Server Automation

软件版本：10.50

重要概念指南

文档发布日期：2016 年 7 月
软件发布日期：2016 年 7 月

Hewlett Packard Enterprise

法律声明

担保

HPE 产品和服务的唯一担保已在此类产品和服务随附的明示担保声明中提出。此处的任何内容均不构成额外担保。HPE 不会为此处出现的技术或编辑错误或遗漏承担任何责任。

此处所含信息如有更改，恕不另行通知。

受限权利声明

机密计算机软件。必须拥有 HPE 授予的有效许可证，方可拥有、使用或复制本软件。按照 FAR 12.211 和 12.212，并根据供应商的标准商业许可的规定，商业计算机软件、计算机软件文档与商品技术数据授权给美国政府使用。

版权声明

商标声明

Adobe® 是 Adobe Systems Incorporated 的商标。

Microsoft® 和 Windows® 是 Microsoft Corporation 在美国的注册商标。

UNIX® 是 The Open Group 的注册商标。

文档更新

本文档的标题页包含以下标识信息：

- 软件版本号，指示软件版本。
- 文档发布日期，该日期将在每次更新文档时更改。
- 软件发布日期，用于指示该版本软件的发布日期。

要检查是否有最新的更新，或者验证是否正在使用最新版本的文档，请访问：https://softwaresupport.hpe.com/。

需要注册 HPE Passport 才能登录此站点。要注册 HPE Passport ID，请单机 HPE 软件支持站点上的 **Register** 或单击“HP Passport”登录页面上的**Create an Account**。

此外，如果订阅了相应的产品支持服务，则还会收到更新的版本或新版本。有关详细信息，请与您的 HPE 销售代表联系。

支持

访问 HPE 软件支持网站，地址为:https://softwaresupport.hpe.com。

此网站提供了联系信息，以及有关 HPE 软件提供的产品、服务和支持的详细信息。

HPE 软件联机支持提供客户自助解决功能。通过该联机支持，可快速高效地访问用于管理业务的各种交互式技术支持工具。作为尊贵的支持客户，您可以通过该支持网站获得下列支持：

- 搜索感兴趣的知识文档
- 提交并跟踪支持案例和改进请求
- 下载软件修补程序
- 管理支持合同
- 查找 HPE 支持联系人
- 查看有关可用服务的信息
- 参与其他软件客户的讨论
- 研究和注册软件培训

大多数提供支持的区域都要求您注册为 HPE Passport 用户再登录，很多区域还要求用户提供支持合同。要注册 HPE Passport ID, 请单击 HPE 支持站点上的 **Register**，或单击“HP Passport”登录页面上的 **Create an Account**。

要查找有关访问级别的详细信息，请访问：https://softwaresupport.hpe.com/web/softwaresupport/access-levels。

HPE Software Solutions Now 可访问 HPSW 解决方案和集成门户网站。此网站将帮助您寻找可满足您业务需求的 HPE 产品解决方案，包括 HPE 产品之间的集成的完整列表以及 ITIL 流程的列表。此网站的 URL 为 https://softwaresupport.hpe.com/。

内容

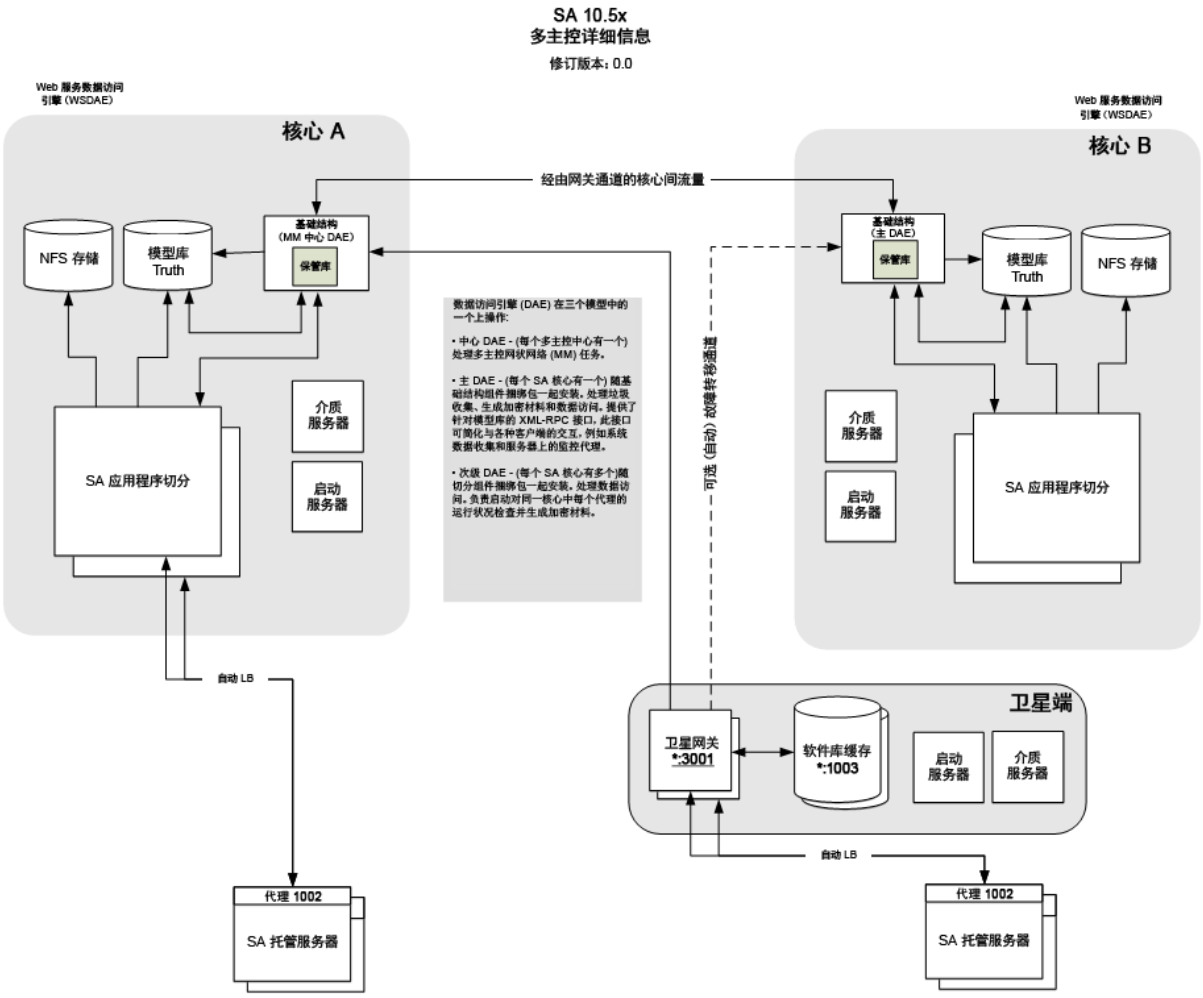
主要概念

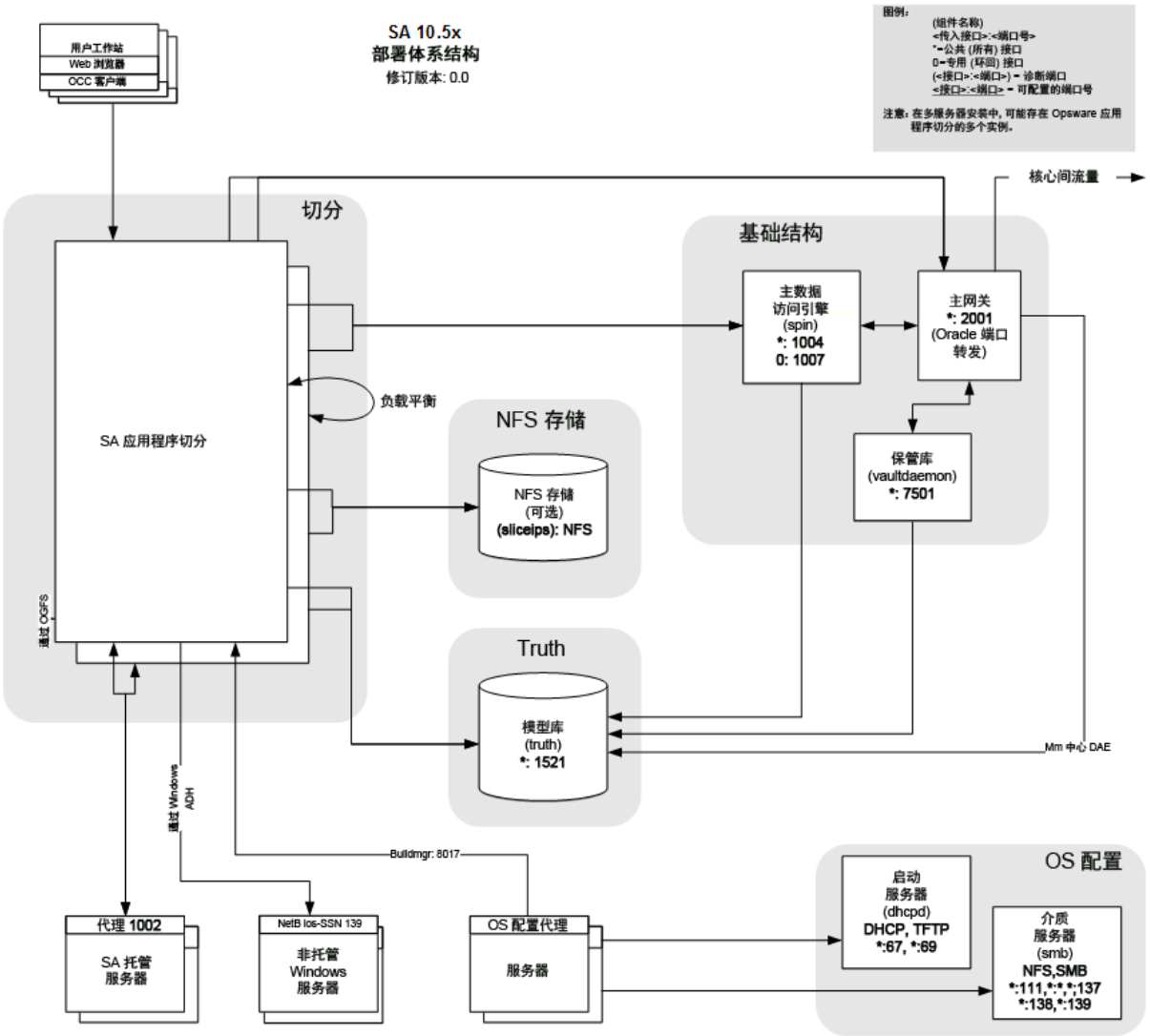
Server Automation (SA) 是数据中心自动化软件，用于集中和简化多个数据中心功能，以及自动化数据中心服务器管理的关键区域。

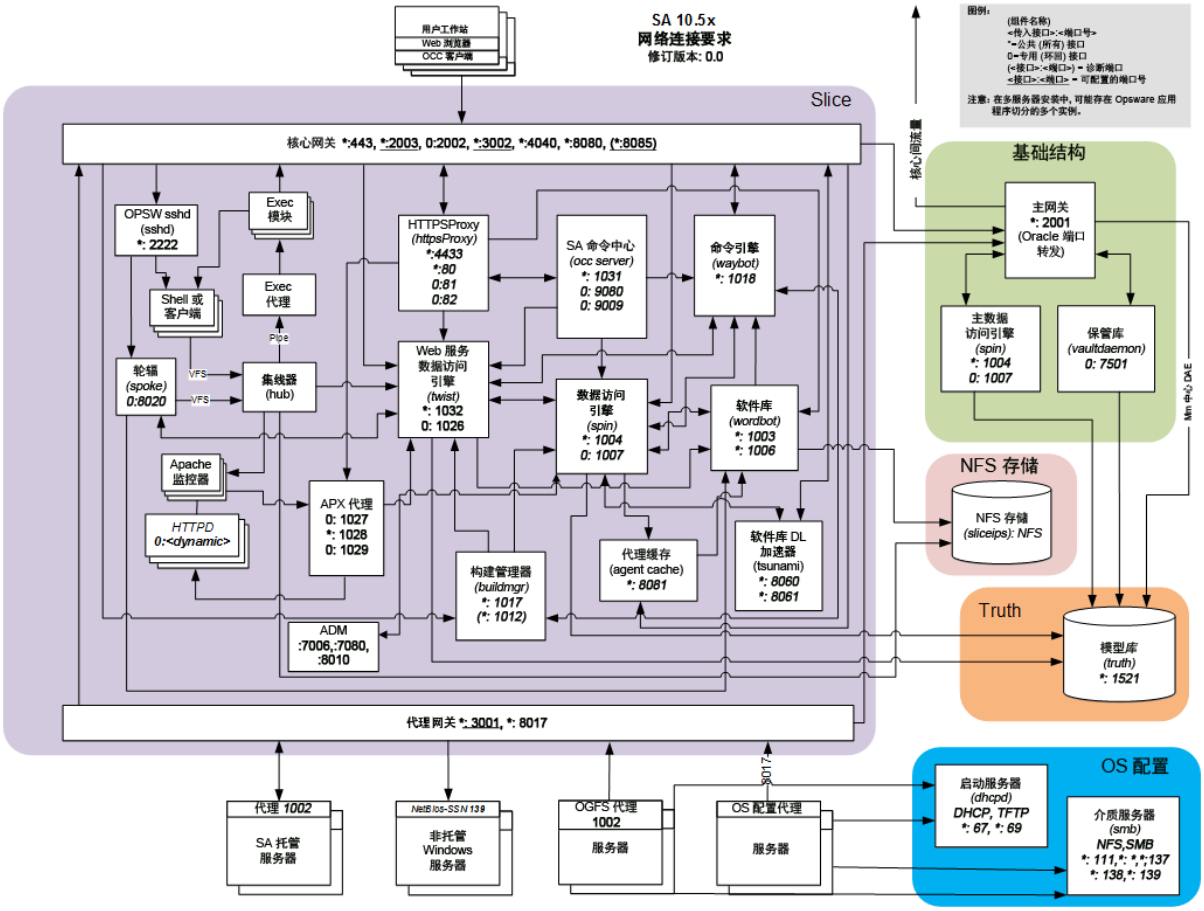
以下主题提供 SA 的详细信息：

体系结构

本节适用于希望更加深入了解 SA 体系结构的用户，这些用户希望自定义 SA 核心布局、创建多主控网状网络、进行远程数据库安装等。您将了解 SA 核心及其核心组件，以及核心、服务器代理和卫星端之间的关系。




