名

建议的操作：无需执行任何操作。

113013

错误消息：`%ASA-6-113013: AAA unable to complete the request Error: reason = reason : user = user`

说明：与 IPsec 或 WebVPN 连接关联的用户的 AAA 事务由于错误而失败，或者由于违反策略而被拒绝。

- **reason** - 原因的详细信息

- **user** - 与连接关联的用户名

建议的操作：无需执行任何操作。

113014

错误消息：`%ASA-6-113014: AAA authentication server not accessible: server = server_IP_address : user = user`

说明：执行与 IPsec 或 WebVPN 连接关联的 AAA 事务期间，设备无法与配置的 AAA 服务器通信。这可能会也可能不会导致用户连接尝试失败，具体取决于在 **aaa-server** 组中配置的备份服务器以及这些服务器的可用性。用户名在无效或未知时隐藏，但在有效或配置了 **no logging hide username** 命令时显示。

建议的操作：验证与已配置 AAA 服务器的连接。

113015

错误消息：`%ASA-6-113015: AAA user authentication Rejected: reason = reason : local database: user = user:  user IP = xxx.xxx.xxx.xxx`

说明：对于与 IPsec 或 WebVPN 连接关联的用户，向本地用户数据库进行身份验证的请求已被拒绝。用户名在无效或未知时隐藏，但在有效或配置了 **no logging hide username** 命令时显示。

- **Reason** - 请求被拒绝的原因的详细信息
- **user** - 与连接关联的用户名
- **user_ip** - 发起身份验证或授权请求的用户的 IP 地址<915CLI>

建议的操作：无需执行任何操作。

113016

错误消息：`%ASA-6-113016: AAA credentials rejected: reason = reason : server = server_IP_address : user = user<915CLI>:  user IP = xxx.xxx.xxx.xxx`

说明：与 IPsec 或 WebVPN 连接关联的用户的 AAA 事务由于错误而失败，或者由于违反策略而被拒绝。用户名在无效或未知时隐藏，但在有效或配置了 **no logging hide username** 命令时显示。

- **Reason** - 请求被拒绝的原因的详细信息
- **server_IP_address** - 相关 AAA 服务器的 IP 地址
- **user** - 与连接关联的用户名
- *<915CLI>user_ip* - 发起身份验证或授权请求的用户的 IP 地址

建议的操作：无需执行任何操作。

113017

错误消息：`%ASA-6-113017: AAA credentials rejected: reason = reason : local database: user = user:  user IP = xxx.xxx.xxx.xxx`

说明：与 IPsec 或 WebVPN 连接关联的用户的 AAA 事务由于错误而失败，或者由于违反策略而被拒绝。只有当 AAA 事务在本地用户数据库中进行而不是在外部 AAA 服务器中进行时，才会显示此事件。

- **Reason** - 请求被拒绝的原因的详细信息
- **user** - 与连接关联的用户名
- **user_ip** - 发起身份验证或授权请求的用户的 IP 地址

建议的操作：无需执行任何操作。

113018

错误消息：`%ASA-3-113018: User: user , Unsupported downloaded ACL Entry: ACL_entry , Action: action`

说明：从身份验证服务器下载了不支持格式的 ACL 条目。下表介绍消息值：

- **User** - 尝试登录的用户
- **ACL_entry** - 从身份验证服务器下载了不受支持的 ACL 条目
- **action** - 遇到不受支持的 ACL 条目时采取的操作

建议的操作：必须由管理员更改身份验证服务器上的 ACL 条目，以符合支持的 ACL 条目格式。

113019

错误消息：`%ASA-4-113019: Group = group , Username = username , IP = peer_address , Session disconnected.Session Type: type , Duration: duration , Bytes xmt: count , Bytes rcv: count , Reason: reason`

说明：指示空闲时间最长的用户断开连接的时间和原因。

- **group** - 组名称
- **username** - 用户名
- **IP** - 对等体地址
- **Session Type** - 会话类型（例如 IPsec 或 UDP）
- **duration** - 连接持续时间，以小时、分钟和秒为单位
- **Bytes xmt** - 传输的字节数
- *Bytes rcv* - 接收的字节数
- **reason** - 断开连接的原因

用户已请求

丢失运营商连接

服务丢失

空闲超时

超过最长时间限制

管理员重置

管理员重启

管理员关闭

端口错误

NAS 错误

NAS 请求

NAS 重启

不需要端口

连接被抢占。表示已超过允许的（相同用户）同时登录次数。要解决此问题，请增大同时登录数，或者要求用户仅使用给定的用户名和密码登录一次。

端口已暂挂

服务不可用

执行回调

用户错误

已请求主机

SA 已过期

IKE 删除

带宽管理错误

证书已过期

第 2 阶段不匹配

防火墙不匹配

对等体地址已更改

ACL 解析错误

第 2 阶段错误

配置错误

对等体已断开

内部错误

找不到加密映射策略

已发起 L2TP

VLAN 映射错误

NAC 策略错误

动态访问策略终止

不支持客户端类型

未知

建议的操作：除非终止原因表明存在问题，否则无需执行任何操作。

113020

错误消息： `%ASA-3-113020: Kerberos error: Clock skew with server ip_address greater than 300 seconds`

说明：由于Firepower威胁防御设备和服务器上的时钟相差超过五分钟（300秒），因此通过Kerberos服务器对 IPsec 或 WebVPN 用户进行身份验证失败。在这种情况下，系统拒绝连接尝试。

- *ip_address* - Kerberos 服务器的 IP 地址

建议的操作：同步 Firepower 威胁防御设备和 Kerberos 服务器上的时钟。

113021

错误消息：`%ASA-3-113021: Attempted console login failed.User username did NOT have appropriate Admin Rights.`

说明：用户尝试访问管理控制台，但被拒绝。

- *username* - 用户输入的用户名

建议的操作：如果用户是新添加的管理员权限用户，请检查该用户的服务类型（LOCAL或RADIUS身份验证服务器）是否设置为允许访问：

- nas-prompt - 允许以所需级别登录控制台并授予执行权限，但不允许（配置修改）访问
- admin - 允许所有访问权限，并且可通过命令权限进一步进行约束

否则，用户将以不适当的方式尝试访问管理控制台；采取的操作应符合公司针对这些事项的政策。

113022

错误消息：`%ASA-2-113022: AAA Marking RADIUS server servername in aaa-server group AAA-Using-DNS as FAILED`

说明：Firepower 威胁防御设备已尝试向 AAA 服务器发送身份验证、授权或记账请求，但未在配置的超时时间段内收到响应。AAA 服务器将被标记为有故障并从服务中删除。

- *protocol* - 身份验证协议的类型，可以是以下类型之一：

- RADIUS

- TACACS+

- NT

- RSA SecurID

- Kerberos

- LDAP

- *ip-addr* - AAA 服务器的 IP 地址

- *tag* - 服务器组名称

建议的操作：验证 AAA 服务器是否处于在线状态并且可从 Firepower 威胁防御设备访问。

113023

错误消息：`%ASA-2-113023: AAA Marking protocol server ip-addr in server group tag as ACTIVE`

说明：Firepower 威胁防御设备已重新激活之前标记为故障的 AAA 服务器。AAA 服务器现可用于服务 AAA 请求。

- *protocol* - 身份验证协议的类型，可以是以下类型之一：

- RADIUS

- TACACS+

- NT

- RSA SecurID

- Kerberos

- LDAP

- *ip-addr* - AAA 服务器的 IP 地址
- *tag* - 服务器组名称

建议的操作：无需执行任何操作。

113024

错误消息：`%ASA-5-113024: Group tg : Authenticating type connection from ip with username, user_name , from client certificate`

说明：预填用户名功能通过从客户端证书提取以用于 AAA 中的名称覆盖该用户名。

- *tg* - 隧道组
- *type* - 连接类型（SSL 客户端或无客户端）
- *ip* - 连接用户的 IP 地址
- *user_name* - 从客户端证书提取以用于 AAA 中的名称

建议的操作：无需执行任何操作。

113025

错误消息：`%ASA-5-113025: Group tg : fields  Could not authenticate connection type connection from ip`

说明：无法从证书中成功提取用户名。

- *tg* - 隧道组
- *fields* - 要搜索的 DN 字段
- *connection type* - 连接类型（SSL 客户端或无客户端）

- *ip* - 连接用户的 IP 地址

建议的操作：管理员应检查是否正确设置了 **authentication aaa certificate**、**ssl certificate-authentication** 和 **authorization-dn-attributes** 关键字。

113026

错误消息：`%ASA-4-113026: Error error while executing Lua script for group tunnel group`

说明：从客户端证书提取以用于 AAA 中的用户名时出错。只有在启用了 username-from-certificate use-script 选项时，才会生成此消息。

- *error* - 从 Lua 环境返回的错误字符串
- *tunnel group* - 尝试从证书中提取用户名的隧道组

建议的操作：检查 username-from-certificate use-script 选项使用的脚本是否存在错误。

113027

错误消息：`%ASA-2-113027: Error activating tunnel-group scripts`

说明：无法成功加载脚本文件。使用 username-from-certificate use-script 选项的隧道组无法正常工作。

建议的操作：管理员应使用 ASDM 检查脚本文件的错误。使用 **debug aaa** 命令获取可能有用的更详细的错误消息。

113028

错误消息：`%ASA-7-113028: Extraction of username from VPN client certificate has string.[Request num ]`

说明：来自证书的用户名的处理请求正在运行或已完成。

- *num* - 请求的 ID（指向光纤的指针的值），这是一个单调递增的数字。
- *string* - 状态消息，可以是下列选项之一：
  - 已请求
  - 已开始
  - 已完成，但包含错误
  - 已成功完成
  - 已完成

建议的操作：无需执行任何操作。

113029

错误消息：`%ASA-4-113029: Group group User user IP ipaddr Session could not be established: session limit of num reached`

说明：由于当前会话数超过了最大会话数，因此无法建立用户会话。

建议的操作：如果可能，请增加配置限制以创建负载均衡的集群。

113030

错误消息：`%ASA-4-113030: Group group User user IP ipaddr User ACL acl from AAA doesn't exist on the device, terminating connection.`

说明：在 Firepower 威胁防御设备上找不到指定的 ACL。

- **Group** - 组的名称
- **User** - 用户的名称
- **Ipaddr** - IP 地址
- **acl** - ACL 的名称

建议的操作：修改配置以添加指定的 ACL 或更正 ACL 名称。

113031

错误消息：`%ASA-4-113031: Group group User user IP ipaddr AnyConnect vpn-filter filter is an IPv6 ACL; ACL not applied.`

说明：要应用的 ACL 类型不正确。已通过 **vpn-filter** 命令将 IPv6 ACL 配置为 IPv4 ACL。

- *group* - 用户的组策略名称
- *user* - 用户名
- *ipaddr* - 用户的公共（未分配）IP 地址
- *filter* - VPN 过滤器的名称

建议的操作：验证 Firepower 威胁防御设备上的 VPN 过滤器和 IPv6 VPN 过滤器的配置以及 AAA (RADIUS) 服务器上的过滤器参数。确保指定了正确的 ACL 类型。

113032

错误消息：`%ASA-4-113032: Group group User user IP ipaddr AnyConnect ipv6-vpn-filter filter is an IPv4 ACL; ACL not applied.`

说明：要应用的 ACL 类型不正确。已通过 **ipv6-vpn-filter** 命令将 IPv4 ACL 配置为 IPv6 ACL。

- *group* - 用户的组策略名称
- *user* - 用户名
- *ipaddr* - 用户的公共（未分配）IP 地址
- *filter* - VPN 过滤器的名称

建议的操作：验证 Firepower 威胁防御设备上的 VPN 过滤器和 IPv6 VPN 过滤器的配置以及 AAA (RADIUS) 服务器上的过滤器参数。确保指定了正确的 ACL 类型。

113033

错误消息： `%ASA-6-113033: Group group User user IP ipaddr AnyConnect session not allowed.ACL parse error.`

说明： 由于未解析关联的ACL，因此系统不允许此组中的指定用户执行WebVPN会话。在更正此错误之前，系统将不允许用户通过 WebVPN 登录。

- *group* - 用户的组策略名称
- *user* - 用户名
- *ipaddr* - 用户的公共（未分配）IP 地址

建议的操作： 更正 WebVPN ACL。

113034

错误消息： `%ASA-4-113034: Group group User user IP ipaddr User ACL acl from AAA ignored, AV-PAIR ACL used instead.`

说明： 由于使用了思科 AV-PAIR ACL，因此系统未使用指定的 ACL。

- **Group** - 组的名称
- **User** - 用户的名称
- **Ipaddr** - IP 地址
- **acl** - ACL 的名称

建议的操作： 确定要使用的正确 ACL 并更正配置。

113035

错误消息： `%ASA-4-113035: Group group User user IP ipaddr Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.`

说明： 用户已通过 AnyConnect 客户端登录。未在全局启用 SVC 服务，或者 SVC 映像无效或已损坏。会话连接已终止。

- *group* - 用户正在尝试连接的组策略的名称
- *user* - 正在尝试连接的用户的名称
- *iaddrp* - 尝试连接的用户的 IP 地址

建议的操作： 使用 **svc-enable** 命令全局启用 SVC。通过使用 **svc image** 命令重新加载新映像，来验证 SVC 映像的完整性和版本。

113036

错误消息： `%ASA-4-113036: Group group User user IP ipaddr AAA parameter name value invalid.`

说明： 给定的参数具有无效值。该值未显示，因为它可能很长。

- **Group** - 组的名称

- **User** - 用户的名称
- **Ipadddr** - IP 地址
- **Name** - 参数的名称

建议的操作：修改配置以更正所指示的参数。

113037

错误消息：`%ASA-6-113037: Reboot pending, new sessions disabled.Denied user login.`

说明：用户无法登录到 WebVPN，因为 Firepower 威胁防御设备正在重启。

建议的操作：无需执行任何操作。

113038

错误消息：`%ASA-4-113038: Group group User user IP ipaddr Unable to create AnyConnect parent session.`

说明：由于资源问题，系统未为指定组中的用户创建 AnyConnect 会话。例如，用户可能已达到最大登录限制。

- **Group** - 组的名称
- **User** - 用户的名称
- **Ipadddr** - IP 地址

建议的操作：无需执行任何操作。

113039

错误消息：`%ASA-6-113039: Group group User user IP ipaddr AnyConnect parent session started.`

说明：系统已为此组中指定 IP 地址的用户启动 AnyConnect 会话。当用户通过 AnyConnect 登录页面登录时，AnyConnect 会话将启动。

- **Group** - 组的名称
- **User** - 用户的名称
- **Ipadddr** - IP 地址

建议的操作：无需执行任何操作。

113040

错误消息：`%ASA-4-113040: Terminating the VPN connection attempt from attempted group .Reason: This connection is group locked to locked group.`

说明：尝试连接的隧道组与组锁定中设置的隧道组不同。

- *attempted group* - 建立连接的隧道组
- *locked group* - 连接被锁定或受限制的隧道组

建议的操作：检查组策略中的组锁定值或用户属性。

113041

错误消息：`%ASA-4-113041: Redirect ACL configured for assigned IP does not exist on the device.`

说明：安装重定向 URL 并从 ISE 接收 ACL 时发生错误，但 Firepower 威胁防御设备上不存在重定向 ACL。

- *assigned IP* - 分配给该客户端的 IP 地址

建议的操作：在 Firepower 威胁防御设备上配置重定向 ACL。

113042

错误消息：`%ASA-4-113042: CoA: Non-HTTP connection from src_if :src_ip /src_port to dest_if :dest_ip /dest_port for user username at client_IP denied by redirect filter; only HTTP connections are supported for redirection.`

说明：对于 CoA 功能，重定向 ACL 过滤器会在重定向处理期间丢弃匹配的非 HTTP 流量，并提供有关已终止流量流的信息。

- *src_if*、*src_ip*、*src_port* - 该流的源接口、IP 地址和端口
- *dest_if*、*dest_ip*、*dest_port* - 该流的目的接口、IP 地址和端口
- *username* - 用户的名称
- *client_IP* - 客户端的 IP 地址

建议的操作：验证 Firepower 威胁防御设备上的重定向 ACL 配置。确保使用正确的过滤器来匹配要重定向的流量，并且不要阻止想要允许通过的流量。

ID 介于 114001 到 199027 之间的消息

本部分包括 ID 介于 114001 到 199027 之间的消息。

114001

错误消息：`%ASA-1-114001: Failed to initialize 4GE SSM I/O card (error error_string ).`

说明：由于 I2C 错误或交换机初始化错误，系统初始化 4GE SSM I/O 卡失败。

- *syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR
- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114002

错误消息：`%ASA-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error error_string ).`

说明：由于 I2C 错误或交换机初始化错误，系统在 4GE SSM I/O 卡中初始化 SFP 连接器失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114003

错误消息：`%ASA-1-114003: Failed to run cached commands in 4GE SSM I/O card (error error_string ).`

说明：由于 I2C 错误或交换机初始化错误，系统在 4GE SSM I/O 卡中运行缓存命令失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114004

错误消息：`%ASA-6-114004: 4GE SSM I/O Initialization start.`

说明：系统通知用户正在启动 4GE SSM I/O 初始化。

- >*syslog_id* - 消息标识符

建议的操作：无需执行任何操作。

114005

错误消息：`%ASA-6-114005: 4GE SSM I/O Initialization end.`

说明：系统通知用户 4GE SSM I/O 初始化已完成。

- >*syslog_id* - 消息标识符

建议的操作：无需执行任何操作。

114006

错误消息：`%ASA-3-114006: Failed to get port statistics in 4GE SSM I/O card (error` *`error_string`* `).`

说明：由于 I2C 错误或交换机初始化错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中获取端口统计数据失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114007

错误消息：`%ASA-3-114007: Failed to get current msr in 4GE SSM I/O card (error error_string ).`

说明：由于 I2C 错误或交换机初始化错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中获取当前模块状态注册信息失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114008

错误消息：`%ASA-3-114008: Failed to enable port after link is up in 4GE SSM I/O card due to either I2C serial bus access error or switch access error.`

说明：由于 I2C 串行总线访问错误或交换机访问错误，在 4GE SSM I/O 卡中检测到链路状态转换为“正常”后，Firepower 威胁防御设备启用端口失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114009

错误消息：`%ASA-3-114009: Failed to set multicast address in 4GE SSM I/O card (error error_string ).`

说明：由于 I2C 错误或交换机初始化错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中设置组播地址失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：

- I2C_BUS_TRANSACTION_ERROR
- I2C_CHKSUM_ERROR
- I2C_TIMEOUT_ERROR
- I2C_BUS_COLLISION_ERROR
- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114010

错误消息：`%ASA-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error` *`error_string`* `).`

说明：由于 I2C 错误或交换机初始化错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中设置组播硬件地址失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR
  - I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。

4. 如果问题仍然存在，请联系思科 TAC。

114011

错误消息：`%ASA-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error error_string ).`

说明：由于 I2C 错误或交换机初始化错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中删除组播地址失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114012

错误消息：`%ASA-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error error_string ).`

说明：由于 I2C 错误或交换机初始化错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中删除组播硬件地址失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114013

错误消息：`%ASA-3-114013: Failed to set mac address table in 4GE SSM I/O card (error error_string ).`

说明：由于 I2C 错误或交换机初始化错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中设置 MAC 地址表失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114014

错误消息： `%ASA-3-114014: Failed to set mac address in 4GE SSM I/O card (error error_string ).`

说明： 由于 I2C 错误或交换机初始化错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中设置 MAC 地址失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

建议的操作： 执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114015

错误消息： `%ASA-3-114015: Failed to set mode in 4GE SSM I/O card (error error_string ).`

说明： 由于 I2C 错误或交换机初始化错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中设置单独或混合模式失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114016

错误消息：`%ASA-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error error_string ).`

说明：由于 I2C 错误或交换机初始化错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中设置组播模式失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114017

错误消息：`%ASA-3-114017: Failed to get link status in 4GE SSM I/O card (error error_string ).`

说明：由于 I2C 串行总线访问错误或交换机访问错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中获取链路状态失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 通知系统管理员。
2. 记录并查看与该事件相关的消息和错误。
3. 重新启动 Firepower 威胁防御设备上运行的软件。
4. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
5. 如果问题仍然存在，请联系思科 TAC。

114018

错误消息：`%ASA-3-114018: Failed to set port speed in 4GE SSM I/O card (error error_string).`

说明：由于 I2C 错误或交换机初始化错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中设置端口速度失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114019

错误消息：`%ASA-3-114019: Failed to set media type in 4GE SSM I/O card (error error_string ).`

说明：由于 I2C 错误或交换机初始化错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中设置介质类型失败。

- >*syslog_id* - 消息标识符
- >*error_string* - I2C 串行总线错误或交换机访问错误，这是一个十进制错误代码。以下是 I2C 串行总线错误：

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114020

错误消息：`%ASA-3-114020: Port link speed is unknown in 4GE SSM I/O card.`

说明：Firepower 威胁防御设备无法在 4GE SSM I/O 卡中检测到端口链路速度。

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息。
2. 重置 4GE SSM I/O 卡，观察软件是否自动从该事件中恢复。
3. 如果软件没有自动恢复，请重新启动设备。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114021

错误消息：`%ASA-3-114021: Failed to set multicast address table in 4GE SSM I/O card due to error .`

说明：由于 I2C 串行总线访问错误或交换机访问错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中设置组播地址表失败。

- **Error** - 交换机访问错误（十进制错误代码）或 I2C 串行总线错误。可能的 I2C 串行总线错误包括：

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息。
2. 尝试重启 Firepower 威胁防御设备。
3. 如果软件没有自动恢复，请重新启动设备。关闭电源后，请确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。

114022

错误消息：`%ASA-3-114022: Failed to pass broadcast traffic in 4GE SSM I/O card due to error_string`

说明：由于交换机访问错误，Firepower 威胁防御设备在 4GE SSM I/O 卡中传递广播流量失败。

- *error_string* - 交换机访问错误，为十进制错误代码

建议的操作：执行以下步骤：

1. 记录与该事件相关的消息和错误。
2. 从紧凑式闪存卡中检索 ssm4ge_dump 文件并将其发送给思科 TAC。
3. 联系思科 TAC，提供在步骤 1 和 2 中收集的信息。

注释 4GE SSM 将自动重置并恢复。

114023

错误消息： `%ASA-3-114023: Failed to cache/flush mac table in 4GE SSM I/O card due to error_string .`

说明： 由于 I2C 串行总线访问错误或交换机访问错误，在 4GE SSM I/O 卡中缓存或刷新 MAC 表失败。此消息很少出现。

- **>error_string** - I2C 串行总线错误（请参阅第二个项目符号下列出的可能值）或交换机访问错误（这是一个十进制错误代码）。
- I2C 串行总线错误如下所示：

I2C_BUS_TRANSACTION_ERROR

I2C_CHKSUM_ERROR

I2C_TIMEOUT_ERROR

I2C_BUS_COLLISION_ERROR

I2C_HOST_BUSY_ERROR

I2C_UNPOPULATED_ERROR

I2C_SMBUS_UNSUPPORT

I2C_BYTE_COUNT_ERROR

I2C_DATA_PTR_ERROR

建议的操作： 执行以下步骤：

1. 记录与该事件相关的系统日志消息和错误。
2. 尝试使用软件重启 Firepower 威胁防御设备。
3. 通过电源重新启动 Firepower 威胁防御设备。

注释 关闭电源后，请确保等待几秒钟再打开电源。完成步骤1-3后，如果问题仍然存在，请联系思科TAC并提供步骤 1 中所述的信息。您可能需要对 Firepower 威胁防御设备执行 RMA 操作。

115000

错误消息： `%ASA-2-115000: Critical assertion in process: process name fiber: fiber name , component: component name , subcomponent: subcomponent name , file: filename , line: line number , cond: condition`

说明： 关键断言已取消，并且只用于已检查的构建版本的开发过程，而绝不会用于生产构建版本中。

- **process name** - 进程的名称

- *fiber name* - 光纤的名称
- *component name* - 指定组件的名称
- *subcomponent name* - 指定子组件的名称
- *filename* - 指定文件的名称
- *line number* - 指定线路的线路号
- *condition* - 指定的条件

建议的操作：应该对优先级较高的缺陷进行归档，调查断言原因并纠正该问题。

115001

错误消息：`%ASA-3-115001: Error in process: process name fiber: fiber name , component: component name , subcomponent: subcomponent name , file: filename , line: line number , cond: condition`

说明：错误断言已取消，并且只用于已检查的构建版本的开发过程，而绝不会用于生产构建版本中。

- **process name** - 进程的名称
- *fiber name* - 光纤的名称
- *component name* - 指定组件的名称
- *subcomponent name* - 指定子组件的名称
- *filename* - 指定文件的名称
- *line number* - 指定线路的线路号
- *condition* - 指定的条件

建议的操作：应该对优先级较高的缺陷进行归档，调查断言原因并解决该问题。

115002

错误消息：`%ASA-4-115002: Warning in process: process name fiber: fiber name , component: component name , subcomponent: subcomponent name , file: filename , line: line number , cond: condition`

说明：警告断言已取消，并且只用于已检查的构建版本的开发过程，而绝不会用于生产构建版本中。

- **process name** - 进程的名称
- *fiber name* - 光纤的名称
- *component name* - 指定组件的名称
- *subcomponent name* - 指定子组件的名称
- *filename* - 指定文件的名称
- *line number* - 指定线路的线路号
- *condition* - 指定的条件

建议的操作：应该调查断言的原因，如果发现问题，应将缺陷归档并纠正问题。

199001

错误消息： `%ASA-5-199001: Reload command executed from Telnet (remote IP_address ).`

说明： 已记录通过 **reload** 命令发起 Firepower 威胁防御设备重启的主机的地址。

建议的操作： 无需执行任何操作。

199002

错误消息： `%ASA-6-199002: startup completed.Beginning operation.`

说明： Firepower 威胁防御设备已完成其首次启动和闪存读取序列，并准备开始正常运行。

注释 您不能使用 no logging message 命令阻止此消息。

建议的操作： 无需执行任何操作。

199003

错误消息： `%ASA-6-199003: Reducing link MTU dec .`

说明： Firepower 威胁防御设备从使用比内部网络更大的 MTU 的外部网络收到数据包。然后，Firepower 威胁防御设备向外部主机发送 ICMP 消息以协商适当的 MTU。日志消息包括 ICMP 消息的序列号。

建议的操作： 无需执行任何操作。

199005

错误消息： `%ASA-6-199005: Startup begin`

说明： Firepower 威胁防御设备已启动。

建议的操作： 无需执行任何操作。

199010

错误消息： `%ASA-1-199010: Signal 11 caught in process/fiber(rtcli async executor process)/(rtcli async executor) at address 0xf132e03b, corrective action at 0xca1961a0`

说明： 系统已从严重错误中恢复。

建议的操作： 联系思科 TAC。

199011

错误消息： `%ASA-2-199011: Close on bad channel in process/fiber process/fiber , channel ID p , channel state s process/fiber  name of the process/fiber that caused the bad channel close operation.`

说明： 已检测到通道意外关闭状况。

- **p** - 通道 ID
- *process/fiber* - 导致通道意外关闭操作的进程/光纤的名称
- **s** - 通道状态

建议的操作： 联系思科 TAC 并提供日志文件。

199012

错误消息： `%ASA-1-1199012: Stack smash during new_stack_call in process/fiber process/fiber , call target f , stack size s , process/fiber  name of the process/fiber that caused the stack smash`

说明： 已检测到堆栈粉碎状况。

- **F** - new_stack_call 的目标
- *process/fiber* - 导致堆栈粉碎的进程/光纤的名称
- **s** - new_stack_call 中指定的新堆栈大小

建议的操作： 联系思科 TAC 并提供日志文件。

199013

错误消息： `%ASA-1-199013: syslog`

说明： 辅助进程生成了变量系统日志。

- **syslog** - 外部进程传递的确切警报系统日志

建议的操作： 联系思科 TAC。

199014

错误消息： `%ASA-2-199014: syslog`

说明： 辅助进程生成了变量系统日志。

- **syslog** - 外部进程传递的确切严重系统日志

建议的操作： 联系思科 TAC。

199015

错误消息： `%ASA-3-199015: syslog`

说明：辅助进程生成了变量系统日志。

- **syslog** - 外部进程传递的确切错误系统日志

建议的操作：联系思科 TAC。

199016

错误消息：`%ASA-4-199016: syslog`

说明：辅助进程生成了变量系统日志。

- **syslog** - 外部进程传递的确切警告系统日志

建议的操作：联系思科 TAC。

199017

错误消息：`%ASA-5-199017: syslog`

说明：辅助进程生成了变量系统日志。

- **syslog** - 外部进程传递的确切通知系统日志

建议的操作：无需执行任何操作。

199018

错误消息：`%ASA-6-199018: syslog`

说明：辅助进程生成了变量系统日志。

- **syslog** - 外部进程传递的确切信息系统日志

建议的操作：无需执行任何操作。

199019

错误消息：`%ASA-7-199019: syslog`

说明：辅助进程生成了变量系统日志。

- **syslog** - 外部进程传递的确切调试系统日志

建议的操作：无需执行任何操作。

199020

错误消息：`%ASA-2-199020: System memory utilization has reached X %.System will reload if memory usage reaches the configured trigger level of Y %.`

说明：系统内存利用率已达到系统内存监视程序工具配置值的 80%。

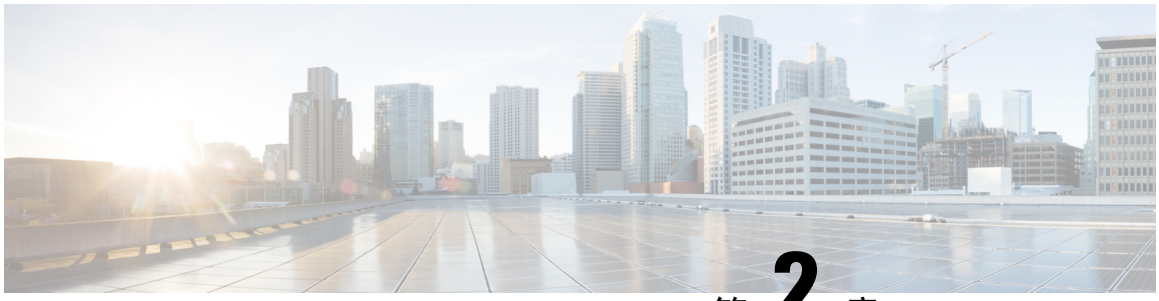
建议的操作：通减少流量负载、取消流量检测、减少ACL条目数等方式来降低系统内存利用率。如果怀疑是内存泄漏问题，请联系思科 TAC。

199021

错误消息：`%ASA-1-199021: System memory utilization has reached the configured watchdog trigger level of Y %.System will now reload`

说明：系统内存利用率已达到系统内存监视程序工具配置值的 100%。系统将自动重新加载。

建议的操作：通减少流量负载、取消流量检测、减少ACL条目数等方式来降低系统内存利用率。如果怀疑是内存泄漏问题，请联系思科 TAC。



第 2 章

系统日志消息 201002-219002

本章包含以下各节：

ID 介于 201002 到 210022 之间的消息

本章包含 ID 介于 201002 到 210022 之间的消息。

201002

错误消息： `%ASA-3-201002: Too many TCP connections on {static|xlate} global_address ! econns nconns`

说明： 已超出到指定全局地址的最大 TCP 连接数。

- econns - 最大初期连接数
- nconns - 针对静态或转换全局地址允许的最大连接数

建议的操作： 使用 **show static** 或 show nat 命令检查对静态地址连接施加的限制。可配置该限制。

201003

错误消息： `%ASA-2-201003: Embryonic limit exceeded nconns/elimit for outside_address/outside_port (global_address ) inside_address /inside_port on interface interface_name`

说明： 从带有指定的静态全局地址的指定外部地址到指定本地地址的初期连接数超出初期限制。当达到 Firepower 威胁防御设备的初期连接限制时，Firepower 威胁防御设备无论如何都会尝试接受这些连接，但会对它们施加时间限制。在这种情况下，即便Firepower威胁防御设备非常繁忙，也会允许部分连接成功。此消息表示出现了比消息 201002 更严重的过载，这可能是由于 SYN 攻击或大量的合法流量所导致的。

- nconns - 接收到的最大初期连接数
- *eimit* - 使用 static 或 nat 命令指定的最大初期连接数

建议的操作：使用 show static 命令检查对静态地址的初期连接施加的限制。

201004

错误消息：`%ASA-3-201004: Too many UDP connections on {static|xlate} global_address!udp connections limit`

说明：已超出到指定全局地址的最大 UDP 连接数。

- udp conn limit - 静态地址或转换允许的最大 UDP 连接数

建议的操作：使用 **show static** 或 show nat 命令检查对静态地址连接施加的限制。您可以配置该限制。

201005

错误消息：`%ASA-3-201005: FTP data connection failed for IP_address IP_address`

说明：由于内存不足，Firepower 威胁防御设备无法分配结构来跟踪 FTP 的数据连接。

建议的操作：减少内存使用量或购买额外内存。

201006

错误消息：`%ASA-3-201006: RCMD backconnection failed for IP_address/port.`

说明：由于内存不足，Firepower 威胁防御设备无法为 **rsh** 命令的入站标准输出预分配连接。

建议的操作：检查 **rsh** 客户端版本；Firepower 威胁防御设备仅支持 Berkeley **rsh** 客户端版本。您还可以减少内存使用量或购买额外内存。

201008

错误消息：`%ASA-3-201008: Disallowing new connections.`

说明：您已启用 TCP 系统日志消息传递，并且无法访问系统日志服务器。

建议的操作：禁用TCP系统日志消息传递。此外，确保系统日志服务器已启动并且您可以从Firepower威胁防御 控制台 Ping 通主机。然后，重新启动 TCP 系统消息日志记录以允许流量通过。

201009

错误消息：`%ASA-3-201009: TCP connection limit of number for host IP_address on interface_name exceeded`

说明：已超出通往指定静态地址的最大连接数。

- number - 针对该主机允许的最大连接数
- **IP_address** - 主机 IP 地址
- *interface_name* - 该主机所连接接口的名称

建议的操作：使用 show static 或 show nat 命令检查对地址连接施加的限制。可配置该限制。

201010

错误消息：`%ASA-6-201010: Embryonic connection limit exceeded econns/limit for dir packet from source_address/source_port to dest_address/dest_port on interface interface_name`

说明：由于超出了初期连接限制而导致尝试建立 TCP 连接的操作失败，其中该限制是使用针对某个流量类别的 **set connection embryonic-conn-max** MPC 命令配置的。

- **econns** - 与配置的流量类别关联的初期连接的当前计数。
- **limit** - 为该流量类别配置的初期连接限制
- **dir** - 输入：发起连接的第一个数据包是接口 **interface_name** 上的输入数据包；输出：发起连接的第一个数据包是接口 **interface_name** 上的输出数据包
- *source_address/source_port* - 源实际 IP 地址和发起连接的数据包的源端口
- *dest_address/dest_port* - 目的实际 IP 地址和发起连接的数据包的目的端口
- **interface_name** - 强制实施策略限制的接口的名称

建议的操作：无需执行任何操作。

201011

错误消息：`%ASA-3-201011: Connection limit exceeded cnt /limit for dir packet from sip /sport to dip /dport on interface if_name .`

说明：通过 Firepower 威胁防御设备的新连接导致超出至少一个已配置的最大连接限制。此消息既适用于使用 **static** 命令配置的连接限制，也适用于使用思科模块化策略框架配置的连接限制。直到一个现有连接断开，使得当前连接计数低于配置的最大值，系统才会允许通过 Firepower 威胁防御设备的新连接。

- *cnt* - 当前连接计数
- *limit* - 配置的连接限制
- *dir* - 流量方向（入站或出站）
- *sip* - 源实际 IP 地址
- *sport* - 源端口
- *dip* - 目的实际 IP 地址
- *dport* - 目的端口
- *if_name* - 接收流量的接口的名称

建议的操作：无需执行任何操作。

201012

错误消息：`%ASA-6-201012: Per-client embryonic connection limit exceeded curr num /limit for [input|output] packet from IP_address / port to ip /port on interface interface_name`

说明：由于超出了每客户端的初期连接限制，因此尝试建立 TCP 连接的操作失败。默认情况下，此消息的速率限制为每 10 秒 1 条。

- **curr num** - 当前数量
- **limit** - 配置的限制
- [input|output] - 接口 **interface_name** 上的输入或输出数据包
- **IP_address** - 实际 IP 地址
- **port** - TCP 或 UDP 端口
- **interface_name** - 在其中应用策略的接口的名称。

建议的操作：达到限制后，将由 Firepower 威胁防御设备代理任何新的连接请求，以防止 SYN 泛洪攻击。只有在客户端能够完成三次握手的情况下，Firepower 威胁防御设备才会连接到服务器。这通常不会影响最终用户或应用。但是，如果这给对较高数量的初期连接有合法需求的任何应用造成问题，则可以通过输入 **set connection per-client-embryonic-max** 命令来调整设置。

201013

错误消息：`%ASA-3-201013: Per-client connection limit exceeded curr num /limit for [input|output] packet from ip /port to ip /port on interface interface_name`

说明：由于超出了每客户端的连接限制，连接被拒绝。

- **curr num** - 当前数量
- **limit** - 配置的限制
- [input|output] - 接口 **interface_name** 上的输入或输出数据包
- **ip** - 实际 IP 地址
- **port** - TCP 或 UDP 端口
- **interface_name** - 在其中应用策略的接口的名称。

建议的操作：达到限制后，系统将以静默方式丢弃任何新的连接请求。通常，应用将重试连接，如果所有重试操作都失败，则将导致延迟甚至超时。如果应用对较高数量的初期连接有合法需求，则可以输入 **set connection per-client-max** 命令来调整设置。

202010

错误消息：`%ASA-3-202010: [NAT | PAT] pool exhausted for pool-name , port range [1-511 | 512-1023 | 1024-65535].Unable to create protocol connection from in-interface :src-ip /src-port to out-interface :dst-ip /dst-port`

说明

- *pool-name* - NAT 或 PAT 池的名称
- *protocol* - 用于创建连接的协议
- *in-interface* - 入口接口
- *src-ip* - 源 IP 地址
- *src-port* - 源端口
- *out-interface* - 出口接口

- *dest-ip* - 目的 IP 地址
- *dst-port* - 目的端口

Firepower 威胁防御设备没有更多可用的地址转换池。

建议的操作：使用 **show nat pool** 和 **show nat detail** 命令确定该池中所有地址和端口都已用完的原因。如果在正常条件下发生这种情况，则向 NAT/PAT 池添加更多的 IP 地址。

202016

错误消息：`%ASA-3-202016: "%d: Unable to pre-allocate SIP %s secondary channel for message" \ "from %s:%A/%d to %s:%A/%d with PAT and missing port information.\n"`

说明

当 SIP 应用生成 SDP 负载并将媒体端口设置为 0 时，您无法为此类无效端口请求分配 PAT 转换，并丢弃包含此系统日志的数据包。

建议的操作：无。这属于应用特定问题。

208005

错误消息：`%ASA-3-208005: (function:line_num) clear command return code`

说明：当Firepower威胁防御设备尝试清除闪存中的配置时，收到了非零值（内部错误）。此消息包含报告子例程文件名和行号。

建议的操作：出于性能原因，应将终端主机配置为不注入 IP 片段。此配置更改可能是由于 NFS 造成的。请将读取和写入大小设置为等于 NFS 的接口 MTU。

209003

错误消息：`%ASA-4-209003: Fragment database limit of number exceeded: src = source_address , dest = dest_address , proto = protocol , id = number`

说明：当前等待重组的 IP 片段过多。默认情况下，最大片段数为 200（要提高最大值，请参阅命令参考指南中的 **fragment size** 命令）。Firepower 威胁防御设备限制可以同时重组的 IP 片段的数量。此限制可防止在异常网络条件下Firepower威胁防御设备内存耗尽。通常情况下，分段流量应占总流量组合的一小部分。例外情况是在通过 UDP 传输 NFS 的网络环境中，大部分流量都是分段流量；如果此类流量通过 Firepower 威胁防御设备中继，则应考虑改用 TCP 传输 NFS。要防止分段，请参阅命令参考指南中的 **sysopt connection tcpmss bytes** 命令。

建议的操作：如果此消息仍然存在，则表示可能正在发生拒绝服务 (DoS) 攻击。联系远程对等体管理员或上游提供商。

209004

错误消息：`%ASA-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes : src = source_address , dest = dest_address , proto = protocol , id = number`

说明：IP 片段格式不正确。重组 IP 数据包的总大小超过了允许的最大大小，即 65,535 字节。

建议的操作：可能正在发生入侵事件。如果此消息仍然存在，请联系远程对等体管理员或上游提供商。

209005

错误消息：`%ASA-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.`

说明：Firepower 威胁防御设备不允许将任何 IP 数据包分为超过 24 个片段。有关详细信息，请参阅命令参考指南中的 **fragment** 命令。

建议的操作：可能正在发生入侵事件。如果此消息仍然存在，请联系远程对等体管理员或上游提供商。您可以使用 **fragment chain xxx interface_name** 命令更改每数据包的分段数。

210001

错误消息：`%ASA-3-210001: LU sw_module_name error = number`

说明：发生了状态故障切换错误。

建议的操作：如果通过 Firepower 威胁防御设备减少流量后，此错误仍然存在，则向思科 TAC 报告此错误。

210002

错误消息：`%ASA-3-210002: LU allocate block (bytes ) failed.`

说明：状态故障切换无法分配内存块，用以将状态信息传输到备用 Firepower 威胁防御设备。

建议的操作：使用 **show interface** 命令检查故障切换接口，以确保其传输正常。此外，使用 **show block** 命令检查当前块内存。如果任何内存块内的当前可用数量为 0，则重新加载 Firepower 威胁防御软件以恢复丢失的内存块。

210003

错误消息：`%ASA-3-210003: Unknown LU Object number`

说明：状态故障切换接收到不受支持的逻辑更新对象，并且无法处理此对象。这可能是由内存损坏、局域网传输和其他事件引起的。

建议的操作：如果只是偶尔遇到此错误，则不需要执行任何操作。如果频繁发生此错误，则检查状态故障切换链路的局域网连接情况。如果错误不是故障切换链路的局域网连接故障引起的，则确定是否有外部用户试图危害受保护的网络。此外，请检查客户端是否配置错误。

210005

错误消息： `%ASA-3-210005: LU allocate secondary (optional ) connection failed for protocol [TCP |UDP ] connection from ingress interface name :Real IP Address /Real Port to egress interface name :Real IP Address /Real Port`

说明： 状态故障切换无法分配备用设备上的新连接。这可能是由Firepower威胁防御设备内几乎没有或完全没有可用 RAM 内存引起的。

注释 系统日志消息中的 *secondary* 字段可选，仅在辅助连接条件下出现。

建议的操作： 使用 **show memory** 命令检查可用内存，以确保 Firepower 威胁防御设备有空余内存。如果没有可用内存，则向 Firepower 威胁防御设备 添加更多物理内存。

210006

错误消息： `%ASA-3-210006: LU look NAT for IP_address failed`

说明： 状态故障切换无法在备用设备上找到NAT 组的 IP 地址。主用和备用 Firepower 威胁防御设备可能不同步。

建议的操作： 在主用设备上使用 **write standby** 命令与备用设备同步系统内存。

210007

错误消息： `%ASA-3-210007: LU allocate xlate failed for type [static | dynamic ]-[NAT | PAT ] secondary(optional) protocol translation from ingress interface name :Real IP Address /real port (Mapped IP Address /Mapped Port ) to egress interface name :Real IP Address /Real Port (Mapped IP Address /Mapped Port )`

说明： 状态故障切换未能分配转换插槽记录。

建议的操作： 使用 **show memory** 命令检查可用内存，以确保 Firepower 威胁防御设备有空余内存。如果没有可用内存，则添加更多内存。

210008

错误消息： `%ASA-3-210008: LU no xlate for inside_address /inside_port outside_address /outside_port`

说明： Firepower 威胁防御设备找不到状态故障切换连接的转换插槽记录；因此，Firepower 威胁防御设备无法处理连接信息。

建议的操作： 在主用设备上使用 **write standby** 命令在主用设备与备用设备之间同步系统内存。

210010

错误消息： `%ASA-3-210010: LU make UDP connection for outside_address :outside_port inside_address :inside_port failed`

说明： 状态故障切换无法为 UDP 连接分配新记录。

建议的操作： 使用 **show memory** 命令检查可用内存，以确保 Firepower 威胁防御设备有空余内存。如果没有可用内存，则添加更多内存。

210020

错误消息： `%ASA-3-210020: LU PAT port port reserve failed`

说明： 状态故障切换无法分配正在使用的特定 PAT 地址。

建议的操作： 在主用设备上使用 **write standby** 命令在主用设备与备用设备之间同步系统内存。

210021

错误消息： `%ASA-3-210021: LU create static xlate global_address ifc interface_name failed`

说明： 状态故障切换无法创建转换插槽。

建议的操作： 在主用设备上输入 **write standby** 命令在主用设备与备用设备之间同步系统内存。

210022

错误消息： `%ASA-6-210022: LU missed number updates`

说明： 状态故障切换为发送到备用设备的每个记录分配一个序列号。当收到的记录序列号与最后更新记录顺序不一致时，系统会认为两者之间有信息丢失，因此发送此错误信息。

建议的操作： 除非 LAN 中断，否则请检查两个 Firepower 威胁防御设备上的可用内存，确保有足够的内存可用于处理状态信息。使用 **show failover** 命令监控状态信息更新质量。

ID 介于 211001 到 219002 之间的消息

本章包含 ID 介于 211001 到 219002 之间的消息。

211001

错误消息： `%ASA-3-211001: Memory allocation Error`

说明： Firepower 威胁防御设备未能分配系统内存。

建议的操作： 如果定期出现此消息，可以忽略。如果经常重复出现，请联系思科 TAC。

211003

错误消息：`%ASA-3-211003: Error in computed percentage CPU usage value`

说明：CPU 使用率百分比大于 100%。

建议的操作：如果定期出现此消息，可以忽略。如果经常重复出现，请联系思科 TAC。

211004

错误消息：`%ASA-1-211004: WARNING: Minimum Memory Requirement for ASA version ver not met for ASA image.min MB required, actual MB found.`

说明：Firepower 威胁防御设备不符合此版本的最小内存要求。

- **ver** - 运行中映像的版本号
- **min** - 运行已安装映像所需 RAM 的最小数量。
- **actual** -系统中当前安装的 RAM 的数量

建议的操作：安装所需数量的 RAM。

212001

错误消息：`%ASA-3-212001: Unable to open SNMP channel (UDP port port ) on interface interface_number , error code = code`

说明：Firepower 威胁防御设备无法从位于此接口上的 SNMP 管理站接收发送至 Firepower 威胁防御设备的 SNMP 请求。通过任何接口上 Firepower 威胁防御设备的 SNMP 流量都不受影响。错误代码如下：

- 错误代码 -1 表示 Firepower 威胁防御设备无法为此接口打开 SNMP 传输。当用户尝试将 SNMP 接受查询的端口更改为已用于另一项功能的端口时，可能发生此错误。在这种情况下，SNMP 使用的端口将重置为传入 SNMP 查询的默认端口 (UDP 161)。
- 错误代码 -2 表示 Firepower 威胁防御设备无法为此接口绑定 SNMP 传输。

建议的操作：在流量减小时 Firepower 威胁防御设备回收其一些资源后，为此接口重新输入 snmp-server host 命令。

212002

错误消息：`%ASA-3-212002: Unable to open SNMP trap channel (UDP port port ) on interface interface_number , error code = code`

说明：Firepower 威胁防御设备 无法将其 SNMP 陷阱从 Firepower 威胁防御设备发送到位于此接口上的 SNMP 管理站。通过任何接口上 Firepower 威胁防御设备的 SNMP 流量都不受影响。错误代码如下：

- 错误代码 -1 表示 Firepower 威胁防御设备无法为此接口打开 SNMP 陷阱传输。
- 错误代码 -2 表示 Firepower 威胁防御设备无法为此接口绑定 SNMP 陷阱传输。
- 错误代码 -3 表示 Firepower 威胁防御设备无法将陷阱通道设置为只写。

建议的操作：在流量减小时 Firepower 威胁防御设备回收其一些资源后，为此接口重新输入 snmp-server host 命令。

212003

错误消息：`%ASA-3-212003: Unable to receive an SNMP request on interface interface_number , error code = code , will try again.`

说明：接收发送至 Firepower 威胁防御设备上指定接口的 SNMP 请求时发生了内部错误。错误代码如下：

- 错误代码 -1 表示 Firepower 威胁防御设备找不到此接口支持的传输类型。
- 错误代码 -5 表示 Firepower 威胁防御设备未从此接口的 UDP 通道收到任何数据。
- 错误代码 -7 表示 Firepower 威胁防御设备收到了超出受支持缓冲区大小的传入请求。
- 错误代码 -14 表示 Firepower 威胁防御设备无法确定 UDP 通道的源 IP 地址。
- 错误代码 -22 表示 Firepower 威胁防御设备收到了无效参数。

建议的操作：无需执行任何操作。Firepower 威胁防御 SNMP 代理返回等待下一个 SNMP 请求。

212004

错误消息：`%ASA-3-212004: Unable to send an SNMP response to IP Address IP_address Port port interface interface_number , error code = code`

说明：从 Firepower 威胁防御设备向指定主机上的指定接口发送 SNMP 响应时发生了内部错误。错误代码如下：

- 错误代码 -1 表示 Firepower 威胁防御设备找不到此接口支持的传输类型。
- 错误代码 -2 表示 Firepower 威胁防御设备发送了无效参数。
- 错误代码 -3 表示 Firepower 威胁防御设备无法在 UDP 通道中设置目的 IP 地址。
- 错误代码 -4 表示 Firepower 威胁防御设备发送了超出受支持 UDP 分段大小的 PDU 长度。
- 错误代码 -5 表示 Firepower 威胁防御设备无法分配系统块来构建 PDU。

建议的操作：无需执行任何操作。

212005

错误消息：`%ASA-3-212005: incoming SNMP request (number bytes) on interface interface_name exceeds data buffer size, discarding this SNMP request.`

说明：发送至 Firepower 威胁防御设备的传入 SNMP 请求的长度超出用于在内部处理过程中存储请求的内部数据缓冲区的大小（512 字节）。Firepower 威胁防御设备无法处理此请求。通过任何接口上 Firepower 威胁防御设备的 SNMP 流量都不受影响。

建议的操作：确保 SNMP 管理站重新发送长度更小的请求。例如，尝试在一个请求中仅查询一个 MIB 变量，而不是多个 MIB 变量。可能需要修改 SNMP 管理器软件的配置。

212006

错误消息：`%ASA-3-212006: Dropping SNMP request from src_addr /src_port to ifc :dst_addr /dst_port because: reason username`

说明：出于以下原因，Firepower 威胁防御设备无法处理向它发送的 SNMP 请求：

- 找不到用户 - 在本地 SNMP 用户数据库中无法找到用户名。
- 用户名超出最大长度 - 在 PDU 中嵌入的用户名超出 SNMP RFC 允许的最大长度。
- 身份验证算法失败 - 密码无效导致身份验证失败或数据包使用了不正确的算法进行身份验证。
- 保密算法失败 - 密码无效导致保密失败或数据包使用了不正确的算法进行加密。
- 错误解密请求 - 解密用户请求的平台加密模块中发生了错误。
- 错误加密响应 - 加密用户响应或陷阱通知的平台加密模块中发生了错误。
- engineBoots 已达到最大值 - engineBoots 变量已达到最大允许值。有关详细信息，请参阅消息 212011。

注释 系统会在所列的每个原因后面显示用户名。

建议的操作：检查 Firepower 威胁防御 SNMP 服务器设置，并确认 NMS 配置正在使用预期用户、身份验证和加密设置。输入 **show crypto accelerator statistics** 命令，以隔离平台加密模块中的错误。

212009

错误消息：`%ASA-5-212009: Configuration request for SNMP group groupname failed.User username , reason .`

说明：用户已尝试更改 SNMP 服务器组配置。引用此组的一个或多个用户没有足够的设置来遵守请求的组更改。

- **groupname** - 表示组名称的字符串
- *username* - 表示用户名的字符串
- **reason** - 表示以下任一原因的字符串：

- 缺少身份验证密码 - 用户已尝试将身份验证添加到组，并且用户未指定身份验证密码

- 缺少隐私密码 - 用户已尝试将隐私添加到组，并且用户未指定加密密码

- 尝试删除引用组 - 用户已尝试删除有用户的组

建议的操作：用户必须在更改组或删除指示的用户前更新指示的用户配置，然后在更改组后重新添加配置。

212010

错误消息：`%ASA-3-212010: Configuration request for SNMP user %s failed.Host %s reason .`

说明：用户已尝试通过删除引用该用户的一个或多个主机来更改 SNMP 服务器用户配置。每个主机会生成一条消息。

- **%s** - 表示用户名或主机名的字符串
- *reason* - 表示以下原因的字符串：

- 尝试删除引用用户 - 要从主机中删除的用户的名称。

建议的操作：用户必须在更改用户前更新指示的主机配置或删除指定的主机，然后在更改用户后重新添加它们。

212011

错误消息：`%ASA-3-212011: SNMP engineBoots is set to maximum value.Reason : %s User intervention necessary.`

例如：

```
%ASA-3-212011: SNMP engineBoots is set to maximum value. Reason: error accessing persistent
 data. User intervention necessary.
```

说明：设备已重新启动 214783647 次，即 engineBoots 变量的最大允许值，或从闪存读取 持续值时发生了错误。engineBoots 值 存储在闪存中的 flash:/snmp/*ctx-name* 文件中，其中 *ctx-name* 是情景的名称。在单情景模式下，此文件的名称是 flash:/snmp/single_vf.在多情景模式下，管理情景文件的名称是 flash:/snmp/admin。重新启动期间，如果设备无法 对该文件执行读写操作，则 engineBoots 值将设置为 最大值。

- **%s** - 表示 engineBoots 值设置为最大允许值的原因的字符串。两个有效字符串分别是“设备重新启动”和“访问持久性数据时出错”。

建议的操作：对于第一个字符串，管理员必须删除 SNMP 第 3 版的所有用户，然后重新添加它们，以将 engineBoots 变量重置为 1。第 3 版的所有后续查询都将失败，直至所有用户都已删除。对于第二个字符串，管理员必须删除特定情景文件，然后删除 SNMP 版本的所有用户，再重新添加它们，以将其 engineBoots 变量重置为 1。第 3 版的所有后续查询都将失败，直至所有用户都已删除。

212012

错误消息：`%ASA-3-212012: Unable to write SNMP engine data to persistent storage.`

说明：SNMP 引擎数据写入文件 flash:/snmp/*context-name*。例如：在单情景模式下，数据将写入文件 flash:/snmp/single_vf。在多情景模式下的管理情景中，文件将写入目录 flash:/snmp/admin。此错误可能由未能创建 flash:/snmp 目录或 flash:/snmp/*context-name* 文件引起。此错误还可能由未能写入文件引起。

建议的操作：系统管理员应删除 flash:/snmp/*context-name* 文件，然后删除 SNMP 第 3 版的所有用户，再重新添加它们。此程序应重新创建 flash:/snmp/*context-name* 文件。如果问题仍然存在，系统管理员应尝试重新格式化闪存。

214001

错误消息：`%ASA-2-214001: Terminating manager session from IP_address on interface interface_name .Reason: incoming encrypted data (number bytes) longer than number  bytes`

说明：发送至 Firepower 威胁防御 管理端口的传入加密数据包指示数据包长度超出规定上限。这可能是恶意事件。Firepower 威胁防御设备将立即终止此管理连接。

建议的操作：确保管理连接已由思科安全策略管理器启动。

215001

错误消息：`%ASA-2-215001:Bad route_compress() call, sdb = number`

说明：发生了内部软件错误。

建议的操作：联系思科 TAC。

216001

错误消息：`%ASA-n-216001: internal error in: function : message`

说明：已发生正常操作期间不会出现的各种内部错误。严重性级别因消息原因而有所不同。

- **n -** 消息严重性
- **function -** 受影响组件
- **message -** 描述问题原因的消息

建议的操作：搜索针对特定文本消息的缺陷工具包，并尝试使用命令输出解释程序来解决问题。如果问题仍然存在，请联系思科 TAC。

216002

错误消息：`ASA-3-216002: Unexpected event (major: major_id , minor: minor_id ) received by task_string in function at line: line_num`

说明：某任务注册了事件通知，但是此任务无法处理特定事件。可以监视的事件包括与队列、布尔值和计时器服务相关联的事件。如果发生任何注册事件，则调度程序会唤醒任务来处理此事件。如果意外事件唤醒了任务，则会生成此消息，但是此消息不知道如何处理该事件。

如果事件保持未处理状态，则该事件会频繁唤醒此任务以确保受到处理，但是在正常条件下不会发生这种情形。出现此消息时，不一定意味着设备不可用，但必定意味着发生了异常情况，需要进行调查。

- *major_id* - 事件标识符
- *minor_id* - 事件标识符
- *task_string* - 任务为标识自身传递的自定义字符串
- *function* - 已接收意外事件的功能
- *line_num* - 代码中的行编号

建议的操作：如果问题仍然存在，请联系思科 TAC。

216003

错误消息： `%ASA-3-216003: Unrecognized timer timer_ptr , timer_id received by task_string in function at line: line_num`

说明： 意外计时器事件唤醒了任务，但任务不知道如何处理此事件。任务可使用调度程序注册一组计时器服务。如果任何计时器到期，则调度程序将唤醒任务以采取行动。如果无法识别的计时器事件唤醒此任务，则会生成此消息。

如果到期计时器保持未处理状态，则会不间断地唤醒任务以确保其受到处理，但是这并不可取。在正常条件下不会发生这种情形。出现此消息时，不一定意味着设备不可用，但必定意味着发生了异常情况，需要进行调查。

- *timer_ptr* - 指向计时器的指针
- *timer_id* - 计时器标识符
- *task_string* - 任务为标识自身传递的自定义字符串
- *function* - 已接收意外事件的功能
- *line_num* - 代码中的行编号

建议的操作： 如果问题仍然存在，请联系思科 TAC。

216004

错误： `%ASA-4-216004:prevented: error in function at file (line ) - stack trace`

说明： 已发生正常操作期间不会出现的内部逻辑错误。

- 错误 - 内部逻辑错误。可能的错误包括：

- 例外情况

- 取消引用空指针

- 阵列索引超出范围

- 缓冲区大小无效

- 根据输入写入

- 源和目的地重叠

- 日期无效

- 阵列索引访问偏移

- *function* - 生成错误的调用函数
- *file(line)* - 生成错误的文件和行编号
- *stack trace* - 完整的调用堆栈回溯，以调用函数开始。例如：(“0x001010a4 0x00304e58 0x00670060 0x00130b04”)

建议的操作： 如果问题仍然存在，请联系思科 TAC。

217001

错误： `%ASA-2-217001: No memory for string in string`

说明： 操作因内存不足而失败。

建议的操作： 如果有足够内存，请向思科 TAC 发送错误消息、配置和有关导致此错误的事件的任何详细信息。

218001

错误消息： `%ASA-2-218001: Failed Identification Test in slot# [fail #/res ].`

说明： Firepower 威胁防御设备的**插槽 #** 中的模块无法识别为正版思科产品。思科担保和支持程序仅适用于正版思科产品。如果思科确定出现支持问题的原因与非思科内存、SSM 模块、SSC 模块或其他模块有关，思科可能会拒绝提供担保或 SmartNet 等思科支持程序项下的支持。

建议的操作： 如果屡次出现此消息，则按照控制台或系统日志中的显示正确复制此消息。使用输出解释程序研究并尝试解决此错误。此外，还可以搜索缺陷工具包。如果问题仍然存在，请联系思科 TAC。

218002

错误消息： `%ASA-2-218002: Module (slot# ) is a registered proto-type for Cisco Lab use only, and not certified for live network operation.`

说明： 指定位置的硬件是来自思科实验室的原型模块。

建议的操作： 如果再次出现此消息，则按照控制台或系统日志中的显示正确复制此消息。使用输出解释程序研究并尝试解决此错误。此外，还可以搜索缺陷工具包。如果问题仍然存在，请联系思科 TAC。

218003

错误消息： `%ASA-2-218003: Module Version in slot# is obsolete.The module in slot = slot# is obsolete and must be returned via RMA to Cisco Manufacturing.If it is a lab unit, it must be returned to Proto Services for upgrade.`

说明： 检测到有过时硬件或已针对此模块运行 **show module** 命令。第一次显示此消息后，系统会每分钟再显示一次。

建议的操作： 如果屡次出现此消息，则按照控制台或系统日志中的显示正确复制此消息。使用输出解释程序研究并尝试解决此错误。此外，还可以搜索缺陷工具包。如果问题仍然存在，请联系思科 TAC。

218004

错误消息： `%ASA-2-218004: Failed Identification Test in slot# [fail# /res ]`

说明： 识别指定位置中的硬件时出现了问题。

建议的操作：如果屡次出现此消息，则按照控制台或系统日志中的显示正确复制此消息。使用输出解释程序研究并尝试解决此错误。此外，还可以搜索缺陷工具包。如果问题仍然存在，请联系思科 TAC。

218005

错误消息：`%ASA-2-218005: Inconsistency detected in the system information programmed in non-volatile memory`

说明：编入非易失性存储器程序中的系统信息不一致。如果Firepower威胁防御设备检测发现IDPROM内容与 ACT2 EEPROM 内容不完全相同，将在启动过程中生成此系统日志。由于 IDPROM 和 ACT2 EEPROM在制造过程中的编程内容完全相同，这种情况可能是由于制造错误或IDPROM内容遭篡改引起的。

建议的操作：如果屡次出现此消息，请收集 show tech-support 命令的输出，并联系思科 TAC。

219002

错误：`%ASA-3-219002: I2C_API_name error, slot = slot_number , device = device_number , address = address , byte count = count .Reason: reason_string`

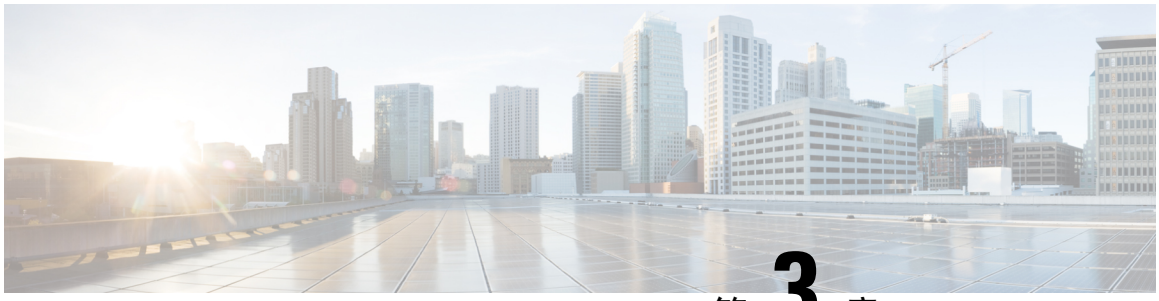
说明：I2C 串行总线 API 由于硬件或软件问题发生故障。

- *I2C_API_name* - 发生故障的 I2C API，可能是以下任意一个：
  - I2C_read_byte_w_wait()
  - I2C_read_word_w_wait()
  - I2C_read_block_w_wait()
  - I2C_write_byte_w_wait()
  - I2C_write_word_w_wait()
  - I2C_write_block_w_wait()
  - I2C_read_byte_w_suspend()
  - I2C_read_word_w_suspend()
  - I2C_read_block_w_suspend()
  - I2C_write_byte_w_suspend()
  - I2C_write_word_w_suspend()
  - I2C_write_block_w_suspend()
- *slot_number* - 发生生成此消息的I/O操作的插槽十六进制编号。插槽号无法作为机箱中插槽的唯一编号。两个不同插槽可能具有相同的 I2C 插槽号，这取决于机箱。此外，具体数值不一定小于或等于插槽数。此值取决于 I2C 硬件的接线方法。
- *device_number* - 用于执行 I/O 操作的插槽上设备的十六进制编号
- *address* - 发生 I/O 操作的设备的十六进制地址
- *byte_count* - I/O 操作十进制格式的字节计数
- *error_string* - 错误原因，可能是以下任意一项：
  - I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR
- I2C_TIMEOUT_ERROR
- I2C_BUS_COLLISION_ERROR
- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

建议的操作：执行以下步骤：

1. 记录并查看与该事件相关的消息和错误。如果此消息不持续出现并在几分钟后消失，则可能是因为 I2C 串行总线繁忙。
2. 重新启动 Firepower 威胁防御设备上运行的软件。
3. 为设备重新通电。关闭电源后，务必确保等待几秒钟再打开电源。
4. 如果问题仍然存在，请联系思科 TAC。



第 3 章

系统日志消息 302003-341011

本章包含以下各节：

ID 介于 302003 到 319004 之间的消息

本章包含 ID 介于 302003 到 319004 之间的消息。

302003

错误消息： `%ASA-6-302003: Built H245 connection for foreign_address` *`outside_address /outside_port`* `local_address` *`inside_address /inside_port`*

说明： 已启动从 **outside_address** 到 **inside_address** 的 H.245 连接。Firepower 威胁防御设备 已检测到使用英特尔互联网电话。外部端口 (*outside_port*) 仅显示在从 Firepower 威胁防御设备外部启动的连接上。本地端口值 (*inside_port*) 仅显示在内部接口上启动的连接上。

建议的操作： 无需执行任何操作。

302004

错误消息： `%ASA-6-302004: Pre-allocate H323 UDP backconnection for foreign_address` *`outside_address /outside_port`* `to local_address` *`inside_address /inside_port`*

说明： H.323 UDP 背面连接已从本地地址 (**inside_address**) 预分配到外部地址 (**outside_address**)。Firepower 威胁防御设备已检测到使用英特尔互联网电话。外部端口 (**outside_port**) 仅显示在从 Firepower 威胁防御设备外部启动的连接上。本地端口值 (**inside_port**) 仅显示在内部接口上启动的连接上。

建议的操作： 无需执行任何操作。

302010

错误消息： `%ASA-6-302010: connections in use, connections most used`

说明： 提供有关正在使用和最常用连接的数量的信息。

- **连接** - 连接数

建议的操作： 无需执行任何操作。

302012

错误消息： `%ASA-6-302012: Pre-allocate H225 Call Signalling Connection for faddr IP_address /port to laddr IP_address`

说明： H.225 辅助信道已预分配。

建议的操作： 无需执行任何操作。

302013

错误消息： `%ASA-6-302013: Built {inbound|outbound} TCP connection_id for interface :real-address /real-port (mapped-address/mapped-port ) [(idfw_user )] to interface :real-address /real-port (mapped-address/mapped-port ) [(idfw_user )] [(user )]`

说明： 两台主机之间创建了 TCP 连接插槽。

- **connection_id** - 唯一标识符
- **interface**, **real-address**, **real-port** - 实际套接字
- **mapped-address, mapped-port** - 映射套接字
- **user** - 用户的 AAA 名称
- *idfw_user* - 身份防火墙用户的名称

如果指定了入站，则从外部启动原控制连接。例如，对于 FTP 而言，如果原控制通道为入站，则所有数据传输通道均为入站。如果指定了出站，则从内部启动原控制连接。

建议的操作： 无需执行任何操作。

302014

错误消息： `%ASA-6-302014: Teardown TCP connection id for interface :real-address /real-port [(idfw_user )] to interface :real-address /real-port [(idfw_user )] duration hh:mm:ss bytes bytes [reason [from teardown-initiator]] [(user )]`

说明： 已删除两台主机之间的 TCP 连接。下表介绍消息值：

- **id** - 唯一标识符
- **interface, real-address, real-port** - 实际套接字
- **duration** - 连接持续时间

- **Bytes** - - 连接的数据传输
- **User** - 用户的 AAA 名称
- **idfw_user** - 身份防火墙用户的名称
- **reason** - 致使连接终止的操作。将 **reason** 变量设置为下表所列的一项 TCP 终止原因。
- **teardown-initiator** - 启动断开端的接口名称。

表 *2: TCP* 终止原因

原因	说明
连接超时	流由于不活动计时器到期而关闭时，连接结束。
拒绝终止	流被应用检查终止。
故障切换主设备关闭	故障切换对中的备用设备因从主用设备收到的消息删除了连接。
FIN 超时	等待最后确认 10 分钟后或半闭连接超时后强制终止。
流被检查关闭	流被检查功能终止。
流被 IPS 终止	流被 IPS 终止。
流被 IPS 重置	流被 IPS 重置。
流被 TCP 拦截终止	流被 TCP 拦截终止。
流超时	流超时。
流超时但已重置	流超时但已重置。
流为环回流	流为环回流。
因数据包注入释放创建的流	由于数据包跟踪器功能通过 Firepower 威胁防御设备发送了模拟数据包，因此建立了连接。
无效 SYN	SYN 数据包无效。
IPS 故障关闭	由于 IPS 卡出现故障，因此流已终止。
没有与区域关联的接口	“no nameif”或者“no zone-member”致使区域不存在任何接口成员后，流被断开。
没有有效邻接	Firepower 威胁防御设备尝试获取邻接但无法获取下一跳 MAC 地址时，此计数器递增。系统丢弃此数据包。
针孔超时	此计数器递增，指出 Firepower 威胁防御设备打开了辅助流，但是在超时间隔内没有数据包流经此流，因此删除了此流。一个辅助流示例是在成功协商 FTP 控制通道后创建的 FTP 数据通道。

原因	说明
路由变化	当 Firepower 威胁防御设备增设更低开销（更高指标）的路由时，即将到达的与新路由匹配的数据包将使其现有连接在达到用户配置超时（浮动连接）值后断开。后续数据包利用拥有更高指标的接口重建连接。要防止增设更低开销的路由影响活动流，可以将浮动连接配置超时值设置为 0:0:0。
SYN 控制	从错误端进行了反向通道初始化。
SYN 超时	30 秒后强制终止，等待三次握手完成。
TCP 重新传输故障	由于 TCP 重新传输故障致使连接终止。
TCP FIN	发生了正常关机程序。IP 地址遵从此原因。
TCP 无效 SYN	TCP SYN 数据包无效。
TCP 重置 - APPLIANCE	Firepower 威胁防御设备生成 TCP 重置时，流被关闭。
TCP 重置 - I	已从内部重置。
TCP 重置 - O	已从外部重置。
TCP 分段部分重叠	已检测到部分重叠分段。
TCP 窗口大小意外变化	由于 TCP 窗口大小变化，连接被终止。
隧道已关闭	由于隧道关闭，流被终止。
拒绝取消授权	URL 过滤器已拒绝授权。
未知	发生未知错误。
转换清除	命令行已删除。

建议的操作：无需执行任何操作。

302015

错误消息：`%ASA-6-302015: Built {inbound|outbound} UDP connection number for interface_name :real_address /real_port (mapped_address /mapped_port ) [(idfw_user )] to interface_name :real_address /real_port (mapped_address /mapped_port )[(idfw_user )] [(user )]`

说明：两台主机之间创建了 UDP 连接插槽。下表介绍消息值：

- **number** - 唯一标识符
- **interface, real_address, real_port** - 实际套接字
- **mapped_address and mapped_port** - 映射套接字
- **user** - 用户的 AAA 名称

- *idfw_user* - 身份防火墙用户的名称

如果指定了入站，则从外部启动原控制连接。例如，对于UDP而言，如果原控制通道为入站，则所有数据传输通道均为入站。如果指定了出站，则从内部启动原控制连接。

建议的操作：无需执行任何操作。

302016

错误消息：`%ASA-6-302016: Teardown UDP connection number for interface :real-address /real-port [(idfw_user )] to interface :real-address /real-port [(idfw_user )] duration hh :mm :ss bytes bytes [(user )]`

说明：已删除两台主机之间的 UDP 连接插槽。下表介绍消息值：

- **number** - 唯一标识符
- **interface, real_address, real_port** - 实际套接字
- **time** - 连接生命周期
- **bytes** - 连接的数据传输
- **id** - 唯一标识符
- **interface, real-address, real-port** - 实际套接字
- **duration** - 连接生命周期
- **bytes** - 连接的数据传输
- **user** - 用户的 AAA 名称
- *idfw_user* - 身份防火墙用户的名称

建议的操作：无需执行任何操作。

302017

错误消息：`%ASA-6-302017: Built {inbound|outbound} GRE connection id from interface :real_address (translated_address ) [(idfw_user )] to interface :real_address /real_cid (translated_address /translated_cid ) [(idfw_user )] [(user )`

说明：两台主机之间创建了 GRE 连接插槽。**id** 是指唯一标识符。**interface, real_address, real_cid** 元组标识两个单工 PPTP GRE 流的其中一个。括号中的 **translated_address**, **translated_cid** 元组标识 NAT 的转换值。如果指示入站，则连接仅可用于入站。如果指示出站，则连接仅可用于出站。下表介绍消息值：

- **id** - 标识连接的唯一编号
- **inbound** - 控制连接用于入站 PPTP GRE 流
- **outbound** - 控制连接用于出站 PPTP GRE 流
- **interface_name** - 接口名称
- **real_address** - 实际主机的 IP 地址
- **real_cid** - 有关连接的未转换调用 ID
- **translated_address** - 转换后的 IP 地址
- **translated_cid** - 已转换调用

- **user** - AAA 用户名
- *idfw_user* - 身份防火墙用户的名称

建议的操作：无需执行任何操作。

302018

错误消息：`%ASA-6-302018: Teardown GRE connection id from interface :real_address (translated_address ) [(idfw_user )] to interface :real_address /real_cid (translated_address /translated_cid ) [(idfw_user )] duration hh :mm :ss bytes bytes [(user )]`

说明：已删除两台主机之间的 GRE 连接插槽。**interface, real_address, real_port** 元组标识实际套接字。**duration** 标识连接生命周期。下表介绍消息值：

- **id** - 标识连接的唯一编号
- **interface** - 接口名称
- **real_address** - 实际主机的 IP 地址
- **real_port** - 实际主机的端口号。
- **hh:mm:ss** - 采用小时:分钟:秒钟格式的时间
- **bytes** - GRE 会话中传输的 PPP 字节数
- **reason** - 连接终止原因
- **user** - AAA 用户名
- *idfw_user* - 身份防火墙用户的名称

建议的操作：无需执行任何操作。

302019

错误消息：`%ASA-3-302019: H.323 library_name ASN Library failed to initialize, error code number`

说明：Firepower 威胁防御设备用于解码 H.323 消息的指定 ASN 库初始化失败；Firepower 威胁防御设备无法解码或检查正在接收的 H.323 数据包。Firepower 威胁防御设备允许 H.323 数据包通过而无需任何修改。收到下一个 H.323 消息时，Firepower 威胁防御设备将尝试重新初始化此库。

建议的操作：如果此消息一致针对特定库而生成，请联系思科 TAC 并向其提供所有日志消息（最好带时间戳）。

302020

错误消息：`%ASA-6-302020: Built {in | out} bound ICMP connection for faddr {faddr | icmp_seq_num } [(idfw_user )] gaddr {gaddr | cmp_type } laddr laddr [(idfw_user )] type {type } code {code }`

说明：当使用 inspect icmp 命令启用状态 ICMP 时，系统在快速路径中建立了 ICMP 会话。下表介绍消息值：

- *faddr* - 指定外部主机的 IP 地址

- *gaddr* - 指定全局主机的 IP 地址
- *laddr* - 指定本地主机的 IP 地址
- *idfw_user* - 身份防火墙用户的名称
- *user* - 与启动连接的主机相关联的用户名
- *Type* - 指定 ICMP 类型
- *code* - 指定 ICMP 代码

建议的操作：无需执行任何操作。

302021

错误代码：`%ASA-6-302021: Teardown ICMP connection for faddr {faddr | icmp_seq_num } [(idfw_user )] gaddr {gaddr | cmp_type } laddr laddr [(idfw_user )] (981) type {type } code {code }`

说明：当使用 inspect icmp 命令启用状态 ICMP 时，系统在快速路径中删除了 ICMP 会话。下表介绍消息值：

- *faddr* - 指定外部主机的 IP 地址
- *gaddr* - 指定全局主机的 IP 地址
- *laddr* - 指定本地主机的 IP 地址
- *idfw_user* - 身份防火墙用户的名称
- *user* - 与启动连接的主机相关联的用户名
- *(981) type* - 指定 ICMP 类型
- *code* - 指定 ICMP 代码 (981)

建议的操作：无需执行任何操作。

302022

错误消息：`%ASA-6-302022: Built role stub TCP connection for interface :real-address /real-port (mapped-address /mapped-port ) to interface :real-address /real-port (mapped-address /mapped-port)`

说明：已创建 TCP 导向器/备份/转发程序流。

建议的操作：无需执行任何操作。

302023

错误消息：`%ASA-6-302023: Teardown stub TCP connection for interface :real-address /real-port to interface :real-address /real-port duration hh:mm:ss forwarded bytes bytes reason`

说明：已断开 TCP 导向器/备份/转发程序流。

建议的操作：无需执行任何操作。

302024

错误消息： `%ASA-6-302024: Built role stub UDP connection for interface :real-address /real-port (mapped-address /mapped-port ) to interface :real-address /real-port (mapped-address /mapped-port )`

说明： 已创建 UDP 导向器/备份/转发程序流。

建议的操作： 无需执行任何操作。

302025

错误消息： `%ASA-6-302025: Teardown stub UDP connection for interface :real-address /real-port to interface :real-address /real-port duration hh:mm:ss forwarded bytes bytes reason`

说明： 已断开 UDP 导向器/备份/转发程序流。

建议的操作： 无需执行任何操作。

302026

错误消息： `%ASA-6-302026: Built role stub ICMP connection for interface :real-address /real-port (mapped-address ) to interface :real-address /real-port (mapped-address )`

说明： 已创建 ICMP 导向器/备份/转发程序流。

建议的操作： 无需执行任何操作。

302027

错误消息： `%ASA-6-302027: Teardown stub ICMP connection for interface :real-address /real-port to interface :real-address /real-port duration hh:mm:ss forwarded bytes bytes reason`

说明： 已断开 ICMP 导向器/备份/转发程序流。

建议的操作： 无需执行任何操作。

302033

错误消息： `%ASA-6-302033:Pre-allocated H323 GUP Connection for faddr interface :foreign address /foreign-port to laddr interface :local-address /local-port`

说明： 已启动从外部地址到本地地址的GUP连接。远端端口（外部端口）仅显示在从安全设备外部启动的连接上。本地端口值（内部端口）仅显示在内部接口上启动的连接上。

- **interface** - 接口名称
- *foreign-address* - 外部主机的 IP 地址
- *foreign-port* - 外部主机的端口号
- *local-address* - 本地主机的 IP 地址
- *local-port* - 本地主机的端口号

建议的操作：无需执行任何操作。

302034

错误消息：`%ASA-4-302034: Unable to pre-allocate H323 GUP Connection for faddr interface :foreign address /foreign-port to laddr interface :local-address /local-port`

说明：启动连接时，模块未能分配 RAM 系统内存或没有更多可用的地址转换插槽。

- **interface** - 接口名称
- *foreign-address* - 外部主机的 IP 地址
- *foreign-port* - 外部主机的端口号
- *local-address* - 本地主机的 IP 地址
- *local-port* - 本地主机的端口号

建议的操作：如果定期出现此消息，可以忽略。如果经常重复出现，请联系思科 TAC。您可以对比内部网络客户端数量来检查全局池的大小。或者，缩短转换和连接的超时间隔。此消息还可能由内存不足引起；请尝试降低内存使用量，或购买更多内存。

302302

错误消息：`%ASA-3-302302: ACL = deny; no sa created`

说明：已发生 IPsec 代理不匹配问题。协商 SA 的代理主机对应于拒绝访问列表命令策略。

建议的操作：检查配置中的访问列表命令语句。与对等体管理员联系。

302303

错误消息：`%ASA-6-302303: Built TCP state-bypass connection conn_id from initiator_interface :real_ip /real_port (mapped_ip /mapped_port ) to responder_interface :real_ip /real_port (mapped_ip /mapped_port )`

说明：新 TCP 连接已创建，并且此连接是 TCP 状态绕行连接。这种连接类型绕过所有 TCP 状态检查以及其他安全检查和检测。

建议的操作：如果您需要通过所有正常的TCP状态检查以及所有其他安全检查和检测来保护TCP流量，您可以使用 **no set connection advanced-options tcp-state-bypass** 命令为 TCP 流量禁用此项功能。

302304

错误消息：`%ASA-6-302304: Teardown TCP state-bypass connection conn_id from initiator_interface :ip/port to responder_interface :ip/port duration , bytes , teardown reason .`

说明：新 TCP 连接已断开，并且此连接是 TCP 状态绕行连接。这种连接类型绕过所有 TCP 状态检查以及其他安全检查和检测。

- *duration* - TCP 连接的持续时间
- *bytes* - 通过 TCP 连接传输的字节总数

- *teardown reason* - TCP 连接断开的原因

建议的操作：如果您需要通过所有正常的TCP状态检查以及所有其他安全检查和检测来保护TCP流量，您可以使用 **no set connection advanced-options tcp-state-bypass** 命令为 TCP 流量禁用此项功能。

303002

错误消息：`%ASA-6-303002: FTP connection from src_ifc :src_ip /src_port to dst_ifc :dst_ip /dst_port , user username action file filename`

说明：客户端已从 FTP 服务器上传或下载文件。

- **src_ifc** - 客户端所在接口。
- **src_ip** - 客户端的 IP 地址。
- **src_port** - 客户端端口。
- **dst_ifc** - 服务器所在接口。
- **dst_ip** - FTP 服务器的 IP 地址。
- **dst_port** - 服务器端口。
- **username** - FTP 用户名。
- **action** - 存储或检索操作。
- **Filename** - 存储或检索的文件。

建议的操作：无需执行任何操作。

303004

错误消息：`%ASA-5-303004: FTP cmd_string command unsupported - failed strict inspection, terminating connection from source_interface :source_address /source_port to dest_interface :dest_address/dest_interface`

说明：已对 FTP 流量执行严格 FTP 检测，并且 FTP 请求消息包含设备无法识别的命令。

建议的操作：无需执行任何操作。

303005

错误消息：`%ASA-5-303005: Strict FTP inspection matched match_string in policy-map policy-name , action_string from src_ifc :sip /sport to dest_ifc :dip /dport`

说明：当 FTP 检测匹配以下任何配置值：文件名、文件类型、请求命令、服务器或用户名时，系统执行此消息中 *action_string* 指定的操作。

- *match_string* - 策略映射中的匹配语句
- **policy-name** - 匹配的策略映射
- **action_string** - 要采取的操作；例如重置连接
- **src_ifc** - 源接口名称
- **sip** - 源 IP 地址
- **sport** - 源端口

- **dest_ifc** - 目的接口名称
- **dip** - 目的 IP 地址
- **dport** - 目的端口

建议的操作：无需执行任何操作。

305006

错误消息：`%ASA-3-305006: {outbound static|identity|portmap|regular) translation creation failed for protocol src interface_name:source_address/source_port [(idfw_user )] dst interface_name:dest_address/dest_port [(idfw_user )]`

说明：协议（UDP、TCP 或 ICMP）通过 Firepower 威胁防御设备创建转换失败。Firepower 威胁防御设备不允许发送至网络或广播地址的数据包通过。Firepower威胁防御设备为静态命令明确标识的地址提供此项检查。对于入站流量，Firepower 威胁防御设备拒绝转换标识为网络或广播地址的 IP 地址。

Firepower 威胁防御设备不会将 PAT 应用于所有 ICMP 消息类型；它仅适用于 PAT ICMP 回应和回应应答数据包（类型 8 和 0）。具体而言，仅 ICMP 回应或回应应答数据包创建 PAT 转换。因此，当丢弃其他 ICMP 消息类型时，系统将生成此消息。

Firepower 威胁防御设备使用全局 IP 地址和已配置静态命令中的掩码来区分常规 IP 地址和网络或广播 IP 地址。如果全局 IP 地址是有效的网络地址并带有匹配的网络掩码，则 Firepower 威胁防御设备不会使用入站数据包为网络或广播 IP 地址创建转换。

例如：

```
static (inside,outside) 10.2.2.128 10.1.1.128 netmask 255.255.255.128
```

Firepower 威胁防御设备将全局地址 10.2.2.128 视为网络地址作出响应，将 10.2.2.255 视为广播地址作出响应。在无现有转换的情况下，Firepower 威胁防御设备会拒绝发送至 10.2.2.128 或 10.2.2.255 的入站数据包，并记录此消息。

当可疑 IP 地址是主机 IP 地址时，在子网 **static** 命令前面使用主机掩码配置单独的静态命令（静态命令的第一条匹配规则）。以下 **static** 命令使 Firepower 威胁防御设备将 10.2.2.128 视为主机地址作出相应：

```
static (inside,outside) 10.2.2.128 10.2.2.128 netmask 255.255.255.255static (inside,outside)
 10.2.2.128 10.2.2.128 netmask 255.255.255.128
```

转换可能由从内部主机开始的流量使用相应 IP 地址创建。由于 Firepower 威胁防御设备将网络或广播 IP 地址视为包含重叠子网静态配置的主机 IP 地址，因此两个 **static** 命令的网络地址转换必须相同。

建议的操作：无需执行任何操作。

305009

错误消息：`%ASA-6-305009: Built {dynamic|static} translation from interface_name [(acl-name)]:real_address [(idfw_user )] to interface_name :mapped_address`

说明：已创建地址转换插槽。此插槽将源地址从本地端转换到全局端。相反地，此插槽将目的地址从全局端转换到本地端。

建议的操作：无需执行任何操作。

305010

错误消息：`%ASA-6-305010: Teardown {dynamic|static} translation from interface_name :real_address [(idfw_user )] to interface_name :mapped_address duration time`

说明：已删除地址转换插槽。

建议的操作：无需执行任何操作。

305011

错误消息：`%ASA-6-305011: Built {dynamic|static} {TCP|UDP|ICMP} translation from interface_name :real_address/real_port [(idfw_user )] to interface_name :mapped_address/mapped_port`

说明：已创建 TCP、UDP 或 ICMP 地址转换插槽。此插槽将源套接字从本地端转换到全局端。相反地，此插槽将目的套接字从全局端转换到本地端。

建议的操作：无需执行任何操作。

305012

错误消息：`%ASA-6-305012: Teardown {dynamic|static} {TCP|UDP|ICMP} translation from interface_name [(acl-name )]:real_address /{real_port |real_ICMP_ID } [(idfw_user )] to interface_name :mapped_address /{mapped_port |mapped_ICMP_ID } duration time`

说明：已删除地址转换插槽。

建议的操作：无需执行任何操作。

305013

错误消息：`%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection protocol src interface_name :source_address /source_port [(idfw_user )] dst interface_name :dst_address /dst_port [(idfw_user )] denied due to NAT reverse path failure.`

说明：已拒绝尝试连接到使用实际地址的映射主机。

建议的操作：与使用NAT的主机不在相同接口上时，使用映射地址而不是实际地址连接到主机。此外，如果此应用嵌入 IP 地址，则启用 **inspect** 命令。

305014

错误消息：`%ASA-6-305014: %d: Allocated %s block of ports for translation from %s:%B to %s:%B/%d-%d\n.`

说明：配置 CGNAT“块分配”时，系统将生成这条有关新端口块分配的系统日志。

建议的操作：无。

305016

错误消息：`%ASA-3-305016: Unable to create protocol connection from real_interface :real_host_ip /real_source_port to real_dest_interface :real_dest_ip /real_dest_port due to reason .`

说明：主机已达到每台主机最大端口块限值或端口块已耗尽。

- *reason* - 可能是以下任一原因：
  - 已达到每台主机的 PAT 端口块限值
  - PAT 池中的端口块耗尽

建议的操作：对于达到每台主机的 PAT 端口块限值的情形，请输入以下命令查看每台主机的最大块限值：

```
xlate block-allocation maximum-per-host 4
```

对于 PAT 池中端口块耗尽的情形，建议扩大池大小。同时，输入以下命令，查看块大小：

```
xlate block-allocation size 512
```

308001

错误消息：`%ASA-6-308001: console enable password incorrect for number tries (from IP_address )`

说明：这是一条 Firepower 威胁防御管理消息。用户在尝试进入特权模式时错误输入密码达到指定次数后，系统将显示此消息。最大尝试次数是三次。

建议的操作：验证密码，然后重试。

308002

错误消息：`%ASA-4-308002: static global_address inside_address netmask netmask overlapped with global_address inside_address`

说明：一个或多个静态命令语句中的 IP 地址重叠。**global_address** 是全局地址，即较低安全性接口上的地址；**inside_address** 是本地地址，即较高安全级别接口上的地址。

建议的操作：使用 show static 命令查看配置中的 static 命令语句并修复重叠命令。最常见的重叠现象是指定网络地址（例如 10.1.1.0），并且在另一个 static 命令中指定此范围内的主机（例如 10.1.1.5）。

311001

错误消息：`%ASA-6-311001: LU loading standby start`

说明：当备用Firepower威胁防御设备首次联机时，状态故障切换更新信息就已发送到备用Firepower威胁防御设备。

建议的操作：无需执行任何操作。

311002

错误消息：`%ASA-6-311002: LU loading standby end`

说明：状态故障切换更新信息停止发送到备用 Firepower 威胁防御设备。

建议的操作：无需执行任何操作。

311003

错误消息：`%ASA-6-311003: LU recv thread up`

说明：已从备用 Firepower 威胁防御设备收到更新确认消息。

建议的操作：无需执行任何操作。

311004

错误消息：`%ASA-6-311004: LU xmit thread up`

说明：状态故障切换更新已传输到备用 Firepower 威胁防御设备。

建议的操作：无需执行任何操作。

312001

错误消息：`%ASA-6-312001: RIP hdr failed from IP_address : cmd=string , version=number domain=string on interface interface_name`

说明：Firepower威胁防御设备收到了一条不同于应答的包含操作代码的RIP消息，此消息的版本号不同于此接口上的预期版本号，并且路由域条目数值为非零值。另一台 RIP 设备可能配置不正确，无法与 Firepower 威胁防御设备通信。

建议的操作：无需执行任何操作。

313001

错误消息：`%ASA-3-313001: Denied ICMP type=number , code=code from IP_address on interface interface_name`

说明：使用带访问列表的 icmp 命令时，如果第一个匹配的条目是允许条目，则 ICMP 数据包将继续处理。如果第一个匹配的条目是拒绝条目或者条目不匹配，Firepower 威胁防御设备会丢弃 ICMP 数据包并生成此消息。**icmp** 命令启用或禁用对接口执行 ping 操作。禁用 ping 命令后，在网络上无法检测到 Firepower 威胁防御设备。此功能也称为可配置的代理 ping。

建议的操作：联系对等体管理员。

313004

错误消息：`%ASA-4-313004:Denied ICMP type=icmp_type , from source_address on interface interface_name to dest_address :no matching session`

说明：ICMP 数据包已被 Firepower 威胁防御设备丢弃，这是因为状态 ICMP 功能增设了安全检查，通常是不包含跨 Firepower 威胁防御设备传递的有效回应请求的 ICMP 回应应答，或与已在 Firepower 威胁防御设备中建立的任何 TCP、UDP 或 ICMP 会话无关的 ICMP 错误消息。

建议的操作：无需执行任何操作。

313005

错误消息：`%ASA-4-313005: No matching connection for ICMP error message: icmp_msg_info on interface_name interface.Original IP payload: embedded_frame_info icmp_msg_info = icmp src src_interface_name :src_address [([idfw_user | FQDN_string], sg_info)] dst dest_interface_name :dest_address [([idfw_user | FQDN_string], sg_info)] (type icmp_type, code icmp_code) embedded_frame_info = prot src source_address /source_port [([idfw_user | FQDN_string], sg_info)] dst dest_address /dest_port [(idfw_user |FQDN_string), sg_info]`

说明：由于 ICMP 错误消息与已在 Firepower 威胁防御设备中建立的任何会话无关，因此 Firepower 威胁防御设备已丢弃 ICMP 错误数据包。

建议的操作：如果是因为受到攻击，则可以使用 ACL 拒绝主机。

313008

错误消息：`%ASA-3-313008: Denied ICMPv6 type=number , code=code from IP_address on interface interface_name`

说明：使用带访问列表的 **icmp** 命令时，如果第一个匹配的条目是允许条目，则 ICMPv6 数据包将继续处理。如果第一个匹配的条目是拒绝条目或者条目不匹配，Firepower 威胁防御设备会丢弃 ICMPv6 数据包并生成此消息。

icmp 命令启用或禁用对接口执行 ping 操作。禁用 ping 命令时，无法在网络上检测到 Firepower 威胁防御设备。此功能也称为“可配置的代理 ping”。

建议的操作：联系对等体管理员。

313009

错误消息：`%ASA-4-313009: Denied invalid ICMP code icmp-code , for src-ifc :src-address /src-port (mapped-src-address/mapped-src-port) to dest-ifc :dest-address /dest-port (mapped-dest-address/mapped-dest-port) [user ], ICMP id icmp-id , ICMP type icmp-type`

说明：已收到带错误格式代码（非零）的 ICMP 回应请求/应答数据包。

建议的操作：如果是间歇性事件，则无需执行任何操作。如果是因为受到攻击，则可以使用ACL拒绝主机。

314001

错误消息：`%ASA-6-314001: Pre-allocated RTSP UDP backconnection for src_intf :src_IP to dst_intf :dst_IP /dst_port.`

说明：Firepower 威胁防御设备为正在从服务器接收数据的 RTSP 客户端打开了 UDP 媒体通道。

- *src_intf* - 源接口名称
- *src_IP* - 源接口 IP 地址
- *dst_intf* - 目的接口名称
- *dst_IP* - 目的 IP 地址
- *dst_port* - 目的端口

建议的操作：无需执行任何操作。

314002

错误消息：`%ASA-6-314002: RTSP failed to allocate UDP media connection from src_intf :src_IP to dst_intf :dst_IP /dst_port : reason_string.`

说明：Firepower 威胁防御设备无法为媒体通道打开新针孔。

- *src_intf* - 源接口名称
- *src_IP* - 源接口 IP 地址
- *dst_intf* - 目的接口名称
- *dst_IP* - 目的 IP 地址
- *dst_port* - 目的端口
- *reason_string* - 针孔已经存在/未知

建议的操作：原因未知时，运行 **show memory** 命令检查空余内存，或运行 **show conn** 命令检查使用的连接数，因为 Firepower 威胁防御设备内存不足。

316001

错误消息：`%ASA-3-316001: Denied new tunnel to IP_address .VPN peer limit (platform_vpn_peer_limit) exceeded`

说明：如果尝试同时建立的 VPN 隧道 (ISAKMP/IPsec) 的数量超出平台 VPN 对等体支持的范围，则超出部分的隧道将会中止。

建议的操作：无需执行任何操作。

316002

错误消息： `%ASA-3-316002: VPN Handle error: protocol=protocol , src in_if_num :src_addr , dst out_if_num :dst_addr`

说明： 由于 VPN 句柄已存在，因此 Firepower 威胁防御设备无法创建 VPN 句柄。

- *protocol* - VPN 流协议
- *in_if_num* - VPN 流的入口接口数
- *src_addr* - VPN 流的源 IP 地址
- *out_if_num* - VPN 流的出口接口数
- *dst_addr* - VPN 流的目的 IP 地址

建议的操作： 正常操作期间可能出现此消息；但是，如果此消息重复出现，并且基于VPN的应用发生重大故障，则可能是因为存在软件缺陷。输入以下命令收集更多信息，并联系思科TAC进一步调查该问题：

```
capture
 name
 type asp-drop vpn-handle-error
show asp table classify crypto detail
show asp table vpn-context
```

317001

错误消息： `%ASA-3-317001: No memory available for limit_slow`

说明： 请求的操作因内存不足而失败。

建议的操作： 减少其他系统活动，从而降低内存需求。如果条件得到保证，则升级到更大内存配置。

317002

错误消息： `%ASA-3-317002: Bad path index of number for IP_address , number max`

说明： 发生了软件错误。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

317003

错误消息： `%ASA-3-317003: IP routing table creation failure - reason`

说明： 发生了内部软件错误，阻碍了新 IP 路由表的创建。

建议的操作： 按照显示正确复制此消息，并将其报告给思科 TAC。

317004

错误消息： `%ASA-3-317004: IP routing table limit warning`

说明：指定 IP 路由表中的路由数量已达到配置的警告限制。

建议的操作：减少表中的路由数量，或重新配置限制。

317005

错误消息：`%ASA-3-317005: IP routing table limit exceeded - reason , IP_address netmask`

说明：更多路由将添加到路由表中。

建议的操作：减少表中的路由数量，或重新配置限制。

317006

错误消息：`%ASA-3-317006: Pdb index error pdb , pdb_index , pdb_type`

说明：PDB 的索引超出范围。

- **pdb** - 协议描述符块，PDB 索引错误的描述符
- **pdb_index** - PDB 索引标识符
- **pdb_type** - PDB 索引错误类型

建议的操作：如果问题依然存在，则按照控制台或系统日志中的显示正确复制此错误消息，然后联系思科 TAC，并向代表提供所收集的信息。

317007

错误消息：`%ASA-6-317007: Added route_type route dest_address netmask via gateway_address [distance /metric ] on interface_name route_type`

说明：已向路由表添加新路由。

路由协议类型：

C - 已连接，S - 静态，I - IGRP，R - RIP，M - 移动

B – BGP，D – EIGRP，EX - EIGRP 外部，O - OSPF

IA - OSPF 中间区域，N1 - OSPF NSSA 外部类型 1

N2 - OSPF NSSA 外部类型 2，E1 - OSPF 外部类型 1

E2 - OSPF 外部类型 2，E – EGP，i - IS-IS，L1 - IS-IS 级别-1

L2 - IS-IS 级别 2，ia - IS-IS 中间区域

- *dest_address* - 此路由的目的网络
- *netmask* - 目的网络的网络掩码
- *gateway_address* - 进入目的网络所使用的网关地址
- *distance* - 此路由的管理距离
- *metric* - 此路由的度量
- *Interface_name* - 用于路由流量的网络接口的名称

建议的操作：无需执行任何操作。

317008

错误消息：`%ASA-6-317007: Deleted route_type route dest_address netmask via gateway_address [distance /metric ] on interface_name route_type`

说明：已从路由表删除新路由。

路由协议类型：

C - 已连接，S - 静态，I - IGRP，R - RIP，M - 移动

B – BGP，D – EIGRP，EX - EIGRP 外部，O - OSPF

IA - OSPF 中间区域，N1 - OSPF NSSA 外部类型 1

N2 - OSPF NSSA 外部类型 2，E1 - OSPF 外部类型 1

E2 - OSPF 外部类型 2，E – EGP，i - IS-IS，L1 - IS-IS 级别-1

L2 - IS-IS 级别 2，ia - IS-IS 中间区域

- *dest_address* - 此路由的目的网络
- *netmask* - 目的网络的网络掩码
- *gateway_address* - 进入目的网络所使用的网关地址
- *distance* - 此路由的管理距离
- *metric* - 此路由的度量
- *interface_name* - 用于路由流量的网络接口的名称

建议的操作：无需执行任何操作。

317012

错误消息：`%ASA-3-317012: Interface IP route counter negative - nameif-string-value`

说明：指示接口路由计数是负值。

- nameif-string-value - 通过 nameif 命令指定的接口名称

建议的操作：无需执行任何操作。

318001

错误消息：`%ASA-3-318001: Internal error: reason`

说明：发生了内部软件错误。此消息每五秒钟显示一次。

建议的操作：按照显示正确复制此消息，并将其报告给思科 TAC。

318002

错误消息： `%ASA-3-318002: Flagged as being an ABR without a backbone area`

说明： 路由器已被标记为区域边界路由器且未在路由器中配置主干区域。此消息每五秒钟显示一次。

建议的操作： 重新启动 OSPF 进程。

318003

错误消息： `%ASA-3-318003: Reached unknow n state in neighbor state machine`

说明： 发生了内部软件错误。此消息每五秒钟显示一次。

建议的操作： 按照显示正确复制此消息，并将其报告给思科 TAC。

318004

错误消息： `%ASA-3-318004: area` *`string`* `lsid` *`IP_address`* `mask` *`netmask`* `adv IP_address type` *`number`*

说明： OSPF 进程在查找链路状态通告时遇到问题，这可能导致内存泄漏。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

318005

错误消息： `%ASA-3-318005: lsid` *`ip_address`* `adv` *`IP_address`* `type` *`number`* `gateway` *`gateway_address`* `metric` *`number`* `network` *`IP_address`* `mask` *`netmask`* `protocol` *`hex`* `attr` *`hex`* `net-metric` *`number`*

说明： OSPF 发现了其数据库与 IP 路由表之间存在不一致。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

318006

错误消息： `%ASA-3-318006: if` *`interface_name`* `if_state` *`number`*

说明： 发生了内部错误。

建议的操作： 按照显示正确复制此消息，并将其报告给思科 TAC。

318007

错误消息： `%ASA-3-318007: OSPF is enabled on` *`interface_name`* `during idb initialization`

说明： 发生了内部错误。

建议的操作： 按照显示正确复制此消息，并将其报告给思科 TAC。

318008

错误消息： `%ASA-3-318008: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id`

说明： 正在重置 OSPF 进程，并将选择新的路由器 ID。此操作将关闭所有虚拟链路。

建议的操作： 更改所有虚拟链路邻居上的虚拟链路配置，以反映新的路由器 ID。

318009

错误消息： `%ASA-3-318009: OSPF: Attempted reference of stale data encountered in function , line: line_num`

说明： OSPF 正在运行且已尝试引用其他位置已删除的某些相关数据结构。清除接口和路由器配置可能会解决该问题。但是，如果出现此消息，某些步骤序列会导致过早删除数据结构，因此需要对此进行调查。

- *function* - 已接收意外事件的功能
- *line_num* - 代码中的行编号

建议的操作： 如果问题仍然存在，请联系思科 TAC。

318101

错误消息： `%ASA-3-318101: Internal error: REASON`

说明： 发生了内部软件错误。

- *REASON* - 事件的详细原因

建议的操作： 无需执行任何操作。

318102

错误消息： `%ASA-3-318102: Flagged as being an ABR without a backbone area`

说明： 路由器已被标记为区域边界路由器 (ABR) 且未在路由器中配置主干区域。

建议的操作： 重新启动 OSPF 进程。

318103

错误消息： `%ASA-3-318103: Reached unknown state in neighbor state machine`

说明： 发生了内部软件错误。

建议的操作： 无需执行任何操作。

318104

错误消息： `%ASA-3-318104: DB already exist: area AREA_ID_STR lsid i adv i type 0x x`

说明： OSPF 在查找 LSA 时遇到问题，这可能导致内存泄漏。

- *AREA_ID_STR* - 表示区域的字符串
- *i* - 整数值
- *x* - 整数值的十六进制表示

建议的操作： 无需执行任何操作。

318105

错误消息： `%ASA-3-318105: lsid i adv i type 0x x gateway i metric d network i mask i protocol #x attr #x net-metric d`

说明： OSPF 发现了其数据库与 IP 路由表之间存在不一致。

- *i* - 整数值
- *x* - 整数值的十六进制表示
- *d* - 编号

建议的操作： 无需执行任何操作。

318106

错误消息： `%ASA-3-318106: if IF_NAME if_state d`

说明： 发生了内部错误。

- *IF_NAME* - 受影响接口的名称
- *d* - 编号

建议的操作： 无需执行任何操作。

318107

错误消息： `%ASA-3-318107: OSPF is enabled on IF_NAME during idb initialization`

说明： 发生了内部错误。

- *IF_NAME* - 受影响接口的名称

建议的操作： 无需执行任何操作。

318108

错误消息： `%ASA-3-318108: OSPF process d is changing router-id. Reconfigure virtual link neighbors with our new router-id`

说明：正在重置 OSPF 进程，并将选择新的路由器 ID，这会关闭所有虚拟链路。要使虚拟链路重新正常工作，需要更改所有虚拟链路邻居上的虚拟链路配置。

- *d* - 表示进程 ID 的编号

建议的操作：更改所有虚拟链路邻居上的虚拟链路配置，以包含新的路由器 ID。

318109

错误消息：`%ASA-3-318109: OSPFv3 has received an unexpected message: 0x / 0x`

说明：OSPFv3 已收到意外进程间消息。

- *x* - 整数值的十六进制表示

建议的操作：无需执行任何操作。

318110

错误消息：`%ASA-3-318110: Invalid encrypted key s .`

说明：指定加密密钥无效。

- *s* - 表示加密密钥的字符串

建议的操作：指定明文密钥并输入 **service password-encryption** 命令进行加密，或确保指定加密密钥有效。如果指定加密密钥无效，则系统将在系统配置期间显示错误消息。

318111

错误消息：`%ASA-3-318111: SPI u is already in use with ospf process d`

说明：已尝试使用先前使用过的 SPI。

- *u* - 表示 SPI 的编号
- *d* - 表示进程 ID 的编号

建议的操作：选择其他 SPI。

318112

错误消息：`%ASA-3-318112: SPI u is already in use by a process other than ospf process d .`

说明：已尝试使用先前使用过的 SPI。

- *u* - 表示 SPI 的编号
- *d* - 表示进程 ID 的编号

建议的操作：选择其他 SPI。输入 **show crypto ipv6 ipsec sa** 命令查看正在使用的 SPI 的列表。

318113

错误消息： `%ASA-3-318113: s s is already configured with SPI u .`

说明： 已尝试使用先前使用过的 SPI。

- *s* - 表示接口的字符串
- *u* - 表示 SPI 的编号

建议的操作： 首先取消配置 SPI，或选择其他 SPI。

318114

错误消息： `%ASA-3-318114: The key length used with SPI u is not valid`

说明： 密钥长度不正确。

- *u* - 表示 SPI 的编号

建议的操作： 选择有效的 IPsec 密钥。IPsec 身份验证密钥的长度必须为 32 个 (MD5) 或 40 个 (SHA-1) 十六进制数字。

318115

错误消息： `%ASA-3-318115: s error occured when attempting to create an IPsec policy for SPI u`

说明： 已发生 IPsec API（内部）错误。

- *s* - 表示错误的字符串
- *u* - 表示 SPI 的编号

建议的操作： 无需执行任何操作。

318116

错误消息： `%asa-3-318116: SPI u 未由 ospf 进程 d 。`

说明： 已尝试取消配置不用于 OSPFv3 的 SPI。

- *u* - 表示 SPI 的编号
- *d* - 表示进程 ID 的编号

建议的操作： 输入 **show** 命令查看 OSPFv3 使用的 SPI。

318117

错误消息： `%ASA-3-318117: The policy for SPI u could not be removed because it is in use.`

