HP Server Automation

Ultimate 版

软件版本：10.10

集成指南

文档发布日期：2014 年 6 月 30 日
软件发布日期：2014 年 6 月 30 日

法律声明

担保

HP 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。HP 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 HP 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。

Intel® 和 Itanium® 是 Intel Corporation 在美国和其他国家 / 地区的商标。

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

Oracle 和 Java 是 Oracle 和 / 或其附属公司的注册商标。

UNIX® 是 The Open Group 的注册商标。

支持

请访问 HP 软件联机支持网站：

http://www.hp.com/go/hpsoftwaresupport

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

HP 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 HP 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 HP Passport 用户再登录，很多区域还要求用户提供支持合同。要注册 HP Passport ID，请访问：

http://h20229.www2.hp.com/passport-registration.html

要查找有关访问级别的详细信息，请访问：

http://h20230.www2.hp.com/new_access_levels.jsp

支持列表

有关完整的支持和兼容性信息，请参见相关产品发布的支持列表。可在 HP 软件联机支持网站上查找所有支持列表和产品手册，地址为：

http://h20230.www2.hp.com/sc/support_matrices.jsp

您还可以从 HP 软件联机支持产品手册网站下载此发布的 《HP Server Automation Support and Compatibility Matrix》，地址为：

http://h20230.www2.hp.com/selfsolve/manuals

文档更新

适用于此发布的所有最新 Server Automation 产品文档都位于以下 SA 文档库中：

http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html

使用 SA 文档库可以访问与此发布相关的任何指南、发布说明、支持列表和白皮书，还能够以捆绑包的形式下载整个文档集。 SA 文档库按每次发布进行更新，并且每当更新了发布说明或引入了新白皮书时，也会更新 SA 文档库。

如何查找信息资源

使用下列任一方法，可以访问 Server Automation 的信息资源：

方法 1：在新 SA 文档库中按标题和版本访问最新的各个文档

方法 2：在下载了所有手册的本地目录中，使用完整的文档集

方法 3：在 HP 软件文档门户中搜索任何受支持发布的任何 HP 产品文档

访问各个文档：

1. 访问 SA 10.x 文档库：

   http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html
2. 使用您的 HP Passport 凭据登录。
3. 找到所需的文档标题和版本，然后单击 “go”。

在本地目录中使用完整的文档集：

1. 要将完整的文档集下载到本地目录，请执行以下操作：
   a. 访问 SA 文档库：

      http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html
   b. 使用您的 HP Passport 凭据登录。
   c. 找到对应于 SA 10.1 版本的所有手册下载标题。
   d. 单击 “go”链接，将 ZIP 文件下载到本地目录。
   e. 解压缩该文件。

2 要在本地目录中查找文档，请使用文档目录 (docCatalog.html)，它提供了一个指向本地目录中已下载文档的索引门户。

3 要在文档集的所有文档中搜索关键字，请执行以下操作：

a 打开本地目录中的任何 PDF 文档。

b 选择 “Edit” > “Advanced Search”（或按 Shift+Ctrl_F）。

c 选择 “All PDF Documents”选项，并浏览本地目录。

d 输入关键字，然后单击 “Search”。

在 HP 软件文档门户中查找更多文档：

访问 HP 软件文档门户：

http://h20230.www2.hp.com/selfsolve/manuals

需要注册 HP Passport 才能登录此站点。要注册 HP Passport ID，请单击 “HP Passport”登录页面上的 **“New users - please register”** 链接。

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 HP 销售代表联系。有关任何版本的列表，请参见 “文档变更说明”。

产品版本

Server Automation 有两种版本：

- Server Automation (SA) 是 Server Automation Ultimate 版。有关 Server Automation 的信息，请参见 《SA Release Notes》、《SA 用户指南：Server Automation》。
- Server Automation Virtual Appliance (SAVA) 是 Server Automation Premium 版。有关 SAVA 所包括内容的详细信息，请参见 《SAVA Release Notes》和 《SAVA 概览》指南。

目录

1 SA-DMA 集成

本章将讨论 HP Database and Middleware Automation (DMA) 流与 HP Server Automation (SA) 的结合使用情况。 DMA 使用 SA 作为其服务器管理工具。

什么是 DMA?

DMA 解决了自定义脚本或使用分散的临时工具所带来的不足。它提供行业标准的最佳实践和主题内容专业技术来应对符合性、中间件和数据库修补、中间件和数据库配置以及代码发布方面的挑战。借助 DMA， IT 团队能够在整个企业内强制执行组织标准。它支持多个供应商的数据库和中间件技术。

集成任务

《HP DMA Installation Guide》中涵盖了 DMA 与 SA 的集成内容，该文档可在以下位置找到：

http://support.openview.hp.com/selfsolve/documents

请参考 《HP DMA Installation Guide》的相应章节完成以下任务：

任务	章节
安装 DMA - 包括所有与 SA 的必需集成	“How to Install HP DMA”
卸载 DMA - 包括从 SA 托管服务器卸载 DMA	“How to Uninstall HP DMA”
升级到新的 DMA 版本 - 包括在 SA 核心上重新安装 DMA APX	“How to Upgrade HP DMA”
将当前 DMA 版本链接到 SA	“How to Link HP DMA into HP Server Automation”

2 SA-NA 集成

SA-NA 集成概述

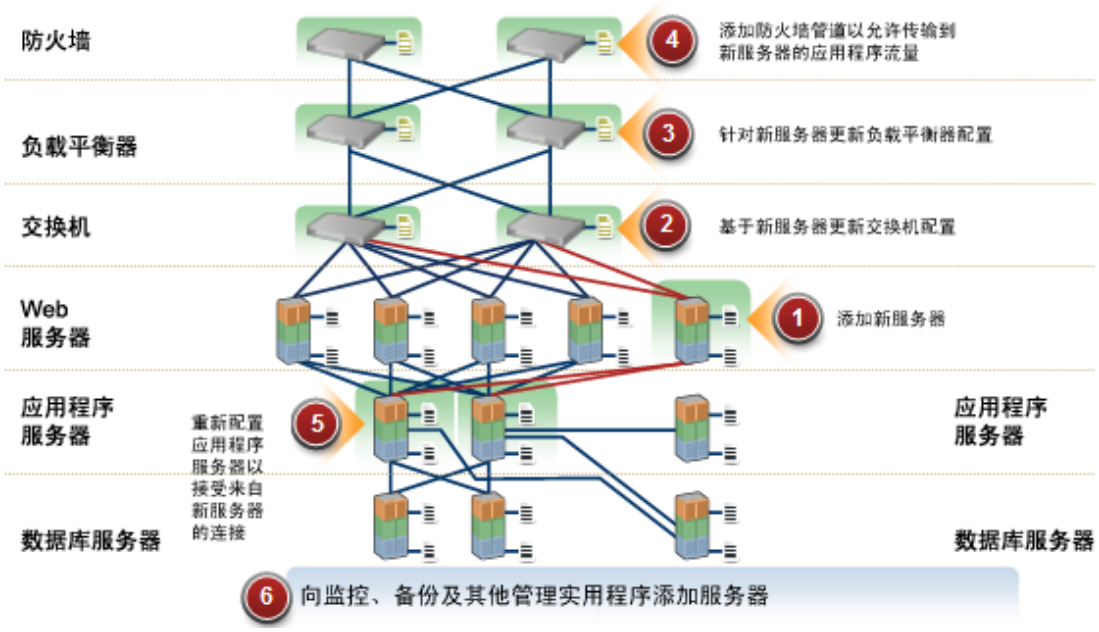
在 IT 环境中实施更改通常要求网络管理员、系统管理员和应用程序架构师的协同合作，其中应用程序架构师必须管理可能由服务器 （具有不同操作系统）和网络设备 （可以包括防火墙、负载平衡器、交换机、服务器、 Web 应用程序等）构成的应用程序环境。

例如，在某些环境中，您需要对应用程序前端的网络设备进行更改，例如负载平衡器、防火墙、交换机等。

SA-NA 集成通过让您了解服务器连接到网络设备的方式，并通过这些设备仔细检查托管服务器，使这个过程变得更加简单。利用此信息，可以确定所有设备之间的关系，以及协调并实施必要的更改。

图 1 显示了您可以通过 SA-NA 集成执行的某些协调任务。

图 1　　使用 SA-NA 集成执行的协调任务的概述



本节包含有关如何配置 NA 与 SA 的集成的信息。在建立集成之后，您可以查看设备详细信息、检查网络设备与服务器之间的连接、确定不匹配的双工以及查看组合设备的历史记录信息。它还包含有关在环境中实施更改以及生成网络报告的信息。

要支持采用集成方法在环境中进行更改 （例如服务器重新分配）、确保服务器和网络设备之间的符合性以及检测和解决双工不匹配， SA-NA 集成提供了以下接口点：

- HP Server Automation (SA)
- Network Automation (NA)
- SA 全局 Shell
- HP Server Automation Visualizer （在 SA 中）
- HP 报告 （在 SA 中）

SA-NA 集成功能

在配置 SA-NA 集成之后，您可以执行以下任务：

- 查看有关 SA 托管服务器及其附加网络设备、以及它们之间的网络连接（接口和端口）的汇总和详细硬件信息。
- 使用 SA 全局文件系统 (OGFS) 执行以下操作：
  - 通过跟踪托管服务器和已连接网络设备关联的物理连接，在它们之间进行导航
  - 查找网络设备配置
  - 在服务器和网络设备之间运行脚本。
- 从 SA 脚本调用 NA 脚本，以自动化服务器和网络设备之间的操作。
- 使用 SA 和 NA 中的功能创建图表，用以阐明环境中的托管服务器、网络设备和层 2 （以及推断层 1）连接。
- 使用 SA 确定、排除和修正托管服务器和网络设备之间的配置双工不匹配。
- 使用 SA 对可以同时包含服务器和网络设备的 SA 设备组执行操作。
- 使用 SA 查看组合服务器和网络设备事件历史记录日志，该日志记录对环境中应用程序所做的更改。
- 使用 SA 将组合事件历史记录日志导出到 CSV 和 / 或 HTML 文件。
- 使用 NA 直接访问其他网络设备详细信息和事件历史记录。
- 使用 SA 运行网络报告，这些报告可确定层 2 和推断层 1 连接以及配置不匹配 （双工符合性）。

本文档中提到的*连接*，除非另有说明，一律为物理连接。

如何收集 NA 数据

SA-NA 集成功能使用 NA 拓扑数据收集和 NA 双工数据收集诊断工具来收集有关网络设备的信息。

NA 拓扑数据收集诊断

NA 拓扑数据收集诊断指示 NA 为所有交换机收集 MAC 地址。 MAC 地址用于发现物理连接并将其添加到 SA 数据模型。

例如，在将服务器添加到交换机之后，会在下一次运行 NA 拓扑数据收集诊断时收集该信息。您也可以针对特定网络设备手动运行 NA 拓扑数据收集诊断或 NA 双工数据收集诊断。有关诊断的详细信息，请参见 《NA User Guide》。

➤ 为提高 NA 性能，请勿在多个设备上每周运行一次以上这些诊断。如果需要频繁刷新 NA 数据，请联系您的支持代表。可在单个设备上多次运行这些诊断。

NA 双工数据收集诊断

对于网络设备，速度和双工由 NA 双工数据收集诊断进行收集，此诊断会在设备初次添加到 NA 之后运行，之后会根据定义的计划运行。

要确保拥有网络设备的最新速度和双工信息，SA 建议您设置一个运行诊断的定期计划。有关此诊断和计划的详细信息，请参见双工不匹配 （第 24 页）和 《NA User Guide》。

NA 数据库 /SA 数据库

NA 和 SA 数据库未集成 - NA 和 SA 管理各自的数据。

身份验证

针对 SA/NA 集成功能，身份验证由 SA 进行处理。有关详细信息，请参见 NA 身份验证配置 （第 17 页）。仅 NA 功能继续使用 NA 凭据进行身份验证。

先决条件

必须符合以下先决条件。

时间要求

必须同步 SA 和 NA 核心服务器，它们必须具有相同的时间和相同的时区设置。

NA 集成端口要求

在配置 NA 集成之前，请确保 SA 和 NA 可以通过以下端口进行相互通信：

- **端口 1032 （NA 到 SA）**

  NA 必须能够访问正在运行 SA Web 服务数据访问引擎组件 （组件切分捆绑包的一部分）的服务器上的端口 1032。默认情况下， Web 服务数据访问引擎侦听端口 1032。

- **端口 8022 (Unix) / 端口 22 (Windows) （SA 到 NA）**

  要使全局文件系统 (OGFS) 功能显示有关网络设备的数据，SA 必须对端口 8022（基于 Unix 的 NA 服务器）或 22 （基于 Windows 的 NA 服务器）具有访问权限。

- **针对 NA API 的 RMI 端口**

  NA API 使用 Java RMI 连接 NA 服务器。 SA 对 NA 集成使用 NA API。 RMI 要求开放以下端口：

  — **端口 1099**

  JNDI

  — **端口 4444** （适用于 NA 版本 9.10 和较早版本）

  RMI 对象

  — **端口 4446** （适用于 NA 版本 9.20 和更高版本）

  RMI 对象

  — **端口 1098**

  RMI 方法

SA-NA 集成配置任务

SA 管理员必须对 SA 核心服务器执行某些任务，才能启用 SA-NA 集成。

配置包括更改 NA 和 SA 中的某些配置设置、针对 NA 拓扑数据运行诊断以及配置某些用户权限。

SA 客户端与 NA 的通信

确保 SA 客户端可以与 NA 进行通信。如果 SA 客户端无法与 NA 服务器进行通信，请参见在 SA 客户端中重置 NA 主机 （第 20 页）。

编辑 jboss_wrapper.conf 文件

仅 7.6 之前的 NA 版本必需。版本 7.6 和更高版本的 `jboss_wrapper.conf` 中不包括这些条目。

您应调整 `wrapper.java.additional.x` 的值，其中 `x > 8` 为连续的值。

例如：

将以下内容：

```
wrapper.java.additional.1=-DTCMgmtEngine=1
wrapper.java.additional.2=-Duser.dir=/opt/NA750/server/ext/jboss/bin
wrapper.java.additional.3=-Xmn170m
wrapper.java.additional.4=-Djava.awt.headless=true
wrapper.java.additional.5=-Dfile.encoding=UTF8

#Following are added for bug 150387
wrapper.java.additional.6=-Dorg.omg.CORBA.ORBClass=com.sun.corba.se.internal.
Interceptors.PIORB
wrapper.java.additional.7=-Dorg.omg.CORBA.ORBSingletonClass=com.sun.corba.se.
internal.corba.ORBSingleton
wrapper.java.additional.8=-Xbootclasspath/p:/opt/NA750/server/ext/wrapper/
lib/CORBA_1.4.2_13.jar

#Add location of keystore. This is used to make SSL request.
wrapper.java.additional.9=-Djavax.net.ssl.trustStore=/opt/NA750/server/ext/
jboss/server/default/conf/truecontrol.keystore

# Bug 171948 - Need more PermGen
wrapper.java.additional.10=-XX:MaxPermSize=80m
```

更改为：

```
wrapper.java.additional.1=-DTCMgmtEngine=1
wrapper.java.additional.2=-Duser.dir=/opt/NA750/server/ext/jboss/bin
wrapper.java.additional.3=-Xmn170m
wrapper.java.additional.4=-Djava.awt.headless=true
wrapper.java.additional.5=-Dfile.encoding=UTF8

#Following are added for bug 150387
#wrapper.java.additional.6=-Dorg.omg.CORBA.ORBClass=com.sun.corba.se.internal
.Interceptors.PIORB
#wrapper.java.additional.7=-Dorg.omg.CORBA.ORBSingletonClass=com.sun.corba.se
.internal.corba.ORBSingleton
#wrapper.java.additional.8=-Xbootclasspath/p:/opt/NA750/server/ext/wrapper/
lib/CORBA_1.4.2_13.jar

#Add location of keystore. This is used to make SSL request.
wrapper.java.additional.6=-Djavax.net.ssl.trustStore=/opt/NA750/server/ext/
jboss/server/default/conf/truecontrol.keystore

# Bug 171948 - Need more PermGen
wrapper.java.additional.7=-XX:MaxPermSize=80m
```

SA 配置更改

请完成以下任务为 NA 集成准备 SA：

- **指定 NA 服务器名称**

  如果在 NA 核心安装程序采访期间未指定 SA 服务器名称，则必须在 `/etc/opt/opsware/twist/twist.conf` 文件中指定 `twist.nasdata.host=<hostname>` 参数的值。

  查找以下条目：

  ```
  twist.nasdata.host=
  ```

添加 NA 服务器的主机名或 IP 地址。

有关修改此文件的详细信息，请参见 《SA 管理指南》。

➤ 如果已安装多个切分组件捆绑包，则必须在所有切分上编辑 `twist.conf` 文件。然后，必须为每个切分组件捆绑包重新启动所有 NA 服务和 Web 服务数据访问引擎。

- **在 SA 中指定 NA 端口 （仅 Windows）**

  如果 NA 正在 Windows 服务器上运行，则必须在 `/etc/opt/opsware/hub/hub.conf` 文件中将端口设置参数从 `nas.port=8022` 更改为 `nas.port=22`。

  默认的 Windows 服务器安装在端口 22/23 上运行代理 SSH/Telnet 服务器，而不是在 Unix 默认端口 8022/8023 上运行。

➤ 在更改此配置之后，必须重新启动托管切分组件捆绑包的服务器。

- **启用 spin.cronbot.check_duplex.enabled 参数**

  必须为 NA 集成启用 `spin.cronbot.check_duplex.enabled` 系统配置参数。

  要启用此系统配置参数，请执行以下步骤：

  a 在 SA 客户端中选择 “管理”选项卡。

  b 在导航窗格中选择 “系统配置”。将显示包含系统配置参数的 SA 组件、设施和领域。

  c 在 SA 组件列表中，选择 “数据访问引擎”。将显示此组件的系统配置参数。

  d 查找参数 `spin.cronbot.check_duplex.enabled`。

  e 在 “值”列中，选择新值按钮  并将值设置为 1。

  f 选择 “还原”按钮放弃所做更改，或者选择 “保存”按钮保存所做更改。

  有关系统配置的详细信息，请参见 《SA 管理指南》。

配置 NA 以进行集成

➤ 要配置 NA 与当前 SA 版本的集成，必须安装兼容的 Network Automation (NA) 版本。有关详细信息，请参见 《NA Support Matrix》。