SA 10.5x
部署体系结构
修订版本: 0.0
图例:
(组件名称)
<传入接口>:<端口号>
*=公共 (所有) 接口
0=专用 (环回) 接口
(<接口>:<端口>) = 诊断端口
<接口>:<端口> = 可配置的端口号
注意: 在多服务器安装中, 可能存在 Opsware 应用程序切分的多个实例。
用户工作站
Web 浏览器
OCC 客户端
核心间流量
切分
SA 应用程序切分
负载平衡
通过 OGFS
基础结构
主数据访问引擎 (spin)
*: 1004
0: 1007
主网关
*: 2001
(Oracle 端口转发)
保管库 (vaultdaemon)
*: 7501
NFS 存储
NFS 存储 (可选)
(sliceips): NFS
Truth
模型库 (truth)
*: 1521
Mm 中心 DAE
通过 VMotions 的 ADV
Buildmgr: 8017
代理 1002
SA 托管服务器
NetB los-SSN 139
非托管 Windows 服务器
OS 配置代理
服务器
OS 配置
启动服务器 (dhcpd)
DHCP, TFTP
*:67, *:69
介质服务器 (smb)
NFS,SMB
:111,:*,*:137
:138,:139



SA 核心

SA 核心是一个核心组件集，这些组件协同合作以支持您发现网络上的服务器、将这些服务器添加到托管服务器池，然后从 SA 客户端界面对服务器进行配置、修补、监控、审核和维护。SA 客户端提供单个界面，用于访问 SA 的所有信息和管理功能。

安装核心组件的服务器称为核心服务器。即使核心组件分布到多个主机，这些组件仍然被视为单个 SA 核心的一部分。

可将所有核心组件均安装在单个主机上，也可将其分布于多个主机，但是典型的 SA 安装使用核心组件绑定，这会将某些组件一起安装在同一台服务器上，以提高性能和方便维护。有关组件绑定的详细信息，请参见 SA 核心组件绑定。

为了进行通信和执行某些服务器管理活动，SA 在每个托管服务器上安装服务器代理，并通过网关 (SA 核心组件的一部分) 与托管服务器进行通信。服务器代理还会根据来自 SA 客户端 的用户输入所示，对托管服务器执行某些操作。

SA服务器代理

SA 服务器代理是安装在要求 SA 管理的所有服务器上的智能软件。在无代理服务器上安装代理后，此代理将使用 SA 核心注册此服务器，之后核心会将该服务器添加到其托管服务器池。SA 代理还会从核心接收用户启动命令，并对其所在的服务器执行适当操作，例如软件安装和删除、软件和硬件配置、服务器状态报告、审核等。

可采用以下方式在服务器上安装 SA 代理：

可使用 SA 代理部署工具 (ADT) 发现网络上尚未安装 SA 服务器代理的服务器(无代理服务器)，并在这些服务器上安装代理。有关 ADT 的详细信息，请参见《SA 10.50 用户指南》。

可使用 SA 配置将操作系统配置到裸机服务器 - 使用此操作系统安装 SA 服务器代理。请参见《SA 10.50 管理指南》。

可将 SA 服务器代理二进制文件复制到服务器，并手动安装它。请参见《SA 10.50 用户指南》。

在注册代理期间，SA 为每台服务器分配一个唯一的 ID(计算机 ID (MID))，并将此 ID 存储在模型库中。服务器也可由其 MAC 地址进行唯一标识(网络接口卡的唯一十六进制硬件标识符，用作网络上设备的物理地址)。

核心组件

核心组件是 SA 核心的重要组成部分，它们使服务器的监控和管理成为可能。在检索有关网络服务器的重要信息、配置服务器、应用修补程序、将服务器联机或脱机、配置和审核服务器和执行更多操作时，此交互将由核心组件进行控制。

下节将描述 SA 核心组件和接口。有关 SA 组件如何协同合作管理服务器的详细信息，请参见《SA 10.50 管理指南》。

模型库

模型库要求具有 SA 提供的 Oracle 数据库，或者进行符合 SA 数据库要求的现有 Oracle 安装。有关这些要求的详细信息，请参见《SA 10.50 安装指南》。

模型库是独立的组件，不与其他核心组件一起绑定。所有 SA 组件从为所有 SA 托管服务器维护的数据模型开始运行或者更新该数据模型。模型库可存储以下信息：

- 受 SA 管理的所有服务器的库存。
- 与这些服务器关联的硬件库存，包括内存、CPU、存储容量等。
- 有关托管服务器配置的信息。
- 托管服务器上安装的操作系统、系统软件和应用程序的库存。
- SA 配置操作系统安装介质库存(介质自身存储在 SA 配置介质服务器中)。
- 可用于安装的软件和可控制如何配置和安装软件的软件策略的库存。软件安装介质自身存储在软件数据库中。
- 身份验证和安全信息。

SA 核心组建绑定

某些 SA 核心组件绑定在一起，在典型安装期间必须作为一个单元进行安装。如果有必要，可将某些组件(例如数据库存储、SA 配置介质服务器以及其他组件)从捆绑包中分离出来，通过执行自定义安装将这些组件安装在其他主机上。但是，更加复杂的安装 (例如分布式核心组件的安装) 则需要 HPE 专业服务或 HPE 认证顾问的服务，客户安装不支持此类安装。

下表显示了 SA 组件捆绑包及其构成的组件。请注意，可以安装切分组件捆绑包的多个实例，以帮助实现工作负载平衡。

组件分布

模型库	基础结构组件	SA 配置组件	切分组件 #1	切分组件 #x
每个核心分布一个	每个核心分布一个	通常每个核心分布一个	每个核心分布一个	每个核心分布多个
模型库	管理网关 主数据访问引擎 模型库多主控组件 软件数据库存储 (可位于其他主机)	介质服务器 (仅限操作系统序列) 启动服务器 (仅限操作系统序列)	核心网关/代理网关 命令中心 全局文件系统 Web 服务数据访问引擎 次级数据访问引擎 构建管理器 命令引擎	核心网关/代理网关 命令中心 全局文件系统 Web 服务数据访问引擎 次级数据访问引擎 构建管理器 命令引擎

模型库	基础结构组件	SA 配置组件	切分组件 #1	切分组件 #x
			软件数据库 HPE Live Network (HPELN) DCML 交换工具 (DET) 软件数据库加速器 (tsunami) Memcache	软件数据库 HPE Live Network (HPELN) DCML 交换工具 (DET) 软件数据库加速器 (tsunami) Memcache

SA 核心组件绑定提供以下优点：

- 使多服务器部署变得更加简单和稳定
- 可安装其他切分组件捆绑包以实现横向扩展
- 改进的高可用性
- 安装多个实例之后保持切分之间的负载平衡

有关 SA 核心组件体系结构和交互的相信信息，请参见《SA 10.50 重要概念指南》。

启动代理 与服务器代理不相关，它作为 SA 配置的一部分执行操作。

核心组件绑定

基础结构组件捆绑包

- **主数据访问引擎**
  数据访问引擎提供了针对模型库的 XML-RPC 接口，此接口可简化与各种客户端的交互，系统数据收集和服务器上的监控代理。随基础结构组件捆绑包一起安装的数据访问引擎被指定为主 数据访问引擎。随切分组件捆绑包一起安装的数据访问引擎被指定为次级 数据访问引擎。

  由于与模型库的交互通过数据访问引擎进行，因此模型库架构的更改对客户端的影响较小。数据访问引擎支持向 SA 添加功能，而无需进行系统范围内的更改。

- **管理网关**
  管理与其他 SA 核心和卫星端的通信。

- **模型库多主控组件**
  模型库多主控组件随基础结构组件捆绑包一同安装。根据定义，多主控网状网络包含多个核心安装，模型库多主控组件可为网状网络中的所有核心同步模型库中的数据，将一个库中所做的更改传播到其他库中。

  每个模型库多主控组件由一个发送方和一个接收方构成。发送方 (出站模型库多主控组件)轮询模型库并将未发布的事务发送到其他模型库。接收方 (入站模型库多主控组件)接受来自其他模型库的事务并将其应用于本地模型库。

- **软件数据库存储**
  软件数据库存储组件可安装在托管基础结构组件捆绑包的任意服务器上。自 SA 10.50 起，软件数据库成为切分组件捆绑包的一部分，其中引入了软件数据库存储组件，该组件可用于处理 NFS 到切分组件捆绑包主机的导出。

  如果选择不安装软件数据库存储，则必须将 NAS(文件管理器)手动配置为允许切分组件捆绑包服务器访问此文件系统。

  切分组件捆绑包

  - **命令引擎**
    切分组件捆绑包的一部分。命令引擎是一个系统，用于运行分布在多台服务器的程序(通常通过 SA 服务器代理实现)。命令引擎脚本在 Python 中进行编写，在命令引擎服务器上运行。命令引擎脚本可对服务器代理执行命令。这些调用均通过安全的方式提供，并可使用模型库中存储的数据对其进行审核。

    由于可以具有多个切分组件捆绑包，因此可以拥有多个命令引擎，这大大增强了横向扩展功能。多个命令引擎实例可通过利用多个切分组件捆绑包提供的负载平衡机制，共享命令传递和脚本执行的负载。此外，还改进了故障转移和高可用性。例如，当命令引擎实例尝试将命令委派给群集中的其他节点时，如果该节点出现故障，它会将故障转移到下一个节点。

    SA 可使用命令引擎脚本来执行功能。

  - **软件数据库**
    切分组件捆绑包的一部分。此组件是一个库，其中上载和存储了用于软件/应用程序配置和修正的二进制文件/包/源。其相关组件为随基础结构组件捆绑包一起安装的软件数据库存储，该组件可处理 NFS 到切分组件捆绑包主机的导出。

    SA 支持软件数据库镜像。您可以控制在网状网络中被指定为镜像的软件数据库，并通过在 SA 客户端中修改配置参数来控制镜像作业的频率。镜像不会影响卫星端软件数据库缓存。

    软件数据库镜像可能需要大量可用磁盘空间。在标准和高级安装期间，可选择关闭默认启动的镜像。

有关如何配置软件数据库镜像的详细信息，请参见《SA 10.50 管理指南》。

有关如何将软件包上载到 SA 库的信息，请参见《SA 10.50 管理指南》。

- **核心网关/代理网关**
  核心网关直接与代理网关进行通信，以传递针对核心组件的请求及其响应。
- **命令中心**
  命令中心 (OCC) 是位于 SA 客户端下的核心组件。OCC 包括一个 HTTPS 代理服务器和一个应用程序服务器。仅能通过 SA 客户端访问 OCC。
- **DCML 交换工具**
  DCML 交换工具随每个切分组件捆绑包一起安装，用于方便导入和导出 SA 内容。请参见《SA 10.50 管理指南》。
- **全局文件系统**
  全局文件系统 (OGFS) 随每个切分组件捆绑包一起安装，用于为 SA 提供中央执行环境。

  OGFS 在一个或多个物理服务器上运行；客户可通过简单地将其他切分组件捆绑包添加到核心中，来扩展 SA 的执行功能。

  OGFS 在虚拟文件系统中运行 SA 内置组件(以及客户编写的程序)，此文件系统将 SA 数据模型、SA 操作和托管服务器显示为虚拟文件和目录。

  通过 SA 的这一独特功能，全局 Shell 和自动化平台扩展 (APX) 的用户可以使用任何脚本或程序语言查询 SA 数据以及管理服务器。由于 OGFS 通过 SA 安全模型来筛选所有数据、操作和托管服务器访问，因此默认情况下，运行在 OGFS 上的程序是安全的。
- **Web 服务数据访问引擎**
  Web 服务数据访问引擎为模型库提供公用对象抽象层，并为其他核心组件提高性能。通过简单对象访问协议 (SOAP) API、第三方集成组件或者组件 (例如 SA 客户端) 的二进制协议，可访问此对象抽象。
- **次级数据访问引擎**
  数据访问引擎提供了针对模型库的 XML-RPC 接口，此接口可简化与各种客户端的交互，系统数据收集和服务器上的监控代理。随基础结构组件捆绑包一起安装的数据访问引擎被指定为主 数据访问引擎。随切分组件捆绑包一起安装的数据访问引擎被指定为次级 数据访问引擎。

  由于与模型库的交互通过数据访问引擎进行，因此模型库架构的更改对客户端的影响较小。数据访问引擎支持向 SA 添加功能，而无需进行系统范围内的更改。

- **构建管理器**
  (仅限 OS 序列)虽然构建管理器是 SA 操作系统配置的一部分，但它作为切分组件捆绑包的一部分进行安装。构建管理器帮助 OS 构建代理和命令引擎进行通信。它接受来自命令引擎的 SA 配置命令。它为特定于平台的内部版本脚本提供运行时环境，以便执行 SA 配置步骤。

- **HPE Live Network (HPELN)**
  HPE Live Network 为 Server Automation (SA)、Network Automation (NA)、Client Automation (CA)、Operations Orchestration (OO) 和 Service Automation Reporter (SAR) 提供内容更新。HPE Live Network (HPELN) 为客户提供安全策略和符合性策略，用以帮助最大化在 SA、NA 和 CA 中的投资回报，并利用可扩展的自动化平台不断提供新的自动化功能。