说明： 已尝试删除用于所指示 SPI 的策略，但安全套接字依然在使用此策略。

- *u* - 表示 SPI 的编号

建议的操作：无需执行任何操作。

318118

错误消息：`%ASA-3-318118: s error occured when attemtping to remove the IPsec policy with SPI u`

说明：已发生 IPsec API（内部）错误。

- *s* - 表示指定错误的字符串
- *u* - 表示 SPI 的编号

建议的操作：无需执行任何操作。

318119

错误消息：`%ASA-3-318119: Unable to close secure socket with SPI u on interface s`

说明：已发生 IPsec API（内部）错误。

- *u* - 表示 SPI 的编号
- *s* - 表示指定接口的字符串

建议的操作：无需执行任何操作。

318120

错误消息：`%ASA-3-318120: OSPFv3 was unable to register with IPsec`

说明：发生了内部错误。

建议的操作：无需执行任何操作。

318121

错误消息：`%ASA-3-318121: IPsec reported a GENERAL ERROR: message s , count d`

说明：发生了内部错误。

- *s* - 表示指定消息的字符串
- *d* - 表示所生成消息总数的数字

建议的操作：无需执行任何操作。

318122

错误消息：`%ASA-3-318122: IPsec sent a s message s to OSPFv3 for interface s .Recovery attempt d`

说明：发生了内部错误。系统正在尝试重新打开安全套接字并进行恢复。

- *s* - 表示指定消息和指定接口的字符串
- *d* - 代表恢复尝试总次数的数字

建议的操作：无需执行任何操作。

318123

错误消息：`%ASA-3-318123: IPsec sent a s message s to OSPFv3 for interface IF_NAME .Recovery aborted`

说明：发生了内部错误。已超出最大恢复尝试次数。

- *s* - 表示指定消息的字符串
- *IF_NAME* - 指定接口

建议的操作：无需执行任何操作。

318125

错误消息：`%ASA-3-318125: Init failed for interface IF_NAME`

说明：接口初始化失败。可能的原因包括：

- 接口连接的区域正在被删除。
- 无法创建链路范围数据库。
- 无法为本地路由器创建邻居数据块。

建议的操作：删除初始化接口的配置命令，然后重试。

318126

错误消息：`%ASA-3-318126: Interface IF_NAME is attached to more than one area`

说明：接口位于接口所连接区域之外的区域的接口列表上。

- *IF_NAME* - 指定接口

建议的操作：无需执行任何操作。

318127

错误消息：`%ASA-3-318127: Could not allocate or find the neighbor`

说明：发生了内部错误。

建议的操作：无需执行任何操作。

ID 介于 320001 到 341011 之间的消息

本章包含 ID 介于 320001 到 341011 之间的消息。

320001

错误消息： `%ASA-3-320001: The subject name of the peer cert is not allowed for connection`

说明： 当Firepower威胁防御设备是Easy VPN远程设备或服务器时，对等体证书包含与 **ca verifycertdn** 命令输出不匹配的使用者名称。可能发生了中间人攻击，有设备伪造对等体IP地址并试图拦截来自Firepower 威胁防御设备 VPN 连接。

建议的操作： 无需执行任何操作。

321001

错误消息： `%ASA-5-321001: Resource var1 limit of var2 reached.`

说明： 已达到所指示资源的配置资源使用量或速率限制。

建议的操作： 无需执行任何操作。

321002

错误消息： `%ASA-5-321002: Resource var1 rate limit of var2 reached.`

说明： 已达到所指示资源的配置资源使用量或速率限制。

建议的操作： 无需执行任何操作。

321003

错误消息： `%ASA-6-321003: Resource var1 log level of var2 reached.`

说明： 已达到所指示资源的配置资源使用量或速率记录级别。

建议的操作： 无需执行任何操作。

321004

错误消息： `%ASA-6-321004: Resource var1 rate log level of var2 reached`

说明： 已达到所指示资源的配置资源使用量或速率记录级别。

建议的操作： 无需执行任何操作。

321005

错误消息： `%ASA-2-321005: System CPU utilization reached utilization %`

说明： 系统 CPU 使用率已达到 95% 或以上，而且这种情况已持续 5 分钟。

- *utilization %* - 当前 CPU 使用率百分比

建议的操作：如果此消息定期出现，则可以忽略。如果此消息频繁出现，请检查 **show cpu** 命令的输出并验证 CPU 使用率。如果使用率过高，请联系思科 TAC。

321006

错误消息：`%ASA-2-321006: System memory usage reached utilization %`

说明：系统内存使用率达到 80% 或以上，而且这种情况已持续 5 分钟。

- *utilization %* - 当前内存使用率百分比

建议的操作：如果此消息定期出现，则可以忽略。如果此消息频繁出现，请检查 **show memory** 命令的输出并验证内存使用率。如果使用率过高，请联系思科 TAC。

321007

错误消息：`%ASA-3-321007: System is low on free memory blocks of size block_size (free_blocks CNT out of max_blocks MAX)`

说明：系统空闲内存块不足。内存块耗尽可能会导致流量中断。

- *block_size* - 内存块大小（例如 4、1550、8192）
- *free_blocks* - 空闲块数量，使用 **show blocks** 命令后可在 CNT 列查看
- *max_blocks* - 系统可以分配的块的最大数量，使用 **show blocks** 命令后可在 MAX 列查看

建议的操作：使用 **show blocks** 命令，在所指示块大小的输出的 CNT 列中，监控空闲块数量。如果 CNT 列保持零值，或长时间接近零值，则 Firepower 威胁防御设备可能已过载或遇到了其他需要深入调查的问题。

322001

错误消息：`%ASA-3-322001: Deny MAC address MAC_address, possible spoof attempt on interface interface`

说明：Firepower 威胁防御设备从指定接口上的违规 MAC 地址收到了数据包，但是数据包中的源 MAC 地址与配置中的其他接口静态绑定。原因可能是发生了 MAC 欺骗攻击或配置错误。

建议的操作：检查配置并采取适当操作，即查找违规主机或校正配置。

322002

错误消息：`%ASA-3-322002: ARP inspection check failed for arp {request|response} received from host MAC_address on interface interface .This host is advertising MAC Address MAC_address_1 for IP Address IP_address , which is {statically|dynamically} bound to MAC Address MAC_address_2 .`

说明：如果启用 ARP 检测模块，则在跨 Firepower 威胁防御设备转发 ARP 数据包之前，此模块会检查数据包中通告的新 ARP 条目是否符合静态配置或动态获知的 IP-MAC 地址绑定。如果检查失败，则 ARP 检测模块会丢弃 ARP 数据包并生成此消息。造成这种情况的原因可能是网络中发生了 ARP 欺骗攻击或配置无效（IP MAC 绑定）。

建议的操作：如果是因为受到攻击，则可以使用 ACL 拒绝主机。如果是因为配置无效，请校正绑定。

322003

错误消息：`%ASA-3-322003:ARP inspection check failed for arp {request|response} received from host MAC_address on interface interface .This host is advertising MAC Address MAC_address_1 for IP Address IP_address , which is not bound to any MAC Address.`

说明：如果启用 ARP 检测模块，则在跨 Firepower 威胁防御设备转发 ARP 数据包之前，此模块会检查数据包中通告的新 ARP 条目是否符合静态配置的 IP-MAC 地址绑定。如果检查失败，则 ARP 检测模块会丢弃 ARP 数据包并生成此消息。造成这种情况的原因可能是网络中发生了 ARP 欺骗攻击或配置无效（IP MAC 绑定）。

建议的操作：如果是因为受到攻击，则可以使用 ACL 拒绝主机。如果是因为配置无效，请校正绑定。

322004

错误消息：`%ASA-6-322004: No management IP address configured for transparent firewall.Dropping protocol protocol packet from interface_in :source_address /source_port to interface_out :dest_address /dest_port`

说明：由于没有在透明模式下配置管理 IP 地址，因此 Firepower 威胁防御设备丢弃了数据包。

- **protocol** - 协议字符串或值
- **interface_in** - 输入接口名称
- **source_address** - 数据包的源 IP 地址
- **source_port** - 数据包的源端口
- **interface_out** - 输出接口名称
- **dest_address** - 数据包的目的 IP 地址
- **dest_port** - 数据包的目的端口

建议的操作：使用管理 IP 地址和掩码值配置设备。

323001

错误消息：`%ASA-3-323001: Module module_id experienced a control channel communications failure.`

`%ASA-3-323001: Module in slot slot_num  experienced a control channel communications failure.`

说明：Firepower 威胁防御设备无法通过控制通道与（在指定插槽中）安装的模块进行通信。

- **module_id** - 对于软件服务模块，此参数指定服务模块名称。
- **slot_num** - 对于硬件服务模块，此参数指定发生故障的插槽。插槽 0 表示系统主板，插槽 1 表示扩展槽中安装的模块。

建议的操作：如果问题仍然存在，请联系思科 TAC。

323002

错误消息： `%ASA-3-323002: Module module_id is not able to shut down, shut down request not answered.`

`%ASA-3-323002: Module in slot slot_num is not able to shut down, shut down request not answered.`

说明：所安装的模块未对关闭请求作出响应。

- **module_id** - 对于软件服务模块，此参数指定服务模块名称。
- **slot_num** - 对于硬件服务模块，此参数指定发生故障的插槽。插槽 0 表示系统主板，插槽 1 表示扩展槽中安装的模块。

建议的操作：如果问题仍然存在，请联系思科 TAC。

323003

错误消息： `%ASA-3-323003: Module module_id is not able to reload, reload request not answered.`

`%ASA-3-323003: Module in slot slotnum is not able to reload, reload request not answered.`

说明：所安装的模块未对重新加载请求作出响应。

- **module_id** - 对于软件服务模块，此参数指定服务模块名称。
- **slot_num** - 对于硬件服务模块，此参数指定发生故障的插槽。插槽 0 表示系统主板，插槽 1 表示扩展槽中安装的模块。

建议的操作：如果问题仍然存在，请联系思科 TAC。

323004

错误消息： `%ASA-3-323004: Module string one failed to write software newver (currently ver), reason .Hw-module reset is required before further use.`

说明：此模块无法接受软件版本，并将转换到无响应状态。更新软件后，此模块才可用。

- **string one** - 指定此模块的文本字符串
- >*newver* - 未成功写入模块的软件的新版本号（例如，1.0(1)0）
- >*ver* - 模块上软件的当前版本号（例如，1.0(1)0）
- >*reason* - 新版本无法写入此模块的原因。>*reason* 的可能值包括：

- 写入失败

- 映像写入线程创建失败

建议的操作：如果模块软件无法更新，则无法使用。如果问题仍然存在，请联系思科 TAC。

323005

错误消息： `% ASA-3-323005: Module module_id can not be started completely`

`%ASA-3-323005: Module in slot slot_num cannot be started completely`

说明：此消息表明该模块无法完全启动。该模块将保持无响应状态，直到这种情况得以解决。模块未完全插入插槽中是造成这种情况的最主要原因。

- **module_id** - 对于软件服务模块，此参数指定服务模块名称。
- **slot_num** - 对于硬件服务模块，此参数指定包含该模块的插槽号。

建议的操作：验证该模块是否已完全插入插槽并检查该模块上的任何状态LED是否亮起。重新完全插入该模块后，Firepower威胁防御设备可能需要一分钟的时间才能识别出该模块是否已上电。如果验证了该模块已插入插槽并使用 **sw-module module** *service-module-name* **reset** 命令或 **hw-module module** *slotnum* **reset** 命令重置该模块后，仍然出现此消息，请联系思科 TAC。

323006

错误消息：`%ASA-1-323006: Module ips experienced a data channel communication failure, data channel is DOWN.`

说明：已发生数据通道通信故障，并且 Firepower 威胁防御设备无法将流量转发到服务模块。当 HA 配置中的主用Firepower威胁防御设备发生故障时，此故障将触发故障切换。此故障还会导致对正常发送到服务模块的流量强制执行已配置的故障开放或故障关闭策略。每当服务模块停止、重置、删除或禁用导致系统模块与服务模块之间的Firepower威胁防御设备数据平面出现通信问题，就会生成此消息。

建议的操作：对于软件服务模块（例如 IPS），使用 **sw-module module ips recover** 命令恢复模块。对于硬件服务模块，如果此消息不是由于 SSM 重新加载或重置引起的，并且相应的系统日志消息 505010 在 SSM 恢复运行状态后未出现，则使用 **hw-module module 1 reset** 命令重置模块。

323007

错误消息：`%ASA-3-323007: Module in slot slot experienced a firware failure and the recovery is in progress.`

说明：安装有 4GE-SSM 的 Firepower 威胁防御设备遇到了短时电涌，然后重新启动。因此，4GE SSM 可能在无响应状态下联机。Firepower 威胁防御设备已检测到 4GE SSM 处于无响应状态，并自动重启 4GE SSM。

建议的操作：无需执行任何操作。

325001

错误消息：`%ASA-3-325001: Router ipv6_address on interface has conflicting ND (Neighbor Discovery) settings`

说明：链路上的另一台路由器发送了包含冲突参数的路由器通告。

- **ipv6_address** - 另一台路由器的 IPv6 地址
- **interface** - 另一台路由器的链路的接口名称

建议的操作：验证链路上的所有 IPv6 路由器是否都具有与路由器通告中相同的 **hop_limit**、**managed_config_flag**、**other_config_flag** 、**reachable_time** 和 **ns_interval** 参数，并验证多台路由器

针对相同前缀通告的首选和有效生命周期相同。要列出每个接口的参数，请输入 **show ipv6 interface** 命令。

325002

错误消息： `%ASA-4-325002: Duplicate address ipv6_address/MAC_address on interface`

说明： 其他系统正在使用您的 IPv6 地址。

- **ipv6_address -** 另一台路由器的 IPv6 地址
- **MAC_address -** 另一个系统的 MAC 地址（若已知）；否则该地址将视为未知。
- **interface -** 另一个系统的链路的接口名称

建议的操作： 更改两个系统其中一个系统的 IPv6 地址。

326001

错误消息： `%ASA-3-326001: Unexpected error in the timer library: error_message`

说明： 收到了不含情景或正确类型的托管计时器事件，或不存在处理程序。或者，如果加入队列的事件数超出系统限制，系统会尝试在稍后处理这些事件。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326002

错误消息： `%ASA-3-326002: Error in error_message : error_message`

说明： IGMP 进程根据请求关闭失败。在准备此关闭操作期间执行的事件可能不同步。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326004

错误消息： `%ASA-3-326004: An internal error occurred while processing a packet queue`

说明： IGMP 数据包队列收到了一个不含数据包的信号。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326005

错误消息： `%ASA-3-326005: Mrib notification failed for (IP_address, IP_address )`

说明： 收到了触发数据驱动型事件的数据包，但尝试通知 MRIB 失败。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326006

错误消息： `%ASA-3-326006: Entry-creation failed for (IP_address, IP_address )`

说明： MFIB 从 MRIB 收到了条目更新，但未能创建与显示的地址有关的条目。这可能是因为内存不足。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326007

错误消息： `%ASA-3-326007: Entry-update failed for (IP_address, IP_address )`

说明： MFIB 从 MRIB 收到了接口更新，但未能创建与显示的地址有关的接口。这可能是因为内存不足。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326008

错误消息： `%ASA-3-326008: MRIB registration failed`

说明： MFIB 向 MRIB 注册失败。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326009

错误消息： `%ASA-3-326009: MRIB connection-open failed`

说明： MFIB 打开 MRIB 连接失败。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326010

错误消息： `%ASA-3-326010: MRIB unbind failed`

说明： MFIB 从 MRIB 取消绑定失败。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326011

错误消息： `%ASA-3-326011: MRIB table deletion failed`

说明： MFIB 未能检索到要删除的表格。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326012

错误消息： `%ASA-3-326012: Initialization of *string* functionality failed`

说明： 指定功能初始化失败。即使没有此项功能，此组件仍可运行。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326013

错误消息： `%ASA-3-326013: Internal error: *string* in *string* line %d (%s )`

说明： MRIB 中发生了根本性错误。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326014

错误消息： `%ASA-3-326014: Initialization failed: error_message *error_message*`

说明： MRIB 初始化失败。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326015

错误消息： `%ASA-3-326015: Communication error: error_message` **`error_message`**

说明： MRIB 收到了格式错误的更新。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326016

错误消息： `%ASA-3-326016: Failed to set un-numbered interface for *interface_name*(*string* )`

说明： 没有源地址，便无法使用 PIM 隧道。由于找不到编号的接口，或由于发生内部错误，才会出现这种情况。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326017

错误消息： `%ASA-3-326017: Interface Manager error - *string* in *string* : *string*`

说明： 创建 PIM 隧道接口时出错。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326019

错误消息： `%ASA-3-326019: string in string : string`

说明： 创建 PIM RP 隧道接口时出错。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326020

错误消息： `%ASA-3-326020: List error in string : string`

说明： 处理 PIM 接口列表时出错。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326021

错误消息： `%ASA-3-326021: Error in string : string`

说明： 设置 PIM 隧道接口的 SRC 时出错。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326022

错误消息： `%ASA-3-326022: Error in string : string`

说明： PIM 进程根据请求关闭失败。在准备此关闭操作期间执行的事件可能不同步。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326023

错误消息： `%ASA-3-326023: string - IP_address : string`

说明： 处理 PIM 组范围时出错。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326024

错误消息： `%ASA-3-326024: An internal error occurred while processing a packet queue.`

说明： PIM 数据包队列收到了一个不含数据包的信号。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

326025

错误消息： `%ASA-3-326025: string`

说明：尝试发送消息时发生内部错误。可能不会发生计划在收到消息时发生的事件，例如删除 PIM 隧道 IDB。

建议的操作：如果问题仍然存在，请联系思科 TAC。

326026

错误消息：`%ASA-3-326026: Server unexpected error: error_message`

说明：MRIB 注册客户端失败。

建议的操作：如果问题仍然存在，请联系思科 TAC。

326027

错误消息：`%ASA-3-326027: Corrupted update: error_message`

说明：MRIB 收到了已损坏的更新。

建议的操作：如果问题仍然存在，请联系思科 TAC。

326028

错误消息：`%ASA-3-326028: Asynchronous error: error_message`

说明：MRIB API 中发生了尚未处理的异步错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

327001

错误消息：`%ASA-3-327001: IP SLA Monitor: Cannot create a new process`

说明：IP SLA 监控器无法启动新进程。

建议的操作：检查系统内存。如果内存不足，则内存不足很可能就是造成这一问题的原因。当内存可用时，请尝试重新输入相应命令。如果问题仍然存在，请联系思科 TAC。

327002

错误消息：`%ASA-3-327002: IP SLA Monitor: Failed to initialize, IP SLA Monitor functionality will not work`

说明：IP SLA 监控器初始化失败。这种情况是由于计时器轮函数初始化失败或未创建进程引起的。可能没有充足的内存来完成此任务。

建议的操作：检查系统内存。如果内存不足，则内存不足很可能就是造成这一问题的原因。当内存可用时，请尝试重新输入相应命令。如果问题仍然存在，请联系思科 TAC。

327003

错误消息： `%ASA-3-327003: IP SLA Monitor: Generic Timer wheel timer functionality failed to initialize`

说明： IP SLA 监控器无法初始化计时器轮。

建议的操作： 检查系统内存。如果内存不足，则表明计时器轮函数未初始化。当内存可用时，请尝试重新输入相应命令。如果问题仍然存在，请联系思科 TAC。

328001

错误消息： `%ASA-3-328001: Attempt made to overwrite a set stub function in` *`string`* `.`

说明： 调用包含检查注册表的存根时，可将单个函数设置为回调。由于回调函数已事先设置，因此尝试设置新回调的操失败。

- **string** - 函数的名称

建议的操作： 如果问题仍然存在，请联系思科 TAC。

328002

错误消息： `%ASA-3-328002: Attempt made in` *`string`* `to register with out of bounds key`

说明： 在 FASTCASE 注册表中，密钥必须小于创建注册表时指定的大小。已尝试使用越界密钥注册。

建议的操作： 按照显示正确复制此消息，并将其报告给思科 TAC。

329001

错误消息： `%ASA-3-329001: The` *`string0`* `subblock named` *`string1`* `was not removed`

说明： 发生了软件错误。IDB 子块无法删除。

- *string0* - SWIDB 或 WIDB
- *string1* - 子块的名称

建议的操作： 如果问题仍然存在，请联系思科 TAC。

331001

错误消息： `ASA-3-331001: Dynamic DNS Update for '`*`fqdn_name`*`' = `*`ip_address`*` failed`

说明： 动态 DNS 子系统更新 DNS 服务器上的资源记录失败。如果 Firepower 威胁防御设备无法联系 DNS 服务器或 DNS 服务未在目的系统上运行，则可能发生此失败情况。

- *fqdn_name* - 已尝试为其更新 DNS 的完全限定域名
- *ip_address* - DNS 更新的 IP 地址

建议的操作：确保 Firepower 威胁防御设备已配置并可到达 DNS 服务器。如果问题仍然存在，请联系思科 TAC。

331002

错误消息：`ASA-5-331002: Dynamic DNS type RR for ('fqdn_name ' - ip_address | ip_address - 'fqdn_name ') successfully updated in DNS server dns_server_ip`

说明：动态 DNS 更新在 DNS 服务器中成功完成。

- *type* - 资源记录类型，可能是 A 或 PTR
- *fqdn_name* - 已尝试为其更新 DNS 的完全限定域名
- *ip_address* - DNS 更新的 IP 地址
- *dns_server_ip* - DNS 服务器的 IP 地址

建议的操作：无需执行任何操作。

332001

错误消息：`%ASA-3-332001: Unable to open cache discovery socket, WCCP V2 closing down.`

说明：内部错误，指示 WCCP 进程无法打开用于侦听来自缓存的协议消息的 UDP 套接字。

建议的操作：确保 IP 配置正确，同时确保已配置至少一个 IP 地址。

332002

错误消息：`%ASA-3-332002: Unable to allocate message buffer, WCCP V2 closing down.`

说明：内部错误，指示 WCCP 进程无法分配内存来存放传入协议消息。

建议的操作：确保有足够的内存可用于所有进程。

332003

错误消息：`%ASA-5-332003: Web Cache IP_address /service_ID acquired`

说明：已从 Firepower 威胁防御设备获取 Web 缓存服务。

- **IP_address** - Web 缓存的 IP 地址
- **service_ID** - WCCP 服务标识符

建议的操作：无需执行任何操作。

332004

错误消息：`%ASA-1-332004: Web Cache IP_address /service_ID lost`

说明：Firepower 威胁防御设备的 Web 缓存服务已中断。

- **IP_address** - Web 缓存的 IP 地址
- **service_ID** - WCCP 服务标识符

建议的操作：验证指定 Web 缓存的操作。

333001

错误消息：`%ASA-6-333001: EAP association initiated - context: EAP-context`

说明：已向远程主机发起 EAP 关联。

- *EAP-context* - EAP 会话的唯一标识符，显示为八位十六进制数字（例如，0x2D890AE0）

建议的操作：无需执行任何操作。

333002

错误消息：`%ASA-5-333002: Timeout waiting for EAP response - context:EAP-context`

说明：等待 EAP 响应时发生超时。

- *EAP-context* - EAP 会话的唯一标识符，显示为八位十六进制数字（例如，0x2D890AE0）

建议的操作：无需执行任何操作。

333003

错误消息：`%ASA-6-333003: EAP association terminated - context:EAP-context`

说明：已终止与远程主机的 EAP 关联。

- *EAP-context* - EAP 会话的唯一标识符，显示为八位十六进制数字（例如，0x2D890AE0）

建议的操作：无需执行任何操作。

333004

错误消息：`%ASA-7-333004: EAP-SQ response invalid - context:EAP-context`

说明：EAP 状态查询响应基本数据包验证失败。

- *EAP-context* - EAP 会话的唯一标识符，显示为八位十六进制数字（例如，0x2D890AE0）

建议的操作：如果问题仍然存在，请联系思科 TAC。

333005

错误消息：`%ASA-7-333005: EAP-SQ response contains invalid TLV(s) - context:EAP-context`

说明：EAP 状态查询响应有一个或多个无效 TLV。

- *EAP-context* - EAP 会话的唯一标识符，显示为八位十六进制数字（例如，0x2D890AE0）

建议的操作：如果问题仍然存在，请联系思科 TAC。

333006

错误消息：`%ASA-7-333006: EAP-SQ response with missing TLV(s) - context:EAP-context`

说明：EAP 状态查询响应缺失一个或多个强制性 TLV。

- *EAP-context* - EAP 会话的唯一标识符，显示为八位十六进制数字（例如，0x2D890AE0）

建议的操作：如果问题仍然存在，请联系思科 TAC。

333007

错误消息：`%ASA-7-333007: EAP-SQ response TLV has invalid length - context:EAP-context`

说明：EAP 状态查询响应包括一个拥有无效长度的 TLV。

- *EAP-context* - EAP 会话的唯一标识符，显示为八位十六进制数字（例如，0x2D890AE0）

建议的操作：如果问题仍然存在，请联系思科 TAC。

333008

错误消息：`%ASA-7-333008: EAP-SQ response has invalid nonce TLV - context:EAP-context`

说明：EAP 状态查询响应包括一个无效的一次性随机 TLV。

- *EAP-context* - EAP 会话的唯一标识符，显示为八位十六进制数字（例如，0x2D890AE0）

建议的操作：如果问题仍然存在，请联系思科 TAC。

333009

错误消息：`%ASA-6-333009: EAP-SQ response MAC TLV is invalid - context:EAP-context`

说明：EAP 状态查询响应包括一个与计算的 MAC 不匹配的 MAC。

- *EAP-context* - EAP 会话的唯一标识符，显示为八位十六进制数字（例如，0x2D890AE0）

建议的操作：如果问题仍然存在，请联系思科 TAC。

333010

错误消息：`%ASA-5-333010: EAP-SQ response Validation Flags TLV indicates PV request - context:EAP-context`

说明：EAP 状态查询响应包括验证标志 TLV，这表示对等体已请求完全安全评估验证。

建议的操作：无需执行任何操作。

334001

错误消息：`%ASA-6-334001: EAPoUDP association initiated - host-address`

说明：已向远程主机发起 EAPoUDP 关联。

- *host-address* - 点分十进制格式的主机 IP 地址，例如，10.86.7.101

建议的操作：无需执行任何操作。

334002

错误消息：`%ASA-5-334002: EAPoUDP association successfully established - host-address`

说明：已与主机成功建立 EAPoUDP 关联。

- *host-address* - 点分十进制格式的主机 IP 地址，例如，10.86.7.101

建议的操作：无需执行任何操作。

334003

错误消息：`%ASA-5-334003: EAPoUDP association failed to establish - host-address`

说明：与主机建立 EAPoUDP 关联失败。

- *host-address* - 点分十进制格式的主机 IP 地址，例如，10.86.7.101

建议的操作：验证思科安全访问控制服务器的配置。

334004

错误消息：`%ASA-6-334004: Authentication request for NAC Clientless host - host-address`

说明：已为 NAC 无客户端主机提出身份验证请求。

- *host-address* - 点分十进制格式的主机 IP 地址，例如，10.86.7.101

建议的操作：无需执行任何操作。

334005

错误消息：`%ASA-5-334005: Host put into NAC Hold state - host-address`

说明：主机的 NAC 会话已置于保留状态。

- *host-address* - 点分十进制格式的主机 IP 地址，例如，10.86.7.101

建议的操作：无需执行任何操作。

334006

错误消息：`%ASA-5-334006: EAPoUDP failed to get a response from host - host-address`

说明：未从主机收到 EAPoUDP 响应。

- *host-address* - 点分十进制格式的主机 IP 地址，例如，10.86.7.101

建议的操作：无需执行任何操作。

334007

错误消息：`%ASA-6-334007: EAPoUDP association terminated - host-address`

说明：与主机的 EAPoUDP 关联已终止。

- *host-address* - 点分十进制格式的主机 IP 地址，例如，10.86.7.101

建议的操作：无需执行任何操作。

334008

错误消息：`%ASA-6-334008: NAC EAP association initiated - host-address , EAP context: EAP-context`

说明：EAPoUDP 已向主机发起 EAP。

- *host-address* - 点分十进制格式的主机 IP 地址，例如，10.86.7.101
- *EAP-context* - EAP 会话的唯一标识符，显示为八位十六进制数字（例如，0x2D890AE0）

建议的操作：无需执行任何操作。

334009

错误消息：`%ASA-6-334009: Audit request for NAC Clientless host - Assigned_IP.`

说明：正在为指定的已分配 IP 地址发送审核请求。

- *Assigned_IP* - 分配给客户端的 IP 地址

建议的操作：无需执行任何操作。

336001

错误消息：`%ASA-3-336001 Route desination_network stuck-in-active state in EIGRP-ddb_name as_num. Cleaning up`

说明：SIA 状态意味着 EIGRP 路由器在分配的时间内（约三分钟）未收到一个或多个邻居的查询应答。发生这种情况时，EIGRP 会清除未发送应答的邻居，并为变为活动状态的路由记录错误消息。

- *destination_network* - 变为活动状态的路由
- *ddb_name* - IPv4
- *as_num* - GRP 路由器

建议的操作：检查造成路由器未收到所有邻居响应的原因以及路由消失的原因。

336002

错误消息：`%ASA-3-336002: Handle handle_id is not allocated in pool.`

说明：EIGRP 路由器无法找到下一跳的句柄。

- *handle_id* - 缺失句柄的标识

建议的操作：如果问题仍然存在，请联系思科 TAC。

336003

错误消息：`%ASA-3-336003: No buffers available for bytes byte packet`

说明：双机软件无法分配数据包缓冲区。Firepower 威胁防御设备可能内存不足。

- *bytes* - 数据包中的字节数

建议的操作：输入 **show mem** 或 **show tech** 命令检查 Firepower 威胁防御设备是否内存不足。如果问题仍然存在，请联系思科 TAC。

336004

错误消息：`%ASA-3-336004: Negative refcount in pakdesc pakdesc.`

说明：引用计数数据包计数变成负数。

- *pakdesc* - 数据包标识符

建议的操作：如果问题仍然存在，请联系思科 TAC。

336005

错误消息：`%ASA-3-336005: Flow control error, error , on interface_name.`

说明：接口组播流受阻止。Qelm 是队列元素，在此情况下，还是此特定接口队列的最后一个组播数据包。

- *error* - 错误语句：Qelm on flow ready
- *interface_name* - 发生错误的接口的名称

建议的操作：如果问题仍然存在，请联系思科 TAC。

336006

错误消息：`%ASA-3-336006: num peers exist on IIDB interface_name.`

说明：EIGRP 的 IDB 清理期间或清理后，特定接口上仍然存在对等体。

- *num* - 对等体的数量
- *interface_name* - 接口名称

建议的操作：如果问题仍然存在，请联系思科 TAC。

336007

错误消息：`%ASA-3-336007: Anchor count negative`

说明：发生了错误，锚点计数在发布时变成了负数。

建议的操作：如果问题仍然存在，请联系思科 TAC。

336008

错误消息：`%ASA-3-336008: Lingering DRDB deleting IIDB, dest network, nexthop address (interface), origin origin_str`

说明：正在删除接口，存在一些拖延的 DRDB 情况。

- network - 目的网络
- address - 下一跳地址
- interface - 下一跳接口
- origin_str - 定义源地址的字符串

建议的操作：如果问题仍然存在，请联系思科 TAC。

336009

错误消息：`%ASA-3-336009 ddb_name as_id: Internal Error`

说明：发生了内部错误。

- *ddb_name* - PDM 名称（例如，IPv4 PDM）
- *as_id* - 自主系统 ID

建议的操作：如果问题仍然存在，请联系思科 TAC。

336010

错误消息：`%ASA-5-336010 EIGRP-ddb_name tableid as_id: Neighbor address (%interface) is event_msg: msg`

说明：邻居已启动或关闭。

- *ddb_name* - IPv4
- *tableid* - RIB 的内部 ID
- *as_id* - 自主系统 ID
- *address* - 邻居的 IP 地址
- *interface* - 接口的名称
- *event_msg* - 邻居正在经历的事件（即启动或关闭）
- *msg* - 事件原因。可能的 *event_msg* 和 *msg* 值对包括：

- 重新同步：对等体平稳重启

- 关闭：保持计时器过期

- 启动：新邻接

- 关闭：身份验证失败

- 关闭：停滞在活动状态

- 关闭：收到接口对等体终止消息

- 关闭：K 值不匹配

- 关闭：收到对等体终止消息

- 关闭：停滞在初始化状态

- 关闭：对等体信息已更改

- 关闭：摘要已配置

- 关闭：最大跳数已更改

- 关闭：度量已更改

- 关闭：[无原因]

建议的操作：检查邻居上的链路发生故障或摆动的原因。这可能表明存在问题，或可能因此出现问题。

336011

错误消息：`%ASA-6-336011: event event`

说明：发生了双重事件。事件可以是以下任意一项：

- 重新分配 rt 发生更改
- 在活动状态下执行 SIA 查询

建议的操作：如果问题仍然存在，请联系思科 TAC。

336012

错误消息：`%ASA-3-336012: Interface interface_names going down and neighbor_links links exist`

说明：接口发生故障或正在从通过 IGRP 的路由中删除，但并非所有链路（邻居）都已从拓扑表中删除。

建议的操作：如果问题仍然存在，请联系思科 TAC。

336013

错误消息：`%ASA-3-336013: Route iproute, iproute_successors successors, db_successors rdbs`

说明：发生了硬件或软件。

建议的操作：如果问题仍然存在，请联系思科 TAC。

336014

错误消息：`%ASA-3-336014: “EIGRP_PDM_Process_name, event_log”`

说明：发生了硬件或软件。

建议的操作：如果问题仍然存在，请联系思科 TAC。

336015

错误消息：`%ASA-3-336015: “Unable to open socket for AS as_number”`

说明：发生了硬件或软件。

建议的操作：如果问题仍然存在，请联系思科 TAC。

336016

错误消息：`%ASA-3-336016: Unknown timer type timer_type expiration`

说明：发生了硬件或软件。

建议的操作：如果问题仍然存在，请联系思科 TAC。

336019

错误消息：`%ASA-3-336019: process_name as_number: prefix_source threshold prefix level (prefix_threshold) reached`

说明：拓扑数据库中前缀的数量已达到配置或默认的阈值水平。前缀源可以是以下任何一项：

- 邻居
- 已重分布
- 汇聚

建议的操作：使用 **show eigrp accounting** 命令获取有关前缀源的详细信息，并采取纠正措施。

337000

错误消息：`%ASA-6-337000: Created BFD session with local discriminator <id> on <real_interface> with neighbor <real_host_ip>`

说明：此系统日志消息表明已创建 BFD 活动会话。

- id - 表示特定 BFD 会话的本地鉴别器值的数字字段
- real_interface - 运行 BFD 会话的接口 nameif
- real_host_ip - 与之建立 BFD 会话的邻居的 IP 地址

建议的操作：无。

337001

错误消息： `%ASA-6-337001: Terminated BFD session with local discriminator <id> on <real_interface> with neighbor <real_host_ip> due to <failure_reason>`

说明： 此系统日志消息指示活动 BFD 会话已终止。

- id - 表示特定 BFD 会话的本地鉴别器值的数字字段
- real_interface - 运行 BFD 会话的接口 nameif
- real_host_ip - 与之建立 BFD 会话的邻居的 IP 地址
- failure_reason - 以下故障原因之一：对等体侧 BFD 发生故障；对等体侧 BEF 配置被删除；检测计时器到期；回应功能发生故障；前往对等体的路径发生故障；本地BFD配置被删除；BFD客户端配置被删除

建议的操作： 无。

337005

错误消息： `%ASA-4-337005: Phone Proxy SRTP: Media session not found for media_term_ip/media_term_port for packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port`

说明： 自适应安全设备收到了发往媒体端接 IP 地址或端口的 SRTP 或 RTP 数据包，但找不到处理此数据包的相应媒体会话。

- in_ifc - 输入接口
- src_ip - 数据包的源 IP 地址
- src_port - 数据包的源端口
- out_ifc - 输出接口
- dest_ip - 数据包的目的 IP 地址
- dest_port - 数据包的目的端口。

建议的操作： 如果呼叫结束时出现此消息，则会被视为正常的消息，这是因为信令消息可能已发布媒体会话，但终端正在继续发送一些 SRTP 或 RTP 数据包。如果奇数媒体端接端口出现此消息，则终端正在发送 RTCP，必须从 CUCM 禁用。如果呼叫时持续出现此消息，使用电话代理调试命令或捕获命令调试信令消息事务，确定信令消息是否正在使用媒体端接 IP 地址和端口进行修改。

340001

错误消息： `%ASA-3-340001: Loopback-proxy error: error_string context id context_id , context type = version /request_type /address_type client socket (internal)= client_address_internal /client_port_internal server socket (internal)= server_address_internal /server_port_internal server socket (external)= server_address_external /server_port_external remote socket (external)= remote_address_external /remote_port_external`

说明： 环回代理允许Firepower威胁防御设备上运行的第三方应用访问网络。环回代理遇到了错误。

- *context_id* - 为每个环回客户端代理请求生成的唯一 32 位情景 ID
- *version* - 协议版本。

- *request_type* - 请求类型，可以是以下其中一种：TC（TCP 连接）、TB（TCP 绑定）或 UA（UDP 关联）
- *address_type* - 地址类型，可以是以下其中一种：IP4 (IPv4)、IP6 (IPv6) 或 DNS（域名服务）
- *client_address_internal/server_address_internal* - 环回客户端和环回服务器用于通信的地址
- *client_port_internal* /*server_port_internal* - 环回客户端和环回服务器用于通信的端口
- *server_address_external* /*remote_address_external* - 环回服务器和远程主机用于通信的地址
- *server_port_external* /*remote_port_external* - 环回服务器和远程主机用于通信的端口
- *error_string* - 可帮助对问题进行故障排除的错误字符串

建议的操作：复制此系统日志消息并联系思科 TAC。

340002

错误消息：`%ASA-6-340002: Loopback-proxy info: error_string context id context_id , context type = version /request_type /address_type client socket (internal)= client_address_internal /client_port_internal server socket (internal)= server_address_internal /server_port_internal server socket (external)= server_address_external /server_port_external remote socket (external)= remote_address_external /remote_port_external`

说明：环回代理允许 Firepower 威胁防御设备上运行的第三方应用访问网络。环回代理生成了调试信息，以供故障排除期间使用。

- *context_id* - 为每个环回客户端代理请求生成的唯一 32 位情景 ID
- *version* - 协议版本。
- *request_type* - 请求类型，可以是以下其中一种：TC（TCP 连接）、TB（TCP 绑定）或 UA（UDP 关联）
- *address_type* - 地址类型，可以是以下其中一种：IP4 (IPv4)、IP6 (IPv6) 或 DNS（域名服务）
- *client_address_internal/server_address_internal* - 环回客户端和环回服务器用于通信的地址
- *client_port_internal* /*server_port_internal* - 环回客户端和环回服务器用于通信的端口
- *server_address_external* /*remote_address_external* - 环回服务器和远程主机用于通信的地址
- *server_port_external* /*remote_port_external* - 环回服务器和远程主机用于通信的端口
- *error_string* - 可帮助对问题进行故障排除的错误字符串

建议的操作：复制此系统日志消息并联系思科 TAC。

341001

错误消息：`%ASA-6-341001: Policy Agent started successfully for VNMC vnmc_ip_addr`

说明：策略代理进程（DME、ducatiAG 和 commonAG）已成功启动。

- *vnmc_ip_addr* - VNMC 服务器的 IP 地址

建议的操作：无。

341002

错误消息： `%ASA-6-341002: Policy Agent stopped successfully for VNMC vnmc_ip_addr`

说明： 策略代理进程（DME、ducatiAG 和 commonAG）已停止。

- *vnmc_ip_addr* - VNMC 服务器的 IP 地址

建议的操作： 无。

341003

错误消息： `%ASA-3-341003: Policy Agent failed to start for VNMC vnmc_ip_addr`

说明： 策略代理启动失败。

- *vnmc_ip_addr* - VNMC 服务器的 IP 地址

建议的操作： 针对错误消息检查控制台历史记录和 disk0:/pa/log/vnm_pa_error_status。要重新尝试启动策略代理，请再次发出 **registration host** 命令。

341004

错误消息： `%ASA-3-341004: Storage device not available: Attempt to shutdown module %s failed.`

说明： 所有 SSD 都已发生故障或在系统处于启动状态下删除。系统已尝试关闭软件模块，但尝试失败。

- *%s* - 软件模块（例如 cxsc）

建议的操作： 替换已删除或发生故障的硬盘并重新加载 Firepower 威胁防御设备。

341005

错误消息： `%ASA-3-341005: Storage device not available.Shutdown issued for module %s .`

说明： 所有 SSD 都已发生故障或在系统处于启动状态下删除。系统正在关闭软件模块。

- *%s* - 软件模块（例如 cxsc）

建议的操作： 替换已删除或发生故障的硬盘并重新加载软件模块。

341006

错误消息： `%ASA-3-341006: Storage device not available.Failed to stop recovery of module %s .`

说明： 所有 SSD 都已发生故障或在系统处于恢复状态下删除。系统尝试了停止恢复，但尝试失败。

- *%s* - 软件模块（例如 cxsc）

建议的操作： 替换已删除或发生故障的硬盘并重新加载 Firepower 威胁防御设备。

341007

错误消息： `%ASA-3-341007: Storage device not available.Further recovery of module %s was stopped.This may take several minutes to complete.`

说明： 所有 SSD 都已发生故障或在系统处于恢复状态下删除。系统正在停止恢复软件模块。

- *%s* - 软件模块（例如 cxsc）

建议的操作： 替换已删除或发生故障的硬盘并重新加载软件模块。

341008

错误消息： `%ASA-3-341008: Storage device not found.Auto-boot of module %s cancelled.Install drive and reload to try again.`

说明： 系统进入启动状态后，所有 SSD 在重新加载系统前都已发生故障或删除。由于启动期间的默认操作是自动启动软件模块，此操作因为没有可用存储设备而受阻止。

建议的操作： 替换已删除或发生故障的硬盘并重新加载软件模块。

341010

错误消息： `%ASA-6-341010: Storage device with serial number ser_no [inserted into | removed from] bay bay_no`

说明： Firepower 威胁防御设备已检测到插入或删除事件，并立即生成此系统日志消息。

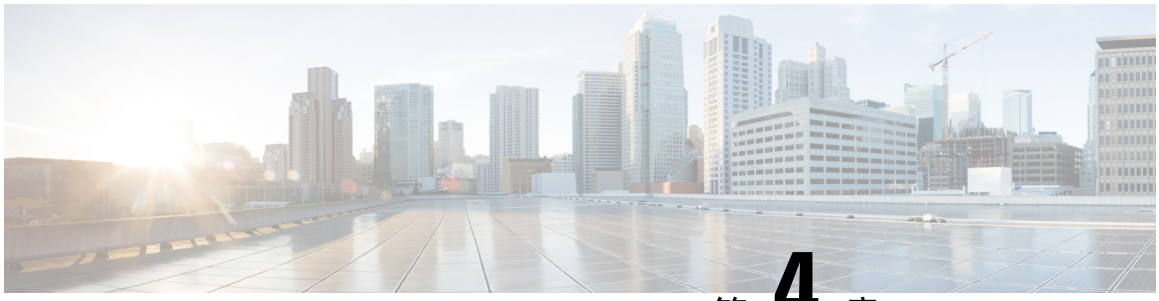
建议的操作： 无需执行任何操作。

341011

错误消息： `%ASA-3-341011: Storage device with serial number ser_no in bay bay_no faulty.`

说明： Firepower 威胁防御设备每 10 分钟轮询一次硬盘驱动器 (HDD) 的运行状态，如果 HDD 处于故障状态，则生成此系统日志消息。

建议的操作： 无需执行任何操作。



第 4 章

系统日志消息 401001-450001

本章包含以下各节：

ID 介于 401001 到 409128 之间的消息

本章包含 ID 介于 401001 到 409128 之间的消息。

401001

错误消息： `%ASA-4-401001: Shuns cleared`

说明： 已输入 **clear shun** 命令以删除内存中的现有规避规则。记录规避活动的机制获得了允许。

建议的操作： 无需执行任何操作。

401002

错误消息： `%ASA-4-401002: Shun added: IP_address` *`IP_address`* `port` *`port`*

说明： 已输入 **shun** 命令，其中第一个 IP 地址是被规避的主机。其他地址和端口可选，用于终止连接（若可用）。记录规避活动的机制获得了允许。

建议的操作： 无需执行任何操作。

401003

错误消息： `%ASA-4-401003: Shun deleted:` *`IP_address`*

说明： 单台被规避的主机已从规避规则数据库中删除。记录规避活动的机制获得了允许。

建议的操作： 无需执行任何操作。

401004

错误消息： `%ASA-4-401004: Shunned packet: IP_address = IP_address on interface interface_name`

说明： 由于IP SRC定义的主机是规避规则数据库中的主机，因此数据包已丢弃。被规避的主机无法在规避它的接口上传输流量。例如，互联网上的外部主机可能会被外部接口规避。系统提供被规避的主机的活动记录。此消息和消息 %ASA-4-401005 可用于进一步评估有关此主机的风险。

建议的操作： 无需执行任何操作。

401005

错误消息： `%ASA-4-401005: Shun add failed: unable to allocate resources for IP_address IP_address port port`

说明： Firepower 威胁防御设备内存不足；无法应用规避规则。

建议的操作： 思科 IPS 应继续尝试应用此规则。请尝试回收内存并重新手动应用规避规则，或等待思科 IPS 执行此操作。

402114

错误消息： `%ASA-4-402114: IPSEC: Received an protocol packet (SPI=spi , sequence number=seq_num ) from remote_IP to local_IP with an invalid SPI.`

- >*protocol* - IPsec 协议
- > *spi* - IPsec 安全参数索引
- seq_num> - IPsec 序列号
- remote_IP> - 隧道远程终端的 IP 地址
- >*username* - 与 IPsec 隧道关联的用户名
- local_IP> - 隧道本地终端的 IP 地址

说明： 收到了指定 SA 数据库中不存在的 SPI 的 IPsec 数据包。这可能是 IPsec 对等体之间 SA 老化存在细微差异引起的临时情况，也可能是因为本地 SA 已清除所引起的。这也可能表示 IPsec 对等体发送的数据包不正确，这可能属于攻击操作。此消息的出现频率限制为每五秒内最多一次。

建议的操作： 对等体可能不会确认本地 SA 已清除。如果从本地路由器建立新连接，则这两个对等体随后可能成功地重新建立连接。否则，如果问题持续超过一小段时间，则请尝试建立新连接或联系对等体管理员。

402115

错误消息： `%ASA-4-402115: IPSEC: Received a packet from remote_IP to local_IP containing act_prot data instead of exp_prot data.`

说明： 收到了缺少预期 ESP 报头的 IPsec 数据包。对等体正在发送与协商的安全策略不匹配的数据包，这可能表示受到了攻击。此消息的出现频率限制为每五秒内最多一次。

- remote_IP> - 隧道远程终端的 IP 地址

- local_IP> - 隧道本地终端的 IP 地址
- >*act_prot* - 收到的 IPsec 协议
- >*exp_prot* - 预期 IPsec 协议

建议的操作：联系对等体管理员。

402116

错误消息：`%ASA-4-402116: IPSEC: Received an protocol packet (SPI=spi , sequence number=seq_num) from remote_IP (username) to local_IP .The decapsulated inner packet doesn't match the negotiated policy in the SA.The packet specifies its destination as pkt_daddr , its source as pkt_saddr , and its protocol as pkt_prot .The SA specifies its local proxy as id_daddr /id_dmask /id_dprot /id_dport and its remote proxy as id_saddr /id_smask /id_sprot /id_sport .`

说明：解封的IPsec数据包与协商的身份不匹配。对等体正在通过此安全关联发送其他流量，这可能由对等体的安全关联选择错误引起，或者也可能是攻击操作。此消息的出现频率限制为每五秒内最多一次。

- >*protocol* - IPsec 协议
- > *spi* - IPsec 安全参数索引
- seq_num> - IPsec 序列号
- remote_IP> - 隧道远程终端的 IP 地址
- >*username* - 与 IPsec 隧道关联的用户名
- local_IP> - 隧道本地终端的 IP 地址
- pkt_daddr - 解封的数据包的目的地址
- pkt_saddr> - 解封的数据包的源地址
- pkt_prot> - 解封的数据包的传输协议
- id_daddr> - 本地代理 IP 地址
- id_dmask> - 本地代理 IP 子网掩码
- id_dprot> - 本地代理传输协议
- id_dport> - 本地代理端口
- id_saddr> - 远程代理 IP 地址
- id_smask> - 远程代理 IP 子网掩码
- id_sprot> - 远程代理传输协议
- id_sport> - 远程代理端口

建议的操作：联系对等体管理员，并比较策略设置。

402117

错误消息：`%ASA-4-402117: IPSEC: Received a non-IPsec (protocol ) packet from remote_IP to local_IP .`

说明：收到的数据包与加密映射 ACL 相匹配，但未使用 IPsec 进行封装。IPsec 对等体正在发送未封装的数据包。此错误可能是由于对等体上发生策略设置错误引起的。例如，防火墙可能会配置为仅

接受传输到外部接口端口 23 的加密 Telnet 流量。如果您尝试使用未经 IPsec 加密的 Telnet 访问端口 23 上的外部接口，则会出现此消息，但对外部接口端口 23 以外的端口使用 Telnet 进行访问或发送流量则不会出现此消息。此错误也可能指示受到了攻击。除非是上述情况，否则不会生成此消息（例如，针对传输到 Firepower 威胁防御接口的流量，就不会生成此消息)。请参阅跟踪 TCP 和 UDP 请求的消息 710001、710002 和 710003。此消息的出现频率限制为每五秒内最多一次。

- >*protocol* - IPsec 协议
- remote_IP> - 隧道远程终端的 IP 地址
- local_IP> - 隧道本地终端的 IP 地址

建议的操作：联系对等体管理员，比较各种策略设置。

402118

错误消息：`%ASA-4-402118: IPSEC: Received an protocol packet (SPI=spi , sequence number seq_num ) from remote_IP (username ) to local_IP containing an illegal IP fragment of length frag_len with offset frag_offset .`

说明：解封的 IPsec 数据包包括偏移量小于或等于 128 字节的 IP 分段。最新版本的 IP RFC 安全架构建议采用最小 128 个字节的 IP 分段偏移量以防受到重组攻击。这可能属于攻击操作。此消息的出现频率限制为每五秒内最多一次。

- >*protocol* - IPsec 协议
- > *spi* - IPsec 安全参数索引
- seq_num> - IPsec 序列号
- remote_IP> - 隧道远程终端的 IP 地址
- >*username* - 与 IPsec 隧道关联的用户名
- local_IP> - 隧道本地终端的 IP 地址
- frag_len> - IP 分段长度
- frag_offset> - IP 分段偏移量字节数

建议的操作：联系远程对等体管理员，比较各种策略设置。

402119

错误消息：`%ASA-4-402119: IPSEC: Received an protocol packet (SPI=spi , sequence number=seq_num ) from remote_IP (username ) to local_IP that failed anti-replay checking.`

说明：收到了带有无效序列号的IPsec数据包。对等体正在发送包括先前可能已使用的序列号的数据包。此消息表明，已收到带超出可接受范围的序列号的 IPsec 数据包。Ipsec 将此数据包视为可能与攻击有关而予以丢弃。此消息的出现频率限制为每五秒内最多一次。

- >*protocol* - IPsec 协议
- > *spi* - IPsec 安全参数索引
- seq_num> - IPsec 序列号
- remote_IP> - 隧道远程终端的 IP 地址
- >*username* - 与 IPsec 隧道关联的用户名

- local_IP> - 隧道本地终端的 IP 地址

建议的操作：联系对等体管理员。

402120

错误消息：`%ASA-4-402120: IPSEC: Received an protocol packet (SPI=spi , sequence number=seq_num ) from remote_IP (username ) to local_IP that failed authentication.`

说明：收到了 IPsec 数据包，但此数据包身份验证失败。系统丢弃此数据包。数据包在传输过程中可能已受损，或对等体可能正在发送无效 IPsec 数据包，如果其中许多数据包都来自同一个对等体，则可能表示正在发生攻击。此消息的出现频率限制为每五秒内最多一次。

- >*protocol* - IPsec 协议
- > *spi* - IPsec 安全参数索引
- seq_num> - IPsec 序列号
- remote_IP> - 隧道远程终端的 IP 地址
- >*username* - 与 IPsec 隧道关联的用户名
- local_IP> - 隧道本地终端的 IP 地址

建议的操作：如果收到许多失败的数据包，则联系远程对等体管理员。

402121

错误消息：`%ASA-4-402121: IPSEC: Received an protocol packet (SPI=spi , sequence number=seq_num ) from peer_addr (username ) to lcl_addr that was dropped by IPsec (drop_reason ).`

说明：收到了待解封的 IPsec 数据包，但随后被 IPsec 子系统丢弃。这可能表示 Firepower 威胁防御配置或 Firepower 威胁防御设备本身存在问题。

- >*protocol* - IPsec 协议
- > *spi* - IPsec 安全参数索引
- seq_num> - IPsec 序列号
- peer_addr> - 隧道远程终端的 IP 地址
- >*username* - 与 IPsec 隧道关联的用户名
- lcl_addr> - 隧道本地终端的 IP 地址
- drop_reason> - 数据包被丢弃的原因

建议的操作：如果问题仍然存在，请联系思科 TAC。

402122

错误消息：`%ASA-4-402122: Received a cleartext packet from src_addr to dest_addr that was to be encapsulated in IPsec that was dropped by IPsec (drop_reason ).`

说明：收到了待封装在 IPsec 中的数据包，但随后被 IPsec 子系统丢弃。这可能表示 Firepower 威胁防御 配置或 Firepower 威胁防御设备本身存在问题。

- *src_addr*> - 源 IP 地址

- *dest_addr* > - 目的 > IP 地址
- drop_reason> - 数据包被丢弃的原因

建议的操作：如果问题仍然存在，请联系思科 TAC。

402123

错误消息：`%ASA-4-402123: CRYPTO: The accel_type hardware accelerator encountered an error (code=error_string ) while executing crypto command command .`

说明：使用硬件加速器运行加密命令时检测到错误，这可能表示加速器存在问题。此错误可能由各种原因引起，此消息是对加密加速器计数器的补充，用于帮助确定原因。

- accel_type - 硬件加速器类型
- > *error_string* - 指示错误类型的代码
- command - 生成了此错误的加密命令

建议的操作：如果问题仍然存在，请联系思科 TAC。

402124

错误消息：`%ASA-4-402124: CRYPTO: The ASA hardware accelerator encountered an error (Hardware error address, Core, Hardware error code, IstatReg, PciErrReg, CoreErrStat, CoreErrAddr, Doorbell Size, DoorBell Outstanding, SWReset).`

说明：加密硬件芯片已报告严重错误，指示此芯片不可操作。此消息中的信息包含进一步分析问题所需的详细信息。检测到这种情况时，系统会重置加密芯片，以使Firepower威胁防御设备可以继续运行而不造成任何中断。此外，检测到此问题时所处的加密环境写入闪存上的加密存档目录，以提供更多调试信息。此消息包括与加密硬件相关的各种参数，如下所示：

- HWErrAddr> - 硬件地址（使用加密芯片设置）
- Core> - 遇到错误的加密核心
- HwErrCode> - 硬件错误代码（使用加密芯片设置）
- IstatReg> - 中断状态寄存器（使用加密芯片设置）
- PciErrReg> - PCI 错误寄存器（使用加密芯片设置）
- CoreErrStat> - 核心错误状态（使用加密芯片设置）
- CoreErrAddr> - 核心错误地址（使用加密芯片设置）
- Doorbell Size> - 允许的最大加密命令数量
- DoorBell Outstanding> - 加密命令尚未处理
- SWReset> - 自启动时执行的加密芯片重置次数

注释 %ASA-vpn-4-402124: CRYPTO: The ASA hardware accelerator encountered an error (HWErrAddr= 0x40EE9800, Core= 0, HwErrCode= 23, IstatReg= 0x8, PciErrReg= 0x0, CoreErrStat= 0x41, CoreErrAddr= 0x844E9800, Doorbell Size[0]= 2048, DoorBell Outstanding[0]= 0, Doorbell Size[1]= 0, DoorBell Outstanding[1]= 0, SWReset= 99) 错误消息指示 AnyConnect 存在问题，而且此问题的解决办法是升级到 AnyConnect 3.1.x。

建议的操作：将消息信息转发给思科 TAC，以进行进一步分析。

402125

错误消息：`%ASA-4-402125: The ASA hardware accelerator ring timed out (parameters ).`

说明：加密驱动程序检测到IPSEC描述符环或SSL/管理员描述符环不再有任何进展，这意味着加密芯片不再运行。检测到这种情况时，系统会重置加密芯片，以使Firepower威胁防御设备可以继续运行而不造成任何中断。此外，检测到此问题时所处的加密环境也已写入闪存上的加密存档目录，以提供更多调试信息。

- >*ring* - IPSEC 或管理员环
- *parameters* > - 包括以下参数：

- Desc> - 描述符地址

- CtrlStat> - 控制/状态值

- ResultP> - 成功指针

- ResultVal> - 成功值

- Cmd> - 加密命令

- CmdSize> - 命令大小

- Param> - 命令参数

- Dlen> - 数据长度

- DataP> - 数据指针

- CtxtP> - VPN 情景指针

- SWReset> - 启动后的加密芯片重置次数

建议的操作：将消息信息转发给思科 TAC，以进行进一步分析。

402126

错误消息：`%ASA-4-402126: CRYPTO: The ASA created Crypto Archive File Archive Filename as a Soft Reset was necessary.Please forward this archived information to Cisco.`

说明：检测到硬件加密芯片存在功能问题（请参阅系统日志消息 402124 和 402125）。为了进一步调试加密问题，系统已生成包含当前加密硬件环境的加密存档文件（硬件寄存器和加密描述项）。启动时，已在闪存文件系统上自动创建crypto_archive目录（若以前不存在）。此目录中最多允许存在两个加密存档文件。

- >*Archive Filename* - 加密存档文件的名称。加密存档文件的名称采用 crypto_arch_x.bin 的形式，其中 x =（1 或 2）。

建议的操作：将加密存档文件转发给思科 TAC，以进行进一步分析。

402127

错误消息： `%ASA-4-402127: CRYPTO: The ASA is skipping the writing of latest Crypto Archive File as the maximum # of files, max_number, allowed have been written to archive_directory .Please archive & remove files from Archive Directory if you want more Crypto Archive Files saved.`

说明： 检测到硬件加密芯片存在功能问题（请参阅消息 4402124 和 4402125）。此消息表明尚未写入加密存档文件，这是因为已存在最大数量的加密存档文件。

- *max_number* > - 存档目录中允许存在的文件的最大数量；目前设置为 2
- >*archive_directory* - 存档目录的名称

建议的操作： 将先前生成的加密存档文件转发给思科 TAC。删除先前生成的存档文件，以便在必要时写入更多文件。

402128

错误消息： `%ASA-5-402128: CRYPTO: An attempt to allocate a large memory block failed, size: size , limit: limit`

说明： SSL 连接正在尝试使用超出允许值的内存。请求已被拒绝。

- *size* - 正在分配的内存块的大小
- *limit* - 所分配内存的最大允许大小

建议的操作： 如果此消息仍然存在，则可能正在遭受 SSL 拒绝服务攻击。联系远程对等体管理员或上游提供商。

402129

错误消息： `%ASA-6-402129: CRYPTO: An attempt to release a DMA memory block failed, location: address`

说明： 发生了内部软件错误。

- *address* - 正在释放的地址

建议的操作： 联系思科 TAC 寻求帮助。

402130

错误消息： `%ASA-6-402130: CRYPTO: Received an ESP packet (SPI = 0x54A5C634, sequence number=0x7B) from 75.2.96.101 (user=user) to 85.2.96.10 with incorrect IPsec padding.`

说明： Firepower 威胁防御设备加密硬件加速器已检测到带无效填充的 IPsec 数据包。ATT VPN 客户端有时会错误填充 IPsec 数据包。

- *SPI* - 与该数据包关联的 SPI
- *sequence number* - 与该数据包关联的序列号
- *user* - 用户名符串

- *padding* - 从数据包填充数据

建议的操作：虽然对于此消息不需要执行任何操作，而且此消息并不表明Firepower威胁防御设备存在问题，但是使用 ATT VPN 客户端的客户可能需要升级其 VPN 客户端软件。

402131

错误消息：`%ASA-4-402131: CRYPTO: status changing the accel_instance hardware accelerator's configuration bias from old_config_bias to new_config_bias .`

说明：在 Firepower 威胁防御设备上已更改硬件加速器配置。一些 Firepower 威胁防御平台配备多个硬件加速器。对于每次硬件加速器更改，系统都会生成一条系统日志消息。

- *status* - 表示成功或失败
- *accel_instance* - 硬件加速器实例
- *old_config_bias* - 旧配置
- *new_config_bias* - 新配置

建议的操作：如果在尝试更改加速器配置时任何加速器发生故障，则收集日志记录信息并联系思科 TAC。如果失败，则软件将多此重试配置更改操作。如果重试尝试失败，则软件将回退到原始配置偏差。如果多次尝试重新配置硬件加速器失败，则可能表明出现了硬件故障。

402140

错误消息：`%ASA-3-402140: CRYPTO: RSA key generation error: modulus len len`

说明：RSA 公钥对生成期间出错。

- *len* - 素数模长度（比特）

建议的操作：联系思科 TAC 寻求帮助。

402141

错误消息：`%ASA-3-402141: CRYPTO: Key zeroization error: key set type , reason reason`

说明：RSA 公钥对生成期间出错。

- *type* - 密钥设置类型，可能是以下任何一种：DH、RSA、DSA 或未知
- *reason* - 意外加密会话类型

建议的操作：联系思科 TAC 寻求帮助。

402142

错误消息：`%ASA-3-402142: CRYPTO: Bulk data op error: algorithm alg , mode mode`

说明：对称密钥操作期间出错。

- *op* - 加密或解密操作
- *alg* - 加密算法，可能是以下任何一种：DES、3DES、AES 或 RC4

- *mode* - 模式，可能是以下任何一种：CBC、CTR、CFB、ECB、状态 RC4 或无状态 RC4

建议的操作：联系思科 TAC 寻求帮助。

402143

错误消息：`%ASA-3-402143: CRYPTO: alg type key op`

说明：非对称密钥操作期间出错。

- *alg* - 加密算法，RSA 或 DSA
- *type* - 密钥类型，公钥或私钥
- *op* - 加密或解密操作

建议的操作：联系思科 TAC 寻求帮助。

402144

错误消息：`%ASA-3-402144: CRYPTO: Digital signature error: signature algorithm sig , hash algorithm hash`

说明：全数字化签名生成期间出错。

- *sig* - 签名算法，RSA 或 DSA
- *hash* - 散列算法，可能是以下任何一项：MD5、SHA1、SHA256、SHA384 或 SHA512

建议的操作：联系思科 TAC 寻求帮助。

402145

错误消息：`%ASA-3-402145: CRYPTO: Hash generation error: algorithm hash`

说明：发生了散列生成错误。

- *hash* - 散列算法，可能是以下任何一项：MD5、SHA1、SHA256、SHA384 或 SHA512

建议的操作：联系思科 TAC 寻求帮助。

402146

错误消息：`%ASA-3-402146: CRYPTO: Keyed hash generation error: algorithm hash , key len len`

说明：发生了加密散列生成错误。

- *hash* - 散列算法，可能是以下任何一项：MD5、SHA1、SHA256、SHA384 或 SHA512
- *len* - 密钥长度（比特）

建议的操作：联系思科 TAC 寻求帮助。

402147

错误消息： `%ASA-3-402147: CRYPTO: HMAC generation error: algorithm alg`

说明： 发生了 HMAC 生成错误。

- *alg* - HMAC 算法，可能是以下任何一种：HMAC-MD5 HMAC-SHA1、HMAC-SHA2 或 AES XCBC

建议的操作： 联系思科 TAC 寻求帮助。

402148

错误消息： `%ASA-3-402148: CRYPTO: Random Number Generator error`

说明： 发生了随机数字生成器错误。

建议的操作： 联系思科 TAC 寻求帮助。

402149

错误消息： `%ASA-3-402149: CRYPTO: weak encryption type (length ).Operation disallowed.Not FIPS 140-2 compliant`

说明： Firepower 威胁防御设备尝试了使用长度小于 2048 位或 DH 组 1、2 或 5 的 RSA 密钥。

- *encryption type* - 加密类型
- *length* - RSA 密钥长度或 DH 组编号

建议的操作： 配置 Firepower 威胁防御设备或外部应用，以使用长度至少为 2048 位的 RSA 密钥或配置 1、2 或 5 以外的 DH 组。

402150

错误消息： `%ASA-3-402150: CRYPTO: Deprecated hash algorithm used for RSA operation (hash alg ).Operation disallowed.Not FIPS 140-2 compliant`

说明： 不可接受的散列算法被用于数字证书签名或 FIPS 140-2 认证验证。

- *operation* - 签名或验证
- *hash alg* - 不可接受的散列算法的名称

建议的操作： 确保将最小的可接受散列算法用于数字证书签名或FIPS 140-2 认证验证，包括 SHA-256、SHA-384 和 SHA-512。

403500

错误消息： `%ASA-6-403500: PPPoE - Service name 'any' not received in PADO.Intf:interface_name AC:ac_name .`

说明：Firepower 威胁防御设备已从互联网运营商访问控制器请求 PPPoE 服务 *any*。运营商响应包括其他服务，但不包括服务 *any*。这是协议实施方面的差异。PADO 数据包正常处理，并且连接协商继续进行。

建议的操作：无需执行任何操作。

403501

错误消息：`%ASA-3-403501: PPPoE - Bad host-unique in PADO - packet dropped.Intf:interface_name AC:ac_name`

说明：Firepower 威胁防御设备向访问控制器发送了一个称为主机唯一值的标识符。访问控制器以其他主机唯一值作出响应。Firepower 威胁防御设备无法识别此响应对应的连接请求。数据包已被丢弃，并且连接协商也已中断。

建议的操作：联系互联网运营商。互联网运营商访问控制器正在错误处理主机唯一值，或正在伪造 PADO 数据包。

403502

错误消息：`%ASA-3-403502: PPPoE - Bad host-unique in PADS - dropping packet.Intf:interface_name AC:ac_name`

说明：Firepower 威胁防御设备向访问控制器发送了一个称为主机唯一值的标识符。访问控制器以其他主机唯一值作出响应。Firepower 威胁防御设备无法识别此响应对应的连接请求。数据包已被丢弃，并且连接协商也已中断。

建议的操作：联系互联网运营商。互联网运营商访问控制器正在错误处理主机唯一值，或正在伪造 PADO 数据包。

403503

错误消息：`%ASA-3-403503: PPPoE:PPP link down:reason`

说明：PPP 链路已关闭。发生这种情况的原因有很多。如果 PPP 提供了一个原因，则第一个格式将显示此原因。

建议的操作：检查网络链路，确保链路已连接。访问集中器可能已关闭。请确保身份验证协议与访问集中器相匹配，同时确保用户名和密码正确。向 ISP 或网络支持人员验证此信息。

403504

错误消息：`%ASA-3-403504: PPPoE:No 'vpdn group group_name ' for PPPoE is created`

说明：PPPoE 在开始 PPPoE 会话之前需要进行拨出配置。一般情况下，配置应指定拨号策略、PPP 身份验证、用户名和密码。以下示例为 PPPoE 拨出配置了 Firepower 威胁防御设备。my-username 和 my-password 命令用于对访问集中器进行身份验证，必要时使用 PAP 执行此操作。

例如：

```
ciscoasa# vpdn group my-pppoe request dialout pppoe
ciscoasa# vpdn group my-pppoe ppp authentication pap
ciscoasa# vpdn group my-pppoe localname my-username
ciscoasa# vpdn username my-username password my-password
ciscoasa# ip address outside pppoe setroute
```

建议的操作：为 PPPoE 配置 VPDN 组。

403505

错误消息：`%ASA-4-403505: PPPoE:PPP - Unable to set default route to IP_address at interface_name`

说明：此消息通常出现在“默认路由已存在”消息之前。

建议的操作：删除当前默认路由或删除 *setroute* 参数，从而使 PPPoE 与手动配置路由之间不存在任何冲突。

403506

错误消息：`%ASA-4-403506: PPPoE:failed to assign PPP IP_address netmask netmask at interface_name`

说明：此消息出现在以下任一消息之前：子网与接口相同或在故障切换通道上。

建议的操作：在第一种情况下，更改导致冲突的地址。在第二种情况下，在除故障切换接口以外的接口上配置 PPPoE。

403507

错误消息：`%ASA-3-403507: PPPoE:PPPoE client on interface interface failed to locate PPPoE vpdn group group_name`

说明：可以输入 **pppoe client vpdn group group_name** 命令，在接口上将 PPPoE 客户端配置为使用特定 VPDN 组。如果在系统启动期间未找到此配置名称的 PPPoE VPDN 组，则会生成此消息。

- *interface* - PPPoE 客户端发生故障的接口
- *group_name* - 此接口上 PPPoe 客户端的 VPDN 组名称

建议的操作：执行以下步骤：

1. 输入 **vpdn group group_name** 命令来添加需要的 VPDN 组。在全局配置模式下请求拨出 PPPoE 并添加所有组属性。
2. 从指示接口删除 **pppoe client vpdn group** *group_name* 命令。在这种情况下，PPPoE 客户端将尝试使用定义的第一个 PPPoE VPDN 组。

注释 输入 **ip address pppoe** 命令重新启动接口上的 PPPoE 客户端后，所有更改才会生效。

405001

错误消息： `%ASA-4-405001: Received ARP {request | response} collision from IP_address /MAC_address on interface interface_name with existing ARP entry IP_address /MAC_address`

说明： Firepower 威胁防御设备收到了 ARP 数据包，并且数据包中的 MAC 地址与 ARP 缓存条目不同。

建议的操作： 此流量可能是合法的，也可能指示系统正在遭受 ARP 毒化攻击。检查源 MAC 地址，确定数据包来源并查看数据包是否属于有效主机。

405002

错误消息： `%ASA-4-405002: Received mac mismatch collision from IP_address /MAC_address for authenticated host`

说明： 发生以下一种情况时，此数据包便会显示：

- Firepower 威胁防御设备收到了具有相同 IP 地址的数据包，但其 MAC 地址不同于其未经授权条目。
- 您在 Firepower 威胁防御设备上配置了 **vpnclient mac-exempt** 命令，并且 Firepower 威胁防御设备收到了带有豁免 MAC 地址的数据包，但其 IP 地址不同于相应的未经授权条目。

建议的操作： 此流量可能是合法的，也可能指示系统正在遭受欺骗攻击。检查源 MAC 地址和 IP 地址，确定数据包来源并查看数据包是否属于有效主机。

405003

错误消息： `%ASA-4-405003: IP address collision detected between host IP_address at MAC_address and interface interface_name , MAC_address .`

说明： 网络中的客户端 IP 地址与 Firepower 威胁防御接口 IP 地址是相同的。

建议的操作： 更改客户端的 IP 地址。

405101

错误消息： `%ASA-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for foreign_address outside_address [/outside_port ] to local_address inside_address [/inside_port ]`

说明： 启动连接时，模块未能分配 RAM 系统内存或没有更多可用的地址转换插槽。

建议的操作： 如果定期出现此消息，可以忽略。您可以对比内部网络客户端数量来检查全局池的大小。可能需要 PAT 地址。或者，缩短转换和连接的超时间隔。此错误消息还可能由内存不足引起；尝试降低内存使用量，或购买更多内存。如果问题仍然存在，请联系思科 TAC。

405102

错误消息： `%ASA-4-405102: Unable to Pre-allocate H245 Connection for foreign_address outside_address [/outside_port ] to local_address inside_address [/inside_port ]`

说明： Firepower威胁防御设备未能在启动连接时分配RAM系统内存或没有更多地址转换插槽可用。

建议的操作： 您可以对比内部网络客户端数量来检查全局池的大小。可能需要 PAT 地址。或者，缩短转换和连接的超时间隔。此外，还可以降低内存使用量，或购买更多内存。如果定期出现此消息，可以忽略。如果问题仍然存在，请联系思科 TAC。

405103

错误消息： `%ASA-4-405103: H225 message from source_address/source_port to dest_address /dest_port contains bad protocol discriminator hex`

说明： Firepower 威胁防御设备期望收到协议鉴别符 0x08，但收到的却不是 0x08。终端可能正在发送不良数据包，或收到了不同于第一个分段的消息分段。允许此数据包通过。

建议的操作： 无需执行任何操作。

405104

错误消息： `%ASA-4-405104: H225 message received from outside_address /outside_port to inside_address /inside_port before SETUP`

说明： 在初始设置消息之前收到了顺序混乱的 H.225 消息，这种情况是绝对禁止的。Firepower 威胁防御设备必须在接收任何其他 H.225 消息之前收到 H.225 呼叫信令通道的初始设置消息。

建议的操作： 无需执行任何操作。

405105

错误消息： `%ASA-4-405105: H323 RAS message AdmissionConfirm received from source_address /source_port to dest_address /dest_port without an AdmissionRequest`

说明： 网守已发送 ACF，但 Firepower 威胁防御设备未向网守发送 ARQ。

建议的操作： 使用指定的**source_address**检查网守，以确定网守在未从Firepower威胁防御设备处收到 ARQ 的情况下发送 ACF 的原因。

406001

错误消息： `%ASA-4-406001: FTP port command low port: IP_address /port to IP_address on interface interface_name`

说明： 客户端输入了FTP端口命令，并提供了小于1024（在通常专用于服务器端口的公认端口范围内）的端口。这表明它尝试避免站点安全策略。Firepower威胁防御设备丢弃数据包，终止连接，并记录此事件。

建议的操作： 无需执行任何操作。

406002

错误消息： `%ASA-4-406002: FTP port command different address: IP_address(IP_address ) to IP_address on interface interface_name`

说明： 客户端输入了 FTP 端口命令，并提供了不同于连接中所使用地址的地址。客户端执行了避免站点安全策略的尝试。例如，攻击者可能会尝试通过更改正在传输的数据包以及正确源信息以外的其他源信息来劫持FTP会话。Firepower威胁防御设备丢弃数据包，终止连接，并记录此事件。括号中的地址是端口命令提供的地址。

建议的操作： 无需执行任何操作。

407001

错误消息： `%ASA-4-407001: Deny traffic for local-host interface_name :inside_address , license limit of number exceeded`

说明： 超出了主机限制。满足以下一个条件时，内部主机便会计入限制：

- 内部主机已在过去五分钟内通过 Firepower 威胁防御设备转发流量。
- 内部主机已保留 Firepower 威胁防御设备处的转换连接或用户身份验证。

建议的操作： 在低端平台上强制实施主机限制。使用 **show version** 命令查看主机限制。使用 **show local-host** 命令查看当前活动主机和在 Firepower 威胁防御设备开展会话的内部用户。要强制断开一个或多个用户，请使用 **clear local-host** 命令。要使内部用户限制更快过期，请将转换、连接和未授权超时设置为下表给定的推荐值或更低值：

表 *3:* 超时值和推荐值

超时	推荐值
转换	00:05:00（5 分钟）
连接	00:01:00（1 小时）
未授权	00:05:00（5 分钟）

407002

错误消息： `%ASA-4-407002: Embryonic limit nconns /elimit for through connections exceeded.outside_address /outside_port to global_address (inside_address )/inside_port on interface interface_name`

说明： 从指定全局地址的指定外部地址到指定本地地址的连接数量超出了静态条件下的最大初期限制。如果Firepower威胁防御设备能够为连接分配内存，则会尝试接受此连接。它代表本地主机执行

代理服务，并向外部主机发送SYN_ACK数据包。Firepower威胁防御设备保留相关状态信息，丢弃数据包，并等待客户端确认。此消息可能表示流量合法或系统正在遭受DoS攻击。

建议的操作：检查源地址，确定数据包来源，同时确定数据包是否由有效主机发送。

407003

错误消息：`%ASA-4-407003: Established limit for RPC services exceeded number`

说明：Firepower威胁防御设备已尝试针对一对在达到最大孔数后配置的RPC服务器或服务打开一个新孔。

建议的操作：等待其他孔关闭（通过相关超时到期），或限制活动服务器或服务对的数量。

408001

错误消息：`%ASA-4-408001: IP route counter negative - reason , IP_address Attempt: number`

说明：将IP路由计数器数量递减至负值的尝试失败。

建议的操作：输入 **clear ip route** 命令重置路由计数器。如果问题仍然存在，请联系思科TAC。

408002

错误消息： `%ASA-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1 ] via source IP :interface1 address2 netmask2 [distance2 /metric2 ] interface2`

说明：从与现有路由具有相同距离但更高度量的其他接口收到了网络更新。新路由会覆盖通过其他接口安装的现有路由。新路由仅用于冗余目的，表示路径已在网络中转移。必须通过拓扑和重新分发控制此更改。受此更改影响的任何现有连接都可能被禁用，并将超时。只有在已专门设计网络拓扑以支持路径冗余的情况下，才会发生这种路径转移，在这种情况下属于预期行为。

建议的操作：无需执行任何操作。

408003

错误消息：`%ASA-4-408003: can't track this type of object hex`

说明：跟踪系统组件遇到了组件不支持的对象类型。组件的预期为状态对象。

- *hex* - 描述变量值或内存中地址的十六进制值

建议的操作：重新配置跟踪对象以使其成为状态对象。

409001

错误消息：`%ASA-4-409001: Database scanner: external LSA IP_address netmask is lost, reinstalls`

说明：软件检测到意外情况。路由器将采取纠正措施并继续运行。

建议的操作：无需执行任何操作。

409002

错误消息：`%ASA-4-409002: db_free: external LSA IP_address netmask`

说明：发生了内部软件错误。

建议的操作：无需执行任何操作。

409003

错误消息：`%ASA-4-409003: Received invalid packet: reason from IP_address , interface_name`

说明：收到无效的 OSPF 数据包。错误消息中包含详细信息。原因可能是 OSPF 配置不正确或发件人存在内部错误。

建议的操作：检查收件人 OSPF 配置和发件人配置是否不一致。

409004

错误消息：`%ASA-4-409004: Received reason from unknown neighbor IP_address`

说明：收到了 OSPF Hello、数据库说明或数据库请求数据包，但路由器无法识别发件人。

建议的操作：无需执行任何操作。

409005

错误消息：`%ASA-4-409005: Invalid length number in OSPF packet from IP_address (ID IP_address ), interface_name`

说明：Firepower 威胁防御设备收到了字段长度小于正常报头大小或与所接收 IP 数据包大小不一致的 OSPF 数据包。这表示数据包发件人存在配置错误。

建议的操作：通过相邻地址找到问题路由器并重新启动此路由器。

409006

错误消息：`%ASA-4-409006: Invalid lsa: reason Type number , LSID IP_address from IP_address , IP_address , interface_name`

说明：路由器收到包含无效 LSA 类型的 LSA。原因是内存损坏或路由器上的意外行为。

建议的操作：通过相邻地址找到问题路由器并重新启动此路由器。如果问题仍然存在，请联系思科 TAC。

409007

错误消息： `%ASA-4-409007: Found LSA with the same host bit set but using different mask LSA ID IP_address netmask New: Destination IP_address netmask`

说明： 发生了内部软件错误。

建议的操作： 按照显示正确复制此消息，并将其报告给思科 TAC。

409008

错误消息： `%ASA-4-409008: Found generating default LSA with non-zero mask LSA type: number Mask: netmask metric: number area: string`

说明： 由于发生内部软件错误，路由器尝试生成带有错误掩码和可能错误度量的默认 LSA。

建议的操作： 按照显示正确复制此消息，并将其报告给思科 TAC。

409009

错误消息： `%ASA-4-409009: OSPF process number cannot start.There must be at least one up IP interface, for OSPF to use as router ID`

说明： OSPF 尝试从一个接口的 IP 地址分配路由器 ID 时失败。

建议的操作： 请确保至少启用一个具有有效 IP 地址的接口。如果有多个 OSPF 进程在路由器上运行，则每个进程都需要唯一的路由器ID。您必须拥有足够数量的接口，以便每个接口均可获得路由器 ID。

409010

错误消息：`%ASA-4-409010: Virtual link information found in non-backbone area: string`

说明： 发生了内部错误。

建议的操作： 按照显示正确复制此消息，并将其报告给思科 TAC。

409011

错误消息： `%ASA-4-409011: OSPF detected duplicate router-id IP_address from IP_address on interface interface_name`

说明： OSPF 从与此路由进程具有相同路由器 ID 的邻居接收了 Hello 数据包。无法建立完全邻接关系。

建议的操作： OSPF 路由器 ID 应该具有唯一性。更改邻居路由器 ID。

409012

错误消息： `%ASA-4-409012: Detected router with duplicate router ID IP_address in area string`

说明：OSPF 从与此路由进程具有相同路由器 ID 的邻居接收了 Hello 数据包。无法建立完全邻接关系。

建议的操作：OSPF 路由器 ID 应该具有唯一性。更改邻居路由器 ID。

409013

错误消息：`%ASA-4-409013: Detected router with duplicate router ID IP_address in Type-4 LSA advertised by IP_address`

说明：OSPF 从与此路由进程具有相同路由器 ID 的邻居接收了 Hello 数据包。无法建立完全邻接关系。

建议的操作：OSPF 路由器 ID 应该具有唯一性。更改邻居路由器 ID。

409023

错误消息：`%ASA-4-409023: Attempting AAA Fallback method method_name for request_type request for user user :Auth-server group server_tag unreachable`

说明：尝试对外部服务器进行身份验证或授权失败，系统将使用本地用户数据库执行操作。

- **aaa_operation** - 身份验证或授权
- **username** - 与该连接关联的用户
- **server_group** - 其中的服务器无法到达的 AAA 服务器名称

建议的操作：对采用第一种方法配置的 AAA 服务器调查任何连接问题。对来自 Firepower 威胁防御设备 的身份验证服务器执行 Ping 操作。请确保在 AAA 服务器中运行守护程序。

409101

错误消息：`%ASA-4-409101: Received invalid packet: s from P , s`

说明：收到无效的 OSPF 数据包。错误消息中包含详细信息。原因可能是 OSPF 配置错误或发件人存在内部错误。

建议的操作：检查收件人和发件人的 OSPF 配置中的不一致。

409102

错误消息：`%ASA-4-409102: Received packet with incorrect area from P , s , area AREA_ID_STR , packet area AREA_ID_STR`

说明：收到 OSPF 数据包，其报头中包含的区域 ID 与此接口区域不匹配。

建议的操作：检查收件人和发件人的 OSPF 配置中的不一致。

409103

错误消息：`%ASA-4-409103: Received s from unknown neighbor i`

说明：收到 EIGRP Hello、数据库说明或数据库请求数据包，但路由器无法识别发件人。

建议的操作：无需执行任何操作。

409104

错误消息：`%ASA-4-409104: Invalid length d in OSPF packet type d from P (ID i ), s`

说明：系统收到一个 OSPF 数据包，其长度字段小于正常报头大小，或与其到达的 IP 数据包大小不一致。数据包发件人出现了错误。

建议的操作：无需执行任何操作。

409105

错误消息：`%ASA-4-409105: Invalid lsa: s : Type 0x x , Length 0x x , LSID u from i`

说明：路由器收到包含无效数据的LSA。由于内存损坏或路由器上的意外行为，导致该LSA包含无效的 LSA 类型、不正确的校验和或不正确的长度。

建议的操作：从相邻地址找到问题路由器，并执行以下操作：

- 输入 **show running-config** 命令，收集路由器的运行配置。
- 输入 **show ipv6 ospf database** 命令，收集可能有助于识别错误性质的数据。
- 输入 **show ipv6 ospf database** *link-state-id* 命令。*link-state-id* 参数是无效 LSA 的 IP 地址。
- 输入 **show logging** 命令，收集可能有助于识别错误性质的数据。
- 重新启动路由器。

如果无法根据收集的信息确定错误性质，请联系思科 TAC 并提供所收集的信息。

409106

错误消息： `%ASA-4-409106: Found generating default LSA with non-zero mask LSA type: 0x x Mask: i metric: lu area: AREA_ID_STR`

说明：由于内部软件错误，路由器尝试生成包含错误掩码和可能错误的度量的默认 LSA。

建议的操作：无需执行任何操作。

409107

错误消息：`%ASA-4-409107: OSPFv3 process d could not pick a router-id, please configure manually`

说明：OSPFv3 尝试从其中一个接口的 IP 地址分配路由器 ID 时失败。

建议的操作：请确保至少启用一个具有有效 IP 地址的接口。如果有多个 OSPF 进程在路由器上运行，则每个进程都需要唯一的路由器ID。您必须拥有足够的已启用接口，以便每个接口均可获得路由器 ID。

409108

错误消息： `%ASA-4-409108: Virtual link information found in non-backbone area: AREA_ID_STR`

说明： 发生了内部错误。

建议的操作： 无需执行任何操作。

409109

错误消息： `%ASA-4-409109: OSPF detected duplicate router-id i from P on interface IF_NAME`

说明： OSPF 从与此路由进程具有相同路由器 ID 的邻居接收了 Hello 数据包。无法建立完全邻接关系。OSPF 路由器 ID 应该具有唯一性。

建议的操作： 更改邻居路由器 ID。

409110

错误消息： `%ASA-4-409110: Detected router with duplicate router ID i in area AREA_ID_STR`

说明： OSPF 从与此路由进程具有相同路由器 ID 的邻居接收了 Hello 数据包。无法建立完全邻接关系。OSPF 路由器 ID 应该具有唯一性。

建议的操作： 更改邻居路由器 ID。

409111

错误消息： `%ASA-4-409111: Multiple interfaces (IF_NAME /IF_NAME ) on a single link detected.`

说明： 不支持在同一链路上多个接口中启用 OSPFv3。

建议的操作： 除一个接口外，应当在其他所有接口上禁用 OSPFv3 或将其设置为被动模式。

409112

错误消息： `%ASA-4-409112: Packet not written to the output queue`

说明： 发生了内部错误。

建议的操作： 无需执行任何操作。

409113

错误消息： `%ASA-4-409113: Doubly linked list linkage is NULL`

说明： 发生了内部错误。

建议的操作： 无需执行任何操作。

409114

错误消息： `%ASA-4-409114: Doubly linked list prev linkage is NULL x`

说明： 发生了内部错误。

建议的操作： 无需执行任何操作。

409115

错误消息： `%ASA-4-409115: Unrecognized timer d in OSPF s`

说明： 发生了内部错误。

建议的操作： 无需执行任何操作。

409116

错误消息： `%ASA-4-409116: Error for timer d in OSPF process s`

说明： 发生了内部错误。

建议的操作： 无需执行任何操作。

409117

错误消息： `%ASA-4-409117: Can't find LSA database type x , area AREA_ID_STR , interface x`

说明： 发生了内部错误。

建议的操作： 无需执行任何操作。

409118

错误消息： `%ASA-4-409118: Could not allocate DBD packet`

说明： 发生了内部错误。

建议的操作： 无需执行任何操作。

409119

错误消息： `%ASA-4-409119: Invalid build flag x for LSA i , type 0x x`

说明： 发生了内部错误。

建议的操作： 无需执行任何操作。

409120

错误消息： `%ASA-4-409120: Router-ID i is in use by ospf process d`

说明：Firepower 威胁防御设备尝试分配一个其他进程正在使用的路由器 ID。

建议的操作：为其中一个进程配置其他路由器 ID。

409121

错误消息：`%ASA-4-409121: Router is currently an ASBR while having only one area which is a stub area`

说明：ASBR 必须连接到可以承载 AS 外部或 NSSA LSA 的区域。

建议的操作：将路由器连接的区域调整为 NSSA 区域或常规区域。

409122

错误消息：`%ASA-4-409122: Could not select a global IPv6 address.Virtual links require at least one global IPv6 address.`

说明：已配置虚拟链路。要让虚拟链路正常运行，必须具备全局 IPv6 地址。但是，并未在路由器中找到全局 Ipv6 地址。

建议的操作：在此路由器的接口上配置全局 IPv6 地址。

409123

错误消息：`%ASA-4-409123: Neighbor command allowed only on NBMA networks`

说明：仅允许在 NBMA 网络中使用 **neighbor** 命令。

建议的操作：检查 **neighbor** 命令的配置选项，为邻居接口更正选项或网络类型。

409125

错误消息： `%ASA-4-409125: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network`

说明：在点对多点网络上发现了已配置的邻居，并且配置了轮询或优先级选项。仅允许在NBMA类型网络上使用这些选项。

建议的操作：检查 **neighbor** 命令的配置选项，为邻居接口更正选项或网络类型。

409128

错误消息：`%ASA-4-409128: OSPFv3-`*`d`* `Area` *`AREA_ID_STR`* `: Router` *`i`* `originating invalid type 0x` *`x`* `LSA, ID` *`u`* `, Metric` *`d`* `on Link ID` *`d`* `Link Type` *`d`*

说明：此消息中指示的路由器已发起具有无效度量的LSA。如果这是一个路由器LSA且链路度量为零，则网络中存在路由环路和流量损失的风险。

建议的操作：为发起所报告 LSA 的路由器中的给定 LSA 类型和链路类型配置有效度量。

ID 介于 410001 到 450001 之间的消息

本章包含 ID 介于 410001 到 450001 之间的消息。

410001

错误消息：`%ASA-4-410001: UDP DNS request from source_interface :source_address /source_port to dest_interface :dest_address /dest_port ; (label length | domain-name length) 52bytes exceeds remaining packet length of 44 bytes.`

说明：UDP DNS 数据包中的域名长度超过 255 个字节。请参阅 RFC 1035 第 3.1 部分以了解详细信息。

建议的操作：无需执行任何操作。

411001

错误消息：`%ASA-4-411001: Line protocol on interface interface_name changed state to up`

说明：线路协议状态已从关闭改为开启。如果 **interface_name** 是逻辑接口名称（例如内部接口和外部接口），此消息表示逻辑接口线路协议已从关闭改为开启状态。如果 **interface_name** 是物理接口名称（例如 Ethernet0 和 GigabitEthernet0/1），此消息表示物理接口线路协议已从关闭改为开启状态。

建议的操作：无需执行任何操作。

411002

错误消息：`%ASA-4-411002:Line protocol on interface interface_name changed state to down`

说明：线路协议状态已从开启改为关闭。如果 **interface_name** 是逻辑接口名称（例如内部接口和外部接口），此消息表示逻辑接口线路协议已从开启改为关闭状态。在这种情况下，物理接口线路协议状态不受影响。如果 **interface_name** 是物理接口名称（例如 Ethernet0 和 GigabitEthernet0/1），此消息表示物理接口线路协议已从开启改为关闭状态。

建议的操作：如果这是接口上的意外事件，请检查物理线路。

411003

错误消息：`%ASA-4-411003: Configuration status on interface interface_name changed state to downup`

说明：接口的配置状态已从关闭改为开启。

建议的操作：如果这是意外事件，请检查物理线路。

411004

错误消息： `%ASA-4-411004: Configuration status on interface interface_name changed state to up`

说明： 接口的配置状态已从关闭改为开启。

建议的操作： 无需执行任何操作。

411005

错误消息： `%ASA-4-411005: Interface variable 1 experienced a hardware transmit hang.The interface has been reset.`

说明： 接口遇到硬件传输冻结，需要重置以太网控制器，使接口完全恢复运行。

- *variable 1* - 接口名称，例如 GigabitEthernet0/0

建议的操作： 无需执行任何操作。

412001

错误消息： `%ASA-4-412001:MAC MAC_address moved from interface_1 to interface_2`

说明： 系统检测到主机在模块接口间移动。在透明 Firepower 威胁防御 中，主机 (MAC) 与 Firepower 威胁防御 端口之间的映射将在第 2 层转发表中维护。该表会将数据包源 MAC 地址与 Firepower 威胁防御 端口动态绑定。在此过程中，只要检测到主机在不同接口间移动，就会生成此消息。

建议的操作： 主机移动可能有效，也可能是尝试伪造其他接口上的主机 MAC。如果这是一次 MAC 欺骗尝试，您可以找出网络中易受攻击的主机，然后将其删除或配置静态 MAC 条目，静态条目不允许更改 MAC 地址和端口绑定。如果的确是主机移动，则无需任何操作。

412002

错误消息： `%ASA-4-412002:Detected bridge table full while inserting MAC MAC_address on interface interface .Number of entries = num`

说明： 桥接表已满，但系统尝试再添加一个条目。Firepower 威胁防御设备 可为每个情景维护单独的第 2 层转发表，但是每当情景超过其大小限制时都会生成此消息。系统将添加 MAC 地址，但它将取代表中最早的现有动态条目（如可用）。这可能是攻击尝试。

建议的操作： 确保新的桥接表条目有效。如果出现攻击，请使用 EtherType ACL 控制对易受攻击主机的访问。

413001

错误消息： `%ASA-4-413001: Module module_id is not able to shut down.Module Error: errnum message`

说明：由 *module_id* 标识的模块无法按照 Firepower 威胁防御 系统模块的请求关闭。此模块可能正在执行不能中断的任务，例如软件升级。**errnum** 和 **message** 文本说明了此模块无法关闭的原因，以及推荐的纠正操作。

建议的操作：等待模块上的任务完成后再关闭此模板，或使用 **session** 命令访问模块上的 CLI 并停止阻止此模块关闭的任务。

413002

错误消息： `%ASA-4-413002: Module module_id is not able to reload.Module Error: errnum message`

说明：由 *module_id* 标识的模块无法按照 Firepower 威胁防御 模块的请求重新加载。此模块可能正在执行不能中断的任务，例如软件升级。**errnum** 和 **message** 文本说明了此模块无法重新加载的原因，以及推荐的纠正操作。

建议的操作：等待此模块上的任务完成后再重新加载模板，或使用 **session** 命令访问此模块上的 CLI 并停止阻止此模块重新加载的任务。

413003

错误消息：`%ASA-4-413003: Module string one is not a recognized type`

说明：系统检测到模块未被识别为有效的模块类型。

建议的操作：将 Firepower 威胁防御 软件升级到支持已安装模块类型的版本。

413004

错误消息：`%ASA-4-413004: Module string one failed to write software newver (currently ver ), reason .Trying again.`

说明：此模块无法接受软件版本，并将转换到无响应状态。系统还会尝试更新模块软件。

- >*string one* - 指定模块的文本字符串
- >*newver* - 未成功写入模块的软件的新版本号（例如，1.0(1)0）
- >*ver* - 模块上软件的当前版本号（例如，1.0(1)0）
- >*reason* - 新版本无法写入此模块的原因。>*reason* 的可能值包括：

- 写入失败

- 映像写入线程创建失败

建议的操作：无需执行任何操作。后续尝试操作将生成一条消息，指示更新成功或失败。使用 **show module** 命令尝试进行后续更新后，可以验证模块是否转换为 UP 状态。

413005

错误消息：`%ASA-4-413005: Module module_id , application is not supported app_name version app_vers type app_type`

错误消息：%ASA-4-413005: Module *prod_id* in slot *slot_num* , application is not supported *app_name* version *app_vers* type *app_type*

说明：插槽 *slot_num* 中安装的模块正在运行不受支持的应用版本或类型。

- *module_id* - 软件服务模块的名称
- *prod_id* - 产品 ID 字符串
- *slot_num* - 安装此模块的插槽号。插槽 0 表示系统主板，插槽 1 表示扩展槽中安装的模块。
- *app_name* - 应用名称（字符串）
- *app_vers* - 应用版本（字符串）
- *app_type* - 应用类型（十进制）

建议的操作：如果问题仍然存在，请联系思科 TAC。

413006

错误消息：`%ASA-4-413006: prod-id Module software version mismatch; slot slot is prod-id version running-vers .Slot slot prod-id requires required-vers .`

说明：插槽 *slot* 中的模块上运行的软件版本不是其他模块所需的版本。

- *slot* - 插槽 0 表示系统主板。插槽 1 表示在扩展插槽中安装的模块。
- *prod_id* - 插槽 *slot* 中安装的设备的产品 ID 字符串
- *running_vers* - 插槽 *slot* 中安装的模块上当前运行的软件版本
- *required_vers* - 插槽 *slot* 中模块所需的软件版本

建议的操作：如果问题仍然存在，请联系思科 TAC。

414001

错误消息：`%ASA-3-414001: Failed to save logging buffer using file name filename to FTP server ftp_server_address on interface interface_name : [fail_reason ]`

说明：日志记录模块无法将日志缓冲区保存到外部 FTP 服务器中。

建议的操作：根据失败原因执行适当操作：

- 协议错误 - 请确保 FTP 服务器和 Firepower 威胁防御设备 之间不存在连接问题，且 FTP 服务器可以接受 FTP 端口命令和 PUT 请求。
- 用户名或密码无效 - 确保配置的 FTP 客户端用户名和密码正确无误。
- 所有其他错误 - 如果问题仍然存在，请联系思科 TAC。

414002

错误消息：`%ASA-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: filename : [fail_reason ]`

说明：日志记录模块无法将日志缓冲区保存到系统闪存中。

建议的操作：如果操作失败的原因是由于空间不足，则检查闪存的可用空间，并确保**logging flash-size**命令的配置限制设置正确。如果是闪存文件系统 I/O 错误，请联系思科 TAC 获取帮助。

414003

错误消息：`%ASA-3-414003: TCP Syslog Server intf : IP_Address /port not responding.New connections are [permitted|denied] based on logging permit-hostdown policy.`

说明：用于远程主机日志记录的 TCP 系统日志服务器成功连接到服务器，并且系统将根据日志记录 permit-hostdown 策略允许或拒绝新连接。如果已配置日志记录 permit-hostdown 策略，则允许新连接。如果未配置，新连接将被拒绝。

- *intf* - 服务器连接的 Firepower 威胁防御设备的接口
- *IP_Address* - 远程 TCP 系统日志服务器的 IP 地址
- *port* - 远程 TCP 系统日志服务器的端口

建议的操作：验证已配置 TCP 系统日志服务器是否启动。要允许新连接，请配置日志记录 permit-hostdown 策略。要拒绝新连接，请勿配置日志记录 permit-hostdown 策略。

414005

错误消息：`%ASA-3-414005: TCP Syslog Server intf : IP_Address /port connected, New connections are permitted based on logging permit-hostdown policy`

说明：用于远程主机日志记录的 TCP 系统日志服务器成功连接到服务器，并且系统将根据日志记录 permit-hostdown 策略允许新连接。如果已配置日志记录 permit-hostdown 策略，则允许新连接。

- *intf* - 服务器连接的 Firepower 威胁防御设备的接口
- *IP_Address* - 远程 TCP 系统日志服务器的 IP 地址
- *port* - 远程 TCP 系统日志服务器的端口

建议的操作：无需执行任何操作。

414006

错误消息：`%ASA-3-414006: TCP Syslog Server configured and logging queue is full.New connections denied based on logging permit-hostdown policy.`

说明：日志记录队列接近配置限制，系统日志消息存在被丢弃的风险。

建议的操作：请参阅《CLI 配置指南》中的“配置日志记录队列”部分，了解有关如何调整队列大小以避免上述情况的信息。在这种情况下，如果您想拒绝新连接，请使用**no logging permit-hostdown**命令。在这种情况下，如果您想允许新连接，请使用 **logging permit-hostdown** 命令。

415020

错误消息： `%ASA-5-415020: HTTP - matched matched_string in policy-map map_name , a non-ASCII character was matched connection_action from int_type :IP_address /port_num to int_type :IP_address /port_num`

说明：找到非 ASCII 字符。

- **matched_string** - 匹配字符串属于以下内容之一：

- 类映射 ID，后跟类映射名称。用户配置类映射时，系统将显示该字符串。

- 发起该消息的实际 **match** 命令。类映射在内部时，系统将显示该字符串。

- *map_name* - 策略映射的名称
- *connection_action* - 丢弃连接或重置连接
- *interface_type* - 接口类型（例如，DMZ 或外部）
- *IP_address* - 接口的 IP 地址
- *port_num* - 端口号

建议的操作：输入 **match** {**request** | **response**} **header non-ascii** 命令来纠正该问题。

417001

错误消息：`%ASA-4-417001: Unexpected event received: number`

说明：进程收到信号，但未发现事件的处理程序。

建议的操作：如果问题仍然存在，请联系思科 TAC。

417004

错误消息：`%ASA-4-417004: Filter violation error: conn number (string :string ) in string`

说明：客户端尝试修改非该客户端所有的路由属性。

建议的操作：如果问题仍然存在，请联系思科 TAC。

417006

错误消息：`%ASA-4-417006: No memory for string ) in string .Handling: string`

说明：内存不足导致操作失败，但系统会使用其他机制进行处理。

建议的操作：如果问题仍然存在，请联系思科 TAC。

418001

错误消息：`%ASA-4-418001: Through-the-device packet to/from management-only network is denied: protocol_string from interface_name IP_address (port) [([idfw_user |FQDN_string ], sg_info )] to interface_name IP_address (port) [(idfw_user |FQDN_string ), sg_info ]`

说明：从指定源向目的地发送的数据包已丢弃，因为它往来经过Firepower威胁防御设备和管理专用网络。

- **protocol_string** - TCP、UDP、ICMP 或协议 ID（十进制数字）
- **interface_name** - 接口名称

- **IP_address** - IP 地址
- **port** - 端口号
- *sg_info* - 安全组名称或特定 IP 地址标记

建议的操作：确定正在生成该数据包的对象及其原因。

419001

错误消息：`%ASA-4-419001: Dropping TCP packet from src_ifc :src_IP /src_port to dest_ifc :dest_IP /dest_port , reason : MSS exceeded, MSS size , data size`

说明：TCP 数据包的长度超过三次握手中通告的 MSS。

- >*src_ifc* - 输入接口名称
- >*src_IP* - 数据包的源 IP 地址
- >*src_port* - 数据包的源端口
- >*dest_ifc* - 输出接口名称
- >*src_IP* - 数据包的目的 IP 地址
- > *dest_port* - 数据包的目的端口

建议的操作：如果需要允许超出 MSS 的数据包，请使用 **exceed-mss** 命令创建 TCP 映射，如以下示例所示：

```
ciscoasa# access-list http-list permit tcp any host server_ip eq 80
ciscoasa# class-map http
 ciscoasa# match access-list http-list
 ciscoasa# tcp-map tmap
ciscoasa# exceed-mss allow
ciscoasa# policy-map global_policy
ciscoasa# class http
ciscoasa# set connection advanced-options tmap
```

419002

错误消息：`%ASA-4-419002: Received duplicate TCP SYN from in_interface :src_address /src_port to out_interface :dest_address /dest_port with different initial sequence number.`

说明：在三次握手期间收到了重复 TCP SYN，其与打开初期连接的 SYN 的初始序列号不同。这可能 SYN 遭遇了伪造。版本 7.0.4.1 及更高版本中会出现此消息。

- **in_interface** - 输入接口
- **src_address** - 数据包的源 IP 地址
- **src_port** - 数据包的源端口
- **Out_interface** - 输出接口
- **dest_address** - 数据包的目的 IP 地址
- **dest_port** - 数据包的目的端口

建议的操作：无需执行任何操作。

419003

错误消息： `%ASA-4-419003: Cleared TCP urgent flag from out_ifc :src_ip /src_port to in_ifc :dest_ip /dest_port.`

说明： 在三次握手期间收到了重复 TCP SYN，其与打开初期连接的 SYN 的初始序列号不同。这可能 SYN 遭遇了伪造。版本 7.0.4.1 及更高版本中会出现此消息。

- **in_ifc** - 输入接口
- **src_ip** - 数据包的源 IP 地址
- **src_port** - 数据包的源端口
- **out_ifc** - 输出接口
- **dest_ip** - 数据包的目的 IP 地址
- **dest_port** - 数据包的目的端口

建议的操作： 如果您需要保留 TCP 报头中的紧急标志，请在 TCP 映射配置模式下使用 **urgent-flag allow** 命令。

错误消息： `%ASA-7-419003: Cleared TCP urgent flag.`

说明： 清除 TCP 数据包的紧急标志或紧急指针时，系统会显示此系统日志。原因可能是用户配置（TCP 映射）问题，或为 TCP 数据包中的紧急指针分配了值，但并未设置紧急标志。

建议的操作： 验证 TCP 映射配置是否将紧急标志设置为清除。

421005

错误消息： `%ASA-6-421005: interface_name :IP_address is counted as a user of application`

说明： 主机已计入许可证限制。指定主机已计为 **application** 用户。系统在午夜进行许可证验证时，会计算 24 小时内的用户总数。

- **Interface_name** - 接口名称
- **IP_address** - IP 地址
- **application** - CSC SSM

建议的操作： 无需执行任何操作。但是，如果总数超过您已购买的用户许可证，请联系思科 TAC 升级许可证。

421007

错误消息： `%ASA-3-421007: TCP|UDP flow from interface_name :IP_address /port to interface_name :IP_address /port is skipped because application has failed.`

说明： 由于服务模块应用故障，系统已跳过流。默认情况下，此消息的速率限制为每 10 秒 1 条。

- **IP_address** - IP 地址
- **port** - 端口号
- **interface_name** - 在其中应用策略的接口的名称。
- **application** - CSC SSM

建议的操作：确定服务模块的问题。

422004

错误消息：`%ASA-4-422004: IP SLA Monitor number0 : Duplicate event received.Event number number1`

说明：IP SLA 监控进程收到了重复事件。目前，此消息适用于销毁事件。系统将仅应用一个销毁请求。这只是一条警告消息。

- *number0* - SLA 操作编号
- *number1* - SLA 操作事件 ID

建议的操作：如果重复出现此消息，请输入 **show sla monitor configuration SLA_operation_id** 命令并复制命令的输出。按照控制台或系统日志中的显示复制此消息。然后联系思科 TAC 并向代表提供现有信息，以及有关配置和轮询 SLA 探测的应用的信息。

422005

错误消息：`%ASA-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.`

说明：由于未设置系统时钟而无法计划一个或多个 IP SLA 监控探测。

建议的操作：通过使用 NTP 或其他机制确保系统时钟正常运行。

422006

错误消息：`%ASA-4-422006: IP SLA Monitor Probe number : string`

说明：无法计划 IP SLA 监控探测。配置的开始时间已经开始或开始时间无效。

- *number* - SLA 操作 ID
- *string* - 描述此错误的字符串

建议的操作：使用有效的开始时间重新计划失败的探测。

424001

错误消息：`%ASA-4-424001: Packet denied protocol_string intf_in :src_ip /src_port [([idfw_user | FQDN_string ], sg_info )] intf_out :dst_ip /dst_port [([idfw_user | FQDN_string ], sg_info )].[Ingress|Egress] interface is in a backup state.`

说明：数据包由于往来经过 Firepower 威胁防御设备 和冗余接口而被丢弃。接口功能仅限于低端平台。由 **backup interface** 命令指定的接口只能作为已配置主接口的备用接口。如果通往主接口的默认路由已启用，则从备用接口通往 Firepower 威胁防御设备 的任何流量都将被拒绝。如果通往主接口的默认路由已关闭，则从主接口通往 Firepower 威胁防御设备 的流量将被拒绝。

- *protocol_string* - 协议字符串；例如，TCP 或协议 ID（十进制数）
- *intf_in* - 输入接口名称

- *src_ip* - 数据包的源 IP 地址
- *src_port* - 数据包的源端口
- *Intf_out* - 输出接口名称
- *dst_ip* - 数据包的目的 IP 地址
- *dst_port* - 数据包的目的端口
- *sg_info* - 安全组名称或特定 IP 地址标记

建议的操作：确定被拒绝数据包的来源。

424002

错误消息：`%ASA-4-424002: Connection to the backup interface is denied: protocol_string intf :src_ip /src_port intf :dst_ip /dst_port`

说明：连接由于处于备用状态而被丢弃。接口功能仅限于低端平台。备用接口仅可用作 **backup interface** 命令指定的主接口的备用接口。如果通往主接口的默认路由已启用，则通过备用接口与 Firepower 威胁防御设备的任何连接都将被拒绝。相反，如果通往主接口的默认路由已关闭，则通过主接口与 Firepower 威胁防御设备的任何连接都将被拒绝。

- *protocol_string* - 协议字符串；例如，TCP 或协议 ID（十进制数）
- *intf_in* - 输入接口名称
- *src_ip* - 数据包的源 IP 地址
- *src_port* - 数据包的源端口
- *Intf_out* - 输出接口名称
- *dst_ip* - 数据包的目的 IP 地址
- *dst_port* - 数据包的目的端口

建议的操作：确定被拒绝数据包的来源。

425001

错误消息：`%ASA-6-425001 Redundant interface redundant _interface_name created.`

说明：已在配置中创建指定的冗余接口。

- *redundant_interface_name* - 冗余接口名称

建议的操作：无需执行任何操作。

425002

错误消息：`%ASA-6-425002 Redundant interface redundant _interface_name removed.`

说明：已从配置中删除指定的冗余接口。

- *redundant_interface_name* - 冗余接口名称

建议的操作：无需执行任何操作。

425003

错误消息：%ASA-6-425003 Interface *interface_name* added into redundant interface *redundant _interface_name* .

