HP Server Automation

软件版本：10.2

SA 管理指南

文档发布日期：2014 年 12 月 22 日
软件发布日期：2014 年 12 月 22 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。

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

此站点需要您注册 HP Passport 并登录。要注册 HP Passport ID，请访问：**http://h20229.www2.hp.com/passport-registration.html**

或单击 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。

支持

访问 HP 软件联机支持网站，地址为：**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

HP 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 HP 产品解决方案，包括 HP 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 **http://h20230.www2.hp.com/sc/solutions/index.jsp**

目录

第 1 章

用户和用户组设置及安全性

SA 提供了基于角色的安全模型，该模型只允许经过授权的用户在特定服务器上执行特定操作。本章面向安全管理员，解释了如何为 SA 设置基于角色的安全结构。

关于 SA 用户和用户组

SA 用户组代表一个角色，并定义执行该角色所需的权限集。您需要为每个用户组授予一组权限，然后将用户分配给一个或多个用户组。每个用户组将一组权限授予属于该组的所有用户。

所有用户可以属于一个或多个 SA 用户组。用户有权执行的任务由用户所属的用户组定义。

每个 SA 用户组：

- **代表一个角色**，该角色是一组任务和责任。
- **定义一组权限**，用于启用执行该角色所需的任务集。
- **包含执行该角色的 SA 用户集**。

图 1 显示了两个示例用户组。一个示例用户组用于符合性管理员，其角色是运行审核报告和确保服务器符合公司策略；另一个示例用户组用于系统操作员，其角色是监控服务器以及安装软件和修补程序。每个用户组包含一组权限和一组用户：

图 1.基于角色的用户组的内容

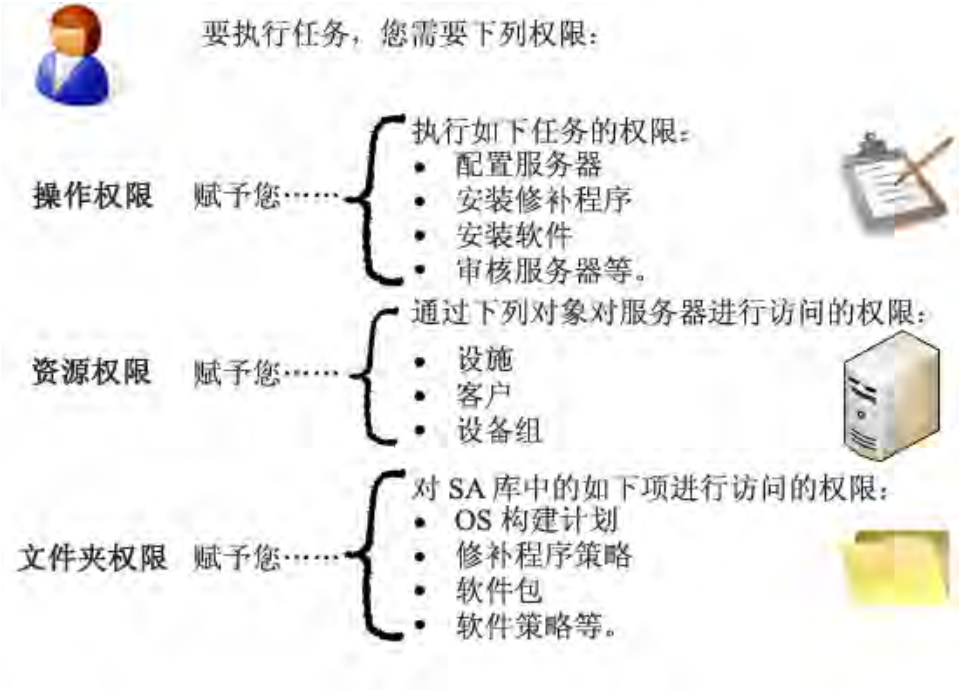
SA 提供一组预定义用户组，但是您可以创建自己的用户组以匹配您的组织中的角色。有关详细信息，请参见预定义用户组。

关于权限类型 - 操作权限、资源权限和文件夹权限

SA 提供三种在服务器上执行任何操作所需的权限：

- **操作权限**指定用户可执行的操作或任务。
- **资源权限**指定用户执行这些操作所在的服务器。所有服务器按设施、客户和设备组分组。您可以通过指定对设施、客户和设备组的访问权限来设置资源权限。
- **文件夹权限**指定对 SA 库中项的访问权限，这些项包括 OS 构建计划、软件包、软件策略、修补程序策略、审核策略等。

图 2.执行任务所需的 SA 权限类型



例如，要使用软件策略安装软件，用户（至少）需要关于权限类型 - 操作权限、资源权限和文件夹权限中显示的权限：

图 3.安装软件所需的权限

这些权限（和其他权限）是在预定义用户组 Software Deployers 中设置的。有关详细信息，请参见预定义用户组。

图 4 显示名为 Software Deployers 的预定义用户组以及作为该组成员的 SA 用户。“视图”导航面板还显示此用户组的资源权限、文件夹权限、操作权限和 OGFS 权限。

图 4.用户组浏览器，显示了作为成员的用户

关于操作权限

操作权限定义用户可以执行的任务。一些操作权限指定下列访问类型：

- **读取**：用户可以执行任务，但是在只读模式下执行。
- **读取和写入**：用户可以完全执行任务。
- **无**：任务不出现在 SA 客户端中。用户无法查看或执行任务。

其他操作权限类型指定下列访问类型：

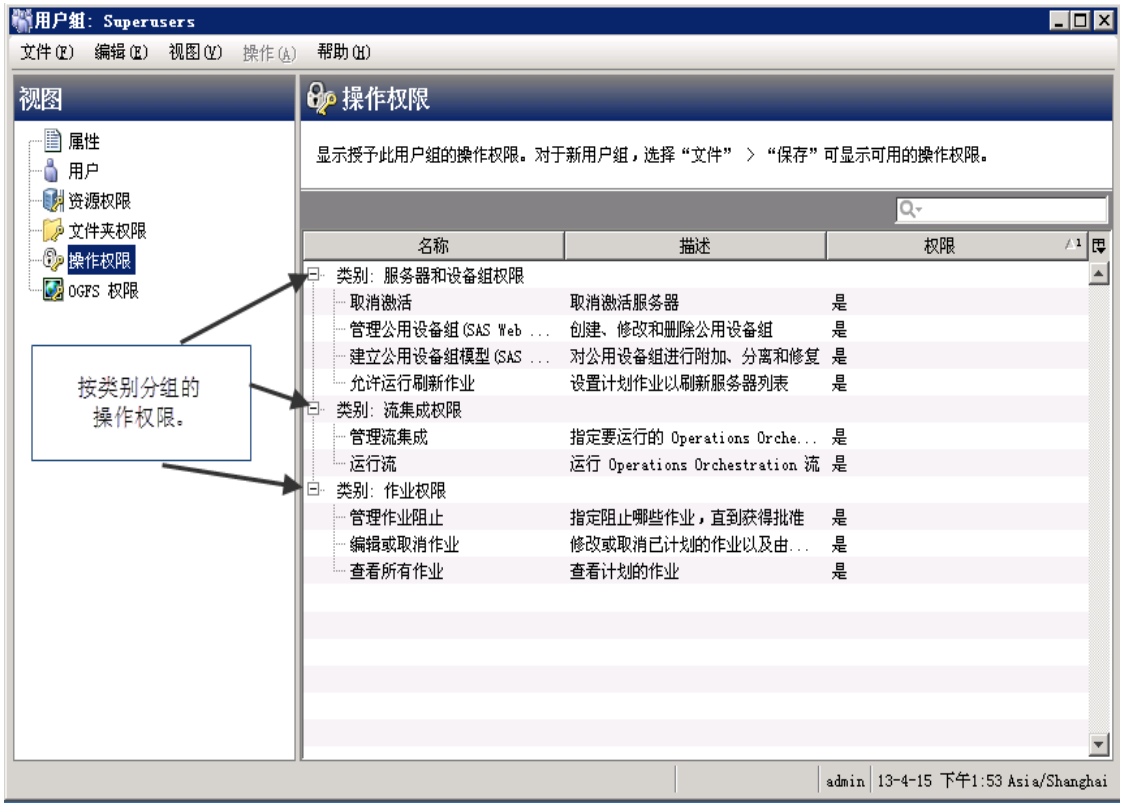
- **是**：用户可以执行任务。
- **否**：用户无法执行任务。

有关操作权限的完整列表，请参见权限参考和设置操作权限。

将操作权限分组

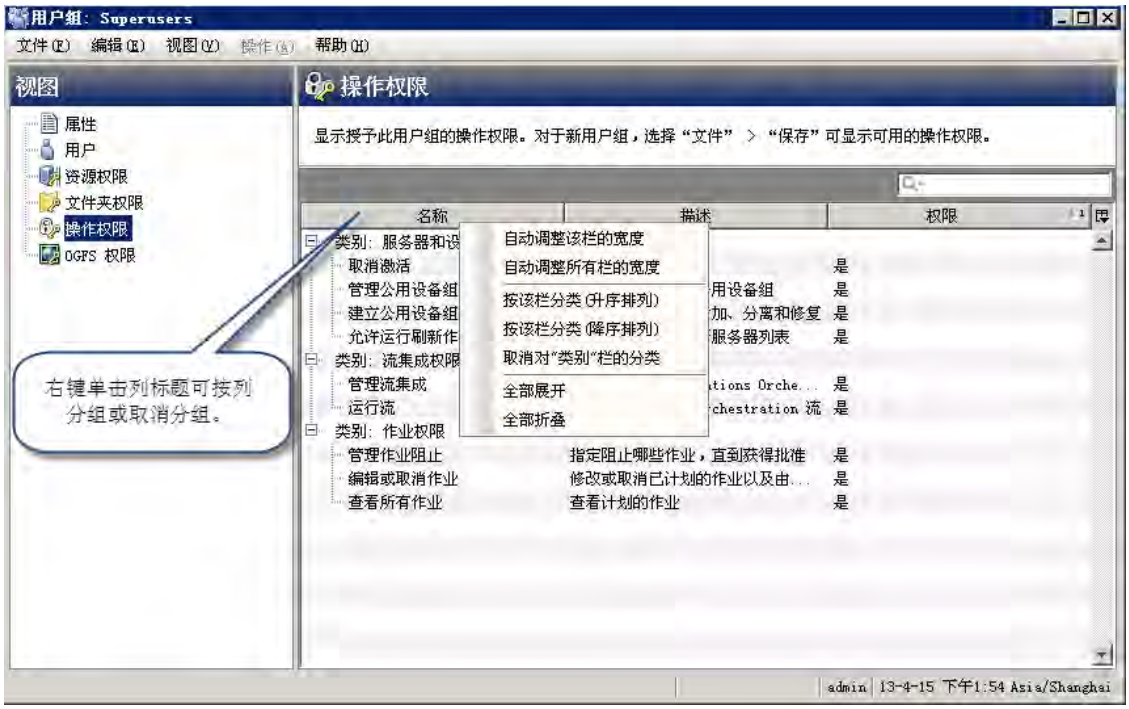
当您打开用户组时，SA 客户端显示用户组的操作权限。操作权限按类别分组，如**图 5** 所示。

图 5.用户组窗口 - 操作权限视图，按类别分组



您可以通过右键单击任何列，取消操作权限的分组，或者按其他列将它们分组，如**图 6** 所示。

图 6.用户组窗口 - 操作权限视图，分组菜单



关于资源权限

资源 是一个或多个托管服务器。服务器资源按下列类别进行组织：

- **设施**：与 SA 设施关联的服务器。每个托管服务器属于且只能属于您的一个设施。
- **客户**：与客户关联的服务器。您可以创建客户，将每个服务器分配给一个客户。每个服务器属于且只属于一个客户，该客户可以是“未分配”客户组。
- **设备组**：属于设备组的服务器。您可以创建设备组，然后将服务器分配给设备组。每个服务器可以属于一个或多个设备组。

用户组的资源权限确定用户组中的用户是可以查看还是可以修改服务器。用户组只有权访问它被授予资源权限的设施、客户和设备组中的服务器。由于每个服务器属于一个设施、一个客户和至少一个设备组，若要有权访问服务器，用户组必须拥有对至少一个设施、至少一个客户和至少一个设备组的权限。

您可以组合客户、设施和设备组权限以实现安全策略。例如，您可以限制对与 Acme Corp. 客户关联的、驻留在 Fresno 设施中的、属于仅包含 Windows 服务器的设备组的服务器的访问权限（请参见资源权限的示例）。

任何一个服务器都位于一个设施中，与一个客户关联，并位于一个或多个设备组中。用户需要访问该设施、该客户和至少一个包含该服务器的设备组，才能获取对该服务器的访问权限。另请参见设置资源权限 - 设施、客户和设备组。

资源访问权限的类型

资源权限必须确定下列访问权限类型之一：

- **读取**：用户只能查看资源。
- **读取和写入**：用户可以查看、创建、修改或删除资源。
- **无**：资源不出现在 SA 客户端中。用户无法查看或修改资源。

关于设施权限

每个服务器位于一个且仅位于一个设施中。要修改特定设施中的服务器，用户必须属于具有该设施的读取和写入权限的用户组。例如，如果您希望某个组的用户能够查看（而不是修改）London 设施中的服务器，请将权限设置为“读取”。

设施权限还控制对设施对象本身的访问权限。例如，要修改设施的属性，用户必须属于具有该设施的读取和写入权限以及用于修改该设施的操作权限的组。

关于客户权限

每个服务器与一个且仅与一个 SA 客户关联（即使该客户是“未分配”客户组）。SA 客户是一个可以放入服务器的逻辑组。您可以对属于 SA 客户的所有服务器执行 IT 管理任务（只要您对该客户具有读取和/或写入权限），从而提供安全性和授权边界。例如，如果您希望某个组的用户能够查看（而不是修改）与 Widget Inc. 客户关联的服务器，请将权限设置为“读取”。

客户权限还控制对客户对象本身的访问权限。例如，要将自定义特性添加到客户，用户必须属于具有该特定客户的读取和写入权限以及用于修改该设施的操作权限的组。

关于设备组权限

每个服务器可以属于一个或多个设备组。通过设置设备组权限，您可以控制用户组中用户拥有的对设备组中服务器的访问权限。例如，如果您希望某个组的用户能够查看（而不是修改）Windows Server 2008 设备组中的服务器，请将权限设置为“读取”。

默认情况下，每个服务器属于一个公用设备组，具体取决于其操作系统。可以通过选择“设备”选项卡并选择“设备组”>“Public”>“Opsware”>“操作系统”，在 SA 客户端中查看这些设备组。

如果服务器属于多个设备组，则用户组只需要这些设备组之一的权限，即可获取对该服务器的访问权限。

虽然设备组可以包含其他设备组，但是被包含的设备组不继承权限。

您不能控制对专用设备组的访问权限。只有创建专用设备组的用户才能看到专用设备组。

设备组权限控制对属于设备组的服务器的访问权限。但是，这些权限不控制设备组的管理。要创建、修改或删除设备组，用户必须属于具有“管理公用设备组”和“建立公用设备组模型”操作权限以及“托管的服务器和组”操作权限的用户组。用户必须是超级管理员，才能将设备添加到正用作访问控制组的设备组。

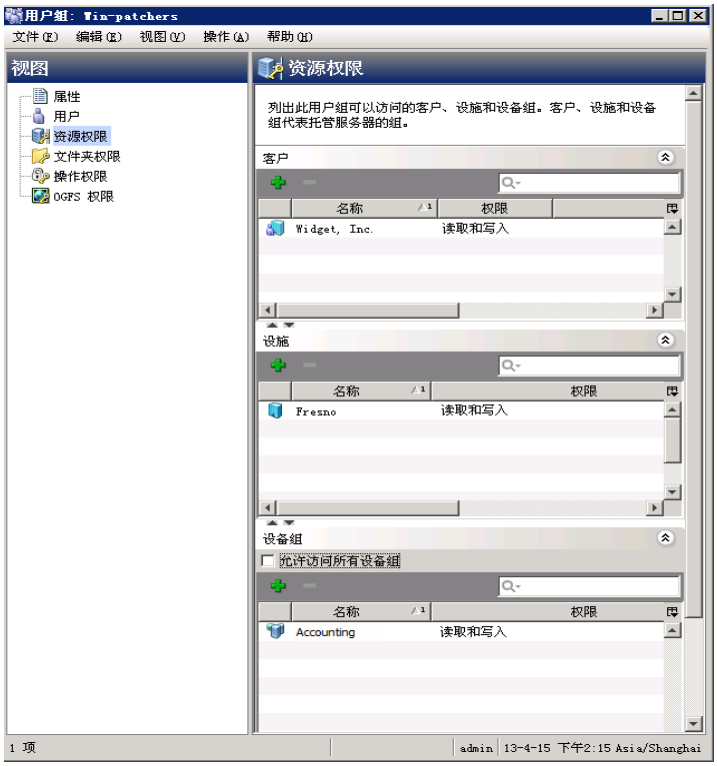
资源权限的示例

假设服务器驻留在 Fresno 设施中，与 Widget, Inc. 客户关联，且属于 Accounting 设备组。要修改服务器，用户组必须具有**表 1** 中所列的权限。这些权限还显示在**图 7** 中（用于名为 Win-patchers 的用户组）。

表 1.资源权限的示例

资源	访问权限
设施：Fresno	读取和写入
客户：Widget, Inc.	读取和写入
设备组：Accounting	读取和写入

图 7.用户组屏幕中的资源权限视图



如果设施、客户或设备组的访问权限不匹配，则强制实施**最严格的**权限。

例如，如**表 2** 所示，如果客户和设备组的权限为“读取和写入”，但是设施的权限为“读取”，则强制实施“读取”权限，用户将无法修改服务器。

如果客户的权限为“无”，则无法查看服务器，即使用户组的其他选项指定“读取”或“读取和写入”也是如此。

表 2.不匹配资源权限的示例

资源	权限
设施：Fresno	读取
客户：Widget, Inc.	读取和写入
设备组：Accounting	读取和写入

组合资源和操作权限 - 示例

要对资源执行操作，用户所属的组必须同时具有操作和资源（服务器）的必需权限。例如，假设某服务器与这些资源关联：Widget, Inc. 客户、Fresno 设施和 Red Hat AS 4 设备组。要在此服务器上安装修补程序，用户所属的组必须具有**表 3** 中所列的权限。

表 3.资源权限和操作权限的示例

资源和操作	权限
客户：Widget, Inc.	读取和写入
设施：Fresno	读取和写入
设备组：Red Hat AS 4	读取和写入
操作：安装修补程序	是

其他资源类型

托管服务器是最常见的资源。其他资源类型有：

- 硬件定义
- 领域
- OS 安装配置文件

这些资源中的每一个资源都可以与客户关联。

文件夹也可以与客户关联，但是对文件夹的访问权限受其他方法控制（请参见关于文件夹权限）。

关于文件夹权限

文件夹权限控制对 SA 库中文件夹内容（例如软件策略、修补程序策略、OS 构建计划、服务器脚本和子文件夹）的访问权限。文件夹权限仅应用于紧邻该文件夹下的项。它们不应用于层次结构中位置更低的项，例如子文件夹的子文件夹。请参见设置文件夹权限。

文件夹权限类型

在 SA 客户端的“文件夹属性”窗口中，可以将下列权限分配给单个用户或用户组：

- **列出文件夹内容**：导航到层次结构中的文件夹，单击文件夹，查看文件夹的属性，查看文件夹内容的名称和类型（但不是内容的特性）。
- **在文件夹中读取对象**：查看文件夹内容的所有特性，在文件夹内容上打开对象浏览器，在操作中使用文件夹内容。

  例如，如果文件夹包含软件策略，则用户可以打开（查看）该策略，使用该策略修正服务器。但是，用户不能修改该策略。（对于修正，还需要操作权限和资源权限。）

  选择此权限会自动添加“列出文件夹内容”权限。
- **在文件夹中写入对象**：查看、使用、创建和修改文件夹内容。

  此权限允许“新建文件夹”和“新软件策略”之类的操作。要执行大多数操作，还需要操作权限。

  选择此权限会自动添加“列出文件夹内容”权限和“在文件夹中读取对象”权限。
- **在文件夹中执行对象**：运行文件夹中包含的脚本，查看文件夹内容的名称。

  此权限允许用户运行脚本，但不支持用户读取或写入脚本。要查看脚本内容，用户需要“在文件夹中读取对象”权限和相应的操作权限。要创建脚本，用户需要“在文件夹中写入对象”权限和相应的操作权限。

  选择“在文件夹中执行对象”权限会自动添加“列出文件夹内容”权限。
- **编辑文件夹权限**：修改权限或者将客户添加到文件夹。

  此权限使用户能够将文件夹（及其内容）的管理权限委托给另一个用户组。

  选择此权限会自动添加“列出文件夹内容”权限。

图 8 显示了名为 Win-patchers 的用户组，其中选择了“文件夹权限”视图。此用户组具有名为 /库/A-WinPatch 的文件夹的列出、读取、写入和执行权限。

图 8.用户组窗口中的文件夹权限视图

文件夹权限和操作权限

操作权限确定用户可使用 SA 客户端执行的操作。文件夹权限指定用户有权访问的 SA 库中的文件夹。

要对文件夹及其包含的项执行大多数操作，用户需要具有文件夹权限和操作权限。例如，要将软件策略添加到文件夹，用户所属的组必须具有特定文件夹的“在文件夹中写入对象”权限和“管理软件策略”操作权限（读取和写入）。

文件夹、客户约束和软件策略

如果向文件夹分配了客户，则该客户可约束对文件夹中包含的软件策略执行的某些操作。通过筛选来强制实施这些约束：可与软件策略关联的对象必须具有匹配的客户。

例如，假设您要将 `quota.rpm` 程序包添加到软件策略。该程序包和软件策略驻留在不同的文件夹中。策略文件夹的客户为 Widget，程序包文件夹的客户为 Acme。当您对策略执行“添加程序包”操作时，您可以选择的程序包将不包括 `quota.rpm`。策略文件夹的客户 (Widget) 充当筛选器来限制可添加到策略中的对象。如果您将 Widget 客户添加到 `quota.rpm` 的文件夹，则可以将 `quota.rpm` 添加到策略。

下表汇总了软件策略操作的客户约束。只有当软件策略的文件夹具有一个或多个客户时，才调用这些约束。此处未列出的软件策略操作（如“新建文件夹”）不具有客户约束。

- **附加软件策略**：附加的服务器的客户必须是软件策略文件夹的客户之一。
- **安装软件策略模板**：服务器的客户必须是模板中包含的每个软件策略文件夹的客户之一。

默认文件夹权限

当首次安装 SA 时，向预定义用户组分配了顶层文件夹（例如“程序包存储库”）的权限。当您创建新文件夹时，它具有与其父级同样的权限和客户。

多个用户组中的成员资格

如果用户属于多个用户组，则从所有组的资源权限和操作权限派生用户的权限。派生权限的方式取决于资源是否是文件夹。

如果资源不是文件夹，则派生的权限是用户所属的所有组的资源权限和操作权限的叉积。使用叉积，所有操作权限应用于所有资源权限。例如，Jane Doe 同时属于 Atlanta 和 Portland 组，它们具有**表 4** 所列的权限。由于派生的权限是叉积，Jane 可以在与 Widget Inc. 客户关联的托管服务器上执行系统诊断任务，即使 Atlanta 或 Portland 组都没有此功能。

表 4.叉积权限的示例

资源或操作	Atlanta 用户组权限	Portland 用户组权限
资源：	读取和写入	无

资源或操作	Atlanta 用户组权限	Portland 用户组权限
客户：Widget, Inc.		
资源： 客户：Acme Corp.	无	读取和写入
操作： 系统诊断	否	是

如果资源是虚拟化容器，则用户的派生权限是累积的，但不跨越用户组。例如，John Miller 属于**表 5** 中所示的 San Diego 和 Raleigh 组。如果 John 对虚拟化库存文件夹 A 中的服务器 X 具有写入权限，则 John 可以对其运行电源控制操作。如果 John 对虚拟化库存文件夹 B 中的服务器 Y 具有写入权限，则他可以修改虚拟机配置。但是，他不能对服务器 Y 运行电源控制，也不能修改服务器 X 的虚拟机配置。

表 5.虚拟化容器的权限示例

资源或操作	San Diego 用户组权限	Raleigh 用户组权限
资源：虚拟机监控程序容器 B	无	列出
资源：虚拟化库存文件夹 A	读取	无
资源：虚拟化库存文件夹	无	读取和写入
操作：虚拟机生命周期管理：电源控制	是	无
操作：虚拟机生命周期管理：修改虚拟机	无	是

如果资源是文件夹（或其内容），则用户的派生权限是累积的，但不跨越用户组。例如，Joe Smith 属于**表 6** 中所示的 Sunnyvale 和 Dallas 组。Joe 可以在 Webster 文件夹下创建程序包，这是因为 Sunnyvale 组具有该文件夹和“管理程序包”操作的“读取和写入”权限。但是，Joe 无法在 Kiley 文件夹下创建程序包，因为没有用户组可以这样做。Joe 可以在 Kiley 文件夹下（而不是在 Webster 文件夹下）创建 OS 序列。

表 6.累积权限的示例

资源或操作	Sunnyvale 用户组权限	Dallas 用户组权限
资源： Webster 文件夹	读取和写入	无
资源： Kiley 文件夹	无	读取和写入
操作： 管理程序包	读取和写入	无

资源或操作	Sunnyvale 用户组权限	Dallas 用户组权限
操作： 管理 OS 序列	无	读取和写入

SA 客户端中基于权限的受限视图

SA 客户端仅显示用户组具有“读取”或“读取和写入”权限的资源。

例如，John Smith 属于基本用户组，该组具有**表 7** 中所列的权限。当 John 登录时，SA 客户端仅显示 Widget Inc.（而不是 Acme Corp.）的服务器。

表 7.权限和受限视图的示例

资源或操作	基本组权限
客户：Widget, Inc.	读取和写入
客户：Acme Corp.	无
向导：准备 OS	是
向导：运行脚本	否

要查找或查看服务器，用户所属的用户组必须具有客户和设施以及至少一个与服务器关联的设备组的“读取”（或“读取和写入”）权限。否则，用户无法查看 SA 客户端中的服务器。

预定义用户组

在 SA 安装或升级期间，SA 根据用户角色创建一组预定义用户组。您必须授予设施和客户读取和/或写入的权限以及授予这些用户组其他适当的权限。预定义用户组的使用是可选的。SA 建议您复制并修改预定义用户组的权限，以创建您自己的自定义用户组，而不是修改默认组。您对预定义用户组的修改或删除操作不受 SA 升级影响。**表 8** 显示了预定义用户组：

表 8.预定义用户组

用户组名称	描述
Opsware System Administrators	具有管理 SA 应用程序所需的访问权限。
Superusers	具有对所有 SA 托管的对象和操作的完整访问权限。
Viewers	具有对所有资源的只读访问权限。

Reporters	仅具有对报告的访问权限。
OS Policy Setters	具有导入和定义 OS 构建计划所需的访问权限。
OS Deployers	具有配置服务器所需的访问权限。
Patch Policy Setters	具有设置修补策略所需的访问权限。
Patch Deployers	具有安装修补程序所需的权限。
Software Policy Setters	具有设置软件策略所需的访问权限。
Software Deployers	具有安装软件所需的权限。
Compliance Policy Setters	具有定义符合性策略所需的访问权限。
Compliance Auditors	具有执行符合性扫描所需的访问权限。
Compliance Enforcers	具有修补符合性失败所需的访问权限。
Virtualization Administrators	具有添加、编辑和删除虚拟化服务，管理虚拟机生命周期和虚拟机模板所需的访问权限以及虚拟化库存的管理权限。
Hypervisor Managers	（*如果核心已从 SA 9.1x* 升级）具有创建、删除和注册虚拟机所需的访问权限。 有关升级路径的详细信息，请参见《SA 10.0 Upgrade Overview guide》。
Virtual Machine Managers	具有启动和停止虚拟机所需的访问权限。
VM Lifecycle Managers	具有创建、修改、迁移、克隆和删除虚拟机以及虚拟机模板部署人员任务所需的访问权限。
VM Template Deployers	具有使用虚拟机模板创建虚拟机、克隆虚拟机、自定义虚拟机来宾 OS、启动和停止虚拟机所需的访问权限。
VM Template Managers	具有创建、修改和删除虚拟机模板以及虚拟机生命周期管理员任务所需的访问权限。
Command Line Administrators	具有对服务器的 Shell 访问权限。
Server Storage Managers	具有管理服务器存储所需的访问权限。
Storage System Managers	具有管理存储系统所需的访问权限。
Storage Fabric Managers	具有管理存储网络结构所需的访问权限。

关于专用用户组

备注: 专用用户组用于将脚本迁移到 SA 库中的文件夹中。您不应当使用专用用户组向用户分配权限。您应当使用常规用户组。有关详细信息，请参见关于 SA 用户和用户组。

当 SA 管理员创建新用户时，SA 自动为新用户创建专用用户组，并将新用户分配到该专用用户组。专用用户组的名称采用用户名。

专用用户组只能包含一个 SA 用户，每个 SA 用户只能属于一个专用用户组。SA 管理员然后可以将操作权限和资源权限分配到专用用户组。您为专用用户组指定的权限决定了用户可以使用 SA 执行的操作。操作权限指定用户可以执行的操作；资源权限指示用户可以在哪些服务器上执行这些操作。全局文件系统 (OGFS) 权限不能分配给专用用户组。

例如，当 SA 管理员创建用户名为 john 的新用户时，还会创建专用用户组 john，并在主目录中创建名为 john 的默认文件夹。SA 管理员然后可以将操作权限和资源权限分配到专用用户组 john。

SA 用户可以是多个用户组的成员，属于用户的专用组。但是，专用用户组的派生权限不是用户所属的所有组的资源权限和操作权限的叉积。

当删除用户时，SA 自动删除相应的专用用户组，该用户的默认文件夹移动到 SA 库中的 `/Home/deleted_users` 位置。

有关详细信息，请参见设置专用用户组权限。

关于超级管理员和超级用户

超级管理员是一个 SA 用户，他/她可以创建用户和用户组，指定用户组的角色，以及将用户分配到用户组。超级管理员还可以管理客户和设施以及设置文件夹权限。要执行本章所述的大多数任务，您必须以超级管理员的身份登录 SA 客户端。

SA 安装程序单一默认用户，即名为 `admin` 的超级管理员。`admin` 的密码是在安装期间指定的，稍后应立即更改。

提示: 作为最佳实践，您不应当将 `admin` 用户添加到其他用户组。

关于超级用户

超级用户与超级管理员不同，不会自动成为超级管理员。超级用户是属于预定义 Superusers 组的任何用户。超级用户具有执行所有操作（创建和修改用户和用户组除外）的完全权限。

不过，超级用户不自动拥有对任何服务器的访问权限。您需要按设置资源权限 - 设施、客户和设备组中所述，授予对设施、客户和设备组的访问权限。

要创建超级用户，请将现有用户添加到 Superusers 预定义用户组。有关详细信息，请参见预定义用户组和将用户添加到用户组。

关于客户管理员和客户组

组织服务器和提供访问控制边界的一种方法是按客户分隔托管服务器。客户代表一组与业务组织（如部门或公司）关联的服务器。由于服务器运行客户的应用程序，因此通常与客户关联。有关创建和管理客户的详细信息，请参见《SA 用户指南：Server Automation》。

将客户管理员与超级管理员比较

超级管理员可以将特定用户组的管理委托给客户管理员。像超级管理员一样，客户管理员可以将用户和权限分配到用户组。但是，客户管理员只能修改具有指定客户的访问权限的用户组。

客户管理员与超级管理员相同，但存在下列约束：

- 超级管理员可以在所有用户组中添加或删除用户，而客户管理员只能在某些用户组（这些用户组具有对客户组中所列特定客户的“读取和写入”访问权限）中添加或删除用户。
- 超级管理员可以在所有用户组中修改权限，而客户管理员只能在某些用户组（这些用户组具有对客户组中所列特定客户的“读取和写入”访问权限）中修改权限。
- 超级管理员可以创建新 SA 用户或删除 SA 用户，而客户管理员不能创建或删除用户。

客户管理员由客户组定义

您可以通过创建客户组来创建客户管理员。**客户组**包含一个或多个 SA 用户，以及一个或多个客户。客户组中的每个用户成为客户组中客户的客户管理员。客户管理员可管理的用户组是具有对客户组中所列客户的“读取和写入”访问权限的用户组。

示例客户组

下面的示例显示名为 Widget Co 的客户和名为 Sunnyvale Admins 的用户组。Sunnyvale Admins 用户组具有对客户 Widget Co 的“读取和写入”访问权限，这意味着 Sunnyvale Admin 用户负责管理分配给 Widget Co 客户的服务器。

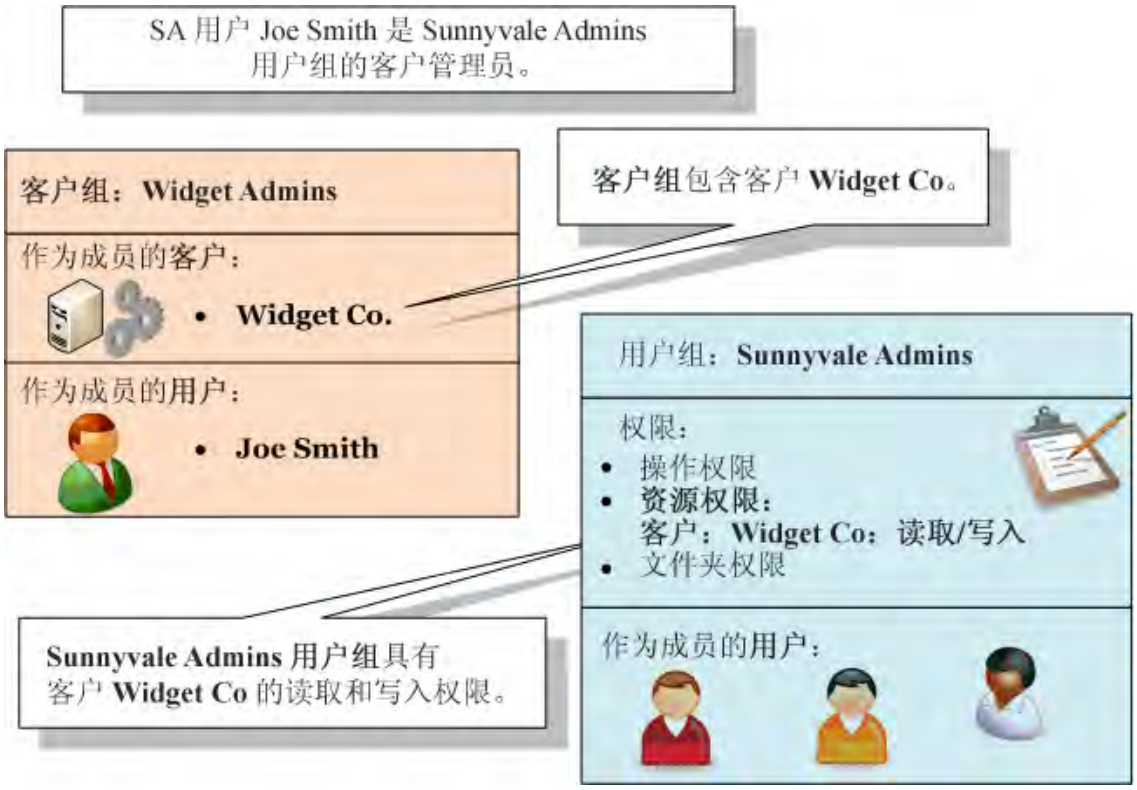
图 9 显示了如何使 SA 用户 Joe Smith 成为 Widget 客户的客户管理员。Widget Admins 客户组列出 Joe Smith 和客户 Widget Co，该客户将 Joe Smith 定义为 Widget 客户的客户管理员。Joe Smith 可以修改 Sunnyvale Admins 用户组，即可以在该用户组中添加和删除用户以及更改权限。