  在 SA 核心安装期间，HPELN 将作为切分组件捆绑包的一部分进行安装。

- **软件数据库加速器** (tsunami)
  它是一个对象存储下载加速器，用于为与基于 Linux 的 SA 核心进行直接通信的任何代理提高修正性能和扩展性。

  在两个关键区域中提高性能和扩展性：

  RPM 修正分析 - RPM 依赖关系分析/预览期间对包标题的提取速度较之先前的 SA 版本更快。

  修正包阶段 - 从软件数据库将单元下载到托管主机的速度较之先前的 SA 版本更快，并且可以使用 10GbE 网络。

- **memcache**
  与软件数据库加速器 (`tsunami`) 一起使用的内存缓存层，用于支持针对与基于 Linux 的 SA 核心直接通信的代理的修正和扩展性增强功能。

  SA 配置组件捆绑包

  - **启动服务器**
    启动服务器是配置的一部分。它支持分别使用 inetboot 和 PXE 通过网络启动 Sun 和 x86 系统。用于提供此支持的进程包括 Internet Software Consortium DHCP 服务器。

  - **介质服务器**
    介质服务器是配置的一部分。它负责提供网络以访问在 SA 配置期间使用的供应商提供的介质。用于提供此支持的进程包括 Samba SMB 服务器和 Linux NFS。可复制有效的操作系统安装介质，并将其上载到介质服务器。

  OS 构建代理是 SA 配置的一部分。它在预配置(网络启动)进程期间运行，负责通过构建管理器使用 SA 核心注册服务器并指导操作系统安装过程。

- **核心网关/代理网关**

  核心网关直接与代理网关进行通信，以传递针对核心组件的请求及其响应。

- **DCML 交换工具**

  DCML 交换工具随每个切分组件捆绑包一起安装，用于方便导入和导出 SA 内容。请参见《SA 10.50 管理指南》。

- **全局文件系统**

  全局文件系统 (OGFS) 随每个切分组件捆绑包一起安装，用于为 SA 提供中央执行环境。

  OGFS 在一个或多个物理服务器上运行；客户可通过简单地将其他切分组件捆绑包添加到核心中，来扩展 SA 的执行功能。

  OGFS 在虚拟文件系统中运行 SA 内置组件(以及客户编写的程序)，此文件系统将 SA 数据模型、SA 操作和托管服务器显示为虚拟文件和目录。

  通过 SA 的这一独特功能，全局 Shell 和自动化平台扩展 (APX) 的用户可以使用任何脚本或程序语言查询 SA 数据以及管理服务器。由于 OGFS 通过 SA 安全模型来筛选所有数据、操作和托管服务器访问，因此默认情况下，运行在 OGFS 上的程序是安全的。

- **Web 服务数据访问引擎**

  Web 服务数据访问引擎为模型库提供公用对象抽象层，并为其他核心组件提高性能。通过简单对象访问协议 (SOAP) API、第三方集成组件，可访问此对象抽象。

- **次级数据访问引擎**

  数据访问引擎提供了针对模型库的 XML-RPC 接口，此接口可简化与各种客户端的交互，系统数据收集和服务器上的监控代理。随基础结构组件捆绑包一起安装的数据访问引擎被指定为主 数据访问引擎。随切分组件捆绑包一起安装的数据访问引擎被指定为次级 数据访问引擎。

  由于与模型库的交互通过数据访问引擎进行，因此模型库架构的更改对客户端的影响较小。数据访问引擎支持向 SA 添加功能，而无需进行系统范围内的更改。

- **构建管理器**

  (仅限 OS 序列)虽然构建管理器是 SA 操作系统配置的一部分，但它作为切分组件捆绑包的一部分进行安装。构建管理器帮助 OS 构建代理和命令引擎进行通信。它接受来自命令引擎的 SA 配置命令。它为特定于平台的内部版本脚本提供运行时环境，以便执行 SA 配置步骤。

- **HPE Live Network (HPELN)**

  HPE Live Network 为 Server Automation (SA)、Network Automation (NA)、Client Automation (CA)、Operations Orchestration (OO) 和 Service Automation Reporter (SAR) 提供内容更新。HPE Live Network (HPELN) 为客户提供安全策略和符合性策略，用以帮助最大化在 SA、NA 和 CA 中的投资回报，并利用可扩展的自动化平台不断提供新的自动化功能。

  在 SA 核心安装期间，HPELN 将作为切分组件捆绑包的一部分进行安装。

- **软件数据库加速器** (tsunami)

  它是一个对象存储下载加速器，用于为与基于 Linux 的 SA 核心进行直接通信的任何代理提高修正性能和扩展性。

  在两个关键区域中提高性能和扩展性：

  RPM 修正分析 - RPM 依赖关系分析/预览期间对包标题的提取速度较之先前的 SA 版本更快。

  修正包阶段 - 从软件数据库将单元下载到托管主机的速度较之先前的 SA 版本更快，并且可以使用 10GbE 网络。

- memcache

  与软件数据库加速器 (`tsunami`) 一起使用的内存缓存层，用于支持针对与基于 Linux 的 SA 核心直接通信的代理的修正和扩展性增强功能。

SA 配置组件捆绑包

- **启动服务器**

  启动服务器是配置的一部分。它支持分别使用 inetboot 和 PXE 通过网络启动 Sun 和 x86 系统。用于提供此支持的进程包括 Internet Software Consortium DHCP 服务器。

- **介质服务器**

  介质服务器是配置的一部分。它负责提供网络以访问在 SA 配置期间使用的供应商提供的介质。用于提供此支持的进程包括 Samba SMB 服务器和 Linux NFS。可复制有效的操作系统安装介质，并将其上载到介质服务器。

  OS 构建代理是 SA 配置的一部分。它在预配置(网络启动)进程期间运行，负责通过构建管理器使用 SA 核心注册服务器并指导操作系统安装过程。

卫星端安装

- **软件数据库缓存**
  软件数据库缓存包含核心软件数据库(或其他卫星端)内容的本地副本。在卫星端的托管服务器上安装或更新软件时，拥有软件数据库的本地备份可以提高性能并且降低网络流量。
- **卫星端代理网关**
  卫星端代理网关通过核心的管理网关来处理卫星端和核心之间的通信。

SA 网关

SA 网关管理托管服务器和 SA 核心之间、多个核心 (多主控网状网络)之间以及卫星端和 SA 核心之间的通信。多主控网状网络 (多个核心)(第 19 页)中讨论了多主控安装，SA 卫星端 (第 24 页)中讨论了卫星端安装。

网关具有多种类型：

- **管理网关**
  此网关管理 SA 核心之间以及 SA 核心和卫星端之间的通信。
- **核心网关/代理网关**
  这些网关协同合作，以便 SA 核心和托管服务器上的 SA 代理进行通信。
- **卫星端网关**
  此网关将通过管理网关或核心网关与核心进行通信，具体取决于您的配置。

多主控主网关备份路由

默认情况下，在多主控网状网络中安装第三个或后续核心会自动创建到第二个核心的备份路由(向第一个核心提供主路由和向第二个核心提供备份路由)。SA 在安装期间自动创建网关备份路由，无需提供任何配置信息，但如果 SA 无法创建备份路由，则您将看到指示此情况的消息，并需要联系 HPE 技术支持来手动配置网关备份路由。

仅在进行 SA 10.50 全新安装时才会创建网关备份路由，而非升级期间。如果从早期版本升级到 SA 10.50，则升级过程将不会创建网关备份路由。您必须手动创建备份路由。有关详细信息，请联系 HPE 技术支持代表。

例如，对于三个或更多核心的网状网络，所有多主控流量均默认通过第一个核心的主网关进行路由。但是，现在将第二个核心的主网关指定为默认的备份主网关，假如第一个核心的主网关失败。所有其他后续添加到网状网络的核心主网关均将按安装顺序被指定为备份

主网关。安装时，第三个以及后续核心均默认拥有两个通道。第一个通道与第一个核心的主网关进行通信，第二个通道与网状网络中的第二个核心进行通信 (请见下图)。

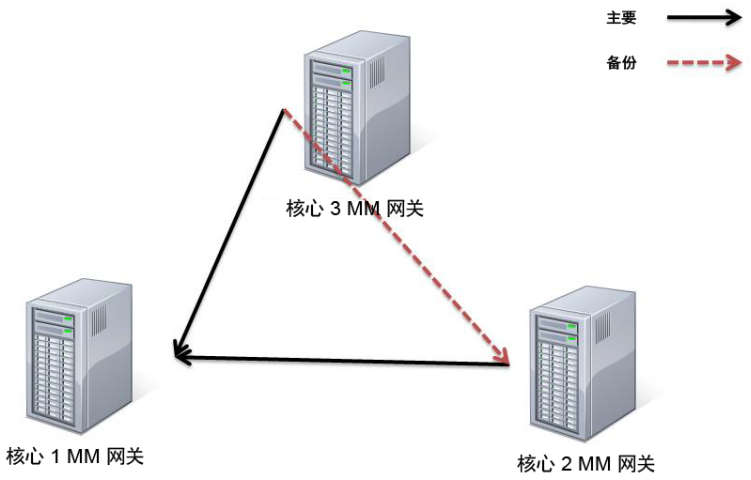


图 2: 建议设置。包含备份路由的 3 核心

包含多个主网关的网状网络也将具有冗余备份路由 (见 (请见下图)。

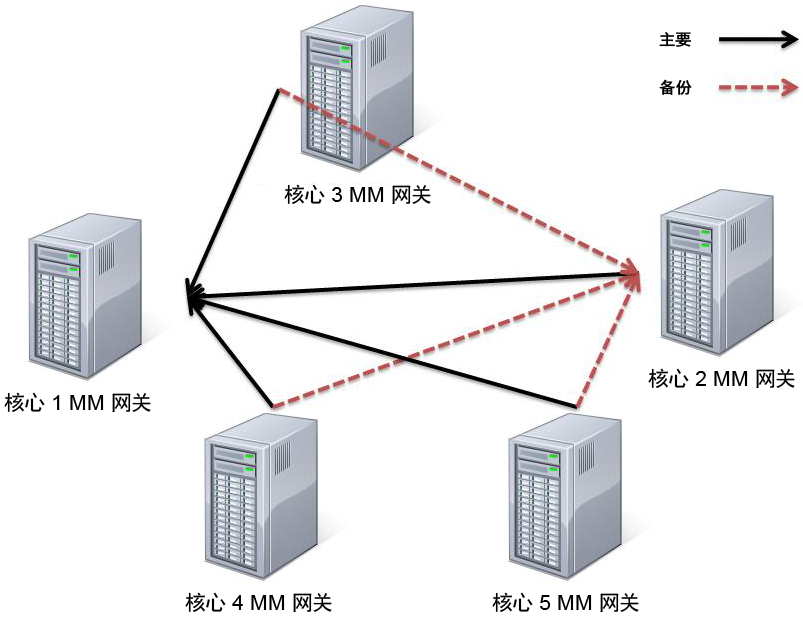


图 3: 建议设置。包含备份路由的 5 核心

如果某一个主网关出现故障，默认情况下，会将备份路由自动用于多主控网状网络流量。当出现故障的主网关恢复运行后，网状网络流量将自动再次通过该网关进行路由。

SA 拓扑

您必须决定符合设施需求的 SA 拓扑。本节提供了有关 SA 拓扑的一些背景信息，以帮助您做出决定。

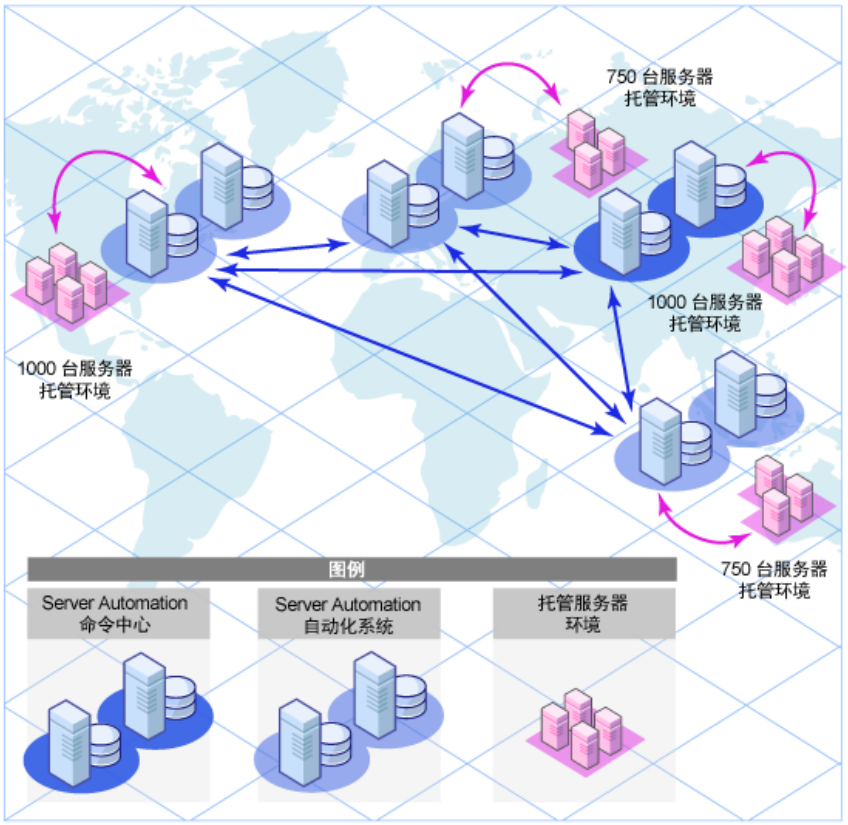
单主机核心

最简单的拓扑是在单个设施中管理服务器的单主机核心(先前称为独立核心)。

单主机核心最适合用于单个设施中包含的小型服务器网络。虽然单主机核心不与其他 SA 核心通信，但是它包含执行此操作所需的所有组件，并且可将其轻松转换为多主控网状网络中的一个核心。

多主控网状网络 (多个核心)