NA 管理员应对 NA 服务器执行以下任务。

SA 网关要求

必须将 NA 配置为使用要集成的 SA 核心的主网关。有关在 NA 中指定 SA 核心主网关的详细信息，请参见 《NA Satellite Guide》。

用户权限

SA-NA 集成的访问权限基于两个单独的数据库：NA 数据库和 SA 数据库。 NA 使用自己的数据库进行授权。 SA 使用其他安全机制进行授权。但是，对于 NA 集成，所有身份验证 （针对 NA 和 SA）都由 SA 进行处理。

在将 NA 配置为使用 SA 身份验证时， NA 会尝试首先针对 SA 进行身份验证。如果 NA 无法对 SA 进行身份验证，它将退回到 NA 数据库。如果 NA 数据库中存在一个帐户，则仅在将该用户配置为允许退回身份验证时，才能允许此退回操作。有关 NA 身份验证的详细信息，请参见 《NA User Guide》。

通过 SA 对新用户进行身份验证时，会在 NA 中创建一个帐户。此帐户位于默认用户组中，该组是在 NA 的 “管理设置” 中启用 SA 身份验证时指定的。此用户组 （可配置）控制系统管理员分配给 SA 用户的默认权限。

您必须具有所需的权限集，才能查看服务器和网络设备。要获取这些权限，请联系您的 SA 管理员，或者参见 《SA 管理指南》获取详细信息。

NA 身份验证配置

要设置 SA-NA 集成，您必须将 NA 配置为使用 SA 身份验证。在开始此配置之前，您必须具有以下信息 （请参见图 3）：

- **Twist 服务器**：托管 Web 服务数据访问引擎的服务器的 IP 地址或主机名 （`twist`：切分组件捆绑包部分，通常安装在 SA 核心主机上，但也可以安装在其他主机上）。
- **Twist 端口号**：Web 服务数据访问引擎侦听的端口号。
- **Twist 用户名**：Web 服务数据访问引擎用户名。
- **Twist 密码**：Web 服务数据访问引擎用户密码。
- **OCC 服务器**：托管命令中心 (OCC) 的服务器的 IP 地址或主机名。
- **默认用户组**：新 SA 用户的默认用户组。

要在 NA 中更改身份验证设置，请执行以下任务：

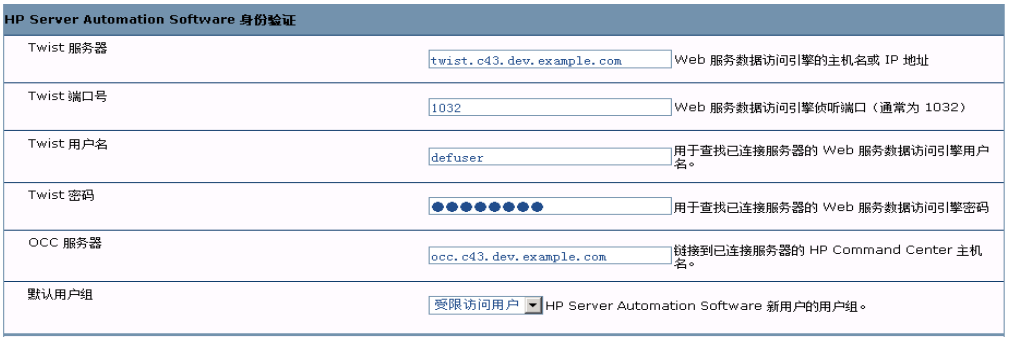
1. 登录到 NA。
2. 选择 “管理” > “管理设置” > “用户身份验证”，显示 “管理设置 — 用户身份验证” 页面。
3. 在 “外部身份验证类型” 部分中，使用单选按钮选择 “HP Server Automation software & TACACS+”（如果使用），如图 2 所示。

图 2　　NA 中的外部身份验证类型

4 向下滚动页面并完成 “HP Server Automation software 身份验证”部分中的所有字段，如图 3 所示。

NA 在收集层 2 数据时使用 Web 服务数据访问引擎 (twist) 用户名和密码。NA 使用 Twist 用户权限按 MAC 地址收集服务器接口信息。 Twist 用户必须对服务器信息具有读取访问权限。

图 3 HP Server Automation Software 身份验证



5 单击 “保存”，保存所做的配置更改。

有关 NA 配置的详细信息，请参见 《NA User Guide》。

配置与 CiscoWorks NCM 的 SA-NA 集成

如果使用 CiscoWorks NCM 1.2 部署 SA，则必须进行某些配置更改。某些 CiscoWorks NCM 部署 （其中 CiscoWorks LMS 与 NCM 共存）使用非标准的端口，这些端口会影响与 SA 的集成。

要确定需要进行哪些更改，请执行以下任务：

阶段 1：编辑 tomcat4-service.xml：

1 登录 NCM 服务器。

2 打开以下 XML 文件：

<NCM_install_dir>/server/ext/jboss/server/default/deploy/tomcat4-service.xml。

3 搜索字符串 'scheme=https'。

4 检查先前条目，此条目应为

port = "port_no"。

如果 port_no 值为 443，则转至阶段 4，否则，注明指定端口并继续进行阶段 2。

阶段 2：分配端口号：

1 登录 SA 客户端。

2 在 SA 客户端的 “工具”菜单中，选择 “选项”。

3 在 “设置选项”窗口中，选择 “Network Automation”。

4 在 “主机”字段中，将 :<port> 附加到主机名后面，其中 <port> 是在步骤 4 的阶段 1 中找到的端口号，例如：

mycore.opsware.com:443

单击 “保存”。

此时将显示以下警告：“General.Host：必须是有效的主机字符串。”忽略此警告。关闭 “设置选项”窗口。

（必须对 SA 客户端的每个用户执行阶段 2。）

阶段 3：编辑主数据访问引擎文件：

1. 登录安装主数据访问引擎 （基础结构组件捆绑包的一部分）的 SA 核心服务器。
2. 打开 `/opt/opsware/twist/twist.sh` 文件并将以下行：

   `https://$NASHOST/tcdocs/truecontrol-client.jar`

   更改为 （假设 443 是在步骤 4 的阶段 1 中注明的端口）：

   `https://${NASHOST}:443/tcdocs/truecontrol-client.jar`
3. 重新启动托管 Web 服务数据访问引擎 （组件切分捆绑包的一部分）的服务器：

   `/etc/init.d/opsware-sas restart twist`

   （您需要为每个 Web 服务数据访问引擎服务器安装执行阶段 3。）

阶段 4：分配 SSH 端口：

1. 登录 NCM。
2. 选择 “管理” > “管理设置” > “Telnet/SSH”，显示 “管理设置 - Telnet/SSH”页面。
3. 在 “SSH 服务器”部分中，查找 SSH 服务器端口。
4. 如果端口为 8022，则此阶段完成；否则，请注明使用的端口并继续进行阶段 4 步骤 5。
5. 登录安装全局文件系统 (OGFS) （切分组件捆绑包的一部分）的 SA 核心服务器。
6. 打开 `/etc/opt/opsware/hub/hub.conf` 文件，并将 `nas.port` 的值更改为在阶段 4 步骤 4 中找到的端口。例如：

   `nas.port=9022`

收集拓扑数据

在完成 SA-NA 集成任务之后，必须运行 NA 拓扑数据收集和 NA 双工数据收集诊断。有关运行这些实用程序的说明，请参见 《NA User Guide》。

故障排除提示

要测试 SA 是否与 NA 进行通信，请检查以下条件：

- 您可以使用 SA 凭据登录 NA。这将验证 NA 是否可以与 SA 进行通信。
- 将 NA “管理设置”的 “外部身份验证类型”下指定的 SA 凭据设置为 SA。这将确保 NA 可以查看服务器 MAC 地址。
- NA 拓扑收集诊断已成功运行。要验证此条件，请搜索任务并检查其结果。这确保 NA 已收集 MAC 地址，并尝试在 SA 中查找这些地址。

在 SA 客户端中重置 NA 主机

某些 SA-NA 集成功能要求 SA 客户端 (Java) 打开 NA Web 接口（直接从 SA 打开），以便您可以访问某些 NA 事件的其他详细信息。如果您的管理员已完成《SA Installation Guide》中的设置任务，但是 SA 客户端无法直接与运行 NA 主机（服务器）Web 接口的服务器进行通信，则可能需要在 SA 客户端中更改 NA 选项。例如，如果防火墙阻止 SA 客户端访问 NA 主机，则需要指定充当 NA 主机代理的服务器名称。这将覆盖默认设置。必须在运行的 SA 客户端无法与 NA 主机通信的每个桌面上执行此任务。

要在 SA 客户端中重置 NA 主机，请执行以下步骤：

1. 在 SA 客户端窗口的 “工具” 菜单中，选择 “选项”。
2. 在 “视图” 窗格中，选择 “HP Network Automation”。
3. 在 “主机” 字段中，输入充当 NA 主机代理的服务器名称，例如 m208，它是 m208.example.com NA 主机的代理。
4. （可选）单击 “恢复默认值”，恢复先前保存的 NA 主机名。
5. （可选）单击 “测试” 打开 NA 登录窗口。
6. 单击 “保存”。

使用 SA-NA 集成

在成功配置 SA-NA 集成之后，以下功能将可用。

网络设备和服务器之间的连接

SA-NA 集成功能基于层 2 连接和推断层 1 连接。请参见图 4 了解 OSI 模型层的定义。

图 4　　OSI 七层模型

数据链路连接

SA-NA 集成功能包括检测数据链路 （层 2）连接以及报告物理 （层 1）和数据链路连接。这些数据链路连接包括直接连接到托管服务器的交换机，以及通过其他交换机间接连接的交换机。这些连接是通过关联由设备报告的 MAC 地址发现的，这些设备具有服务器和交换机的已知 MAC 地址。

物理连接

物理连接是从数据链路连接推断出来的。请参见推断的物理连接 （第 27 页）。物理连接代表服务器和交换机之间的直接连接 （电缆）。

在 SA 客户端中，可以在 “服务器管理器”和 “网络设备资源管理器”中查看物理连接，在 Service Automation Visualizer (SAV) 中查看详细的布局图。在 NA 图表功能中，可以查看物理、数据链路或网络 （层 3）连接。

SA 中的网络设备信息

除有关托管服务器和网络设备的基本硬件详细信息以外， SA-NA 集成 功能还报告有关网络接口和网络端口的以下信息：

- 在服务器端，网络接口具有以下属性：
  - MAC 地址
  - 子网掩码
  - 接口类型
  - IP 地址
  - DHCP 设置
  - 连接交换机端口
  - 速度
  - 双工 （不包括 Windows）。
- 在网络设备端，网络端口具有以下属性：
  - 端口名称
  - 速度
  - 双工设置
  - 连接设备
  - 接口类型。

对于大多数设备，当连接的两端 （服务器和网络设备）设置为自动协商模式时，自动协商将运行得最好。例如，双工策略可以指定应将端口设置为全双工、半双工，还是自动双工和非全 （自动）双工。全 （自动）双工设置表示已将端口设置为自动协商，它与全双工进行协商。

以下任务将描述如何在 SA 中直接访问服务器和网络设备的详细硬件信息。有关如何在 NA 中直接访问有关网络设备的硬件信息的说明，请参见NA 中的网络设备信息 （第 23 页）。

查看网络接口

要查看服务器的硬件信息 （包括网络接口），请执行以下步骤：

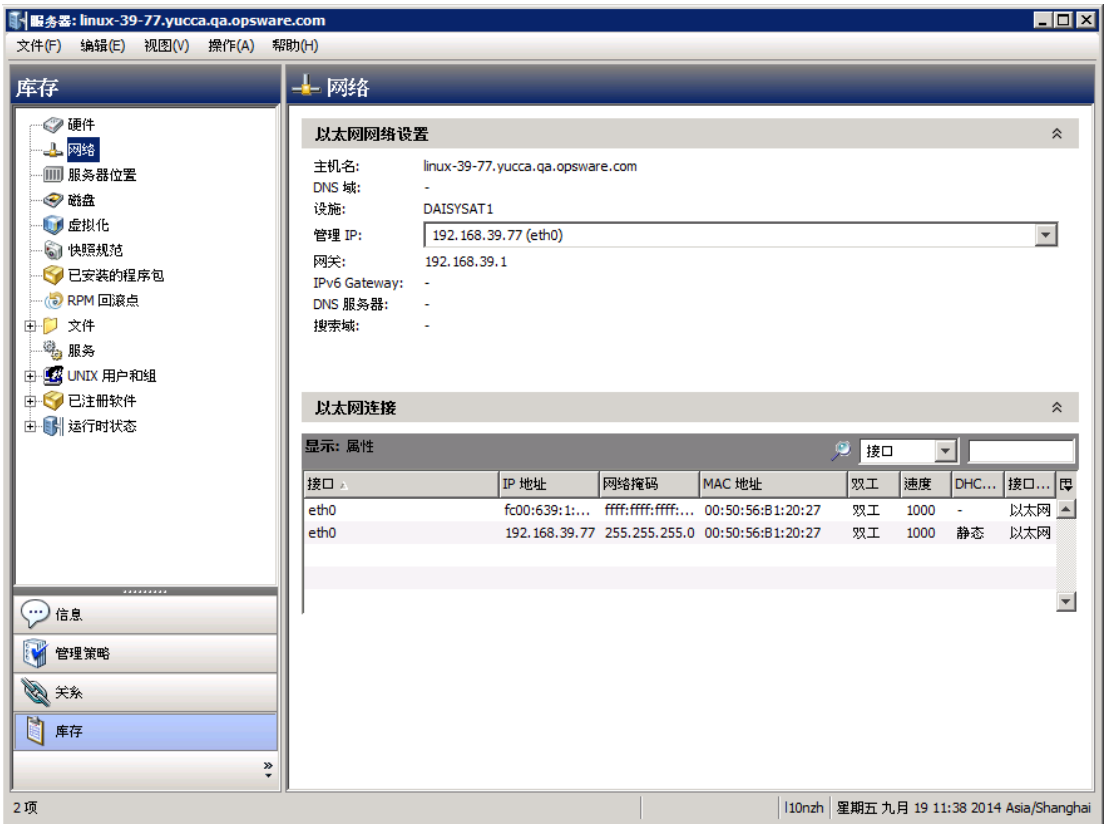
1 登录 SA 客户端。

2 在导航窗格中，选择 “设备” > “所有托管服务器”。

3 在 “视图” 下拉列表中，选择 “网络”。

4 双击内容窗格中的服务器，将在服务器资源管理器中显示硬件详细信息 （请参见图 5）。

图 5 服务器资源管理器中的硬件视图



查看网络端口

要查看网络设备的硬件信息 （包括网络端口），请执行以下步骤：

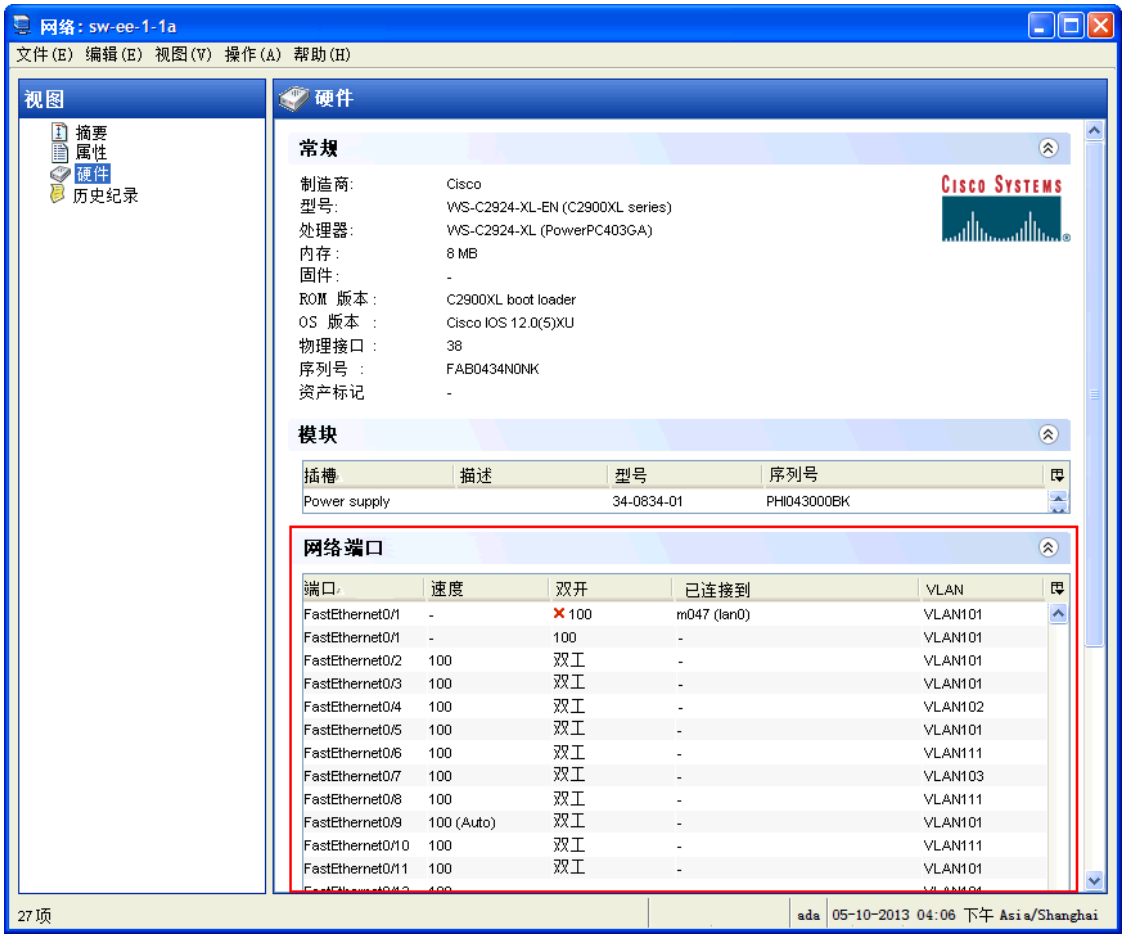
1 登录 SA 客户端。

2 在导航窗格中，选择 “设备” > “设备组” > “Public”，然后选择一个设备组。

3 在 “内容” 窗格中双击网络设备，显示 “网络设备资源管理器”。

4 在“视图”窗格中，选择“硬件”将显示有关选定网络设备的信息。请参见图 6。

图 6 网络设备资源管理器中的硬件视图



NA 中的网络设备信息

为了帮助您执行涉及环境中网络设备的故障排除任务，您可以通过直接登录 NA，检查其他网络设备详细信息和网络设备事件历史记录。 SA-NA 集成功能提供了一个登录选项，通过此选项，您可以访问记录在 NA 中的有关网络设备及其事件历史记录的详细信息。

