Anonymous Reporting 和 Smart Call Home

本章介绍如何配置 Anonymous Reporting 和 Smart Call Home 服务。

关于 Anonymous Reporting

可以通过启用 Anonymous Reporting 服务来帮助改进思科 ASA 平台，此服务使思科能够安全地接收来自设备的最少量错误和运行状况信息。启用此功能后，客户身份将保持匿名，并且不会发送任何识别信息。

启用 Anonymous Reporting 将会创建信任点并安装证书。ASA 需要 CA 证书以验证 Smart Call Home Web 服务器上存在的服务器证书并建立 HTTPS 会话，以使 ASA 能够安全地发送消息。思科将导入软件中预定义的证书。如果决定启用 Anonymous Reporting，则 ASA 上将会安装一个证书，其硬编码的信任点名称为 _SmartCallHome_ServerCA。当启用 Anonymous Reporting 时，系统将会创建此信任点，安装相应的证书，并且您将接收到有关此操作的消息。然后，该证书将出现在配置中。

如果启用 Anonymous Reporting 时相应的证书已存在于配置中，则不会创建信任点，并且不会安装任何证书。

注释 启用 Anonymous Reporting 即表示您同意将指定的数据传输至思科或代表思科运营的供应商（包括美国以外的国家/地区）。思科将保护所有客户的隐私。有关思科对个人信息处理方式的信息，请参阅思科隐私权生命，网址如下： http://www.cisco.com/web/siteassets/legal/privacy.html

ASA 在后台配置 Smart Call Home 匿名报告时，ASA 会自动创建一个包含颁发 Call Home 服务器证书的 CA 的证书的信任点。现在，如果服务器的颁发层次结构发生变化，ASA 支持对证书进行验证，而无需客户来进行证书层次结构更改。您也可以自动导入信任池证书，以便 ASA 可以在不进行任何人工干预的情况下更新证书层次结构。

升级 ASA 9.14(2.14) 时，信任点配置会自动从 CallHome_ServerCA 更改为 CallHome_ServerCA2。

DNS 要求

必须正确配置 DNS 服务器，ASA 才能访问 Cisco Smart Call Home 服务器并向思科发送消息。由于 ASA 可能位于专用网络中，而未接入公用网络，因此思科将验证 DNS 配置，并在必要时通过执行以下任务来配置 DNS：

1. 为所有已配置的 DNS 服务器执行 DNS 查找。
2. 通过在最高安全级别的接口上发送 DHCPINFORM 消息，从 DHCP 服务器获取 DNS 服务器。
3. 使用思科 DNS 服务器进行查找。
4. 将静态 IP 地址随机用于 tools.cisco.com。

执行这些任务并不会更改当前配置。（例如，从 DHCP 获取的 DNS 服务器不会添加到配置中。）

如果未配置任何 DNS 服务器，并且 ASA 无法访问 Cisco Smart Call Home 服务器，则对于发送的每条 Smart Call Home 消息，思科都将生成一条严重性级别为“警告”的系统日志消息，以提醒您正确配置 DNS。

有关系统日志消息的信息，请参阅系统日志消息指南。

关于 Smart Call Home

对 Smart Call Home 服务进行全面配置后，此服务可以检测到站点中的问题，并且通常在您知道这些问题存在之前，向思科报告这些问题或者通过用户定义的其他渠道进行报告（例如通过邮件报告或者直接向您报告）。根据这些问题的严重性，思科将通过提供以下服务，对系统配置问题、产品寿命终止声明以及安全公告问题等等作出回应：

- 通过持续进行监控、发出实时的主动警报以及进行详细诊断，迅速确定问题。
- 通过 Smart Call Home 通知使您知晓潜在的问题，在这些通知中，已提交服务请求，并随附了所有诊断数据。
- 自动直接联系思科 TAC 专家，更迅速地解决紧急问题。
- 缩短故障排除时间，从而更高效地利用员工资源。

- 自动生成发往思科 TAC 的服务请求（如果签订了服务合同），这些请求将发送给适当的支持团队，该支持团队将提供可以加快解决问题的详细诊断信息。

可以通过 Smart Call Home 门户快速访问使您能够执行下列活动的必需信息：

- 在一个位置查看所有 Smart Call Home 消息、诊断信息和建议。
- 检查服务请求状态。
- 查看所有支持 Smart Call Home 的设备的最新资产和配置信息。