要管理多个设施中的服务器，可安装 SA 核心的多主控网状网络，或者是 SA 核心和卫星端的组合。



多主控网状网络是两个或多个 SA 核心的组合，这些核心通过管理网关进行相互通信，并且可以对有关各自模型库中包含的托管服务器的数据执行同步操作。对多主控网状网络的任何模型库中数据的更改将传播到网状网络中的所有其他模型库，并且实现同步。

对一个模型库到所有其他模型库的更改进行传播和同步的 SA 核心组件称为模型库多主控组件，它是基础结构组件捆绑包的一部分。通过这种复制功能，您可以为每个设施存储和维护软件的“蓝图”和环境特征，从而便于重新建立基础结构。它还可以帮助您在多个设施中轻松配置其他功能、分布更新以及共享软件内部版本模板和依赖关系。

多主控网状网络还可以包括卫星端安装。

通过使用 SA 客户端，可从已安装 SA 核心的任何设施管理服务器。

多主控网状网络的优点

多主控网状网络提供以下优点:

- **集中管理** - 可从由多主控网状网络中的 SA 核心管理的任何设施集中管理该多主控网状网络中的托管服务器。管理不会限于单个位置或者甚至是区域上的限制。

- **冗余** - 设施之间的同步 (复制) 数据管理提供了冗余。例如，如果网状网络的某个设施中的 SA 核心损坏，多主控网状网络中的其他核心包含托管服务器数据的同步备份，则这些数据可用于将损坏核心的模型库恢复到上一次已知的良好状态。此外，在损坏的核心不可用时，网状网络中的其他核心可继续运行而不会中断。
  复制还可用于关闭或添加设施，而网状网络中的其他设施仍然可以继续运行而不会中断。
- **性能扩展性** - 在多主控网状网络中，只有多主控数据库同步通过网络传输，从而降低网络带宽负载。
- **地理独立性** - 核心可以在网络中断期间继续管理服务器，而不论核心所在的位置。

设施和领域

SA 网关使用两个构造，以便于路由网络流量和消除 IP 地址冲突的可能性：

设施

设施构造代表服务器集合 (单个 SA 核心通过其模型库中存储的有关托管环境的数据来管理此集合)。设施通常代表特定的地理位置 (例如 Sunnyvale、San Francisco 或 New York)，或者通常为特定的数据中心。

设施是 SA 中的权限边界，即用户在某个设施中的权限不可用于其他设施。每个托管服务器被分配到单个设施。当设备初次注册 SA 核心时，会将其分配到与注册的网关关联的设施。

例如，管理员 A 在 Sunnyvale 中工作并负责维护服务器修补程序。在设施框架中，管理员 A 作为用户被绑定到 Sunnyvale 设施。管理员 A 查看服务器时，仅显示也绑定到 Sunnyvale 设施的服务器。他将无法查看任何其他设施的服务器。

有两种类型的设施:

- **核心设施**:每个核心安装都会包含一个核心设施。
- **卫星端设施**:安装卫星端时创建的默认设施。

领域

领域是 SA 构造，它允许 SA 在同一设施中管理不同网络上的服务器，而无需 IP 地址冲突。领域是附加到设施网络中设备的 IP 地址的唯一标识符，它允许 SA 网关对多主控网状网络中不同网络上 IP 地址可能冲突的设备进行唯一标识。

领域是一个可用于定义 IP 命名空间 (在其中，所有托管服务器 IP 地址必须唯一) 的逻辑实体。但是分配到其他领域的服务器可以具有重复的 IP 地址，在 SA 中仍然可以按各自领域的成员资格对这些重复 IP 地址进行唯一标识。

领域由被描述为网关网状网络 (SA 网关的单个互连网络) 中的网关互连。

在安装期间创建并命名新的设施时，还会创建一个与设施具有相同名称的默认领域。例如，创建设施 Datacenter 时，安装过程还会创建一个名为 Datacenter 的领域。该设施中的后续领域可命名为 Datacenter001、Datacenter002 等。每个领域中的托管服务器由领域名称和 IP 地址的组合进行唯一标识。

网状网络内的连接具有入口(源)领域(是连接进入该网状网络的位置)，和出口(目标)领域(是连接退出该网状网络的位置)。

所有 SA 托管设备都会明确分配到一个领域。可动态更改它们所分配到的领域(即使通常不会更改该领域)。当设备注册核心时，核心将使用网关标识服务器查找注册的入口领域，然后将该设备分配到该领域。

如果使用直接连接时发生注册，则设备将关联到过渡领域。可将过渡领域视为非领域。它的存在仅仅用于表示使用直接连接注册核心的设备。

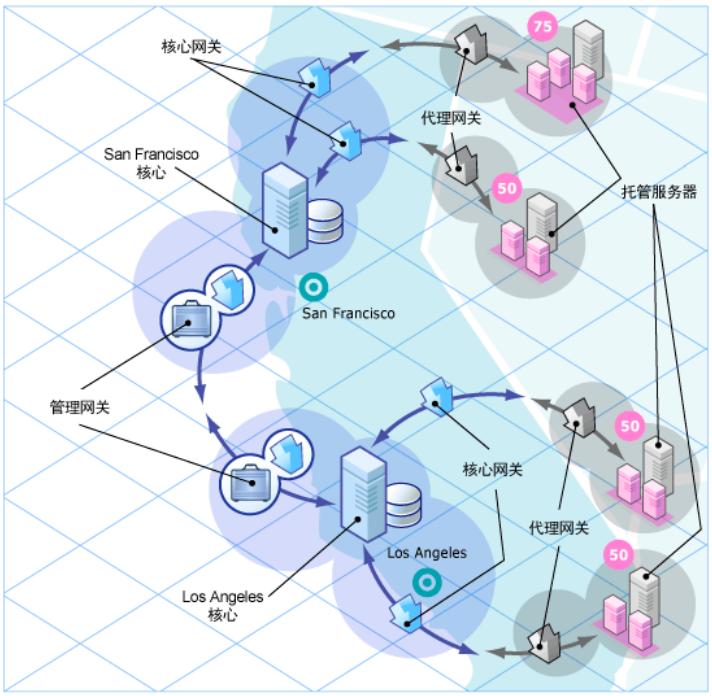
除了过渡领域，其他领域均不跨设施(也即，除了过渡领域外，每个领域都与某个设施有明确的关系)。

网状网络内，有两种领域类别：

- 非 root 网状网络
- root 网状网络位于网状网络的“中心”，网状网络有一个或多个领域。这些领域称为 root 领域。当要求使用网关路由连接时，如果该连接未指定目标领域，则连接将被路由到“最近的”root 领域，其中“最近的”意思是使用最低网络成本可访问的任何 root 领域。SA 中的 root 领域还与设施具有特殊关系。每安装一个 SA 核心，均将创建一个设施。同时，创建与新设施具有一对一关系的 root 领域。

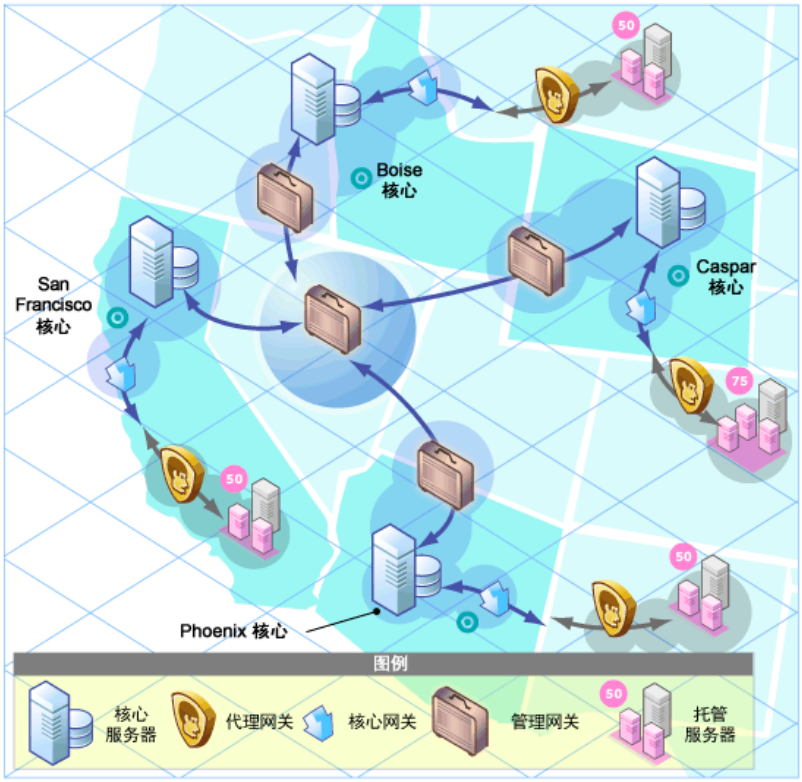
多主控网状网络拓扑示例

下图显示了核心安装在两个不同设施 (San Francisco 和 Los Angeles) 中的多主控网状网络。每个设施的核心均具有一个模型库，其中包含有关两个设施中托管服务器的数据。两个设施的模型库之间持续同步(复制)该数据。核心通过各自的管理网关进行通信。



Los Angeles 设施中的托管服务器与 San Francisco 核心的通信从 Los Angeles 代理网关传到核心网关，然后传到 Los Angeles 管理网关，之后此网关会通过 San Francisco 管理网关和核心网关与 San Francisco 核心进行通信。

下图显示了包含四个核心的多主控网状网络。此网状网络拓扑被称为星形结构，San Francisco 核心位于此网状网络的中心。SA 安装程序配置星形拓扑中的多主控网状网络，并默认使用备份网关路由。



SA 卫星端

对于没有大量足够潜在托管服务器的远程位置，卫星端安装可以是用于调整完整 SA 核心安装的一个解决方案。通过卫星端安装，您可以在卫星端主机上仅安装所需最少的核心组件，然后卫星端主机可通过 SA 网关连接访问主核心的数据库和其他服务。

卫星端安装还可缓解远程站点(可能通过有限的网络连接与主设施进行连接)的带宽问题。可以将卫星端的网络带宽使用限定在指定的比特率内。这可以帮助您确保卫星端的网络流量不会影响同一个管道上的其他关键系统的网络带宽要求。

卫星端安装通常至少由卫星端网关和软件数据库缓存组成，这仍然可支持您在远程设施中全面管理服务器。软件数据库缓存包含要安装在卫星端托管服务器上的软件包的本地备份，而卫星端网关则处理与主核心的通信。

可以选择在卫星端主机上安装 SA 配置启动服务器和介质服务器，用于支持远程 SA 配置。不支持在卫星端主机上安装其他组件。

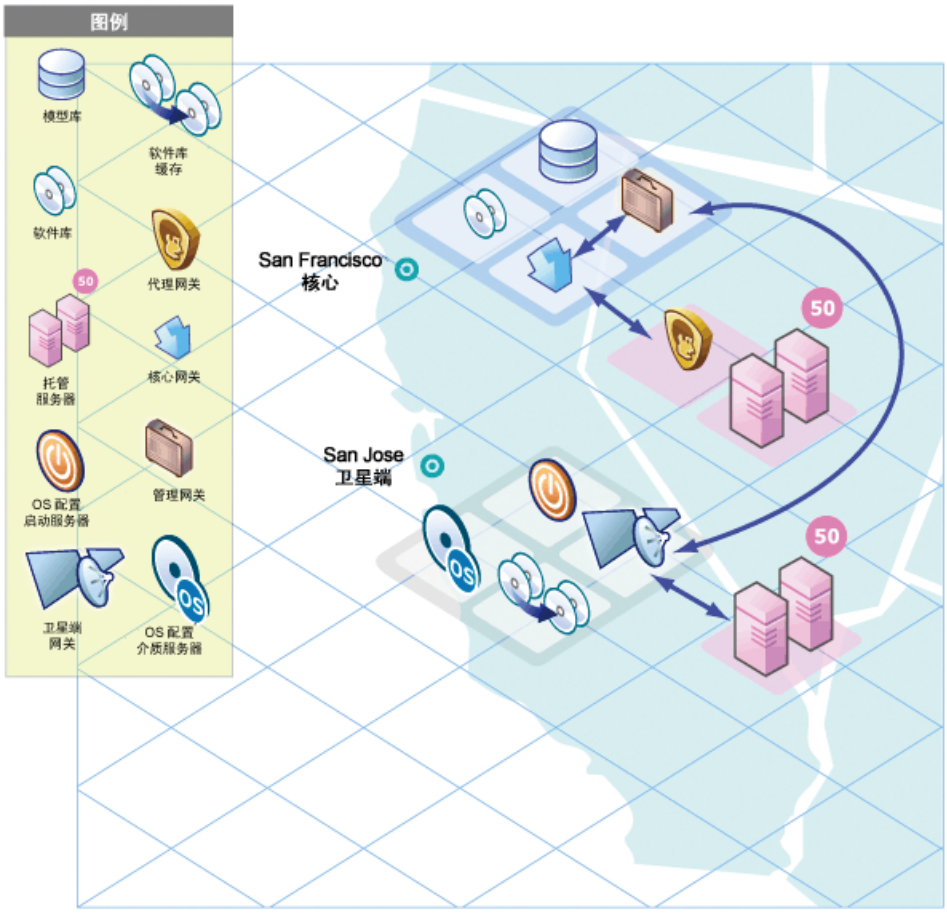
卫星端拓扑示例

简单的单个核心-卫星端链接

下图显示了链接到单个核心的单个卫星端。本示例中，主设施位于 San Francisco，较小的远程设施位于 San Jose。

San Francisco 单个核心由多个组件构成，包括软件数据库、模型库、一个代理网关和一个管理网关。为简单起见，此图没有显示所有所需的核心组件，例如命令引擎。