查看网络设备

要查看网络设备的详细信息，请执行以下操作：

1 在导航窗格中，选择“设备” > “设备组” > “Public”。

2 在“内容”窗格中选择一个网络设备。

图 7 NA 中的网络设备详细信息

查看事件历史记录

在“事件详细信息”窗口中，单击“设备”链接查看其他信息，例如添加此设备的时间戳、上一次快照以及上一次配置更改。

图 8 NA 中网络设备的事件详细信息

双工不匹配

SA-NA 集成功能提供对双工不匹配的自动检测。双工不匹配是托管服务器和连接的网络设备的速度和双工之间的配置不匹配。

对于服务器网络接口，会在每次硬件注册期间收集速度和双工信息 （每隔 24 小时收集一次）。

由于缺少用于确定服务器（运行 Windows 操作系统）双工的独立于设备的方法， Windows 的服务器代理不会报告预置的双工设置。可将自定义脚本添加到服务器代理，以便收集和报告某个网络接口的速度和双工设置。有关如何创建此脚本并将此脚本与代理集成的说明，请联系您的支持代表。

在 SA 客户端中选择 “视图” > “刷新” 或按 F5，将不会 更新服务器的速度和双工信息。在运行 NA 双工数据收集诊断时，会更新此数据。请参见 NA 双工数据收集诊断 （第 13 页）。

对于网络设备，速度和双工由 NA 双工数据收集诊断进行收集，该诊断会按照定义的计划运行。要确保拥有网络设备的最新速度和双工信息，建议您设置一个运行诊断的定期计划。请参见 《NA User Guide》。

如果服务器的网络接口信息 （速度和双工）与连接的网络设备的网络端口信息 （速度和双工）不匹配，则此设备会被认为不兼容。

在 SA-NA 集成功能中，您可以通过使用图表板查看在顶部级别确定的双工不匹配。还可以通过分别使用服务器管理器和网络设备资源管理器，查看按服务器和网络设备确定的双工不匹配。

在图表板中查看双工不匹配

有关双工符合性级别及其在图表板中的显示方式的信息，请参见 《SA 用户指南：审核与符合性》。

查看按服务器的双工不匹配

要使用服务器管理器查看双工不匹配，请执行以下步骤：

1. 在导航窗格中，选择 “设备” > “所有托管服务器”。
2. 在内容窗格中选择一个服务器。
3. 双击此服务器以显示 “服务器管理器”。
4. 在 “视图” 窗格中选择 “硬件”。
5. 在 “网络接口” 部分的 “双工” 列中，查看检测到的不匹配。在 “双工” 列中，位于双工设置 （全双工、半双工、自动双工）前面的  图标可确定不匹配。

查看按网络设备的双工不匹配

要使用网络设备资源管理器查看双工不匹配，请执行以下步骤：

1. 在导航窗格中，选择 “设备” > “设备组” > “Public”。
2. 在 “内容” 窗格中选择一个网络设备。
3. 双击此网络设备以显示 “网络设备资源管理器”。
4. 在 “视图” 窗格中选择 “硬件”。
5. 在 “网络端口” 部分的 “双工” 列中，查看检测到的不匹配。在 “双工” 列中，位于双工设置 （全双工、半双工、自动双工）前面的  图标可确定不匹配。请参见图 5。

网络报告

为了帮助排除有关物理连接和双工符合性的问题，您可以运行和检查网络报告。通过使用 SA 客户端的报告功能，您可以生成以下网络报告，这些报告可以确定环境中托管服务器和网络设备之间的层 1 连接：

按网络设备的连接

此报告列出到某个选定网络设备的所有物理连接。

按服务器的连接

此报告列出到某个选定托管服务器的所有物理连接。

有关如何运行、导出和打印这些报告的信息，请参见 《SA 报告指南》。

网络图表

您可以使用 SA 中的 Service Automation Visualizer (SAV) 功能和 NA 中的图表功能创建详细的图表，这些图表可以阐明环境中的托管服务器、网络设备以及层 2 和层 1 连接。此外，还可以将这些网络图表导出到 `.gif`、 `.jpg` 和 `.svg` 文件，对其进行批注和将其用于其他应用程序。

有关 SAV 和图表工具的详细信息，请参见 《SA 用户指南：Service Automation Visualizer (SAV)》 和 《NA User Guide》。

启动 HP Server Automation Visualizer

要访问 SAV，请执行以下步骤：

1. 从导航窗格中，选择 “设备” > “所有托管服务器”。
2. 在内容窗格中，选择一个或多个服务器。
3. 在 “工具” 菜单中，选择 “HP Server Automation Visualizer”，然后选择以下选项之一：
   - 选择 “新建” 打开 SAV 窗口。
   - 选择 “打开” 将打开先前保存的拓扑。
4. 要创建和导出拓扑图，请参见 《SA 用户指南：Service Automation Visualizer (SAV)》 中使用 HP Server Automation Visualizer 的步骤。

启动 NA 图表

有关如何启动和使用 NA 图表功能的说明，请参见 《NA User Guide》。

NA 和 SA 全局 Shell

您可以使用 SA 全局文件系统 (OGFS) 在服务器和连接的网络设备之间进行导航，方法是跟踪 OGFS 的 /opsw/Servers/@ 和 /opsw/Network/@ 目录中服务器和网络设备之间的物理连接。

此外，还可以在 OGFS 中运行三种类型的 NA 脚本：

- 命令
- 高级
- 诊断

这些脚本与 OGFS 中的 /opsw/Scripts/Network 下的三个目录相对应。请参见 《SA 用户指南：Server Automation》中的 “网络目录”。

您还可以编写 Bourne shell 和 Python 脚本，它们在 OGFS 中运行时可执行以下任务：

- 查找服务器和网络设备。
- 查找连接到指定交换机的所有服务器。
- 查找双工不匹配的服务器。
- 显示特定服务器的网络接口。
- 获取所有设备的 IP 地址。
- 比较两个文件以确定网络设备的配置更改。
- 更改设备详细信息，例如 snmp-location。

启动 OGFS

要在全局 Shell 功能中访问 OGFS，请执行以下步骤：

1. 在 “工具”菜单中，选择 “全局 Shell”启动终端窗口。有关如何使用 OGFS 的详细信息，请参见 《SA 用户指南：Server Automation》中的 “打开全局 Shell 会话”。
2. 要在服务器和连接的网络设备之间进行导航，请使用《SA 用户指南：Server Automation》的“SA 全局 Shell”和 “OGFS 目录”中描述的指南。

远程终端 (rosh)

通过 rosh 实用程序，您可以登录设备 （服务器和网络设备）并运行本地命令。您将从全局 Shell 会话中调用 rosh。可以交互运行 rosh 和输入本地命令，也可以将本地命令指定为 rosh 的一个选项。例如，可以使用 rosh 登录交换机，然后运行 show vlan 命令查看所有 VLAN 详细信息。

有关如何使用 rosh 实用程序的详细信息，请参见 《SA 用户指南：Server Automation》中的 “远程终端”和 “使用 rosh 登录托管服务器”。

推断的物理连接

SA-NA 集成功能还包括针对推断的物理 （层 1）连接的检测和报告功能。这些连接是从数据 （例如由交换机发现的 MAC 地址）推断而来，系统将捕获这些连接并将其添加到 SA 数据模型。

这些物理连接 （推断的层 1 数据）基于启发。在 OSI 模型中，每个层是用于将此层隐藏在下方的一个抽象层。因此，从设备收集的层 2 数据无法生成 100% 精确的层 1 数据。尤其是在任意以下条件存在时，层 1 数据可能不正确：

- 设备没有返回发现 MAC 地址的端口号。
- 在 NA 收集拓扑数据 （在发现 MAC 地址的位置）的几分钟内设备之间无流量。
- 两个托管设备之间存在一个非托管设备。
- 两个托管设备之间存在一个集线器。

在 SA 客户端中，可以通过在全局 Shell 中的网络设备目录之间导航，查看推断的层 1 连接。

设备组和 NA

设备组可帮助您以对组织有意义的方式将设备分类 （服务器和网络设备）。例如，可以按客户、设施、使用情况、应用程序等对设备进行分组，然后对组中的所有设备执行操作。

在 SA 中，设备组可以包含托管服务器和 网络设备，也可以只 包含托管服务器。在 NA 中，设备组只包含网络设备。只能在 NA 中创建和编辑网络设备组。有关如何使用 `rosh` 实用程序的详细信息，请参见 《NA User Guide》。

要监控在多个服务器上运行并依赖于环境中多个网络设备的某个应用程序，HP 建议您将此应用程序建模为设备组，其中包含运行此应用程序的所有服务器和网络设备。这可以帮助您通过使用 SA 来排除应用程序问题。

关联 NA 设备组

将 SA 中的公用设备组与 NA 中的设备组关联时，您将能够监控感兴趣的所有服务器和网络设备的信息。通过使用相同组名称，可关联设备组。

关联的设备组具有以下要求：

- SA 设备组是公用组。
- SA 设备组是静态组。
- 关联的 NA 和 SA 设备组的名称相同。

要关联 SA 和 NA 中的设备组，请执行以下步骤：

1. 在导航窗格中，选择 “设备” > “设备组” > “Public”。
2. 在内容窗格中选择一个设备组。
3. 双击此设备组，然后选择 “打开” 以显示 “设备组管理器”。
4. 在 “视图” 下拉列表中，选择 “属性”。
5. 选中 “与同名 NA 设备组关联” 复选框，启用此功能。
6. 从 “文件” 菜单中，选择 “保存”。

3 SA-OO 集成 - 运行流

本章描述系统集成员和流管理员如何使用 Server Automation (SA) 设置和运行流。它还描述用户如何运行流。流是用于执行某些最常见自动任务的操作。

通过 SA-Operations Orchestration (OO) 集成，流作者可以构建与 SA 集成的 OO 流，用户可以从 SA 运行流。有关流的详细信息，请参见 OO 文档。

您必须熟悉 SA、 OO 和 OO 流，才能实施本章中描述的过程。

本章包括以下主题：

要检查最新更新、确定您是否在使用最新版本的文档或检查发行说明中的最新信息，请转至：

http://h20230.www2.hp.com/selfsolve/manuals

SA-OO 集成的新增功能

本节将描述此版本的 SA-OO 集成的新增功能。

对 OO 10.10 的支持

对于 SA-OO 集成， SA 10.10 或更高版本支持 HP Operation Orchestration 10。

版本支持和兼容性信息随时更改。有关完整最新的支持和兼容性信息，请参见相关产品发布的支持列表。可在 HP 软件联机支持网站上查找所有支持列表和产品手册，网址为：

http://support.openview.hp.com/sc/support_matrices.jsp

您还可以从 HP 软件联机支持产品手册网站下载此发布的 《HP Server Automation Support and Compatibility Matrix》，网址为：

http://support.openview.hp.com/selfsolve/manuals

管理员：设置流

本节将描述系统管理员和流管理员如何在 SA 中设置 OO 流。

先决条件

本节描述要在 SA 客户端中设置和运行流所必须符合的先决条件。

使用 OO 的先决条件

本节描述使用 OO 所需的环境和权限。

注意：只能对一个版本的 OO 执行 SA 集成。

环境

要将 OO 与 SA 一起使用来设置和运行流，您的环境必须符合以下要求：

- SA 版本 10.0
- HP Operations Orchestration (OO) 版本 9.X 和 10.x。
- 通过网络连接到 SA 核心服务器的 OO 安装服务器
- 与 OO 进行通信所使用的有效的 OO SDK 客户端证书

导入 OO SDK 客户端证书

本节将描述如何导入所需的 OO SDK 客户端证书。您必须导入此证书，才能从 SA 运行 OO 流。

注意：如果您的体系结构包括一个主核心和一个或多个次级核心，则请针对此主核心和每个次级核心，按本节中的步骤执行操作。同样，如果使用一个或多个切分对 SA 计算机进行核心切分安装，则请针对每个切分重复执行这些步骤。

要导入 SDK，请执行以下操作：

1. 停止 Web 服务数据访问引擎 (Twist)：

   ```
   /etc/init.d/opsware-sas stop twist
   ```

2. 将 OO Central 证书转移到 SA：

   （当系统提示您针对接下来的步骤提供一个密码时，请使用：`changeit`）

   a. 导出 OO Central 证书：

OO 客户端证书的导出过程取决于要连接到的 OO 版本：

OO 版本	说明
OO 9.0	在 SA 核心上打开终端，并执行： `/opt/opsware/jdk1.7/jre/bin/keytool -exportcert -alias oocert2007 -file /tmp/oocentral.crt -keystore /var/opt/opsware/twist/oocert`
OO 9.0X （OO 9.02.0002 或更高版本）	在 SA 核心上打开终端，并执行： `/opt/opsware/jdk1.7/jre/bin/keytool -exportcert -alias oocert2011 -file /tmp/oocentral.crt -keystore /var/opt/opsware/twist/oocert`
OO 10.X	从 OO 10.0 开始，证书的导出过程可能有所差异，具体取决于 OO 服务器上的 OS 版本。有关详细信息，请参见 OO 文档。 注意：证书导出命令必须在 OO 服务器上运行。自 SA 10.0 起，客户端证书不与 SA 绑定。

从 Windows 服务器上安装的 OO 10.0 实例中导出证书的命令示例如下：

```
<OO_INSTALL_DIR>\java\win64\bin\keytool.exe -exportcert -alias tomcat
-file C:\oocentral.crt -keystore
<OO_INSTALL_DIR>\central\var\security\key.store
```

下一步，确保将 `C:\oocentral.crt` 文件复制到 SA 核心的 `/tmp/oocentral.crt` 下。

b **注意：**仅当 SA *未在*FIPS 模式下运行时，才能执行此步骤。
将 OO Central 证书导入到 SA Java 运行时环境 (JRE) 密钥库：

```
/opt/opsware/jdk1.7/jre/bin/keytool -importcert -alias oocert -file /
tmp/oocentral.crt -keystore /opt/opsware/jdk1.7/jre/lib/security/
cacerts
```

c **注意：**仅当 SA *在*FIPS 模式下运行时，才能执行此步骤。
当 SA 在 FIPS 模式下运行时，请确保使用 SHA-1 （SHA-256 证书不起作用）对 OO central 证书进行签名。

为验证 OO 证书，请在 SA 核心上运行以下命令 （在检索 OO 证书后）：

```
/opt/opsware/jdk1.7/jre/bin/keytool -printcert -file /tmp/oocentral.crt
```

然后查找类似以下内容的结果：

```
Signature algorithm name:SHA1withRSA
```

此结果表示证书为 SHA-1，可以进行集成。如果没有获得这些结果 （即没有使用 SHA-1 对证书进行签名），请参考 OO 文档获取有关如何更改 OO 证书的说明。

为将证书导入 SA 密钥库，请执行以下命令：

```
/opt/opsware/nss/nssimport.sh cert /tmp/oocentral.crt twist
```

以上示例使用别名：oocert。但是，导入证书时可以使用任何别名，只要该密钥库中未使用此别名。

3 检查是否已成功导入 OO Central 证书：

```
/opt/opsware/jdk1.7/jre/bin/keytool -list -alias oocert -keystore /opt/
opsware/jdk1.7/jre/lib/security/cacerts
```

示例输出：

```
oocert, Feb 3, 2010, trustedCertEntry,
Certificate fingerprint
(MD5):DF:DD:22:1B:A2:1E:A9:9C:1C:AF:8F:E0:14:1F:B5:E0
```

4 **注意：**仅当 SA 在 FIPS 模式下运行时，才能执行此步骤。

输入以下路径：

```
export LD_LIBRARY_PATH=/opt/opsware/nss/lib/opt/opsware/nss/bin/certutil
-d /var/opt/opsware/crypto/nss/twist/db -L
```

结果应包括 oocentral 证书。

示例输出：

```
Certificate Nickname
Trust Attributes
SSL,S/MIME,JAR/XPI
spog - Opsware Inc.
u,u,u
8p00ooe6qgonaf0mrlu21i4nta-oocentral
CT,C,C
opsware-ca
CT,C,C
```

5 重新启动 Web 服务数据访问引擎 (Twist)：

```
/etc/init.d/opsware-sas restart twist
```

权限

为使用 SA-OO 集成，必须为用户授予以下权限：

表 1 检查用户权限

权限	描述	在 SA 客户端中检查
AdministerFlowIntegrations	配置 OO 集成设置	在导航面板中选择“管理”。如果“流程集成”选项显示在导航树的选择列表中，则已授予此权限。
RunFlowOption （针对要运行流的用户）	运行 OO 流	在导航面板中选择“设备”。选择“服务器”>“所有托管服务器”。右键单击服务器名称并选择“运行”。如果“流 ...”选项可见，则已授予此权限。

