CA Spectrum®

Secure Domain Manager 用户指南

版本 9.3

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA Spectrum® (CA Spectrum)
- CA Spectrum® Secure Domain Manager
- CA Spectrum® Secure Domain Connector

联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

目录

第 1 章： 简介

此部分包含以下主题：

管理高度安全网络的挑战

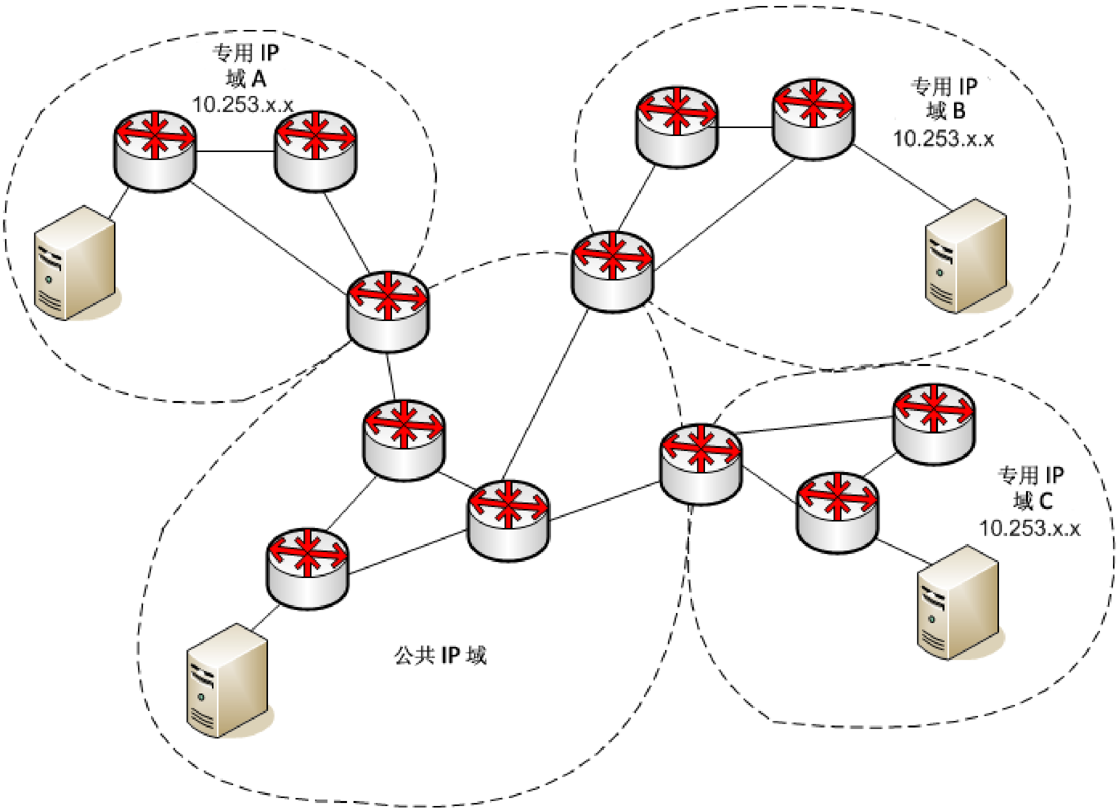
近来，计算机网络日趋安全。相应地，管理安全网络中的设备和应用程序所面临的挑战也越来越大。这些挑战包括：

- 在重叠（或专用）IP 域（NAT 环境）中管理网络元素
- 管理配置为阻止 SNMP 和 ICMP 通信的防火墙后面的网络元素
- 管理跨不安全网络域的网络元素

Secure Domain Manager 产品提供了应对这些管理挑战的独特解决方案。

重叠的 IP 域

在下图显示的 NAT 网络中，有一个公共 IP 域和三个包含相同 IP 子网络的专用 IP 域。



这些域可能代表公司的托管网络、大型企业新收购的分部或机场候机楼中的托管无线热点。

以下类型的 CA Spectrum 客户会面临重叠 IP 方面的挑战：

托管服务提供商 (MSP)

MSP 使用 CA Spectrum 管理其他组织的网络。MSP 管理的客户总是使用通常用于专用 IP（如 10.x.x.x 或 172.16.x.x）的 IP 范围。因此，MSP 必须解决管理重复或重叠 IP 地址的挑战。过去，让使用相同 IP 地址空间的每个客户使用一个专用的 CA Spectrum 管理服务器（即 SpectroSERVER），便可以解决该挑战。

但这造成了两个问题。第一个是成本。对于每个客户，不管托管环境的大小和所使用的重叠 IP 地址的数目如何，都需要一个专用管理服务器。第二个问题就是管理。MSP 需要承担维护更多管理系统的负担。MSP 期盼有一种成本更低但同样有效的备选方式来代替专用管理系统，尤其是当具有重叠 IP 地址的元素数目较少且无法负担专用管理服务器的费用时更是如此。

热点 (Wi-Fi) 访问提供商

热点访问提供商在诸如机场候机楼、机场休息室、宾馆客房以及咖啡店之类的位置提供 Wi-Fi 访问。对于每个位置，将发布相同的专用 IP 地址空间。此方法可简化配置、安装和管理。一个提供商可能具有成千上万个热点。为了快速部署新热点，会在属性中对建立热点的每组设备进行相同的配置（包括 IP 地址空间）。热点一旦开启并运行后，如何主动管理热点以保持最佳服务水平就成了新的挑战。

企业经理

在组织并购方案中，企业管理人员通常必须组合两个完全不同且分别构造的 IP 网络，在很多情况下，这都会导致多个重叠的 IP 地址。在这种情况下，新的 IT 组织现在必须解决组合网络的管理问题，尤其是具有相同 IP 地址空间的网络的管理。应对这种挑战的一种解决方案是，为每个 IP 实体重新分配 IP，以确保没有重复的 IP 地址。这种解决方案所涉及的任务量巨大，在执行这些任务时还会面临各种各样的挑战。

Secure Domain Manager 可以帮助这些客户克服管理重叠 IP 域的挑战，主要体现在以下几个方面：

- 允许 MSP 在每个客户的远程网络中的主机上仅部署单个轻型代理进程，这样就不必部署和管理完整的 CA Spectrum 安装。
- 允许热点访问提供商和大型企业保持重叠的专用 IP 域不动，并使用轻型代理进程来管理网络。

阻止 SNMP 和 ICMP 通信的防火墙

防火墙可提供对很多网络环境至关紧要的安全性。在管理防火墙后面的网络方面存在某些挑战。首先，网络管理员通常配置防火墙以阻止 SNMP 和 ICMP 通信（提供网络基础架构的可见性）到达未授权的源。其次，通过高度安全的防火墙管理网络元素所需的配置很复杂。因为，涉及的所有主机和端口都需要在防火墙上标识并打开，这样才能启用全部管理功能。

使用 Secure Domain Manager，网络管理器就能克服通过安全防火墙管理网络所面临的挑战，主要体现在以下几个方面：

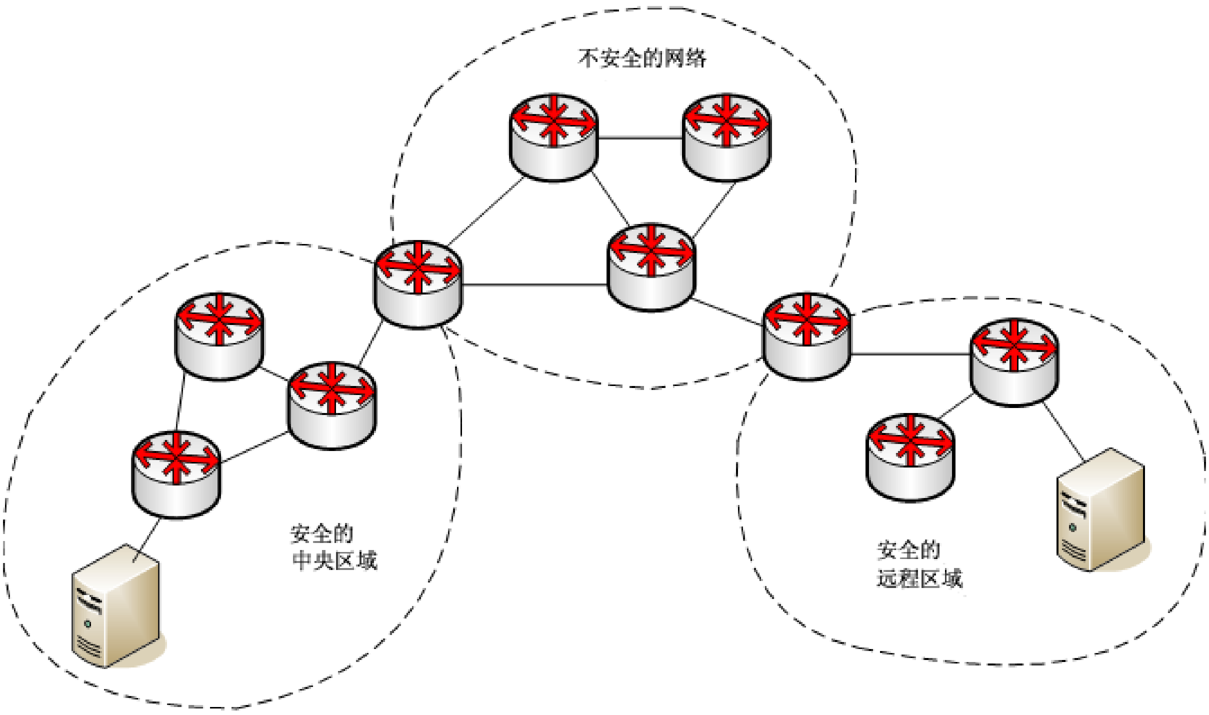
- 根据基于 TCP/IP 的协议对基于 UDP 的 SNMP 和 ICMP 数据包进行编码，以克服防火墙对 SNMP 和 ICMP 通信的限制。
- 打开单个端口以允许 SNMP 和 ICMP 通信在两个定义好的主机（在定义好的端口上）之间流动，从而简化了防火墙的配置。