说明：指定的物理接口已作为成员接口添加到指定冗余接口中。

- *interface_name* - 接口名称
- *redundant_interface_name* - 冗余接口名称

建议的操作：无需执行任何操作。

425004

错误消息：%ASA-6-425004 Interface *interface_name* removed from redundant interface *redundant _interface_name* .

说明：已从指定的冗余接口中移除指定冗余接口。

- *interface_name* - 接口名称
- *redundant_interface_name* - 冗余接口名称

建议的操作：无需执行任何操作。

425005

错误消息：%ASA-5-425005 Interface *interface_name* become active in redundant interface *redundant _interface_name*

说明：在冗余接口内，有一个成员接口处于活动状态。流量仅通过活动成员接口。指定的物理接口成为指定冗余接口的活动成员。出现以下情况时，成员接口会进行切换：

-
  - 执行了 **redundant-interface interface-name active-member interface-name** 命令。
  - 活动成员接口关闭，而备用成员接口已启用。
  - 备用成员接口状态已从关闭切换为启用，而活动成员接口仍然关闭。
- *interface_name* - 接口名称
- *redundant_interface_name* - 冗余接口名称

建议的操作：检查成员接口的状态。

425006

错误消息：%ASA-3-425006 Redundant interface *redundant _interface_name* switch active member to *interface_name* failed.

说明：尝试进行成员接口切换时发生错误。

- *redundant_interface_name* - 冗余接口名称
- *interface_name* - 接口名称

建议的操作：如果问题仍然存在，请联系思科 TAC。

426001

错误消息： `%ASA-6-426001: PORT-CHANNEL:Interface ifc_name bundled into EtherChannel interface Port-channel num`

说明： 系统已对不存在的端口通道使用 **interface port-channel** *num* 或 **channel-group** *num* **mode** *mode* 命令。

- *ifc_name* - EtherChannel 接口名称
- *num* - 端口通道编号

建议的操作： 无需执行任何操作。

426002

错误消息： `%ASA-6-426002: PORT-CHANNEL:Interface ifc_name unbundled from EtherChannel interface Port-channel num`

说明： 已使用 **no interface port-channel** *num* 命令。

- *ifc_name* - EtherChannel 接口名称
- *num* - 端口通道编号

建议的操作： 无需执行任何操作。

426003

错误消息： `%ASA-6-426003: PORT-CHANNEL:Interface ifc_name1 has become standby in EtherChannel interface Port-channel num`

说明： 已使用 **channel-group** *num* **mode** *mode* 命令。

- *Ifc_name1* - EtherChannel 接口名称
- *num* - 端口通道编号

建议的操作： 无需执行任何操作。

426004

错误消息： `%ASA-4-426004: PORT-CHANNEL: Interface ifc_name1 is not compatible with ifc_name and will be suspended (speed of ifc_name1 is X Mbps, Y is 1000 Mbps).`

错误消息： %ASA-4-426004: Interface *ifc_name1* is not compatible with *ifc_name1* and will be suspended (*ifc_name1* is Full-duplex, *ifc_name1* is Half-duplex)

说明： 已在物理接口中执行 **channel-group** *num* **mode** *mode* 命令，此物理接口与端口通道之间存在速度或双工不匹配。

- *ifc_name* - 即将添加到端口通道的接口
- *Ifc_name1* - 已位于端口通道且处于捆绑状态的接口

建议的操作： 请执行以下操作之一：

- 将物理接口的速度改为端口通道速度，然后再次执行 **channel-group** *num* **mode** *mode* 命令。
- 让成员接口保持挂起状态。删除最后一个活动成员时，该成员将尝试在挂起的成员中重建LACP。

426101

错误消息： `%ASA-6-426101: PORT-CHANNEL:Interface ifc_name is allowed to bundle into EtherChannel interface port-channel id by CLACP`

说明： 已在 span-cluster 通道组中捆绑端口。

建议的操作： 无需执行任何操作。

426102

错误消息： `%ASA-6-426102: PORT-CHANNEL:Interface ifc_name is moved to standby in EtherChannel interface port-channel id by CLACP`

说明： span-cluster 通道组中的端口已改为热备份状态。

建议的操作： 无需执行任何操作。

426103

错误消息： `%ASA-6-426103: PORT-CHANNEL:Interface ifc_name is selected to move from standby to bundle in EtherChannel interface port-channel id by CLACP`

说明： 已在 span-cluster 通道组中选定一个备用端口以将其改为捆绑状态。

建议的操作： 无需执行任何操作。

426104

错误消息： `%ASA-6-426104: PORT-CHANNEL:Interface ifc_name is unselected in EtherChannel interface port-channel id by CLACP`

说明： 已将 span-cluster 通道组中的捆绑端口解绑，从而为其他需要捆绑的端口留出空间。

建议的操作： 无需执行任何操作。

428002

错误消息： `%ASA-6-428002: WAAS confirmed from in_interface :src_ip_addr/src_port to out_interface :dest_ip_addr/dest_port , inspection services bypassed on this connection.`

说明： 在连接中检测到 WAAS 优化。系统将在 WAAS 优化连接中绕过所有第 7 层检测服务（包括 IPS）。

建议的操作： 如果网络中包含 WAE 设备，则无需执行任何操作；否则，网络管理员应调查此连接中 WAAS 选项的使用情况。

429008

错误消息： `%ASA-4-429008: Unable to respond to VPN query from CX for session 0x%x .Reason %s`

说明：CX 向 Firepower 威胁防御设备发送了 VPN 会话查询，但由于会话 ID 无效或其他原因导致无响应。可能的原因如下：

- TLV 长度无效
- TLV 内存分配失败
- VPN 会话查询消息入队失败
- VPN 会话 ID 无效

建议的操作：无需执行任何操作。

4302310

错误消息： `%ASA-5-4302310: SCTP packet received from src_ifc:src_ip/src_port to dst_ifc:dst_ip/dst_port contains unsupported Hostname Parameter.`

说明：收到 init/init-ack 数据包以及主机名参数。

- **packet init/init-ack** - 传输主机名参数的消息
- **src-ifc** - 表示入口接口
- **src-ip/src-port** - 表示数据包中的源 IP 和端口
- **dst-ifc** - 表示出口接口
- **dst_ip/dst_port** - 表示数据包中的目的 IP 和端口

建议的操作：使用终端的真实 IP 地址而不是主机名。禁用主机名参数。

434001

错误消息： `%ASA-4-434001: SFR card not up and fail-close mode used, dropping protocol packet from ingress interface:source IP address /source port to egress interface :destination IP address /destination port`

说明：模块的故障关闭配置导致数据包被丢弃。将流重定向至模块会导致所有流失去连接，这是由于根据故障关闭配置，如果模块关闭，系统会丢弃所有流。

建议的操作：尝试了解故障原因并恢复服务。或者，如果卡未立即恢复，您也可以使用故障开放选项。请注意，根据故障开放配置，如果卡处于关闭状态，系统将会绕过通往该模块的所有数据包。

434004

错误消息： `%ASA-5-434004: SFR requested ASA to bypass further packet redirection and process flow from %s:%A/%d to %s:%A/%d locally`

说明：SourceFire (SFR) 已决定不检查流的更多流量，并请求 Firepower 威胁防御设备停止将流量流重定向至 SFR。

建议的操作：无需执行任何操作。

446003

错误消息：`%ASA-4-446003: Denied TLS Proxy session from src_int :src_ip /src_port to dst_int :dst_ip /dst_port , UC-IME license is disabled.`

说明：UC IME 许可证处于打开或关闭状态。UC IME 在启用后可以根据 Firepower 威胁防御 限制和 K8 导出限制使用任意数量的可用 TLS 会话。

- *src_int* - 源接口名称（内部或外部）
- *src_ip* - 源 IP 地址
- *src_port* - 源端口
- *dst_int* - 目的接口名称（内部或外部）
- *dst_ip* - 目的 IP 地址
- *dst_port* - 目的端口

建议的操作：检查是否已禁用 UC-IME。如果已禁用，请将其激活。

447001

错误消息：`%ASA-4-447001: ASP DP to CP queue_name was full.Queue length length , limit limit`

说明：此消息表示特定数据路径 (DP) 到控制点 (CP) 的事件队列已满，且已有一个或多个入队操作失败。如果事件包含数据包块（例如用于 CP 应用检查），DP 将会丢弃数据包，而且 **show asp drop** 命令中的计数器将递增。如果事件为转出到 CP，则典型计数器为转出无内存 ASP-drop 计数器。

- *queue* - DP-CP 事件队列的名称。
- *length* - 队列中当前事件数量。
- *limit* - 队列中允许的最大事件数量。

建议的操作：队列已满的状况说明 CP 上的负载超过 CP 处理能力，这可能是（也可能不时）临时状况。如果此消息反复出现，应考虑减少 CP 上的功能负载。使用 **show asp event dp-cp** 命令识别事件队列中负载最高的功能。

448001

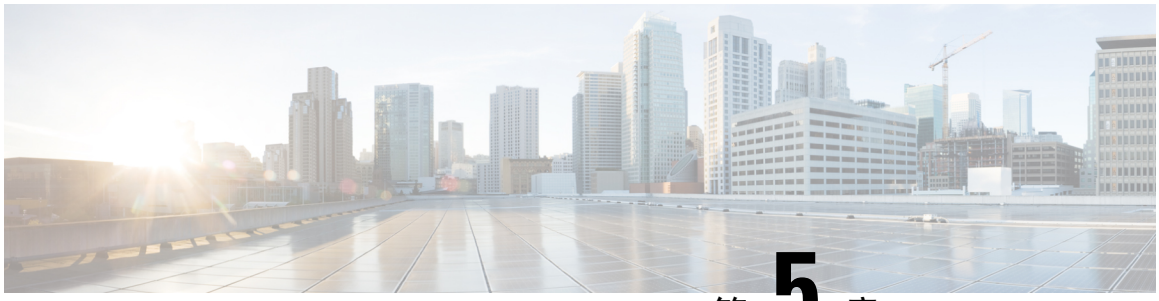
错误消息：`%ASA-4-448001: Denied SRTP crypto session setup on flow from src_int :src_ip /src_port to dst_int :dst_ip /dst_port , licensed K8 SRTP crypto session of limit exceeded`

说明：系统对 K8 平台实施 250 个 SRTP 加密会话的限制。每一对 SRTP 加密或解密会话计为一个 SRTP 加密会话。仅当介质需要加密或解密时，调用才会计入此限制，这就表示，如果对调用设置了透传，则即使双方都使用 SRTP，调用也不会计入此限制。

- *src_int* - 源接口名称（内部或外部）
- *src_ip* - 源 IP 地址
- *src_port* - 源端口
- *dst_int* - 目的接口名称（内部或外部）

- *dst_ip* - 目的 IP 地址
- *dst_port* - 目的端口
- *limit* - SRTP 加密会话 (250) 的 K8 限制

建议的操作：无需执行任何操作。只有当现有 SRTP 加密会话释放后，才能设置新的 SRTP 加密会话。



第 5 章

系统日志消息 500001-520025

本章包含以下各节：

ID 介于 500001 到 504002 之间的消息

本章包含 ID 介于 500001 到 504002 之间的消息。

500001

错误消息： `%ASA-5-500001: ActiveX content in java script is modified: src` *`src ip`* `dest` *`dest ip`* `on interface` *`interface name`*

说明： 在 Firepower 威胁防御设备中启用策略（过滤 Java（或）过滤 ActiveX）时，请确保阻止 Java 脚本中出现 Java/ActiveX 内容。

建议的操作： 无需执行任何操作。

500002

错误消息： `%ASA-5-500002: Java content in java script is modified: src` *`src ip`* `dest` *`dest ip`* `on interface` *`interface name`*

说明： 在 Firepower 威胁防御设备中启用策略（过滤 Java（或）过滤 ActiveX）时，请确保阻止 Java 脚本中出现 Java/ActiveX 内容。

建议的操作： 无需执行任何操作。

500003

错误消息： `%ASA-5-500003: Bad TCP hdr length (hdrlen=`*`bytes`*` , pktlen=`*`bytes`*` ) from` *`source_address /source_port`* `to` *`dest_address /dest_port`* `, flags:` *`tcp_flags`* `, on interface` *`interface_name`*

说明：TCP 中的报头长度不正确。某些操作系统在响应指向已禁用套接字的连接请求时无法正确处理 TCP 重置 (RST)。如果客户端尝试连接到 Firepower 威胁防御设备外部的 FTP 服务器，而 FTP 服务器并未侦听，系统将发送 RST。某些操作系统发送的 TCP 报头长度不正确，就会导致此问题。UDP 使用 ICMP 端口不可达消息。

TCP报头长度可能表明它大于数据包长度，这会导致传输负数字节。消息中的负数显示为无符号数，使字节数看起来比正常情况大得多；例如，系统可能显示在1秒内传输了4GB数据。此消息通常很少出现。

建议的操作：无需执行任何操作。

500004

错误消息：`%ASA-4-500004: Invalid transport field for protocol=`*`protocol`* `, from` *`source_address`* `/`*`source_port`* `to` *`dest_address`* `/`*`dest_port`*

说明：使用了无效的传输编号，其中协议的源端口或目的端口号为零。TCP 的 **protocol** 值为 6，而 UDP 的为 17。

建议的操作：如果这些消息仍然存在，请与对等体管理员联系。

500005

错误消息：`%ASA-3-500005: connection terminated for` *`protocol`* `from` *`in_ifc_name`* `:`*`src_adddress`* `/`*`src_port`* `to` *`out_ifc_name`* `:`*`dest_address`* `/`*`dest_port`* `due to invalid combination of inspections on same flow.Inspect` *`inspect_name`* `is not compatible with filter` *`filter_name`* `.`

说明：连接与不允许用于该连接的单项或多项检测和/或单个或多个过滤器功能匹配。

- *protocol* - 连接使用的协议
- *in_ifc_name* - 输入接口名称
- *src_address* - 连接的源 IP 地址
- *src_port* - 连接的源端口
- *out_ifc_name* - 输出接口名称
- *dest_address* - 连接的目的 IP 地址
- *dest_port* - 数据包的目的端口
- *inspect_name* - 检测或过滤器功能名称
- *filter_name* - 过滤器功能名称

建议的操作：查看 **class-map**、**policy-map**、**service-policy** 和/或 **filter** 命令配置，这些配置导致引用的检测和/或过滤器功能与连接匹配。连接的检查和过滤器功能组合规则如下所示：

-
  - **inspect http [http-policy-map]** 和/或 **filter url** 和/或 **filter java** 和/或 **filter activex** 命令有效。
  - **inspect ftp [ftp-policy-map]** 和/或 **filter ftp** 命令有效。
  - 包含任何其他 **inspect** 命令或 **filter** 命令的 **filter https** 命令均无效。

除了所列组合，任何其他检测和/或过滤器功能组合均无效。

501101

错误消息： `%ASA-5-501101: User transitioning priv level`

说明： 命令的权限级别已更改。

建议的操作： 无需执行任何操作。

502101

错误消息： `%ASA-5-502101: New user added to local dbase: Uname: user Priv: privilege_level Encpass: string`

说明： 系统创建了新的用户名记录，其中包括用户名、权限级别和加密密码。

建议的操作： 无需执行任何操作。

502102

错误消息： `%ASA-5-502102: User deleted from local dbase: Uname: user Priv: privilege_level Encpass: string`

说明： 用户名记录已删除，其中包括用户名、权限级别和加密密码。

建议的操作： 无需执行任何操作。

502103

错误消息： `%ASA-5-502103: User priv level changed: Uname: user From: privilege_level To: privilege_level`

说明： 用户权限级别已更改。

建议的操作： 无需执行任何操作。

502111

错误消息： `%ASA-5-502111: New group policy added: name: policy_name Type: policy_type`

说明： 使用 **group-policy** CLI 命令配置了组策略。

- **policy_name** - 组策略名称
- **policy_type** - 内部或外部

建议的操作： 无需执行任何操作。

502112

错误消息： `%ASA-5-502112: Group policy deleted: name: policy_name Type: policy_type`

说明： 已使用 **group-policy** CLI 命令删除组策略。

- **policy_name** - 组策略名称
- **policy_type** - 内部或外部

建议的操作：无需执行任何操作。

503001

错误消息：`%ASA-5-503001: Process number, Nbr IP_address on interface_name from string to string , reason`

说明：一个 OSPFv2 邻居已更改状态。此消息说明具体更改及其原因。只有为 OSPF 进程配置了 **log-adjacency-changes** 命令后，系统才会显示此消息。

建议的操作：按照显示正确复制此消息，并将其报告给思科 TAC。

503101

错误消息： `%ASA-5-503101: Process d , Nbr i on s from s to s , s`

说明：一个 OSPFv3 邻居已更改状态。此消息说明具体更改及其原因。只有为 OSPF 进程配置了 **log-adjacency-changes** 命令后，系统才会显示此消息。

建议的操作：无需执行任何操作。

504001

错误消息：`%ASA-5-504001: Security context context_name was added to the system`

说明：安全情景已成功添加至 Firepower 威胁防御设备。

建议的操作：无需执行任何操作。

504002

错误消息：`%ASA-5-504002: Security context context_name was removed from the system`

说明：安全情景已从 Firepower 威胁防御设备中成功删除。

建议的操作：无需执行任何操作。

ID 介于 505001 到 520025 之间的消息

本章包含 ID 介于 505001 到 520025 之间的消息。

505001

错误消息：`%ASA-5-505001: Module string one is shutting down.Please wait...`

说明：正在关闭模块。

建议的操作：无需执行任何操作。

505002

错误消息：`%ASA-5-505002: Module ips is reloading.Please wait...`

说明：系统正在重新加载 IPS 模块。

建议的操作：无需执行任何操作。

505003

错误消息：`%ASA-5-505003: Module string one is resetting.Please wait...`

说明：系统正在重置模块。

建议的操作：无需执行任何操作。

505004

错误消息：`%ASA-5-505004: Module string one shutdown is complete.`

说明：模块已关闭。

建议的操作：无需执行任何操作。

505005

错误消息：`%ASA-5-505005: Module module_name is initializing control communication.Please wait...`

说明：系统检测到一个模块，Firepower 威胁防御设备正在初始化与其通信的控制通道。

建议的操作：无需执行任何操作。

505006

错误消息：`%ASA-5-505006: Module string one is Up.`

说明：模块已完成控制通道初始化，现在处于打开状态。

建议的操作：无需执行任何操作。

505007

错误消息：`%ASA-5-505007: Module module_id is recovering.Please wait...`

错误消息：`%ASA-5-505007: Module prod_id  in slot slot_num  is recovering.Please wait...`

说明：正在使用 **sw-module module** *service-module-name* **recover boot** 命令恢复软件模块，或使用 **hw-module module** *slotnum* **recover boot** 命令恢复硬件模块。

- **module_id** - 软件服务模块的名称。
- **prod_id** - 产品 ID 字符串。
- *slot_num* - 安装硬件服务模块的插槽。插槽 0 表示系统主板，插槽 1 表示扩展槽中安装的模块。

建议的操作：无需执行任何操作。

505008

错误消息：`%ASA-5-505008: Module module_id software is being updated to newver (currently ver )`

错误消息：`%ASA-5-505008: Module` *module_id* in slot *slot_num* software is being updated to *newver* (currently *ver*)

说明：服务模块软件正在升级。更新正常进行。

- *module_id* - 软件服务模块的名称
- *slot_num* - 包含硬件服务模块的插槽号
- >*newver* - 未成功写入模块的软件的新版本号（例如，1.0(1)0）
- >*ver* - 模块上软件的当前版本号（例如，1.0(1)0）

建议的操作：无需执行任何操作。

505009

错误消息：`%ASA-5-505009: Module string one software was updated to newver`

说明：4GE SSM 模块软件已成功升级。

- *string one* - 指定模块的文本字符串
- *newver* - 未成功写入模块的软件新版本号（例如，1.0(1)0）
- *ver* - 模块上软件的当前版本号（例如，1.0(1)0）

建议的操作：无需执行任何操作。

505010

错误消息：`%ASA-5-505010: Module in slot slot removed.`

说明：已从 Firepower 威胁防御设备机箱中移除 SSM。

- **slot** - 移除了此 SSM 的插槽

建议的操作：无需执行任何操作。

505011

错误消息：`%ASA-1-505011: Module ips , data channel communication is UP.`

说明：数据通道通信已从关闭状态恢复。

建议的操作：无需执行任何操作。

505012

错误消息：`%ASA-5-505012: Module module_id , application stopped application , version version`

错误消息：`%ASA-5-505012: Module prod_id  in slot slot_num , application stopped application , version version`

说明：应用已停止或已从服务模块中删除。当服务模块升级应用或服务模块上的应用已停止或已卸载时，可能出现这种情况。

- **module_id** - 软件服务模块的名称
- *prod_id* - 硬件服务模块中已安装设备的产品 ID 字符串
- *slot_num* - 应用已停止的插槽
- **application** - 已停止的应用名称
- **version** - 已停止的应用版本

建议的操作：如果 4GE SSM 未升级，或未有意停止或卸载应用，请查看 4GE SSM 日志以确定应用停止的原因。

505013

错误消息：`%ASA-5-505013: Module module_id application changed from: application version version to: newapplicationversion newversion .`

错误消息：`%ASA-5-505013: Module prod_id  in slot slot_nunm  application changed from: application version version to: newapplicationversion newversion .`

说明：应用版本已更改（例如，在升级后）。服务模块上的应用已完成软件更新。

- **module_id** - 软件服务模块的名称
- **application** - 已升级应用的名称
- **version** - 已升级应用的版本
- **prod_id** - 硬件服务模块中已安装设备的产品 ID 字符串
- **slot_num** - 应用已升级的插槽
- **application** - 已升级应用的名称
- **version** - 已升级应用的版本
- **newapplication** - 新应用名称
- **newversion** - 新应用版本

建议的操作：验证升级是否为预期操作，以及新版本是否正确。

505014

错误消息：`%ASA-1-505014: Module module_id , application down name , version version reason`

错误消息：`%ASA-1-505014: Module prod_id  in slot slot_num , application down name , version version reason`

说明：模块上运行的应用已禁用。

- **module_id** - 软件服务模块的名称
- **prod_id** - 硬件服务模块中已安装设备的产品 ID 字符串
- *slot_num* - 应用已禁用的插槽。插槽 0 表示系统主板，插槽 1 表示扩展槽中安装的模块。
- **name** - 应用名称（字符串）
- **application** - 已升级应用的名称
- **version** - 应用版本（字符串）
- **reason** - 故障原因（字符串）

建议的操作：如果问题仍然存在，请联系思科 TAC。

505015

错误消息：`%ASA-1-505015: Module module_id , application up application , version version`

错误消息：`%ASA-1-505015: Module prod_id in slot slot_num , application up application , version version`

说明：在插槽 *slot_num* 中的 SSM 上运行的应用已打开并运行。

- **module_id** - 软件服务模块的名称
- **prod_id** - 硬件服务模块中已安装设备的产品 ID 字符串
- *slot_num* - 正在运行应用的插槽。插槽 0 表示系统主板，插槽 1 表示扩展槽中安装的模块。
- **application** - 应用名称（字符串）
- **version** - 应用版本（字符串）

建议的操作：无需执行任何操作。

505016

错误消息：`%ASA-3-505016: Module module_id application changed from: name version version state state to: name version state state .`

错误消息：`%ASA-3-505016: Module` *prod_id* in slot *slot_num* application changed from: *name* version *version* state *state* to: *name version* state *state* .

说明：系统检测到应用版本或名称已更改。

- **module_id** - 软件服务模块的名称
- **prod_id** - 硬件服务模块中已安装设备的产品 ID 字符串
- *slot_num* - 应用已更改的插槽。插槽 0 表示系统主板，插槽 1 表示扩展槽中安装的模块。
- **name** - 应用名称（字符串）
- **version** - 应用版本（字符串）
- **state** - 应用状态（字符串）
- **application** - 已更改应用的名称。

建议的操作：验证更改是否为预期操作，以及新版本是否正确。

506001

错误消息： `%ASA-5-506001: event_source_string event_string`

说明： 文件系统状态已更改。系统将显示导致文件系统变为可用或不可用的事件或事件原因。可能导致文件系统状态更改的原因和事件示例如下所示：

- 外部 CompactFlash 已删除
- 外部 CompactFlash 已插入
- 外部 CompactFlash 未知事件

建议的操作： 无需执行任何操作。

507001

错误消息： `%ASA-5-507001: Terminating TCP-Proxy connection from interface_inside:source_address/source_port to interface_outside :dest_address /dest_port - reassembly limit of limit bytes exceeded`

说明： 在 TCP 数据分段重组过程中超出了组件缓冲区限制。

- **source_address/source_port** - 发起连接的数据包的源 IP 地址和源端口
- **dest_address/dest_port** - 发起连接的数据包的目的 IP 地址和目的端口
- **interface_inside** - 发起连接的数据包到达的接口的名称
- **Interface_outside** - 发起连接的数据包退出的接口的名称
- **limit** - 为该流量类别配置的初期连接限制

建议的操作： 无需执行任何操作。

507002

错误消息： `%ASA-4-507002: Data copy in proxy-mode exceeded the buffer limit`

说明： 处理分段 TCP 消息期间发生操作错误。

建议的操作： 无需执行任何操作。

507003

错误消息： `%ASA-3-507003: The flow of type protocol from the originating interface: src_ip /src_port to dest_if :dest_ip /dest_port terminated by inspection engine, reason-`

说明： 出于消息中提供的各种原因，TCP 代理服务器或会话 API 终止连接。

- **protocol** - 流协议
- **src_ip** - 流的源 IP 地址
- *src_port* - 流的源端口名称
- *dest_if* - 流的目的接口
- *dst_ip* - 流的目的 IP 地址

- *dest_port* - 流的目的端口
- *reason* - 检测引擎终止流的原因说明。有效的原因包括：

- 无法创建流

- 无法初始化会话 API

- 安装/匹配的过滤器规则不兼容

- 无法将新缓冲区数据与原始缓冲区整合

- 无条件重置

- 基于“服务重置入站”配置重置

- 已断开连接、已丢弃数据包

- 已更改数据包长度

- 重置反射回发件人

- 无条件重置代理检测器

- 代理检测器丢弃重置

- 代理检测器在 FIN 之后接收到数据

- 代理检测器已断开连接、已丢弃数据包

- 无条件重置检测器

- 检测器丢弃重置

- 检测器在 FIN 之后接收到数据

- 检测器已断开连接、已丢弃数据包

- 无法缓冲未处理的数据

- 会话 API 代理转发失败

- 将检测数据转换为检查数据失败

- 面向 TLS 代理的 SSL 通道已关闭

建议的操作：无需执行任何操作。

509001

错误消息：`%ASA-5-509001: Connection attempt from src_intf :src_ip /src_port [([idfw_user | FQDN_string ], sg_info )] to dst_intf :dst_ip /dst_port [([idfw_user | FQDN_string ], sg_info )] was prevented by "no forward" command.`

说明：已输入 **no forward interface** 命令以阻止从消息中的给定源接口通往目的接口的流量。低端平台上需要通过此命令允许创建超过许可限制的接口。

- **src_intf** - 应用 **no forward interface** 命令限制的源接口名称
- **Dst_intf** - 应用 **no forward interface** 命令限制的目的接口名称

- *sg_info* - 安全组名称或特定 IP 地址标记

建议的操作：升级许可证，在低端平台上消除此命令要求，然后从配置中删除该命令。

520001

错误消息：`%ASA-3-520001: error_string`

说明：ID 管理器中发生 malloc 故障。错误字符串可能是以下任一项：

- Malloc failure—id_reserve
- Malloc failure—id_get

建议的操作：联系思科 TAC。

520002

错误消息：`%ASA-3-520002: bad new ID table size`

说明：ID 管理器发生了错误新表请求。

建议的操作：联系思科 TAC。

520003

错误消息：`%ASA-3-520003: bad id in error_string (id: 0xid_num)`

说明：发生 ID 管理器错误。错误字符串可能是以下任何一项：

- id_create_new_table（不允许更多条目）
- id_destroy_table（错误表 ID）
- id_reserve
- id_reserve（错误 ID）
- id_reserve：ID 超出范围
- id_reserve（未分配的表 ID）
- id_get（错误表 ID）
- id_get（未分配的表 ID）
- id_get（ID 不足！）
- id_to_ptr
- id_to_ptr（错误 ID）
- id_to_pt（错误表 ID）
- id_get_next_id_ptr（错误表 ID）
- id_delete
- id_delete（错误 ID）
- id_delete（错误表密钥）

建议的操作：联系思科 TAC。

520004

错误消息： `%ASA-3-520004: error_string`

说明： 尝试在中断级别执行 id_get。

建议的操作： 联系思科 TAC。

520005

错误消息： `%ASA-3-520005: error_string`

说明： ID 管理器发生内部错误。

建议的操作： 联系思科 TAC。

520010

错误消息： `%ASA-3-520010: Bad queue elem - qelem_ptr : flink flink_ptr , blink blink_ptr , flink-blink flink_blink_ptr , blink-flink blink_flink_ptr`

说明： 发生内部软件错误，可能是以下任何一项：

- *qelem_ptr* - 指向队列数据结构的指针
- *flink_ptr* - 指向队列数据结构前向元素的指针
- *blink_ptr* - 指向队列数据结构后向元素的指针
- *flink_blink_ptr* - 指向队列数据结构正向元素的后向指针的指针
- *blink_flink_ptr* - 指向队列数据结构后向元素的前向指针的指针

建议的操作： 联系思科 TAC。

520011

错误消息： `%ASA-3-520011: Null queue elem`

说明： 发生了内部软件错误。

建议的操作： 联系思科 TAC。

520013

错误消息： `%ASA-3-520013: Regular expression access check with bad list acl_ID`

说明： 指向访问列表的指针无效。

建议的操作： 导致生成此消息的事件不应发生。它可能表示一个或多个数据结构已被覆盖。如果此消息重复出现，而且您决定向 TAC 代表报告，则应该按显示正确复制消息文本并包含关联的堆叠跟踪。因为访问列表可能已损坏，TAC 代表应当验证访问列表是否正常运行。

520020

错误消息： `%ASA-3-520020: No memory available`

说明： 系统内存不足。

建议的操作： 请尝试以下操作之一，以解决问题：

- 减少此路由器接受的路由数量。
- 升级硬件。
- 在从 RAM 运行的平台上使用较小的子集映像。

520021

错误消息： `%ASA-3-520021: Error deleting trie entry, error_message`

说明： 发生软件编程错误。错误消息可能是以下任何一项：

- 注记不一致
- 找不到我们的注记
- 找不到删除目标

建议的操作： 按显示正确复制错误消息，并将其报告给思科 TAC。

520022

错误消息： `%ASA-3-520022: Error adding mask entry, error_message`

说明： 发生软件或硬件错误。错误消息可能是以下任何一项：

- 已在树中的掩码
- 未输入路由的掩码
- 非唯一的正常路由，未输入掩码

建议的操作： 按显示正确复制错误消息，并将其报告给思科 TAC。

520023

错误消息： `%ASA-3-520023: Invalid pointer to head of tree, 0x radix_node_ptr`

说明： 发生软件编程错误。

建议的操作： 按显示正确复制错误消息，并将其报告给思科 TAC。

520024

错误消息： `%ASA-3-520024: Orphaned mask #radix_mask_ptr, refcount= radix_mask_ptr's ref count at #radix_node_address, next= #radix_node_nxt`

说明： 发生软件编程错误。

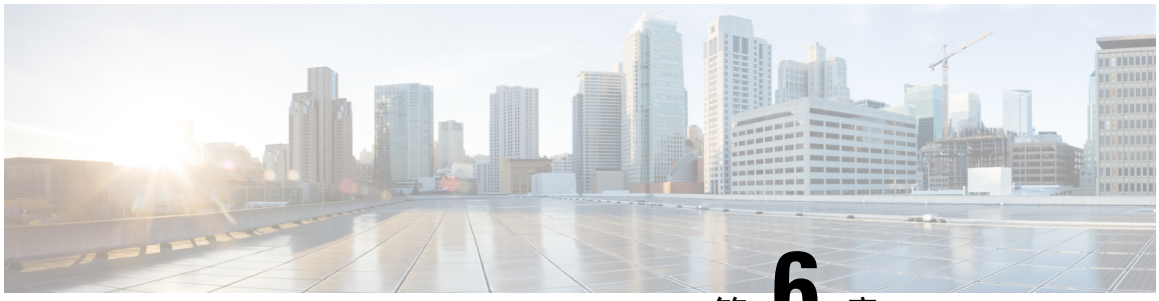
建议的操作：按显示正确复制错误消息，并将其报告给思科 TAC。

520025

错误消息：`%ASA-3-520025: No memory for radix initialization: err_msg`

说明：系统在初始化期间耗尽了内存。只有当映像太大，不适合现有动态内存时才会出现这种情况。错误消息可能是以下任何一项：Initializing leaf nodes 或 Mask housekeeping

建议的操作：使用较小的子集映像或升级硬件。



第 6 章

系统日志消息 602101-622102

本章包含以下各节：

ID 介于 602101 到 609002 之间的消息

本部分包括 ID 介于 602101 到 609002 之间的消息。

602101

错误消息： `%ASA-6-602101: PMTU-D packet number bytes greater than effective mtu number dest_addr=dest_address , src_addr=source_address , prot=protocol`

说明： Firepower 威胁防御设备 发送了 ICMP 目的地不可达的消息，需要分段。

建议的操作： 确保正确发送数据。

602103

错误消息： `%ASA-6-602103: IPSEC: Received an ICMP Destination Unreachable from src_addr with suggested PMTU of rcvd_mtu; PMTU updated for SA with peer peer_addr, SPI spi, tunnel name username, old PMTU old_mtu, new PMTU new_mtu.`

说明： SA 的 MTU 已更改。从 IPsec 隧道收到数据包时，系统会找到对应的 SA，并且根据 ICMP 数据包中建议的 MTU 更新 MTU。如果建议 MTU 大于 0，但小于 256，则系统会将新 MTU 设置为 256。如果建议 MTU 为 0、旧 MTU 会减少 256 或设置为 256（以较大值为准）。如果建议 MTU 超过 256，则系统会将新 MTU 设置为建议值。

- src_addr - PMTU 发件人的 IP 地址
- rcvd_mtu - PMTU 消息中收到的建议 MTU
- peer_addr - IPsec 对等体的 IP 地址
- spi - Ipsec 安全参数索引
- username - 与 IPsec 隧道关联的用户名

- old_mtu - 与 IPsec 隧道关联的过往 MTU
- new_mtu - 与 IPsec 隧道关联的新 MTU

建议的操作：无需执行任何操作。

602104

错误消息：`%ASA-6-602104: IPSEC: Received an ICMP Destination Unreachable from src_addr , PMTU is unchanged because suggested PMTU of rcvd_mtu is equal to or greater than the current PMTU of curr_mtu , for SA with peer peer_addr , SPI spi , tunnel name username .`

说明：系统收到 ICMP 消息，指示通过 IPsec 隧道发送的数据包超过路径 MTU，且建议的 MTU 大于或等于当前 MTU。因为 MTU 值已经是正确的，因此无需调整 MTU。当系统从不同的中间站接收多条 PMTU 消息时可能发生这种情况，而且系统会在处理当前的 PMTU 消息之前调整 MTU。

- **src_addr** - PMTU 发件人的 IP 地址
- **rcvd_mtu** - PMTU 消息中收到的建议 MTU
- **curr_mtu** - 与 IPsec 隧道关联的当前 MTU
- **peer_addr** - IPsec 对等体的 IP 地址
- **spi** - Ipsec 安全参数索引
- *username* - 与 IPsec 隧道关联的用户名

建议的操作：无需执行任何操作。

602303

错误消息：`%ASA-6-602303: IPSEC: An direction tunnel_type SA (SPI=spi ) between local_IP and remote_IP (username ) has been created.`

说明：已创建一个新 SA。

- direction - SA 方向（入站或出站）
- tunnel_type - SA 类型（远程访问或 L2L）
- spi - Ipsec 安全参数索引
- local_IP - 隧道本地终端的 IP 地址
- remote_IP - 隧道远程终端的 IP 地址
- >*username* - 与 IPsec 隧道关联的用户名

建议的操作：无需执行任何操作。

602304

错误消息：`%ASA-6-602304: IPSEC: An direction tunnel_type SA (SPI=spi ) between local_IP and remote_IP (username ) has been deleted.`

说明：SA 已删除。

- direction - SA 方向（入站或出站）
- tunnel_type - SA 类型（远程访问或 L2L）

- spi - Ipsec 安全参数索引
- local_IP - 隧道本地终端的 IP 地址
- remote_IP - 隧道远程终端的 IP 地址
- >*username* - 与 IPsec 隧道关联的用户名

建议的操作：无需执行任何操作。

602305

错误消息：`%ASA-3-602305: IPSEC: SA creation error, source source address , destination destination address , reason error string`

说明：创建 IPsec 安全关联时发生错误。

建议的操作：这通常是暂时性错误状况。如果此消息持续出现，请联系思科 TAC。

602306

错误消息：`%ASA-3-602306: IPSEC: SA change peer IP error, SPI: IPsec SPI, (src {original src IP address | original src port}, dest {original dest IP address| original dest port} => src {new src IP address | new src port}, dest: {new dest IP address | new dest port}), reason failure reason`

说明：为 Mobile IKE 更新 IPsec 隧道的对等体地址时发生错误，对等体地址无法更改。

建议的操作：这通常是暂时性错误状况。如果此消息持续出现，请联系思科 TAC。

604101

错误消息：`%ASA-6-604101: DHCP client interface interface_name : Allocated ip = IP_address , mask = netmask , gw = gateway_address`

说明：Firepower 威胁防御 DHCP 客户端已从 DHCP 服务器成功获取 IP 地址。dhcpc 命令语句允许 Firepower 威胁防御设备从 DHCP 服务器及默认路由获取网络接口的 IP 地址和网络掩码。默认路由语句使用网关地址作为默认路由器的地址。

建议的操作：无需执行任何操作。

604102

错误消息：`%ASA-6-604102: DHCP client interface interface_name : address released`

说明：Firepower 威胁防御 DHCP 客户端将已分配 IP 地址释放回 DHCP 服务器。

建议的操作：无需执行任何操作。

604103

错误消息：`%ASA-6-604103: DHCP daemon interface interface_name : address granted MAC_address (IP_address )`

说明：Firepower 威胁防御 DHCP 服务器向外部客户端授予 IP 地址。

建议的操作：无需执行任何操作。

604104

错误消息：`%ASA-6-604104: DHCP daemon interface interface_name : address released build_number (IP_address )`

说明：外部客户端将 IP 地址释放回 Firepower 威胁防御 DHCP 服务器。

建议的操作：无需执行任何操作。

604105

错误消息：`%ASA-4-604105: DHCPD: Unable to send DHCP reply to client hardware_address on interface interface_name .Reply exceeds options field size (options_field_size ) by number_of_octets octets.`

说明：管理员可以配置返回 DHCP 客户端的 DHCP 选项。根据 DHCP 客户端请求的选项，提议的 DHCP 选项可能超过消息长度限制。无法发送 DHCP 提议，原因是它不符合消息限制。

- *hardware_address* - 请求客户端的硬件地址。
- *interface_name* - 发送和接收服务器消息的接口
- *options_field_size* - 最大选项字段长度。默认值为 312 个八位组，其中包括 4 个要终止的八位组。
- *number_of_octets* - 超出的八位组数量。

建议的操作：减少已配置 DHCP 选项的大小或数量。

604201

错误消息：`%ASA-6-604201: DHCPv6 PD client on interface <pd-client-iface> received delegated prefix <prefix> from DHCPv6 PD server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.`

说明：每当系统从 PD 服务器收到具有代理前缀的 DHCPv6 PD 客户端作为初始 4 次握手交换的一部分，就会显示此系统日志。如果存在多个前缀，系统将为每个前缀显示系统日志。

- *pd-client-iface* - 启用了此 DHCPv6 PD 客户端的接口名称。
- *prefix* - 从 DHCPv6 PD 服务器接收的前缀。
- *server-address* - DHCPv6 PD 服务器地址。
- *in-seconds* - 为代理前缀关联的首选和有效生命周期（以秒为单位）。

建议的操作：无。

604202

错误消息：`%ASA-6-604202: DHCPv6 PD client on interface <pd-client-iface> releasing delegated prefix <prefix> received from DHCPv6 PD server <server-address>.`

说明：每当 DHCPv6 PD 客户端在无配置时释放从 PD 服务器接收的代理前缀，就会显示此系统日志。如果存在多个前缀，系统将为每个前缀显示系统日志。

- *pd-client-iface* - 启用了此 DHCPv6 PD 客户端的接口名称。
- *prefix* - 从 DHCPv6 PD 服务器接收的前缀。
- *server-address* - DHCPv6 PD 服务器地址。

建议的操作：无。

604203

错误消息：`%ASA-6-604203: DHCPv6 PD client on interface <pd-client-iface> renewed delegated prefix <prefix> from DHCPv6 PD server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.`

说明：每当 DHCPv6 PD 客户端从 PD 服务器启动续订之前分配的代理前缀并成功时，就会显示此系统日志。如果存在多个前缀，系统将为每个前缀显示系统日志。

- *pd-client-iface* - 启用了此 DHCPv6 PD 客户端的接口名称。
- *prefix* - 从 DHCPv6 PD 服务器接收的前缀。
- *server-address* - DHCPv6 PD 服务器地址。
- *in-seconds* - 为代理前缀关联的首选和有效生命周期（以秒为单位）。

建议的操作：无。

604204

错误消息：`%ASA-6-604204: DHCPv6 delegated prefix <delegated prefix> got expired on interface <pd-client-iface>, received from DHCPv6 PD server <server-address>.`

说明：每当 DHCPv6 PD 客户端收到代理前缀即将过期的消息，就会显示此系统日志。

- *pd-client-iface* - 启用了此 DHCPv6 PD 客户端的接口名称。
- *prefix* - 从 DHCPv6 PD 服务器接收的前缀。
- *delegated prefix* - 从 DHCPv6 PD 服务器接收的代理前缀。

建议的操作：无。

604205

错误消息：`%ASA-6-604205: DHCPv6 client on interface <client-iface> allocated address <ipv6-address> from DHCPv6 server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds`

说明：每当系统从 DHCPv6 服务器收到作为初始 4 次握手交换一部分的 DHCPv6 客户端地址，且该地址有效，就会显示此系统日志。如果存在多个地址，系统将为接收的每个地址显示系统日志。

- *client-iface* - 启用了此 DHCPv6 客户端地址的接口名称。
- *ipv6-address* - 从 DHCPv6 服务器接收的 IPv6 地址。
- *server-address* - DHCPv6 服务器地址。

- *in-seconds* - 用于客户端地址的关联首选和有效生命周期（以秒为单位）

建议的操作：无。

604206

错误消息：`%ASA-6-604206: DHCPv6 client on interface <client-iface> releasing address <ipv6-address> received from DHCPv6 server <server-address>.`

说明：每当 DHCPv6 客户端地址配置未执行时，DHCPv6 客户端将会释放已接收的客户端地址。如果释放多个地址，系统将为每个地址显示系统日志。

- *client-iface* - 启用了此 DHCPv6 客户端地址的接口名称。
- *ipv6-address* - 从 DHCPv6 服务器接收的 IPv6 地址。
- *server-address* - DHCPv6 服务器地址。

建议的操作：无。

604207

错误消息：`%ASA-6-604207: DHCPv6 client on interface <client-iface> renewed address <ipv6-address> from DHCPv6 server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.`

说明：每当 DHCPv6 客户端从 DHCPv6 服务器启动续订之前分配的地址，就会显示此系统日志。如果存在多个地址，系统将为每个续订地址显示系统日志。

- *client-iface* - 启用了此 DHCPv6 客户端地址的接口名称。
- *ipv6-address* - 从 DHCPv6 服务器接收的 IPv6 地址。
- *server-address* - DHCPv6 服务器地址。
- *in-seconds* - 用于客户端地址的关联首选和有效生命周期（以秒为单位）

建议的操作：无。

604208

错误消息：`%ASA-6-604208: DHCPv6 client address <ipv6-address> got expired on interface <client-iface>, received from DHCPv6 server <server-address>`

说明：每当 DHCPv6 客户端收到地址即将过期的消息，就会显示此系统日志。

- *client-iface* - 启用了此 DHCPv6 客户端地址的接口名称。
- *ipv6-address* - 从 DHCPv6 服务器接收的 IPv6 地址。
- *server-address* - DHCPv6 服务器地址。

建议的操作：无。

605004

错误消息：`%ASA-6-605004: Login denied from source-address/source-port to interface:destination/service for user "username"`

说明：用户尝试登录控制台时，系统将显示以下形式的消息：

```
Login denied from serial to console for user "username"
```

登录尝试不正确或登录Firepower威胁防御设备失败。每次会话允许尝试登录三次，三次尝试不正确将终止会话。对于 SSH 和 Telnet 登录，第三次尝试失败或在一次或多次尝试后 TCP 会话终止时，系统将会生成此消息。对于其他类型的管理会话，每次尝试失败后都会生成此消息。用户名在无效或未知时隐藏，但在有效或配置了 **no logging hide username** 命令时显示。

- *source-address* - 尝试登录的源地址
- *source-port* - 尝试登录的源端口
- *interface* - 目的管理接口
- *destination* - 目的 IP 地址
- *service* - 目的服务
- *username* - 目的管理接口

建议的操作：如果此消息不经常出现，则无需执行任何操作。如果此消息经常出现，则可能表示发生了攻击。与用户沟通，验证用户名和密码。

605005

错误消息：`%ASA-6-605005: Login permitted from source-address /source-port to interface:destination /service for user "username"`

当用户登录控制台时，系统将显示以下形式的消息：

```
Login permitted from serial to console for user "username"
```

说明： 用户成功通过身份验证，并且启动了管理 会话。

- *source-address* - 尝试登录的源地址
- *source-port* - 尝试登录的源端口
- *interface* - 目的管理接口
- *destination* - 目的 IP 地址
- *service* - 目的服务
- *username* - 目的管理接口

建议的操作：无需执行任何操作。

607001

错误消息：`%ASA-6-607001: Pre-allocate SIP connection_type secondary channel for interface_name:IP_address/port to interface_name:IP_address from string message`

说明：fixup sip 命令在检测 SIP 消息后预分配了 SIP 连接。**Connection_type** 可能是以下一个字符串：

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- 路由
- RTP
- RTCP

建议的操作：无需执行任何操作。

608001

错误消息： `%ASA-6-608001: Pre-allocate Skinny connection_type secondary channel for interface_name:IP_address to interface_name:IP_address from string message`

说明：inspect skinny 命令在检测瘦客户端消息后预分配了瘦客户端连接。**Connection_type** 可能是以下一个字符串：

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- 路由
- RTP
- RTCP

建议的操作：无需执行任何操作。

608002

错误消息： `%ASA-4-608002: Dropping Skinny message for in_ifc :src_ip /src_port to out_ifc :dest_ip /dest_port , SCCP Prefix length value too small`

说明：系统收到瘦客户端 (SSCP) 消息，此消息的 SCCP 前缀长度小于配置的最小长度。

- *in_ifc* - 输入接口
- *src_ip* - 数据包的源 IP 地址
- *src_port* - 数据包的源端口
- *out_ifc* - 输出接口
- *dest_ip* - 数据包的目的 IP 地址
- *dest_port* - 数据包的目的端口
- *value* - 数据包的 SCCP 前缀长度

建议的操作：如果SCCP消息有效，请自定义瘦客户端策略映射，以增加SSCP前缀的最小长度值。

608003

错误消息：`%ASA-4-608003: Dropping Skinny message for in_ifc :src_ip /src_port to out_ifc :dest_ip /dest_port , SCCP Prefix length value too large`

说明：系统收到瘦客户端 (SSCP) 消息，此消息的 SCCP 前缀长度超过配置的最大长度。

- *in_ifc* - 输入接口
- *src_ip* - 数据包的源 IP 地址
- *src_port* - 数据包的源端口
- *out_ifc* - 输出接口
- *dest_ip* - 数据包的目的 IP 地址
- *dest_port* - 数据包的目的端口
- *value* - 数据包的 SCCP 前缀长度

建议的操作：如果SCCP消息有效，请自定义瘦客户端策略映射，以增加SCCP前缀的最大长度值。

609001

错误消息：`%ASA-7-609001: Built local-host zone-name/* :ip-address`

说明：系统为连接到区域 *zone-name* 的主机 **ip-address** 保留了网络状态容器。如果创建主机的接口属于区域的一部分，则会使用 zone-name/* 参数。星号代表所有接口，因为主机不属于任何一个接口。

建议的操作：无需执行任何操作。

609002

错误消息：`%ASA-7-609002: Teardown local-host zone-name/* :ip-address duration time`

说明：连接到区域 **zone-name** 的主机 **ip-address** 的网络状态容器已删除。如果创建主机的接口属于区域的一部分，则会使用 zone-name/* 参数。星号代表所有接口，因为主机不属于任何一个接口。

建议的操作：无需执行任何操作。

ID 介于 610101 到 622102 之间的消息

本部分包括 ID 介于 610101 到 622102 之间的消息。

611101

错误消息：`%ASA-6-611101: User authentication succeeded: IP, IP address : Uname: user`

说明：访问 Firepower 威胁防御设备时，用户身份验证成功。用户名在无效或未知时隐藏，但在有效或配置了 **no logging hide username** 命令时显示。

- *IP address* - 用户身份验证失败的客户端 IP 地址
- *user* - 通过身份验证的用户

建议的操作：无需执行任何操作。

611102

错误消息：`%ASA-6-611102: User authentication failed: IP = IP address, Uname: user`

说明：系统尝试访问 Firepower 威胁防御设备时，用户身份验证失败。用户名在无效或未知时隐藏，但在有效或配置了 **no logging hide username** 命令时显示。

- *IP address* - 用户身份验证失败的客户端 IP 地址
- *user* - 通过身份验证的用户

建议的操作：无需执行任何操作。

611103

错误消息：`%ASA-5-611103: User logged out: Uname: user`

说明：指定的用户已注销。

建议的操作：无需执行任何操作。

611104

错误消息：`%ASA-5-611104: Serial console idle timeout exceeded`

说明：由于没有用户活动，为 Firepower 威胁防御 串行控制台配置的空闲超时。

建议的操作：无需执行任何操作。

611301

错误消息：`%ASA-6-611301: VPNClient: NAT configured for Client Mode with no split tunneling: NAT address: mapped_address`

说明：系统已为不具备拆分隧道的客户端模式安装 VPN 客户端策略。

建议的操作：无需执行任何操作。

611302

错误消息：`%ASA-6-611302: VPNClient: NAT exemption configured for Network Extension Mode with no split tunneling`

说明：系统已为不具备拆分隧道的网络扩展模式安装 VPN 客户端策略。

建议的操作：无需执行任何操作。

611303

错误消息：`%ASA-6-611303: VPNClient: NAT configured for Client Mode with split tunneling: NAT address: mapped_address Split Tunnel Networks: IP_address/netmask IP_address/netmask`

说明：系统已为具有拆分隧道的客户端模式安装 VPN 客户端策略。

建议的操作：无需执行任何操作。

611304

错误消息：`%ASA-6-611304: VPNClient: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: IP_address/netmask IP_address/netmask`

说明：系统已为具有拆分隧道的网络扩展模式安装 VPN 客户端策略。

建议的操作：无需执行任何操作。

611305

错误消息：`%ASA-6-611305: VPNClient: DHCP Policy installed: Primary DNS: IP_address Secondary DNS: IP_address Primary WINS: IP_address Secondary WINS: IP_address`

说明：系统已为 DHCP 安装 VPN 客户端策略。

建议的操作：无需执行任何操作。

611306

错误消息：`%ASA-6-611306: VPNClient: Perfect Forward Secrecy Policy installed`

说明：完美前向保密已作为 VPN 客户端下载策略的一部分配置。

建议的操作：无需执行任何操作。

611307

错误消息：`%ASA-6-611307: VPNClient: Head end: IP_address`

说明：VPN 客户端已连接到指定前端。

建议的操作：无需执行任何操作。

611308

错误消息：`%ASA-6-611308: VPNClient: Split DNS Policy installed: List of domains: string string`

说明：拆分 DNS 策略已作为 VPN 客户端已下载策略的一部分安装。

建议的操作：无需执行任何操作。

611309

错误消息：`%ASA-6-611309: VPNClient: Disconnecting from head end and uninstalling previously downloaded policy: Head End: IP_address`

说明：VPN 客户端正在断开连接并卸载之前安装的策略。

建议的操作：无需执行任何操作。

611310

错误消息：`%ASA-6-611310: VNPClient: XAUTH Succeeded: Peer: IP_address`

说明：VPN 客户端 Xauth 在指定前端成功。

建议的操作：无需执行任何操作。

611311

错误消息：`%ASA-6-611311: VNPClient: XAUTH Failed: Peer: IP_address`

说明：VPN 客户端 Xauth 在指定前端失败。

建议的操作：无需执行任何操作。

611312

错误消息：`%ASA-6-611312: VPNClient: Backup Server List: reason`

说明：当 Firepower 威胁防御设备是 Easy VPN Remote 设备时，Easy VPN 服务器将一个备份服务器列表下载到了 Firepower 威胁防御设备。此列表会覆盖您在本地配置的任何备份服务器。如果已下载列表为空，则 Firepower 威胁防御设备不使用备份服务器。**reason** 是以下一条消息：

- 备份服务器 IP 地址列表
- 收到了 NULL 列表。正在删除当前备份服务器

建议的操作：无需执行任何操作。

611313

错误消息：`%ASA-3-611313: VPNClient: Backup Server List Error: reason`

说明：当 Firepower 威胁防御设备是 Easy VPN 远程设备且 Easy VPN 服务器将一个备份服务器列表下载到了 Firepower 威胁防御设备 时，列表中包含无效 IP 地址或主机名。Firepower 威胁防御设备不支持 DNS，因此不支持服务器的主机名，除非您使用 **name** 命令将名称手动映射到 IP 地址。

建议的操作：在 Easy VPN 服务器上，请确保服务器 IP 地址正确，并将服务器配置为 IP 地址而不是主机名。如果必须在服务器上使用主机名，请在 Easy VPN 远程设备上使用 **name** 命令将 IP 地址映射到名称。

611314

错误消息：`%ASA-6-611314: VPNClient: Load Balancing Cluster with Virtual IP: IP_address has redirected the to server IP_address`

说明：当 Firepower 威胁防御设备是 Easy VPN 远程设备时，负载均衡集群的主服务器会将 Firepower 威胁防御设备重定向至连接特定服务器。

建议的操作：无需执行任何操作。

611315

错误消息：`%ASA-6-611315: VPNClient: Disconnecting from Load Balancing Cluster member IP_address`

说明：当 Firepower 威胁防御设备是 Easy VPN 远程设备时，它将从负载均衡集群服务器断开连接。

建议的操作：无需执行任何操作。

611316

错误消息：`%ASA-6-611316: VPNClient: Secure Unit Authentication Enabled`

说明：当 Firepower 威胁防御设备是 Easy VPN 远程设备时，下载的 VPN 策略会启用 SUA。

建议的操作：无需执行任何操作。

611317

错误消息：`%ASA-6-611317: VPNClient: Secure Unit Authentication Disabled`

说明：当 Firepower 威胁防御设备是 Easy VPN 远程设备时，下载的 VPN 策略会禁用 SUA。

建议的操作：无需执行任何操作。

611318

错误消息：`%ASA-6-611318: VPNClient: User Authentication Enabled: Auth Server IP: IP_address Auth Server Port: port Idle Timeout: time`

说明：当 Firepower 威胁防御设备是 Easy VPN 远程设备时，下载的 VPN 策略对 Firepower 威胁防御设备内部网络中的用户启用 IUA。

- **IP_address** - Firepower 威胁防御设备 对其发送身份验证请求的服务器 IP 地址。
- **port** - Firepower 威胁防御设备 对其发送身份验证请求的服务器端口
- **time** - 身份验证凭证的空闲超时值

建议的操作：无需执行任何操作。

611319

错误消息：`%ASA-6-611319: VPNClient: User Authentication Disabled`

说明：当 Firepower 威胁防御设备是Easy VPN 远程设备时，下载的 VPN 策略对 Firepower 威胁防御内部网络中的用户禁用了 IUA。

建议的操作：无需执行任何操作。

611320

错误消息：`%ASA-6-611320: VPNClient: Device Pass Thru Enabled`

说明：当 Firepower 威胁防御设备是 Easy VPN 远程设备时，下载的 VPN 策略启用了设备透传。设备透传功能允许无法执行身份验证的设备（例如IP电话）在启用IUA时免于执行身份验证。如果在 Easy VPN 服务器中启用此功能，可以在 Firepower 威胁防御设备上使用 **vpnclient mac-exempt** 命令指定应当免于身份验证 (IUA) 的设备。

建议的操作：无需执行任何操作。

611321

错误消息：`%ASA-6-611321: VPNClient: Device Pass Thru Disabled`

说明：当 Firepower 威胁防御设备是 Easy VPN 远程设备时，下载的 VPN 策略禁用了设备透传。

建议的操作：无需执行任何操作。

611322

错误消息：`%ASA-6-611322: VPNClient: Extended XAUTH conversation initiated when SUA disabled`

说明：当 Firepower 威胁防御设备是 Easy VPN 远程设备且下载的 VPN 策略已禁用 SUA 时，Easy VPN 服务器将使用双因素/SecurID/基于 cryptocard 的身份验证机制对使用 XAUTH 的 Firepower 威胁防御设备进行身份验证。

建议的操作：如果您想使用双因素/SecurID/基于 cryptocard 的身份验证机制对 Easy VPN 远程设备进行身份验证，请在服务器中启用 SUA。

611323

错误消息：`%ASA-6-611323: VPNClient: Duplicate split nw entry`

说明：当 Firepower 威胁防御设备是 Easy VPN 远程设备时，下载的 VPN 策略中包含了重复拆分网络条目。如果条目同时匹配网络地址和网络掩码，则视为重复条目。

建议的操作：从 Easy VPN 服务器的 VPN 策略中删除重复的拆分网络条目。

612001

错误消息： `%ASA-5-612001: Auto Update succeeded:filename , version:number`

说明： 成功完成来自 Auto Update 服务器的更新。**Filename** 变量是映像、ASDM 文件或配置。**version number** 变量是更新的版本号。

建议的操作： 无需执行任何操作。

612002

错误消息： `%ASA-4-612002: Auto Update failed:filename , version:number , reason:reason`

说明： 来自自动更新服务器的更新失败。

- **filename** - 映像文件、ASDM 文件或配置文件。
- **version** - 更新的版本号。
- **reason** - 失败原因，可能是以下原因之一：

- 故障切换模块无法打开流缓冲区

- 故障切换模块无法将数据写入流缓冲区

- 故障切换模块无法在流缓冲区执行控制操作

- 故障切换模块无法打开闪存文件

- 故障切换模块无法将数据写入闪存

- 故障切换模块操作超时

- 故障切换命令链路已关闭

- 故障切换资源不可用

- 对等设备上的故障切换状态无效

- 故障切换模块遇到文件传输数据损坏

- 故障切换活动状态更改

- 故障切换命令执行失败

- 该映像无法在当前系统上运行

- 文件类型不受支持

建议的操作： 检查自动更新服务器的配置。检查备用设备是否处于故障状态。如果自动更新服务器配置正确，且备用设备未处于故障状态，请联系思科 TAC。

612003

错误消息： `%ASA-4-612003:Auto Update failed to contact:url , reason:reason`

说明：自动更新后台守护进程无法访问指定的 URL **url**，这可能是自动更新服务器 URL 或一个由自动更新服务器返回的文件服务器 URL。**reason** 字段说明访问失败的原因。可能的失败原因包括服务器未响应、身份验证失败或找不到文件。

建议的操作：检查自动更新服务器的配置。

613001

错误消息：`%ASA-6-613001: Checksum Failure in database in area string Link State Id IP_address Old Checksum number New Checksum number`

说明：由于内存损坏，OSPF 在数据库中检测到了校验和错误。

建议的操作：重新启动 OSPF 进程。

613002

错误消息：`%ASA-6-613002: interface interface_name has zero bandwidth`

说明：接口报告带宽为零。

建议的操作：按照显示正确复制此消息，并将其报告给思科 TAC。

613003

错误消息：`%ASA-6-613003: IP_address netmask changed from area string to area string`

说明：OSPF 配置更改导致网络范围更改区域。

建议的操作：在正确的网络范围内重新配置 OSPF。

613004

错误消息：`%ASA-3-613004: Internal error: memory allocation failure`

说明：发生了内部软件错误。

建议的操作：按显示正确复制错误消息，并将其报告给思科 TAC。

613005

错误消息：`%ASA-3-613005: Flagged as being an ABR without a backbone area`

说明：路由器已被标记为区域边界路由器 (ABR) 且未在路由器中配置主干区域。

建议的操作：重新启动 OSPF 进程。

613006

错误消息：`%ASA-3-613006: Reached unknown state in neighbor state machine`

说明：此路由器中发生内部软件错误，导致在数据库交换过程中出现无效邻居状态。

建议的操作：复制错误信息、配置以及任何导致此错误的事件详细信息，并将其提交给思科 TAC。

613007

错误消息：`%ASA-3-613007: area string lsid IP_address mask netmask type number`

说明：OSPF 尝试将现有 LSA 添加到数据库。

建议的操作：复制错误信息、配置以及任何导致此错误的事件详细信息，并将其提交给思科 TAC。

613008

错误消息：`%ASA-3-613008: if inside if_state number`

说明：发生了内部错误。

建议的操作：复制错误信息、配置以及任何导致此错误的事件详细信息，并将其提交给思科 TAC。

613011

错误消息：`%ASA-3-613011: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id`

说明：系统正在重置 OSPF 进程，并将选择新的路由器 ID。此操作将关闭所有虚拟链路。要让它们重新运行，需要在所有虚拟链路邻居上修改虚拟链路配置。

建议的操作：对所有虚拟链路邻居更改虚拟链路配置，从而反映新的路由器 ID。

613013

错误消息：`%ASA-3-613013: OSPF LSID IP_address adv IP_address type number gateway IP_address metric number forwarding addr route IP_address/mask type number has no corresponding LSA`

说明：OSPF 发现其数据库和 IP 路由表之间不一致。

建议的操作：复制错误信息、配置以及任何导致此错误的事件详细信息，并将其提交给思科 TAC。

613014

错误消息：`%ASA-6-613014: Base topology enabled on interface string attached to MTR compatible mode area string`

说明：连接到 MTR 兼容 OSPF 区域的 OSPF 接口需要启用基本拓扑。

建议的操作：无。

613015

错误消息： `%ASA-4-613015: Process 1 flushes LSA ID IP_address type-number adv-rtr IP_address in area mask`

说明： 路由器广泛重新发起或刷新此错误消息中报告的 LSA。

建议的操作： 如果此路由器正在刷新网络 LSA，这意味着路由器收到了 LSA ID 与路由器一个接口的 IP 地址冲突的网络 LSA，因此路由器从网络中清除了该 LSA。为了让 OSPF 正常运行，传输网络的 IP 地址必须具有唯一性。发生冲突的路由器即，报告此错误信息的路由器和使用此消息中报告为 adv-rtr 的 OSPF 路由器 ID 的路由器。如果此路由器重新发起 LSA，其他路由器很有可能会将此 LSA 从网络中清除。查找路由器并避免冲突。第 2 类 LSA 冲突可能是由于 LSA ID 重复。对于第 5 类 LSA，可能是由于报告此错误消息的路由器和连接到其他区域的路由器上存在重复路由器 ID。在不稳定的网络中，此消息可能是在警告其他原因导致了大量重新发起 LSA。请联系思科 TAC 调查这种情况。

613016

错误消息： `%ASA-3-613016: Area string router-LSA of length number bytes plus update overhead bytes is too large to flood.`

说明： 路由器尝试构建一个超过巨大系统缓冲区大小或 OSPF 协议规定最大值的路由器 LSA。

建议的操作： 如果报告的总长度（LSA 大小加上开销）大于巨大系统缓冲区大小，但小于 65535 字节（OSPF 协议规定最大值），则可以增加巨大系统缓冲区大小。如果报告的总长度大于 65535 字节，则需要减少报告区域中的 OSPF 接口数量。

613017

错误消息： `%ASA-4-613017: Bad LSA mask: Type number, LSID IP_address Mask` *`mask`* `from IP_address`

说明： 由于 LSA 发起方配置错误，路由器收到了具有无效 LSA 掩码的 LSA。因此，未在路由表中安装此路由。

建议的操作： 查找具有错误掩码的始发路由器，然后更正此 LSA 网络中的任何配置错误。如需进一步调试，请致电思科 TAC 获取帮助。

613018

错误消息： `%ASA-4-613018: Maximum number of non self-generated LSA has been exceeded “OSPF number” - number LSAs`

说明： 已超过非自生成 LSA 的最大数量。

建议的操作： 检查网络中的路由器是否由于配置错误而生成了大量 LSA。

613019

错误消息： `%ASA-4-613019: Threshold for maximum number of non self-generated LSA has been reached "OSPF number" - number LSAs`

说明： 已达到非自动生成 LSA 的最大数量阈值。

建议的操作： 检查网络中的路由器是否由于配置错误而生成了大量 LSA。

613021

错误消息： `%ASA-4-613021: Packet not written to the output queue`

说明： 发生了内部错误。

建议的操作： 复制错误信息、配置以及任何导致此错误的事件详细信息，并将其提交给思科 TAC。

613022

错误消息： `%ASA-4-613022: Doubly linked list linkage is NULL`

说明： 发生了内部错误。

建议的操作： 复制错误信息、配置以及任何导致此错误的事件详细信息，并将其提交给思科 TAC。

613023

错误消息： `%ASA-4-613023: Doubly linked list prev linkage is NULL number`

说明： 发生了内部错误。

建议的操作： 复制错误信息、配置以及任何导致此错误的事件详细信息，并将其提交给思科 TAC。

613024

错误消息： `%ASA-4-613024: Unrecognized timer number in OSPF string`

说明： 发生了内部错误。

建议的操作： 复制错误信息、配置以及任何导致此错误的事件详细信息，并将其提交给思科 TAC。

613025

错误消息： `%ASA-4-613025: Invalid build flag number for LSA IP_address, type number`

说明： 发生了内部错误。

建议的操作： 复制错误信息、配置以及任何导致此错误的事件详细信息，并将其提交给思科 TAC。

613026

错误消息： `%ASA-4-613026: Can not allocate memory for area structure`

说明： 发生了内部错误。

建议的操作： 复制错误信息、配置以及任何导致此错误的事件详细信息，并将其提交给思科 TAC。

613027

错误消息： `%ASA-6-613027: OSPF process number removed from interface interface_name`

说明： IP VRF 导致从接口中删除了 OSPF 进程。

建议的操作： 无。

613028

错误消息： `%ASA-6-613028: Unrecognized virtual interface intetface_name.Treat it as loopback stub route`

说明： OSPF 无法识别虚拟接口类型，因此该接口被视为环回接口末节路由。

建议的操作： 无。

613029

错误消息： `%ASA-3-613029: Router-ID IP_address is in use by ospf process number`

说明： Firepower 威胁防御设备尝试分配一个其他进程正在使用的路由器 ID。

建议的操作： 为其中一个进程配置其他路由器 ID。

613030

错误消息： `%ASA-4-613030: Router is currently an ASBR while having only one area which is a stub area`

说明： ASBR 必须连接到可以承载 AS 外部或 NSSA LSA 的区域。

建议的操作： 将路由器连接的区域调整为 NSSA 区域或常规区域。

613031

错误消息： `%ASA-4-613031: No IP address for interface inside`

说明： 此接口不是点到点接口，且未编号。

建议的操作： 更改接口类型，或为接口指定 IP 地址。

613032

错误消息： `%ASA-3-613032: Init failed for interface inside, area is being deleted.请重试。`

说明： 接口初始化失败。可能的原因包括：

- 接口连接的区域正在被删除。
- 无法为本地路由器创建邻居数据块。

建议的操作： 删除涵盖此接口的配置命令并重试。

613033

错误消息： `%ASA-3-613033: Interface inside is attached to more than one area`

说明： 接口位于接口所连接区域之外的区域的接口列表上。

建议的操作： 复制错误信息、配置以及任何导致此错误的事件详细信息，并将其提交给思科 TAC。

613034

错误消息： `%ASA-3-613034: Neighbor IP_address not configured`

说明： 配置的邻居选项无效。

建议的操作： 检查 **neighbor** 命令的配置选项，为邻居接口更正选项或网络类型。

613035

错误消息： `%ASA-3-613035: Could not allocate or find neighbor IP_address`

说明： 发生了内部错误。

建议的操作： 按显示正确复制错误消息，并将其报告给思科 TAC。

613036

错误消息： `%ASA-4-613036: Can not use configured neighbor: cost and database-filter options are allowed only for a point-to-multipoint network`

说明： 在NBMA网络上发现了已配置邻居，且已配置开销或数据库过滤器选项。仅允许在点对多点类型网络上使用这些选项。

建议的操作： 检查 **neighbor** 命令的配置选项，为邻居接口更正选项或网络类型。

613037

错误消息： `%ASA-4-613037: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network`

说明：在点对多点网络上发现了已配置邻居，且已配置轮询或优先级选项。仅允许在NBMA类型网络上使用这些选项。

建议的操作：检查 **neighbor** 命令的配置选项，为邻居接口更正选项或网络类型。

613038

错误消息：`%ASA-4-613038: Can not use configured neighbor: cost or database-filter option is required for point-to-multipoint broadcast network`

说明：系统在点对多点广播网络中发现了已配置邻居。需要配置 **cost** 或 **database-filter** 选项。

建议的操作：检查 **neighbor** 命令的配置选项，为邻居接口更正选项或网络类型。

613039

错误消息：`%ASA-4-613039: Can not use configured neighbor: neighbor command is allowed only on NBMA and point-to-multipoint networks`

说明：系统在网络中发现了已配置邻居，其网络类型既不是 NBMA，也不是点对多点。

建议的操作：无。

613040

错误消息：`%ASA-4-613040: OSPF-1 Area string: Router IP_address originating invalid type number LSA, ID IP_address, Metric number on Link ID IP_address Link Type number`

说明：此消息中指示的路由器发起了具有无效度量的LSA。如果这是一个路由器LSA且链路度量为零，则网络中存在路由环路和流量损失的风险。

建议的操作：为源于报告 LSA 的路由器中的给定 LSA 类型和链路类型配置有效度量。

613041

错误消息：`%ASA-6-613041: OSPF-100 Areav string: LSA ID IP_address, Type number, Adv-rtr IP_address, LSA counter DoNotAge`

说明：内部错误已自行更正。此错误消息未造成相关操作影响。

建议的操作：检查系统内存。如果内存过低，则计时器轮函数未初始化。当内存可用时，请尝试重新输入相应命令。如果内存不足，请联系思科 TAC，并且提供 **show memory**、**show processes** 和 **show tech-support ospf** 命令的输出。

613042

错误消息：`%ASA-4-613042: OSPF process number lacks forwarding address for type 7 LSA IP_address in NSSA string - P-bit cleared`

说明：NSSA 区域中没有可行转发地址。因此，必须清除 P 位，而 NSSA 转换器未能将第 7 类 LSA 转换为第 5 类 LSA。请参见 RFC 3101。

建议的操作：在具有通告 IP 地址的 NSSA 中至少配置一个接口。由于通告不依赖于底层第 2 层状态，因此首选环回接口。

613043

错误消息：`%ASA-6-613043:`

说明：发生负数据库引用计数。

建议的操作：检查系统内存。如果内存过低，则计时器轮函数未初始化。当内存可用时，请尝试重新输入相应命令。如果内存不足，请联系思科 TAC，并且提供 **show memory**、**show processes** 和 **show tech-support ospf** 命令的输出。

613101

错误消息：`%ASA-6-613101: Checksum Failure in database in area` *`s`* `Link State Id` *`i`* `Old Checksum` *`#x`* `New Checksum` *`#x`*

说明：由于内存损坏，OSPF 在数据库中检测到了校验和错误。

建议的操作：重新启动 OSPF 进程。

613102

错误消息：`%ASA-6-613102: interface` *`s`* `has zero bandwidth`

说明：接口将带宽报告为零。

建议的操作：无需执行任何操作。

613103

错误消息：`%ASA-6-613103:` *`i m`* `changed from area` *`AREA_ID_STR`* `to area` *`AREA_ID_STR`*

说明：OSPF 配置更改导致网络范围更改区域。

建议的操作：无需执行任何操作。

613104

错误消息：`%ASA-6-613104: Unrecognized virtual interface` *`IF_NAME`* `.`

说明：OSPFv3 无法识别虚拟接口类型，因此该接口被视为环回接口末节路由。

建议的操作：无需执行任何操作。

614001

错误消息： `%ASA-6-614001: Split DNS: request patched from server: IP_address to server: IP_address`

说明： 拆分 DNS 正在将来自原始目的服务器的 DNS 查询重定向至主企业 DNS 服务器。

建议的操作： 无需执行任何操作。

614002

错误消息： `%ASA-6-614002: Split DNS: reply from server:IP_address reverse patched back to original server:IP_address`

说明： 拆分 DNS 正在将来自企业 DNS 服务器的 DNS 查询重定向至原始目的服务器。

建议的操作： 无需执行任何操作。

615001

错误消息： `%ASA-6-615001: vlan number not available for firewall interface`

说明： 交换机已从 Firepower 威胁防御设备中删除 VLAN。

建议的操作： 无需执行任何操作。

615002

错误消息： `%ASA-6-615002: vlan number available for firewall interface`

说明： 交换机已将 VLAN 添加到 Firepower 威胁防御设备。

建议的操作： 无需执行任何操作。

621001

错误消息： `%ASA-6-621001: Interface` *interface_name* does not support multicast, not enabled

说明： 系统尝试在不支持组播的接口上启用 PIM。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

621002

错误消息： `%ASA-6-621002: Interface` *interface_name* does not support multicast, not enabled

说明： 用户尝试在不支持组播的接口上启用 IGMP。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

621003

错误消息：`%ASA-6-621003: The event queue size has exceeded` *number*

说明：创建的事件管理器数量超过预期数量。

建议的操作：如果问题仍然存在，请联系思科 TAC。

621006

错误消息：`%ASA-6-621006: Mrib disconnected`, (*IP_address* ,*IP_address*) event cancelled

说明：系统收到触发数据驱动型事件的数据包，但与 MRIB 的连接已关闭。通知已取消。

建议的操作：如果问题仍然存在，请联系思科 TAC。

621007

错误消息：`%ASA-6-621007: Bad register from` *interface_name* :*IP_address* to *IP_address* for (*IP_address* , *IP_address*)

说明：配置为交汇点或具有 NAT 的 PIM 路由器收到了来自其他 PIM 路由器的 PIM 注册数据包。此数据包中封装的数据无效。

建议的操作：发送端路由器会错误地发送非 RFC 寄存器。请升级发送端路由器。

622001

错误消息：`%ASA-6-622001:` *string* tracked route *network mask address* , distance *number* , table *string* , on interface *interface-name*

说明：系统已将跟踪路由添加到路由表，或已从路由表中删除该路由，这意味着跟踪对象的状态在启用和关闭间切换。

- *string* - 添加或删除
- *network* - 网络地址
- *mask* - 网络掩码
- *address* - 网关地址
- *number* - 路由管理距离
- *string* - 路由表名称
- *interface-name* - 通过 **nameif** 命令指定的接口名称

建议的操作：无需执行任何操作。

622101

错误消息：`%ASA-6-622101:` Starting regex table compilation for *match_command* ; table entries = *regex_num* entries

说明：系统显示正则表达式编译的背景活动信息。

- *match_command* - 与正则表达式表关联的匹配命令
- *regex_num* - 要编译的正则表达式条目

建议的操作：无需执行任何操作。

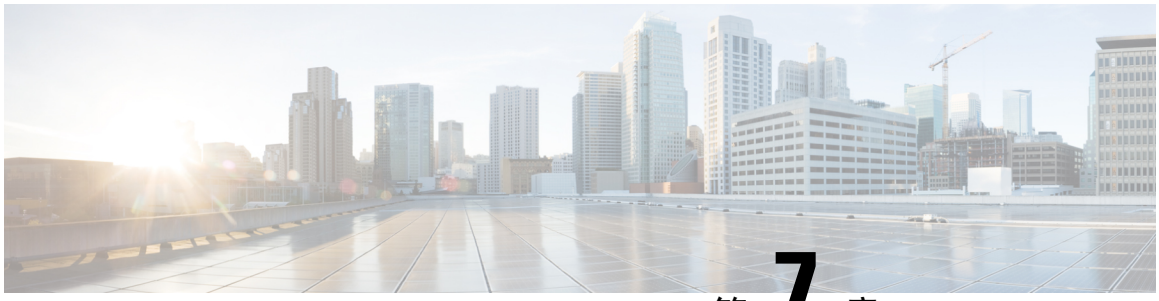
622102

错误消息：`%ASA-6-622102`: Completed regex table compilation for *match_command* ; table size = *num* bytes

说明：系统显示正则表达式编译的背景活动信息。

- *match_command* - 与正则表达式表关联的匹配命令
- *num* - 编译表大小（以字节为单位）

建议的操作：无需执行任何操作。



第 7 章

系统日志消息 701001-714011

本章包含以下各节：

ID 介于 701001 到 713109 之间的消息

本部分包括 ID 介于 701001 到 713109 之间的消息。

701001

错误消息： `%ASA-7-701001: alloc_user() out of Tcp_user objects`

说明： 如果用户身份验证频率太高而导致模块无法处理新的 AAA 请求，系统将显示 AAA 消息。

建议的操作： 通过泛洪防范启用命令启用 Flood Defender。

701002

错误消息： `%ASA-7-701002: alloc_user() out of Tcp_proxy objects`

说明： 如果用户身份验证频率太高而导致模块无法处理新的 AAA 请求，系统将显示 AAA 消息。

建议的操作： 通过泛洪防范启用命令启用 Flood Defender。

703001

错误消息： `%ASA-7-703001: H.225 message received from` *`interface_name :IP_address /port`* `to` *`interface_name :IP_address /port`* `is using an unsupported version` *`number`*

说明： Firepower 威胁防御设备收到 H.323 数据包，其中包含不受支持的版本号。Firepower 威胁防御设备可能对数据包的协议版本字段重新编码，更改为最高支持版本。

建议的操作： 使用 Firepower 威胁防御设备在 VoIP 网络中支持的 H.323 版本。

703002

错误消息： `%ASA-7-703002: Received H.225 Release Complete with newConnectionNeeded for interface_name :IP_address to interface_name :IP_address /port`

说明： Firepower 威胁防御设备收到了指定的 H.225 消息，Firepower 威胁防御设备为两个指定的 H.323 终端打开了新的信令连接对象。

建议的操作： 无需执行任何操作。

703008

错误消息： `%ASA-7-703008: Allowing early-message: %s before SETUP from %s:%Q/%d to %s:%Q/%d`

说明： 此消息表示，外部终端请求向内部主机进行传入呼叫，并且希望内部主机向网守先发送 FACILITY 消息再发送 SETUP 消息，同时希望遵循 H.460.18 的要求。

建议的操作： 确保设置的确计划根据 H.640.18 中的说明，在传入 H323 呼叫中先允许 FACILITY 消息再允许 SETUP 消息。

709001、709002

错误消息： `%ASA-7-709001: FO replication failed: cmd=command returned=code`

错误消息： `%ASA-7-709002: FO unreplicable: cmd=command`

说明： 系统仅在开发调试和测试阶段显示故障切换消息。

建议的操作： 无需执行任何操作。

709003

错误消息： `%ASA-1-709003: (Primary) Beginning configuration replication: Sending to mate.`

说明： 主用设备开始向备用设备复制配置时，系统会显示此故障切换消息。主设备也可列为辅助设备的辅助设备。

建议的操作： 无需执行任何操作。

709004

错误消息： `%ASA-1-709004: (Primary) End Configuration Replication (ACT)`

说明： 主用设备完成将自身配置复制到备用设备上时，系统会显示此故障切换消息。主设备也可列为辅助设备的辅助设备。

建议的操作： 无需执行任何操作。

709005

错误消息： `%ASA-1-709005: (Primary) Beginning configuration replication: Receiving from mate.`

说明： 备用 Firepower 威胁防御设备从主用 Firepower 威胁防御设备接收了配置复制的第一部分。主设备也可列为辅助设备的辅助设备。

建议的操作： 无需执行任何操作。

709006

错误消息： `%ASA-1-709006: (Primary) End Configuration Replication (STB)`

说明： 备用设备完成复制主用设备发送的配置后，系统会显示此故障切换消息。主设备也可列为辅助设备的辅助设备。

建议的操作： 无需执行任何操作。

709007

错误消息： `%ASA-2-709007: Configuration replication failed for command`

说明： 当备用设备无法完成复制主用设备发送的配置时，系统会显示此故障切换消息。消息结尾处将显示导致故障的命令。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

709008

错误消息： `%ASA-4-709008: (Primary | Secondary) Configuration sync in progress.Command: ‘command ’ executed from (terminal/http) will not be replicated to or executed by the standby unit.`

说明： 在配置同步期间发出了一条命令，这将触发交互式提示，指出系统不会在备用设备上发出此命令。要继续操作，请注意，系统只会在主用设备上发出此命令，而且不会在备用设备上复制该命令。

- Primary | Secondary - 这是主设备或辅助设备
- *command* - 在配置同步期间发出的命令
- terminal/http - 从终端或通过 HTTP 发出。

建议的操作： 无。

710001

错误消息： `%ASA-7-710001: TCP access requested from source_address /source_port to interface_name :dest_address /service`

说明：发往 Firepower 威胁防御设备的第一个 TCP 数据包请求建立 TCP 会话。此数据包是三次握手中的第一个 SYN 数据包。当各方（Telnet、HTTP 或 SSH）允许该数据包时，系统将显示此消息。但是，SYN cookie 验证尚未完成，状态未保留。

建议的操作：无需执行任何操作。

710002

错误消息：`%ASA-7-710002: {TCP|UDP} access permitted from source_address /source_port to interface_name :dest_address /service`

说明：对于 TCP 连接，发往 Firepower 威胁防御设备的第二个 TCP 数据包请求建立 TCP 会话。此数据包是三次握手中的最终 ACK。各方（Telnet、HTTP 或 SSH）已允许该数据包。此外，SYN cookie 验证成功并为 TCP 会话保留了该状态。

对于 UDP 连接，系统已允许连接。例如，该模块从授权的 SNMP 管理站收到一条 SNMP 请求，并且已处理请求。此消息的速率限制为每 10 秒一条消息。

建议的操作：无需执行任何操作。

710003

错误消息：`%ASA-3-710003: {TCP|UDP} access denied by ACL from source_IP/source_port to interface_name :dest_IP/service`

说明：Firepower 威胁防御设备已拒绝与接口服务的连接尝试。例如，Firepower 威胁防御设备从未授权的 SNMP 管理站收到 SNMP 请求。如果此消息经常出现，则可能表示发生了攻击。

例如：

```
%ASA-3-710003: UDP access denied by ACL from 95.1.1.14/5000 to outside:95.1.1.13/1005
```

建议的操作：使用 **show run http**、**show run ssh** 或 **show run telnet** 命令验证是否已将 Firepower 威胁防御设备配置为允许来自主机或网络的服务访问。

710004

错误消息：`%ASA-7-710004: TCP connection limit exceeded from Src_ip /Src_port to In_name :Dest_ip /Dest_port (current connections/connection limit = Curr_conn/Conn_lmt)`

说明：现已超过服务的 Firepower 威胁防御 管理连接最大数量。Firepower 威胁防御设备允许每项管理服务最多五个并发管理连接。或者，传入连接计数器中可能发生了错误。

- *Src_ip* - 数据包的源 IP 地址
- *Src_por* t - 数据包源端口
- *In_ifc* - 输入接口
- *Dest_ip* - 数据包的目的 IP 地址
- *Dest_port* - 数据包的目的端口
- *Curr_conn* - 当前传入管理连接数量

- *Conn_lmt* - 连接限制

建议的操作：在控制台中使用 **kill** 命令释放不需要的会话。如果由于传入计数器错误而导致生成此消息，请运行 **show conn all** 命令显示连接详细信息。

710005

错误消息：`%ASA-7-710005: {TCP|UDP} request discarded from source_address /source_port to interface_name :dest_address /service`

说明：Firepower 威胁防御设备 没有为 UDP 请求提供服务的 UDP 服务器。而且，不属于 Firepower 威胁防御设备上任何会话的 TCP 数据包可能被丢弃。此外，当 Firepower 威胁防御设备收到具有空负载的 SNMP 请求时，即使请求来自授权主机，也会出现此消息（对于 SNMP 服务）。对于 SNMP 服务，消息最多每 10 秒出现一次，防止日志接收器被淹没。

建议的操作：在广泛使用广播服务（例如 DHCP、RIP 或 NetBIOS）的网络中可能经常出现此消息。如果此消息过于频繁出现，则可能表示发生了攻击。

710006

错误消息：`%ASA-7-710006: protocol request discarded from source_address to interface_name :dest_address`

说明：Firepower 威胁防御设备不具备为 IP 协议请求提供服务的 IP 服务器；例如，Firepower 威胁防御设备接收非 TCP 或 UDP 的 IP 数据包，但 Firepower 威胁防御设备无法为请求提供服务。

建议的操作：在广泛使用广播服务（例如 DHCP、RIP 或 NetBIOS）的网络中可能经常出现此消息。如果此消息过于频繁出现，则可能表示发生了攻击。

710007

错误消息：`%ASA-7-710007: NAT-T keepalive received from 86.1.161.1/1028 to outside:86:1.129.1/4500`

说明：Firepower 威胁防御设备 收到了 NAT-T 保持连接消息。

建议的操作：无需执行任何操作。

711001

错误消息：`%ASA-7-711001: debug_trace_msg`

说明：您为日志记录功能输入了 **logging debug-trace** 命令。启用 **logging debug-trace** 命令后，所有调试消息将重定向至待处理消息。出于安全原因，消息输出必须加密或通过安全的带外网络发送。

建议的操作：无需执行任何操作。

711002

错误消息： `%ASA-4-711002: Task ran for elapsed_time msecs, process = process_name , PC = PC Tracebeback = traceback`

说明： 进程使用 CPU 超过 100 毫秒。此消息用于调试 CPU，并且对于每个违规进程每隔 5 秒显示一次。

- **PC** - CPU 占用进程的指令指针。
- **traceback** - CPU 占用进程的堆叠跟踪，最多可以包含 12 个地址

建议的操作： 无需执行任何操作。

711003

错误消息： `ASA-7-711003: Unknown/Invalid interface identifier(vpifnum ) detected.`

说明： 发生了正常操作期间本不应发生的内部不一致。但是，此类消息偶尔出现并无危害。如果经常发生，则可能需要调试。

- *vpifnum* - 与接口对应的 32 位值

建议的操作： 如果问题仍然存在，请联系思科 TAC。

711004

错误消息： `%ASA-4-711004: Task ran for msec msec, Process = process_name , PC = pc , Call stack = call stack`

说明： 进程使用 CPU 超过 100 毫秒。此消息用于调试 CPU，并且对于每个违规进程每隔 5 秒显示一次。

- **msec -** 检测到的 CPU 占用长度（以毫秒为单位）
- *process_name* - 占用进程的名称
- **pc** - CPU 占用进程的指令指针。
- **call stack** - CPU 占用进程的堆叠跟踪，最多可以包含 12 个地址

建议的操作： 无需执行任何操作。

711005

错误消息： `%ASA-5-711005: Traceback: call_stack`

说明： 发生了本不应出现的内部软件问题。设备通常可以从此错误中恢复，而且不会影响设备结果。

- *call_stack* - 调用堆叠的 EIP

建议的操作： 联系思科 TAC。

711006

错误消息： `%ASA-7-711006: CPU profiling has started for n-samples samples.Reason: reason-string .`

说明： CPU 分析已启动。

- *n-samples* - 指定的 CPU 分析样本数量
- *reason-string* - 可能的值包括：

“CPU utilization passed *cpu-utilization* %”

“Process process-name CPU utilization passed *cpu-utilization* %”

建议的操作： “未指定”

建议的操作： 收集 CPU 分析结果，并将其提供给思科 TAC。

713004

错误消息： %ASA-3-713004: dev`ice scheduled for reboot or shutdown, IKE key acquire message on interface interface num , for Peer IP_address ignored`

说明： Firepower 威胁防御设备 从尝试启动隧道的远程实体收到 IKE 数据包。因为系统计划重新启动或关闭 Firepower 威胁防御设备，因此不允许建立更多隧道。IKE 数据包被忽略并丢弃。

建议的操作： 无需执行任何操作。

713201

错误消息： `%ASA-5-713201: Duplicate Phase Phase  packet detected.`操作

说明： Firepower 威胁防御设备收到了与先前的第 1 阶段或第 2 阶段重复的数据包，并将传输最后一条消息。可能发生了网络性能或连接问题，导致对等体未及时接收已发送的数据包。

- **Phase** - 第 1 或第 2 阶段
- **Action** - 正在重新传输最后一个数据包，或者没有要传输的最后一个数据包。

建议的操作： 验证网络性能或连接。

713202

错误消息： `%ASA-6-713202: Duplicate IP_addr packet detected.`

说明： Firepower 威胁防御设备已收到 Firepower 威胁防御设备已经获知并正在协商的隧道的重复第一个数据包，这表示 Firepower 威胁防御设备可能从对等体收到了重新传输的数据包。

- **IP_addr** - 发出重复第一个数据包的对等体 IP 地址

建议的操作： 除非连接尝试失败，否则无需执行任何操作。如果连接尝试失败，请进一步调试并诊断问题。

713006

错误消息： `%ASA-5-713006: Failed to obtain state for message Id message_number , Peer Address: IP_address`

说明： Firepower 威胁防御设备 不了解接收的消息 ID。此消息 ID 用于标识特定 IKE 第 2 阶段协商。Firepower 威胁防御设备 中可能出现了错误情况，也可能是两个 IKE 对等体不同步。

建议的操作： 无需执行任何操作。

713008

错误消息： `%ASA-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel`

说明： ID 负载中收到的密钥 ID 值超过了此 IKE 会话（使用预共享密钥身份验证）组名称的最大允许大小。这是无效值，并且此会话将被拒绝。请注意，由于无法在Firepower威胁防御设备中创建如此大小的组名称，因此指定密钥 ID 无法运行。

建议的操作： 确保客户端对等体（最有可能是 Altiga 远程访问客户端）指定有效的组名称。通知用户更改客户端上不正确的组名称。组名称的当前最大长度为 32 个字符。

713009

错误消息： `%ASA-3-713009: OU in DN in ID payload too big for Certs IKE tunnel`

说明： ID 负载收到 DN 中的 OU 值，该值超过了此 IKE 会话（使用证书身份验证）组名称的最大允许大小。系统会跳过此 OU，另一个 OU 或其他条件可能会发现匹配组。

建议的操作： 为使客户端能够使用 OU 在 Firepower 威胁防御设备中查找组，组名称的长度必须有效。组名称的当前最大长度为 32 个字符。

713010

%ASA-5-713010: IKE area: failed to find centry for message Id *message_number*

系统尝试使用唯一消息 ID 查找 conn_entry（与 IPsec SA 对应的 IKE 第 2 阶段结构），但操作失败。未找到内部结构，以非标准方式终止会话时可能会出现这个问题，但更有可能是发生了内部错误。

如果此问题仍然存在，请检查对等体。

713012

错误消息： `%ASA-3-713012: Unknown protocol (protocol ).Not adding SA w/spi=SPI value`

说明： 从对等体收到非法或不受支持的 IPsec 协议。

建议的操作： 检查对等体上的 ISAKMP 第 2 阶段配置，确保与 Firepower 威胁防御设备兼容。

713014

错误消息： %ASA-3-713014: Unknown Domain of Interpretation (DOI): *DOI value*

说明： 从对等体接收的 ISAKMP ID 不受支持。

建议的操作： 检查对等体上的 ISAKMP DOI 配置。

713016

错误消息： %ASA-3-713016: Unknown identification type, Phase 1 or 2, Type *ID_Type*

说明： 从对等体接收的 ID 未知。这个 ID 可能是不熟悉的有效 ID，也可能是无效或已损坏的 ID。

建议的操作： 检查前端和对等体上的配置。

713017

错误消息： %ASA-3-713017: Identification type not supported, Phase 1 or 2, Type *ID_Type*

说明： 从对等体接收的第 1 阶段或第 2 阶段 ID 合法，但不受支持。

建议的操作： 检查前端和对等体上的配置。

713018

错误消息： %ASA-3-713018: Unknown ID type during find of group name for certs, Type *ID_Type*

说明： 发生了内部软件错误。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

713020

错误消息： : No Group found by matching OU(s) from ID payload: *OU_value*

说明： 发生了内部软件错误。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

713022

错误消息： %ASA-3-713022: No Group found matching *peer_ID* or *IP_address* for Pre-shared key peer *IP_address*

说明： 组位于与对等体指定的值（密钥 ID 或 IP 地址）具有相同名称的组数据库中。

建议的操作： 验证对等体上的配置。

713024

错误消息： `%ASA-7-713024: Group group IP ip Received local Proxy Host data in ID Payload: Address IP_address , Protocol protocol , Port port`

说明： Firepower 威胁防御设备 已从远程对等体收到第 2 阶段本地代理 ID 负载。

建议的操作： 无需执行任何操作。

713025

错误消息： `%ASA-7-713025: Received remote Proxy Host data in ID Payload: Address IP_address , Protocol protocol , Port port`

说明： Firepower 威胁防御设备 已从远程对等体收到第 2 阶段本地代理 ID 负载。

建议的操作： 无需执行任何操作。

713028

错误消息： `%ASA-7-713028: Received local Proxy Range data in ID Payload: Addresses IP_address-IP_address , Protocol protocol , Port port`

说明： Firepower 威胁防御设备已收到远程对等体的第 2 阶段本地代理 ID 负载，其中包括 IP 地址范围。

建议的操作： 无需执行任何操作。

713029

错误消息： `%ASA-7-713029: Received remote Proxy Range data in ID Payload: Addresses IP_address-IP_address , Protocol protocol , Port port`

说明： Firepower 威胁防御设备已收到远程对等体的第 2 阶段本地代理 ID 负载，其中包括 IP 地址范围。

建议的操作： 无需执行任何操作。

713032

错误消息： `%ASA-3-713032: Received invalid local Proxy Range IP_address- IP_address`

说明： 本地 ID 负载包括范围 ID 类型，且指定低位地址不小于高位地址。可能存在配置问题。

建议的操作： 检查 ISAKMP 第 2 阶段参数的配置。

713033

错误消息： `%ASA-3-713033:` Received invalid remote Proxy Range *IP_address* - *IP_address*

说明： 远程 ID 负载包括范围 ID 类型，且指定低位地址不小于高位地址。可能存在配置问题。

建议的操作：检查 ISAKMP 第 2 阶段参数的配置。

713034

错误消息：`%ASA-7-713034: Received local IP Proxy Subnet data in ID Payload: Address IP_address , Mask netmask , Protocol protocol , Port port`

说明：在第 2 阶段 ID 负载中收到了本地 IP 代理子网数据。

建议的操作：无需执行任何操作。

713035

错误消息：`%ASA-7-713035: Group group IP ip Received remote IP Proxy Subnet data in ID Payload: Address IP_address , Mask netmask , Protocol protocol , Port port`

说明：在第 2 阶段 ID 负载中收到了远程 IP 代理子网数据。

建议的操作：无需执行任何操作。

713039

错误消息：`%ASA-7-713039: Send failure: Bytes (number ), Peer: IP_address`

说明：发生了内部软件错误，并且无法传输 ISAKMP 数据包。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713040

错误消息：`%ASA-7-713040: Could not find connection entry and can not encrypt: msgid message_number`

说明：发生了内部软件错误，而且找不到第 2 阶段数据结构。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713041

错误消息：`%ASA-5-713041: IKE Initiator: new or rekey Phase 1 or 2, Intf interface_number , IKE Peer IP_address local Proxy Address IP_address , remote Proxy Address IP_address , Crypto map (crypto map tag )`

说明：Firepower 威胁防御设备 正在担任发起者协商隧道。

建议的操作：无需执行任何操作。

713042

错误消息： `%ASA-3-713042: IKE Initiator unable to find policy: Intf interface_number , Src: source_address , Dst: dest_address`

说明： IPsec 快速路径处理了触发 IKE 的数据包，但是 IKE 策略查找失败。此错误可能与时序相关。在 IKE 处理发起请求之前，触发 IKE 的 ACL 可能已被删除。此问题很有可能会自行更正。

建议的操作： 如果这种状况仍然存在，请检查 L2L 配置，特别应注意与加密映射关联的 ACL 类型。

713043

错误消息： `%ASA-3-713043: Cookie/peer address IP_address session already in progress`

说明： 在原始隧道进程中再次触发了 IKE。

建议的操作： 无需执行任何操作。

713048

错误消息： `%ASA-3-713048: Error processing payload: Payload ID: id`

说明： 在无法处理的负载中收到了数据包。

建议的操作： 如果此问题仍然存在，则对等体上可能存在配置错误。

713049

错误消息： `%ASA-5-713049: Security negotiation complete for tunnel_type type (group_name ) Initiator /Responder , Inbound SPI = SPI , Outbound SPI = SPI`

说明： 已启动 IPsec 隧道。

建议的操作： 无需执行任何操作。

713050

错误消息： `%ASA-5-713050: Connection terminated for peer IP_address .Reason: termination reason Remote Proxy IP_address , Local Proxy IP_address`

说明： IPsec 隧道已终止。可能的终止原因包括：

- IPsec SA 空闲超时
- 超出 IPsec SA 最长时间限制
- 管理员重置
- 管理员重启
- 管理员关闭
- 会话断开连接
- 会话错误已终止
- 对等体终止

建议的操作：无需执行任何操作。

713052

错误消息：`%ASA-7-713052: User (user ) authenticated.`

说明：远程访问用户已通过身份验证。

建议的操作：无需执行任何操作。

713056

错误消息：`%ASA-3-713056: Tunnel rejected: SA (SA_name ) not found for group (group_name )!`

说明：找不到 IPsec SA。

建议的操作：如果这是远程访问隧道，请检查组和用户配置，并验证是否为特定用户组配置了隧道组和组策略。对于通过外部身份验证的用户和组，请检查返回的身份验证属性。

713060

错误消息：`%ASA-3-713060: Tunnel Rejected: User (user ) not member of group (group_name ), group-lock check failed.`

说明：用户被配置进入 IPsec 协商中发送的组之外的其他组。

建议的操作：如果使用思科 VPN 客户端和预共享密钥，请确保在客户端上配置的组与 Firepower 威胁防御设备中用户关联的组相同。如果使用数字证书，则该组由证书的 OU 字段决定，或者用户自动默认为远程访问默认组。

713061

错误消息：`%ASA-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:source_address , Dst: dest_address !`

说明：Firepower威胁防御设备无法找到消息中所示的专用网络或主机的安全策略信息。这些网络或主机由发起方发送，与Firepower威胁防御设备中的任何加密ACL均不匹配。这很可能是配置错误。

建议的操作：检查在双方加密ACL中受保护的网络配置，确保发起方的本地网是响应方的远程网，反之亦然。特别注意通配符掩码和主机地址（而不是网络地址）。非思科实施可能具有标记为代理地址或红色网络的专用地址。

713062

错误消息：`%ASA-3-713062: IKE Peer address same as our interface address IP_address`

说明：配置为 IKE 对等体的 IP 地址与在一个 Firepower 威胁防御 IP 接口上配置的 IP 地址相同。

建议的操作：检查 L2L 和 IP 接口配置。

713063

错误消息： `%ASA-3-713063: IKE Peer address not configured for destination IP_address`

说明： 未为 L2L 隧道配置 IKE 对等体地址。

建议的操作： 检查 L2L 配置。

713065

错误消息： `%ASA-3-713065: IKE Remote Peer did not negotiate the following: proposal attribute`

说明： 发生了内部软件错误。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

713066

错误消息： `%ASA-7-713066: IKE Remote Peer configured for SA: SA_name`

说明： 已配置对等体的加密策略设置。

建议的操作： 无需执行任何操作。

713068

错误消息： `%ASA-5-713068: Received non-routine Notify message: notify_type (notify_value)`

说明： 导致此事件的通知消息未通过通知处理代码显式处理。

建议的操作： 检查具体原因以确定要采取的操作。许多通知消息都会指示 IKE 对等体之间的配置不匹配。

713072

错误消息： `%ASA-3-713072: Password for user (user ) too long, truncating to number characters`

说明： 用户密码过长。

建议的操作： 更正身份验证服务器上的密码长度。

713073

错误消息： `%ASA-5-713073: Responder forcing change of Phase 1 /Phase 2 rekeying duration from larger_value to smaller_value seconds`

说明： 密钥更新持续时间始终设置为 IKE 对等体建议的较低值。发起方的值较低。

建议的操作： 无需执行任何操作。

713074

错误消息： `%ASA-5-713074: Responder forcing change of IPsec rekeying duration from larger_value to smaller_value Kbs`

说明： 密钥更新持续时间始终设置为 IKE 对等体建议的较低值。发起方的值较低。

建议的操作： 无需执行任何操作。

713075

错误消息： `%ASA-5-713075: Overriding Initiator's IPsec rekeying duration from larger_value to smaller_value seconds`

说明： 密钥更新持续时间始终设置为 IKE 对等体建议的较低值。响应方的值较低。

建议的操作： 无需执行任何操作。

713076

错误消息： `%ASA-5-713076: Overriding Initiator's IPsec rekeying duration from larger_value to smaller_value Kbs`

说明： 密钥更新持续时间始终设置为 IKE 对等体建议的较低值。响应方的值较低。

建议的操作： 无需执行任何操作。

713078

错误消息： `%ASA-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available_size , used value`

说明： 处理 modecfg 属性时发生了内部软件错误。

建议的操作： 禁用任何不必要的隧道组属性，或缩短任何过长的文本消息。如果问题仍然存在，请联系思科 TAC。

713081

错误消息： `%ASA-3-713081: Unsupported certificate encoding type encoding_type`

说明： 有一个已加载证书无法读取，而且可能是不受支持的编码方案。

建议的操作： 检查数字证书和信任点配置。

713082

错误消息： `%ASA-3-713082: Failed to retrieve identity certificate`

说明： 找不到此隧道的身份证书。

建议的操作：检查数字证书和信任点配置。

713083

错误消息：`%ASA-3-713083: Invalid certificate handle`

说明：找不到此隧道的身份证书。

建议的操作：检查数字证书和信任点配置。

713084

错误消息：`%ASA-3-713084: Received invalid phase 1 port value (`*port*` ) in ID payload`

说明：IKE 第 1 阶段 ID 负载中收到的端口值不正确。可接受的值为 0 或 500 （ISAKMP 也称为 IKE）。

建议的操作：确保对等体符合 IKE 标准，以免网络问题导致数据包损坏。

713085

错误消息：`%ASA-3-713085: Received invalid phase 1 protocol (`*protocol*` ) in ID payload`

说明：IKE 第 1 阶段 ID 负载中收到的协议值不正确。可接受的值为 0 或 17 (UDP)。

建议的操作：确保对等体符合 IKE 标准，以免网络问题导致数据包损坏。

713086

错误消息：`%ASA-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (Auth method (auth numerical value))`

说明：系统已收到证书负载，但我们的内部证书句柄表示我们没有身份证书。系统未通过正常的注册方法获取证书句柄。出现这种情况的一种可能原因是，未通过 RSA 或 DSS 签名进行身份验证，但任何一方配置错误也都会导致 IKE SA 协商失败。