此图显示了 Joe Smith 管理 Sunnyvale Admins 用户组所需的关系：

- Sunnyvale Admins 用户组具有 Widget Co 客户的“读取和写入”权限。
- Widget Admins 客户组包含 Widget Co 客户。

- Widget Admins 客户组包含用户 Joe Smith。

图 9.定义客户管理员



有关详细信息，请参见管理客户管理员和客户组 - SA 客户端。

安全管理员进程概述

负责 SA 安全性的人员创建并维护用户和用户组，设置用户组的权限，并将用户分配到用户组。此人必须能够以超级管理员用户的身份登录 SA 客户端。有关详细信息，请参见关于超级管理员和超级用户。

以下步骤概述了 SA 的安全性管理：

1. 标识您的组织中将管理 SA 安全性的人员。
2. 为上面步骤中标识的每个用户创建一个超级管理员。

   有关说明，请参见创建超级管理员。
3. 注意托管服务器所属的设施。

   设施代表一个数据中心或物理位置。取决于您的组织，您可能需要按服务器驻留的城市、建筑或房间来命名设施。安装 SA 的人员指定核心的设施名称。

4. 将托管服务器与客户关联。

   在 SA 中，客户代表一组与业务组织（如部门或公司）关联的服务器。由于服务器运行客户的应用程序，因此通常与客户关联。

   有关按客户对服务器分组的详细信息，请参见《SA 用户指南：Server Automation》。

5. （可选）创建设备组，然后将服务器分配给设备组。设备组是对托管服务器进行组织的另一种方法。

   有关设备组的详细信息，请参见《SA 用户指南：Server Automation》。

6. 计划用户组。

   决定特定用户组将执行哪些 SA 任务，以及在哪些服务器上执行。用户组通常代表一个角色或一个作业类别。用户组的示例有：UNIX System Admins、Windows Admins、DBAs、Policy Setters、Patch Admins 等等。请参见预定义用户组。

7. 如果自定义用户组不符合您的需求，请创建您自己的用户组。

   有关说明，请参见创建新用户组。

8. 设置用户组的资源权限。

   这些权限指定对与设施、客户和设备组关联的服务器的读取和写入访问权限。资源权限控制用户组成员可以访问的服务器。有关详细信息，请参见设置资源权限 - 设施、客户和设备组。

9. 设置用户组的操作权限。

   要确定执行特定任务所需的操作权限，请参见权限参考中的表。例如，如果您有一个名为 Software Managers 的用户组，请参见表 45.用户操作所需的软件管理权限。有关详细信息，请参见设置操作权限。

10. 设置用户组的 OGFS 权限。

    某些操作（例如需要访问托管服务器文件系统的操作）需要 OGFS 权限。权限参考中的表中包括了 OGFS 权限。

    有关说明，请参见设置 OGFS 权限。

11. 在 SA 库中使用 SA 客户端创建文件夹层次结构。

    有关 SA 库的详细信息，请参见《SA 用户指南：Server Automation》。

12. 设置文件夹权限。

    通常，您需要文件夹的读取权限以在操作中使用其内容，需要写入权限以创建或修改文件夹内容，或者需要执行权限以运行该文件夹中驻留的脚本。有关详细信息，请参见设置文件夹权限。

13. （可选）将文件夹权限的管理委托给某些用户组。

    有关说明，请参见设置文件夹权限。

14. 在 SA 中创建新用户，或者从外部轻量目录访问协议 (LDAP) 目录导入现有用户。

有关说明，请参见创建新用户和使用外部 LDAP 目录服务进行身份验证。

15. 将用户分配到相应的组。

有关说明，请参见将用户添加到用户组。

关于全局文件系统权限

要使用 OGFS，您需要授予 OGFS 权限。OGFS 权限是单独的，但是与关于权限类型 - 操作权限、资源权限和文件夹权限中所述的操作权限、资源权限和文件夹权限相关（另请参见设置 OGFS 权限）。

OGFS 是一种虚拟文件系统，为您提供访问所有托管服务器及其所有文件系统的权限。它构成了许多 SA 客户端操作（例如浏览托管服务器文件系统和扫描服务器以检查符合性）的基础。要执行使用 OGFS 的操作，您必须属于具有 OGFS 权限的用户组。**表 9** 列出了您使用 OGFS 权限控制的操作。

表 9.OGFS 权限

OGFS 权限	此权限允许的任务
启动全局 Shell	启动全局 Shell。
登录到服务器	在 UNIX 服务器上打开 Shell 会话。在 SA 客户端中，打开远程终端。在全局 Shell 中，可以使用 `rosh` 命令。
读取 COM+ 数据库	以特定登录的身份读取 COM Plus 对象。在 SA 客户端中，使用设备资源管理器在 Windows 服务器上浏览这些对象。
读取服务器文件系统	以特定登录的身份读取托管服务器。在 SA 客户端中，使用设备资源管理器浏览托管服务器的文件系统。
读取 IIS 元数据库	以特定登录的身份读取 IIS 元数据库对象。在 SA 客户端中，使用设备资源管理器在 Windows 服务器上浏览这些对象。
读取服务器注册表	以特定登录的身份读取注册表文件。在 SA 客户端中，使用设备浏览器查看 Windows 注册表。
传递 RDP 会话到服务器	在 Windows 服务器上打开 RDP 会话。在 SA 客户端中，这是用于为 Windows 服务器打开 RDP 客户端窗口的远程终端菜单。
在服务器上运行命令	使用 `rosh` 实用程序在命令或脚本已存在的托管服务器上运行命令或脚本。在 SA 客户端中，这用于设备资源管理器所访问的 Windows 服务。

OGFS 权限	此权限允许的任务
写入服务器文件系统	以特定登录的形式修改托管服务器上的文件。在 SA 客户端中，可以使用设备浏览器修改托管服务器的文件系统。

当设置 OGFS 权限时，除了指定诸如“写入服务器文件系统”之类的操作，还可以指定操作可应用于的托管服务器。您可以通过选择设施、客户或设备组指定托管服务器。您还可以指定运行操作的托管服务器的登录名称。（“启动全局 Shell”操作是例外。）

例如，假设您指定“读取服务器文件系统”权限。对于服务器，您选择名为 Sunnyvale Servers 的设备组。对于登录名，您选择 SA 用户名。稍后，在 SA 客户端中，SA 用户 jdoe 在设备资源管理器中打开属于 Sunnyvale Servers 设备组的服务器。在“视图”窗格中，jdoe 字符串出现在“文件系统”标签旁的括号中。当用户向下钻取文件系统时，设备资源管理器显示 UNIX 用户 jdoe 有权访问的文件和目录。

如果您指定超级用户（如 root）作为登录名，请确保您选择的资源仅允许访问正确的服务器集。对于 root，您应当限制客户或设备组（但不限制设施）对服务器的访问。

对于“启动全局 Shell”权限，不要指定托管服务器，因为全局 Shell 会话不与特定服务器关联。另外，不要为此权限指定登录用户。如果您使用 SA 客户端打开全局 Shell 会话，则可以用当前 SA 登录身份执行该操作。如果使用 `ssh` 命令打开全局 Shell 会话，则系统提示您输入 SA 登录名（用户名）。

管理用户 - SA 客户端

本节描述如何使用 SA 客户端管理用户。要管理用户，您必须以超级管理员 (`admin`) 身份登录 SA 客户端，并选择“管理”选项卡，如**图 10** 所示。

图 10.“管理”选项卡下列出的用户

创建新用户

要从 SA 客户端创建新 SA 用户，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户”节点。
3. 选择“用户”节点。这会显示您的所有 SA 用户。
4. 选择“操作”>“新建”菜单或选择“新建用户”图标。这会显示“新建用户”窗口。
5. 输入用户的名字、姓氏和全名。
6. 要允许新用户管理用户和用户组，请选中标签为“超级管理员”的复选框。有关详细信息，请参见关于超级管理员和超级用户。
7. 输入新用户的联系信息。需要填写电子邮件地址。
8. 输入新用户的登录信息。
   - 用户凭据可以存储在 HP SA 中或与 SA 连接的 RSA SecurID 服务器上。只有当凭据存储为 HP SA 时，您才可以在 SA 客户端中更改用户密码。
   - SA 用户名必须由字母、数字、句点、连字符和下划线组成。SA 用户名不区分大小写。
   - 密码长度必须至少为六个 ASCII 字符，且不能包含“\”或“^”字符。
9. 输入区域设置、时区和日期格式首选项。
10. 选择“用户组”视图将用户分配到一个或多个用户组。将用户分配到用户组会向用户授予相应的权限。使用“+”按钮可将用户添加到用户组。使用“-”按钮可从选定用户组中删除用户。

11. 选择“文件”>“还原”以放弃更改。
12. 选择“文件”>“保存”以保存新用户。

更改用户权限

用户组包含所有权限。每个用户的权限由他们所属的用户组决定。要修改用户权限，您必须修改用户所属的用户组中定义的权限，或者更改用户所属的用户组。有关详细信息，请参见将用户分配到用户组和设置用户组的权限 - SA 客户端。

更改用户密码

只有超级管理员 (`admin`) 才能更改其他 SA 用户的密码。如果从外部 LDAP 目录导入用户名，则不能使用 SA 客户端更改密码。有关详细信息，请参见使用外部 LDAP 目录服务进行身份验证。

要更改用户的密码，您需要在用户窗口中打开用户并选择“属性”视图。请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户”节点。
3. 选择“用户”节点。这会显示您的所有 SA 用户。
4. 选择要修改的用户。
5. 选择“操作”菜单或右键单击，然后选择“打开”。这会在新窗口中显示用户信息。
6. 选择“属性”视图。这会显示用户的登录信息（包括“更改密码”链接）。
7. 选择“更改密码”链接。这会显示“更改密码”对话框。
8. 输入新密码。请注意，当您修改用户密码时，更改将立即生效。
9. 选择“确定”。这会修改用户的密码。

更改其自己的密码和其他属性的用户

任何用户都可以更改自己的密码及其配置文件信息。

图 11.更改自己的密码的用户

1. 从 SA 客户端屏幕，选择右上角中的“登录用户”链接，如上图中所示。这会显示用户属性窗口，如**图 12** 中所示。

图 12.用户属性窗口和更改密码链接

2. 要更改密码，请选择“更改密码”链接。请注意，当修改用户密码时，更改将立即生效。
3. 根据需要，更改其他属性。
4. 如果任何属性已更改，请选择“文件>“保存”。
5. 选择“文件”>“关闭”。

更改用户

要从 SA 客户端修改 SA 用户，请执行以下步骤。

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户”节点。
3. 选择“用户”节点。这会显示您的所有 SA 用户。
4. 选择要修改的用户。
5. 选择“操作”菜单或右键单击，然后选择“打开”。这会在新窗口中显示用户信息。
6. 可以选择修改任何用户属性。“属性”视图列出用户姓名、联系信息、登录信息、其凭据的存储位置、其用户名、用于更改其密码的链接，以及他们的日期和时间设置。请注意，当您修改用户密码时，更改将立即生效。
7. 可以选择在用户组中添加或删除用户。“用户组”视图列出用户所属的用户组。每个用户组将一组权限授予属于该组的所有用户。
8. 可以在用户窗口中看见这些权限，但是不能修改它们。要修改权限，您需要按照设置用户组的权限 - SA 客户端中所述修改用户组。
9. 选择“文件”>“还原”以放弃更改。
10. 选择“文件”>“保存”以保存更改。

删除用户

要从 SA 客户端删除 SA 用户，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户”节点。
3. 选择“用户”节点。这会显示您的所有 SA 用户。
4. 选择一个或多个要删除的用户。
5. 选择“操作”>“删除”菜单或选择删除图标。

查找特定操作权限所属的用户组

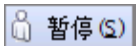
如果用户属于多个用户组，则您可以确定哪个用户组授予特定操作权限，如下所述。

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户”节点。
3. 选择“用户”节点。这会显示您的所有 SA 用户。
4. 选择要查看的用户。
5. 选择“操作”菜单或右键单击，然后选择“打开”。这会在新窗口中显示用户信息。
6. 选择“操作权限”视图。这会显示按用户所属的用户组进行组织的所有操作权限。
7. 您还可以右键单击任何列标题，取消“用户组”列的分组，然后使用列标题右上角的列选择器显示“用户组”列。这将显示每个权限，后跟授予该权限的用户组。

挂起用户

挂起的用户无法登录 SA，但是用户名尚未删除。挂起的用户由 SA 客户端中的“已挂起”状态指示。可以通过下列方法挂起用户：

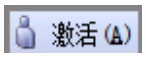
- **登录失败**：如果您在“安全设置”选项卡中选中标有“登录失败”的复选框，而某人尝试使用错误的密码登录达到指定的次数，则挂起用户帐户。有关访问“安全设置”选项卡的说明，请参见重置初始密码中的前两个步骤。
- **帐户不活动**：如果您在“安全设置”选项卡中选中标有“帐户不活动”的复选框，而用户在指定的天数内一直未登录，则挂起用户帐户。
- **过期的密码**：如果密码已过期且过期计数已满，则会挂起用户。
- **挂起**：您可以按如下所述挂起用户帐户。如果用户已登录，将显示一条消息，他们将注销。

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户”节点。
3. 选择“用户”节点。这会显示所有用户。
4. 选择要挂起的用户。
5. 选择 

按钮或选择“操作”>“挂起”。

激活挂起的用户

要激活挂起的用户，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户”节点。
3. 选择“用户”节点。这会显示所有用户。
4. 选择要激活的已挂起用户。
5. 选择 

按钮或选择“操作”>“激活”。

将用户分配到用户组

通过在您的组织中反映用户角色，将每个 SA 用户分配到组。要将 SA 用户分配到用户组，请执行以下步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户”节点。
3. 选择“用户”节点。这会显示您的所有 SA 用户。
4. 选择要分配的用户。
5. 选择“操作”菜单或右键单击，然后选择“打开”。这会在新屏幕中显示用户信息。
6. 选择“用户组”视图。这会显示用户作为成员的用户组。
7. 选择“+”按钮，或选择“操作”>“添加”菜单。这会显示所有用户组。
8. 选择一个或多个用户组。
9. 选择“选择”按钮。这会将该用户添加到这些用户组。

10. 选择“文件”>“还原”以放弃更改。
11. 选择“文件”>“保存”。

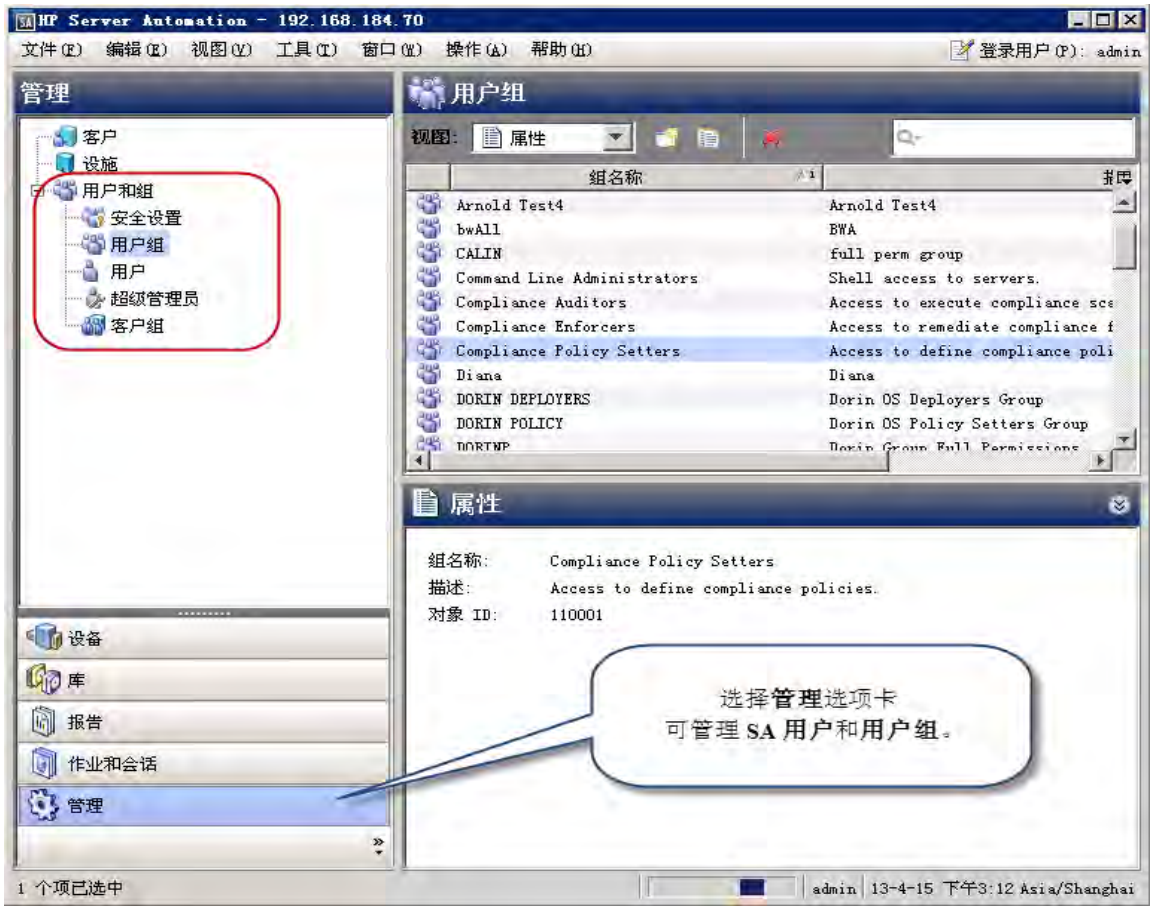
从 LDAP 目录导入用户

您可以从 LDAP 目录导入用户信息，并在登录 SA 时使用 LDAP 目录进行身份验证。有关详细信息，请参见使用外部 LDAP 目录服务进行身份验证。

管理用户组 - SA 客户端

本节描述如何使用用户组执行任务。要管理用户组，您必须以超级管理员 (admin) 身份登录 SA 客户端，并选择“管理”选项卡，如图 13 所示。

图 13. “管理”选项卡下列出的用户组



创建新用户组

要从 SA 客户端创建新用户组，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户组”节点。
3. 选择“用户组”节点。这会显示所有用户组。
4. 选择“操作”菜单或右键单击，然后选择“新建”菜单。这会显示“新建用户组”窗口。
5. 选择“属性”视图。输入用户组的名称和描述。
6. 选择“文件”>“保存”以保存新用户组。
7. 按照设置用户组的权限 - SA 客户端所述，设置用户组的权限，并将用户添加到用户组。
8. 选择“文件”>“还原”以放弃更改。
9. 选择“文件”>“保存”以保存更改。

查看用户组

要从 SA 客户端查看用户组，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户组”节点。
3. 选择“用户组”节点。这会显示所有用户组。
4. 选择用户组可显示有关该用户组的信息。
5. 在“视图”下拉列表中选择下列任何选项：
   - **属性**显示选定用户组的名称、描述和 SA 对象 ID。
   - **用户**显示作为选定用户组成员的所有 SA 用户。
   - **资源权限**显示用户组成员有权访问的客户、设施和设备组。它还列出对每个客户、设施和设备组的访问权限类型：“读取”访问权限或者“读取和写入”访问权限。
   - **文件夹权限**显示授予组成员的对 SA 库中文件夹的访问权限。
   - **操作权限**显示用户组成员可使用 SA 客户端执行的操作。
   - **OGFS 权限**显示用户组成员可执行的全局 Shell 和全局文件系统操作、他们有权访问的资源、全局文件系统以及他们用来登录托管服务器以执行这些操作的用户名。

复制用户组

您可以按如下所述复制现有用户组。

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户组”节点。
3. 选择“用户组”节点。这会显示所有用户组。
4. 选择要复制的用户组。
5. 选择复制图标，或者选择“操作”>“复制”菜单，或者右键单击用户组，然后选择“复制”菜单。这会显示“复制用户组”屏幕。
6. 输入新用户组的名称和描述。名称必须唯一。
7. 选择“复制”按钮。这会创建一个作为现有用户组副本的新用户组。

更改用户组

用户组定义资源、文件夹、操作和 OGFS 权限。每个作为用户组成员的用户都具有这些权限。要从 SA 客户端修改用户组，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户组”节点。
3. 选择“用户组”节点。这会显示所有用户组。
4. 选择一个用户组。这会在屏幕下半部分显示有关该用户组的信息。
5. 选择“操作”菜单或右键单击，然后选择“打开”菜单。这会在新窗口中显示用户组。
6. 在导航窗格中选择下列任何视图：
   - **属性**显示选定用户组的名称、描述和 SA 对象 ID。您可以更改用户组的名称和描述。
   - **用户**显示作为选定用户组成员的所有 SA 用户。使用“+”和“-”按钮可在用户组中添加和删除用户。有关详细信息，请参见将用户添加到用户组。
   - **资源权限**显示用户组成员有权访问的设施、客户和设备组。它还列出授予的对每个设施、客户和设备组的访问权限类型：“读取”访问权限或“读取和写入”访问权限。使用“+”和“-”按钮可在用户组中添加和删除设施、客户和设备组以及设置访问权限类型。有关详细信息，请参见设置资源权限 - 设施、客户和设备组。
   - **文件夹权限**显示 SA 库中的文件夹以及授予的对用户组中每个文件夹的访问权限。选择文件夹，然后选择“操作”菜单，或者右键单击并选择“文件夹属性”菜单以显示文件夹属性窗口。选择“权限”选项卡以查看和修改权限。有关详细信息，请参见设置文件夹权限。
   - **操作权限**显示用户组成员可执行的任务。选择要更改的权限旁的“权限”列，然后选择新权限。有关详细信息，请参见设置操作权限。
   - **OGFS 权限**显示 OGFS 和全局 Shell (OGSH) 权限。选择“+”和“-”图标可添加和删除权限。有关详细信息，请参见设置 OGFS 权限。
7. 选择“文件”>“还原”以放弃更改。
8. 选择“文件”>“保存”。

删除用户组

您可以按如下所述删除一个或多个现有用户组。

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户组”节点。
3. 选择“用户组”节点。这会显示所有用户组。
4. 选择要删除的一个或多个用户组。
5. 选择删除图标，或者选择“操作”>“删除”菜单，或者右键单击用户组，然后选择“删除”菜单，或者按键盘上的 Delete 键。

将用户添加到用户组

您可以按如下所述，将一个或多个用户添加到任何用户组。

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户组”节点。
3. 选择“用户组”节点。这会显示所有用户组。
4. 选择一个用户组。这会在屏幕下半部分显示有关该用户组的信息。
5. 选择“操作”菜单或右键单击，然后选择“打开”菜单。这会在新屏幕中显示用户组。
6. 在导航窗格中选择“用户”视图。这会显示作为组成员的所有用户。
7. 选择“+”图标，或选择“操作”>“添加”菜单。这会显示所有 SA 用户。
8. 选择一个或多个用户。
9. 选择“选择”按钮。这会向用户组添加这些用户。
10. 选择“文件”>“还原”以放弃更改。
11. 选择“文件”>“保存”。

设置用户组的权限 - SA 客户端

本节描述如何设置用户组的“操作权限”、“资源权限”、“文件夹权限”和“OGFS 权限”。所有这些权限都授予作为用户组成员的用户。

设置资源权限 - 设施、客户和设备组

所有托管服务器按客户、设施和设备组分组。“资源权限”视图列出用户组有权访问的“客户”、“设施”和“设备组”。有关详细信息，请参见关于资源权限。

要修改用户组的资源权限，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户组”节点。
3. 选择“用户组”节点。这会显示所有用户组。
4. 选择一个用户组。这会在屏幕下半部分显示有关该用户组的信息。
5. 选择“操作”菜单或右键单击，然后选择“打开”菜单。这会在新屏幕中显示用户组。
6. 在导航窗格中选择“资源权限”视图。这会显示用户组有权访问的所有设施、客户和设备组。
7. 要添加对客户的访问权限，请执行下列步骤：
    1. 选择“客户”标题下的“+”图标。这会在单独的窗口中显示所有客户的列表。
    2. 选择一个或多个客户。
    3. 选择“读取”或“读取和写入”访问权限。
    4. 选择“添加”按钮。
8. 要删除对客户的访问权限，请选择客户，然后选择“-”按钮。

9. 要添加对设施的访问权限，请执行下列步骤：
    1. 选择“设施”标题下的“+”图标。这会在单独的窗口中显示所有设施的列表。
    2. 选择一个或多个设施。
    3. 选择“读取”或“读取和写入”访问权限。
    4. 选择“添加”按钮。
10. 要删除对设施的访问权限，请选择设施，然后选择“-”按钮。
11. 要添加对所有设备组的访问权限，请选中标为“允许访问所有设备组”的复选框。
12. 要添加对设备组子集的访问权限，请执行下列步骤：
    1. 清除标为“允许访问所有设备组”的复选框。这会显示“+”图标。
    2. 选择“设备组”标题下的“+”图标。这会在单独的窗口中显示所有公用设备组的列表。
    3. 选择一个或多个设备组。
    4. 选择“读取”或“读取和写入”访问权限。
    5. 选择“添加”按钮。
13. 要删除对设备组的访问权限，请选择设备组，然后选择“-”按钮。
14. 选择“文件”>“还原”以放弃更改。
15. 选择“文件”>“保存”。

设置操作权限

本节描述如何设置用户组的操作权限。有关详细信息，请参见关于操作权限。

要修改用户组的操作权限，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户组”节点。
3. 选择“用户组”节点。这会显示所有用户组。
4. 选择一个用户组。这会在屏幕下半部分显示有关该用户组的信息。
5. 选择“操作”菜单或右键单击，然后选择“打开”菜单。这会在新屏幕中显示用户组。
6. 在导航窗格中选择“操作权限”视图。
7. 使用“名称”和“描述”列找到要修改的权限。您可以右键单击任何列，按该列分组或取消分组，以便于浏览。
8. 在“权限”列中选择权限的当前值。这会显示可用值的下拉列表。选择所需的值。

提示： 可以同时选择和设置多个权限。通过拖动鼠标，或者使用键盘上的 Shift 和 Control 键及鼠标，选择多个权限。右键单击以显示可用权限值，然后选择所需的值。如果权限值灰显，则该权限由其他权限控制，必须首先更改相关权限。例如，需要先将“访问应用程序部署”权限设置为“是”，然后才能设置“创建应用程序”和“管理应用程序部署”这两个权限。

9. 选择“文件”>“还原”以放弃更改。
10. 选择“文件”>“保存”。

设置文件夹权限

本节描述如何设置用户组的文件夹权限。有关详细信息，请参见关于文件夹权限。

要修改用户组的文件夹权限，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户组”节点。
3. 选择“用户组”节点。这会显示所有用户组。
4. 选择一个用户组。这会在屏幕下半部分显示有关该用户组的信息。
5. 选择“操作”菜单或右键单击，然后选择“打开”菜单。这会在新屏幕中显示用户组。
6. 在导航窗格中选择“文件夹权限”视图。这会显示 SA 库中的所有文件夹及其当前权限。
7. 找到并选择要修改的文件夹。
8. 选择“操作”菜单或右键单击，然后选择“文件夹属性”菜单。这会在新窗口中显示文件夹属性。
9. 选择“权限”选项卡。这会显示有权访问文件夹的所有用户和用户组。
10. 选择用户或用户组。这会在窗口底部显示当前访问权限。
11. 在窗口底部设置访问权限。
12. （可选）要将访问权限授予其他用户或用户组，请选择“添加”按钮，选择一个或多个用户或用户组，然后选择“添加”按钮。
13. （可选）要删除用户或用户组的访问权限，请选择用户或用户组，然后选择“删除”按钮。
14. 选择“确定”按钮。
15. 选择“文件”>“还原”以放弃更改。
16. 选择“文件”>“保存”。

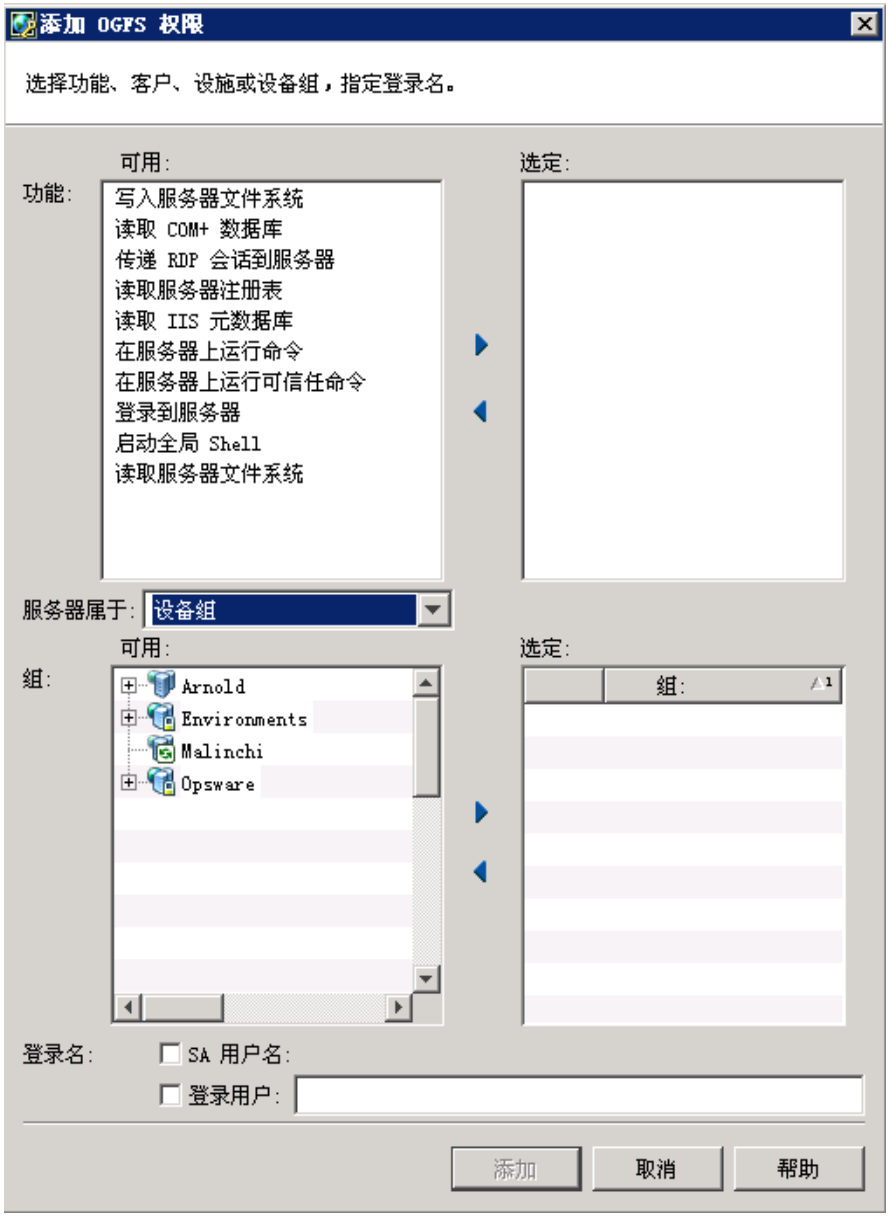
设置 OGFS 权限

本节描述如何设置用户组的 OGFS 权限。有关详细信息，请参见关于全局文件系统权限。

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户组”节点。
3. 选择“用户组”节点。这会显示所有用户组。
4. 选择一个用户组。这会在屏幕下半部分显示有关该用户组的信息。
5. 选择“操作”菜单或右键单击，然后选择“打开”菜单。这会在新窗口中显示用户组。
6. 在导航窗格中选择 OGFS 权限。这会显示当前 OGFS 权限。
7. 要添加权限，请选择“+”图标。这会显示“添加 OGFS 权限”窗口，如**图 14** 中所示。此屏幕有三个主要部分：

- “功能”部分列出使用 OGFS 和 OGSH 执行任务的操作权限。
- “组”部分列出可以对其执行操作的服务器。服务器按设施、客户或设备组分组。
- “登录”部分指定使用 OGFS 和 OGSH 连接服务器时要使用的登录名。

图 14.“添加 OGFS 权限”窗口



8. 在“功能”部分中的“可用”列表下，选择要授权的 OGFS 操作。选择箭头将这些操作移动到“选定”列表中。
9. 在“组”选择中，首先从“服务器属于”下拉列表中选择要选择的服务器组的类型。选择“客户”、“设施”或“设备组”。

10. 选择一个或多个客户、设施或设备组。选择箭头将它们移动到“选定”列表中。
11. 如果您希望 OGFS 用户使用他们的 SA 用户名登录，请在“登录”部分中，选中标有 SA 用户名的复选框。否则，选中标有“登录用户”的复选框，输入一个或多个使用 OGFS 登录服务器的用户名。
12. 选择“添加”按钮。
13. 要删除权限，请选择一个或多个权限，然后选择“-”按钮。
14. 选择“文件”>“还原”以放弃更改。
15. 选择“文件”>“保存”以保存更改。

有关 OGFS 权限的详细信息，请参见关于全局文件系统权限。

设置专用用户组权限

备注: 专用用户组用于将脚本迁移到 SA 库中的文件夹中。您不应当使用专用用户组向用户分配权限。您应当使用常规用户组。有关详细信息，请参见关于 SA 用户和用户组。

有关专用用户组的信息，请参见关于专用用户组。要修改专用用户组，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户”节点。
3. 选择“用户”节点。这会显示您的所有 SA 用户。
4. 选择您要设置其专用用户组权限的用户。
5. 选择“操作”菜单或右键单击，然后选择“打开”。这会在新窗口中显示用户信息。
6. 选择“用户组”视图。这会显示该用户作为成员的所有用户组，包括专用用户组。专用用户组与该用户同名。
7. 选择专用用户组。
8. 选择“操作”菜单或右键单击，然后选择“打开”。这会在新窗口中显示该专用用户组。
9. 要修改资源权限，请选择“资源权限”视图。有关详细信息，请参见设置资源权限 - 设施、客户和设备组。
10. 要修改操作权限，请选择“操作权限”视图。有关详细信息，请参见设置操作权限。
11. 选择“文件”>“还原”以放弃更改。
12. 选择“文件”>“保存”以保存更改。

设置密码、帐户和会话安全策略 - SA 客户端

您可以设置一些策略以保证 SA 用户密码安全，自动禁用不活动的用户帐户，以及自动锁定不活动的用户会话。请执行以下步骤：

1. 在 SA 客户端中，选择“管理”选项卡。
2. 在导航窗格中，打开“用户和组”节点。这会显示“安全设置”节点。
3. 选择“安全设置”节点。这会显示密码策略设置。
4. 设置任意下列策略：
   - **重置**强制每个用户在第一次登录 SA 时重置其密码。
   - **过期**强制每个用户在经过指定的天数后更改其密码。您还可以通过指定“允许宽限登录”次数，指定在要求更改之前用户可推迟更改的次数。
   - **保留**指定要保存多少个以前的密码。此设置阻止用户重用密码。例如，如果您指定 10，则用户不能重用他们以前的十个密码。
   - **登录失败**指定用户帐户挂起之前某人使用错误密码可尝试登录的次数。如果用户帐户处于挂起状态，您可以通过以下方法重新激活它：选择“管理”>“用户和组”，选择用户，然后选择“激活”按钮。有关详细信息，请参见挂起用户。
   - **帐户不活动**指定用户帐户挂起之前可处于未使用状态的时间。当用户帐户处于未使用状态达到指定的天数时，将挂起用户帐户。如果用户帐户处于挂起状态，您可以通过以下方法重新激活它：选择“管理”>“用户和组”，选择用户，然后选择“激活”按钮。有关详细信息，请参见挂起用户。
   - **SA 客户端会话不活动**指定 SA 客户端处于锁定之前用户会话可空闲的时间。以分钟为单位指定值。
5. 要还原到以前保存的设置，请选择“视图”>“刷新”菜单，或者按键盘上的 F5 键。
6. 设置所需的值后，选择“保存”按钮。