订用警报组

警报组是 ASA 上支持的 Smart Call Home 警报的预定义子集。各种类型的 Smart Call Home 警报根据其类型分组到不同的警报组中。每个警报组都报告特定 CLI 的输出。受支持的 Smart Call Home 警报组如下所示：

- 系统日志
- 诊断
- 环境
- 资产
- 配置
- 威胁
- 快照
- 遥测
- 测试

警报组的属性

警报组具有下列属性：

- 事件首先向一个警报组注册。
- 一个组可以与多个事件相关联。
- 可以订用特定警报组。
- 可以启用和禁用特定警报组。对所有警报组都启用了默认设置。
- 诊断和环境警报组支持订用周期性消息。
- 系统日志警报组支持基于消息 ID 的订用。
- 对于环境警报组，可以配置 CPU 和内存使用率阈值。当某个参数超过预定义的阈值时，将发送消息。大部分阈值依赖于平台，并且不可更改。

- 可以配置快照警报组，以便发送所指定的 CLI 的输出。

警报组向思科发送的消息

消息定期发送到思科，每当 ASA 重新加载时，也会发送这些消息。这些消息按警报组进行分类。

资产警报包含下列命令的输出：

- **show version** - 显示设备的 ASA 软件版本、硬件配置、许可密钥和相关运行时间数据。
- **show inventory**—检索并显示网络设备中安装的每款思科产品的相关资产信息。每款产品都由唯一的设备信息（称为UDI）进行标识，UDI是以下三个不同数据元素的组合：产品标识符(PID)、版本标识符 (VID) 和序列号 (SN)。
- **show failover state** - 显示故障切换对中的两个装置的故障切换状态。显示的信息包括设备的主要或辅助状态、设备的主用/备用状态以及最新报告的故障切换原因。
- **show module** - 显示 ASA 上安装的任何模块的相关信息。
- **show environment** - 显示 ASA 系统组件的系统环境信息，例如机箱、驱动器、风扇和电源的硬件运行状态以及温度状态、电压和 CPU 利用率。

配置警报包含下列命令的输出：

- **show context**- 显示已分配的接口、配置文件URL以及配置的情景数目，如果在系统执行空间中启用了匿名报告，则显示所有情景的列表。
- **show call-home registered-module status**- 显示已注册的模块状态。如果使用系统配置模式，则此命令将根据整台设备（而不是每个情景）显示系统模块状态。
- **show running-config** - 显示 ASA 上当前正在运行的配置。
- **show startup-config** - 显示启动配置。
- **show access-list | include elements** - 显示命中计数器和访问列表的时间戳值。

诊断警报包含下列命令的输出：

- **show failover** - 显示有关装置的故障切换状态的信息。
- **show interface - 显示接口统计信息**。
- **show cluster info - 显示群集信息**。
- **show cluster history - 显示集群历史记录**。
- **show crashinfo**（截断） - 发生意外的软件重新加载之后，设备将发送修改后的崩溃信息文件（仅包括该文件的回溯部分），以便仅向思科报告函数调用、注册表值和堆栈转储。
- **show tech-support no-config - 显示由技术支持分析师用于诊断的信息**。

环境警报包含下列命令的输出：

- **show environment** - 显示 ASA 系统组件的系统环境信息，例如机箱、驱动器、风扇和电源的硬件运行状态以及温度状态、电压和 CPU 利用率。
- **show cpu usage** - 显示 CPU 利用率信息。
- **show memory detail** - 显示有关可用系统内存和已分配系统内存的详细信息。

威胁警报包含下列命令的输出：

- **show threat-detection rate** - 显示威胁检测统计信息。
- **show threat-detection shun** - 显示当前绕过的主机。
- **show shun** - 显示绕过信息。
- **show dynamic-filter reports top** - 生成按僵尸网络流量过滤器分类的前 10 个恶意软件站点、端口和受感染主机的报告。

快照警报可能包含下列命令的输出：

- **show conn count** - 显示处于活动状态的连接的数目。
- **show asp drop** - 显示加速安全路径丢弃的数据包或连接数。