编辑流集成设置

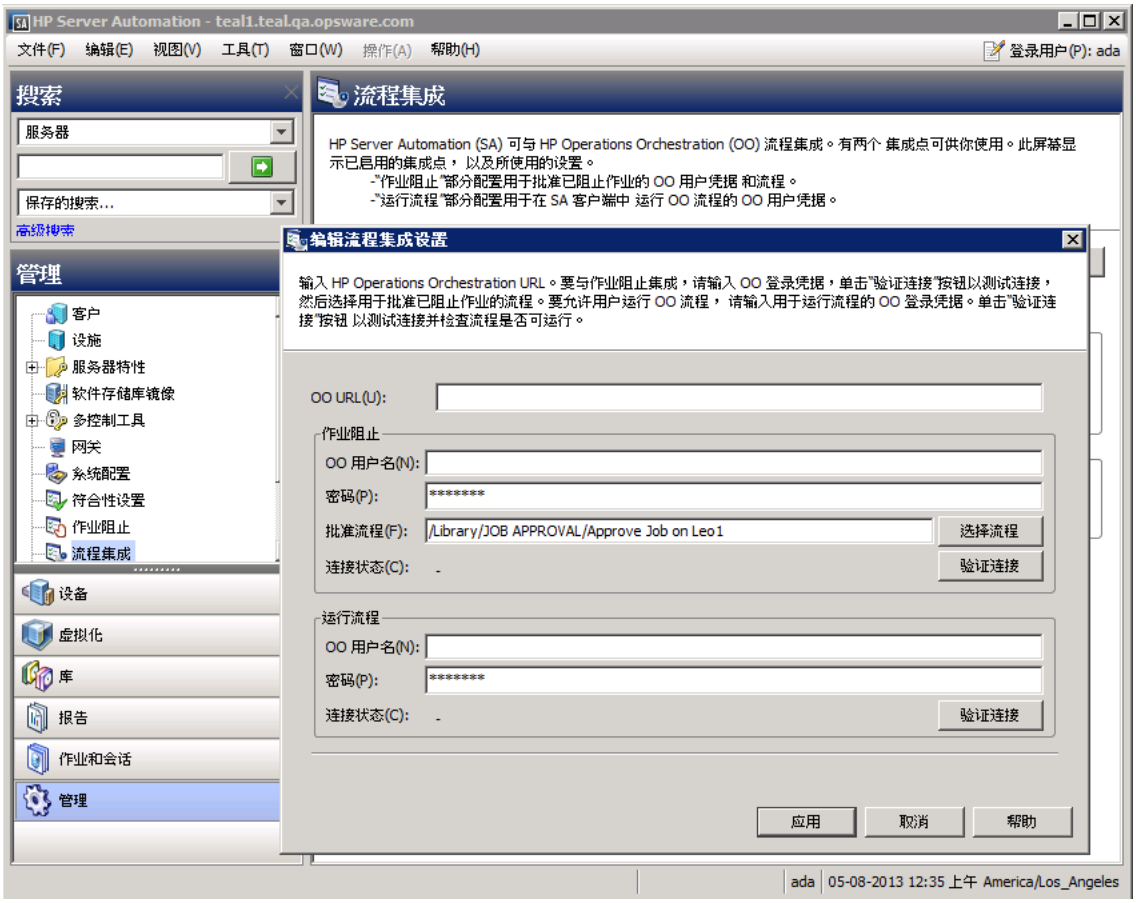
使用 SA 中的“流程集成设置”可配置 Server Automation 和 HP Operations Orchestration 之间的集成。

要配置或编辑流集成设置，请执行以下操作：

1 在 SA 客户端导航面板中，选择 “管理” > “流程集成”。

2 在 “流程集成”面板中单击 “编辑设置”，将显示 “编辑流程集成设置”窗口。

图 9 编辑流集成设置窗口



“流程集成”面板为以下用户显示实时信息：

a 针对作业阻止：具有权限运行批准流的 OO 用户。

b 针对运行流：其凭据用于从 SA 运行流的 OO 用户。

打开此面板时会即时显示对用户帐户所做的任何更改 （例如禁用帐户或更改 OO 凭据 （用户名、密码或 URL））。

3 要运行流，请输入或更改以下信息：

— OO URL - OO 服务器的位置，格式如下：

```
<protocol>://<hostname or host IP address>:<port number>/
```

示例：

```
https://10.255.166.110:8443/
```

https://10.255.166.110:8443/PAS/

— OO 用户名和密码 ()

有关阻止作业和此窗口的阻止作业部分的信息，请参见 “SA-OO - 阻止作业”一章。

连字符代表未配置的状态，红色对号代表无效状态，绿色对号代表有效状态。有效状态和无效状态均显示有最新的验证时间戳。

4 单击 “验证连接”，检查所输入的凭据的有效性。

如果连接状态有效，则将显示一个对号。

5 单击 “应用”，保存所做的流集成设置更改。

如果 “编辑流程集成设置”面板中不存在数据、字段中的数据不正确或者对号没有显示在连接状态旁边，则会禁用 “应用”按钮。

SA-OO 集成流

本节将列出流输入。流作者可以在 OO 中定义输入名称、输入类型和模板。在定义这些输入并运行流之后， SA 会将这些值自动填充到 OO-SA 库 SACoreInputs 表中 - 您无需手动输入这些值。

对于这些输入：

- 如果此输入具有文本、加密字段或自由格式列表字段，并且 OO 提供默认值，则将使用此默认值填充该字段。如果没有默认值，则如果您按照表 2 中的指南执行操作， SA 将使用以下已知输入（可修改）之一填充该文本字段。
- 如果此输入具有单个或多个选择列表字段，则 OO 将提供值 - 您无法修改这些值。

有关如何定义流输入的详细信息，请参见 OO 文档。

表 2 流输入

流输入	相关组件	SA 自动分配的值
coreHost and coreIPAddress	SA 核心	与登录到 SA 客户端的 SA 用户关联的 SA 核心的主机和 IP 地址
coreUsername or coreUser	SA 核心	与登录到 SA 客户端的 SA 用户关联的用户名
corePassword	SA 核心	与登录到 SA 客户端的 SA 用户关联的密码 此字段的内容被加密。
coreVersion	SA 核心	当前 SA 核心版本 SA 提供这些值

表 2　流输入 （续）

流输入	相关组件	SA 自动分配的值
saServerIdentifier	SA 托管服务器	选定服务器标识符： 可设置两个可能的值 （在 OO 中）： • 未分配 （针对一个值） • 值列表 （针对多个值） - 在 OO 中将此输入定义为 freeFormList 类型。
saServerScriptName	SA 托管服务器	在 SA 核心中可用的针对该特定服务器操作系统的服务器脚本名称。 自动分配的值：无 相反， SA 客户端提供一个小控件，通过此小组件，用户可以选择服务器脚本 （不包括 OGFS 脚本）。
saServerName/ hostName	SA 托管服务器	选定服务器的 DNS 名称 仅在选定服务器时，才会填充此值。 可设置两个可能的值 （在 OO 中）： • 未分配 （针对一个值） • 值列表 （针对多个值） 在 OO 中将此输入定义为 freeFormList 类型。
platformName	SA 托管服务器	选定服务器的操作系统名称 仅在选定服务器时，才会填充此值。
customerName	SA 托管服务器	选定服务器的选定客户名称 仅在选定服务器时，才会填充此值。
facilityName	SA 托管服务器	选定服务器所在的设施名称 仅在选定服务器时，才会填充此值。
saJobId	OO	用于运行 OO 流 （使用报告功能在 OO 中对其进行跟踪）的 SA 作业的作业 ID 未显示此输入。

验证更改和设置

本节将描述如何验证是否已应用更改或设置。

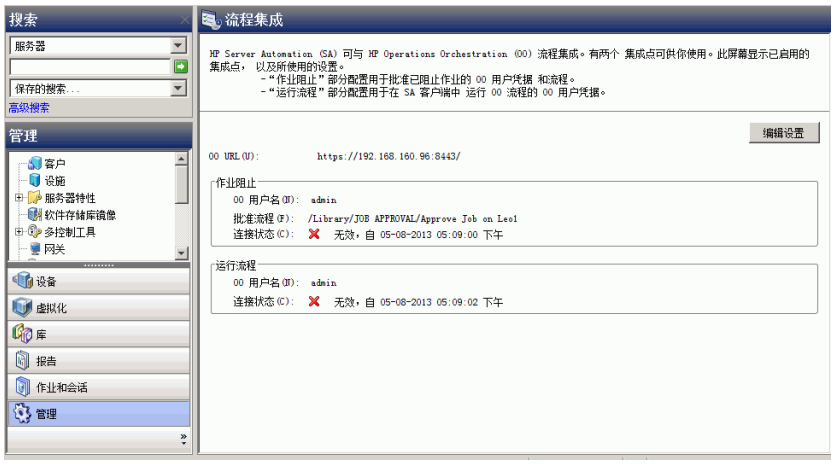
流编辑和流状态

1 登录到 SA 客户端。

2 在导航面板中选择 “管理”。

3 在导航树中选择 “流程集成”。

图 10 “流程集成”面板



“流程集成”面板为以下用户显示实时信息：

a 针对作业阻止：具有权限运行批准流的 OO 用户。

b 针对运行流：其凭据用于从 SA 运行流的 OO 用户。

打开此面板时会即时显示对用户帐户所做的任何更改 （例如禁用帐户或更改 OO 凭据 （用户名、密码或 URL））。

流或作业阻止操作完成后，状态旁边将显示对号。

用户：运行流

本节将描述用户如何运行流、选择服务器和选择流输入。

用户必须具有 “运行流”权限，才能在 SA 中运行流。

选择要运行的流

要选择运行的流，请执行以下操作：

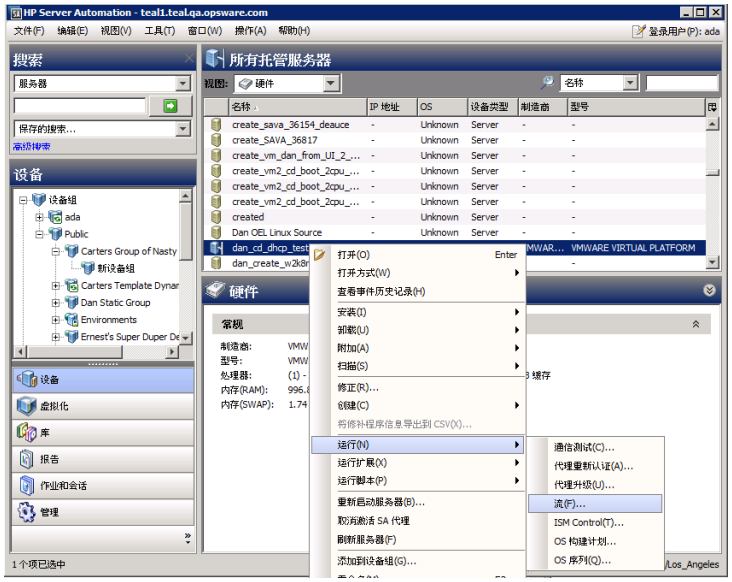
1 在 SA 客户端导航面板中，选择 “设备”。

2 在顶部面板中，选择 “服务器” > “所有托管服务器”。

必须选择服务器，才能选择流。

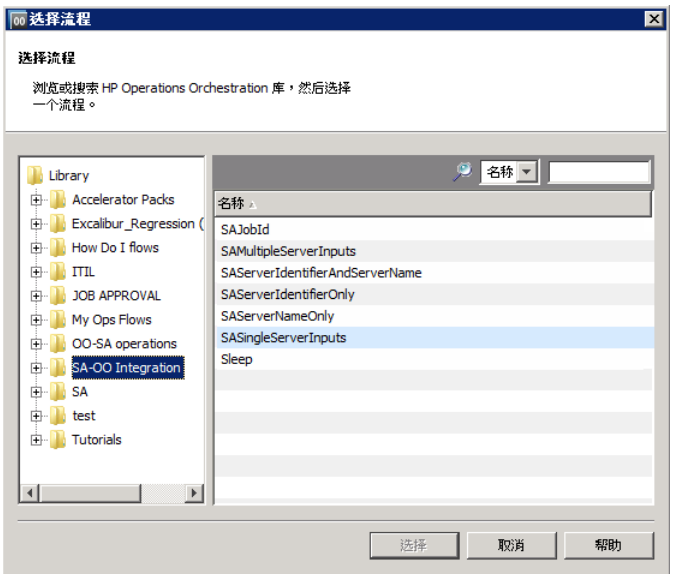
3 右键单击服务器名称。

图 11 运行流选项



4 选择 “运行” > “流 ...”，显示 “选择流程” 00 窗口。

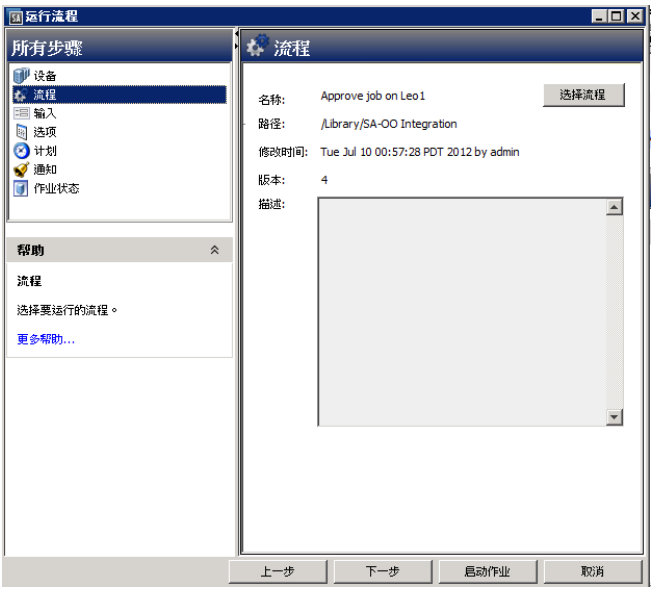
图 12 “选择流程” 窗口



5 在 “选择流程” 窗口中，从库树选择流类别，将显示其组件流。

6 在名称列表中，选择一个流并单击 “选择”，将在 “运行流程”窗口中显示流详细信息。

图 13 “运行流程”窗口



您可以选择流输入、运行时选项、计划选项和通知参数。请参见选择流输入、运行时选项、计划选项和通知参数 （第 38 页）。

添加或删除服务器

要添加或删除服务器，请执行以下操作：

1 首先，按照选择要运行的流 （第 36 页）中的步骤执行操作。

2 在 “运行流程”窗口的 “所有步骤”导航面板中，选择 “设备”。

3 右键单击服务器图标并选择 “添加”或 “删除”，或者单击加号或减号。

此时将显示 “选择服务器和设备组”窗口。

4 单击 “选择”将服务器添加到服务器列表。

“运行流程”窗口的 “设备”面板中将显示新的服务器，或显示删除的服务器不存在。

选择流输入、运行时选项、计划选项和通知参数

您可以为流输入、运行时选项、计划和通知输入值。某些参数将被自动填充。

1 按照选择要运行的流 （第 36 页）中的步骤执行操作，然后：

2 在 “运行流程”窗口的 “所有步骤”面板中，轮流选择每种类别（输入、选项、计划和通知），按此过程剩余步骤的说明，输入其参数的值。或者，也可以在每个面板中选择 “下一步”以查看类别。

3 要输入流输入的值，请在 “所有步骤”面板中选择 “输入”，然后为面板显示的输入来输入值。例如：

a `saServerScriptName` 或单击 “选择脚本”以显示脚本列表。

b `saServerName`

c `saServerIdentifier`

有关输入的详细信息，请参见表 2。

4 要输入运行时选项的值，请在 “所有步骤” 面板中选择 “选项”，然后输入作业超时的值。这是服务器在超时之前运行作业的分钟数。默认值为：180 分钟，超时值介于 1 和 1440 分钟之间。

5 要选择计划选项，请在 “所有步骤” 面板中选择 “计划”，然后为以下参数输入值：

a 计划频率

b 时间和持续时间

6 要输入通知信息，请在 “所有步骤” 面板中单击 “通知”，然后为以下参数添加值：

a 收件人电子邮件地址

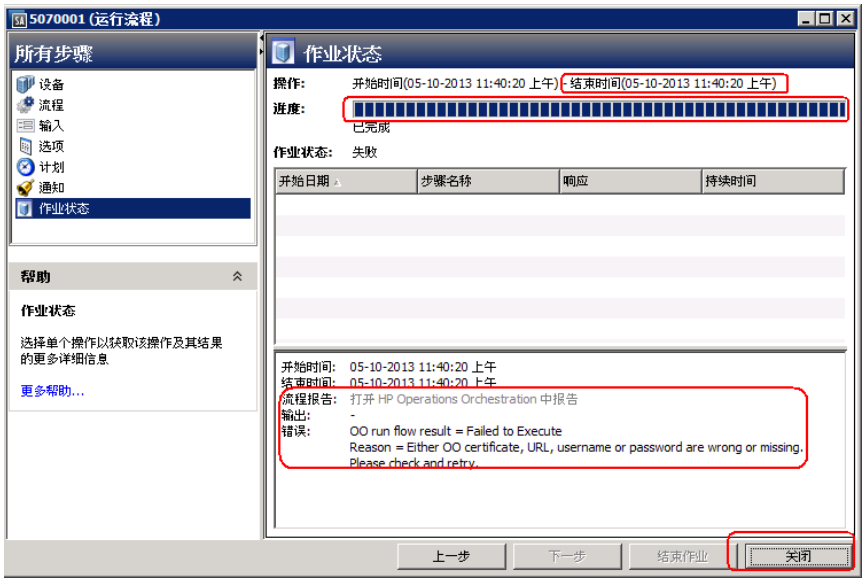
b 通知者 （单击 “添加通知者”）

c 工单标识号 （对此标识号没有任何约定 - 可选择任何号码）

7 单击 “启动作业” 将启动此作业，或者单击 “取消” 擦除在此会话中所做的选择。

8 单击 “作业状态”，可查看 SA 作业的状态。（可选）

图 14 SA 作业状态



“作业状态” 窗口不会 显示流运行状态，而是显示用于在 OO 中启动和监控流的 SA 作业的状态。

SA 作业完成时，此窗口将显示流中每个步骤的状态 （在 “响应” 字段中）以及一个 URL，该 URL 指向 OO 上有关流的更加详细的信息。

有可能在至少一个步骤失败的情况下，仍然成功完成 SA 作业监控。OO API 不提供调用来精确确定整个 OO 流的成功或失败。因此，无法从 “SA 作业状态” 屏幕或 URL 提供的信息来确定 OO 流的成功或失败。