跨不安全网络传递的 SNMP 通信

SNMPv1 和 SNMPv2 都是不安全的协议，因为其数据都未加密，可以使用网络协议探查器进行查看。因此，您不希望通过不安全网络发送 SNMPv1 或 SNMPv2 通信。允许 SNMP 通信跨越不安全网络到达要管理的网络就变得非常有挑战性。

如下图所示，网络管理系统可能位于“安全的中央区域”中的主机上来管理位于“安全的远程网络”中的设备。为了实现这种管理，管理流量必须流经“不安全的网络”区域。网络经理希望避免不安全协议数据包（如 SNMPv1 和 SNMPv2）中的数据在这部分网络中发生泄露。

跨不安全网络的 SNMP



使用 Secure Domain Manager，网络管理器能够加密在 SpectroSERVER 主机和远程托管网络中主机之间传递的所有管理通信。这样，就可以克服跨不安全网络安全传递不安全 SNMP 通信的挑战。这有助于确保当通信穿过中间不安全网络时数据的安全性。

Secure Domain Manager

Secure Domain Manager 是一个 CA Spectrum 网络管理解决方案，可以帮助用户在安全网络中管理设备。您不必部署本地 SpectroSERVER 就可以管理设备。Secure Domain Manager 可让您通过安全连接以隧道方式安全传送 SNMP 和 ICMP 流量来管理安全域。仅在防火墙上打开单个端口，这既扩展了可管理性，又不会影响现有的安全策略。此解决方案对最终用户和客户端应用程序都是透明的，无需执行更多管理任务。

Secure Domain Manager 的工作原理

Secure Domain Manager 支持 SNMPv1、SNMPv2 和 SNMPv3 通信。它包括两个不同的进程，即 SDManager 和 SDConnector：

SDManager

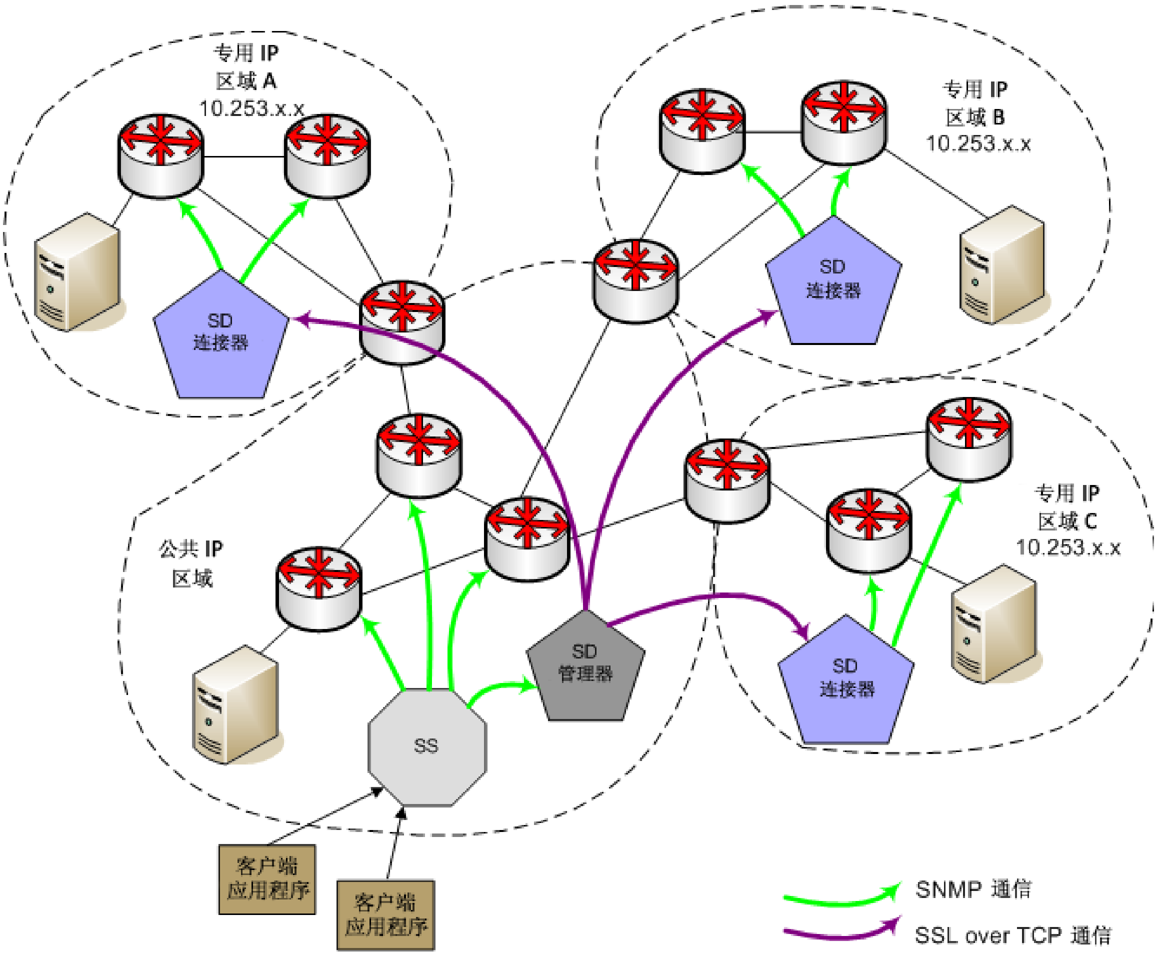
SDManager 是由 SpectroSERVER 加载的服务器消息库。

SDConnector

SDConnector 是负责与 SpectroSERVER 上的 SDManager 通信的远程进程。它在位于远程专用网络中的主机上运行，能够代表 SpectroSERVER（通常部署在专用 IP 区域中）转发 SNMP 和 ICMP 消息，以便其能够管理专用网络中的设备。SDConnector 使用可包含主要和备份 SpectroSERVER 信息的配置文件 (sdc.config) 进行配置。它是 Secure Domain Manager 解决方案的一部分。

下图显示了如何在安全网络环境中部署这些进程。

使用 Secure Domain Manager 的 NAT 网络环境



注意： 与 SpectroSERVER 位于相同区域中的设备是使用 SNMP 而不是 Secure Domain Manager 来管理的。

当位于公共 IP 区域的 SpectroSERVER 必须与位于远程安全区域中的设备通信时，SpectroSERVER 会将请求发送到 SDManager。SDManager 将 SMNP 数据转换为专用格式，并将该数据发送到与该设备位于相同区域中的 SDConnector。如果已将 SDManager 和 SDConnector 配置为通过 SSL 运行，则使用 SSL over TCP 加密数据并通过安全隧道将其发送到 SDConnector。当 SDConnector 接收到数据时，它会将数据转换回 SNMP，并向相应设备发送请求。