遥测警报包含下列命令的输出：

- **show perfmon detail** - 显示 **ASA** 性能详细信息。
- **show traffic** - 显示接口发送和接收活动。
- **show conn count** - 显示处于活动状态的连接的数目。
- **show vpn-sessiondb summary** - 显示 **VPN** 会话摘要信息。
- **show vpn load-balancing** - 显示 **VPN** 负载均衡虚拟群集配置的运行时统计信息。
- **show local-host | include interface** - 显示本地主机的网络状态。
- **show memory** - 显示可供操作系统使用的最大物理内存量和当前可用内存量的摘要。
- **show context**- 显示已分配的接口、配置文件URL 以及配置的情景数目，如果在系统执行空间中启用了匿名报告，则显示所有情景的列表。
- **show access-list | include elements** - 显示命中计数器和访问列表的时间戳值。
- **show interface** - 显示接口统计信息。
- **show threat-detection statistics protocol** - 显示 **IP** 协议统计信息。
- **show phone-proxy media-sessions count** - 显示 **Phone Proxy** 所存储的相应介质会话数。
- **show phone-proxy secure-phones count** - 显示数据库中存储的支持安全模式的电话数。
- **show route** - 显示路由表。
- **show xlate count** - 显示 **NAT** 会话 **(xlate)** 的数目。

消息严重性阈值

使目标配置文件订用某些警报组时，可以设置阈值，以便根据消息严重性级别发送警报组消息。值小于目标配置文件的指定阈值的所有消息都不会发送到目标。

下表显示消息严重性级别与系统日志严重性级别之间的对应关系。

表 *1:* 消息严重性级别与系统日志级别对应关系

Level	消息 严重性级别	系统日志 严重性级别	说明
9	巨大灾难	不适用	全网范围的灾难性故障。
8	灾难	不适用	重大网络影响。
7	由指定的 CLI 关键字确定： **subscribe-to-alert-group** 警报组名称 **severity** 严重性级别	0	紧急。系统不可用。
6	由指定的 CLI 关键字确定： **subscribe-to-alert-group** 警报组名称 **severity** 严重性级别	1	警报。严重情况；需要立即引起注意。
5	由指定的 CLI 关键字确定： **subscribe-to-alert-group** 警报组名称 **severity** 严重性级别	2	严重。严重情况。
4	由指定的 CLI 关键字确定： **subscribe-to-alert-group** 警报组名称 **severity** 严重性级别	3	错误。轻微情况。
3	警告	4	警告情况。
2	通知	5	基本通知和信息消息。可能是独立的无关紧要情况。
1	正常状态	6	信息。正常事件，表示恢复正常状态。
0	调试	7	调试消息（默认设置）。

订用配置文件

订用配置文件使您能够将目标收件人与感兴趣的组相关联。在配置文件中向订用的组注册的事件被触发时，与该事件相关联的消息将发送到配置的收件人。订用配置文件具有下列属性：

- 可以创建并配置多个配置文件。
- 一个配置文件可以配置多个邮件或 HTTPS 收件人。
- 一个配置文件可以使多个组订用指定的严重性级别。
- 配置文件支持三种消息格式：短文本、长文本和 XML。
- 可以启用和禁用特定配置文件。默认情况下，配置文件处于禁用状态。
- 可以指定最大消息大小。默认为 3 MB。

已提供一个默认配置文件“Cisco TAC”。默认配置文件包含一组要监控的预定义组（诊断、环境、资产、配置和遥测）以及预定义的目标邮件地址和 HTTPS URL。最初配置 Smart Call Home 时，系统将自动创建默认配置文件。目标邮件地址为 callhome@cisco.com，目标 URL 为 https://tools.cisco.com/its/service/oddce/services/DDCEService。

注释 无法更改默认配置文件的目标邮件地址或目标 URL。

在使目标配置文件订用配置、资产、遥测或快照警报组时，可以选择以异步方式接收或者在指定时间定期接收警报组消息。

下表将默认警报组映射到其严重性级别订用和周期（如果适用）：

表 *2:* 警报组到严重性级别订用的映射

警报组	严重性级别	周期
配置	信息	每月
诊断	信息及更高级别	不适用
环境	通知及更高级别	不适用
库存	信息	每月
快照	信息	不适用
系统日志	等效系统日志	不适用
遥测	信息	每天
测试	不适用	不适用
威胁	通知	不适用