建议的操作：检查 Firepower 威胁防御设备及其对等体上的信任点和 ISAKMP 配置设置。

713088

错误消息：`%ASA-3-713088: Set Cert filehandle failure: no IPsec SA in group `*group_name*

说明：系统无法根据数字证书信息找到隧道组。

建议的操作：验证隧道组是否设置正确，可处理对等体的证书信息。

713092

错误消息：`%ASA-5-713092: Failure during phase 1 rekeying attempt due to collision`

说明：发生了内部软件错误。这通常是良性事件。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713094

错误消息：`%ASA-7-713094: Cert validation failure: handle invalid for Main /Aggressive Mode Initiator /Responder !`

说明：发生了内部软件错误。

建议的操作：您可能需要重新注册信任点。如果问题仍然存在，请联系思科 TAC。

713098

错误消息：`%ASA-3-713098: Aborting: No identity cert specified in IPsec SA (SA_name )!`

说明：系统尝试建立基于证书的 IKE 会话，但加密策略中未指定身份证书。

建议的操作：指定您希望向对等体传输的身份证书或信任点。

713099

错误消息：`%ASA-7-713099: Tunnel Rejected: Received NONCE length number is out of range!`

说明：发生了内部软件错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713102

错误消息：`%ASA-3-713102: Phase 1 ID Data length number too long - reject tunnel!`

说明：IKE 收到的 ID 负载包含的标识数据字段达到 2K 字节或更大。

建议的操作：无需执行任何操作。

713103

错误消息：`%ASA-7-713103: Invalid (NULL) secret key detected while computing hash`

说明：发生了内部软件错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713104

错误消息：`%ASA-7-713104: Attempt to get Phase 1 ID data failed while hash computation`

说明：发生了内部软件错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713105

错误消息：`%ASA-3-713105: Zero length data in ID payload received during phase 1 or 2 processing`

说明：对等体发送的 ID 负载不包括任何 ID 数据，这是无效的。

建议的操作：检查对等体的配置。

713107

错误消息：`%ASA-3-713107: IP_Address request attempt failed!`

说明：发生了内部软件错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713109

错误消息：`%ASA-3-713109: Unable to process the received peer certificate`

说明：Firepower 威胁防御设备无法处理从远程对等体接收的证书，可能是由于证书数据格式不正确（例如，公钥大小超过 4096 位），或 Firepower 威胁防御设备无法存储证书中的数据。

建议的操作：尝试使用远程对等体上的其他证书重新建立连接。

ID 介于 713112 到 714011 之间的消息

本部分包括 ID 介于 713112 到 714011 之间的消息。

713112

错误消息：`%ASA-3-713112: Failed to process CONNECTED notify (SPI` *`SPI_value`* `)!`

说明：Firepower 威胁防御设备 无法成功处理包含“已连接”通知类型的通知负载。如果无法使用 SPI 找到 IKE 第 2 阶段结构，或是接收的 ISAKMP 报头中未设置提交位，就可能出现这种错误。后一种情况可能表示 IKE 对等体不合规。

建议的操作：如果问题仍然存在，请检查对等体的配置和/或禁用提交位处理。

713113

错误消息：`%ASA-7-713113: Deleting IKE SA with associated IPsec connection entries.IKE peer:` *`IP_address`* `, SA address:` *`internal_SA_address`* `, tunnel count:` *`count`*

说明：正在使用非零隧道计数删除 IKE SA，这意味着 IKE SA 隧道计数与关联连接条目失去同步，或是这些条目的关联连接 cookie 字段与连接条目指向的 IKE SA 的 cookie 字段失去同步。如果发生这种情况，系统将不会释放 IKE SA 及其关联的数据结构，以便指向它的条目不存在过时指针。

建议的操作：无需执行任何操作。内置错误恢复功能。

713114

错误消息：`%ASA-7-713114: Connection entry (conn entry internal address) points to IKE SA (SA_internal_address ) for peer IP_address , but cookies don't match`

说明：发生了内部软件错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713115

错误消息：`%ASA-5-713115: Client rejected NAT enabled IPsec request, falling back to standard IPsec`

说明：客户端拒绝 Firepower 威胁防御设备尝试使用 IPsec over UDP。使用 IPsec over UDP，系统可允许多个客户端通过 NAT 设备建立通往 Firepower 威胁防御设备的并行隧道。由于客户端不支持此功能或配置为不使用此功能，客户端可能已拒绝该请求。

建议的操作：验证前端和对等体上的配置。

713117

错误消息：`%ASA-7-713117: Received Invalid SPI notify (SPI SPI_Value )!`

说明：在远程对等体上，由 SPI 值标识的 IPsec SA 未处于活动状态，这可能表示远程对等体已重新启动或重置。

建议的操作：当 DPD 意识到对等体未建立适当的 SA 时，该问题可自行解决。如果未启用 DPD，您可能需要手动重建受影响的隧道。

713118

错误消息：`%ASA-3-713118: Detected invalid Diffie-Helmann group_descriptor group_number , in IKE area`

说明：**group_descriptor** 字段包含不受支持的值。目前仅支持租 1、2、5 和 7。对于 centry，系统可能将 **group_descriptor** 字段设置为 0，表示完美前向保密已禁用。

建议的操作：检查对等体的 Diffie Hellman 配置。

713119

错误消息： `%ASA-5-713119: Group group IP ip  PHASE 1 COMPLETED`

说明：IKE 第 1 阶段成功完成。

建议的操作：无需执行任何操作。

713120

错误消息： `%ASA-5-713120: PHASE 2 COMPLETED (msgid=msg_id )`

说明：IKE 第 2 阶段成功完成。

建议的操作：无需执行任何操作。

713121

错误消息：`%ASA-7-713121: Keep-alive type for this connection: keepalive_type`

说明：此消息指示用于此隧道的保持连接机制类型。

建议的操作：无需执行任何操作。

713122

错误消息：`%ASA-3-713122: Keep-alives configured keepalive_type but peer IP_address support keep-alives (type = keepalive_type )`

说明：此设备的保持连接机制设置为打开或关闭，但 IKE 对等体可能会/不会支持保持连接机制。

建议的操作：如果此配置是有意为之，则无需执行任何操作。否则，请在两台设备上更改保持连接配置。

713123

错误消息：`%ASA-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: keepalive_type )`

说明：远程 IKE 对等体未能在预期时间窗口内响应保持连接请求，因此与 IKE 对等体的连接已终止。消息中包含采用的保持连接机制。

建议的操作：无需执行任何操作。

713124

错误消息：`%ASA-3-713124: Received DPD sequence number rcv_sequence_# in DPD Action, description expected seq #`

说明：远程IKE对等体发送的DPD序列号与预期序列号不匹配。数据包被丢弃。这可能表示网络中出现了丢包问题。

建议的操作：无需执行任何操作。

713127

错误消息： `%ASA-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list`

说明： 对等体希望执行 XAUTH，但 Firepower 威胁防御设备未选择 XAUTH IKE 方案。

建议的操作： 检查 IKE 方案列表中 IKE xauth 方案的优先级。

713128

错误消息： `%ASA-6-713128: Connection attempt to VCPIP redirected to VCA peer IP_address via load balancing`

说明： 系统尝试连接 VCPIP，但通过负载均衡被重定向至负载较小的对等体。

建议的操作： 无需执行任何操作。

713129

错误消息： `%ASA-3-713129: Received unexpected Transaction Exchange payload type: payload_id`

说明： 系统在执行 XAUTH 或 Mode Cfg 期间收到意外负载，这可能表示两个对等体不同步、XAUTH 或 Mode Cfg 版本不匹配，或远程对等体未遵循适当的 RFC。

建议的操作： 验证对等体之间的配置。

713130

错误消息： `%ASA-5-713130: Received unsupported transaction mode attribute: attribute id`

说明： 设备收到了当前不支持的有效事务模式属性（XAUTH 或 Mode Cfg）请求。这通常是良性状况。

建议的操作： 无需执行任何操作。

713131

错误消息： `%ASA-5-713131: Received unknown transaction mode attribute: attribute_id`

说明： Firepower 威胁防御设备 已收到对事务模式属性（XAUTH 或 Mode Cfg）的请求，但该属性超出已知属性范围。属性可能有效，但仅在更高版本的配置模式中受支持，也可能是对等体发送了非法值或专有值。这应该不会导致连接问题，但可能会影响对等体的功能。

建议的操作： 无需执行任何操作。

713132

错误消息： `%ASA-3-713132: Cannot obtain an IP_address for remote peer`

说明： 无法从提供 IP 地址的内部实用程序中请求远程访问客户端的 IP 地址。

建议的操作：检查 IP 地址分配方法的配置。

713133

错误消息： `%ASA-3-713133: Mismatch: Overriding phase 2 DH Group(DH group` *`DH group_id`* `) with phase 1 group(DH group` *`DH group_number`*

说明：已配置的第 2 阶段 PFS 组不同于为第 1 阶段协商的 DH 组。

建议的操作：无需执行任何操作。

713134

错误消息：`%ASA-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection`

说明：已配置的局域网互联方案不同于局域网互联连接中接受的方案。系统将根据不同的发起方使用不同的方案。

建议的操作：无需执行任何操作。

713135

错误消息：`%ASA-5-713135: message received, redirecting tunnel to` *`IP_address`* `.`

说明：远程 Firepower 威胁防御设备负载均衡导致隧道重定向。收到了 REDIRECT_CONNECTION 通知数据包。

建议的操作：无需执行任何操作。

713136

错误消息：`%ASA-5-713136: IKE session establishment timed out [`*`IKE_state_name`*`], aborting!`

说明：获取器检测到 Firepower 威胁防御设备处于非活动状态。获取器将尝试删除非活动 Firepower 威胁防御设备。

建议的操作：无需执行任何操作。

713137

错误消息：`%ASA-5-713137: Reaper overriding refCnt [ref_count] and tunnelCnt [tunnel_count] -- deleting SA!`

说明：发生了内部软件错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713138

错误消息： `%ASA-3-713138: Group group_name not found and BASE GROUP default preshared key not configured`

说明： 组数据库中不存在与对等体 IP 地址同名的组。在主模式下，Firepower 威胁防御设备将回退并尝试使用其中一个默认组中配置的默认预共享密钥。未配置默认预共享密钥。

建议的操作： 验证预共享密钥的配置。

713139

错误消息： `%ASA-5-713139: group_name not found, using BASE GROUP default preshared key`

说明： 组数据库中不存在与对等体 IP 地址同名的隧道组。在主模式下，Firepower 威胁防御设备将回退并使用默认组中配置的默认预共享密钥。

建议的操作： 无需执行任何操作。

713140

错误消息： `%ASA-3-713140: Split Tunneling Policy requires network list but none configured`

说明： 拆分隧道策略设置为拆分隧道或允许本地 LAN 访问。必须定义拆分隧道 ACL 来表示 VPN 客户端所需的信息。

建议的操作： 检查 ACL 的配置。

713141

错误消息： `%ASA-3-713141: Client-reported firewall does not match configured firewall: action tunnel.Received -- Vendor: vendor(id) , Product product(id) , Caps: capability_value .Expected -- Vendor: vendor(id) , Product: product(id) , Caps: capability_value`

说明： 客户端上安装的 Firepower 威胁防御设备与已配置的所需 Firepower 威胁防御设备不匹配。此消息列出实际值和预期值，以及是终止还是允许隧道。

建议的操作： 您可能需要在客户端上安装其他个人 Firepower 威胁防御设备或更改 Firepower 威胁防御设备上的配置。

713142

错误消息： `%ASA-3-713142: Client did not report firewall in use, but there is a configured firewall: action tunnel.Expected -- Vendor: vendor(id) , Product product(id) , Caps: capability_value`

说明： 客户端未使用 ModeCfg 来报告正在使用的 Firepower 威胁防御设备，但是必需该设备。该事件列出预期值，以及是终止还是允许隧道。请注意，产品字符串后面的数字是所有允许的产品的位掩码。

建议的操作：您可能需要在客户端上安装其他个人 Firepower 威胁防御设备或更改 Firepower 威胁防御设备上的配置。

713143

错误消息：`%ASA-7-713143: Processing firewall record.Vendor: vendor(id) , Product: product(id) , Caps: capability_value , Version Number: version_number , Version String: version_text`

说明：系统将显示有关客户端上安装的 Firepower 威胁防御设备的调试信息。

建议的操作：无需执行任何操作。

713144

错误消息：`%ASA-5-713144: Ignoring received malformed firewall record; reason - error_reason TLV type attribute_value correction`

说明：从客户端收到了错误的 Firepower 威胁防御设备信息。

建议的操作：检查客户端和 Firepower 威胁防御设备上的个人配置。

713145

错误消息：`%ASA-6-713145: Detected Hardware Client in network extension mode, adding static route for address: IP_address , mask: netmask`

说明：已协商与处于网络扩展模式的硬件客户端之间的隧道，并且正在为硬件客户端背后的专用网络添加静态路由。通过此配置，Firepower 威胁防御设备使头端的所有专用路由器可以获知远程网络。

建议的操作：无需执行任何操作。

713146

错误消息：`%ASA-3-713146: Could not add route for Hardware Client in network extension mode, address: IP_address , mask: netmask`

说明：发生了内部软件错误。已协商与处于网络扩展模式的硬件客户端之间的隧道，但是尝试为硬件客户端背后的专用网络添加静态路由的操作失败。路由表可能已满，或者可能发生了寻址错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713147

错误消息：`%ASA-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address , mask: netmask`

说明：系统正在移除通向处于网络扩展模式的硬件客户端的隧道，并且正在删除硬件客户端背后的专用网络的静态路由。

建议的操作：无需执行任何操作。

713148

错误消息：`%ASA-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address , mask: netmask`

说明：在移除通向处于网络扩展模式的硬件客户端的隧道时，无法删除通向硬件客户端背后的专用网络的路由。这可能表示编址或软件有问题。

建议的操作：检查路由表以确保该路由不存在于其中。如果路由表包含该路由，则可能必须手动将其移除，但仅当已完全移除通向硬件客户端的隧道时才能执行此操作。

713149

错误消息：`%ASA-3-713149: Hardware client security attribute attribute_name was enabled but not requested.`

说明：头端 Firepower 威胁防御设备已启用指定的硬件客户端安全属性，但是 VPN 3002 硬件客户端未请求该属性。

建议的操作：检查硬件客户端上的配置。

713152

错误消息：`%ASA-3-713152: Unable to obtain any rules from filter ACL_tag to send to client for CPP, terminating connection.`

说明：客户端需要使用 CPP 来调配其 Firepower 威胁防御设备，但是头端设备无法获取要发送到客户端的任何 ACL。这可能是配置错误导致的。

建议的操作：检查客户端的组策略中为 CPP 指定的 ACL。

713154

错误消息：`%ASA-4-713154: DNS lookup for peer_description Server [server_name] failed!`

说明：当未解析对于指定服务器的 DNS 查询时，系统会显示此消息。

建议的操作：检查 Firepower 威胁防御设备上的 DNS 服务器配置。此外，请检查 DNS 服务器，以确保其正常运行并具有主机名到 IP 地址的映射。

713155

错误消息：`%ASA-5-713155: DNS lookup for Primary VPN Server [server_name] successfully resolved after a previous failure.Resetting any Backup Server init.`

说明：主服务器先前的 DNS 查询故障可能已导致 Firepower 威胁防御设备将备份对等体初始化。此消息表示主服务器上后来的DNS查询最终成功，并且正在重置任何备份服务器初始化。此后启动的隧道将以主服务器为目标。

建议的操作：无需执行任何操作。

713156

错误消息：`%ASA-5-713156: Initializing Backup Server [server_name or IP_address]`

说明：客户端由于故障正在切换到备份服务器，或者主服务器的 DNS 查询失败导致了 Firepower 威胁防御设备将备份服务器初始化。此后启动的隧道将以指定的备份服务器为目标。

建议的操作：无需执行任何操作。

713157

错误消息：`%ASA-4-713157: Timed out on initial contact to server [server_name or IP_address ] Tunnel could not be established.`

说明：客户端已尝试通过发出 IKE MSG1 来启动隧道，但未从另一端的 Firepower 威胁防御设备收到响应。如果备份服务器可用，则客户端将尝试连接到其中一个备份服务器。

建议的操作：验证与头端 Firepower 威胁防御设备的连接。

713158

错误消息：`%ASA-5-713158: Client rejected NAT enabled IPsec Over UDP request, falling back to IPsec Over TCP`

说明：客户端配置为使用 IPsec over TCP。客户端已拒绝 Firepower 威胁防御设备对于使用 IPsec over UDP 的尝试。

建议的操作：如果期望使用 TCP，则无需执行任何操作。否则，请检查客户端配置。

713159

错误消息：`%ASA-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access`

说明：由于某个原因（例如服务器已重启，发生了网络问题，或者出现 SSL 不匹配），与 Firepower 威胁防御服务器的 TCP 连接已中断。

建议的操作：如果在建立初始连接后丢失服务器连接，则必须检查服务器和网络连接。如果初始连接立即丢失，这可能表示发生了 SSL 身份验证问题。

713160

错误消息：`%ASA-7-713160: Remote user (session Id - id) has been granted access by the Firewall Server`

说明：已对 Firepower 威胁防御服务器的远程用户进行常规身份验证。

建议的操作：无需执行任何操作。

713161

错误消息： `%ASA-3-713161: Remote user (session Id - id) network access has been restricted by the Firewall Server`

说明： Firepower 威胁防御服务器已向 Firepower 威胁防御设备发送一条消息，指示必须限制此用户。发生此情况有多个原因，包括 Firepower 威胁防御软件升级或权限更改。完成操作后，Firepower 威胁防御服务器随即会使用户重新切换回完全访问模式。

建议的操作： 除非用户永远不重新切换回完全访问状态，否则无需执行任何操作。如果用户需要切换，请访问 Firepower 威胁防御服务器，获取有关正在执行的操作以及在远程设备上运行的 Firepower 威胁防御软件状态的更多信息。

713162

错误消息： `%ASA-3-713162: Remote user (session Id - id) has been rejected by the Firewall Server`

说明： Firepower 威胁防御服务器已拒绝此用户。

建议的操作： 查看有关 Firepower 威胁防御服务器的策略信息以确保用户配置正确。

713163

错误消息： `%ASA-3-713163: Remote user (session Id - id) has been terminated by the Firewall Server`

说明： Firepower 威胁防御服务器已终止此用户会话，如果完整性代理在客户端设备上停止运行，或者远程用户以任何方式修改了安全策略，就可能会出现这种情况。

建议的操作： 验证客户端设备上的 Firepower 威胁防御软件是否仍在运行，以及策略是否正确。

713164

错误消息： `%ASA-7-713164: The Firewall Server has requested a list of active user sessions`

说明： 如果 Firepower 威胁防御服务器检测到其具有过时数据，或者丢失了会话数据（由于重启），则将请求会话信息。

建议的操作： 无需执行任何操作。

713165

错误消息： `%ASA-3-713165: Client IKE Auth mode differs from the group's configured Auth mode`

说明： 客户端在其隧道组指向配置为使用数字证书的策略时使用预共享密钥进行了协商。

建议的操作： 检查客户端配置。

713166

错误消息： `%ASA-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password`

说明： 硬件客户端未能通过扩展身份验证。这很可能是由于用户名和密码存在问题，或者身份验证服务器发生问题。

建议的操作： 验证每一端上已配置的用户名和密码值是否匹配。此外，请验证头端的身份验证服务器是否正常运行。

713167

错误消息： `%ASA-3-713167: Remote peer has failed user authentication - check configured username and password`

说明： 远程用户未能扩展身份验证。这很可能是由于用户名或密码存在问题，或者身份验证服务器发生问题。

建议的操作： 验证每一端上已配置的用户名和密码值是否匹配。此外，请验证用于对远程用户进行身份验证的身份验证服务器是否正常运行。

713168

错误消息： `%ASA-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!`

说明： 已启用对重新生成密钥的重新身份验证，但是隧道身份验证需要人工干预。

建议的操作： 如果需要人工干预，则无需执行任何操作。否则，请检查交互式身份验证配置。

713169

错误消息： `%ASA-7-713169: IKE Received delete for rekeyed SA IKE peer: IP_address , SA address: internal_SA_address , tunnelCnt: tunnel_count`

说明： IKE 已从远程对等体收到一条删除消息，表明在重新生成密钥完成后将删除其旧 IKE SA。

建议的操作： 无需执行任何操作。

713170

错误消息： `%ASA-7-713170: Group group IP ip  IKE Received delete for rekeyed centry IKE peer: IP_address , centry address: internal_address , msgid: id`

说明： IKE 已从远程对等体收到一条删除消息，表明在第 2 阶段重新生成密钥完成后将删除其旧 centry。

建议的操作： 无需执行任何操作。

713171

错误消息： `%ASA-7-713171: NAT-Traversal sending NAT-Original-Address payload`

说明： 在第 2 阶段建议或选择了 UDP 封装传输。在此情况下，请为 NAT 穿越发送此负载。

建议的操作： 无需执行任何操作。

713172

错误消息： `%ASA-6-713172: Automatic NAT Detection Status: Remote end is |is not behind a NAT device This end is |is not behind a NAT device`

说明： NAT 穿越自动检测到 NAT。

建议的操作： 无需执行任何操作。

713174

错误消息： `%ASA-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!`

说明： 硬件客户端正在尝试使用网络扩展模式进入隧道，但是系统不允许网络扩展模式。

建议的操作： 验证网络扩展模式与 PAT 模式的配置。

713176

错误消息： `%ASA-2-713176: Device_type memory resources are critical, IKE key acquire message on interface interface_number , for Peer IP_address ignored`

说明： Firepower 威胁防御设备正在处理旨在触发通向所指示对等体的 IPsec 隧道的数据。由于内存资源处于临界状态，因此不会再启动任何隧道。系统已忽略并丢弃数据包。

建议的操作： 如果此情况仍然存在，请验证是否高效配置了 Firepower 威胁防御设备。此应用可能需要具有更多内存的 Firepower 威胁防御设备。

713177

错误消息： `%ASA-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host_name Address IP_address , Protocol protocol , Port port`

说明： 已从对等体收到包含 FQDN 的第 2 阶段 ID 负载。

建议的操作： 无需执行任何操作。

713178

错误消息： `%ASA-5-713178: IKE Initiator received a packet from its peer without a Responder cookie`

说明：发生了内部软件错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713179

错误消息：`%ASA-5-713179: IKE AM Initiator received a packet from its peer without a payload_type payload`

说明：发生了内部软件错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713182

错误消息：`%ASA-3-713182: IKE could not recognize the version of the client! IPsec Fragmentation Policy will be ignored for this connection!`

说明：发生了内部软件错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713184

错误消息：`%ASA-6-713184: Client Type: Client_type Client Application Version: Application_version_string`

说明：系统显示客户端操作系统和应用版本。如果这些信息不可用，则系统将指示不适用。

建议的操作：无需执行任何操作。

713185

错误消息：`%ASA-3-713185: Error: Username too long - connection aborted`

说明：客户端返回了长度无效的用户名，并且隧道已断开。

建议的操作：检查用户名，并在必要时进行更改。

713186

错误消息：`%ASA-3-713186: Invalid secondary domain name list received from the authentication server.List Received: list_text Character index (value ) is illegal`

说明：从外部 RADIUS 身份验证服务器收到了无效的辅助域名列表。使用拆分隧道后，此列表将标识客户端应通过隧道解析的域。

建议的操作：更正 RADIUS 服务器上指定的 Secondary-Domain-Name-List 属性（供应商特定属性 29）。必须将列表指定为域名的逗号分隔列表。域名只能包含字母数字字符、连字符、下划线和句点。

713187

错误消息： `%ASA-7-713187: Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy IKE peer address: IP_address , Remote peer address: IP_address`

说明： 正在尝试启用此隧道的 IKE 对等体不是 ISAKMP 配置中配置的绑定到已接收远程子网的对等体。

建议的操作： 验证在头端和对等体上， L2L 设置是否正确。

713189

错误消息： `%ASA-3-713189: Attempted to assign network or broadcast IP_address , removing ( IP_address ) from pool.`

说明： 池中的 IP 地址是此子网的网络地址或广播地址。此地址将标记为不可用。

建议的操作： 此错误通常为良性，但是应检查 IP 地址池配置。

713190

错误消息： `%ASA-7-713190: Got bad refCnt ( ref_count_value ) assigning IP_address ( IP_address )`

说明： 此 SA 的参考计数器无效。

建议的操作： 无需执行任何操作。

713191

错误消息： `%ASA-3-713191: Maximum concurrent IKE negotiations exceeded!`

说明： 为尽量减少 CPU 密集型加密计算，Firepower 威胁防御设备会限制正在进行中的连接协商的数量。在请求新协商且Firepower威胁防御设备已到达其限制后，系统将拒绝此新协商。在现有连接协商完成后，系统将再次允许新连接协商。

建议的操作： 请参阅 **crypto ikev1 limit max-in-negotiation-sa** 命令。增大限制可能会降低性能。

713193

错误消息： `%ASA-3-713193: Received packet with missing payload, Expected payload: payload_id`

说明： Firepower威胁防御设备收到指定交换类型的具有一个或多个缺失负载的已加密或未加密数据包。这通常表示对等体发生了问题。

建议的操作： 验证对等体是否发送的是有效的 IKE 消息。

713194

错误消息： `%ASA-3-713194: Sending IKE |IPsec Delete With Reason message: termination_reason`

说明：收到了包含终止原因代码的删除消息。

建议的操作：无需执行任何操作。

713195

错误消息：`%ASA-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!`

说明：仅发起对等体只有在其启用第一条P2隧道后，才能接受传入连接。此时，来自任一方向的数据都可以启动其他第 2 阶段隧道。

建议的操作：如果期望出现其他行为，则需要修改仅发起配置。

713196

错误消息：`%ASA-5-713196: Remote L2L Peer IP_address initiated a tunnel with same outer and inner addresses.Peer could be Originate Only - Possible misconfiguration!`

说明：远程 L2L 对等体已启动公用-公用隧道。远程 L2L 对等体期望从另一端的对等体获取响应，但是可能由于配置错误，并未收到响应。

建议的操作：检查两端的 L2L 配置。

713197

错误消息：`%ASA-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel_type connection.Enforcing the second default.`

说明：组中配置的置信区间超出有效范围。

建议的操作：检查组中的置信度设置以确保其在有效范围内。

713198

错误消息：`%ASA-3-713198: User Authorization failed: user User authorization failed.Username could not be found in the certificate`

说明：系统显示用于声明无法在证书中找到用户名的原因字符串。

建议的操作：检查组配置和客户端授权。

713199

错误消息：`%ASA-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter ( counter_value )!`

说明：获取器已更正内部软件错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713203

错误消息： `%ASA-3-713203: IKE Receiver: Error reading from socket.`

说明： 读取收到的 IKE 数据包时发生了错误。这通常是内部错误，可能表示软件出现了问题。

建议的操作： 此问题通常为良性，系统将自行更正。如果问题仍然存在，请联系思科 TAC。

713204

错误消息： `%ASA-7-713204: Adding static route for client address: IP_address`

说明： 此消息表示已向路由表添加通向对等体分配的地址或受硬件客户端保护的网络的路由。

建议的操作： 无需执行任何操作。

713205

错误消息： `%ASA-3-713205: Could not add static route for client address: IP_address`

说明： 尝试添加通向客户端分配的地址或受硬件客户端保护的网络的路由失败。这可能表示路由表中的路由重复或网络地址已损坏。重复路由可能是未正确清除路由或者多个客户端共享网络或地址导致的。

建议的操作： 检查 IP 本地池配置，以及当前使用的任何其他 IP 地址分配机制（例如，DHCP 或 RADIUS）。请确保从路由表中清除路由。此外，请检查对等体上的网络和/或地址的配置。

713206

错误消息： `%ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy`

说明： 由于组策略中指定的允许隧道与隧道组配置中的允许隧道不同，因此隧道被丢弃。

建议的操作： 检查隧道组和组策略配置。

713207

错误消息： `%ASA-4-713207: Terminating connection: IKE Initiator and tunnel group specifies L2TP Over IPSec`

说明： 如果网关是发起方且隧道组类型为 L2TP over IPSEC，则在终止连接的同时会为 ikev1 显示此系统日志。

建议的操作： 无需执行任何操作。

713208

错误消息： `%ASA-3-713208: Cannot create dynamic rule for Backup L2L entry rule rule_id`

说明：创建用于触发 IKE 并使 IPsec 数据能够正确处理的 ACL 失败。该失败情况特定于备份 L2L 配置，这可能表示配置错误、容量错误或内部软件错误。

建议的操作：如果 Firepower 威胁防御设备运行的是最大数量的连接和 VPN 隧道，则可能存在内存问题。否则，请检查备份 L2L 和加密映射配置，特别是与加密映射关联的 ACL。

713209

错误消息：`%ASA-3-713209: Cannot delete dynamic rule for Backup L2L entry rule id`

说明：删除用于触发 IKE 并使 IPsec 数据能够正确处理的 ACL 失败。该失败情况特定于备份 L2L 配置。这可能表示内部软件错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713210

错误消息：`%ASA-3-713210: Cannot create dynamic map for Backup L2L entry rule_id`

说明：创建与备份 L2L 配置关联的动态加密映射的运行时实例失败。这可能表示配置错误、容量错误或内部软件错误。

建议的操作：如果 Firepower 威胁防御设备运行的是最大数量的连接和 VPN 隧道，则可能存在内存问题。否则，请检查备份 L2L 和加密映射配置，特别是与加密映射关联的 ACL。

713212

错误消息：`%ASA-3-713212`: Could not add route for L2L peer coming in on a dynamic map. address: *IP_address* , mask: *netmask*

说明：Firepower 威胁防御设备在尝试为对等体的专用地址或网络添加路由时发生故障。在此情况下，对等体是具有未知地址的客户端或 L2L 对等体。这两种情况均使用动态加密映射以允许隧道。这可能表示路由重复，路由表已满或 Firepower 威胁防御设备未能删除先前使用的路由。

检查路由表以确保可以添加其他路由，并且不存在过时路由。如果路由表已满或包含过时路由，请删除路由并重试。如果问题仍然存在，请联系思科 TAC。

713213

错误消息：`%ASA-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address , mask: netmask`

说明：Firepower威胁防御设备正在删除对等体的专用地址或网络的路由。在此情况下，对等体是具有未知地址的客户端或 L2L 对等体。这两种情况均使用动态加密映射以允许隧道。

建议的操作：无需执行任何操作。

713214

错误消息： `%ASA-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address , mask: netmask`

说明： Firepower威胁防御设备删除对等体的专用地址或网络的路由失败。在此情况下，对等体是具有未知地址的客户端或 L2L 对等体。这两种情况均使用动态加密映射以允许隧道。可能已删除路由，或者发生了内部软件错误。

建议的操作： 如果已删除路由，则情况为良性，并且设备将正常运行。如果问题仍然存在或者可能与 VPN 隧道链路上的路由问题有关，请检查 VPN L2L 配置的路由和寻址部分。检查反向路由注入以及与相应加密映射关联的 ACL。如果问题仍然存在，请联系思科 TAC。

713215

错误消息： `%ASA-6-713215: No match against Client Type and Version rules.Client: type version is /is not allowed by default`

说明： 客户端的客户端类型和版本与Firepower威胁防御设备上配置的任何规则都不匹配。系统将显示默认操作。

建议的操作： 确定默认操作和部署要求，并进行适用的更改。

713216

错误消息： `%ASA-5-713216: Rule: action [Client type]: version Client: type version allowed/not allowed`

说明： 客户端的客户端类型和版本已与一个规则相匹配。系统将显示匹配结果和该规则。

建议的操作： 确定部署要求，并进行相应的更改。

713217

错误消息： `%ASA-3-713217: Skipping unrecognized rule: action: action client type: client_type client version: client_version`

说明： 存在格式不正确的客户端类型和版本规则。格式应为“操作客户端类型|客户端版本操作”。“会话管理”下会显示允许或拒绝客户端类型和客户端版本。仅支持每个参数使用一个通配符(*)。

建议的操作： 更正规则。

713218

错误消息： `%ASA-3-713218: Tunnel Rejected: Client Type or Version not allowed.`

根据所配置的规则，系统已拒绝客户端进行访问。

无需执行任何操作。

713219

错误消息： `%ASA-6-713219: Queuing KEY-ACQUIRE messages to be processed when P1 SA is complete.`

说明： 在第 1 阶段完成后，第 2 阶段消息正在入队等待处理。

建议的操作： 无需执行任何操作。

713220

错误消息： `%ASA-6-713220: De-queuing KEY-ACQUIRE messages that were left pending.`

说明： 正在处理已入队的第 2 阶段消息。

建议的操作： 无需执行任何操作。

713221

错误消息： `%ASA-7-713221: Static Crypto Map check, checking map = crypto_map_tag , seq = seq_number...`

说明： Firepower 威胁防御设备正在迭代加密映射，从而查找配置信息。

建议的操作： 无需执行任何操作。

713222

错误消息： `%ASA-7-713222: Group group Username username IP ip  Static Crypto Map check, map = crypto_map_tag , seq = seq_number , ACL does not match proxy IDs src:source_address dst:dest_address`

说明： 在迭代已配置的加密映射时，Firepower 威胁防御设备无法与任何关联的 ACL 匹配。这通常意味着 ACL 配置错误。

建议的操作： 检查与此隧道对等体关联的 ACL，并确保它们从 VPN 隧道的两端指定相应的专用网络。

713223

错误消息： `%ASA-7-713223: Static Crypto Map check, map = crypto_map_tag , seq = seq_number , no ACL configured`

说明： 与此对等体关联的加密映射未链接到 ACL。

建议的操作： 确保存在与此加密映射关联的 ACL，并且该 ACL 包含来自 VPN 隧道两端的相应专用地址或网络。

713224

错误消息： `%ASA-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!`

说明：与此 VPN 隧道关联的加密映射缺少重要信息。

建议的操作：验证加密映射是否正确配置了 VPN 对等体、转换集和关联 ACL。

713225

错误消息：`%ASA-7-713225: [IKEv1], Static Crypto Map check, map map_name , seq = sequence_number is a successful match`

说明：Firepower 威胁防御设备找到了此 VPN 隧道的有效匹配加密映射。

建议的操作：无需执行任何操作。

713226

错误消息：`%ASA-3-713226: Connection failed with peer IP_address , no trust-point defined in tunnel-group tunnel_group`

说明：当设备配置为使用数字证书时，必须在配置中指定信任点。当配置中缺少信任点时，会生成此消息来标记错误。

- **IP_address** - 对等体的 IP 地址
- **tunnel_group** - 配置中缺少其信任点的隧道组

建议的操作：设备的管理员必须在配置中指定信任点。

713227

错误消息：`%ASA-3-713227: Rejecting new IPsec SA negotiation for peer Peer_address.A negotiation was already in progress for local Proxy Local_address /Local_netmask , remote Proxy Remote_address /Remote_netmask`

说明：在建立阶段 SA 时，Firepower 威胁防御设备将拒绝与此代理相匹配的第 2 阶段。

建议的操作：无需执行任何操作。

713228

错误消息：`%ASA-6-713228: Group = group , Username = uname , IP = remote_IP_address Assigned private IP address assigned_private_IP  to remote user`

说明：IKE 从 DHCP 或从地址池获取了客户端的专用 IP 地址。

- *group* - 组的名称
- *uname* - 用户的名称
- *remote_IP_address* - 远程客户端的 IP 地址
- *assigned_private_IP* - 由 DHCP 分配或来自本地地址池的客户端 IP 地址

建议的操作：无需执行任何操作。

713229

错误消息： `%ASA-5-713229: Auto Update - Notification to client client_ip of update string: message_string.`

说明： VPN 远程接入客户端收到通知，指示有已更新的软件可供下载。远程客户端用户负责选择更新客户端访问软件。

- **client_ip** - 远程客户端的 IP 地址
- **message_string** - 发送到远程客户端的消息文本

建议的操作： 无需执行任何操作。

713230

错误消息： `%ASA-3-713230 Internal Error, ike_lock trying to lock bit that is already locked for type type`

说明： 发生内部错误，系统报告 IKE 子系统正在尝试锁定已锁定的内存。这表示用于防止 IKE SA 出现内存违规的信号发生了错误。此消息并不表示出现了任何严重错误。但是，发生了意外事件，并且正在自动执行相应的步骤以进行恢复。

- >*type* - 用于描述发生了锁定问题的信号类型的字符串

建议的操作： 如果问题仍然存在，请联系思科 TAC。

713231

错误消息： `%ASA-3-713231 Internal Error, ike_lock trying to unlock bit that is not locked for type type`

说明： 发生内部错误，报告表明 IKE 子系统正在尝试解锁当前未锁定的内存。这表示用于防止 IKE SA 出现内存违规的信号发生了错误。此消息并不表示出现了任何严重错误。但是，发生了意外事件，并且正在自动执行相应的步骤以进行恢复。

- *type* - 用于描述发生了锁定问题的信号类型的字符串

建议的操作： 如果问题仍然存在，请联系思科 TAC。

713232

错误消息： `%ASA-3-713232 SA lock refCnt = value , bitmask = hexvalue , p1_decrypt_cb = value , qm_decrypt_cb = value , qm_hash_cb = value , qm_spi_ok_cb = value , qm_dh_cb = value , qm_secret_key_cb = value , qm_encrypt_cb = value`

说明： 所有 IKE SA 都已锁定，并已检测到可能的错误。此消息报告用于防止 IKE SA 出现内存违规的信号发生了错误。

- >*value* - 十进制值
- >*hexvalue* - 十六进制值

建议的操作： 如果问题仍然存在，请联系思科 TAC。

713233

错误消息： `%ASA-7-713233: (VPN-unit ) Remote network (remote network ) validated for network extension mode.`

说明： 已验证在第 2 阶段协商期间接收的远程网络。该消息表示在网络扩展模式客户端的第 2 阶段协商期间远程网络检查的结果。这是现有功能的一部分，用于防止用户错误配置硬件客户端网络（例如，在多个客户端上配置重叠网络或同一网络）。

- *remote network* - 来自第 2 阶段代理的子网地址和子网掩码

建议的操作： 无需执行任何操作。

713234

错误消息： `%ASA-7-713234: (VPN-unit) Remote network (remote network ) from network extension mode client mismatches AAA configuration (aaa network).`

说明： 在第 2 阶段协商期间接收的远程网络与此会话从 AAA 服务器返回的 framed-ip-address 和 ramed-subnet-mask 不匹配。

- *remote network* - 来自第 2 阶段代理的子网地址和子网掩码
- *aaa network* - 通过 AAA 配置的子网地址和子网掩码

建议的操作： 请执行以下操作之一：

- 检查此用户和组的地址分配，然后检查硬件客户端上的网络配置，并更正任何不一致情况。
- 禁用此用户和组的地址分配。

713235

错误消息： `%ASA-6-713235: Attempt to send an IKE packet from standby unit.Dropping the packet!`

说明： 通常情况下，绝不应将 IKE 数据包从备用设备发送到远程对等体。如果进行了此类尝试，则表示可能已发生内部逻辑错误。由于保护代码，数据包永远不会离开备用设备。此消息有助于执行调试。

建议的操作： 无需执行任何操作。

713236

错误消息： `%ASA-7-713236: IKE_DECODE tx/rx Message (msgid=msgid) with payloads:payload1 (payload1_len) + payload2 (payload2_len)...total length: tlen`

说明： IKE 已发送或收到各种消息。

以下示例显示 IKE 在收到包含 8 字节散列负载、11 字节通知负载和两个 13 字节供应商特定负载的消息时的输出。

```
%ASA-7-713236: IKE_DECODE RECEIVED Message msgid=0) with payloads: HDR + HASH (8) + NOTIFY
 (11) + VENDOR (13) + VENDOR (13) + NONE (0)
```

建议的操作：无需执行任何操作。

713237

错误消息：`%ASA-5-713237: ACL update (access_list ) received during re-key re-authentication will not be applied to the tunnel.`

说明：在以下情况下会出现远程接入 IPsec 隧道的第 1 阶段密钥更新：

- 隧道配置为在隧道密钥更新后，对用户重新进行身份验证。
- RADIUS 服务器返回访问列表或对本地配置的访问列表的引用，该访问列表与首次建立隧道时返回的访问列表不同。

建议的操作：在这些情况下，Firepower 威胁防御设备会忽略新访问列表并生成此消息。

- >*access_list* - 与静态或动态访问列表关联的名称，如 **show access-list** 命令的输出中所示

IPsec 用户必须重新连接，才能使新用户特定访问列表生效。

713238

错误消息：`%ASA-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client`

说明：网络扩展模式客户端的专用端地址显示为 0.0.0.0。这通常表示未在硬件客户端的专用接口上设置任何 IP 地址。

建议的操作：验证远程客户端的配置。

713239

错误消息：`%ASA-4-713239: IP_Address : Tunnel Rejected: The maximum tunnel count allowed has been reached`

说明：已在达到允许的最大隧道数后尝试创建隧道。

- **IP_Address** - 对等体的 IP 地址

建议的操作：无需执行任何操作。

713240

错误消息：`%ASA-4-713240: Received DH key with bad length: received length=rlength expected length=elength`

说明：从对等体收到长度不正确的 Diffie-Hellman 密钥。

- rlength - 收到的 DH 密钥的长度
- elength - 预期长度（基于 DH 密钥大小）

建议的操作：无需执行任何操作。

713241

错误消息：`%ASA-4-713241: IE Browser Proxy Method setting_number is Invalid`

说明：在 ModeCfg 处理期间发现代理设置无效。P1 协商将会失败。

建议的操作：检查 **msie-proxy method** 命令设置（**group-policy** 命令的子命令），这些设置应符合下列其中一项：[**auto-detect** | **no-modify** | **no-proxy** | **use-server**]。任何其他值或空值都不正确。请尝试重置 **msie-proxy method** 命令设置。如果问题仍然存在，请联系思科 TAC。

713242

错误消息：`%ASA-4-713242: Remote user is authenticated using Hybrid Authentication.Not starting IKE rekey.`

说明：Firepower 威胁防御设备检测到对配置为使用 Hybrid Xauth 的隧道启动 IKE 密钥更新的请求，但是未启动密钥更新。Firepower 威胁防御设备将等待客户端检测并启动 IKE 密钥更新。

建议的操作：无需执行任何操作。

713243

错误消息：`%ASA-4-713243: META-DATA Unable to find the requested certificate`

说明：IKE 对等体已从 cert-req 负载请求证书。但是，找不到由所请求的 DN 颁发的有效身份证书。

建议的操作：执行以下步骤：

1. 检查身份证书。
2. 注册或导入所需证书。
3. 启用证书调试，获取更多详细信息。

713244

错误消息：`%ASA-4-713244: META-DATA Received Legacy Authentication Method(LAM) type type is different from the last type received type.`

说明：收到的 LAM 属性类型与收到的最后一个类型不同。在整个用户身份验证过程中，类型必须一致。无法继续执行用户身份验证进程，并将不会建立 VPN 连接。

- **type** - LAM 类型

建议的操作：如果问题仍然存在，请联系思科 TAC。

713245

错误消息：`%ASA-4-713245: META-DATA Unknown Legacy Authentication Method(LAM) type type received.`

说明：在 CRACK 质询或响应用户身份验证进程中收到了不支持的 LAM 类型。无法继续执行用户身份验证进程，并将不会建立 VPN 连接。

- **type** - LAM 类型

建议的操作：如果问题仍然存在，请联系思科 TAC。

713246

错误消息：`%ASA-4-713246: META-DATA Unknown Legacy Authentication Method(LAM) attribute type type received.`

说明：Firepower 威胁防御设备收到未知 LAM 属性类型，这应该不会导致连接问题，但可能会影响对等体的功能。

- **type** - LAM 属性类型

建议的操作：无需执行任何操作。

713247

错误消息：`%ASA-4-713247: META-DATA Unexpected error: in Next Card Code mode while not doing SDI.`

说明：状态处理期间发生了意外错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

713248

错误消息：`%ASA-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.`

说明：使用 CRACK 身份验证方法协商 IKE SA 后，头端的第 1 阶段 SA 密钥更新计时器在密钥更新成功之前已到期。由于在使用 CRACK 身份验证方法时远程客户端始终是交换的发起方，因此头端将不会发起密钥更新。除非远程对等体在 IKE SA 到期之前成功发起密钥更新，否则在 IKE SA 到期时连接将会关闭。

建议的操作：无需执行任何操作。

713249

错误消息：`%ASA-4-713249: META-DATA Received unsupported authentication results: result`

说明：使用 CRACK 身份验证方法协商 IKE SA 时，IKE 子系统从身份验证子系统收到在 CRACK 身份验证期间不受支持的结果。用户身份验证失败，并且 VPN 连接已断开。

- *result* - 从身份验证子系统返回的结果

建议的操作：如果问题仍然存在，请联系思科 TAC。

713250

错误消息：`%ASA-5-713250: META-DATA Received unknown Internal Address attribute: attribute`

说明：Firepower威胁防御设备收到对无法识别的内部地址属性的请求。属性可能有效，但当前不受支持，或者对等体可能发送的是非法值。这应该不会导致连接问题，但可能会影响对等体的功能。

建议的操作：无需执行任何操作。

713251

错误消息：`%ASA-4-713251: META-DATA Received authentication failure message`

说明：Firepower 威胁防御设备收到一条通知消息，指示在使用 CRACK 身份验证方法协商 IKE SA 时身份验证失败。连接已断开。

建议的操作：无需执行任何操作。

713252

错误消息：`%ASA-5-713252: Group = group , Username = user , IP = ip , Integrity Firewall Server is not available.VPN Tunnel creation rejected for client.`

说明：当组策略配置为要求客户端使用 Zonelab Integrity Server 进行身份验证时，服务器可能需要连接到集中器，具体取决于所配置的失败策略。如果失败策略是拒绝客户端连接，则在客户端进行连接时 Zonelab Integrity Server 未连接到 Firepower 威胁防御设备的情况下，系统将会生成此消息。

- *group* - 远程访问用户连接到的隧道组
- *user* - 远程访问用户
- *ip* - 远程访问用户的 IP 地址

建议的操作：检查集中器和Zonelab Integrity Server上的配置是否匹配。然后，验证集中器和Zonelab Integrity Server之间是否存在通信。

713253

错误消息：`%ASA-5-713253: Group = group , Username = user , IP = ip , Integrity Firewall Server is not available.Entering ALLOW mode.VPN Tunnel created for client.`

说明：当组策略配置为要求客户端使用 Zonelab Integrity Server 进行身份验证时，服务器可能需要连接到集中器，具体取决于所配置的失败策略。如果失败策略是接受客户端连接，并提供不受限制的网络接入，则在客户端进行连接时 Zonelab Integrity Server 未连接到 Firepower 威胁防御设备的情况下，系统将会生成此消息。

- *group* - 远程访问用户连接到的隧道组
- *user* - 远程访问用户
- *ip* - 远程访问用户的 IP 地址

建议的操作：检查 Firepower 威胁防御设备和 Zonelab Integrity Server 上的配置是否匹配，并验证 Firepower 威胁防御设备和 Zonelab Integrity Server 之间是否存在通信。

713254

错误消息： `%ASA-3-713254: Group = groupname , Username = username , IP = peerip , Invalid IPsec/UDP port = portnum , valid range is minport - maxport , except port 4500, which is reserved for IPsec/NAT-T`

说明： 您无法使用 UDP 端口 4500 进行 IPsec/UDP 连接，因为它应保留用于 IPsec 或 NAT-T 连接。CLI 不允许对本地组使用此配置。仅对于外部定义的组才会出现此消息。

- *groupname* - 用户组的名称
- *username* - 用户的名称
- *peerip* - 客户端的 IP 地址
- *portnum* - 外部服务器上的 IPsec/UDP 端口号
- *minport* - 用户可配置端口的最小有效端口号，即 4001
- *maxport* - 用户可配置端口的最大有效端口号，即 49151

建议的操作： 将外部服务器上的 IPsec 或 UDP 端口号更改为另一个端口号。有效端口号为 4001 到 49151。

713255

错误消息： `%ASA-4-713255: IP = peer-IP , Received ISAKMP Aggressive Mode message 1 with unknown tunnel group name group-name`

说明： 在 ISAKMP 积极模式消息 1 中指定了未知隧道组。

- *peer-ip* - 对等体的地址
- *group-name* - 对等体指定的组名称

建议的操作： 检查隧道组和客户端配置以确保其有效。

713256

错误消息： `%ASA-6-713256: IP = peer-IP , Sending spoofed ISAKMP Aggressive Mode message 2 due to receipt of unknown tunnel group.Aborting connection.`

说明： 当对等体指定无效隧道组时，Firepower 威胁防御设备仍将发送消息 2 以防止对等体收集隧道组信息。

- *peer-ip* - 对等体的地址

建议的操作： 无需执行任何操作。

713257

错误消息： `%ASA-5-713257: Phase var1 failure: Mismatched attribute types for class var2 : Rcv'd: var3 Cfg'd: var4`

说明：Firepower 威胁防御设备已用作局域网间连接中的响应方。它表示 Firepower 威胁防御加密配置与发起方的配置不匹配。该消息指定在哪个阶段出现了不匹配，以及发起方和响应方均具有的属性有哪些不同。

- *var1* - 出现了不匹配的阶段
- *var2* - 不匹配的属性所属的类
- *var3* - 从发起方收到的属性
- *var4* - 配置的属性

建议的操作：检查两个局域网间设备上的加密配置是否存在不一致情况。具体而言，如果系统报告 UDP 隧道 (NAT-T) 和其他设备之间存在不一致，请检查加密映射。如果一个配置在匹配的加密映射上禁用了 NAT-T，而另一个配置未禁用，则此情况将导致失败。

713258

错误消息：`%ASA-3-713258: IP = var1 , Attempting to establish a phase2 tunnel on var2 interface but phase1 tunnel is on var3 interface.Tearing down old phase1 tunnel due to a potential routing change.`

说明：Firepower 威胁防御设备尝试在接口上建立第 2 阶段隧道，并且在其他接口上已存在第 1 阶段隧道。现有第 1 阶段隧道已断开，从而允许在新接口上建立新隧道。

- *var1* - 对等体的 IP 地址
- *var2* - Firepower 威胁防御设备尝试建立第 2 阶段隧道时所在的接口
- *var3* - 第 1 阶段隧道所在的接口

建议的操作：检查对等体的路由是否已更改。如果路由尚未更改，则可能存在配置错误。

713259

错误消息：`%ASA-5-713259: Group = groupname , Username = username , IP = peerIP , Session is being torn down.Reason: reason`

说明：系统显示 ISAKMP 会话的终止原因，在通过会话管理断开会话时会出现此消息。

- *groupname* - 正在终止的会话的隧道组
- *username* - 正在终止的会话的用户名
- *peerIP* - 正在终止的会话的对等体地址
- *reason* - 正在终止的会话的 RADIUS 终止原因，包括：

- 端口已被占用（同时登录）

- 空闲超时

- 超过最长时间限制

- 管理员重置

建议的操作：无需执行任何操作。

713260

错误消息： `%ASA-3-713260: Output interface %d to peer was not found`

说明： 当尝试创建第 1 阶段 SA 时，系统无法找到与接口 ID 对应的接口数据库。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

713261

错误消息： `%ASA-3-713261: IPV6 address on output interface %d was not found`

说明： 当尝试创建第 1 阶段 SA 时，本地接口上未指定任何 IPv6 地址。

建议的操作： 有关如何在所需接口上设置 IPv6 地址的信息，请参阅《CLI 配置指南》中的“配置 IPv6 寻址”一节。

713262

错误消息： `%ASA-3-713262: Rejecting new IPSec SA negotiation for peer Peer_address.A negotiation was already in progress for local Proxy Local_address /Local_prefix_len , remote Proxy Remote_address /Remote_prefix_len`

说明： 在建立阶段 SA 时，Firepower 威胁防御设备将拒绝与此代理匹配的新的第 2 阶段 SA。

- *Peer_address* - 尝试使用与现有协商匹配的代理启动第 2 阶段的新地址
- *Local_address* - 当前正在协商第 2 阶段的先前本地对等体的地址
- *Local_prefix_len* - 根据 CIDR 表示法而定的子网前缀长度
- *Remote_address* - 代理的地址
- *Remote_prefix_len* - 根据 CIDR 表示法而定的子网前缀长度

建议的操作： 无需执行任何操作。

713263

错误消息： `%ASA-7-713263: Received local IP Proxy Subnet data in ID Payload: Address IP_address , Mask /prefix_len , Protocol protocol , Port port`

说明： Firepower 威胁防御设备正在为对等体的专用地址或网络添加路由。在此情况下，对等体是具有未知地址的客户端或 L2L 对等体。这两种情况均使用动态加密映射以允许隧道。

- *IP_address* - 对等体的目的网络的基本 IP 地址
- *prefix_len* - 根据 CIDR 表示法而定的子网前缀长度
- *protocol* - 代理协议
- *port* - 代理端口

建议的操作： 无需执行任何操作。

713264

错误消息： `%ASA-7-713264: Received local IP Proxy Subnet data in ID Payload: Address IP_address , Mask/prefix_len , Protocol protocol , Port port {“Received remote IP Proxy Subnet data in ID Payload: Address %a , Mask/%d , Protocol %u , Port %u ”}`

说明： Firepower威胁防御设备正在为对等体的专用地址或网络添加路由。在此情况下，对等体是具有未知地址的客户端或 L2L 对等体。这两种情况均使用动态加密映射以允许隧道。

- *IP_address* - 对等体的目的网络的基本 IP 地址
- *prefix_len* - 根据 CIDR 表示法而定的子网前缀长度
- *protocol* - 代理协议
- *port* - 代理端口

建议的操作： 无需执行任何操作。

713265

错误消息： `%ASA-6-713265: Adding static route for L2L peer coming in on a dynamic map. address: IP_address , mask: /prefix_len`

说明： Firepower威胁防御设备正在为对等体的专用地址或网络添加路由。在此情况下，对等体是具有未知地址的客户端或 L2L 对等体。这两种情况均使用动态加密映射以允许隧道。

- *IP_address* - 对等体的目的网络的基本 IP 地址
- *prefix_len* - 根据 CIDR 表示法而定的子网前缀长度

建议的操作： 无需执行任何操作。

713266

错误消息： `%ASA-3-713266: Could not add route for L2L peer coming in on a dynamic map. address: IP_address , mask: /prefix_len`

说明： Firepower 威胁防御设备在尝试为对等体的专用地址或网络添加路由时发生故障。在此情况下，对等体是具有未知地址的客户端或 L2L 对等体。这两种情况均使用动态加密映射以允许隧道。这可能表示路由重复，IPv6 路由表已满或 Firepower 威胁防御设备未删除先前使用的路由。

- *IP_address* - 对等体的目的网络的基本 IP 地址
- *prefix_len* - 根据 CIDR 表示法而定的子网前缀长度

建议的操作： 检查IPv6路由表，确保可以添加其他路由，并且不存在过时路由。如果路由表已满或包含过时路由，请删除路由并重试。如果问题仍然存在，请联系思科 TAC。

713267

错误消息： `%ASA-6-713267: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address , mask: /prefix_len`

说明：Firepower 威胁防御设备在尝试为对等体的专用地址或网络添加路由时发生故障。在此情况下，对等体是具有未知地址的客户端或 L2L 对等体。这两种情况均使用动态加密映射以允许隧道。

- *IP_address* - 对等体的目的网络的基本 IP 地址
- *prefix_len* - 根据 CIDR 表示法而定的子网前缀长度

建议的操作：无需执行任何操作。

713268

错误消息：`%ASA-3-713268: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address , mask: /prefix_len`

说明：Firepower威胁防御设备删除对等体的专用地址或网络的路由失败。在此情况下，对等体是具有未知地址的客户端或 L2L 对等体。这两种情况均使用动态加密映射以允许隧道。可能已删除该路由，或者已发生内部软件错误。

- *IP_address* - 对等体的目的网络的基本 IP 地址
- *prefix_len* - 根据 CIDR 表示法而定的子网前缀长度

建议的操作：如果已删除路由，则情况为良性，并且设备将正常运行。如果问题仍然存在或者可能与 VPN 隧道链路上的路由问题有关，请检查 VPN L2L 配置的路由和寻址部分。此外，请检查反向路由注入以及与相应加密映射关联的 ACL。如果问题仍然存在，请联系思科 TAC。

713269

错误消息：`%ASA-6-713269: Detected Hardware Client in network extension mode, adding static route for address: IP_address , mask: /prefix_len`

说明：已协商与处于网络扩展模式的硬件客户端之间的隧道，并且正在为硬件客户端背后的专用网络添加静态路由。通过此配置，Firepower 威胁防御设备使头端的所有专用路由器可以获知远程网络。

- *IP_address* - 对等体的目的网络的基本 IP 地址
- *prefix_len* - 根据 CIDR 表示法而定的子网前缀长度

建议的操作：无需执行任何操作。

713270

错误消息：`%ASA-3-713270: Could not add route for Hardware Client in network extension mode, address: IP_address , mask: /prefix_len`

说明：发生了内部软件错误。已协商与处于网络扩展模式的硬件客户端之间的隧道，但是尝试为硬件客户端背后的专用网络添加静态路由的操作失败。IPv6 路由表可能已满，或者可能发生了寻址错误。

- *IP_address* - 对等体的目的网络的基本 IP 地址
- *prefix_len* - 根据 CIDR 表示法而定的子网前缀长度

建议的操作：如果问题仍然存在，请联系思科 TAC。

713271

错误消息： `%ASA-6-713271: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address , mask:/prefix_len`

说明： 系统正在移除通向处于网络扩展模式的硬件客户端的隧道，并且正在删除硬件客户端背后的专用网络的静态路由。

- *IP_address* - 对等体的目的网络的基本 IP 地址
- *prefix_len* - 根据 CIDR 表示法而定的子网前缀长度

建议的操作： 无需执行任何操作。

713272

错误消息： `%ASA-3-713272: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address , mask: /prefix_len`

说明： 在移除通向处于网络扩展模式的硬件客户端的隧道时，无法删除通向硬件客户端背后的专用网络的路由。这可能表示编址或软件有问题。

- *IP_address* - 对等体的目的网络的基本 IP 地址
- *prefix_len* - 根据 CIDR 表示法而定的子网前缀长度

建议的操作： 检查 IPv6 路由表，确保该路由不存在于其中。如果路由表包含该路由，则可能必须手动将其移除，但仅当已完全移除通向硬件客户端的隧道时才能执行此操作。

713273

错误消息： `%ASA-7-713273: Deleting static route for client address: IP_Address IP_Address address of client whose route is being removed`

说明： 已从路由表中删除通向对等体分配的地址或受硬件客户端保护的网络的路由。

建议的操作： 无需执行任何操作。

713274

错误消息： `%ASA-3-713274: Could not delete static route for client address: IP_Address IP_Address address of client whose route is being removed`

说明： 在删除通向 IPsec 客户端的隧道时，无法删除其在路由表中的对应条目。此情况可能表示网络或软件发生了问题。

建议的操作： 检查路由表，确保该路由不存在于其中。如果该路由已存在于路由表中，则可能需要手动将其删除，但仅在成功关闭隧道后才能执行此操作。

713275

错误消息： `%ASA-3-713275: IKEv1 Unsupported certificate keytype %s found at trustpoint %s`

说明：当证书密钥类型不是 ECDSA 类型时，对于 ikev1 会显示此系统日志。请确保在网关上安装密钥类型有效的证书。

建议的操作：无需执行任何操作。

713276

错误消息：`%ASA-3-713276: Dropping new negotiation - IKEv1 in-negotiation context limit of %u reached`

说明：当到达最大协商限制时，在多情景下对于 ikev1 会显示此系统日志消息。

建议的操作：无需执行任何操作。

713900

错误消息：`%ASA-1-713900: Descriptive_event_string.`

说明：发生了严重事件或故障。例如，Firepower 威胁防御设备正在尝试生成第 2 阶段删除，但 SPI 不与任何现有第 2 阶段 SA 匹配。

建议的操作：在所述示例中，两个对等体均在同一时间删除第 2 阶段 SA。在此情况下，该错误为良性并可忽略。如果错误仍然存在并造成负面影响（例如导致隧道断开连接或设备重启），则可能表示软件有故障。在此情况下，请完全按照控制台上或系统日志中的显示正确复制该错误消息，然后联系思科 TAC 以获得进一步帮助。

713901

错误消息：`%ASA-2-713901: Descriptive_event_string .`

说明：已发生错误，这可能是头端或远程访问客户端上的配置错误导致的。事件字符串提供关于所发生的错误的详细信息。

建议的操作：可能需要对消息进行排除故障，以确定导致错误的原因。检查两个对等体上的 ISAKMP 和加密映射配置。

713902

错误消息：`%ASA-3-713902: Descriptive_event_string.`

说明：已发生错误，这可能是头端或远程访问客户端上的配置错误导致的。

建议的操作：可能需要对配置进行故障排除，以确定错误的原因。检查两个对等体上的 ISAKMP 和加密映射配置。

713903

错误消息： `%ASA-4-713903: Group = group policy , Username = user name , IP = remote IP , ERROR: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP.`

说明： 安装重定向 URL 后，IPsec/IKEv1 VPN 连接发生错误，并系统从 ISE 收到了 ACL，但在 Firepower 威胁防御设备上不存在重定向 ACL。

- *group policy* - 允许用户获取访问权限的组策略
- *user name* - 远程访问的请求者的用户名
- *remote IP* - 发送该连接请求的远程 IP 地址
- *redirect URL* - 用于 HTTP 流量重定向的 URL
- *assigned IP* - 分配给用户的 IP 地址

建议的操作： 无需执行任何操作。

713904

错误消息： `%ASA-5-713904: Descriptive_event_string .`

说明： 系统将显示通知状态信息，用于跟踪已发生的事件。

建议的操作： 无需执行任何操作。

713905

错误消息： `%ASA-6-713905: Descriptive_event_string .`

说明： 系统将显示信息状态详情，用于跟踪已发生的事件。

建议的操作： 无需执行任何操作。

713906

错误消息： `%ASA-7-713906: Descriptive_event_string .`

说明： 系统将显示调试状态信息，用于跟踪已发生的事件。

建议的操作： 无需执行任何操作。

714001

错误消息： `%ASA-7-714001: description_of_event_or_packet`

说明： 此消息提供对 IKE 协议事件或数据包的说明。

建议的操作： 无需执行任何操作。

714002

错误消息： `%ASA-7-714002: IKE Initiator starting QM: msg id = message_number`

说明： Firepower 威胁防御设备已作为第 2 阶段发起方发送了快速模式交换的第一个数据包。

建议的操作： 无需执行任何操作。

714003

错误消息： `%ASA-7-714003: IKE Responder starting QM: msg id = message_number`

说明： Firepower 威胁防御设备已作为第 2 阶段响应方收到了快速模式交换的第一个数据包。

建议的操作： 无需执行任何操作。

714004

错误消息： `%ASA-7-714004: IKE Initiator sending 1st QM pkt: msg id = message_number`

说明： 已解码第一个快速模式数据包的协议。

建议的操作： 无需执行任何操作。

714005

错误消息： `%ASA-7-714005: IKE Responder sending 2nd QM pkt: msg id = message_number`

说明： 已解码第二个快速模式数据包的协议。

建议的操作： 无需执行任何操作。

714006

错误消息： `%ASA-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message_number`

说明： 已解码第三个快速模式数据包的协议。

建议的操作： 无需执行任何操作。

714007

错误消息： `%ASA-7-714007: IKE Initiator sending Initial Contact`

说明： Firepower 威胁防御设备正在构建并发送初始联系负载。

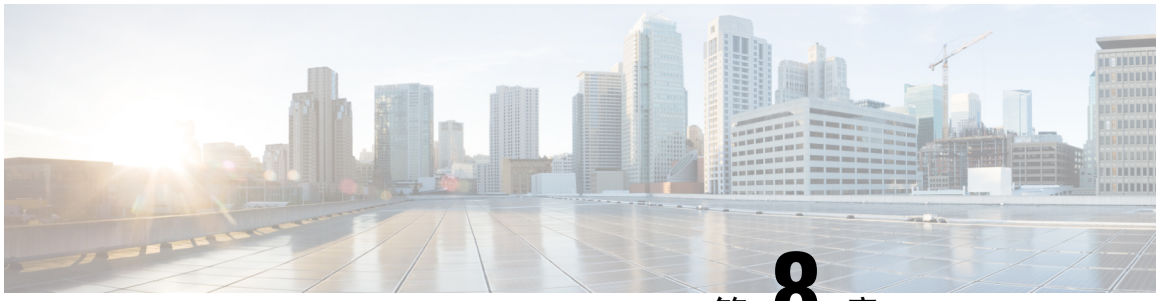
建议的操作： 无需执行任何操作。

714011

错误消息： `%ASA-7-714011: Description of received ID values`

说明：Firepower 威胁防御设备收到了在协商期间显示的 ID 信息。

建议的操作：无需执行任何操作。



第 8 章

系统日志消息 715001-721019

本章包含以下各节：

ID 介于 715001 到 715080 之间的消息

本部分包括 ID 介于 715001 到 715080 之间的消息。

715001

错误消息：`%ASA-7-715001: Descriptive statement`

说明：系统将显示对 Firepower 威胁防御设备遇到的事件或问题的说明。

建议的操作：操作取决于该说明的具体内容。

715004

错误消息：`%ASA-7-715004: subroutine name () Q Send failure: RetCode (return_code)`

说明：尝试将消息放入队列时发生了内部错误。

建议的操作：这通常是良性情况。如果问题仍然存在，请联系思科 TAC。

715005

错误消息：`%ASA-7-715005: subroutine name() Bad message code: Code (message_code)`

说明：内部子例程收到了错误的消息代码。

建议的操作：这通常是良性情况。如果问题仍然存在，请联系思科 TAC。

715006

错误消息： `%ASA-7-715006: IKE got SPI from key engine: SPI = SPI_value`

说明： IKE 子系统从 IPsec 收到了 SPI 值。

建议的操作： 无需执行任何操作。

715007

错误消息： `%ASA-7-715007: IKE got a KEY_ADD msg for SA: SPI = SPI_value`

说明： IKE 已完成隧道协商，并已成功加载了适当的加密和散列密钥供 IPsec 使用。

建议的操作： 无需执行任何操作。

715008

错误消息： `%ASA-7-715008: Could not delete SA SA_address, refCnt = number , caller = calling_subroutine_address`

说明： 调用子例程无法删除 IPsec SA。这可能表示存在参考计数问题。

建议的操作： 如果过时 SA 的数量由于此事件而增长，请联系思科 TAC。

715009

错误消息： `%ASA-7-715009: IKE Deleting SA: Remote Proxy IP_address , Local Proxy IP_address`

说明： 正在删除具有所列代理地址的 SA。

建议的操作： 无需执行任何操作。

715013

错误消息： `%ASA-7-715013: Tunnel negotiation in progress for destination IP_address , discarding data`

说明： IKE 正在为此数据建立隧道。在完全建立隧道之前，系统将会丢弃要受此隧道保护的所有数据包。

建议的操作： 无需执行任何操作。

715018

错误消息： `%ASA-7-715018: IP Range type id was loaded: Direction %s, From: %a, Through: %a`

说明： 在更新 IPSEC SA 详细信息时会生成此系统日志消息。

建议的操作： 无需执行任何操作。

715019

错误消息： %ASA-7-715019: Group *group* Username *username* IP *ip* IKEGetUserAttributes: Attribute name = *name*

说明： 系统显示由 Firepower 威胁防御设备处理的 **modecfg** 属性名称和值对。

建议的操作： 无需执行任何操作。

715020

错误消息： %ASA-7-715020: construct_cfg_set: Attribute name = *name*

说明： 系统显示由 Firepower 威胁防御设备传输的 **modecfg** 属性名称和值对。

建议的操作： 无需执行任何操作。

715021

错误消息： %ASA-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

说明： 系统会延迟快速模式处理，直至所有第 1 阶段处理都已完成（针对事务模式）。

建议的操作： 无需执行任何操作。

715022

错误消息： %ASA-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

说明： 第 1 阶段处理已完成，并且正在恢复快速模式。

建议的操作： 无需执行任何操作。

715027

错误消息： %ASA-7-715027: IPsec SA Proposal # *chosen_proposal* , Transform # *chosen_transform* acceptable Matches global IPsec SA entry # *crypto_map_index*

说明： 已从响应方收到的负载中选择所指示的 IPsec SA 提议和转换。在尝试调试 IKE 协商问题时，此数据可能有用。

建议的操作： 无需执行任何操作。

715028

错误消息： %ASA-7-715028: IKE SA Proposal # 1, Transform # **chosen_transform** acceptable Matches global IKE entry # *crypto_map_index*

说明： 已从响应方收到的负载中选择所指示的 IKE SA 转换。在尝试调试 IKE 协商问题时，此数据可能有用。

建议的操作：无需执行任何操作。

715031

错误消息：`%ASA-7-715031: Obtained IP addr (%s) prior to initiating Mode Cfg (XAuth %s)`

说明：在 IP 实用程序子系统分配 IP 地址后，将会生成此系统日志。

建议的操作：无需执行任何操作。

715032

错误消息：`%ASA-7-715032: Sending subnet mask (%s) to remote client`

说明：在 IP 实用程序子系统分配 IP 地址后，将会生成此系统日志。

建议的操作：无需执行任何操作。

715033

错误消息：`%ASA-7-715033: Processing CONNECTED notify (MsgId` *`message_number`*`)`

说明：Firepower 威胁防御设备正在处理包含通知类型为“已连接”(16384) 的通知负载的消息。“已连接”通知类型用于完成提交位处理，并且应包含在从响应方发送到发起方的第四个整体快速模式数据包中。

建议的操作：无需执行任何操作。

715034

错误消息：`%ASA-7-715034: action IOS keep alive payload: proposal=`*`time 1 /time 2`*` sec.`

说明：正在执行对于发送或接收保持连接负载消息的处理。

建议的操作：无需执行任何操作。

715035

错误消息：`%ASA-7-715035: Starting IOS keepalive monitor:` *`seconds`* `sec.`

说明：保持连接计时器将对保持连接消息进行监控，时长可变且单位为秒。

建议的操作：无需执行任何操作。

715036

错误消息：`%ASA-7-715036: Sending keep-alive of type` *`notify_type`* `(seq number` *`number`*`)`

说明：正在执行对于发送保持连接通知消息的处理。

建议的操作：无需执行任何操作。

715037

错误消息： %ASA-7-715037: Unknown IOS Vendor ID version: *major.minor.variance*

说明： 此版本的思科 IOS 的功能未知。

建议的操作： 可能与 IKE 保持连接等功能存在互通问题。如果问题仍然存在，请联系思科 TAC。

715038

错误消息： %ASA-7-715038: *action Spoofing_information* Vendor ID payload (version: *major.minor.variance* , capabilities: *value*)

说明： 已执行对于思科 IOS 供应商 ID 负载的处理。正在执行的操作可能是 Altiga 在监听思科 IOS。

建议的操作： 无需执行任何操作。

715039

错误消息： %ASA-7-715039: Unexpected cleanup of tunnel table entry during SA delete.

说明： 释放 SA 后，系统永远不会删除 IKE 隧道表中的条目。这表示状态机存在缺陷。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

715040

错误消息： %ASA-7-715040: Deleting active auth handle during SA deletion: handle = *internal_authentication_handle*

错误消息： 身份验证句柄在 SA 删除期间仍然处于活动状态。这是在错误状况下清除恢复过程的环节。

建议的操作： 无需执行任何操作。

715041

错误消息： %ASA-7-715041: Received keep-alive of type *keepalive_type* , not the negotiated type

说明： 意外收到了消息中指示的类型的保持连接连接。

建议的操作： 检查两个对等体上的保持连接配置。

715042

错误消息： %ASA-7-715042: IKE received response of type *failure_type* to a request from the *IP_address* utility

说明： 无法从提供 IP 地址的内部实用程序中请求远程访问客户端的 IP 地址。消息字符串中的变量文本更具体地指示出错原因。

建议的操作：检查 IP 地址分配配置并相应地调整。

715044

错误消息：`%ASA-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability`

说明：收到了来自供应商的思科 IOS 保持连接负载，但未设置保持连接功能。系统将忽略该负载。

建议的操作：无需执行任何操作。

715045

错误消息：`%ASA-7-715045: ERROR: malformed Keepalive payload`

说明：收到了格式错误的保持连接负载。系统将忽略该负载。

建议的操作：无需执行任何操作。

715046

错误消息：`%ASA-7-715046: Group = groupname , Username = username , IP = IP_address , constructing payload_description payload`

说明：来自特定组和用户的远程客户端的 IP 地址显示有关正在构建的 IKE 负载的详细信息。

建议的操作：无需执行任何操作。

715047

错误消息：`%ASA-7-715047: processing payload_description payload`

说明：系统显示已收到和正在处理的 IKE 负载的详细信息。

建议的操作：无需执行任何操作。

715048

错误消息：`%ASA-7-715048: Send VID_type VID`

说明：系统显示正在发送的供应商 ID 负载的类型。

建议的操作：无需执行任何操作。

715049

错误消息：`%ASA-7-715049: Received VID_type VID`

说明：系统显示已收到的供应商 ID 负载的类型。

建议的操作：无需执行任何操作。

715050

错误消息： `%ASA-7-715050: Claims to be IOS but failed authentication`

说明： 收到的供应商 ID 类似于思科 IOS VID，但与 **hmac_sha** 不匹配。

建议的操作： 检查两个对等体上的供应商ID配置。如果此问题影响互通性且问题仍然存在，请联系思科 TAC。

715051

错误消息： `%ASA-7-715051: Received unexpected TLV type` *`TLV_type`* `while processing FWTYPE ModeCfg Reply`

说明： 处理 FWTYPE ModeCfg 应答时，在 Firepower 威胁防御记录中收到了未知 TLV。系统将丢弃该 TLV。在数据包损坏或连接客户端支持更高版本的 Firepower 威胁防御协议时，可能会发生此情况。

建议的操作： 检查思科 VPN 客户端上安装的个人防火墙和 Firepower 威胁防御设备上的个人防火墙配置。这也可能表示 VPN 客户端和 Firepower 威胁防御设备之间的版本不匹配。

715052

错误消息： `%ASA-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centries`

说明： 正在删除旧 P1 SA，但没有任何要转换到的新 SA，因为它也已标记为删除。这通常表示两个 IKE 对等体不同步，并且可能使用的是不同的密钥更新时间。该问题应会自行更正，但在重新建立全新 P1 SA 之前，可能会有少量的数据丢失。

建议的操作： 无需执行任何操作。

715053

错误消息： `%ASA-7-715053: MODE_CFG: Received request for` *`attribute_info`*`!`

说明： Firepower 威胁防御设备收到了请求指定属性的模式配置消息。

建议的操作： 无需执行任何操作。

715054

错误消息： `%ASA-7-715054: MODE_CFG: Received` *`attribute_name`* `reply:` *`value`*

说明： Firepower 威胁防御从远程对等体收到了模式配置应答消息。

建议的操作： 无需执行任何操作。

715055

错误消息： `%ASA-7-715055: Send attribute_name`

说明： Firepower 威胁防御设备已向远程对等体发送模式配置消息。

建议的操作： 无需执行任何操作。

715056

错误消息： `%ASA-7-715056: Client is configured for TCP_transparency`

说明： 由于为 IPsec over TCP 配置了远程端（客户端），因此头端 Firepower 威胁防御设备不得与客户端协商 IPsec over UDP 或 IPsec over NAT-T。

建议的操作： 如果隧道未启动，则 NAT 透明度配置可能需要调整其中一个对等体。

715057

错误消息： `%ASA-7-715057: Auto-detected a NAT device with NAT-Traversal.Ignoring IPsec-over-UDP configuration.`

说明： 由于检测到 NAT 穿越，因此将不交换 IPsec-over-UDP 模式配置信息。

建议的操作： 无需执行任何操作。

715058

错误消息： `%ASA-7-715058: NAT-Discovery payloads missing.Aborting NAT-Traversal.`

说明： 在交换 NAT 穿越 VID 后，远程端未提供 NAT 穿越所需的 NAT 发现负载。必须至少收到两个 NAT 发现负载。

建议的操作： 这可能表示 NAT-T 实施不合格。如果违规对等体是思科产品，并且问题仍然存在，请联系思科 TAC。如果违规对等体不是思科产品，则联系制造商支持团队。

715059

错误消息： `%ASA-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal`

说明： 需要使用这些模式而不是 SA 中定义的普通传输和隧道模式，才能成功协商 NAT 穿越。

建议的操作： 无需执行任何操作。

715060

错误消息： `%ASA-7-715060: Dropped received IKE fragment.Reason: reason`

说明： 系统将显示丢弃片段的原因。

建议的操作：建议的操作取决于丢弃原因，但可能表示有 NAT 设备干预或对等体不合格问题。

715061

错误消息：`%ASA-7-715061: Rcv'd fragment from a new fragmentation set.Deleting any old fragments.`

说明：发生了重新发送分段为其他 MTU 的相同数据包或整体重新发送另一个数据包的情况。

建议的操作：无需执行任何操作。

715062

错误消息：`%ASA-7-715062: Error assembling fragments! Fragment numbers are non-continuous.`

说明：片段编号存在间隔。

建议的操作：这可能表示存在网络问题。如果该情况仍然存在并导致隧道断开或阻止特定对等体与 Firepower 威胁防御设备进行协商，请联系思科 TAC。

715063

错误消息：`%ASA-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!`

说明：收到的分段数据包组装成功。

建议的操作：无需执行任何操作。

715064

错误消息：`%ASA-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: true /false Aggressive Mode: true /false`

说明：对等体支持基于消息中提供的信息的 IKE 分段。

建议的操作：无需执行任何操作。

715065

错误消息：`%ASA-7-715065: IKE state_machine subtype FSM error history (struct data_structure_address ) state , event : state /event pairs`

错误消息：发生第 1 阶段错误，并且 **state**/**event** 历史记录对将按反向时间顺序显示。

建议的操作：大多数这些错误都是良性的。如果问题仍然存在，请联系思科 TAC。

715066

错误消息：`%ASA-7-715066: Can't load an IPsec SA! The corresponding IKE SA contains an invalid logical ID.`

错误消息：IKE SA 中的逻辑 ID 为空。第二阶段协商将中断。

建议的操作：发生了内部错误。如果问题仍然存在，请联系思科 TAC。

715067

错误消息：`%ASA-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa`

错误消息：正在建立的局域网间 SA 已存在，即，具有同一远程网络但源自不同对等体的 SA。系统将删除此新 SA，因为这不是合法配置。

建议的操作：检查所有关联对等体上的局域网间配置。具体而言，多个对等体不应共享专用网络。

715068

错误消息：`%ASA-7-715068: QM IsRekeyed: duplicate sa found by address, deleting old sa`

错误消息：正在建立的远程访问 SA 已存在，即，具有同一远程网络但源自不同对等体的 SA。系统将删除旧 SA，因为对等体可能已更改其 IP 地址。

建议的操作：这可能是良性情况，尤其是如果突然终止了客户端隧道。如果问题仍然存在，请联系思科 TAC。

715069

错误消息：`%ASA-7-715069: Invalid ESP SPI size of SPI_size`

错误消息：Firepower 威胁防御设备收到了 ESP SPI 大小无效的 IPsec SA 提议。系统将跳过此提议。

建议的操作：通常，这是良性情况，但可能表示对等体不合格。如果问题仍然存在，请联系思科 TAC。

715070

错误消息：`%ASA-7-715070: Invalid IPComp SPI size of SPI_size`

错误消息：Firepower 威胁防御设备收到了 IPComp SPI 大小无效的 IPsec SA 提议。系统将跳过此提议。

建议的操作：通常，这是良性情况，但可能表示对等体不合格。如果问题仍然存在，请联系思科 TAC。

715071

错误消息：`%ASA-7-715071: AH proposal not supported`

错误消息：不支持该 IPsec AH 提议。系统将跳过此提议。

建议的操作：无需执行任何操作。

715072

错误消息： `%ASA-7-715072: Received proposal with unknown protocol ID protocol_ID`

错误消息： Firepower 威胁防御设备收到了具有未知协议 ID 的 IPsec SA 提议。系统将跳过此提议。

建议的操作： 通常，这是良性情况，但可能表示对等体不合格。如果问题仍然存在，请联系思科 TAC。

715074

错误消息： `%ASA-7-715074: Could not retrieve authentication attributes for peer IP_address`

错误消息： Firepower 威胁防御设备无法获取远程用户的授权信息。

建议的操作： 确保已正确配置身份验证和授权设置。如果问题仍然存在，请联系思科 TAC。

715075

错误消息： `%ASA-7-715075: Group = group_name , IP = IP_addressReceived keep-alive of type message_type (seq number number)`

错误消息： 此消息与 DPD R-U-THERE 消息 715036（记录 DPD 发送消息）配对。

- **group_name** - 对等体的 VPN 组名称
- **IP_address** - VPN 对等体的 IP 地址
- **message_type** - 消息类型（DPD R-U-THERE 或 DPD R-U-THERE-ACK）
- **number** - DPD 序列号

可能会出现以下两种情况：

- 收到对等体发送 DPD R-U-THERE 消息
- 收到对等体应答 DPD R-U-THERE-ACK 消息

请注意下列说明：

- 收到 DPD R-U-THERE 消息，并且其序列号与传出 DPD 应答消息匹配。

如果 Firepower 威胁防御设备在未先从对等体收到 DPD R-U-THERE 消息的情况下发送 DPD R-U-THERE-ACK 消息，则可能会出现安全漏洞。

- 收到的 DPD R-U-THERE-ACK 消息的序列号与先前发送的 DPD 消息匹配。

如果 Firepower 威胁防御设备在向对等体发送 DPD R-U-THERE 消息后未在合理的时间内收到 DPD R-U-THERE-ACK 消息，则隧道很可能已关闭。

建议的操作： 无需执行任何操作。

715076

错误消息： `%ASA-7-715076: Computing hash for ISAKMP`

错误消息： IKE 已计算各种散列值。

此对象将按如下所示进行前置：

Group = >*groupname* , Username = >*username* , IP = >*ip_address* ...

建议的操作：无需执行任何操作。

715077

错误消息：`%ASA-7-715077: Pitcher: msg string , spi spi`

错误消息：已将各种消息发送到 IKE。

Msg_string 可以是下列其中一项：

- Received a key acquire message
- Received SPI for nonexistent SA
- Received key delete msg
- Received KEY_UPDATE
- Received KEY_REKEY_IB
- Received KEY_REKEY_OB
- Received KEY_SA_ACTIVE
- Could not find IKE SA to activate IPSEC (OB)
- Could not find IKE SA to rekey IPSEC (OB)
- KEY_SA_ACTIVE no centry found
- KEY_ADD centry not found
- KEY_UPDATE centry not found

此对象将按如下所示进行前置：

Group = >*groupname* , Username = >*username* , IP = >*ip_address* ,...

建议的操作：无需执行任何操作。

715078

错误消息：`%ASA-7-715078: Received %s LAM attribute`

说明：在解析质询/响应负载期间将生成此系统日志。

建议的操作：无需执行任何操作。

715079

错误消息：`%ASA-7-715079: INTERNAL_ADDRESS: Received request for %s`

说明：在处理内部地址负载期间将生成此系统日志。

建议的操作：无需执行任何操作。

715080

错误消息： `%ASA-7-715080: VPN: Starting P2 rekey timer: 28800 seconds.`

错误消息：IKE 密钥更新计时器已启动。

建议的操作：无需执行任何操作。

ID 介于 716001 到 716603 之间的消息

本部分包括 ID 介于 716001 到 716603 之间的消息。

716001

错误消息： `%ASA-6-716001: Group group User user IP ip WebVPN session started.`

说明：已对该组中位于指定 IP 地址的用户启动 WebVPN 会话。当用户通过 WebVPN 登录页面登录时，WebVPN 会话将启动。

建议的操作：无需执行任何操作。

716002

错误消息： `%ASA-6-716002: Group GroupPolicy User username IP ip WebVPN session terminated: User requested.`

说明：用户请求已终止 WebVPN 会话。可能的原因包括：

- 丢失运营商连接
- 服务丢失
- 空闲超时
- 超过最长时间限制
- 管理员重置
- 管理员重启
- 管理员关闭
- 端口错误
- NAS 错误
- NAS 请求
- NAS 重启
- 不需要端口
- 端口已被占用。此原因表示已超过允许的同时（同一用户）登录数。要解决此问题，请增大同时登录数，或者要求用户仅使用给定的用户名和密码登录一次。
- 端口已暂挂
- 服务不可用
- 执行回调

- 用户错误
- 已请求主机
- 带宽管理错误
- ACL 解析错误
- 组策略中指定了 VPN 同时登录数限制
- 未知

建议的操作：除非终止原因表明存在问题，否则无需执行任何操作。

716003

错误消息：`%ASA-6-716003: Group group User user IP ip WebVPN access "GRANTED: url "`

说明：已授予该组中位于指定 IP 地址的 WebVPN 用户对此 URL 的访问权限。可以使用 WebVPN 特定 ACL 来控制对各种位置的用户访问权限。

建议的操作：无需执行任何操作。

716004

错误消息：`%ASA-6-716004: Group group User user WebVPN access DENIED to specified location: url`

说明：已拒绝该组中的 WebVPN 用户对此 URL 的访问。可以使用 WebVPN 特定 ACL 来控制对各种位置的 WebVPN 用户访问权限。在此情况下，特定条目将拒绝用户访问此 URL。

建议的操作：无需执行任何操作。

716005

错误消息：`%ASA-6-716005: Group group User user WebVPN ACL Parse Error: reason`

说明：指定组中的 WebVPN 用户的 ACL 未能正确解析。

建议的操作：更正 WebVPN ACL。

716006

错误消息：`%ASA-6-716006: Group name User user WebVPN session terminated.Idle timeout.`

说明：由于 VPN 隧道协议未设置为 WebVPN，因此没有为指定组中的用户创建 WebVPN 会话。

建议的操作：无需执行任何操作。

716007

错误消息：`%ASA-4-716007: Group group User user WebVPN Unable to create session.`

说明：由于资源问题，系统没有为指定组中的用户创建 WebVPN 会话。例如，用户可能已达到最大登录限制。

建议的操作：无需执行任何操作。

716008

错误消息：`%ASA-7-716008: WebVPN ACL: action`

说明：WebVPN ACL 已开始执行操作（例如，开始解析）。

建议的操作：无需执行任何操作。

716009

错误消息：`%ASA-6-716009: Group group User user WebVPN session not allowed.WebVPN ACL parse error.`

说明：由于未解析关联的 ACL，因此系统不允许此组中的指定用户执行 WebVPN 会话。在更正此错误之前，系统将不允许用户通过 WebVPN 登录。

建议的操作：更正 WebVPN ACL。

716010

错误消息：`%ASA-7-716010: Group group User user Browse network.`

说明：指定组中的 WebVPN 用户已浏览网络。

建议的操作：无需执行任何操作。

716011

错误消息：`%ASA-7-716011: Group group User user Browse domain domain.`

说明：该组中的 WebVPN 指定用户已浏览指定的域。

建议的操作：无需执行任何操作。

716012

错误消息：`%ASA-7-716012: Group group User user Browse directory directory.`

说明：指定的 WebVPN 用户已浏览指定的目录。

建议的操作：无需执行任何操作。

716013

错误消息：`%ASA-7-716013: Group group User user Close file filename.`

说明：指定的 WebVPN 用户已关闭指定的文件。

建议的操作：无需执行任何操作。

716014

错误消息：`%ASA-7-716014: Group group User user View file filename.`

说明：指定的 WebVPN 用户已查看指定的文件。

建议的操作：无需执行任何操作。

716015

错误消息：`%ASA-7-716015: Group group User user Remove file filename.`

说明：指定的组中的 WebVPN 用户已删除指定的文件。

建议的操作：无需执行任何操作。

716016

错误消息：`%ASA-7-716016: Group group User user Rename file old_filename to new_filename.`

说明：指定的 WebVPN 用户已重命名指定的文件。

建议的操作：无需执行任何操作。

716017

错误消息：`%ASA-7-716017: Group group User user Modify file filename.`

说明：指定的 WebVPN 用户已修改指定的文件。

建议的操作：无需执行任何操作。

716018

错误消息：`%ASA-7-716018: Group group User userCreate file filename.`

说明：指定的 WebVPN 用户已创建指定的文件。

建议的操作：无需执行任何操作。

716019

错误消息：`%ASA-7-716019: Group group User userCreate directory directory.`

说明：指定的 WebVPN 用户已创建指定的目录。

建议的操作：无需执行任何操作。

716020

错误消息： `%ASA-7-716020: Group group User userRemove directory directory.`

说明： 指定的 WebVPN 用户已删除指定的目录。

建议的操作： 无需执行任何操作。

716021

错误消息： `%ASA-7-716021: File access DENIED, filename.`

说明： 已拒绝指定的 WebVPN 用户访问指定的文件。

建议的操作： 无需执行任何操作。

716022

错误消息： `%ASA-4-716022: Unable to connect to proxy server reason.`

说明： 由于所指出的原因，WebVPN HTTP/HTTPS 重定向失败。

建议的操作： 检查 HTTP/HTTPS 代理配置。

716023

错误消息： `%ASA-4-716023: Group name User user Session could not be established: session limit of maximum_sessions reached.`

说明： 由于当前会话数超过了最大会话数，因此无法建立用户会话。

建议的操作： 如果可能，请增加配置限制以创建负载均衡的集群。

716024

错误消息： `%ASA-7-716024: Group name User user Unable to browse the network.Error: description`

说明： 用户无法使用 CIFS 协议浏览 Windows 网络，如说明中所示。例如，“Unable to contact necessary server”表示远程服务器不可用或无法访问。这可能是一种瞬时情况，也可能需要进一步执行故障排除。

建议的操作： 检查 WebVPN 设备和 CIFS 协议所访问的服务器之间的连接。此外，请检查 Firepower 威胁防御设备上的 NetBIOS 名称服务器配置。

716025

错误消息： `%ASA-7-716025: Group name User user Unable to browse domain domain.Error: description`

说明： 用户无法使用 CIFS 协议浏览远程域。

建议的操作：检查 WebVPN 设备和 CIFS 协议所访问的服务器之间的连接。检查 Firepower 威胁防御设备上的 NetBIOS 名称服务器配置。

716026

错误消息：`%ASA-7-716026: Group name User user Unable to browse directory directory.Error: description`

说明：用户无法使用 CIFS 协议浏览远程目录。

建议的操作：检查 WebVPN 设备和 CIFS 协议所访问的服务器之间的连接。此外，请检查 Firepower 威胁防御设备上的 NetBIOS 名称服务器配置。

716027

错误消息：`%ASA-7-716027: Group name User user Unable to view file filename.Error: description`

说明：用户无法使用 CIFS 协议查看远程文件。

建议的操作：检查 WebVPN 设备和 CIFS 协议所访问的服务器之间的连接。此外，请检查 Firepower 威胁防御设备上的 NetBIOS 名称服务器配置。

716028

错误消息：`%ASA-7-716028: Group name User user Unable to remove file filename.Error: description`

说明：用户无法使用 CIFS 协议删除远程文件，这可能是缺少文件权限导致的。

建议的操作：检查 WebVPN 设备和 CIFS 协议所访问的服务器之间的连接。此外，请检查 Firepower 威胁防御设备上的 NetBIOS 名称服务器配置和文件权限。

716029

错误消息：`%ASA-7-716029: Group name User user Unable to rename file filename.Error: description`

说明：用户无法使用 CIFS 协议重命名远程文件，这可能是缺少文件权限导致的。

建议的操作：检查 WebVPN 设备和 CIFS 协议所访问的服务器之间的连接。此外，请检查 Firepower 威胁防御设备上的 NetBIOS 名称服务器配置和文件权限。

716030

错误消息：`%ASA-7-716030: Group name User user Unable to modify file filename.Error: description`

说明：当用户尝试使用 CIFS 协议修改现有文件时发生了问题，这可能是缺少文件权限导致的。

建议的操作：检查 WebVPN 设备和 CIFS 协议所访问的服务器之间的连接。此外，请检查 Firepower 威胁防御设备上的 NetBIOS 名称服务器配置和文件权限。

716031

错误消息：`%ASA-7-716031: Group name User user Unable to create file filename.Error: description`

说明：当用户尝试使用 CIFS 协议创建文件时发生了问题，这可能是文件权限问题导致的。

建议的操作：检查 WebVPN 设备和 CIFS 协议所访问的服务器之间的连接。此外，请检查 Firepower 威胁防御设备上的 NetBIOS 名称服务器配置和文件权限。

716032

错误消息：`%ASA-7-716032: Group name User user Unable to create folder folder.Error: description`

说明：当用户尝试使用 CIFS 协议创建文件夹时发生了问题，这可能是文件权限问题导致的。

建议的操作：检查 WebVPN 设备和 CIFS 协议所访问的服务器之间的连接。此外，请检查 Firepower 威胁防御设备上的 NetBIOS 名称服务器配置和文件权限。

716033

错误消息：`%ASA-7-716033: Group name User user Unable to remove folder folder.Error: description`

说明：当CIFS协议用户尝试删除文件夹时发生了问题，这可能是权限问题或者与该文件所在的服务器通信时发生问题导致的。

建议的操作：检查 WebVPN 设备和 CIFS 协议所访问的服务器之间的连接。此外，请检查 Firepower 威胁防御设备上的 NetBIOS 名称服务器配置。

716034

错误消息：`%ASA-7-716034: Group name User user Unable to write to file filename.`

说明：当用户尝试使用CIFS协议对文件进行写入时发生了问题，这可能是权限问题或者与该文件所在的服务器通信时发生问题导致的。

建议的操作：无需执行任何操作。

716035

错误消息：`%ASA-7-716035: Group name User user Unable to read file filename.`

说明：当 CIFS 协议用户尝试读取文件时发生了问题，这可能是文件权限问题导致的。

建议的操作：检查文件权限。

716036

错误消息： `%ASA-7-716036: Group name User user File Access: User user logged into the server server.`

说明： 用户已成功使用 CIFS 协议登录服务器

建议的操作： 无需执行任何操作。

716037

错误消息： `%ASA-7-716037: Group name User user File Access: User user failed to login into the server server.`

说明： 用户已尝试使用 CIFS 协议登录服务器，但未成功。

建议的操作： 验证用户是否输入了正确的用户名和密码。

716038

错误消息： `%ASA-6-716038: Group group User user IP ip Authentication: successful, Session Type: WebVPN.`

说明： 必须在本地或远程服务器（例如RADIUS或TACACS+）成功对用户进行身份验证后，WebVPN会话才能启动。

建议的操作： 无需执行任何操作。

716039

错误消息： `%ASA-6-716039: Authentication: rejected, group = name user = user , Session Type: %s`

说明： 必须在本地或远程服务器（例如RADIUS或TACACS+）成功对用户进行身份验证后，WebVPN会话才能启动。在此情况下，用户凭证（用户名和密码）未匹配，或者用户不具有启动 WebVPN 会话的权限。用户名在无效或未知时隐藏，但在有效或配置了 **no logging hide username** 命令时显示。

- **%s** - 会话类型，可以是 WebVPN 或 admin

建议的操作： 验证本地或远程服务器上的用户凭证，并且验证是否为用户配置了 WebVPN。

716040

错误消息： `%ASA-6-716040: Reboot pending, new sessions disabled.Denied user login.`

说明： 用户无法登录到 WebVPN，因为 Firepower 威胁防御设备正在重启。

- **user** - 会话用户

建议的操作： 无需执行任何操作。

716041

错误消息： `%ASA-6-716041: access-list acl_ID action url url hit_cnt count`

说明： 系统允许或拒绝其 **action** 的位置 **url** 已 **count** 次命中名为 **acl_ID** 的 WebVPN URL。

- **acl_ID** - WebVPN URL ACL
- *count* - 已访问该 URL 的次数
- *url* - 已访问的 URL
- *action* - 用户操作

建议的操作： 无需执行任何操作。

716042

错误消息： `%ASA-6-716042: access-list acl_ID action tcp source_interface /source_address (source_port ) - dest_interface /dest_address (dest_port ) hit-cnt count`

说明： 在系统允许或拒绝其 **action** 的源接口 **source_interface/source_address** 和转发到 **dest_interface/dest_address** 目的 **dest_port** 的源端口 **source_port** 上收到的数据包已 **count** 次命中名为 **acl_ID** 的 WebVPN TCP。

- *count* - 已访问该 ACL 的次数
- *source_interface* - 源接口
- *source_address* - 源 IP 地址
- *source_port* - 源端口
- *dest_interface* - 目的接口
- *dest_address* - 目的 IP 地址
- *action* - 用户操作

建议的操作： 无需执行任何操作。

716043

错误消息： `%ASA-6-716043 Group group-name , User user-name , IP IP_address : WebVPN Port Forwarding Java applet started.Created new hosts file mappings.`

说明： 用户已从 WebVPN 会话启动 TCP 端口转发小应用程序。

- **group-name** - 与此会话关联的组名称
- **user-name** - 与此会话关联的用户名
- **IP_address** - 与此会话关联的源 IP 地址

建议的操作： 无需执行任何操作。

716044

错误消息： `%ASA-4-716044: Group group-nameUser user-name IP IP_address AAA parameter param-name value param-value out of range.`

说明：给定参数的值错误。

- **group-name** - 组的名称
- **user-name** - 用户的名称
- **IP_address** - IP 地址
- **param-name** - 参数的名称
- **param-value** - 参数的值

建议的操作：修改配置以更正所指示的参数。如果参数为 vlan 或 nac-settings，请验证是否在 AAA 服务器和 Firepower 威胁防御设备上正确配置了该参数。

716045

错误消息：`%ASA-4-716045: Group group-name User user-name IP IP_address AAA parameter param-name value invalid.`

说明：给定的参数具有无效值。该值未显示，因为它可能很长。

- **group-name** - 组的名称
- **user-name** - 用户的名称
- **IP_address** - IP 地址
- **param-name** - 参数的名称

建议的操作：修改配置以更正所指示的参数。

716046

错误消息：`%ASA-4-716046: Group group-name User user-name IP IP_addressUser ACL access-list-name from AAA doesn't exist on the device, terminating connection.`

说明：在 Firepower 威胁防御设备上找不到指定的 ACL。

- **group-name** - 组的名称
- **user-name** - 用户的名称
- **IP_address** - IP 地址
- **access-list-name** - ACL 的名称

建议的操作：修改配置以添加指定的 ACL 或更正 ACL 名称。

716047

错误消息：`%ASA-4-716047: Group group-name User user-name IP IP_addressUser ACL access-list-name from AAA ignored, AV-PAIR ACL used instead.`

说明：由于使用了思科 AV-PAIR ACL，因此系统未使用指定的 ACL。

- **group-name** - 组的名称
- **user-name** - 用户的名称
- **IP_address** - IP 地址

- **access-list-name** - ACL 的名称

建议的操作：确定要使用的正确 ACL 并更正配置。

716048

错误消息：`%ASA-4-716048: Group group-name User user-name IP IP_addressNo memory to parse ACL.`

说明：没有足够的内存来解析 ACL。

- **group-name** - 组的名称
- **user-name** - 用户的名称
- **IP_address** - IP 地址

建议的操作：购买更多内存，升级 Firepower 威胁防御设备或减少其负载。

716049

错误消息：`%ASA-6-716049: Group group-name User user-name IP IP_addressEmpty SVC ACL.`

说明：客户端要使用的 ACL 为空。

- **group-name** - 组的名称
- **user-name** - 用户的名称
- **IP_address** - IP 地址

建议的操作：确定要使用的正确 ACL 使用并修改配置。

716050

错误消息：`%ASA-6-716050: Error adding to ACL: ace_command_line`

说明：ACL 条目有语法错误。

- **ace_command_line** - 导致此错误的 ACL 条目

建议的操作：更正可下载的 ACL 配置。

716051

错误消息：`%ASA-6-716051: Group group-name User user-name IP IP_addressError adding dynamic ACL for user.`

说明：没有足够的内存来执行操作。

- **group-name** - 组的名称
- **user-name** - 用户的名称
- **IP_address** - IP 地址

建议的操作：购买更多内存，升级 Firepower 威胁防御设备或减少其负载。

716052

错误消息： `%ASA-4-716052: Group group-name User user-name IP IP_addressPending session terminated.`

说明： 用户未完成登录，并且待处理会话已终止。这可能是由于 SVC 无法连接。

- **group-name** - 组的名称
- **user-name** - 用户的名称
- **IP_address** - IP 地址

建议的操作： 检查用户 PC 的 SVC 兼容性。

716053

错误消息： `%ASA-5-716053: SSO Server added: name: name Type: type`

说明： 已配置指定类型的 SSO 服务器名称。

- **name** - 服务器的名称
- **type** - 服务器的类型（唯一服务器类型为 SiteMinder）

建议的操作： 无需执行任何操作。

716054

错误消息： `%ASA-5-716054: SSO Server deleted: name: name Type: type`

说明： 已从配置中删除指定类型的 SSO 服务器名称。

- **name** - 服务器的名称
- **type** - 服务器的类型（唯一服务器类型为 SiteMinder）

建议的操作： 无需执行任何操作。

716055

错误消息： `%ASA-6-716055: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type succeeded`

说明： WebVPN 用户已成功向 SSO 服务器进行身份验证。

- **group-name** - 组名称
- **user-name** - 用户名
- **IP_address** - 服务器的 IP 地址
- **name** - 服务器的名称
- **type** - 服务器的类型（唯一服务器类型为 SiteMinder）

建议的操作： 无需执行任何操作。

716056

错误消息： `%ASA-3-716056: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type failed reason: reason`

说明： WebVPN 用户未能向 SSO 服务器进行身份验证。

- **group-name** - 组名称
- **user-name** - 用户名
- **IP_address** - 服务器的 IP 地址
- **name** - 服务器的名称
- **type** - 服务器的类型（唯一服务器类型为 SiteMinder）
- **reason** - 身份验证失败的原因

建议的操作： 用户或 Firepower 威胁防御管理员需要根据失败的原因来更正该问题。

716057

错误消息： `%ASA-3-716057: Group group User user IP ip Session terminated, no type license available.`

说明： 用户已尝试使用未经许可的客户端来连接 Firepower 威胁防御设备。如果临时许可证已到期，也可能会出现此消息。

- *group* - 用户登录所使用的组策略
- *user* - 用户的名称
- *IP* - 用户的 IP 地址
- *type* - 所请求的许可证类型，可以是下列其中一项：

- AnyConnect Mobile

- LinkSys Phone

- 客户端请求的许可证类型（如果不是 AnyConnect Mobile 或 LinkSys Phone）

- 未知

建议的操作： 应购买并安装具有相应功能的永久许可证。

716058

错误消息： `%ASA-6-716058: Group group User user IP ip AnyConnect session lost connection.Waiting to resume.`

说明： SSL 隧道已断开连接，并且 AnyConnect 会话进入非活动状态，这可能是主机休眠，主机处于备用状态或网络连接丢失导致的。

- *group* - 与 AnyConnect 会话关联的隧道组名称
- *user* - 与会话关联的用户的名称
- *ip* - 会话的源 IP 地址

建议的操作：无需执行任何操作。

716059

错误消息：`%ASA-6-716059: Group group User user IP ip AnyConnect session resumed.Connection from ip2.`

说明：AnyConnect 会话已从从非活动状态中恢复。

- *group* - 与 AnyConnect 会话关联的隧道组名称
- *user* - 与会话关联的用户的名称
- *ip* - 会话的源 IP 地址
- *ip2* - 恢复该会话的主机的源 IP 地址

建议的操作：无需执行任何操作。

716060

错误消息：`%ASA-6-716060: Group group User user IP ip Terminated AnyConnect session in inactive state to accept a new connection.License limit reached.`

说明：处于非活动状态的 AnyConnect 会话已注销，从而允许新的传入 SSL VPN（AnyConnect 或无客户端）连接。

- *group* - 与 AnyConnect 会话关联的隧道组名称
- *user* - 与会话关联的用户的名称
- *ip* - 会话的源 IP 地址

建议的操作：无需执行任何操作。

716061

错误消息：`%ASA-3-716061: Group DfltGrpPolicy User user IP ip addr IPv6 User Filter tempipv6 configured for AnyConnect.This setting has been deprecated, terminating connection`

说明：IPv6 VPN 过滤器已弃用，如果为 IPv6 流量访问控制配置了 IPv6 VPN 过滤器而不是统一过滤器，连接将被终止。

建议的操作：为统一过滤器配置 IPv6 条目，以控制用户的 IPv6 流量。

716500

错误消息：`%ASA-2-716500: internal error in: function : Fiber library cannot locate AK47 instance`

说明：光纤库无法找到应用内核层 4 到 7 的实例。

建议的操作：要确定问题的原因，请联系思科 TAC。

716501

错误消息： `%ASA-2-716501: internal error in: function : Fiber library cannot attach AK47 instance`

说明： 光纤库无法附加应用内核层 4 到 7 的实例。

建议的操作： 要确定问题的原因，请联系思科 TAC。

716502

错误消息： `%ASA-2-716502: internal error in: function : Fiber library cannot allocate default arena`

说明： 光纤库无法分配默认领域。

建议的操作： 要确定问题的原因，请联系思科 TAC。

716503

错误消息： `%ASA-2-716503: internal error in: function : Fiber library cannot allocate fiber descriptors pool`

说明： 光纤库无法分配光纤描述符池。

建议的操作： 要确定问题的原因，请联系思科 TAC。

716504

错误消息： `%ASA-2-716504: internal error in: function : Fiber library cannot allocate fiber stacks pool`

说明： 光纤库无法分配光纤堆栈池。

建议的操作： 要确定问题的原因，请联系思科 TAC。

716505

错误消息： `%ASA-2-716505: internal error in: function : Fiber has joined fiber in unfinished state`

说明： 光纤已加入处于未完成状态的光纤。

建议的操作： 要确定问题的原因，请联系思科 TAC。

716506

错误消息： `%ASA-2-716506: UNICORN_SYSLOGID_JOINED_UNEXPECTED_FIBER`

说明： 已生成内部光纤库。

建议的操作：联系思科 TAC。

716507

错误消息：`%ASA-1-716507: Fiber scheduler has reached unreachable code.Cannot continue, terminating.`