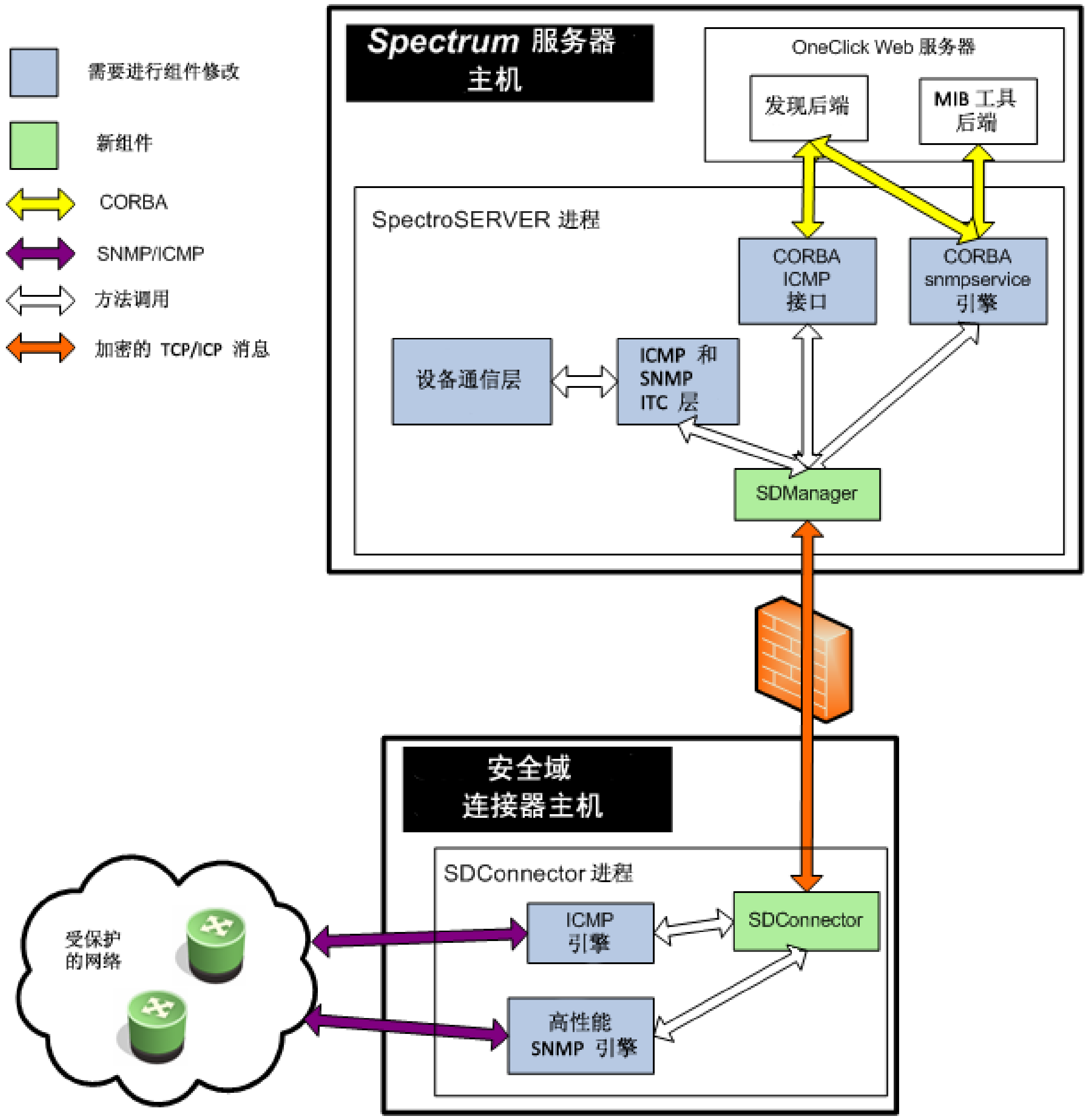
如果部署了防火墙，则防火墙也会以相同的方式工作。网络管理员必须在专用于两个已知主机的每个防火墙上打一个“洞”。使用此解决方案还可以管理位于穿过多个防火墙的区域中的设备。要启用此通信，请在每个防火墙上打开一个端口。该端口必须是已知端口并且允许相邻区域中的已知主机对使用 TCP 进行通信。

当部署 Secure Domain Manager 以管理重叠 IP 域时，每个 SDConnector 主机都必须具有唯一的公共 IP 地址。该主机必须能够与 SDConnector 必须与之通信的所有设备通信，包括 SpectroSERVER 主机及其管理的单个专用 IP 域中的所有设备。此 SDConnector 主机的可能候选主机将是位于 NAT 后面的计算机，它具有从 NAT 静态分配的唯一 IP 地址。SpectroSERVER 将 SDConnector 主机的唯一 IP 地址用作唯一标识具有相同专用 IP 地址的多个设备的附加标识符。

注意：诸如 Network Configuration Manager (NCM) 和 IP 服务管理应用程序（包括 Multicast Manager 和 Enterprise VPN Manager）之类的某些 CA Spectrum 产品无法管理重叠的 IP 地址。但是，如果在 SDConnector（而不是 SpectroSERVER）上为这些应用程序的设备建模，您仍然可以将 Secure Domain Manager 与其结合使用。在这种配置中，可以为每个 SpectroSERVER 部署多个 SDConnector，前提是 SDConnector 不管理配置了重叠 IP 地址的设备。使用此方法，您还可以为本地 SpectroSERVER 上的设备建模，但前提是设备的 IP 地址未与已通过 SDConnector 管理的设备上配置的 IP 地址相重叠。

Secure Domain Manager 体系结构

下图说明了 Secure Domain Manager 是如何运行的：



使用 Secure Domain Manager 的好处

Secure Domain Manager 解决方案可通过以下方式增强 CA Spectrum 中实现的管理功能：

- 允许 CA Spectrum 与所有兼容 SNMP 的设备通信：SNMPv1、SNMPv2 和 SNMPv3
- 允许 CA Spectrum 与位于阻止 SNMP 和 ICMP 流量的防火墙后面的设备通信
- 简化防火墙配置。原因是仅会打开一个“洞”以便两个已知主机（在已知端口上）之间进行通信
- 允许 CA Spectrum 通过不安全网络安全地传递 SNMP 和 ICMP 通信
- 允许 CA Spectrum 使用单个 SpectroSERVER 管理重叠 IP 域（NAT 环境）中的设备
- 增强发现功能以发现安全环境中的设备并为其建模，一次一个 IP 地址空间

第 2 章： 安装和配置 Secure Domain Manager 进程

本章介绍如何安装和配置 Secure Domain Manager 解决方案，即涉及安装和配置 SDConnector 和 SDManager 的进程。

此部分包含以下主题：

如何设置 Secure Domain Manager 进程

设置 Secure Domain Manager 涉及安装和配置 Secure Domain Manager 进程以及之后使用 OneClick 在 SpectroSERVER 上对其进行设置。

安装和配置进程

安装和配置 Secure Domain Manager 进程需要执行下列步骤：

1. 在目标主机上安装 SDConnector 进程 (p. 19)。

   注意：安装核心 CA Spectrum 产品时，便已安装了 SDManager；但是，仅当您公司购买的捆绑包中包含它时，它才能激活。

2. （可选）为 SSL 加密创建和部署 SSL 证书 (p. 21)。
3. 在 SDConnector 主机上设置 SDConnector 配置文件中的参数 (p. 23)。
4. 在 SpectroSERVER. 上设置 SDManager 配置文件中的参数 (p. 26)。

在 SpectroSERVER 上设置 Secure Domain Manager

安装并配置 SDConnector 和 SDManager 进程之后，使用 OneClick 在 SpectroSERVER 主机上设置 Secure Domain Manager。此设置涉及下列步骤：

1. 导入 SDManager 配置文件 (p. 31)。
2. 为 SDConnector 主机建模 (p. 32)。
3. 为要管理的安全域中的设备建模 (p. 34)。

硬件建议

采纳这些建议，以实现最佳的 Secure Domain Manager 性能：

- 为了维持最佳的 SpectroSERVER 建模容量，SpectroSERVER/SDManager 安装计算机必须具有两个 CPU：一个专用于 SpectroSERVER，另一个专用来为 SDManager 功能提供服务。如果 SDManager 和 SpectroSERVER 需要共享单个处理器来管理网络元素，则 SpectroSERVER 建模容量会降低 40%。
- 建议您使用一台专用主机来运行您部署的每个 SDConnector 进程。SDConnector 安装系统的要求与仅安装 SpectroSERVER 的要求相同。多磁盘配置的特殊要求除外。

  注意：有关安装要求的详细信息，请参阅 *《安装指南》*。
- 一个 SDConnector 只有一个 SDManager 与之连接。容错 SpectroSERVER 中的两个 SDManager 可以连接到单个 SDConnector（当设置这样要求时）。有关详细信息，请参阅在容错环境中设置进程 (p. 41)。

关于 SDConnector CPU 和内存使用率

SDConnector 使用 SpectroSERVER 用于管理设备的一半的 CPU 容量。在同样强大的系统上，如果 SpectroSERVER 计算机使用 50% 的总 CPU 容量，且所有设备都使用 SDManager 管理，则 SDConnector 使用约 25% 的 CPU 容量。主要差异是，SDConnector 不会使用大量的内存。如果它仅用作 SDConnector，那么 512 MB 的 RAM 就足够了，当然 RAM 越多越好。

安装 SDConnector 进程

在使用 Secure Domain Manager 功能管理部署了 CA Spectrum 的安全网络中的设备和应用程序之前，请在安全网络中的主机上安装单个 SDConnector 进程。Secure Domain Manager 不支持在同一个主机上运行多个 SDConnector 进程。安装 SDConnector 时，您必须是 Windows 系统上的管理用户，或者是 Solaris 和 Linux 系统上的 root 用户。