Anonymous Reporting 和 Smart Call Home 指南

本节介绍在配置 Anonymous Reporting 和 Smart Call Home 之前应查看的准则和限制。

Anonymous Reporting 准则

- 必须配置 DNS。
- 如果首次尝试无法发送 Anonymous Reporting 消息，则 ASA 将再重试两次，然后才丢弃该消息。
- Anonymous Reporting 可以与其他 Smart Call Home 配置共存，而不会更改现有配置。例如，如果启用 Anonymous Reporting 之前 Smart Call Home 处于禁用状态，那么 Smart Call Home 将保持禁用状态，即使在 Anonymous Reporting 启用后也是如此。
- 如果 Anonymous Reporting 处于启用状态，将无法删除信任点，并且禁用 Anonymous Reporting 时，信任点仍保留。如果 Anonymous Reporting 处于禁用状态，则可以删除信任点，但禁用 Anonymous Reporting 不会导致删除信任点。
- 如果使用的是多情景模式配置，则 **dns**、**interface** 和 **trustpoint** 命令处于管理情景中，而 **call-home** 命令处于系统情景中。
- 您可以按照定期间隔自动进行 trustpool 捆绑包的更新，以便在 CA 服务器的自签名证书更改时，Smart Call Home 可以保持活动状态 。此 trustpool 自动续订功能在多情景部署下不受支持。

Smart Call Home 准则

- 在多情景模式下，subscribe-to-alert-group snapshot periodic 命令划分成两条命令：一条命令用于从系统配置中获取信息，另一条命令用于从用户情景中获取信息。
- Smart Call Home 后台服务器只能接受 XML 格式的消息。
- 如果已启用集群功能，并且已将 Smart Call Home 配置为订用严重性级别为“严重”的诊断警报组，那么将向思科发送 Smart Call Home 消息以报告重要的集群事件。仅对于下列事件，才会发送 Smart Call Home 集群消息：
  - 当装置加入集群时
  - 当装置离开集群时
  - 当集群装置变成集群控制设备时
  - 当集群中的辅助装置发生故障时

  发送的每条消息都包含以下信息：
  - 处于活动状态的集群成员的计数
  - 对集群控制设备运行的 **show cluster info** 命令和 **show cluster history** 命令的输出

配置 Anonymous Reporting 和 Smart Call Home

虽然 Anonymous Reporting 是 Smart Call Home 服务的组成部分，并且使思科能够以匿名方式接收来自设备的最少量错误和运行状况信息，但是 Smart Call Home 服务提供了对系统运行状况的自定义支持，从而使思科 TAC 能够监控设备，并且在存在问题时（通常在知道问题已发生之前）提交个案。

可以在系统上同时配置这两个服务，尽管配置 Smart Call Home 服务将会提供与 Anonymous Reporting 相同的功能以及自定义服务。

进入配置模式时，系统将会显示提示符，要求您根据下列准则启用 Anonymous Reporting 和 Smart Call Home 服务：

- 在提示符处，可以选择 [Y]（是）、[N]（否）或 [A]（稍后询问）。如果选择 [A]（稍后询问），则系统将在 7 天后或者在 ASA 重新加载时再次提醒您。如果继续选择 [A]（稍后询问），则 ASA 将以 7 天作为时间间隔再次提示 2 次，然后采用 [N]（否）响应并且不再询问。
- 如果未收到提示符，可通过执行配置 Anonymous Reporting，第 9 页或配置 Smart Call Home，第 10 页中的步骤启用 Anonymous Reporting 或 Smart Call Home。

配置 Anonymous Reporting

要配置 Anonymous Reporting，请执行以下步骤：

过程

步骤 1 启用 Anonymous Reporting 功能并创建新的匿名配置文件。

call-home reporting anonymous

示例：

```
ciscoasa(config)# call-home reporting anonymous
```

输入此命令将会创建信任点，并安装用来验证思科 Web 服务器身份的证书。

步骤 2 （可选）确保已连接到服务器并且系统能够发送消息。

call-home test reporting anonymous

示例：

```
ciscoasa(config)# call-home test reporting anonymous

INFO: Sending test message to
https://tools.cisco.com/its/service/oddce/services/DDCEService...

INFO: Succeeded
```