重置初始密码

如果要求用户在第一次登录 SA 时重置他们的密码，请执行下列步骤：

1. 在 SA 客户端中，选择“管理”选项卡。
2. 在导航窗格中，打开“用户和组”节点。这会显示“安全设置”节点。
3. 选择“安全设置”节点。这会显示密码策略设置。
4. 设置标有“在第一次登录时重置密码”的复选框。
5. 选择“保存”按钮。

设置密码过期

如要要求 SA 用户在经过特定天数后更改密码，请执行下列步骤：

1. 在 SA 客户端中，选择“管理”选项卡。
2. 在导航窗格中，打开“用户和组”节点。这会显示“安全设置”节点。
3. 选择“安全设置”节点。这会显示密码策略设置。
4. 选中标有“过期”的复选框。
5. 输入密码过期之前的天数。
6. 输入挂起用户之前允许使用旧密码的宽限登录次数。
7. 选择“保存”按钮。

要激活挂起的用户，请参见激活挂起的用户。

禁止重用旧密码

要保存用户旧密码的副本并阻止他们重用旧密码，请执行下列步骤。

1. 在 SA 客户端中，选择“管理”选项卡。
2. 在导航窗格中，打开“用户和组”节点。这会显示“安全设置”节点。
3. 选择“安全设置”节点。这会显示密码策略设置。
4. 设置标有“保留”的复选框。
5. 输入要保存并禁止的旧密码数量。
6. 选择“保存”按钮。

登录失败后挂起用户帐户

如果某人尝试使用错误密码登录已达到特定的次数，您可以挂起用户帐户，如下所示。

1. 在 SA 客户端中，选择“管理”选项卡。
2. 在导航窗格中，打开“用户和组”节点。这会显示“安全设置”节点。
3. 选择“安全设置”节点。这会显示密码策略设置。
4. 设置标有“登录失败”的复选框。
5. 输入失败登录尝试次数。如果某人尝试登录任何帐户，经过指定次数的尝试后仍失败，则将挂起用户帐户。
6. 选择“保存”按钮。

要激活挂起的用户，请参见激活挂起的用户。

挂起不活动的用户帐户

如果用户在一段特定时间后未登录，您可以自动挂起用户帐户。

1. 在 SA 客户端中，选择“管理”选项卡。
2. 在导航窗格中，打开“用户和组”节点。这会显示“安全设置”节点。
3. 选择“安全设置”节点。这会显示密码策略设置。
4. 设置标有“帐户不活动”的复选框。
5. 输入天数。当任何用户未登录达到指定的天数时，将挂起用户帐户。
6. 选择“保存”按钮。

要激活挂起的用户，请参见激活挂起的用户。

锁定不活动的会话

在用户处于不活动状态达到一段特定时间后，您可以自动锁定任何 SA 客户端会话。用户必须输入其密码才能解锁会话。

1. 在 SA 客户端中，选择“管理”选项卡。
2. 在导航窗格中，打开“用户和组”节点。这会显示“安全设置”节点。
3. 选择“安全设置”节点。这会显示密码策略设置。

4. 设置标有“SA 客户端会话不活动”的复选框。
5. 输入分钟数。如果任何登录的用户使用 SA 客户端达到指定的分钟数，则 SA 客户端将被锁定，用户将必须输入其密码。
6. 选择“保存”按钮。

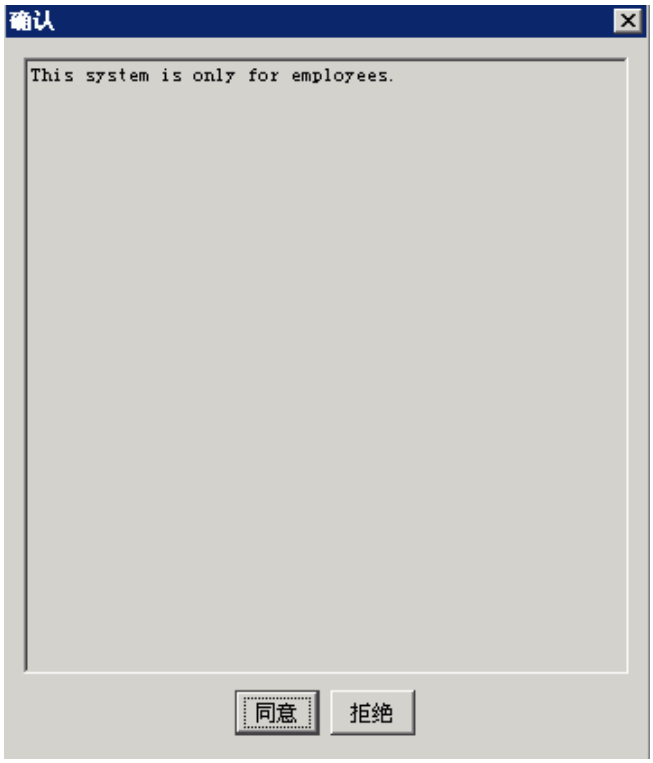
显示用户登录协议

您可以在用户登录时显示一条消息，并要求用户确认该消息。请执行下列步骤：

1. 在 SA 客户端中，选择“管理”选项卡。
2. 在导航窗格中，打开“用户和组”节点。这会显示“安全设置”节点。
3. 选择“安全设置”节点。这会显示用户协议设置和标题设置。
4. 在“用户协议设置”下，选择“启用显示”。
5. 输入要在用户协议中显示的文本。
6. 选择“保存”按钮。

当任何用户登录 SA 客户端时，将显示指定的消息，用户必须确认该消息，如**图 15** 所示。

图 15.用户登录确认对话框

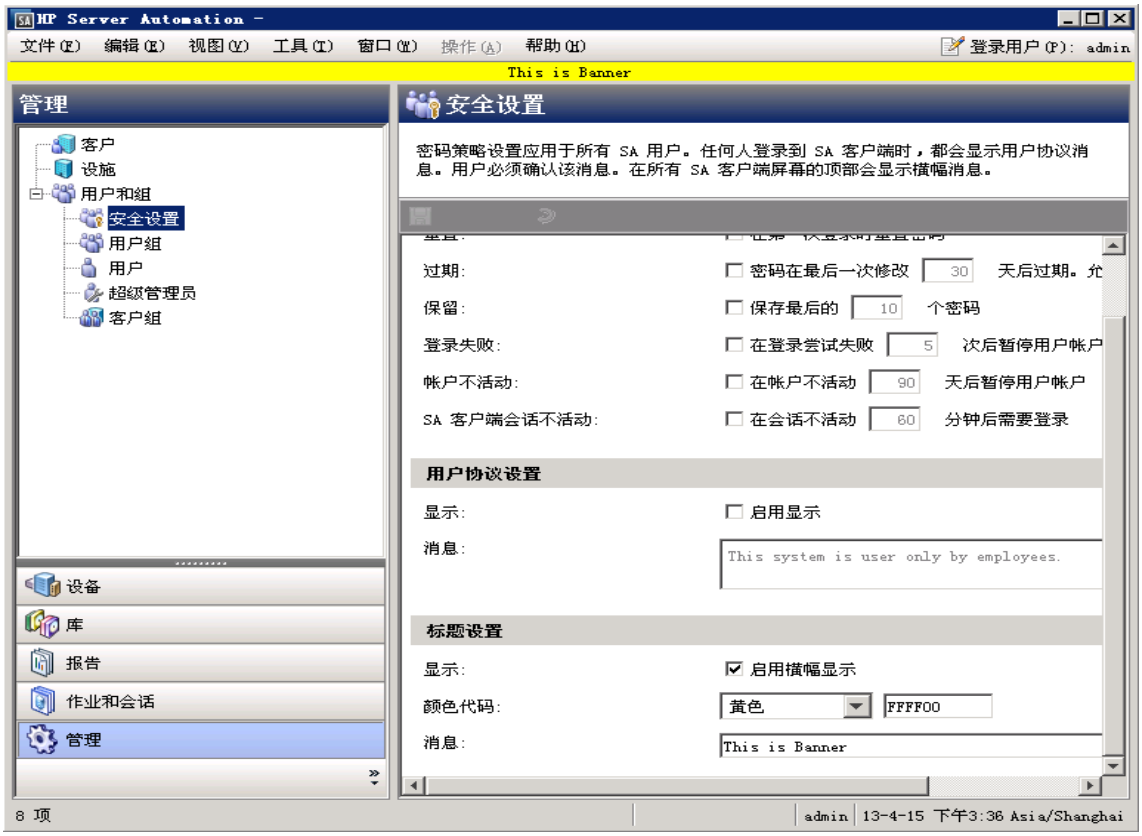


在 SA 客户端屏幕上显示标题

您可以在每个 SA 客户端屏幕顶部以任意背景色显示消息。请执行下列步骤：

1. 在 SA 客户端中，选择“管理”选项卡。
2. 在导航窗格中，打开“用户和组”节点。这会显示“安全设置”节点。
3. 选择“安全设置”节点。这会显示用户协议设置和标题设置。
4. 在“标题设置”下，选择“启用横幅显示”。
5. 从下拉列表中选择一种颜色，或者指定一个 000000 到 FFFFFF 之间的十六进制颜色代码。第一个 2 位数是红色成分，第二个 2 位数是绿色成分，最后一个 2 位数是蓝色成分。
6. 输入要在标题中显示的文本。
7. 选择“保存”按钮。这会在所有 SA 客户端屏幕顶部显示标题，如**图 16** 所示。

图 16.SA 客户端标题设置



管理超级管理员 - SA 客户端

“超级管理员”可以将权限分配给用户组，以及将用户分配到用户组。要管理超级管理员，您必须以超级管理员身份登录 SA 客户端。当首次安装 SA 时，默认超级管理员是 `admin` 用户。另请参见关于超级管理员和超级用户。

查看所有 SA 超级管理员

要查看所有 SA 超级管理员，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“超级管理员”节点。
3. 选择“超级管理员”节点。这会显示所有超级管理员。

创建超级管理员

SA 超级管理员是可以创建和修改 SA 用户和用户组的 SA 用户。要创建 SA 超级管理员，请按照创建新用户所述的步骤操作，并选中标有“超级管理员”的框。

要使现有用户成为超级管理员，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“超级管理员”节点。
3. 选择“超级管理员”节点。这会显示所有超级管理员。
4. 选择“操作”>“添加”菜单或选择“新建用户”图标。这会显示所有 SA 用户的列表。
5. 选择一个或多个您希望其成为超级管理员的用户。
6. 单击“选择”按钮。这会将选定用户更改为超级管理员。

删除超级管理员

要从 SA 用户删除超级管理员权限，并保留该用户的其他权限，请按更改用户中所述的步骤操作，并清除标有“超级管理员”的复选框。或者，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“超级管理员”节点。
3. 选择“超级管理员”节点。这会显示所有超级管理员。
4. 选择一个或多个用户。
5. 选择“操作”>“删除”菜单，或者右键单击并选择“删除”，或者选择删除按钮。

管理客户管理员和客户组 - SA 客户端

组织服务器和提供访问控制边界的一种方法是按客户组织托管服务器。客户代表一组与业务组织（如部门或公司）关联的服务器。由于服务器运行客户的应用程序，因此通常与客户关联。有关创建和管理客户的详细信息，请参见《SA 用户指南：Server Automation》。

您可以将超级管理员任务委托给客户管理员。**客户管理员**管理对分配给客户的服务器进行管理的用户。客户管理员是仅对某些用户组具有访问权限的超级管理员。

您可以通过创建客户组并将客户和用户分配到客户组，来创建客户管理员。有关详细信息，请参见关于客户管理员和客户组。

查看所有客户管理员

客户管理员是客户组中列出的用户。要查看所有 SA 客户管理员，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“超级管理员”节点。
3. 选择“超级管理员”节点。这会显示所有超级管理员和客户管理员。您可以通过如下显示的图标区分两种管理员：

 客户管理员图标

 超级管理员图标

查看客户组的所有客户管理员

客户管理员是客户组中列出的用户。要查看客户组的所有 SA 客户管理员，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中的“用户和组”节点下，选择“客户组”节点。这会显示所有客户组。
3. 选择一个客户组。
4. 选择“用户”视图。这会显示作为客户组成员的所有用户。这些用户是客户组中所列客户的客户管理员。

查看客户组的所有客户

客户管理员是客户组中列出的用户。要查看客户组中的所有客户，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中的“用户和组”节点下，选择“客户组”节点。这会显示所有客户组。
3. 选择一个客户组。
4. 选择“客户”视图。这会显示作为客户组成员的所有客户。

创建客户组

客户组将一个或多个用户与一个或多个客户相关联，使这些用户成为客户管理员。SA 客户管理员是可以对具有该客户的访问权限的所有用户组进行修改的 SA 用户。要创建 SA 客户管理员，必须创建客户组。请执行下列步骤：

1. 以超级管理员的身份（例如 admin）登录 SA 客户端。
2. 在导航窗格中选择“管理”选项卡。
3. 在导航窗格中的“用户和组”节点下，选择“客户组”节点。这会显示所有现有客户组。
4. 选择“操作”>“添加”菜单或选择“创建新项目”图标。

5. 输入客户组的名称和描述。
6. 选择“客户”视图。
7. 选择“+”图标，或选择“操作”>“添加”菜单。这会显示所有客户。
8. 选择一个或多个客户，然后按“选择”。
9. 选择“用户”视图。
10. 选择“+”图标，或选择“操作”>“添加”菜单。这会显示您的所有 SA 用户。
11. 选择一个或多个要添加到客户组的用户，然后按“选择”。
12. 选择“文件”>“保存”。
13. 选择“文件”>“关闭”。

删除客户组

客户组将一个或多个用户与一个或多个客户相关联，使这些用户成为客户管理员。SA 客户管理员是可以修改特定用户组的 SA 用户。要删除客户组，请执行下列步骤：

1. 以超级管理员的身份（例如 admin）登录 SA 客户端。
2. 在导航窗格中选择“管理”选项卡。
3. 在导航窗格中的“用户和组”节点下，选择“客户组”节点。这会显示所有现有客户组。
4. 选择要删除的客户组。
5. 选择“X”图标，或者选择“操作”>“删除”菜单，或者右键单击并选择“删除”，或者按键盘上的 Delete 键。此操作将删除所选的客户组。

从客户组视图创建客户管理员

SA 客户管理员是可以修改特定用户组的 SA 用户。要创建 SA 客户管理员，请将 SA 用户添加到客户组。请执行下列步骤：

1. 以超级管理员的身份（例如 admin）登录 SA 客户端。
2. 在导航窗格中选择“管理”选项卡。
3. 在导航窗格中的“用户和组”节点下，选择“客户组”节点。这会显示所有现有客户组。
4. 选择一个客户组。另请参见创建客户组。
5. 选择“操作”>“打开”菜单，或者右键单击并选择“打开”。这会在单独的窗口中打开客户组。
6. 选择“用户”视图。这会显示作为客户组成员的所有 SA 用户。
7. 选择“+”图标，或选择“操作”>“添加”菜单。这会显示您的所有 SA 用户。另请参见创建新用户。
8. 选择一个或多个要使其成为客户管理员的用户，然后按“选择”。
9. 选择“文件”>“保存”。
10. 选择“文件”>“关闭”。

这将允许新客户管理员修改具有客户的资源权限的用户组。

从用户视图创建客户管理员

SA 客户管理员是可以修改特定用户组的 SA 用户。要创建 SA 客户管理员，请将 SA 用户添加到客户组。请执行下列步骤：

1. 以超级管理员的身份（例如 admin）登录 SA 客户端。
2. 在导航窗格中选择“管理”选项卡。
3. 在导航窗格中的“用户和组”节点下，选择“用户”节点。这会显示所有现有 SA 用户。
4. 选择一个用户（另请参见创建新用户）。
5. 选择“操作”>“打开”菜单，或者右键单击并选择“打开”。这会在单独的窗口中打开用户。
6. 选择“客户组”视图。这会显示该用户所属的所有客户组。
7. 选择“+”图标，或选择“操作”>“添加”菜单。这会显示所有客户组（另请参见创建客户组）。
8. 选择一个或多个客户组，然后按“选择”。
9. 选择“文件”>“保存”。
10. 选择“文件”>“关闭”。

这将允许新客户管理员修改具有客户的资源权限的用户组。

从客户组视图删除客户管理员

SA 客户管理员是可以修改特定用户组的 SA 用户。要删除 SA 客户管理员，请从用户所属的客户组删除该 SA 用户。请执行下列步骤：

1. 以超级管理员的身份（例如 admin）登录 SA 客户端。
2. 在导航窗格中选择“管理”选项卡。
3. 在导航窗格中的“用户和组”节点下，选择“客户组”节点。这会显示所有现有客户组。
4. 选择一个客户组。
5. 选择“操作”>“打开”菜单，或者右键单击并选择“打开”。这会在单独的窗口中打开客户组。
6. 选择“用户”视图。这会显示作为客户组成员的所有 SA 用户。
7. 选择一个或多个要从客户组删除的用户，然后选择“－”图标，或者选择“操作”>“删除”菜单，或者右键单击并选择“删除”，或者按键盘上的 Delete 键。这将从客户组删除选定的 SA 用户，以使他们不再成为客户管理员。不过，这些用户仍是有效的 SA 用户。
8. 选择“文件”>“保存”。
9. 选择“文件”>“关闭”。

从用户视图删除客户管理员

SA 客户管理员是可以修改特定用户组的 SA 用户。要删除 SA 客户管理员，请从用户所属的客户组删除该 SA 用户。请执行下列步骤：

1. 以超级管理员的身份（例如 admin）登录 SA 客户端。
2. 在导航窗格中选择“管理”选项卡。
3. 在导航窗格中的“用户和组”节点下，选择“用户”节点。这会显示所有现有 SA 用户。
4. 选择一个用户。
5. 选择“操作”>“打开”菜单，或者右键单击并选择“打开”。这会在单独的窗口中打开用户。
6. 选择“客户组”视图。这会显示该用户所属的所有客户组。
7. 选择一个或多个要从中删除用户的客户组，然后选择“－”图标，或者选择“操作”>“删除”菜单，或者右键单击并选择“删除”，或者按键盘上的 Delete 键。这会从选定客户组中删除该用户。
8. 选择“文件”>“保存”。
9. 选择“文件”>“关闭”。

指定密码字符要求

要指定 SA 用户密码的字符要求，请执行以下步骤：

1. 在 SA 客户端中选择“管理”选项卡。
2. 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。
3. 在 SA 组件列表中，选择“Server Automation 系统 Web 客户端”。将显示此组件的系统配置参数。
4. 查找参数 owm.features.MiniPasswordPolicy.allow 并将其设置为 true。

   此参数必须为 true，才能使此页上的其他密码参数生效。要禁用其他密码参数，请将 owm.features.MiniPasswordPolicy.allow 设置为 false。
5. 设置**表 10** 中列出的密码参数的值。
6. 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。
7. 要将这些参数更改应用于多主控网状网络中的其他核心，您必须重新启动其他核心。有关说明，请参见 SA 维护。

表 10. “修改配置参数”页面上的密码要求

密码要求	参数	允许的值	默认值
最大重复、连续字符数	owm.pwpolicy.maxRepeats	必须大于 0	2
最小字符数	owm.pwpolicy.minChars	正整数	6
最小非字母字符数	owm.pwpolicy.minNonAlphaChars	必须小于 owm.pwpolicy.minChars 的值	0

使用外部 LDAP 目录服务进行身份验证

您可以将 SA 配置为使用外部 LDAP 目录服务进行用户身份验证。使用外部身份验证，您不必维护单独的 SA 用户名和密码。当用户登录 SA 客户端时，他们输入其 LDAP 用户名和密码。

LDAP 目录对于 SA 是只读的。导入所有 LDAP 用户后，对目录中用户特性进行的任何更改都要求您重新从 LDAP 目录导入用户。

备注: 必须在所有域控制器上安装 SA 代理，才能让使用 Active Directory 凭据的 `rosh/ttlg` 正常工作。

从 LDAP 服务器导入 SA 的用户

无论身份验证机制如何，所有 SA 用户名都必须唯一。

LDAP 用户必须成功导入 SA，然后才能登录 SA。

从 LDAP 目录导入用户的操作必须由 SA 用户管理员完成。

对导入用户进行管理的方式与 SA 客户端创建用户的方式相同。例如，使用 SA 客户端将导入的用户分配到用户组，并从 SA 删除导入的用户。

如果您使用 SA 客户端删除导入的用户，该用户不会从外部 LDAP 目录中删除。

使用 SA 客户端，在外部 LDAP 中搜索用户，然后将选定用户导入 SA。您可以通过指定筛选器来限制搜索结果。

LDAP 导入过程从 LDAP 目录获取下列用户特性：

```
firstName
lastName
fullName
emailAddress
phoneNumber
street
city
state
country
```

SA 还在导入期间获取 LDAP 用户识别名 (DN)。用户 DN 映射到 SA 用户名。

导入过程之后，您可以在 SA 客户端中编辑导入的用户信息。不过，您不能更改用户登录名或密码。导入用户是一次性单向过程。使用 SA 客户端对用户特性进行的更改不会传播回外部 LDAP 目录服务器。

如果您使用外部身份验证，则仍可以使用 SA 客户端创建单独的用户。不过，不建议这种实践，因为有可能在 LDAP 目录和 SA 客户端中创建重复用户。如果存在重复用户，将使用 SA 客户端中定义的用户，忽略 LDAP 目录中的用户。

要查看 SA 客户端中已导入哪些用户，请选择“管理”选项卡，然后在“用户和组”视图下选择“用户”。确保“凭据库”列已显示。在“凭据库”列中具有目录服务器的用户已从 LDAP 服务器导入。

SSL 和外部身份验证

虽然进行外部身份验证不需要 SSL，但强烈建议这样做。LDAP over SSL 所需的证书文件必须采用“隐私增强邮件”(PEM) 格式。根据 LDAP 服务器，您可能需要将服务器的证书颁发机构 (CA) 证书转换为 PEM 格式。

受支持的外部 LDAP 目录服务器

可以将下列目录服务器产品与 SA 一同使用：

- Microsoft Active Directory（Windows Server 2000、2003、2008 或 2012）
- Novell eDirectory 8.7
- SunDS 5.2

将服务器证书从 LDAP 导入 SA

对于 SSL，必须从 LDAP 目录提取所需的证书，然后将其复制到 SA。要将服务器证书从 LDAP 目录导入 SA，请执行以下步骤：

1. 从外部 LDAP 目录提取服务器证书。有关说明，请参见下列章节。
2. 将提取的证书转换为 PEM 格式。

   在 Windows 系统中创建的证书采用“区分编码规则”(DER) 格式。下面的示例使用 `openssl` 实用程序将证书从 DER 转换为 PEM 格式：

   ```
   OpenSSL> x509 -inform DER -outform PEM -in mycert.der -out mycert.pem
   ```
3. 将服务器证书复制到 LDAP 配置文件 (`twist_custom.conf`) 指定的位置。例如，`twist_custom.conf` 文件可能具有以下行：

   ```
   aaa.ldap.servercert.ca.fname=/var/opt/opsware/crypto/twist/ldapcert.pem
   ```

从 Microsoft Active Directory 提取服务器证书

要提取服务器证书，请执行以下步骤：

1. 运行证书 MMC 管理单元控制台或证书服务 Web 界面。
2. 将 Root CA 证书从 Windows CA 导出为 DER 格式。

从 Novell eDirectory 提取服务器证书

要提取服务器证书，请执行以下步骤：

1. 找出本地 CA 条目的名称。（示例：CN=CORP-TREE CA.CN=Security）
2. 打开 eDirectory 管理实用程序，单击“修改对象”。
3. 输入条目名称 (CN=CORP-TREE CA.CN=Security)。
4. 选择“证书”选项卡。
5. 单击“自签名证书”。
6. 单击“导出”。
7. 在对话框中，单击“否”以导出私钥，然后单击“下一步”。
8. 选择适当的格式（通常是 DER）。
9. 单击“将导出的证书保存到文件”。

从 SunDS 提取服务器证书

通常，不从 SunDS 导出服务器 CA 证书，而是获取导入 SunDS 的证书。

导入外部 LDAP 用户和用户组

完成本节中的任务后，您的用户将能够使用其 LDAP 用户名和密码登录 SA 客户端。

备注: 此方法不导入 LDAP 用户组。如果要导入用户和用户组，请参见使用 LDAP 身份验证配置导入 LDAP 用户和组。

要使用 SA 客户端导入外部用户，请执行下列步骤：

1. 在 SA 客户端导航窗格中，选择“管理”选项卡。这会在导航窗格中显示“用户和组”节点。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户”节点。
3. 选择“用户”节点。这会显示您的所有 SA 用户。
4. 选择“操作”>“导入用户”菜单。这会显示来自 LDAP 目录的信息。
5. 选择“导入用户”选项卡。这会显示 LDAP 目录中的所有用户。
6. 选择一个或多个用户。
7. 您可以选择将用户分配给一个或多个用户组。选择“分配组”选项卡，并选择一个或多个用户组。
8. 选择“导入用户”按钮。此会将用户导入 SA。

使用 LDAP 身份验证配置导入 LDAP 用户和组

LDAP 身份验证配置：LDAP 身份验证配置是命令行工具，用于配置 LDAP 以及将用户和用户组导入 SA。这是一个复杂的过程，需要进行一些准备。

配置 LDAP 后，还可以使用 LDAP 用户和用户组同步 APX 将 LDAP 用户和用户组导入 SA。

备注: 您不应当编辑 LDAP 同步正在维护的用户组。这些用户组由 __DO_NOT_EDIT__ MAINTAINED_BY_LDAP_SYNC_ 描述来指示。

LDAP 身份验证配置先决条件

LDAP 身份验证配置工具是必须在 SA 核心的切分组件捆绑包主机上运行的脚本。在运行该脚本之前，您必须提供下列信息:

表 11.LDAP 身份验证配置先决条件

先决条件	描述
主机名	SA 要使用的 LDAP 目录服务器的完全限定主机名 (FQHN) 或 IP 地址的分号分隔列表。仅首先列出的主机被用于通信，其他主机用于处理故障转移场景。
LDAP 服务器端口	LDAP 目录服务器端口。默认 SSL 端口为 636，默认非 SSL 端口为 389。SA 不支持 StartTLS。
SSL	您的 LDAP 目录服务器是否需要 SSL 身份验证？如果已启用 SSL，则您必须提供用来验证服务器的 SSL 证书的可信 CA 证书。
用于验证服务器 SSL 证书的可信 CA 证书	包含可信 CA 证书的 LDAP 目录服务器上文件的完整路径，该 CA 证书采用 PEM 格式，用于验证 LDAP 目录服务器的 SSL 证书。
具有相互（双向）身份验证的 SSL	您必须提供下列信息: 1 用于验证服务器 SSL 证书的可信 CA 证书 2 用于验证客户端 SSL 证书的可信 CA 证书 3 客户端证书和（未加密的）私钥。
启用了客户端身份验证的 SSL	1 包含可信 CA 证书的文件的完整路径，该证书采用 PEM 格式，用于验证 SSL 客户端证书。 2 包含客户端 SSL 证书及其对应私钥的文件的完整路径，该证书采用 PEM 格式。客户端私钥不能加密。
对目录信息树 (DIT) 的匿名搜索	LDAP 目录是否允许对存储用户信息的 DIT 的匿名搜索？请注意，这将暗示允许匿名绑定。例如，匿名用户（未提供绑定 DN 和密码的用户）是否具有 DIT 的读取访问权限？对于大多数企业，不允许匿名搜索。如果禁用了匿名搜索，则您必须提供具有 DIT 的读取访问权限的用户的绑定 DN 和密码。
绑定 DN	仅在禁用匿名搜索时需要。具有 DIT 的读取访问权限的用户的绑定 DN。
绑定密码	仅在禁用匿名搜索时需要。具有 DIT 的读取访问权限的用户的绑定密码。

先决条件	描述
唯一用户名的特性	唯一用户名的特性。 · 对于 Active Directory，默认值为 `SAMAccountName`。 · 对于 Novell eDirectory，默认值为 `cn`。 · 对于所有其他供应商，默认值为 `uid`。
用户显示名称的特性	用户显示名称的特性。 · 对于 Active Directory，默认值为 `displayName`。 · 对于 Novell eDirectory，默认值为 `fullName`。 · 对于所有其他供应商，默认值为 `cn`。
基本 DN	在用户导入操作期间搜索用户时要考虑的基本 (DN) 或 DIT 部分。LDAP 身份验证配置工具使用子树搜索；因此，搜索筛选器仅适用于处于或低于基本 DN 的用户。
搜索筛选器模板	当 LDAP 中的筛选器搜索用户导入时，使用搜索筛选器模板以及可选筛选器替换。 模板中的任何美元符号 (`$`) 字符将替换为 SA 客户端“导入用户”页中指定的筛选器字符串。（默认值为匹配所有条目的星号 (`*`)。） · 对于 Active Directory，默认值为 `(&(sAMAccountName=$)(objectCategory=person)(objectClass=user)(sAMAccountType=805306368))`。 · 对于 Novell eDirectory，默认值为 `(&(cn=$)(objectClass=person))`。 · 对于所有其他供应商，默认值为 `uid=$`。

LDAP 身份验证配置进程

当您运行 LDAP 身份验证配置时，系统将根据您的 LDAP 目录服务器是否需要 SSL 身份验证以及是否允许匿名搜索来给出提示。

匿名搜索：**否**

SSL：**否**

1. 登录托管您的 SA 核心的切分组件捆绑包的服务器。
2. 以 `twist` 用户身份登录：

```
su twist
```

3. 发出以下命令：

   ```
   cd /opt/opsware/twist
   ```

4. 调用 LDAP 身份验证配置：

   ```
   ./ldap_config.sh
   ```

5. 输入必需的信息。当系统询问是否允许匿名搜索时，输入 N。当系统询问是否需要 SSL 设置时，输入 N。
6. 在该工具完成后，确保成功验证和存储 LDAP 身份验证配置。
7. 登录命令中心，确保外部用户导入正常运行。
8. 确保您可以以 LDAP 用户身份登录命令中心。

匿名搜索： **是**

SSL：**否**

1. 登录托管您的 SA 核心的切分组件捆绑包的服务器。
2. 以 `twist` 用户身份登录：

   ```
   su twist
   ```

3. 发出以下命令：

   ```
   cd /opt/opsware/twist
   ```

4. 调用 LDAP 身份验证配置：

   ```
   ./ldap_config.sh
   ```

5. 输入必需的信息。当系统询问是否允许匿名搜索时，输入 N。当系统询问是否需要 SSL 设置时，输入 N。
6. 在该工具完成后，确保成功验证和存储 LDAP 身份验证配置。
7. 登录命令中心，确保外部用户导入正常运行。
8. 确保您可以以 LDAP 用户身份登录命令中心。

匿名搜索： **否**

SSL：**是**（仅限 SSL 服务器身份验证）

1. 登录托管您的 SA 核心的切分组件捆绑包的服务器。
2. 以 `twist` 用户身份登录：

   ```
   su twist
   ```

3. 发出以下命令：

   ```
   cd /opt/opsware/twist
   ```

4. 调用 LDAP 身份验证配置：

   ```
   ./ldap_config.sh
   ```

5. 当系统询问是否允许匿名搜索时，输入 N。当系统询问是否需要 SSL 设置时，输入 Y。当系统询问是否使用 SSL 客户端身份验证时，回答 N。
6. 在该工具完成后，确保成功验证和存储 LDAP 身份验证配置。

7. 登录命令中心，确保外部用户导入正常运行。
8. 确保您可以以 LDAP 用户身份登录命令中心。

匿名搜索： **否**

SSL：**是（需要 SSL 相互身份验证）**

1. 登录托管您的 SA 核心的切分组件捆绑包的服务器。
2. 以 `twist` 用户身份登录：

   ```
   su twist
   ```

3. 发出以下命令：

   ```
   cd /opt/opsware/twist
   ```

4. 调用 LDAP 身份验证配置：

   ```
   ./ldap_config.sh
   ```

5. 当系统询问是否允许匿名搜索时，输入 `N`。当系统询问是否需要 SSL 设置时，输入 `Y`。当系统询问是否使用 SSL 客户端身份验证时，输入 `Y`。
6. 在该工具完成后，确保成功验证和存储 LDAP 身份验证配置。
7. 登录命令中心，确保外部用户导入正常运行。
8. 确保您可以以 LDAP 用户身份登录命令中心。