> **注意：**最佳实践为，在任何平台上升级 SDConnector 进程之前，先停止并在必要时终止该进程。停止或终止该进程可确保其在升级后正常运行。

安装 SDConnector

1. 在您希望运行 SDConnector 的非 SpectroSERVER 主机上，启动适用于所用平台的 CA Spectrum 安装程序。

   注意：只能安装与您的 SpectroSERVER 具有相同操作环境的 SDConnector。如果要安装适用于其他操作环境的 SDConnector，请联系 CA 支持人员。有关启动安装程序的信息，请参阅*《安装指南》*。

   将打开“安装”对话框。

2. 选择“安装 CA Secure Domain Connector”。

   将打开“简介”对话框。

3. 单击“下一步”继续。

   将打开“许可协议”对话框。

4. 滚动阅读并接受许可协议，然后单击“下一步”。

   将打开“目标位置”对话框。

5. 单击“下一步”以在默认目录中安装 SDConnector。默认目录为 C:\Program Files\CA\SDMConnector (Windows) 或 /usr/SDMConnector（Solaris 和 Linux）。

   要在默认文件夹以外的位置中安装 SDConnector，请单击“选择”，选择一个文件夹，然后单击“下一步”。“选择”按钮仅针对本地安装显示（而不用于非本地、远程安装）。

   注意：您不能将 SDConnector 安装到名称中包含空格的目录中。

   将打开“安装前摘要”对话框。

6. 单击“安装”。

   将打开“安装 SPECTRUM_SDM_Connector”对话框。在安装 SDConnector 之后，状态更改为“安装完成”，且“完成”按钮处于启用状态。

7. 单击“完成”。

   此时对话框关闭。

8. 在初始“安装”对话框上单击“关闭”。

   SDConnector 便已安装在此主机上。SDConnector 是作为服务安装的，会在每次重新启动系统时自动启动。

   注意：您还可以检查位于 SDConnector 安装目录中的安装日志，以验证是否已成功完成安装。

安装文件

注意在安装过程中创建的以下目录和文件。

在 SpectroSERVER 上

CA Spectrum 安装过程在 SpectroSERVER 上的 *<$SPECROOT>*/SDM 目录中安装下列 Secure Domain Manager 目录和文件：

cert

此目录是存放您为 SDManager 创建的 SSL 证书的存储库。

Logs

此目录包含将配置文件导入 SpectroSERVER 时生成的输出日志。所执行工作的详细信息， 包括发生的任何错误，均包含在日志文件中。

README

此文件提供有关如何在 SpectroSERVER 主机上配置 Secure Domain Manager 的详细信息。

在 SDConnector 主机上

SDConnector 安装过程在 SDConnector 主机上的 SDMConnector 目录中安装下列目录和文件：

bin

此文件夹包含以下使用 SDConnector 时所需的项：

cert

此目录是存放您为 SDConnector 创建的 SSL 证书的存储库。

README

此文件提供有关如何在 SDConnector 主机上配置 SDConnector 进程的详细信息。

SdmConnectorService[.exe]

SDConnector 的可执行文件。

使用证书

默认情况下会为 SDManager 和 SDConnector 加载证书。这允许您使用 SSL 加密保护跨非安全网络在 SDManager 与 SDConnector 主机之间传输的 ICMP 和 SNMP（SNMPv1、SNMPv2c 和 SNMPv3）数据。如果您不希望对网络环境中的任何 SDManager-SDConnector 连接使用 SSL 加密，可以在 SDManager 和 SDConnector 的配置文件中包括非安全选项。有关如何使用非安全选项的详细信息，请参阅配置 SDConnector 进程设置 (p. 23)。

升级时删除旧证书文件

从早于 9.*x* 的版本升级 Secure Domain Manager 时，请删除旧的证书文件。旧证书（早于 9.*x*）无法用于此版本的 Secure Domain Manager。删除默认情况下为早期版本的 Secure Domain Manager 安装在 SDManager 主机上的 <*$SPECROOT*>/SDM/srconf/mgr 目录中的下列证书文件：

- snmpricacert.pem：主证书颁发机构
- dsspmastercert.pem：SDManager 证书颁发机构
- dsspremotecert.pem：SDConnector 证书颁发机构

创建证书

Secure Domain Manager 使用数字证书确保安全性。默认证书随 CA Spectrum 安装提供，而站点特定的证书可以使用 CertGen 工具创建。

默认证书

如果您希望使用默认证书，请不要执行任何操作。所有默认文件都驻留在 <*$SPECROOT*>/SDM/cert 目录中，包括下列文件：

SDMCA.pem

证书颁发机构。将此文件分发给以任何容量使用 Secure Domain Manager 或 Secure Domain Connector 的任何计算机，可将其视为受信任的 CA 文件。

SDMCAKey.pem

CA 的私钥。它可用于颁发证书，但不必将其分发到所有计算机。

SDMCert.p12

由 SDMCA.pem 签名的应用程序证书。此证书文件在 SDManager 与 SDConnector 之间使用。应当谨慎地将其分发给值得信任的计算机，其用于断言这些计算机的身份。

CertGen[.exe]

用于生成站点特定的证书颁发机构、密钥文件和证书文件的程序。运行 CertGen -h 可查看所有可用的证书选项。

openssl[.exe]

SSL 协议的 OpenSSL 开源实现。

站点特定的证书

如果您希望创建站点特定的证书，请将默认证书文件（*.pem 和 *.p12）移至硬盘驱动器上的其他位置。执行以下过程以创建和部署自定义证书。

创建站点特定的证书

创建站点特定的证书以获取更好的安全性。在仅专业人员可以访问的单台计算机上创建这些证书。此计算机可以是 SDManager 主机。

重要说明！您必须具有管理员权限或 root 用户权限才能为 Secure Domain Manager 创建 SSL 证书。

遵循这些步骤:

1. 运行以下命令，创建证书颁发机构证书和证书颁发机构证书的私钥：

   ```
   CertGen -t ca -c US
   ```

   您只需执行此步骤一次，为组织创建必要的证书颁发机构证书。

   将创建以下文件：

   SDMCA.pem

   SDMCAKey.pem

   注意：与 Secure Domain Manager 一起提供的默认证书颁发机构和密钥文件都是只读文件。如果您接收到权限错误，请检查用户权限，或者将 SDMCA.pem 和 SDMCAKey.pem 移至其他位置并再次运行该命令。

2. 运行以下命令，为 SDManager 创建证书：

   `CertGen -t cert -c <国家/地区代码>`

   将创建 SDMCert.01.p12 文件。

3. （可选）为了增加安全性，请使用 -p 选项生成带有密码的证书，如下所示：

   `CertGen -t cert -p <密码> -c <国家/地区代码>`

   在 sdc.config 文件和 sdm.config 文件中输入密码。

4. 将 SDMCert.01.p12 重命名为 SDMCert.p12。

   新的站点特定证书就可使用了。

部署站点特定的证书

在创建证书文件之后，执行以下任务：

- 在 SDManager 主机和 SDConnector 主机上部署证书文件。
- 重新启动 SDManager 主机上的 SpectroSERVER 和 SDC 主机上的 SDConnector 进程。

要部署证书，请将您创建的 SDMCA.pem 文件复制到 SDManager 主机上的 <*$SPECROOT*>/SDM/cert 目录以及将连接到 SDManager 主机的 SDConnector 主机上 SDConnector 安装下的 cert 目录中。管理员或 root 用户应当拥有 SDMCert.p12 文件。

重要说明！在您计划创建更多证书的计算机上保留 SDMCAKey.pem 文件。仅限授权人员使用该文件。此计算机可以是 SDManager 主机，但这不是必需的。

在部署这些证书之后，重新启动 SDManager 主机上的 SpectroSERVER 和 SDC 主机上的 SDConnector 进程。有关重新启动 SDConnector 进程的信息，请参阅在 Windows 上启动、停止和重新启动 SDConnector 进程 (p. 29)或在 Solaris 和 Linux 上启动、停止和重新启动 SDConnector 进程 (p. 29)。

配置 SDConnector 进程设置

本节描述您可以在 SDConnector 配置文件 (sdc.config) 中设置的配置选项。此配置文件在启动时读取，并在此时应用指定的选项。sdc.config 中只能接受一行选项。下面是来自 sdc.config 文件的一个示例行。它指定 SDConnector 将接受来自 SDManager (192.168.0.2) 的连接：

```
-accept 192.168.0.2
```

配置 SDConnector 设置

1. 使用文本编辑器在 SDConnector 主机上的 SDMConnector\bin 目录中创建（如果已存在，请打开）名为“sdc.config”的文件。
2. 根据您的特定需求，在文件中的一行上添加并指定下列选项的详细信息：

-accept remote_ipaddr:[local_port]

接受来自位于地址 *<ip>* 和本地端口号 *<port>* 的主机上运行的 SDManager 的连接。连接必须源自指定的 IP 地址；否则，将忽略连接尝试。