说明：Firepower 威胁防御设备遇到意外错误并已恢复。

建议的操作：检查高 CPU 使用率或 CPU 占用，以及潜在的内存泄漏。如果问题仍然存在，请联系思科 TAC。

716508

错误消息：`%ASA-1-716508: internal error in: function : Fiber scheduler is scheduling rotten fiber.Cannot continuing terminating`

说明：光纤调度程序调度的是腐坏光纤，因此其无法继续终止。

建议的操作：要确定问题的原因，请联系思科 TAC。

716509

错误消息：`%ASA-1-716509:internal error in: function : Fiber scheduler is scheduling alien fiber.Cannot continue terminating`

说明：光纤调度程序调度的是外来光纤，因此其无法继续终止。

建议的操作：要确定问题的原因，请联系思科 TAC。

716510

错误消息：`%ASA-1-716510:internal error in: function : Fiber scheduler is scheduling finished fiber.Cannot continue terminating`

说明：光纤调度程序调度的是成品光纤，因此其无法继续终止。

建议的操作：要确定问题的原因，请联系思科 TAC。

716512

错误消息：`%ASA-2-716512:internal error in: function : Fiber has joined fiber waited upon by someone else`

说明：光纤已加入其他人员等待的光纤。

建议的操作：要确定问题的原因，请联系思科 TAC。

716513

错误消息：`%ASA-2-716513: internal error in: function : Fiber in callback blocked on other channel`

说明：回调中的光纤在另一条通道上已堵塞。

建议的操作：要确定问题的原因，请联系思科 TAC。

716515

错误消息：`%ASA-2-716515:internal error in: function : OCCAM failed to allocate memory for AK47 instance`

说明：OCCAM 未能为 AK47 实例分配内存。

建议的操作：要确定问题的原因，请联系思科 TAC。

716516

错误消息：`%ASA-1-716516: internal error in: function : OCCAM has corrupted ROL array.Cannot continue terminating`

说明：OCCAM 具有已损坏的 ROL 阵列，因此其无法继续终止。

建议的操作：要确定问题的原因，请联系思科 TAC。

716517

错误消息：`%ASA-2-716517: internal error in: function : OCCAM cached block has no associated arena`

说明：OCCAM 缓存块没有任何关联领域。

建议的操作：要确定问题的原因，请联系思科 TAC。

716518

错误消息：`%ASA-2-716518: internal error in: function : OCCAM pool has no associated arena`

说明：OCCAM 池没有任何关联领域。

建议的操作：要确定问题的原因，请联系思科 TAC。

716519

错误消息：`%ASA-1-716519: internal error in: function : OCCAM has corrupted pool list.Cannot continue terminating`

说明：OCCAM 具有已损坏的池列表，因此其无法继续终止。

建议的操作：要确定问题的原因，请联系思科 TAC。

716520

错误消息：`%ASA-2-716520:internal error in: function : OCCAM pool has no block list`

说明：OCCAM 池没有任何阻止列表。

建议的操作：要确定问题的原因，请联系思科 TAC。

716521

错误消息：`%ASA-2-716521: internal error in: function : OCCAM no realloc allowed in named pool`

说明：OCCAM 不允许在指定池中重新分配。

建议的操作：要确定问题的原因，请联系思科 TAC。

716522

错误消息：`%ASA-2-716522: internal error in: function : OCCAM corrupted standalone block`

说明：OCCAM 具有已损坏的独立块。

建议的操作：要确定问题的原因，请联系思科 TAC。

716525

错误消息：`%ASA-2-716525: UNICORN_SYSLOGID_SAL_CLOSE_PRIVDATA_CHANGED`

说明：发生内部 SAL 错误。

建议的操作：联系思科 TAC。

716526

错误消息：`%ASA-2-716526: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_LOAD_FAIL`

说明：安装永久存储服务器目录失败。

建议的操作：联系思科 TAC。

716527

错误消息：`%ASA-2-716527: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_STORE_FAIL`

说明：安装永久存储文件失败。

建议的操作：联系思科 TAC。

716528

错误消息： `%ASA-1-716528: Unexpected fiber scheduler error; possible out-of-memory condition`

说明： Firepower 威胁防御设备遇到意外错误并已恢复。

建议的操作： 检查高 CPU 使用率或 CPU 占用，以及潜在的内存泄漏。如果问题仍然存在，请联系思科 TAC。

716600

错误消息： `%ASA-3-716600: Rejected size-recv KB Hostscan data from IP src-ip.Hostscan results exceed default | configured limit of size-conf KB.`

说明： 当接收到的 Hostscan 数据的大小超出 Firepower 威胁防御设备上配置的限制时，将会丢弃这些数据。

- *size-recv* - 收到的 Hostscan 数据的大小（以千字节为单位）
- *src-ip* - 源 IP 地址
- *default* | *configured* - 指定 Hostscan 数据限制的值是采用默认值还是由管理员进行配置的关键字
- *size-conf* - Firepower 威胁防御设备从客户端接受的 Hostscan 数据大小的已配置上限

建议的操作： 联系思科 TAC 以增大 Firepower 威胁防御设备从客户端接受的 Hostscan 数据大小的上限。

716601

错误消息： `%ASA-3-716601: Rejected size-recv KB Hostscan data from IP src-ip.System-wide limit on the amount of Hostscan data stored on ASA exceeds the limit of data-max KB.`

说明： 当 Firepower 威胁防御设备上存储的 Hostscan 数据量超出限制时，将会拒绝新的 Hostscan 结果。

- *size-recv* - 收到的 Hostscan 数据的大小（以千字节为单位）
- *src-ip* - 源 IP 地址
- *data-max* - 要由 Firepower 威胁防御设备存储的 Hostscan 结果量的限制（以千字节为单位）

建议的操作： 联系思科 TAC 以更改对存储的 Hostscan 数据的限制。

716602

错误消息： `%ASA-3-716602: Memory allocation error.Rejected size-recv KB Hostscan data from IP src-ip.`

说明： 在为 Hostscan 数据分配内存时发生错误。

- *size-recv* - 收到的 Hostscan 数据的大小（以千字节为单位）
- *src-ip* - 源 IP 地址

建议的操作：如果已配置 Hostscan 限制，请将该限制设置为默认值。如果问题仍然存在，请联系思科 TAC。

716603

错误消息：`%ASA-7-716603: Received size-recv KB Hostscan data from IP src-ip.`

说明：已成功收到指定大小的 Hostscan 数据。

- *size-recv* - 收到的 Hostscan 数据的大小（以千字节为单位）
- *src-ip* - 源 IP 地址

建议的操作：无需执行任何操作。

ID 介于 717001 到 717064 之间的消息

本部分包括 ID 介于 717001 到 717064 之间的消息。

717001

错误消息：`%ASA-3-717001: Querying keypair failed.`

说明：在注册请求期间找不到所需的密钥对。

建议的操作：验证信任点配置中是否存在有效的密钥对，然后重新提交注册请求。

717002

错误消息：`%ASA-3-717002: Certificate enrollment failed for trustpoint trustpoint_name.Reason: reason_string.`

说明：此信任点的注册请求失败。

- *trustpoint name* - 注册请求所对应的信任点名称
- *reason_string* - 注册请求失败的原因

建议的操作 - 检查 CA 服务器以查明失败原因。

717003

错误消息：`%ASA-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint_name.`

说明：已从此信任点的 CA 成功收到证书。

- *trustpoint_name* - 信任点名称

建议的操作：无需执行任何操作

717004

错误消息： `%ASA-6-717004: PKCS #12 export failed for trustpoint trustpoint_name.`

说明： 由于以下情况之一，信任点未能导出：仅存在 CA 证书，并且信任点不存在身份证书，或者缺少所需的密钥对。

- *trustpoint_name* - 信任点名称

建议的操作： 确保给定信任点存在所需的证书和密钥对。

717005

错误消息： `%ASA-6-717005: PKCS #12 export succeeded for trustpoint trustpoint_name.`

说明： 已成功导出信任点。

- *trustpoint_name* - 信任点名称

建议的操作： 无需执行任何操作

717006

错误消息： `%ASA-6-717006: PKCS #12 import failed for trustpoint trustpoint_name.`

说明： 未能处理对请求的信任点的导入。

- *trustpoint_name* - 信任点名称

建议的操作： 验证导入数据的完整性。然后，确保正确粘贴整个 pkcs12 记录，并重新导入数据。

717007

错误消息： `%ASA-6-717007: PKCS #12 import succeeded for trustpoint trustpoint_name.`

说明： 已成功完成对请求的信任点的导入。

- *trustpoint_name* - 信任点名称

建议的操作： 无需执行任何操作。

717008

错误消息： `%ASA-2-717008: Insufficient memory to process_requiring_memory.`

说明： 在尝试为需要内存的进程分配内存时发生内部错误。其他进程在分配内存时可能会遇到问题并阻止进一步处理。

- **process_requiring_memory** - 需要内存的指定进程

建议的操作： 收集内存统计信息和日志以进一步调试并重新加载 Firepower 威胁防御设备。

717009

错误消息： `%ASA-3-717009: Certificate validation failed.Reason: reason_string.`

说明： 证书验证失败，这可能是由尝试验证已吊销的证书、证书属性无效或配置问题所导致。

- *reason_string* - 证书验证失败的原因

建议的操作： 如果原因表示找不到合适的信任点，请确保配置具有配置用于验证的有效信任点。检查Firepower威胁防御设备时间以确保其相对于证书颁发机构时间是准确的。检查失败原因并更正所指示的任何问题。

717010

错误消息： `%ASA-3-717010: CRL polling failed for trustpoint trustpoint_name.`

说明： CRL 轮询失败，并且可能导致拒绝连接（如果要求进行 CRL 检查）。

- **trustpoint_name** - 已请求 CRL 的信任点的名称

建议的操作： 验证是否存在含已配置的CRL分发点的连接，并确保手动CRL检索也能够正常运行。

717011

错误消息： `%ASA-2-717011: Unexpected event event event_ID`

说明： 发生了在正常条件下预期不会发生的事件。

建议的操作： 如果问题仍然存在，请联系思科 TAC。

717012

错误消息： `%ASA-3-717012: Failed to refresh CRL cache entry from the server for trustpoint trustpoint_name at time_of_failure`

说明： 在所示失败时间尝试为指定信任点刷新缓存 CRL 条目失败。这可能会造成 Firepower 威胁防御设备上的 CRL 过时，从而导致拒绝需要有效 CRL 的连接。

- **trustpoint_name** - 信任点的名称
- *time_of_failure*-- 失败时间

建议的操作： 检查服务器的连接问题，例如网络或服务器已关闭。尝试使用 **crypto ca crl retrieve** 命令手动检索 CRL。

717013

错误消息： `%ASA-5-717013: Removing a cached CRL to accommodate an incoming CRL.Issuer: issuer`

说明： 当设备配置为使用数字证书对 IPsec 隧道进行身份验证时，可将 CRL 缓存在内存中，以避免每个连接期间都需要下载 CRL。如果缓存填充至无法容纳传入 CRL 的程度，系统将删除较旧的 CRL，直到腾出所需的空间为止。每个清除的 CRL 都会生成此消息。

- **issuer** - 用于删除缓存 CRL 的设备的名称

建议的操作：无需执行任何操作。

717014

错误消息：`%ASA-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = size , available cache space = space)`

说明：当设备配置为使用数字证书对 IPsec 隧道进行身份验证时，可将 CRL 缓存在内存中，以避免每个连接期间都需要下载CRL。当收到的CRL太大而无法进行缓存时，会生成此消息。即使未进行缓存，仍然支持大 CRL。这意味着每个 IPsec 连接都将下载 CRL，这可能会在 IPsec 连接激增期间影响性能。

建议的操作：无需执行任何操作。

717015

错误消息：`%ASA-3-717015: CRL received from issuer is too large to process (CRL size = crl_size , maximum CRL size = max_crl_size)`

说明：IPsec 连接已导致下载大于最大允许 CRL 大小的 CRL。此错误情况会导致连接失败。此消息的速率限制为每 10 秒一条消息。

建议的操作：可扩展性可能是CRL吊销检查方法的最大缺点。要解决此问题，仅有的两个选择是调查基于 CA 的解决方案来减小 CRL 大小或将 Firepower 威胁防御设备配置为无需 CRL 验证。

717016

错误消息：`%ASA-6-717016: Removing expired CRL from the CRL cache.Issuer: issuer`

说明：当 Firepower 威胁防御设备配置为使用数字证书对 IPsec 隧道进行身份验证时，可将 CRL 缓存在内存中，以避免每个连接期间都需要下载 CRL。当 CA 指定的到期时间或配置的缓存时间已过并从缓存中删除了 CRL 时，将会生成此消息。

建议的操作：无需执行任何操作。

717017

错误消息：`%ASA-3-717017: Failed to query CA certificate for trustpoint trustpoint_name from enrollment_url`

说明：在尝试通过从证书颁发机构请求 CA 证书来对信任点进行身份验证时发生错误。

建议的操作：确保注册 URL 配置有此信任点，确保与 CA 服务器的连接，然后重试请求。

717018

错误消息：`%ASA-3-717018: CRL received from issuer has too many entries to process (number of entries = number_of_entries , maximum number allowed = max_allowed)`

说明：IPsec 连接已导致下载所包含的吊销条目数超过支持的条目数的 CRL。此错误情况将导致连接失败。此消息的速率限制为每 10 秒一条消息。

- **issuer** - CRL 颁发者的 X.500 名称
- **number_of_entries** - 收到的 CRL 中的吊销条目数
- **max_allowed** - Firepower 威胁防御设备支持的最大 CRL 条目数

建议的操作：可扩展性可能是 CRL 吊销检查方法的最大缺点。解决此问题的仅有的两个选择是调查基于 CA 的解决方案来减小 CRL 大小或将 Firepower 威胁防御设备配置为无需 CRL 验证。

717019

错误消息：`%ASA-3-717019: Failed to insert CRL for trustpoint` *`trustpoint_name`*`.Reason:` *`failure_reason`* `.`

说明：系统检索到 CRL，但发现其无效且无法插入到缓存中，原因是 **failure_reason**。

- **trustpoint_name** - 已请求 CRL 的信任点的名称
- **failure_reason** - CRL 未能插入到缓存中的原因

建议的操作：确保当前 Firepower 威胁防御设备时间相对于 CA 时间正确。如果 NextUpdate 字段缺失，请将信任点配置为忽略 NextUpdate 字段。

717020

错误消息：`%ASA-3-717020: Failed to install device certificate for trustpoint` *`label`*`.Reason:` *`reason string`*`.`

说明：在尝试将已注册证书注册到或导入到信任点中时发生错误。

- *label* - 未能安装已注册 Firepower 威胁防御证书的信任点的标签
- *reason_string* - 无法验证证书的原因

建议的操作：根据失败原因对失败的原因进行纠正，然后重试注册。常见失败原因是将无效证书导入到 Firepower 威胁防御设备中，或者已注册证书中包含的公钥与信任点中引用的密钥对不匹配。

717021

错误消息：`%ASA-3-717021: Certificate data could not be verified.Locate Reason:` *`reason_string`* `serial number:` *`serial number`* `, subject name:` *`subject name`* `, key length` *`key length`* `bits.`

说明：由于指定的原因，尝试验证通过序列号和使用者名称识别的证书未成功。当使用签名来验证证书数据时，可能会发生多个应记录的错误，包括密钥类型无效和密钥大小不受支持。

- *reason_string* - 无法验证证书的原因
- *serial number* - 正在验证的证书的序列号
- *subject name* - 正在验证的证书中包含的使用者名称
- *key length* - 用于对此证书进行签名的密钥的位数

建议的操作：检查指定的证书以确保其有效，即它包含有效的密钥类型，并且不超过支持的最大密钥大小。

717022

错误消息：`%ASA-6-717022: Certificate was successfully validated.`*`certificate_identifiers`*

说明：已成功验证所识别的证书。

- *certificate_identifiers* - 用于识别已成功验证的证书的信息，其中可能包括原因、序列号、使用者名称和其他信息。

建议的操作：无需执行任何操作。

717023

错误消息：`%ASA-3-717023: SSL failed to set device certificate for trustpoint` *`trustpoint name`*`.Reason:` *`reason_string`*`.`

说明：在尝试为给定信任点设置 Firepower 威胁防御证书以对 SSL 连接进行身份验证时发生错误。

- *trustpoint name* - SSL 未能为其设置 Firepower 威胁防御证书的信任点的名称
- *reason_string* - 表示无法设置 Firepower 威胁防御证书的原因

建议的操作：通过执行以下操作来解决所报告的失败原因指示的问题：

- 确保指定的信任点已注册并具有 Firepower 威胁防御证书。
- 确保 Firepower 威胁防御证书有效。
- 如果需要，重新注册信任点。

717024

错误消息：`%ASA-7-717024: Checking CRL from trustpoint:` *`trustpoint name`* `for` *`purpose`*

说明：正在检索 CRL。

- *trustpoint name* - 正在为其检索 CRL 的信任点的名称
- *purpose* - 检索 CRL 的原因

建议的操作：无需执行任何操作。

717025

错误消息：`%ASA-7-717025: Validating certificate chain containing` *`number of certs`* `certificate(s).`

说明：正在验证证书链。

- >*number of certs* - 链中的证书数量

建议的操作：无需执行任何操作。

717026

错误消息： `%ASA-4-717026: Name lookup failed for hostname hostname during PKI operation.`

说明： 在尝试 PKI 操作时无法解析给定主机名。

- >*hostname* - 未能解析的主机名

建议的操作： 检查配置和给定主机名的 DNS 服务器条目，以确保其可以解析。然后，重试操作。

717027

错误消息： `%ASA-3-717027: Certificate chain failed validation.reason_string.`

说明： 无法验证证书链。

- *reason_string* - 验证证书链失败的原因

建议的操作： 解决原因注明的问题，然后通过执行以下任意操作来重试验证尝试：

- 确保与 CA 的连接可用（如果需要 CRL 检查）。
- 确保信任点已进行身份验证并可供验证。
- 确保链中的身份证书有效（基于有效期）。
- 确保证书未吊销。

717028

错误消息： `%ASA-6-717028: Certificate chain was successfully validated additional info.`

说明： 已成功验证证书链。

- >*additional info* - 有关如何验证证书链的详细信息（例如，“with warning”表示未执行 CRL 检查）

建议的操作： 无需执行任何操作。

717029

错误消息： `%ASA-7-717029: Identified client certificate within certificate chain. serial number: serial_number , subject name: subject_name.`

说明： 已识别指定为客户端证书的证书。

- **serial_number** - 识别为客户端证书的证书的序列号
- **subject_name** - 识别为客户端证书的证书中包含的使用者名称

建议的操作： 无需执行任何操作。

717030

错误消息： `%ASA-7-717030: Found a suitable trustpoint trustpoint name to validate certificate.`

说明：找到可用于验证证书的合适或可用的信任点。

- *trustpoint name* - 将用于验证证书的信任点

建议的操作：无需执行任何操作。

717031

错误消息：`%ASA-4-717031: Failed to find a suitable trustpoint for the issuer: issuer Reason: reason_string`

说明：无法找到可用的信任点。在证书验证期间，必须具有合适的信任点，以便验证证书。

- >*issuer* - 正在验证的证书的颁发者
- *reason_string* - 无法找到合适信任点的原因

建议的操作：通过检查配置以确保信任点已配置、已进行身份验证并已注册来解决原因中指示的问题。此外确保配置允许特定类型的证书，例如身份证书。

717033

错误消息：`%ASA-6-717033: OCSP response status - Successful.`

说明：成功收到 OCSP 状态检查响应。

建议的操作：无需执行任何操作。

717034

错误消息：`%ASA-7-717034: No-check extension found in certificate.OCSP check bypassed.`

说明：收到包含“id-pkix-ocsp-nocheck”扩展的 OCSP 响应方证书，通过该扩展可验证此证书，而无需 OCSP 状态检查。

建议的操作：无需执行任何操作。

717035

错误消息：`%ASA-4-717035: OCSP status is being checked for certificate.certificate_identifier.`

说明：识别发生 OCSP 状态检查的证书。

- *certificate_identifier* - 用于识别通过证书映射规则来处理的证书的信息

建议的操作：无需执行任何操作。

717036

错误消息：`ASA-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with certificate_identifier.`

说明：按证书标识符识别的对等证书正在通过所配置的证书映射进行处理，从而尝试可能的隧道匹配。

- *certificate_identifier* - 用于识别通过证书映射规则来处理的证书的信息

建议的操作：无需执行任何操作。

717037

错误消息：`%ASA-4-717037: Tunnel group search using certificate maps failed for peer certificate: certificate_identifier.`

说明：按证书标识符识别的对等证书已通过所配置的证书映射进行处理，从而尝试可能的隧道组匹配，但无法找到任何匹配项。

- *certificate_identifier* - 用于识别通过证书映射规则来处理的证书的信息

建议的操作：确保将会根据收到的对等证书和配置的加密 CA 证书映射规则发出警告。

717038

错误消息：`%ASA-7-717038: Tunnel group match found.Tunnel Group: tunnel_group_name , Peer certificate: certificate_identifier.`

说明：按证书标识符识别的对等证书已通过所配置的证书映射进行处理，并且找到隧道组的匹配项。

- *certificate_identifier* - 用于识别通过证书映射规则来处理的证书的信息
- *tunnel_group_name* - 按证书映射规则匹配的隧道组的名称

建议的操作：无需执行任何操作。

717050

错误消息：`%ASA-5-717050: SCEP Proxy: Processed request type type from IP client ip address , User username , TunnelGroup tunnel_group name , GroupPolicy group-policy name to CA IP ca ip address`

说明：SCEP 代理收到一条消息，并将其中继到 CA。来自 CA 的响应会中继回客户端。

- *type* - SCEP 代理收到的请求类型字符串，可以是以下 SCEP 消息类型之一：PKIOperation、GetCACaps、GetCACert、GetNextCACert 和 GetCACertChain。
- *client ip address* - 收到的请求的源 IP 地址
- *username* - 与收到 SCEP 请求的 VPN 会话关联的用户名
- *tunnel-group name* - 与收到 SCEP 请求的 VPN 会话关联的隧道组
- *group-policy name* - 与收到 SCEP 请求的 VPN 会话关联的组策略
- *ca ip address* - 组策略中配置的 CA 的 IP 地址

建议的操作：无需执行任何操作。

717051

错误消息： `%ASA-3-717051: SCEP Proxy: Denied processing the request type type received from IP client ip address , User username , TunnelGroup tunnel group name , GroupPolicy group policy name to CA ca ip address.Reason: msg`

说明： SCEP代理已拒绝处理请求，这可能是由于配置错误、代理中发生错误情况或请求无效所导致的。

- *type* - SCEP 代理收到的请求类型字符串，可以是以下 SCEP 消息类型之一：PKIOperation、GetCACaps、GetCACert、GetNextCACert 和 GetCACertChain。
- *client ip address* - 收到的请求的源 IP 地址
- *username* - 与收到 SCEP 请求的 VPN 会话关联的用户名
- *tunnel-group name* - 与收到 SCEP 请求的 VPN 会话关联的隧道组
- *group-policy name* - 与收到 SCEP 请求的 VPN 会话关联的组策略
- *ca ip address* - 组策略中配置的 CA 的 IP 地址
- **msg** - 用于说明拒绝请求处理的原因或错误的原因字符串

建议操作： 根据列出的原因来确定原因。如果原因指出请求无效，请检查 CA URL 配置。否则，请确认是否已启用隧道组进行SCEP注册，并通过使用 **debug crypto ca scep-proxy** 命令来进一步调试。

717052

错误消息： `%ASA-4-717052: Group group name User user name IP IP Address Session disconnected due to periodic certificate authentication failure.Subject Name id subject name Issuer Name id issuer name Serial Number id serial number`

说明： 定期证书身份验证失败，并且会话已断开连接。

- *group name* - 会话所属的组策略的名称
- *user name* - 会话的用户名
- *IP* - 会话的公共 IP 地址
- *id subject name* - 会话 ID 证书中的使用者名称
- *id issuer name* - 会话 ID 证书中的颁发者名称
- *id serial number* - 会话 ID 证书中的序列号

建议的操作： 无需执行任何操作。

717053

SSP 整体主题

错误消息： `%ASA-5-717053: Group group name User user name IP IP Address Periodic certificate authentication succeeded.Subject Name id subject name Issuer Name id issuer name Serial Number id serial number`

说明： 定期证书身份验证已成功。

- *group name* - 会话所属的组策略的名称

- *user name* - 会话的用户名
- *id subject name* - 会话 ID 证书中的使用者名称
- *id issuer name* - 会话 ID 证书中的颁发者名称
- *id serial number* - 会话 ID 证书中的序列号

建议的操作：无需执行任何操作。

717054

SSP 整体主题

错误消息：`%ASA-1-717054: The type certificate in the trustpoint tp name is due to expire in number days.Expiration date and time Subject Name subject name Issuer Name issuer name Serial Number serial number`

说明：信任点中的指定证书即将到期。

- *type* - 证书的类型：CA 或 ID
- *tp name* - 证书所属的信任点的名称
- *number* - 到期前所剩天数
- *date and time*：到期日期和时间
- *subject name* - 证书中的使用者名称
- *issuer name* - 证书中的颁发者名称
- *serial number* - 证书中的序列号

建议的操作：续订证书。

717055

错误消息：`%ASA-1-717055: The type certificate in the trustpoint tp name has expired.Expiration date and time Subject Name subject name Issuer Name issuer name Serial Number serial number`

说明：信任点中的指定证书已到期。

- *type* - 证书的类型：CA 或 ID
- *tp name* - 证书所属的信任点的名称
- *date and time*：到期日期和时间
- *subject name* - 证书中的使用者名称
- *issuer name* - 证书中的颁发者名称
- *serial number* - 证书中的序列号

建议的操作：续订证书。

717056

仅标题 SSP

错误消息：`%ASA-6-717056: Attempting type revocation check from Src Interface :Src IP /Src Port to Dst IP /Dst Port using protocol`

说明：CA 正在尝试下载 CRL 或发送 OCSP 吊销检查请求。

- *type* - 吊销检查的类型，可以为 OCSP 或 CRL
- *Src Interface* - 正在从其进行吊销检查的接口的名称
- *Src IP* - 正在从其进行吊销检查的 IP 地址
- *Src Port* - 正在从其进行吊销检查的端口号
- *Dst IP* - 正在向其发送吊销检查请求的服务器的 IP 地址
- *Dst Port* - 正在向其发送吊销检查请求的服务器的端口号
- *Protocol* - 正在用于吊销检查的协议，可以为 HTTP、LDAP 或 SCEP

建议的操作：无需执行任何操作。

717057

错误消息：`%ASA-3-717057: Automatic import of trustpool certificate bundle has failed.< Maximum retry attempts reached.Failed to reach CA server> | <Cisco root bundle signature validation failed> | <Failed to update trustpool bundle in flash> | <Failed to install trustpool bundle in memory>`

说明：系统根据其中一条错误消息生成了此系统日志。此系统日志旨在使用自动导入操作的结果来更新用户，并将这些结果转发给适当的调试消息，尤其是在失败情况下。调试输出中提供了每个错误的详细信息。

建议的操作：验证 CA 可访问性并在闪存 CA 根证书上腾出空间。

717058

错误消息：`%ASA-6-717058: Automatic import of trustpool certificate bundle is successful: <No change in trustpool bundle> | <Trustpool updated in flash>.`

说明：系统根据其中一条成功消息生成了此系统日志。此系统日志旨在使用自动导入操作的结果来更新用户，并将这些结果转发给适当的调试消息，尤其是在失败情况下。调试输出中提供了每个错误的详细信息。

建议的操作：无。

717059

错误消息：`%ASA-6-717059: Peer certificate with serial number: <serial>, subject: <subject_name>, issuer: <issuer_name> matched the configured certificate map <map_name>`

说明：在通过证书对 ASDM 连接进行身份验证并根据所配置的证书映射规则允许该连接后，将会生成此日志。

建议的操作：无需执行任何操作。

717060

错误消息： `%ASA-3-717060: Peer certificate with serial number: <serial>, subject: <subject_name>, issuer: <issuer_name> failed to match the configured certificate map <map_name>`

说明： 在通过证书对 ASDM 连接进行身份验证，但根据所配置的证书映射规则不允许该连接时，将会生成此日志。

建议的操作： 如果应该允许日志中引用的对等证书，请检查证书映射配置以查找所引用的map_name，并根据需要将映射更正为允许该连接。

717061

仅 SSP 标题

错误消息： `%ASA-5-717061: Starting protocol certificate enrollment for the trustpoint tpname with the CA ca_name.Request Type type Mode mode`

说明： 已触发 CMP 注册请求。

- *tpname* - 进行注册的信任点的名称
- *ca* - CMP 配置中提供的 CA 主机名或 IP 地址
- *type* - CMP 请求类型，包括：“初始化请求”、“认证请求”和“密钥更新请求”
- *mode* - 注册触发模式：“手动”或“自动”
- *protocol* - 注册协议：CMP

建议的操作： 无需执行任何操作。

717062

错误消息： `%ASA-5-717062: protocol Certificate enrollment succeeded for the trustpoint tpname with the CA ca. Received a new certificate with Subject Name subject Issuer Name issuer Serial Number serial`

说明： CMP 注册请求已成功。系统收到新证书。

- *tpname* - 进行注册的信任点的名称
- *ca* - CMP 配置中提供的 CA 主机名或 IP 地址
- *subject* - 收到的证书中的使用者名称
- *issuer* - 收到的证书中的颁发者名称
- serial - 收到的证书中的序列号
- *protocol* - 注册协议：CMP

建议的操作： 无需执行任何操作。

717063

仅 SSP 标题

错误消息：`%ASA-3-717063: protocol Certificate enrollment failed for the trustpoint tpname with the CA ca`

说明：CMP 注册请求失败。

- *tpname* - 进行注册的信任点的名称
- *ca* - CMP 配置中提供的 CA 主机名或 IP 地址
- *protocol* - 注册协议：CMP

建议的操作：使用 CMP 调试跟踪来修复注册失败问题。

717064

仅 SSP 标题

错误消息：`%ASA-5-717064: Keypair keyname in the trustpoint tpname is regenerated for mode protocol certificate renewal`

说明：对于使用 CMP 的证书注册，将会重新生成信任点中的密钥对。

- *tpname* - 进行注册的信任点的名称
- *keyname* - 信任点中的密钥对的名称
- mode - 注册触发模式：Manual 或 Automatic
- *protocol* - 注册协议：CMP

建议的操作：无需执行任何操作。

ID 介于 718001 到 719026 之间的消息

本部分包括 ID 介于 718001 到 719026 之间的消息。

718001

错误消息：`%ASA-7-718001: Internal interprocess communication queue send failure: code error_code`

说明：在尝试将 VPN 负载均衡队列中的消息排队时发生内部软件错误。

建议的操作：这通常是良性情况。如果问题仍然存在，请联系思科 TAC。

718002

错误消息：`%ASA-5-718002: Create peer IP_address failure, already at maximum of number_of_peers`

说明：已超出最大负载均衡对等体数量。系统将忽略新的对等体。

建议的操作：检查负载均衡和网络配置，以确保负载均衡对等体的数量不超出允许的最大值。

718003

错误消息： `%ASA-6-718003: Got unknown peer message message_number from IP_address , local version version_number , remote version version_number`

说明： 从其中一个负载均衡对等体收到了无法识别的负载均衡消息。这可能表示对等体之间的版本不匹配，但很可能是由内部软件错误导致的。

建议的操作： 验证所有负载均衡对等体是否兼容。如果兼容并且此情况仍然存在或与不良行为相关，请联系思科 TAC。

718004

错误消息： `%ASA-6-718004: Got unknown internal message message_number`

说明： 发生了内部软件错误。

建议的操作： 这通常是良性情况。如果问题仍然存在，请联系思科 TAC。

718005

错误消息： `%ASA-5-718005: Fail to send to IP_address , port port`

说明： 在负载均衡套接字上传输数据包期间发生内部软件错误。这可能表示网络问题。

建议的操作： 检查Firepower威胁防御设备上基于网络的配置，并验证接口是否处于活动状态且协议数据流经 Firepower 威胁防御设备。如果问题仍然存在，请联系思科 TAC。

718006

错误消息： `%ASA-5-718006: Invalid load balancing state transition [cur=state_number] [event=event_number]`

说明： 发生了状态机错误。这可能表示存在内部软件错误。

建议的操作： 这通常是良性情况。如果问题仍然存在，请联系思科 TAC。

718007

错误消息： `%ASA-5-718007: Socket open failure failure_code`

说明： 在负载均衡套接字尝试打开时发生错误。这可能表示网络问题或内部软件错误。

建议的操作： 检查Firepower威胁防御设备上基于网络的配置，并验证接口是否处于活动状态且协议数据流经 Firepower 威胁防御设备。如果问题仍然存在，请联系思科 TAC。

718008

错误消息： `%ASA-5-718008: Socket bind failure failure_code`

说明：在Firepower威胁防御设备尝试绑定到负载均衡套接字时发生错误。这可能表示网络问题或内部软件错误。

建议的操作：检查Firepower威胁防御设备上基于网络的配置，并验证接口是否处于活动状态且协议数据流经 Firepower 威胁防御设备。如果问题仍然存在，请联系思科 TAC。

718009

错误消息：`%ASA-5-718009: Send HELLO response failure to IP_address`

说明：在Firepower威胁防御设备尝试将hello响应消息发送到其中一个负载均衡对等体时发生错误。这可能表示网络问题或内部软件错误。

建议的操作：检查Firepower威胁防御设备上基于网络的配置，并验证接口是否处于活动状态且协议数据流经 Firepower 威胁防御设备。如果问题仍然存在，请联系思科 TAC。

718010

错误消息：`%ASA-5-718010: Sent HELLO response to IP_address`

说明：Firepower 威胁防御设备已将 hello 响应消息传输到负载均衡对等体。

建议的操作：无需执行任何操作。

718011

错误消息：`%ASA-5-718011: Send HELLO request failure to IP_address`

说明：在Firepower威胁防御设备尝试将hello请求消息发送到其中一个负载均衡对等体时发生错误。这可能表示网络问题或内部软件错误。

建议的操作：检查Firepower威胁防御设备上基于网络的配置，并验证接口是否处于活动状态且协议数据流经 Firepower 威胁防御设备。如果问题仍然存在，请联系思科 TAC。

718012

错误消息：`%ASA-5-718012: Sent HELLO request to IP_address`

说明：Firepower 威胁防御设备已将 hello 请求消息传输到负载均衡对等体。

建议的操作：无需执行任何操作。

718013

错误消息：`%ASA-6-718013: Peer IP_addressis not answering HELLO`

说明：负载均衡对等体未在应答 hello 请求消息。

建议的操作：检查负载均衡 SSF 对等体和网络连接的状态。

718014

错误消息： `%ASA-5-718014: Master peer IP_addressis not answering HELLO`

说明： 负载均衡主对等体未在应答 hello 请求消息。

建议的操作： 检查负载均衡 SSF 主对等体和网络连接的状态。

718015

错误消息： `%ASA-5-718015: Received HELLO request from IP_address`

说明： Firepower 威胁防御设备从负载均衡对等体收到 hello 请求消息。

建议的操作： 无需执行任何操作。

718016

错误消息： `%ASA-5-718016: Received HELLO response from IP_address`

说明： Firepower 威胁防御设备从负载均衡对等体收到 Hello 响应数据包。

建议的操作： 无需执行任何操作。

718017

错误消息： `%ASA-7-718017: Got timeout for unknown peer IP_addressmsg type message_type`

说明： Firepower威胁防御设备已处理未知对等体的超时问题。由于此对等体可能已从活动列表中删除，因此忽略了该消息。

建议的操作： 如果该消息仍然存在或与不良行为相关，请检查负载均衡对等体并验证所有对等体都已正确配置。

718018

错误消息： `%ASA-7-718018: Send KEEPALIVE request failure to IP_address`

说明： 在尝试将保持连接请求消息发送到其中一个负载均衡对等体时发生错误。这可能表示网络问题或内部软件错误。

建议的操作： 检查Firepower威胁防御设备上基于网络的配置，并验证接口是否处于活动状态且协议数据流经 Firepower 威胁防御设备。如果问题仍然存在，请联系思科 TAC。

718019

错误消息： `%ASA-7-718019: Sent KEEPALIVE request to IP_address`

说明： Firepower 威胁防御设备已将保持连接请求消息传输到负载均衡对等体。

建议的操作： 无需执行任何操作。

718020

错误消息： `%ASA-7-718020: Send KEEPALIVE response failure to IP_address`

说明： 在尝试将保持连接响应消息发送到其中一个负载均衡对等体时发生错误。这可能表示网络问题或内部软件错误。

建议的操作： 检查Firepower威胁防御设备上基于网络的配置，并验证接口是否处于活动状态且协议数据流经 Firepower 威胁防御设备。如果问题仍然存在，请联系思科 TAC。

718021

错误消息： `%ASA-7-718021: Sent KEEPALIVE response to IP_address`

说明： Firepower 威胁防御设备已将保持连接响应消息传输到负载均衡对等体。

建议的操作： 无需执行任何操作。

718022

错误消息： `%ASA-7-718022: Received KEEPALIVE request from IP_address`

说明： Firepower 威胁防御设备从负载均衡对等体收到保持连接请求消息。

建议的操作： 无需执行任何操作。

718023

错误消息： `%ASA-7-718023: Received KEEPALIVE response from IP_address`

说明： Firepower 威胁防御设备从负载均衡对等体收到保持连接响应消息。

建议的操作： 无需执行任何操作。

718024

错误消息： `%ASA-5-718024: Send CFG UPDATE failure to IP_address`

说明： 在尝试将配置更新消息发送到其中一个负载均衡对等体时发生错误。这可能表示网络问题或内部软件错误。

建议的操作： 检查Firepower威胁防御设备上基于网络的配置，并验证接口是否处于活动状态且协议数据流经 Firepower 威胁防御设备。如果问题仍然存在，请联系思科 TAC。

718025

错误消息： `%ASA-7-718025: Sent CFG UPDATE to IP_address`

说明： Firepower 威胁防御设备已将配置更新消息传输到负载均衡对等体。

建议的操作： 无需执行任何操作。

718026

错误消息： `%ASA-7-718026: Received CFG UPDATE from IP_address`

说明： Firepower 威胁防御设备从负载均衡对等体收到配置更新消息。

建议的操作： 无需执行任何操作。

718027

错误消息： `%ASA-6-718027: Received unexpected KEEPALIVE request from IP_address`

说明： Firepower 威胁防御设备从负载均衡对等体收到意外的保持连接请求消息。

建议的操作： 如果问题仍然存在或与不良行为相关，请验证是否已正确配置并发现所有负载均衡对等体。

718028

错误消息： `%ASA-5-718028: Send OOS indicator failure to IP_address`

说明： 在尝试将OOS指示器消息发送到其中一个负载均衡对等体时发生错误。这可能表示网络问题或内部软件错误。

建议的操作： 检查Firepower威胁防御设备上基于网络的配置，并验证接口是否处于活动状态且协议数据流经 Firepower 威胁防御设备。如果问题仍然存在，请联系思科 TAC。

718029

错误消息： `%ASA-7-718029: Sent OOS indicator to IP_address`

说明： Firepower 威胁防御设备已将 OOS 指示器消息传输到负载均衡对等体。

建议的操作： 无需执行任何操作。

718030

错误消息： `%ASA-6-718030: Received planned OOS from IP_address`

说明： Firepower 威胁防御设备从负载均衡对等体收到计划的 OOS 消息。

建议的操作： 无需执行任何操作。

718031

错误消息： `%ASA-5-718031: Received OOS obituary for IP_address`

说明： Firepower 威胁防御设备从负载均衡对等体收到 OOS 失效消息。

建议的操作： 无需执行任何操作。

718032

错误消息： `%ASA-5-718032: Received OOS indicator from IP_address`

说明： Firepower 威胁防御设备从负载均衡对等体收到 OOS 指示器消息。

建议的操作： 无需执行任何操作。

718033

错误消息： `%ASA-5-718033: Send TOPOLOGY indicator failure to IP_address`

说明： 在尝试将拓扑指示器消息发送到其中一个负载均衡对等体时发生错误。这可能表示网络问题或内部软件错误。

建议的操作： 检查 Firepower 威胁防御设备上基于网络的配置。验证接口是否处于活动状态，以及协议数据是否流经 Firepower 威胁防御设备。如果问题仍然存在，请联系思科 TAC。

718034

错误消息： `%ASA-7-718034: Sent TOPOLOGY indicator to IP_address`

说明： Firepower 威胁防御设备已将拓扑指示器消息发送到负载均衡对等体。

建议的操作： 无需执行任何操作。

718035

错误消息： `%ASA-7-718035: Received TOPOLOGY indicator from IP_address`

说明： Firepower 威胁防御设备从负载均衡对等体收到拓扑指示器消息。

建议的操作： 无需执行任何操作。

718036

错误消息： `%ASA-7-718036: Process timeout for req-type type_value , exid exchange_ID , peer IP_address`

说明： Firepower 威胁防御设备已处理对等体超时问题。

建议的操作： 验证对等体是否应已超时。如果未超时，请检查对等体与 Firepower 威胁防御设备之间的负载均衡对等体配置和网络连接。

718037

错误消息： `%ASA-6-718037: Master processed number_of_timeouts timeouts`

说明： 承担主角色的 Firepower 威胁防御设备已处理指定数量的对等体超时。

建议的操作：验证超时是否合法。如果不合法，请检查对等体与Firepower威胁防御设备之间的对等体负载均衡配置和网络连接。

718038

错误消息：`%ASA-6-718038: Slave processed number_of_timeouts timeouts`

说明：承担从属角色的 Firepower 威胁防御设备已处理指定数量的对等体超时。

建议的操作：验证超时是否合法。如果不合法，请检查对等体与Firepower威胁防御设备之间的对等体负载均衡配置和网络连接。

718039

错误消息：`%ASA-6-718039: Process dead peer IP_address`

说明：Firepower 威胁防御设备已检测到失效对等体。

建议的操作：验证失效对等体检测是否合法。如果不合法，请检查对等体与Firepower威胁防御设备之间的对等体负载均衡配置和网络连接。

718040

错误消息：`%ASA-6-718040: Timed-out exchange ID exchange_ID not found`

说明：Firepower 威胁防御设备检测到失效对等体，但未识别交换 ID。

建议的操作：无需执行任何操作。

718041

错误消息：`%ASA-7-718041: Timeout [msgType=type ] processed with no callback`

说明：Firepower 威胁防御设备检测到失效对等体，但在处理中未使用回拨。

建议的操作：无需执行任何操作。

718042

错误消息：`%ASA-5-718042: Unable to ARP for IP_address`

说明：Firepower 威胁防御设备在尝试访问对等体时遇到 ARP 失败。

建议的操作：验证网络是否正常运行且所有对等体都可以相互通信。

718043

错误消息：`%ASA-5-718043: Updating/removing duplicate peer entry IP_address`

说明：Firepower 威胁防御设备找到并正在删除重复对等体条目。

建议的操作：无需执行任何操作。

718044

错误消息： `%ASA-5-718044: Deleted peer IP_address`

说明：Firepower 威胁防御设备正在删除负载均衡对等体。

建议的操作：无需执行任何操作。

718045

错误消息：`%ASA-5-718045: Created peer IP_address`

说明：Firepower 威胁防御设备已检测到负载均衡对等体。

建议的操作：无需执行任何操作。

718046

错误消息：`%ASA-7-718046: Create group policy policy_name`

说明：Firepower 威胁防御设备已创建组策略来与负载均衡对等体安全地通信。

建议的操作：无需执行任何操作。

718047

错误消息：`%ASA-7-718047: Fail to create group policy policy_name`

说明：Firepower 威胁防御设备在尝试创建组策略以保护负载均衡对等体之间的通信时失败。

建议的操作：验证负载均衡配置是否正确。

718048

错误消息：`%ASA-5-718048: Create of secure tunnel failure for peer IP_address`

说明：Firepower 威胁防御设备在尝试建立通向负载均衡对等体的 IPsec 隧道时遇到失败。

建议的操作：验证负载均衡配置是否正确以及网络是否正常运行。

718049

错误消息：`%ASA-7-718049: Created secure tunnel to peer IP_address`

说明：Firepower 威胁防御设备已成功建立通向负载均衡对等体的 IPsec 隧道。

建议的操作：无需执行任何操作。

718050

错误消息： `%ASA-5-718050: Delete of secure tunnel failure for peer IP_address`

说明： Firepower 威胁防御设备在尝试终止通向负载均衡对等体的 IPsec 隧道时遇到失败。

建议的操作： 验证负载均衡配置是否正确以及网络是否正常运行。

718051

错误消息： `%ASA-6-718051: Deleted secure tunnel to peer IP_address`

说明： Firepower 威胁防御设备已成功终止通向负载均衡对等体的 IPsec 隧道。

建议的操作： 无需执行任何操作。

718052

错误消息： `%ASA-5-718052: Received GRAT-ARP from duplicate master MAC_address`

说明： Firepower 威胁防御设备从重复的主对等体收到免费 ARP。

建议的操作： 检查负载均衡配置并验证网络是否正常运行。

718053

错误消息： `%ASA-5-718053: Detected duplicate master, mastership stolen MAC_address`

说明： Firepower 威胁防御设备检测到重复的主对等体和盗用的主对等体。

建议的操作： 检查负载均衡配置并验证网络是否正常运行。

718054

错误消息： `%ASA-5-718054: Detected duplicate master MAC_addressand going to SLAVE`

说明： Firepower 威胁防御设备检测到重复的主对等体并正在切换到从属模式。

建议的操作： 检查负载均衡配置并验证网络是否正常运行。

718055

错误消息： `%ASA-5-718055: Detected duplicate master MAC_addressand staying MASTER`

说明： Firepower 威胁防御设备检测到重复的主对等体并保持处于从属模式。

建议的操作： 检查负载均衡配置并验证网络是否正常运行。

718056

错误消息： `%ASA-7-718056: Deleted Master peer, IP IP_address`

说明：Firepower 威胁防御设备已从其内部表中删除负载均衡主对等体。

建议的操作：无需执行任何操作。

718057

错误消息：`%ASA-5-718057: Queue send failure from ISR, msg type failure_code`

说明：在尝试根据中断服务路由将 VPN 负载均衡队列中的消息排队时发生内部软件错误。

建议的操作：这通常是良性情况。如果问题仍然存在，请联系思科 TAC。

718058

错误消息：`%ASA-7-718058: State machine return code: action_routine , return_code`

说明：正在跟踪属于负载均衡有限状态机的操作例程的返回代码。

建议的操作：无需执行任何操作。

718059

错误消息：`%ASA-7-718059: State machine function trace: state=state_name , event=event_name , func=action_routine`

说明：正在跟踪负载均衡有限状态机的事件和状态。

建议的操作：无需执行任何操作。

718060

错误消息：`%ASA-5-718060: Inbound socket select fail: context=context_ID.`

说明：套接字选择调用返回了错误，因此无法读取套接字。这可能表示存在内部软件错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

718061

错误消息：`%ASA-5-718061: Inbound socket read fail: context=context_ID .`

说明：通过所选择的调用检测到数据之后套接字读取失败。这可能表示存在内部软件错误。

建议的操作：如果问题仍然存在，请联系思科 TAC。

718062

错误消息：`%ASA-5-718062: Inbound thread is awake (context=context_ID ).`

说明：负载均衡进程被唤醒并开始处理。

建议的操作：无需执行任何操作。

718063

错误消息：`%ASA-5-718063: Interface interface_name is down.`

说明：负载均衡进程发现此接口处于关闭状态。

建议的操作：检查接口配置，以确保此接口运行正常。

718064

错误消息：`%ASA-5-718064: Admin. interface interface_name is down.`

说明：负载均衡进程发现管理接口处于关闭状态。

建议的操作：检查管理接口配置，以确保此接口运行正常。

718065

错误消息：`%ASA-5-718065: Cannot continue to run (public=up /down , private=up /down , enable=LB_state , master=IP_address , session=Enable /Disable ).`

说明：负载均衡进程无法运行，因为不满足所有前提条件。前提条件是两个活动接口和负载均衡均已启用。

建议的操作：检查接口配置，以确保至少两个接口处于正常运行状态，并且负载均衡功能已启用。

718066

错误消息：`%ASA-5-718066: Cannot add secondary address to interface interface_name , ip IP_address .`

说明：负载均衡需要将辅助地址添加到外部接口。在添加此辅助地址过程中发生故障。

建议的操作：检查用作辅助地址的地址并确保其有效且是唯一的。检查外部接口的配置。

718067

错误消息：`%ASA-5-718067: Cannot delete secondary address to interface interface_name , ip IP_address .`

说明：辅助地址删除失败，这可能表示存在寻址问题或内部软件错误。

建议的操作：检查外部接口的寻址信息，并确保辅助地址有效且是唯一的。如果问题仍然存在，请联系思科 TAC。

718068

错误消息：`%ASA-5-718068: Start VPN Load Balancing in context context_ID .`

说明：负载均衡进程已启动并完成初始化。

建议的操作：无需执行任何操作。

718069

错误消息：`%ASA-5-718069: Stop VPN Load Balancing in context context_ID .`

说明：负载均衡进程已停止。

建议的操作：无需执行任何操作。

718070

错误消息：`%ASA-5-718070: Reset VPN Load Balancing in context context_ID .`

说明：LB 进程已重置。

建议的操作：无需执行任何操作。

718071

错误消息：`%ASA-5-718071: Terminate VPN Load Balancing in context context_ID .`

说明：LB 进程已终止。

建议的操作：无需执行任何操作。

718072

错误消息：`%ASA-5-718072: Becoming master of Load Balancing in context context_ID .`

说明：Firepower 威胁防御设备已成为 LB 主设备。

建议的操作：无需执行任何操作。

718073

错误消息：`%ASA-5-718073: Becoming slave of Load Balancing in context context_ID .`

说明：Firepower 威胁防御设备已成为 LB 从属设备。

建议的操作：无需执行任何操作。

718074

错误消息：`%ASA-5-718074: Fail to create access list for peer context_ID .`

说明：ACL 用于创建 LB 对等体可以通信的安全隧道。Firepower 威胁防御设备无法创建其中的一个 ACL。这可能表示存在寻址问题或内部软件问题。

建议的操作：检查所有对等体上的内部接口的寻址信息，并确保正确发现所有对等体。如果问题仍然存在，请联系思科 TAC。

718075

错误消息：`%ASA-5-718075: Peer IP_address access list not set.`

说明：删除安全隧道时，Firepower 威胁防御设备检测到没有关联 ACL 的对等条目。

建议的操作：无需执行任何操作。

718076

错误消息：`%ASA-5-718076: Fail to create tunnel group for peer IP_address .`

说明：Firepower 威胁防御设备在尝试创建隧道组以确保负载均衡对等体之间的通信时发生故障。

建议的操作：验证负载均衡配置是否正确。

718077

错误消息：`%ASA-5-718077: Fail to delete tunnel group for peer IP_address .`

说明：Firepower 威胁防御设备在尝试删除用于确保负载均衡对等体之间的通信的隧道组时发生故障。

建议的操作：无需执行任何操作。

718078

错误消息：`%ASA-5-718078: Fail to create crypto map for peer IP_address .`

说明：Firepower威胁防御设备在尝试创建加密映射以确保负载均衡对等体之间的通信时发生故障。

建议的操作：验证负载均衡配置是否正确。

718079

错误消息：`%ASA-5-718079: Fail to delete crypto map for peer IP_address .`

说明：Firepower威胁防御设备在尝试删除用于确保负载均衡对等体之间的通信的加密映射时发生故障。

建议的操作：无需执行任何操作。

718080

错误消息：`%ASA-5-718080: Fail to create crypto policy for peer IP_address .`

说明：Firepower威胁防御设备在尝试创建转换集以确保负载均衡对等体之间的通信时发生故障。这可能表示存在内部软件问题。

建议的操作：如果问题仍然存在，请联系思科 TAC。

718081

错误消息：`%ASA-5-718081: Fail to delete crypto policy for peer IP_address .`

说明：Firepower 威胁防御设备在尝试删除用于确保负载均衡对等体之间的通信的转换集时发生故障。

建议的操作：无需执行任何操作。

718082

错误消息：`%ASA-5-718082: Fail to create crypto ipsec for peer IP_address .`

说明：启用 VPN 负载均衡的集群加密后，VPN 负载均衡设备将为负载均衡集群中的每个其他设备创建一组站点到站点隧道。对于每个隧道，将动态创建一组加密参数（访问列表、加密映射和转换集）。一个或多个加密参数创建或配置失败。

- **IP_address** - 远程对等体的 IP 地址

建议的操作：检查创建失败的加密参数类型特定的其他条目消息。

718083

错误消息：`%ASA-5-718083: Fail to delete crypto ipsec for peer IP_address .`

说明：从集群中删除本地 VPN 负载均衡设备后，加密参数将被删除。一个或多个加密参数删除失败。

- **IP_address** - 远程对等体的 IP 地址

建议的操作：检查删除失败的加密参数类型特定的其他条目消息。

718084

错误消息：`%ASA-5-718084: Public/cluster IP not on the same subnet: public IP_address , mask netmask , cluster IP_address`

说明：集群 IP 地址与 Firepower 威胁防御设备外部接口不在同一网络中。

建议的操作：确保两个集群（或虚拟）IP 地址与外部接口地址位于同一网络中。

718085

错误消息：`%ASA-5-718085: Interface interface_name has no IP address defined.`

说明：接口没有配置 IP 地址。

建议的操作：配置接口的 IP 地址。

718086

错误消息：`%ASA-5-718086: Fail to install LB NP rules: type rule_type , dst interface_name , port port .`

说明：Firepower 威胁防御设备在尝试创建 SoftNP ACL 规则以确保负载均衡对等体之间的通信时发生故障。这可能表示存在内部软件问题。

建议的操作：如果问题仍然存在，请联系思科 TAC。

718087

错误消息：`%ASA-5-718087: Fail to delete LB NP rules: type rule_type , rule rule_ID .`

说明：Firepower 威胁防御设备在尝试删除用于确保负载均衡对等体之间的通信的 SoftNP ACL 规则时发生故障。

建议的操作：无需执行任何操作。

718088

错误消息：`%ASA-7-718088: Possible VPN LB misconfiguration.Offending device MAC MAC_address .`

说明：存在重复的主设备表示其中一个负载均衡对等体可能配置错误。

建议的操作：检查所有对等体上的负载均衡配置，但需特别注意已识别的对等体。

719001

错误消息：`%ASA-6-719001: Email Proxy session could not be established: session limit of maximum_sessions has been reached.`

说明：由于已达到最大会话限制，无法建立传入邮件代理会话。

- **maximum_sessions** - 最大会话数

建议的操作：无需执行任何操作。

719002

错误消息：`%ASA-3-719002: Email Proxy session pointer from source_address has been terminated due to reason error.`

说明：由于发生错误，会话已终止。可能的错误包括无法将会话添加到会话数据库、无法分配内存以及无法将数据写入通道。

- **pointer** - 会话指针
- **source_address** - 邮件代理客户端 IP 地址

- **reason** - 错误类型

建议的操作：无需执行任何操作。

719003

错误消息：`%ASA-6-719003: Email Proxy session pointer resources have been freed for source_address .`

说明：分配的动态会话结构已释放，并在会话终止后设置为了 NULL。

- **pointer** - 会话指针
- **source_address** - 邮件代理客户端 IP 地址

建议的操作：无需执行任何操作。

719004

错误消息：`%ASA-6-719004: Email Proxy session pointer has been successfully established for source_address .`

说明：已建立新的传入邮件客户端会话。

建议的操作：无需执行任何操作。

719005

错误消息：`%ASA-7-719005: FSM NAME has been created using protocol for session pointer from source_address .`

说明：已为传入的新会话创建 FSM。

- 名称 - 此会话的 FSM 实例名称
- **协议** - 邮件协议类型（例如，POP3、IMAP 和 SMTP）
- **pointer** - 会话指针
- **source_address** - 邮件代理客户端 IP 地址

建议的操作：无需执行任何操作。

719006

错误消息：`%ASA-7-719006: Email Proxy session pointer has timed out for source_address because of network congestion.`

说明：发生网络堵塞，数据无法发送到邮件客户端或邮件服务器。这种情况会启动块计时器。块计时器超时后，会话过期。

- **pointer** - 会话指针
- **source_address** - 邮件代理客户端 IP 地址

建议的操作：几分钟后重试此操作。

719007

错误消息：`%ASA-7-719007: Email Proxy session pointer cannot be found for source_address .`

说明：无法在会话数据库中找到匹配的会话。会话指针已损坏。

- **pointer** - 会话指针
- **source_address** - 邮件代理客户端 IP 地址

建议的操作：无需执行任何操作。

719008

错误消息：`%ASA-3-719008: Email Proxy service is shutting down.`

说明：邮件代理被禁用。系统将清理所有资源，并终止所有线程。

建议的操作：无需执行任何操作。

719009

错误消息：`%ASA-7-719009: Email Proxy service is starting.`

说明：邮件代理已启用。

建议的操作：无需执行任何操作。

719010

错误消息：`%ASA-6-719010: protocol Email Proxy feature is disabled on interface interface_name .`

说明：从 CLI 调用的特定入口点禁用了邮件代理功能。这是用户的主关闭交换机。当所有接口的所有协议都关闭时，将调用主关闭例程来清理全局资源和线程。

- **protocol** - 邮件代理协议类型（例如，POP3、IMAP 和 SMTP）
- **interface_name** - Firepower 威胁防御接口名称

建议的操作：无需执行任何操作。

719011

错误消息：`%ASA-6-719011: Protocol Email Proxy feature is enabled on interface interface_name .`

说明：从 CLI 调用的特定入口点启用了邮件代理功能。这是用户的主开启交换机。首次使用时，将调用主启动例程来分配全局资源和线程。后续调用只需启动特定协议的侦听线程。

- **protocol** - 邮件代理协议类型（例如，POP3、IMAP 和 SMTP）
- **interface_name** - Firepower 威胁防御接口名称

建议的操作：无需执行任何操作。

719012

错误消息：`%ASA-6-719012: Email Proxy server listening on port port for mail protocol protocol .`

说明：在所配置的端口上为特定协议打开了侦听通道，并已将该侦听通道添加到 TCP 选择组。

- **port** - 所配置的端口号
- **protocol** - 邮件代理协议类型（例如，POP3、IMAP 和 SMTP）

建议的操作：无需执行任何操作。

719013

错误消息：`%ASA-6-719013: Email Proxy server closing port port for mail protocol protocol .`

说明：在所配置的端口上为特定协议关闭了侦听通道，并已将该侦听通道从 TCP 选择组中删除。

- **port** - 所配置的端口号
- **protocol** - 邮件代理协议类型（例如，POP3、IMAP 和 SMTP）

建议的操作：无需执行任何操作。

719014

错误消息：`%ASA-5-719014: Email Proxy is changing listen port from old_port to new_port for mail protocol protocol .`

说明：指定协议的侦听端口中发出更改信号。此端口的所有已启用接口均已关闭其侦听通道并已重新启动新端口的侦听。从 CLI 调用此操作。

- **old_port** - 之前配置的端口号
- **new_port** - 新配置的端口号
- **protocol** - 邮件代理协议类型（例如，POP3、IMAP 和 SMTP）

建议的操作：无需执行任何操作。

719015

错误消息：`%ASA-7-719015: Parsed emailproxy session pointer from source_address username: mailuser = mail_user , vpnuser = VPN_user , mailserver = server`

说明：以 vpnuser（名称分隔符）mailuser（服务器分隔符）邮件服务器的格式（例如：xxx：yyy@cisco.com）从客户端接收用户名字符串。名称分隔符为可选项。不存在名称分隔符时，VPN用户名和邮件用户名相同。服务器分隔符为可选项。如果不存在，将使用配置的默认邮件服务器。

- **pointer** - 会话指针
- **source_address** - 邮件代理客户端 IP 地址

- mail_user - 邮件账户用户名
- **VPN_user** - WebVPN 用户名
- **server** - 邮件服务器

建议的操作：无需执行任何操作。

719016

错误消息：`%ASA-7-719016: Parsed emailproxy session pointer from source_address password: mailpass = ******, vpnpass= ******`

说明：以 vpnpass（名称分隔符）mailpass 的格式（例如 xxx:yyy）从客户端接收密码字符串。名称分隔符为可选项。如果不存在，VPN 密码和邮件密码相同。

- **pointer** - 会话指针
- **source_address** - 邮件代理客户端 IP 地址

建议的操作：无需执行任何操作。

719017

错误消息：`%ASA-6-719017: WebVPN user: vpnuser invalid dynamic ACL.`

说明：WebVPN 会话已中止，因为 ACL 未能解析此用户。ACL 决定用户对邮件账户访问的限制。ACL 是从 AAA 服务器下载的。由于此错误，继续登录不再安全。

- **vpnuser** - WebVPN 用户名

建议的操作：检查 AAA 服务器并修复此用户的动态 ACL。

719018

错误消息：`%ASA-6-719018: WebVPN user: vpnuser ACL ID acl_ID not found`

说明：无法在本地维护的 ACL 列表中找到 ACL。ACL 决定用户对邮件账户访问的限制。ACL 在本地进行配置。由于此错误，您无权继续操作。

- **vpnuser** - WebVPN 用户名
- **acl_ID** - 本地配置的 ACL 标识字符串

建议的操作：检查本地 ACL 配置。

719019

错误消息：`%ASA-6-719019: WebVPN user: vpnuser authorization failed.`

说明：ACL 决定用户对邮件账户访问的限制。由于授权检查失败，用户无法访问邮件账户。

- **vpnuser** - WebVPN 用户名

建议的操作：无需执行任何操作。

719020

错误消息： `%ASA-6-719020: WebVPN user vpnuser authorization completed successfully.`

说明： ACL 决定用户对邮件账户访问的限制。用户有权访问邮件账户。

- **vpnuser** - WebVPN 用户名

建议的操作： 无需执行任何操作。

719021

错误消息： `%ASA-6-719021: WebVPN user: vpnuser is not checked against ACL.`

说明： ACL 决定用户对邮件账户访问的限制。未启用使用 ACL 进行的授权检查。

- **vpnuser** - WebVPN 用户名

建议的操作： 如有必要，启用 ACL 检查功能。

719022

错误消息： `%ASA-6-719022: WebVPN user vpnuser has been authenticated.`

说明： 用户名由 AAA 服务器进行身份验证。

- **vpnuser** - WebVPN 用户名

建议的操作： 无需执行任何操作。

719023

错误消息： `%ASA-6-719023: WebVPN user vpnuser has not been successfully authenticated.Access denied.`

说明： 用户名被 AAA 服务器拒绝。会话将被终止。不允许用户访问邮件账户。

- **vpnuser** - WebVPN 用户名

建议的操作： 无需执行任何操作。

719024

错误消息： `%ASA-6-719024: Email Proxy piggyback auth fail: session = pointer user=vpnuser addr=source_address`

说明： 捎带身份验证使用已建立的 WebVPN 会话来验证 WebVPN 会话数据库中的用户名和 IP 地址是否匹配。这基于以下假设：WebVPN 会话和邮件代理会话由同一个用户发起，且已建立 WebVPN 会话。由于身份验证失败，会话将被终止。不允许用户访问邮件账户。

- **pointer** - 会话指针
- **vpnuser** - WebVPN 用户名

- **source_address** - 客户端 IP 地址

建议的操作：无需执行任何操作。

719025

错误消息：`%ASA-6-719025: Email Proxy DNS name resolution failed for hostname .`

说明：无法使用 IP 地址解析主机名，主机名无效或者没有可用的 DNS 服务器。

- **hostname** - 需要解析的主机名

建议的操作：检查 DNS 服务器的可用性以及所配置的邮件服务器名称是否有效。

719026

错误消息：`%ASA-6-719026: Email Proxy DNS name hostname resolved to IP_address .`

说明：已使用 IP 地址成功解析主机名。

- **hostname** - 需要解析的主机名
- **IP_address** - 从已配置的邮件服务器名称中解析的 IP 地址

建议的操作：无需执行任何操作。

ID 介于 720001 到 721019 之间的消息

本部分包括 ID 介于 720001 到 721019 之间的消息。

720001

错误消息：`%ASA-4-720001: (VPN-unit ) Failed to initialize with Chunk Manager.`

说明：VPN 故障切换子系统未能使用内存缓冲区管理子系统进行初始化。发生了系统范围的问题，且 VPN 故障切换子系统无法启动。

- **unit** - 主设备或辅助设备

建议的操作：检查消息以确定是否有任何系统级初始化问题的迹象。

720002

错误消息：`%ASA-6-720002: (VPN-unit ) Starting VPN Stateful Failover Subsystem...`

说明：VPN 故障切换子系统正在启动和引导。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720003

错误消息：`%ASA-6-720003: (VPN-unit ) Initialization of VPN Stateful Failover Component completed successfully`

说明：VPN 故障切换子系统初始化已在引导时完成。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720004

错误消息：`%ASA-6-720004: (VPN-unit ) VPN failover main thread started.`

说明：VPN 故障切换主处理线程在引导时启动。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720005

错误消息：`%ASA-6-720005: (VPN-unit ) VPN failover timer thread started.`

说明：VPN 故障切换计时器处理线程在引导时启动。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720006

错误消息：`%ASA-6-720006: (VPN-unit ) VPN failover sync thread started.`

说明：VPN 故障切换批量同步处理线程在引导时启动。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720007

错误消息：`%ASA-4-720007: (VPN-unit ) Failed to allocate chunk from Chunk Manager.`

说明：预分配的内存缓冲区集已用完。Firepower 威胁防御设备存在资源问题。处理消息过多时，Firepower 威胁防御设备可能处于高负载状态。

- **unit** - 主设备或辅助设备

建议的操作：稍后当VPN故障切换子系统处理未完成的消息并释放先前分配的内存后，可以改善这种情况。

720008

错误消息： `%ASA-4-720008: (VPN-unit ) Failed to register to High Availability Framework.`

说明： VPN故障切换子系统未能注册到核心故障切换子系统。VPN故障切换子系统无法启动，这可能是由其他子系统的初始化问题导致的。

- **unit** - 主设备或辅助设备

建议的操作： 搜索消息以确定是否有系统范围初始化问题的迹象。

720009

错误消息： `%ASA-4-720009: (VPN-unit ) Failed to create version control block.`

说明： VPN故障切换子系统未能创建版本控制块。VPN故障切换子系统需要执行此步骤，才能找出当前版本的向后兼容固件版本。VPN 故障切换子系统无法启动，这可能是由其他子系统的初始化问题导致的。

- **unit** - 主设备或辅助设备

建议的操作： 搜索消息以确定是否有系统范围初始化问题的迹象。

720010

错误消息： `%ASA-6-720010: (VPN-unit ) VPN failover client is being disabled`

说明： 操作人员在未定义故障切换密钥的情况下启用了故障切换。要使用VPN故障切换，必须定义故障切换密钥。

- **unit** - 主设备或辅助设备

建议的操作： 使用 **failover key** 命令定义主用设备和备用设备之间的共享密钥。

720011

错误消息： `%ASA-4-720011: (VPN-unit ) Failed to allocate memory`

说明： VPN 故障切换子系统无法分配内存缓冲区，这表示存在系统范围的资源问题。Firepower 威胁防御设备可能处于高负载状态。

- **unit** - 主设备或辅助设备

建议的操作： 稍后通过减少传入流量来降低Firepower威胁防御设备的负载时，可以改善这种情况。通过减少传入流量，将提供分配用于处理现有工作负载的内存，Firepower威胁防御设备可以恢复正常运行。

720012

错误消息： `%ASA-6-720012: (VPN-unit ) Failed to update IPsec failover runtime data on the standby unit.`

说明：VPN 故障切换子系统无法更新与 IPsec 相关的运行时数据，因为已在备用设备上删除相应的 IPsec 隧道。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720013

错误消息：`%ASA-4-720013: (VPN-unit ) Failed to insert certificate in trustpoint trustpoint_name`

说明：VPN 故障切换子系统尝试将证书插入信任点中。

- **unit** - 主设备或辅助设备
- **trustpoint_name** - 信任点的名称

建议的操作：检查证书内容以确定其是否无效。

720014

错误消息：`%ASA-6-720014: (VPN-unit ) Phase 2 connection entry (msg_id=message_number , my cookie=mine , his cookie=his ) contains no SA list.`

说明：没有安全关联链接到第 2 阶段连接条目。

- **unit** - 主设备或辅助设备
- **message_number** - 第 2 阶段连接条目的消息 ID
- **mine** - 我的第 1 阶段 Cookie
- **his** - 对等体的第 1 阶段 Cookie

建议的操作：无需执行任何操作。

720015

错误消息：`%ASA-6-720015: (VPN-unit ) Cannot found Phase 1 SA for Phase 2 connection entry (msg_id=message_number ,my cookie=mine , his cookie=his ).`

说明：找不到给定第 2 阶段连接条目对应的第 1 阶段安全关联。

- **unit** - 主设备或辅助设备
- **message_number** - 第 2 阶段连接条目的消息 ID
- **mine** - 我的第 1 阶段 Cookie
- **his** - 对等体的第 1 阶段 Cookie

建议的操作：无需执行任何操作。

720016

错误消息：`%ASA-5-720016: (VPN-unit) Failed to initialize default timer #index .`

说明：VPN 故障切换子系统未能初始化给定的计时器事件。VPN 故障切换子系统无法在引导时启动。

- **unit** - 主设备或辅助设备
- **index** - 计时器事件的内部索引

建议的操作：搜索消息以确定是否有系统范围初始化问题的迹象。

720017

错误消息：`%ASA-5-720017: (VPN-unit ) Failed to update LB runtime data`

说明：VPN 故障切换子系统未能更新 VPN 负载均衡运行时数据。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720018

错误消息：`%ASA-5-720018: (VPN-unit ) Failed to get a buffer from the underlying core high availability subsystem.Error code code.`

说明：Firepower 威胁防御设备可能处于高负载状态。VPN 故障切换子系统未能获取故障切换缓冲区。

- **unit** - 主设备或辅助设备
- **code** - 高可用性子系统返回的错误代码

建议的操作：减少传入流量以改善当前负载状况。随着传入流量的减少，Firepower 威胁防御设备将释放分配用于处理传入负载的内存。

720019

错误消息：`%ASA-5-720019: (VPN-unit ) Failed to update cTCP statistics.`

说明：VPN 故障切换子系统未能更新 IPsec/cTCP 相关统计信息。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。更新会定期发送，因此应使用下一条更新消息更新备用设备 IPsec/cTCP 统计信息。

720020

错误消息：`%ASA-5-720020: (VPN-unit ) Failed to send type timer message.`

说明：VPN 故障切换子系统未能将定期计时器消息发送到备用设备。

- **unit** - 主设备或辅助设备
- **type** - 计时器消息的类型。

建议的操作：无需执行任何操作。定期计时器消息将在下一次超时期间重新发送。

720021

错误消息：`%ASA-5-720021: (VPN-unit ) HA non-block send failed for peer msg message_number .HA error code .`

说明：VPN 故障切换子系统未能发送非块消息。这是一种由 Firepower 威胁防御设备处于负载状态或资源不足导致的暂时情况。

- **unit** - 主设备或辅助设备
- **message_number** - 对等消息的 ID 编号
- **code** - 错误返回代码

建议的操作：随着 Firepower 威胁防御设备可用的资源不断增加，这种情况将会得到改善。

720022

错误消息：`%ASA-4-720022: (VPN-unit ) Cannot find trustpoint trustpoint`

说明：VPN 故障切换子系统尝试按名称查找信任点时发生错误。

- **unit** - 主设备或辅助设备
- **trustpoint** - 信任点的名称。

建议的操作：信任点可能已被操作人员删除。

720023

错误消息：`%ASA-6-720023: (VPN-unit ) HA status callback: Peer is not present.`

说明：当本地 Firepower 威胁防御设备检测到对等体可用或不可用时，核心故障切换子系统将通知 VPN 故障切换子系统。

- **unit** - 主设备或辅助设备
- **not** -“不”或留空

建议的操作：无需执行任何操作。

720024

错误消息：`%ASA-6-720024: (VPN-unit ) HA status callback: Control channel is status .`

说明：故障切换控制通道为打开或关闭状态。故障切换控制通道由 **failover link** 和 **show failover** 命令定义，这表示故障切换链路通道为打开还是关闭状态。

- **unit** - 主设备或辅助设备
- **status** - 打开或关闭

建议的操作：无需执行任何操作。

720025

错误消息： `%ASA-6-720025: (VPN-unit ) HA status callback: Data channel is status .`

说明： 故障切换数据通道为打开或关闭状态。

- **unit** - 主设备或辅助设备
- **status** - 打开或关闭

建议的操作： 无需执行任何操作。

720026

错误消息： `%ASA-6-720026: (VPN-unit ) HA status callback: Current progression is being aborted.`

说明： 在故障切换对等体同意该角色（主用或备用）之前，操作人员中止了当前故障切换进程，或者发生了其他外部情况，导致了当前故障切换进程中止。例如，在协商期间在备用设备上输入**failover active** 命令时，或在重新引导主用设备时。

- **unit** - 主设备或辅助设备

建议的操作： 无需执行任何操作。

720027

错误消息： `%ASA-6-720027: (VPN-unit ) HA status callback: My state state .`

说明： 本地故障切换设备的状态发生更改。

- **unit** - 主设备或辅助设备
- **state** - 本地故障切换设备的当前状态

建议的操作： 无需执行任何操作。

720028

错误消息： `%ASA-6-720028: (VPN-unit ) HA status callback: Peer state state .`

说明： 报告故障切换对等体的当前状态。

- **unit** - 主设备或辅助设备
- **state** - 故障切换对等体的当前状态

建议的操作： 无需执行任何操作。

720029

错误消息： `%ASA-6-720029: (VPN-unit ) HA status callback: Start VPN bulk sync state.`

说明： 主用设备已准备好将所有状态信息发送到备用设备。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720030

错误消息：`%ASA-6-720030: (VPN-unit ) HA status callback: Stop bulk sync state.`

说明：主用设备已将所有状态信息发送到备用设备。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720031

错误消息： `%ASA-7-720031: (VPN-unit ) HA status callback: Invalid event received. event=event_ID .`

说明：VPN 故障切换子系统从基础故障切换子系统收到无效的回调事件。

- **unit** - 主设备或辅助设备
- **event_ID** - 接收到的无效事件 ID

建议的操作：无需执行任何操作。

720032

错误消息：`%ASA-6-720032: (VPN-unit) HA status callback: id=ID , seq=sequence_# , grp=group , event=event , op=operand , my=my_state , peer=peer_state .`

说明：VPN 故障切换子系统指示基础故障切换子系统发出了状态更新通知。

- **unit** - 主设备或辅助设备
- **ID** - 客户端 ID 编号
- **sequence_#** - 序列号
- **group** - 组 ID
- **event** - 当前事件
- **operand** - 当前操作数
- **my_state** - 当前系统状态
- **peer_state** - 对等体的当前状态

建议的操作：无需执行任何操作。

720033

错误消息：`%ASA-4-720033: (VPN-unit ) Failed to queue add to message queue.`

说明：系统资源可能不足。VPN 故障切换子系统尝试对内部消息进行排队时发生错误。这可能是一种暂时情况，表明 Firepower 威胁防御设备处于高负载状态，且 VPN 故障切换子系统无法分配资源来处理传入流量。

- **unit** - 主设备或辅助设备

建议的操作：如果降低Firepower威胁防御设备的当前负载并提供额外系统资源用于处理新消息，可以消除此错误情况。

720034

错误消息：`%ASA-7-720034: (VPN-unit ) Invalid type (type ) for message handler.`

说明：VPN 故障切换子系统尝试处理无效消息类型时发生错误。

- **unit** - 主设备或辅助设备
- **type** - 消息类型

建议的操作：无需执行任何操作。

720035

错误消息：`%ASA-5-720035: (VPN-unit ) Fail to look up CTCP flow handle`

说明：在 VPN 故障切换子系统尝试执行查找之前，可能已在备用设备上删除 cTCP 流。

- **unit** - 主设备或辅助设备

建议的操作：在消息中查找任何 cTCP 流删除迹象，以确定删除流的原因（例如，空闲超时）。

720036

错误消息：`%ASA-5-720036: (VPN-unit ) Failed to process state update message from the active peer.`

说明：VPN 故障切换子系统尝试处理备用设备收到的状态更新消息时发生错误。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。这可能是一种当前负载或系统资源较低导致的暂时情况。

720037

错误消息：`%ASA-6-720037: (VPN-unit ) HA progression callback: id=id ,seq=sequence_number ,grp=group ,event=event ,op=operand , my=my_state ,peer=peer_state .`

说明：报告当前故障切换进程的状态。

- **unit** - 主设备或辅助设备
- **id** - 客户端 ID
- **sequence_number** - 序列号

- **group** - 组 ID
- **event** - 当前事件
- **operand** - 当前操作数
- **my_state** - Firepower 威胁防御设备的当前状态
- **peer_state** - 对等体的当前状态

建议的操作：无需执行任何操作。

720038

错误消息：`%ASA-4-720038: (VPN-unit ) Corrupted message from active unit.`

说明：备用设备收到来自主用设备的已损坏消息。来自主用设备的消息已损坏，这可能是由主用设备和备用设备之间运行的固件不兼容导致的。本地设备已成为故障切换对的主用设备。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720039

错误消息：`%ASA-6-720039: (VPN-unit ) VPN failover client is transitioning to active state`

说明：本地设备已成为故障切换对的主用设备。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720040

错误消息：`%ASA-6-720040: (VPN-unit ) VPN failover client is transitioning to standby state.`

说明：本地设备已成为故障切换对的备用设备。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720041

错误消息：`%ASA-7-720041: (VPN-unit ) Sending type message id to standby unit`

说明：从主用设备向备用设备发送了一条消息。

- **unit** - 主设备或辅助设备
- **type** - 消息类型
- **id** - 消息标识符

建议的操作：无需执行任何操作。

720042

错误消息： `%ASA-7-720042: (VPN-unit ) Receiving type message id from active unit`

说明： 备用设备从主用设备接收到一条消息。

- **unit** - 主设备或辅助设备
- **type** - 消息类型
- **id** - 消息标识符

建议的操作： 无需执行任何操作。

720043

错误消息： `%ASA-4-720043: (VPN-unit ) Failed to send type message id to standby unit`

说明： VPN 故障切换子系统尝试将消息从主用设备发送到备用设备时发生错误。此错误可能是由消息 720018 引起的，此消息的表现是，核心故障切换子系统的故障切换缓冲区用尽或故障切换 LAN 链路为关闭状态。

- **unit** - 主设备或辅助设备
- **type** - 消息类型
- **id** - 消息标识符

建议的操作： 使用 **show failover** 命令查看故障切换对是否正常运行以及故障切换 LAN 链路是否为打开状态。

720044

错误消息： `%ASA-4-720044: (VPN-unit ) Failed to receive message from active unit`

说明： VPN 故障切换子系统尝试接收备用设备上的消息时发生错误。此错误可能是由于消息损坏或分配用于存储传入消息的内存不足导致的。

- **unit** - 主设备或辅助设备

建议的操作： 使用 **show failover** 命令并查找接收错误，来确定这是 VPN 故障切换特定问题，还是常规故障切换问题。消息损坏可能是由主用设备和备用设备上运行的固件版本不兼容导致的。使用 **show memory** 命令确定是否存在内存不足情况。

720045

错误消息： `%ASA-6-720045: (VPN-unit ) Start bulk syncing of state information on standby unit.`

说明： 已通知备用设备开始从主用设备接收批量同步信息。

- **unit** - 主设备或辅助设备

建议的操作： 无需执行任何操作。

720046

错误消息：`%ASA-6-720046: (VPN-unit ) End bulk syncing of state information on standby unit`

说明：已通知备用设备，从主用设备的批量同步已完成。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720047

错误消息：`%ASA-4-720047: (VPN-unit ) Failed to sync SDI node secret file for server IP_address on the standby unit.`

说明：VPN 故障切换子系统尝试在备用设备上同步 SDI 服务器节点密钥文件时发生错误。SDI 节点密钥文件存储在闪存中。此错误可能表示闪存文件系统已满或已损坏。

- **unit** - 主设备或辅助设备
- **IP_address** - 服务器的 IP 地址。

建议的操作：使用 **dir** 命令显示闪存内容。节点密钥文件的文件名为 *ip*.sdi。

720048

错误消息：`%ASA-7-720048: (VPN-unit ) FSM action trace begin: state=state , last event=event , func=function .`

说明：VPN 故障切换子系统有限状态机功能已启动。

- **unit** - 主设备或辅助设备
- **state** - 当前状态
- **event** - 最后一个事件
- **function** - 当前执行的功能

建议的操作：无需执行任何操作。

720049

错误消息：`%ASA-7-720049: (VPN-unit ) FSM action trace end: state=state , last event=event , return=return , func=function .`

说明：VPN 故障切换子系统有限状态机功能已完成。

- **unit** - 主设备或辅助设备
- **state** - 当前状态
- **event** - 最后一个事件
- **return** - 返回代码
- **function** - 当前执行的功能

建议的操作：无需执行任何操作。

720050

错误消息： `%ASA-7-720050: (VPN-unit ) Failed to remove timer.ID = id .`

说明： 无法从计时器处理线程中删除计时器。

- **unit** - 主设备或辅助设备
- **id** - 计时器 ID

建议的操作： 无需执行任何操作。

720051

错误消息： `%ASA-4-720051: (VPN-unit ) Failed to add new SDI node secret file for server id on the standby unit.`

说明： VPN 故障切换子系统尝试在备用设备上添加 SDI 服务器节点密钥文件时发生错误。SDI 节点密钥文件存储在闪存中。此错误可能表示闪存文件系统已满或已损坏。

- **unit** - 主设备或辅助设备
- **id** - SDI 服务器的 IP 地址

建议的操作： 使用 **dir** 命令显示闪存内容。节点密钥文件的文件名为 **ip**.sdi。

720052

错误消息： `%ASA-4-720052: (VPN-unit ) Failed to delete SDI node secret file for server id on the standby unit.`

说明： VPN 故障切换子系统尝试删除主用设备上的节点密钥文件时发生错误。闪存文件系统中可能不存在正在删除的节点密钥文件，或者读取闪存文件系统时出现问题。

- **unit** - 主设备或辅助设备
- **IP_address** - SDI 服务器的 IP 地址

建议的操作： 使用 **dir** 命令显示闪存内容。节点密钥文件的文件名为 **ip**.sdi。

720053

错误消息： `%ASA-4-720053: (VPN-unit ) Failed to add cTCP IKE rule during bulk sync, peer=IP_address , port=port`

说明： VPN 故障切换子系统在批量同步期间尝试在备用设备上加载 cTCP IKE 规则时发生错误。备用设备可能处于高负载状态，且新的 IKE 规则请求可能在完成之前超时。

- **unit** - 主设备或辅助设备
- **IP_address** - 对等体 IP 地址
- **port** - 对等体端口号

建议的操作： 无需执行任何操作。

720054

错误消息：`%ASA-4-720054: (VPN-unit ) Failed to add new cTCP record, peer=IP_address , port=port .`

说明：cTCP 记录复制到备用设备，但无法更新。进行故障切换后，cTCP 隧道上相应的 IPsec 可能无法正常运行。cTCP 数据库可能已满，或者已存在具有相同对等体 IP 地址和端口号的记录。

- **unit** - 主设备或辅助设备
- **IP_address** - 对等体 IP 地址
- **port** - 对等体端口号

建议的操作：这可能是一种暂时情况，当现有 cTCP 隧道恢复后可能会有所改善。

720055

错误消息：`%ASA-4-720055: (VPN-unit ) VPN Stateful failover can only be run in single/non-transparent mode.`

说明：除非以单一（非透明）模式运行，否则 VPN 子系统不会启动。

- **unit** - 主设备或辅助设备

建议的操作：将 Firepower 威胁防御设备配置为适当的模式，以支持 VPN 故障切换并重新启动 Firepower 威胁防御设备。

720056

错误消息：`%ASA-6-720056: (VPN-unit ) VPN Stateful failover Message Thread is being disabled.`

说明：已尝试启用故障切换但未定义故障切换密钥时，VPN 故障切换子系统主消息处理线程将被禁用。VPN 故障切换需要故障切换密钥。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720057

错误消息：`%ASA-6-720057: (VPN-unit ) VPN Stateful failover Message Thread is enabled.`

说明：已启用故障切换并定义故障切换密钥时，VPN 故障切换子系统主消息处理线程将启用。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720058

错误消息：`%ASA-6-720058: (VPN-unit ) VPN Stateful failover Timer Thread is disabled.`

说明：未定义故障切换密钥但启用故障切换时，VPN 故障切换子系统主计时器处理线程将被禁用。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720059

错误消息：`%ASA-6-720059: (VPN-unit ) VPN Stateful failover Timer Thread is enabled.`

说明：已定义故障切换密钥并启用故障切换时，VPN 故障切换子系统主计时器处理线程将启用。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720060

错误消息：`%ASA-6-720060: (VPN-unit ) VPN Stateful failover Sync Thread is disabled.`

说明：已启用故障切换但未定义故障切换密钥时，VPN 故障切换子系统主批量同步处理线程将被禁用。

- **unit** - 主设备或辅助设备。

建议的操作：无需执行任何操作。

720061

错误消息：`%ASA-6-720061: (VPN-unit ) VPN Stateful failover Sync Thread is enabled.`

说明：已启用故障切换并定义故障切换密钥时，VPN 故障切换子系统主批量同步处理线程将启用。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720062

错误消息：`%ASA-6-720062: (VPN-unit ) Active unit started bulk sync of state information to standby unit.`

说明：VPN 故障切换子系统主用设备已开始将状态信息批量同步到备用设备。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720063

错误消息：`%ASA-6-720063: (VPN-unit ) Active unit completed bulk sync of state information to standby.`

说明：VPN 故障切换子系统主用设备已完成状态信息到备用设备的批量同步。

- **unit** - 主设备或辅助设备

建议的操作：无需执行任何操作。

720064

错误消息：`%ASA-4-720064: (VPN-unit ) Failed to update cTCP database record for peer=IP_address , port=port during bulk sync.`

说明：VPN 故障切换子系统在批量同步期间尝试更新现有 cTCP 记录时发生错误。cTCP 记录可能已从备用设备上的 cTCP 数据库中删除，无法找到。

- **unit** - 主设备或辅助设备
- **IP_address** - 对等体 IP 地址
- **port** - 对等体端口号

建议的操作：在消息中搜索。

720065

错误消息：`%ASA-4-720065: (VPN-unit ) Failed to add new cTCP IKE rule, peer=peer , port=port .`

说明：VPN 故障切换子系统尝试在备用设备上为 cTCP 数据库条目添加新 IKE 规则时发生错误。Firepower 威胁防御设备可能处于高负载状态，并且添加 IKE 规则的请求超时且从未完成。

- **unit** - 主设备或辅助设备
- **IP_address** - 对等体 IP 地址
- **port** - 对等体端口号

建议的操作：这可能是一种暂时情况。

720066

错误消息：`%ASA-4-720066: (VPN-unit ) Failed to activate IKE database.`

说明：VPN 故障切换子系统在备用设备转换为主用状态期间尝试激活 IKE 安全关联数据库时发生错误。备用设备上可能存在与资源相关的问题，导致 IKE 安全关联数据库无法激活。

- **unit** - 主设备或辅助设备

建议的操作：使用 **show failover** 命令查看故障切换对是否仍正常工作和/或在消息中查找其他 IKE 相关错误。

720067

错误消息：`%ASA-4-720067: (VPN-unit ) Failed to deactivate IKE database.`

说明：VPN 故障切换子系统在主用设备转换为备用状态期间尝试停用 IKE 安全关联数据库时发生错误。主用设备上可能存在与资源相关的问题，导致 IKE 安全关联数据库无法停用。

- **unit** - 主设备或辅助设备

建议的操作：使用 **show failover** 命令查看故障切换对是否仍正常工作和/或在消息中查找 IKE 相关错误。

720068

错误消息：`%ASA-4-720068: (VPN-unit ) Failed to parse peer message.`

说明：VPN 故障切换子系统尝试解析备用设备上收到的对等消息时发生错误。无法解析备用设备上收到的对等消息。

- **unit** - 主设备或辅助设备

建议的操作：确保主用设备和备用设备运行相同版本的固件。此外，使用 **show failover** 命令确保故障切换对仍正常工作。

720069

错误消息：`%ASA-4-720069: (VPN-unit ) Failed to activate cTCP database.`

说明：VPN 故障切换子系统在备用设备转换为活动状态期间尝试激活 cTCP 数据库时发生错误。备用设备上可能存在与资源相关的问题，导致 cTCP 数据库无法激活。

- **unit** - 主设备或辅助设备

建议的操作：使用 **show failover** 命令查看故障切换对是否仍正常工作和/或在消息中查找其他 cTCP 相关错误。

720070

错误消息：`%ASA-4-720070: (VPN-unit ) Failed to deactivate cTCP database.`

说明：VPN 故障切换子系统在主用设备转换为备用状态期间尝试停用 cTCP 数据库时发生错误。主用设备上可能存在与资源相关的问题，导致 cTCP 数据库无法停用。

- **unit** - 主设备或辅助设备。

建议的操作：使用 **show failover** 命令查看故障切换对是否仍正常工作和/或在消息中查找 cTCP 相关错误。

720071

错误消息：`%ASA-5-720071: (VPN-unit ) Failed to update cTCP dynamic data.`

说明：VPN 故障切换子系统尝试更新 cTCP 动态数据时发生错误。

- **unit** - 主设备或辅助设备。

建议的操作：这可能是一种暂时情况。因为这是定期更新，请等待以查看是否再次出现相同的错误。此外，在消息中查找与故障切换相关的其他消息。

720072

错误消息： `%ASA-5-720072: Timeout waiting for Integrity Firewall Server [interface ,ip ] to become available.`

说明： Zonelab Integrity 服务器无法在超时前重新建立连接。在主用/备用故障切换设置中，需要在故障切换后重新建立 Zonelab Integrity 服务器与 Firepower 威胁防御设备之间的 SSL 连接。

- *interface* - 与 Zonelab Integrity 服务器连接的接口
- *ip* - Zonelab Integrity 服务器的 IP 地址

建议的操作： 检查 Firepower 威胁防御设备和 Zonelab Integrity 服务器的配置是否匹配，并验证 Firepower 威胁防御设备和 Zonelab Integrity 服务器之间的通信。

720073

错误消息： `%ASA-4-720073: VPN Session failed to replicate - ACL acl_name not found`

说明： 将 VPN 会话复制到备用设备时，备用设备未能找到关联的过滤器 ACL。

- **acl_name** - 未找到的 ACL 的名称

建议的操作： 验证备用设备上的配置在备用状态下是否未被修改。通过在主用设备上发出 **write standby** 命令重新同步备用设备。

721001

错误消息： `%ASA-6-721001: (device ) WebVPN Failover SubSystem started successfully.(device ) either WebVPN-primary or WebVPN-secondary.`

说明： 当前故障切换设备（主设备或辅助设备）中的 WebVPN 故障切换子系统已成功启动。

- **(device)** - WebVPN 主设备或 WebVPN 辅助设备

建议的操作： 无需执行任何操作。

721002

错误消息： `%ASA-6-721002: (device ) HA status change: event event , my state my_state , peer state peer .`

说明： WebVPN 故障切换子系统定期从核心 HA 组件接收状态通知。系统会报告传入事件、本地 Firepower 威胁防御设备的新状态以及故障切换对等体的新状态。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **event** - 新 HA 事件
- **my_state** - 本地 Firepower 威胁防御设备的新状态
- **peer** - 对等体的新状态

建议的操作： 无需执行任何操作。

721003

错误消息： `%ASA-6-721003: (device ) HA progression change: event event , my state my_state , peer state peer .`

说明： WebVPN 故障切换子系统根据核心 HA 组件通知的事件从一种状态转换为另一种状态。系统将报告传入事件、本地 Firepower 威胁防御设备的新状态以及故障切换对等体的新状态。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **event** - 新 HA 事件
- **my_state** - 本地 Firepower 威胁防御设备的新状态
- **peer** - 对等体的新状态

建议的操作： 无需执行任何操作。

721004

错误消息： `%ASA-6-721004: (device ) Create access list list_name on standby unit.`

说明： 已将 WebVPN 特定访问列表从主用设备复制到备用设备。已成功在备用设备上安装 WebVPN 访问列表。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **list_name** - 访问列表名称

建议的操作： 无需执行任何操作。

721005

错误消息： `%ASA-6-721005: (device ) Fail to create access list list_name on standby unit.`

说明： 在主用设备上安装 WebVPN 特定访问列表时，会在备用设备上安装副本。此访问列表在备用设备上安装失败。此访问列表已存在于备用设备上。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **list_name** - 在备用设备上安装失败的访问列表的名称

建议的操作： 在主用设备和备用设备上使用 **show access-list** 命令。比较输出内容并确定是否存在任何差异。如有需要，通过在主用设备上使用 **write standby** 命令重新同步备用设备。

721006

错误消息： `%ASA-6-721006: (device ) Update access list list_name on standby unit.`

说明： 已在备用设备上更新访问列表的内容。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **list_name** - 已更新的访问列表的名称

建议的操作： 无需执行任何操作。

721007

错误消息：`%ASA-4-721007: (device ) Fail to update access list list_name on standby unit.`

说明：备用设备尝试更新 WebVPN 特定访问列表时发生错误。在备用设备上找不到此访问列表。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **list_name** - 未更新的访问列表的名称

建议的操作：在主用设备和备用设备上使用 **show access-list** 命令。比较输出内容并确定是否存在任何差异。如有需要，通过在主用设备上使用 **write standby** 命令重新同步备用设备。

721008

错误消息：`%ASA-6-721008: (device ) Delete access list list_name on standby unit.`

说明：从主用设备中删除 WebVPN 特定访问列表，系统会向备用设备发送一条消息，请求删除相同的访问列表。因此，WebVPN 特定访问列表已从备用设备中删除。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **list_name** - 已删除的访问列表的名称

建议的操作：无需执行任何操作。

721009

错误消息：`%ASA-6-721009: (device ) Fail to delete access list list_name on standby unit.`

说明：从主用设备上删除 WebVPN 特定访问列表时，系统会向备用设备发送一条消息，请求删除相同的访问列表。尝试删除备用设备上的相应访问列表时发生错误。备用设备上不存在此访问列表。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **list_name** - 已删除的访问列表的名称

建议的操作：在主用设备和备用设备上使用 **show access-list** 命令。比较输出内容并确定是否存在任何差异。如有需要，通过在主用设备上使用 **write standby** 命令重新同步备用设备。

721010

错误消息：`%ASA-6-721010: (device ) Add access list rule list_name , line line_no on standby unit.`

说明：向主用设备添加访问列表规则时，会在备用设备上添加相同的规则。新的访问列表规则已成功添加到备用设备上。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **list_name** - 已删除的访问列表的名称
- **line_no** - 添加到访问列表的规则的行号

建议的操作：无需执行任何操作。

721011

错误消息： `%ASA-4-721011: (device ) Fail to add access list rule list_name , line line_no on standby unit.`

说明： 向主用设备添加访问列表规则时，会尝试向备用设备添加相同的访问列表规则。尝试向备用设备添加新访问列表规则时发生错误。备用设备上可能存在相同的访问列表规则。

- *(device)* - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **list_name** - 已删除的访问列表的名称
- **line_no** - 添加到访问列表的规则的行号

建议的操作： 在主用设备和备用设备上使用 **show access-list** 命令。比较输出内容并确定是否存在任何差异。如有需要，通过在主用设备上使用 **write standby** 命令重新同步备用设备。

721012

错误消息： `%ASA-6-721012: (device ) Enable APCF XML file file_name on the standby unit.`

说明： 在主用设备上安装 APCF XML 文件时，会尝试在备用设备上安装相同的文件。在备用设备上成功安装了 APCF XML 文件。在备用设备上使用 **dir** 命令来显示闪存文件系统中存在 XML 文件。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **file_name** - 闪存文件系统上的 XML 文件的名称

建议的操作： 无需执行任何操作。

721013

错误消息： `%ASA-4-721013: (device ) Fail to enable APCF XML file file_name on the standby unit.`

说明： 在主用设备上安装 APCF XML 文件时，会尝试在备用设备上安装相同的文件。在备用设备上安装 APCF XML 文件失败。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **file_name** - 闪存文件系统上的 XML 文件的名称

建议的操作： 在主用设备和备用设备上使用 **dir** 命令。比较目录列表并确定是否存在任何差异。如有需要，通过在主用设备上使用 **write standby** 命令重新同步备用设备。

721014

错误消息： `%ASA-6-721014: (device ) Disable APCF XML file file_name on the standby unit.`

说明： 从主用设备上删除 APCF XML 文件时，会尝试从备用设备上删除相同的文件。已成功从备用设备中删除 APCF XML 文件。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **file_name** - 闪存文件系统上的 XML 文件的名称

建议的操作：无需执行任何操作。

721015

错误消息： `%ASA-4-721015: (device ) Fail to disable APCF XML file file_name on the standby unit.`

说明：从主用设备上删除 APCF XML 文件时，会尝试从备用设备上删除相同的文件。尝试从备用设备中删除 APCF XML 文件时发生错误。此文件可能未安装在备用设备上。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **file_name** - 闪存文件系统上的 XML 文件的名称

建议的操作：使用 **show running-config webvpn** 命令，确保未启用相关的 APCF XML 文件。只要未启用此文件，您就可以忽略此消息。否则，请尝试使用 **no apcf file_name** 命令在 WebVPN 配置子模式中禁用此文件。

721016

错误消息：`%ASA-6-721016: (device ) WebVPN session for client user user_name , IP ip_address has been created.`

说明：远程 WebVPN 用户已成功登录且备用设备上已安装登录信息。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **user_name** - 用户的名称
- **ip_address** - 远程用户的 IP 地址

建议的操作：无需执行任何操作。

721017

错误消息：`%ASA-4-721017: (device ) Fail to create WebVPN session for user user_name , IP ip_address .`

说明：WebVPN 用户登录到主用设备后，登录信息将被复制到备用设备。将登录信息复制到备用设备时发生错误。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **user_name** - 用户的名称
- **ip_address** - 远程用户的 IP 地址

建议的操作：在主用设备和备用设备上，对常规 WebVPN 用户使用 **show vpn-sessiondb detail webvpn** 命令，或者对 WebVPN SVC 用户使用 **show vpn-sessiondb detail svc** 命令。比较条目并确定两台 Firepower 威胁防御设备上是否显示相同的用户会话记录。如有需要，通过在主用设备上使用 **write standby** 命令重新同步备用设备。

721018

错误消息： `%ASA-6-721018: (device ) WebVPN session for client user user_name , IP ip_address has been deleted.`

说明： 当 WebVPN 用户注销主用设备时，系统将向备用设备发送一条注销消息，以从备用设备中删除用户会话。已成功从备用设备中删除 WebVPN 用户记录。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **user_name** - 用户的名称
- **ip_address** - 远程用户的 IP 地址

建议的操作： 无需执行任何操作。

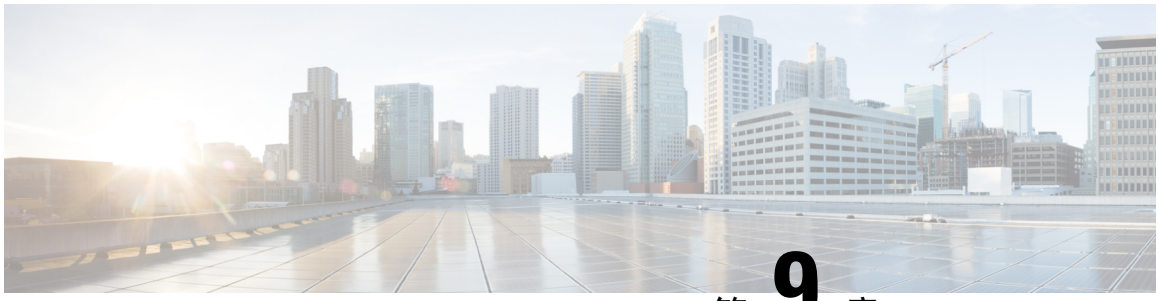
721019

错误消息： `%ASA-4-721019: (device ) Fail to delete WebVPN session for client user user_name , IP ip_address .`

说明： 当 WebVPN 用户注销主用设备时，系统将向备用设备发送一条注销消息，以从备用设备中删除用户会话。尝试从备用设备中删除 WebVPN 用户记录时发生错误。

- **(device)** - WebVPN 主或 WebVPN 辅助 Firepower 威胁防御设备
- **user_name** - 用户的名称
- **ip_address** - 远程用户的 IP 地址

建议的操作： 在主用设备和备用设备上，对常规 WebVPN 用户使用 **show vpn-sessiondb detail webvpn** 命令，或者对 WebVPN SVC 用户使用 **show vpn-sessiondb detail svc** 命令。检查是否存在任何差异。如有需要，通过在主用设备上使用 **write standby** 命令重新同步备用设备。



第 9 章

系统日志消息 722001-776020

本章包含以下各节：

ID 介于 722001 到 722056 之间的消息

本部分包括 ID 介于 722001 到 722056 之间的消息。

722001

错误消息： `%ASA-4-722001: IP IP_address Error parsing SVC connect request.`

说明： SVC 的请求无效。

建议的操作： 必要时进行调查以确定此错误是否由SVC缺陷、SVC版本不兼容或针对设备的攻击所导致。

722002

错误消息： `%ASA-4-722002: IP IP_address Error consolidating SVC connect request.`

说明： 没有足够的内存来执行操作。

建议的操作： 购买更多内存，升级设备或降低设备负载。

722003

错误消息： `%ASA-4-722003: IP IP_address Error authenticating SVC connect request.`

说明： 用户下载和连接时间过长。

建议的操作： 增加会话空闲超时值和最长连接时间。

722004

错误消息： %ASA-4-722004: Group *group* User *user-name* IP *IP_address*Error responding to SVC connect request.

说明：没有足够的内存来执行操作。

建议的操作：购买更多内存，升级设备或降低设备负载。

722005

错误消息： %ASA-5-722005: Group *group* User *user-name* IP *IP_address*Unable to update session information for SVC connection.

说明：没有足够的内存来执行操作。

建议的操作：购买更多内存，升级设备或降低设备负载。

722006

错误消息： %ASA-5-722006: Group *group* User *user-name* IP *IP_address*Invalid address **IP_address** assigned to SVC connection.

说明：为用户分配了无效地址。

建议的操作：如有可能，验证并更正地址分配。否则，通知网络管理员或根据安全策略上报此问题。如需获取其他帮助，请联系思科 TAC。

722007

错误消息： %ASA-3-722007: Group *group* User *user-name* IP *IP_address*SVC Message: *type-num* /ERROR: *message*

说明：SVC 发出一条消息。

- **type-num** - 介于 0 到 31 之间的数字，表示消息类型。消息类型如下：

- 0 - 正常

- 16 - 注销

- 17 - 因错误关闭

- 18 - 因密钥更新关闭

- 1-15、19-31 - 已保留和未使用

- **message** - 来自 SVC 的文本消息

建议的操作：无需执行任何操作。

722008

错误消息： `%ASA-3-722008: Group group User user-name IP IP_addressSVC Message: type-num /ERROR: message`

说明： SVC 发出一条消息。

- **type-num** - 介于 0 到 31 之间的数字，表示消息类型。消息类型如下：

- 0 - 正常

- 16 - 注销

- 17 - 因错误关闭

- 18 - 因密钥更新关闭

- 1-15、19-31 - 已保留和未使用

- **message** - 来自 SVC 的文本消息

建议的操作： 无需执行任何操作。

722009

错误消息： `%ASA-3-722009: Group group User user-name IP IP_addressSVC Message: type-num /ERROR: message`

说明： SVC 发出一条消息。

- **type-num** - 介于 0 到 31 之间的数字，表示消息类型。消息类型如下：

- 0 - 正常

- 16 - 注销

- 17 - 因错误关闭

- 18 - 因密钥更新关闭

- 1-15、19-31 - 已保留和未使用

- **message** - 来自 SVC 的文本消息

建议的操作： 无需执行任何操作。

722010

错误消息： `%ASA-5-722010: Group group User user-name IP IP_addressSVC Message: type-num /NOTICE: message`

说明： SVC 发出一条消息。

- **type-num** - 介于 0 到 31 之间的数字，表示消息类型。消息类型如下：

- 0 - 正常

- 16 - 注销

- 17 - 因错误关闭

- 18 - 因密钥更新关闭

- 1-15、19-31 - 已保留和未使用

- **message** - 来自 SVC 的文本消息

建议的操作：无需执行任何操作。

722011

错误消息：`%ASA-5-722011: Group group User user-name IP IP_addressSVC Message: type-num /NOTICE: message`

说明：SVC 发出一条消息。

- **type-num** - 介于 0 到 31 之间的数字，表示消息类型。消息类型如下：

- 0 - 正常

- 16 - 注销

- 17 - 因错误关闭

- 18 - 因密钥更新关闭

- 1-15、19-31 - 已保留和未使用

- **message** - 来自 SVC 的文本消息

建议的操作：无需执行任何操作。

722012

错误消息：`%ASA-5-722012: Group group User user-name IP IP_addressSVC Message: type-num /INFO: message`

说明：SVC 发出一条消息。

- **type-num** - 介于 0 到 31 之间的数字，表示消息类型。消息类型如下：

- 0 - 正常

- 16 - 注销

- 17 - 因错误关闭

- 18 - 因密钥更新关闭

- 1-15、19-31 - 已保留和未使用

- **message** - 来自 SVC 的文本消息

建议的操作：无需执行任何操作。

722013

错误消息：%ASA-6-722013: Group *group* User *user-name* IP *IP_address*SVC Message: *type-num* /INFO: *message*

说明：SVC 发出一条消息。

- **type-num** - 介于 0 到 31 之间的数字，表示消息类型。消息类型如下：

- 0 - 正常

- 16 - 注销

- 17 - 因错误关闭

- 18 - 因密钥更新关闭

- 1-15、19-31 - 已保留和未使用

- **message** - 来自 SVC 的文本消息

建议的操作：无需执行任何操作。

722014

错误消息：%ASA-6-722014: Group *group* User *user-name* IP *IP_address*SVC Message: *type-num* /INFO: *message*

说明：SVC 发出一条消息。

- **type-num** - 介于 0 到 31 之间的数字，表示消息类型。消息类型如下：

- 0 - 正常。

- 16 - 注销

- 17 - 因错误关闭

- 18 - 因密钥更新关闭

- 1-15、19-31 - 已保留和未使用

- **message** - 来自 SVC 的文本消息

建议的操作：无需执行任何操作。

722015

错误消息：%ASA-4-722015: Group *group* User *user-name* IP *IP_address*Unknown SVC frame type: *type-num*

说明：SVC 向设备发送了无效的帧类型，这可能是 SVC 版本不兼容导致的。

- **type-num** - 帧类型的数字标识符

建议的操作：验证 SVC 版本。

722016

错误消息： `%ASA-4-722016: Group group User user-name IP IP_addressBad SVC frame length: length expected: expected-length`

说明： 无法从 SVC 获取预期数量的数据，这可能是由 SVC 版本不兼容导致的。

建议的操作： 验证 SVC 版本。

722017

错误消息： `%ASA-4-722017: Group group User user-name IP IP_addressBad SVC framing: 525446, reserved: 0`

说明： SVC 发送了严重错误的数据报，这可能是由 SVC 版本不兼容导致的。

建议的操作： 验证 SVC 版本。

722018

错误消息： `%ASA-4-722018: Group group User user-name IP IP_addressBad SVC protocol version: version , expected: expected-version`

说明： SVC 发送了设备未知的版本，这可能是由 SVC 版本不兼容导致的。

建议的操作： 验证 SVC 版本。

722019

错误消息： `%ASA-4-722019: Group group User user-name IP IP_addressNot enough data for an SVC header: length`

说明： 无法从 SVC 获取预期数量的数据，这可能是由 SVC 版本不兼容导致的。

建议的操作： 验证 SVC 版本。

722020

错误消息： `%ASA-3-722020: TunnelGroup tunnel_group GroupPolicy group_policy User user-name IP IP_addressNo address available for SVC connection`

说明： AnyConnect 会话的地址分配失败。没有可用的 IP 地址。

- **tunnel_group** - 为用户分配或用于登录的隧道组的名称
- *group_policy* - 为用户分配的组策略的名称
- *user-name* - 与此消息关联的用户的名称
- *IP_address* - 客户端计算机的公共 IP（互联网）地址

建议的操作： 检查 **ip local ip** 命令中列出的配置，以查看已分配给隧道组和组策略的池中是否有足够的地址。检查 DHCP 配置和状态。检查地址分配配置。启用 IPAA 系统日志消息，以确定 AnyConnect 客户端无法获取 IP 地址的原因。

722028

错误消息： %ASA-5-722028: Group *group* User *user-name* IP *IP_address*Stale SVC connection closed.