故障排除

SA-OO 连接错误

如果 SA 无法连接到 OO，则管理员可以：

- 检查“编辑流程集成设置”窗口字段中的设置是否正确。（请参见编辑流集成设置（第 33 页）。）
- 在命令引擎服务器上检查错误消息的以下日志文件：

  /var/log/opsware/waybot/waybot.err

  错误消息不会显示在 SA 客户端中。
- 检查 OO URL、用户名和密码是否正确。
- 确保指定的 OO 用户具有运行流的正确权限。

要检查流状态，请参见“流程集成面板”。有关此面板的详细信息，请参见编辑流集成设置（第 33 页）。

如果您是用户并且看到此错误，请联系您的管理员。

流运行错误

本节将描述以用户身份运行流时可能遇到的错误。

不正确的输入

在尝试运行流时，可能会接收到以下错误之一：

- SA 不会将选定设备传递到此流。
- SA-OO 集成配置错误：流集成设置不正确。请验证流集成 URL、用户名和密码是否正确。

通常，在发生以下一种或多种情况时，会显示这些错误：

- 您 （用户）已选择运行错误的流。
- OO 服务器未响应。询问管理员获取帮助。
- 管理员在“编辑流程集成设置”窗口中的输入不正确。请要求管理员检查“编辑流程集成设置”窗口中的信息。有关详细信息，请参见编辑流集成设置 （第 33 页）。
- 流作者必须修改流定义，才能使用命名约定。

未定义输入或服务器仅接受一个设备

在尝试运行流时，可能会接收到以下错误：

SA 不会将选定设备传递到此流。没有为此流定义所需的 ServerIdentifier 输入，或者此输入仅接受单个设备。

如果收到此错误，请要求管理员检查 ServerIdentifier 输入。

4 SA-OO 集成 - 作业阻止和批准

软件自动化 (SA) 作业是您在 SA 客户端中运行的主要过程，例如安装修补程序或检查符合性。

本章将描述系统集成员和软件开发人员如何在 SA 中使用称为 SA API 的流阻止、批准或取消 SA 作业。

有关 SA 作业的详细信息，请参见 《SA Application Deployment User Guide》。

您必须熟悉 SA、 Operations Orchestration (OO)、 SA 作业和 OO 流，才能阻止和取消阻止作业。

本章包括以下主题：

有关作业的详细信息，请参见 《SA Application Deployment User Guide》。有关使用 OO 的详细信息，请参见 OO 文档。

要检查最新更新、确定您是否在使用最新版本的文档或检查发行说明中的最新信息，请转至：

http://h20230.www2.hp.com/selfsolve/manuals

阻止作业

如果在执行 SA 作业之前需要审核和批准它们，您可以阻止它们运行。本节定义了已阻止作业，描述了阻止作业的多个场景、可以阻止的作业类型、阻止作业所需的权限、如何阻止作业、如何禁用作业阻止以及如何查看与已阻止作业相关的信息。

什么是已阻止作业？

已阻止作业是这样一种作业：

- 属于可以阻止的作业类型。
- 属于已由系统管理员启用阻止的作业类型。
- 作业上有阻止标记。
- 运行之前需审核。
- 运行之前必须获得批准。

为什么要阻止作业？

本节包含三个示例作业场景 （其中的作业是用于作业阻止的备选作业）并阐明在何种情况下需要阻止作业。

场景 1

如果运行作业要求重新启动系统，则在清晨可运行此作业之前，应推迟作业的批准。如果此作业在常规业务时间运行，则将中断正常的工作进程。

场景 2

在运行某些作业之前，需对其做进一步检查。例如，如果某个作业更新服务器上的特定软件应用程序，则变更咨询委员会 (CAB) 可能需要检查计划的升级，确保它不会与环境中运行的其他应用程序发生冲突。委员会将确定是否应运行此作业以及何时运行。

场景 3

在很多 IT 环境中，必须为某些操作分配工单、对其进行评估和批准，才能执行或取消这些操作。需要阻止这些作业，以便在工单系统中创建、评估和解决工单。

可以阻止哪些 SA 作业类型？

下表描述了可以阻止的 SA 作业类型。

表 3　　可阻止的 SA 作业类型

作业类型	功能
将主机添加到虚拟化服务	将主机添加到虚拟化服务。
添加虚拟化服务	添加虚拟化服务 （目标添加对象？）。
克隆虚拟机	在 VMware 服务器上克隆虚拟机。
将虚拟机转换成虚拟机模板	将虚拟机转换成虚拟机模板。
创建快照	创建用于捕获特定时间点托管服务器配置的快照。
创建虚拟机 (Hyper-V)	配置虚拟机并在 Hyper-V 虚拟机上安装操作系统。
创建虚拟机 (VMWare)	配置虚拟机并在 VMware ESX Server 上安装操作系统。
创建虚拟区	在全局区域 （虚拟机监控程序）上配置 Solaris 虚拟机 （非全局区域）。
删除虚拟机	删除虚拟机。
从虚拟机模板部署虚拟机	从虚拟机模板部署虚拟机。
编辑虚拟化服务	编辑虚拟化服务 （编辑内容？编辑字段？）。
安装修补程序	在托管服务器上安装修补程序。
安装软件	在托管服务器上安装软件。
迁移虚拟机	迁移虚拟机。
修改虚拟机 (VMware)	修改 VMware 虚拟机的属性。
修改虚拟机 (Hyper-V)	修改 Hyper-V 虚拟机的属性。

表 3　　可阻止的 SA 作业类型 （续）

作业类型	功能
修改虚拟区	修改 Solaris 虚拟机的属性。
电源控制虚拟机	（？）
推送配置	修改托管服务器上的配置文件。
重新启动服务器	重新启动服务器。
重新加载虚拟化数据	重新加载虚拟化数据。
修正审核结果	基于审核操作的结果修正服务器。
修正策略	基于软件策略或修补程序策略修正服务器。
修正快照结果	基于快照修正服务器。快照可捕获特定时间点的托管服务器配置。
删除虚拟机	从 VMware ESX Server （虚拟机监控程序）删除虚拟机。
删除虚拟区	从全局区域 （虚拟机监控程序）中删除 Solaris 虚拟机 （非全局区域）。
删除虚拟化服务	删除虚拟化服务。
恢复配置	恢复服务器上先前版本的配置文件。 每次将配置推送到服务器之后，都会保存先前的配置并且可以恢复此配置。
运行审核	运行审核。
运行自定义扩展	运行自定义扩展。
运行 ISM 控制	运行 ISM （智能软件模块）控制。 ISM 是随 ISM 开发套件 (IDK) 创建的可安装的软件包。 ISM 可以包含控制脚本，用于执行日常特定于应用程序的任务，例如启动软件服务器。
运行 OGFS 脚本	在服务器上运行 OGFS （全局文件系统）脚本。 OGFS 脚本允许您通过 SA 客户端在全局 Shell 中执行脚本。
运行 OS 构建计划	运行 OS 构建计划。
运行 OS 序列	配置服务器并使用 OS 序列安装操作系统。 操作系统序列用于定义要在未配置的服务器上安装的内容，包括来自操作系统安装配置文件的操作系统构建信息、软件和修补程序策略以及修正设置。
运行程序扩展	运行添加到 SA 的自定义功能。 通过创建自定义扩展， HP 可以扩展 SA 的功能，用以满足特定的客户需求。
运行服务器脚本	运行服务器上的脚本。

表 3　　可阻止的 SA 作业类型 （续）

作业类型	功能
运行 Chef Recipe	运行服务器上的 Chef Recipe。
卸载修补程序	卸载服务器上的修补程序。
卸载软件	卸载服务器上的软件。

所需权限

需要以下权限：

- *编辑或取消任何作业*（允许在启动流之后编辑或取消作业）
- *查看所有作业*（允许在启动流之后查看作业）
- *管理作业阻止*（允许阻止和取消阻止作业）
- *管理流集成*（允许配置与 OO 的 SA-OO 集成连接设置和指定批准流）

如何阻止和取消阻止作业？

本节将描述如何指定要阻止的作业类型和如何禁用作业阻止。

如何指定要阻止的作业类型？

为了指定要阻止的作业类型，请执行以下操作：

1　在 SA 客户端的导航窗格中，选择 “管理”。

2 在导航树中选择“作业阻止”。右窗格中将显示作业类型列表，每种类型旁边均有一个复选框。

图 15 阻止 SA 作业类型

请参见表 3 了解可阻止的作业类型。

3 选中此复选框：启用阻止作业。

此操作可阻止面板中列出的所有作业类型。

4 在 “启用阻止作业”复选框下方的面板中，选中要阻止的每种作业类型旁边的复选框。与阻止的作业类型对应的作业将无法运行，直到它们接收相应批准为止。

此操作可指定单个要阻止的作业类型。

5 单击 “应用更改”，将阻止属于选定作业类型的作业。

注意：阻止特定类型的作业将阻止属于该类型的所有将来的作业，直到取消选中该作业的 “所需批准”框为止。

如何禁用作业阻止？

要禁用作业阻止，请执行以下操作：

1 在 SA 客户端的导航窗格中，选择 “管理”。

2 在导航窗格中选择 “作业阻止”。

3 取消选中与不再阻止的作业对应的复选框。

此操作可禁用单个作业类型的作业阻止。

4 在作业类型列表的上方，取消选中 “启用阻止作业”复选框。（请参见图 15。）

此操作可禁用所有作业类型的作业阻止。

5 单击 “应用更改”。

取消选中 “启用阻止作业”复选框时将仍然保持选中指定用于阻止的作业类型旁边的复选框，以便于您执行操作。

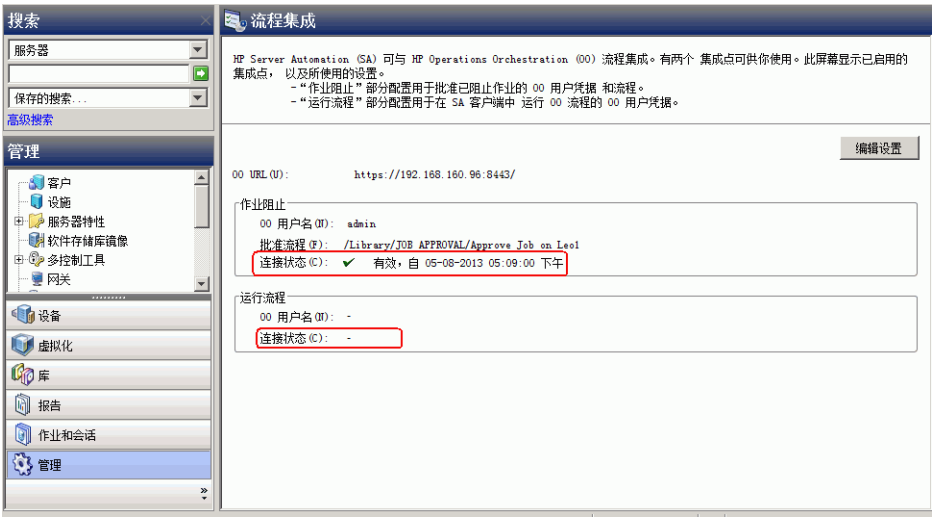
如何查看阻止的作业信息？

您可在 “流程集成”面板中查看 OO 连接信息，在作业日志中检查作业状态信息。

在 SA “流程集成”面板中检查 OO 连接信息

选择 “管理” > “流程集成”，访问 “流程集成”面板。

图 16 “流程集成”面板



“流程集成”面板为以下用户显示实时信息：

a 针对作业阻止：具有权限运行批准流的 OO 用户

b 针对运行流：其凭据用于从 SA 运行流的 OO 用户

打开此面板时会即时显示对用户帐户所做的任何更改（例如禁用帐户或更改 OO 凭据（用户名、密码或 URL））。

如果与 OO 的连接为活动状态，则此状态旁边将显示对号。

在作业日志中检查阻止的作业状态

如果您知道某个作业已被阻止且希望查看是否已提升此作业阻止，请检查作业日志（选择 “作业和会话” > “作业日志” > “任何状态”）。

有关可能的作业状态值及其意义的列表，请参见表 5。

配置或编辑流设置

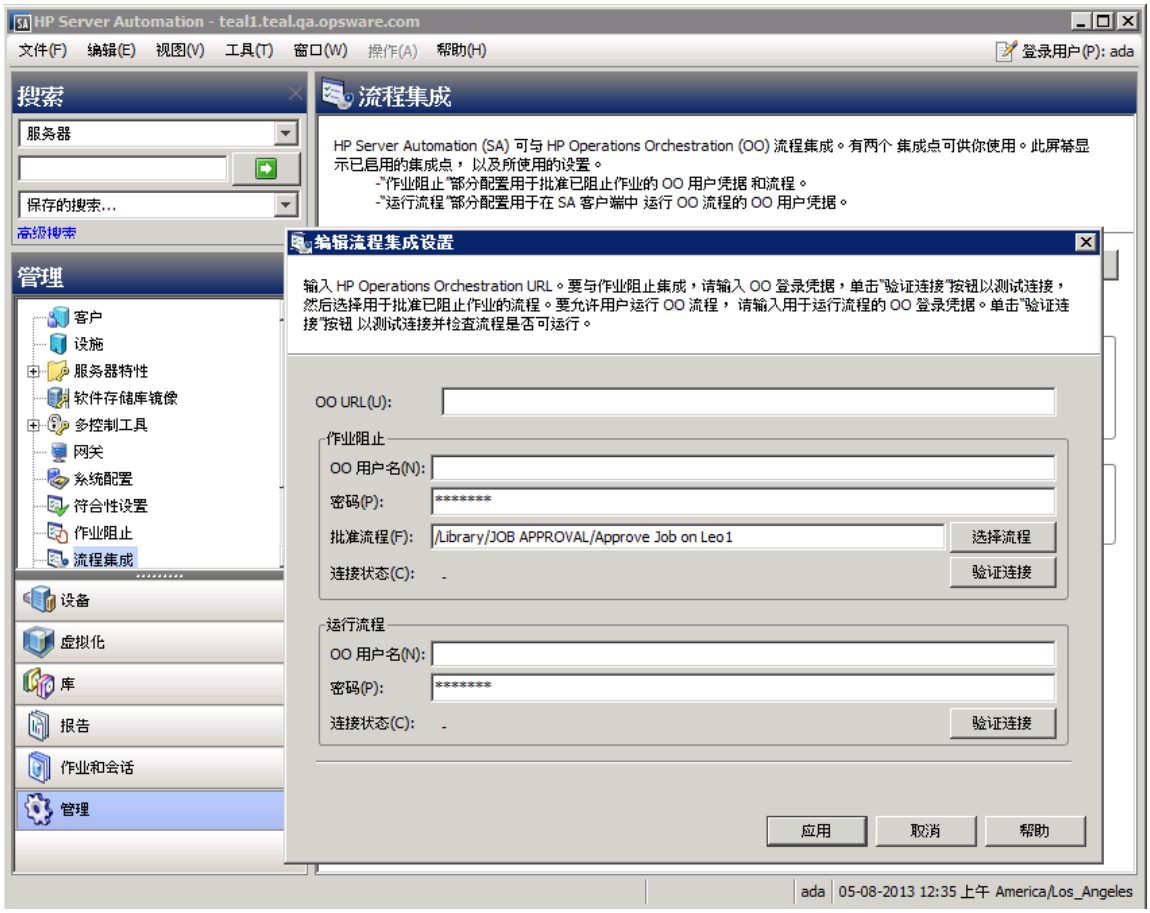
要编辑或配置流设置，必须登录到 OO 和 SA。

在 SA 客户端导航面板中：

1 选择 “管理” > “流程集成”。

2 在 “流程集成” 面板中单击 “编辑设置”，将显示 “编辑流程集成设置” 窗口。

图 17 编辑流集成设置窗口



“流程集成” 面板为以下用户显示实时信息：

a 针对作业阻止：具有权限运行批准流的 OO 用户。

b 针对运行流：其凭据用于从 SA 运行流的 OO 用户。

打开此面板时会即时显示对用户帐户所做的任何更改 （例如禁用帐户或更改 OO 凭据 （用户名、密码或 URL））。

3 要运行流，请输入或更改以下信息：

— OO URL - OO 服务器的位置，格式如下：

```
<protocol>://<hostname or host IP address>:<port number>/
```

示例：

```
https://10.255.166.110:8443/
https://10.255.166.110:8443/PAS/
```

— 批准流 - 批准流的位置

— 被授权与 OO 进行通信的用户的 OO 用户名和密码

连字符代表未配置的状态，红色对号代表无效状态，绿色对号代表有效状态。有效状态和无效状态均显示有最新的验证时间戳。

4 单击 “验证连接”，检查所输入的凭据的有效性。

如果连接状态有效，则将显示一个对号。

5 单击 “应用”，保存所做的流集成设置更改。

如果 “编辑流程集成设置”面板中不存在数据、字段中的数据不正确或者对号没有显示在连接状态旁边，则会禁用 “应用”按钮。

批准和删除已阻止的作业

可以使用 SA 应用程序编程接口 (SA API) 批准或删除作业。此 API 是管理已阻止作业的唯一方式。您无法通过 SA 客户端批准已阻止的作业。有关使用 SA API 的信息，请参见《SA 平台开发人员指南》。