如果指定此选项，则连接到此 SDConnector 的 SDManager 在其配置文件 (sdm.config) 中必须具有指定此 SDConnector 的 *<ip>* 的 -remoteconnect 选项。此外，如果指定此选项，则无法连接 (-connect) 到该 SDManager。

-buffersize *<size>*

指定发送与接收套接字缓冲区的大小（以字节为单位）。

默认值：262144（256k，这在大多数部署中应该足够了）

-certdir *<dir>*

如果 SSL 证书（应用程序证书、私钥和证书颁发机构证书）没有位于默认目录 (/cert) 中，则为其指定该目录。

如果指定 -nosecure 选项，则不访问证书。

-certpassword <passwd>

提供证书密码。如果您正在使用 Secure Domain Manager 附带的默认证书，则不必提供 -certpassword。否则，使用此选项提供证书密码。如果密码包含空格，则必须用引号（“”）将其括起来。CA Spectrum 假定将加密应用程序证书的密码。

注意：如果使用 -certpassword，则必须为 config 文件中声明的第一个选项。

-connect remote_ipaddr:[remote_port]

连接到位于 IP 地址 *<ip>* 和端口 *<port>* 的主机上运行的 SDManager。如果未指定 *<port>*，则假定其为 6844。

如果指定此选项，则此 SDConnector 连接到的 SDManager 在其配置文件 (sdm.config) 中必须具有指定此 SDConnector 的 IP 地址的 -remoteaccept 选项。

如果指定此选项，则此 SDConnector 无法从指定的 SDManager (sdm.config) 接受 (-accept) 连接，也无法从其侦听 (-listen) 连接。

-keepalive *<n>*

当 SDManager 或 SDConnector 发出小型消息以验证网络连接是否仍为活动状态时，更改默认内部超时（以秒为单位）。如果 SDManager 或 SDConnector 在三倍的 *<n>* 值之内都不能收到另一方的消息，则将终止连接。

默认值：10 秒

-listen [port]

默认情况下，SDConnector 在端口 6844 上侦听来自任何 SDManager 的连接请求。但如果指定 -connect 或 -accept 选项，则默认情况下 SDConnector 不再侦听。

在 -listen 选项中指定的端口优先于在 -accept 选项中指定的端口。也就是说，如果某个端口是在 -listen 选项中指定的，将不为该端口的源 IP 地址执行任何验证。

注意：-listen 和 -listen6 互斥。

-listen6 [local_port]

接受来自给定端口上任何 IPv6 SDManager 的连接。

注意：-listen 和 -listen6 互斥。

-loglevel fatal|error|warning|info|debug

指定要记录的消息类型。

默认值：警告（还包括错误和致命）

-maxlogsize *<n>*

设置最大 sdmLog.log 大小（以兆字节为单位）。

默认值：5M

最小值：1M

-nosecure

禁用安全套接字层 (SSL) 安全性（默认情况下启用）。如果在任何 -connect 或 -accept 条目之前使用了 -nosecure 选项，则为所有连接禁用 SSL。否则，您可以在每个 -connect 或 -accept 条目之后指定 -nosecure 选项，它将仅与该条目有关。

如果请求了 SSL 安全性，则加密数据流，并实施相互加密身份验证。如果 SDManager 或 SDConnector 请求安全性，那么在该连接上安全性为强制性的。

-trappoll <*n*>

每隔 <*n*> 秒向 SDManager 转发一次陷阱。

默认值：15 秒

-withfips

指定使用 FIPS 模式运行。默认情况下，FIPS 模式处于关闭状态。

注意：如果创建了空的 sdc.config，SDConnector 将在端口 6844 上侦听来自任何 SDManager 的连接；SDManager 将启动该连接。

3. 保存并退出文件。

SDConnector 即已配置。

注意：在每次更新 sdc.config 文件时，都必须重新启动 SDConnector 进程。

配置 SDManager 进程设置

SDManager 配置文件 (sdm.config) 指定 SDManager 进程的操作设置。默认情况下，会禁用 SDManager 进程。在创建 sdm.config 文件并根据需要配置该文件之后，SDManager 进程才会运行。在首次配置 sdm.config 文件之后，或者在修改其设置的任何时候，都必须将它导入 CA Spectrum，以便 SDManager 设置在 SpectroSERVER 上生效。有关详细信息，请参阅导入 SDManager 配置文件 (p. 31)。您可以在启动 SpectroSERVER 之前或之后配置 sdm.config。

sdm.config. 中只能接受一行选项。下面是来自 sdm.config. 的一个示例选项行。它指定到两个 SDConnector（172.24.148.196 和 172.19.32.199）的连接 (-remoteconnect)：

```
-remoteconnect 172.24.148.196 -remoteconnect 172.19.32.199
```

注意：如果使用 -nosecure 选项启动一个或多个 SDConnector 进程，则必须在 SDManager 选项中为相应的 -remoteconnect/-remoteaccept 条目指定相同的 -nosecure 选项，或者仅在所有 -remoteconnect/-remoteaccept 条目之前指定 -nosecure，以便为所有连接禁用 SSL。

配置 SDManager 设置

1. 使用文本编辑器在 SpectroSERVER 主机上的 <*SPECROOT*>\SDM 目录中创建（或打开，如果其已存在）名为“sdm.config”的文件。
2. 根据您的特定需求，在文件中的一行上添加并指定下列选项的详细信息：

   -apiclientport [port]

   设置用于侦听 API 客户端连接的端口。此参数仅适用于独立的 SDManager 进程。

   -buffersize <*size*>

   指定发送与接收套接字缓冲区的大小（以字节为单位）。

   默认值：262144（256k，这在大多数部署中应该足够了）

   -certdir <*dir*>

   如果 SSL 证书（应用程序证书、私钥和证书颁发机构证书）没有位于默认目录 (/cert) 中，则为其指定该目录。

   如果指定 -nosecure 选项，则不访问证书。

   -certpassword <passwd>

   提供证书密码。如果您正在使用 Secure Domain Manager 附带的默认证书，则不必提供 -certpassword。否则，使用此选项提供证书密码。如果密码包含空格，则必须用引号（“”）将其括起来。CA Spectrum 假定将加密应用程序证书的密码。

   注意：如果使用 -certpassword，则必须为 config 文件中声明的第一个选项。

   -clientServiceThreads <*n*>

   设置每个客户端用于处理请求的线程数。此参数仅适用于独立的 SDManager 进程。

   -keepalive <*n*>

   当 SDManager 或 SDConnector 发出小型消息以验证网络连接是否仍为活动状态时，更改默认内部超时（以秒为单位）。

   默认值：10 秒

   如果 SDManager 或 SDConnector 在三倍的 <*n*> 值之内都不能收到另一方的消息，则将终止连接。

   -loglevel fatal|error|warning|info|debug

   指定要记录的消息类型。

   默认值：警告（还包括错误和致命）

-maxapiconnections <*n*>

将 API 客户端连接的最大数目设置为 <*n*>。此参数仅适用于独立的 SDManager 进程。

-maxlogsize <*n*>

设置最大 sdmLog.log 大小（以兆字节为单位）。

默认值：5M

最小值：1M

-nosecure

禁用安全套接字层 (SSL) 功能（默认情况下启用）。如果在任何 -remoteconnect 或 -remoteaccept 条目之前使用了 -nosecure 选项，则为所有连接禁用 SSL。否则，您可以在每个 -remoteconnect 或 -remoteaccept 条目之后指定 -nosecure 选项，它将仅与该条目有关。

如果请求了 SSL 安全性，则加密数据流，并实施相互加密身份验证。如果 SDManager 或 SDConnector 请求安全性，那么在该连接上安全性为强制性的。

-remoteaccept (-rema) remote_ipaddr[:local_port]

接受来自位于地址 <*ip*> 和本地端口号 <*port*> 的主机上运行的 SDManager 的连接。您必须指定 SDConnector 的公共 IP 地址。

如果指定此选项，则连接到此 SDManager 的 SDConnector 在其配置文件 (sdc.config) 中必须具有指定此 SDManager 的 IP 地址的 -connect 选项。此外，如果指定此选项，则无法连接 (-remoteconnect) 到 SDConnector (sdc.config)。

-remotebackup (-remb) remote_ipaddr[:remote_port]

使用 SDConnector 的公共 IP 地址，在容错 Secure Domain Manager 设置中指定备份 SDConnector。有关详细信息，请参阅在容错环境中设置进程 (p. 41)。

-remoteconnect (-remc) remote_ipaddr[:remote_port]

连接到位于 IP 地址 <*ip*> 和 <*port*> 的主机上运行的 SDManager。如果未指定 <*port*>，则假定其为 6844。您必须指定 SDConnector 的公共 IP 地址。

如果指定此选项，则此 SDManager 连接到的 SDConnector 在其配置文件 (sdc.config) 中必须具有指定此 SDManager 的 -accept 选项或 -listen 选项。此外，如果指定此选项，则无法接受来自此配置文件中指定 SDConnector 的连接 (-remoteaccept)。