说明： 未使用的 SVC 连接已关闭。

建议的操作： 无需执行任何操作。但是，如果已建立多个连接，则客户端可能无法连接。应检查 SVC 日志。

722029

错误消息： %ASA-7-722029: Group *group* User *user-name* IP *IP_address*SVC Session Termination: Conns: *connections* , DPD Conns: *DPD_conns* , Comp resets: *compression_resets* , Dcmp resets: *decompression_resets*

说明： 系统会报告连接次数、重新连接次数和重置次数。如果 **connections** 大于 1 或 **DPD_conns** 、**compression_resets** 或 **decompression_resets** 对应的次数大于 0，则可能表示存在网络可靠性问题，这可能超出了 Firepower 威胁防御管理员的控制范围。如果连接次数或 DPD 连接次数较多，则用户可能无法连接且可能遇到性能不佳问题。

- **connections** - 此会话期间的连接总次数（一次属正常情况）
- **DPD_conns** - 由 DPD 引起的重新连接次数
- **compression_resets** - 压缩历史记录重置次数
- **decompression_resets** - 解压缩历史记录重置次数

建议的操作： 应检查SVC日志。您可能希望研究并采取适当的措施来解决可能存在的网络可靠性问题。

722030

错误消息： %ASA-7-722030: Group *group* User *user-name* IP *IP_address*SVC Session Termination: In: *data_bytes* (+*ctrl_bytes*) bytes, *data_pkts* (+*ctrl_pkts*) packets, *drop_pkts* drops

说明： 正在记录会话结束时的统计信息。

- **data_bytes** - 入站（自 SVC）数据字节数
- **ctrl_bytes** - 入站控制字节数
- **data_pkts** - 入站数据包数
- **ctrl_pkts** - 入站控制数据包数
- **drop_pkts** - 丢弃的入站数据包数

建议的操作： 无需执行任何操作。

722031

错误消息： %ASA-7-722031: Group *group* User *user-name* IP *IP_address*SVC Session Termination: Out: *data_bytes* (+*ctrl_bytes*) bytes, *data_pkts* (+*ctrl_pkts*) packets, *drop_pkts* drops.

说明： 正在记录会话结束时的统计信息。

- **data_bytes** - 出站（到 SVC）数据字节数
- **ctrl_bytes** - 出站控制字节数
- **data_pkts** - 出站数据包数
- **ctrl_pkts** - 出站控制数据包数
- **ctrl_pkts** - 丢弃的出站数据包数

建议的操作：无需执行任何操作。

722032

错误消息：`%ASA-5-722032: Group group User user-name IP IP_addressNew SVC connection replacing old connection.`

说明：新的 SVC 连接将替换现有连接。您可能无法连接。

建议的操作：检查 SVC 日志。

722033

错误消息：`%ASA-5-722033: Group group User user-name IP IP_addressFirst SVC connection established for SVC session.`

说明：已为 SVC 会话建立第一个 SVC 连接。

建议的操作：无需执行任何操作。

722034

错误消息：`%ASA-5-722034: Group group User user-name IP IP_addressNew SVC connection, no existing connection.`

说明：已发生重新连接尝试。SVC 连接将替换先前关闭的连接。此会话没有现有连接，因为连接已被 SVC 或 Firepower 威胁防御设备丢弃。您可能无法连接。

建议的操作：检查 Firepower 威胁防御设备日志和 SVC 日志。

722035

错误消息：`%ASA-3-722035: Group group User user-name IP IP_addressReceived large packet length (threshold num ).`

说明：从客户端收到了一个大型数据包。

- **length** - 大型数据包的长度
- **num** - 阈值

建议的操作：在组策略下输入 **anyconnect ssl df-bit-ignore enable** 命令，以允许 Firepower 威胁防御设备对以 DF 位集形式收到的数据包进行分段。

722036

错误消息： `%ASA-3-722036: Group group User user-name IP IP_addressTransmitting large packet length (threshold num ).`

说明： 大型数据包已发送到客户端。数据包的源可能不知道客户端的MTU。这也可能是由于压缩了不可压缩的数据导致的。

- **length** - 大型数据包的长度
- **num** - 阈值

建议的操作： 关闭 SVC 压缩，否则无需执行任何操作。

722037

错误消息： `%ASA-5-722037: Group group User user-name IP IP_addressSVC closing connection: reason .`

说明： 出于给定原因，SVC 连接已终止。这可能是正常行为，也可能是无法连接。

- **reason** - SVC 连接终止的原因

建议的操作： 检查 SVC 日志。

722038

错误消息： `%ASA-5-722038: Group group-name User user-name IP IP_addressSVC terminating session: reason .`

说明： 出于给定原因，SVC 会话已终止。这可能是正常行为，也可能是无法连接。

- **reason** - SVC 会话终止的原因

建议的操作： 如果终止原因是意外原因，请检查 SVC 日志。

722041

错误消息： `%ASA-4-722041: TunnelGroup tunnel_group GroupPolicy group_policy User username IP peer_address No IPv6 address available for SVC connection.`

说明： IPv6 地址无法分配给远程 SVC 客户端。

- *n* - SVC 连接标识符

建议的操作： 如有需要，扩充或创建 IPv6 地址池。

722042

错误消息： `%ASA-4-722042: Group group User user IP ip Invalid Cisco SSL Tunneling Protocol version.`

说明： 无效 SVC 或 AnyConnect 客户端正在尝试连接。

- *group* - 用户正在尝试连接的组策略的名称
- *user* - 正在尝试连接的用户的名称
- *ip* - 正在尝试连接的用户的 IP 地址

建议的操作：验证 SVC 或 AnyConnect 客户端是否与 Firepower 威胁防御设备兼容。

722043

错误消息：`%ASA-5-722043: Group group User user IP ip DTLS disabled: unable to negotiate cipher.`

说明：无法建立 DTLS（UDP 传输）。SSL 加密配置可能已更改。

- *group* - 用户正在尝试连接的组策略的名称
- *user* - 正在尝试连接的用户的名称
- *ip* - 正在尝试连接的用户的 IP 地址

建议的操作：恢复SSL加密配置。确保SSL加密配置中至少有一个分组密式（AES、DES或3DES）。

722044

错误消息：`%ASA-5-722044: Group group User user IP ip Unable to request ver address for SSL tunnel.`

说明：由于 Firepower 威胁防御设备上的内存不足，无法请求 IP 地址。

- *group* - 用户正在尝试连接的组策略的名称
- *user* - 正在尝试连接的用户的名称
- *ip* - 正在尝试连接的用户的 IP 地址
- *ver* - IPv4 或 IPv6，基于所请求的 IP 地址版本

建议的操作：降低 Firepower 威胁防御设备的负载或增加更多内存。

722045

错误消息：`%ASA-3-722045: Connection terminated: no SSL tunnel initialization data.`

说明：缺少建立连接的数据。这是 Firepower 威胁防御软件缺陷。

建议的操作：联系思科 TAC 寻求帮助。

722046

错误消息：`%ASA-3-722046: Group group User user IP ip Session terminated: unable to establish tunnel.`

说明：Firepower 威胁防御设备无法设置连接参数。这是 Firepower 威胁防御软件缺陷。

- *group* - 用户正在尝试连接的组策略的名称
- *user* - 正在尝试连接的用户的名称

- *ip* - 正在尝试连接的用户的 IP 地址

建议的操作：联系思科 TAC 寻求帮助。

722047

错误消息：`%ASA-4-722047: Group group User user IP ip Tunnel terminated: SVC not enabled or invalid SVC image on the ASA.`

说明：用户通过 Web 浏览器登录并尝试启动 SVC 或 AnyConnect 客户端。未在全局启用 SVC 服务，或者 SVC 映像无效或已损坏。隧道连接已终止，但无客户端连接仍然存在。

- *group* - 用户正在尝试连接的组策略的名称
- *user* - 正在尝试连接的用户的名称
- *ip* - 正在尝试连接的用户的 IP 地址

建议的操作：使用 **svc enable** 命令全局启用 SVC。通过使用 **svc image** 命令重新加载新映像，来验证 SVC 映像版本的完整性。

722048

错误消息：`%ASA-4-722048: Group group User user IP ip Tunnel terminated: SVC not enabled for the user.`

说明：用户通过 Web 浏览器登录并尝试启动 SVC 或 AnyConnect 客户端。没有为此用户启用 SVC 服务。隧道连接已终止，但无客户端连接仍然存在。

- *group* - 用户正在尝试连接的组策略的名称
- *user* - 正在尝试连接的用户的名称
- *ip* - 正在尝试连接的用户的 IP 地址

建议的操作：使用 **group-policy** 和 **username** 命令为此用户启用该服务。

722049

错误消息：`%ASA-4-722049: Group group User user IP ip Session terminated: SVC not enabled or invalid image on the ASA.`

说明：用户已通过 AnyConnect 客户端登录。未在全局启用 SVC 服务，或者 SVC 映像无效或已损坏。会话连接已终止。

- *group* - 用户正在尝试连接的组策略的名称
- *user* - 正在尝试连接的用户的名称
- *ip* - 正在尝试连接的用户的 IP 地址

建议的操作：使用 **svc-enable** 命令全局启用 SVC。通过使用 **svc image** 命令重新加载新映像，来验证 SVC 映像的完整性和版本。

722050

错误消息： `%ASA-4-722050: Group group User user IP ip Session terminated: SVC not enabled for the user.`

说明： 用户已通过 AnyConnect 客户端登录。没有为此用户启用 SVC 服务。会话连接已终止。

- *group* - 用户正在尝试连接的组策略的名称
- *user* - 正在尝试连接的用户的名称
- *ip* - 正在尝试连接的用户的 IP 地址

建议的操作： 使用 **group-policy** 和 **username** 命令为此用户启用该服务。

722051

错误消息： `%ASA-6-722051: Group group-policy User username IP public-ip IPv4 Address assigned-ip IPv6 Address assigned-ip assigned to session`

说明： 指定的地址已分配给指定用户。

- *group-policy* - 允许用户获取访问权限的组策略
- *username* - 用户的名称
- *public-ip* - 已连接客户端的公共 IP 地址
- *assigned-ip* - 分配给客户端的 IPv4 或 IPv6 地址

建议的操作： 无需执行任何操作。

722053

错误消息： `%ASA-6-722053: Group g User u IP ip Unknown client user-agent connection.`

说明： 未知或不受支持的 SSL VPN 客户端已连接到 Firepower 威胁防御设备。旧客户端包括早于 2.3.1 版的思科 SVC 和思科 AnyConnect 客户端。

- *g* - 用户登录的组策略
- *u* - 用户的名称
- *ip* - 客户端的 IP 地址
- *user-agent* - 从客户端收到的用户代理（通常包括版本）

建议的操作： 升级到受支持的思科 SSL VPN 客户端。

722054

错误消息： `%ASA-4-722054: Group group policy User user name IP remote IP SVC terminating connection: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP`

说明： 安装重定向 URL 时 AnyConnect VPN 连接发生错误，从 ISE 接收到了 ACL，但 Firepower 威胁防御设备上不存在重定向 ACL。

- *group policy* - 允许用户获取访问权限的组策略
- *user name* - 远程访问的请求者的用户名
- *remote IP* - 发送该连接请求的远程 IP 地址
- *redirect URL* - 用于 HTTP 流量重定向的 URL
- *assigned IP* - 分配给用户的 IP 地址

建议的操作：在 Firepower 威胁防御设备上配置重定向 ACL。

722055

错误消息：`%ASA-6-722055: Group group-policy User username IP public-ip Client Type: user-agent`

说明：指示的用户正在尝试连接给定的用户代理。

- *group-policy* - 允许用户获取访问权限的组策略
- *username* - 用户的名称
- *public-ip* - 已连接客户端的公共 IP 地址
- *user-agent* - 连接客户端提供的用户代理字符串。通常包括 AnyConnect 版本和 AnyConnect 客户端的主机操作系统。

建议的操作：无需执行任何操作。

722056

错误消息：`%ASA-4-722055: Unsupported AnyConnect client connection rejected from ip address.Client info: user-agent string.Reason: reason`

说明：此系统日志指示 AnyConnect 客户端连接被拒绝。系统日志中提供了拒绝原因以及客户端信息。

- *ip address* - 尝试与旧客户端连接的 IP 地址。
- *user- agent string* - 客户端请求中的用户代理报头。通常包括 AnyConnect 版本和 AnyConnect 客户端的主机操作系统
- *reason* - 拒绝原因

建议的操作：使用系统日志中提供的客户端信息和原因解决此问题。

ID 介于 723001 到 737036 之间的消息

本部分包括 ID 介于 723001 到 737036 之间的消息。

723001

错误消息：`%ASA-6-723001: Group group-name , User user-name , IP IP_address : WebVPN Citrix ICA connection connection is up.`

说明：Citrix 连接已打开。

- **group-name** - Citrix 组的名称
- **user-name** - Citrix 用户的名称
- **IP_address** - Citrix 用户的 IP 地址
- **connection** - Citrix 连接标识符

建议的操作：无需执行任何操作。

723002

错误消息： `%ASA-6-723002: Group group-name , User user-name , IP IP_address : WebVPN Citrix ICA connection connection is down.`

说明：Citrix 连接断开。

- **group-name** - Citrix 组的名称
- **user-name** - Citrix 用户的名称
- **IP_address** - Citrix 用户的 IP 地址
- **connection** - Citrix 连接标识符

建议的操作：当 Citrix ICA 连接由客户端、服务器或 Firepower 威胁防御管理员有意终止时，无需执行任何操作。但是，如果情况并非如此，验证在其中设置 Citrix ICA 连接的 WebVPN 会话是否仍处于活动状态。如果会话处于非活动状态，则收到此消息是正常的。如果 WebVPN 会话仍处于活动状态，验证 ICA 客户端和 Citrix 服务器是否均正常工作并且没有显示任何错误。如果情况并非如此，调用其中一个或两者，或对任何错误进行响应。如果仍收到此消息，请联系思科 TAC 并提供以下信息：

- 网络拓扑
- 延迟和丢包
- Citrix 服务器配置
- Citrix ICA 客户端信息
- 重现问题的步骤
- 所有相关消息的完整文本

723003

错误消息： `%ASA-7-723003: No memory for WebVPN Citrix ICA connection connection .`

说明：Firepower 威胁防御设备内存不足。Citrix 连接被拒绝。

- **connection** - Citrix 连接标识符

建议的操作：验证 Firepower 威胁防御设备是否正常工作。特别注意内存和缓冲区的使用情况。如果 Firepower 威胁防御设备处于高负载状态，购买更多内存并升级 Firepower 威胁防御设备或降低 Firepower 威胁防御设备的负载。如果问题仍然存在，请联系思科 TAC。

723004

错误消息： `%ASA-7-723004: WebVPN Citrix encountered bad flow control flow .`

说明：Firepower威胁防御设备遇到内部流控制不匹配问题，这可能是由大量数据流导致的，例如在压力测试期间或具有大量 ICA 连接时可能会发生这种情况。

建议的操作：减少与 Firepower 威胁防御设备的 ICA 连接。如果问题仍然存在，请联系思科 TAC。

723005

错误消息：`%ASA-7-723005: No channel to set up WebVPN Citrix ICA connection.`

说明：Firepower 威胁防御设备无法为 Citrix 创建新通道。

建议的操作：验证 Citrix ICA 客户端和 Citrix 服务器是否仍处于活动状态。如果情况并非如此，重新启动并重新测试。检查 Firepower 威胁防御设备负载，特别注意内存和缓冲区的使用情况。如果 Firepower 威胁防御设备处于高负载状态，升级 Firepower 威胁防御设备、添加内存或降低负载。如果问题仍然存在，请联系思科 TAC。

723006

错误消息：`%ASA-7-723006: WebVPN Citrix SOCKS errors.`

说明：Firepower 威胁防御设备上发生内部 Citrix SOCKS 错误。

建议的操作：验证 Citrix ICA 客户端是否正常工作。此外，检查 Citrix ICA 客户端和 Firepower 威胁防御设备之间的网络连接状态，特别注意丢包情况。解决任何异常网络状况。如果问题仍然存在，请联系思科 TAC。

723007

错误消息：`%ASA-7-723007: WebVPN Citrix ICA connection` *`connection`* `list is broken.`

说明：Firepower 威胁防御设备内部 Citrix 连接列表已损坏。

- **connection** - Citrix 连接标识符

建议的操作：验证Firepower威胁防御设备是否正常工作，特别注意内存和缓冲区的使用情况。如果 Firepower 威胁防御设备处于高负载状态，升级 Firepower 威胁防御设备、添加内存或降低负载。如果问题仍然存在，请联系思科 TAC。

723008

错误消息：`%ASA-7-723008: WebVPN Citrix ICA SOCKS Server` *`server`* `is invalid.`

说明：尝试了访问不存在的 Citrix Socks 服务器。

- **server** - Citrix 服务器标识符

建议的操作：验证Firepower威胁防御设备是否正常工作。注意是否有任何内存或缓冲区泄漏现象。如果经常出现此问题，捕获有关内存使用率、网络拓扑以及收到此消息期间的情况的信息。将这些信息发送给思科 TAC 进行审查。收到此消息时，请确保 WebVPN 会话仍处于活动状态。否则，请

确定 WebVPN 会话关闭的原因。如果 Firepower 威胁防御设备处于高负载状态，升级 Firepower 威胁防御设备、添加内存或降低负载。如果问题仍然存在，请联系思科 TAC。

723009

错误消息：`%ASA-7-723009: Group group-name , User user-name , IP IP_address : WebVPN Citrix received data on invalid connection connection .`

说明：收到有关不存在的 Citrix 连接的数据。

- **group-name** - Citrix 组的名称
- **user-name** - Citrix 用户的名称
- **IP_address** - Citrix 用户的 IP 地址
- **connection** - Citrix 连接标识符

建议的操作：最初发布的 Citrix 应用连接可能已终止，其余已发布的活动应用中断了连接。重新启动所有已发布应用，以生成新的 Citrix ICA 隧道。如果 Firepower 威胁防御设备处于高负载状态，升级 Firepower 威胁防御设备、添加内存或降低负载。如果问题仍然存在，请联系思科 TAC。

723010

错误消息：`%ASA-7-723010: Group group-name , User user-name , IP IP_address : WebVPN Citrix received closing channel channel for invalid connection connection .`

说明：收到有关不存在的 Citrix 连接的中止消息，这可能是由大量数据流（例如压力测试）或大量 ICA 连接导致的，尤其是在网络延迟或丢包期间。

- **group-name** - Citrix 组的名称
- **user-name** - Citrix 用户的名称
- **IP_address** - Citrix 用户的 IP 地址
- channel - Citrix 通道标识符
- **connection** - Citrix 连接标识符

建议的操作：减少与 Firepower 威胁防御设备的 ICA 连接数，为 Firepower 威胁防御设备获取更多内存，或解决网络问题。

723011

错误消息：`%ASA-7-723011: Group group-name , User user-name , IP IP_address : WebVPN Citrix receives bad SOCKS socks message length msg-length.Expected length is exp-msg-length .`

说明：Citrix SOCKS 消息长度不正确。

- **group-name** - Citrix 组的名称
- **user-name** - Citrix 用户的名称
- **IP_address** - Citrix 用户的 IP 地址

建议的操作：验证 Citrix ICA 客户端是否正常工作。此外，检查 ICA 客户端和 Firepower 威胁防御设备之间的网络连接状态，特别注意丢包情况。解决任何异常网络状况后，如果问题仍然存在，请联系思科 TAC。

723012

错误消息：`%ASA-7-723012: Group group-name , User user-name , IP IP_address : WebVPN Citrix received bad SOCKS socks message format.`

说明：Citrix SOCKS 消息格式不正确。

- **group-name** - Citrix 组的名称
- **user-name** - Citrix 用户的名称
- **IP_address** - Citrix 用户的 IP 地址

建议的操作：验证 Citrix ICA 客户端是否正常工作。此外，检查 ICA 客户端和 Firepower 威胁防御设备之间的网络连接状态，特别注意丢包情况。解决任何异常网络状况后，如果问题仍然存在，请联系思科 TAC。

723013

错误消息：`%ASA-7-723013: WebVPN Citrix encountered invalid connection connection during periodic timeout.`

说明：Firepower 威胁防御内部 Citrix 计时器已过期，且 Citrix 连接无效。

- **connection** - Citrix 连接标识符

建议的操作：检查 Citrix ICA 客户端和 Firepower 威胁防御设备之间以及 Firepower 威胁防御设备和 Citrix 服务器之间的网络连接。解决任何异常网络状况，尤其是延迟和丢包。验证 Firepower 威胁防御设备是否正常工作，特别注意内存或缓冲区问题。如果 Firepower 威胁防御设备处于高负载状态，获取更多内存，升级 Firepower 威胁防御设备或降低负载。如果问题仍然存在，请联系思科 TAC。

723014

错误消息：`%ASA-7-723014: Group group-name , User user-name , IP IP_address : WebVPN Citrix TCP connection connection to server server on channel channel initiated.`

说明：Firepower 威胁防御内部 Citrix 安全网关连接至 Citrix 服务器。

- **group-name** - Citrix 组的名称
- **user-name** - Citrix 用户的名称
- **IP_address** - Citrix 用户的 IP 地址
- **connection** - 连接名称
- server - Citrix 服务器标识符
- channel - Citrix 通道标识符（十六进制）

建议的操作：无需执行任何操作。

724001

错误消息： `%ASA-4-724001: Group group-name User user-name IP IP_addressWebVPN session not allowed.Unable to determine if Cisco Secure Desktop was running on the client's workstation.`

说明： 由于在 Firepower 威胁防御设备上处理 CSD 主机完整性检查结果期间发生错误，不允许此会话。

- **group-name** - 组的名称
- **user-name** - 用户的名称
- **IP_address** - IP 地址

建议的操作： 确定客户端防火墙是否会截断长 URL。从客户端卸载 CSD 并重新连接到 Firepower 威胁防御设备。

724002

错误消息： `%ASA-4-724002: Group group-name User user-name IP IP_addressWebVPN session not terminated.Cisco Secure Desktop was not running on the client's workstation.`

说明： CSD 未在客户端计算机上运行。

- **group-name** - 组的名称
- **user-name** - 用户的名称
- **IP_address** - IP 地址

建议的操作： 验证最终用户是否可以在客户端计算机上安装和运行 CSD。

725001

错误消息： `%ASA-6-725001: Starting SSL handshake with peer-type interface :src-ip /src-port to dst-ip /dst-port for protocol session.`

说明： 已开始与远程设备（可以是客户端或服务器）的 SSL 握手。

- **peer-type** - 服务器或客户端，具体取决于发起连接的设备
- **interface** - SSL 会话使用的接口名称
- **source-ip** - 源 IPv4 或 IPv6 地址
- **src-port** - 源端口号
- **dst-ip** - 目的 IP 地址
- **dst-port** - 目的端口号
- **protocol** - 用于 SSL 握手的 SSL 版本

建议的操作： 无需执行任何操作。

725002

错误消息： `%ASA-6-725002: Device completed SSL handshake with peer-type interface :src-ip /src-port to dst-ip /dst-port for protocol-version session`

说明：已成功完成与远程设备的 SSL 握手。

- **peer-type** - 服务器或客户端，具体取决于发起连接的设备
- **interface** - SSL 会话使用的接口名称
- **source-ip** - 源 IPv4 或 IPv6 地址
- **src-port** - 源端口号
- *dst-ip* - 目的 IP 地址
- *dst-port* - 目的端口号
- *protocol-version* - 正在使用的 SSL 协议版本：SSLv3、TLSv1、DTLSv1、TLSv1.1 或 TLSv1.2

建议的操作：无需执行任何操作。

725003

错误消息：`%ASA-6-725003: SSL peer-type interface :src-ip /src-port to dst-ip /dst-port request to resume previous session.`

说明：远程设备正在尝试恢复之前的 SSL 会话。

- **peer-type** - 服务器或客户端，具体取决于发起连接的设备
- **interface** - SSL 会话使用的接口名称
- **source-ip** - 源 IPv4 或 IPv6 地址
- **src-port** - 源端口号
- *dst-ip* - 目的 IP 地址
- *dst-port* - 目的端口号

建议的操作：无需执行任何操作。

725004

错误消息：`%ASA-6-725004: Device requesting certificate from SSL peer-type interface :src-ip /src-port to dst-ip /dst-port for authentication.`

说明：Firepower 威胁防御设备已请求客户端证书以进行身份验证。

- **peer-type** - 服务器或客户端，具体取决于发起连接的设备
- **interface** - SSL 会话使用的接口名称
- **source-ip** - 源 IPv4 或 IPv6 地址
- **src-port** - 源端口号
- *dst-ip* - 目的 IP 地址
- *dst-port* - 目的端口号

建议的操作：无需执行任何操作。

725005

错误消息：`%ASA-6-725005: SSL peer-type interface :src-ip /src-port to dst-ip /dst-port requesting our device certificate for authentication.`

说明：服务器已请求 Firepower 威胁防御设备的证书以进行身份验证。

- **peer-type** - 服务器或客户端，具体取决于发起连接的设备
- **interface** - SSL 会话使用的接口名称
- **source-ip** - 源 IPv4 或 IPv6 地址
- **src-port** - 源端口号
- *dst-ip* - 目的 IP 地址
- *dst-port* - 目的端口号

建议的操作：无需执行任何操作。

725006

错误消息：`%ASA-6-725006: Device failed SSL handshake with peer-type interface :src-ip /src-port to dst-ip /dst-port`

说明：与远程设备的 SSL 握手失败。

- **peer-type** - 服务器或客户端，具体取决于发起连接的设备
- **interface** - SSL 会话使用的接口名称
- **source-ip** - 源 IPv4 或 IPv6 地址
- **src-port** - 源端口号
- *dst-ip* - 目的 IP 地址
- *dst-port* - 目的端口号

建议的操作：查找系统日志消息 725014，它说明了失败原因。

725007

错误消息：`%ASA-6-725007: SSL session with peer-type interface :src-ip /src-port to dst-ip /dst-port terminated.`

说明：SSL 会话已终止。

- **peer-type** - 服务器或客户端，具体取决于发起连接的设备
- **interface** - SSL 会话使用的接口名称
- **source-ip** - 源 IPv4 或 IPv6 地址
- **src-port** - 源端口号
- *dst-ip* - 目的 IP 地址
- *dst-port* - 目的端口号

建议的操作：无需执行任何操作。

725008

错误消息：`%ASA-7-725008: SSL peer-type interface :src-ip /src-port to dst-ip /dst-port proposes the following n cipher(s).`

说明：列出远程 SSL 设备建议的密式数量。

- **peer-type** - 服务器或客户端，具体取决于发起连接的设备
- **interface** - SSL 会话使用的接口名称
- **source-ip** - 源 IPv4 或 IPv6 地址
- **src-port** - 源端口号
- *dst-ip* - 目的 IP 地址
- *dst-port* - 目的端口号
- *n* - 受支持的密式数量

建议的操作：无需执行任何操作。

725009

错误消息：`%ASA-7-725009 Device proposes the following n cipher(s) peer-type interface :src-ip /src-port to dst-ip /dst-port .`

说明：列出向 SSL 服务器建议的密式数量。

- **peer-type** - 服务器或客户端，具体取决于发起连接的设备
- **interface** - SSL 会话使用的接口名称
- **source-ip** - 源 IPv4 或 IPv6 地址
- **src-port** - 源端口号
- *dst-ip* - 目的 IP 地址
- *dst-port* - 目的端口号
- *n* - 受支持的密式数量

建议的操作：无需执行任何操作。

725010

错误消息：`%ASA-7-725010: Device supports the following n cipher(s).`

说明：列出 Firepower 威胁防御设备支持的用于 SSL 会话的密式数量。

- **n** - 受支持的密式数量

建议的操作：无需执行任何操作。

725011

错误消息：`%ASA-7-725011 Cipher[order ]: cipher_name`

说明：始终关注消息 725008、725009 和 725010，此消息指示密式名称及其首选顺序。

- **order** - 密式列表中密式的顺序
- **cipher_name** - 密式列表中的 OpenSSL 密式名称

建议的操作：无需执行任何操作。

725012

错误消息： `%ASA-7-725012: Device chooses cipher cipher for the SSL session with peer-type interface :src-ip /src-port to dst-ip /dst-port.`

说明： 列出思科设备选择用于 SSL 会话的密式。

- **cipher** - 密式列表中的 OpenSSL 密式名称
- **peer-type** - 服务器或客户端，具体取决于发起连接的设备
- **interface** - SSL 会话使用的接口名称
- **source-ip** - 源 IPv4 或 IPv6 地址
- **src-port** - 源端口号
- *dst-ip* - 目的 IP 地址
- *dst-port* - 目的端口号

建议的操作： 无需执行任何操作。

725013

错误消息： `%ASA-7-725013 SSL peer-type interface :src-ip /src-port to dst-ip /dst-port chooses cipher cipher`

说明： 识别服务器选择用于 SSL 会话的密式。

- **peer-type** - 服务器或客户端，具体取决于发起连接的设备
- **interface** - SSL 会话使用的接口名称
- **source-ip** - 源 IPv4 或 IPv6 地址
- **src-port** - 源端口号
- *dst-ip* - 目的 IP 地址
- *dst-port* - 目的端口号
- **cipher** - 密式列表中的 OpenSSL 密式名称

建议的操作： 无需执行任何操作。

725014

错误消息： `%ASA-7-725014 SSL lib error.Function: function Reason: reason`

说明： 指示 SSL 握手失败的原因。

- **function** - 报告失败的函数名称
- **reason** - 失败情况的说明

建议的操作： 在向思科 TAC 报告任何 SSL 相关问题时添加此消息。

725015

错误消息： `%ASA-3-725015 Error verifying client certificate.Public key size in client certificate exceeds the maximum supported key size.`

说明： 由于不受支持的（大型）密钥大小，SSL 客户端证书验证失败。

建议的操作： 使用密钥大小小于或等于 4096 位的客户端证书。

725016

错误消息： `%ASA-6-725016: Device selects trust-point trustpoint for peer-type interface :src-ip /src-port to dst-ip /dst-port`

说明： 使用服务器名称指示(SNI)，用于给定连接的证书可能并非接口上配置的证书。此外，没有指示选择了哪个证书信任点。此系统日志指示连接使用的信任点（由 *interface*:*src-ip*/*src-port* 指定）。

- *trustpoint* - 用于指定连接的已配置信任点的名称
- *nterface* - Firepower 威胁防御设备上的接口名称
- *src-ip* - 对等体的 IP 地址
- *src-port* - 对等体的端口号
- *dst-ip* - 目标的 IP 地址
- *dst-port* - 目标的端口号

建议的操作： 无需执行任何操作。

725017

错误消息： `%ASA-7-725017: No certificates received during the handshake with %s %s :%B /%d to %B /%d for %s session`

说明： 远程客户端未发送有效证书。

- *remote_device* - 标识是否与客户端或服务器执行了握手
- *ctm->interface* - 发送握手的接口名称
- *ctm->src_ip* - SSL 服务器的 IP 地址，其将与客户端通信
- *ctm->src_port* - SSL 服务器的端口，其将与客户端通信
- *ctm->dst_ip* - 客户端的 IP 地址
- *ctm->dst_port* - 客户端做出响应所使用的端口
- *s->method->version* - 事务中所涉及的协议版本（SSLv3、TLSv1 或 DTLSv1）

建议的操作： 无需执行任何操作。

726001

错误消息： `%ASA-6-726001: Inspected im_protocol im_service Session between Client im_client_1 and im_client_2 Packet flow from src_ifc :/sip /sport to dest_ifc :/dip /dport Action: action Matched Class class_map_id class_map_name`

说明：已对 IM 消息执行 IM 检测且满足指定的条件。已执行所配置的操作。

- *im_protocol* - MSN IM 或 Yahoo IM
- *im_service* - IM 服务，例如聊天、会议、文件传输、语音、视频、游戏或未知
- *im_client_1* , *im_client_2* - 在会话中使用 IM 服务的客户端对等体：*client_login_name* 或“?”
- *src_ifc* - 源接口名称
- *sip* - 源 IP 地址
- *sport* - 源端口
- *dest_ifc* - 目的接口名称
- *dip* - 目标 IP 地址
- *dport* - 目的端口
- *action* - 所采取的操作：重置连接、丢弃连接或接收
- *class_map_id* - 匹配的类映射 ID
- *class_map_name* - 匹配的类映射名称

建议的操作：无需执行任何操作。

733100

错误消息：`%ASA-4-733100: Object drop rate rate_ID exceeded.Current burst rate is rate_val per second, max configured rate is rate_val ; Current average rate is rate_val per second, max configured rate is rate_val ; Cumulative total count is total_cnt`

说明：消息中的指定对象已超出指定的峰值阈值速率或平均阈值速率。此对象可以是主机、TCP/UDP 端口、IP 协议的丢包活动或由潜在攻击导致的各种丢包。Firepower 威胁防御设备可能会受到攻击。

- *Object* - 丢包速率计数的一般或特定来源，可能包括以下各项：

- 防火墙

- 坏包

- 速率限制

- DoS 攻击

- ACL 丢包

- 连接限制

- ICMP 攻击

- 扫描

- SYN 攻击

- 检查

- 接口

（特定接口对象的引用可能有多种形式。例如，您可能会看到 80/HTTP，这将表示使用已知协议 HTTP 的端口 80。）

- *rate_ID* - -超出的配置速率。大多数对象最多可以配置三种不同的速率，用于不同的时间间隔。
- *rate_val* - 特定速率值。
- *total_cnt* - 创建或清除对象之后的总数。

以下三个示例显示了这些变量是如何发生的：

- • 对于由 CPU 或总线限制导致的接口丢包：

```
%ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per second, max
configured rate is 8000; Current average rate is 2030 per second, max configured rate is
2000; Cumulative total count is 3930654."
```

- • 对于由潜在攻击导致的扫描丢包：

```
ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per second_max
configured rate is 10; Current average rate is 245 per second_max configured rate is 5;
Cumulative total count is 147409 (35 instances received)
```

- • 对于由潜在攻击导致的坏包：

```
%ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per second, max
configured rate is 400; Current average rate is 760 per second, max configured rate is 100;
 Cumulative total count is 1938933
```

- • 由于所配置的扫描速率和 **threat-detection rate scanning-rate 3600 average-rate 15** 命令：

```
%ASA-4-733100: [144.60.88.2] drop rate-2 exceeded. Current burst rate is 0 per second, max
 configured rate is 8; Current average rate is 5 per second, max configured rate is 4;
Cumulative total count is 38086
```

根据消息中显示的指定对象类型执行以下步骤：

1. 如果消息中的对象是以下其中一项：
   - 防火墙
   - 坏包
   - 速率限制
   - DoS 攻击
   - ACL 丢包
   - 连接限制
   - ICMP 攻击
   - 扫描
   - SYN 攻击
   - 检测
   - 接口

建议的操作：检查运行环境的丢包速率是否可接受。

1. 使用 threat-detection rate xxx 命令将特定丢包的阈值速率调整为适当的值，其中，*xxx* 为以下其中一项：

- acl-drop
- bad-packet-drop
- conn-limit-drop
- dos-drop
- fw-drop
- icmp-drop
- inspect-drop
- interface-drop
- scanning-threat
- syn-attack

2. 如果消息中的对象是 TCP 或 UDP 端口、IP 地址或主机丢包，检查运行环境的丢包速率是否可接受。
3. 使用 threat-detection rate bad-packet-drop 命令将特定丢包的阈值速率调整为适当的值。

注释 如果您不希望显示丢包速率超出警告，可以使用 no threat-detection basic-threat 命令禁用它。

733101

错误消息：`%ASA-4-733101: Object objectIP (is targeted|is attacking).Current burst rate is rate_val per second, max configured rate is rate_val ; Current average rate is rate_val per second, max configured rate is rate_val ; Cumulative total count is total_cnt.`

说明：Firepower 威胁防御设备检测到特定主机（或同一 1024 节点子网中的多台主机）正在扫描网络（攻击）或正在被扫描（目标）。

- *object* - 攻击者或目标（特定主机或同一 1024 节点子网中的多台主机）
- *objectIP* - 执行扫描的攻击者或被扫描目标的 IP 地址
- *rate_val* - 特定速率值
- *total_cnt* - 总数

以下两个示例显示了这些变量是如何发生的：

```
%ASA-4-733101: Subnet 100.0.0.0 is targeted. Current burst rate is 200 per second, max
configured rate is 0; Current average rate is 0 per second, max configured rate is 0;
Cumulative total count is 2028.
%ASA-4-733101: Host 175.0.0.1 is attacking. Current burst rate is 200 per second, max
configured rate is 0; Current average rate is 0 per second, max configured rate is 0;
Cumulative total count is 2024
```

建议的操作：对于特定主机或子网，使用 **show threat-detection statistics host ip-address ip-mask** 命令检查整体情况，然后将扫描威胁的阈值速率调整为适当的值。 确定适当的值后，可以通过配置 **threat-detection scanning-threat shun-host** 命令，执行可选操作来避开这些主机攻击者（而不是子网攻击者）。您可以在主机规避例外列表中指定某些主机或对象组。有关详细信息，请参阅《CLI 配置指南》。如果扫描检测不可取，您可以使用 **no threat-detection scanning** 命令禁用此功能。

733102

错误消息： `%ASA-4-733102:Threat-detection adds host %I to shun list`

说明： 主机已被威胁检测引擎规避。配置 **threat-detection scanning-threat shun** 命令后，攻击主机将被威胁检测引擎规避。

- *%I* - 特定主机名

以下消息显示了如何执行此命令：

```
%ASA-4-733102: Threat-detection add host 11.1.1.40 to shun list
```

建议的操作： 要调查规避的主机是否是实际的攻击者，请使用 **threat-detection statistics host ip-address** 命令。如果规避的主机不是攻击者，可以使用 **clear threat-detection shun ip address** 命令将规避主机从威胁检测引擎中删除。要从威胁检测引擎中删除所有规避主机，请使用 **clear shun** 命令。

如果由于设置了不适当的阈值速率来触发威胁检测引擎而收到此消息，则使用 **threat-detection rate scanning-threat rate-interval x average-rate y burst-rate z** 命令调整阈值速率。

733103

错误消息： `%ASA-4-733103: Threat-detection removes host %I from shun list`

说明： 主机已被威胁检测引擎规避。使用 **clear-threat-detection shun** 命令时，将从规避列表中删除指定主机。

- *%I* - 特定主机名

以下消息显示了如何执行此命令：

```
%ASA-4-733103: Threat-detection removes host 11.1.1.40 from shun list
```

建议的操作： 无需执行任何操作。

733104

错误消息： `%ASA-4-733104: TD_SYSLOG_TCP_INTERCEPT_AVERAGE_RATE_EXCEED`

说明： 如果被拦截的攻击的平均速率超出所配置的阈值，则Firepower威胁防御设备将遭受攻击并受到 TCP 拦截机制的保护。此消息显示遭受攻击的服务器以及攻击来源。

建议的操作： 编写 ACL 以过滤掉攻击。

733105

错误消息： `%ASA-4-733105: TD_SYSLOG_TCP_INTERCEPT_BURST_RATE_EXCEED`

说明： 如果被拦截的攻击的突发速率超出所配置的阈值，则Firepower威胁防御设备将遭受攻击并受到 TCP 拦截机制的保护。此消息显示遭受攻击的服务器以及攻击来源。

建议的操作： 编写 ACL 以过滤掉攻击。

734001

错误消息： `%ASA-6-734001: DAP: User user, Addr ipaddr , Connection connection : The following DAP records were selected for this connection: DAP record names`

说明： 列出选择用于连接的 DAP 记录。

- *user* - 经过身份验证的用户名
- *ipaddr* - 远程客户端的 IP 地址
- *connection* - 客户端连接类型，可以是以下类型之一：

- IPsec

- AnyConnect

- 无客户端（Web 浏览器）

- 直接转发代理

- L2TP

- *DAP record names* - 以逗号分隔的 DAP 记录名称列表

建议的操作： 无需执行任何操作。

734002

错误消息： `%ASA-5-734002: DAP: User user, Addr ipaddr : Connection terrminated by the following DAP records: DAP record names`

说明： 列出终止连接的 DAP 记录。

- *user* - 经过身份验证的用户名
- *ipaddr* - 远程客户端的 IP 地址
- *DAP record names* - 以逗号分隔的 DAP 记录名称列表

建议的操作： 无需执行任何操作。

734003

错误消息： `%ASA-7-734003: DAP: User name , Addr ipaddr : Session Attribute: attr name/value`

说明： 列出与连接关联的 AAA 和终端会话属性。

- *user* - 经过身份验证的用户名
- *ipaddr* - 远程客户端的 IP 地址
- *attr/value* - AAA 或终端属性的名称和值

建议的操作： 无需执行任何操作。

734004

错误消息： `%ASA-3-734004: DAP: Processing error: internal error code`

说明：发生 DAP 处理错误。

- *internal error code* - 内部错误字符串

建议的操作：启用 **debug dap errors** 命令并重新运行 DAP 处理以获取更多调试信息。如果上述操作没能解决问题，请联系思科 TAC 并提供内部错误代码以及任何有关产生错误的条件的信息。

735001

错误消息：`%ASA-1-735001 IPMI: Cooling Fan var1 : OK`

说明：冷却风扇已恢复正常运行。

- *var1* - 设备编号标记

建议的操作：无需执行任何操作。

735002

错误消息：`%ASA-1-735002 IPMI: Cooling Fan var1 : Failure Detected`

说明：冷却风扇出现故障。

- *var1* - 设备编号标记

建议的操作：执行以下步骤：

1. 检查是否有阻碍风扇旋转的障碍物。
2. 更换冷却风扇。
3. 如果问题仍然存在，记录所显示的消息并联系思科 TAC。

735003

错误消息：`%ASA-1-735003 IPMI: Power Supply var1 : OK`

说明：电源已恢复正常运行。

- *var1* - 设备编号标记

建议的操作：无需执行任何操作。

735004

错误消息：`%ASA-1-735004 IPMI: Power Supply var1 : Failure Detected`

说明：交流电源已丢失，或电源出现故障。

- *var1* - 设备编号标记

建议的操作：执行以下步骤：

1. 检查交流电源故障。
2. 更换电源。

3. 如果问题仍然存在，记录所显示的消息并联系思科 TAC。

735005

错误消息： `%ASA-1-735005 IPMI: Power Supply Unit Redundancy OK`

说明： 电源设备冗余已恢复。

建议的操作： 无需执行任何操作。

735006

错误消息： `%ASA-1-735006 IPMI: Power Supply Unit Redundancy Lost`

说明： 发生电源故障。电源设备冗余已丢失，但Firepower威胁防御设备可在最低资源条件下正常运行。任何其他故障都将导致 Firepower 威胁防御设备关闭。

建议的操作： 要重新获得完全冗余，请执行以下步骤：

1. 检查交流电源故障。
2. 更换电源。
3. 如果问题仍然存在，记录所显示的消息并联系思科 TAC。

735007

错误消息： `%ASA-1-735007 IPMI: CPU var1 : Temp: var2 var3 , Critical`

说明： CPU 已达到临界温度。

- *var1* - 设备编号标记
- *var2* - 温度值
- *var3* - 温度值单位（C、F）

建议的操作： 记录所显示的消息并联系思科 TAC。

735008

错误消息： `%ASA-1-735008 IPMI: Chassis Ambient var1 : Temp: var2 var3 , Critical`

说明： 机箱环境温度传感器达到临界水平。

- *var1* - 设备编号标记
- *var2* - 温度值
- *var3* - 温度值单位（C、F）

建议的操作： 记录所显示的消息并联系思科 TAC。

735009

错误消息： `%ASA-2-735009: IPMI: Environment Monitoring has failed initialization and configuration.Environment Monitoring is not running.`

说明： 初始化期间环境监控出现致命错误，无法继续。

建议的操作： 收集 **show environment** 和 **debug ipmi** 命令的输出。记录所显示的消息并联系思科 TAC。

735010

错误消息： `%ASA-3-735010: IPMI: Environment Monitoring has failed to update one or more of its records.`

说明： 环境监控出现错误，导致暂时无法更新它的一个或多个记录。

建议的操作： 如果重复出现此消息，收集 **show environment driver** 和 **debug ipmi** 命令的输出。记录所显示的消息并联系思科 TAC。

735011

错误消息： `%ASA-1-735011: Power Supply *var1* : Fan OK`

说明： 电源风扇已恢复正常工作状态。

- *var1* - 风扇编号

建议的操作： 无需执行任何操作。

735012

错误消息： `%ASA-1-735012: Power Supply *var1* : Fan Failure Detected`

说明： 电源风扇出现故障。

- *var1* - 风扇编号

建议的操作： 联系思科 TAC 进行故障排除。解决此故障之前关闭设备电源。

735013

错误消息： `%ASA-1-735013: Voltage Channel *var1* : Voltage OK`

说明： 电压通道已恢复正常工作水平。

- *var1* - 电压通道编号

建议的操作： 无需执行任何操作。

735014

错误消息： `%ASA-1-735014: Voltage Channel var1: Voltage Critical`

说明： 电压通道已变为临界水平。

- *var1* - 电压通道编号

建议的操作： 联系思科 TAC 进行故障排除。解决此故障之前关闭设备电源。

735015

错误消息： `%ASA-4-735015: CPU var1 : Temp: var2 var3 , Warm`

说明： CPU 温度高于正常工作温度范围。

- *var1* - CPU 编号
- *var2* - 温度值
- *var3* - 设备

建议的操作： 继续监控此组件，确保其不会达到临界温度。

735016

错误消息： `%ASA-4-735016: Chassis Ambient var1 : Temp: var2 var3 , Warm`

说明： 机箱温度高于正常工作温度范围。

- *var1* - 机箱传感器编号
- *var2* - 温度值
- *var3* - 设备

建议的操作： 继续监控此组件，确保其不会达到临界温度。

735017

错误消息： `%ASA-1-735017: Power Supply var1 : Temp: var2 var3 , OK`

说明： 电源温度已恢复正常工作温度。

- *var1* - 电源编号
- *var2* - 温度值
- *var3* - 设备

建议的操作： 无需执行任何操作。

735018

错误消息： `%ASA-4-735018: Power Supply var1 : Temp: var2 var3 , Critical`

说明： 电源已达到临界工作温度。

- *var1* - 电源编号
- *var2* - 温度值
- *var3* - 设备

建议的操作：联系思科 TAC 进行故障排除。解决此故障之前关闭设备电源。

735019

错误消息：`%ASA-4-735019: Power Supply var1 : Temp: var2 var3 , Warm`

说明：电源温度高于正常工作温度范围。

- *var1* - 电源编号
- *var2* - 温度值
- *var3* - 设备

建议的操作：继续监控此组件，确保其不会达到临界温度。

735020

错误消息：`%ASA-1-735020: CPU var1: Temp: var2 var3 OK`

说明：CPU 温度已恢复正常工作温度。

- *var1* - CPU 编号
- *var2* - 温度值
- *var3* - 设备

建议的操作：无需执行任何操作。

735021

错误消息：`%ASA-1-735021: Chassis var1: Temp: var2 var3 OK`

说明：机箱温度已恢复正常工作温度。

- *var1* - 机箱传感器编号
- *var2* - 温度值
- *var3* - 设备

建议的操作：无需执行任何操作。

735022

错误消息：`%ASA-1-735022: CPU# is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the CPU.`

说明：Firepower 威胁防御设备检测到 CPU 的运行温度超出了最高热工作温度，并将在检测后立即关闭。

建议的操作：需要立即检查机箱和 CPU，以确定是否存在通风问题。

735023

错误消息：`%ASA-2-735023: ASA was previously shutdown due to the CPU complex running beyond the maximum thermal operating temperature.The chassis needs to be inspected immediately for ventilation issues.`

说明：启动时，Firepower 威胁防御设备检测到因 CPU 的运行温度超出了最高安全工作温度而发生关闭事件。使用 **show environment** 命令将指示发生了此事件。

建议的操作：需要立即检查机箱，以确定是否存在通风问题。

735024

错误消息： `%ASA-1-735024: IO Hub` *`var1`* `: Temp:` *`var2 var3`* `, OK`

说明：IO 集线器温度已恢复正常工作温度。

- *ar1* - IO 集线器编号
- *var2* - 温度值
- *var3* - 单位

建议的操作：无需执行任何操作。

735025

错误消息：`%ASA-1-735025: IO Hub` *`var1`* `: Temp:` *`var2 var3`* `, Critical`

说明：IO 集线器温度具有临界温度。

- *ar1* - IO 集线器编号
- *var2* - 温度值
- *var3* - 单位

建议的操作：记录所显示的消息并联系思科 TAC。

735026

错误消息：`%ASA-4-735026: IO Hub` *`var1`* `: Temp:` *`var2 var3`* `, Warm`

说明：IO 集线器温度高于正常工作温度范围。

- *ar1* - IO 集线器编号
- *var2* - 温度值
- *var3* - 单位

建议的操作：继续监控此组件，确保其不会达到临界温度。

735027

错误消息： `%ASA-1-735027: CPU cpu_num Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately.The chassis and CPU need to be inspected immediately for ventilation issues.`

说明： Firepower 威胁防御设备检测到 CPU 调压器的运行温度超出了最高热工作温度，并在检测后立即关闭。

- *cpu_num* - 用于识别经历了热事件的 CPU 调压器的编号

建议的操作： 需要立即检查机箱和 CPU，以确定是否存在通风问题。

735028

错误消息： `%ASA-2-735028: ASA was previously shutdown due to a CPU Voltage Regulator running beyond the max thermal operating temperature.The chassis and CPU need to be inspected immediately for ventilation issues.`

说明： 启动时，Firepower 威胁防御设备检测到因 CPU 调压器的运行温度超出了最高安全工作温度而发生关闭事件。输入 **show environment** 命令，以指示发生了此事件。

建议的操作： 需要立即检查机箱和 CPU，以确定是否存在通风问题。

735029

错误消息： `%ASA-1-735029: IO Hub is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the circuit.`

说明： Firepower 威胁防御设备检测到 IO 集线器的运行温度超出了最高热工作温度，并将在检测后立即关闭。

建议的操作： 需要立即检查机箱和 IO 集线器，以确定是否存在通风问题。

736001

错误消息： `%ASA-2-736001: Unable to allocate enough memory at boot for jumbo-frame reservation.Jumbo-frame support has been disabled.`

说明： 配置巨帧支持时检测到内存不足。因此，已禁用巨帧支持。

建议的操作： 使用 **jumbo-frame reservation** 命令尝试重新启用巨帧支持。保存运行配置并重启 Firepower 威胁防御设备。如果问题仍然存在，请联系思科 TAC。

737001

错误消息： `%ASA-7-737001: IPAA: Received message message-type`

说明： IP 地址分配进程收到一条消息。

- *message-type* - IP 地址分配进程收到的消息

建议的操作：无需执行任何操作。

737002

错误消息：`%ASA-3-737002: IPAA: Received unknown message num variables`

说明：IP 地址分配进程收到一条消息。

- *num* - IP 地址分配进程收到的消息的标识符

建议的操作：无需执行任何操作。

737003

错误消息：`%ASA-5-737003: IPAA: DHCP configured, no viable servers found for tunnel-group tunnel-group`

说明：给定隧道组的 DHCP 服务器配置无效。

- *tunnel-group* - IP 地址分配用于配置的隧道组

建议的操作：验证隧道组的 DHCP 配置。确保 DHCP 服务器处于在线状态。

737004

错误消息：`%ASA-5-737004: IPAA: DHCP configured, request failed for tunnel-group 'tunnel-group'`

说明：给定隧道组的 DHCP 服务器配置无效。

- *tunnel-group* - IP 地址分配用于配置的隧道组

建议的操作：验证隧道组的 DHCP 配置。确保 DHCP 服务器处于在线状态。

737005

错误消息：`%ASA-6-737005: IPAA: DHCP configured, request succeeded for tunnel-group tunnel-group`

说明：DHCP 服务器请求成功。

- *tunnel-group* - IP 地址分配用于配置的隧道组

建议的操作：无需执行任何操作。

737006

错误消息：`%ASA-6-737006: IPAA: Local pool request succeeded for tunnel-group tunnel-group`

说明：本地池请求成功。

- *tunnel-group* - IP 地址分配用于配置的隧道组

建议的操作：无需执行任何操作。

737007

错误消息： `%ASA-5-737007: IPAA: Local pool request failed for tunnel-group tunnel-group`

说明： 本地池请求失败。分配给隧道组的池可能已耗尽。

- *tunnel-group* - IP 地址分配用于配置的隧道组

建议的操作： 使用 **show ip local pool** 命令验证 IP 本地池配置。

737008

错误消息： `%ASA-5-737008: IPAA: 'tunnel-group' not found`

说明： 尝试获取用于配置的 IP 地址时未找到隧道组。软件缺陷可能导致生成此消息。

- *tunnel-group* - IP 地址分配用于配置的隧道组

建议的操作： 检查隧道组配置。联系思科 TAC 并报告问题。

737009

错误消息： `%ASA-6-737009: IPAA: AAA assigned address ip-address , request failed`

说明： 远程访问客户端软件请求使用特定地址。向 AAA 服务器发送的使用此地址的请求失败。此地址可能正在使用。

- *ip-address* - 客户端请求的 IPv4 或 IPv6 地址

建议的操作： 检查 AAA 服务器状态和 IP 本地池的状态。

737010

错误消息： `%ASA-6-737010: IPAA: AAA assigned address ip-address , request succeeded`

说明： 远程访问客户端软件请求使用特定地址并成功接收此地址。

- *ip-address* - 客户端请求的 IPv4 或 IPv6 地址

建议的操作： 无需执行任何操作。

737011

错误消息： `%ASA-5-737011: IPAA: AAA assigned ip-address , not permitted, retrying`

说明： 远程访问客户端软件请求使用特定地址。未配置 **vpn-addr-assign aaa** 命令。将使用备选配置的地址分配方法。

- *ip-address* - 客户端请求的 IPv4 或 IPv6 地址

建议的操作： 如果要允许客户端指定自己的地址，请启用 **vpn-addr-assign aaa** 命令。

737012

错误消息： `%ASA-4-737012: IPAA: Address assignment failed`

说明： 远程访问客户端软件的特定地址请求失败。

- *ip-address* - 客户端请求的 IP 地址

建议的操作： 如果使用 IP 本地池，验证本地池配置。如果使用 AAA，验证 AAA 服务器的配置和状态。如果使用 DHCP，验证 DHCP 服务器的配置和状态。增加日志记录级别（使用通知或信息消息）以获取更多消息来确定失败原因。

737013

错误消息： `%ASA-4-737013: IPAA: Error freeing address ip-address , not found`

说明： Firepower 威胁防御设备尝试释放一个地址，但由于最近的配置更改，此地址不在已分配列表中。

- *ip-address* - 要释放的 IPv4 或 IPv6 地址

建议的操作： 验证地址分配配置。如果再次出现此消息，则可能是由于软件缺陷导致的。联系思科 TAC 并报告问题。

737014

错误消息： `%ASA-6-737014: IPAA: Freeing AAA address ip-address`

说明： Firepower 威胁防御设备成功释放通过 AAA 分配的 IP 地址。

- *ip-address* - 要释放的 IPv4 或 IPv6 地址

建议的操作： 无需执行任何操作。

737015

错误消息： `%ASA-6-737015: IPAA: Freeing DHCP address ip-address`

说明： Firepower 威胁防御设备成功释放通过 DHCP 分配的 IP 地址。

- *ip-address* - 要释放的 IP 地址

建议的操作： 无需执行任何操作。

737016

错误消息： `%ASA-6-737016: IPAA: Freeing local pool address ip-address`

说明： Firepower 威胁防御设备成功释放通过本地池分配的 IP 地址。

- *ip-address* - 要释放的 IPv4 或 IPv6 地址

建议的操作： 无需执行任何操作。

737017

错误消息： `%ASA-6-737017: IPAA: DHCP request attempt num succeeded`

说明： Firepower 威胁防御设备已成功向 DHCP 服务器发送请求。

- *num* - 尝试次数

建议的操作： 无需执行任何操作。

737018

错误消息： `%ASA-5-737018: IPAA: DHCP request attempt num failed`

说明： Firepower 威胁防御设备未能向 DHCP 服务器发送请求。

- *num* - 尝试次数

建议的操作： 验证 DHCP 配置和 DHCP 服务器的连接。

737019

错误消息： `%ASA-4-737019: IPAA: Unable to get address from group-policy or tunnel-group local pools`

说明： Firepower 威胁防御设备未能从组策略或隧道组上配置的本地池中获取地址。本地池可能已耗尽。

建议的操作： 验证本地池的配置和状态。验证本地池的组策略和隧道组配置。

737023

错误消息： `%ASA-5-737023: IPAA: Unable to allocate memory to store local pool address ip-address`

说明： Firepower 威胁防御设备内存不足。

- *ip-address* - 已获取的 IP 地址

建议的操作： Firepower 威胁防御设备可能过载并需要更多内存，或者可能存在软件缺陷导致的内存泄漏。联系思科 TAC 并报告问题。

737024

错误消息： `%ASA-5-737024: IPAA: Client requested address ip-address , already in use, retrying`

说明： 客户端请求了已在使用的 IP 地址。将使用新的 IP 地址尝试此请求。

- *ip-address* - 客户端请求的 IP 地址

建议的操作： 无需执行任何操作。

737025

错误消息： `%ASA-5-737025: IPAA: Duplicate local pool address found, ip-address in quarantine`

说明： 要提供给客户端的 IP 地址已在使用。此 IP 地址已从池中删除，且不会重复使用。

- *ip-address* - 已获取的 IP 地址

建议的操作： 验证本地池的配置；可能存在软件缺陷导致的重叠问题。联系思科 TAC 并报告问题。

737026

错误消息： `%ASA-6-737026: IPAA: Client assigned ip-address from local pool`

说明： 客户端已从本地池分配指定地址。

- *ip-address* - 分配给客户端的 IP 地址

建议的操作： 无需执行任何操作。

737027

错误消息： `%ASA-3-737027: IPAA: No data for address request`

说明： 发现了软件缺陷。

建议的操作： 联系思科 TAC 并报告问题。

737028

错误消息： `%ASA-4-737028: IPAA: Unable to send ip-address to standby: communication failure`

说明： 主用 Firepower 威胁防御设备无法与备用 Firepower 威胁防御设备通信。故障切换对可能不同步。

- *ip-address* - 分配给客户端的 IP 地址

建议的操作： 验证故障切换配置和状态。

737029

错误消息： `%ASA-6-737029: IPAA: Added ip-address to standby`

说明： 备用 Firepower 威胁防御设备已接受 IP 地址分配。

- *ip-address* - 分配给客户端的 IP 地址

建议的操作： 无需执行任何操作。

737030

错误消息： `%ASA-4-737030: IPAA: Unable to send ip-address to standby: address in use`

说明：当主用 Firepower 威胁防御设备尝试获取给定地址时，备用 Firepower 威胁防御设备已在使用此地址。故障切换对可能不同步。

- *ip-address* - 分配给客户端的 IP 地址

建议的操作：验证故障切换配置和状态。

737031

错误消息：`%ASA-6-737031: IPAA: Removed ip-address from standby`

说明：备用 Firepower 威胁防御设备清除了 IP 地址分配。

- *ip-address* - 分配给客户端的 IP 地址

建议的操作：无需执行任何操作。

737032

错误消息：`%ASA-4-737032: IPAA: Unable to remove ip-address from standby: address not found`

说明：当主用 Firepower 威胁防御设备尝试释放备用 Firepower 威胁防御设备时，此备用设备没有正在使用的 IP 地址。故障切换对可能不同步。

- *ip-address* - 分配给客户端的 IP 地址

建议的操作：验证故障切换配置和状态。

737033

错误消息：`%ASA-4-737033: IPAA: Unable to assign addr_allocator provided IP address ip_addr to client.This IP address has already been assigned by previous_addr_allocator`

说明：AAA/DHCP/本地池分配的地址已在使用。

- *addr_allocator* - DHCP/AAA/本地池
- *ip_addr* - DHCP/AAA/本地池分配的 IP 地址
- *previous_ addr_allocator* - 已分配 IP 地址的地址分配器（本地池、AAA 或 DHCP）

建议的操作：验证 AAA/DHCP/本地池地址配置。可能会发生重叠。

737034

错误消息：`%ASA-5-737034: IPAA: Session=<session>, <IP version> address: <explanation>`

说明：IP 地址分配过程无法提供地址。<explanation> 文本将说明原因。

建议的操作：需要执行的操作取决于说明。

737035

错误消息： `%ASA-7-737035: IPAA: Session=<session>, '<message type>' message queued`

说明： 消息已排入IP地址分配队列。此消息与系统日志消息737001相对应。此消息没有速率限制。

建议的操作： 无需执行任何操作。

737036

错误消息： `%ASA-6-737035: IPAA: Session=<session>, Client assigned <address> from DHCP`

说明： IP 地址分配过程已向 VPN 客户端返回了 DHCP 分配的地址。此消息没有速率限制。

建议的操作： 无需执行任何操作。

ID 介于 741000 到 776020 之间的消息

本部分包括 ID 介于 741000 到 776020 之间的消息。

741000

错误消息： `%ASA-6-741000: Coredump filesystem image created on variable 1 -size variable 2 MB`

说明： 核心转储文件系统已成功创建。此文件系统用于通过限制核心转储可能使用的磁盘空间量来管理核心转储。

- *variable 1* - 存放核心转储的文件系统（例如，disk0:、disk1: 和 flash:）
- *variable 2* - 创建的核心转储文件系统的大小 (MB)

建议的操作： 确保在创建核心转储文件系统后保存配置。

741001

错误消息： `%ASA-6-741001: Coredump filesystem image on variable 1 - resized from variable 2 MB to variable 3 MB`

说明： 核心转储文件系统已成功调整大小。

- *variable 1* - 存放核心转储的文件系统
- *variable 2* - 之前的核心转储文件系统的大小 (MB)
- *variable 3* - 当前重新调整大小后的核心转储文件系统的大小 (MB)

建议的操作： 确保在调整核心转储文件系统的大小后保存配置。调整核心转储文件系统的大小会删除现有核心转储文件系统的内容。因此，请确保在调整核心转储文件系统的大小之前存档所有信息。

741002

错误消息： `%ASA-6-741002: Coredump log and filesystem contents cleared on variable 1`

说明： 所有核心转储均已从核心转储文件系统中删除，并且核心转储日志已清除。核心转储文件系统和核心转储日志始终保持彼此同步。

- *variable 1* - 存放核心转储的文件系统（例如，disk0:、disk1: 和 flash:）

建议的操作： 无需执行任何操作。您可以使用 **clear coredump** 命令清除核心转储文件系统，以便将其重置为已知状态。

741003

错误消息： `%ASA-6-741003: Coredump filesystem and its contents removed on variable 1`

说明： 核心转储文件系统及其内容已被删除，核心转储功能已被禁用。

- *variable 1* - 存放核心转储的文件系统（例如，disk0:、disk1: 和 flash:）

建议的操作： 确保在禁用核心转储功能后保存配置。

741004

错误消息： `%ASA-6-741004: Coredump configuration reset to default values`

说明： 核心转储功能处于禁用状态，核心转储配置已重置为其默认值。

建议的操作： 确保在禁用核心转储功能后保存配置。

741005

错误消息： `%ASA-4-741005: Coredump operation variable 1 failed with error variable 2 variable 3`

说明： 执行核心转储相关操作时发生错误。

- *variable 1* - 此变量可以具有以下值：

- CREATE_FSYS - 创建核心转储文件系统时发生错误。

- CLEAR_LOG - 清除核心转储日志时发生错误。

- DELETE_FSYS - 删除核心转储文件系统时发生错误。

- CLEAR_FSYS - 删除核心转储文件系统的内容时发生错误。

- MOUNT_FSYS - 安装核心转储文件系统时发生错误。

- *variable 2* - 十进制数字，提供有关 *variable 1* 中指定的错误原因的其他信息。
- *variable 3* - 与 *variable 2* 关联的描述性 ASCII 字符串。 ASCII 字符串可以具有以下值：

- 核心转储文件已存在

- 无法创建核心转储文件系统

- 无法创建环回设备
- 文件系统类型不受支持
- 无法删除核心转储文件系统
- 无法删除环回设备
- 无法卸载核心转储文件系统
- 无法安装核心转储文件系统
- 无法安装环回设备
- 无法清除核心转储文件系统
- 找不到核心转储文件系统
- 请求的核心转储文件系统过大
- 管理员已中止核心转储操作
- 核心转储命令执行失败
- 发生核心转储 IFS 错误
- 核心转储遇到未识别的错误

建议的操作：确保在配置中禁用核心转储功能，并将消息发送给思科 TAC 以进行进一步分析。

741006

错误消息：`%ASA-4-741006: Unable to write Coredump Helper configuration, reason variable 1`

说明：写入核心转储帮助程序配置文件时发生错误。只有当 disk0: 已满时才会发生此错误。配置文件位于 disk0:.coredumpinfo/coredump.cfg 中。

- *variable 1* - 此变量包含与文件系统相关的基本字符串，该字符串说明了核心转储帮助程序配置文件写入失败的原因。

建议的操作：禁用核心转储功能，从 disk0: 中删除不需要的项目，然后根据需要重新启用核心转储功能。

742001

错误消息：`%ASA-3-742001: failed to read master key for password encryption from persistent store`

说明：启动后，从非易失性存储器中读取主密码加密密钥失败。除非使用 **key config-key password encryption** 命令将主密钥设置为正确的值，否则不会解密配置中的加密密码。

建议的操作：如果配置中存在必须使用的加密密码，请使用 **key config-key password encryption** 命令将主密钥设置为用于加密密码的先前值。如果有未加密的密码或者可以丢弃这些密码，请设置新的主密钥。如果不使用密码加密，则不需要执行任何操作。

742002

错误消息：`%ASA-3-742002: failed to set master key for password encryption`

说明：尝试读取 **key config-key password encryption** 命令失败。此错误可能由以下原因导致：

- 从非安全终端进行配置（例如，通过 Telnet 连接）。
- 已启用故障切换，但它未使用加密链路。
- 其他用户同时也在设置密钥。
- 尝试更改密钥时，旧密钥不正确。
- 密钥过短而不安全。

此错误还可能有其他原因。在这些情况下，将输出实际错误以响应该命令。

建议的操作：更正命令响应中指示的问题。

742003

错误消息：`%ASA-3-742003: failed to save master key for password encryption, reason reason_text`

说明：尝试将主密钥保存到非易失性内存失败。*reason_text* 参数说明了失败的实际原因。原因可能是内存不足，或者非易失性存储可能不一致。

建议的操作：如果问题仍然存在，请使用 **write erase** 命令重新格式化用于保存密钥的非易失性存储。在执行此步骤之前，请确保备份开箱即用配置。然后重新输入 **write erase** 命令。

742004

错误消息：`%ASA-3-742004: failed to sync master key for password encryption, reason reason_text`

说明：尝试将主密钥同步到对等体失败。*reason_text* 参数说明了失败的实际原因。

建议的操作：尝试更正 *reason_text* 参数中指出的问题。

742005

错误消息：`%ASA-3-742005: cipher text enc_pass is not compatible with the configured master key or the cipher text has been tampered with`

说明：尝试解密密码失败。密码可能已使用与当前主密钥不同的主密钥进行加密，或者加密密码的原始格式已被更改。

建议的操作：如果未使用正确的主密钥，请更正此错误。如果加密密码已被修改，请使用新密码重新应用相关配置。

742006

错误消息：`%ASA-3-742006: password decryption failed due to unavailable memory`

说明：尝试解密密码失败，原因是没有可用内存。使用此密码的功能将不会正常工作。

建议的操作：更正内存问题。

742007

错误消息：`%ASA-3-742007: password encryption failed due to unavailable memory`

说明：尝试加密密码失败，原因是没有可用内存。密码可以在配置中以明文形式保留。

建议的操作：更正内存问题，并重新应用密码加密失败的配置。

742008

错误消息：`%ASA-3-742008: password enc_pass decryption failed due to decoding error`

说明：因解码错误导致密码解密失败。如果加密密码在加密后进行了修改，可能会发生这种情况。

建议的操作：使用明文密码重新应用相关配置。

742009

错误消息：`%ASA-3-742009: password encryption failed due to decoding error`

说明：因解码错误导致密码加密失败，这可能是内部软件错误。

建议的操作：使用明文密码重新应用相关配置。如果问题仍然存在，请联系思科 TAC。

742010

错误消息：`%ASA-3-742010: encrypted password enc_pass is not well formed`

说明：命令中提供的加密密码格式不正确。此密码可能不是有效的加密密码，也可能在加密后进行了修改。

- *reason_text* - 代表实际失败原因的字符串
- *enc_pass* - 与问题相关的加密密码

建议的操作：使用明文密码重新应用相关配置。

743000

错误消息：`%ASA-1-743000: The PCI device with vendor ID: vendor_id device ID: device_id located at bus:device.function bus_num:dev_num, func_num has a link link_attr_name of actual_link_attr_val when it should have a link link_attr_name of expected_link_attr_val .`

说明：系统中的 PCI 设备未正确配置，这可能导致系统无法以最佳状态运行。

建议的操作：收集 **show controller pci detail** 命令的输出，并联系思科 TAC。

743001

错误消息： `%ASA-1-743001: Backplane health monitoring detected link failure`

说明： 可能出现了硬件故障，并且在Firepower威胁防御服务模块和交换机机箱之间的其中一条链路上检测到该故障。

建议的操作： 联系思科 TAC。

743002

错误消息： `%ASA-1-743002: Backplane health monitoring detected link OK`

说明： Firepower威胁防御服务模块和交换机机箱之间的链路已恢复。但是，此故障和随后的恢复可能表示存在硬件故障。

建议的操作： 联系思科 TAC。

743004

错误消息： `%ASA-1-743004: System is not fully operational - PCI device with vendor ID vendor_id (vendor_name ), device ID device_id (device_name ) not found`

说明： 系统中找不到保持系统完全正常运行所需的 PCI 设备。

- *vendor_id* - 标识设备供应商的十六进制值
- *vendor_name* - 标识供应商名称的文本字符串
- *device_id* - 标识供应商设备的十六进制值
- *device_name* - 标识设备名称的文本字符串

建议的操作： 收集 **show controller pci detail** 命令的输出，并联系思科 TAC。

743010

错误消息： `%ASA-3-743010: EOBC RPC server failed to start for client module client name .`

说明： 服务器上的 EOBC RPC 服务的特定客户端启动该服务失败。

建议的操作： 致电思科 TAC。

743011

错误消息： `%ASA-3-743011: EOBC RPC call failed, return code code string.`

说明： EOBC RPC 客户端未能向目标服务器发送 RPC。

建议的操作： 致电思科 TAC。

747001

错误消息： %ASA-3-747001: Clustering: Recovered from state machine event queue depleted.Event (*event-id* , *ptr-in-hex* , *ptr-in-hex*) dropped.Current state *state-name* , stack *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex*

说明： 集群 FSM 事件队列已满，并且删除了新事件。

建议的操作： 无。

747002

错误消息： %ASA-5-747002: Clustering: Recovered from state machine dropped event (*event-id* , *ptr-in-hex* , *ptr-in-hex*).Intended state: *state-name* .Current state: *state-name* .

说明： 集群 FSM 收到与当前状态不相配的事件。

建议的操作： 无。

747003

错误消息： %ASA-5-747003: Clustering: Recovered from state machine failure to process event (*event-id* , *ptr-in-hex* , *ptr-in-hex*) at state *state-name* .

说明： 由于给出的各种原因，集群 FSM 未能处理事件。

建议的操作： 无。

747004

错误消息： %ASA-6-747004: Clustering: state machine changed from state *state-name* to *state-name* .

说明： 集群 FSM 已进入新状态。

建议的操作： 无。

747005

错误消息： %ASA-7-747005: Clustering: State machine notify event *event-name* (*event-id* , *ptr-in-hex* , *ptr-in-hex*)

说明： 集群 FSM 向客户端通知了事件。

建议的操作： 无。

747006

错误消息： %ASA-7-747006: Clustering: State machine is at state *state-name*

说明： 集群 FSM 进入稳定状态，即禁用状态、从属状态或者主状态。

建议的操作：无。

747007

错误消息：`%ASA-5-747007: Clustering: Recovered from finding stray config sync thread, stack ptr-in-hex , ptr-in-hex , ptr-in-hex , ptr-in-hex , ptr-in-hex , ptr-in-hex .`

说明：已检测到 Astray 配置同步线程。

建议的操作：无。

747008

错误消息：`%ASA-4-747008: Clustering: New cluster member name with serial number serial-number-A rejected due to name conflict with existing unit with serial number serial-number-B .`

说明：在多台设备上配置了相同设备名称。

建议的操作：无。

747009

错误消息：`%ASA-2-747009: Clustering: Fatal error due to failure to create RPC server for module module name .`

说明：Firepower 威胁防御设备创建 RPC 服务器失败。

建议的操作：禁用此设备上的集群功能并尝试重新启用此功能。如果问题仍然存在，请联系思科 TAC。

747010

错误消息：`%ASA-3-747010: Clustering: RPC call failed, message message-name , return code code-value .`

说明：RPC 调用失败。系统尝试从失败中恢复。

建议的操作：无。

747011

错误消息：`%ASA-2-747011: Clustering: Memory allocation error.`

说明：集群中发生了内存分配失败事件。

建议的操作：禁用此设备上的集群功能并尝试重新启用此功能。如果问题仍然存在，请检查Firepower 威胁防御设备上的内存使用情况。

747012

错误消息： `%ASA-3-747012: Clustering: Failed to replicate global object id hex-id-value in domain domain-name to peer unit-name , continuing operation.`

说明： 全局对象 ID 复制失败。

建议的操作： 无。

747013

错误消息： `%ASA-3-747013: Clustering: Failed to remove global object id hex-id-value in domain domain-name from peer unit-name , continuing operation.`

说明： 全局对象 ID 删除失败。

建议的操作： 无。

747014

错误消息： `%ASA-3-747014: Clustering: Failed to install global object id hex-id-value in domain domain-name , continuing operation.`

说明： 全局对象 ID 安装失败。

建议的操作： 无。

747015

错误消息： `%ASA-4-747015: Clustering: Forcing stray member unit-name to leave the cluster.`

说明： 找到了离群的集群成员。

建议的操作： 无。

747016

错误消息： `%ASA-4-747016: Clustering: Found a split cluster with both unit-name-A and unit-name-B as master units.Master role retained by unit-name-A , unit-name-B will leave, then join as a slave.`

说明： 找到了拆分集群。

建议的操作： 无。

747017

错误消息： `%ASA-4-747017: Clustering: Failed to enroll unit unit-name due to maximum member limit limit-value reached.`

说明： Firepower 威胁防御设备未能注册新设备，因为已达到最大成员数限制。

建议的操作：无。

747018

错误消息：`%ASA-3-747018: Clustering: State progression failed due to timeout in module module-name .`

说明：集群 FSM 进程已超时。

建议的操作：无。

747019

错误消息：`%ASA-4-747019: Clustering: New cluster member name rejected due to Cluster Control Link IP subnet mismatch (ip-address /ip-mask on new unit, ip-address /ip-mask on local unit).`

说明：主设备发现新加入设备的集群接口 IP 地址不匹配。

建议的操作：无。

747020

错误消息：`%ASA-4-747020: Clustering: New cluster member unit-name rejected due to encryption license mismatch.`

说明：主设备发现新加入设备的加密许可证不匹配。

建议的操作：无。

747021

错误消息：`%ASA-3-747021: Clustering: Master unit unit-name is quitting due to interface health check failure on interface-name .`

说明：由于接口运行状况检查失败，因此主设备已禁用集群功能。

建议的操作：无。

747022

错误消息：`%ASA-3-747022: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times, rejoin will be attempted after y min. Failed interface: interface-name .`

说明：在未超出最大重新加入尝试次数的情况下，出现了此系统日志消息。由于在指定的时间内接口运行状况检查失败，因此从属设备已禁用集群功能。在指定的时间（毫秒）后，此设备将自动重新启用。

建议的操作：无。

747025

错误消息： `%ASA-4-747025: Clustering: New cluster member unit-name rejected due to firewall mode mismatch.`

说明： 主设备发现加入设备的防火墙模式不匹配。

建议的操作： 无。

747026

错误消息： `%ASA-4-747026: Clustering: New cluster member unit-name rejected due to cluster interface name mismatch (ifc-name on new unit, ifc-name on local unit).`

说明： 主设备发现加入设备的集群控制链路接口名称不匹配。

建议的操作： 无。

747027

错误消息： `%ASA-4-747027: Clustering: Failed to enroll unit unit-name due to insufficient size of cluster pool pool-name in context-name .`

说明： 由于配置的最小集群池的大小限制，主设备无法注册加入设备。

建议的操作： 无。

747028

错误消息： `%ASA-4-747028: Clustering: New cluster member unit-name rejected due to interface mode mismatch (mode-name on new unit, mode-name on local unit).`

说明： 主设备发现加入设备的接口模式不匹配，无论是跨接口模式还是单个接口模式。

建议的操作： 无。

747029

错误消息： `%ASA-4-747029: Clustering: Unit unit-name is quitting due to Cluster Control Link down.`

说明： 由于出现集群接口故障，因此设备禁用了集群功能。

建议的操作： 无。

747030

错误消息： `%ASA-3-747030: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times (last failure on interface-name ), Clustering must be manually enabled on the unit to re-join.`

说明：接口运行状况检查失败，并且已超出最大重新加入尝试次数。由于接口运行状况检查失败，从属设备已禁用集群功能。

建议的操作：无。

747031

错误消息：`%ASA-3-747031: Clustering: Platform mismatch between cluster master (platform-type ) and joining unit unit-name (platform-type ).unit-name aborting cluster join.`

说明：加入设备的平台类型与集群主设备的平台类型不匹配。

- *unit-name* - 集群引导程序中的设备的名称
- *platform-type* - Firepower 威胁防御平台的类型

建议的操作：确保加入设备与集群主设备具有相同类型的平台。

747032

错误消息：`%ASA-3-747032: Clustering: Service module mismatch between cluster master (module-name ) and joining unit unit-name (module-name )in slot slot-number .unit-name aborting cluster join.`

说明：加入设备的外部模块与集群主设备中的模块不一致（模块类型和安装顺序）。

- *module-name* - 外部模块的名称
- *unit-name* - 集群引导程序中的设备的名称
- *slot-number* - 发生不匹配的插槽的编号

建议的操作：确保加入设备中安装的模块与集群主设备中的模块属于相同类型，并且与集群主设备中的模块顺序相同。

747033

错误消息：`%ASA-3-747033: Clustering: Interface mismatch between cluster master and joining unit unit-name .unit-name aborting cluster join.`

说明：加入设备的接口与集群主设备上的接口不同。

- *unit-name* - 集群引导程序中的设备的名称

建议的操作：确保加入设备上的接口与集群主设备上的接口相同。

747034

错误消息：`%ASA-4-747034: Unit %s is quitting due to Cluster Control Link down (%d times after last rejoin).Rejoin will be attempted after %d minutes.`

说明：集群控制链路处于关闭状态，设备被踢出且尝试了重新加入。

建议的操作：等待设备重新加入。

747035

错误消息： `%ASA-4-747035: Unit %s is quitting due to Cluster Control Link down.Clustering must be manually enabled on the unit to rejoin.`

说明： 集群控制链路处于关闭状态，设备被踢出且没有尝试重新加入。

建议的操作： 手动重新加入该设备。

747036

错误消息： `%ASA-3-747036: Application software mismatch between cluster master %s[Master unit name] (%s[Master application software name]) and joining unit (%s[Joining unit application software name]).%s[Joining member name] aborting cluster join.`

说明： 主设备和加入的从属设备上的应用不相同。从属设备将被踢出。

建议的操作： 确保从属设备运行相同的应用/服务，并手动重新加入该设备。

748001

错误消息： `%ASA-5-748001: Module slot_number in chassis chassis_number is leaving the cluster due to a chassis configuration change`

说明： 在 MIO 中更改了集群控制链路、从 MIO 中删除了集群组，或者在 MIO 配置中删除了板卡模块。

- *slot_number* - 机箱内的板卡插槽 ID
- *chassis_number* - 机箱 ID（对于每个机箱是唯一的）

建议的操作： 无需执行任何操作。

748002

错误消息： `%ASA-4-748002: Clustering configuration on the chassis is missing or incomplete; clustering is disabled`

说明： MIO 中缺少配置或配置不完整（例如，未配置集群组或集群控制链路）。

- *slot_number* - 机箱内的板卡插槽 ID
- *chassis_number* - 机箱 ID（对于每个机箱是唯一的）

建议的操作： 转到MIO控制台并配置集群服务类型，将模块添加到服务类型，并相应地定义集群控制链路。

748003

错误消息： `%ASA-4-748003: Module slot_number in chassis chassis_number is leaving the cluster due to a chassis health check failure`

说明：板卡无法与 MIO 通信，因此它依赖 MIO 来检测此通信问题并对数据端口解除捆绑。如果数据端口已解除捆绑，接口运行状况检查会踢出 Firepower 威胁防御设备。

- *slot_number* - 机箱内的板卡插槽 ID
- *chassis_number* - 机箱 ID（对于每个机箱是唯一的）

建议的操作：检查 MIO 卡是否可以正常运行，或者 MIO 和板卡之间是否仍能正常通信。

748004

错误消息：`%ASA-5-748004: Module slot_number in chassis chassis_number is re-joining the cluster due to a chassis health check recovery`

说明：由于 MIO 板卡运行状况检查已恢复，因此 Firepower 威胁防御设备尝试重新加入集群。

- *slot_number* - 机箱内的板卡插槽 ID
- *chassis_number* - 机箱 ID（对于每个机箱是唯一的）

建议的操作：检查 MIO 卡是否可以正常运行，或者 MIO 和板卡之间是否仍能正常通信

748005

错误消息：`%ASA-3-748005: Failed to bundle the ports for module slot_number in chassis chassis_number ; clustering is disabled`

说明：MIO 未能为自己捆绑端口。

- *slot_number* - 机箱内的板卡插槽 ID
- *chassis_number* - 机箱 ID（对于每个机箱是唯一的）

建议的操作：检查 MIO 是否正常运行。

748006

错误消息：`%ASA-3-748006: Asking module slot_number in chassis chassis_number to leave the cluster due to a port bundling failure`

说明：MIO 未能为板卡捆绑端口，因此板卡已被踢出。

- *slot_number* - 机箱内的板卡插槽 ID
- *chassis_number* - 机箱 ID（对于每个机箱是唯一的）

建议的操作：检查 MIO 是否正常运行。

748007

错误消息：`%ASA-2-748007: Failed to de-bundle the ports for module slot_number in chassis chassis_number ; traffic may be black holed`

说明：MIO 未能取消捆绑端口。

- *slot_number* - 机箱内的板卡插槽 ID

- *chassis_number* - 机箱 ID（对于每个机箱是唯一的）

建议的操作：检查 MIO 是否正常运行。

748008

错误消息：`%ASA-6-748008: [CPU load percentage | memory load percentage ] of module slot_number in chassis chassis_number (member-name ) exceeds overflow protection threshold [CPU percentage | memory percentage ].System may be oversubscribed on member failure.`

说明：CPU 负载已超过 (N-1)/N，其中 N 代表活动集群成员的总数；或者内存负载已超过 (100 - x) * (N - 1) / N + x，其中 N 代表集群成员数，x 是上次加入成员的基准内存使用率。

- *percentage* - CPU 负载或内存负载百分比数据
- *slot_number* - 机箱内的板卡插槽 ID
- *chassis_number* - 机箱 ID（对于每个机箱是唯一的）

建议的操作：重新规划网络和集群部署。减少流量或添加更多的板卡/机箱。

748009

错误消息：`%ASA-6-748009: [CPU load percentage | memory load percentage ] of chassis chassis_number exceeds overflow protection threshold [CPU percentage | memory percentage }.System may be oversubscribed on chassis failure.`

说明：机箱流量负载超出特定阈值。

- *percentage* - CPU 负载或内存负载百分比数据
- *chassis_number* - 机箱 ID（对于每个机箱是唯一的）

建议的操作：重新规划网络和集群部署。减少流量或添加更多的板卡/机箱。

748100

错误消息：`%ASA-3-748100: <application_name> application status is changed from <status> to <status>.`

说明：检测到应用状态从一种状态变为另一种状态。应用状态变化会触发应用运行状况检查机制。

- application name - snort 或 disk_full
- status - 初始、正常、异常

建议的操作：验证应用的状态。

748101

错误消息：`%ASA-3-748101: Peer unit <unit_id> reported its <application_name> application status is <status>.`

说明：对等体设备报告了应用状态更改，此状态更改将触发应用运行状况检查机制。

- unit id - 设备 ID
- application name - snort 或 disk_full
- status - 初始、正常、异常

建议的操作：验证应用的状态。

748102

错误消息：`%ASA-3-748102: Master unit <unit_id> is quitting due to <application_name> Application health check failure, and master's application state is <status>.`

说明：应用运行状况检查检测到主设备运行状况异常。主设备将离开集群组。

- unit id - 设备 ID
- application name - snort 或 disk_full
- status - 初始、正常、异常

建议的操作：验证应用的状态。应用 (snort) 恢复正常运行后，设备将自动重新加入。

748103

错误消息：`%ASA-3-748103: Asking slave unit <unit_id> to quit due to <application_name> Application health check failure, and slave's application state is <status>.`

说明：应用运行状况检查检测到从属设备运行状况异常。主设备将逐出从属节点。

- unit id - 设备 ID
- application name - snort 或 disk_full
- status - 初始、正常、异常

建议的操作：验证应用的状态。应用 (snort) 恢复正常运行后，设备将自动重新加入。

748201

错误消息：`%ASA-4-748201: <Application name> application on module <module id> in chassis <chassis id> is <status>.`

说明：服务链中应用的状态发生了变化。

- status - 正常、异常

建议的操作：验证服务链中应用的状态。

748202

错误消息： `%ASA-3-748202: Module <module_id> in chassis <chassis id> is leaving the cluster due to <application name> application failure\n.`

说明： 如果应用（例如 vDP）出现故障，则设备将被踢出集群。

建议的操作： 验证服务链中应用的状态。

748203

错误消息： `%ASA-5-748203: Module <module_id> in chassis <chassis id> is re-joining the cluster due to a service chain application recovery\n.`

说明： 如果服务链应用（例如 vDP）恢复，设备会自动重新加入集群

建议的操作： 验证服务链中应用的状态。

750001

错误消息： `%ASA-5-750001: Local:`*`local IP`*` :`*`local port`*` Remote:`*`remote IP`*` : `*`remote port`*` Username:`*`username`*` Received request to `*`request`*` an IPsec tunnel; local traffic selector = `*`local selectors: range, protocol, port range`*` ; remote traffic selector = `*`remote selectors: range, protocol, port range`*

说明： 正在请求对 IPsec 隧道执行某项操作，例如密钥更新、建立连接的请求等。

- *local IP:local port* - 此请求的本地 IP 地址。用于此连接的 Firepower 威胁防御 IP 地址和端口号
- *remote IP:remote port* - 此请求的远程 IP 地址。发出连接请求的对等体 IP 地址和端口号
- *username* - 远程访问请求者的用户名（如果已知）或隧道组
- *local selectors* - 本地配置的用于此 IPsec 隧道的流量选择器或代理
- *remote selectors* - 远程对等体请求的用于此 IPsec 隧道的流量选择器或代理

建议的操作： 无需执行任何操作。

750002

错误消息： `%ASA-5-750002: Local:`*`local IP`*` :`*`local port`*` Remote: `*`remote IP`*` : `*`remote port`*` Username:`*`username`*` Received a IKE_INIT_SA request`

说明： 已收到传入的隧道或 SA 发起请求（IKE_INIT_SA 请求）。

- *local IP:local port* - 此请求的本地 IP 地址。用于此连接的 Firepower 威胁防御 IP 地址和端口号
- *remote IP:remote port* - 此请求的远程 IP 地址。发出连接请求的对等体 IP 地址和端口号
- *username* - 远程访问请求者的用户名（如果已知）或隧道组

建议的操作： 无需执行任何操作。

750003

错误消息： `%ASA- 4- 750003: Local: local IP:local port Remote: remote IP:remote port Username: username Negotiation aborted due to ERROR: error`

说明： 出于提供的错误原因，已中止 SA 协商。

- *local IP:local port* - 此请求的本地 IP 地址。用于此连接的 Firepower 威胁防御 IP 地址和端口号
- *remote IP:remote port* - 此请求的远程 IP 地址。发出连接请求的对等体 IP 地址和端口号
- *username* - 远程访问请求者的用户名（如果已知）
- *error* - 中止协商的错误原因。错误原因包括：

- 未能在网络上发送数据

- 异步请求已排入队列

- 未能将数据包排入队列

- 提供的参数不正确

- 未能分配内存

- Cookie 协商失败

- 未能找到匹配的策略

- 未能在数据库中找到项目

- 未能初始化策略数据库

- 未能将策略插入到数据库

- 对等体的建议无效

- 未能计算 DH 值

- 未能构建 NONCE

- 数据包中缺少预期的负载

- 未能计算 SKEYSEED

- 未能创建子 SA 密钥

- 对等体的 KE 负载包含错误的 DH 组

- 收到无效的 KE 通知，但我们已经尝试了所有已配置的 DH 组

- 未能计算散列值

- 未能验证 IKE SA 的身份

- 未能计算或验证签名

- 未能验证证书

- 证书已被撤销，因此无效

- 未能构建或处理证书请求

- 我们请求了证书，但是对等体没有提供证书
- 发送证书链时，对等体没有将其证书作为链中的第一个发送
- 检测到不受支持的 ID 类型
- 未能构建加密的负载
- 未能解密加密的负载
- 检测到数据包中的无效值
- 发起方位在来自原始响应方的数据包中被断言
- 发起方位未在来自原始发起方的数据包中被断言
- 消息响应位在来自交换发起方的数据包中被断言
- 消息响应位未在来自交换响应方的数据包中被断言
- 检测到无效的 IKE SPI
- 数据包为重传
- 检测到无效的协议 ID
- 检测到不受支持的关键负载
- 检测到无效的流量选择器类型
- 未能创建新的 SA
- 未能删除 SA
- 未能将新的 SA 添加到会话 DB 中
- 未能将会话添加到 PSH 中
- 未能从 OSAL 删除会话
- 未能从数据库中删除会话
- 未能将请求添加到 SA
- 限制请求队列超出合理限制，增加对等体的窗口大小
- 收到不在支持的范围内的 IKE 消息 ID
- 检测到不受支持的版本号
- 收到没有选择建议的通知
- 检测到错误通知负载
- 检测到 NAT- d 散列不匹配
- 初始化 SADB 失败
- 初始化会话数据库失败
- 未能获取 PSH

- 协商上下文已锁定，目前正在使用

- 协商上下文没有释放！

- 找到无效的数据状态

- 未能打开 PKI 会话

- 未能插入公钥

- 找不到证书

- 找到不受支持的证书编码，或者虽然对等体已请求 HTTP URL，但从未发送 HTTP_LOOKUP_SUPPORTED 通知

- 至少目前不支持发送捆绑包 URL。但是，支持处理捆绑包 URL

- 本地证书已过期

- 未能构建状态机

- 导航状态机时发生错误

- SM 验证失败

- 找不到协商上下文

- 未能将工作请求添加到 SM Q

- 缺少 Nonce 负载

- 缺少流量选择器负载

- DH 组不受支持

- 预期的密钥对不可用

- 数据包未加密

- 数据包缺少 KE 负载

- 数据包缺少 SA 负载

- SA 无效

- 协商上下文无效

- 未定义远程或本地 ID

- 连接 ID 无效

- 身份验证方法不受支持

- 找不到的 IPsec 策略

- 未能初始化事件优先级队列

- 未能将项目排入列表

- 未能从列表中删除项目

- 数据在事件优先级队列中为空或已损坏

- 未找到本地 IKE 策略
- 由于有正在进行的任务，因此无法删除 IKE SA
- 未收到预期 Cookie 通知
- 未能生成身份验证数据：缺少我的身份验证信息
- 未能生成身份验证数据：未能进行数据签名
- 未能生成身份验证数据：签名操作成功，但无法找到生成的身份验证材料
- 未能在计时器到期之前接收身份验证消息
- 已达到最大重传次数
- 初始交换失败
- 身份验证交换失败
- 创建子交换失败
- 平台错误
- 未能记录消息
- 打开了不需要的调试级别
- 可能还有其他 TS
- 需要一对地址
- 会话无效
- 没有为收到的 TS 找到任何 IPSec 策略
- 无法从窗口中删除请求
- 没有在配置的策略中找到任何建议
- Nat-t 测试失败
- 找不到 PSKEY
- 压缩算法无效
- 未能从平台服务句柄获取配置文件名称
- 未能找到配置文件
- 发起方未能将 IPSec 发送的配置文件与通过对等体 ID 或证书找到的配置文件进行匹配
- 未能从平台服务句柄获取对等体 ID
- 转换属性无效
- 可扩展身份验证协议失败
- 身份验证程序发送了 NULL EAP 消息
- 配置属性无效

- 未能计算数据包散列值
- AAA 上下文已删除
- 无法分配 AAA ID
- 无法分配 AAA 请求
- 无法初始化 AAA 请求
- 未配置身份验证列表
- 未能发送 AAA 请求
- 未能分配 IP 地址
- 消息上下文无效
- 密钥身份验证内存故障
- EAP 方法未生成 MSK
- 未能在平台上注册新的 SA
- 未能异步处理会话注册，错误：%d
- 由于 IPsec 密钥更新冲突，未能插入 SA
- 处理 IPsec 密钥更新冲突失败
- 未能接受导致密钥更新冲突的 SA 上的密钥更新
- 未能启动计时器，以确保对等体将删除 IPsec 冲突 SA SPI %s/%s
- 错误/调试代码和字符串不匹配
- 未能初始化 SA 生命周期
- 未能找到密钥更新 SA
- 未能生成 DH 共享密钥
- 未能检索颁发者公钥散列列表
- 未能构建证书负载
- 未能初始化计时器
- 未能生成 DH 共享密钥
- 未能初始化授权请求
- 从 AAA 收到的作者记录不正确
- 未能从 AAA 获取密钥
- 未能将属性添加到 AAA 请求
- 未能将隧道密码请求发送到 AAA
- 未能分配 AAA 上下文

- 插入策略 AVL 树失败
- 从策略 AVL 树中删除失败
- 策略 AVL 树中找不到任何匹配节点
- 找不到匹配策略
- 找不到匹配建议
- 建议不完整，无法附加到策略
- 建议正在使用中
- 配置的对等体身份验证方法与对等体建议的方法不匹配
- 未能在 OSAL 中找到会话
- 未能分配事件
- 未能创建审计记录
- 不需要审计
- 没有为此会话启动审计
- 已通过 CLI 禁用 NAT-T
- 已达到协商限制，拒绝 SA 请求
- SA 已在协商中，因此无需再次协商
- AAA 组授权失败
- AAA 用户授权失败
- %% 正在删除收到的分段，因为此 SA 未协商分段！
- 已达到此 SA 的最大接收分段数
- 分段数超出允许的最大值
- 组合的数据包长度 %d 大于最大 IKEv2 数据包大小 (%d)
- 收到的分段编号不连续或在错误数据包上设置了 IKEV2_FRAG_FLAG_LAST_FRAGMENT 标记
- 收到的分段无效，因此被删除
- AAA 组授权失败
- AAA 用户授权失败
- 未在 IKEv2 配置文件中配置 AAA 作者
- 未能提取 SKEYID
- 未能将故障切换消息发送到备用设备
- 检测到不受支持的故障切换版本
- 已收到请求，但未启用故障切换

- 已收到主用设备请求，但协商角色为 %s

- 已收到备用设备请求，但协商角色为 %s

- IP 版本无效

- IKEv2 中尚不支持 GDOI

- 未能从平台分配 PSH

- 将会话重定向到另一个网关

- 重定向检查失败

- 重定向检查后，在此网关上接受会话

- 检测到不受支持的重定向网关 ID 类型

- 重定向已接受，发起新请求

- 重定向已接受，清理 IKEv2 SA，平台将发起新请求

- SA 已被重定向，它不应执行任何 CREATE_CHILD_SA 交换

- DH 公钥计算失败

- DH 密钥计算失败

- IN-NEG IKEv2 密钥更新 SA 已被删除

- 证书请求数超出合理限制 (%d)

- 协商上下文已被释放

- 组合的数据包长度 %d 大于最大 IKEv2 数据包大小 (%d)

- 收到的分段编号不连续或在错误数据包上设置了 IKEV2_FRAG_FLAG_LAST_FRAGMENT 标记

- 未在 IKEv2 配置文件中配置 AAA 作者

- 组合的数据包无效，因此被删除

- VCID 上下文无效

建议的操作：查看系统日志，并按日志流程确定此系统日志是否是交换中的最终版本，以及是否是导致潜在故障或重新协商的临时错误的原因。例如，对等体可以通过未配置的KE负载建议DH组，这会导致初始请求失败，但是系统会提供正确的 DH 组，这样对等体就可以在新请求中使用正确的组。

750004

错误消息：`%ASA-5-750004: Local: local IP: local port Remote: remote IP: remote port Username: username Sending COOKIE challenge to throttle possible DoS`

说明：传入的连接请求受到基于 Cookie 挑战阈值的 Cookie 挑战，配置这些阈值是为了防止可能的 DoS 攻击。

- *local IP:local port* - 此请求的本地 IP 地址。用于此连接的 Firepower 威胁防御 IP 地址和端口号

- *remote IP:remote port* - 此请求的远程 IP 地址。发出连接请求的对等体 IP 地址和端口号
- *username* - 远程访问请求者的用户名（如果已知）

建议的操作：无需执行任何操作。

750005

错误消息：`%ASA-5-750005: Local: local IP: local port Remote: remote IP: remote port Username: username IPsec rekey collision detected.I am lowest nonce initiator, deleting SA with inbound SPI SPI`

说明：检测到密钥更新冲突（两个对等体同时尝试发起密钥更新），并已通过保留由此Firepower威胁防御设备发起的密钥更新来解决此冲突，因为它具有最低的随机数。此操作导致 SPI 引用的所示 SA 被删除。

- *local IP:local port* - 此请求的本地 IP 地址。用于此连接的 Firepower 威胁防御 IP 地址和端口号
- *remote IP:remote port* - 此请求的远程 IP 地址。发出连接请求的对等体 IP 地址和端口号
- *username* - 远程访问请求者的用户名（如果已知）
- *SPI* - 通过解决检测到的密钥更新冲突而被删除的 SA 的 SPI 句柄

建议的操作：无需执行任何操作。

750006

错误消息：`%ASA-5-750006: Local: local IP: local port Remote: remote IP: remote port Username: username SA UP.Reason: reason`

说明：SA 因特定原因进入正常运行状态，例如新建立连接或密钥更新。

- *local IP:local port* - 此请求的本地 IP 地址。用于此连接的 Firepower 威胁防御 IP 地址和端口号
- *remote IP:remote port* - 此请求的远程 IP 地址。发出连接请求的对等体 IP 地址和端口号
- *username* - 远程访问请求者的用户名（如果已知）
- *reason* - SA 进入正常运行状态的原因

建议的操作：无需执行任何操作。

750007

错误消息：`%ASA-5-750007: Local: local IP: local port Remote: remote IP: remote port Username: username SA DOWN.Reason: reason`

说明：SA因特定原因被拆散或删除，例如应对等体的请求、操作人员的请求（通过管理员操作）、密钥更新等。

- *local IP:local port* - 此请求的本地 IP 地址。用于此连接的 Firepower 威胁防御 IP 地址和端口号
- *remote IP:remote port* - 此请求的远程 IP 地址。发出连接请求的对等体 IP 地址和端口号
- *username* - 远程访问请求者的用户名（如果已知）
- *reason* - SA 陷入异常状态的原因

建议的操作：无需执行任何操作。

750008

错误消息：`%ASA-5-750008: Local: local IP: local port Remote: remote IP: remote port Username: username SA rejected due to system resource low`

说明：SA 请求被拒绝以缓解系统资源不足的状况。

- *local IP:local port* - 此请求的本地 IP 地址。用于此连接的 Firepower 威胁防御 IP 地址和端口号
- *remote IP:remote port* - 此请求的远程 IP 地址。发出连接请求的对等体 IP 地址和端口号
- *username* - 远程访问请求者的用户名（如果已知）

建议的操作：检查 IKEv2 的 CAC 设置，以根据配置的阈值确定这是否是预期的行为；否则，如果此状况仍然存在，请进一步调查以缓解此问题。

750009

错误消息：`%ASA-5-750009: Local: local IP: local port Remote: remote IP: remote port Username: username SA request rejected due to CAC limit reached: Rejection reason: reason`

说明：达到连接准入控制 (CAC) 限制阈值，这导致了 SA 请求被拒绝。

- *local IP:local port* - 此请求的本地 IP 地址。用于此连接的 Firepower 威胁防御 IP 地址和端口号
- *remote IP:remote port* - 此请求的远程 IP 地址。发出连接请求的对等体 IP 地址和端口号
- *username* - 远程访问请求者的用户名（如果已知）
- *reason* - SA 被拒绝的原因

建议的操作：检查 IKEv2 的 CAC 设置，以根据配置的阈值确定这是否是预期的行为；否则，如果此状况仍然存在，请进一步调查以缓解此问题。

750010

错误消息：`%ASA-5-750010: Local: local-ip Remote: remote-ip Username:username IKEv2 local throttle-request queue depth threshold of threshold reached; increase the window size on peer peer for better performance`

- *local-ip* - 本地对等体 IP 地址
- *remote-ip* - 远程对等体 IP 地址
- *username* - 远程访问请求者的用户名或 L2L 的隧道组名称（如果已知）
- *threshold* - 达到本地限制请求队列的队列深度阈值
- *peer* - 远程对等体 IP 地址

说明：Firepower 威胁防御设备的限制请求队列从指定的对等体溢出，表明对等体处理速度很慢。限制请求队列会搁置发往对等体的请求，这些请求不能立即发送，因为已达到基于 IKEv2 窗口大小允许发送的最大请求数。进行中的请求完成后，请求会从限制请求队列中释放出来并发送到对等体如果对等体未快速处理这些请求，限制队列会执行备份。

建议的操作：如果可能，请增加远程对等体上的 IKEv2 窗口大小，以允许处理更多并发请求，这可以提高性能。

注释 Firepower 威胁防御设备目前不支持增加的 IKEv2 窗口大小设置。

750011

错误消息：`%ASA-3-750011: Tunnel Rejected: Selected IKEv2 encryption algorithm (IKEV2 encry algo ) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo ).`

说明：由于所选择的 IKEv2 加密算法不足以保护建议的 IPSEC 加密算法，因此该隧道被拒绝。

建议的操作：配置更强大的 IKEv2 加密算法，以匹配或超出 IPsec 子 SA 加密算法的强度。

750012

错误消息：`%ASA-4-750012: Selected IKEv2 encryption algorithm (IKEV2 encry algo ) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo ).`

说明：所选择的 IKEv2 加密算法不足以保护建议的 IPSEC 加密算法。

建议的操作：配置更强大的 IKEv2 加密算法，以匹配或超出 IPsec 子 SA 加密算法的强度。

750013

错误消息：`%ASA-5-750013 - IKEv2 SA (iSPI <ISPI> rRSP <rSPI>) Peer Moved: Previous <prev_remote_ip>:<prev_remote_port>/<prev_local_ip>:<prev_local_port>.Updated <new_remote_ip>:<new_remote_port>/<new_local_ip>:<new_local_port>`

说明：新的移动功能允许在不断开隧道的情况下更改对等体 IP。例如，移动设备（智能手机）在连接到其他网络后获取新 IP。以下列表列出了消息值：

- *ip* - 指定之前的 IP 地址、新的本地 IP 地址和远程 IP 地址
- *port* - 指定之前的端口信息、新的本地端口信息和远程端口信息
- *SPI* - 表示发起方和响应方 SPI
- *iSPI* - 指定发起方 SPI
- *rSPI* - 指定响应方 SPI

建议的操作：联系开发工程师。

751001

错误消息：`%ASA-3-751001: Local: localIP:port Remote:remoteIP:port Username: username/group Failed to complete Diffie-Hellman operation.Error: error`

