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 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 的设备的最新清单和配置信息。

Anonymous Reporting 和 Smart Call Home 准则

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。

配置 Anonymous Reporting

要配置 Anonymous Reporting，请执行以下步骤：

过程

步骤 1 依次选择 **Configuration** > **Device Management** > **Smart Call Home**。

步骤 2 选中 **Enable Anonymous Reporting** 复选框。

步骤 3 点击 **Test Connection** 以确保系统能够发送消息。

ASDM 将返回一条成功或错误消息，以便向您通知测试结果。

步骤 4 点击 **Apply** 以保存配置并启用 Anonymous Reporting。

配置 Smart Call Home

要配置 Smart Call Home 服务、系统设置和警报订用配置文件，请执行以下步骤。

过程

步骤 1 依次选择**配置** > **设备管理** > **Smart Call Home**。

步骤 2 选中 **Enable Registered Smart Call Home** 复选框，以启用 Smart Call Home 并向思科 TAC 注册 ASA。

步骤 3 双击 **Advanced** 系统设置。此区域包含三个窗格。双击标题行可以展开或折叠每个窗格。

a) 可以在 **Mail Servers** 窗格中设置邮件服务器，用于将 Smart Call Home 消息传递给邮件用户。

b) 可以在 ASA 的 **Contact Information** 窗格中输入联系人信息，此信息将显示在 Smart Call Home 消息中。此窗格包含以下信息：

- 联系人的姓名。
- 联系人的电话号码。
- 联系人的邮寄地址。
- 联系人的邮件地址。
- Smart Call Home 邮件中的“发件人”邮件地址。
- Smart Call Home 邮件中的“回复”邮件地址。
- 客户 ID。
- 站点 ID。
- 合同 ID。

c) 可以在 **Alert Control** 窗格中调整警报控制参数。此窗格包含 **Alert Group Status** 窗格，后者列出以下警报组的状态（已启用或已禁用）：

- 诊断警报组。
- 配置警报组。
- 环境警报组。
- 清单警报组。
- 快照警报组。
- 系统日志警报组。
- 遥测警报组。
- 威胁警报组。
- 每分钟处理的最大 Smart Call Home 消息数。
- Smart Call Home 邮件中的“发件人”邮件地址。

步骤 4 双击 **Alert Subscription Profiles**。每个指定的订用配置文件都标识了感兴趣的用户和警报组。

a) 点击 **Add** 或 **Edit** 以显示 **Subscription Profile Editor**，可以在其中创建新的订用配置文件或者编辑现有订用配置文件。

b) 点击 **Delete** 以删除所选配置文件。

c) 选中 **Active** 复选框，以便向用户发送所选订用配置文件的 Smart Call Home 消息。

步骤 5 点击 **Add** 或 **Edit** 以显示 **Add** 或 **Edit Alert Subscription Profile** 对话框。

a) **Name** 字段是只读字段，不可编辑。
b) 选中 **Enable this subscription profile** 复选框以启用或禁用此特定配置文件。
c) 点击 **Alert Delivery Method** 区域中的 **HTTP** 或 **Email** 单选按钮。
d) 在 **Subscribers** 字段中输入邮件地址或 Web 地址。
e) 按名称指定一个 **Reference Identity** 对象，以对通过系统日志服务器收到的证书启用 RFC 6125 引用标识检查。

有关引用标识对象的详细信息，请参阅配置引用标识。

步骤 6 管理员可以在 **Alert Dispatch** 区域中指定要向用户发送的 Smart Call Home 信息类型以及要在哪些情况下发送这些信息。根据警报触发方式，已选中两种类型的警报，即基于时间的警报和基于事件的警报。下列警报组基于时间：配置、清单、快照和遥测。下列警报组基于事件：诊断、环境、系统日志和威胁。

步骤 7 可以在 **Message Parameters** 区域中调整用于控制向用户发送的消息的参数，包括首选消息格式和最大消息大小。

步骤 8 对于基于时间的警报，请点击**警报发送**区域中的**添加**或**编辑**，以显示**添加**或**编辑配置警报发送条件**对话框。

a) 在 **Alert Dispatch Frequency** 区域中指定向用户发送信息的频率：

- 对于每月订用，请指定要在一个月中的哪一天的什么时间发送信息。如果未指定这些信息，则 ASA 将选择适当的值。
- 对于每周订用，请指定要在一周中的哪一天的什么时间发送信息。如果未指定这些信息，则 ASA 将选择适当的值。
- 对于每日订用，请指定要在一天中的什么时间发送信息。如果未指定此信息，则 ASA 将选择适当的值。
- 对于每小时订用，请指定要在一个小时内的第几分钟发送信息。如果未指定此信息，则ASA 将选择适当的值。每小时订用仅适用于快照和遥测警报组。

b) 点击 **Basic** 或 **Detailed** 单选按钮，以便向用户提供所需级别的信息。
c) 点击 **OK** 以保存配置。

步骤 9 对于基于诊断、环境和威胁事件的警报，请点击 **Alert Dispatch** 区域中的 **Add** 或 **Edit**，以显示 **Create** 或 **Edit Diagnostic Alert Dispatch Condition** 对话框。