-withfips

指定使用 FIPS 模式运行。默认情况下，FIPS 模式处于关闭状态。如果将配置从 FIPS 模式更改为非 FIPS 模式(或者从非 FIPS 模式更改为 FIPS 模式），则必须重新启动应用程序。

注意：如果 sdm.config 文件为空，则会禁用 SDManager 进程。

3. 保存并关闭 sdm.config 文件。

   SDManager 即已配置。

详细信息：

导入 SDManager 配置文件 (p. 31)

在 Windows 上启动、停止和重新启动 SDConnector 进程

使用服务管理器启动、停止或重新启动 SDConnector 进程。名称“Secure Domain Connector”下列出了 SDConnector 进程。

在 Solaris 和 Linux 上启动、停止和重新启动 SDConnector 进程

要启动 SDConnector 进程，请以 root 用户身份登录，打开命令行控制台，并输入以下命令：

```
$ cd /etc/init.d
$ ./sdmconnector start
```

要停止 SDConnector 进程，请发出 **./sdmconnector stop** 命令。

要重新启动 SDConnector 进程，请发出 **./sdmconnector restart** 命令。

第 3 章： 使用 Secure Domain Manager

本章描述如何将 SDManager 配置文件 (sdm.config) 导入 CA Spectrum 以及如何在安全域中为 SDConnector 主机和设备建模。本章还描述用于查找 Secure Domain Manager 组件的 OneClick 工具。这些组件用于在安全域中 ping 设备。Ping 设备以查看设备 MIB，并查看有关 SDManager 和 SDConnector 模型的信息。

此部分包含以下主题：

导入 SDManager 配置文件

在您可以开始将 OneClick 与 Secure Domain Manager 产品结合使用之前，在希望更新 SDManager 配置时，将 sdm.config 文件导入 CA Spectrum。有关设置 sdm.config 参数的信息，请参阅配置 SDManager 进程设置 (p. 26)。

注意：您可以在为 SDConnector 主机创建模型之前或之后，导入 SDManager 配置文件。但是，如果您在为 SDConnector 主机创建模型之前导入 sdm.config 文件，CA Spectrum 会自动将主机建模为 SDConnectorProcess 模型类型。有关建模选项的详细信息（包括如何将 SDConnector 建模为 Pingable 模型类型和 Host_Device 模型类型），请参阅为 SDConnector 主机建模 (p. 32)。

导入 SDManager 配置文件

1. 单击 OneClick 控制台“导航”面板中的“Secure Domain Manager ”。
2. 单击“组件详细信息”面板中的“信息”选项卡并展开“配置”子视图。
3. 单击“导入”。

   将打开“导入 Secure Domain Manager 配置”确认对话框。

4. 单击“是”以确认您希望导入 SDManager 配置文件 (sdm.config)。

   “导入 Secure Domain Manager 配置”对话框指示导入是否成功开始。该对话框还提供用于检查输出日志以确定导入是否运行的信息。SDM/Logs 目录中的导入日志文件提供故障排除信息。此信息用于在导入失败后修复错误。

5. 单击“确定”。

   如果已正确导入配置文件，则“Secure Domain Manager 状态”字段显示“已配置”。如果导入了不包含用于定义如何在 SDManager 与 SDConnector 之间建立连接的参数的 sdm.config 文件，则会禁用 SDManager，并且“Secure Domain Manager 状态”字段显示“未配置”。

   注意： 如果在 SpectroSERVER 未运行时编辑 sdm.config 文件，则 SpectroSERVER 在启动时会自动导入新的 sdm.config 文件。您可以通过检查最新的日志文件来验证导入是否成功。

为 SDConnector 主机建模

使用 OneClick 拓扑视图中的“按类型建模”选项将 SDConnector 主机建模为以下三种模型类型之一：

SDConnectorProcess

SDConnectorProcess 模型类型是 SDConnector 的默认模型类型。此模型类型不允许您管理设备状态，但允许您查看 OneClick Secure Domain Manager 模型层次结构中表示的主机，并提供访问 SDConnector 模型信息视图 (p. 39)中所讨论视图的权限。

注意： 将可明确标识主机的有意义的名称用于 SDConnector 主机模型。OneClick 的 Secure Domain Manager 视图中显示了模型名称。

Host_Device

如果主机正在运行 SNMP 代理，则使用 Host_Device 模型类型。

Pingable

如果主机仅支持 ICMP，则使用 Pingable 模型类型。

如果使用 Host_Device 或 Pingable 模型类型，则可以监控主机的状态。有关通过将 SDConnector 主机建模为 Host_Device 或 Pingable 模型来充分利用 CA Spectrum 故障隔离功能的详细信息，请参阅 SDConnector 建模和 CA Spectrum 故障隔离 (p. 33)。

SDConnector 建模注意事项

- 默认情况下，如果在您最初导入 SDManager 配置文件之前，没有为计算机创建模型，那么 CA Spectrum 会自动将 SDConnector 主机建模为 SDConnectorProcess 模型类型。
- 如果您希望将主机建模为 Pingable 或 Host_Device，则在导入之前将主机建模为首选类型。或者，在导入之后销毁 SDConnectorProcess 模型。然后，将主机建模为 Pingable 或 Host_Device。

  注意：如果您使用“按 IP 地址创建模型”选项创建表示 SDConnector 主机的模型，而不首先销毁现有的 SDConnectorProcess 模型，那么 CA Spectrum 会复制 SDConnectorProcess 模型并将其粘贴到从中调用“按 IP 地址创建模型”选项的拓扑视图中。

- 在 OneClick 中销毁 SDConnector 主机模型不会阻止 CA Spectrum 将实际 SDConnector 用于设备通信。只能通过重新导入 SDManager 配置（在编辑 sdm.config 文件以删除 SDConnector 之后）销毁 SDConnector。
- 如果您意外地销毁了 SDConnectorProcess 模型，则在下次导入 SDManager 配置文件时，CA Spectrum 会重新创建该模型。如果您销毁了 Pingable 模型或 Host_Device 模型，则在下次导入 SDManager 配置文件时，CA Spectrum 将创建 SDConnectorProcess 模型。如果您希望还原 Pingable 模型或 Host_Device 模型，则显式重新创建该模型，然后导入配置文件。

SDConnector 建模和 CA Spectrum 故障隔离

如为 SDConnector 主机建模 (p. 32)中所述，在为 SDConnector 建模时，可以选择下列模型类型之一：

- SDConnectorProcess
- Host_Device
- Pingable

我们建议您将 SDConnector 主机建模为 Host_Device 或 Pingable 模型类型。当远程 SDConnector 进程关闭或失去连接时，此模型类型可允许 CA Spectrum 故障隔离正常工作。CA Spectrum 完全确定停机原因与 SDConnector 主机模型相关，这可从基本上消除未解决的故障警报。

虽然 SDConnector 主机主要连接到网络边缘的交换机。但在逻辑上，它是公共域与安全域区域之间的网桥，必须相应地对其进行建模。在路由公共域与安全域区域之间通信的设备的两个模型之间放置 SDConnector 主机模型。下图说明了此连接，显示 SDConnector 作为 Host_Device 模型。

在安全网络域中为设备建模

在为 SDConnector 主机建模之后，为您希望在 SDConnector 主机所在的安全域中管理的网络设备进行建模。使用 OneClick“按 IP 地址创建模型”选项或“发现”一次建模一个网络设备。您可以在拓扑视图中的任何位置放置模型。在您成功创建模型之后，CA Spectrum 可以使用 SDConnector 进程与它们通信。

按 IP 地址创建模型

使用 OneClick“按 IP 地址创建模型”选项在安全域中为每个设备建模。

注意： 有关在 OneClick 中建模的详细信息，请参阅 *《IT 基础架构建模与管理 - 管理员指南》*。

使用“按 IP 地址创建模型”选项在安全域中为设备建模

1. 在拓扑视图中单击“按 IP 地址创建模型”选项。

   将打开“按 IP 地址创建模型”对话框。

2. 在“网络地址”字段中键入您希望建模的设备的网络地址。

3. 在“安全域”下拉列表中，选择运行 SDConnector 的主机的 IP 地址，或者在您正在建模的设备所在的安全域中为 SDConnector 主机配置的名称。

   注意：您可以通过在 OneClick 中更改主机模型名称，来提供 SDConnector 主机的安全域名。有关启用安全域名作为选择选项的信息，请参阅 SDManager 模型信息视图 (p. 38)。