说明：如错误所示，未能完成 Diffie-Hellman 操作。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组
- *error* - 指示特定错误的错误字符串

建议的操作：发生了低内存问题或应解决的其他内部错误。如果问题仍然存在，请使用内存跟踪工具来隔离问题。

751002

错误消息：`%ASA-3-751002: Local: localIP:port Remote:remoteIP:port Username: username/group No preshared key or trustpoint configured for self in tunnel group group`

说明：Firepower威胁防御设备无法在隧道组中找到可用于向对等体验证自身身份的任何类型的身份验证信息。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组
- *group* - 隧道组的名称

建议的操作：检查隧道组的配置，并在指定的隧道组中配置预共享密钥或证书以进行自我身份验证。

751003

错误消息：`%ASA-7-751003: Local: localIP:port Remote:remoteIP:port Username: username/group Need to send a DPD message to peer`

说明：需要对指定的对等体执行失效对等体检测，以确定它是否仍然处于活动状态。Firepower威胁防御设备可能已终止与对等体的连接。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组

建议的操作：无需执行任何操作。

751004

错误消息：`%ASA-3-751004: Local: localIP:port Remote:remoteIP:port Username: username/group No remote authentication method configured for peer in tunnel group group`

说明：在配置中未找到用于验证远程对等体身份的方法以允许连接。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组
- *group* - 隧道组的名称

建议的操作：检查配置以确保存在有效的远程对等体身份验证设置。

751005

错误消息：`%ASA-3-751005: Local: localIP:port Remote:remoteIP:port Username: username/group AnyConnect client reconnect authentication failed.Session ID: sessionID , Error: error`

说明：使用会话令牌尝试重新连接 AnyConnect 客户端期间发生故障。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组
- *sessionID* - 用于尝试重新连接的会话 ID
- *error* - 指示重新连接尝试期间发生的特定错误的错误字符串

建议的操作：如有必要，根据指定的错误采取相应操作。该错误可能表示会话已被删除而不是保持处于恢复状态，这是因为检测到客户端断开连接或已在Firepower威胁防御设备上清除了会话。如有必要，还可将此消息与 Anyconnect 客户端上的事件日志进行比较。

751006

错误消息：`%ASA-3-751006: Local: localIP:port Remote:remoteIP:port Username: username/group Certificate authentication failed.Error: error`

说明：发生与证书身份验证相关的错误。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组
- *error* - 用于指示特定证书身份验证错误的错误字符串

建议的操作：如有必要，根据指定的错误采取相应操作。检查证书信任点配置，并确保存在必要的 CA 证书，以便能够正确验证客户端证书链。使用 **debug crypto ca** 命令来排除此错误。

751007

错误消息：`%ASA-5-751007: Local: localIP:port Remote:remoteIP:port Username: username/group Configured attribute not supported for IKEv2.Attribute:attribute`

说明：已配置的属性无法应用于 IKEv2 连接，因为 IKEv2 连接不支持该属性。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组
- *attribute* - 配置要应用的属性

建议的操作：无需执行任何操作。要杜绝生成此消息，可以删除 IKEv2 配置设置。

751008

错误消息： `%ASA-3-751008: Local: localIP:port Remote:remoteIP:port Username: username/group Group=group , Tunnel rejected: IKEv2 not enabled in group policy`

说明： 根据连接尝试映射至的指定组的已启用协议，并且连接被拒绝，因此不允许使用 IKEv2。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组
- *group* - 用于连接的隧道组

建议的操作： 检查组策略 VPN 隧道协议设置，并根据需要启用 IKEv2。

751009

错误消息： `%ASA-3-751009: Local: localIP:port Remote:remoteIP:port Username: username/group Unable to find tunnel group for peer.`

说明： 找不到对等体的隧道组。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组

建议的操作： 检查配置和隧道组映射规则，然后对其进行配置以允许对等体登陆已配置的组。

751010

错误消息： `%ASA-3-751010: Local: localIP:port Remote:remoteIP:port Username: username/group Unable to determine self-authentication method.No crypto map setting or tunnel group found.`

说明： 在隧道组或加密映射中找不到用于向对等体验证 Firepower 威胁防御设备身份的方法。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组

建议的操作： 检查配置，并在发起方 L2L 的加密映射或适用的隧道组中配置自我身份验证方法。

751011

错误消息： `%ASA-3-751011: Local: localIP:port Remote:remoteIP:port Username: username/group Failed user authentication.Error: error`

说明： 在 EAP 中针对 IKEv2 远程访问连接进行用户身份验证期间发生错误。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组

- *error* - 指示特定错误的错误字符串

建议的操作：确保提供了正确的身份验证凭证，如有必要，进一步调试以确定确切的失败原因。

751012

错误消息：`%ASA-3-751012: Local: localIP:port Remote:remoteIP:port Username: username/group Failure occurred during Configuration Mode processing.Error: error`

说明：将设置应用于连接时，配置模式处理期间发生错误。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组
- *error* - 指示特定错误的错误字符串

建议的操作：根据指示的错误采取相应操作。使用 **debug crypto ikev2** 命令确定错误的原因，或者如有必要，调试此错误指定的所示子系统。

751013

错误消息：`%ASA-3-751013: Local: localIP:port Remote:remoteIP:port Username: username/group Failed to process Configuration Payload request for attribute attribute ID .Error: error`

说明：配置负载请求未能为对等体请求的属性处理并生成配置负载响应。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组
- *attribute ID* - 出现故障的属性 ID
- *error* - 指示特定错误的错误字符串

建议的操作：发生了内存错误、配置错误或其他类型的错误。使用 **debug crypto ikev2** 命令来帮助隔离故障原因。

751014

错误消息：`%ASA-4-751014: Local: localIP:port Remote remoteIP:port Username: username/group Warning Configuration Payload request for attribute attribute ID could not be processed.Error: error`

说明：处理 CP 请求以生成所请求属性的 CP 响应时发生警告。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组
- *attribute ID* - 出现故障的属性 ID
- *error* - 指示特定错误的错误字符串

建议的操作：根据警告中所示的属性和显示的警告消息执行操作。例如，将较新的客户端与较早的 Firepower 威胁防御映像一起使用，而该映像不能理解已添加到客户端的新属性。可能需要升级 Firepower 威胁防御映像，才可以处理该属性。

751015

错误消息：`%ASA-4-751015: Local: localIP:port Remote remoteIP:port Username: username/group SA request rejected by CAC.Reason: reason`

说明：根据配置的阈值或所列原因指示的条件，呼叫准入控制拒绝了连接以保护 Firepower 威胁防御设备。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组
- *reason* - SA 请求被拒绝的原因

建议的操作：如果应接受新连接，请检查原因并解决问题，或者更改配置的阈值。

751016

错误消息：`%ASA-4-751016: Local: localIP:port Remote remoteIP:port Username: username/group L2L peer initiated a tunnel with the same outer and inner addresses.Peer could be Originate only - Possible misconfiguration!`

说明：根据收到的隧道外部和内部 IP 地址，对等体可能配置为用于“仅发起”连接。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组

建议的操作：检查 L2L 对等体的配置。

751017

错误消息：`%ASA-3-751017: Local: localIP:port Remote remoteIP:port Username: username/group Configuration Error error description`

说明：检测到阻止连接的配置错误。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组
- *error description* - 配置错误的简短说明

建议的操作：根据指示的错误更正配置。

751018

错误消息： `%ASA-3-751018: Terminating the VPN connection attempt from attempted group .Reason: This connection is group locked to locked group .`

说明： 尝试连接的隧道组与组锁定中设置的隧道组不同。

- *attempted group* - 建立连接的隧道组
- *locked group* - 连接被锁定或限制的隧道组

建议的操作： 检查组策略中的组锁定值或用户属性。

751019

错误消息： `%ASA-4-751019: Local:LocalAddr Remote:RemoteAddr Username:username Failed to obtain an licenseType license.Maximum license limit limit exceeded.`

说明： 由于超出了最大许可证限制，导致无法发起或响应隧道请求，因此会话创建失败。

- *LocalAddr* - 用于此连接尝试的本地地址
- *RemoteAddr* - 用于此连接尝试的远程对等体地址
- *username* - 对等体尝试连接时使用的用户名
- *licenseType* - 超出限制的许可证类型（其他 VPN 或 AnyConnect Premium/Essentials）
- *limit* - 允许且超出的许可证数量

建议的操作： 确保为所有允许的用户提供足够数量的许可证和/或获取更多许可证以允许拒绝的连接。在多情景模式下，如有必要，请允许报告故障的情景使用更多许可证。

751020

错误消息： `%ASA-3-751020: Local:%A:%u Remote:%A:%u Username:%s An %s remote access connection failed.Attempting to use an NSA Suite B crypto algorithm (%s) without an AnyConnect Premium license.`

说明： 无法创建 IKEv2 远程访问隧道，这是因为虽已应用 AnyConnect Premium 许可证，但在 webvpn 配置模式下使用 **anyconnect-essentials** 命令明确禁用了该许可证。

建议的操作： 确保在远程访问 IKEv2 策略或 Ipsec 建议中配置的 Firepower 威胁防御设备上安装了 AnyConnect Premium 许可证。

751021

错误消息： `%ASA-4-751021: Local:variable 1 :variable 2  Remote:variable 3 :variable 4 Username:variable 5 variable 6 with variable 7 encryption is not supported with this version of the AnyConnect Client.Please upgrade to the latest Anyconnect Client.`

说明： 过期的 AnyConnect 客户端尝试连接到具有配置了 AES-GCM 加密策略的 IKEv2 的 Firepower 威胁防御设备。

- *variable 1* - 本地 IP 地址

- *variable 2* - 本地端口
- *variable 3* - 远程客户端 IP 地址
- *variable 4* - 远程客户端端口
- *variable 5* - AnyConnect 客户端的用户名（可能未知，因为这发生在用户输入用户名之前）
- *variable 6* - 连接协议类型（IKEv1、IKEv2）
- *variable 7* - 组合模式加密类型（AES-GCM、AES-GCM-256）

建议的操作：将 AnyConnect 客户端升级到最新版本方可使用采用 AES-GCM 加密的 IKEv2。

751022

错误消息：`%ASA-3-751022: Local: local-ip Remote: remote-ip Username:username Tunnel rejected: Crypto Map Policy not found for remote traffic selector rem-ts-start /rem-ts-end /rem-ts.startport /rem-ts.endport /rem-ts.protocol local traffic selector local-ts-start /local-ts-end /local-ts.startport /local-ts.endport /local-ts.protocol !`

说明：Firepower 威胁防御设备无法找到消息中所示的专用网络或主机的安全策略信息。这些网络或主机由发起方发送，与 Firepower 威胁防御设备中的任何加密 ACL 均不匹配。这很可能是配置错误。

- *local-ip* - 本地对等体 IP 地址
- *remote-ip* - 远程对等体 IP 地址
- *username* - 远程访问请求者的用户名（如果已知）
- *rem-ts-start* - 远程流量选择器的起始地址
- *rem-ts-end* - 远程流量选择器的结束地址
- *rem-ts.startport* - 远程流量选择器的起始端口
- *rem-ts.endport* - 远程流量选择器的结束端口
- *rem-ts.protocol* - 远程流量选择器的协议
- *local-ts-start* - 本地流量选择器的起始地址
- *local-ts-end* - 本地流量选择器的结束地址
- *local-ts.startport* - 本地流量选择器的起始端口
- *local-ts.endport* - 本地流量选择器的结束端口
- *local-ts.protocol* - 本地流量选择器的协议

建议的操作：检查两端加密 ACL 中受保护的网络配置，并确保发起方的本地网络是响应方的远程网络，反之亦然。与网络地址相比，要特别注意通配符掩码和主机地址。非思科实施可能将专用地址标记为代理地址或“红色”网络。

751023

错误消息：`%ASA-6-751023: Local a :p Remote: a :p Username:n Unknown client connection`

说明：未知的非思科 IKEv2 客户端已连接到 Firepower 威胁防御设备。

- *n* - 组或用户名（具体取决于情景）
- *a* - IP 地址
- *p* - 端口号

- *ua* - 客户端向 Firepower 威胁防御设备提供的用户代理

建议的操作：升级到思科支持的 IKEv2 客户端。

751024

错误消息：`%ASA-3-751024: Local:ip-addr Remote:ip-addr Username:username IKEv2 IPv6 User Filter tempipv6 configured.This setting has been deprecated, terminating connection`

说明：IPv6 VPN 过滤器已弃用，如果为 IPv6 流量访问控制配置了 IPv6 VPN 过滤器而不是统一过滤器，连接将被终止。

建议的操作：为统一过滤器配置 IPv6 条目，以控制用户的 IPv6 流量。

751025

错误消息：`%ASA-5-751025: Local: local IP :local port Remote: remote IP :remote port Username:username Group:group-policy IPv4 Address=assigned_IPv4_addr IPv6 address=assigned_IPv6_addr assigned to session.`

说明：此消息显示为指定用户的 AnyConnect IKEv2 连接分配的 IP 地址信息。

- *local IP* :*local port* - 此请求的本地 IP 地址。用于此连接的 Firepower 威胁防御 IP 地址和端口号
- *remote IP* :*remote port* - 此请求的远程 IP 地址。发出连接请求的对等体 IP 地址和端口号
- *username* - 远程访问请求者的用户名（如果已知）
- *group-policy* - 允许用户获取访问权限的组策略
- *assigned_IPv4_addr* - 分配给该客户端的 IPv4 地址
- *assigned_IPv6_addr* - 分配给该客户端的 IPv6 地址

建议的操作：无需执行任何操作。

751026

错误消息：`%ASA-6-751026: Local: localIP:port Remote: remoteIP:port Username: username/group IKEv2 Client OS: client-os Client: client-name client-version`

说明：指示的用户正在尝试连接所示的操作系统和客户端版本。

- *localIP:port* - 本地 IP 地址和端口号
- *remoteIP:port* - 远程 IP 地址和端口号
- *username/group* - 与此连接尝试关联的用户名或组
- *client-os* - 客户端报告的操作系统
- *client-name* - 客户端报告的客户端名称（通常为 AnyConnect）
- *client-version* - 客户端报告的客户端版本

建议的操作：无需执行任何操作。

751027

错误消息： `%ASA-4-751027: Local:local IP :local port Remote:peer IP :peer port Username:username IKEv2 Received INVALID_SELECTORS Notification from peer.Peer received a packet (SPI=spi).The decapsulated inner packet didn't match the negotiated policy in the SA.Packet destination pkt_daddr , port pkt_dest_port , source pkt_saddr , port pkt_src_port , protocol pkt_prot .`

说明： 对等体在 IPsec 安全关联 (SA) 上接收到的数据包与该 SA 的协商流量描述符不匹配。对等体发送了包含违规数据包的 SPI 和数据包数据的 INVALID_SELECTORS 通知。

- *local IP* - Firepower 威胁防御本地 IP 地址
- *local port* - Firepower 威胁防御本地端口
- *peer IP* - 对等体 IP 地址
- *peer port* - 对等体端口
- *username* - 用户名
- *spi* - 该数据包的 IPsec SA 的 SPI
- *pkt_daddr* - 数据包目的 IP 地址
- *pkt_dest_port* - 数据包目的端口
- *pkt_saddr* - 数据包源 IP 地址
- *pkt_src_port* - 数据包源端口
- *pkt_prot* - 数据包协议

建议的操作： 复制错误消息、配置以及导致此错误的事件的任何详细信息，然后将这些信息提交给思科 TAC。

752001

错误消息： `%ASA-2-752001: Tunnel Manager received invalid parameter to remove record`

说明： 从隧道管理器中删除可能阻止同一对等体的未来隧道启动的记录失败。

建议的操作： 重新加载设备将删除该记录，但如果错误仍然存在或再次发生，请尝试对特定隧道执行其他调试。

752002

错误消息： `%ASA-7-752002: Tunnel Manager Removed entry.Map Tag = mapTag .Map Sequence Number = mapSeq .`

说明： 用于启动隧道的条目已成功删除。

- *mapTag* - 删除了启动条目的加密映射的名称
- *mapSeq* - 删除了启动条目的加密映射的序列号

建议的操作： 无需执行任何操作。

752003

错误消息： `%ASA-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2.Map Tag = mapTag .Map Sequence Number = mapSeq`

说明： 正在尝试启动基于所示加密映射的 IKEv2 隧道。

- *mapTag* - 删除了启动条目的加密映射的名称
- *mapSeq* - 删除了启动条目的加密映射的序列号

建议的操作： 无需执行任何操作。

752004

错误消息： `%ASA-5-752004: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1.Map Tag = mapTag .Map Sequence Number = mapSeq`

说明： 正在尝试启动基于所示加密映射的 IKEv1 隧道。

- *mapTag* - 删除了启动条目的加密映射的名称
- *mapSeq* - 删除了启动条目的加密映射的序列号

建议的操作： 无需执行任何操作。

752005

错误消息： `%ASA-2-752005: Tunnel Manager failed to dispatch a KEY_ACQUIRE message.Memory may be low.Map Tag = mapTag .Map Sequence Number = mapSeq.`

说明： 由于内部错误（例如内存分配失败），尝试调度隧道启动的操作失败。

- *mapTag* - 删除了启动条目的加密映射的名称
- *mapSeq* - 删除了启动条目的加密映射的序列号

建议的操作： 使用内存跟踪工具和其他调试操作来隔离问题。

752006

错误消息： `%ASA-3-752006: Tunnel Manager failed to dispatch a KEY_ACQUIRE message.Probable mis-configuration of the crypto map or tunnel-group.Map Tag = Tag .Map Sequence Number = num, SRC Addr: address port: port Dst Addr: address port: port .`

说明： 由于所示加密映射或关联的隧道组的配置错误，因此尝试调度隧道启动的操作失败。

- *Tag* - 删除了启动条目的加密映射的名称
- *num* - 删除了启动条目的加密映射的序列号
- *address* - 源 IP 地址或目的 IP 地址
- *port* - 源端口号或目的端口号

建议的操作： 检查指示的隧道组和加密映射的配置，确保配置是完整的。

752007

错误消息： `%ASA-3-752007: Tunnel Manager failed to dispatch a KEY_ACQUIRE message.Entry already in Tunnel Manager.Map Tag = mapTag .Map Sequence Number = mapSeq`

说明： 尝试了将现有条目重新添加到隧道管理器。

- *mapTag* - 删除了启动条目的加密映射的名称
- *mapSeq* - 删除了启动条目的加密映射的序列号

建议的操作： 如果问题仍然存在，请确保对等体的配置允许隧道，并进一步调试以确保在隧道启动以及成功或失败的启动尝试期间可正确添加和删除隧道管理器条目。进一步调试 IKE 版本 2 或 IKE 版本 1 连接，因为它们可能仍处于创建隧道的过程中。

752008

错误消息： `%ASA-7-752008: Duplicate entry already in Tunnel Manager`

说明： 发出了重复的隧道启动请求，并且隧道管理器已经在尝试启动隧道。

建议的操作： 无需执行任何操作。如果问题仍然存在，则 IKEv1 或 IKEv2 可能尝试了启动隧道并且尚未超时。使用适用的命令进一步调试，以确保在成功或失败的启动尝试后删除隧道管理器条目。

752009

`%ASA-4-752009: IKEv2 Doesn't support Multiple Peers`

说明： 尝试启动 IKEv2 隧道失败，这是因为加密映射配置了多个对等体，而 IKEv2 不支持多个对等体。只有 IKEv1 支持多个对等体。

建议的操作： 检查配置，以确保 IKEv2 站点对站点启动不需要多个对等体。

752010

错误消息： `%ASA-4-752010: IKEv2 Doesn't have a proposal specified`

说明： 未找到能够启动 IKEv2 隧道的 IPsec 方案。

建议的操作： 检查配置，如有必要，配置可用于启动隧道的 IKEv2 方案。

752011

错误消息： `%ASA-4-752011: IKEv1 Doesn't have a transform set specified`

说明： 未找到能够启动 IKEv2 隧道的 IKEv1 转换集。

建议的操作： 检查配置，如有必要，配置可用于启动隧道的 IKEv2 转换集。

752012

错误消息： `%ASA-4-752012: IKEv protocol was unsuccessful at setting up a tunnel.Map Tag = mapTag .Map Sequence Number = mapSeq .`

说明： 指示的协议未能使用配置的加密映射启动隧道。

- *protocol* - IKE 版本号，对于 IKEv1 而言为 1，对于 IKEv2 而言为 2
- *mapTag* - 删除了启动条目的加密映射的名称
- *mapSeq* - 删除了启动条目的加密映射的序列号

建议的操作： 检查配置，然后在指示的协议中进一步调试，以确定隧道启动尝试失败的原因。

752013

错误消息： `%ASA-4-752013: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2 after a failed attempt.Map Tag = mapTag .Map Sequence Number = mapSeq .`

说明： 隧道管理器在隧道启动尝试失败后再次尝试启动该隧道。

- *mapTag* - 删除了启动条目的加密映射的名称
- *mapSeq* - 删除了启动条目的加密映射的序列号

建议的操作： 检查配置，并确保正确配置了加密映射。然后确定在第二次尝试时是否成功创建了隧道。

752014

错误消息： `%ASA-4-752014: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1 after a failed attempt.Map Tag = mapTag .Map Sequence Number = mapSeq .`

说明： 启动隧道失败后，隧道管理器正在回退并尝试使用 IKEv1 启动隧道。

- *mapTag* - 删除了启动条目的加密映射的名称
- *mapSeq* - 删除了启动条目的加密映射的序列号

建议的操作： 检查配置，并确保正确配置了加密映射。然后确定在第二次尝试时是否成功创建了隧道。

752015

错误消息： `%ASA-3-752015: Tunnel Manager has failed to establish an L2L SA.All configured IKE versions failed to establish the tunnel.Map Tag = mapTag .Map Sequence Number = mapSeq .`

说明： 尝试使用所有已配置的协议后，尝试启动对等体的 L2L 隧道失败。

- *mapTag* - 删除了启动条目的加密映射的名称
- *mapSeq* - 删除了启动条目的加密映射的序列号

建议的操作： 检查配置，并确保正确配置了加密映射。调试各个协议以隔离失败原因。

752016

错误消息： `%ASA-5-752016: IKEv protocol was successful at setting up a tunnel.Map Tag = mapTag .Map Sequence Number = mapSeq.`

说明： 指示的协议（IKEv1 或 IKEv2）已成功创建 L2L 隧道。

- *protocol* - IKE 版本号，对于 IKEv1 而言为 1，对于 IKEv2 而言为 2
- *mapTag* - 删除了启动条目的加密映射的名称
- *mapSeq* - 删除了启动条目的加密映射的序列号

建议的操作： 无需执行任何操作。

752017

错误消息： `%ASA-4-752017: IKEv2 Backup L2L tunnel initiation denied on interface interface matching crypto map name , sequence number number .Unsupported configuration.`

说明： Firepower 威胁防御设备使用 IKEv1 启动连接，因为 IKEv2 不支持备份 L2L 功能。

建议的操作： 如果启用了 IKEv1，则无需执行任何操作。您必须启用 IKEv1 方可使用备份 L2L 功能。

753001

错误消息： `%ASA-4-753001: Unexpected IKEv2 packet received from <IP>:<port>.Error: <reason>`

说明： 如果集群在分布式 VPN 集群模式下运行并且在数据路径中对其执行的早期一致性检查和/或错误检查失败，则收到 IKEv2 数据包时会生成此系统日志。

- <IP> - 发送该数据包的源 IP 地址
- <port> - 发送该数据包的源端口
- <reason> - 将该数据包视为无效的原因。此值可以是 *Corrupted SPI detected* 或 *Expired SPI received*。

建议的操作： 如果启用了 IKEv1，则无需执行任何操作。您必须启用 IKEv1 方可使用备份 L2L 功能。

767001

错误消息： `%ASA-6-767001: Inspect-name : Dropping an unsupported IPv6/IP46/IP64 packet from interface :IP Addr to interface :IP Addr (fail-close)`

说明： 为服务策略设置了故障关闭选项，并且特定检查收到IPv6、IP64或IP46数据包。根据故障关闭选项的设置，系统会生成此系统日志消息并丢弃该数据包。

建议的操作： 无需执行任何操作。

768001

错误消息： `%ASA-3-768001: QUOTA: resource utilization is high: requested req , current curr , warning level level`

说明： 系统资源分配级别已达到其警告阈值。如果是管理会话，则资源是同时管理会话。

- *resource* - 系统资源的名称；在此情况下，是管理会话。
- *req* - 请求的数量；对于管理会话，该值始终是 1。
- *curr* - 当前分配的数量；对于管理会话，该值等于 *level*
- *level* - 警告阈值，即已配置限制的 90%

建议的操作： 无需执行任何操作。

768002

错误消息： `%ASA-3-768002: QUOTA: resource quota exceeded: requested req , current curr , limit limit`

说明： 对系统资源的请求将超出其配置的限制并被拒绝。如果是管理会话，则已达到系统的最大同时管理会话数。

- *resource* - 系统资源的名称；在此情况下，是管理会话。
- *req* - 请求的数量；对于管理会话，该值始终是 1。
- *curr* - 当前分配的数量；对于管理会话，该值等于 *level*
- *limit* - 配置的资源限制

建议的操作： 无需执行任何操作。

768003

错误消息： `%ASA-4-768003: SSH: connection timed out: username username , IP ip`

说明： SSH 会话由于不活动而断开。

- *username* - 用户的名称
- *ip* - 用户的 IP 地址

建议的操作： 无需执行任何操作。

769001

错误消息： `%ASA-5-769001: UPDATE: ASA image src was added to system boot list`

说明： 系统映像已更新。先前下载到系统的文件的名称已添加到系统引导列表中。

- *src* - 源映像文件的名称或 URL

建议的操作： 无需执行任何操作。

769002

错误消息： `%ASA-5-769002: UPDATE: ASA image src was copied to dest`

说明： 系统映像已更新。映像文件已复制到系统。

- *src* - 源映像文件的名称或 URL
- *dest* - 目的映像文件的名称

建议的操作： 无需执行任何操作。

769003

错误消息： `%ASA-5-769003: UPDATE: ASA image src was renamed to dest`

说明： 系统映像已更新。现有映像文件已重命名为系统引导列表中的映像文件名。

- *src* - 源映像文件的名称或 URL
- *dest* - 目的映像文件的名称

建议的操作： 无需执行任何操作。

769004

错误消息： `%ASA-2-769004: UPDATE: ASA image src_file failed verification, reason: failure_reason`

说明： 通过 copy 命令或 verify 命令验证映像失败。

- *src_file* - 源映像文件的文件名或 URL
- *failure_reason* - 目的映像文件的文件名

建议的操作： 可能的失败原因如下：系统内存不足，未在文件中找到映像，校验和失败，未在文件中找到签名，签名无效，签名算法不受支持，签名处理问题

769005

错误消息： `%ASA-5-769005: UPDATE: ASA image image_name passed image verification.`

说明： 这是表示映像已通过验证的通知消息。

- *image_name* - Firepower 威胁防御映像文件的文件名

建议的操作： 无需执行任何操作。

769006

错误消息： `%ASA-3-769006: UPDATE: ASA boot system image image_name was not found on disk.`

说明： 这是一条错误消息，表明在磁盘上找不到在启动系统列表中配置的文件。

- *image_name* - Firepower 威胁防御映像文件的文件名

建议的操作：如果设备未能启动，请更改 boot system 命令以指向有效的文件，或者在重启设备之前将缺失的文件安装到磁盘中。

770001

错误消息：`%ASA-4-770001: Resource resource allocation is more than the permitted list of limit for this platform.If this condition persists, the ASA will be rebooted.`

说明：Firepower 威胁防御虚拟机的 CPU 或内存资源分配已超出此平台的允许限制。除非已根据从 Cisco.com 下载的软件中指定的设置更改了 Firepower 威胁防御虚拟机的设置，否则不会发生这种情况。

建议的操作：要使 Firepower 威胁防御继续运行，请将虚拟机的 CPU 或内存资源分配更改为从 Cisco.com 下载的软件指定的设置，

770002

错误消息：`%ASA-1-770002: Resource resource allocation is more than the permitted limit for this platform.ASA will be rebooted.`

说明：Firepower 威胁防御虚拟机的 CPU 或内存资源分配已超出此平台的允许限制。除非已根据从 Cisco.com 下载的软件中指定的设置更改了 Firepower 威胁防御虚拟机的设置，否则不会发生这种情况。如果未更改资源分配，Firepower 威胁防御设备将继续重新启动。

建议的操作：将虚拟机的 CPU 或内存资源分配更改为从 Cisco.com 下载的软件指定的设置，

770003

错误消息：`%ASA-4-770003: Resource resource allocation is less than the minimum requirement of value for this platform.If this condition persists, performance will be lower than normal.`

说明：Firepower 威胁防御虚拟机的 CPU 或内存资源分配低于此平台的最低要求。If this condition persists, performance will be lower than normal.

建议的操作：要使 Firepower 威胁防御继续运行，请将此虚拟机的 CPU 或内存资源分配更改为从思科下载的软件指定的设置，或查看此平台的思科 *ASA 1000V CLI* 配置指南中指定的内存限制和 CPU 保留设置。

772002

错误消息：`%ASA-3-772002: PASSWORD: console login warning, user username , cause: password expired`

说明：用户使用过期密码登录系统控制台，系统允许用户这样做以避免系统锁定。

- *username* - 用户的名称

建议的操作：用户应更改登录密码。

772003

错误消息：`%ASA-2-772003: PASSWORD: session login failed, user username , IP ip , cause: password expired`

说明：登录的用户尝试使用过期密码登录系统并被拒绝访问。

- *session* - 会话类型，可以是 SSH 或 Telnet
- *username* - 用户的名称
- *ip* - 用户的 IP 地址

建议的操作：如果用户已被授权访问，则管理员必须更改该用户的密码。未经授权的访问尝试应触发相应的响应，例如，阻止来自该 IP 地址的流量。

772004

错误消息：`%ASA-3-772004: PASSWORD: session login failed, user username , IP ip , cause: password expired`

说明：登录的用户尝试使用过期密码登录系统并被拒绝访问。

- *session* - 会话类型，ASDM
- *username* - 用户的名称
- *ip* - 用户的 IP 地址

建议的操作：如果用户已被授权访问，则管理员必须更改该用户的密码。未经授权的访问尝试应触发相应的响应，例如，阻止来自该 IP 地址的流量。

772005

错误消息：`%ASA-6-772005: REAUTH: user username passed authentication`

说明：更改密码后，用户成功通过身份验证。

- *username* - 用户的名称

建议的操作：无需执行任何操作。

772006

错误消息：`%ASA-2-772006: REAUTH: user username failed authentication`

说明：尝试更改密码时，用户输入了错误的密码。因此，密码未能更改。

- *username* - 用户的名称

建议的操作：用户应使用 **change-password** 命令重新尝试更改密码。

774001

错误消息：`%ASA-2-774001: POST: unspecified error`

说明：加密运营商进行通电自检时失败。

建议的操作：联系思科 TAC。

774002

错误消息：`%ASA-2-774002: POST: error err , func func , engine eng , algorithm alg , mode mode , dir dir , key len len`

说明：加密运营商进行通电自检时失败。

- *err* - 失败原因
- *func* - 函数
- *eng* - 引擎，可以是 NPX、Nlite 或软件
- *alg* - 算法，可以是以下任一项：RSA、DSA，DES、3DES、AES、RC4、MD5、SHA1、SHA256、SHA386、SHA512、HMAC-MD5、HMAC-SHA1、HMAC-SHA2 或 AES XCBC
- *mode* - 模式，可以是以下任一项：无、CBC、CTR、CFB、ECB、状态 RC4 或无状态 RC4
- *dir* - 加密或解密
- *len* - 密钥长度（比特）

建议的操作：联系思科 TAC。

第 10 章

系统日志消息 778001-785001 以及 8300001-8300006

本章包含以下各节：

ID 介于 之间以及 778001 到 785001 之间的消息

本部分包括 ID 介于 之间以及 778001 到 785001 的消息。

778001

错误消息： `%ASA-6-778001: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name :(IP-address/port) to ifc-name :(IP-address/port).`

说明： Firepower 威胁防御设备尝试为 VXLAN 数据包创建内部连接，但 VXLAN 数据包的网段 ID 无效。

建议的操作： 无需执行任何操作。

778002

错误消息： `%ASA-6-778002: VXLAN: There is no VNI interface for segment-id segment-id .`

说明： 解封的入口 VXLAN 数据包将被丢弃，这是因为 VXLAN 报头中的网段 ID 与在 Firepower 威胁防御设备上配置的任何 VNI 接口的网段 ID 均不匹配。

建议的操作： 无需执行任何操作。

778003

错误消息： `%ASA-6-778003: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name :(IP-address/port) to ifc-name :(IP-address/port) in FP.`

说明：Firepower 威胁防御快速路径看到网段 ID 无效的 VXLAN 数据包。

建议的操作：检查 VNI 接口网段 ID 的配置，以查看丢弃的数据包是否包含与任何 VNI 网段 ID 配置均不匹配的 VXLAN 网段 ID。

778004

错误消息：`%ASA-6-778004: VXLAN: Invalid VXLAN header for protocol from ifc-name :(IP-address/port) to ifc-name :(IP-address/port) in FP.`

说明：Firepower 威胁防御 VTEP 看到 VXLAN 报头无效的 VXLAN 数据包。

建议的操作：无需执行任何操作。

778005

错误消息：`%ASA-6-778005: VXLAN: Packet with VXLAN segment-id segment-id from ifc-name is denied by FP L2 check.`

说明：VXLAN 数据包被快速路径 L2 检查拒绝。

建议的操作：检查 VNI 接口网段 ID 的配置，以查看丢弃的数据包是否包含与任何 VNI 网段 ID 配置均不匹配的 VXLAN 网段 ID。检查 STS 表是否包含与已丢弃数据包的网段 ID 匹配的条目。

778006

错误消息：`%ASA-6-778006: VXLAN: Invalid VXLAN UDP checksum from ifc-name :(IP-address/port) to ifc-name :(IP-address/port) in FP.`

说明：Firepower 威胁防御 VTEP 收到包含无效 UDP 校验和值的 VXLAN 数据包。

建议的操作：无需执行任何操作。

778007

错误消息：`%ASA-6-778007: VXLAN: Packet from ifc-name :IP-address/port to IP-address/port was discarded due to invalid NVE peer.`

说明：Firepower 威胁防御 VTEP 从不同于已配置的 NVE 对等体的 IP 地址收到 VXLAN 数据包。

建议的操作：无需执行任何操作。

779001

错误消息：`%ASA-6-779001: STS: Out-tag lookup failed for in-tag segment-id of protocol from ifc-name :IP-address /port to IP-address /port .`

说明：Firepower 威胁防御设备尝试为 VXLAN 数据包创建连接，但未能使用 STS 查询表找到 VXLAN 数据包中 in-tag（网段 ID）的 out-tag。

建议的操作：无需执行任何操作。

779002

错误消息： `%ASA-6-779002: STS: STS and NAT locate different egress interface for segment-id segment-id , protocol from ifc-name :IP-address /port to IP-address /port`

说明： Firepower 威胁防御设备尝试为 VXLAN 数据包创建连接，但 STS 查询表和 NAT 策略找到了不同的出口接口。

建议的操作： 无需执行任何操作。

779003

错误消息： `%ASA-3-779003: STS: Failed to read tag-switching table - reason`

说明： Firepower 威胁防御设备尝试读取标签交换表失败。

建议的操作： 无需执行任何操作。

779004

错误消息： `%ASA-3-779004: STS: Failed to write tag-switching table - reason`

说明： Firepower 威胁防御设备尝试写入标签交换表失败。

建议的操作： 无需执行任何操作。

779005

错误消息： `%ASA-3-779005: STS: Failed to parse tag-switching request from http - reason`

说明： Firepower 威胁防御设备尝试解析 HTTP 请求以了解在标签交换表中执行的操作时失败。

建议的操作： 无需执行任何操作。

779006

错误消息： `%ASA-3-779006: STS: Failed to save tag-switching table to flash - reason`

说明： Firepower 威胁防御设备尝试将标签交换表保存到闪存时失败。

建议的操作： 无需执行任何操作。

779007

错误消息： `%ASA-3-779007: STS: Failed to replicate tag-switching table to peer - reason`

说明： Firepower威胁防御设备尝试将标签交换表复制到故障切换备用设备或集群从属设备时失败。

建议的操作： 无需执行任何操作。

785001

错误消息： `%ASA-7-785001: Clustering: Ownership for existing flow from <in_interface>:<src_ip_addr>/<src_port> to <out_interface>:<dest_ip_addr>/<dest_port> moved from unit <old-owner-unit-id> at site <old-site-id> to <new-owner-unit-id> at site <old-site-id> due to <reason>.`

说明： 当集群在 DC 间环境下将流从一个站点中的一台设备移动到另一个站点中的另一台设备时，将生成此系统日志。原因必须是触发移动的任何内容，例如 LISP 通知。

建议的操作： 验证新站点的新设备上的流状态。

ID 介于 803001 到 840001 之间以及 8300001 到 8300006 之间的消息

本部分包含 ID 介于 803001 到 840001 之间以及 8300001 到 8300006 之间的消息。

803001

错误消息： `%ASA-6-803001: bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2`

说明： 向用户发出表示启动后将继续使用硬件旁路的信息消息。

建议的操作： 无需执行任何操作。

错误消息： `%ASA-6-803001: bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/3-1/4`

说明： 向用户发出表示启动后将继续使用硬件旁路的信息消息。

建议的操作： 无需执行任何操作。

803002

错误消息： `%ASA-6-803002: no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2`

说明： 向用户发出表示硬件旁路已手动启用的信息消息。

建议的操作： 无需执行任何操作。

错误消息： `%ASA-6-803002: no protection will be provided by the system for traffic over GigabitEthernet 1/3-1/4`

说明： 向用户发出表示硬件旁路已手动启用的信息消息。

建议的操作： 无需执行任何操作。

803003

错误消息： `%ASA-6-803003: User disabled bypass manually on GigabitEthernet 1/1-1/2.`

说明： 向用户发出表示硬件旁路已手动禁用的信息消息。

建议的操作： 无需执行任何操作。

错误消息： `%ASA-6-803003: User disabled bypass manually on GigabitEthernet 1/3-1/4.`

说明： 向用户发出表示硬件旁路已手动禁用的信息消息。

建议的操作： 无需执行任何操作。

804001

错误消息： `%ASA-6-804001: Interface GigabitEthernet1/3 1000BaseSX SFP has been inserted`

说明： 向用户发出有关在线插入支持的 SFP 模块的信息消息。

建议的操作： 无需执行任何操作。

804002

错误消息： `%ASA-6-804002: Interface GigabitEthernet1/3 SFP has been removed`

说明： 向用户发出有关删除支持的 SFP 模块的信息消息。

建议的操作： 无需执行任何操作。

805001

错误消息： `%ASA-6-805001: Flow offloaded: connection conn_id outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol`

说明： 表示流分流到超快路径。

建议的操作： 无需执行任何操作。

805002

错误消息： `%ASA-6-805002: Flow is no longer offloaded: connection conn_id outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol`

说明： 表示对分流到超快路径的流禁用流分流功能。

建议的操作： 无需执行任何操作。

805003

错误消息： `%ASA-6-805003: Flow is no longer offloaded: connection conn_id outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol`

说明： 表示无法分流流。例如，由于分流流表中的流条目冲突而无法分流流。

建议的操作： 无需执行任何操作。

840001

错误消息： `%ASA-3-840001: Failed to create the backup for an IKEv2 session <Local IP>, <Remote IP>`

说明： 在分布式站点对站点 VPN 的高可用性设置中，当建立 IKEv2 会话或更改集群成员身份时，会尝试创建备份会话。但是，由于容量限制等原因，尝试可能会失败。因此，每当收到创建备份失败的通知时，系统就会在会话所有者的设备上生成此消息。

建议的操作： 无。

8300001

错误消息： `%ASA-6-8300001: VPN session redistribution <variable 1>`

说明： 这些事件通知管理员与“cluster redistribute vpn-sessiondb”相关的操作已启动或已完成。其中，

- <variable 1> - 操作：已启动或已完成

建议的操作： 无。

8300002

错误消息： `%ASA-6-8300002: Moved <variable 1> sessions to <variable 2>`

说明： 提供有关将多少个活动会话移动到了集群的另一个成员的详细信息。

- <variable 1> - 移动的活动会话数量（可以少于请求的数量）
- <variable 2> - 会话移动至的集群成员的名称

建议的操作： 无。

8300003

错误消息： `%ASA-3-8300003: Failed to send session redistribution message to <variable 1>`

说明： 向另一个集群成员发送请求时出错。这可能是由于内部错误或消息所发往的集群成员不可用导致的。

- <variable 1> - 消息所发往的集群成员的名称

建议的操作：如果此消息仍然显示，请联系客户支持部门。

8300004

错误消息：`%ASA-6-8300004: <variable 1> request to move <variable 2> sessions from <variable 3> to <variable 4>`

说明：当集群成员收到来自主设备的请求将特定数量的活动会话移动到该集群中的另一个成员时，将显示此事件。

- <variable 1> - 操作：已接收，已发送
- <variable 2> - 要移动的活动会话的数量
- <variable 3> - 接收移动会话请求的集群成员的名称
- <variable 4> - 接收活动会话的集群成员的名称

建议的操作：无。

8300005

错误消息：`%ASA-3-8300005: Failed to receive session move response from <variable 1>`

说明：集群主设备已请求某个集群成员将活动会话移动至另一个成员。如果主设备在定义的时间段内未收到对此请求的响应，则会显示此事件并终止重新分发进程。

- <variable 1> - 在超时期限内未能发送移动响应的集群成员的名称

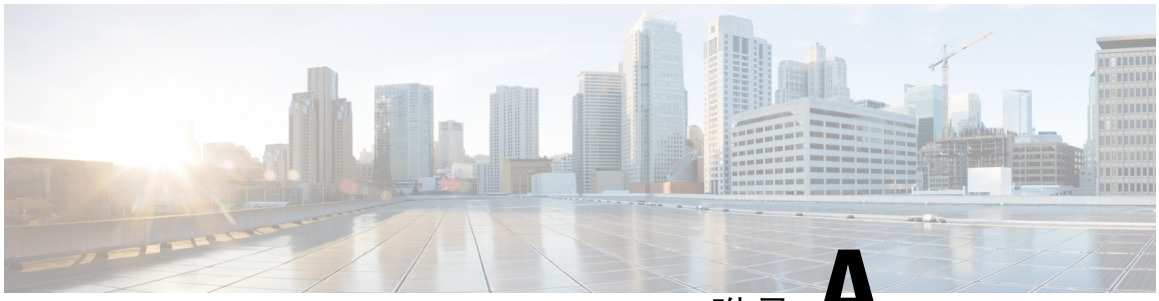
建议的操作：重新发出“cluster redistribute vpn-sessiondb”，如果问题仍然存在，请联系支持部门。

8300006

错误消息：`%ASA-5-8300006: Cluster topology change detected.VPN session redistribution aborted.`

说明：VPN 会话重新分发移动计算基于此过程开始时的活动集群成员数。如果集群成员在此过程中加入或离开，主设备将终止会话的重新分发。

建议的操作：当所有成员加入或离开集群时重试此操作。



附录 A

按严重性级别列出的消息

本附录包含以下部分：

严重性级别为 1 的警报消息

以下警报消息的严重性级别为 1：

- %ASA-1-101001: (Primary) Failover cable OK.
- %ASA-1-101002: (Primary) Bad failover cable.
- %ASA-1-101003: (Primary) Failover cable not connected (this unit).
- %ASA-1-101004: (Primary) Failover cable not connected (other unit).
- %ASA-1-101005: (Primary) Error reading failover cable status.
- %ASA-1-103001: (Primary) No response from other firewall (reason code = code).
- %ASA-1-103002: (Primary) Other firewall network interface interface_number OK.
- %ASA-1-103003: (Primary) Other firewall network interface interface_number failed.
- %ASA-1-103004: (Primary) Other firewall reports this firewall failed.Reason: reason-string
- %ASA-1-103005: (Primary) Other firewall reporting failure.Reason: SSM card failure
- %ASA-1-103006: (Primary|Secondary) Mate version ver_num is not compatible with ours ver_num
- %ASA-1-103007: (Primary|Secondary) Mate version ver_num is not identical with ours ver_num%ASA-1-104001: (Primary) Switching to ACTIVE (cause: string).
- %ASA-1-103008: Mate hwdib index is not compatible.
- %ASA-1-104002: (Primary) Switching to STANDBY (cause: string).
- %ASA-1-104003: (Primary) Switching to FAILED.

按严重性级别列出的消息

- %ASA-1-104004: (Primary) Switching to OK.
- %ASA-1-105001: (Primary) Disabling failover.
- %ASA-1-105002: (Primary) Enabling failover.
- %ASA-1-105003: (Primary) Monitoring on interface interface_name waiting
- %ASA-1-105004: (Primary) Monitoring on interface interface_name normal
- %ASA-1-105005: (Primary) Lost Failover communications with mate on interface interface_name.
- %ASA-1-105006: (Primary) Link status Up on interface interface_name.
- %ASA-1-105007: (Primary) Link status Down on interface interface_name.
- %ASA-1-105008: (Primary) Testing interface interface_name.
- %ASA-1-105009: (Primary) Testing on interface interface_name {Passed|Failed}.
- %ASA-1-105011: (Primary) Failover cable communication failure
- %ASA-1-105020: (Primary) Incomplete/slow config replication
- %ASA-1-105021: (failover_unit) Standby unit failed to sync due to a locked context_name config.Lock held by lock_owner_name
- %ASA-1-105031: Failover LAN interface is up
- %ASA-1-105032: LAN Failover interface is down
- %ASA-1-105034: Receive a LAN_FAILOVER_UP message from peer.
- %ASA-1-105035: Receive a LAN failover interface down msg from peer.
- %ASA-1-105036: dropped a LAN Failover command message.
- %ASA-1-105037: The primary and standby units are switching back and forth as the active unit.
- %ASA-1-105038: (Primary) Interface count mismatch
- %ASA-1-105039: (Primary) Unable to verify the Interface count with mate.Failover may be disabled in mate.
- %ASA-1-105040: (Primary) Mate failover version is not compatible.
- %ASA-1-105041: cmd failed during sync.
- %ASA-1-105042: (Primary) Failover interface OK
- %ASA-1-105043: (Primary) Failover interface failed
- %ASA-1-105044: (Primary) Mate operational mode mode is not compatible with my mode mode.
- %ASA-1-105045: (Primary) Mate license (number contexts) is not compatible with my license (number contexts).
- %ASA-1-105046 (Primary|Secondary) Mate has a different chassis
- %ASA-1-105047: Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
- %ASA-1-105048: (unit) Mate’s service module (application) is different from mine (application)
- %ASA-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name
- %ASA-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name
- %ASA-1-106101 The number of ACL log deny-flows has reached limit (number).
- %ASA-1-107001: RIP auth failed from IP_address: version=number, type=string, mode=string, sequence=number on interface interface_name
- %ASA-1-107002: RIP pkt failed from IP_address: version=number on interface interface_name

- %ASA-1-111111 error_message
- %ASA-1-114001: Failed to initialize 4GE SSM I/O card (error error_string).
- %ASA-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error error_string).
- %ASA-1-114003: Failed to run cached commands in 4GE SSM I/O card (error error_string).
- %ASA-1-1199012: Stack smash during new_stack_call in process/fiber process/fiber, call target f, stack size s, process/fiber name of the process/fiber that caused the stack smash
- %ASA-1-199010: Signal 11 caught in process/fiber(rtcli async executor process)/(rtcli async executor) at address 0xf132e03b, corrective action at 0xca1961a0%ASA-1-199013: syslog
- %ASA-1-199021: System memory utilization has reached the configured watchdog trigger level of Y%.System will now reload
- %ASA-1-211004: WARNING: Minimum Memory Requirement for ASA version ver not met for ASA image. min MB required, actual MB found.
- %ASA-n-216001: internal error in: function: message
- %ASA-1-323006: Module ips experienced a data channel communication failure, data channel is DOWN.
- %ASA-1-332004: Web Cache IP_address/service_ID lost
- %ASA-1-505011: Module ips data channel communication is UP.
- %ASA-1-505014: Module module_id, application down name, version version reason
- %ASA-1-505015: Module module_id, application up application, version version
- %ASA-1-709003: (Primary) Beginning configuration replication: Sending to mate.
- %ASA-1-709004: (Primary) End Configuration Replication (ACT)
- %ASA-1-709005: (Primary) Beginning configuration replication: Receiving from mate.
- %ASA-1-709006: (Primary) End Configuration Replication (STB)
- %ASA-1-713900: Descriptive_event_string.
- %ASA-1-716507: Fiber scheduler has reached unreachable code.Cannot continue, terminating.
- %ASA-1-716508: internal error in: function: Fiber scheduler is scheduling rotten fiber.Cannot continuing terminating
- %ASA-1-716509: internal error in: function: Fiber scheduler is scheduling alien fiber.Cannot continue terminating
- %ASA-1-716510: internal error in: function: Fiber scheduler is scheduling finished fiber.Cannot continue terminating
- %ASA-1-716516: internal error in: function: OCCAM has corrupted ROL array.Cannot continue terminating
- %ASA-1-716519: internal error in: function: OCCAM has corrupted pool list.Cannot continue terminating
- %ASA-1-716528: Unexpected fiber scheduler error; possible out-of-memory condition
- %ASA-1-717049: Local CA Server certificate is due to expire in number days and a replacement certificate is available for export.
- %ASA-1-717054: The type certificate in the trustpoint tp name is due to expire in number days.Expiration date and time Subject Name subject name Issuer Name issuer name Serial Number serial number
- %ASA-1-717055: The type certificate in the trustpoint tp name has expired.Expiration date and time Subject Name subject name Issuer Name issuer name Serial Number serial number
- %ASA-1-735001 Cooling Fan var1: OK
- %ASA-1-735002 Cooling Fan var1: Failure Detected
- %ASA-1-735003 Power Supply var1: OK

- %ASA-1-735004 Power Supply var1: Failure Detected
- %ASA-1-735005 Power Supply Unit Redundancy OK
- %ASA-1-735006 Power Supply Unit Redundancy Lost
- %ASA-1-735007 CPU var1: Temp: var2 var3, Critical
- %ASA-1-735008 IPMI: Chassis Ambient var1: Temp: var2 var3, Critical
- %ASA-1-735011: Power Supply var1: Fan OK
- %ASA-1-735012: Power Supply var1: Fan Failure Detected
- %ASA-1-735013: Voltage Channel var1: Voltage OK
- %ASA-1-735014: Voltage Channel var1: Voltage Critical
- %ASA-1-735017: Power Supply var1: Temp: var2 var3, OK
- %ASA-1-735020: CPU var1: Temp: var2 var3 OK
- %ASA-1-735021: Chassis var1: Temp: var2 var3 OK
- %ASA-1-735022: CPU# is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the CPU.
- %ASA-1-735024: IO Hub var1: Temp: var2 var3, OK
- %ASA-1-735025: IO Hub var1: Temp: var2 var3, Critical
- %ASA-1-735027: CPU cpu_num Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately.The chassis and CPU need to be inspected immediately for ventilation issues.
- %ASA-1-735029: IO Hub is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the circuit.
- %ASA-1-743000: The PCI device with vendor ID: vendor_id device ID: device_id located at bus:device.function bus_num:dev_num, func_num has a link link_attr_name of actual_link_attr_val when it should have a link link_attr_name of expected_link_attr_val.
- %ASA-1-743001: Backplane health monitoring detected link failure
- %ASA-1-743002: Backplane health monitoring detected link OK
- %ASA-1-743004: System is not fully operational - PCI device with vendor ID vendor_id (vendor_name), device ID device_id (device_name) not found
- %ASA-1-770002: Resource resource allocation is more than the permitted limit for this platform.ASA will be rebooted.

严重性级别为 2 的重要消息

以下严重消息的严重性级别为 2：

- %ASA-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name
- %ASA-2-106002: protocol Connection denied by outbound list acl_ID src inside_address dest outside_address
- %ASA-2-106006: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port on interface interface_name.
- %ASA-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}.

- %ASA-2-106013: Dropping echo request from IP_address to PAT address IP_address
- %ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.
- %ASA-2-106017: Deny IP due to Land Attack from IP_address to IP_address
- %ASA-2-106018: ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address
- %ASA-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address
- %ASA-2-106024: Access rules memory exhausted
- %ASA-2-108003: Terminating ESMTP/SMTP connection; malicious pattern detected in the mail address from source_interface:source_address/source_port to dest_interface:dest_address/dset_port.Data:string
- %ASA-2-109011: Authen Session Start: user 'user', sid number
- %ASA-2-112001: (string:dec) Clear complete.
- %ASA-2-113022: AAA Marking RADIUS server servername in aaa-server group AAA-Using-DNS as FAILED
- %ASA-2-113023: AAA Marking protocol server ip-addr in server group tag as ACTIVE
- %ASA-2-113027: Username could not be found in certificate
- %ASA-2-115000: Critical assertion in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition
- %ASA-2-199011: Close on bad channel in process/fiber process/fiber, channel ID p, channel state s process/fiber name of the process/fiber that caused the bad channel close operation.
- %ASA-2-199014: syslog
- %ASA-2-199020: System memory utilization has reached X%.System will reload if memory usage reaches the configured trigger level of Y%.
- %ASA-2-201003: Embryonic limit exceeded nconns/elimit for outside_address/outside_port (global_address) inside_address/inside_port on interface interface_name
- %ASA-2-214001: Terminating manager session from IP_address on interface interface_name.Reason: incoming encrypted data (number bytes) longer than number bytes
- %ASA-2-215001:Bad route_compress() call, sdb= number
- %ASA-2-217001: No memory for string in string
- %ASA-2-218001: Failed Identification Test in slot# [fail#/res].
- %ASA-2-218002: Module (slot#) is a registered proto-type for Cisco Lab use only, and not certified for live network operation.
- %ASA-2-218003: Module Version in slot# is obsolete.The module in slot = slot# is obsolete and must be returned via RMA to Cisco Manufacturing.If it is a lab unit, it must be returned to Proto Services for upgrade.
- %ASA-2-218004: Failed Identification Test in slot# [fail#/res]
- %ASA-2-218005: Inconsistency detected in the system information programmed in non-volatile memory
- %ASA-2-321005: System CPU utilization reached utilization %
- %ASA-2-321006: System memory usage reached utilization %
- %ASA-2-410002: Dropped num DNS responses with mis-matched id in the past sec second(s): from src_ifc:sip/sport to dest_ifc:dip/dport
- %ASA-2-709007: Configuration replication failed for command command
- %ASA-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available_size, used value

按严重性级别列出的消息

- %ASA-2-713176: Device_type memory resources are critical, IKE key acquire message on interface interface_number, for Peer IP_address ignored
- %ASA-2-713901: Descriptive_text_string.
- %ASA-2-716500: internal error in: function: Fiber library cannot locate AK47 instance
- %ASA-2-716501: internal error in: function: Fiber library cannot attach AK47 instance
- %ASA-2-716502: internal error in: function: Fiber library cannot allocate default arena
- %ASA-2-716503: internal error in: function: Fiber library cannot allocate fiber descriptors pool
- %ASA-2-716504: internal error in: function: Fiber library cannot allocate fiber stacks pool
- %ASA-2-716505: internal error in: function: Fiber has joined fiber in unfinished state
- %ASA-2-716506: UNICORN_SYSLOGID_JOINED_UNEXPECTED_FIBER
- %ASA-2-716512: internal error in: function: Fiber has joined fiber waited upon by someone else
- %ASA-2-716513: internal error in: function: Fiber in callback blocked on other channel
- %ASA-2-716515: internal error in: function: OCCAM failed to allocate memory for AK47 instance
- %ASA-2-716517: internal error in: function: OCCAM cached block has no associated arena
- %ASWA-2-716518: internal error in: function: OCCAM pool has no associated arena
- %ASA-2-716520: internal error in: function: OCCAM pool has no block list
- %ASA-2-716521: internal error in: function: OCCAM no realloc allowed in named pool
- %ASA-2-716522: internal error in: function: OCCAM corrupted standalone block
- %ASA-2-716525: UNICORN_SYSLOGID_SAL_CLOSE_PRIVDATA_CHANGED
- %ASA-2-716526: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_LOAD_FAIL
- %ASA-2-716527: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_STORE_FAI
- %ASA-2-717008: Insufficient memory to process_requiring_memory.
- %ASA-2-717011: Unexpected event event event_ID
- %ASA-2-735009: IPMI: Environment Monitoring has failed initialization and configuration.Environment Monitoring is not running.
- %ASA-2-735023: ASA was previously shutdown due to the CPU complex running beyond the maximum thermal operating temperature.The chassis needs to be inspected immediately for ventilation issues.
- %ASA-2-735028: ASA was previously shutdown due to a CPU Voltage Regulator running beyond the max thermal operating temperature.The chassis and CPU need to be inspected immediately for ventilation issues.
- %ASA-2-736001: Unable to allocate enough memory at boot for jumbo-frame reservation.Jumbo-frame support has been disabled.
- %ASA-2-747009: Clustering: Fatal error due to failure to create RPC server for module module name.
- %ASA-2-747011: Clustering: Memory allocation error.%ASA-2-752001: Tunnel Manager received invalid parameter to remove record.
- %ASA-2-748007: Failed to de-bundle the ports for module slot_number in chassis chassis_number; traffic may be black holed
- %ASA-2-752001: Tunnel Manager received invalid parameter to remove record.
- %ASA-2-752005: Tunnel Manager failed to dispatch a KEY_ACQUIRE message.Memory may be low.Map Tag = mapTag.Map Sequence Number = mapSeq.
- %ASA-2-772003: PASSWORD: session login failed, user username, IP ip, cause: password expired
- %ASA-2-772006: REAUTH: user username failed authentication
- %ASA-2-774001: POST: unspecified error

- %ASA-2-774002: POST: error err, func func, engine eng, algorithm alg, mode mode, dir dir, key len len

严重性级别为 3 的错误消息

以下错误消息的严重性级别为 3：

- %ASA-3-105010: (Primary) Failover message block alloc failed
- %ASA-3-106010: Deny inbound protocol src [interface_name: source_address/source_port] [([idfw_user | FQDN_string], sg_info)] dst [interface_name: dest_address/dest_port}[([idfw_user | FQDN_string], sg_info)]
- %ASA-3-106011: Deny inbound (No xlate) string
- %ASA-3-106014: Deny inbound icmp src interface_name: IP_address [([idfw_user | FQDN_string], sg_info)] dst interface_name: IP_address [([idfw_user | FQDN_string], sg_info)] (type dec, code dec)
- %ASA-3-109013: User must authenticate before using this service
- %ASA-3-109016: Can't find authorization ACL acl_ID for user 'user'
- %ASA-3-109018: Downloaded ACL acl_ID is empty
- %ASA-3-109019: Downloaded ACL acl_ID has parsing error; ACE string
- %ASA-3-109020: Downloaded ACL has config error; ACE
- %ASA-3-109026: [aaa protocol] Invalid reply digest received; shared server key may be mismatched.
- %ASA-3-109032: Unable to install ACL access_list, downloaded for user username; Error in ACE: ace.
- %ASA-3-109037: Exceeded 5000 attribute values for the attribute name attribute for user username
- %ASA-3-109038: Attribute internal-attribute-name value string-from-server from AAA server could not be parsed as a type internal-attribute-name string representation of the attribute name
- %ASA-3-109103: CoA action-type from coa-source-ip failed for user username, with session ID: audit-session-id.
- %ASA-3-109104: CoA action-type from coa-source-ip failed for user username, session ID: audit-session-id. Action not supported.
- %ASA-3-113001: Unable to open AAA session.Session limit [limit] reached.
- %ASA-3-113018: User: user, Unsupported downloaded ACL Entry: ACL_entry, Action: action
- %ASA-3-113020: Kerberos error: Clock skew with server ip_address greater than 300 seconds
- %ASA-3-113021: Attempted console login failed.User username did NOT have appropriate Admin Rights.
- %ASA-3-114006: Failed to get port statistics in 4GE SSM I/O card (error error_string).
- %ASA-3-114007: Failed to get current msr in 4GE SSM I/O card (error error_string).
- %ASA-3-114008: Failed to enable port after link is up in 4GE SSM I/O card due to either I2C serial bus access error or switch access error.
- %ASA-3-114009: Failed to set multicast address in 4GE SSM I/O card (error error_string).
- %ASA-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error error_string).
- %ASA-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error error_string).
- %ASA-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error error_string).
- %ASA-3-114013: Failed to set mac address table in 4GE SSM I/O card (error error_string).
- %ASA-3-114014: Failed to set mac address in 4GE SSM I/O card (error error_string).

按严重性级别列出的消息

- %ASA-3-114015: Failed to set mode in 4GE SSM I/O card (error error_string).
- %ASA-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error error_string).
- %ASA-3-114017: Failed to get link status in 4GE SSM I/O card (error error_string).
- %ASA-3-114018: Failed to set port speed in 4GE SSM I/O card (error error_string).
- %ASA-3-114019: Failed to set media type in 4GE SSM I/O card (error error_string).
- %ASA-3-114020: Port link speed is unknown in 4GE SSM I/O card.
- %ASA-3-114021: Failed to set multicast address table in 4GE SSM I/O card due to error.
- %ASA-3-114022: Failed to pass broadcast traffic in 4GE SSM I/O card due to error_string
- %ASA-3-114023: Failed to cache/flush mac table in 4GE SSM I/O card due to error_string.
- %ASA-3-115001: Error in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition.
- %ASA-3-199015: syslog
- %ASA-3-201002: Too many TCP connections on {static|xlate} global_address! econns nconns
- %ASA-3-201004: Too many UDP connections on {static|xlate} global_address! udp connections limit
- %ASA-3-201005: FTP data connection failed for IP_address IP_address
- %ASA-3-201006: RCMD backconnection failed for IP_address/port.
- %ASA-3-201008: Disallowing new connections.
- %ASA-3-201009: TCP connection limit of number for host IP_address on interface_name exceeded
- %ASA-3-201011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name.
- %ASA-3-201013: Per-client connection limit exceeded curr num/limit for [input|output] packet from ip/port to ip/port on interface interface_name
- %ASA-3-202010: [NAT | PAT] pool exhausted for pool-name, port range [1-511 | 512-1023 | 1024-65535].Unable to create protocol connection from in-interface:src-ip/src-port to out-interface:dst-ip/dst-port
- %ASA-3-208005: (function:line_num) clear command return code
- %ASA-3-210001: LU sw_module_name error = number
- %ASA-3-210002: LU allocate block (bytes) failed.
- %ASA-3-210003: Unknown LU Object number
- %ASA-3-210005: LU allocate secondary(optional) connection failed for protocol[TCP|UDP] connection from ingress interface name:Real IP Address/Real Port to egress interface name:Real IP Address/Real Port
- %ASA-3-210006: LU look NAT for IP_address failed
- %ASA-3-210007: LU allocate xlate failed for type[static | dynamic]-[NAT | PAT] secondary(optional) protocol translation from ingress interface name:Real IP Address/real port (Mapped IP Address/Mapped Port) to egress interface name:Real IP Address/Real Port (Mapped IP Address/Mapped Port)
- %ASA-3-210008: LU no xlate for inside_address/inside_port outside_address/outside_port
- %ASA-3-210010: LU make UDP connection for outside_address:outside_port inside_address:inside_port failed
- %ASA-3-210020: LU PAT port port reserve failed
- %ASA-3-210021: LU create static xlate global_address ifc interface_name failed
- %ASA-3-211001: Memory allocation Error
- %ASA-3-211003: Error in computed percentage CPU usage value

- %ASA-3-212001: Unable to open SNMP channel (UDP port port) on interface interface_number, error code = code
- %ASA-3-212002: Unable to open SNMP trap channel (UDP port port) on interface interface_number, error code = code
- %ASA-3-212003: Unable to receive an SNMP request on interface interface_number, error code = code, will try again.
- %ASA-3-212004: Unable to send an SNMP response to IP Address IP_address Port port interface interface_number, error code = code
- %ASA-3-212005: incoming SNMP request (number bytes) on interface interface_name exceeds data buffer size, discarding this SNMP request.
- %ASA-3-212006: Dropping SNMP request from src_addr/src_port to ifc:dst_addr/dst_port because: reason username.
- %ASA-3-212010: Configuration request for SNMP user %s failed.Host %s reason.
- %ASA-3-212011: SNMP engineBoots is set to maximum value.Reason: %s User intervention necessary.
- %ASA-3-212012: Unable to write SNMP engine data to persistent storage.
- %ASA-3-216002: Unexpected event (major: major_id, minor: minor_id) received by task_string in function at line: line_num
- %ASA-3-216003: Unrecognized timer timer_ptr, timer_id received by task_string in function at line: line_num
- %ASA-3-219002: I2C_API_name error, slot = slot_number, device = device_number, address = address, byte count = count.Reason: reason_string
- %ASA-3-302019: H.323 library_name ASN Library failed to initialize, error code number
- %ASA-3-302302: ACL = deny; no sa created
- %ASA-3-305006: {outbound static|identity|portmap|regular) translation creation failed for protocol src interface_name:source_address/source_port [(idfw_user)] dst interface_name:dest_address/dest_port [(idfw_user)]
- %ASA-3-305016: Unable to create protocol connection from real_interface:real_host_ip/real_source_port to real_dest_interface:real_dest_ip/real_dest_port due to reason.
- %ASA-3-313001: Denied ICMP type=number, code=code from IP_address on interface interface_name
- %ASA-3-313008: Denied ICMPv6 type=number, code=code from IP_address on interface interface_name
- %ASA-3-316001: Denied new tunnel to IP_address.VPN peer limit (platform_vpn_peer_limit) exceeded
- %ASA-3-316002: VPN Handle error: protocol=protocol, src in_if_num:src_addr, dst out_if_num:dst_addr
- %ASA-3-317001: No memory available for limit_slow
- %ASA-3-317002: Bad path index of number for IP_address, number max
- %ASA-3-317003: IP routing table creation failure - reason
- %ASA-3-317004: IP routing table limit warning
- %ASA-3-317005: IP routing table limit exceeded - reason, IP_address netmask
- %ASA-3-317006: Pdb index error pdb, pdb_index, pdb_type
- %ASA-3-317012: Interface IP route counter negative - nameif-string-value
- %ASA-3-318001: Internal error: reason
- %ASA-3-318002: Flagged as being an ABR without a backbone area
- %ASA-3-318003: Reached unknown state in neighbor state machine
- %ASA-3-318004: area string lsid IP_address mask netmask adv IP_address type number

按严重性级别列出的消息

- %ASA-3-318005: lsid ip_address adv IP_address type number gateway gateway_address metric number network IP_address mask netmask protocol hex attr hex net-metric number
- %ASA-3-318006: if interface_name if_state number
- %ASA-3-318007: OSPF is enabled on interface_name during idb initialization
- %ASA-3-318008: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id
- %ASA-3-318009: OSPF: Attempted reference of stale data encountered in function, line: line_num
- %ASA-3-318101: Internal error: %REASON
- %ASA-3-318102: Flagged as being an ABR without a backbone area T
- %ASA-3-318103: Reached unknown state in neighbor state machine
- %ASA-3-318104: DB already exist : area %AREA_ID_STR lsid %i adv %i type 0x%x
- %ASA-3-318105: lsid %i adv %i type 0x%x gateway %i metric %d network %i mask %i protocol %#x attr %#x net-metric %d
- %ASA-3-318106: if %IF_NAME if_state %d
- %ASA-3-318107: OSPF is enabled on %IF_NAME during idb initialization
- %ASA-3-318108: OSPF process %d is changing router-id. Reconfigure virtual link neighbors with our new router-id
- %ASA-3-318109: OSPFv3 has received an unexpected message: %0x/%0x
- %ASA-3-318110: Invalid encrypted key %s.
- %ASA-3-318111: SPI %u is already in use with ospf process %d
- %ASA-3-318112: SPI %u is already in use by a process other than ospf process %d.
- %ASA-3-318113: %s %s is already configured with SPI %u.
- %ASA-3-318114: The key length used with SPI %u is not valid
- %ASA-3-318115: %s error occured when attempting to create an IPsec policy for SPI %u
- %ASA-3-318116: SPI %u is not being used by ospf process %d.
- %ASA-3-318117: The policy for SPI %u could not be removed because it is in use.
- %ASA-3-318118: %s error occured when attemtping to remove the IPsec policy with SPI %u
- %ASA-3-318119: Unable to close secure socket with SPI %u on interface %s
- %ASA-3-318120: OSPFv3 was unable to register with IPsec
- %ASA-3-318121: IPsec reported a GENERAL ERROR: message %s, count %d
- %ASA-3-318122: IPsec sent a %s message %s to OSPFv3 for interface %s.Recovery attempt %d .
- %ASA-3-318123: IPsec sent a %s message %s to OSPFv3 for interface %IF_NAME.Recovery aborted
- %ASA-3-318125: Init failed for interface %IF_NAME
- %ASA-3-318126: Interface %IF_NAME is attached to more than one area
- %ASA-3-318127: Could not allocate or find the neighbor
- %ASA-3-320001: The subject name of the peer cert is not allowed for connection
- %ASA-3-321007: System is low on free memory blocks of size block_size (free_blocks CNT out of max_blocks MAX)
- %ASA-3-322001: Deny MAC address MAC_address, possible spoof attempt on interface interface
- %ASA-3-322002: ARP inspection check failed for arp {request|response} received from host MAC_address on interface interface.This host is advertising MAC Address MAC_address_1 for IP Address IP_address, which is {statically|dynamically} bound to MAC Address MAC_address_2.

- %ASA-3-322003:ARP inspection check failed for arp {request|response} received from host MAC_address on interface interface.This host is advertising MAC Address MAC_address_1 for IP Address IP_address, which is not bound to any MAC Address.
- %ASA-3-323001: Module module_id experienced a control channel communications failure.
- %ASA-3-323002: Module module_id is not able to shut down, shut down request not answered.
- %ASA-3-323003: Module module_id is not able to reload, reload request not answered.
- %ASA-3-323004: Module module_id failed to write software vnewver (currently vver), reason.Hw-module reset is required before further use.
- %ASA-3-323005: Module module_id can not be started completely
- %ASA-3-323007: Module in slot slot experienced a firware failure and the recovery is in progress.
- %ASA-3-325001: Router ipv6_address on interface has conflicting ND (Neighbor Discovery) settings
- %ASA-3-326001: Unexpected error in the timer library: error_message
- %ASA-3-326002: Error in error_message: error_message
- %ASA-3-326004: An internal error occurred while processing a packet queue
- %ASA-3-326005: Mrib notification failed for (IP_address, IP_address)
- %ASA-3-326006: Entry-creation failed for (IP_address, IP_address)
- %ASA-3-326007: Entry-update failed for (IP_address, IP_address)
- %ASA-3-326008: MRIB registration failed
- %ASA-3-326009: MRIB connection-open failed
- %ASA-3-326010: MRIB unbind failed
- %ASA-3-326011: MRIB table deletion failed
- %ASA-3-326012: Initialization of string functionality failed
- %ASA-3-326013: Internal error: string in string line %d (%s)
- %ASA-3-326014: Initialization failed: error_message error_message
- %ASA-3-326015: Communication error: error_message error_message
- %ASA-3-326016: Failed to set un-numbered interface for interface_name (string)
- %ASA-3-326017: Interface Manager error - string in string: string
- %ASA-3-326019: string in string: string
- %ASA-3-326020: List error in string: string
- %ASA-3-326021: Error in string: string
- %ASA-3-326022: Error in string: string
- %ASA-3-326023: string - IP_address: string
- %ASA-3-326024: An internal error occurred while processing a packet queue.
- %ASA-3-326025: string
- %ASA-3-326026: Server unexpected error: error_message
- %ASA-3-326027: Corrupted update: error_message
- %ASA-3-326028: Asynchronous error: error_message
- %ASA-3-327001: IP SLA Monitor: Cannot create a new process
- %ASA-3-327002: IP SLA Monitor: Failed to initialize, IP SLA Monitor functionality will not work
- %ASA-3-327003: IP SLA Monitor: Generic Timer wheel timer functionality failed to initialize
- %ASA-3-328001: Attempt made to overwrite a set stub function in string.

按严重性级别列出的消息

- %ASA-3-329001: The string0 subblock named string1 was not removed
- ASA-3-331001: Dynamic DNS Update for 'fqdn_name' = ip_address failed
- %ASA-3-332001: Unable to open cache discovery socket, WCCP V2 closing down.
- %ASA-3-332002: Unable to allocate message buffer, WCCP V2 closing down.
- %ASA-3-336001 Route desination_network stuck-in-active state in EIGRP-ddb_name as_num.Cleaning up
- %ASA-3-336002: Handle handle_id is not allocated in pool.
- %ASA-3-336003: No buffers available for bytes byte packet
- %ASA-3-336004: Negative refcount in pakdesc pakdesc.
- %ASA-3-336005: Flow control error, error, on interface_name.
- %ASA-3-336006: num peers exist on IIDB interface_name.
- %ASA-3-336007: Anchor count negative
- %ASA-3-336008: Lingering DRDB deleting IIDB, dest network, nexthop address (interface), origin origin_str
- %ASA-3-336009 ddb_name as_id: Internal Error
- %ASA-3-336012: Interface interface_names going down and neighbor_links links exist
- %ASA-3-336013: Route iproute, iproute_successors successors, db_successors rdbs
- %ASA-3-336014: "EIGRP_PDM_Process_name, event_log"
- %ASA-3-336015: Unable to open socket for AS as_number"
- %ASA-3-336016: Unknown timer type timer_type expiration
- %ASA-3-336018: process_name as_number: prefix_source threshold prefix level (prefix_threshold) reached
- %ASA-3-336019: process_name as_number: prefix_source prefix limit reached (prefix_threshold).
- %ASA-3-340001: Loopback-proxy info: error_string context id context_id, context type = version/request_type/address_type client socket (internal)= client_address_internal/client_port_internal server socket (internal)= server_address_internal/server_port_internal server socket (external)= server_address_external/server_port_external remote socket (external)= remote_address_external/remote_port_external
- %ASA-3-341003: Policy Agent failed to start for VNMC vnmc_ip_addr
- %ASA-3-341004: Storage device not available: Attempt to shutdown module %s failed.
- %ASA-3-341005: Storage device not available.Shutdown issued for module %s.
- %ASA-3-341006: Storage device not available.Failed to stop recovery of module *%s* .
- %ASA-3-341007: Storage device not available.Further recovery of module *%s* was stopped.This may take several minutes to complete.
- %ASA-3-341008: Storage device not found.Auto-boot of module %s cancelled.Install drive and reload to try again.
- %ASA-3-341011: Storage device with serial number ser_no in bay bay_no faulty.
- %ASA-3-402140: CRYPTO: RSA key generation error: modulus len len
- %ASA-3-402141: CRYPTO: Key zeroization error: key set type, reason reason
- %ASA-3-402142: CRYPTO: Bulk data op error: algorithm alg, mode mode
- %ASA-3-402143: CRYPTO: alg type key op
- %ASA-3-402144: CRYPTO: Digital signature error: signature algorithm sig, hash algorithm hash
- %ASA-3-402145: CRYPTO: Hash generation error: algorithm hash

- %ASA-3-402146: CRYPTO: Keyed hash generation error: algorithm hash, key len len
- %ASA-3-402147: CRYPTO: HMAC generation error: algorithm alg
- %ASA-3-402148: CRYPTO: Random Number Generator error
- %ASA-3-402149: CRYPTO: weak encryption type (length).Operation disallowed.Not FIPS 140-2 compliant
- %ASA-3-402150: CRYPTO: Deprecated hash algorithm used for RSA operation (hash alg).Operation disallowed.Not FIPS 140-2 compliant
- %ASA-3-403501: PPPoE - Bad host-unique in PADO - packet dropped.Intf:interface_name AC:ac_name
- %ASA-3-403502: PPPoE - Bad host-unique in PADS - dropping packet.Intf:interface_name AC:ac_name
- %ASA-3-403503: PPPoE:PPP link down:reason
- %ASA-3-403504: PPPoE:No vpdn group group_name for PPPoE is created
- %ASA-3-403507: PPPoE:PPPoE client on interface interface failed to locate PPPoE vpdn group group_name
- %ASA-3-414001: Failed to save logging buffer using file name filename to FTP server ftp_server_address on interface interface_name: [fail_reason]
- %ASA-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: filename: [fail_reason]
- %ASA-3-414003: TCP Syslog Server intf: IP_Address/port not responding.New connections are [permitted|denied] based on logging permit-hostdown policy.
- %ASA-3-414005: TCP Syslog Server intf: IP_Address/port connected, New connections are permitted based on logging permit-hostdown policy
- %ASA-3-414006: TCP Syslog Server configured and logging queue is full.New connections denied based on logging permit-hostdown policy.
- %ASA-3-421001: TCP|UDP flow from interface_name:ip/port to interface_name:ip/port is dropped because application has failed.
- %ASA-3-421007: TCP|UDP flow from interface_name:IP_address/port to interface_name:IP_address/port is skipped because application has failed.
- %ASA-3-425006 Redundant interface redundant_interface_name switch active member to interface_name failed.
- %ASA-3-505016: Module module_id application changed from: name version version state state to: name version state state.
- %ASA-3-500005: connection terminated from in_ifc_name:src_adddress/src_port to out_ifc_name:dest_address/dest_port due to invalid combination of inspections on same flow.Inspect inspect_name is not compatible with inspect inspect_name_2
- %ASA-3-507003: The flow of type protocol from the originating interface: src_ip/src_port to dest_if:dest_ip/dest_port terminated by inspection engine, reason -
- %ASA-3-520001: error_string
- %ASA-3-520002: bad new ID table size
- %ASA-3-520003: bad id in error_string (id: 0xid_num)
- %ASA-3-520004: error_string
- %ASA-3-520005: error_string
- %ASA-3-520010: Bad queue elem – qelem_ptr: flink flink_ptr, blink blink_ptr, flink->blink flink_blink_ptr, blink->flink blink_flink_ptr
- %ASA-3-520011: Null queue elem

按严重性级别列出的消息

- %ASA-3-520013: Regular expression access check with bad list acl_ID
- %ASA-3-520020: No memory available
- %ASA-3-520021: Error deleting trie entry, error_message
- %ASA-3-520022: "Error adding mask entry, error_message
- %ASA-3-520023: Invalid pointer to head of tree, 0x<radix_node_ptr>
- %ASA-3-520024: Orphaned mask #radix_mask_ptr, refcount= radix_mask_ptr ‘s ref count at # radix_node_address, next=# radix_node_next
- %ASA-3-520025: No memory for radix initialization: error_msg%ASA-3-602305: IPSEC: SA creation error, source source address, destination destination address, reason error string
- %ASA-3-611313: VPN Client: Backup Server List Error: reason
- %ASA-3-613004: Internal error: memory allocation failure
- %ASA-3-613005: Flagged as being an ABR without a backbone area
- %ASA-3-613006: Reached unknown state in neighbor state machine
- %ASA-3-613007: area string lsid IP_address mask netmask type number
- %ASA-3-613008: if inside if_state number
- %ASA-3-613011: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id
- %ASA-3-613013: OSPF LSID IP_address adv IP_address type number gateway IP_address metric number forwarding addr route IP_address /mask type number has no corresponding LSA
- %ASA-3-613029: Router-ID IP_address is in use by ospf process number%ASA-3-613016: Area string router-LSA of length number bytes plus update overhead bytes is too large to flood.
- %ASA-3-613032: Init failed for interface inside, area is being deleted.Try again.%ASA-3-613033: Interface inside is attached to more than one area
- %ASA-3-613034: Neighbor IP_address not configured
- %ASA-3-613035: Could not allocate or find neighbor IP_address%ASA-4-613015: Process 1 flushes LSA ID IP_address type-number adv-rtr IP_address in area mask.
- %ASA-3-710003: {TCP|UDP} access denied by ACL from source_IP/source_port to interface_name:dest_IP/service
- %ASA-3-713004: device scheduled for reboot or shutdown, IKE key acquire message on interface interface num, for Peer IP_address ignored
- %ASA-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel
- %ASA-3-713009: OU in DN in ID payload too big for Certs IKE tunnel
- %ASA-3-713012: Unknown protocol (protocol).Not adding SA w/spi=SPI value
- %ASA-3-713014: Unknown Domain of Interpretation (DOI): DOI value
- %ASA-3-713016: Unknown identification type, Phase 1 or 2, Type ID_Type
- %ASA-3-713017: Identification type not supported, Phase 1 or 2, Type ID_Type
- %ASA-3-713018: Unknown ID type during find of group name for certs, Type ID_Type
- %ASA-3-713020: No Group found by matching OU(s) from ID payload: OU_value
- %ASA-3-713022: No Group found matching peer_ID or IP_address for Pre-shared key peer IP_address
- %ASA-3-713032: Received invalid local Proxy Range IP_address - IP_address
- %ASA-3-713033: Received invalid remote Proxy Range IP_address - IP_address
- %ASA-3-713042: IKE Initiator unable to find policy: Intf interface_number, Src: source_address, Dst: dest_address

- %ASA-3-713043: Cookie/peer address IP_address session already in progress
- %ASA-3-713048: Error processing payload: Payload ID: id
- %ASA-3-713056: Tunnel rejected: SA (SA_name) not found for group (group_name)!
- %ASA-3-713060: Tunnel Rejected: User (user) not member of group (group_name), group-lock check failed.
- %ASA-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:source_address, Dst: dest_address!
- %ASA-3-713062: IKE Peer address same as our interface address IP_address
- %ASA-3-713063: IKE Peer address not configured for destination IP_address
- %ASA-3-713065: IKE Remote Peer did not negotiate the following: proposal attribute
- %ASA-3-713072: Password for user (user) too long, truncating to number characters
- %ASA-3-713081: Unsupported certificate encoding type encoding_type
- %ASA-3-713082: Failed to retrieve identity certificate
- %ASA-3-713083: Invalid certificate handle
- %ASA-3-713084: Received invalid phase 1 port value (port) in ID payload
- %ASA-3-713085: Received invalid phase 1 protocol (protocol) in ID payload
- %ASA-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (Auth method (auth numerical value))
- %ASA-3-713088: Set Cert file handle failure: no IPSec SA in group group_name
- %ASA-3-713098: Aborting: No identity cert specified in IPSec SA (SA_name)!
- %ASA-3-713102: Phase 1 ID Data length number too long - reject tunnel!
- %ASA-3-713105: Zero length data in ID payload received during phase 1 or 2 processing
- %ASA-3-713107: IP_Address request attempt failed!
- %ASA-3-713109: Unable to process the received peer certificate
- %ASA-3-713112: Failed to process CONNECTED notify (SPI SPI_value)!
- %ASA-3-713014: Unknown Domain of Interpretation (DOI): DOI value
- %ASA-3-713016: Unknown identification type, Phase 1 or 2, Type ID_Type
- %ASA-3-713017: Identification type not supported, Phase 1 or 2, Type ID_Type
- %ASA-3-713118: Detected invalid Diffie-Helmann group_descriptor group_number, in IKE area
- %ASA-3-713122: Keep-alives configured keepalive_type but peer IP_address support keep-alives (type = keepalive_type)
- %ASA-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: keepalive_type)
- %ASA-3-713124: Received DPD sequence number rcv_sequence_# in DPD Action, description expected seq #
- %ASA-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list
- %ASA-3-713129: Received unexpected Transaction Exchange payload type: payload_id
- %ASA-3-713132: Cannot obtain an IP_address for remote peer
- %ASA-3-713133: Mismatch: Overriding phase 2 DH Group(DH group DH group_id) with phase 1 group(DH group DH group_number
- %ASA-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection

按严重性级别列出的消息

- %ASA-3-713138: Group group_name not found and BASE GROUP default preshared key not configured
- %ASA-3-713140: Split Tunneling Policy requires network list but none configured
- %ASA-3-713141: Client-reported firewall does not match configured firewall: action tunnel.Received -- Vendor: vendor(id), Product product(id), Caps: capability_value.Expected -- Vendor: vendor(id), Product: product(id), Caps: capability_value
- %ASA-3-713142: Client did not report firewall in use, but there is a configured firewall: action tunnel.Expected -- Vendor: vendor(id), Product product(id), Caps: capability_value
- %ASA-3-713146: Could not add route for Hardware Client in network extension mode, address: IP_address, mask: netmask
- %ASA-3-713149: Hardware client security attribute attribute_name was enabled but not requested.
- %ASA-3-713152: Unable to obtain any rules from filter ACL_tag to send to client for CPP, terminating connection.
- %ASA-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access
- %ASA-3-713161: Remote user (session Id - id) network access has been restricted by the Firewall Server
- %ASA-3-713162: Remote user (session Id - id) has been rejected by the Firewall Server
- %ASA-3-713163: Remote user (session Id - id) has been terminated by the Firewall Server
- %ASA-3-713165: Client IKE Auth mode differs from the group's configured Auth mode
- %ASA-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password
- %ASA-3-713167: Remote peer has failed user authentication - check configured username and password
- %ASA-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!
- %ASA-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!
- %ASA-3-713182: IKE could not recognize the version of the client! IPSec Fragmentation Policy will be ignored for this connection!
- %ASA-3-713185: Error: Username too long - connection aborted
- %ASA-3-713186: Invalid secondary domain name list received from the authentication server.List Received: list_text Character index (value) is illegal
- %ASA-3-713189: Attempted to assign network or broadcast IP_address, removing (IP_address) from pool.
- %ASA-3-713191: Maximum concurrent IKE negotiations exceeded!
- %ASA-3-713193: Received packet with missing payload, Expected payload: payload_id
- %ASA-3-713194: Sending IKE|IPSec Delete With Reason message: termination_reason
- %ASA-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!
- %ASA-3-713198: User Authorization failed: user User authorization failed.
- %ASA-3-713203: IKE Receiver: Error reading from socket.
- %ASA-3-713205: Could not add static route for client address: IP_address
- %ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy
- %ASA-3-713208: Cannot create dynamic rule for Backup L2L entry rule rule_id
- %ASA-3-713209: Cannot delete dynamic rule for Backup L2L entry rule id
- %ASA-3-713210: Cannot create dynamic map for Backup L2L entry rule_id

- %ASA-3-713212: Could not add route for L2L peer coming in on a dynamic map. address: IP_address, mask: netmask
- %ASA-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask
- %ASA-3-713217: Skipping unrecognized rule: action: action client type: client_type client version: client_version
- %ASA-3-713218: Tunnel Rejected: Client Type or Version not allowed.
- %ASA-3-713226: Connection failed with peer IP_address, no trust-point defined in tunnel-group tunnel_group
- %ASA-3-713227: Rejecting new IPSec SA negotiation for peer Peer_address.A negotiation was already in progress for local Proxy Local_address/Local_netmask, remote Proxy Remote_address/Remote_netmask
- %ASA-3-713230: Internal Error, ike_lock trying to lock bit that is already locked for type type
- %ASA-3-713231: Internal Error, ike_lock trying to unlock bit that is not locked for type type
- %ASA-3-713232: SA lock refCnt = value, bitmask = hexvalue, p1_decrypt_cb = value, qm_decrypt_cb = value, qm_hash_cb = value, qm_spi_ok_cb = value, qm_dh_cb = value, qm_secret_key_cb = value, qm_encrypt_cb = value
- %ASA-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client
- %ASA-3-713258: IP = var1, Attempting to establish a phase2 tunnel on var2 interface but phase1 tunnel is on var3 interface.Tearing down old phase1 tunnel due to a potential routing change.
- %ASA-3-713254: Group = groupname, Username = username, IP = peerip, Invalid IPSec/UDP port = portnum, valid range is minport - maxport, except port 4500, which is reserved for IPSec/NAT-T
- %ASA-3-713260: Output interface %d to peer was not found
- %ASA-3-713261: IPV6 address on output interface %d was not found
- %ASA-3-713262: Rejecting new IPSec SA negotiation for peer Peer_address.A negotiation was already in progress for local Proxy Local_address/Local_prefix_len, remote Proxy Remote_address/Remote_prefix_len
- %ASA-3-713266: Could not add route for L2L peer coming in on a dynamic map. address: IP_address, mask: /prefix_len
- %ASA-3-713268: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address, mask: /prefix_len
- %ASA-3-713270: Could not add route for Hardware Client in network extension mode, address: IP_addres>, mask: /prefix_len
- %ASA-3-713272: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address, mask: /prefix_len
- %ASA-3-713274: Could not delete static route for client address: IP_Address IP_Address address of client whose route is being removed
- %ASA-3-713902: Descriptive_event_string.
- %ASA-3-716056: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type failed reason: reason
- %ASA-3-716057: Group group User user IP ip Session terminated, no type license available.
- %ASA-3-716061: Group DfltGrpPolicy User user IP ip addr IPv6 User Filter tempipv6 configured for AnyConnect.This setting has been deprecated, terminating connection
- %ASA-3-716600: Rejected size-recv KB Hostscan data from IP src-ip.Hostscan results exceed default | configured limit of size-conf KB.

按严重性级别列出的消息

- %ASA-3-716601: Rejected size-recv KB Hostscan data from IP src-ip.System-wide limit onthe amount of Hostscan data stored on ASA exceeds the limit of data-max KB.
- %ASA-3-716602: Memory allocation error.Rejected size-recv KB Hostscan data from IP src-ip.
- %ASA-3-717001: Querying keypair failed.
- %ASA-3-717002: Certificate enrollment failed for trustpoint trustpoint_name.Reason: reason_string.
- %ASA-3-717009: Certificate validation failed.Reason: reason_string.
- %ASA-3-717010: CRL polling failed for trustpoint trustpoint_name.
- %ASA-3-717012: Failed to refresh CRL cache entry from the server for trustpoint trustpoint_name at time_of_failure
- %ASA-3-717015: CRL received from issuer is too large to process (CRL size = crl_size, maximum CRL size = max_crl_size)
- %ASA-3-717017: Failed to query CA certificate for trustpoint trustpoint_name from enrollment_url
- %ASA-3-717018: CRL received from issuer has too many entries to process (number of entries = number_of_entries, maximum number allowed = max_allowed)
- %ASA-3-717019: Failed to insert CRL for trustpoint trustpoint_name.Reason: failure_reason.
- %ASA-3-717020: Failed to install device certificate for trustpoint label.Reason: reason string.
- %ASA-3-717021: Certificate data could not be verified.Locate Reason: reason_string serial number: serial number, subject name: subject name, key length key length bits.
- %ASA-3-717023: SSL failed to set device certificate for trustpoint trustpoint name.Reason: reason_string.
- %ASA-3-717027: Certificate chain failed validation. reason_string.
- %ASA-3-717051: SCEP Proxy: Denied processing the request type type received from IP client ip address, User username, TunnelGroup tunnel group name, GroupPolicy group policy name to CA ca ip address.Reason: msg
- %ASA-3-717063: protocol Certificate enrollment failed for the trustpoint tpname with the CA ca
- %ASA-3-719002: Email Proxy session pointer from source_address has been terminated due to reason error.
- %ASA-3-719008: Email Proxy service is shutting down.
- %ASA-3-722007: Group group User user-name IP IP_address SVC Message: type-num/ERROR: message
- %ASA-3-722008: Group group User user-name IP IP_address SVC Message: type-num/ERROR: message
- %ASA-3-722009: Group group User user-name IP IP_address SVC Message: type-num/ERROR: message
- %ASA-3-722020: TunnelGroup tunnel_group GroupPolicy group_policy User user-name IP IP_address No address available for SVC connection
- %ASA-3-722035: Group group User user-name IP IP_address Received large packet length threshold num).
- %ASA-3-722036: Group group User user-name IP IP_address Transmitting large packet length (threshold num).
- %ASA-3-722045: Connection terminated: no SSL tunnel initialization data.
- %ASA-3-722046: Group group User user IP ip Session terminated: unable to establish tunnel.
- %ASA-3-725015 Error verifying client certificate.Public key size in client certificate exceeds the maximum supported key size.
- %ASA-3-734004: DAP: Processing error: internal error code
- %ASA-3-735010: IPMI: Environment Monitoring has failed to update one or more of its records.
- %ASA-3-737002: IPAA: Received unknown message 'num'

- %ASA-3-737027: IPAA: No data for address request
- %ASA-3-742001: failed to read master key for password encryption from persistent store
- %ASA-3-742002: failed to set master key for password encryption
- %ASA-3-742003: failed to save master key for password encryption, reason reason_text
- %ASA-3-742004: failed to sync master key for password encryption, reason reason_text
- %ASA-3-742005: cipher text enc_pass is not compatible with the configured master key or the cipher text has been tampered with
- %ASA-3-742006: password decryption failed due to unavailable memory
- %ASA-3-742007: password encryption failed due to unavailable memory
- %ASA-3-742008: password enc_pass decryption failed due to decoding error
- %ASA-3-742009: password encryption failed due to decoding error
- %ASA-3-742010: encrypted password enc_pass is not well formed
- %ASA-3-743010: EOBC RPC server failed to start for client module client name.
- %ASA-3-743011: EOBC RPC call failed, return code code string.
- %ASA-3-747001: Clustering: Recovered from state machine event queue depleted.Event (event-id, ptr-in-hex, ptr-in-hex) dropped.Current state state-name, stack ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex
- %ASA-3-747010: Clustering: RPC call failed, message message-name, return code code-value.
- %ASA-3-747012: Clustering: Failed to replicate global object id hex-id-value in domain domain-name to peer unit-name, continuing operation.
- %ASA-3-747013: Clustering: Failed to remove global object id hex-id-value in domain domain-name from peer unit-name, continuing operation.
- %ASA-3-747014: Clustering: Failed to install global object id hex-id-value in domain domain-name, continuing operation.
- %ASA-3-747018: Clustering: State progression failed due to timeout in module module-name.
- %ASA-3-747021: Clustering: Master unit unit-name is quitting due to interface health check failure on failed-interface.
- %ASA-3-747022: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times, rejoin will be attempted after y min. Failed interface: interface-name.
- %ASA-3-747030: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times (last failure on interface-name), Clustering must be manually enabled on the unit to re-join.
- %ASA-3-747031: Clustering: Platform mismatch between cluster master (platform-type) and joining unit unit-name (platform-type). unit-name aborting cluster join.
- %ASA-3-747032: Clustering: Service module mismatch between cluster master (module-name) and joining unit unit-name (module-name) in slot slot-number. unit-name aborting cluster join.
- %ASA-3-747033: Clustering: Interface mismatch between cluster master and joining unit unit-name. unit-name aborting cluster join.
- %ASA-3-748005: Failed to bundle the ports for module slot_number in chassis chassis_number; clustering is disabled
- %ASA-3-748006: Asking module slot_number in chassis chassis_number to leave the cluster due to a port bundling failure
- %ASA-3-750011: Tunnel Rejected: Selected IKEv2 encryption algorithm (IKEV2 encry algo) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo).

按严重性级别列出的消息

- %ASA-3-751001: Local: localIP:port Remote:remoteIP:port Username: username/group Failed to complete Diffie-Hellman operation.Error: error
- %ASA-3-751002: Local: localIP:port Remote:remoteIP:port Username: username/group No preshared key or trustpoint configured for self in tunnel group group
- %ASA-3-751004: Local: localIP:port Remote:remoteIP:port Username: username/group No remote authentication method configured for peer in tunnel group group
- %ASA-3-751005: Local: localIP:port Remote:remoteIP:port Username: username/group AnyConnect client reconnect authentication failed.Session ID: sessionID, Error: error
- %ASA-3-751006: Local: localIP:port Remote:remoteIP:port Username: username/group Certificate authentication failed.Error: error
- %ASA-3-751008: Local: localIP:port Remote:remoteIP:port Username: username/group Group=group, Tunnel rejected: IKEv2 not enabled in group policy
- %ASA-3-751009: Local: localIP:port Remote:remoteIP:port Username: username/group Unable to find tunnel group for peer.
- %ASA-3-751010: Local: localIP:port Remote:remoteIP:port Username: username/group Unable to determine self-authentication method.No crypto map setting or tunnel group found.
- %ASA-3-751011: Local: localIP:port Remote:remoteIP:port Username: username/group Failed user authentication.Error: error
- %ASA-3-751012: Local: localIP:port Remote:remoteIP:port Username: username/group Failure occurred during Configuration Mode processing.Error: error
- %ASA-3-751013: Local: localIP:port Remote:remoteIP:port Username: username/group Failed to process Configuration Payload request for attribute attribute ID.Error: error
- %ASA-3-751017: Local: localIP:port Remote remoteIP:port Username: username/group Configuration Error error description
- %ASA-3-751018: Terminating the VPN connection attempt from landing group.Reason: This connection is group locked to locked group.
- %ASA-3-751020: Local:%A:%u Remote:%A:%u Username:%s An %s remote access connection failed.Attempting to use an NSA Suite B crypto algorithm (%s) without an AnyConnect Premium license.
- %ASA-3-751022: Local: local-ip Remote: remote-ip Username:username Tunnel rejected: Crypto Map Policy not found for remote traffic selector rem-ts-start/rem-ts-end/rem-ts.startport/rem-ts.endport/rem-ts.protocol local traffic selector local-ts-start/local-ts-end/local-ts.startport/local-ts.endport/local-ts.protocol!
- %ASA-3-751024: Local:ip addr Remote:ip addr Username:username IKEv2 IPv6 User Filter tempipv6 configured.This setting has been deprecated, terminating connection
- %ASA-3-752006: Tunnel Manager failed to dispatch a KEY_ACQUIRE message.Probable mis-configuration of the crypto map or tunnel-group.Map Tag = Tag.Map Sequence Number = num, SRC Addr: address port: port Dst Addr: address port: port.
- %ASA-3-752007: Tunnel Manager failed to dispatch a KEY_ACQUIRE message.Entry already in Tunnel Manager.Map Tag = mapTag.Map Sequence Number = mapSeq.
- %ASA-3-752015: Tunnel Manager has failed to establish an L2L SA.All configured IKE versions failed to establish the tunnel.Map Tag = mapTag.Map Sequence Number = mapSeq.
- %ASA-3-769006: UPDATE: ASA boot system image image_name was not found on disk
- %ASA-3-776202: CTS PAC for Server IP_address, A-ID PAC issuer name has expired
- %ASA-3-768001: QUOTA: resource utilization is high: requested req, current curr, warning level level
- %ASA-3-768002: QUOTA: resource quota exceeded: requested req, current curr, limit limit

- %ASA-3-772002: PASSWORD: console login warning, user username, cause: password expired
- %ASA-3-772004: PASSWORD: session login failed, user username, IP ip, cause: password expired
- %ASA-3-779003: STS: Failed to read tag-switching table - reason
- %ASA-3-779004: STS: Failed to write tag-switching table - reason
- %ASA-3-779005: STS: Failed to parse tag-switching request from http - reason
- %ASA-3-779006: STS: Failed to save tag-switching table to flash - reason
- %ASA-3-779007: STS: Failed to replicate tag-switching table to peer - reason
- %ASA-3-840001: Failed to create the backup for an IKEv2 session <Local IP>, <Remote IP>
- %ASA-3-8300003: Failed to send session redistribution message to <variable 1>
- %ASA-3-8300005: Failed to receive session move response from <variable 1>

严重性级别为 4 的警告消息

以下警告消息的严重性级别为 4：

- %ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] [([idfw_user|FQDN_string], sg_info)] dst interface_name:dest_address/dest_port [([idfw_user|FQDN_string], sg_info)] [type {string}, code {code}] by access_group acl_ID [0x8ed66b60, 0xf8852875]
- %ASA-4-106027: Deny src [source address] dst [destination address] by access-group “access-list name”.
- %ASA-4-106103: access-list acl_ID denied protocol for user username interface_name/source_address source_port interface_name/dest_address dest_port hit-cnt number first hit hash codes
- %ASA-4-109027: [aaa protocol] Unable to decipher response message Server = server_IP_address, User = user
- %ASA-4-109030: Autodetect ACL convert wildcard did not convert ACL access_list source | dest netmask netmask.
- %ASA-4-109033: Authentication failed for admin user user from src_IP.Interactive challenge processing is not supported for protocol connections
- %ASA-4-109034: Authentication failed for network user user from src_IP/port to dst_IP/port.Interactive challenge processing is not supported for protocol connections
- %ASA-4-109102: Received CoA action-type from coa-source-ip, but cannot find named session audit-session-id
- %ASA-4-113019: Group = group, Username = user, IP = peer_address, Session disconnected.Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason
- %ASA-4-113026: Error error while executing Lua script for group tunnel group
- %ASA-4-113029: Group group User user IP ipaddr Session could not be established: session limit of num reached
- %ASA-4-113030: Group group User user IP ipaddr User ACL acl from AAA doesn't exist on the device, terminating connection.
- %ASA-4-113031: Group group User user IP ipaddr AnyConnect vpn-filter filter is an IPv6 ACL; ACL not applied.
- %ASA-4-113032: Group group User user IP ipaddr AnyConnect ipv6-vpn-filter filter is an IPv4 ACL; ACL not applied.

按严重性级别列出的消息

- %ASA-4-113034: Group group User user IP ipaddr User ACL acl from AAA ignored, AV-PAIR ACL used instead.
- %ASA-4-113035: Group group User user IP ipaddr Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
- %ASA-4-113036: Group group User user IP ipaddr AAA parameter name value invalid.
- %ASA-4-113038: Group group User user IP ipaddr Unable to create AnyConnect p0arent session.
- %ASA-4-113040: Terminating the VPN connection attempt from attempted group.Reason: This connection is group locked to locked group.
- %ASA-4-113041: Redirect ACL configured for assigned IP does not exist on the device.
- %ASA-4-113042: CoA: Non-HTTP connection from src_if:src_ip/src_port to dest_if:dest_ip/dest_port for user username at client_IP denied by redirect filter; only HTTP connections are supported for redirection.
- %ASA-4-115002: Warning in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition
- %ASA-4-199016: syslog
- %ASA-4-209003: Fragment database limit of number exceeded: src = source_address, dest = dest_address, proto = protocol, id = number
- %ASA-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes: src = source_address, dest = dest_address, proto = protocol, id = number
- %ASA-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.
- %ASA-4-216004: prevented: error in function at file(line) - stack trace
- %ASA-4-302034: Unable to pre-allocate H323 GUP Connection for faddr interface: foreign address/foreign-port to laddr interface:local-address/local-port
- %ASA-4-308002: static global_address inside_address netmask netmask overlapped with global_address inside_address
- %ASA-4-313004: Denied ICMP type=icmp_type, from source_address on interface interface_name to dest_address:no matching session
- %ASA-4-313005: No matching connection for ICMP error message: icmp_msg_info on interface_name interface.Original IP payload: embedded_frame_info icmp_msg_info = icmp src src_interface_name:src_address [([idfw_user | FQDN_string], sg_info)] dst dest_interface_name:dest_address [([idfw_user | FQDN_string], sg_info)] (type icmp_type, code icmp_code) embedded_frame_info = prot src source_address/source_port [([idfw_user | FQDN_string], sg_info)] dst dest_address/dest_port [(idfw_user|FQDN_string), sg_info]
- %ASA-4-313009: Denied invalid ICMP code icmp-code, for src-ifc:src-address/src-port (mapped-src-address/mapped-src-port) to dest-ifc:dest-address/dest-port (mapped-dest-address/mapped-dest-port) [user], ICMP id icmp-id, ICMP type icmp-type
- %ASA-4-325002: Duplicate address ipv6_address/MAC_address on interface
- %ASA-4-337005: Phone Proxy SRTP: Media session not found for media_term_ip/media_term_port for packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port
- %ASA-4-338101: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port (mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port, (mapped-ip/mapped-port), source malicious address resolved from local or dynamic list: domain name
- %ASA-4-338102: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port (mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port (mapped-ip/mapped-port), destination malicious address resolved from local or dynamic list: domain name

- %ASA-4-338103: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port (mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port, (mapped-ip/mapped-port), source malicious address resolved
- %ASA-4-338104: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port (mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port (mapped-ip/mapped-port), destination malicious address resolved from local or dynamic list: ip address/netmask
- from local or dynamic list: ip address/netmask
- %ASA-4-338301: Intercepted DNS reply for domain name from in_interface:src_ip_addr/src_port to out_interface:dest_ip_addr/dest_port, matched list
- %ASA-4-401001: Shuns cleared
- %ASA-4-401002: Shun added: IP_address IP_address port port
- %ASA-4-401003: Shun deleted: IP_address
- %ASA-4-401004: Shunned packet: IP_address = IP_address on interface interface_name
- %ASA-4-401005: Shun add failed: unable to allocate resources for IP_address IP_address port port
- %ASA-4-402114: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP to local_IP with an invalid SPI.
- %ASA-4-402115: IPSEC: Received a packet from remote_IP to local_IP containing act_prot data instead of exp_prot data.
- %ASA-4-402116: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP.The decapsulated inner packet doesn’ t match the negotiated policy in the SA.The packet specifies its destination as pkt_daddr, its source as pkt_saddr, and its protocol as pkt_prot.The SA specifies its local proxy as id_daddr /id_dmask /id_dprot /id_dport and its remote proxy as id_saddr /id_smask /id_sprot /id_sport .
- %ASA-4-402117: IPSEC: Received a non-IPSec (protocol) packet from remote_IP to local_IP.
- %ASA-4-402118: IPSEC: Received an protocol packet (SPI=spi, sequence number seq_num) from remote_IP (username) to local_IP containing an illegal IP fragment of length frag_len with offset frag_offset.
- %ASA-4-402119: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed anti-replay checking.
- %ASA-4-402120: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed authentication.
- %ASA-4-402121: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from peer_addr (username) to lcl_addr that was dropped by IPSec (drop_reason).
- %ASA-4-402122: Received a cleartext packet from src_addr to dest_addr that was to be encapsulated in IPSec that was dropped by IPSec (drop_reason).
- %ASA-4-402123: CRYPTO: The accel_type hardware accelerator encountered an error (code= error_string) while executing crypto command command.
- %ASA-4-402124: CRYPTO: The ASA hardware accelerator encountered an error (Hardware error address, Core, Hardware error code, IstatReg, PciErrReg, CoreErrStat, CoreErrAddr, Doorbell Size,DoorBell Outstanding, SWReset).
- %ASA-4-402125: The ASA hardware accelerator ring timed out (parameters).
- %ASA-4-402126: CRYPTO: The ASA created Crypto Archive File Archive Filename as a Soft Reset was necessary.Please forward this archived information to Cisco.