San Jose 卫星端由软件数据库缓存、一个卫星端网关、一个可选的 SA 配置启动服务器和介质服务器组成。



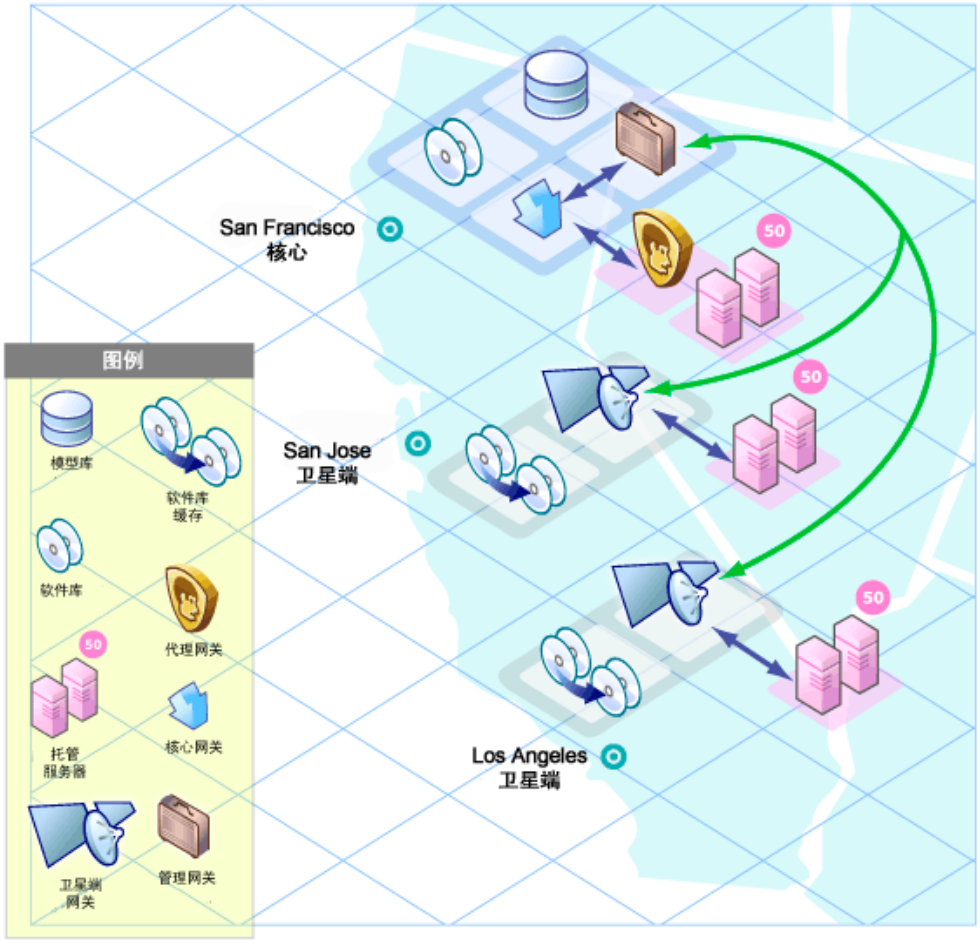
San Jose 卫星端的软件数据库缓存包含要安装在该设施托管服务器上的软件包的本地备份。

安装在 San Jose 设施托管服务器上的服务器代理通过 San Jose 卫星端网关 (该网关与 San Francisco 管理网关通信，然后通过 San Francisco 核心网关，最后与所需的核心组件通信) 连接 San Francisco 核心。

返回通信将反向该路径。安装在 San Francisco 设施的托管服务器上的服务器代理通过 San Francisco 设施的代理和核心网关与核心组件进行通信。

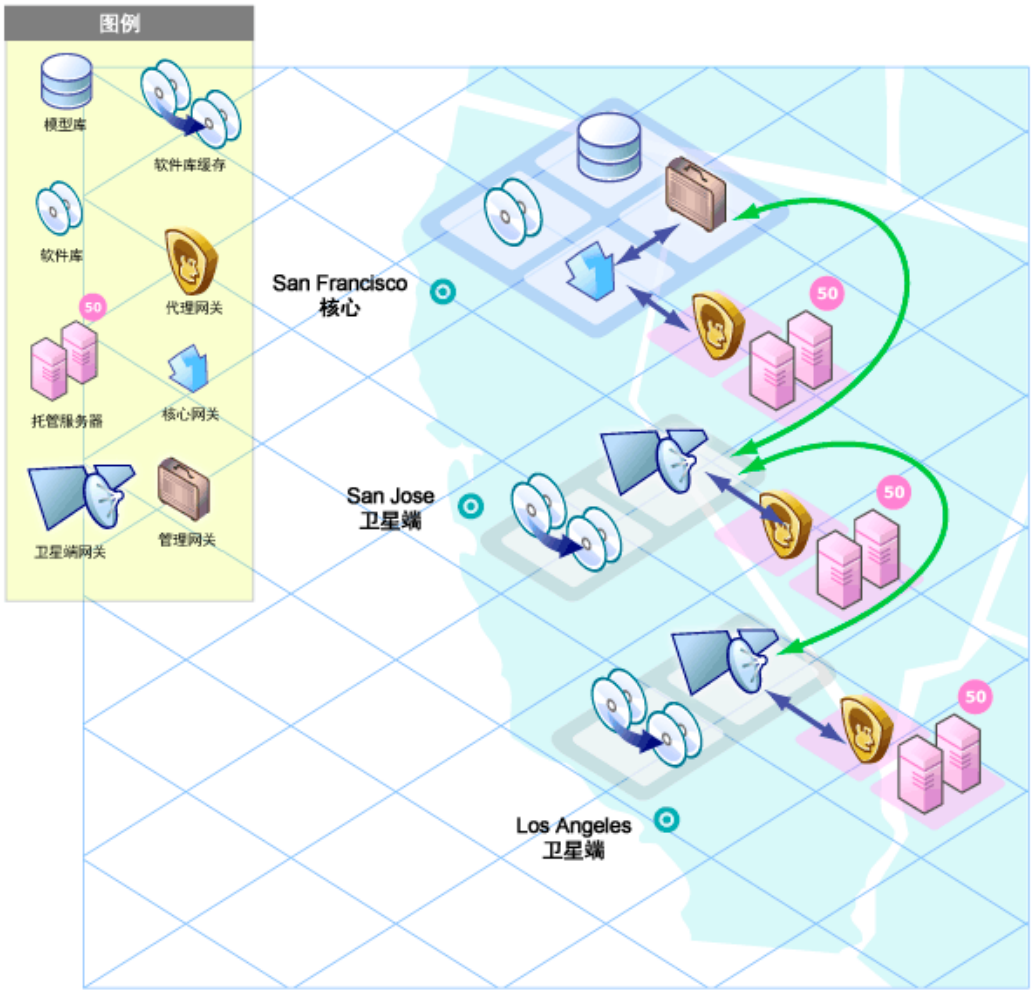
两个卫星端-单个核心的链接

下图显示了链接到单个核心的两个卫星端。本示例中，San Francisco 是主设施，Los Angels 和 San Jose 是卫星端设施。



级联卫星端链接

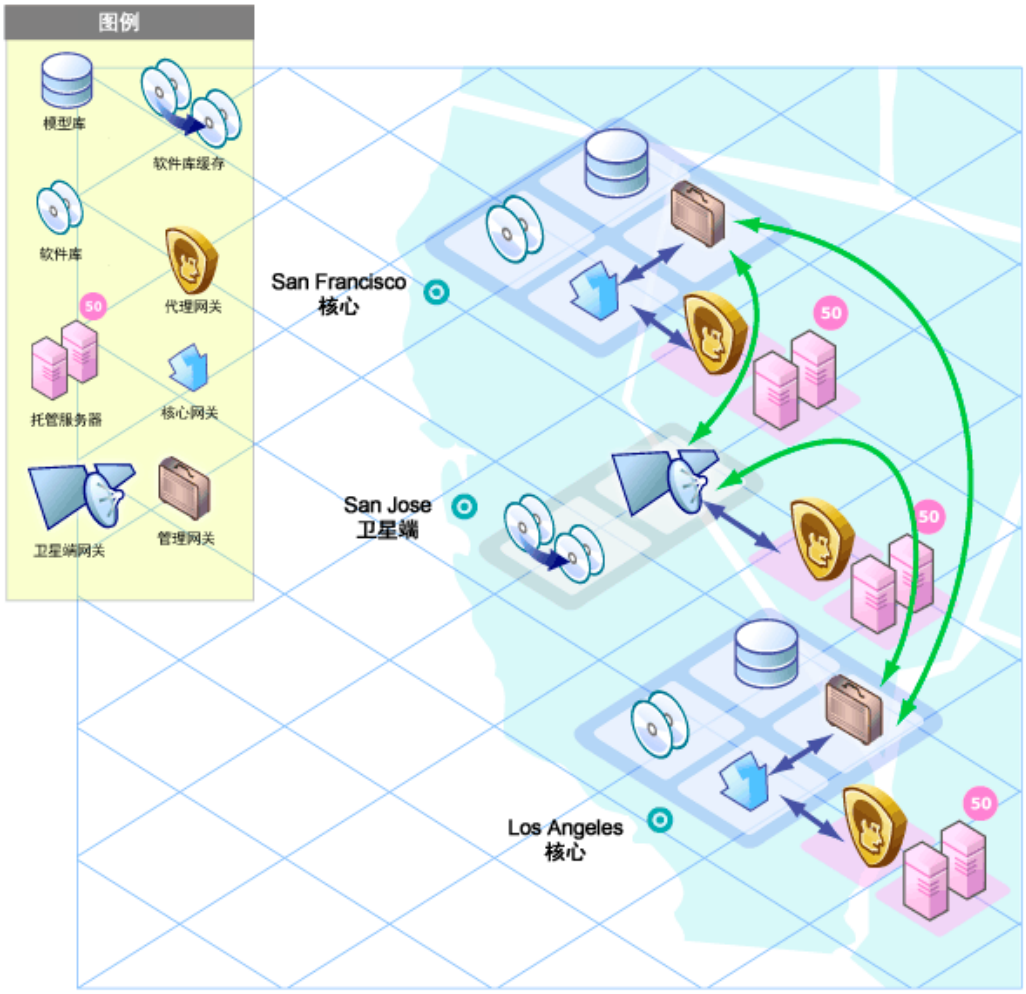
下图显示了级联卫星端的拓扑 (在其中，卫星端网关连接在一个链中)。此拓扑支持您创建软件数据库缓存的层次结构。请注意，此拓扑中的卫星端网关必须属于不同的 SA 领域。



当任务要求在 Los Angeles 设施的托管服务器上安装包时，SA 会首先检查 Los Angeles 的软件数据库缓存中是否存在此包。如果 Los Angeles 中没有此包，则 SA 会检查 San Jose 中的软件数据库缓存。最后，如果 San Jose 中没有此包，SA 会转向检查 San Francisco 核心中的软件数据库。有关详细信息，请参见《SA 10.50 管理指南》

在多主控网状网络中的卫星端

下图显示了多主控网状网络中连接到两个 SA 核心的 San Jose 卫星端。



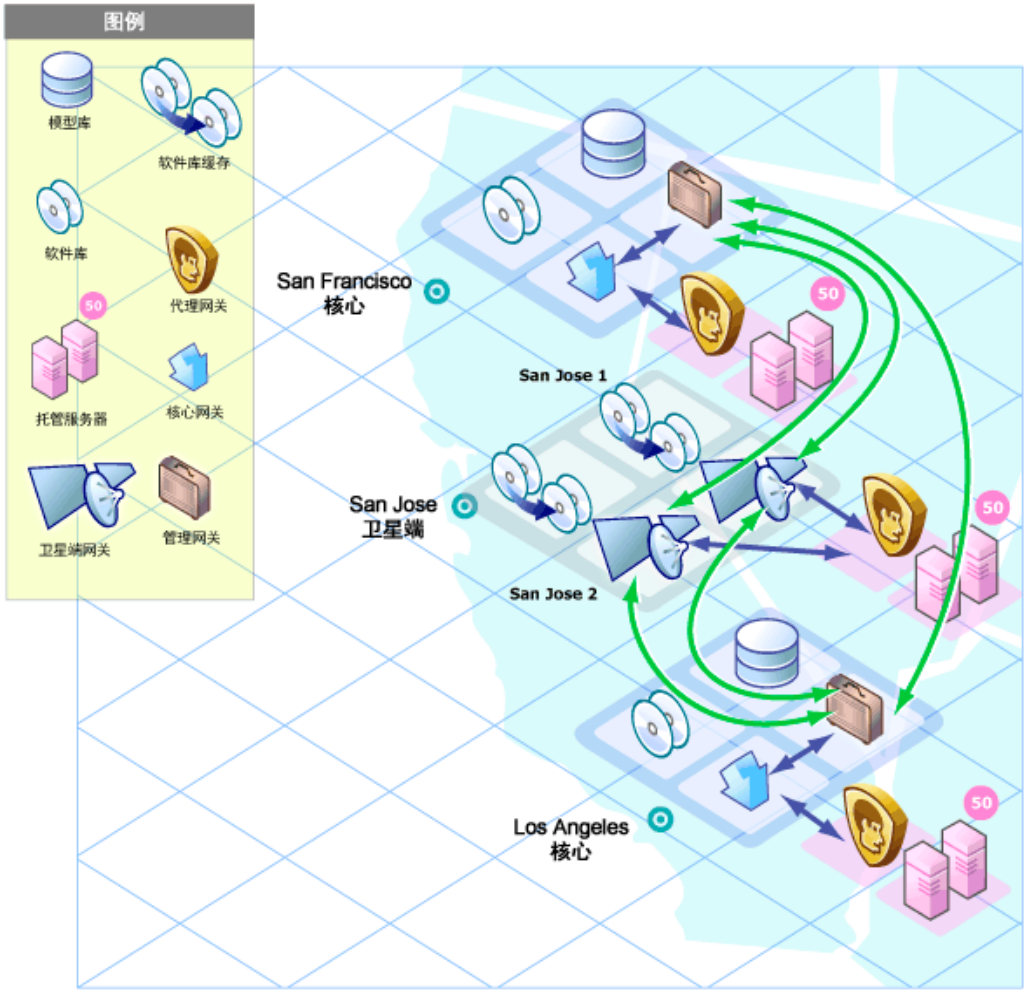
即使可同时与 Los Angeles 和 San Francisco 进行通信，管理网关还是会选择成本最低的路由(在此图中，为 San Francisco 路由)。可通过使用网关安装期间指定的参数来控制成本评估。系统设计者可指定规则来控制要使用的 SA 网关路由，从而最大化降低网络连接成本。