系统将通过一条成功或错误消息返回测试结果。

配置 Smart Call Home

在 ASA 上配置 Smart Call Home 服务包括下列任务：

过程

步骤 1 启用 Smart Call Home 服务。请参阅启用 Smart Call Home，第 10 页。

步骤 2 配置用于将 Smart Call Home 消息传递给用户的邮件服务器。请参阅配置邮件服务器，第 15 页。

步骤 3 为 Smart Call Home 消息设置联系人信息。请参阅配置客户联系信息，第 13 页。

步骤 4 定义警报处理参数，例如可以处理的最大事件率。请参阅配置警报组订用，第 12 页。

步骤 5 设置警报订用配置文件。请参阅配置目标配置文件，第 17 页。

每个警报订用配置文件都标识了以下信息：

- Smart Call Home 消息所发送到的用户，例如思科的 Smart Call Home 服务器或一系列邮件收件人。
- 要针对其接收警报的信息类别，例如配置或资产信息。

启用 Smart Call Home

要启用 Smart Call Home 并激活报障配置文件，请执行以下步骤：

过程

步骤 1 启用 Smart Call Home 服务。

service call-home

示例：

```
ciscoasa(config)# service call-home
```

步骤 2 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call home
```

声明证书签发信任点并对其进行身份验证

如果 Smart Call Home 配置为通过 HTTPS 向网络服务器发送消息，则需要将 ASA 配置为信任该 Web 服务器的证书或签发该证书的证书颁发机构 (CA) 的证书。Cisco Smart Call Home Production 服务器证书由 Verisign 签发。Cisco Smart Call Home Staging 服务器证书由 Digital Signature Trust Company 签发。

注释 不应该为客户端类型或验证用途设置信任点，以避免将信任点用于 VPN 验证。

要声明思科服务器安全认证并对其进行身份验证，然后与 Smart Call Home 服务的思科 HTTPS 服务器进行通信，请执行以下步骤：

过程

步骤 1 （仅限多情景模式）在管理情景中安装证书。

changeto context *admincontext*

示例：

```
ciscoasa(config)# changeto context contextA
```

步骤 2 配置信任点并为认证登记作准备。

crypto ca trustpoint *trustpoint-name*

示例：

```
ciscoasa(config)# crypto ca trustpoint cisco
```

注释 如果使用 HTTP 作为传输方法，则必须通过信任点安装 HTTPS 所需的安全认证。请在以下 URL 处查找要安装的特定证书：

http://www.cisco.com/en/US/docs/switches/lan/smart_call_home/SCH31_Ch6.html#wp1035380

步骤 3 指定以手动剪切并粘贴的方法进行认证登记。

enroll terminal

示例：

```
ciscoasa(ca-trustpoint)# enroll terminal
```

步骤 4 对指定的 CA 进行身份验证。CA 名称应与 **crypto ca trustpoint** 命令中指定的信任点名称匹配。在提示符处，粘贴安全认证文本。

crypto ca authenticate trustpoint

示例：

```
ciscoasa(ca-trustpoint)# crypto ca authenticate cisco
```

步骤 5 指定安全认证文本结束，并确认接受所输入的安全证书。

quit

示例：

```
ciscoasa(ca-trustpoint)# quit
%Do you accept this certificate [yes/no]:
yes
```

配置环境警报组和快照警报组

要配置环境警报组和快照警报组，请执行以下步骤：

过程

进入警报组配置模式。

alert-group-config {**environment** | **snapshot**}

示例：

```
ciscoasa(config)# alert-group-config environment
```

配置警报组订用

要使目标配置文件订用警报组，请执行以下步骤：

过程

步骤 1 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2 启用指定的 Smart Call Home 警报组。

alert-group {**all** | **configuration** | **diagnostic** | **environment** | **inventory** | **syslog**}

示例：

```
ciscoasa(cfg-call-home)# alert-group syslog
```

使用 **all** 关键字启用所有警报组。默认情况下，所有警报组都处于启用状态。

步骤 3 进入指定目标配置文件的配置文件配置模式。

profile *profile-name*

示例：