按严重性级别列出的消息

- %ASA-4-402127: CRYPTO: The ASA is skipping the writing of latest Crypto Archive File as the maximum # of files, max_number, allowed have been written to archive_directory.Please archive & remove files from Archive Directory if you want more Crypto Archive Files saved.
- %ASA-4-402131: CRYPTO: status changing the accel_instance hardware accelerator's configuration bias from old_config_bias to new_config_bias.
- %ASA-4-403505: PPPoE:PPP - Unable to set default route to IP_address at interface_name
- %ASA-4-403506: PPPoE:failed to assign PPP IP_address netmask netmask at interface_name
- %ASA-4-405001: Received ARP {request | response} collision from IP_address/MAC_address on interface interface_name to IP_address/MAC_address on interface interface_name
- %ASA-4-405002: Received mac mismatch collision from IP_address/MAC_address for authenticated host
- %ASA-4-405003: IP address collision detected between host IP_address at MAC_address and interface interface_name, MAC_address.
- %ASA-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for foreign_address outside_address[/outside_port] to local_address inside_address[/inside_port]
- %ASA-4-405102: Unable to Pre-allocate H245 Connection for foreign_address outside_address[/outside_port] to local_address inside_address[/inside_port]
- %ASA-4-405103: H225 message from source_address/source_port to dest_address/dest_port contains bad protocol discriminator hex
- %ASA-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP
- %ASA-4-405105: H323 RAS message AdmissionConfirm received from source_address/source_port to dest_address/dest_port without an AdmissionRequest
- %ASA-4-406001: FTP port command low port: IP_address/port to IP_address on interface interface_name
- %ASA-4-406002: FTP port command different address: IP_address(IP_address) to IP_address on interface interface_name
- %ASA-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded
- %ASA-4-407002: Embryonic limit nconns/elimit for through connections exceeded.outside_address/outside_port to global_address (inside_address)/inside_port on interface interface_name
- %ASA-4-407003: Established limit for RPC services exceeded number
- %ASA-4-408001: IP route counter negative - reason, IP_address Attempt: number
- %ASA-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1] via source IP:interface1 address2 netmask2 [distance2/metric2] interface2
- %ASA-4-408003: can't track this type of object hex
- %ASA-4-409001: Database scanner: external LSA IP_address netmask is lost, reinstalls
- %ASA-4-409002: db_free: external LSA IP_address netmask
- %ASA-4-409003: Received invalid packet: reason from IP_address, interface_name
- %ASA-4-409004: Received reason from unknown neighbor IP_address
- %ASA-4-409005: Invalid length number in OSPF packet from IP_address (ID IP_address), interface_name
- %ASA-4-409006: Invalid lsa: reason Type number, LSID IP_address from IP_address, IP_address, interface_name

- %ASA-4-409007: Found LSA with the same host bit set but using different mask LSA ID IP_address netmask New: Destination IP_address netmask
- %ASA-4-409008: Found generating default LSA with non-zero mask LSA type : number Mask: netmask metric: number area: string
- %ASA-4-409009: OSPF process number cannot start.There must be at least one up IP interface, for OSPF to use as router ID
- %ASA-4-409010: Virtual link information found in non-backbone area: string
- %ASA-4-409011: OSPF detected duplicate router-id IP_address from IP_address on interface interface_name
- %ASA-4-409012: Detected router with duplicate router ID IP_address in area string
- %ASA-4-409013: Detected router with duplicate router ID IP_address in Type-4 LSA advertised by IP_address
- %ASA-4-409023: Attempting AAA Fallback method method_name for request_type request for user user:Auth-server group server_tag unreachable
- %ASA-4-409101: Received invalid packet: %s from %P, %s
- %ASA-4-409102: Received packet with incorrect area from %P, %s, area %AREA_ID_STR, packet area %AREA_ID_STR
- %ASA-4-409103: Received %s from unknown neighbor %i
- %ASA-4-409104: Invalid length %d in OSPF packet type %d from %P (ID %i), %s
- %ASA-4-409105: Invalid lsa: %s: Type 0x%x, Length 0x%x, LSID %u from %i
- %ASA-4-409106: Found generating default LSA with non-zero mask LSA type: 0x%x Mask: %i metric: %lu area: %AREA_ID_STR
- %ASA-4-409107: OSPFv3 process %d could not pick a router-id, please configure manually
- %ASA-4-409108: Virtual link information found in non-backbone area: %AREA_ID_STR
- %ASA-4-409109: OSPF detected duplicate router-id %i from %P on interface %IF_NAME
- %ASA-4-409110: Detected router with duplicate router ID %i in area %AREA_ID_STR
- %ASA-4-409111: Multiple interfaces (%IF_NAME /%IF_NAME) on a single link detected.
- %ASA-4-409112: Packet not written to the output queue
- %ASA-4-409113: Doubly linked list linkage is NULL
- %ASA-4-409114: Doubly linked list prev linkage is NULL %x
- %ASA-4-409115: Unrecognized timer %d in OSPF %s
- %ASA-4-409116: Error for timer %d in OSPF process %s
- %ASA-4-409117: Can't find LSA database type %x, area %AREA_ID_STR, interface %x
- %ASA-4-409118: Could not allocate DBD packet
- %ASA-4-409119: Invalid build flag %x for LSA %i, type 0x%x
- %ASA-4-409120: Router-ID %i is in use by ospf process %d
- %ASA-4-409121: Router is currently an ASBR while having only one area which is a stub area
- %ASA-4-409122: Could not select a global IPv6 address.Virtual links require at least one global IPv6 address.
- %ASA-4-409123: Neighbor command allowed only on NBMA networks
- %ASA-4-409125: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network

按严重性级别列出的消息

- %ASA-4-409128: OSPFv3-%d Area %AREA_ID_STR: Router %i originating invalid type 0x%x LSA, ID %u, Metric %d on Link ID %d Link Type %d
- %ASA-4-410001: UDP DNS request from source_interface:source_address/source_port to dest_interface:dest_address/dest_port; (label length | domain-name length) 52 bytes exceeds remaining packet length of 44 bytes.
- %ASA-4-411001: Line protocol on interface interface_name changed state to up
- %ASA-4-411002: Line protocol on interface interface_name changed state to down
- %ASA-4-411003: Configuration status on interface interface_name changed state to downup
- %ASA-4-411004: Configuration status on interface interface_name changed state to up
- %ASA-4-411005: Interface variable 1 experienced a hardware transmit hang.The interface has been reset.
- %ASA-4-412001: MAC MAC_address moved from interface_1 to interface_2
- %ASA-4-412002: Detected bridge table full while inserting MAC MAC_address on interface interface.Number of entries = num
- %ASA-4-413001: Module module_id is not able to shut down.Module Error: errnum message
- %ASA-4-413002: Module module_id is not able to reload.Module Error: errnum message
- %ASA-4-413003: Module module_id is not a recognized type
- %ASA-4-413004: Module module_id failed to write software vnewver (currently vver), reason.Trying again.
- %ASA-4-413005: Module module_id, application is not supported app_name version app_vers type app_type
- %ASA-4-413006: prod-id Module software version mismatch; slot slot is prod-id version running-vers.Slot slot prod-id requires required-vers .
- %ASA-4-415016: policy-map map_name:Maximum number of unanswered HTTP requests exceeded connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %ASA-4-417001: Unexpected event received: number
- %ASA-4-417004: Filter violation error: conn number (string:string) in string
- %ASA-4-417006: No memory for string) in string.Handling: string
- %ASA-4-418001: Through-the-device packet to/from management-only network is denied: protocol_string from interface_name IP_address (port) [([idfw_user|FQDN_string], sg_info)] to interface_name IP_address (port) [(idfw_user|FQDN_string), sg_info]
- %ASA-4-419001: Dropping TCP packet from src_ifc:src_IP/src_port to dest_ifc:dest_IP/dest_port, reason: MSS exceeded, MSS size, data size
- %ASA-4-419002: Received duplicate TCP SYN from in_interface:src_address/src_port to out_interface:dest_address/dest_port with different initial sequence number.
- %ASA-4-419003: Cleared TCP urgent flag from out_ifc:src_ip/src_port to in_ifc:dest_ip/dest_port.
- %ASA-4-422004: IP SLA Monitor number0: Duplicate event received.Event number number1
- %ASA-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.
- %ASA-4-422006: IP SLA Monitor Probe number: string
- %ASA-4-424001: Packet denied protocol_string intf_in:src_ip/src_port [([idfw_user | FQDN_string], sg_info)] intf_out:dst_ip/dst_port[([idfw_user | FQDN_string], sg_info)].[Ingress|Egress] interface is in a backup state.
- %ASA-4-424002: Connection to the backup interface is denied: protocol_string intf:src_ip/src_port intf:dst_ip/dst_port

- %ASA-4-426004: PORT-CHANNEL: Interface ifc_name1 is not compatible with ifc_name and will be suspended (speed of ifc_name1 is X Mbps, Y is 1000 Mbps).
- %ASA-4-429008: Unable to respond to VPN query from CX for session 0x%x.Reason %s
- %ASA-4-434001: SFR card not up and fail-close mode used, dropping protocol packet from ingress interface:source IP address/source port to egress interface:destination IP address/destination port
- %ASA-4-434007: SFR redirect will override Scansafe redirect for flow from ingress interface:source IP address/source port to egress interface:destination IP address/destination port (user)
- %ASA-4-446003: Denied TLS Proxy session from src_int:src_ip/src_port to dst_int:dst_ip/dst_port, UC-IME license is disabled.
- %ASA-4-447001: ASP DP to CP queue_name was full.Queue length length, limit limit
- %ASA-4-448001: Denied SRTP crypto session setup on flow from src_int:src_ip/src_port to dst_int:dst_ip/dst_port, licensed K8 SRTP crypto session of limit exceeded
- %ASA-4-500004: Invalid transport field for protocol=protocol, from source_address/source_port to dest_address/dest_port
- %ASA-4-507002: Data copy in proxy-mode exceeded the buffer limit
- %ASA-4-603110: Failed to establish L2TP session, tunnel_id = tunnel_id, remote_peer_ip = peer_ip, user = username.Multiple sessions per tunnel are not supported
- %ASA-4-604105: DHCPD: Unable to send DHCP reply to client hardware_address on interface interface_name.Reply exceeds options field size (options_field_size) by number_of_octets octets.
- %ASA-4-608002: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, SCCPPrefix length value too small
- %ASA-4-608003: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, SCCPPrefix length value too large
- %ASA-4-612002: Auto Update failed:filename, version:number, reason:reason
- %ASA-4-612003: Auto Update failed to contact:url, reason:reason
- %ASA-4-613017: Bad LSA mask: Type number, LSID IP_address Mask mask from IP_address
- %ASA-4-613018: Maximum number of non self-generated LSA has been exceeded “OSPF number” - number LSAs
- %ASA-4-613019: Threshold for maximum number of non self-generated LSA has been reached "OSPF number" - number LSAs
- %ASA-4-613021: Packet not written to the output queue
- %ASA-4-613022: Doubly linked list linkage is NULL
- %ASA-4-613023: Doubly linked list prev linkage is NULL number
- %ASA-4-613024: Unrecognized timer number in OSPF string
- %ASA-4-613025: Invalid build flag number for LSA IP_address, type number
- %ASA-4-613026: Can not allocate memory for area structure
- %ASA-4-613030: Router is currently an ASBR while having only one area which is a stub area
- %ASA-4-613031: No IP address for interface inside
- %ASA-4-613036: Can not use configured neighbor: cost and database-filter options are allowed only for a point-to-multipoint network
- %ASA-4-613037: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network
- %ASA-4-613038: Can not use configured neighbor: cost or database-filter option is required for point-to-multipoint broadcast network

按严重性级别列出的消息

- %ASA-4-613039: Can not use configured neighbor: neighbor command is allowed only on NBMA and point-to-multipoint networks
- %ASA-4-613040: OSPF-1 Area string: Router IP_address originating invalid type number LSA, ID IP_address, Metric number on Link ID IP_address Link Type number
- %ASA-4-613042: OSPF process number lacks forwarding address for type 7 LSA IP_address in NSSA string - P-bit cleared
- %ASA-4-620002: Unsupported CTIQBE version: hex: from interface_name:IP_address/port to interface_name:IP_address/port
- %ASA-4-709008: (Primary | Secondary) Configuration sync in progress.Command: ‘command’ executed from (terminal/http) will not be replicated to or executed by the standby unit.
- %ASA-4-711002: Task ran for elapsed_time msecs, process = process_name, PC = PC Tracebeback = traceback
- %ASA-4-711004: Task ran for msec msec, Process = process_name, PC = pc, Call stack = call stack
- %ASA-4-713154: DNS lookup for peer_description Server [server_name] failed!
- %ASA-4-713157: Timed out on initial contact to server [server_name or IP_address] Tunnel could not be established.
- %ASA-4-713239: IP_Address: Tunnel Rejected: The maximum tunnel count allowed has been reached
- %ASA-4-713240: Received DH key with bad length: received length=rlength expected length=elength
- %ASA-4-713241: IE Browser Proxy Method setting_number is Invalid
- %ASA-4-713242: Remote user is authenticated using Hybrid Authentication.Not starting IKE rekey.
- %ASA-4-713243: META-DATA Unable to find the requested certificate
- %ASA-4-713244: META-DATA Received Legacy Authentication Method(LAM) type type is different from the last type received type.
- %ASA-4-713245: META-DATA Unknown Legacy Authentication Method(LAM) type type received.
- %ASA-4-713246: META-DATA Unknown Legacy Authentication Method(LAM) attribute type type received.
- %ASA-4-713247: META-DATA Unexpected error: in Next Card Code mode while not doing SDI.
- %ASA-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.
- %ASA-4-713249: META-DATA Received unsupported authentication results: result
- %ASA-4-713251: META-DATA Received authentication failure message
- %ASA-4-713255: IP = peer-IP, Received ISAKMP Aggressive Mode message 1 with unknown tunnel group name group-name
- %ASA-4-713903: Group = group policy, Username = user name, IP = remote IP, ERROR: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP.
- %ASA-4-716007: Group group User user WebVPN Unable to create session.
- %ASA-4-716022: Unable to connect to proxy server reason.
- %ASA-4-716023: Group name User user Session could not be established: session limit of maximum_sessions reached.
- %ASA-4-716044: Group group-name User user-name IP IP_address AAA parameter param-name value param-value out of range.
- %ASA-4-716045: Group group-name User user-name IP IP_address AAA parameter param-name value invalid.
- %ASA-4-716046: Group group-name-name User user-name IP IP_address User ACL access-list-name from AAA doesn't exist on the device, terminating connection.

- %ASA-4-716047: Group group-name User user-name IP IP_address User ACL access-list from AAA ignored, AV-PAIR ACL used instead.
- %ASA-4-716048: Group group-name User user-name IP IP_address No memory to parse ACL.
- %ASA-4-716052: Group group-name User user-name IP IP_address Pending session terminated.
- %ASA-4-717026: Name lookup failed for hostname hostname during PKI operation.
- %ASA-4-717031: Failed to find a suitable trustpoint for the issuer: issuer Reason: reason_string
- %ASA-4-717035: OCSP status is being checked for certificate. certificate_identifier.
- %ASA-4-717037: Tunnel group search using certificate maps failed for peer certificate: certificate_identifier.
- %ASA-4-717052: Group group name User user name IP IP Address Session disconnected due to periodic certificate authentication failure.Subject Name id subject name Issuer Name id issuer name Serial Number id serial number
- %ASA-4-720001: (VPN-unit) Failed to initialize with Chunk Manager.
- %ASA-4-720007: (VPN-unit) Failed to allocate chunk from Chunk Manager.
- %ASA-4-720008: (VPN-unit) Failed to register to High Availability Framework.
- %ASA-4-720009: (VPN-unit) Failed to create version control block.
- %ASA-4-720011: (VPN-unit) Failed to allocate memory
- %ASA-4-720013: (VPN-unit) Failed to insert certificate in trust point trustpoint_name
- %ASA-4-720022: (VPN-unit) Cannot find trust point trustpoint
- %ASA-4-720033: (VPN-unit) Failed to queue add to message queue.
- %ASA-4-720038: (VPN-unit) Corrupted message from active unit.
- %ASA-4-720043: (VPN-unit) Failed to send type message id to standby unit
- %ASA-4-720044: (VPN-unit) Failed to receive message from active unit
- %ASA-4-720047: (VPN-unit) Failed to sync SDI node secret file for server IP_address on the standby unit.
- %ASA-4-720051: (VPN-unit) Failed to add new SDI node secret file for server id on the standby unit.
- %ASA-4-720052: (VPN-unit) Failed to delete SDI node secret file for server id on the standby unit.
- %ASA-4-720053: (VPN-unit) Failed to add cTCP IKE rule during bulk sync, peer=IP_address, port=port
- %ASA-4-720054: (VPN-unit) Failed to add new cTCP record, peer=IP_address, port=port.
- %ASA-4-720055: (VPN-unit) VPN Stateful failover can only be run in single/non-transparent mode.
- %ASA-4-720064: (VPN-unit) Failed to update cTCP database record for peer=IP_address, port=port during bulk sync.
- %ASA-4-720065: (VPN-unit) Failed to add new cTCP IKE rule, peer=peer, port=port.
- %ASA-4-720066: (VPN-unit) Failed to activate IKE database.
- %ASA-4-720067: (VPN-unit) Failed to deactivate IKE database.
- %ASA-4-720068: (VPN-unit) Failed to parse peer message.
- %ASA-4-720069: (VPN-unit) Failed to activate cTCP database.
- %ASA-4-720070: (VPN-unit) Failed to deactivate cTCP database.
- %ASA-4-720073: VPN Session failed to replicate - ACL acl_name not found
- %ASA-4-721007: (device) Fail to update access list list_name on standby unit.
- %ASA-4-721011: (device) Fail to add access list rule list_name, line line_no on standby unit.
- %ASA-4-721013: (device) Fail to enable APCF XML file file_name on the standby unit.

按严重性级别列出的消息

- %ASA-4-721015: (device) Fail to disable APCF XML file file_name on the standby unit.
- %ASA-4-721017: (device) Fail to create WebVPN session for user user_name, IP ip_address.
- %ASA-4-721019: (device) Fail to delete WebVPN session for client user user_name, IP ip_address.
- %ASA-4-722001: IP IP_address Error parsing SVC connect request.
- %ASA-4-722002: IP IP_address Error consolidating SVC connect request.
- %ASA-4-722003: IP IP_address Error authenticating SVC connect request.
- %ASA-4-722004: Group group User user-name IP IP_address Error responding to SVC connect request.
- %ASA-4-722015: Group group User user-name IP IP_address Unknown SVC frame type: type-num
- %ASA-4-722016: Group group User user-name IP IP_address Bad SVC frame length: length expected: expected-length
- %ASA-4-722017: Group group User user-name IP IP_address Bad SVC framing: 525446, reserved: 0
- %ASA-4-722018: Group group User user-name IP IP_address Bad SVC protocol version: version, expected: expected-version
- %ASA-4-722019: Group group User user-name IP IP_address Not enough data for an SVC header: length
- %ASA-4-722041: TunnelGroup tunnel_group GroupPolicy group_policy User username IP peer_address No IPv6 address available for SVC connection
- %ASA-4-722042: Group group User user IP ip Invalid Cisco SSL Tunneling Protocol version.
- %ASA-4-722047: Group group User user IP ip Tunnel terminated: SVC not enabled or invalid SVC image on the ASA.
- %ASA-4-722048: Group group User user IP ip Tunnel terminated: SVC not enabled for the user.
- %ASA-4-722049: Group group User user IP ip Session terminated: SVC not enabled or invalid image on the ASA.
- %ASA-4-722050: Group group User user IP ip Session terminated: SVC not enabled for the user.
- %ASA-4-722054: Group group policy User user name IP remote IP SVC terminating connection: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP
- %ASA-4-724001: Group group-name User user-name IP IP_address WebVPN session not allowed.Unable to determine if Cisco Secure Desktop was running on the client's workstation.
- %ASA-4-724002: Group group-name User user-name IP IP_address WebVPN session not terminated.Cisco Secure Desktop was not running on the client's workstation.
- %ASA-4-733100: Object drop rate rate_ID exceeded.Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt
- %ASA-4-733101: Object objectIP (is targeted|is attacking).Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt.
- %ASA-4-733102: Threat-detection adds host %I to shun list
- %ASA-4-733103: Threat-detection removes host %I from shun list
- %ASA-4-733104: TD_SYSLOG_TCP_INTERCEPT_AVERAGE_RATE_EXCEED
- %ASA-4-733105: TD_SYSLOG_TCP_INTERCEPT_BURST_RATE_EXCEED
- %ASA-4-735015: CPU var1: Temp: var2 var3, Warm
- %ASA-4-735016: Chassis Ambient var1: Temp: var2 var3, Warm
- %ASA-4-735018: Power Supply var1: Temp: var2 var3, Critical

- %ASA-4-735019: Power Supply var1: Temp: var2 var3, Warm
- %ASA-4-735026: CPU cpu_num Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately.The chassis and CPU need to be inspected immediately for ventilation issues.
- %ASA-4-737012: IPAA: Address assignment failed
- %ASA-4-737013: IPAA: Error freeing address ip-address, not found
- %ASA-4-737019: IPAA: Unable to get address from group-policy or tunnel-group local pools
- %ASA-4-737028: IPAA: Adding ip-address to standby: failed
- %ASA-4-737030: IPAA: Adding %m to standby: address already in use
- %ASA-4-737032: IPAA: Removing ip-address from standby: not found
- %ASA-4-737033: IPAA: Unable to assign addr_allocator provided IP address ip_addr to client.This IP address has already been assigned by previous_addr_allocator
- %ASA-4-741005: Coredump operation variable 1 failed with error variable 2 variable 3
- %ASA-4-741006: Unable to write Coredump Helper configuration, reason variable 1
- %ASA-4-747008: Clustering: New cluster member name with serial number serial-number-A rejected due to name conflict with existing unit with serial number serial-number-B.
- %ASA-4-747015: Clustering: Forcing stray member unit-name to leave the cluster.
- %ASA-4-747016: Clustering: Found a split cluster with both unit-name-A and unit-name-B as master units.Master role retained by unit-name-A, unit-name-B will leave, then join as a slave.
- %ASA-4-747017: Clustering: Failed to enroll unit unit-name due to maximum member limit limit-value reached.
- %ASA-4-747019: Clustering: New cluster member name rejected due to Cluster Control Link IP subnet mismatch (ip-address/ip-mask on new unit, ip-address/ip-mask on local unit).
- %ASA-4-747020: Clustering: New cluster member unit-name rejected due to encryption license mismatch.
- %ASA-4-747025: Clustering: New cluster member unit-name rejected due to firewall mode mismatch.
- %ASA-4-747026: Clustering: New cluster member unit-name rejected due to cluster interface name mismatch (ifc-name on new unit, ifc-name on local unit).
- %ASA-4-747027: Clustering: Failed to enroll unit unit-name due to insufficient size of cluster pool pool-name in context-name.
- %ASA-4-747028: Clustering: New cluster member unit-name rejected due to interface mode mismatch (mode-name on new unit, mode-name on local unit).
- %ASA-4-747029: Clustering: Unit unit-name is quitting due to Cluster Control Link down.
- %ASA-4-748002: Clustering configuration on the chassis is missing or incomplete; clustering is disabled
- %ASA-4-748003: Module slot_number in chassis chassis_number is leaving the cluster due to a chassis health check failure
- %ASA-4-750003: Local: local IP:local port Remote: remote IP:remote port Username: username Negotiation aborted due to ERROR: error
- %ASA-4-750012: Selected IKEv2 encryption algorithm (IKEV2 encry algo) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo).
- %ASA-4-750014: Local:<self ip>:<self port> Remote:<peer ip>:<peer port> Username:<TG or Username> IKEv2 Session aborted.Reason: Initial Contact received for Local ID: <self ID>, Remote ID: <peer ID> from remote peer:<peer ip>:<peer port> to <self ip>:<self port>
- %ASA-4-751014: Local: localIP:port Remote remoteIP:port Username: username/group Warning Configuration Payload request for attribute attribute ID could not be processed.Error: error

- %ASA-4-751015: Local: localIP:port Remote remoteIP:port Username: username/group SA request rejected by CAC.Reason: reason
- %ASA-4-751016: Local: localIP:port Remote remoteIP:port Username: username/group L2L peer initiated a tunnel with the same outer and inner addresses.Peer could be Originate only - Possible misconfiguration!
- %ASA-4-751019: Local:LocalAddr Remote:RemoteAddr Username:username Failed to obtain an licenseType license.Maximum license limit limit exceeded.
- %ASA-4-751021: Local:variable 1:variable 2 Remote:variable 3:variable 4 Username:variable 5 variable 6 with variable 7 encryption is not supported with this version of the AnyConnect Client.Please upgrade to the latest Anyconnect Client.
- %ASA-4-751027: Local:local IP:local port Remote:peer IP:peer port Username:username IKEv2 Received INVALID_SELECTORS Notification from peer.Peer received a packet (SPI=spi).The decapsulated inner packet didn’t match the negotiated policy in the SA.Packet destination pkt_daddr, port pkt_dest_port, source pkt_saddr, port pkt_src_port, protocol pkt_prot.
- %ASA-4-752009: IKEv2 Doesn't support Multiple Peers
- %ASA-4-752010: IKEv2 Doesn't have a proposal specified
- %ASA-4-752011: IKEv1 Doesn't have a transform set specified
- %ASA-4-752012: IKEv protocol was unsuccessful at setting up a tunnel.Map Tag = mapTag.Map Sequence Number = mapSeq.
- %ASA-4-752013: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2 after a failed attempt.Map Tag = mapTag.Map Sequence Number = mapSeq.
- %ASA-4-752014: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1 after a failed attempt.Map Tag = mapTag.Map Sequence Number = mapSeq.
- %ASA-4-752017: IKEv2 Backup L2L tunnel initiation denied on interface interface matching crypto map name, sequence number number.Unsupported configuration.
- %ASA-4-753001: Unexpected IKEv2 packet received from <IP>:<port>.Error: <reason>
- %ASA-4-768003: SSH: connection timed out: username username, IP ip
- %ASA-4-770001: Resource resource allocation is more than the permitted list of limit for this platform.If this condition persists, the ASA will be rebooted.
- %ASA-4-770003: Resource resource allocation is less than the minimum requirement of value for this platform.If this condition persists, performance will be lower than normal.
- %ASA-4-775002: Reason - protocol connection conn_id from interface_name:real_address/real_port [(idfw_user)] to interface_name:real_address/real_port is action locally
- %ASA-4-802006: IP ip_address MDM request details has been rejected: details.

严重性级别为 5 的通知消息

以下通知消息的严重性级别为 5：

- %ASA-5-109012: Authen Session End: user 'user', sid number, elapsed number seconds
- %ASA-5-109029: Parsing downloaded ACL: string
- %ASA-5-109039: AAA Authentication:Dropping an unsupported IPv6/IP46/IP64 packet from lifc:laddr to fifc:faddr
- %ASA-5-111001: Begin configuration: IP_address writing to device

- %ASA-5-111002: Begin configuration: IP_address reading from device
- %ASA-5-111003: IP_address Erase configuration
- %ASA-5-111004: IP_address end configuration: {FAILED|OK}
- %ASA-5-111005: IP_address end configuration: OK
- %ASA-5-111007: Begin configuration: IP_address reading from device.
- %ASA-5-111008: User user executed the command string
- %ASA-5-111010: User username, running application-name from IP ip addr, executed cmd
- %ASA-5-113024: Group tg: Authenticating type connection from ip with username, user_name, from client certificate
- %ASA-5-113025: Group tg: FAILED to extract username from certificate while authenticating type connection from ip
- %ASA-5-199001: Reload command executed from Telnet (remote IP_address).
- %ASA-5-199017: syslog
- %ASA-5-212009: Configuration request for SNMP group groupname failed.User username, reason.
- %ASA-5-303004: FTP cmd_string command unsupported - failed strict inspection, terminating connection from source_interface:source_address/source_port to dest_interface:dest_address/dest_interface
- %ASA-5-303005: Strict FTP inspection matched match_string in policy-map policy-name, action_string from src_ifc:sip/sport to dest_ifc:dip/dport
- %ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection protocol src interface_name:source_address/source_port [(idfw_user)] dst interface_name:dest_address/dst_port [(idfw_user)] denied due to NAT reverse path failure.
- %ASA-5-321001: Resource var1 limit of var2 reached.
- %ASA-5-321002: Resource var1 rate limit of var2 reached.
- ASA-5-331002: Dynamic DNS type RR for ('fqdn_name' - ip_address | ip_address - 'fqdn_name') successfully updated in DNS server dns_server_ip
- %ASA-5-332003: Web Cache IP_address/service_ID acquired
- %ASA-5-333002: Timeout waiting for EAP response - context:EAP-context
- %ASA-5-333010: EAP-SQ response Validation Flags TLV indicates PV request - context:EAP-context
- %ASA-5-334002: EAPoUDP association successfully established - host-address
- %ASA-5-334003: EAPoUDP association failed to establish - host-address
- %ASA-5-334005: Host put into NAC Hold state - host-address
- %ASA-5-334006: EAPoUDP failed to get a response from host - host-address
- %ASA-5-336010 EIGRP-ddb_name tableid as_id: Neighbor address (%interface) is event_msg: msg
- %ASA-5-402128: CRYPTO: An attempt to allocate a large memory block failed, size: size, limit: limit
- %ASA-5-425005 Interface interface_name become active in redundant interface redundant_interface_name
- %ASA-5-4302310: SCTP packet received from src_ifc:src_ip/src_port to dst_ifc:dst_ip/dst_port contains unsupported Hostname Parameter.
- %ASA-5-434004: SFR requested ASA to bypass further packet redirection and process flow from %s:%A/%d to %s:%A/%d locally
- %ASA-5-500001: ActiveX content in java script is modified: src src ip dest dest ip on interface interface name
- %ASA-5-500002: Java content in java script is modified: src src ip dest dest ip on interface interface name

按严重性级别列出的消息

- %ASA-5-500003: Bad TCP hdr length (hdrlen=bytes, pktlen=bytes) from source_address/source_port to dest_address/dest_port, flags: tcp_flags, on interface interface_name
- %ASA-5-501101: User transitioning priv level
- %ASA-5-502101: New user added to local dbase: Uname: user Priv: privilege_level Encpass: string
- %ASA-5-502102: User deleted from local dbase: Uname: user Priv: privilege_level Encpass: string
- %ASA-5-502103: User priv level changed: Uname: user From: privilege_level To: privilege_level
- %ASA-5-502111: New group policy added: name: policy_name Type: policy_type
- %ASA-5-502112: Group policy deleted: name: policy_name Type: policy_type
- %ASA-5-503001: Process number, Nbr IP_address on interface_name from string to string, reason
- %ASA-5-504001: Security context context_name was added to the system
- %ASA-5-504002: Security context context_name was removed from the system
- %ASA-5-505001: Module module_id is shutting down.Please wait...
- %ASA-5-505002: Module ips is reloading.Please wait...
- %ASA-5-505003: Module module_id is resetting.Please wait...
- %ASA-5-505004: Module module_id shutdown is complete.
- %ASA-5-505005: Module module_name is initializing control communication.Please wait...
- %ASA-5-505006: Module module_id is Up.
- %ASA-5-505007: Module module_id is recovering.Please wait...
- %ASA-5-505008: Module module_id software is being updated to vnewver (currently vver)
- %ASA-5-505009: Module module_id software was updated to vnewver (previously vver)
- %ASA-5-505010: Module in slot slot removed.
- %ASA-5-505012: Module module_id, application stopped application, version version
- %ASA-5-505013: Module module_id application changed from: application version version to: newapplication version newversion.
- %ASA-5-506001: event_source_string event_string
- %ASA-5-507001: Terminating TCP-Proxy connection from interface_inside:source_address/source_port to interface_outside:dest_address/dest_port - reassembly limit of limit bytes exceeded
- %ASA-5-509001: Connection attempt from src_intf:src_ip/src_port [([idfw_user | FQDN_string], sg_info)] to dst_intf:dst_ip/dst_port [([idfw_user | FQDN_string], sg_info)] was prevented by "no forward" command.
- %ASA-5-503101: Process %d, Nbr %i on %s from %s to %s, %s
- %ASA-5-611104: Serial console idle timeout exceeded
- %ASA-5-612001: Auto Update succeeded:filename, version:number
- %ASA-5-711005: Traceback: call_stack
- %ASA-5-713006: Failed to obtain state for message Id message_number, Peer Address: IP_address
- %ASA-5-713010: IKE area: failed to find centry for message Id message_number
- %ASA-5-713041: IKE Initiator: new or rekey Phase 1 or 2, Intf interface_number, IKE Peer IP_address local Proxy Address IP_address, remote Proxy Address IP_address, Crypto map (crypto map tag)
- %ASA-5-713049: Security negotiation complete for tunnel_type type (group_name) Initiator/Responder, Inbound SPI = SPI, Outbound SPI = SPI
- %ASA-5-713050: Connection terminated for peer IP_address.Reason: termination reason Remote Proxy IP_address, Local Proxy IP_address

- %ASA-5-713068: Received non-routine Notify message: notify_type (notify_value)
- %ASA-5-713073: Responder forcing change of Phase 1/Phase 2 rekeying duration from larger_value to smaller_value seconds
- %ASA-5-713074: Responder forcing change of IPSec rekeying duration from larger_value to smaller_value Kbs
- %ASA-5-713075: Overriding Initiator's IPSec rekeying duration from larger_value to smaller_value seconds
- %ASA-5-713076: Overriding Initiator's IPSec rekeying duration from larger_value to smaller_value Kbs
- %ASA-5-713092: Failure during phase 1 rekeying attempt due to collision
- %ASA-5-713115: Client rejected NAT enabled IPSec request, falling back to standard IPSec
- %ASA-5-713119: Group group IP ip PHASE 1 COMPLETED
- %ASA-5-713120: PHASE 2 COMPLETED (msgid=msg_id)
- %ASA-5-713130: Received unsupported transaction mode attribute: attribute id
- %ASA-5-713131: Received unknown transaction mode attribute: attribute_id
- %ASA-5-713135: message received, redirecting tunnel to IP_address.
- %ASA-5-713136: IKE session establishment timed out [IKE_state_name], aborting!
- %ASA-5-713137: Reaper overriding refCnt [ref_count] and tunnelCnt [tunnel_count] -- deleting SA!
- %ASA-5-713139: group_name not found, using BASE GROUP default preshared key
- %ASA-5-713144: Ignoring received malformed firewall record; reason - error_reason TLV type attribute_value correction
- %ASA-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address, mask: netmask
- %ASA-5-713155: DNS lookup for Primary VPN Server [server_name] successfully resolved after a previous failure.Resetting any Backup Server init.
- %ASA-5-713156: Initializing Backup Server [server_name or IP_address]
- %ASA-5-713158: Client rejected NAT enabled IPSec Over UDP request, falling back to IPSec Over TCP
- %ASA-5-713178: IKE Initiator received a packet from its peer without a Responder cookie
- %ASA-5-713179: IKE AM Initiator received a packet from its peer without a payload_type payload
- %ASA-5-713196: Remote L2L Peer IP_address initiated a tunnel with same outer and inner addresses.Peer could be Originate Only - Possible misconfiguration!
- %ASA-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel_type connection.Enforcing the second default.
- %ASA-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter (counter_value)!
- %ASA-5-713201: Duplicate Phase Phase packet detected.操作
- %ASA-5-713216: Rule: action [Client type]: version Client: type version allowed/ not allowed
- %ASA-5-713229: Auto Update - Notification to client client_ip of update string: message_string.
- %ASA-5-713237: ACL update (access_list) received during re-key re-authentication will not be applied to the tunnel.
- %ASA-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.
- %ASA-5-713250: META-DATA Received unknown Internal Address attribute: attribute

按严重性级别列出的消息

- %ASA-5-713252: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available.VPN Tunnel creation rejected for client.
- %ASA-5-713253: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available.Entering ALLOW mode.VPN Tunnel created for client.
- %ASA-5-713257: Phase *var1* failure: Mismatched attribute types for class *var2* : Rcv'd: *var3* Cfg'd: *var4*
- %ASA-5-713259: Group = groupname, Username = username, IP = peerIP, Session is being torn down.Reason: reason
- %ASA-5-713904: Descriptive_event_string.
- %ASA-5-716053: SSO Server added: name: name Type: type
- %ASA-5-716054: SSO Server deleted: name: name Type: type
- %ASA-5-717013: Removing a cached CRL to accommodate an incoming CRL.Issuer: issuer
- %ASA-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = size, available cache space = space)
- %ASA-5-717050: SCEP Proxy: Processed request type type from IP client ip address, User username, TunnelGroup tunnel_group name, GroupPolicy group-policy name to CA IP ca ip address
- %ASA-5-717053: Group group name User user name IP IP Address Periodic certificate authentication succeeded.Subject Name id subject name Issuer Name id issuer name Serial Number id serial number
- %ASA-5-717061: Starting protocol certificate enrollment for the trustpoint tpname with the CA ca_name.Request Type type Mode mode
- %ASA-5-717062: protocol Certificate enrollment succeeded for the trustpoint tpname with the CA ca. Received a new certificate with Subject Name subject Issuer Name issuer Serial Number serial
- %ASA-5-717064: Keypair keyname in the trustpoint tpname is regenerated for mode protocol certificate renewal
- %ASA-5-718002: Create peer IP_address failure, already at maximum of number_of_peers
- %ASA-5-718005: Fail to send to IP_address, port port
- %ASA-5-718006: Invalid load balancing state transition [cur=state_number][event=event_number]
- %ASA-5-718007: Socket open failure failure_code
- %ASA-5-718008: Socket bind failure failure_code
- %ASA-5-718009: Send HELLO response failure to IP_address
- %ASA-5-718010: Sent HELLO response to IP_address
- %ASA-5-718011: Send HELLO request failure to IP_address
- %ASA-5-718012: Sent HELLO request to IP_address
- %ASA-5-718014: Master peer IP_address is not answering HELLO
- %ASA-5-718015: Received HELLO request from IP_address
- %ASA-5-718016: Received HELLO response from IP_address
- %ASA-5-718024: Send CFG UPDATE failure to IP_address
- %ASA-5-718028: Send OOS indicator failure to IP_address
- %ASA-5-718031: Received OOS obituary for IP_address
- %ASA-5-718032: Received OOS indicator from IP_address
- %ASA-5-718033: Send TOPOLOGY indicator failure to IP_address
- %ASA-5-718042: Unable to ARP for IP_address
- %ASA-5-718043: Updating/removing duplicate peer entry IP_address
- %ASA-5-718044: Deleted peer IP_address

- %ASA-5-718045: Created peer IP_address
- %ASA-5-718048: Create of secure tunnel failure for peer IP_address
- %ASA-5-718050: Delete of secure tunnel failure for peer IP_address
- %ASA-5-718052: Received GRAT-ARP from duplicate master MAC_address
- %ASA-5-718053: Detected duplicate master, mastership stolen MAC_address
- %ASA-5-718054: Detected duplicate master MAC_address and going to SLAVE
- %ASA-5-718055: Detected duplicate master MAC_address and staying MASTER
- %ASA-5-718057: Queue send failure from ISR, msg type failure_code
- %ASA-5-718060: Inbound socket select fail: context=context_ID.
- %ASA-5-718061: Inbound socket read fail: context=context_ID.
- %ASA-5-718062: Inbound thread is awake (context=context_ID).
- %ASA-5-718063: Interface interface_name is down.
- %ASA-5-718064: Admin. interface interface_name is down.
- %ASA-5-718065: Cannot continue to run (public=up/down, private=up/down, enable=LB_state, master=IP_address, session=Enable/Disable).
- %ASA-5-718066: Cannot add secondary address to interface interface_name, ip IP_address.
- %ASA-5-718067: Cannot delete secondary address to interface interface_name, ip IP_address.
- %ASA-5-718068: Start VPN Load Balancing in context context_ID.
- %ASA-5-718069: Stop VPN Load Balancing in context context_ID.
- %ASA-5-718070: Reset VPN Load Balancing in context context_ID.
- %ASA-5-718071: Terminate VPN Load Balancing in context context_ID.
- %ASA-5-718072: Becoming master of Load Balancing in context context_ID.
- %ASA-5-718073: Becoming slave of Load Balancing in context context_ID.
- %ASA-5-718074: Fail to create access list for peer context_ID.
- %ASA-5-718075: Peer IP_address access list not set.
- %ASA-5-718076: Fail to create tunnel group for peer IP_address.
- %ASA-5-718077: Fail to delete tunnel group for peer IP_address.
- %ASA-5-718078: Fail to create crypto map for peer IP_address.
- %ASA-5-718079: Fail to delete crypto map for peer IP_address.
- %ASA-5-718080: Fail to create crypto policy for peer IP_address.
- %ASA-5-718081: Fail to delete crypto policy for peer IP_address.
- %ASA-5-718082: Fail to create crypto ipsec for peer IP_address.
- %ASA-5-718083: Fail to delete crypto ipsec for peer IP_address.
- %ASA-5-718084: Public/cluster IP not on the same subnet: public IP_address, mask netmask, cluster IP_address
- %ASA-5-718085: Interface interface_name has no IP address defined.
- %ASA-5-718086: Fail to install LB NP rules: type rule_type, dst interface_name, port port.
- %ASA-5-718087: Fail to delete LB NP rules: type rule_type, rule rule_ID.
- %ASA-5-719014: Email Proxy is changing listen port from old_port to new_port for mail protocol protocol.
- %ASA-5-720016: (VPN-unit) Failed to initialize default timer #index.

按严重性级别列出的消息

- %ASA-5-720017: (VPN-unit) Failed to update LB runtime data
- %ASA-5-720018: (VPN-unit) Failed to get a buffer from the underlying core high availability subsystem.Error code code.
- %ASA-5-720019: (VPN-unit) Failed to update cTCP statistics.
- %ASA-5-720020: (VPN-unit) Failed to send type timer message.
- %ASA-5-720021: (VPN-unit) HA non-block send failed for peer msg message_number.HA error code.
- %ASA-5-720035: (VPN-unit) Fail to look up CTCP flow handle
- %ASA-5-720036: (VPN-unit) Failed to process state update message from the active peer.
- %ASA-5-720071: (VPN-unit) Failed to update cTCP dynamic data.
- %ASA-5-720072: Timeout waiting for Integrity Firewall Server [interface,ip] to become available.
- %ASA-5-722037: Group group User user-name IP IP_address SVC closing connection: reason.
- %ASA-5-722038: Group group-name User user-name IP IP_address SVC terminating session: reason.
- %ASA-5-722005: Group group User user-name IP IP_address Unable to update session information for SVC connection.
- %ASA-5-722006: Group group User user-name IP IP_address Invalid address IP_address assigned to SVC connection.
- %ASA-5-722010: Group group User user-name IP IP_address SVC Message: type-num/NOTICE: message
- %ASA-5-722011: Group group User user-name IP IP_address SVC Message: type-num/NOTICE: message
- %ASA-5-722012: Group group User user-name IP IP_address SVC Message: type-num/INFO: message
- %ASA-5-722028: Group group User user-name IP IP_address Stale SVC connection closed.
- %ASA-5-722032: Group group User user-name IP IP_address New SVC connection replacing old connection.
- %ASA-5-722033: Group group User user-name IP IP_address First SVC connection established for SVC session.
- %ASA-5-722034: Group group User user-name IP IP_address New SVC connection, no existing connection.
- %ASA-5-722037: Group group User user-name IP IP_address SVC closing connection: reason.
- %ASA-5-722038: Group group-name User user-name IP IP_address SVC terminating session: reason.
- %ASA-5-722043: Group group User user IP ip DTLS disabled: unable to negotiate cipher.
- %ASA-5-722044: Group group User user IP ip Unable to request ver address for SSL tunnel.
- %ASA-5-734002: DAP: User user, Addr ipaddr: Connection terminated by the following DAP records: DAP record names
- %ASA-5-737003: IPAA: DHCP configured, no viable servers found for tunnel-group 'tunnel-group'
- %ASA-5-737004: IPAA: DHCP configured, request failed for tunnel-group 'tunnel-group'
- %ASA-5-737007: IPAA: Local pool request failed for tunnel-group 'tunnel-group'
- %ASA-5-737008: IPAA: 'tunnel-group' not found
- %ASA-5-737011: IPAA: AAA assigned address ip-address, not permitted, retrying
- %ASA-5-737018: IPAA: DHCP request attempt num failed
- %ASA-5-737021: IPAA: Address from local pool (ip-address) duplicates address from DHCP
- %ASA-5-737022: IPAA: Address from local pool (ip-address) duplicates address from AAA
- %ASA-5-737023: IPAA: Unable to allocate memory to store local pool address ip-address

- %ASA-5-737024: IPAA: Local pool assignment failed for suggested IP ip-address, retrying
- %ASA-5-737025: IPAA: Not releasing local pool ip-address, due to local pool duplicate issue
- %ASA-5-737034: IPAA: Session=<session>, <IP version> address: <explanation>
- %ASA-5-747002: Clustering: Recovered from state machine dropped event (event-id, ptr-in-hex, ptr-in-hex).Intended state: state-name.Current state: state-name.
- %ASA-5-747003: Clustering: Recovered from state machine failure to process event (event-id, ptr-in-hex, ptr-in-hex) at state state-name.
- %ASA-5-747007: Clustering: Recovered from finding stray config sync thread, stack ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex.
- %ASA-5-748001: Module *slot_number* in chassis *chassis_number* is leaving the cluster due to a chassis configuration change
- %ASA-5-748004: Module *slot_number* in chassis *chassis_number* is re-joining the cluster due to a chassis health check recovery
- %ASA-5-750001: Local:local IP:local port Remote:remote IP: remote port Username: username Received request to request an IPsec tunnel; local traffic selector = local selectors: range, protocol, port range; remote traffic selector = remote selectors: range, protocol, port range
- %ASA-5-750002: Local:local IP:local port Remote: remote IP: remote port Username: username Received a IKE_INIT_SA request
- %ASA-5-750004: Local: local IP: local port Remote: remote IP: remote port Username: username Sending COOKIE challenge to throttle possible DoS
- %ASA-5-750005: Local: local IP: local port Remote: remote IP: remote port Username: username IPsec rekey collision detected.I am lowest nonce initiator, deleting SA with inbound SPI SPI
- %ASA-5-750006: Local: local IP: local port Remote: remote IP: remote port Username: username SA UP.Reason: reason
- %ASA-5-750007: Local: local IP: local port Remote: remote IP: remote port Username: username SA DOWN.Reason: reason
- %ASA-5-750008: Local: local IP: local port Remote: remote IP: remote port Username: username SA rejected due to system resource low
- %ASA-5-750009: Local: local IP: local port Remote: remote IP: remote port Username: username SA request rejected due to CAC limit reached: Rejection reason: reason
- %ASA-5-750010: Local: local-ip Remote: remote-ip Username:username IKEv2 local throttle-request queue depth threshold of threshold reached; increase the window size on peer peer for better performance
- %ASA-5-750013 - IKEv2 SA (iSPI <ISPI> rRSP <rSPI>) Peer Moved: Previous <prev_remote_ip>:<prev_remote_port>/<prev_local_ip>:<prev_local_port>.Updated <new_remote_ip>:<new_remote_port>/<new_local_ip>:<new_local_port>
- %ASA-5-751007: Local: localIP:port Remote:remoteIP:port Username: username/group Configured attribute not supported for IKEv2.Attribute: attribute
- %ASA-5-751025: Local: local IP:local port Remote: remote IP:remote port Username:username Group:group-policy IPv4 Address=assigned_IPv4_addr IPv6 address=assigned_IPv6_addr assigned to session.
- %ASA-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2.Map Tag = mapTag.Map Sequence Number = mapSeq.
- %ASA-5-752004: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1.Map Tag = mapTag.Map Sequence Number = mapSeq.
- %ASA-5-752016: IKEv protocol was successful at setting up a tunnel.Map Tag = mapTag.Map Sequence Number = mapSeq.

- %ASA-5-776252: CTS SGT-MAP: CTS SGT-MAP: Binding binding IP - SGname(SGT) from source name deleted from binding manager.
- %ASA-5-769001: UPDATE: ASA image src was added to system boot list
- %ASA-5-769002: UPDATE: ASA image src was copied to dest
- %ASA-5-769003: UPDATE: ASA image src was renamed to dest
- %ASA-5-769004: UPDATE: ASA image src_file failed verification, reason: failure_reason
- %ASA-5-769005: UPDATE: ASA image image_name passed image verification
- %ASA-5-8300006: Cluster topology change detected.VPN session redistribution aborted.

严重级别为 6 的信息性消息

以下信息性消息的严重性级别为 6：

- %ASA-6-106012: Deny IP from IP_address to IP_address, IP options hex.
- %ASA-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name.
- %ASA-6-106100: access-list acl_ID {permitted | denied | est-allowed} protocol interface_name/source_address(source_port)(idfw_user, sg_info) interface_name/dest_address(dest_port)(idfw_user, sg_info) hit-cnt number ({first hit | number-second interval})
- %ASA-6-106102: access-list acl_ID {permitted | denied} protocol for user username interface_name/source_address source_port interface_name/dest_address dest_port hit-cnt number {first hit | number-second interval} hash codes
- %ASA-6-109036: Exceeded 1000 attribute values for the attribute name attribute for user username.
- %ASA-6-109100: Received CoA update from *coa-source-ip* for user *username* , with session ID: *audit-session-id* , changing authorization attributes
- %ASA-6-109101: Received CoA disconnect request from *coa-source-ip* for user *username* , with audit-session-id: *audit-session-id*
- %ASA-6-110002: Failed to locate egress interface for protocol from src interface:src IP/src port to dest IP/dest port
- %ASA-6-110003: Routing failed to locate next-hop for protocol from src interface:src IP/src port to dest interface:dest IP/dest port
- %ASA-6-110004: Egress interface changed from old_active_ifc to new_active_ifc on ip_protocol connection conn_id for outside_zone/parent_outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) to inside_zone/parent_inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port)
- %ASA-6-113003: AAA group policy for user user is being set to policy_name.
- %ASA-6-113004: AAA user aaa_type Successful: server = server_IP_address, User = user
- %ASA-6-113005: AAA user authentication Rejected: reason = string: server = server_IP_address, User = user: user IP = user_ip
- %ASA-6-113006: User user locked out on exceeding number successive failed authentication attempts
- %ASA-6-113007: User user unlocked by administrator
- %ASA-6-113008: AAA transaction status ACCEPT: user = user
- %ASA-6-113009: AAA retrieved default group policy policy for user user
- %ASA-6-113010: AAA challenge received for user user from server server_IP_address

- %ASA-6-113011: AAA retrieved user specific group policy policy for user user
- %ASA-6-113012: AAA user authentication Successful: local database: user = user
- %ASA-6-113013: AAA unable to complete the request Error: reason = reason: user = user
- %ASA-6-113014: AAA authentication server not accessible: server = server_IP_address: user = user
- %ASA-6-113015: AAA user authentication Rejected: reason = reason: local database: user = user: user IP =xxx.xxx.xxx.xxx
- %ASA-6-113016: AAA credentials rejected: reason = reason: server = server_IP_address: user = user: user IP = xxx.xxx.xxx.xxx
- %ASA-6-113017: AAA credentials rejected: reason = reason: local database: user = user: user IP = user_ip=xxx.xxx.xxx.xxx
- %ASA-6-113033: Group group User user IP ipaddr AnyConnect session not allowed.ACL parse error.
- %ASA-6-113037: Reboot pending, new sessions disabled.Denied user login.
- %ASA-6-113039: Group group User user IP ipaddr AnyConnect parent session started.
- %ASA-6-114004: 4GE SSM I/O Initialization start.
- %ASA-6-114005: 4GE SSM I/O Initialization end.
- %ASA-6-199002: startup completed.Beginning operation.
- %ASA-6-199003: Reducing link MTU dec.
- %ASA-6-199005: Startup begin
- %ASA-6-199018: syslog
- %ASA-6-201010: Embryonic connection limit exceeded econns/limit for dir packet from source_address/source_port to dest_address/dest_port on interface interface_name
- %ASA-6-201012: Per-client embryonic connection limit exceeded curr num/limit for [input|output] packet from IP_address/ port to ip/port on interface interface_name
- %ASA-6-210022: LU missed number updates
- %ASA-6-302003: Built H245 connection for foreign_address outside_address/outside_port local_address inside_address/inside_port
- %ASA-6-302004: Pre-allocate H323 UDP backconnection for foreign_address outside_address/outside_port to local_address inside_address/inside_port
- %ASA-6-302010: connections in use, connections most used
- %ASA-6-302012: Pre-allocate H225 Call Signalling Connection for faddr IP_address/port to laddr IP_address
- %ASA-6-302013: Built {inbound|outbound} TCP connection_id for interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] to interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] [(user)]
- %ASA-6-302014: Teardown TCP connection id for interface:real-address/real-port [(idfw_user)] to interface:real-address/real-port [(idfw_user)] duration hh:mm:ss bytes bytes [reason] [(user)]
- %ASA-6-302015: Built {inbound|outbound} UDP connection number for interface_name:real_address/real_port (mapped_address/mapped_port) [(idfw_user)] to interface_name:real_address/real_port (mapped_address/mapped_port) [(idfw_user)] [(user)]
- %ASA-6-302016: Teardown UDP connection number for interface:real-address/real-port [(idfw_user)] to interface:real-address/real-port [(idfw_user)] duration hh:mm:ss bytes bytes [(user)]
- %ASA-6-302017: Built {inbound|outbound} GRE connection id from interface:real_address (translated_address) [(idfw_user)] to interface:real_address/real_cid (translated_address/translated_cid) [(idfw_user)] [(user)

按严重性级别列出的消息

- %ASA-6-302018: Teardown GRE connection id from interface:real_address (translated_address) [(idfw_user)] to interface:real_address/real_cid (translated_address/translated_cid) [(idfw_user)] duration hh:mm:ss bytes bytes [(user)]
- %ASA-6-302020: Built ICMP connection connection_id from interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] to interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] [(user)]
- %ASA-6-302021: Teardown ICMP connection connection_id from interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] to interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] [(user)]
- %ASA-6-302022: Built role stub TCP connection for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port)
- %ASA-6-302023: Teardown stub TCP connection for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss forwarded bytes bytes reason
- %ASA-6-302024: Built role stub UDP connection for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port)
- %ASA-6-302025: Teardown stub UDP connection for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss forwarded bytes bytes reason
- %ASA-6-302026: Built role stub ICMP connection for interface:real-address/real-port (mapped-address) to interface:real-address/real-port (mapped-address)
- %ASA-6-302027: Teardown stub ICMP connection for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss forwarded bytes bytes reason
- %ASA-6-302033: Pre-allocated H323 GUP Connection for faddr interface:foreign address/foreign-port to laddr interface:local-address/local-port
- %ASA-6-302303: Built TCP state-bypass connection conn_id from initiator_interface:real_ip/real_port(mapped_ip/mapped_port) to responder_interface:real_ip/real_port (mapped_ip/mapped_port)
- %ASA-6-302304: Teardown TCP state-bypass connection conn_id from initiator_interface:ip/port to responder_interface:ip/port duration, bytes, teardown reason.
- %ASA-6-303002: FTP connection from src_ifc:src_ip/src_port to dst_ifc:dst_ip/dst_port, user username action file filename
- %ASA-6-305009: Built {dynamic|static} translation from interface_name [(acl-name)]:real_address [(idfw_user)] to interface_name:mapped_address
- %ASA-6-305010: Teardown {dynamic|static} translation from interface_name:real_address [(idfw_user)] to interface_name:mapped_address duration time
- %ASA-6-305011: Built {dynamic|static} {TCP|UDP|ICMP} translation from interface_name:real_address/real_port [(idfw_user)] to interface_name:mapped_address/mapped_port
- %ASA-6-305012: Teardown {dynamic|static} {TCP|UDP|ICMP} translation from interface_name [(acl-name)]:real_address/{real_port|real_ICMP_ID} [(idfw_user)] to interface_name:mapped_address/{mapped_port|mapped_ICMP_ID} duration time
- %ASA-6-308001: console enable password incorrect for number tries (from IP_address)
- %ASA-6-311001: LU loading standby start
- %ASA-6-311002: LU loading standby end
- %ASA-6-311003: LU recv thread up
- %ASA-6-311004: LU xmit thread up
- %ASA-6-312001: RIP hdr failed from IP_address: cmd=string, version=number domain=string on interface interface_name

- %ASA-6-314001: Pre-allocated RTSP UDP backconnection for src_intf:src_IP to dst_intf:dst_IP/dst_port.
- %ASA-6-314002: RTSP failed to allocate UDP media connection from src_intf:src_IP to dst_intf:dst_IP/dst_port: reason_string.
- %ASA-6-317007: Added route_type route dest_address netmask via gateway_address [distance/metric] on interface_name route_type
- %ASA-6-317008: Deleted route_type route dest_address netmask via gateway_address [distance/metric] on interface_name route_type
- %ASA-6-321003: Resource var1 log level of var2 reached.
- %ASA-6-321004: Resource var1 rate log level of var2 reached
- %ASA-6-322004: No management IP address configured for transparent firewall.Dropping protocol protocol packet from interface_in:source_address/source_port to interface_out:dest_address/dest_port
- %ASA-6-333001: EAP association initiated - context:EAP-context
- %ASA-6-333003: EAP association terminated - context:EAP-context
- %ASA-6-333009: EAP-SQ response MAC TLV is invalid - context:EAP-context
- %ASA-6-334001: EAPoUDP association initiated - host-address
- %ASA-6-334004: Authentication request for NAC Clientless host - host-address
- %ASA-6-334007: EAPoUDP association terminated - host-address
- %ASA-6-334008: NAC EAP association initiated - host-address, EAP context:EAP-context
- %ASA-6-334009: Audit request for NAC Clientless host - Assigned_IP.
- %ASA-6-336011: event event
- %ASA-6-337000: Created BFD session with local discriminator id on real_interface with neighbor real_host_ip.
- %ASA-6-337001: Terminated BFD session with local discriminator id on real_interface with neighbor real_host_ip due to failure_reason.
-
- %ASA-6-340002: Loopback-proxy info: error_string context id context_id, context type = version/request_type/address_type client socket (internal)= client_address_internal/client_port_internal server socket (internal)= server_address_internal/server_port_internal server socket (external)= server_address_external/server_port_external remote socket (external)= remote_address_external/remote_port_external
- %ASA-6-341001: Policy Agent started successfully for VNMC vnmc_ip_addr
- %ASA-6-341002: Policy Agent stopped successfully for VNMC vnmc_ip_add
- %ASA-6-341010: Storage device with serial number ser_no [inserted into | removed from] bay bay_no
- %ASA-6-402129: CRYPTO: An attempt to release a DMA memory block failed, location: address
- %ASA-6-402130: CRYPTO: Received an ESP packet (SPI = 0x54A5C634, sequence number= 0x7B) from 75.2.96.101 (user= user) to 85.2.96.10 with incorrect IPsec padding
- %ASA-6-403500: PPPoE - Service name 'any' not received in PADO.Intf:interface_name AC:ac_name.
- %ASA-6-421006: There are number users of application accounted during the past 24 hours.
- %ASA-6-425001 Redundant interface redundant_interface_name created.
- %ASA-6-425002 Redundant interface redundant_interface_name removed.
- %ASA-6-425003 Interface interface_name added into redundant interface redundant_interface_name.
- %ASA-6-425004 Interface interface_name removed from redundant interface redundant_interface_name.

按严重性级别列出的消息

- %ASA-6-426001: PORT-CHANNEL:Interface ifc_name bundled into EtherChannel interface Port-channel num
- %ASA-6-426002: PORT-CHANNEL:Interface ifc_name unbundled from EtherChannel interface Port-channel num
- %ASA-6-426003: PORT-CHANNEL:Interface ifc_name1 has become standby in EtherChannel interface Port-channel num
- %ASA-6-426101: PORT-CHANNEL:Interface ifc_name is allowed to bundle into EtherChannel interface port-channel id by CLACP
- %ASA-6-426102: PORT-CHANNEL:Interface ifc_name is moved to standby in EtherChannel interface port-channel id by CLACP
- %ASA-6-426103: PORT-CHANNEL:Interface ifc_name is selected to move from standby to bundle in EtherChannel interface port-channel id by CLACP
- %ASA-6-426104: PORT-CHANNEL:Interface ifc_name is unselected in EtherChannel interface port-channel id by CLACP
- %ASA-6-602101: PMTU-D packet number bytes greater than effective mtu number dest_addr=dest_address, src_addr=source_address, prot=protocol
- %ASA-6-602103: IPSEC: Received an ICMP Destination Unreachable from src_addr with suggested PMTU of rcvd_mtu; PMTU updated for SA with peer peer_addr, SPI spi, tunnel name username, old PMTU old_mtu, new PMTU new_mtu.%ASA-7-703001: H.225 message received from interface_name:IP_address/port to interface_name:IP_address/port is using an unsupported version number
- %ASA-6-602104: IPSEC: Received an ICMP Destination Unreachable from src_addr, PMTU is unchanged because suggested PMTU of rcvd_mtu is equal to or greater than the current PMTU of curr_mtu, for SA with peer peer_addr, SPI spi, tunnel name username.
- %ASA-6-602303: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) has been created.
- %ASA-6-602304: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) has been deleted.
- %ASA-6-604101: DHCP client interface interface_name: Allocated ip = IP_address, mask = netmask, gw = gateway_address
- %ASA-6-604102: DHCP client interface interface_name: address released
- %ASA-6-604103: DHCP daemon interface interface_name: address granted MAC_address (IP_address)
- %ASA-6-604104: DHCP daemon interface interface_name: address released build_name (IP_address)
- %ASA-6-605004: Login denied from source-address/source-port to interface:destination/service for user “username”
- %ASA-6-605005: Login permitted from source-address/source-port to interface:destination/service for user “username”
- %ASA-6-607001: Pre-allocate SIP connection_type secondary channel for interface_name:IP_address/port to interface_name:IP_address from string message
- %ASA-6-608001: Pre-allocate Skinny connection_type secondary channel for interface_name:IP_address to interface_name:IP_address from string message
- %ASA-6-610101: Authorization failed: Cmd: command Cmdtype: command_modifier
- %ASA-6-611301: VPN Client: NAT configured for Client Mode with no split tunneling: NAT address: mapped_address

- %ASA-6-611302: VPN Client: NAT exemption configured for Network Extension Mode with no split tunneling
- %ASA-6-611303: VPN Client: NAT configured for Client Mode with split tunneling: NAT address: mapped_address Split Tunnel Networks: IP_address/netmask IP_address/netmask
- %ASA-6-611304: VPN Client: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: IP_address/netmask IP_address/netmask
- %ASA-6-611305: VPN Client: DHCP Policy installed: Primary DNS: IP_address Secondary DNS: IP_address Primary WINS: IP_address Secondary WINS: IP_address
- %ASA-6-611306: VPN Client: Perfect Forward Secrecy Policy installed
- %ASA-6-611307: VPN Client: Head end: IP_address
- %ASA-6-611308: VPN Client: Split DNS Policy installed: List of domains: string string
- %ASA-6-611309: VPN Client: Disconnecting from head end and uninstalling previously downloaded policy: Head End: IP_address
- %ASA-6-611310: VNP Client: XAUTH Succeeded: Peer: IP_address
- %ASA-6-611311: VNP Client: XAUTH Failed: Peer: IP_address
- %ASA-6-611312: VPN Client: Backup Server List: reason
- %ASA-6-611314: VPN Client: Load Balancing Cluster with Virtual IP: IP_address has redirected the to server IP_address
- %ASA-6-611315: VPN Client: Disconnecting from Load Balancing Cluster member IP_address
- %ASA-6-611316: VPN Client: Secure Unit Authentication Enabled
- %ASA-6-611317: VPN Client: Secure Unit Authentication Disabled
- %ASA-6-611318: VPN Client: User Authentication Enabled: Auth Server IP: IP_address Auth Server Port: port Idle Timeout: time
- %ASA-6-611319: VPN Client: User Authentication Disabled
- %ASA-6-611320: VPN Client: Device Pass Thru Enabled
- %ASA-6-611321: VPN Client: Device Pass Thru Disabled
- %ASA-6-611322: VPN Client: Extended XAUTH conversation initiated when SUA disabled
- %ASA-6-611323: VPN Client: Duplicate split nw entry
- %ASA-6-613001: Checksum Failure in database in area string Link State Id IP_address Old Checksum number New Checksum number
- %ASA-6-613002: interface interface_name has zero bandwidth
- %ASA-6-613003: IP_address netmask changed from area string to area string
- %ASA-6-613014: Base topology enabled on interface string attached to MTR compatible mode area string%ASA-6-613027: OSPF process number removed from interface interface_name
- %ASA-6-613028: Unrecognized virtual interface intetface_name.Treat it as loopback stub route
- %ASA-6-613041: OSPF-100 Areav string: LSA ID IP_address, Type number, Adv-rtr IP_address, LSA counter DoNotAge
- %ASA-6-613043:
- %ASA-6-613101: Checksum Failure in database in area %s\n Link State Id %i Old Checksum %#x New Checksum %#x\n
- %ASA-6-613102: interface %s has zero bandwidth
- %ASA-6-613103: %i%m changed from area %AREA_ID_STR to area %AREA_ID_STR
- %ASA-6-613104: Unrecognized virtual interface %IF_NAME.

按严重性级别列出的消息

- %ASA-6-614001: Split DNS: request patched from server: IP_address to server: IP_address
- %ASA-6-614002: Split DNS: reply from server: IP_address reverse patched back to original server: IP_address
- %ASA-6-615001: vlan number not available for firewall interface
- %ASA-6-615002: vlan number available for firewall interface
- %ASA-6-621001: Interface interface_name does not support multicast, not enabled
- %ASA-6-621002: Interface interface_name does not support multicast, not enabled
- %ASA-6-621003: The event queue size has exceeded number
- %ASA-6-621006: Mrib disconnected, (IP_address, IP_address) event cancelled
- %ASA-6-621007: Bad register from interface_name:IP_address to IP_address for (IP_address, IP_address)
- %ASA-6-622001: string tracked route network mask address, distance number, table string, on interface interface-name
- %ASA-6-622101: Starting regex table compilation for match_command; table entries = regex_num entries
- %ASA-6-622102: Completed regex table compilation for match_command; table size = num bytes
- %ASA-6-634001: DAP: User user, Addr ipaddr, Connection connection; The following DAP records were selected for this connection: DAP Record names
- %ASA-6-713128: Connection attempt to VCPIP redirected to VCA peer IP_address via load balancing
- %ASA-6-713145: Detected Hardware Client in network extension mode, adding static route for address: IP_address, mask: netmask
- %ASA-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address, mask: netmask
- %ASA-6-713172: Automatic NAT Detection Status: Remote end is|is not behind a NAT device This end is|is_not behind a NAT device
- %ASA-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host_name Address IP_address, Protocol protocol, Port port
- %ASA-6-713184: Client Type: Client_type Client Application Version: Application_version_string
- %ASA-6-713202: Duplicate IP_addr packet detected.
- %ASA-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask
- %ASA-6-713215: No match against Client Type and Version rules.Client: type version is/is not allowed by default
- %ASA-6-713219: Queuing KEY-ACQUIRE messages to be processed when P1 SA is complete.
- %ASA-6-713220: De-queuing KEY-ACQUIRE messages that were left pending.
- %ASA-6-713228: Assigned private IP address assigned_private_IP
- %ASA-6-713235: Attempt to send an IKE packet from standby unit.Dropping the packet!
- %ASA-6-713256: IP = peer-IP, Sending spoofed ISAKMP Aggressive Mode message 2 due to receipt of unknown tunnel group.Aborting connection.
- %ASA-6-713265: Adding static route for L2L peer coming in on a dynamic map. address: IP_address, mask: /prefix_len
- %ASA-6-713267: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address, mask: /prefix_len
- %ASA-6-713269: Detected Hardware Client in network extension mode, adding static route for address: IP_address, mask: /prefix_len

- %ASA-6-713271: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address, mask: /prefix_len
- %ASA-6-713905: Descriptive_event_string.
- %ASA-6-716001: Group group User user WebVPN session started.
- %ASA-6-716002: Group group User user WebVPN session terminated: reason.
- %ASA-6-716003: Group group User user WebVPN access GRANTED: url
- %ASA-6-716004: Group group User user WebVPN access DENIED to specified location: url
- %ASA-6-716005: Group group User user WebVPN ACL Parse Error: reason
- %ASA-6-716006: Group name User user WebVPN session terminated.Idle timeout.
- %ASA-6-716009: Group group User user WebVPN session not allowed.WebVPN ACL parse error.
- %ASA-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint_name.
- %ASA-6-716038: Authentication: successful, group = name user = user, Session Type: WebVPN
- %ASA-6-716039: Authentication: rejected, group = name user = user, Session Type: %s
- %ASA-6-716040: Reboot pending, new sessions disabled.Denied user login.
- %ASA-6-716041: access-list acl_ID action url url hit_cnt count
- %ASA-6-716042: access-list acl_ID action tcp source_interface/source_address (source_port) - dest_interface/dest_address(dest_port) hit-cnt count
- %ASA-6-716043 Group group-name, User user-name, IP IP_address: WebVPN Port Forwarding Java applet started.Created new hosts file mappings
- %ASA-6-716049: Group group-name User user-name IP IP_address Empty SVC ACL.
- %ASA-6-716050: Error adding to ACL: ace_command_line
- %ASA-6-716051: Group group-name User user-name IP IP_address Error adding dynamic ACL for user.
- %ASA-6-716055: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type succeeded
- %ASA-6-716058: Group group User user IP ip AnyConnect session lost connection.Waiting to resume.
- %ASA-6-716059: Group group User user IP ip AnyConnect session resumed.Connection from ip2
- %ASA-6-716060: Group group User user IP ip Terminated AnyConnect session in inactive state to accept a new connection.License limit reached.
- %ASA-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint_name.
- %ASA-6-717004: PKCS #12 export failed for trustpoint trustpoint_name.
- %ASA-6-717005: PKCS #12 export succeeded for trustpoint trustpoint_name.
- %ASA-6-717006: PKCS #12 import failed for trustpoint trustpoint_name.
- %ASA-6-717007: PKCS #12 import succeeded for trustpoint trustpoint_name.
- %ASA-6-717016: Removing expired CRL from the CRL cache.Issuer: issuer
- %ASA-6-717022: Certificate was successfully validated. certificate_identifiers
- %ASA-6-717028: Certificate chain was successfully validated additional info.
- %ASA-6-717033: OCSP response status - Successful.
- %ASA-6-717056: Attempting type revocation check from Src Interface:Src IP/Src Port to Dst IP/Dst Port using protocol
- %ASA-6-718003: Got unknown peer message message_number from IP_address, local version version_number, remote version version_number

按严重性级别列出的消息

- %ASA-6-718004: Got unknown internal message message_number
- %ASA-6-718013: Peer IP_address is not answering HELLO
- %ASA-6-718027: Received unexpected KEEPALIVE request from IP_address
- %ASA-6-718030: Received planned OOS from IP_address
- %ASA-6-718037: Master processed number_of_timeouts timeouts
- %ASA-6-718038: Slave processed number_of_timeouts timeouts
- %ASA-6-718039: Process dead peer IP_address
- %ASA-6-718040: Timed-out exchange ID exchange_ID not found
- %ASA-6-718051: Deleted secure tunnel to peer IP_address
- %ASA-6-719001: Email Proxy session could not be established: session limit of maximum_sessions has been reached.
- %ASA-6-719003: Email Proxy session pointer resources have been freed for source_address.
- %ASA-6-719004: Email Proxy session pointer has been successfully established for source_address.
- %ASA-6-719010: protocol Email Proxy feature is disabled on interface interface_name.
- %ASA-6-719011: Protocol Email Proxy feature is enabled on interface interface_name.
- %ASA-6-719012: Email Proxy server listening on port port for mail protocol protocol.
- %ASA-6-719013: Email Proxy server closing port port for mail protocol protocol.
- %ASA-6-719017: WebVPN user: vpnuser invalid dynamic ACL.
- %ASA-6-719018: WebVPN user: vpnuser ACL ID acl_ID not found
- %ASA-6-719019: WebVPN user: vpnuser authorization failed.
- %ASA-6-719020: WebVPN user vpnuser authorization completed successfully.
- %ASA-6-719021: WebVPN user: vpnuser is not checked against ACL.
- %ASA-6-719022: WebVPN user vpnuser has been authenticated.
- %ASA-6-719023: WebVPN user vpnuser has not been successfully authenticated.Access denied.
- %ASA-6-719024: Email Proxy piggyback auth fail: session = pointer user=vpnuser addr=source_address
- %ASA-6-719025: Email Proxy DNS name resolution failed for hostname.
- %ASA-6-719026: Email Proxy DNS name hostname resolved to IP_address.
- %ASA-6-720002: (VPN-unit) Starting VPN Stateful Failover Subsystem...
- %ASA-6-720003: (VPN-unit) Initialization of VPN Stateful Failover Component completed successfully
- %ASA-6-720004: (VPN-unit) VPN failover main thread started.
- %ASA-6-720005: (VPN-unit) VPN failover timer thread started.
- %ASA-6-720006: (VPN-unit) VPN failover sync thread started.
- %ASA-6-720010: (VPN-unit) VPN failover client is being disabled
- %ASA-6-720012: (VPN-unit) Failed to update IPSec failover runtime data on the standby unit.
- %ASA-6-722013: Group group User user-name IP IP_address SVC Message: type-num/INFO: message
- %ASA-6-720014: (VPN-unit) Phase 2 connection entry (msg_id=message_number, my cookie=mine, his cookie=his) contains no SA list.
- %ASA-6-720015: (VPN-unit) Cannot found Phase 1 SA for Phase 2 connection entry (msg_id=message_number, my cookie=mine, his cookie=his).
- %ASA-6-720023: (VPN-unit) HA status callback: Peer is not present.
- %ASA-6-720024: (VPN-unit) HA status callback: Control channel is status.

- %ASA-6-720025: (VPN-unit) HA status callback: Data channel is status.
- %ASA-6-720026: (VPN-unit) HA status callback: Current progression is being aborted.
- %ASA-6-720027: (VPN-unit) HA status callback: My state state.
- %ASA-6-720028: (VPN-unit) HA status callback: Peer state state.
- %ASA-6-720029: (VPN-unit) HA status callback: Start VPN bulk sync state.
- %ASA-6-720030: (VPN-unit) HA status callback: Stop bulk sync state.
- %ASA-6-720032: (VPN-unit) HA status callback: id=ID, seq=sequence_#, grp=group, event=event, op=operand, my=my_state, peer=peer_state.
- %ASA-6-720037: (VPN-unit) HA progression callback: id=id,seq=sequence_number,grp=group,event=event,op=operand, my=my_state,peer=peer_state.
- %ASA-6-720039: (VPN-unit) VPN failover client is transitioning to active state
- %ASA-6-720040: (VPN-unit) VPN failover client is transitioning to standby state.
- %ASA-6-720045: (VPN-unit) Start bulk syncing of state information on standby unit.
- %ASA-6-720046: (VPN-unit) End bulk syncing of state information on standby unit
- %ASA-6-720056: (VPN-unit) VPN Stateful failover Message Thread is being disabled.
- %ASA-6-720057: (VPN-unit) VPN Stateful failover Message Thread is enabled.
- %ASA-6-720058: (VPN-unit) VPN Stateful failover Timer Thread is disabled.
- %ASA-6-720059: (VPN-unit) VPN Stateful failover Timer Thread is enabled.
- %ASA-6-720060: (VPN-unit) VPN Stateful failover Sync Thread is disabled.
- %ASA-6-720061: (VPN-unit) VPN Stateful failover Sync Thread is enabled.
- %ASA-6-720062: (VPN-unit) Active unit started bulk sync of state information to standby unit.
- %ASA-6-720063: (VPN-unit) Active unit completed bulk sync of state information to standby.
- %ASA-6-721001: (device) WebVPN Failover SubSystem started successfully.(device) either WebVPN-primary or WebVPN-secondary.
- %ASA-6-721002: (device) HA status change: event event, my state my_state, peer state peer.
- %ASA-6-721003: (device) HA progression change: event event, my state my_state, peer state peer.
- %ASA-6-721004: (device) Create access list list_name on standby unit.
- %ASA-6-721005: (device) Fail to create access list list_name on standby unit.
- %ASA-6-721006: (device) Update access list list_name on standby unit.
- %ASA-6-721008: (device) Delete access list list_name on standby unit.
- %ASA-6-721009: (device) Fail to delete access list list_name on standby unit.
- %ASA-6-721010: (device) Add access list rule list_name, line line_no on standby unit.
- %ASA-6-721012: (device) Enable APCF XML file file_name on the standby unit.
- %ASA-6-721014: (device) Disable APCF XML file file_name on the standby unit.
- %ASA-6-721016: (device) WebVPN session for client user user_name, IP ip_address has been created.
- %ASA-6-721018: (device) WebVPN session for client user user_name, IP ip_address has been deleted.
- %ASA-6-722013: Group group User user-name IP IP_address SVC Message: type-num/INFO: message
- %ASA-6-722014: Group group User user-name IP IP_address SVC Message: type-num/INFO: message
- %ASA-6-722051: Group group-policy User username IP public-ip Address assigned-ip assigned to session
- %ASA-6-722053: Group g User u IP ip Unknown client user-agent connection.

按严重性级别列出的消息

- %ASA-6-722055: Group group-policy User username IP public-ip Client Type: user-agent
- %ASA-6-723001: Group group-name, User user-name, IP IP_address: WebVPN Citrix ICA connection connection is up.
- %ASA-6-723002: Group group-name, User user-name, IP IP_address: WebVPN Citrix ICA connection connection is down.
- %ASA-6-725001: Starting SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port for protocol session.
- %ASA-6-725002: Device completed SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port for protocol-version session
- %ASA-6-725003: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port request to resume previous session.
- %ASA-6-725004: Device requesting certificate from SSL peer-type interface:src-ip/src-port to dst-ip/dst-port for authentication.
- %ASA-6-725005: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port requesting our device certificate for authentication.
- %ASA-6-725006: Device failed SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port
- %ASA-6-725007: SSL session with peer-type interface:src-ip/src-port to dst-ip/dst-port terminated.
- %ASA-6-726001: Inspected im_protocol im_service Session between Client im_client_1 and im_client_2 Packet flow from src_ifc:/sip/sport to dest_ifc:/dip/dport Action: action Matched Class class_map_id class_map_name
- %ASA-6-725016: Device selects trust-point <trustpoint> for peer-type interface:src-ip/src-port to dst-ip/dst-port
- %ASA-6-734001: DAP: User user, Addr ipaddr, Connection connection: The following DAP records were selected for this connection: DAP record names
- %ASA-6-737005: IPAA: DHCP configured, request succeeded for tunnel-group 'tunnel-group'
- %ASA-6-737006: IPAA: Local pool request succeeded for tunnel-group 'tunnel-group'
- %ASA-6-737009: IPAA: AAA assigned address ip-address, request failed
- %ASA-6-737010: IPAA: AAA assigned address ip-address, request succeeded
- %ASA-6-737014: IPAA: Freeing AAA address ip-address
- %ASA-6-737015: IPAA: Freeing DHCP address ip-address
- %ASA-6-737016: IPAA: Freeing local pool address ip-address
- %ASA-6-737017: IPAA: DHCP request attempt num succeeded
- %ASA-6-737026: IPAA: Client assigned ip-address from local pool
- %ASA-6-737029: IPAA: Adding ip-address to standby: succeeded
- %ASA-6-737031: IPAA: Removing %m from standby: succeeded
- %ASA-6-737036: IPAA: Session=<session>, Client assigned <address> from DHCP
- %ASA-6-741000: Coredump filesystem image created on variable 1 -size variable 2 MB
- %ASA-6-741001: Coredump filesystem image on variable 1 - resized from variable 2 MB to variable 3 MB
- %ASA-6-741002: Coredump log and filesystem contents cleared on variable 1
- %ASA-6-741003: Coredump filesystem and its contents removed on variable 1
- %ASA-6-741004: Coredump configuration reset to default values
- %ASA-6-747004: Clustering: state machine changed from state state-name to state-name.

- %ASA-6-748008: [CPU load *percentage* | memory load *percentage*] of module *slot_number* in chassis *chassis_number* (*member-name*) exceeds overflow protection threshold [CPU *percentage* | memory *percentage*].System may be oversubscribed on member failure.
- %ASA-6-748009: [CPU load percentage | memory load percentage] of chassis chassis_number exceeds overflow protection threshold [CPU percentage | memory percentage}.System may be oversubscribed on chassis failure.
- %ASA-6-803001: Flow offloaded: connection conn_id outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol
- %ASA-6-803002: Flow is no longer offloaded: connection conn_id outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol
- %ASA-6-751023: Local a:p Remote: a:p Username:n Unknown client connection
- %ASA-6-751026: Local: localIP:port Remote: remoteIP:port Username: username/group IKEv2 Client OS: client-os Client: client-name client-version
- %ASA-6-767001: Inspect-name: Dropping an unsupported IPv6/IP46/IP64 packet from interface:IP Addr to interface:IP Addr (fail-close)
- %ASA-6-772005: REAUTH: user username passed authentication
- %ASA-6-778001: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name:(IP-address/port) to ifc-name:(IP-address/port).
- %ASA-6-778002: VXLAN: There is no VNI interface for segment-id segment-id.
- %ASA-6-778003: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name:(IP-address/port) to ifc-name:(IP-address/port) in FP.
- %ASA-6-778004: VXLAN: Invalid VXLAN header for protocol from ifc-name:(IP-address/port) to ifc-name:(IP-address/port) in FP.
- %ASA-6-778005: VXLAN: Packet with VXLAN segment-id segment-id from ifc-name is denied by FP L2 check.
- %ASA-6-778006: VXLAN: Invalid VXLAN UDP checksum from ifc-name:(IP-address/port) to ifc-name:(IP-address/port) in FP.
- %ASA-6-778007: VXLAN: Packet from ifc-name:IP-address/port to IP-address/port was discarded due to invalid NVE peer.
- %ASA-6-779001: STS: Out-tag lookup failed for in-tag segment-id of protocol from ifc-name:IP-address/port to IP-address/port.
- %ASA-6-779002: STS: STS and NAT locate different egress interface for segment-id segment-id, protocol from ifc-name:IP-address/port to IP-address/port
- %ASA-6-802005: IP ip_address Received MDM request details.
- %ASA-6-803001:Bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2
- %ASA-6-803002: No protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2
- %ASA-6-803003: User disabled bypass manually on GigabitEthernet 1/1-1/2
- %ASA-6-804001: Interface GigabitEthernet1/3 1000BaseSX SFP has been inserted
- %ASA-6-804002: Interface GigabitEthernet1/3 SFP has been removed
- %ASA-6-805001: Flow offloaded: connection conn_id outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol
- %ASA-6-805002: Flow is no longer offloaded: connection conn_id outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol

- %ASA-6-805003: Flow could not be offloaded: connection <conn_id> <outside_ifc>:<outside_addr>/<outside_port> (<mapped_addr>/<mapped_port>) < inside_ifc>:<inside_addr>/<inside_port> (<mapped_addr>/<mapped_port>) <Protocol>
- %ASA-6-8300001: VPN session redistribution <variable 1>
- %ASA-6-8300002: Moved <variable 1> sessions to <variable 2>
- %ASA-6-8300004: <variable 1> request to move <variable 2> sessions from <variable 3> to <variable 4>

严重性级别为 7 的调试消息

以下调试消息的严重性级别为 7：

- %ASA-7-111009: User user executed cmd:string
- %ASA-7-113028: Extraction of username from VPN client certificate has string.[Request num]
- %ASA-7-199019: syslog
- %ASA-7-333004: EAP-SQ response invalid - context:EAP-context
- %ASA-7-333005: EAP-SQ response contains invalid TLV(s) - context:EAP-context
- %ASA-7-333006: EAP-SQ response with missing TLV(s) - context:EAP-context
- %ASA-7-333007: EAP-SQ response TLV has invalid length - context:EAP-context
- %ASA-7-333008: EAP-SQ response has invalid nonce TLV - context:EAP-context
- %ASA-7-609001: Built local-host zone_name/*: ip_address
- %ASA-7-609002: Teardown local-host zone_name/*: ip_address duration time
- %ASA-7-701001: alloc_user() out of Tcp_user objects
- %ASA-7-701002: alloc_user() out of Tcp_proxy objects
- %ASA-7-702307: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) is rekeying due to data rollover.
- %ASA-7-703001: H.225 message received from interface_name:IP_address/port to interface_name:IP_address/port is using an unsupported version number
- %ASA-7-703002: Received H.225 Release Complete with newConnectionNeeded for interface_name:IP_address to interface_name:IP_address/port
- %ASA-7-703008: Allowing early-message: %s before SETUP from %s:%Q/%d to %s:%Q/%d\n
- %ASA-7-709001: FO replication failed: cmd=command returned=code
- %ASA-7-709002: FO unreplicable: cmd=command
- %ASA-7-710001: TCP access requested from source_address/source_port to interface_name:dest_address/service
- %ASA-7-710002: {TCP|UDP} access permitted from source_address/source_port to interface_name:dest_address/service
- %ASA-7-710004: TCP connection limit exceeded from Src_ip/Src_port to In_name:Dest_ip/Dest_port (current connections/connection limit = Curr_conn/Conn_lmt)
- %ASA-7-710005: {TCP|UDP} request discarded from source_address/source_port to interface_name:dest_address/service
- %ASA-7-710006: protocol request discarded from source_address to interface_name:dest_address
- %ASA-7-710007: NAT-T keepalive received from 86.1.161.1/1028 to outside:86:1.129.1/4500

- %ASA-7-711001: debug_trace_msg
- %ASA-7-711003: Unknown/Invalid interface identifier(vpifnum) detected.
- %ASA-7-711006: CPU profiling has started for n-samples samples.Reason: reason-string.
- %ASA-7-713024: Group group IP ip Received local Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %ASA-7-713025: Received remote Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %ASA-7-713028: Received local Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %ASA-7-713029: Received remote Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %ASA-7-713034: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %ASA-7-713035: Group group IP ip Received remote IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %ASA-7-713039: Send failure: Bytes (number), Peer: IP_address
- %ASA-7-713040: Could not find connection entry and can not encrypt: msgid message_number
- %ASA-7-713052: User (user) authenticated.
- %ASA-7-713066: IKE Remote Peer configured for SA: SA_name
- %ASA-7-713094: Cert validation failure: handle invalid for Main/Aggressive Mode Initiator/Responder!
- %ASA-7-713099: Tunnel Rejected: Received NONCE length number is out of range!
- %ASA-7-713103: Invalid (NULL) secret key detected while computing hash
- %ASA-7-713104: Attempt to get Phase 1 ID data failed while hash computation
- %ASA-7-713113: Deleting IKE SA with associated IPSec connection entries.IKE peer: IP_address, SA address: internal_SA_address, tunnel count: count
- %ASA-7-713114: Connection entry (conn entry internal address) points to IKE SA (SA_internal_address) for peer IP_address, but cookies don't match
- %ASA-7-713117: Received Invalid SPI notify (SPI SPI_Value)!
- %ASA-7-713121: Keep-alive type for this connection: keepalive_type
- %ASA-7-713143: Processing firewall record.Vendor: vendor(id), Product: product(id), Caps: capability_value, Version Number: version_number, Version String: version_text
- %ASA-7-713160: Remote user (session Id - id) has been granted access by the Firewall Server
- %ASA-7-713164: The Firewall Server has requested a list of active user sessions
- %ASA-7-713169: IKE Received delete for rekeyed SA IKE peer: IP_address, SA address: internal_SA_address, tunnelCnt: tunnel_count
- %ASA-7-713170: Group group IP ip IKE Received delete for rekeyed centry IKE peer: IP_address, centry address: internal_address, msgid: id
- %ASA-7-713171: NAT-Traversal sending NAT-Original-Address payload
- %ASA-7-713187: Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy IKE peer address: IP_address, Remote peer address: IP_address
- %ASA-7-713190: Got bad refCnt (ref_count_value) assigning IP_address (IP_address)
- %ASA-7-713204: Adding static route for client address: IP_address
- %ASA-7-713221: Static Crypto Map check, checking map = crypto_map_tag, seq = seq_number...

按严重性级别列出的消息

- %ASA-7-713222: Group group Username username IP ip Static Crypto Map check, map = crypto_map_tag, seq = seq_number, ACL does not match proxy IDs src:source_address dst:dest_address
- %ASA-7-713223: Static Crypto Map check, map = crypto_map_tag, seq = seq_number, no ACL configured
- %ASA-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!
- %ASA-7-713225: [IKEv1], Static Crypto Map check, map map_name, seq = sequence_number is a successful match
- %ASA-7-713233: (VPN-unit) Remote network (remote network) validated for network extension mode.
- %ASA-7-713234: (VPN-unit) Remote network (remote network) from network extension mode client mismatches AAA configuration (aaa network).
- %ASA-7-713236: IKE_DECODE tx/rx Message (msgid=msgid) with payloads:payload1 (payload1_len) + payload2 (payload2_len)...total length: tlen
- %ASA-7-713263: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask /prefix_len, Protocol protocol, Port port
- %ASA-7-713264: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask /prefix_len, Protocol protocol, Port port {“Received remote IP Proxy Subnet data in ID Payload: Address %a, Mask/%d, Protocol %u, Port %u”}
- %ASA-7-713273: Deleting static route for client address: IP_Address IP_Address address of client whose route is being removed
- %ASA-7-713906: Descriptive_event_string.
- %ASA-7-714001: description_of_event_or_packet
- %ASA-7-714002: IKE Initiator starting QM: msg id = message_number
- %ASA-7-714003: IKE Responder starting QM: msg id = message_number
- %ASA-7-714004: IKE Initiator sending 1st QM pkt: msg id = message_number
- %ASA-7-714005: IKE Responder sending 2nd QM pkt: msg id = message_number
- %ASA-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message_number
- %ASA-7-714007: IKE Initiator sending Initial Contact
- %ASA-7-714011: Description of received ID values
- %ASA-7-715001: Descriptive statement
- %ASA-7-715004: subroutine name() Q Send failure: RetCode (return_code)
- %ASA-7-715005: subroutine name() Bad message code: Code (message_code)
- %ASA-7-715006: IKE got SPI from key engine: SPI = SPI_value
- %ASA-7-715007: IKE got a KEY_ADD msg for SA: SPI = SPI_value
- %ASA-7-715008: Could not delete SA SA_address, refCnt = number, caller = calling_subroutine_address
- %ASA-7-715009: IKE Deleting SA: Remote Proxy IP_address, Local Proxy IP_address
- %ASA-7-715013: Tunnel negotiation in progress for destination IP_address, discarding data
- %ASA-7-715019: Group group Username username IP ip IKEGetUserAttributes: Attribute name = name
- %ASA-7-715020: construct_cfg_set: Attribute name = name
- %ASA-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
- %ASA-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
- %ASA-7-715027: IPSec SA Proposal # chosen_proposal, Transform # chosen_transform acceptable Matches global IPSec SA entry # crypto_map_index

- %ASA-7-715028: IKE SA Proposal # 1, Transform # chosen_transform acceptable Matches global IKE entry # crypto_map_index
- %ASA-7-715033: Processing CONNECTED notify (MsgId message_number)
- %ASA-7-715034: action IOS keep alive payload: proposal=time 1/time 2 sec.
- %ASA-7-715035: Starting IOS keepalive monitor: seconds sec.
- %ASA-7-715036: Sending keep-alive of type notify_type (seq number number)
- %ASA-7-715037: Unknown IOS Vendor ID version: major.minor.variance
- %ASA-7-715038: action Spoofing_information Vendor ID payload (version: major.minor.variance, capabilities: value)
- %ASA-7-715039: Unexpected cleanup of tunnel table entry during SA delete.
- %ASA-7-715040: Deleting active auth handle during SA deletion: handle = internal_authentication_handle
- %ASA-7-715041: Received keep-alive of type keepalive_type, not the negotiated type
- %ASA-7-715042: IKE received response of type failure_type to a request from the IP_address utility
- %ASA-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability
- %ASA-7-715045: ERROR: malformed Keepalive payload
- %ASA-7-715046: Group = groupname, Username = username, IP = IP_address, constructing payload_description payload
- %ASA-7-715047: processing payload_description payload
- %ASA-7-715048: Send VID_type VID
- %ASA-7-715049: Received VID_type VID
- %ASA-7-715050: Claims to be IOS but failed authentication
- %ASA-7-715051: Received unexpected TLV type TLV_type while processing FWTYPE ModeCfg Reply
- %ASA-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centries
- %ASA-7-715053: MODE_CFG: Received request for attribute_info!
- %ASA-7-715054: MODE_CFG: Received attribute_name reply: value
- %ASA-7-715055: Send attribute_name
- %ASA-7-715056: Client is configured for TCP_transparency
- %ASA-7-715057: Auto-detected a NAT device with NAT-Traversal.Ignoring IPSec-over-UDP configuration.
- %ASA-7-715058: NAT-Discovery payloads missing.Aborting NAT-Traversal.
- %ASA-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal
- %ASA-7-715060: Dropped received IKE fragment.Reason: reason
- %ASA-7-715061: Rcv'd fragment from a new fragmentation set.Deleting any old fragments.
- %ASA-7-715062: Error assembling fragments! Fragment numbers are non-continuous.
- %ASA-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!
- %ASA-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: true/false Aggressive Mode: true/false
- %ASA-7-715065: IKE state_machine subtype FSM error history (struct data_structure_address) state, event: state/event pairs
- %ASA-7-715066: Can't load an IPSec SA! The corresponding IKE SA contains an invalid logical ID.

按严重性级别列出的消息

- %ASA-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
- %ASA-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
- %ASA-7-715068: QM IsRekeyed: duplicate sa found by address, deleting old sa
- %ASA-7-715069: Invalid ESP SPI size of SPI_size
- %ASA-7-715070: Invalid IPComp SPI size of SPI_size
- %ASA-7-715071: AH proposal not supported
- %ASA-7-715072: Received proposal with unknown protocol ID protocol_ID
- %ASA-7-715074: Could not retrieve authentication attributes for peer IP_address
- %ASA-7-715075: Group = group_name, IP = IP_address Received keep-alive of type message_type (seq number number)
- %ASA-7-715076: Computing hash for ISAKMP
- %ASA-7-715077: Pitcher: msg string, spi spi
- %ASA-7-715080: VPN: Starting P2 rekey timer: 28800 seconds.
- %ASA-7-716008: WebVPN ACL: action
- %ASA-7-716010: Group group User user Browse network.
- %ASA-7-716011: Group group User user Browse domain domain.
- %ASA-7-716012: Group group User user Browse directory directory.
- %ASA-7-716013: Group group User user Close file filename.
- %ASA-7-716014: Group group User user View file filename.
- %ASA-7-716015: Group group User user Remove file filename.
- %ASA-7-716016: Group group User user Rename file old_filename to new_filename.
- %ASA-7-716017: Group group User user Modify file filename.
- %ASA-7-716018: Group group User user Create file filename.
- %ASA-7-716019: Group group User user Create directory directory.
- %ASA-7-716020: Group group User user Remove directory directory.
- %ASA-7-716021: File access DENIED, filename.
- %ASA-7-716024: Group name User user Unable to browse the network.Error: description
- %ASA-7-716025: Group name User user Unable to browse domain domain.Error: description
- %ASA-7-716026: Group name User user Unable to browse directory directory.Error: description
- %ASA-7-716027: Group name User user Unable to view file filename.Error: description
- %ASA-7-716028: Group name User user Unable to remove file filename.Error: description
- %ASA-7-716029: Group name User user Unable to rename file filename.Error: description
- %ASA-7-716030: Group name User user Unable to modify file filename.Error: description
- %ASA-7-716031: Group name User user Unable to create file filename.Error: description
- %ASA-7-716032: Group name User user Unable to create folder folder.Error: description
- %ASA-7-716033: Group name User user Unable to remove folder folder.Error: description
- %ASA-7-716034: Group name User user Unable to write to file filename.
- %ASA-7-716035: Group name User user Unable to read file filename.
- %ASA-7-716036: Group name User user File Access: User user logged into the server server.
- %ASA-7-716037: Group name User user File Access: User user failed to login into the server server.
- %ASA-7-716603: Received size-recv KB Hostscan data from IP src-ip.

- %ASA-7-717024: Checking CRL from trustpoint: trustpoint name for purpose
- %ASA-7-717025: Validating certificate chain containing number of certs certificate(s).
- %ASA-7-717029: Identified client certificate within certificate chain. serial number: serial_number, subject name: subject_name.
- %ASA-7-717030: Found a suitable trustpoint trustpoint name to validate certificate.
- %ASA-7-717034: No-check extension found in certificate.OCSP check bypassed.
- ASA-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with certificate_identifier.
- %ASA-7-717038: Tunnel group match found.Tunnel Group: tunnel_group_name, Peer certificate: certificate_identifier.
- %ASA-7-718001: Internal interprocess communication queue send failure: code error_code
- %ASA-7-718017: Got timeout for unknown peer IP_address msg type message_type
- %ASA-7-718018: Send KEEPALIVE request failure to IP_address
- %ASA-7-718019: Sent KEEPALIVE request to IP_address
- %ASA-7-718020: Send KEEPALIVE response failure to IP_address
- %ASA-7-718021: Sent KEEPALIVE response to IP_address
- %ASA-7-718022: Received KEEPALIVE request from IP_address
- %ASA-7-718023: Received KEEPALIVE response from IP_address
- %ASA-7-718025: Sent CFG UPDATE to IP_address
- %ASA-7-718026: Received CFG UPDATE from IP_address
- %ASA-7-718029: Sent OOS indicator to IP_address
- %ASA-7-718034: Sent TOPOLOGY indicator to IP_address
- %ASA-7-718035: Received TOPOLOGY indicator from IP_address
- %ASA-7-718036: Process timeout for req-type type_value, exid exchange_ID, peer IP_address
- %ASA-7-718041: Timeout [msgType=type] processed with no callback
- %ASA-7-718046: Create group policy policy_name
- %ASA-7-718047: Fail to create group policy policy_name
- %ASA-7-718049: Created secure tunnel to peer IP_address
- %ASA-7-718056: Deleted Master peer, IP IP_address
- %ASA-7-718058: State machine return code: action_routine, return_code
- %ASA-7-718059: State machine function trace: state=state_name, event=event_name, func=action_routine
- %ASA-7-718088: Possible VPN LB misconfiguration.Offending device MAC MAC_address.
- %ASA-7-719005: FSM NAME has been created using protocol for session pointer from source_address.
- %ASA-7-719006: Email Proxy session pointer has timed out for source_address because of network congestion.
- %ASA-7-719007: Email Proxy session pointer cannot be found for source_address.
- %ASA-7-719009: Email Proxy service is starting.
- %ASA-7-719015: Parsed emailproxy session pointer from source_address username: mailuser = mail_user, vpnuser = VPN_user, mailserver = server
- %ASA-7-719016: Parsed emailproxy session pointer from source_address password: mailpass = ******, vpnpass= ******
- %ASA-7-720031: (VPN-unit) HA status callback: Invalid event received. event=event_ID.

按严重性级别列出的消息

- %ASA-7-720034: (VPN-unit) Invalid type (type) for message handler.
- %ASA-7-720041: (VPN-unit) Sending type message id to standby unit
- %ASA-7-720042: (VPN-unit) Receiving type message id from active unit
- %ASA-7-720048: (VPN-unit) FSM action trace begin: state=state, last event=event, func=function.
- %ASA-7-720049: (VPN-unit) FSM action trace end: state=state, last event=event, return=return, func=function.
- %ASA-7-720050: (VPN-unit) Failed to remove timer.ID = id.
- %ASA-7-722029: Group group User user-name IP IP_address SVC Session Termination: Conns: connections, DPD Conns: DPD_conns, Comp resets: compression_resets, Dcmp resets: decompression_resets
- %ASA-7-722030: Group group User user-name IP IP_address SVC Session Termination: In: data_bytes (+ctrl_bytes) bytes, data_pkts (+ctrl_pkts) packets, drop_pkts drops
- %ASA-7-722031: Group group User user-name IP IP_address SVC Session Termination: Out: data_bytes (+ctrl_bytes) bytes, data_pkts (+ctrl_pkts) packets, drop_pkts drops.
- %ASA-7-723003: No memory for WebVPN Citrix ICA connection connection.
- %ASA-7-723004: WebVPN Citrix encountered bad flow control flow.
- %ASA-7-723005: No channel to set up WebVPN Citrix ICA connection.
- %ASA-7-723006: WebVPN Citrix SOCKS errors.
- %ASA-7-723007: WebVPN Citrix ICA connection connection list is broken.
- %ASA-7-723008: WebVPN Citrix ICA SOCKS Server server is invalid.
- %ASA-7-723009: Group group-name, User user-name, IP IP_address: WebVPN Citrix received data on invalid connection connection.
- %ASA-7-723010: Group group-name, User user-name, IP IP_address: WebVPN Citrix received closing channel channel for invalid connection connection.
- %ASA-7-723011: Group group-name, User user-name, IP IP_address: WebVPN Citrix receives bad SOCKS socks message length msg-length.Expected length is exp-msg-length.
- %ASA-7-723012: Group group-name, User user-name, IP IP_address: WebVPN Citrix received bad SOCKS socks message format.
- %ASA-7-723013: WebVPN Citrix encountered invalid connection connection during periodic timeout.
- %ASA-7-723014: Group group-name, User user-name, IP IP_address: WebVPN Citrix TCP connection connection to server server on channel channel initiated.
- %ASA-7-725008: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port proposes the following n cipher(s).
- %ASA-7-725009: Device proposes the following n cipher(s) peer-type interface:src-ip/src-port to dst-ip/dst-port.
- %ASA-7-725010: Device supports the following n cipher(s).
- %ASA-7-725011: Cipher[order]: cipher_name
- %ASA-7-725012: Device chooses cipher cipher for the SSL session with peer-type interface:src-ip/src-port to dst-ip/dst-port.
- %ASA-7-725013: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port chooses cipher cipher
- %ASA-7-725014: SSL lib error.Function: function Reason: reason
- %ASA-7-725017: No certificates received during the handshake with %s %s:%B/%d to %B/%d for %s session

- %ASA-7-730002: Group groupname, User username, IP ipaddr: VLAN MAPPING to VLAN vlanid failed
- %ASA-7-734003: DAP: User name, Addr ipaddr: Session Attribute: attr name/value
- %ASA-7-737001: IPAA: Received message ‘message-type’
- %ASA-7-737035: IPAA: Session=<session>, '<message type>' message queued
- %ASA-7-747005: Clustering: State machine notify event event-name (event-id, ptr-in-hex, ptr-in-hex)
- %ASA-7-747006: Clustering: State machine is at state state-name
- %ASA-7-751003: Local: localIP:port Remote:remoteIP:port Username: username/group Need to send a DPD message to peer
- %ASA-7-752002: Tunnel Manager Removed entry.Map Tag = mapTag.Map Sequence Number = mapSeq.
- %ASA-7-752008: Duplicate entry already in Tunnel Manager.
- %ASA-7-785001: Clustering: Ownership for existing flow from <in_interface>:<src_ip_addr>/<src_port> to <out_interface>:<dest_ip_addr>/<dest_port> moved from unit <old-owner-unit-id> at site <old-site-id> to <new-owner-unit-id> at site <old-site-id> due to <reason>.

系统日志消息中使用的变量

系统日志消息通常包含变量。下表列出了本指南中用于描述系统日志消息的大多数变量，而不包含只出现在一个系统日志消息中的某些变量。

系统日志消息中的变量字段

变量	说明
acl_ID	ACL 名称。
bytes	字节数。
code	根据生成的系统日志消息，系统日志消息返回的十进制数，表示错误的原因或来源。
command	命令名称。
command_modifier	**command_modifier** 可以是以下任一个字符串： • cmd（此字符串表示该命令没有修饰符） • clear • no • show
connections	连接数。

按严重性级别列出的消息

变量	说明
connection_type	连接类型： • SIGNALLING UDP • SIGNALLING TCP • SUBSCRIBE UDP • SUBSCRIBE TCP • 通过 UDP • 路由 • RTP • RTCP
dec	十进制数。
dest_address	数据包的目的地址。
dest_port	目的端口号。
device	内存存储设备。例如，软盘、内部闪存、TFTP、故障切换备用设备或控制台终端。
econns	初期连接的数量。
elimit	**static** 或 **nat** 命令中指定的初期连接数。
filename	ASAimage、ASDM 文件或配置类型的文件名。
ftp-server	外部 FTP 服务器名称或 IP 地址。
gateway_address	网络网关 IP 地址。
global_address	全局 IP 地址，较低安全级别接口上的地址。
global_port	全局端口号。
hex	十六进制数。
inside_address	内部（或本地）IP 地址，较高安全级别接口上的地址。
inside_port	内部端口号。
interface_name	接口的名称。
IP_address	*n n n n* 形式的 IP 地址，其中 *n* 是 1 到 255 之间的整数。
MAC_address	MAC 地址。
mapped_address	转换的 IP 地址。
mapped_port	转换的端口号。

变量	说明
message_class	与 ASA 的功能区域关联的系统日志消息类别。
message_list	您创建的文件的名称，其中包含系统日志消息 ID 号、类或严重性级别的列表。
message_number	系统日志消息 ID。
nconns	静态或转换表允许的连接数。
netmask	子网掩码。
number	数字。确切的形式取决于系统日志消息。
octal	八进制数。
outside_address	外部 IP 地址，系统日志服务器的地址，该服务器通常位于网络中外部路由器之外的较低安全级别接口上。
outside_port	外部端口号。
port	TCP 或 UDP 端口号。
privilege_level	用户权限级别。
protocol	数据包协议，例如 ICMP、TCP 或 UDP。
real_address	NAT 地址转换之前的实际 IP 地址。
real_port	NAT 地址转换之前的实际端口号。
reason	描述系统日志消息原因的文本字符串。
service	数据包指定的服务，例如 SNMP 或 Telnet 服务。
severity_level	系统日志消息的严重性级别。
source_address	数据包的源地址。
source_port	源端口号。
string	文本字符串（例如用户名）。
tcp_flags	TCP 报头中的标志，例如： • ACK • FIN • PSH • RST • SYN • URG

按严重性级别列出的消息

变量	说明
time	格式为 *hh mm ss* 的持续时间
url	URL。
user	用户名。

索 引

数字

A

B

C

D

E

F

G

R

S

W

X

Y

Z