借助故障转移场景中的相同示例环境，在正常操作期间，San Jose 卫星端中的服务器受 San Francisco 核心管理。但是请注意，San Francisco 和 Los Angeles 核心是通过各自的管理网关直接连接的。

如果 San Jose 卫星端和 San Francisco 核心的连接失败，则 San Jose 卫星端网关可立即将通信从 San Francisc 移动到 Los Angeles 核心，以允许该核心保持对 San Jose 服务器的管理。Los Angeles 核心将包含有关 San Jose 位置的最新信息，因为作为正常 SA 操作的一部分，San Francisco 核心的模型库数据将被复制到 Los Angeles 模型库。

多主控网状网络中具有多个网关的卫星端

下图显示了可采用两种方式提供故障转移功能的拓扑。第一种方式，San Jose 卫星端 1 和 2 的网关同时与 San Francisco 和 Los Angeles 管理网关连接。如果 Los Angeles 核心不可用，San Francisco 核心仍然可以管理 San Jose 卫星端中的服务器。



第二种方式，安装在 San Jose 设施的托管服务器上的代理同时指向卫星端的代理网关。SA 代理自动通过可用代理网关进行负载平衡，因此可以直接与 San Francisco 或 Los Angeles 核心进行通信。

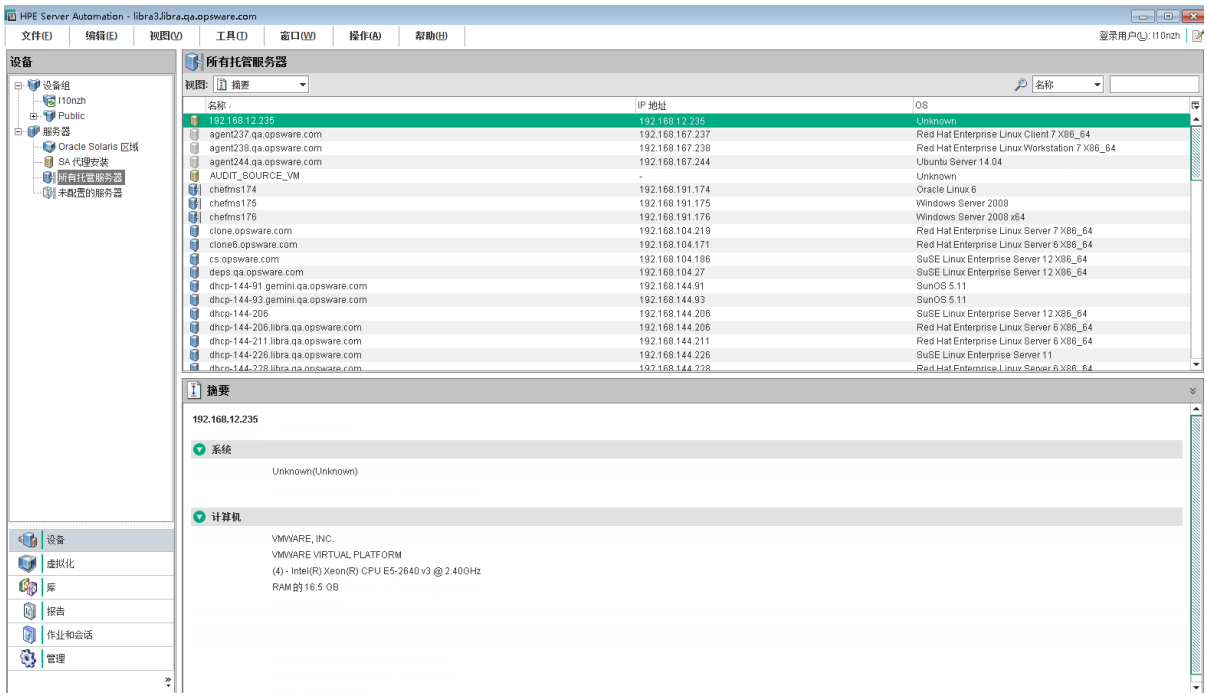
如果某个网关不可用，则正在以不可用的网关作为主网关的代理将自动进行故障转移以使用次级网关。在例行的代理到核心的通信过程中，SA 代理将发现卫星端中添加 (或删除) 的新网关。

SA 客户端

SA 客户端是安装 SA 后安装的 Windows 应用程序。它提供 SA 功能的界面。

要安装 SA 客户端，必须下载并安装 SA 客户端，方法是: 打开核心的主页并单击“Download Server Automation Client”。

下图显示了 SA 客户端主屏幕。您可以在使用中找到有关 SA 客户端的更多详细信息。

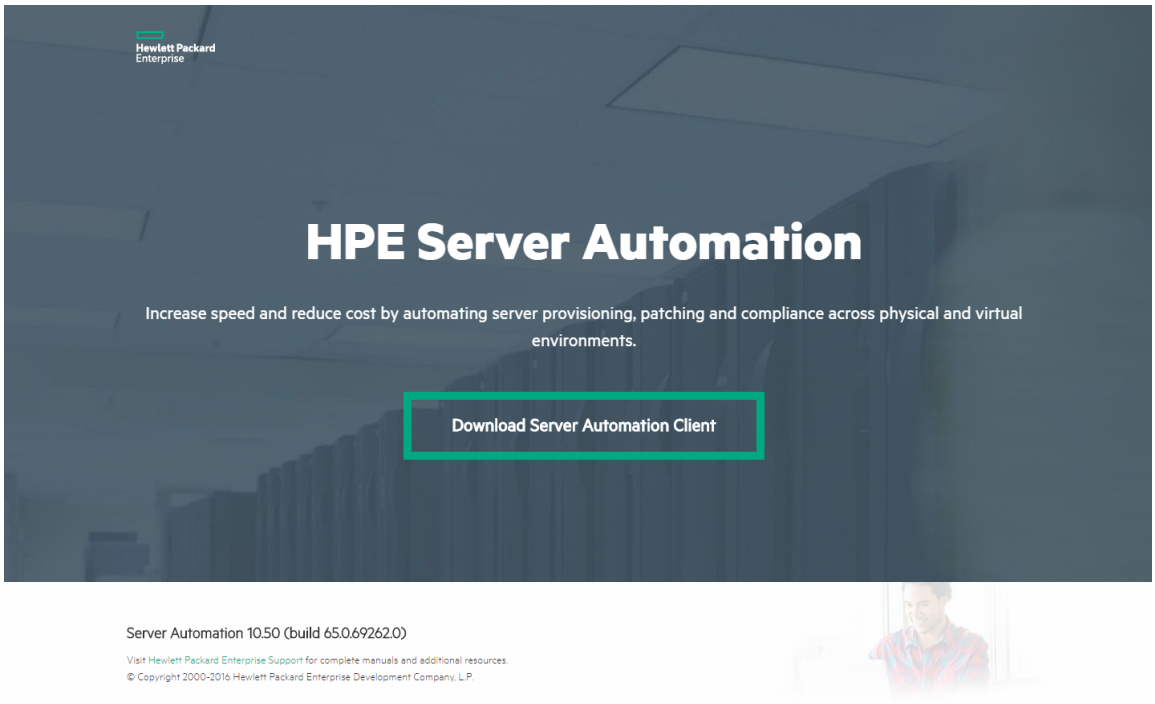


SA Web 客户端

已弃用 SA Web 客户端。某些 SA 功能仍然通过 SA Web 客户端提供，但是您应使用 SA 客户端 (如果可能)。

SA Web 客户端是基于 Web 的 SA 用户界面，可通过此界面下载 SA 客户端启动程序。《用户指南》中提供了有关在浏览器中启动 SA Web 客户端的说明:Server Automation》。在启动 SA Web 客户端后，您可以下载并安装 SA 客户端启动程序可执行文件。

下图显示了 SA Web 客户端主页


Hewlett Packard Enterprise
HPE Server Automation
Increase speed and reduce cost by automating server provisioning, patching and compliance across physical and virtual environments.
Download Server Automation Client
Server Automation 10.50 (build 65.0.69262.0)
Visit Hewlett Packard Enterprise Support for complete manuals and additional resources.
© Copyright 2000-2016 Hewlett Packard Enterprise Development Company, L.P.

功能

SA 可自动化数据中心进程，替换临时、易于出错的手动进程。例如，通过使用 SA 配置，您可以为不同类型的服务器设置标准并自动配置服务器，从而节省时间和确保操作系统构建一致。

可建立修补程序策略，以便为 IT 环境中托管服务器上运行的受支持操作系统安装和维护修补程序。

通过使用符合性，可检查托管服务器，以便了解哪些服务器不符合要求。然后基于创建的策略修正不符合要求的服务器，使其重新符合要求。

SA 提供以下功能：

SA 支持跨平台环境，可用于同时自动化新的和现有数据中心环境。

设备资源管理器

设备资源管理器支持您查看有关托管环境中服务器的信息。

在“服务器资源管理器”中，可以执行以下任务：

- 创建服务器快照、执行服务器审核、审核应用程序配置、创建包以及打开远程服务器上的远程终端会话。
- 浏览服务器的文件系统、注册表、硬件库存、软件和修补程序列表，以及服务。
- 浏览 SA 信息，例如属性、可配置的应用程序，甚至服务器历史记录。
- 在“组浏览器”中，可以执行以下任务：
- 审核系统信息、创建服务器快照和配置应用程序。
- 查看和访问组成员(服务器和其他组)。
- 查看组摘要和历史记录信息。

虚拟化管理

HP 支持的与虚拟化供应商和云计算解决方案的集成统称为虚拟化服务。

在虚拟化环境中，虚拟化供应商管理多个虚拟机监控程序和虚拟机。HP 支持与 VMware vCenter Server 和 Microsoft System Center Virtual Machine Manager (SCVMM) 的集成。

云计算解决方案(例如 OpenStack)提供基础设施即服务 (IaaS)。HPE 支持与 OpenStack 的有限集成。

HPE Server Automation 中的虚拟化管理具有以下功能：

- 提供数据中心和所有物理及虚拟机 (VM) 的可见性。
- 遵守您的所有规定和企业策略。
- 控制整个虚拟环境，允许您控制虚拟机增长，以及快速检测并解决问题。

应用程序配置管理

应用程序配置管理 (ACM) 允许您创建模板，以便修改和管理与服务器应用程序关联的应用程序配置。通过 ACM，您可以从中心位置管理、更新和修改这些配置，从而确保对设施中的应用程序进行准确一致地配置。

通过使用 ACM，您可执行以下任务：

- 基于文件和对象(例如 Windows 注册表、IIS 元数据库、WebSphere、COM+ 等更多对象)管理配置。
- 在应用配置更改之前，预览这些更改。
- 编辑并将配置更改推送到单台服务器或服务器组。
- 使用 SA 数据模型中的信息设置配置值。
- 通过构建配置模板管理任何应用程序的配置。
- 审核服务器上的应用程序配置，确定服务器上的任何配置文件是否与模板中存储的值同步。

有关详细信息，请参见《SA 10.50 开发人员指南》。

审核和修正

审核和修正支持您确定在 IT 环境中要检查的对象、要检查这些对象的位置以及何时检查它们。

- 审核策略 定义要检查的内容 - 例如文件、目录、配置值等。
- 审核 定义要检查的位置 - 例如服务器和服务器组。
- 审核计划 定义何时检查 - 例如一次性作业或重复作业。

这些功能将帮助您了解如何使托管服务器环境以及服务器符合要求。在 SA 中，可以定义服务器配置策略，以便确保设施中的服务器符合这些策略标准。如果发现服务器不符合要求(未按所需的方式配置)，可以对其进行修正以符合组织标准。

通过使用 SA 客户端，可以基于自定义值或预配置的审核策略来审核基于活动服务器或服务器快照的服务器配置值。此外，还可以创建服务器配置快照，以捕获系统的当前状态，以便将其他服务器与已知基线进行比较。

审核策略支持您定义公司或行业范围内的符合性和安全标准，然后可将这些标准用于审核、快照规范和其他审核策略中。引用审核或快照规范中的审核策略可帮助您更新组织中的最新符合性定义。

通过使用审核和修正，您可执行以下任务：

- 将服务器或快照与参考服务器或快照进行对比
- 创建审核，以便于重复使用
- 创建用于为企业定义符合性和安全标准的审核策略
- 将审核与单台服务器或动态服务器组关联
- 在多个级别修正问题，包括文件、目录、修补程序、注册表项和包

Windows 修补程序管理

Windows 修补程序管理支持您确认、安装和删除 Microsoft® Windows 修补程序，以及为组织中的托管服务器维持高级别的安全性。您可以为 Windows 操作系统确认和安装用于避免安全漏洞的修补程序。

有关详细信息，请参见SA 10.5 Support and Compatibility Matrix。

由于 Windows 修补程序通常发布用于解决安全威胁，因此组织必须能够在系统受到威胁之前快速运用修补程序。但是与此同时，修补程序本身可能会引起严重问题，包括性能下降和服务器故障。

修补程序管理在支持您对新发现的威胁做出快速反应的同时，还可对修补程序的安装进行严格的测试和标准化。如果修补程序引起问题(即使已经过测试和批准)，Windows 修补程序管理仍然可以帮助您以安全和标准化的方式卸载修补程序。