匿名搜索：是

SSL：是（仅限 SSL 服务器身份验证）

1. 登录托管您的 SA 核心的切分组件捆绑包的服务器。
2. 以 `twist` 用户身份登录：

   ```
   su twist
   ```

3. 发出以下命令：

   ```
   cd /opt/opsware/twist
   ```

4. 调用 LDAP 身份验证配置：

   ```
   ./ldap_config.sh
   ```

5. 当系统询问是否允许匿名搜索时，输入 `Y`。当系统询问是否需要 SSL 设置时，输入 `Y`。当系统询问是否使用 SSL 客户端身份验证时，输入 `N`。

匿名搜索： **是**

SSL：**是（需要 SSL 相互身份验证）**

1. 登录托管您的 SA 核心的切分组件捆绑包的服务器。
2. 以 `twist` 用户身份登录：

   ```
   su twist
   ```

3. 发出以下命令：

   ```
   cd /opt/opsware/twist
   ```

4. 调用 LDAP 身份验证配置：

   ```
   ./ldap_config.sh
   ```

5. 当系统询问是否允许匿名搜索时，输入 Y。当系统询问是否需要 SSL 设置时，输入 Y。当系统询问是否使用 SSL 客户端身份验证时，输入 Y。

备注: 显示的默认值是上一个 LDAP 身份验证配置工具会话期间保存的值。

LDAP 身份验证配置会话示例

```
./ldap_config.sh


Retrieving LDAP configuration ...

LDAP Connectivity Configuration

Enter the fully-qualified host name or IP for the LDAP directory
server [sample-centos.example.com] :

Does the LDAP directory server require SSL?[N] :

Enter the port number for the LDAP directory server [8389] :

Does the LDAP directory server support anonymous bind and
anonymous read access to the directory information tree?[N] :

Enter the bind distinguished name (DN) of the user who has read
access to the directory information tree (DIT)
[cn=Administrator,cn=users,dc=hyrule,dc=local] :

Do you want to change the bind password for
cn=Administrator,cn=users,dc=hyrule,dc=local [N] :


You have entered the following information:

LDAP Directory Server FQHN/IP                    : sample-
centos.example.com

LDAP Directory Server Port                       :8389

SSL Enabled?                                     : false

Bind DN                                          :
cn=Administrator, cn=users,dc=hyrule,dc=local

Bind Password Provided?                          : true
```

```
Is this correct?[Y] :

Verifying LDAP directory server connectivity ...
found naming context :DC=hyrule,DC=local
found naming context :CN=Configuration,DC=hyrule,DC=local
found naming context
:CN=Schema,CN=Configuration,DC=hyrule,DC=local
found naming context :DC=DomainDnsZones,DC=hyrule,DC=local
found naming context :DC=ForestDnsZones,DC=hyrule,DC=local
LDAP directory server connectivity successfully verified.

LDAP Search Configuration
Is the LDAP directory server an Active Directory (AD) directory
server?[Y] :
Enter the LDAP attribute for the unique username [SamAccountName]
:
Enter the LDAP attribute for the user's display name [cn] :
Enter the LDAP search filter template [(&(sAMAccountName=$)
(objectCategory=person)(objectClass=user)
(sAMAccountType=805306368))] :
Enter the LDAP search base distinguished name (DN).Usually this
is the root naming context.[cn=users,dc=hyrule,dc=local] :

You have entered the following information:
LDAP Unique Username Attribute :SamAccountName
LDAP User Display Name Attribute : cn
LDAP Search Filter Template :(&(sAMAccountName=$)
(objectCategory=person)(objectClass=user)
(sAMAccountType=805306368))
LDAP Search Base Distinguished Name (DN) :
cn=users,dc=hyrule,dc=local

Is this correct?[Y] :
```

```
Verifying LDAP search configuration ...

To test LDAP search configuration, you must provide a username of
a LDAP directory user to search.

LDAP search configuration is successfully verified only if the
given user is successfully returned by the LDAP

directory server.

Enter a username to search :*


You have entered the following information:

Username To Search :*


Is this correct?[Y] :


Resulting LDAP Search Filter :(&(sAMAccountName=*)
(objectCategory=person)(objectClass=user)(sAMAcco

untType=805306368))

Searching LDAP directory server for user * ...

Found 4 users


DN :CN=Administrator,cn=users,dc=hyrule,dc=local

cn :Administrator

SamAccountName :Administrator


DN :CN=Guest,cn=users,dc=hyrule,dc=local

cn :Guest

SamAccountName :Guest


DN :CN=krbtgt,cn=users,dc=hyrule,dc=local

cn : krbtgt

SamAccountName : krbtgt


DN :CN=link,cn=users,dc=hyrule,dc=local

cn : link
```

```
SamAccountName : link

Is this correct?[Y] :
LDAP search configuration successfully verified.

Enter the LDAP search filter template to search user groups [(&
(cn=$)(objectCategory=group))] :
Enter the LDAP attribute for the unique user group name
[SamAccountName] :
Enter the LDAP attribute in the user group LDAP object class
which contains the DNs of its members [
member] :

You have entered the following information:
LDAP Search User Group Base DN : cn=users,dc=hyrule,dc=local
LDAP Search User Group Search Filter Template :(&(cn=$)
(objectCategory=group))
LDAP Unique User Group Name Attribute :SamAccountName
LDAP Search User Group Membership Attribute : member

Is this correct?[Y] :

Verifying LDAP user group synchronization configuration ...
Searching LDAP directory server for all users and user groups ...
Searching LDAP directory server for all LDAP users ...

Resulting LDAP Search Filter For All LDAP Users :(&
(sAMAccountName=*)(objectCategory=person)(object
Class=user)(sAMAccountType=805306368))
Found 4 LDAP users

Parsing search results ...
Searching LDAP directory server for all LDAP user groups ...
```

```
Resulting LDAP Search Filter For All LDAP User Groups :(&(cn=*)
(objectCategory=group))
Found 16 LDAP user groups

Parsing search results ...
Do you wish to display detail search result?[N] : y
Parsing search results ...
Denied RODC Password Replication Group:2 members
 Administrator : cn=administrator,cn=users,dc=hyrule,dc=local
 krbtgt : cn=krbtgt,cn=users,dc=hyrule,dc=local
Allowed RODC Password Replication Group:0 members
Enterprise Read-only Domain Controllers:0 members
Group Policy Creator Owners:1 members
 Administrator : cn=administrator,cn=users,dc=hyrule,dc=local
Domain Controllers:0 members
Cert Publishers:0 members
Domain Users:0 members
Enterprise Admins:1 members
 Administrator : cn=administrator,cn=users,dc=hyrule,dc=local
Schema Admins:1 members
 Administrator : cn=administrator,cn=users,dc=hyrule,dc=local
DnsAdmins:0 members
Read-only Domain Controllers:0 members
RAS and IAS Servers:0 members
Domain Guests:0 members
Domain Admins:1 members
 Administrator : cn=administrator,cn=users,dc=hyrule,dc=local
Domain Computers:0 members
DnsUpdateProxy:0 members
Is this correct?[Y] :
LDAP user group synchronization configuration successfully
verified.
```

```
The following properties will be stored into global
configuration.

aaa.ldap.hostname=gyee-centos.cup.hp.com

aaa.ldap.port=8389

aaa.ldap.ssl=false

aaa.ldap.search.binddn=cn=Administrator,cn=users,dc=hyrule,dc=loc-
al

aaa.ldap.search.pw=true

aaa.ldap.search.naming.attribute=SamAccountName

aaa.ldap.search.display.name.attribute=cn

aaa.ldap.search.filter.template=(&(sAMAccountName=$)
(objectCategory=person)
  (objectClass=user)(sAMAccountType=805306368))

aaa.ldap.search.base.template=cn=users,dc=hyrule,dc=local

aaa.ldap.enable.users.groups.sync=true

aaa.ldap.search.usergroup.naming.attribute=SamAccountName

aaa.ldap.search.usergroup.membership.naming.attribute=member

aaa.ldap.search.usergroup.base.template=cn=users,dc=hyrule,dc=loc-
al

aaa.ldap.search.usergroup.filter.template=(&(cn=$)
(objectCategory=group))


Are you sure?[Y] :

Saving LDAP configuration ...

LDAP configuration successfully saved.
```

同步 LDAP 用户

如下所述，在 LDAP 身份验证配置进程完成后，可以使用 `ldap_sync.sh` 工具从命令行将 LDAP 用户和组与 SA 数据库同步。

也可以从 SA 客户端运行 LDAP 用户和用户组同步 APX，来计划同步进程。在 SA 客户端中的“SA 库”>“按类型”>“扩展”>“程序”下列出此程序 APX（先前称为“ldap.user_and_usergroups_sync”）

备注: 有关运行 APX 的说明，请参见*《SA 用户指南：Server Automation》*中的“在托管服务器上运行扩展”。在 SA 客户端帮助中也能找到该主题：在 SA 客户端的程序 APX

列表中，单击“F1”打开页面帮助，然后单击标题链接（扩展：属性）来打开帮助主题。

要使用 ldap_sync.sh 同步 LDAP 用户和用户组，请执行以下操作：

1. **在托管您的 SA 核心的切分组件捆绑包的服务器上，以 twist 用户登录：**

   ```
   su twist
   ```

2. **发出以下命令：**

   ```
   cd /opt/opsware/twist
   ```

3. **调用 LDAP 同步：**

   ```
   ./ldap_sync.sh
   ```

   您将看到类似如下的输出：

   ```
   Retrieving LDAP configuration ...
   Verifying LDAP server connectivity ...

   User Synchronization Phase
   Searching LDAP directory server for all LDAP users ...
   Found 4 LDAP users
   Parsing search results ...
   4 LDAP users do not exist in SA
   Creating them now ...
   Creating user cn=link,cn=users,dc=hyrule,dc=local
   Creating user cn=krbtgt,cn=users,dc=hyrule,dc=local
   Creating user cn=guest,cn=users,dc=hyrule,dc=local
   Creating user cn=administrator,cn=users,dc=hyrule,dc=local

   User Group Synchronization Phase
   Searching LDAP directory server for all LDAP user groups ...
   Found 16 LDAP user groups
   Parsing search results ...
   creating user group Denied RODC Password Replication Group
   creating user group Allowed RODC Password Replication Group
   creating user group Enterprise Read-only Domain Controllers
   creating user group Group Policy Creator Owners
   creating user group Domain Controllers
   creating user group Cert Publishers
   creating user group Domain Users
   creating user group Enterprise Admins
   creating user group Schema Admins
   creating user group DnsAdmins
   creating user group Read-only Domain Controllers
   creating user group RAS and IAS Servers
   creating user group Domain Guests
   creating user group Domain Admins
   creating user group Domain Computers
   creating user group DnsUpdateProxy
   ```

```
Updating user groups no longer found in LDAP ...

LDAP Users & User Groups Sync Results
================================================================
=
Number of LDAP Users Found :4
Number of LDAP Users Does Not Exist In SA :4
Number of LDAP Users Successfully Created in SA :4
Number of LDAP Users Failed To Create In SA :0

Number of LDAP User Groups Found :16
Number of LDAP User Groups Successfully Updated in SA :0
Number of LDAP User Groups Successfully Created in SA :16
Number of SA User Groups No Longer in LDAP :0
Number of SA User Groups Failed To Update :0
Number of LDAP User Groups Failed To Process :0

Elapsed Time :0:00:27
================================================================
```

从 LDAP 目录删除的 LDAP 用户不会从 SA 中删除，但是，这些用户将无法登录 SA，这是因为其对应的身份验证信息已从 LDAP 目录中删除。

将跳过用户 ID 与现有 SA 用户相同的 LDAP 用户，无论该用户的凭据存储类型如何。SA 将不创建或更新重复的用户。

SA 通用访问卡 (CAC) 和个人身份验证 (PIV) 智能卡集成

通用访问卡（或 CAC 卡）是一种信用卡大小的智能卡。它是标准标识，适用于现役军人、后备军人、美国国防部 (DoD) 文职雇员和合格的承包商人员。它还是一种主卡，用于在访问建筑和控制区域时出示，并且提供对国防计算机网络和系统的访问权限。它用作日内瓦公约（尤其是日内瓦第三公约）下的标识卡。CAC 卡满足双重身份验证标准（属于用户的某些标准和仅对用户可知的某些标准）以及数字签名和数据加密技术标准（身份验证、完整性和不可否认性）。

备注: 仅在登录到 SA 客户端时，SA/智能卡集成才可用。

智能卡/SA 集成身份验证基础知识

SA 客户端发现智能卡并为用户提供登录选项：使用常规 SA 身份验证屏幕或使用基于新智能卡的身份验证登录。在用户提供必要的 PIN 后，SA 客户端使用读卡器 API 访问智能卡证书。对智能卡的证书进行吊销验证，并将证书的唯一字段映射到内部 SA 用户帐户。SA 管理员创建这些唯一字段的原始映射。

用于标识用户的信息会存储在智能卡上称为证书的文档中。此证书包含称为公钥的加密密钥。它还包含用于标识用户的文本字段，例如人员姓名（通常是名字、姓氏和中间名首字

母缩写）或者可能是用户在组织内的电子邮件地址。为了使用户的智能卡身份验证信息与现有SA用户名匹配，系统会根据智能卡证书中的文本数据构造用户名。

存储在智能卡上的证书类似以下内容：

```
Certificate:
 Data:
 Version:3 (0x2)
 Serial Number:1501 (0x5dd)
 Signature Algorithm: ecdsa-with-SHA256
 Issuer:C=US, O=Test Certificates 2010, OU=Test CA, CN=Test ECC P-256 CA
 Validity
Not Before:Oct 1 08:30:00 2010 GMT
Not After :Oct 1 08:30:00 2030 GMT
Subject:CN=Test E. Cardholder XV, C=US, O=Test Government, OU=Test Agency
Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
EC Public Key:
pub:
04:03:a0:ad:22:46:01:b8:9b:1b:65:b0:94:3f:5e:
…
```

为了从证书派生用户名，SA使用在 `/etc/opt/opsware/twist/twist.conf` 文件中设置的模式规范字符串和用于构造用户名的匹配组装算法。模式规范可能类似以下内容：

```
sc.usernameMakeRule.1=%Subject#CN$1%Subject#CN$2%Subject#CN$3
```

用户名创建逻辑将使用上述规范字符串来创建用户名：

```
TestE.Cardholder
```

证书中的字段名使用百分号 (`%`) 指定，特性（子字段）使用井号 (`#`) 指定，特性中的位置字段使用美元符号 (`$`) 后跟一个数字（字段在文本行中的位置）指定。

这将是随SA安装提供的默认模式。SA管理员必须意识到此模式创建的用户名可能不是唯一的，他们应制定相应的计划。

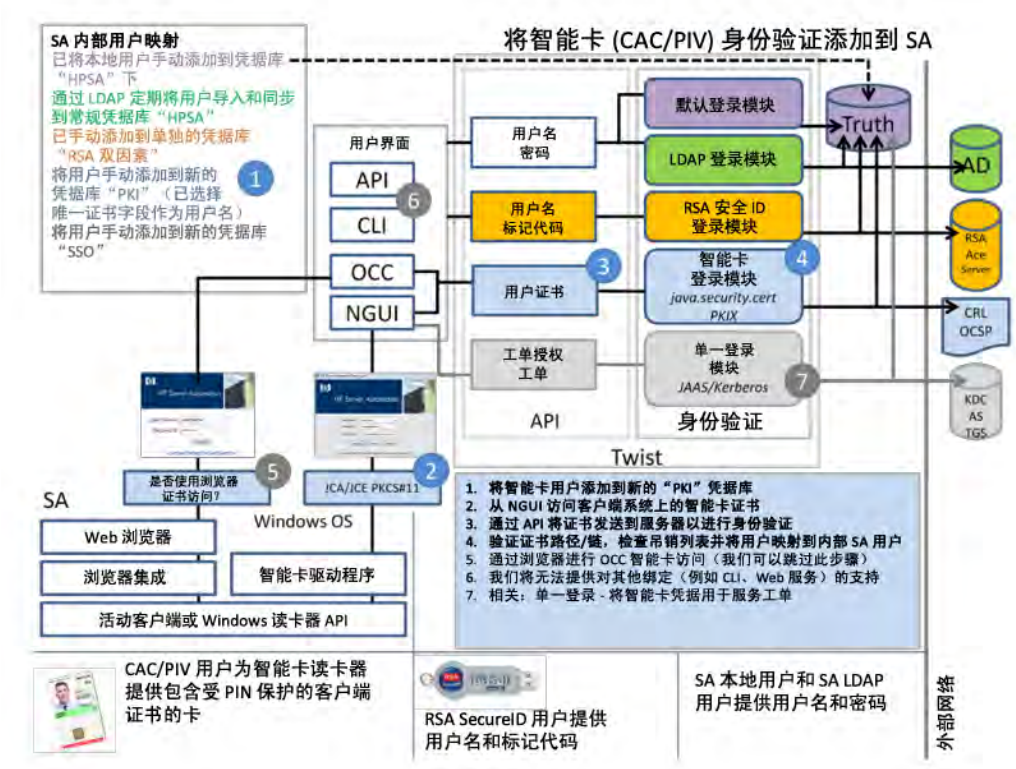
备注: 请勿将算法中的“SmartCard”特性用于构造用户名。

您必须在安装之前决定从智能卡证书创建用户名的模式。了解机制、确定用户名的创建模式（可以接受默认模式或指定其他模式）以及确保训练管理员使用正确的基于模式的用户名在SA中创建智能卡用户帐户，这些至关重要。

SA 智能卡集成体系结构

图 17 阐明 CAC/PIV 智能卡功能如何与 SA 集成：

图 17.SA/CAC 智能卡集成体系结构



设置 SA/智能卡集成

设置新用户以使用 CAC 智能卡登录十分简单：

- 创建新用户并将凭据库指定为“SmartCard”。
- 在该用户登录 SA 客户端时，将扫描其智能卡并输入其唯一的 PIN 号码。

设置智能卡证书

- 必须按以下方式修改 `/etc/opt/opsware/twist/twist.conf` 文件：
- 对于每个签名算法，必须包含名为 `sc.sigAlrgName.N` 的条目，其中 `N` 是系列中的编号。
- 对于每个算法，必须包含名为 `sc.trustedCertPath.N` 的证书文件（格式为 `.pem`）路径。

  例如：

  ```
  sc.sigAlgName.0=SHA256withECDSA
  ```

```
sc.trustedCertPath.0=/var/opt/opsware/crypto/twist/smartcard/ECCP256
IssuingCACertificate.pem
sc.sigAlgName.1=SHA384withECDSA
sc.trustedCertPath.1=/var/opt/opsware/crypto/twist/smartcard/ECCP384
IssuingCACertificate.pem
sc.sigAlgName.2=SHA256withRSA
sc.trustedCertPath.2=/var/opt/opsware/crypto/twist/smartcard/RSA2048
IssuingCACertificate.pem
```

证书文件的位置可选，但建议将证书文件存储在以下目录中：

```
/var/opt/opsware/crypto/twist/smartcard/
```

在所有切分主机上设置智能卡证书

*您必须对托管切分组件捆绑包的 SA 核心中的每个服务器*执行下列步骤。

1. 创建以下文件夹：

   ```
   mkdir /var/opt/opsware/crypto/twist/smartcard
   ```

2. 对于每个切分主机，将用户的智能卡证书导入步骤 1 中创建的文件夹：

   ```
   /var/opt/opsware/crypto/twist/smartcard
   ```

3. 务必将这些证书的所有权更改为 `twist`：

   ```
   chown -R twist:user /var/opt/opsware/crypto/twist/smartcard
   ```

4. 在每个切分主机上重新启动 Web 服务数据访问引擎 (`twist`)。
5. 设置用户并验证是否可以使用智能卡对此用户进行身份验证。

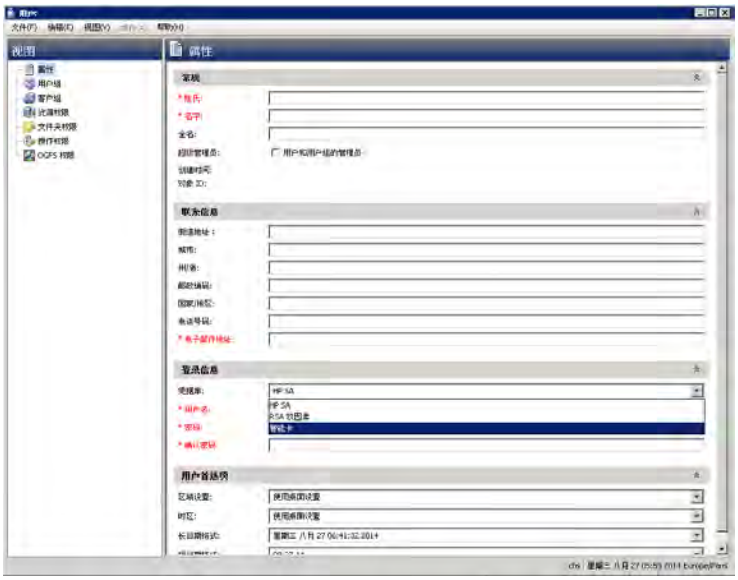
创建新的智能卡用户

要从 SA 客户端创建新 SA 用户，请执行下列步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中打开“用户和组”节点。这会显示“用户”节点。
3. 选择“用户”节点。这会显示您的所有 SA 用户。
4. 选择“操作”>“新建”菜单或选择“新建用户”图标。这会显示“新建用户”窗口。

完成创建新用户中所述的用户信息字段，并指定“智能卡”作为凭据库。

备注：选择“智能卡”作为凭据库时，屏幕中删除密码字段，因为智能卡访问是通过使用智能卡加密技术实现的，而非预设的密码。



备注: 如上所述，根据智能卡/SA 集成身份验证基础知识 中所述的规则，“用户名”字段中包含的名称必须与用户智能卡证书中派生的名称匹配。创建新智能卡用户的管理员必须了解用户名构造模式规则的作用方式，这样才能输入与这些规则匹配的文本字符串。

以智能卡用户身份初始登录 SA 客户端

启动 SA 客户端时，您会看到显示以下类似内容的屏幕：

图 18.标准的 SA 客户端登录对话框

要启用智能卡登录，请单击“More>>”按钮访问高级登录设置。您会看到类似**图 19** 内容的屏幕：

图 19.设置 SA 客户端以使用智能卡登录

要启用智能卡登录，请选择“Use Smart Card”，方法是选中此选项左侧的框。登录屏幕将类似**图 20**:

图 20.启用智能卡的 SA 客户端登录屏幕

所有后续的登录均将显示此屏幕。要还原到标准的用户名/密码登录，请选择“Advanced Settings”并取消选中“Use Smart Card”选项。

在智能卡登录屏幕上，用户使用的 PC 必须正在运行智能卡读卡器设备。为使 SA 可以使用读卡器，请确保 Windows 设备在“介质”图标应用程序中可见。如果用于通过智能卡访

问 SA 的 PC 不具备有效的读卡器，请与 IT 管理员联系。要继续访问 SA，用户必须输入智能卡的 PIN 并按“Log In”按钮。

SA/RSA SecurID® 集成

RSA SecurID® 是 RSA Security, Inc.（EMC 的分公司）提供的双因素身份验证系统。双因素身份验证基于*您知道的内容*（密码或 PIN）和*您拥有的内容*（身份验证器）的概念，提供比密码更强的用户身份验证。本节描述如何在您的 SA 系统中利用 SecurID 身份验证；但是本节不解释如何安装、配置或维护 RSA SecurID。

有关 RSA SecurID 的详细信息，请参见 *http://www.rsa.com*。

本节描述 SA 身份验证如何与 RSA SecurID 集成。假设您已经使用 RSA SecurID 或者将要安装它。必须先安装并完全配置 RSA SecurID 服务器（RSA Authentication Manager 或 ACE Server），然后才能开始将 SecurID 身份验证与 SA 一同使用。

RSA SecurID/SA 集成概述

SA 用户需要向 SA 进行身份验证，才能执行任何操作。SecurID 集成允许他们使用其现有的 RSA SecurID 标记来进行身份验证。SA 身份验证可以无缝集成到现有 SecurID 环境中。对于 RSA 身份验证服务器而言，SA（更具体而言，是 Web 服务数据访问引擎服务器）只是另一个 SecurID 代理。

SA 核心的安装自动提供 SecurID 支持。只需要一些配置步骤即可启用该支持：

备注: 必须在多主控网状网络中的每个 Web 服务数据访问引擎主机上，或者在具有多个 Web 服务数据访问引擎的 SA 安装中，执行前两个任务。

- 将名为 sdconf.rec 的 RSA SecurID 配置文件复制到托管 Web 服务数据访问引擎 (twist) 的任意 SA 核心服务器上的目录中。sdconf.rec 位于 RSA Authentication Manager/ACE Server 主机上，包含必须提供给 SA 核心的有关 RSA Authentication Manager 的必需信息。
- 在编辑 loginModule.conf 文件后关闭 Web 服务数据访问引擎并重新启动，以在 SA 中启用 SecurID 身份验证。
- 在 SA 客户端中创建或修改用户以使用 SecurID 身份验证。

SA 对 SecurID 身份验证方法的支持

RSA SecurID 基于双因素身份验证，将 SecurID 标记作为第一个因素，个人识别码 (PIN) 作为第二个因素。

SecurID 标记是*您拥有的内容*，PIN 是*您知道的内容*。这两个因素提供比用户密码强很多的身份验证。

SecurID 标记可以基于硬件（*硬件标记*或*硬标记*）或基于软件（*软件标记*或*软标记*）。标记提供标记代码，当与预先分配的（配置的）PIN 组合时，称为*通行码*。

表 12 显示了 SA/SecurID 集成支持的典型身份验证方法。

表 12.SecurID 身份验证方法

身份验证方法	描述
普通身份验证	最常用的方法。分配（*配置*）用户的 PIN。接受或拒绝通行码。
下一标记代码模式（不支持）	当用户未正确输入通行码时使用此方法。在下一标记代码模式中，用户必须等待标记代码更改，然后提交新的标记代码。默认情况下，如果用户连续三次提交错误的通行码，则用户将进入下一标记代码模式。
新 PIN 模式 （不支持）	当用户必须创建新 PIN 或修改现有 PIN 时，会发生此情况。

限制

RSA SecurID 身份验证不适合于非交互脚本，因为标记代码每 60 秒更改一次，因此导致非交互脚本失败。您的选择是重写要交互的脚本，或者避免使用此类脚本将受影响的 SecurID。

SecurID/SA 集成平台要求

- Solaris
- Linux x86 和 x86_64
- RSA ACE Server 6.1 或更高版本。

配置 SA/SecurID 集成

支持 RSA SecurID 身份验证集成到 SA 核心中，并支持在安装 SA 核心时安装 RSA SecurID 身份验证。不过，要开始使用 RSA SecurID/SA 身份验证，您必须完成一些配置步骤。SA 核心还必须具有 SecurID 身份验证服务器的 IP 地址，且能够以安全的方式与该服务器通信。

要求: 如果您在一个 SA 核心中安装了多个切分，则必须针对每个切分组件捆绑包主机执行下列步骤。

阶段 1：RSA SecurID 身份验证配置文件

1. 联系您的 RSA SecurID 管理员，获取下列文件：

   ```
   sdconf.rec
   ```

2. 将此文件复制到托管 Web 服务数据访问引擎 (twist) 的核心中的所有服务器上的以下位置：

   ```
   /var/opt/opsware/crypto/twist
   ```

3. 在每个服务器上设置文件权限，以便授予此文件的 `twist` 用户所有权和读取权限：

   ```
   chmod 400 /var/opt/opsware/crypto/twist/sdconf.rec
   chown twist /var/opt/opsware/crypto/twist/sdconf.rec
   ```

4. 请确保 `/var/opt/opsware/crypto/twist` 目录中不存在 `securid` 或 `sdstatus.12` 文件。如果任一文件存在，请将其删除。

阶段 2：在 SA 中启用 RSA SecurID 身份验证

1. 默认情况下，不启用 RSA SecurID 身份验证。要启用它，请在托管 Web 服务数据访问引擎 (twist) 的核心中的每个服务器上，使用以下命令关闭此组件：

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

2. 查找此文件：

   ```
   /etc/opt/opsware/twist/loginModule.conf
   ```

   编辑此文件，添加下面示例中的粗体行：

   ```
   TruthLoginModule {
   com.opsware.login.SecurIDLoginModule sufficient debug=false
   next_tokencode_mode=false new_pin_mode=false;
   com.opsware.login.TruthLoginModule sufficient debug=false;
    };
   ```

3. 使用以下命令在所有服务器上重新启动 Web 服务数据访问引擎：

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

4. 如果您安装了多个切分组件捆绑包，请在所有其他切分组件捆绑包主机上停止命令中心 (OCC) 服务器和 HTTPs 代理。
5. 此时，只有配置为 RSA 服务器的切分组件捆绑包主机的命令中心正在运行。登录该主机的 OCC。这将在 `/var/opt/opsware/crypto/twist` 子目录中生成节点加密 (`securid`) 文件和 `sdstatus.12` 文件，并向 ACE 注册切分组件捆绑包服务器。

6. 现在，您可以在核心中的所有其他切分组件捆绑包主机上启动 OCC 和 HTTPs 代理。

阶段 3：创建/修改 SA 用户以使用 SecurID 身份验证

每个要使用 SecurID 身份验证的用户必须首先是 RSA SecurID 身份验证服务器（ACE 服务器）中经过身份验证的用户，然后必须在 SA 客户端中进行创建或修改，才能使用 SecurID 身份验证。

在 SA 客户端中用户的“配置文件”页上，指定用户的凭据库应当为“RSA 双因素”。

有关创建或修改用户的详细信息，请参见管理用户 - SA 客户端。

故障排除

如果您收到多个“验证失败”错误消息，请首先咨询 RSA SecurID 管理员，以确保用户和通行码仍有效。如果您无法解决问题，请与技术支持代表联系。

用户和安全报告

SA 允许您生成报告，这些报告提供跨服务器的客户端和功能权限的摘要。只有当您以管理员身份登录 SA 客户端时，这些报告才可用。有关详细信息，请参见SA 报告指南。

SA 提供下列用户和安全报告：

- 客户端和功能权限
- 客户/设施权限和设备组权限覆盖
- 用户组成员资格
- 用户登录
- 管理员操作
- 用户和授权（按用户组）
- 用户和授权（按单用户组）
- 管理员客户组
- 服务器权限（按用户）
- 服务器权限（按服务器）
- OGFS 权限（按用户）
- OGFS 权限（按服务器）

第 2 章

SA 核心和组件安全性

SA 核心和组件安全性体系结构简介

- SA 可以明显帮助提高典型数据中心的安全性。具体而言，SA 可以启用：
- 在所有数据中心中一致地配置安全性已强化的服务器操作系统和应用程序软件。
- 在整个数据中心环境中引入更强的控制和责任；例如，通过减少服务器上需要管理员级别密码的人员的数量，创建对特定服务器上所执行任务的已数字签名的审核跟踪。
- 自动应对保持强大安全性的当前配置管理挑战：标识缺少修补程序的服务器，一致地应用修补程序，当配置文件更改以便于回滚时备份配置文件，等等。

虽然自动化数据中心带来的好处是引人注目的，但是组织需要保证自动化系统本身没有产生新安全漏洞的可能性。随着威胁的复杂性不断增加，无论是在组织内部还是外部，都应当绝对确保您的自动化软件体系结构在设计时将安全性作为首要考虑因素。SA 在设计时已将安全性作为首要考虑因素。

本节描述 SA 如何将最新安全性最佳实践用在具有最严格安全性要求和下列设计目标的组织中：

- **严格的控制和责任**：您可以确信只有经过授权的管理员可以执行管理操作，这是因为 SA 强制执行精细的基于角色的访问控制，并生成针对帐户活动的已数字签名的审核跟踪。
- **在整个系统中确保通信通道的安全**：SA 是分布式计算环境，在该环境中，各个组件通过 IP 网络彼此安全地进行通信。为此，SA 使用 SSL/TLS 和 X.509 证书确保这些组件之间通信的安全。
- **自动交付基于行业标准的符合性策略**：SA 提供基于行业标准的可立即操作的符合性策略的当前流。符合性策略充分利用 SA 针对精细特性（例如已安装的修补程序、已安装的软件、最小密码长度、注册表项设置甚至文件中的各个配置设置）的广泛审核和修正功能。

强制严格的控制和责任

SA 提供强大安全性和责任，如下面章节所述。

更强的控制和责任

SA 使用强大的控制和责任提高了整个数据中心的安全性。使用 SA，安全性架构师或 IT 管理人员可以控制哪些人可以在服务器上执行特定任务。任务控制是精细的；例如，管理员可以授予包含更改特权的广义只读访问权，这些更改特权仅限于修补程序安装和 SA 全局 Shell 命令的特定列表。

SA 自动创建防篡改审核跟踪以捕获详细信息，例如哪些 SA 用户在给定的时间在服务器上执行了特定管理任务。SA 精细的基于角色的访问控制系统是围绕用户、服务器组、管理任务、描述环境的 SA 数据模型之间的交互而设计的。此强大访问控制模型的一个直接的安全性好处是有较少的人需要在服务器上使用管理员帐户。相反，可以向他们授予 SA 用户帐户以仅执行他们必须执行的管理任务，这是一个安全性最佳实践。

每个登录 SA 的人都必须有唯一的 SA 用户名和密码。管理员可以在 SA 中创建用户名，或者从外部 LDAP 系统导入用户名。例如，如果某公司具有现有的 Microsoft Active Directory 实现，则可以与目录服务器同步，以重用已存在的用户帐户。

当创建用户帐户时，SA 用户分配到 SA 组。组是一种描述哪些服务器用户可以在服务器上操作、他们可以在服务器上执行哪些管理任务的简便方法。

默认情况下，SA 中提供一些预定义组。可以根据需要自定义这些组的权限，您可以创建新的具有自定义权限级别的组，以满足任何组织的需要。您为用户组指定的权限决定了组成员可以对 SA 执行的操作。*操作权限* 指定用户可以执行的操作；*资源权限* 指定用户可以在哪些对象（通常是服务器）上执行这些操作。SA 图形用户界面（称为 SA 客户端）和全局 Shell 界面都由这些任务规则绑定，以便用户只能查看和执行安全管理员授权他们执行的任务。

安全管理员还可以控制基于策略的软件安装环境，该环境自动执行在服务器上安装软件和配置应用程序的过程。指定的用户可以在文件夹层次结构中对组织的应用程序软件结构建模，为创建、查看、修改和执行设置精细的权限。此模型提供了明确的专业划分，主题内容专家可以实现和调整策略，系统管理员可以通过将软件策略应用于服务器来管理他们环境中的服务器。

备注: 请参见用户和用户组设置及安全性用户组和权限。

只读的已数字签名的审核跟踪

除了仔细控制 SA 用户可以在托管服务器上执行的操作外，SA 还自动维护针对 SA 用户执行的事件的详细审核跟踪。审核跟踪日志详细记录了用户、事件、操作的服务器、执行任务的时间、已用时间总计，以及与任务关联的所有错误情况。

审核跟踪本身以只读的已数字签名的数据形式存储在 Oracle 数据库中，以阻止用户篡改数据。此审核跟踪数据可帮助组织在其环境中建立严格的责任制 - 在出台《萨班斯-奥克斯利法案》、《金融服务现代化法》(GLB Act) 以及《医疗信息流通与责任法案》(HIPAA) 时期，这是一个日益紧迫的话题。用户可以选择审核跟踪的存储期限（默认期限为 6 个月），他们可以轻松创建数据仓库以将审核跟踪（和其他 SA 数据）存储更长的时间。

审核记录包含在 AUDIT_DATA 表空间中，且包含以下表：

AUDIT_OBJTYPE_ATTR

AUDIT_OBJECT_TYPES

AUDIT_OBJECT_COLLECTORS

AUDIT_OBJECT_ATTR

AUDIT_FEATURES

AUDIT_EVENT_OBJECTS

AUDIT_EVENT_DETAIL_VALUES

AUDIT_EVENT_DETAILS

AUDIT_EVENTS

AUDIT_DATA_TYPES

AUDIT_DATA_OBJECTS

AUDIT_DATAOBJ_VALUES

AUDIT_CONFIG_PARAMS

AUDIT_COMPONENTS

AUDIT_ACTIONS

软件数据库中程序包的已签名 SHA 校验和

当 SA 用户将软件上载到软件数据库时，SA 自动计算程序包的 RSA-with-SHA1 签名。为了生成该签名，SA 使用 SHA1 校验和计算、软件包内容和仅软件数据库知晓的内部 RSA 私钥的组合。该私钥不可修改。这可以阻止用户篡改软件数据库中的软件。程序包及其对应的数字签名本地存储在软件数据库中。当 SA 在托管服务器上安装软件时，它在允许下载之前对软件的 RSA 密钥和 SHA1 签名进行验证。这有助于确保 SA 安装的软件是上载到软件数据库的同一软件。

基于角色的授权

- SA 实施一套非常精细的基于角色的访问控制系统。安全管理员可以设置针对下列参数的授权：
- **设施**：设施是单一 SA 核心管理的服务器的集合。设施可以是数据中心、服务器机房或计算机实验室的全部或一部分。设施是基于角色的精细允许模型中的最高级别的抽象。
- **服务器组（按客户）**：服务器由客户分组，可以代表单一数据中心中的任意服务器组。服务器组可以代表支付客户、成本中心，或者运行特定业务应用程序（例如 Siebel 或费用报告应用程序）的服务器。SA 管理的每个软件包都属于特定客户（尽管它们还可能属于称为*独立于客户*的特殊帐户），这意味着软件可以在任何客户的服务器进行配置（例如，修补程序属于*独立于客户*的客户帐户）。这使得安全管理员能够准确控制可在特定服务器组中应用的软件包集合。
- **动态服务器组（基于角色）**：安全管理员还可以根据*动态规则评估*（从简单到复杂）创建服务器组，向所有属于该组的服务器授予权限。例如，安全管理员可以对运行 Linux 操作系统和驻留在特定 IP 地址空间中的托管服务器进行分组，然后指定哪些 SA 用户组有权在此服务器组中执行管理任务。
- **软件策略建模和分发**：软件策略建模提供强大的机制，使用文件夹模型为软件建模。文件夹提供了定义安全权限的能力以在整个用户组中控制对其内容的访问权限。您可以设置文件夹权限以确定哪些用户组可以查看、使用和修改文件夹中的项。