```
ciscoasa(cfg-call-home)# profile CiscoTAC-1
```

步骤 4 订用所有的可用警报组。

subscribe-to-alert-group all

示例：

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group all
```

步骤 5 使此目标配置文件订用配置警报组。

subscribe-to-alert-group configuration periodic {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}

示例：

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
```

periodic 关键字可为配置警报组配置定期通知。默认周期为每日。

daily 关键字以 *hh:mm* 格式指定每天的发送时间（采用 24 小时制，例如 14:30）。

weekly 关键字以 *day hh:mm* 格式指定一周内的哪几天和一天内的时间，其中星期几将拼写出来（例如 Monday）。

monthly 关键字以 *date hh:mm* 格式指定数字日期（1 到 31）和一天内的时间。

配置客户联系信息

要配置客户联系信息，请执行以下步骤：

过程

步骤 1 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2 指定客户电话号码。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

phone-number *phone-number-string*

示例：

```
ciscoasa(cfg-call-home)# phone-number 8005551122
```

步骤 3 指定客户地址，地址是长度最多为 255 个字符的自由格式字符串。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

street-address *street-address*

示例：

```
ciscoasa(cfg-call-home)# street-address “1234 Any Street, Any city, Any state, 12345”
```

步骤 4 指定客户姓名，姓名长度可达 128 个字符。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

contact-name *contact-name*

示例：

```
ciscoasa(cfg-call-home)# contact-name contactname1234
```

步骤 5 指定思科客户 ID，此 ID 的长度最多为 64 个字符。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

customer-id *customer-id-string*

示例：

```
ciscoasa(cfg-call-home)# customer-id customer1234
```

步骤 6 指定思科客户 ID，此 ID 的长度最多为 64 个字符。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

site-id *site-id-string*

示例：

```
ciscoasa(cfg-call-home)# site-id site1234
```

步骤 7 指定客户合同 ID，此 ID 的长度最多为 128 个字符。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

contract-id *contract-id-string*

示例：

```
ciscoasa(cfg-call-home)# contract-id contract1234
```

示例

以下示例显示如何配置联系信息：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# contact-email-addr username@example.com
ciscoasa(cfg-call-home)# phone-number 8005551122
ciscoasa(cfg-call-home)# street-address “1234 Any Street, Any city, Any state, 12345”
ciscoasa(cfg-call-home)# contact-name contactname1234
ciscoasa(cfg-call-home)# customer-id customer1234
ciscoasa(cfg-call-home)# site-id site1234
ciscoasa(cfg-call-home)# contract-id contract1234
```

配置邮件服务器

建议您使用 HTTPS 进行消息传输，因为此协议最安全。但是，您可以为 Smart Call Home 配置邮件目标，然后将邮件服务器配置为使用邮件消息传输。

要配置邮件服务器，请执行以下步骤：

过程

步骤 1 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2 指定 SMTP 邮件服务器。

mail-server*ip-address* **name priority** [**1-100**] [**all**]

示例：

```
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 smtp.example.com priority 1
```

可以使用 5 个单独的命令指定多达 5 个邮件服务器。必须至少将一个邮件服务器配置为使用邮件传输方法来传输 Smart Call Home 消息。

数字越小，邮件服务器的优先级越高。

ip-address 参数可以是 IPv4 或 IPv6 邮件服务器地址。

示例

以下示例显示如何配置主邮件服务器（名为“smtp.example.com”）和辅助邮件服务器（IP 地址为 10.10.1.1）：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# mail-server smtp.example.com priority 1
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 priority 2
ciscoasa(cfg-call-home)# exit
ciscoasa(config)#
```

配置流量速率限制

要配置流量速率限制，请执行以下步骤：

过程

步骤 1 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2 指定 Smart Call Home 每分钟可以发送的消息数。默认值为 10 条消息/分钟。

rate-limit *msg-count*

示例：

```
ciscoasa(cfg-call-home)# rate-limit 5
```

发送 Smart Call Home 通信

要发送特定 Smart Call Home 通信，请执行以下步骤：

过程

选择以下其中一个选项：

- 选项 1 - 使用配置文件配置来手动发送测试消息。

  call-home test [*test-message*] **profile** *profile-name*

  示例：