有关详细信息，请参见《SA 10.50 用户指南》。

HP-UX 修补程序管理

通过实现以下功能，SA 可自动化 HP-UX 修补程序管理：

- 定义 HP-UX 软件策略，这些策略可提供用于管理 HP-UX 服务器的基于模型的方法。Server Automation 支持您使用 HP-UX 软件策略创建 IT 环境的模型。这些软件策略用于指定托管服务器上可安装的修补程序和脚本。
- 在托管服务器上安装 HP-UX 修补程序和修补程序捆绑包。

- 建立修补程序安装过程。
- 计划修补程序管理阶段：分析、下载和安装。此外，还可以设置每个阶段的电子邮件通知并关联每个作业的工单 ID。
- 基于软件策略验证服务器的符合性状态。
- 显示“符合性”视图，以查看是否根据软件策略配置服务器以及修正不符合要求的服务器。
- 搜索软件资源和服务器。
- 在 SA 库中使用强大且灵活的搜索条件(例如可用性、体系结构、操作系统、重新启动选项、版本等)来搜索 HP-UX 包、修补程序和软件策略。还可以按名称、文件夹名称、可用性和操作系统来搜索 HP-UX 软件策略。
- 在预览修补程序安装时，查看修补程序依赖关系以及适用性分析。

有关详细信息，请参见《SA 10.50 用户指南》。

Solaris 和 Solaris 11 修补程序管理

Server Automation Solaris 修补程序管理支持您确认、安装和删除 Solaris 修补程序，以及为组织中的托管服务器维持高级别的安全性。

Server Automation Solaris 修补程序管理支持您通过使用修补程序策略，实现在 Sun Solaris 上自动安装和卸载 Solaris 修补程序和修补程序群集。此外，SA 分析策略中修补程序之间的依赖关系、取代和适用性关系，以及显示应在服务器上安装的修补程序的更新有序的列表。通过此功能，您可以验证服务器的符合性状态并修正不符合要求的服务器，以及将 Solaris 修补程序自动下载到 SA 并将其组织到修补程序策略中。

通过实现以下功能，SA 可自动化 Solaris 修补：

- 确定托管服务器所需的修补程序。
- 创建 Solaris 修补程序策略。
- 下载 Solaris 修补程序、修补程序群集以及修补程序捆绑包，并将它们及其相关的供应商信息存储在 SA 库中。
- 解析 Solaris 修补程序的所有依赖修补程序。
- 在托管服务器上安装 Solaris 修补程序和修补程序群集。
- 在单个用户模式中安装 Solaris 修补程序。
- 按 Oracle Solaris 区域安装修补程序。

- 建立修补程序安装过程。
- 使用修补程序策略验证服务器的符合性状态。
- 搜索软件资源和服务器。

有关详细信息，请参见《SA 10.50用户指南》。

Ubuntu 修补程序管理

HPE Server Automation Ubuntu修补程序管理支持您确认、安装和删除 Ubuntu Debian程序包更新，以及为组织中的托管服务器维持高级别的安全性。您可以为 SA支持的托管服务器平台确认和安装用于避免安全漏洞的 Ubuntu程序包。

SA可自动化修补程序管理的关键方面，同时提供针对如何安装 Ubuntu程序包及安装条件的一定程度控制。通过自动化修补过程，修补程序管理可以减少修补过程所需的停机时间。SA还支持您计划修补程序活动，以便在非高峰时间段进行修补。

借助 SA中的 Ubuntu修补，可以在导入二进制程序包之前先导入元数据。可以运行仅具有下载的元数据的 Ubuntu扫描器来确定服务器漏洞。然后，可以运行 Ubuntu程序包导入程序以仅导入托管服务器所需的程序包。这种做法可以节省存储空间以及缩短扫描和修正处理时间。

Ubuntu修补程序管理文档包含有关如何导入 Ubuntu元数据和程序包、扫描漏洞以及使用修补程序策略安装 Ubuntu程序包更新的信息。

SA通过提供以下功能自动化 Ubuntu修补：

- 存储程序包并按其本地格式组织程序包的**中心存储库**。
- 存储已应用的每个程序包相关信息的**数据库**。
- 基于供应商提供的最新元数据分析平台漏洞的**动态修补程序策略**。
- 用于确定需要程序包更新的服务器的**高级搜索**功能。
- 用于跟踪重要程序包更新的部署的**审核功能**。

有关详细信息，请参见《SA 10.50用户指南》。

UNIX 修补程序管理

UNIX 修补程序管理支持您确认、安装和删除修补程序，以及为组织中的托管服务器维持高级别的安全性。通过使用 SA 客户端，可以为 AIX 操作系统确定和安装用于避免安全漏洞的修补程序。

SA 支持您对新发现的安全威胁做出快速反应，还可对修补程序的安装进行严格的测试和标准化。如果修补程序在经测试和批准之后引起问题，SA 可以帮助您以安全和标准化的方式卸载修补程序。

SA 将修补程序信息存储在 SA 库中，这些信息包括每个受管理的服务器、服务器上安装的修补程序和软件，以及可用于安装的修补程序和软件的详细信息。可以使用此数据确定暴露于新发现威胁的严重性，以及帮助评估使用修补程序的优点与停机成本和测试要求。

通过自动化修补过程，SA 可以减少修补过程所需的停机时间。SA 还支持您计划修补程序活动，以便在非高峰时间段进行修补程序安装。

UNIX 修补程序管理提供以下功能，以便您能够通过某个操作系统浏览修补程序、计划修补程序下载和安装、设置电子邮件通知、预览修补程序安装、使用软件策略和修正来安装和卸载修补程序，以及将修补程序信息导出到可重用的文件格式：

- 存储并按其格式组织修补程序的 SA 库
- 包含已应用的每个修补程序信息的数据库
- 可在安装修补程序之前和之后运行的自定义脚本
- 用于确定需要安装修补程序的服务器的高级搜索功能
- 可启用安全人员对重要修补程序部署进行跟踪的审核功能

有关详细信息，请参见《SA 10.50 用户指南》。

报告

SA 报告全面提供有关以下方面的实时信息：托管服务器、网络设备、软件、修补程序、客户、设施、操作系统、符合性策略，以及环境中的用户和安全性。这些报告以图形和表格的格式显示，并且可操作 - 您可对报告中的对象(如策略或审核)执行适当的操作。此外，还可以将这些报告(以 `.html` 和 `.xls` 格式的形式)导出到您的本地文件系统，以便于在组织中使用。

SA 配置

SA 配置可以将预配置的操作系统基线快速、一致地安装 (或配置) 到裸机虚拟服务器，并且只需最少的手动干预。裸机虚拟服务器 SA 配置是将服务器投入生产的整个过程中的关键部分。

SA 配置可确保设施中的每台服务器具有您可以控制的标准默认操作系统配置。有关 SA 配置的详细信息，请参见《SA 10.50 管理指南》。

SA 配置的优点包括：

- **与其他 SA 功能的集成**
  因为 SA 配置与 SA 自动化功能套件(包括修补程序管理、软件管理和分布式脚本执行)的集成，IT 组之间可实现无缝递交。SA 可确保所有 IT 组在了解当前环境状态的基础上共同协作，这是提供高质量运营和可靠变更管理的基本要素。
- **更新服务器基线而无需重新映像**: 不同于很多其他配置解决方案，随配置的系统在配置之后可被轻松更改，以适应新的要求。此优点的关键在于模板的使用以及基于安装的配置方法。
- **可在多个环境中工作的灵活体系结构**: 配置支持多种类型的服务器、网络、安全体系结构和操作流程。使用计划或按需的工作流程可在跨多种硬件模型的 CD (Linux 配置) 或网络引导环境 (DHCP 和非 DHCP 环境) 中有效地工作。这种灵活性将确保您可以配置符合组织要求的操作系统。

可以从 SA 客户端执行 SA 配置功能。SA 将自动化综合服务器基线配置的整个过程，这个过程通常包括以下任务：

- 使用操作系统安装配置文件为操作系统安装准备硬件(仅操作系统序列需要)。
- 定义操作系统构建计划，这些计划是操作系统安装前后要在服务器上执行的任务列表。操作系统构建计划更加强大，可用于替代操作系统序列。
- 定义操作系统序列，这些序列是服务器安装期间要在服务器上执行的任务列表。操作系统序列可包括应用程序、修补程序和修正策略。SA 建议您使用更加灵活的操作系统构建计划。
- 使用操作系统构建计划或操作系统序列安装基本操作系统和默认操作系统配置。
- 应用最新 OS 修补程序集。确切的列表取决于服务器上运行的应用程序。
- 执行预安装或安装后脚本，这些脚本使用一些值(例如 root 用户密码)配置系统。

- 安装系统代理和实用程序，例如 SSH、PC Anywhere、备份代理、监控代理或防病毒软件。
- 安装广泛共享的系统软件，例如 Java 虚拟机。

SA 配置可支持：

- Windows、Solaris 和 Linux。
- 基于网络或 CD/DVD 的安装。
- 数据中心员工和系统管理员之间的职责分工。
- 基于模型的方式 - 采用此方式在 SA 中创建标准内部版本，之后可将其安装在多个系统上。

SA 配置集成了操作系统供应商的本地安装技术，特别是：

- Windows 安装应答文件：`unattend.xml, sysprep.inf`
- Red Hat Kickstart
- SuSE YaST(其他安装工具)
- Solaris Jumpstart
- WINPE/WIN-BCOM/UNDI

可在以下位置配置操作系统：

- 在 SA 无代理服务器池中尚未安装操作系统的服务器 (裸机服务器)
- 虚拟服务器
- 在 SA 非托管服务器池中已安装操作系统的服务器
- 在 SA 托管服务器池中已安装操作系统的服务器 (预配置)

应用程序部署

通过应用程序部署，可在数据中心中创建、测试自定义软件应用程序，并将其部署到目标服务器。例如，可将应用程序从开发团队移动到质量保证团队，以便于进行测试。测试完成后，可将应用程序移动到其他阶段，例如再生产、暂存并最终移动到生产阶段。应用程序部署工具可通过提供单点访问(每个涉及的人员都可通过此访问点查看或输入与他们或他们的角色有关的数据)来减少部署应用程序所需的复杂通信过程。

通过应用程序部署，您可以：

- 为应用程序组件建模，例如代码、脚本、配置文件和层(例如应用程序服务器、Web 服务器和数据库)。
- 管理应用程序的多个并发版本。
- 在目标服务器上部署、回滚和取消部署应用程序。
- 为运行应用程序所需层的目标服务器建模。这些目标服务器是 Server Automation 中的托管服务器。
- 为软件应用程序开发人员、质量保证和测试人员、系统管理员以及其他操作人员提供清晰简明的通信。
- 为生命周期建模(从应用程序开发、QA、再生产、暂存、再到生产)并进行实施。可以自定义 SA 以匹配企业生命周期。

有关详细信息，请参见《SA 10.50 开发人员指南》。

脚本执行

SA 脚本执行支持您在整个 SA 托管服务器场中共享和运行临时或保存的脚本。

通过使用 SA 执行脚本而无需手动执行，管理员可从中获益：

- 在多个 UNIX 和/或 Windows 服务器中并列执行脚本，从而节省时间和确保一致性。
- 基于角色的访问控制，确保仅被授权的管理员可以在对其具有访问权限的主机上执行脚本。
- 通过将脚本存储在私用或公用库中，控制对脚本的访问。
- 一次查看和下载一台服务器的脚本输出，或在合并的报告(在单个位置中捕获所有服务器的输出)中查看和下载多台服务器的脚本输出。
- 可批量自定义脚本。管理员可以在 SA 中访问有关环境和服务器状态的信息。这对于确保在正确的服务器上执行正确的脚本至关重要。
- 用于报告特定脚本执行人、执行内容、执行时间和执行位置的全面审核记录。

由于脚本执行是 SA 的一个集成部分，因此相较于独立脚本执行工具，管理员可以利用其独特优点：

- 借助已知状态和配置信息来自定义脚本执行，用户可以通过参考和访问 SA 中存储的丰富信息(例如拥有服务器的客户或业务、服务器是否为暂存或生产服务器、服务器所在的设施以及自定义名称-值对)，来定制每个脚本。

- 通过共享脚本而不危及安全性，用户可以与其他人共享脚本而不会危及安全性，因为 SA 对哪些人可以在哪些服务器上执行脚本保持严格的控制，并且针对脚本执行生成全面的审核记录。

无代理服务器发现和 SA 代理安装

无代理服务器发现和 SA 代理安装允许您将服务器代理部署到设施中的大量服务器，并使其受 SA 管理。

您可执行以下任务：

- 扫描网络中的无代理服务器。
- 选择用于 SA 代理安装的服务器。
- 选择通信工具和提供用户/密码组合。
- 选择代理安装选项和部署代理。

Service Automation Visualizer (SAV)

Service Automation Visualizer (SAV) 旨在帮助您更好地理解和管理 IT 环境中分布式业务应用程序的操作体系结构和行为。由于这些应用程序是由服务组成的复杂的集合，它们通常跨多台服务器以及网络运行，因此要了解 (或记住) 相互连接的应用程序、性能问题的起始位置、如何排除和解决问题以及在环境中进行更改后会出现的结果，会变得越来越困难。

SAV 通过物理图和逻辑图帮助您查看此类型的信息。

SA 客户端的符合性

在 SA 客户端中，“符合性”视图可支持您查看设施中所有服务器和服务器组的整体符合性级别。从此视图(通常称为符合性图表板)中，您可以修正不符合要求 的服务器。可以查看单台服务器、多台服务器、服务器组或受 SA 管理的所有服务器的符合性。

符合性图表板显示了针对审核、审核策略、软件策略、修补程序策略和应用程序配置的服务器或服务器组的所有符合性状态的结果。服务器的符合性状态基于符合性策略。符合性策略可定义唯一的服务器配置设置或值，用于确保将 IT 环境配置为所需的环境。

符合性策略通常由策略设置员 创建和定义。在某些环境中，可能需要系统管理员创建临时的策略。策略设置员创建符合性策略，然后将其附加到服务器，以确保服务器符合组织的标准和策略。