用户活动的审核日志记录

SA 将审核跟踪集中存储在模型库中，每个条目都进行了数字签名。SA 采用自下向上的设计，带有强加密控制，可阻止对审核日志的任何无法检测的修改。由于审核日志是集中存储的，因此不能从托管服务器删除它们。实际上，SA 的整个安全设计具有防御性，它基于这样的假设：受到威胁的单个托管服务器不能危害整个系统的安全。

确保 SA 内部通信的安全

SA 包括一些核心组件，这些组件通过安全通信通道（通常是诸如 HTTPS 的行业标准的协议）彼此进行通信。这些组件包括：

- 在用户本地桌面或服务器上运行安全浏览器的 SA 用户。SA 浏览器使用 HTTPS 与 SA 命令中心进行安全通信。用户提供用户名和密码以登录 SA；凭据在 SA 中进行验证，也可以通过外部集成的 LDAP 服务器进行验证。
- 在托管服务器上运行的 SA 服务器代理。当与 SA 核心组件通信时，SA 服务器代理充当客户端和服务器。所有通信都已使用 SSL/TLS 进行了加密、完整性检查，并使用客户端证书进行身份验证。少数核心组件可以通过特定 TCP/IP 端口将命令发布到 SA 代理；SA 代理还可以回调到核心组件，每次回调都使用其自己的指定端口。
- SA 核心组件，它们是在少数服务器上运行的后端进程。SA 核心组件也使用强验证的 SSL/TLS 彼此通信和与 SA 代理进行通信。

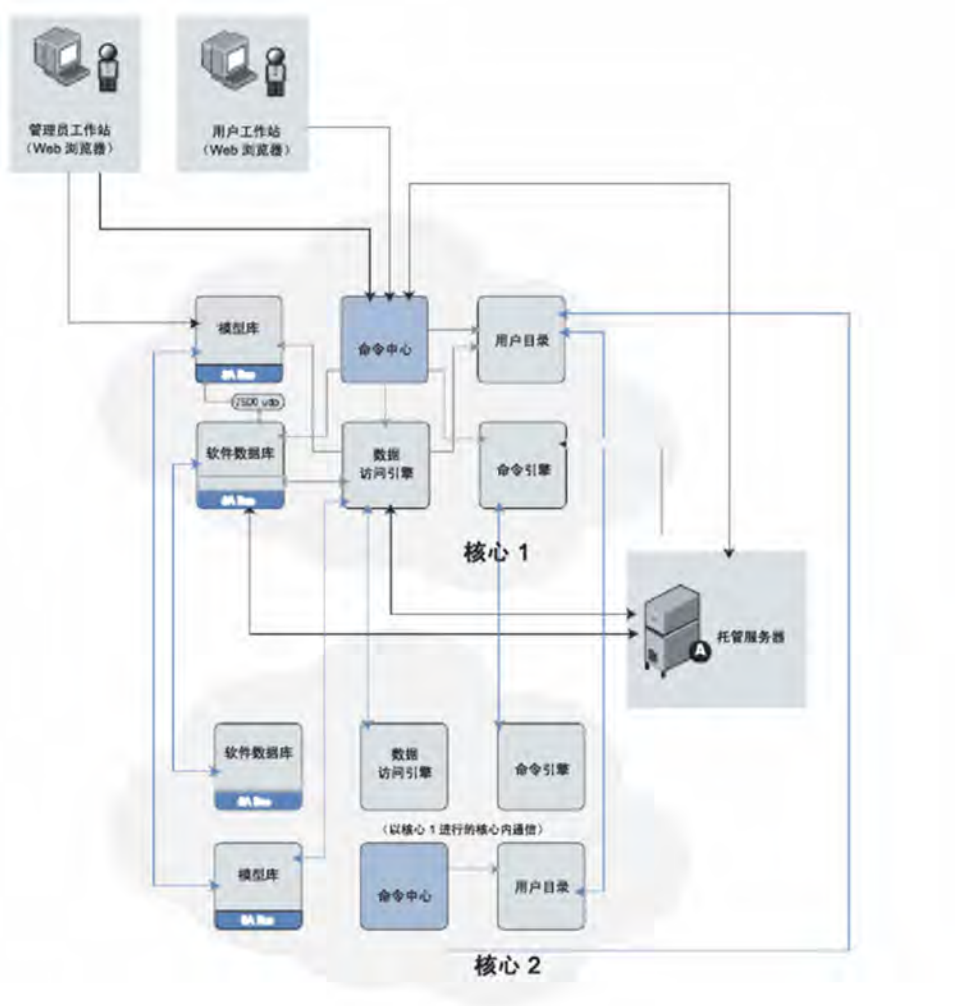
对于跨多个数据中心运行 SA 的客户，SA 核心之间还使用 SA（SA 总线）中包括的集成认证消息，通过提供的安全通道进行通信。

通过保护分布式组件之间的通信通道，SA 可阻止入侵者探查网络流量或导致 SA 在 SA 管理的服务器上执行未经授权的任务。

SA 核心中组件之间的通信

当 SA 组件必须与另一个组件通信时，它打开一个使用已知端口的安全通信通道（通常是 SSL/TLS）。每个 SA 组件有一个公钥证书，该证书是在安装 SA 时生成的。当组件向另一个组件进行身份验证时，将使用其公钥证书。大多数进程间通信都采用这种方式进行强身份验证（使用最强的可用密码加密）和完整性检查。

图 21.组件通信



代理与 SA 核心组件之间的通信

服务器代理参与上述强身份验证和加密 SSL/TLS 流量。另外，当代理被指示执行服务器上的管理任务时，典型的控制消息流（如下所述）将帮助确保只有经授权的用户才能执行这些操作。入侵者很难生成有效命令序列来指示代理执行未经授权的任务。

下面的序列描述典型的 SA 管理任务，即在托管服务器上配置软件。托管服务器上的其他操作遵循相同的常规协议：

1. 数据访问引擎打开通过 HTTPS 连接到 SA 服务器代理的通信通道，指示该代理执行管理任务。
2. SA 代理回调数据访问引擎，以检索有关要执行的任务的具体信息。要打开通信通道，代理必须提供其公钥证书，即 SA 核心将用于验证内部数据库是否映射证书本身到该计算机的 IP，它是安装此代理时 SA 生成的唯一计算机标识符。这一保护可防止用户将数字证书和相应密钥简单地复制到另一个想要假扮成原始托管服务器的计算机。

成功打开通信通道后，SA 代理会收到要安装和删除的软件（以及任何要执行的脚本、软件安装顺序和配置过程期间何时重新启动）的准确列表。

3. SA 代理打开通往软件数据库的通信通道（还通过 HTTPS），请求下载它需要安装的软件。在软件数据库启动下载之前，它会重新计算该包的 SHA 校验和以及它所知的密钥。只有当 SHA 校验和与上载数据包时生成的校验和相匹配时，SA 代理才会收到它请求的软件。

代理启用的对 SA 核心的异步调用为进度报告和长时间运行的操作提供了可扩展的支持，因为 SA 核心不需要直接管理数以千计的同步代理操作。即使是在防火墙阻止代理启动 TCP 连接的网络环境中，SA 也支持这些从代理到核心的异步调用，这是因为 SA 网关基础结构可通过单向连接提供双向隧道连接。

代理/核心通信的其他技术详细信息包括：

- 连接是 SSL v3，则与 X.509 证书进行相互验证（服务器检查此客户端证书，反之亦然）。
- 核心和代理证书的私钥存储在只有 root 可读取的文件中。
- 所有证书都在安装时生成，由客户拥有，对于 HP 是未知的。
- 证书在安装 10 年后到期。SA 提供了重新认证工具，以便在证书到期之前重新认证核心和代理。
- 证书由 SA 内部自签名证书颁发机构签名。要避免在 Web 浏览器中出现 HTTPS 安全警告，客户可在 Apache SA 实例中安装外部签名的证书。

SA 核心间的通信

如果您跨多个数据中心运行 SA，SA 会自动在所有 SA 管理的数据中心中同步相关数据。从广义上讲，SA 同步两种数据：服务器（包括所有硬件、软件和配置特性信息）和软件包自身的 SA 模型。

- **复制 SA 模型**：SA 使用集成认证的消息来同步 SA 模型数据。SA 实现 SSL 来确保跨消息总线流动的消息的安全。实际消息自身描述在通信接收结束时需要对 SA 数据库进行的 SQL 更改。
- **复制软件包**：SA 按需复制软件包。也就是说，仅在需要时复制软件包。当在新泽西州数据中心管理服务器的管理员指示 SA 安装新泽西州软件数据库中不存在的软件包时，SA 会从另一个数据中心请求该软件包。实际文件传输使用开放源实用程序 rsync，使用 SSH 确保通信通道的安全。

SA 卫星体系结构和安全性

可以将 SA 卫星（而不是整个 SA 核心）安装在次要位置以启用对远程服务器的管理。卫星提供与 SA 核心相同的针对数据中心服务器的无缝管理。卫星由 SA 网关和软件数据库缓存组成。卫星网关为卫星提供网络连接和带宽管理。卫星可以包含多个网关。软件数据库缓存包含要安装在该卫星端托管服务器上的软件包的本地备份。（可选）卫星可以包含 OS 配置启动服务器和介质服务器组件。卫星必须至少链接到一个核心，该核心可以是单一核心或多主控网状网络的一部分。多个卫星可以链接到单一核心。

卫星具有下列主要功能：

- **自动执行（无论网络复杂性如何）**：卫星经过优化，可以跨低带宽连接、通过复杂的重叠 IP 地址空间和跨防火墙边界工作。
- **响应网络失败**：SA 卫星实现复杂链接状态路由算法，该算法针对失败的网络链接启用动态路由，以实现冗余。
- **确保远程服务器安全性**：卫星端使 IT 组织能够通过基于策略的修补程序管理、已数字签名和加密的程序包安装、跟踪完整服务器更改历史记录的全面审核跟踪，主动确保远程服务器安全性。

SA 网络：使风险降低

持续报告新的漏洞。SA 网络是独特的服务，为您的 SA 安装提供可操作、多供应商、按优先顺序排列的安全警报。使用 SA 网络，您可以在了解到漏洞时识别漏洞，无需使用额外的资源即可部署相应的修补程序。

由于认识到没有一个标准可以覆盖所有需求，SA 网络提供了符合性策略的广泛集合，该集合可轻松自定义且可扩展以满足每个客户的特定需求。

SA 网络当前关注下列三个符合性标准：

- **Center for Internet Security (CIS) 标准**：一组标准，详述了如何根据操作系统确保服务器的安全。(*http://www.cisecurity.org/*)
- **Microsoft (MS) 安全指南**：Microsoft 建立的标准，详述了加强 Windows 服务器的配置设置。(*http://www.microsoft.com/*)
- **国家安全局 (NSA) 安全配置指南 (SCG)**：美国国家安全局建立的标准，详述了加强不同 OS 和应用程序的配置设置。(*http://www.nsa.gov/*)

SA 与其他安全工具的兼容性

SA 对许多现有安全工具（例如入侵检测系统、漏洞评估套件、防病毒扫描程序、完整性确保产品）进行了补充。SA 可用来推动更改管理实践，使这些工具为服务器提供有效保护。具体而言，SA 可用来一致地安装和配置这些系统所需的代理，保持配置（如最新防病毒定义文件）最新，对这些系统报告的一些漏洞（如缺少的修补程序或错误的配置）采取措施。

SA 核心重新认证

SA 提供*核心重新认证工具*，支持您重新认证 SA 核心和代理。核心重新认证工具自动进行并加速发行新安全证书的过程。

备注: 此工具区别于现有代理重新认证工具，又与其兼容。有关详细信息，请参见代理重新认证。

核心重新认证工具的主要优点有:

- 能够在所有 SA 证书到期之前重新生成这些证书，从而有效缩短了它们的寿命。
- 能够减少证书受到危害。

SA 是一个闭合公钥基础结构 (PKI) 系统，它使用 X.509 v3 证书为身份验证、授权提供便利和确保网络通信的安全。X.509 证书是将指定主体与公钥绑定的一种标识形式。

证书与其相应的私钥一起构成了数字标识。像许多其他形式的标识一样，证书的有效期为固定时间。X.509 证书的有效期是通过 `Not Before` 和 `Not After` 日期指定的。只有在当前日期处于给定 X.509 证书有效期内的情况下，才将该证书视为有效。相反，如果当前日期超出给定 X.509 证书的有效期，则将该证书视为无效。SA 不接受无效证书。

SA CA 在启动时自动生成，之后用于颁发核心组件证书的其余部分。SA 代理证书由代理 CA 在初始代理注册时颁发。

默认情况下，所有 SA 证书的有效期为 10 年。不能通过配置更改 SA 证书的寿命。更改 SA 证书策略的唯一方法是通过自动化。

SA 使用*类证书*，即一个类的所有核心组件都共享一个证书。例如，所有命令引擎共享一个命令引擎证书。威胁一个命令引擎证书意味着所有命令引擎证书都受到威胁。而且，SA 不支持*证书吊销*。使受到威胁的核心组件证书失效的唯一方法是重新认证整个核心。

备注: 此发布的核心重新认证工具不支持自定义核心安装。任何已在 SA 安装程序领域外完成的自定义（要求某些 SA 证书和密钥位于另一个主机或另一个目录中）将不受此工具支持。

代理与核心重新认证

代理与核心重新认证之间有很大区别。核心重新认证重新生成核心的证书和所有托管服务器上的所有代理证书。代理重新认证仅重新生成托管服务器上的代理证书。

本节描述完整核心重新认证。有关仅重新认证托管服务器上的代理的说明，请参见代理重新认证。

核心重新认证后升级

核心重新认证不会更新所有核心上的加密数据库 (CADB)。只有第一个核心具有最新 CADB。您可以通过在执行重新认证的核心的 `/opt/opsware/oi_util/OpswareCertTool/recert_utils/` 中运行以下命令

```
./corerecert --status
```

来确定第一个核心。

在升级到更新的 SA 发布或修补程序之前，必须执行下列操作:

1. 将 CADB (`/var/opt/opsware/crypto/cadb/realm/*`) 从第一个核心复制到要升级的核心服务器上的相同目录中。
2. 在要升级的核心服务器上，发出以下命令：

```
rm -rf /var/opt/opsware/crypto/oi
rm -rf /var/opt/opsware/crypto/gateway
rm -rf /var/opt/opsware/crypto/dhcp
rm -rf /var/opt/opsware/crypto/word_upload
```

向重新认证的 SA 核心多主控网状网络添加新核心

核心重新认证过程不会对模型库 (truth) 数据重新签名，在操作期间，会加载旧的/存档 CA 和新 CA 来验证签名。

在向重新认证的网状网络添加新核心时，必须将所有旧的/存档 CA 手动复制到新核心。

核心重新认证阶段

核心重新认证有多个阶段。所需的阶段取决于您的多主控配置。

表 13 描述了核心重新认证阶段：

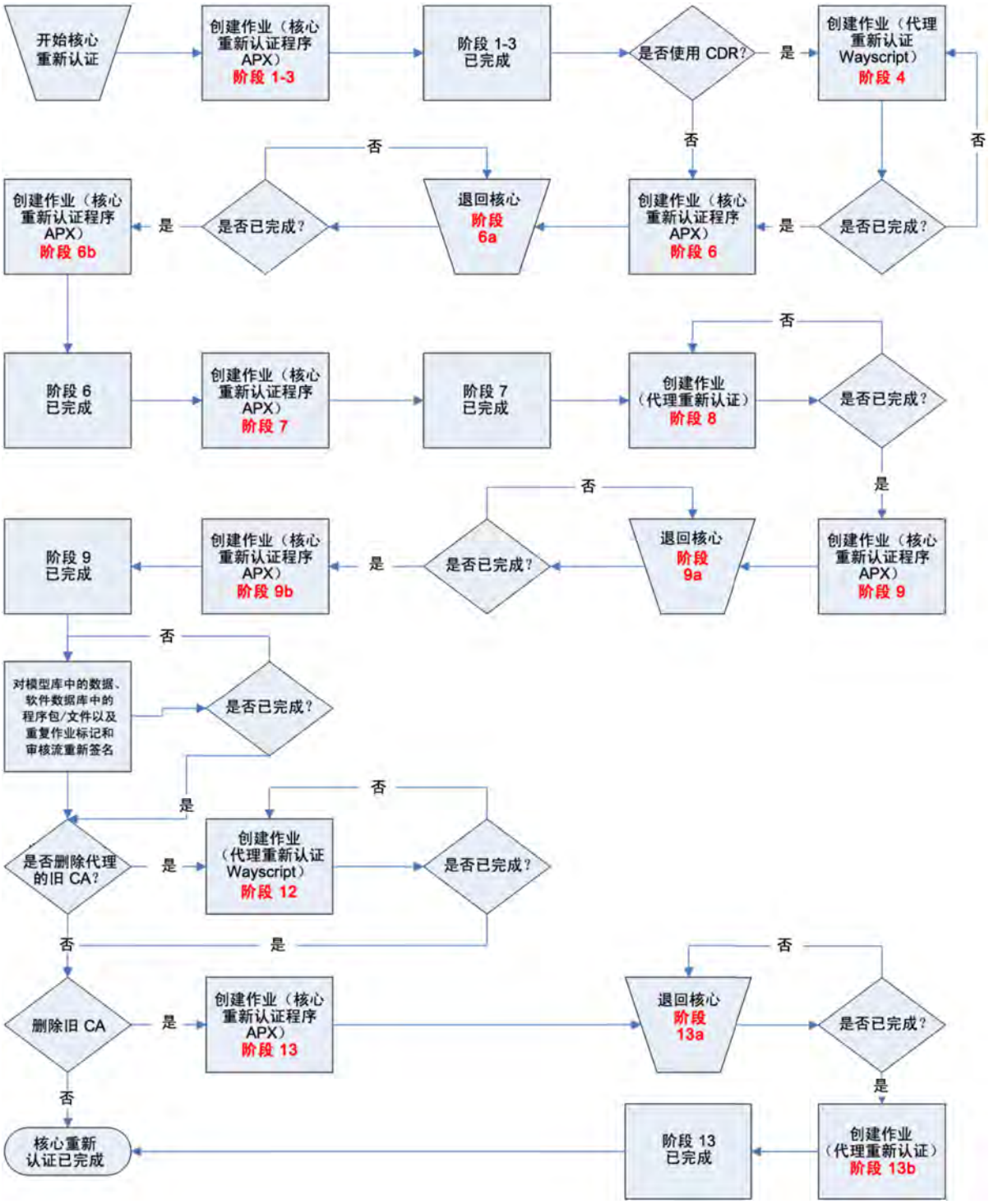
表 13.核心重新认证阶段

阶段	**描述**
1-3	备份现有加密材料，生成新加密材料，将新 CA 分发到所有核心组件。这三个阶段在核心重新认证工具第一次运行期间按顺序进行。所有现有加密材料都备份到 `crypto.<session number>` 目录。每个核心组件具有其自己的备份目录。 如果缺少，请创建 /etc/opt/opsware/crypto/security.conf。更新现有的 /etc/opt/opsware/crypto/security.conf。
4	将新代理 CA 分发给所有代理，以便代理同时信任新代理 CA 和旧代理 CA。这是为了确保代理与代理之间的通信不中断。 **注意**：如果 corerecert.conf 文件中的 agent_recert.using_cdr 参数值为零 (0)，则跳过此阶段（阶段 4）。HP 建议将 agent_recert.using_cdr 参数设置为零 (0)，因为 CDR 功能已不再受支持。
6a	**网状网络重新启动**：重新启动网状网络，以便它信任新的和旧的 CA 层次结构。
6b	**启动计划的网状网络重新启动**：使用配置文件参数，您可以计划适用于您的维护窗口的多主控网状网络重新启动的延迟启动。
7	重新认证网关。

阶段	描述
8	重新认证代理。 **注意**：确保整个阶段 8 中所有托管服务器都正常工作并且可访问，否则在核心重新认证进程完成后，核心将无法与服务器通信。
9a	重新认证核心组件；在第一个核心上发出命令 `touch /var/opt/opsware/crypto/twist/upgradeInProgress`；网状网络重新启动；重新生成签名。
9b	检查网状网络重新启动状态。如果网状网络已成功重新启动，则所有核心组件现在使用新的加密材料，同时仍信任旧的加密材料。
11	对模型库中的数据、软件数据库中的程序包/文件以及重复作业标记和审核流重新签名。
12	[*可选*] 删除旧代理 CA。仅当代理 CA 已受到威胁或者您不再信任旧 CA 时才需要。 **注意**：当某托管服务器同时有较旧和较新 CA 在代理重新认证阶段（阶段 8）没有重新认证时，该服务器将不能够与仅有较旧 CA 的另一托管服务器通信。 **注意**：对于使用自定义证书的核心重新认证，HP 建议通过阶段 12 从代理信任的 CA 存储删除旧证书，因此认证将仅使用客户证书。
13a	[*可选*] 删除旧代理 CA 层次结构。仅当代理 CA 已受到威胁或者您不再信任旧 CA 层次结构时才需要。 **注意**：当某托管服务器同时有较旧和较新 CA 在代理重新认证阶段（阶段 8）没有重新认证时，该服务器将不能够与仅有较旧 CA 的另一托管服务器通信。 **注意**：对于使用自定义证书的核心重新认证，HP 建议通过阶段 13 从信任的 CA 存储删除旧核心组件证书，因此认证将仅使用客户证书链
13b	[*可选*] 网状网络重新启动。仅当也需要 13a 时才需要。

图 22 显示了重新认证流程的流和阶段：

图 22.核心重新认证阶段和流



代理重新认证阶段

图 22 中描述的三个阶段是**代理重新认证阶段**：

- **阶段 4**：分发新代理 CA。此阶段的目的是确保代理与代理的连续通信（已重新认证的代理与尚未重新认证的代理进行的通信）。
- **阶段 8**：重新认证代理。这是*必需*阶段。此阶段的目的是将新的加密材料发布到代理。
- **阶段 12**：清理旧代理 CA。此阶段是*可选的*。如果您不想同时信任旧的和新的 CA 层次结构，则必须使用此阶段删除旧 CA。否则，可以跳过此阶段。

代理重新认证作业

每个代理重新认证阶段都由重复作业完成。此作业受**表 14** 中所示的下列属性控制（您必须在核心重新认证配置文件中指定这些属性）：

表 14.核心重新认证配置文件：代理重新认证属性

属性名称	是否必需？	描述	示例
agent_recert.all.facilities.start_time=<HH:mm>	是	代理重新认证阶段的开始时间。您可以通过指定 agent_recert.facility.<facility name>.start 属性覆盖给定设施的该值。 开始时间必须采用以下格式： HH:mm，其中 00 <= HH < 24 且 00 <= mm < 60。 只需要小时和分钟组件。如果指定的时间已经过，则代理重新认证作业将在第二天的指定时间启动。	agent_recert.all.facilities.start_time=18:30
agent_recert.facility.<facility_name>.start_time=<HH:mm>	否	如果已提供，则使用给定设施的开始时间，不使用 agent_recert.all.facilities.sta-	agent_recert.facility.sacramento.start_time=8:00

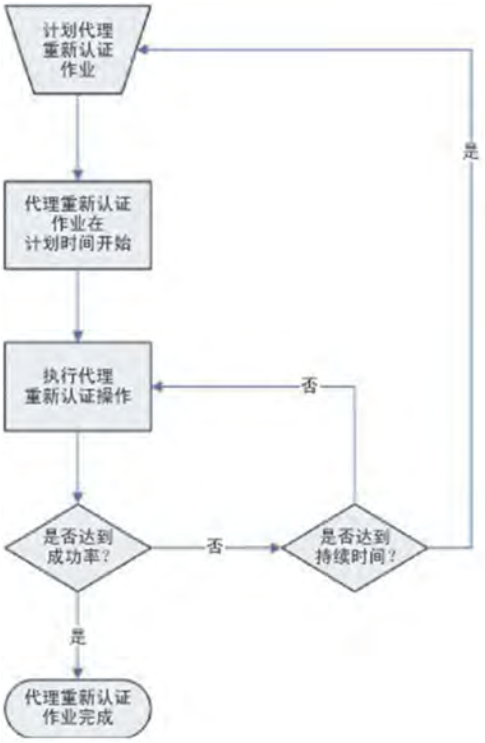
属性名称	是否必需？	描述 rt_ time。	示例
agent_recert.all. facilities.duration=- <hours>	是	代理重新认证作业的持续时间（以小时为单位）。持续时间决定了代理重新认证作业停止之前运行的时间。如果持续时间已过，而尚未达到成功率，则代理重新认证作业将在下次开始时继续。您可以通过指定 agent_ recert. facility. <facility_ name>. duration 属性覆盖给定设施的该值。 持续时间必须是 1 到 24 之间的整数。	agent.recert.al- l. facilities.durat- ion=8
agent_recert. facility.<facility_ name>.duration= <hours>	否	如果已提供，则使用给定设施的持续时间，不使用 agent_ recert.all. facilities.dur- ation	agent_ recert.facility. sacramento.durat- ion=10
agent_recert.all. facilities.success_ rate= <whole percentage>	是	代理重新认证作业的每个设施的成功率（全百分比）。例如，如果设施 X 中有 1000 个托管服务器 且成功率为 98%，则如果已成功重新认证 980 个托管服务器，代理重新认证作业将停止。	agent_ recert.all. facilities.succe- ss_rate= 100

属性名称	是否必需？	描述 您可以通过指定 agent_recert.facility.<facility_name>.success_rate 属性覆盖给定设施的该值。 成功率必须是 1 到 100 之间的整数。	示例
agent_recert.facility.<facility_name>.success_rate=<whole percentage>	否	如果已提供，则使用给定设施的成功率，不使用 agent_recert.all.facilities.success_rate。	agent_recert.facility.sacramento.success_rate=99
agent_recert.all.facilities.job_notification=<email addresses>	否	代理重新认证作业的作业通知。您可以通过指定 agent_recert.facility.<facility_name>.job_notification 属性覆盖给定设施的该值。	agent_recert.all.facilities.job_notification=admin@example.com
agent_recert.facility.<facility_name>.job_notification=<email addresses>	否	如果已提供，则使用给定设施的作业通知，不使用 agent_recert.all.facilities.job_notification。	agent_recert.facility.sacramento.job_notification=admin3@example.com
agent_recert.using _cdr	否	表示正在利用代码部署和回滚 (CDR) 功能。默认为 1。 **注意**：HP 建议将此参数设置为零 (0)，因为 CDR 功能已不再受支持。	agent_recert.using _cdr=0

代理重新认证作业流程

图 23 显示了代理重新认证作业流程：

图 23.代理重新认证作业流程



在任意给定时间，每个设施只能有一个代理重新认证作业（计划或活动作业）。仅当发生以下情况时，代理重新认证作业终止：

- 已达到成功率
- 您明确取消作业
- 发生致命错误

SA 核心重新认证工具用法

要运行核心重新认证工具，请输入以下命令：

```
/opt/opsware/oi_util/OpswareCertTool/recert_utils/corerecert [--
phase <phase number>] [--config <complete path to the config
file>] [--doit]] [-h, --help] [-v, --version] [-s, --status] [-d,
--debug] [--summary] [--cancel_all_agent_recert_jobs] [--cancel_
agent_recert_jobs_for_facility <facility name>] [--cancel_all_
jobs] [--reason <reason for job cancellation>] [--force_resume
<facility_name>]
```

核心重新认证工具的参数

表 15 描述了核心重新认证工具的有效参数：

表 15.核心重新认证工具参数

参数	描述
`-h, --help`	显示帮助。
`--phase`	开始指定的核心重新认证阶段。有效阶段编号为 1、4、6、7、8、9、12 和 13。
`--config <config file>`	核心重新认证配置文件的完全限定路径。默认配置文件是 `/opt/opsware/oi_util/OpswareCertTool/recert_utils/corerecert.conf`。
--doit	重新运行或者强制重新运行给定的核心重新认证阶段。这在某些新添加的组件错过重新认证过程时非常有用。它还用于跳过指定的阶段，例如新代理 CA 推送或旧代理 CA 删除。
`-v, --version`	打印 `corerecert` 可执行文件的版本号。
-s, --status	显示重新认证过程的当前状态。
-d, --debug	将核心重新认证设置为调试模式，`/tmp/recerttool.log` 中提供了调试日志。
--summary	打印当前状态摘要，`--status` 的简短版本。
--cancel_all_agent_recert_jobs	取消所有当前计划的代理重新认证作业。
--cancel_agent_recert_jobs_for_facility <facility name>	取消针对给定设施计划的代理重新认证作业。
--cancel_all_jobs	取消所有核心和代理重新认证作业。
--reason <reason for job cancellation>	指定作业取消的可选原因。
`--force_resume <facility_name>`	指定为任何包含失败代理重新认证作业的设施自动计划新作业。将跳过不包含失败作业的设施。或者，如果没有指定此参数，可以单独为每个设施恢复作业。

警告: 不建议在核心重新认证期间添加新核心组件。虽然在某些情况下可以在核心重新认证期间添加新核心组件（例如切分组件捆绑包、卫星端等），但除非有绝对必要，否则 HP 不建议这样做。*如果您要在核心重新认证期间添加新核心组件，则必须先联系 HP 专业服务人员*。

警告: 不支持替换将 SA 证书替换为第三方证书（不是由 SA CA 颁发的证书）。在核心重新认证期间，如果第三方证书的文件名与 SA 证书相同，则第三方证书将被覆盖。如果您已将任何 SA 证书替换为第三方 CA 颁发的证书，则应当先联系 HP Server Automation 支持人员，然后再执行核心重新认证。

安全注意事项

请考虑下列安全问题:

加密数据库文件

SA 核心重新认证工具需要在重新认证期间访问 SA 加密数据库文件。

SA 加密数据库包含以下文件:

`/var/opt/opsware/crypto/cadb/realm/opsware-crypto.db.e`

此文件受加密材料密码 (`decrypt_passwd`) 保护，该密码是在网状网络的首次核心安装时指定的。在后续核心安装期间，此文件还将复制到新的次要核心主机。必须保护好这个密码，因为威胁加密数据库文件就意味着威胁您的整个多主控网状网络。

只有在 SA 安装或升级时才需要加密数据库文件，但是在核心重新认证期间会重新生成它。因此，HP 强烈建议您创建保护加密数据库文件的过程。所以，在核心重新认证之前，必须将该文件备份到安全位置。

在核心重新认证期间，SA 仅在您调用核心重新认证工具的主机上重新生成加密数据库。在重新认证期间，核心重新认证不将新生成的加密数据库文件复制到网状网络中的任何其他主机。您还应当在核心重新认证刚完成时将该文件备份到安全位置。

严格控制对核心主机的 root 访问也同样重要。核心主机上的加密材料（证书及其对应的私钥）未加密。它们受 root 用户帐户保护。也就是说，这些文件受 root 用户的只读访问权保护。因此，对核心主机具有 root 访问权意味着用户对加密材料密码和加密数据库文件具有访问权，并且核心重新认证只应由 SA 系统管理员或对核心主机具有合法 root 访问权的人员执行。

核心重新认证用户

通常有三种用户将使用 SA 核心重新认证工具:

- **核心重新认证用户**：此用户具有运行核心重新认证工具的所有必需权限。在所有实际用途中，这是与 SA 系统管理员/操作员相同的用户。
- **SA 管理员**：将 SA 核心重新认证角色授予核心重新认证用户或吊销该角色。

- SA **系统管理员/操作员**：此用户负责重新启动给定的核心。此用户没有核心主机的 root 访问权。

创建核心重新认证用户

为了授予核心重新认证工具，您必须创建 Core Recertification 组和用户，并授予必需的权限：

1. 以 SA 管理员身份登录 SA 命令中心。
2. 创建具有下列权限的 *Core Recertification 用户组*：
   - 所有设施的读取和写入访问权限
   - 所有客户的读取和写入访问权限
   - 所有设备组的读取和写入访问权限
   - 管理客户
   - 管理设施
   - 管理服务器和组
   - 操作权限 > 类别（核心重新认证 > 核心重新认证）
   - 操作权限 -> 核心重新认证） -> 操作的代理重新认证
   - 核心重新认证（“客户端”>“核心重新认证”）
   - 代理重新认证（“客户端”>“代理重新认证”）
3. 将核心重新认证用户添加到 SA System Administrators 用户组。
4. 列出并执行 Library/Tools/Administrative Extensions 文件夹的文件夹权限。

删除核心重新认证用户

要删除核心重新认证用户，请执行以下任务：

1. 以 SA 管理员身份登录 SA 命令中心。
2. 从 `Core Recertification` 用户组删除用户。

核心重新认证先决条件

在开始核心重新认证之前，必须执行下列任务：

- 选择新密码以保护加密材料，并决定如何提供该密码。
- 使用正确的值配置核心重新认证配置文件。
- 确保所有核心已开启并正在运行。
- 确保核心重新认证工具正确识别您的网状网络设置。
- 通过在调用核心重新认证前对所有托管服务器运行通信测试来检查所有托管服务器的可访问性。

选择新密码以保护加密材料

核心重新认证期间，需要加密数据库密码以保护新生成的加密数据库、PKCS #12 文件和 CA 私钥。核心重新认证由多个阶段组成，大多数阶段都需要加密数据库密码。保护加密

数据库密码非常重要。

警告: 某些核心重新认证任务由自动化平台扩展 (APX) 作业完成。因此，加密数据库密码（虽然有所混淆）会短暂出现在作业参数或作业审核日志中。

为了避免加密数据库密码出现在作业参数或审核日志中，您可以按照下列过程使用文件传送加密数据库密码：

1. 在核心主机上调用核心重新认证工具之前，确定核心主机的服务器 ID。可以从 SA Web 客户端中或者通过在 `/etc/opt/opsware/agent/mid` 中查找来获取服务器 ID。您必须在核心重新认证配置文件中指定 `base_core_server_ref` 的服务器 ID 值。
2. 创建包含新加密数据库密码的文件 `/var/opt/opsware/crypto/cadb/__recert_overwrite__`。例如，`cadb_password=<new crypto database password>`。确保该文件对于 root 用户是只读的。
3. 在核心重新认证成功完成后，删除 `/var/opt/opsware/crypto/cadb/__recert_overwrite__` 文件。

由于核心重新认证配置文件中需要加密数据库密码，因此作为安全措施，您可以在该文件中指定一个无效密码。

核心重新认证仅允许使用一个密码来保护所有加密材料。这些材料包括加密数据库、PKCS #12 文件和所有 CA 私钥。如果您正在运行 `OpswareCertTool` 的自定义版本（其中加密材料受多个密码保护）并希望继续运行，则*在运行核心重新认证工具之前必须联系 HP 专业服务人员*。

配置核心重新认证

必须在配置文件中指定所有核心重新认证属性。当调用核心重新认证工具时，可以使用 `-config` 参数指定配置文件的位置。如果忽略 `-config` 参数，则核心重新认证工具使用 `/opt/opsware/oi_util/OpswareCertTool/recert_utils/corerecert.conf` 中的默认配置文件。

您可以直接编辑默认配置文件，也可以创建新配置文件。由于配置文件包含敏感信息，相应地保护该文件是十分重要的。例如，确保只有 root 用户可以读取和写入该文件：

对于 SA 9.1x 或 10.0x 到 SA 10.2 的核心环境升级，核心或卫星端 /etc/opt/opsware/crypto/security.conf 文件仅在核心重新认证进程期间生成。

对于 SA 10.1 到 SA 10.2 的核心环境升级、全新安装 SA 10.01 或全新安装 SA 10.2，/etc/opt/opsware/crypto/security.conf 文件已经生成。