有关使用 OO 阻止作业的信息，请参见 OO 文档。

用于处理已阻止作业的 Java 方法

SA API 中的 `JobService` Java 接口提供用于处理已阻止作业的 Java 方法。这些方法是可启用作业批准集成的 SA 回调。

调用这些方法的用户必须具有以下所需权限：
编辑或取消任何作业 和 *查看所有作业*

下表描述了可用于处理已阻止作业的 SA JobService Java 方法。

表 4　SA JobService Java 方法

Java 方法	方法描述	SA CLI 方法示例
JobService.approveBlockedJob	向作业授予权限并取消阻止它，以允许执行此作业。	在全局 Shell 会话中： cd /opsw/api/com/opsware/job/JobService/method./approveBlockedJob self:i=$job_id
JobService.updateBlockedJob	更改 SA 客户端的 “作业状态” 窗口中已阻止作业的 “工单 ID” 字段（与 userTag 参数对应）和 “原因” 字段 （与 blockReason 参数对应）的值。 **注意：**无法使用 SA 接口更改这些字段。	cd /opsw/api/com/opsware/job/JobService/method./updateBlockedJob self:i=$job_id userTag=$ticket_id \blockReason= "This type of job requires approval of CMB."
JobService.cancelScheduledJob	取消已阻止作业并阻止其执行。 将已阻止作业的状态从 “待批准” 更改为 “已取消”。	请注意， ID 参数为 jobRef，不是 self） cd /opsw/api/com/opsware/job/JobService/method./cancelScheduledJob jobRef:i=$job_id \reason="Job was scheduled to run outside of change window." 无法取消当前正在运行的作业 (job_status = "ACTIVE")。
JobService.findJobRefs	搜索所有现有作业并返回所有已阻止作业或处于其他状态的作业 （例如正在进行的作业、过期作业和计划作业）的 ID。 可以查看由其他用户启动的作业。	（在筛选器中指定 job_status 字符串，而不是 JobInfoVO.status 整数。） cd /opsw/api/com/opsware/job/JobService/method./.findJobRefs:i filter='job:{job_status = "BLOCKED" }'

当流必须返回 SA 并与作业进行交互时，需要使用 job_id 特性。需要将此特性从 SA 发送到 OO 以进行作业阻止。

作业状态值

本节将描述可在 job_status 可搜索特性中使用的作业状态值，以及 JobInfoVO.status 对应的整数值 （您可以通过此特性检查客户端代码是否已接收值对象 (VO)）。

表 5 列出了允许的作业状态值。

在 Java 客户端中，您可以将 JobInfoVO.status 与字段常量（例如 STATUS_ACTIVE）进行比较，而无需使用此表中列出的整数。

表 5　作业状态值

job_status 可搜索特性的值	JobInfoVO.status 的值	在 SA 客户端中显示的作业状态	作业状态描述
已中止	0	命令引擎脚本失败	作业已完成运行。 已检测到命令引擎失败。
活动	1	正在进行	作业当前正在运行。
已阻止	11	挂起批准	作业已启动，但需要批准才能运行。
已取消	2	N/A	计划已删除。
已删除	3	已取消	已计划作业，但稍后已将其取消。
过期	13	过期	当前日期晚于作业计划的结束日期，因此作业计划不再有效。
失败	4	完成但出错	作业已完成运行，但是检测到错误。
待定	5	已计划	计划在将来运行一次作业。
重复	12	重复	计划在将来重复运行作业。
过时	10	过时	已阻止作业的运行机会已过期，因为未获得批准。
成功	6	已完成	作业已成功完成运行。
已修改	9	已修改	
未知	7	未知	
警告	8	完成但出现警告	作业已完成运行，但是检测到警告。
僵停	14	孤立	

5 SA-uCMDB 连接器

SA-uCMDB 集成

本章将描述如何使用 SA-uCMDB 连接器将 HP Server Automation (SA) 与 HP 通用配置管理数据库 (UCMDB) 集成。 SA-uCMDB 连接器为资产符合性报告提供配置数据的单个源。

HP SA 在 SA 数据库中存储大量有关服务器和软件的信息。 SA-uCMDB 连接器将部分数据复制到 HP uCMDB。 SA 中的数据发生更改时， SA-uCMDB 连接器会将更新的数据自动发送到 uCMDB 服务器。

HP Universal CMDB 是企业 IT 组织的配置管理数据库 (CMDB)，用于记录、存储和管理业务服务定义和关联基础结构关系。uCMDB 提供共享的单个版本的 truth，用以支持业务服务管理、IT 服务管理、变更管理以及资产管理步骤。这些步骤可帮助将 IT 工作与业务要求协调一致，从而更加有效和高效地实施 IT 运营。

HP Server Automation 为企业服务器和应用程序提供生命周期管理，从发现到配置、修补、到配置管理和脚本执行、再到符合性保证。HP Server Automation 可自动化不同 IT 团队和系统的操作和过程。

突出功能

- 扩展的预置映射
- 可扩展的 ETL 映射和数据标准化功能
- 全局 uCMDB ID
- 按需同步
- 与 uCMDB 服务器和 uCMDB 浏览器的 SSL 连接
- 对 SA 自定义特性的支持
- 对 uCMDB 服务器版本 9.05 和 10.01 的支持

uCMDB 浏览器

借助 SA-uCMDB 连接器， SA 客户端能够针对 SA 托管服务器启动受 uCMDB 浏览器影响的小组件。

有关详细信息，请参见 SA 客户端中对 uCMDB 浏览器集成的支持。

安装和配置 SA-uCMDB 连接器

在安装 SA 时将安装 SA-uCMDB 连接器。无需进行单独安装。

如果要升级到 Server Automation 10.0，则必须已将 uCMDB 服务器升级到 9.05、 10.01 或更高版本。

> 此处的版本兼容性信息在发布此文档时是正确的。但是，跨产品版本支持会随产品版本生命周期的更改而变化。有关最新的支持和兼容性信息，请参见相关产品发布的《HP Server Automation Support and Compatibility Matrix》。

要下载最新的累积更新程序包，请执行以下操作：

1 SA 10.0 SA-uCMDB 连接器要求运行 uCMDB 9.05 或 uCMDB 10.01 或更高版本。

- uCMDB 9.05 必须包括累积更新程序包 6 (CUP 6) 或更高版本。
- uCMDB 10.01 包括内容包 12。
- 上述两项是使用 SA-uCMDB 连接器的最低要求。

最新的 CUP HP 软件修补程序可在 SSO 门户的以下位置中获得：

- Windows：

  http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_uCMDB_00094

- Linux：

  http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_uCMDB_00095

有关版本支持信息，请参见对 uCMDB 服务器版本 9.05 和 10.01 的支持。

此站点需要您注册 HP Passport 并登录。

2 运行 **enable** 命令以使用新的 uCMDB 服务器配置 SA-uCMDB 连接器。

> **enable** 命令的语法随环境而变化。有关 enable 命令语法和选项的说明，请参见本文档中的 enable 命令。

3 输入以下命令以启动 SA-uCMDB 连接器：

```
/etc/init.d/opsware-sas start telldaemon
```

4 可以选择使用以下命令检查 SA-uCMDB 连接器的状态：

```
/etc/init.d/opsware-sas status telldaemon
```

自定义发送给 uCMDB 服务器的 SA 数据

映射文件

SA-uCMDB 连接器 XML 映射文件描述由 SA-uCMDB 连接器转移的数据并支持您自定义数据映射。

初始的 mapping.xml 将在首次运行连接器时生成。生成此文件后，可在以下位置找到新的映射文件：

```
/etc/opt/opsware/tell/metadata/mapping.xml
```

此映射文件允许您控制：

- 填充 uCMDB 的数据类型和特性以及
- 可选 SA 自定义特性和 uCMDB 数据模型配置项 (CI) 特性之间的映射。

➤ 有关完整的原始映射文件内容，请参见示例 - SA-uCMDB 连接器映射文件。

自定义映射文件

为自定义数据映射方式，需要创建和修改 **mapping_custom.xml** 文件，然后重新启动连接器。

➤ 默认情况下不使用 **mapping_custom.xml** 文件，因此需要重新启动连接器才能使用自定义映射文件。

要自定义 uCMDB 连接器映射，请执行以下操作：

1 如果 uCMDB 连接器正在运行，则必须停止并禁用连接器，才能编辑映射文件。

➤ 有关说明，请参见停止并禁用 SA-uCMDB 连接器。

重要提示：请确保连接器已停止并禁用。如果在编辑映射文件时未停止和禁用连接器，则在尝试重新启动连接器时可能遇到问题。

2 创建自定义映射文件：

a 转到：**/etc/opt/opsware/tell/metadata**

b 将 **mapping.xml** 文件复制到同一文件夹并将此副本命名为 **mapping_custom.xml**。

➤ **mapping_custom.xml** 文件必须与 **mapping.xml** 文件位于同一指定文件夹中，才能正常运行。

3 根据需要编辑 **/etc/opt/opsware/tell/metadata/mapping_custom.xml**。

➤ 有关如何针对不同目的编辑映射文件的详细信息，请参见编辑映射文件。

4 运行 **enable** 命令更改 SA-uCMDB 连接器的配置。

➤ **enable** 命令的语法随环境而变化。有关 enable 命令语法和选项的说明，请参见本文档中的 enable 命令。

5 运行 **start** 命令重新启动 SA-uCMDB 连接器：

```
/etc/init.d/opsware-sas start telldaemon
```

6 可以选择使用以下命令检查 SA-uCMDB 连接器的状态：

```
/etc/init.d/opsware-sas status telldaemon
```

编辑映射文件

所有自定义映射均在 **mapping_custom.xml** 配置文件中定义，因此管理员可以轻松查看和编辑它们。可以修改 XML 映射文件来更改由 SA-uCMDB 连接器转移的数据。通过映射文件，还可以选择忽略特定的 CI 和特性。如果 mapping_custom.xml 不存在，则默认情况下，连接器将考虑使用预置的 mapping.xml。

权限：为查看或编辑 **mapping_custom.xml** 文件，必须首先以 **root** 身份登录到 SA 核心，然后才能具备读取 / 写入权限。

本节描述自定义映射文件中的编辑选项。有关自定义映射文件的过程的说明，包括何时需要停止和启动连接器以使更改生效，请参见自定义映射文件。

映射文件说明

以下是预置映射文件的片段：

```
<Model-Definition model-name='hosts'>
   <CI ucmdb-ci-type-name='node' enable='true' base-class='node'
      <Attribute source='Node/Name' target-attr='name' enable='true'/>
      <Attribute source='Node/Description' target-attr='description'
   enable='true'/>
   </CI>
</Model-Definition>
```

其中，突出显示的文本表示可编辑的字段。

有关完整的预置映射文件，请参见示例 - SA-uCMDB 连接器映射文件。

映射文件中的每个模型定义标记定义一个特定的模型名称。在此示例中， Model-Definition 定义“hosts”模型。

每个模型可以包含多个配置项 (CI)。每个 CI 标记定义该 CI 的组合。在此示例中，“node”是正在定义的 CI。

对于每个特性， **source** 表示源数据库中的默认特性名称。

- **target-attr** 字段指定源映射到的 uCMDB 特性名称。
- **enable** 字段定义是否映射此特性。 **enable** 的默认值为 'true' ；这意味着此特性将加载到 uCMDB 中。将 **enable** 设置为 'false'，将选择不映射此特性；这意味着该特性将不会加载到 uCMDB。

XML 特性值

表 6 显示 XML 特性值，表示可编辑和不可编辑的值：

警告：请勿更改不可编辑的特性值。将不可编辑的值 （例如， source='Node/Name'）保持不变至关重要。更改这些值会使同步运行异常，并且导致错误。

表 6　XML 特性值

XML 特性标记	特性	特性值示例和说明	是否可编辑？
Model-Definition	**model-name**	'hosts'、 'sa'、 'software'、 'compliance'、 'hypervisor'、 'vmrelations'、 'compliance_status'	不可编辑
	enable	'true' 表示启用此特性； 'false' 表示禁用	可编辑
CI	**ucmdb-ci-type-name**	指定 uCMDB CI 类型。例如： 'node'、 'ip_address'	可编辑
	enable	'true' 表示启用此特性； 'false' 表示禁用	可编辑
特性	**source**	指定 SA 自定义特性名称。例如： 'Node/Name'、 'Node/Description'、 'Node/BiosAssetTag'、 'Node/BiosSerialNumber'、 'Node/Facility'、 'Node/VirtualizationTypeId' 警告：请勿编辑 Source 值。修改 Source 值将损坏映射并可能导致错误。	不可编辑
	target-attr	指定源映射到的 uCMDB 特性名称。例如： 'name'、 'description' 注意：**target-attr** 值必须是唯一名称。	可编辑
	enable	'true' 表示启用此特性； 'false' 表示禁用	可编辑
	conversion-name	仅用于会话功能。有关详细信息，请参见自定义的数据转换函数。例如： 'com.hp.tell.ConversionMethod$com.hp.tell.MyConvertVirtualizationType'	可编辑
Attribute-Custom	**sa-custom-attribute-key-value**	指定 SA 自定义特性名称。例如： 'HW_RACK'、 'DEVICE_RACK' 注意：请参见对 SA 自定义特性的支持。	可编辑
	target-attr	指定源映射到的 uCMDB 特性名称。例如： 'serial_number'、 'facility' 注意：**target-attr** 值必须是唯一名称。	可编辑
	enable	'true' 表示启用此特性； 'false' 表示禁用	可编辑
CI-Filter	**enable**	'true' 表示启用此特性； 'false' 表示禁用 注意：有关修改 CDATA 块的说明，请参见查询的筛选支持。	可编辑

表 6　XML 特性值 （续）

XML 特性标记	特性	特性值示例和说明	是否可编辑？
Relation	**ucmdb-relation-type-name**	指定 CI 之间的 uCMDB 关系。 例如：'containment'、 'aggregation'	可编辑
	ucmdb-relation-from-ci-type-name	指定 'from' CI 的 CI 之间的 uCMDB 关系。 例如，如果指定从 *node* 到 *ip_address* 的包含关系，则 'node' 在此关系中将为 'from' CI。	可编辑
	ucmdb-relation-to-ci-type-name	指定 'to' CI 的 CI 之间的 uCMDB 关系。 例如，如果指定从 *node* 到 *ip_address* 的包含关系，则 'ip-address' 在此关系中将为 'to' CI。	可编辑
	enable	'true' 表示启用此特性； 'false' 表示禁用	可编辑
	ucmdb-relation-id-link	如果关系包含 ID 链接，则为 'true'。此 'true' 值要求存在 'from' CI，如果关系不包含 ID 链接，则为 'false'	可编辑

模型定义

表 7 显示模型定义。映射文件中定义了 7 种模型，用于定义数据对象在 uCMDB 中的表示方式。例如， SA 模型表示 uCMDB 中的 SA。

表 7　模型定义

模型定义 model-name	描述
'sa'	生成 installed_software.xml
'hosts'	生成 node.xml
'software'	生成 installed_software.xml
'compliance'	生成 policy-xml
'hypervisor'	生成 hypervisor.xml
'vmrelations'	生成 hypervisor.Relationxml
'compliance_status'	生成 policyResult.xml

这些 XML 文件是基于映射文件在内部生成的，不应直接编辑它们。不支持直接编辑生成的 XML 文件。将覆盖对所生成文件的任何更改。

对 SA 自定义特性的支持

重要提示：对映射文件的所有编辑操作都必须在 mapping_custom.xml 文件中完成。请勿编辑预置的 mapping.xml 文件。直接编辑 mapping.xml 文件会使同步运行异常，并且导致错误。

如何将 SA 自定义特性转移到 uCMDB

也可以将自定义特性加载到 uCMDB。

除了与 uCMDB 同步的 SA 特性以外， **mapping_custom.xml** 文件中的映射还支持您指定使用 SA 设备定义或从 SA 设施继承的任何 SA 自定义特性。

自定义特性可以在 **mapping_custom.xml** 文件中指定，如下所示：

以下示例显示用户如何配置映射文件以提取自定义特性 *DEVICE_RACK* 并将其加载到 uCMDB 中的 *my_location_rack* 目标。将 **enable** 特性设置为 'true'，表明用户选择将此特性加载到 uCMDB。

```
<CI ucmdb-ci-type-name='node' enable='true' base-class='node'>
   <Attribute-Custom sa-custom-attribute-key-value='DEVICE_RACK' target-
   attr='my_location_rack' enable='true' />
</CI>
```

其中，突出显示的文本表示可编辑的字段。

查询的筛选支持

mapping_custom.xml 文件能够筛选特定条件。

要按特定条件进行筛选，请执行以下操作：

- 在 CI-Filter 标记下的 CDATA 部分中嵌入筛选子句。
- 通过提供 **enable** 特性的值 （'true' 表示启用， 'false' 表示禁用），指定是否启用此筛选。

CI-Filter 规范基于 SA 数据库，要求了解 SA 架构的知识。您只能针对每种 CI 类型提供一个 CI-Filter。如果需要多个筛选，则可以使用 AND 和 OR 子句指定简单的筛选表达式。

单个筛选的示例 （**mapping.xml** 文件中的预置映射）：

```
<CI ucmdb-ci-type-name='node' enable='true' base-class='node'>
   <Attribute source='Node/Name' target-attr='name' enable='true' />
   <CI-Filter enable='true'><![CDATA[(DEVICES.OPSW_LIFECYCLE =
   'MANAGED')]]></CI-Filter>
</CI>
```

在以上示例中，筛选将选择状态为 'managed' 的 SA 设备。默认情况下， SA-uCMDB 连接器仅同步托管设备对象。

包括 AND 子句的筛选示例 （**mapping_custom.xml** 中修改的映射）：

```
<CI-Filter enable='true'><![CDATA[(DEVICES.DVC_MODEL = 'POWEREDGE 2950') and
(DEVICES.DVC_ID > 300000000)]]></CI-Filter>
```

在以上示例中，筛选将选择型号为 'POWEREDGE 2950'、 ID 大于 300000000 的 SA 设备。

扩展的预置映射

通过此映射文件，您可以：

- 更改 uCMDB 中填充的特性的名称
- 更改 uCMDB 中数据的填充方式
- 指定填充哪种 uCMDB CI 类型

其他预置映射

预置的映射文件中默认禁用 **Facility** 和 **VirtualizationType** 特性。但是，您可以启用它们，如下所示：

ServerVO.getFacility()

```
<Attribute source='Node/Facility' target-attr='facility' enable='true'/>
```