步骤 10 在 **Event Severity** 下拉列表中指定将会触发向用户发送警报的事件严重性，然后点击 **OK**。

步骤 11 对于基于时间的清单警报，请点击**警报发送 (Alert Dispatch)** 区域中的 **添加 (Add)** 或**编辑 (Edit)**，以显示**创建 (Create)** 或**编辑清单警报发送条件 (Edit Inventory Alert Dispatch Condition)** 对话框。

步骤 12 在 **Alert Dispatch Frequency** 下拉列表中指定向用户发送警报的频率，然后点击 **OK**。

步骤 13 对于基于快照时间的警报，请点击**警报发送**区域中的**添加**或**编辑**，以显示**创建**或**编辑快照警报发送条件**对话框。

a) 在 **Alert Dispatch Frequency** 区域中指定向用户发送信息的频率：

- 对于每月订用，请指定要在一个月中的哪一天的什么时间发送信息。如果未指定这些信息，则 ASA 将选择适当的值。

- 对于每周订用，请指定要在一周中的哪一天的什么时间发送信息。如果未指定这些信息，则 ASA 将选择适当的值。
- 对于每日订用，请指定要在一天中的什么时间发送信息。如果未指定此信息，则 ASA 将选择适当的值。
- 对于每小时订用，请指定要在一个小时内的第几分钟发送信息。如果未指定此信息，则ASA 将选择适当的值。每小时订用仅适用于快照和遥测警报组。
- 对于时间间隔订用，请指定向用户发送信息的频率（以分钟为单位）。此要求仅适用于快照警报组。

b) 点击 **OK** 以保存配置。

步骤 14 对于基于事件的系统日志警报，请点击 **Alert Dispatch** 区域中的 **Add** 或 **Edit**，以显示 **Create** 或 **Edit Syslog Alert Dispatch Condition** 对话框。

a) 选中 **Specify the event severity which triggers the dispatch of alert to subscribers** 复选框，然后从下拉列表中选择事件严重性。
b) 选中 **Specify the message IDs of syslogs which trigger the dispatch of alert to subscribers** 复选框。
c) 根据屏幕上的说明，指定将会触发向用户发送警报的系统日志消息 ID。
d) 点击 **OK** 以保存配置。

步骤 15 对于基于遥感勘测事件的警报，请点击**警报发送**区域中的**添加**或**编辑**，以显示**创建**或**编辑遥感勘测警报发送条件**对话框。

a) 在 **Alert Dispatch Frequency** 区域中指定向用户发送信息的频率：
   - 对于每月订用，请指定要在一个月中的哪一天的什么时间发送信息。如果未指定这些信息，则 ASA 将选择适当的值。
   - 对于每周订用，请指定要在一周中的哪一天的什么时间发送信息。如果未指定这些信息，则 ASA 将选择适当的值。
   - 对于每日订用，请指定要在一天中的什么时间发送信息。如果未指定此信息，则 ASA 将选择适当的值。
   - 对于每小时订用，请指定要在一个小时内的第几分钟发送信息。如果未指定此信息，则ASA 将选择适当的值。每小时订用仅适用于快照和遥测警报组。

b) 点击 **OK** 以保存配置。

步骤 16 点击 **Test** 以确定所配置的警报是否正常工作。

配置信任池证书的自动导入

智能许可使用 Smart Call Home 基础设施。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，而无需客户来调整证书层次结构变化。您可以按照定期

的间隔自动执行信任池捆绑包的更新，以便在 CA 服务器的自签名证书发生变化时 Smart Call Home 可以保持活动状态。此功能在多情景部署环境下不受支持。

信任池证书捆绑包的自动导入需要您指定 ASA 下载和导入捆绑包所用的 URL。使用以下命令，以便每天可以按照固定的间隔使用默认的思科 URL 和 22 小时的默认时间进行导入：

```
ciscoasa(config-ca-trustpool)# auto-import-url Default
```

您还可以使用以下命令以自定义 URL 启用 自动导入：

```
ciscoasa(config-ca-trustpool)# auto-import url http://www.thawte.com
```

为了能让您在非高峰时段或其他便利时间灵活地设置下载，请输入以下命令，以使用自定义时间启用导入：

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23
```

使用自定义 URL 和自定义时间 设置自动导入需要使用以下 命令：

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23 url http://www.thawte.com
```

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。您可以依次使用 **Tools > Command Line Interface** 输入这些命令。

- **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。

Anonymous Reporting 和 Smart Call Home 历史记录

表 *1: Anonymous Reporting* 和 *Smart Call Home* 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。 引入了以下屏幕： Configuration > Device Management > Smart Call Home。
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。 修改了以下屏幕：Configuration > Device Management > Smart Call Home。
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

功能名称	平台版本	说明
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针对 RFC 6125 第 6 节中定义的服务器身份验证的规则。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。 修改了以下页面：**Configuration > Device Management > Smart Call Home**。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。