HP 不支持手动创建 /edit /etc/opt/opsware/crypto/security.conf 文件。

表 16 中所列的参数可以在 corerecert.conf 文件中找到。部分这些参数（fips_enabled 值、密钥大小、签名算法和自定义 CA）表示核心的值，也可以在 security.conf 文件中找到。

表 16.核心重新认证配置文件：属性

属性名称	是否必需？	描述	示例
全局属性			
username=<username>	是	有权执行核心重新认证操作的用户的用户名。	username=jdoe
password=<password>	是	有权执行核心重新认证操作的用户的密码。	password=dontask
代理重新认证属性			
agent_ recert.cleanup_old_ agent_ca= <0 | 1>	否	指示在核心重新认证后是否清理旧代理 CA。旧代理 CA 阶段不需要清理，可以禁用。 有效值为 1 (true) 或 0 (false)。任何其他值将导致无效属性错误。 这是可选属性。默认值：0。 **注意**：如果指定 custom_ca，则 HP 建议 agent_ recert.cleanup_old_agent_ca 参数应设置为 1，以便只信任可用的客户证书。	agent_ recert.cleanup_ old_ agent_ca=0
agent_recert.all. facilities. start_time= <YYYY:MM:DD:HH:mm>	是	所有设施的代理重新认证操作的默认开始时间。 您可以覆盖指定设施的该值（通过使用 agent_recert. facility. <facilityname>.start 属性指定默认设施开始时间）。 开始时间必须采用以下格式： YYYY:MM:DD:HH:mm，其中 2008 <= YYYY <=9999, 0 < MM <= 12, 0 < DD <= 31, 0 <= mm < 12 且 0 <= MM < 60。	agent_ recert.all. facilities.star t_time= 2009:02:15:23:00
agent_recert. facility.<facility name>.start_time	否	可以通过指定此属性覆盖给定设施的默认设施开始时间。 开始时间必须采用以下格式： YYYY:MM:DD:HH:mm，其中 2008 <= YYYY <=9999,	agent_ recert.facility. yellow.start_ time= 2008:05:01:10:00

属性名称	是否必需？	描述 0 < MM <= 12，0 < DD <= 31，0 <= mm < 12 且 0 <= MM < 60。	示例
agent_recert.all.facilities.duration=<HH>	是	所有设施中代理重新认证操作的默认持续时间（以小时为单位）。 持续时间必须是 1 到 24 之间的整数。 您可以通过指定 agent_recert.facility.<facility name>.duration 属性覆盖给定设施的持续时间	agent_recert.all.facilities.duration=2
agent_recert.facility.<facility name>.duration=<HH>	否	覆盖指定设施的默认持续时间。	agent_recert.facility.yellow.duration=10
agent_recert.all.facilities.success_rate=<%>	是	所有设施中代理重新认证操作的默认成功率（以全百分比表示）。 您可以通过指定 agent_recert.facility.<facility name>.success_rate 属性覆盖特定设施的该值	agent_recert.all.facilities.success_rate=50
agent_recert.facility.yellow.success_rate=<%>	否	覆盖给定设施的默认成功率。	agent_recert.facility.yellow.success_rate=98
agent_recert.all.facilities.job_notification=<email_address>	否	代理重新认证操作的默认作业电子邮件通知。 可以通过指定 agent_recert.facility.<facility name>.job_notification 属性覆盖特定设施的默认作业电子邮件通知	agent_recert.all.facilities.job_notification=admin@example.com
agent_recert.	否	覆盖特定设施的默认作业电子	agent_

属性名称	是否必需？	描述	示例
facility. <facility name>. job_notification= <email_address>		邮件通知。	recert.yellow. job_ notification= saadmin@example. com
核心重新认证属性			
cadb_password=<pswd>	是	用于保护新生成的加密数据库的密码。	cadb_ password=crypto1 23
debug=<0 | 1>	否	指定是否在调试模式下运行核心重新认证作业。它可以是 1 (true) 或 0 (false)。 可以在调用核心重新认证的核心计算机上找到调试日志： /var/log/opsware/waybot/rec-ert.log。 默认设置：0。	debug =1
fips_enablement	否	表示网状网络和卫星端的 FIPS 启用情况。默认为使用 /etc/opt/opsware/crypto/security.conf 中的值。如果此值未设置或不能读取，则默认值为零 (0)。如果将 fips_enablement 值设置为 1（启用），则 signing_algorithm 值必须为 sha1。值为：1（FIPS 已启用）和 0（FIPS 已禁用）。 **注意**：启用 FIPS 要求 SA AGENTS 版本 10.1 和更高版本。如果使用核心重新认证进程，您可以从 SA 9.1x 或 10.0x 升级到 SA 10.20 并启用 FIPS 支持。	fips_ enablement=0
base_core_server_ ref=<n>	否	从其启动核心重新认证的主机的服务器引用。	base_core_ server_ref=10010
job_schedule= <YYYY:MM:DD:HH:mm>	否	当前核心重新认证阶段作业的作业计划。它必须采用以下格式：YYYY:MM:DD:HH:mm,	job_schedule= 2009:02:12:23:05

属性名称	是否必需？	描述	示例
		其中2008 <= YYYY <=9999, 0 < MM <= 12, 0 < DD <= 31, 0 <= HH < 12, and 0 <= mm < 60。 如果未指定此属性，则作业立即开始。	
job_ schedule.gateway_ recert. <facility name>= <YYYY:MM:DD:HH:mm>	否	给定设施的网关重新认证阶段的作业计划。它必须采用以下格式：YYYY:MM:DD:HH:mm，其中2008 <= YYYY <=9999, 0 < MM <= 12, 0 < DD <= 31, 0 <= HH < 12, and 0 <= mm < 60。 如果未指定此属性，则使用网关重新认证阶段的 job_ schedule 属性。	job_ schedule.gatewa y_ recert.<facility name>= 2009:02:12:23:05
keysize	否	keysize 参数为用于验证证书的公共密钥指定密钥长度，以字节为单位。默认为当前 SA 证书中的值。如果也使用了 custom_ca，且已设置值，则该值必须符合 custom_ca 中的 keysize 值。值为：2048 和 4096。	keysize=2048
job_notification= <email_address>	否	所有核心重新认证阶段作业的作业通知。 您可以通过指定 job_ notification. <phase_number> 属性覆盖给定阶段的该值。	job_ notification= admin@example.co m>
job_notification. <phase_number>= <email_address>	否	指定核心重新认证阶段的作业通知。	job_ notification.7= saadmin@example. com
job_notification.	否	给定设施的网关重新认证阶段的作业通知。	job_

属性名称	是否必需？	描述	示例
gateway_recert.<facility name>=<email_address>			notification.gateway_recert.yellow=admin@acme.com
cleanup_old_opsware_ca=<0 | 1>	否	指定是否在核心重新认证后清理旧 SA CA。 除非 SA CA 受到威胁，否则不需要清理该 CA。在大多数情况下，不需要旧 SA CA 清理，应当将其禁用。 有效值为 1 (true) 或 0 (false)。任何其他值将导致无效属性错误。 默认值：0 (false) **注意**：HP 建议参数应设置为 1，以便只信任可用的客户证书。	cleanup_old_opsware_ca=1
custom_ca	否	符合自定义证书要求的有效自定义证书文件的完整路径。如果将此参数值设置为有效证书颁发机构的路径，则默认行为是核心重新认证使用该值生成 SA 使用的所有自签名（特定于客户）证书。核心重新认证使用 custom_ca 参数的值或 signing_algorithm 参数的值。另外，请注意以下情况：包含证书的文件也必须包括级联的私钥。如果 fips_enablement 设置为 1，custom_ca 必须具有相符的 signing_algorithm 和 keysize 值。如果值冲突，则您将会看到错误消息。 **注意**：启用 FIPS 要求 SA AGENTS 版本 10.1 和更高版本。如果使用核心重新认证进程，您可以从 SA 9.1x 或 10.0x 升级到 SA 10.20 并启用 FIPS 支持。 有效值为自定义证书的完整路径。	custom_ca=/tmp/custom-ca.crt

属性名称	是否必需？	描述	示例
signing_algorithm	否	signing_algorithm 参数用于在提供了支持的 keysize 值时生成证书签名。如果也使用了 custom_ca，且已设置 signing_algorithm 值，则此值必须符合 custom_ca 中签名算法的值。默认为现有 SA 证书中的值。值为：“sha1”和“sha256”。仅当核心现有证书是基于 md5 时，可选支持 md5。	signing_ algorithm=sha1

注意：在核心重新认证期间，会比较 corerecert.conf 文件和 security.conf 文件中的值。security.conf 文件（作为核心重新认证进程的一部分而生成）包含 signing_algorithm 值和 keysize 值。如果两个文件中的值冲突，则进程会显示消息，询问您是否覆盖 security.conf 文件中的值。如果输入“y”，则 SA 使用 corerecert.conf 文件中的值替换 security.conf 文件中的值。如果不想覆盖值，请输入“n”。核心重新认证将退出，security.conf 文件中的现有值保持不变。

确保所有核心都在运行/解决冲突

在执行核心重新认证之前，强烈建议在所有要重新认证的核心上运行系统诊断，以确保它们运行正常。您还应当使用多控制工具检测和解决任何事务冲突。有关详细信息，请参见运行系统诊断和解决网状网络冲突 - SA 客户端。

确保核心重新认证工具正确识别网状网络设置

您必须执行下列任务，以确保核心重新认证工具正确识别多主控网状网络设置：

1. 从命令行，以 root 用户身份登录 SA 核心主机。
2. 运行

   ```
   /opt/opsware/oi_util/OpswareCertTool/recert_utils/discover_mesh -p
   ```

3. 检查输出以确保它反映您当前的网状网络设置。如果未反映您当前的网状网络设置，请在继续核心重新认证之前联系 HP 专业服务人员。

重新认证 SA 核心

备注： 在启动核心重新认证之前，必须清除多主控网状网络上的所有后备日志和冲突。

要重新认证 SA 核心，请执行下列任务：

1. 确保您已归类为核心重新认证用户。如果不是这样，请咨询您的 SA 系统管理员。

2. 登录 SA 核心主机。
3. 将目录更改为 /opt/opsware/oi_util/OpswareCertTool/recert_utils/。
4. 编辑：

   ```
   corerecert.conf
   ```

   以确保环境信息正确。
5. 运行：

   ```
   corerecert --status
   ```

   以确保核心重新认证当前未进行。
6. 运行：

   ```
   discover_mesh -p
   ```

   以确保核心重新认证工具可以正确检测您的网状网络设置。
7. 从命令行运行：

   ```
   corerecert --phase 1
   ```

   以初始化核心重新认证。
8. 通过运行以下命令监控屏幕上的进度：

   ```
   corerecert --status
   ```

   直到屏幕上指示阶段 4 正在进行。
9. 运行：

   ```
   corerecert --phase 4
   ```

   以启动阶段 4，在该阶段，新的代理 CA 将附加到所有代理。

   注意：如果 corerecert.conf 文件中的 agent_recert.using_cdr 参数值为 0，则将跳过运行阶段 4 进程，且将在下一个阶段开始时开始进程。
10. 通过运行以下命令监控屏幕上的进度：

    ```
    corerecert --status
    ```

    直到所有代理已成功附加新代理 CA。

备注: 此步骤可能花费数日，具体取决于您的维护窗口和代理可用性。在任意给定时间，每个设施只能有一个计划的或活动的代理重新认证作业。如果您在此阶段遇到任何错误，请解决错误，然后返回运行： corerecert --phase 4以启动阶段 4，在该阶段，新的代理 CA 将附加到所有代理。 注意：如果 corerecert.conf 文件中的 agent_recert.using_cdr 参数值为 0，则将跳过运行阶段 4 进程，且将在下一个阶段开始时开始进程。。您只需要重新计划出现错误的设施，不需要重新计划成功设施的代理重新认证作业。

11. 运行：

    ```
    corerecert --phase 6
    ```

    以启动核心重新认证阶段 6。
12. 通过运行以下命令监控屏幕上的进度：

    ```
    corerecert --status
    ```

    直到屏幕上指示 `mesh_restart_pending`。

    此时，必须重新启动网状网络，请使用《SA 管理指南》的“SA 维护”部分中的重新启动指令和序列。

此步骤可能花费数日，具体取决于您的维护窗口。如果您在此阶段遇到任何错误，请确保解决错误，然后返回运行： corerecert --phase 6以启动核心重新认证阶段 6。 。

13. 网状网络成功重新启动后，从命令行运行：

    ```
    corerecert --phase 6
    ```

    以继续阶段 6。
14. 通过运行以下命令监控屏幕上的进度：

    ```
    corerecert --status
    ```

    直到阶段 7 应当启动。如果您在此阶段遇到任何错误，请确保解决错误，然后返回网状网络成功重新启动后，从命令行运行： corerecert --phase 6以继续阶段 6。 。

15. 运行：

    ```
    corerecert --phase 7
    ```

    以启动阶段 7。
16. 通过运行以下命令监控屏幕上的进度：

    ```
    corerecert --status
    ```

    直到阶段 8 应当启动。如果您在此阶段遇到任何错误，请确保解决错误，然后返回运行： corerecert --phase 7以启动阶段 7。 。

17. 运行：

    ```
    corerecert --phase 8
    ```

    以启动阶段 8，在该阶段，将重新认证所有代理。
18. 通过运行以下命令监控屏幕上的进度：

    ```
    corerecert --status
    ```

    直到已成功重新认证所有代理。

备注: 此步骤可能花费数日，具体取决于客户的维护窗口和代理可用性。在任意给定时间，每个设施只能有一个计划的或活动的代理重新认证作业。如果您在此阶段遇到任何错误，请解决错误，然后返回运行： corerecert --phase 8以启动阶段 8，在该阶段，将重新认证所有代理。 。您只需要重新计划出现错误的设施，不需要重新计划成功设施的代理重新认证作业。

19. 运行：

    ```
    corerecert --phase 9
    ```

    以启动阶段 9。核心重新认证工具提示您确认想要开始阶段 9。按 `y` 以继续。
20. 通过运行以下命令监控屏幕上的进度：

    ```
    corerecert --status
    ```

    直到屏幕上指示 `mesh_restart_pending`。如果您在此阶段遇到任何错误，请确保解决错误，然后返回运行： corerecert --phase 9以启动阶段 9。核心重新认证工具提示您确认想要开始阶段 9。按 y 以继续。 。

    此时，必须重新启动网状网络，请使用《SA 管理指南》的“SA 维护”部分中的重新启动指令和序列。

备注: 此步骤可能花费数日，具体取决于客户的维护窗口。如果您在此阶段遇到任何错误，请解决错误，然后返回运行： corerecert --phase 9以启动阶段 9。核心重新认证工具提示您确认想要开始阶段 9。按 y 以继续。 。您只需要重新计划出现错误的设施，不需要重新计划成功设施的代理重新认证作业。

21. 在基本切分核心服务器上：
    1. 发出以下命令：

       ```
       touch /var/opt/opsware/crypto/twist/upgradeInProgress

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

    2. 等待重新启动成功完成，然后
    3. 重新启动网状网络的其余部分。
22. 在网状网络成功重新启动后，重新认证用户必须从命令行运行：

    ```
    corerecert --phase 9
    ```

    以继续阶段 9。
23. 通过运行以下命令监控屏幕上的进度：

    ```
    corerecert --status
    ```

    直到阶段 11 应当启动。如果您在此阶段遇到任何错误，请确保解决错误，然后返回在网状网络成功重新启动后，重新认证用户必须从命令行运行：corerecert --phase 9以继续阶段 9。 。

24. 在基本切分核心服务器上：
    1. 发出以下命令：

       ```
       touch /opt/opsware/oi_util/OpswareCertTool/recert_
       utils/TruthResignStatus.txt /opt/opsware/oi_
       util/OpswareCertTool/recert_utils/WordResignStatus.txt
       ```

    2. 从命令行运行阶段 11：

       ```
       corerecert -phase 11
       ```

       以启动阶段 11，对模型库中的数据、软件数据库、重复作业以及审核流重新签名。
25. 通过运行以下命令监控屏幕上的进度：

    ```
    corerecert --status
    ```

    直到阶段 12 应当启动。如果您在此阶段遇到任何错误，请解决错误，然后返回步骤 24b。
26. 如果您不想删除代理 CA，请跳到运行： corerecert --phase 13 --doit以启动阶段 13。如果您不想删除旧 CA，则此阶段不需要网状网络重新启动。。否则，从命令行运行：

    ```
    corerecert --phase 12
    ```

    以启动阶段 12，在该阶段，将从所有代理删除旧代理 CA。

    注意：此时，必须重新启动网状网络，请使用《SA 管理指南》的“SA 维护”部分中的重新启动指令和序列。
27. 通过运行以下命令监控屏幕上的进度：

    ```
    corerecert --status
    ```

    直到已从所有代理中删除旧代理 CA。

备注: 此步骤可能花费数日，具体取决于客户的维护窗口和代理可用性。如果您在此阶段遇到任何错误，请解决错误，然后返回如果您不想删除代理 CA，请跳到运行： corerecert --phase 13 --doit以启动阶段 13。如果您不想删除旧 CA，则此阶段不需要网状网络重新启动。。否则，从命令行运行： corerecert --phase 12以启动阶段 12，在该阶段，将从所有代理删除旧代理 CA。注意：此时，必须重新启动网状网络，请使用《SA 管理指南》的“SA 维护”部分中的重新启动指令和序列。。您只需要重新计划出现错误的设施，不需要重新计划成功设施的代理重新认证作业。

注意：对于使用自定义证书的核心重新认证，HP 建议通过阶段 13 从信任的 CA 存储删除旧核心组件证书，因此认证将仅使用客户证书链。

28. 运行：

    ```
    corerecert --phase 13 --doit
    ```

    以启动阶段 13。如果您不想删除旧 CA，则此阶段不需要网状网络重新启动。

29. 通过运行以下命令监控屏幕上的进度：

    ```
    corerecert --status
    ```

    直到屏幕上指示 `mesh_restart_pend`。

    注意：此时，必须重新启动网状网络，请使用《SA 管理指南》的“SA 维护”部分中的重新启动指令和序列。

备注: 此步骤可能花费数日，具体取决于客户的维护窗口。如果您在此阶段遇到任何错误，请解决错误，然后返回运行： corerecert --phase 13 --doit以启动阶段 13。如果您不想删除旧 CA，则此阶段不需要网状网络重新启动。。

30. 网状网络成功重新启动后，从命令行运行：

    ```
    corerecert --phase 13
    ```

    以继续阶段 13。
31. 通过运行以下命令监控屏幕上的进度：

    ```
    corerecert --status
    ```

    直到屏幕上指示核心重新认证已成功完成。

代理重新认证

本节描述如何在一个或多个托管服务器上重新认证代理。您可以在完整核心重新认证过程中，单独在一个或多个服务器上重新认证代理。完整核心重新认证过程重新认证核心和所有代理。有关详细信息，请参见代理与核心重新认证和SA 核心重新认证。

要在一个或多个托管服务器上重新认证代理，请执行以下步骤：

1. 在 SA 客户端中，选择“设备”选项卡。
2. 在“服务器”节点下，选择“所有托管服务器”或“虚拟服务器”。此时将显示所有相应的服务器。

   或在“设备组”下，选择一个或多个设备组。
3. 选择“操作”菜单或右键单击并选择“运行”>“代理重新认证”。
4. 选择“操作”菜单或右键单击并选择“运行”>“代理重新认证”。

   或者如果“运行扩展”>“重新认证代理”未显示，则选择“运行扩展”>“选择扩展”。此时将显示“选择扩展”窗口，列出可用的扩展。在“选择扩展”窗口中选择托管服务器的“重新认证代理”，然后选择“确定”。

   将显示“运行程序扩展”窗口，该窗口显示了您选择的服务器或设备组。
5. 您可以随时选择“启动作业”按钮以接受所有其余的默认设置并运行作业。
6. 可以选择使用“包括设备”按钮来添加服务器或设备组。
7. 可以选择使用“删除”按钮删除服务器或设备组。

8. 选择“下一步”按钮。将显示“程序”屏幕。不要在“程序”屏幕上进行任何更改。
9. 选择“下一步”按钮。将显示“选项”屏幕。
10. 在“选项”屏幕上，可以更改程序超时值，使用 -debug 选项请求有关作业的详细信息，或者指定要保存的作业输出量。
    1. 程序超时 – 指定希望代理重新认证作业运行的最大时间（以分钟为单位）。如果代理重新认证作业失败，它将继续运行一段指定的时间。如果在该时间段后它仍不成功，则它将中止，并显示错误消息。
    2. 使用情况选项 – 如果您希望获取有关要显示的作业的其他详细信息，请在文本框中输入“-debug”。
    3. 输出选项 – 指定您在作业完成后希望对程序输出执行的操作。如果指定“丢弃所有程序输出”，则在您打开完成的作业时，所有输出将不可用。
11. 选择“下一步”按钮。将显示“计划”屏幕。指定希望作业运行的时间。
12. 选择“下一步”按钮。将显示“通知”屏幕。
13. 在“通知”屏幕上，指定电子邮件收件人，以及当作业失败和/或成功时他们是否应当收到电子邮件。
14. 选择“下一步”按钮。将显示“作业状态”屏幕。
15. 选择“启动作业”按钮。将启动作业并显示状态。
16. 选择任意服务器可显示该服务器上的作业状态的详细信息。
17. 代理重新认证作业完成后，您可以选择在服务器上运行通信测试以验证这些服务器上的代理。

第 3 章

多主控网状网络管理

本节解释如何管理和维护多主控网状网络。本节将不说明如何为多主控网状网络配置 SA。有关多主控体系结构以及计划和安装多主控网状网络的详细信息，请参见《SA 概述和体系结构》指南和《SA Installation Guide》。

多主控网状网络的内置冗余

每个 SA 核心管理一个数据中心。在 SA 中，每个数据中心表示为一个设施。多主控网状网络是两个或更多个管理相同数量设施的 SA 核心。多主控网状网络可以包括一个或多个 SA 卫星端。SA 卫星端是“微型”SA 核心，它管理的服务器数量比完整 SA 核心少。

SA 多主控网状网络配置经过设计，具有冗余、可靠性和高可用性。多主控网状网络由多个同步核心组成。每个核心中的所有数据与每个其他核心同步，以便当一个核心出现问题时，其他核心可以处理所有请求和作业。

多主控网状网络还提供负载平衡以获得更好的性能。

什么是多主控网状网络冲突？

在多主控网状网络（按照定义由两个或更多个 SA 核心组成）中，当 SA 用户在任何核心上执行任何操作时，每个核心将事务详细信息转发到网状网络中的所有其他核心，以保持它们同步。如果两个用户在两个不同的核心上执行重复或冲突的操作，则当核心将事务转发到其他核心时，将发生冲突。

SA 可以检测这些种类的冲突，当它们发生时通知您，帮助您解决这些冲突。

SA 核心自身无法解决冲突。在发生冲突时，SA 管理员必须使用 SA 客户端中的“多控制工具”在目标数据库解决冲突，以确保事务不丢失。

1. 要查看冲突，请参见查看多主控网状网络的状态 - SA 客户端。
2. 要解决冲突，请参见解决网状网络冲突 - SA 客户端。
3. 您还可以使用 SA 客户端中的系统诊断工具查看有关多主控组件的运行状况的信息。有关详细信息，请参见SA 故障排除 - 诊断测试。

SA 如何处理网状网络冲突

每个 SA 核心管理一个设施。当 SA 核心（源核心）将事务发送到另一个核心（目标核心）且发生冲突时，SA 检测到冲突并采取以下操作：

1. 取消事务。
2. 锁定受事务影响的所有 SA 数据库行，阻止对这些行的进一步更改。
3. 源核心将事务锁传播到网状网络中的所有其他核心，因此锁定所有核心中的行。
4. 包含冲突信息的警报消息通过电子邮件发送到用户配置的邮件列表。有关详细信息，请参见多主控电子邮件警报。
5. 源核心和目标核心都继续到下一个事务。

如果源核心或目标核心遇到异常，阻止它继续下一个事务，它将向用户配置的邮件列表中发送一封说明该问题的电子邮件，然后关闭。

要手动解决冲突和解锁数据库行，请参见解决网状网络冲突 - SA 客户端。

阻止网状网络冲突的最佳实践

本节列出为了最大程度地减少多主控网状网络冲突可采取的措施。

多主控冲突的可能性因下列因素而异：

- 处于管理下的服务器数量 — 服务器越多，冲突发生的可能性越大。
- 多主控网状网络中的核心数。
- 您的 SA 用户使用的 SA 客户端数量 — 进行更新的用户越多，冲突的可能性越大。
- 用户在多个使用不同 SA 客户端的设施中进行更改的偏好。

用户

您的用户应当知晓下列事项：

- 多个设施中的用户能够同时修改相同的数据，因此，尽可能协调更新以避免冲突。
- 用户不应当在一个设施中更改数据后在另一个设施中进行同样的更改，因为 SA 会自动传播更改。对多个设施进行同样的更改通常会导致网状网络冲突。
- 在用户进行的更改传播到其他 SA 设施之前，会有轻微的时间延迟。延迟的长度因多种因素而异，其中包括网络连接和带宽。如果更新尚未传播到网状网络中的所有其他模型库，请在尝试重做事务或执行依赖于其他最近事务的另一个更新之前等待一段合理的时间，以确保事务未延迟。

管理员

实现下列最佳实践以减少数据冲突的机会：

- 确保您的网络连接可靠，且网状网络中的设施之间有足够的网络带宽。冲突的风险会随着带宽下降而增加。

  有关详细信息，请参见多主控网状网络的网络管理。

请参见《SA Installation Guide》，以获取有关在多主控网状网络中运行 SA 时的网络连接的信息。

- 在可能的情况下，请将数据空间分区，以便只有一个用户可以同时更改不同设施中的相同对象。
- 让一个用户或一小组协调用户管理一组给定的服务器。将数据空间分区可确保服务器所有权的责任并防止用户更改彼此的数据。

  SA 客户端通过允许您按客户、设施和用户组类型设置权限，简化了数据空间分区。

  有关用户组和 SA 权限的详细信息，请参见权限参考。

查看多主控网状网络的状态 - SA 客户端

多控制工具为您显示了 SA 部署中每对设施之间的事务状态。它们还允许您解决发生的任何冲突。您可以按如下所述，查看有关多主控网状网络中设施间的所有事务的详细信息：

1. 在 SA 客户端中，选择“管理”选项卡。
2. 在“多控制工具”节点下，选择“状态视图”。这将显示一个表，表中显示了您的所有设施（每个设施对应一个 SA 核心）和每对设施间所有事务的状态。**表 17** 显示了状态视图中颜色代码的含义。

表 17.多主控事务状态颜色代码

事务颜色	事务状态
蓝色	已发送 - 列出已成功发送到其他设施的事务的数量。
绿色	已接收 - 列出设施已成功接收的事务的数量。
紫色	未发送 - 设施中的一个或多个事务尚未发送到网状网络中的其他设施。
黄色	未接收 - 设施尚未收到从另一个设施发来的一个或多个事务。
红色	冲突 - 已发生一个或多个冲突。

3. 要查看有关所有冲突的事务的详细信息，请在导航栏中选择“冲突视图”。这将显示有关每个事务的详细信息，包括：
   - 事务 - 这是事务标识符和链接，您可以从中获取有关冲突的事务的更多详细信息。
   - 操作 - 这将描述事务的组成，例如数据库更新、插入和删除。
   - 表 - 列出受事务影响的数据库表。
   - 计数 - 列出对数据库元素执行了多少操作。
   - 用户 - 列出执行导致冲突的操作的 SA 用户。与此人联系以验证他尝试执行的操作，以便您可以准确解决冲突。

- 创建时间 - 这是发生事务时的日期和时间。
- 源设施 - 这是发送事务的核心。
- 冲突设施 - 这些是收到事务并检测到冲突的核心。

4. 要查看有关特定事务冲突的详细信息，请选择“事务”链接。这将显示有关选定事务的详细信息。
   - 表 - 它显示发生冲突的 SA 数据库表。
   - DB 字段 - 它显示发生冲突的数据库表中的所有 SA 数据库字段名称。
   - 设施列 - 其余列用于 SA 部署中的每个设施。每个列列出对应设施中的值。在发生冲突的位置，值以红色文本显示。
5. 要解决冲突，请参见解决网状网络冲突 - SA 客户端。

图 24 显示了没有冲突的多主控网状网络状态视图。多主控网状网络中的所有三个核心 - 伦敦、巴黎和维也纳 - 都是最新的。所有核心中的所有更改都已成功发送到所有其他核心。

图 24.多主控网状网络冲突，状态视图 - 没有冲突

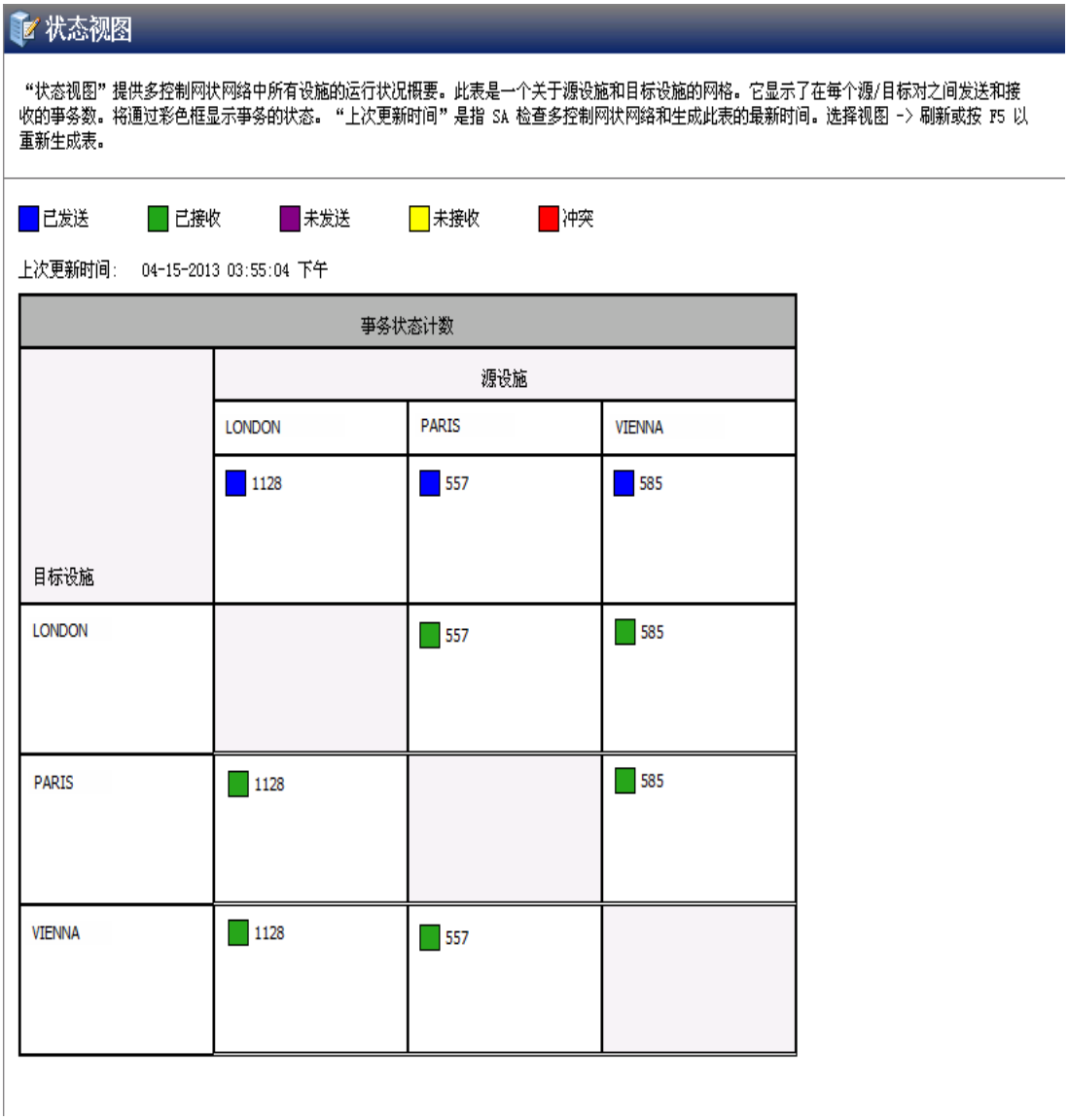


图 25 显示了没有冲突的网状网络状态视图，但是对两个核心进行了两项更改，这些更改将要传播到其他核心。对伦敦核心进行了两项更改，对维也纳核心进行了两项更改。

图 25.多主控网状网络冲突，状态视图 - 更改正等待发送

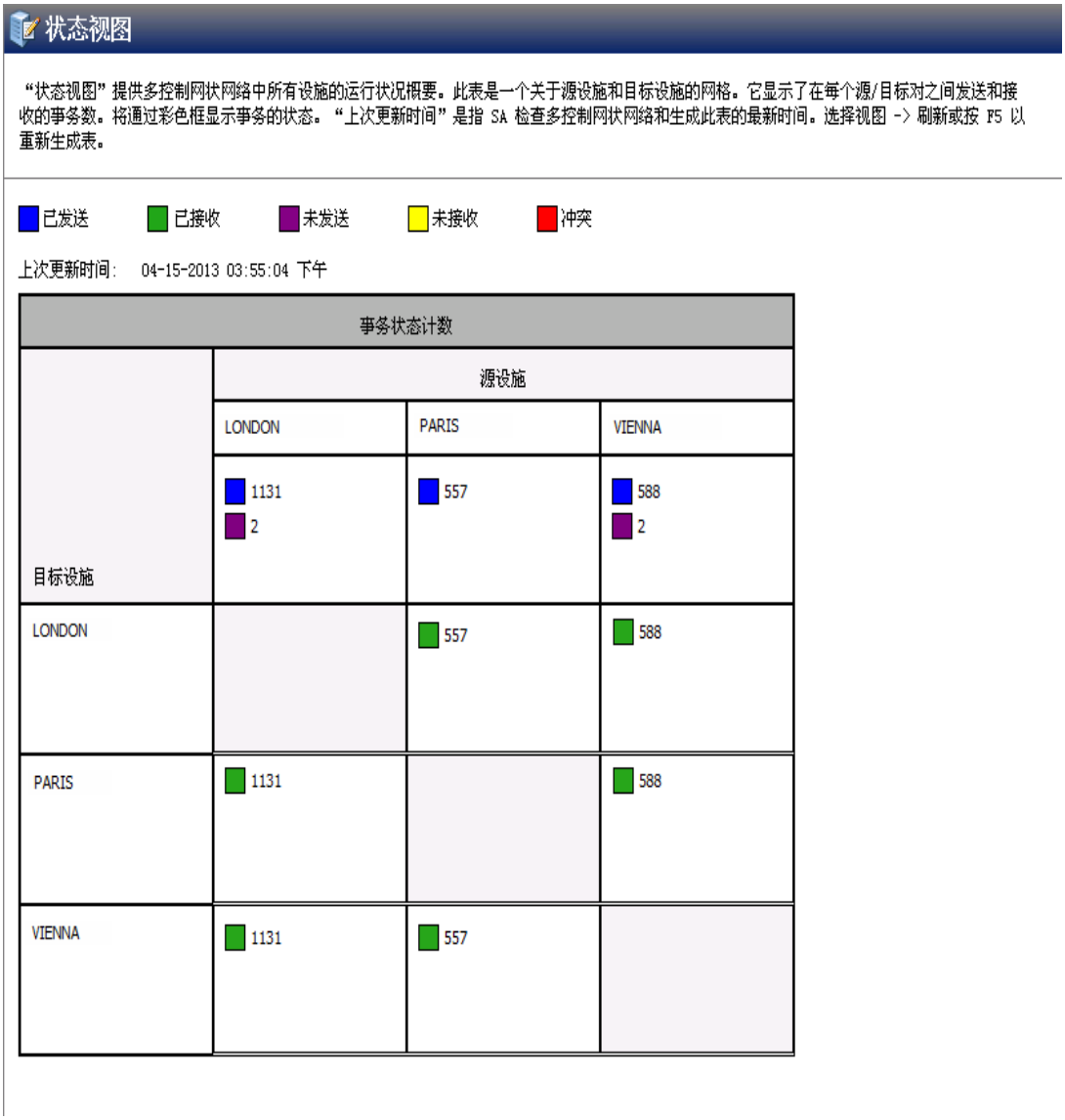
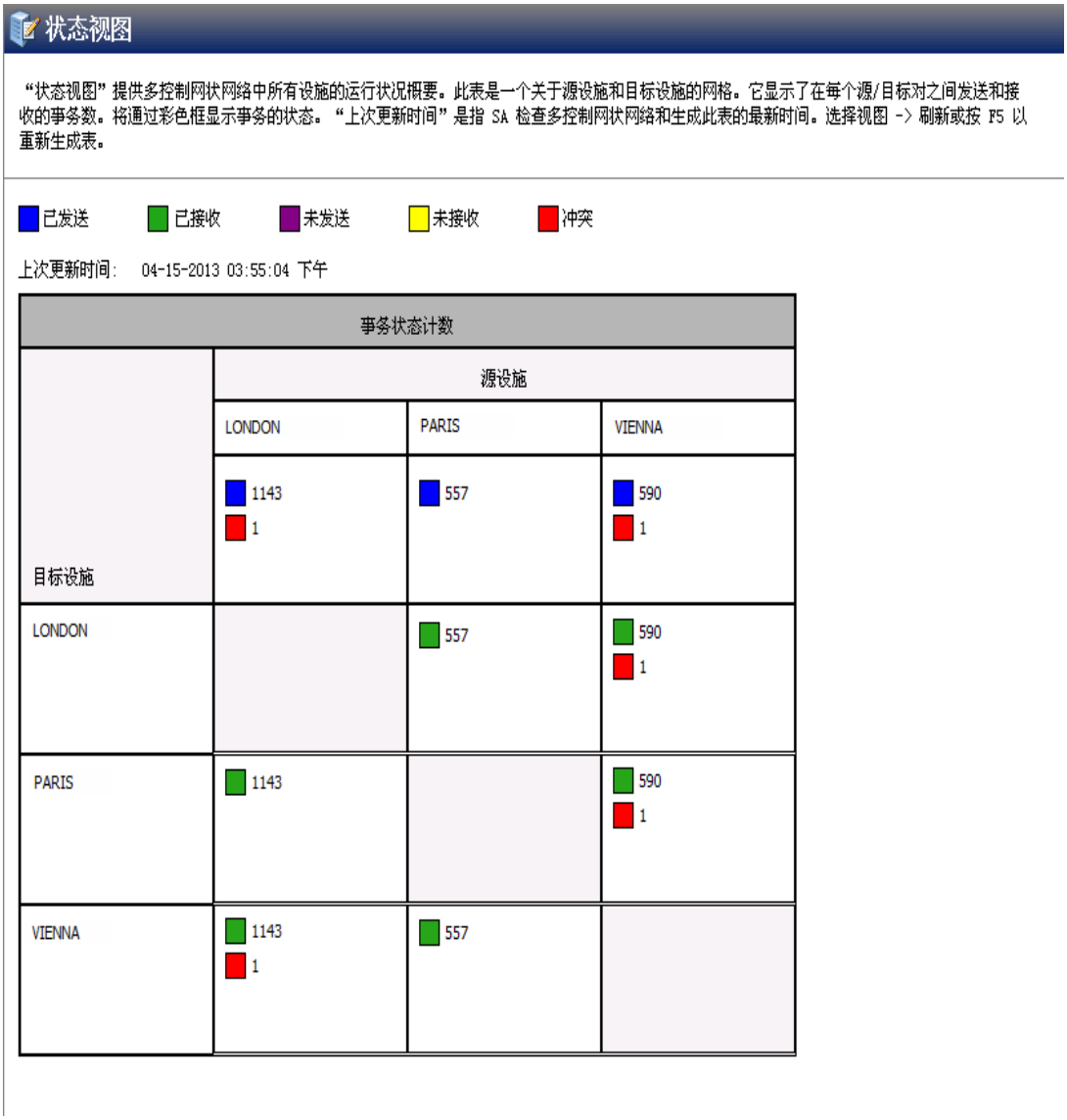