ServerVO.getVirtualizationType()

```
<Attribute source='Node/VirtualizationTypeId'
target-attr='virtualization_type_id' enable='true'/>
```

自定义的数据转换函数

如果需要定制同步期间 uCMDB 中填充的数据，可以编写*自定义转换方法*，并提供给 SA-uCMDB 连接器。之后， SA-uCMDB 连接器可以应用这些函数，将数据从 SA 语法转换为所需的 uCMDB 语法。例如，您可以编写自定义转换方法，将小写转换为大写或将字节转换为兆字节等。

自定义转换函数应通过名为 **tell_conversions.jar** 的 jar 文件提供给 SA-uCMDB 连接器，并且应在启动连接器之前将此文件置于 **/etc/opt/opsware/tell/lib** 中。在重新启动连接器后，自定义转换 java 类应扩展 **ConversionMethod** 类并导入 **com.hp.tell.ConversionMethod** 程序包。

要自定义数据转换，请执行以下操作：

1 如果 SA-uCMDB 连接器正在运行，则必须停止并禁用连接器，才能编辑映射文件。

- 运行 **stop** 命令停止 SA-uCMDB 连接器：

  ```
  /etc/init.d/opsware-sas stop telldaemon
  ```

- 运行 disable 命令禁用 SA-uCMDB 连接器：

  ```
  disable
  ```

重要提示：请确保连接器已停止并禁用。如果在编辑映射文件时未停止和禁用连接器，则在尝试重新启动连接器时可能遇到问题。

2 采用 java 编写自定义转换函数代码。

有关示例，请参见示例转换文件 – MyConvertVirtualizationType.Java。在此示例中，转换文件的名称为 **MyConvertVirtualizationType.java**。

3 修改 **mapping_custom.xml** 文件以使用刚刚创建的转换文件。

例如，您可以将以下行置于 mapping_custom.xml 文件以指向 java 文件 MyConvertVirtualizationType.java：

映射文件中的原始文本

```
<Attribute source='Node/VirtualizationTypeId'
target-attr='virtualization_type_id' enable='false'/>
```

映射文件中的自定义文本

```
<Attribute source='Node/VirtualizationTypeId' target-attr='device_isVirtual'
enable='true'
conversion-name='com.hp.tell.ConversionMethod$com.hp.tell.MyConvertVirtualizationType'/>
```

修改的 XML 行具有以下值：

- `'device_isVirtual'` 是 **target-attr** 的新特性值。由于此转换更改了数据类型，因此应将其映射到其他 uCMDB 特性。但是，如果不更改数据类型，则应映射到相同的 **target-attr** 值。 *
- `conversion-name` 是转换特性的 XML 名称。这是 verbatim 标签，不可替代。
- `'com.hp.tell.ConversionMethod$com.hp.tell.MyConvertVirtualizationType'` 是 conversion-name 的特性值， MyConvertVirtualizationType.java 是 java 转换代码文件名。

target-attr 值对转换操作的成功至关重要：

更改数据类型

如果转换将更改特性的数据类型，请确保目标特性 （由 **target-attr** 指定）具有相同或兼容的要求，例如长度和格式。在上一个示例中，我们修改了 **target-attr** 值，因为转换更改实际的数据类型。如果只是转换计量单位 (UOM)，则可以指定相同的 **target-attr** 值，因为实际数据类型没有更改。

每个 target-attr 的唯一文件名

每个 **target-attr** 转换要求唯一的 java 转换代码文件名。此 java 转换文件代表单个 **target-attr** （输出）。例如，针对单个源特性可以有多个 **target-attr** 转换场景；但是，每个 **target-attr** 必须在映射文件中的单个特性标记上指定，如下例所示：

```
<Attribute source='Node/VirtualizationTypeId'
target-attr='virtualization_type_id1'
enable='true'
conversion-name='com.hp.tell.ConversionMethod$com.hp.tell.MyConvertVirtualizationType1'/>
```

```
<Attribute source='Node/VirtualizationTypeId'
target-attr='virtualization_type_id2'
enable='true'
conversion-name='com.hp.tell.ConversionMethod$com.hp.tell.MyConvertVirtualizationType2'/>
```

4 编译自定义转换文件 （在此示例中为 **MyConvertVirtualizationType.java**）。将生成可执行的二进制文件。

5 将所有转换二进制文件压缩到具有以下名称的 jar 文件：**tell_conversions.jar**。

➤ 您必须使用此 jar 文件名，以便 SA-uCMDB 连接器可以识别它。

6 在启动 uCMDB 连接器之前，将此 jar 文件置于 SA 核心目录 **/etc/opt/opsware/tell/lib** 中。

➤ 您必须使用此目录路径，以便 SA-uCMDB 连接器可以识别它。

7 启动 SA-uCMDB 连接器。

此转换函数将在 SA-uCMDB 连接器重新启动时动态转换数据。

示例转换文件 – MyConvertVirtualizationType.Java

此示例转换文件提供示例 java 代码作为准则。此示例 java 将 SA **VirtualizationType** 从 *Numeric* 类型转换为适用于 uCMDB 的 *String* 类型。

➤ 每个 java 文件只能转换一个特性。要转换多个特性，需要具有多个 java 文件。每个目标特性只能具有一个转换。

提示：请基于修改的特性命名转换文件。在此示例中，java 文件名为 **MyConvertVirtualizationType**，因为它修改 **VirtualizationType** 特性。

```
package com.hp.tell;

import java.math.BigDecimal;

import com.hp.tell.ConversionMethod;

public class MyConvertVirtualizationType extends ConversionMethod {

   public Object convert(Object value) throws Exception{

      Integer vType = putInteger(value);
      String vValue;

      /*
       * Function to convert SA VirtualizationType (numeric) to string type For
uCMDB.
       */

      if (vType > 0) {
         vValue = "True";
      } else {
         vValue = "False";
```

```
        }

        return vValue;
    }


    private Integer putInteger(Object o) throws Exception {
          if (o instanceof String) {
              return Integer.valueOf((String) o);
          }
          if (o instanceof BigDecimal) {
          return ((BigDecimal)o).intValue();
          }
          if (o instanceof Integer) {
          return (Integer)o;
          }

          throw new Exception("Invalid conversion in putInteger
"+o.getClass().toString());
      }
}
```

管理 SA-uCMDB 连接器

停止并禁用 SA-uCMDB 连接器

如果 SA-uCMDB 连接器正在运行，则必须停止并禁用连接器，才能进行任何类型的配置更改。

要停止并禁用 SA-uCMDB 连接器，请执行以下操作：

1 运行 **stop** 命令停止 SA-uCMDB 连接器：

```
/etc/init.d/opsware-sas stop telldaemon
```

2 运行 **disable** 命令禁用 SA-uCMDB 连接器：

```
disable
```

重要提示：在进行任何配置更改之前，请确保已停止并禁用连接器。如果未停止和禁用连接器，则在尝试重新启动连接器时可能遇到问题。

stop 命令

在停止 SA-uCMDB 连接器时，会停止将数据从 SA 数据库转移到 uCMDB。要停止 SA-uCMDB 连接器，请在 SA 核心服务器上输入以下命令：

```
/etc/init.d/opsware-sas stop telldaemon
```

这将停止 SA-uCMDB 连接器。

如果 SA-uCMDB 连接器被禁用，则输出将与以下类似：

```
opsware-sas:One or more of the specified components does not exist
```

```
in the following file:
   /opt/opsware/oi_util/startup/components.config
```

如果不再需要 SA-uCMDB 连接器，则可使用 disable 命令禁用它。有关详细信息，请参见 disable 命令。

disable 命令

使用 **disable** 命令禁用 SA-uCMDB 连接器。如果正在运行 SA-uCMDB 连接器，则 **disable** 命令会首先停止它，然后再将其禁用。如果 SA-uCMDB 连接器被禁用，则将无法启动它。

disable 命令修改 **/opt/opsware/oi_util/startup/components.config** 文件，并取消注释 **telldaemon**（SA-uCMDB 连接器的进程）的行。

disable 命令的位置

disable 命令位于 SA 核心服务器的 **/opt/opsware/tell/bin** 目录中。

disable 命令的语法

```
/opt/opsware/tell/bin/disable
```

启用并启动 SA-uCMDB 连接器

在启动 SA-uCMDB 连接器之前，必须启用它以确保使用最新的配置元素。

要启用并启动 SA-uCMDB 连接器，请执行以下操作：

1. 运行 **enable** 命令更改 SA-uCMDB 连接器的配置。 enable 命令有多种选项，具体取决于您的配置。

   以下是此命令的一个简单示例：

   ```
   enable --host myserver01.hp.com --port 8888 --user ucmdb-admin
    --password leM93A3dme
   ```

   有关完整的参数、语法和选项集的详细信息，请参见 enable 命令。

2. 运行 **start** 命令重新启动 SA-uCMDB 连接器：

   ```
   /etc/init.d/opsware-sas start telldaemon
   ```

3. 可以选择使用以下命令检查 SA-uCMDB 连接器的状态：

   ```
   /etc/init.d/opsware-sas status telldaemon
   ```

   有关详细信息，请参见显示 SA-uCMDB 连接器的状态。

enable 命令

在启动 SA-uCMDB 连接器之前，必须使用 **enable** 命令启用它。在启用它时，需提供 uCMDB 服务器名称或 IP 地址、端口号、登录名和密码。

使用 **enable** 命令配置和启用 SA-uCMDB 连接器。本节将描述 **enable** 命令。您必须启用 SA-uCMDB 连接器，才能启动它。

enable 命令将执行以下操作：

- 创建自定义的 SA-uCMDB 连接器配置文件 **/etc/opt/opsware/tell/tell_custom.conf**（如果它不存在）。（默认情况下，除非手动创建自定义配置文件，否则部署时不会预先存在。）
- 修改自定义配置文件 **/etc/opt/opsware/tell/tell_custom.conf**，并将 uCMDB 服务器的主机名或 IP 地址、端口号以及登录名输入到此文件中。
- 保存用户密码。
- 修改文件 **/opt/opsware/oi_util/startup/components.config**，并取消注释 **telldaemon**（SA-uCMDB 连接器的进程）的行。

如果在运行 SA-uCMDB 连接器时修改任意 uCMDB 配置参数，则必须停止并重新启动 SA-uCMDB 连接器，才能使更改生效。

enable 命令的位置

enable 命令位于 SA 核心服务器的 `/opt/opsware/tell/bin` 目录中。

enable 命令中的新语法

在 SA 9.14 中，已向 SA-uCMDB 连接器的 **enable** 命令添加其他参数，以便支持新的 uCMDB 浏览器。本节和表 8 对这些参数进行了描述。

```
enable [--protocol <ucmdb_protocol>] [--host <ucmdb_host_ip>] [--port
<ucmdb_host_port_number>] [--browser_protocol <ucmdb_browser_protocol>]
[--browser_host <ucmdb_browser_host_ip>] [--browser_port
<ucmdb_browser_host_port>] [--user <ucmdb_admin_user>] [--password
<ucmdb_admin_password>] [--help]
```

表 8　　enable 命令的新参数

参数	描述	新
`--protocol <ucmdb_protocol>`	uCMDB 服务器协议：http 或 https。默认值为 http。	新
`--host <ucmdb_host_ip>`	此选项提供 HP uCMDB 服务器的 IP 地址或主机名。默认值为 localhost。	—
`--port <ucmdb_host_port_number>`	此选项提供 HP uCMDB 服务器的端口号。默认值为 8080。	—
`--browser_protocol <ucmdb_browser_protocol>`	uCMDB 浏览器服务器协议: http 或 https。默认值为 http。	新
`--browser_host <ucmdb_browser_host_ip>`	此选项提供 HP uCMDB 浏览器的 IP 地址或主机名。默认值为 localhost。	新
`--browser_port <ucmdb_browser_host_ port>`	此选项提供 uCMDB 浏览器的主机端口。默认值为 8080。	新
`--user <ucmdb_admin_user>`	此选项提供 HP uCMDB 服务器管理用户的用户名。默认值为 admin。	—
`--password <ucmdb_admin_password>`	此选项提供 `--user` 选项中用户的密码。默认值为 admin。	—

未启用 SSL 的 **enable** 命令的示例：

```
enable --protocol http --host 192.168.8.93 --port 9999 --browser_protocol
http --browser_host 192.168.8.100 --browser_port 8888 --user john-ucmdb
--password mypass1234
```

已针对 uMCDB 服务器和 uMCDB 浏览器启用 SSL 的 **enable** 命令的示例：

```
enable --protocol https --host 192.168.8.93 --port 9999 --browser_protocol
https --browser_host 192.168.8.100 --browser_port 8888 --user john-ucmdb
--password mypass1234
```

显示 SA-uCMDB 连接器的状态

要显示 SA-uCMDB 连接器的状态，请在 SA 核心服务器上输入以下命令：

```
/etc/init.d/opsware-sas status telldaemon
```

如果 SA-uCMDB 连接器启用但未运行，则输出将与以下类似：

```
Verify "telldaemon" running:FAILURE (pidfile does not exist)
Failed to perform "status" operation on Opsware SAS components.
```

如果 SA-uCMDB 连接器被禁用，则输出将与以下类似：

```
opsware-sas:One or more of the specified components does not exist in the
following file:
  /opt/opsware/oi_util/startup/components.config
```

SA-uCMDB 数据关系和转移

保留的 CI 关系

表 9 列出了 SA-uCMDB 连接器保留的配置项 (CI) 关系。

表 9　　保留的 CI 关系

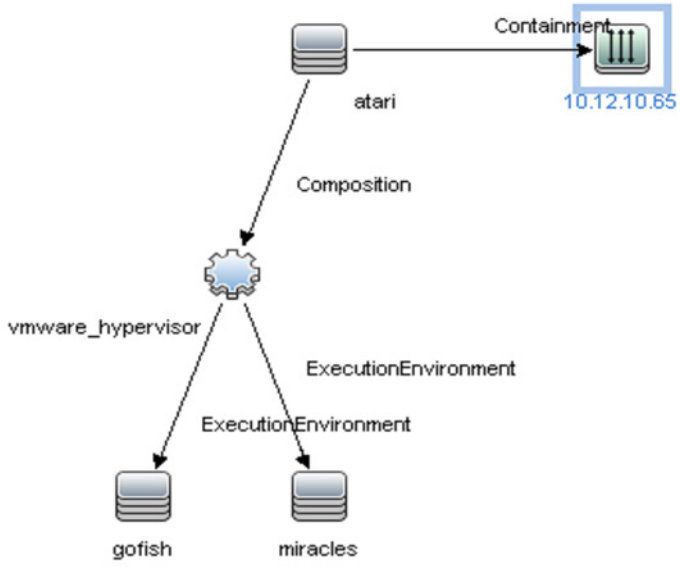
来自 uCMDB CI	方式	来自 uCMDB CI
Node	包含	IpAddress
Node	复合	InstalledSoftware
Node	复合	Hypervisor
Node	聚合	PolicyResult
Hypervisor	执行环境	Node
Policy	复合	PolicyResult
SaSystem	聚合	Node
SaSystem	聚合	Policy

示例：显示 SA 托管服务器的 uCMDB

图 18 来自 HP uCMDB 屏幕，它显示以下内容：

- 名为 “atari”的 SA 托管服务器。
- 此托管服务器的 IP 地址 10.12.10.65。
- 托管服务器 “atari”正在运行一个 VMware 虚拟机监控程序。
- 名为 “gofish”和 “miracles”的两个虚拟机正在该虚拟机监控程序上运行。

图 18　显示在 uCMDB 中的 SA 托管服务器



转移到 uCMDB 的 SA 数据

SA 数据库中的以下数据会转移到 uCMDB 配置项 (CI) 和特性 （请参见表 10）：

表 10　由 SA 填充的 uCMDB CI 和特性

uCMDB CI	uCMDB 特性
Node	Name
Node	Description
Node	BiosAssetTag
Node	DefaultGatewayIpAddress
Node	NodeModel
Node	SerialNumber
Node	BiosUuid
Node	NetBiosName
Node	MemorySize
Node	OsDescription

表 10　由 SA 填充的 uCMDB CI 和特性 （续）

uCMDB CI	uCMDB 特性
Node	OsFamily
Node	TenantOwner
IpAddress	Name
IpAddress	RoutingDomain
InstalledSoftware	Name
InstalledSoftware	Vendor
InstalledSoftware	BuildNumber
InstalledSoftware	DmlProductName
Hypervisor	Name
Hypervisor	Description
Hypervisor	ProductName
Policy	Name
Policy	Description
Policy	PolicyCategory
Policy	PolicyDefinedBy
PolicyResult	Name
PolicyResult	PolicyResultDateTime
PolicyResult	ComplianceStatus
PolicyResult	RulesCompliant
PolicyResult	RulesNonCompliant
PolicyResult	ComplianceLevel
SASystem	Name
SASystem	Description
SASystem	Version

数据转移到 uCMDB 的频率

在 SA-uCMDB 连接器首次开始运行时，会查询 SA 数据库、在 uCMDB 中创建 CI 以及将数据从 SA 转移到 uCMDB。在此之后，当 SA 数据库中的数据发生更改时，SA-uCMDB 连接器会自动检测更改并将修改的数据转移到 uCMDB。连接器会将信息记录在日志文件 /var/log/opsware/tell/LOAD_STATS.0.log 中。

有关从 SA 转移到 uCMDB 的数据的完整列表，请参见转移到 uCMDB 的 SA 数据。

从 SA 客户端访问 uCMDB 浏览器

uCMDB 浏览器窗口

您可以在 uCMDB 浏览器窗口中查看服务器详细信息。

要查看服务器详细信息，请执行以下操作：

1 登录到 SA 客户端。

2 转到 “设备” > “所有托管服务器”。

3 选择任意服务器，然后单击 “操作” > “Open with uCMDB Browser”。

可选：还可以使用此处或搜索面板上的上下文菜单。选择此服务器，然后右键单击并选择 “打开方式” > “uCMDB 浏览器”。

SA 用于打开特定托管服务器的 uCMDB 浏览器的示例 URL：

```
http://my-ucmdb.mycomp.com:8080/ucmdb-api/ucmdb-browser/
?locale=en&theme=LIGHT#refocus-selection=<global_ucmdb_id>
```