4. 在“SNMP 通信选项”部分中选择与您希望管理的设备兼容的 SNMP 版本。
5. 单击“确定”。

发现

使用 OneClick“发现”通过 SDConnector 主机在安全域中发现并建模所有设备。在发现具有重叠 IP 地址的设备时，请记住以下几点：

- 每次发现只能使用一个 SDConnector。
- 尽管您可以使用第 2 层映射，其有效性还是依赖于源地址和生成树表的准确性。
- “协议选项”设置：
  - 不要使用第 3 层 Autodiscovery 映射。取消选择“协议选项”对话框中的“IP 地址表”和“IP 路由器表”。
  - 不要使用 Cisco 中的专有发现协议或 Nortel 环境，因为它们使用 IP 地址传达邻居关系。取消选择“协议选项”对话框中的“专有发现表”。
  - 不要使用 Pingable 映射。取消选择“协议选项”对话框中的“可 Ping 项的 ARP 表”。

使用 SDConnector 主机发现设备

遵循这些步骤:

1. 从主菜单依次单击“工具”、“实用工具”、“发现控制台”。

   将打开“发现控制台”。

2. 完成您希望在其中建模设备的安全域的发现配置。

   注意：有关配置发现的详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

3. 单击“配置”选项卡中的“高级选项”。

   将打开“高级选项”对话框。

4. 在“发现选项”部分中，从“安全域”下拉列表选择在此安全域中运行 SDConnector 的主机的 IP 地址，或者为该安全域指定的名称。

   注意：您可以通过在 OneClick 中更改主机模型名称，来提供 SDConnector 主机的安全域名。有关启用安全域名作为选择选项的信息，请参阅 SDManager 模型信息视图 (p. 38)。

5. 单击“确定”。

   将关闭“高级选项”对话框，所做更改即会保存。

6. 单击“发现控制台”中的“发现”。

   您配置的发现将运行。在发现之后，查看其相应 SDConnector 主机图标的“Secure Domain Connector 设备表”中列出的所有设备。

   注意：如果您已使用 SDConnectorProcess 模型为运行远程 SDConnector 进程的主机建模，并在该主机所在的网络区域上执行发现，则发现功能可能使用 Host_Device 或 Pingable 模型创建该主机的其他模型。在创建此重复模型后将其删除，或者您可以从创建此模型前设置的发现结果中将其筛选掉。

关于维护设备安全域成员资格

在 NAT 环境中，多个 SDConnector 用于管理相同的 IP 范围。当存在重复的 IP 范围时，CA Spectrum 无法确定每台设备必须管理的 SDConnector。因此，请指定此信息。

在 CA Spectrum 中发现或建模新设备时，您可以使用 OneClick“按 IP 地址创建模型”视图或 OneClick“发现”设置安全域。要更新现有设备模型的安全域，请使用 OneClick 属性编辑器编辑“安全域地址”属性。这会自动更新安全域名。将新的 SDManager 配置文件 (sdm.config) 导入 CA Spectrum 后，仍将分配给旧安全域的所有现有设备分配给它。这些模型上将可能生成红色警报。

访问 Secure Domain Manager 搜索

OneClick 包括各种预定义的 Secure Domain Manager 搜索选项。

要访问 Secure Domain Manager 搜索选项，请在 OneClick 控制台的“定位器”选项卡中，展开“Secure Domain Manager”文件夹。

将显示您可以使用的预定义 Secure Domain Manager 搜索。

在安全域中检查设备可访问性

通过使用 OneClick“ping”菜单选项 ping 位于安全域中的设备，确定设备是否可访问。

注意：成功的 ping 不显示安全域中经过 ping 测试的设备返回的字节数。

要在安全域中检查设备可访问性，请右键单击您希望在 OneClick 控制台中评估其可访问性的设备，然后单击“Ping”。

将打开“Ping”对话框，其中列出了 ping 请求的结果。例如：

```
Secure reply from 10.254.1.5: icmp_seq=4. time =140. ms
```

如果此设备不在安全域中，则结果将如下所示：

```
64 bytes from 10.254.1.5: icmp_seq=4. time =140. ms
```

在安全域中查看设备 MIB

使用 MIB 工具在安全域中查看设备 MIB。首先，为设备所在的安全域指定 SDConnector。以下过程描述如何指定 SDConnector。

注意：有关使用 MIB 工具的详细信息，请参阅 *《认证用户指南》*。

遵循这些步骤:

1. 选择您希望使用 MIB 工具调查的设备。
2. 右键单击该设备并依次选择“实用工具”、“MIB 工具”。

   将打开 MIB 工具。“联系标准”使用该设备的选定 SNMP 联系信息进行了预填充。MIB 工具会尝试联系该设备。

   如果 MIB 工具*无法*联系该设备，则会显示一条错误消息，并且联系状态指示器变成红色。

   如果 MIB 工具*可以*联系该设备，则联系状态指示器变成绿色。

   还将会出现状态对话框，其中显示了检索和加载 MIB 工具数据库的进度。
3. 单击“联系标准”部分中的“高级选项”。

   将显示“MIB 工具: 高级选项”对话框。
4. 从“安全域”下拉列表中选择适用的安全域。
5. 单击“确定”。

   将关闭“高级选项”对话框，所做更改即会保存。

6. 在“联系标准”部分中单击“联系”，并验证 MIB 工具是否可以成功联系该设备。
7. 关闭 MIB 工具。

   MIB 工具将关闭，并且您已为该设备指定了 SDConnector。

SDManager 模型信息视图

“组件详细信息”面板中的“信息”选项卡在以下部分中提供了有关选定 SDManager 模型的配置控件的信息：

常规信息

“常规信息”部分提供有关 Secure Domain Manager 模型的标准信息，如模型类和安全字符串。

配置

配置部分包括以下内容：

导入

将 SDManager 配置文件 (sdm.config) 导入 CA Spectrum 中。

Secure Domain Manager 状态

指示 SDManager 的配置状态，如下所示：

- **已配置**：指示已成功导入该文件。
- **未配置**：指示从未导入自定义或编辑后的 sdm.config 文件，已导入不带参数的 sdm.config 文件，或者已导入包含错误的 sdm.config 文件。

安全域显示选项

指定 CA Spectrum 是否显示用于标识 SDConnector 主机（及其域）或 SDConnector 主机 IP 地址的名称。您可以从下拉列表中选择“显示安全域名”或“显示安全域地址”。这可确定在所有 OneClick 视图中将使用的 SDConnector 标识符类型。

本地域

指定在“安全域”列中为本地管理的模型（安全域中不包括的模型）显示的文本。

默认值：直接管理

注意：仅当安装 Secure Domain Manager 时，OneClick 列表视图中才显示“安全域”列。

Secure Domain Connector 列表

显示当前在远程网络区域中运行 SDConnector 进程的所有主机。

下图显示了选定 SDManager 模型的“组件详细信息”面板的示例：

详细信息：

导入 SDManager 配置文件 (p. 31)

SDConnector 模型信息视图

位于“组件详细信息”面板中的“信息”选项卡上提供了有关选定 SDConnector 的信息。“常规信息”和“SPECTRUM 建模信息”类别提供了有关 SDConnector 模型的标准信息。此外还有一个“Secure Domain Connector”部分，该部分包括以下子部分：

Secure Domain Connector 设备表

“Secure Domain Connector 设备表”列出了由选定 SDConnector 管理的所有设备。它还允许您打印、导出和筛选设备列表。您可以单击此列表中设备的“名称”超链接，以在拓扑视图中直接导航到该设备。

第 4 章： 在容错环境中设置进程

本章介绍如何在容错 SpectroSERVER 环境中设置 SDConnector 以连接到主要和备份 SpectroSERVER 上的 SDManager。本章还介绍如何设置主要和备份 SDConnector。

此部分包含以下主题：

在容错 SpectroSERVER 环境中设置 SDManager

在容错 SpectroSERVER 环境中，在主要 SpectroSERVER 和备份 SpectroSERVER 上安装 SDManager。将与此 SDManager 通信的每个 SDConnector 配置为连接到主要和备份 SpectroSERVER。如果主要 SpectroSERVER 失败，则备份 SpectroSERVER 接管与每个 SDConnector 的通信。

遵循这些步骤:

1. 在您希望管理的每个安全域上部署 SDConnector。

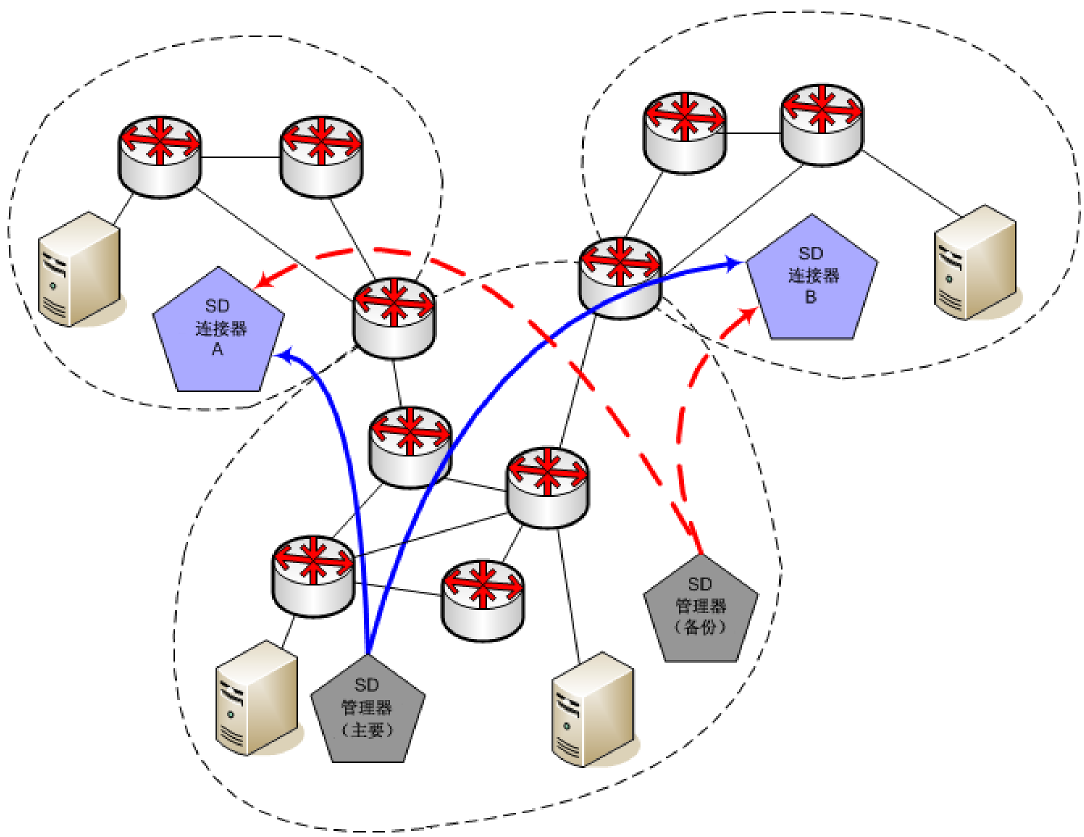
   注意：有关如何部署 SDConnector 的详细说明，请参阅安装和配置 Secure Domain Manager 进程 (p. 17)。

2. 配置每个 SDConnector 以接受来自主要 SpectroSERVER 和备份 SpectroSERVER 的连接。例如，分别为 172.24.1.2 和 172.24.3.4：

   ```
   -accept 172.24.1.2 -accept 172.24.3.4
   ```

容错 SpectroSERVER (SDManager)

下图显示如何将两个 SDConnector 连接到主要 SDManager 和备份 SDManager：



sdm.config 中两个 SDManager 的配置设置：

-remoteconnect <*SDConnector A 的 IP*> -remoteconnect <*SDConnector B 的 IP*>

sdc.config 中两个 SDConnector 的配置设置：

-accept <*主要 SDManager 的 IP*> -accept <*备份 SDManager 的 IP*>

设置容错 SDConnector

Secure Domain Manager 基于每个 SDConnector 支持备份功能。备份 SDConnector 必须能够管理主要 SDConnector 管理的所有设备，而不仅仅是它们的子集。

当您将备份配置导入 CA Spectrum 中时，不会自动为备份 SDConnector 建模。如果主要 SDConnector 关闭，备份功能将*以透明方式*进行接管。没有任何可见迹象表示，主要 SDConnector 已关闭。此外，因为没有为备份建模，所以 OneClick 控制台“按 IP 地址创建模型”或“发现配置”视图中或者 MIB 工具中不显示这些备份。

遵循这些步骤:

1. 为您希望管理的每个远程域部署主要和备份 SDConnector。

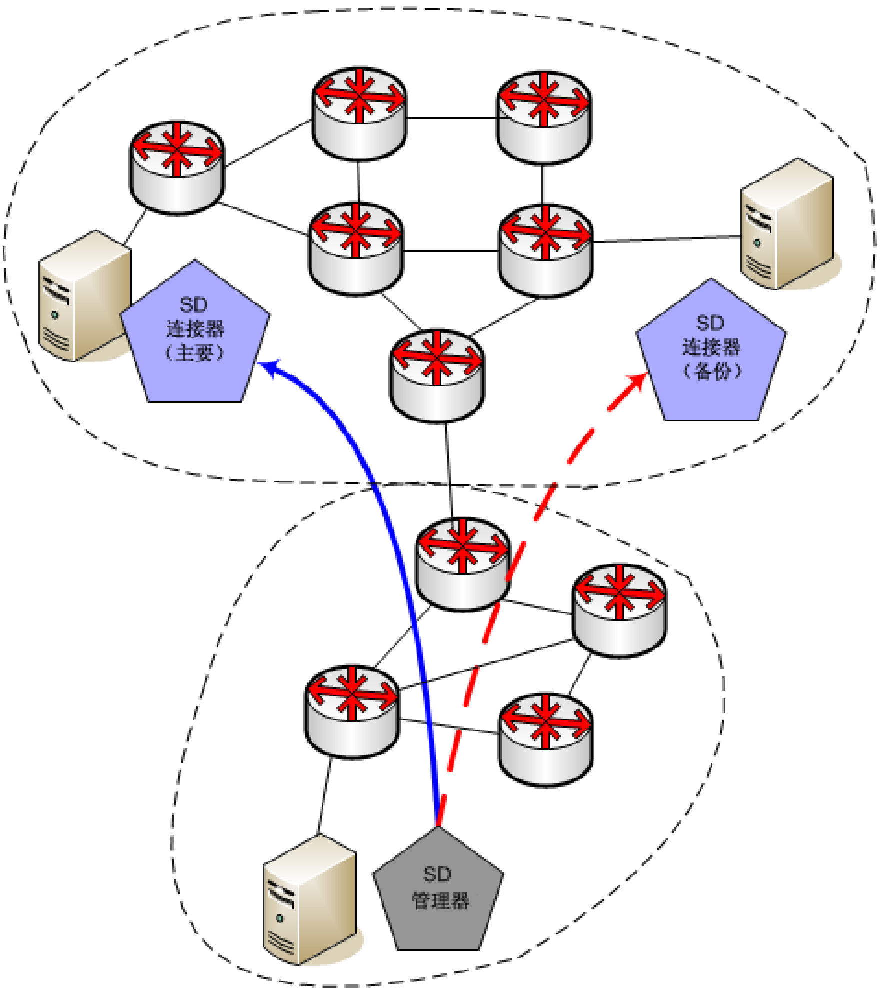
   注意：有关如何部署 SDConnector 的详细说明，请参阅安装和配置 Secure Domain Manager 进程 (p. 17)。

2. 通过修改 sdm.config 文件（如以下示例中所示），配置 SDManager 以连接到主要和备份 SDConnector：

   `-remoteconnect <主要 SDC 的 IP> -remotebackup <备份 SDC 的 IP>`

容错 SDConnector

下图描述了连接到单个 SDManager 的两个 SDConnector：



sdm.config 中 SDManager 的配置设置：

`-remoteconnect` <*主要 SDConnector 的 IP*> `-remotebackup` <*备份 SDConnector 的 IP*>

sdc.config 中两个 SDConnector 的配置设置：

`-accept` <*SDManager 的 IP*>

附录 A： Secure Domain Manager 故障排除

本节介绍了一些潜在的 Secure Domain Manager 问题及其解决方案。

此部分包含以下主题：

错误消息

本节提供有关 Secure Domain Manager 错误消息的信息。SDManager 错误显示在 SDManager.out 文件中；SDConnector 错误显示在终端显示器上。

证书无效错误

在 Linux、Solaris 和 Windows 上有效

症状：

在证书或安全设置中发现不匹配时，将显示以下 SDConnector 错误消息：

`SdmEtpkiConnectEndpoint run() invalid socket security`。将不对主机进行任何连接尝试。

请确认证书和安全配置都是正确的。

解决方案：

确认部署 SSL 的计算机具有匹配的证书。

端口冲突

SDConnector 需要自定义 SNMP 陷阱端口

在 Linux、Solaris 和 Windows 上有效

如果需要更改 SDConnector 在其上侦听 SNMP 陷阱的陷阱端口，请配置自定义侦听端口。

注意：在以下过程中，端口 951 用作新的自定义侦听端口的示例。

遵循这些步骤:

1. 通过修改 sdc.rc 文件，配置 SDConnector 在自定义端口上侦听陷阱，如下所示：

   `snmp_trap_port = 951`

2. 通过重新启动计算机来重新启动 SDConnector 进程。

   SDConnector 现在在端口 951 上侦听陷阱。

安装问题

当某些 Windows 安装上未安装 SDConnector 服务时。或者，当安装了该服务但未启动它时。那么，请手动在 Windows 上安装 SDConnector 服务。

遵循这些步骤:

1. 从命令提示符导航到以下文件夹：

   <*SDC 安装目录*>/bin

2. 运行以下命令：

   `SdmConnectorService.exe --install`

3. 从“服务”窗口启动该服务或者运行以下命令：

   `SdmConnectorService.exe --start`