图 26 显示了在伦敦核心和维也纳核心中包含两个冲突的网状网络状态视图。伦敦核心有一个与维也纳核心的冲突，维也纳核心有一个与伦敦和巴黎核心的冲突。要解决冲突，请参见解决网状网络冲突 - SA 客户端。

图 26.多主控网状网络冲突，状态视图 - 两个冲突


状态视图

“状态视图”提供多控制网状网络中所有设施的运行状况概要。此表是一个关于源设施和目标设施的网格。它显示了在每个源/目标对之间发送和接收的事务数。将通过彩色框显示事务的状态。“上次更新时间”是指 SA 检查多控制网状网络和生成此表的最新时间。选择视图 -> 刷新或按 F5 以重新生成表。

已发送 已接收 未发送 未接收 冲突

上次更新时间: 04-15-2013 03:55:04 下午

事务状态计数			
目标设施 \ 源设施	LONDON	PARIS	VIENNA
	1143 1	557	590 1
LONDON		557	590 1
PARIS	1143		590 1
VIENNA	1143 1	557	

解决网状网络冲突 - SA 客户端

要解决与 SA 客户端的多主控网状网络冲突，请执行下列步骤。

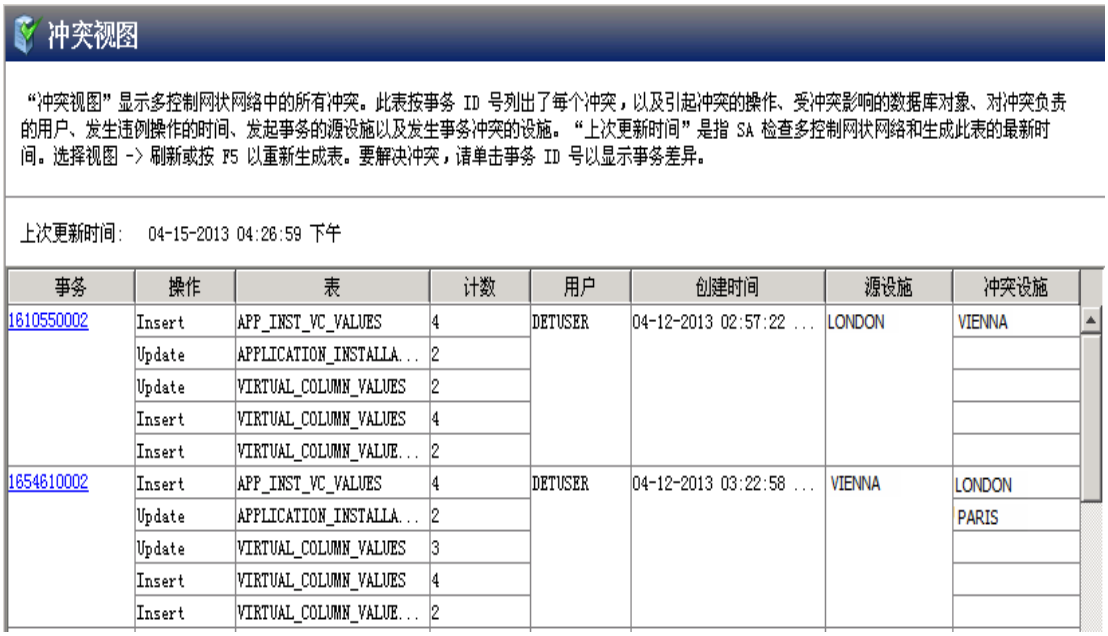
提示: 解决冲突之前，请将电子邮件警报别名通知给订户。通知这些用户有助于阻止其他 SA 管理员撤销或影响彼此的冲突解决投入。当解决冲突时，您应当从单一设施的 SA 客户端解决冲突。不要尝试从不同设施的 SA 客户端多次解决相同的冲突。

备注: 如果您看到大量使用多控制工具无法解决的冲突，请联系 HP Server Automation 支持代表，以获取有关同步数据库的帮助。

确保您有足够的 SA 权限来查看和解决冲突。有关权限的详细信息，请参见权限参考。

1. 在 SA 客户端中，选择“管理”选项卡。
2. 在“多控制工具”节点下，选择“冲突视图”。这将显示有关网状网络中所有冲突的详细信息。**图 27** 显示了冲突视图，其中包含从伦敦设施和维也纳设施产生的两个冲突。有关冲突的概述，请选择“状态视图”。

图 27.多主控网状网络冲突 - 冲突视图



事务	操作	表	计数	用户	创建时间	源设施	冲突设施
1610550002	Insert	APP_INST_VC_VALUES	4	DETUSER	04-12-2013 02:57:22 ...	LONDON	VIENNA
	Update	APPLICATION_INSTALLA...	2				
	Update	VIRTUAL_COLUMN_VALUES	2				
	Insert	VIRTUAL_COLUMN_VALUES	4				
	Insert	VIRTUAL_COLUMN_VALUE...	2				
1654610002	Insert	APP_INST_VC_VALUES	4	DETUSER	04-12-2013 03:22:58 ...	VIENNA	LONDON
	Update	APPLICATION_INSTALLA...	2				PARIS
	Update	VIRTUAL_COLUMN_VALUES	3				
	Insert	VIRTUAL_COLUMN_VALUES	4				
	Insert	VIRTUAL_COLUMN_VALUE...	2				

3. （可选）按键盘上的 Control-F（Ctrl + F 键）。将显示查找工具，以便您搜索特定的冲突。按 Escape (Esc) 键关闭查找工具。
4. 检查每个冲突，注意执行操作的用户、源设施和冲突设施。
5. 从“事务”列选择事务标识符链接。这将显示有关事务的详细信息。
6. （可选）按键盘上的 Control-F（Ctrl + F 键）。将显示查找工具，以便您搜索特定冲突的详细信息。按 Escape (Esc) 键关闭查找工具。
7. 检查每个冲突，关注其详细信息。您可能必须调查每个冲突，以确定冲突内容、用户执行了哪些导致冲突的操作、执行操作的用户以及每个用户的目的。
8. 如果可能，确定具有正确数据的设施，并从该设施同步。从设施同步会将该设施中的数据复制到所有其他设施，因而可解决冲突。

   如果没有任何设施具有正确的数据，您可以从一个设施同步，然后在避免导致冲突的同时重做操作。

   您还可以选择同步每个单独的数据库表，不过，不建议此方法，除非您具有 SA 数据库知识。要同步每个单独的表，请在每列底部选择标有“从此设施同步”的相应按钮，然后转到在“标记已解决冲突”窗口中选择“确定”。此操作将删除该冲突。。
9. 一旦您确定具有正确数据的设施，请从窗口顶部附近标有“同步所有对象的设施”的下拉列表中选择该设施。

10. 选择“同步”按钮。此操作会将选定设施中的数据复制到所有其他设施以解决冲突，并将显示“事务同步结果”窗口。
11. 在“事务同步结果”窗口中选择“确定”。
12. 选择“标记已解决”按钮。将显示“标记已解决冲突”窗口，该窗口显示了您已解决的网状网络冲突的状态。
13. 在“标记已解决冲突”窗口中选择“确定”。此操作将删除该冲突。
14. 在“冲突视图”中检查冲突并验证已解决的冲突是否已删除。

网状网络冲突的高级类型和原因

本节描述多主控网状网络冲突的一些原因和类型。

用户重叠冲突

如果某用户使用 SA 客户端在一个设施中进行更改，而同时另一个用户在另一个设施中对相同的对象进行更改，则会发生冲突。

例如：

1. Alice 从亚特兰大设施中的服务器删除节点 A。
2. Bob 从波士顿设施中的相同服务器删除节点 A。
3. SA 会将亚特兰大设施中的更改传播到波士顿设施，但是 Bob 已经从波士顿设施中的服务器删除了节点 A。SA 生成一个模型库多主控组件冲突警报，因为现在似乎 Alice 正在请求删除不存在的节点。
4. SA 还会将 Bob 在步骤 2 中进行的更新从波士顿设施传播到亚特兰大设施，但是 Alice 已经从亚特兰大设施中的服务器删除了节点 A。SA 生成第二个模型库多主控组件冲突警报。

用户操作重复导致的冲突

在以下情况下也会发生冲突：用户出于各种原因尝试对模型库进行更新，但未等待足够长的时间让更新传播到网状网络中的其他模型库，由于更新失败，用户再次尝试更新，因此创建了重复的更新。

例如，会发生以下事件序列：

1. Carol 从西雅图设施中的服务器，使用 SA 命令行界面 (CLI) 上载程序包 `carol.conf`。
2. Carol 立即登录凤凰城设施中的 SA 客户端，搜索搜索该程序包。她未看到该程序包，因为数据尚未从西雅图传播到凤凰城。Carol 允许有足够的时间让数据在设施间传播。
3. Carol 使用凤凰城中的 SA 客户端上载程序包 `carol.conf`。
4. 当数据最终从西雅图传播过来时，SA 生成一个冲突，因为该数据在凤凰城已存在。

无序事务导致的冲突

两个设施间的事务通常按它们的发送顺序到达。但是，如果第三方设施参与到事务中来，则无法保证正确的顺序。例如：

1. 用户在设施 A（模型库 A）更改或插入数据。
2. 该更改事务传播到设施 B（模型库 B）和设施 C（模型库 C）。
3. 但是，该数据在设施 B（模型库 B）处再次被修改或引用，然后传播到设施 A 和 C。
4. 如果设施 B 中的事务（步骤 3）在设施 A 中的事务（步骤 1）之前到达设施 C（模型库 C），则会发生冲突。

当用户使用 SA CLI 在一个设施中上载程序包，又立即使用 SA 客户端将程序包添加到另一个设施中的软件策略时，通常会发生此冲突。

不同设施中的并发更新或设施间网络连接出现问题，会加重无序事务的发生。

例如：

1. Henry 使用丹佛设施中服务器上的 SA CLI 上载程序包 `henry.conf`。
2. SA 将有关该程序包的数据传播到网状网络中的所有设施，但是，由于网络连接断开，他无法将数据传播到巴黎设施。
3. Henry 登录迈阿密设施中的服务器，使用 SA 客户端来更新 `henry.conf` 程序包的描述。
4. SA 将有关更新程序包描述的数据传播到网状网络中的所有其他设施，但是，由于网络连接仍断开，它无法将数据传播到巴黎设施。
5. 与巴黎设施的网络连接恢复，步骤 2 和 4 中的延迟事务传播到巴黎设施。
6. 更新程序包描述的事务比上载 `henry.conf` 的事务*先*到达巴黎设施。因此，巴黎设施中的模型库不包含有关 `henry.conf` 的数据，SA 因而生成冲突警报。
7. 上载 henry.conf 的事务到达巴黎设施，进行处理时未出现任何错误。现在，程序包数据在巴黎模型库中已存在，但是程序包描述与网状网络中的所有其他设施不同。

数据库冲突

本节提供有关识别您可能遇到的冲突种类和可用来解决冲突的步骤的基本信息。请参见 Oracle 数据库管理文档，以获取有关识别和解决数据和事务冲突的详细信息。

表 18 显示了几种冲突类型：

表 18.冲突类型

冲突	描述
相同数据冲突	多控制工具显示冲突事务，但是数据在设施间相同。数据相同是因为用户在不同的设施中进行了相同的更改。

冲突	描述
简单事务冲突	行在所有设施中存在，但是在某些设施中，某些列具有不同的值或者行不存在（缺失对象）。
唯一键约束冲突	对象在设施中不存在，且无法插入到其中，因为插入它会违反唯一键约束。
外键约束冲突	行在某些设施中不存在，且无法插入，这是因为数据包含该设施中也不存在的另一个对象的外键。
链接对象冲突	一种很少遇到的冲突类型。SA 包括业务逻辑，即：将 SA 中的特定相关对象（例如自定义特性名称和值）与 SA 客户端中创建的客户（显示在列表中）和节点层次结构中该客户的关联节点进行链接。SA 确保维持相关对象间的链接。解决链接对象冲突是很复杂的，因为您必须尝试保留导致冲突的事务的意图。请联系 HP Server Automation 支持代表以帮助您解决链接对象冲突。

解决每种冲突的指南

一般情况下，当您解决冲突时，会应用更新，以便目标始终基于启动更改的时间戳反映最新数据。

当您无法按照上述指南操作时，请尝试保留事务的意图。请与生成事务的用户联系，确定每个用户在托管环境中尝试进行了何种更改。

相同数据冲突

事务中的所有对象在所有设施中包含完全相同的数据。此类冲突包括对象在所有设施中不存在的情况。

要解决相同数据冲突，只需将冲突标记为已解决。

相同数据冲突（已锁定）

事务中的所有对象在所有设施中包含完全相同的数据，但是事务中的对象仍是锁定的（标记为冲突）。

要解决此类冲突，请选取任意一个设施，从它同步所有对象。执行此操作可解锁对象。同步数据后，将冲突标记为已解决。

简单事务冲突

数据在设施间不同，或者某些设施中某些对象缺失。没有任何一个对象依赖于其他冲突事务的操作。同步对象的结果不会导致违反数据库外键或唯一键约束。

要解决简单事务冲突，请选择包含正确数据的设施，从它进行同步。您确定哪个设施包含正确数据的方式因事务类型而异：

- 如果冲突是两个用户彼此覆盖工作所致，请联系这两个用户，确定哪个用户的更改是正确的。
- 如果冲突是覆盖彼此数据的自动化过程所致，则最近的更改通常是正确的。
- 如果冲突是无序事务所致，则最近的更改通常是正确的。

同步数据后，将冲突标记为已解决。

唯一键约束冲突

解决这些冲突会导致违反唯一键约束。

例如，会发生以下事件序列：

1. John 从伦敦设施中的 SA 客户端，将节点 A1 创建为节点 A 的下属节点。
2. Ann 从旧金山设施中的 SA 客户端执行了同样的操作。她将节点 A1 创建为节点 A 的下属节点。
3. 节点名称在节点层次结构的每个分支中必须唯一。
4. SA 将伦敦和旧金山设施中的节点更改传播到其他设施。在其他设施的模型库数据库中插入行会导致违反唯一键约束和引发冲突。

通过将伦敦设施中的更新插入到所有设施中来解决此冲突会失败，因为违反了相同唯一键约束。

请执行下列步骤来解决唯一键约束冲突：

1. 查找所有涉及的事务，从对象不存在的设施中同步一个事务，这样便会将其从所有设施中删除。
2. 从对象存在的设施中同步其他事务，这样便会将对象插入所有设施中。两个唯一冲突对象中的一个对象将替换另一个。

外键约束冲突

解决这些冲突会导致违反外键约束。

例如，会发生以下事件序列：

1. Jerry 在设施 1 中创建节点 B。
2. 在该事务花费时间传播到其他设施之前，Jerry 将节点 C 创建为节点 B 的下属节点。
3. 当第一个事务到达设施 2 时，它由于不相关的原因产生冲突。
4. 当第二个事务到达设施 2 时，插入节点 C 的行会导致外键约束冲突，因为父节点（节点 B）不存在。

通过将节点 C 的更新插入到所有设施中来首先解决第二个冲突会失败，因为违反了相同外键约束。

请执行下列步骤来解决外键约束冲突：

1. 通过从对象存在的设施同步第一个事务，解决节点 B（父节点）的冲突事务。
2. 从对象存在的设施同步第二个事务（节点 C 更新）。

一般而言，按冲突创建的顺序解决冲突可避免生成外键约束冲突。

多主控网状网络的网络管理

SA 不要求多主控网状网络配置符合有关网络运行时间的特定原则。多主控网状网络配置在设施间网络暂时中断的生产环境中仍可正常工作。

不过，随着网络中断持续时间的延长，冲突的可能性将增加。设施间网络中断延长会导致下列问题：

- 多主控消息无法在设施间传播
- 多控制工具停止工作
- SA Web 客户端无法与多主控中心数据访问引擎联系

多主控配置的生产经验支持**表 19** 显示的性能数据。

表 19.多主控配置的性能数据

设施数	网络中断持续时间	多主控冲突数 *
8 个设施 （每个设施都安装了 SA 核心）	12 小时中断 （1 个设施失去与其他设施的网络连接）	12 到 24 个冲突 （产生的平均冲突数）
* 用户使用其他设施中的 SA Web 客户端对断开连接的设施中的服务器进行管理的偏好会导致冲突数增加。		

网络连接问题包括 SA 总线或多播路由问题。

多主控电子邮件警报

当发生多主控冲突或多主控组件出现问题时，SA 向用户配置的多主控电子邮件别名发送一封电子邮件。您可以在安装 SA 时配置此电子邮件地址。如果必须更改此电子邮件地址，请联系 HP Server Automation 支持代表，或者参见SA 通知配置以获取详细信息。

警报电子邮件的主题行指定：

- 当事务应用于模块库数据库时发生的错误类型
- 导致多主控操作出现问题的错误类型

请联系 HP Server Automation 支持代表，以获取有关排除和解决影响多主控操作的 SA 问题的帮助。

表 20 显示了错误消息。

表 20.多主控错误消息

主题行	错误类型	详细信息
vault.ApplyTransactionError	多主控事务冲突	未能成功使用其他数据库中的更改更新本地数据库。每次更新必须仅影响一行，且不会导致任何数据库错误。
vault.configValueMissing	SA 问题	没有为给定配置参数指定任何值。 登录 SA Web 客户端，提供此配置参数的值。联系 HP Server Automation 支持代表以获取有关设置 SA 配置值的帮助。
vault.DatabaseError	多主控事务冲突	当查询数据库以查找要发送到其他数据库的更新或者从其他数据库应用更新时，发生错误。重新启动模型库多主控组件。
vault.InitializationError	SA 问题	当模型库多主控组件进程启动时，发生错误。应用程序返回指定的消息。出现错误的线程停止运行。当在多主控模式下运行 SA 时会出现此错误。 解决错误情况。重新启动模型库多主控组件。
vault.ParserError	多主控事务冲突	当解析事务的 XML 表示时发生错误。应用程序返回指定的消息。当在多主控模式下运行 SA 时会出现此错误。 运行 SA 管理多控制工具，确认事务数据不包含 XML 分析器可能无法解释的特殊字符。
vault.SOAPError	多主控事务冲突	当使用 SOAP 库将事务打包或解包到 XML 中时发生错误。应用程序返回指定的消息。当在多主控模式下

主题行	错误类型	详细信息
		运行 SA 时会出现此错误。 运行 SA 管理多控制工具，确认事务数据不包含 SOAP 可能无法解释的特殊字符。
vault.UnknownError	SA 问题	模型库多主控组件进程遇到未知错误。请联系技术支持，并提供数据库名称和 SA 组件的日志文件。

设施管理

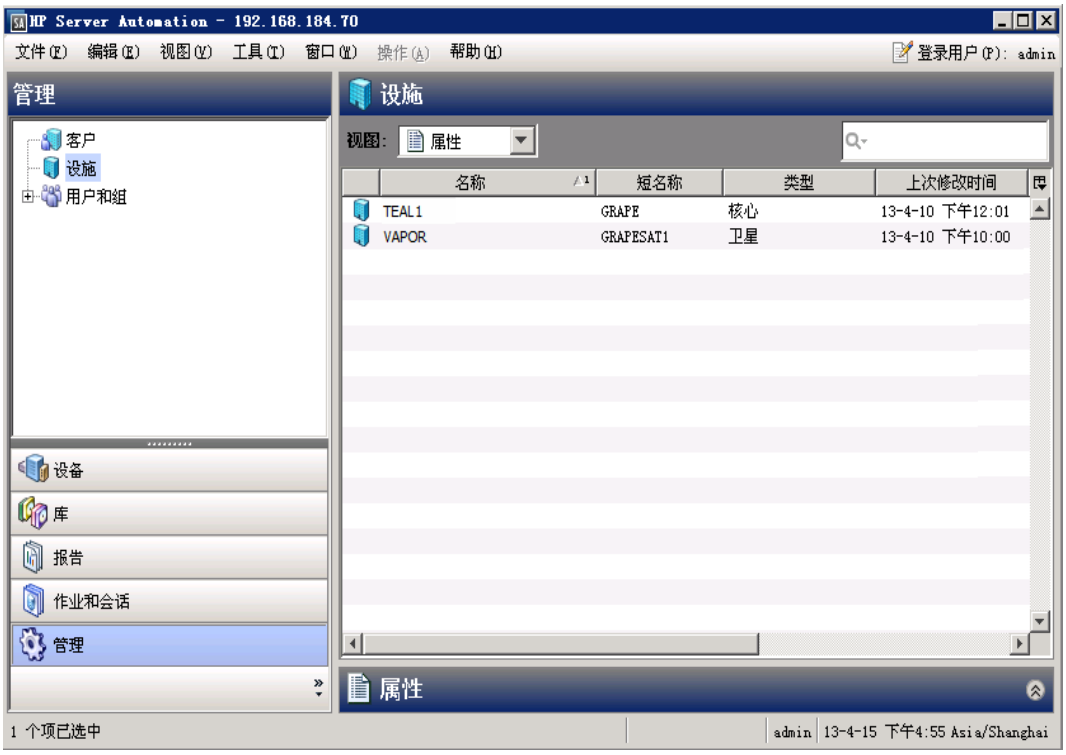
设施 指的是单一 SA 核心或卫星端管理的一组服务器。无论何时安装 SA 核心或 SA 卫星端，都会创建新的设施。多主控网状网络由主 SA 核心、一个或多个次要 SA 核心以及零个或多个卫星端组成。无论何时安装另一个 SA 核心或另一个 SA 卫星端，都会创建新的设施。

有关设施、核心、卫星端以及它们如何融入多主控网状网络体系结构的详细信息，请参见《SA 概述和体系结构》指南和《SA Installation Guide》。

查看设施信息

您可以通过在 SA 客户端中选择“管理”选项卡，然后选择“设施”，查看有关设施的信息。**图 28** 显示了 SA 客户端中的两个设施：Teal1 和 Vapor。

图 28.SA 客户端中的两个设施



您可以通过打开设施查看有关设施的详细信息。**图 29** 显示了有关 Vapor 设施的详细信息，包括设施属性、自定义特性和领域。

图 29.设施的详细信息

更改与设施关联的客户

客户是根据您的服务器用户来组织服务器的一种方式。客户只是提供访问控制边界的托管服务器组。您可以定义所需数量的客户，并将任何服务器分配到每个客户组。不过，您必须先将客户与一个或多个设施关联，然后才能将该设施中的服务器放到客户组中。每个服务器属于且只能属于一个设施，每个服务器属于且只能属于一个客户（即使它属于“未分配”客户）。

有关客户的详细信息，请参见《SA 用户指南：Server Automation》。

要更改与设施关联的客户，请执行下列步骤：

- 在 SA 客户端中，选择“管理”选项卡。
- 在导航窗格中选择“设施”。这会显示所有设施。
- 选择要更改的设施。
- 选择“操作”菜单或右键单击，然后选择“打开”菜单。这会在单独的窗口中显示设施。
- 在“设施”窗口中，在导航窗格中选择“属性”视图。这将显示有关设施（包括与设施关联的客户）的信息。
- 要添加新客户，请选择“+”图标。这会显示现有客户的列表。
- 选择一个或多个客户。
- 单击“选择”按钮。此操作会将选定客户与设施关联起来。
- 要删除客户，请选择客户，并选择“-”图标。此操作会从设施中删除客户。
- 选择“文件”>“还原”以放弃更改。
- 选择“文件”>“保存”以保存更改。
- 选择“文件”>“关闭”以关闭设施窗口。

添加或修改设施的自定义特性 - SA 客户端

您可以创建或修改设施的自定义特性。自定义特性为您提供了快速轻松存储有关服务器的其他信息的方法。自定义特性是您可以为 SA 中的设施、服务器和其他对象创建的数据元素。有关自定义特性的详细信息，请参见《SA 用户指南：Server Automation》。

警告: 当您更新或删除现有自定义特性设置时一定要加以小心，因为它会影响或中断依赖于自定义特性的操作。

要添加、修改或删除设施的自定义特性，请执行下列步骤：

1. 登录 SA 客户端。
2. 选择“管理”选项卡。
3. 在导航窗格中选择“设施”。这会显示所有设施。
4. 选择要更改的设施。
5. 选择“操作”菜单或右键单击，然后选择“打开”菜单。这会在单独的窗口中显示设施。
6. 在“设施”窗口中，在导航窗格中选择“自定义特性”视图。此操作将显示为该设施定义的所有自定义特性。

7. 要添加新的自定义特性，请选择“+”图标或“操作”>“添加”菜单。输入新的自定义特性的名称和值。
8. 要修改自定义特性，请选择值字段并输入新值。
9. 要删除自定义特性，请选择自定义特性，然后选择“-”图标或“操作”>“删除”菜单。
10. 选择“文件”>“还原”以放弃更改。
11. 选择“文件”>“保存”以保存更改。
12. 选择“文件”>“关闭”以关闭设施窗口。

修改设施名称 - SA 客户端

要修改设施名称，您必须使用“管理设施”权限登录 SA 客户端。设施的短名称是不能修改的内部名称。可以修改显示名称。

执行下列步骤以修改设施的显示名称：

1. 登录 SA 客户端。
2. 选择“管理”选项卡。
3. 在导航窗格中选择“设施”。这会显示所有设施。
4. 选择要更改的设施。
5. 选择“操作”菜单或右键单击，然后选择“打开”菜单。这会在单独的窗口中显示设施。
6. 在“设施”窗口中，在导航窗格中选择“属性”视图。
7. 在“名称”字段中输入新设施名称。
8. 选择“文件”>“还原”以放弃更改。
9. 选择“文件”>“保存”以保存更改。

第 4 章

卫星端管理

本节描述基本 SA 卫星端拓扑和概念以及下列管理任务：

启动/重新启动卫星端

要启动卫星端，请发出以下命令：

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

要重新启动卫星端，请发出以下命令：

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

备注： 如果卫星端代理未能重新启动（通常是由于阻止卫星端代理通信所需端口 1002 的可用性而导致 NFS 错误），请重新启动卫星端主机，或者临时禁用阻止 1002 的服务，重新启动代理，然后重新启动该阻止服务。

停止卫星端

要停止卫星端，请发出以下命令：

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

验证卫星端与主核心的通信

要验证核心管理网关是否与卫星端通信，请执行下列步骤：

1. 作为具有管理网关权限的用户组成员登录到 SA 客户端。
2. 从导航面板中，单击“管理”>“网关”。
3. 验证“管理网关”页的左上角是否显示新卫星端的链接。

   如果“管理网关”页未显示卫星端的链接，您可能需要编辑卫星端的属性。属性文件的完整路径名如下：

   ```
   /etc/opt/opsware/opswgw/opswgw.properties
   ```

   修改属性文件后，必须重新启动卫星端：

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

4. 以具有卫星端设施的读取（或读取和写入）权限的用户组成员的身份，登录 SA Web 客户端。
5. 从导航面板中，单击“服务器”>“管理服务器”。
6. 验证“管理服务器”页是否显示卫星端服务器的主机名。

有关进一步信息，另请参见《SA 用户指南：Server Automation》中的“更多服务器通信测试故障排除”。

管理卫星端所需的权限

要管理 SA 网关，您必须具有管理网关权限。默认情况下，SA System Administrators 组中包括此权限。要查看设施信息，您必须具有特定设施的读取（或读取和写入）权限。有关用户组和 SA 权限的详细信息，请参见权限参考。

查看卫星端信息

本节将讨论下列主题：

- 查看卫星端设施和领域
- 查看卫星端托管服务器的领域
- 查看和管理卫星端网关信息

查看卫星端设施和领域

您可以通过在 SA 客户端中选择“管理”选项卡，然后选择“设施”，查看核心和卫星端设施。选择设施，然后选择“领域”视图查看与该设施关联的领域（包括设施中领域之间的带宽）。有关设施的详细信息，请参见设施管理。

查看卫星端托管服务器的领域

当在卫星端配置中安装时，SA 可以管理具有重叠 IP 地址的服务器。当服务器位于 NAT 设备或防火墙的后面时，会发生这种情况。具有重叠 IP 地址的服务器必须驻留在不同的领域中。

当检索从搜索得到的服务器列表时，您会看到具有相同 IP 地址但位于不同领域中的多个服务器。当您打算运行自定义扩展，而系统提示您选择运行扩展的服务器时，您也会看到具有相同 IP 地址的多个服务器。

SA 客户端中服务器的“属性”视图显示了用于标识与 IP 地址对应的服务器的附加信息。

查看和管理卫星端网关信息

要查看卫星端网关信息，请在 SA 客户端导航面板中，选择“管理”选项卡，然后选择“网关”。将显示网关状态，如**图 30** 所示。从左侧的网关列表中，选择要查看的网关。从横跨页面顶部的链接中选择要查看的具体网关信息。

图 30.网关状态

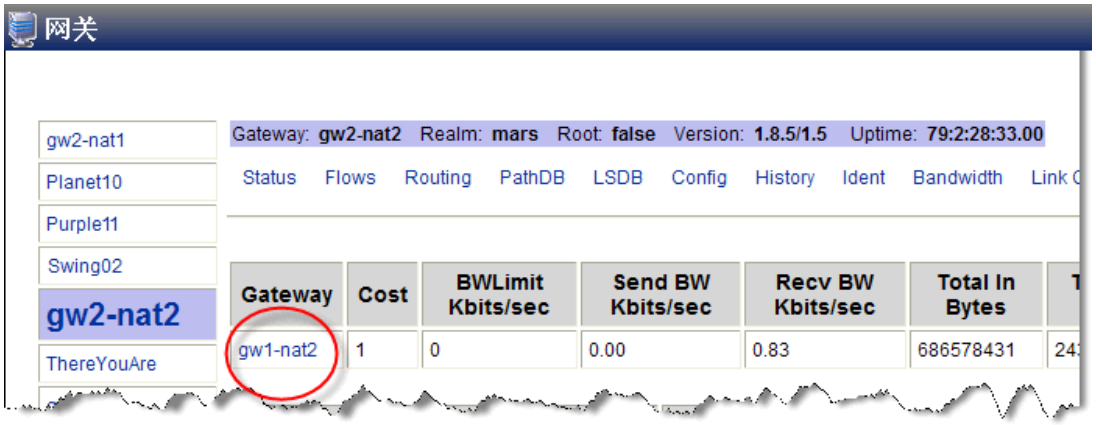
使用网关状态完成下列任务：

- 获取有关网关以及网关间隧道的状态信息。这对调试网关很有帮助。
- 更改网关实例之间的带宽限制或隧道成本。
- 重新启动网关进程。
- 更改网关进程的日志记录级别。

查看网关诊断和调试信息

1. 在 SA 客户端中，选择“管理”选项卡，然后选择“网关”。
2. 从左边的网关列表，选择要查看其信息的网关。这会显示选定网关的下列“状态”：
   - 活动隧道表，包括：
     - Tunnel Cost
     - Bandwidth Constraints
     - Bandwidth Estimates
     - Age of the tunnels
   - 有关内部消息队列的信息。队列表中的每一列使用以下格式显示数据：
     - 队列中的消息数
     - 队列的消息高水位标记
     - 为队列配置的最大值
     - 上次为队列保留消息高水位标记的时间。您可以使用时间戳指示上次达到消息高水位标记的时间，以解决网关问题。时间戳的显示格式为 `DD:HH:mm:ss`。
3. 要查看网关间隧道的详细信息和统计信息，请选择*终止* 隧道的网关链接，如 **图 31** 所示。该页显示隧道详细信息和统计信息。