  ```
  ciscoasa# call-home test [testing123] profile CiscoTAC-1
  ```

- 选项2 - 向一个目标配置文件（如果已指定）发送警报组消息。如果未指定配置文件，则向订用了资产、配置、快照或遥测警报组的所有配置文件发送消息。

  call-home send alert-group inventory { | **configuration** | **snapshot** | **telemetry**} [**profile** *profile-name*]

  示例：

  ```
  ciscoasa# call-home send alert-group inventory
  ```

- 选项3 - 将命令输出发送到邮件地址。指定的CLI命令可以是任何命令，包括用于所有已注册的模块的命令。

  call-home send*cli command* [**email** *email*]

  示例：

  ```
  ciscoasa# call-home send cli destination email username@example.com
  ```

  如果已指定邮件地址， 命令输出将被发送到该地址。如果未指定邮件地址，则输出将发送到思科 TAC。邮件将以日志文本格式发送，服务编号（如果已指定）将包括在主题行中。

  仅在未指定邮件地址或已指定思科 TAC 邮件地址时， 才需要服务编号。

配置目标配置文件

要配置目标配置文件以进行邮件或 HTTP 传输，请执行以下步骤：

过程

步骤 1 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2 进入指定目标配置文件的配置文件配置模式。如果指定的目标配置文件不存在，将会创建该文件。

profile *profile-name*

示例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

最多可以创建 10 个处于活动状态的配置文件。默认配置文件将向思科 TAC 报告。如果要将报障信息发送到其他位置（例如您自己的服务器），则可以配置一个单独的配置文件。

步骤 3 配置 Smart Call Home 消息接收方的目标、消息大小、消息格式和传输方法。默认消息格式为 XML，默认启用的传输方法为邮件。

destination address {**email** *address* | **http** *url*[**reference-identity** *ref-id-name*]} | **message-size-limit** *size* | **preferred-msg-format** {**long-text** | **short-text** | **xml**} **transport-method** {**email** | **http**}}

示例：

```
ciscoasa(cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService reference-identity
ExampleService
ciscoasa(cfg-call-home-profile)# destination address email username@example.com
ciscoasa(cfg-call-home-profile)# destination preferred-msg-format long-text
```

reference-identity 选项可启用对收到的服务器证书的 RFC 6125 参考身份检查。这些检查仅适用于配置了 http 地址的目标。ID 检查根据以前配置的参考身份对象执行。有关参考身份对象的详细信息，请参阅配置引用标识。

邮件地址是 Smart Call Home 消息接收方的邮件地址，此地址的长度可达 100 个字符。默认情况下，最大 URL 大小为 5 MB。

在移动设备上，使用短文本格式来发送和读取消息；在计算机上，使用长文本格式来发送和读取消息。

如果消息接收方是 Smart Call Home 后台服务器，请确保 **preferred-msg-format** 值是 XML，这是因为后端服务器只能接受 XML 格式的消息。

使用此命令可以将传输方法重新更改为邮件。

复制目标配置文件

要通过复制现有的目标配置文件来创建新的目标配置文件，请执行以下步骤：

过程

步骤 1 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2 指定要复制的配置文件。

profile *profile-name*

示例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

步骤 3 将现有配置文件的内容复制到新配置文件。

copy profile *src-profile-name dest-profile-name*

示例：

```
ciscoasa(cfg-call-home)# copy profile newprofile profile1
```

现有配置文件 (*src-profile-name*) 和新配置文件 (*dest-profile-name*) 的长度可达 23 个字符。

示例

以下示例显示如何复制现有配置文件：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# copy profile newprofile profile1
```