4 如果尚未登录 uCMDB 浏览器，则此 URL 将调用 uCMDB 浏览器登录屏幕。使用 uCMDB 登录凭据完成登录。您只需要针对每个会话登录一次。

提示：如果打开 uCMDB 浏览器时出现空白页面或发生 “找不到页面” 错误，则可能意味着 uCMDB 未设置或 uCMDB 服务器未运行或配置错误。请确保已配置 uCMDB 服务器并且 Tellconnector 正在运行。

如果 SA-uCMDB 连接器尚未配置并且需要禁用 “Open with uCMDB Browser” 菜单项，请转到 “系统配置” > “Opsware” > “Tell” 并将 “uCMDB 浏览器 URL” 和 “uCMDB URL” 的值设置为空。

配置 uCMDB 浏览器

如果需要从 SA 客户端调用 uCMDB 浏览器，则需要在使用以下 **/opt/opsware/tell/bin/enable** 参数启用 SA-uCMDB 连接器之后指定 uCMDB 浏览器的相关参数：

```
--browser_protocol      - uCMDB 浏览器服务器协议：http 或 https
--browser_host          - uCMDB 浏览器主机名或 IP
--browser_port          - uCMDB 浏览器主机端口
```

此外，默认情况下， SA 客户端通过可兼容 uCMDB 9.05 的 URL 前缀调用 uCMDB 浏览器。

例如，要使用基于 uCMDB 10.01 的浏览器，请执行以下操作：

1 通过运行 **stop** 命令，停止 SA-uCMDB 连接器：

```
/etc/init.d/opsware-sas stop telldaemon
```

2 通过运行 **disable** 命令，禁用 SA-uCMDB 连接器：

```
disable
```

重要提示：请确保连接器已停止并禁用。如果在修改配置文件时未停止和禁用连接器，则在尝试重新启动连接器时可能遇到问题。

3 在自定义 SA-uCMDB 连接器配置文件 /etc/opt/opsware/tell/tell_custom.conf 中更新 uCMDB 浏览器前缀，以显示正确的 uCMDB 版本。

例如：

将以下 uCMDB 9.05 默认值：

```
com.hp.sa.tell.ucmdb.browser.path.suffix=/ucmdb-api/ucmdb-browser
```

更改为 uCMDB 10.01 前缀：

```
com.hp.sa.tell.ucmdb.browser.path.suffix=/ucmdb-browser
```

4 更新此配置文件后，运行 **enable** 命令启用 SA-uCMDB 连接器。

➤ enable 命令的语法随环境而变化。有关 enable 命令语法和选项的说明，请参见本文档中的 enable 命令。

5 重新启动 uCMDB 连接器。输入以下命令以启动 SA-uCMDB 连接器：

```
/etc/init.d/opsware-sas start telldaemon
```

6 可以选择使用以下命令检查 SA-uCMDB 连接器的状态：

```
/etc/init.d/opsware-sas status telldaemon
```

对 uCMDB 服务器版本 9.05 和 10.01 的支持

对于 SA-uCMDB 集成， SA 9.14 或更高版本支持以下 uCMDB 服务器集成：

- uCMDB 9.05 内容包 10 或更高版本、累积更新程序包 6 或更高版本
- uCMDB 10.01 内容包 12

➤ 版本支持和兼容性信息随时更改。有关完整最新的支持和兼容性信息，请参见相关产品发布的支持列表。可在 HP 软件联机支持网站上查找所有支持列表和产品手册，网址为：

http://support.openview.hp.com/sc/support_matrices.jsp

您还可以从 HP 软件联机支持产品手册网站下载此发布的《HP Server Automation Support and Compatibility Matrix》，网址为：

http://support.openview.hp.com/selfsolve/manuals

全局 uCMDB ID

使用 uCMDB 9.04 和早期版本时， SA 中仅同步该 uCMDB 服务器所知的本地 uCMDB ID。

使用 uCMDB 9.05 和更高版本时，可以将 uCMDB 服务器配置为 uCMDB 全局 ID 生成器，其中，生成的 uCMDB ID 在多个 uCMDB 服务器环境中是全局 和唯一 的。在这类环境中，需要这些全局 ID 来正确调用 uCMDB 浏览器。

SA 9.14 SA-uCMDB 连接器已得到增强，在将 uCMDB 服务器配置为全局 ID 生成器时，此连接器会自动使用 CI 的全局 uCMDB ID。无需对 SA-uCMDB 连接器进行特殊配置。

与 uCMDB 服务器和 uCMDB 浏览器的 SSL 连接

SA-uCMDB 连接器支持 uCMDB 服务器和 uCMDB 浏览器的 SSL 协议。

在启用安全套接字层 (SSL) 通信时，需要为 SA-uCMDB 连接器提供适合的证书和密钥库。

要启用 SSL，请执行以下操作：

1 遵循 《uCMDB 部署指南》的 “启用安全套接字层通信” 中的说明，创建 uCMDB 密钥库并将证书导出到文件。

2 将步骤 1 中导出的证书导入到安装 SA-uCMDB 连接器的位置。例如，密钥库必须位于 **/var/opt/opsware/crypto/tell** 中，并且密钥库文件名为 **tell.keystore**，密钥库密码为 **hppass**。

import 命令的示例：

```
/opt/opsware/jdk1.6/bin/keytool -import -noprompt -alias hpsaucmdb -file
<path_to_the_exported_hpcert> -keypass hppass -keystore /var/opt/opsware/
crypto/tell/tell.keystore -storepass hppass
```

升级期间存档的可配置文件

升级期间，将存档某些可自定义和可配置的文件，以便保留。

如果从 SA-uCMDB 连接器 9.14 升级到 10.0，则以下文件将存档在 `/var/opt/opsware/install_opsware/config_file_archive/<respective path for file>` 中

- `tell.conf`
- `mapping.xml`
- `logging.properties`
- `tell_conversions.jar`
- `tell.pwd`
- `tell.keystore`

  例如，位于 **/etc/opt/opsware/tell/tell_custom.com** 的 **tell_custom.conf** 将存档到 `/var/opt/opsware/install_opsware/config_file_archive/etc/opt/opsware/tell/tell_custom.com<time_stamp_of_upgrade>`

对于 SA-uCMDB 连接器 10.0 和未来的升级，还会存档 **tell_custom.conf** 和 **mapping_custom.xml**，以便保留。

故障排除提示

在第二个核心上运行 SA-uCMDB 连接器

在某些情况下，需要停用多主控 SA 网状网络中的某个特定核心，因此有必要从该网状网络中的其他核心运行 SA-uCMDB 连接器。有时，如果其他核心到 uCMDB 服务器的网络性能是首选，则也需要执行此操作。在这些场景中，有必要执行下列步骤：

要在第二个核心上运行连接器，请执行以下操作：

1 在第一个核心上停止 SA-uCMDB 连接器并删除其与此核心的关联。

```
/etc/init.d/opsware-sas stop telldaemon
/opt/opsware/tell/bin/tell --release
```

2 在第二个核心上，运行 **enable** 命令启用 SA-uCMDB 连接器。

enable 命令的语法随环境而变化。有关 enable 命令语法和选项的说明，请参见本文档中的 enable 命令。

3 执行 SA-uCMDB 集成，然后重新启动 SA-uCMDB 连接器。

```
/opt/opsware/tell/bin/tell --take
/etc/init.d/opsware-sas start telldaemon
```

要启用其他日志记录，请执行以下操作：

1 启动 SA-uCMDB 连接器。

正常的日志记录将存储在 **/var/log/opsware/tell** 目录中。默认文件名包括：

```
tell.0.log              （正常启动日志）
ucmdb_failure.*.log     （同步期间看到的 uCMDB 失败日志）
LOAD_STATS.*.log        （处理的数据量）
```

2 要请求其他日志记录详细信息，请在 **/etc/opt/opsware/tell/logging.properties** 文件中指定请求的信息，如表 11 中所示。

表 11 /etc/opt/opsware/tell/logging.properties 字段

字段	描述
java.util.logging.FileHandler.limit	指定要写入任意一个文件的最大字节数。默认值为 10000000。
java.util.logging.FileHandler.count	指定要使用的文件数。默认值为 10。
java.util.logging.FileHandler.append	指定附加模式，默认值为 true。
java.util.logging.FileHandler.pattern	指定可找到日志文件的输出文件的命名模式。默认值为 **/var/log/opsware/tell/tell.%g.log**

警告：修改文件限制时务必谨慎。数量太大可能会影响性能。

按需同步

重新启动 SA 后，SA-uCMDB 连接器通常会从重新启动之前结束的位置继续将 SA 数据同步到 uCMDB。连接器还会定期运行完全同步。但是，在某些情况下，例如存在阻止 uCMDB 服务器获取更新的网络或服务器问题时，则可能需要按需触发完全同步。

要触发按需同步，请执行以下操作：

1 停止 SA-uCMDB 连接器。

2 使用以下选项重新启动 SA-uCMDB 连接器：

```
/opt/opsware/tell/bin/tell --startfresh
```

查看日志文件

SA-uCMDB 连接器生成以下文本日志文件。您可以在文本编辑器中查看这些日志文本，以获取更多信息。

- **/var/log/opsware/tell/tell.0.log** 是主日志文件，用于记录 SA-uCMDB 连接器遇到的信息、警告和错误。
- **/var/log/opsware/tell/LOAD_STATS.0.log** 包含初始数据加载的状态和统计信息，以及完成初始数据加载的大约次数。
- **/var/log/opsware/tell/ucmdb_failure.0.log** 包含 uCMDB 错误，主要是协调错误（例如，SA 数据不完整、所需 uCMDB 键缺失）。例如，如果服务器没有序列号或 IP 地址，则可能发生这种情况。此日志文件包含 uCMDB 异常、失败原因以及对导致此异常的 CI 的跟踪。

SA-uCMDB 连接器守护程序

SA-uCMDB 连接器在 SA 核心服务器上运行守护程序 **/etc/opt/opsware/startup/telldaemon**。请确保在 SA 核心服务器上运行此进程。

如果没有运行此进程，请按照启用并启动 SA-uCMDB 连接器中所述启动它。

如果正在运行此进程，请按照显示 SA-uCMDB 连接器的状态中所述检查其状态。

示例 - SA-uCMDB 连接器映射文件

```
<DB-UCMBD-HIGHLEVEL-MAPPING>
    <!-- generates installed_software.xml -->
    <Model-Definition model-name='sa' enable='true'>
        <CI ucmdb-ci-type-name='server_automation_system' enable='true'
base-class='server_automation_system'>
            <Attribute source='SA/Description' target-attr='description'
enable='true'/>
            <Attribute source='SA/Name'  target-attr='name' enable='true'/>
           <Attribute-Default target-attr='version' target-attr-value='9.14'
enable='true'/>
        </CI>
    </Model-Definition>


    <!-- generates node.xml -->
    <Model-Definition model-name='hosts' enable='true'>
       <CI ucmdb-ci-type-name='server_automation_system' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='ip_address' enable='true' base-class='node'>
```

```
            <Attribute source='IpAddress/PrimaryIpName' target-attr='name'
enable='true'/>
            <Attribute source='IpAddress/RoutingDomain'
target-attr='routing_domain' enable='true'/>
        </CI>

        <CI ucmdb-ci-type-name='node' enable='true' base-class='node'>
            <Attribute source='Node/Name' target-attr='name' enable='true'/>
            <Attribute source='Node/Description' target-attr='description'
enable='true'/>
           <Attribute source='Node/BiosAssetTag' target-attr='bios_asset_tag'
enable='true'/>
            <Attribute source='Node/BiosSerialNumber'
target-attr='serial_number' enable='true'/>
            <Attribute source='Node/BiosUuid' target-attr='bios_uuid'
enable='true'/>
            <Attribute source='Node/DefaultGatewayIpAddress'
target-attr='default_gateway_ip_address' enable='true'/>
            <Attribute source='Node/NetBiosName' target-attr='net_bios_name'
enable='true'/>
            <Attribute source='Node/NodeModel' target-attr='node_model'
enable='true'/>
            <Attribute source='Node/MemorySize' target-attr='memory_size'
enable='true'/>
            <Attribute source='Node/OsDescription'
target-attr='os_description' enable='true'/>
            <Attribute source='Node/OsFamily' target-attr='os_family'
enable='true'/>
            <Attribute source='Node/TenantOwner' target-attr='TenantOwner'
enable='true'/>
            <Attribute source='Node/Facility' target-attr='facility'
enable='false'/>
            <Attribute source='Node/VirtualizationTypeId'
target-attr='virtualization_type_id' enable='false'/>
            <Attribute source='IpAddress/ManagementIpName'
target-attr='ip_address' enable='false'/>
            <CI-Filter enable='true'><![CDATA[(DEVICES.OPSW_LIFECYCLE =
'MANAGED')]]></CI-Filter>
        </CI>

        <Relation ucmdb-relation-type-name='containment'
ucmdb-relation-from-ci-type-name='node'
ucmdb-relation-to-ci-type-name='ip_address' enable='true'
ucmdb-relation-id-link='true'/>
        <Relation ucmdb-relation-type-name='aggregation'
ucmdb-relation-from-ci-type-name='server_automation_system'
ucmdb-relation-to-ci-type-name='node' enable='true'
ucmdb-relation-id-link='false'/>
    </Model-Definition>


    <!-- generates installed_software.xml -->
    <Model-Definition model-name='software' enable='true'>
        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>
```

```
        <CI ucmdb-ci-type-name='installed_software' enable='true'
base-class='installed_software'>
            <Attribute source='InstalledSoftware/DmlProductName'
target-attr='dml_product_name' enable='true'/>
            <Attribute source='InstalledSoftware/Name'  target-attr='name'
enable='true'/>
            <Attribute source='InstalledSoftware/Version'
target-attr='version' enable='true'/>
           <Attribute source='InstalledSoftware/Vendor' target-attr='vendor'
enable='true'/>
        </CI>

        <Relation ucmdb-relation-type-name='composition'
ucmdb-relation-from-ci-type-name='node'
ucmdb-relation-to-ci-type-name='installed_software'
ucmdb-relation-id-link='true' enable='true'/>
    </Model-Definition>


    <!-- generates policy.xml -->
    <Model-Definition model-name='compliance' enable='true'>
       <CI ucmdb-ci-type-name='server_automation_system' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='policy' base-class='policy' enable='true'>
           <Attribute source='Policy/Name' target-attr='name' enable='true'/>
            <Attribute source='Policy/Description' target-attr='description'
enable='true'/>
            <Attribute-Default target-attr='policy_defined_by'
target-attr-value='SA' enable='true'/>
            <Attribute-Default target-attr='policy_category'
target-attr-value='audit' enable='true'/>
        </CI>

        <Relation ucmdb-relation-type-name='aggregation'
ucmdb-relation-from-ci-type-name='server_automation_system'
ucmdb-relation-to-ci-type-name='policy' enable='true'
ucmdb-relation-id-link='false'/>
     </Model-Definition>


    <!-- generates hypervisor.xml -->
    <Model-Definition model-name='hypervisor' enable='true'>
        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='hypervisor' base-class='hypervisor'
enable='true'>
            <Attribute source='Hypervisor/Name' target-attr='name'
enable='true'/>
            <Attribute source='Hypervisor/Description'
target-attr='description' enable='true'/>
            <Attribute source='Hypervisor/ProductName'
target-attr='product_name' enable='true'/>
```

```
        </CI>

        <Relation ucmdb-relation-type-name='composition'
ucmdb-relation-from-ci-type-name='node'
ucmdb-relation-to-ci-type-name='hypervisor' ucmdb-relation-id-link='true'
enable='true'/>
    </Model-Definition>


    <!-- generates hypervisorRelation.xml -->
    <Model-Definition model-name='vmrelations' enable='true'>
        <CI ucmdb-ci-type-name='hypervisor' base-class='hypervisor'
reference-ci='true' enable='true'/>

        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>

        <Relation ucmdb-relation-type-name='execution_environment'
ucmdb-relation-from-ci-type-name='hypervisor'
ucmdb-relation-to-ci-type-name='node' ucmdb-relation-id-link='false'
enable='true'/>
    </Model-Definition>

    <!-- generates policyResult.xml -->
    <Model-Definition model-name='compliance_status' enable='true'>
        <CI ucmdb-ci-type-name='policy' base-class='policy'
reference-ci='true' enable='true'/>

        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='policy_result' base-class='policy_result'
enable='true'>
            <Attribute source='PolicyResult/Name' target-attr='name'
enable='true'/>
            <Attribute source='PolicyResult/ComplianceStatus'
target-attr='compliance_status' enable='true'/>
            <Attribute source='PolicyResult/PolicyResultDateTime'
target-attr='policy_result_date_time' enable='true'/>
            <Attribute source='PolicyResult/RulesCompliant'
target-attr='rules_compliant' enable='true'/>
            <Attribute source='PolicyResult/RulesNonCompliant'
target-attr='rules_non_compliant' enable='true'/>
            <Attribute source='PolicyResult/ComplianceLevel'
target-attr='compliance_level' enable='true'/>
        </CI>

        <Relation ucmdb-relation-type-name='composition'
ucmdb-relation-from-ci-type-name='policy'
ucmdb-relation-to-ci-type-name='policy_result' ucmdb-relation-id-link='false'
enable='true'/>
        <Relation ucmdb-relation-type-name='aggregation'
ucmdb-relation-from-ci-type-name='node'
ucmdb-relation-to-ci-type-name='policy_result' ucmdb-relation-id-link='true'
enable='true'/>
```

```
    </Model-Definition>
</DB-UCMBD-HIGHLEVEL-MAPPING>
```