例如，策略设置员可以创建软件策略，用于定义服务器上必须安装的修补程序和包标准集。策略设置员还可定义必须采用何种方式在服务器上配置某些应用程序文件。如果服务器或服务器组的配置与策略设置员在符合性策略中定义的规则匹配，则会将它们视为符合要求。

通过符合性图表板，您可以确定服务器实际安装的软件、程序包、修补程序和配置文件设置是否与软件策略 中定义的配置相匹配。“符合性”视图允许您查看服务器组的符合性，它显示了组的所有成员及子组成员的符合性状态汇总。在“符合性”视图中，可以发现不符合要求 的服务器和服务器组，然后修正任何问题。

软件管理

SA 软件管理提供了强大的机制，通过使用软件策略对软件进行建模，以及一步实现在服务器上进行软件部署和应用程序配置的自动化过程。此外，SA 软件管理 提供了一个结构来组织文件夹中的软件资源并定义访问它们的安全权限。SA 软件管理允许您验证服务器的符合性状态并修补不兼容的服务器。

SA 软件管理 提供以下功能：

- 创建软件的组织结构
- 定义文件夹的安全边界
- 定义基于模型的方法来管理组织中的 IT 环境
- 启用用户组之间的软件资源共享
- 同时部署和配置应用程序
- 在一台服务器上部署多个应用程序实例
- 建立软件部署过程
- 针对软件策略验证服务器符合性状态
- 生成报告
- 全面搜索软件资源和服务器

有关进一步信息，请参见《SA 10.50 用户指南》。

全局 Shell

SA 全局 Shell 支持您使用命令行界面来管理服务器。您可以远程执行以下任务：

- 完成托管服务器上的例行维护任务。
- 排除、确定和修正托管服务器上的问题。

全局 Shell 由一个文件系统和用于管理 SA 中服务器的针对该文件系统的命令行界面构成。此文件系统称为 SA 全局文件系统 (OGFS)。OGFS 中的所有对象类型(例如服务器、客户和设施)都代表此文件系统中的目录结构。

此外，SA 全局 Shell 还管理用于访问托管服务器上的文件系统、Windows 注册表以及 Windows 服务对象的用户权限。

FIPS 140-2 符合性

HPE Server Automation (SA) 符合联邦信息处理标准出版物 140-2，它是一项安全标准，确保政府机构采购使用已通过验证的加密模块的设备。

本节介绍 SA 核心、卫星端和托管服务器与 FIPS 140-2 的符合情况以及用于使 SA 符合 FIPS 140-2 要求的方法。

- SA 核心 (第 44 页)
- SA 代理 (第 45 页)
- SA 网关 (第 45 页)
- SA 卫星端 (第 46 页)
- SA 托管服务器 (第 46 页)

SA 核心

SA 核心是一个核心组件集，这些组件协同合作以支持您发现网络上的服务器、将这些服务器添加到托管服务器池，然后从中心 SA 客户端界面对服务器进行配置、修补、监控、审核和维护。SA 客户端提供单个界面，用于访问 SA 的所有信息和管理功能。

安装核心组件的服务器称为核心服务器。即使核心组件分布到多个主机，这些组件仍然被视为单个 SA 核心的一部分。可将所有核心组件均安装在单个主机上，也可将其分布于多个主机，但是典型的 SA 安装使用核心组件绑定，这会将某些组件一起安装在同一台服务器上，以提高性能和方便维护。

为了进行通信和执行某些服务器管理活动，SA 在每个托管服务器上安装服务器代理，并通过网关 (SA 核心组件的一部分) 与托管服务器进行通信。服务器代理还会根据来自 SA 客户端的用户输入所示，对托管服务器执行某些操作。

> **备注：** 在 FIPS 模式下，为了确保 SA 组件正常启动和运行，核心服务器上的字符设备 /dev/random 中必须有足够的熵词干可用。

SA 代理

SA 代理是安装在要使用 SA 管理的服务器上的智能软件。在非托管服务器上安装代理后，它将在 SA 核心中注册，之后核心会将该服务器添加到其托管服务器池。SA 代理还会从核心接收命令，并在其本地服务器上启动适当操作，例如软件安装和删除、软件和硬件配置、服务器状态报告、审核等。

在注册代理期间，SA 为每台服务器分配一个唯一的 ID (计算机 ID (MID))，并将此 ID 存储在模型库中。服务器也可由其 MAC 地址进行唯一标识 (网络接口卡的唯一十六进制硬件标识符，用作网络上设备的物理地址)。

SA 网关

SA 网关管理托管服务器和 SA 核心之间、多个核心之间以及卫星端安装和 SA 核心之间的通信。

网关具有多种类型：

- 管理网关
  此网关管理 SA 核心之间以及 SA 核心和卫星端之间的通信。
- 核心网关/代理网关
  这些网关协同合作，以便 SA 核心和代理进行通信。
- 卫星端网关
  此网关将通过管理网关或核心网关与 SA 核心进行通信，具体取决于您的配置。

SA 卫星端

对于没有大量足够潜在托管服务器的远程站点，卫星端安装可以是用于调整完整 SA 核心安装的一个解决方案。通过卫星端安装，您可以在卫星端主机上仅安装所需最少的核心组件，然后卫星端主机可通过 SA 网关连接访问主核心的数据库和其他服务。

卫星端安装还可缓解远程站点(可能通过有限的网络连接与主设施进行连接)的带宽问题。可以将卫星端的网络带宽使用限定在指定的比特率内。这可以帮助您确保卫星端的网络流量不会影响同一个管道上的其他关键系统的网络带宽要求。

卫星端安装通常至少由卫星端网关和软件库缓存组成，这仍然可支持您在远程设施中全面管理服务器。软件数据库缓存包含要安装在卫星端托管服务器上的软件包的本地备份，而卫星端网关则处理与主核心的通信。

SA 托管服务器

SA 托管服务器是已安装 SA 代理并主动受 SA 管理的服务器。

相关主题

- 关于 FIPS 140-2
- 符合 FIPS 140-2 的技术
- 支持的 SA 核心和卫星端操作系统
- 支持的托管服务器操作系统
- 支持的 FIPS 140-2 安全级别
- 首字母缩略词
- 相关行业文档

关于 FIPS 140-2

2001 年 5 月，美国国家标准技术研究院 (NIST) 发布了联邦信息处理标准出版物 140-2《加密模块的安全要求》。该标准规定了在安全系统中利用加密模块保护敏感非加密信息的安全要求。FIPS 140-2 是美国和加拿大政府采用的一项标准，其目的是推广应用已通过验证的加密模块并为联邦机构提供一项安全指标，用于采购符合标准并包含已通过验证的加密模块的设备。

HPE Server Automation (SA) 通过使用符合 FIPS 的加密模块支持 FIPS 140-2。

符合 FIPS 140-2 的技术

SA 使用已通过 NIST 认证过程的加密模块实现 FIPS 140-2 符合性。SA 使用以下符合 FIPS 140-2 的技术。

NSS 加密模块

SA 采用经过 FIPS 140-2 认证的网络安全服务 (NSS) 加密模块，这是一种获得 Mozilla 公共许可证的通用开源加密库。

NSS 加密模块包含基于行业标准 - 公钥加密标准 (PKCS) #11 加密令牌接口版本 2.20 (由 EMC Corporation 安全部门 RSA 发布) 的 API。

TLS/SSL 传输协议

SA 还使用新一代安全套接字层 (SSL)，即传输层安全性 (TLS)。

SA 平台由多个分布式组件构成，这些组件通过不安全的网络传达敏感信息。SSL 是一项经过验证的行业标准，可提供:

- 加密，以确保数据 (事件/用户交互) 无法被截获
- 数据完整性 (MAC)，以防止有意地或无意中在线修改数据
- 身份验证，以防止跨网泄露凭据

尽管 TLS 和 SSL 使用不同的算法建立安全的密钥交换，但是由于它们的功能相同，因此这些协议统称为 TLS/SSL。

SSL 2.0 和 3.0 协议不符合 FIPS 140-2。TLS 是唯一根据 Internet 工程任务组 (IETF) 标准融合了经过 FIPS 140-2 批准的算法的 SSL 变体。

SHA-1/SHA-2 族

安全哈希算法是由国家标准技术研究院 (NIST) 作为美国联邦信息处理标准 (FIPS) 发布的一组加密哈希函数。SA 使用 SHA-256，但也支持 SHA-1 以及 SHA-2 族中的其他哈希函数。

支持的 SA 核心和卫星端操作系统

启用 FIPS 140-2 的 SA 核心在所有支持的 SA 托管平台上受支持。

支持的托管服务器操作系统

启用 FIPS 140-2 的托管服务器在所有支持的 SA 托管平台上受支持，但以下各项除外:

- Red Hat Enterprise Linux 5 on IA 64
- Red Hat Enterprise Linux 5 和 6 on S390X 平台 (Z 系列)
- SUSE Linux Enterprise Server 10 和 11 on S390X 平台 (Z 系列)
- HPUX PA-RISC 11.11、11.23、11.31
- HPUS IA64 11.11、11.23、11.31
- Windows Server 2008 R2 on IA 64

支持的 FIPS 140-2 安全级别

FIPS 140-2 安全级别

SA 组件	支持的 FIPS 140-2 安全级别	NSS 版本	OpenSSL 版本
SA 10.10 及更高版本	级别 1	3.15.1	1.0.1h (2.0.5 FIPS 模块)

SA 加密模式

SA 提供两种加密模式:

- FIPS 140-2 模式 (敏感非加密信息)
- ESM 标准加密 (默认模式)

FIPS 140-2 模式

FIPS 140-2 模式为敏感非加密信息 (SBU) 启用安全性。FIPS 140-2 模式意味着在连接到 SA 核心并与其交换数据的所有相关 SA 组件上部署并启用了 NSS 加密模块。

FIPS 140-2 模式基于 RSA 公钥加密技术，是一个独立于 ESM 标准加密系统的安全加密系统。一旦启用 FIPS 140-2 模式，将不使用 ESM 标准加密系统。

ESM 标准加密

为支持不强制要求 FIPS 140-2 加密的部署，SA 将继续使用其现有的加密算法和密钥库格式。

首字母缩略词

首字母缩略词	全写
ESM	Enterprise Security Management (企业安全管理)
FIPS	Federal Information Processing Standards (联邦信息处理标准)
HMAC	Keyed-Hash Message Authentication Codes (键控哈希消息身份验证代码)
HTTPS	Secure Hypertext Transfer Protocol (安全超文本传输协议) (通过 TLS/SSL)
ECDSA	Elliptical Curve Digital Signature Algorithm (椭圆曲线数字签名算法)。用于为归入最高机密的信息提供 Suite B 安全支持。
IDS	Intrusion Detection System (入侵检测系统)

IEC	International Electrotechnical Commission (国际电工委员会)
IETF	Internet Engineering Task Force (Internet 工程任务组)
ISO	International Organization for Standardization (国际标准化组织)
MD5	Message-Digest Algorithm 5 (消息摘要算法 5)
NIST	National Institute of Standards and Technology (国家标准技术研究院)
NSA	National Security Agency (国家安全局)
NSS	Network Security Services (网络安全服务)
PKCS	Public Key Cryptography Standards (公钥加密标准)
RSA	由 EMC Corporation 安全部门 RSA Security, Inc. 开发的公钥加密技术。该首字母缩略词表示这项技术的发明者 Rivest、Shamir 和 Adelman。
SBU	Sensitive But Unclassified (敏感非加密)。是指通过加密方法保护的信息。
SHA	Secure Hash Algorithm (安全哈希算法)
SSL	Secure Sockets Layer (安全套接字层)；与 TLS 相关
TSL	Transport Security Layer (传输安全层)；新一代 SSL
W3C	World Wide Web Consortium (万维网联合会)

相关行业文档

有关 FIPS 140-2 标准和 OpenSSL 加密模块及其基础技术的详细信息，请参考以下行业资源。

相关行业文档

主题	资源
FIPS PUB 140-2	美国国家标准和技术协会信息技术实验室 (NIST) 发布的信息处理标准 (FIPS) 文档。发布于 2001 年 5 月 25 日。 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
OpenSSL 加密模块	OpenSSL.org 发布的 OpenSSL 加密模块版本 0.9.8j 的 FIPS 140-2 非专有安全策略级别 1 和级别 2 验证。 http://www.openssl.org/docs/fips/fipsvalidation.html http://www.openssl.org/docs/fips/UserGuide-2.0.pdf

相关行业文档(续)

主题	资源
批准的加密模块	NIST 批准的所有加密模块的列表。 http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140valall.htm
PKCS #11	公钥加密标准 (PKCS) #11 的描述。描述加密标记接口 API，允许设备保持独立并在访问多台设备的多个应用程序之间共享资源。 http://www.rsa.com/rsalabs/node.asp?id=2133
传输层协议 (TLS)	新一代安全套接字层 (SSL) - 传输层协议 (TLS) 的概述。 http://en.wikipedia.org/wiki/Transport_Layer_Security 有关如何以及为何执行 TLS 的注释: NIST 于 2005 年发布的《Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations》: http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf
Internet Engineering Task Force (Internet 工程任务组) (IETF)	IETF 的概述。IETF 是一家致力于研发 TLS 协议的组织，旨在促进万维网联合会 (W3C)、标准化国际组织 (ISO) 和国际电工委员会 (IEC) 公认的互联网标准。 http://en.wikipedia.org/wiki/IETF IETF 网站: http://www.ietf.org/

发送文档反馈

如果您对本文档有任何意见，可以通过电子邮件与文档团队联系。如果在此系统上配置了电子邮件客户端，请单击以上链接，此时将打开一个电子邮件窗口，主题行中为以下信息：

重要概念指南 (Server Automation 10.50) 反馈

只需在电子邮件中添加反馈并单击“发送”即可。

如果没有可用的电子邮件客户端，请将以上信息复制到 Web 邮件客户端的新邮件中，然后将您的反馈发送至 hpe_sa_docs@hpe.com 。

我们感谢您提出宝贵的意见！