重命名目标配置文件

要更改现有配置文件的名称，请执行以下步骤：

过程

步骤 1 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2 指定要重命名的配置文件。

profile *profilename*

示例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

步骤 3 更改现有配置文件的名称。

rename profile *src-profile-name dest-profile-name*

示例：

```
ciscoasa(cfg-call-home)# rename profile newprofile profile1
```

现有配置文件 (*src-profile-name*) 和新配置文件 (*dest-profile-name*) 的长度可达 23 个字符。

示例

以下示例显示如何重命名现有配置文件：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# rename profile newprofile profile1
```

监控 Anonymous Reporting 和 Smart Call Home

请参阅以下命令来监控 Anonymous Reporting 和 Smart Call Home 服务。

- **show call-home detail**

  此命令显示当前 Smart Call Home 详细配置。

- **show call-home mail-server status**

  此命令显示当前邮件服务器状态。

- **show call-home profile** {profile name | **all**}

  此命令显示 Smart Call Home 配置文件的配置。

- **show call-home registered-module status** [**all**]

  此命令显示已注册的模块状态。

- **show call-home statistics**

  此命令显示报障详细状态。

- **show call-home**

  此命令显示当前 Smart Call Home 配置。

- **show running-config call-home**

  此命令显示当前 Smart Call Home 运行配置。

- **show smart-call-home alert-group**

  此命令显示 Smart Call Home 警报组的当前状态。

- **show running-config all**

  此命令显示有关 Anonymous Reporting 用户配置文件的详细信息。

Smart Call Home 示例

以下示例显示如何配置 Smart Call Home 服务：

```
ciscoasa (config)# service call-home
ciscoasa (config)# call-home
ciscoasa (cfg-call-home)# contact-email-addr customer@example.com
ciscoasa (cfg-call-home)# profile CiscoTAC-1
ciscoasa (cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService
ciscoasa (cfg-call-home-profile)# destination address email callhome@example.com
ciscoasa (cfg-call-home-profile)# destination transport-method http
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group environment
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group diagnostic
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group telemetry periodic weekly Monday
 23:30
```

Anonymous Reporting 和 Smart Call Home 的历史记录

表 *3: Anonymous Reporting* 和 *Smart Call Home* 的历史记录

功能名称	平台版本	说明
Smart Call Home	8.2(2)	Smart Call Home 服务用于在 ASA 上提供主动诊断和实时警报，并提供更高的网络可用性和运行效率。 引入或修改了下列命令： **active (call home)**、**call-home**、**call-home send alert-group**、**call-home test**、**contact-email-addr**、**customer-id (call home)**、**destination (call home)**、**profile**、**rename profile**、**service call-home**、**show call-home**、**show call-home detail**、**show smart-call-home alert-group**、**show call-home profile**、**show call-home statistics**、**show call-home mail-server status**、**show running-config call-home**、**show call-home registered-module status all**、**site-id**、**street-address**、**subscribe-to-alert-group all**、**alert-group-config**、**subscribe-to-alert-group configuration**、**subscribe-to-alert-group diagnostic**、**subscribe-to-alert-group environment**、**subscribe-to-alert-group inventory periodic**、**subscribe-to-alert-group snapshot periodic**、**subscribe-to-alert-group syslog** 和 **subscribe-to-alert-group telemetry periodic**。
Anonymous Reporting	9.0(1)	可以通过启用 Anonymous Reporting 服务来帮助改进 ASA 平台，此服务使思科能够安全地接收来自设备的最少量错误和运行状况信息。 引入了以下命令：**call-home reporting anonymous** 和 **call-home test reporting anonymous**。

功能名称	平台版本	说明
Smart Call Home	9.1(2)	**show local-host** 命令已更改为 **show local-host | include interface** 命令，以进行遥测警报组报告。
Smart Call Home	9.1(3)	如果已启用集群功能，并且已将 Smart Call Home 配置为订用严重性级别为“严重”的诊断警报组，那么将向思科发送 Smart Call Home 消息以报告重要的集群事件。仅对于以下三个事件，才会发送 Smart Call Home 集群消息： • 当装置加入集群时 • 当装置离开集群时 • 当集群装置变成集群控制设备时 发送的每条消息都包含以下信息： • 处于活动状态的集群成员的计数 • 对集群控制设备运行的 **show cluster info** 命令和 **show cluster history** 命令的输出
安全 Smart Call Home 服务器连接的引用标识	9.6(2)	TLS 客户端处理现在支持用于验证 RFC 6125 第 6 节中定义的服务器标识的规则。标识验证将在对通向 Smart Call Home 服务器的 TLS 连接进行 PKI 验证时完成。如果提供的标识无法与配置的引用标识相匹配，则不会建立连接。 添加或修改了以下命令：**[no] crypto ca reference-identity**、**call home profile destination address http**。