图 31.管理网关 — 状态页



4. 要查看包含诊断信息的以下页面，请选择页面顶部的以下链接之一：
   - “Flows”显示有关选定网关的所有开放连接的信息。
   - “Routing”显示网关间路由表。此表显示哪个隧道将用于连接到网状网络中的另一个网关。路由表是根据路径数据库中的数据计算而得的。当连接的链接成本更改时，路由计算自动更新。

> **备注:** 默认情况下，隧道折叠，路由信息保存在路由表中达两分钟，以提供网状网络的连续性。

- “PathDB”- 路径数据库显示网状网络中所有可连接网关的成本最低的路由。SA 根据链接状态数据库中的数据，确定所有所有可连接网关的成本最低的路由。
- “LSDB”- 链接状态数据库包含有关每个网关实例的所有隧道状态的信息。LSDB 包含所有隧道的数据和每个隧道的带宽限制。
- “Config”显示选定网关的属性文件，包括运行网关组件的服务器上的属性文件的路径。在属性值下方，页面包含了加密文件信息和网状网络属性数据库。“Properties Cache”字段位于属性值上方。当您更改网关间连接的带宽或链接成本时，如果更新成功，则更新的值将显示在此字段中。
- “History”显示有关使用网关网状网络的主机间的入站（入口）和出站（出口）连接的历史信息。例如，当领域 A 中的主机 A 与到领域 B 中的主机 B 连接时。

标识连接的源 IP 地址和领域

“Ident”链接提供实时连接标识数据库的接口。如有必要，请联系 HP 支持人员以获取有关如何运行此工具的其他信息。

1. 在 SA 客户端中，选择“管理”选项卡，然后选择“网关”。
2. 选择“Ident”链接。这将显示实时连接标识数据库。
3. 在编辑框中，输入活动连接的协议和源端口，用冒号分隔；例如，TCP:25679。
4. 选择“查找”按钮。这将显示客户端领域和进行连接的客户端 IP 地址。

更改网关间的带宽使用情况或链接成本

通过“编辑”链接可以修改链接带宽约束、链接成本以及负载平衡规则。

备注: 您只能对核心网关上的网关间带宽应用任何更改。对其他网关的更改不会生效。

1. 在 SA 客户端中，选择“管理”选项卡，然后选择“网关”。
2. 指定连接的带宽限制：
    1. 选择页面顶部的“编辑”链接。这将显示“修改链接带宽限制”控件。
    2. 指定隧道连接的两个网关实例的名称。
    3. 指定所需的带宽限制（以 Kbps 为单位）。指定零 (0) 可删除连接的带宽限制。
    4. 单击“应用”。
3. 设置连接的链接成本：
    1. 选择页面顶部的“编辑”链接。这将显示“修改链接成本”控件。
    2. 指定隧道连接的两个网关实例的名称。
    3. 在“成本”字段中指定所需的成本。
    4. 单击“应用”。

4. 设置连接的负载平衡规则：
    1. 选择页面顶部的“编辑”链接。这将显示“修改负载平衡规则”控件。
    2. 指定网关实例名称。
    3. 指定负载平衡规则。
    4. 单击“应用”。

查看网关日志或更改日志级别

备注：将日志记录级别更改为 `LOG_DEBUG` 或 `LOG_TRACE` 会大量增加网关日志输出，对网关性能产生负面影响。

1. 在 SA 客户端中，选择“管理”选项卡，然后选择“网关”。
2. 选择页面顶部的“日志记录”链接。这将显示网关日志文件的结尾。
3. 要更改日志记录级别，请选择 `LOG_INFO`、`LOG_DEBUG` 或 `LOG_TRACE` 之一。
4. 选择“提交”。

重新启动或停止网关进程

1. 在 SA 客户端中，选择“管理”选项卡，然后选择“网关”。
2. 选择页面顶部的“进程控制”链接。
3. 要重新启动网关进程，请单击“重新启动”。
4. 要停止网关监视程序和网关，请单击“关闭”。

警告：停止网关进程可能导致 SA 核心出现问题。例如，如果停止核心网关进程，则到该 SA 核心的所有多主控通信都将停止，并且您将无法从 SA 客户端控制此网关。

要求：要在停止网关后从 SA 客户端重新启动它，则必须登录运行网关组件的服务器，手动重新启动进程。

卫星端监控

请参见中的以下章节：

- 代理缓存监控
- 网关监控

远程连接的带宽管理

带宽管理是一项部署在通信网络中的措施，用于调节网络通信和最小化网络拥挤。SA 的远程站点管理模型通常使用卫星端配置，该配置在每个逻辑位置（例如分支机构）部署远程网关，以处理与远程服务器的连接和管理这些连接的网络带宽。但是，对于仅管理几个服务器的站点，这种配置的成本效益明显减少了。

使用新的 SA 带宽管理功能，无需为只有少量服务器的远程站点安装卫星端。SA 提供带宽配置管理 (BCM) 工具控制在与远程服务器进行通信时代理或卫星端网关使用的带宽。

可通过使用 BCM 工具将带宽配置推送到一个对等组中。配置推送到对等组后，将保存到文件。在网关启动期间，配置从此文件加载，并与对等组同步。当客户端协商通过 SA 网关网状网络的连接以连接到远程 TCP 服务时，客户端于是建立了与入口网关的 TCP 连接。同样，建立了一个从出口网关连接到远程服务的 TCP 连接。

当建立通过网关网状网络的代理连接后，入口/出口连接的对等地址便进行分类，并为每种类别创建运行时队列。此时，带宽限制对这些连接生效。随着数据通过连接流动，对应的队列将随带宽使用信息进行更新。带宽使用信息还可以在对等组之间共享，以便本地队列可以在每个网关群集中更新。数据可以通过该连接流动，直到达到最大允许带宽。队列带宽使用信息每隔一秒进行重置。

备注: 同一领域中的所有代理网关还必须运行相同的 SA 版本，才能参与代理网关带宽协商和通信。不支持混合核心配置（核心和卫星端运行不同的 SA 版本）。

SA 带宽配置管理工具

备注: 运行 Solaris 或 Red Hat Enterprise Linux 3 x86 的 SA 核心/卫星端不支持 SA BCM。

备注: BCM 工具要求防火墙允许在端口 3001 和 8086 上进行 SA 网络通信。如果您打算使用 BCM 工具管理界面，还必须打开端口 8089。

本节描述了使用 BCM 工具创建带宽管理配置。然后，这些配置可以跨对等网关自动同步。

只有具有网关主机的 root 访问权限的管理用户才可以使用 BCM 工具执行网关配置推送操作。

备注: 尽管 BCM 工具是使用默认配置文件

```
/etc/opt/opsware/gateway_name/BWT.conf
```

，但是不应直接修改该文件。您应当制作该文件的副本，对副本进行编辑以满足您的

配置。然后，可以使用 gwctl -f 命令将已修改的配置文件推送到领域中的所有网关。请参见调用带宽管理配置工具。

指定的带宽配置保存到配置文件。下面是典型的网关配置文件示例：

```
enabled

# Branch offices have only 3M bytes per sec connections, SA
should never use
# more than 512K bytes per sec.

queue branch_office bandwidth 512KB


# Branch offices A and B (non standard addresses)

class 192.168.1.[1-5,10-15,20,30] for branch_office


# Other branch offices

class 192.168.2.0/24 for branch_office
```

调用带宽管理配置工具

将 BCM 工具作为命令行工具进行调用。

在要管理其 SA 代理配置的卫星端上，使用下列命令：

```
gwctl:[OPTIONS] ...
```

表 21.带宽配置管理工具选项

选项	描述
-?, --help	显示用法。
-p, --port	当指定 -l 时，列出代理网关代理服务器端口（默认 3001）。 当指定其他选项时（如 -d、-e、-f、-v、-c、-s 等），显示带宽限制配置端口（默认 8086）。
-l, --list_gws	列出此领域中的所有网关。
-f, --conf	配置文件。
-v, --verify_conf	验证配置文件并退出；不将其推送到网关。**注意**：此选项仅与 -f <conf_path> 选项一起使用。
-c, --cksum	显示配置文件的校验和。**注意**：此选项仅与 -f <conf_path> 选项一起使用。

选项	描述
-e, --enable_bwt	启用针对此领域的带宽限制。
-d, --disable_bwt	禁用针对此领域的带宽限制。
-r, --request_conf	从给定网关请求配置。
-s, --signature	从给定网关请求配置签名。
-z, --verbose	显示所有消息。

下面是示例命令。

列出领域中的网关：

```
gwctl -l
```

指定另一个代理网关端口：

```
gwctl --port 2003 -l
```

仅验证配置文件：

```
gwctl -f myconf.conf -v
```

将配置文件推送到领域中的所有代理网关（包括 localhost）：

```
gwctl -f mytconf.conf
```

启用/禁用远程连接带宽管理

必须以下列两种方式之一启用或禁用远程连接带宽管理：

- 推送将 `enabled` 或 `disabled` 关键字作为文件中的第一个条目的带宽配置文件。每个配置文件必须在文件的第一行包含 `enabled` 或 `disabled` 以指示带宽限制状态。
- 从命令行中，使用 `gwctl -e` 启用带宽管理，或者使用 `gwctl -d` 禁用带宽管理。只要没有版本升级，带宽管理状态 enabled 或 disabled 便一直保持在带宽管理配置文件中。

带宽配置语法

EBNF 格式的带宽配置上下文无关语法 (CFG) 如下：

```
config :((queue | class | version | config_source |
config_user | disabled |
comment)?'\n')\*
```

```
queue :'queue' queue_name 'bandwidth' d_number bandwidth_
spec
('rtt' d_number)?('parent' queue_name 'borrow')?

queue_name :"[a-zA-Z0-9_]+"

class :'class' pattern (',' pattern)* 'for' queue_name

pattern : ipv4 | ipv4_cidr

ipv4 : ipv4_address_pattern_element ('.' ipv4_address_
pattern_element)@1:3

ipv4_cidr : d_number ('.' d_number)@1:3 '/' d_number

ipv4_address_pattern_element : single_number | range |
range_class | wildcard range_class :'[' (number ('-'
number)?',')+ ']'

wildcard :'*'

range :'[' number '-' number ']'

single_number : d_number

number : d_number

d_number :"[0-9]+"

x_number :"[a-fA-F0-9]+"

bandwidth_spec :"[GMK]?[bB]"

config_source :'config-source' ':'"[a-zA-Z0-9.:\-]+"
```

```
config_user :'config-user' ':'"[a-zA-Z0-9_!@#$%^&*();.`~\-
\\]+"


disabled :'disabled'


comment :'#' "[^\n]*"
```

卫星端软件数据库缓存管理

SA 核心中的最大网络流量发生在：

- 应用程序软件或 OS 修补程序安装期间软件数据库与托管服务器上的服务器代理之间。
- OS 正在配置的服务器与为配置提供 OS 介质的 OS 配置介质服务器之间。

如果网络通过低带宽网络链接进行连接，在执行这些进程时性能将下降。您可以通过在卫星端的软件数据库缓存中创建核心软件数据库内容的副本，或者安装本地卫星端 OS 配置介质服务器/启动服务器，最大程度地降低网络流量。

因为软件数据库缓存存储 SA 核心软件数据库（或来自其他卫星端软件数据库缓存）的文件副本，SA 可在本地提出软件请求而无需在卫星端和 SA 核心之间跨网络传送请求。同样，OS 配置介质服务器可以在本地提供 OS 映像。SA 卫星端还支持每个领域有多个软件数据库缓存。

下面的章节讨论如何配置和更新本地软件数据库缓存以及（可选）OS 配置介质和启动服务器。

卫星端软件数据库缓存内容的可用性

软件数据库内容不会自动复制到卫星端软件数据库缓存中；因此并非所有内容都可本地用于网状网络中的卫星端。您必须使用想要本地安装的软件，手动更新卫星端的软件数据库缓存。只有当软件数据库缓存领域的缓存策略为“按需”时，才通过按需更新。

SA 只能警告您请求的软件本地不可用，您必须从第一个核心软件数据库或另一个卫星端软件数据库缓存更新内容。SA 跟踪程序包是否本地可用。

当 SA 尝试修正请求的无法从本地向托管服务器传送的软件时，SA Web 客户端生成错误，并显示丢失的程序包的完整列表，以帮助您识别需要复制到缓存的程序包。您将软件复制到缓存后，该软件将继续在本地可用，以便将来安装。

备注： SA Web 客户端不为将程序包*推送*到卫星端的操作提供用户界面。不过，您可以使用命令行工具 `stage_pkg_in_realm` 将程序包推送到卫星端。

此工具可在第一个核心的模型数据库主机的

`/opt/opsware/mm_wordbot/util/stage_pkg_in_realm` 中找到。

如果在针对该文件的 URL 请求中使用 checkonly=1 参数，则实用程序请求文件，但软件数据库将不发送该文件。如果该文件尚未缓存，则在缓存策略允许的情况下，软件数据库缓存将从父软件数据库缓存中获取它。

更新卫星端软件数据库缓存中的软件

要更新卫星端软件数据库缓存中的文件，您可以将缓存配置为在收到请求时更新缓存的文件副本（*按需更新*），或者手动更新缓存的文件副本（*手动更新*）：

- 按需更新：本地软件数据库缓存根据需要从 SA 核心中的软件数据库获取当前文件。
- 手动更新：SA 在软件包安装之前，将软件包暂存到卫星端的软件数据库缓存，以使性能与托管服务器位于核心所在的数据中心时一样。

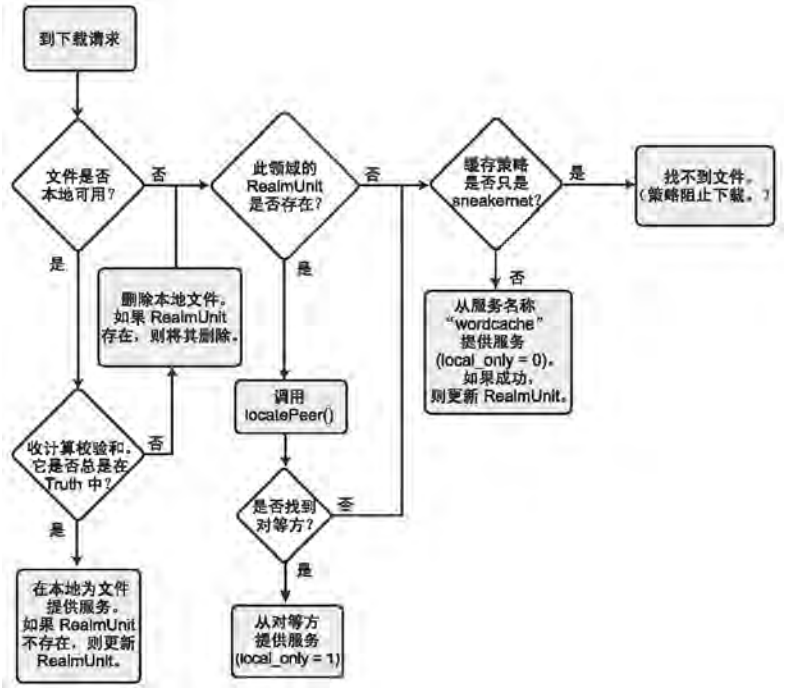
当启用按需更新时，如果请求的软件已在本地软件数据库缓存中存在，而且是最新的，则不需要采取任何操作。如果软件在本地不存在，或者不是最新的，则软件数据库缓存尝试在后台从最近的上游软件数据库缓存或从核心的软件数据库中下载文件。

如果缓存策略是手动更新，而您请求按需软件更新，则软件数据库缓存将生成 `wordbot.unableToCacheFile exception`。

无论缓存策略如何，始终可以将文件暂存到软件数据库缓存中。请参见将文件暂存到软件数据库缓存。

图 32 展示了软件数据库缓存在卫星端更新程序包时使用的逻辑。

图 32.软件数据库缓存更新逻辑



设置软件数据库缓存更新策略

您可以通过执行下列任务，为每个设施指定软件数据库缓存更新策略：

1. 在 SA 客户端中选择“管理”选项卡。
2. 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。
3. 选择要为其设置软件数据库缓存更新策略的领域。将显示该领域的所有系统配置。
4. 查找配置参数 `word.caching_policy`。
5. 将此参数的值设置为下列值之一：
   - 选择“默认值：JIT”。这将指定 JIT 或按需更新。
   - 选择新值按钮  ，在编辑字段中输入“SNEAKERNET”。这将指定手动更新。
6. 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。

按需更新

启用按需更新将允许当请求的软件在本地尚不可用时将其下载到卫星端软件数据库缓存中。如果您有低带宽网络连接，则手动更新可能是更好的解决方案，因为手动更新将允许您将最常请求的软件预先下载到软件数据库缓存中。请参见手动更新。

每当卫星端中托管服务器上的服务器代理请求软件时，本地软件数据库缓存都检查其缓存的软件副本是否是最新的。如果缓存的文件不是当前的或者已丢失，则软件数据库缓存从最近的上游软件数据库缓存或从核心的软件数据库获取更新的或新的本地文件副本，并将其发送到请求的服务器代理。

配置按需更新时，软件数据库缓存收到软件请求后，会首先对照核心软件数据库的校验和请求软件的校验和以确保其是最新副本。

备注： 出于安全目的，SA 将软件校验和缓存一段时间（用户可对该时间段进行配置）。

如果该校验和与本地存储的文件相同，则软件数据库缓存将该软件提供给请求者。如果校验和不匹配，或者本地文件不存在，则软件数据库缓存从最近的上游软件数据库缓存或核心的软件数据库请求软件的更新副本。

如果在软件数据库缓存下载软件时网络连接断开，则服务器代理下次请求同一软件时，软件数据库缓存将从它停止的那一点继续文件下载。

手动更新

对于具有低带宽网络链接的卫星端而言，手动软件数据库缓存更新允许您在安装时*预先填充*软件数据库缓存。您还可以配置现有缓存的刷新。软件数据库缓存通过带外方法填充，例如通过刻录所需程序包的 CD 并将它们发送到卫星端。要执行手动更新，请使用 SA DCML 交换工具 (DET) 从 SA 核心复制当前程序包或使用暂存实用程序执行更新。请参见创建软件数据库缓存手动更新和将文件暂存到软件数据库缓存。

如果配置为手动更新，则软件数据库缓存不与上游软件数据库缓存或核心的软件数据库进行通信，直到您启动更新为止。卫星端将其自己的软件数据库缓存视为权威。

如果缓存策略是手动更新，而您请求按需软件更新，则软件数据库缓存将生成 `wordbot.unableToCacheFile exception`。

即使您已将软件数据库配置为按需更新，您也可以应用手动更新，无论其更新策略如何。

备注: 当在具有多个软件数据库缓存的卫星端安装中应用手动更新时，您必须将更新应用到卫星端中的每个软件数据库缓存。否则，当执行从缓存检索文件的操作时（例如当在受影响卫星端中的服务器上安装软件时），您可以收到 `wordbot.unableToCache file` 错误。

紧急软件数据库缓存更新

即使缓存策略为手动更新，您也可以通过网络将紧急更新手动推送到卫星端。您不需要重新配置软件数据库缓存的缓存策略，即可将紧急更新推送到软件数据库缓存。例如，紧急修补程序可以暂存到卫星端并应用，无需等待发送的 CD 到达。

软件数据库缓存大小管理

当将手动更新应用到软件数据库缓存时，SA 将在缓存大小超过限制时删除最近未访问过的文件。

将首先删除最近最少访问的程序包。

软件数据库缓存在下次清理其缓存时删除文件。默认情况下，每 12 小时清理一次缓存。程序包将被删除，以使可用磁盘空间低于高水位标记。

要求: 您必须有足够的磁盘空间来存储软件数据库缓存的所有必需程序包，以确保软件数据库缓存不超过缓存大小限制。

创建软件数据库缓存手动更新

要创建手动更新，您可以使用 SA DCML 交换工具 (DET) 从 SA 核心复制现有的软件。然后保存导出文件，您可以通过网络将其复制到卫星端的软件数据库缓存，或者刻录成 CD 或 DVD 以稍后应用到缓存。您还可以使用暂存实用程序上载软件。请参见将文件暂存到软件数据库缓存。

本节将讨论下列主题：

使用 DCML 交换工具 (DET) 创建手动更新

通过使用 DET 执行此过程。使用 DET，导出用于手动更新的软件并导出与选定软件策略关联的程序包。

有关使用 DET 的详细信息，请参见《SA 内容实用程序》指南。

要创建手动更新，请执行下列步骤：

1. 在安装 DET 组件的服务器上，运行下列命令以创建下列目录：

   ```
   # mkdir /var/tmp/sneakernet
   ```

2. 从运行 SA 客户端的服务器的 `/var/opt/opsware/crypto/occ` 目录中复制以下文件：

   ```
   opsware-ca.crt
   spog.pkcs.8
   ```

   复制到以下目录：

   ```
   /usr/cbt/crypto
   ```

   这是安装 DET 的目录。

3. 创建文件 `/usr/cbt/conf/cbt.conf`，以便它包含下列内容：

   ```
   twist.host=<twist's hostname>
   twist.port=1032
   twist.protocol=t3s
   twist.username=buildmgr
   twist.password=buildmgr
   twist.certPaths=/usr/cbt/crypto/opsware-ca.crt
   spike.username=<your username>
   spike.password=<your password>
   spike.host=<way's hostname>
   way.host=<way's hostname>
   spin.host=<spin's hostname>
   word.host=<word's hostname>
   ssl.keyPairs=/usr/cbt/crypto/spog.pkcs8
   ssl.trustCerts=/usr/cbt/crypto/opsware-ca.crt
   ```

4. 创建 DCML Exchange Tool 筛选器文件 `/usr/cbt/filters/myfilter.rdf`，该文件包含以下内容：

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   ```

```
<!DOCTYPE rdf:RDF [
<!ENTITY filter "http://www.opsware.com/ns/cbt/0.1/filter#">
]>
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
xmlns="http://www.opsware.com/ns/cbt/0.1/filter#">
<ApplicationFilter rdf:ID="a1">
<path>/Other Applications</path>
<directive rdf:resource="&filter;Descendants" />
</ApplicationFilter>
</rdf:RDF>
```

在筛选器文件的 `<path>` 指令中，将 `/Other Applications` 替换为您要导出的节点的路径（将导出有关该节点的所有节点信息、其子级以及所有关联的程序包）。

此筛选器将从 SA 客户端的应用程序区域导出。如果您希望从 SA 客户端中软件的某些其他目录导出程序包，则需要创建另一个筛选器。有关信息，请参见《SA 内容实用程序》指南。

5. 在安装 DET 组件的服务器上，通过输入下列命令运行 DCML Exchange Tool:

```
# /usr/cbt/bin/cbt -e /var/tmp/myexport --config
/usr/cbt/conf/cbt.conf --filter
/usr/cbt/filters/myfilter.rdf
```

DCML Exchange Tool 将与导出节点关联的程序包放在下列目录中:

```
/var/tmp/myexport/blob
```

程序包名为 `unitid_`*`nnnnnnn`*`.pkg`。

6. 通过网络，或者通过将文件刻录到一套 CD 或 DVD 上，将所有 `.pkg` 文件复制到运行软件数据库缓存的服务器上的目录中。

对软件数据库缓存应用手动更新

要将手动更新应用于软件数据库缓存，请运行实用程序 (`import_sneakernet`)，该实用程序将您要更新的软件移动或复制到软件数据库缓存上的正确位置，并将其注册到 SA 核心中的模型库。

要将手动更新应用到软件数据库缓存，请执行以下步骤:

1. 以 `root` 身份登录到运行卫星端的软件数据库缓存的服务器。
2. 将导出文件复制到软件数据库缓存服务器上的目录中，安装包含软件导出文件的 CD，或者将 CD 内容复制到临时目录。

3. 输入以下命令以更改目录：

   ```
   # cd /opt/opsware/mm_wordbot/util
   ```

4. 输入以下命令将导出文件的内容导入到软件数据库缓存：

   ```
   # ./import_sneakernet -d dir
   ```

   其中，*dir* 是 CD 安装点或包含该导出文件的临时目录。

将文件暂存到软件数据库缓存

托管服务器上的服务器代理可以有效覆盖领域的缓存策略。借助覆盖软件数据库缓存的缓存策略的功能，您可以将软件暂存到配置为仅手动更新的缓存，以应对下列情况：

- 您必须发行紧急修补程序，而您没时间创建手动更新导出文件和实际访问某个设施来上载软件。
- 在指定的维护期间必须安装必需的修补程序，而该期间的长度不足以下载修补程序和将其安装到所有托管服务器上。
- 众所周知，卫星端网络链接的利用率在一天的特定时间是很低的，这个时候非常适合上载。

要强制程序包暂存，暂存实用程序提供参数 `override_caching_policy=1`，该参数在软件的 URL 请求中指定。

软件数据库缓存允许客户端请求它获取文件，但是实际上它不将文件发送到客户端。如果该文件尚未缓存，则在缓存策略允许的情况下，软件数据库缓存将从父软件数据库缓存中获取它。为了使用此功能，客户端在针对文件的 URL 请求中包括了参数 `checkonly=1`。

运行暂存实用程序

要运行暂存实用程序，请执行以下步骤：

1. 在运行软件数据库组件（切分组件捆绑包的一部分）的服务器上，验证证书 `token.srv` 是否位于您的 `CRYPTO_PATH` 中。安装期间 `token.srv` 被复制到：

   `/var/opt/opsware/crypto/gateway/token.srv`。

2. 登录运行核心的软件数据库的服务器。
3. 输入以下命令以更改目录：

   ```
   # cd /opt/opsware/mm_wordbot/util
   ```

4. 要暂存想要的文件，请运行实用程序 `stage_pkg_in_realm`，其语法如下：

   ./**stage_pkg_in_realm** [-h | --help] [-d | --debug] [--user <*USER*>] --pkgid *<ID>* --realm *<REALM>* [--gw <*IP*:*PORT*>] [--spinurl <*URL*>] [--wayurl <*URL*>] [--word <*IP*:*PORT*>]

要强制程序包暂存，暂存实用程序提供参数 `override_caching_policy=1`，该参数在软件的 URL 请求中指定。例如：

```
./stage_pkg_in_realm --user admin --pkgid 80002 --realm
luna
--gw 192.168.164.131:3001
Password for admin:<password>
Package /packages/opsware/Linux/3ES/miniagent is now being
staged in realm luna
```

Microsoft 实用程序上载和手动更新

当上载新的 Microsoft 修补实用程序（《SA Installation Guide》中“系统要求”一章所述）时，应当立即将这些文件暂存到软件数据库缓存配置为仅手动更新的所有领域中。

如果不将这些文件暂存到远程领域，则在这些领域中的 Windows 服务器上运行的服务器代理将无法下载实用程序的新版本，而且将无法注册其软件包。无需将程序包缓存到其中的软件数据库已配置为按需更新的领域。

软件数据库缓存允许客户端请求它获取文件，但是实际上它不将文件发送到客户端。如果该文件尚未缓存，则在缓存策略允许的情况下，软件数据库缓存将从父软件数据库缓存中获取它。为了使用此功能，客户端在针对文件的 URL 请求中包括了参数 checkonly=1。有关如何暂存文件的信息，请参见运行暂存实用程序。

SA 卫星端安装和拓扑

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（第一个）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* 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（第一个）核心的通信。可以选择在卫星端主机上安装 *OS 配置启动服务器* 和 *介质服务器*，用于支持卫星端 OS 配置。

备注: 不支持在卫星端主机上安装其他 SA 核心组件。

有关如何安装和配置卫星端的信息，请参见《SA Installation Guide》。

可以使用各种拓扑安装卫星端。有关卫星端拓扑的详细信息，请参见《SA 概述和体系结构》指南。

备注: 某些高级拓扑需要 HP 专业服务人员的服务指导才能进行安装和升级。如果文档中未说明拓扑的具体安装步骤，请联系 HP 技术支持人员或专业服务人员以获取帮助。

第 5 章

SA 远程通信管理

此部分描述了可用于控制 SA 网关带宽使用（带宽管理）和在无需安装完整 SA 卫星端（托管服务器对等内容缓存）的情况下对配备少于 50 台托管服务器的小型远程站点配置软件缓存的方法：

- 远程连接的带宽管理
- SA 中的 IPv6
- SA 托管服务器对等内容缓存
- 概念：SA 核心通信基础结构

备注： 有关 SA 卫星端、网关和代理的详细信息，请参见《SA 概述和体系结构》指南。

远程连接的带宽管理

带宽管理是一项部署在通信网络中的措施，用于调节网络通信和最小化网络拥挤。SA 的远程站点管理模型通常使用卫星端配置，该配置在每个逻辑位置（例如分支机构）部署远程网关，以处理与远程服务器的连接和管理这些连接的网络带宽。但是，对于仅管理几个服务器的站点，这种配置的成本效益明显减少了。

使用新的 SA 带宽管理功能，无需为只有少量服务器的远程站点安装卫星端。SA 提供 BCM 工具控制在与远程服务器进行通信时代理或卫星端网关使用的带宽。

可通过使用 BCM 工具将带宽配置推送到一个对等组中。配置推送到对等组后，将保存到文件。在网关启动期间，配置从此文件加载，并与对等组同步。当客户端协商通过 SA 网关网状网络的连接以连接到远程 TCP 服务时，客户端于是建立了与入口网关的 TCP 连接。同样，建立了一个从出口网关连接到远程服务的 TCP 连接。

当建立通过网关网状网络的代理连接后，入口/出口连接的对等地址便进行分类，并为每种类别创建运行时队列。此时，带宽限制对这些连接生效。随着数据通过连接流动，对应的队列将随带宽使用信息进行更新。带宽使用信息还可以在对等组之间共享，以便本地队列可以在每个网关群集中更新。在达到允许的最大带宽之前，数据可通过连接流动。队列带宽使用信息每隔一秒进行重置。

备注： 同一领域中的所有代理网关还必须运行相同的 SA 版本，才能参与代理网关带宽协商和通信。不支持混合核心配置（核心和卫星端运行不同的 SA 版本）。

SA 带宽配置管理工具

备注： 运行 Solaris 或 Red Hat Enterprise Linux 3 x86 的 SA 核心/卫星端不支持 SA BCM。

备注: BCM 工具要求防火墙允许在端口 3001 和 8086 上进行 SA 网络通信。如果您打算使用 BCM 工具管理界面，还必须打开端口 8089。

本节描述了使用 BCM 工具创建带宽管理配置。然后，这些配置可以跨对等网关自动同步。

只有具有网关主机的 root 访问权限的管理用户才可以使用 BCM 工具执行网关配置推送操作。

备注: 尽管 BCM 工具是使用默认配置文件

```
/etc/opt/opsware/gateway_name/BWT.conf
```

，但是不应直接修改该文件。您应当制作该文件的副本，对副本进行编辑以满足您的配置。然后，可以使用 `gwctl -f` 命令将已修改的配置文件推送到领域中的所有网关。请参见调用带宽管理配置工具。

指定的带宽配置保存到配置文件。下面是典型的网关配置文件示例：

```
enabled

# Branch offices have only 3M bytes per sec connections, SA
should never use
# more than 512K bytes per sec.

queue branch_office bandwidth 512KB


# Branch offices A and B (non standard addresses)

class 192.168.1.[1-5,10-15,20,30] for branch_office


# Other branch offices

class 192.168.2.0/24 for branch_office
```

调用带宽管理配置工具

将 BCM 工具作为命令行工具进行调用。

在要管理其 SA 代理配置的卫星端上，使用下列命令：

```
gwctl:[OPTIONS] ...
```

表 21.带宽配置管理工具选项

选项	描述
`-?, --help`	显示用法。

选项	描述
-p, --port	当指定 -l 时，列出代理网关代理服务器端口（默认 3001）。 当指定其他选项时（如 -d、-e、-f、-v、-c、-s 等），显示带宽限制配置端口（默认 8086）。
-l, --list_gws	列出此领域中的所有网关。
-f, --conf	配置文件。
-v, --verify_conf	验证配置文件并退出；不将其推送到网关。**注意**：此选项仅与 -f <conf_path> 选项一起使用。
-c, --cksum	显示配置文件的校验和。**注意**：此选项仅与 -f <conf_path> 选项一起使用。
-e, --enable_bwt	启用针对此领域的带宽限制。
-d, --disable_bwt	禁用针对此领域的带宽限制。
-r, --request_conf	从给定网关请求配置。
-s, --signature	从给定网关请求配置签名。
-z, --verbose	显示所有消息。

下面是示例命令。

列出领域中的网关：

```
gwctl -l
```

指定另一个代理网关端口：

```
gwctl --port 2003 -l
```

仅验证配置文件：

```
gwctl -f myconf.conf -v
```

将配置文件推送到领域中的所有代理网关（包括 localhost）：

```
gwctl -f mytconf.conf
```

启用/禁用远程连接带宽管理

必须以下列两种方式之一启用或禁用远程连接带宽管理：

- 推送将 enabled 或 disabled 关键字作为文件中的第一个条目的带宽配置文件。每个配置文件必须在文件的第一行包含 enabled 或 disabled 以指

示带宽限制状态。
- 从命令行中，使用 `gwctl -e` 启用带宽管理，或者使用 `gwctl -d` 禁用带宽管理。只要没有版本升级，带宽管理状态 enabled 或 disabled 便一直保持在带宽管理配置文件中。

带宽配置语法

EBNF 格式的带宽配置上下文无关语法 (CFG) 如下：

```
config :((queue | class | version | config_source |
config_user | disabled |
comment)?'\n')\*


queue :'queue' queue_name 'bandwidth' d_number bandwidth_
spec
('rtt' d_number)?('parent' queue_name 'borrow')?


queue_name :"[a-zA-Z0-9_]+"


class :'class' pattern (',' pattern)* 'for' queue_name


pattern : ipv4 | ipv4_cidr


ipv4 : ipv4_address_pattern_element ('.' ipv4_address_
pattern_element)@1:3


ipv4_cidr : d_number ('.' d_number)@1:3 '/' d_number


ipv4_address_pattern_element : single_number | range |
range_class | wildcard range_class :'[' (number ('-'
number)?',')+ ']'


wildcard :'*'


range :'[' number '-' number ']'


single_number : d_number
```

```
number : d_number

d_number :"[0-9]+"

x_number :"[a-fA-F0-9]+"

bandwidth_spec :"[GMK]?[bB]"

config_source :'config-source' ':'"[a-zA-Z0-9.:\-]+"

config_user :'config-user' ':'"[a-zA-Z0-9_!@#$%^&*();.`~\-
\\]+"

disabled :'disabled'

comment :'#' "[^\n]*"
```

SA 中的 IPv6

Internet 协议版本 6 (IPv6) 是 TCP/IP 协议栈中的第 3 层网络协议。IPv6 将网络地址位数从 32 位（IPv4 中）扩展到 128 位。Internet 工程任务组 (IETF) 设计的 IPv6 寻址方案可提供与现有 IPv4 网络体系结构的互操作性，并允许 IPv6 网络与现有 IPv4 网络共存（请参见 RFC 4291）。

IPv6 解决了 IPv4 中 IP 地址短缺的问题，并且增强和改善了 IPv4 的某些重要功能。IPv6:

- 增强了路由和寻址功能
- 简化了 IP 标头
- 支持将多种类型的 IP 地址和较大的地址块用于多播路由

IPv4/IPv6 双协议栈实施

操作系统中的双协议栈实施是一种基础的 IPv4 到 IPv6 转换技术。它采用独立方式或混合方式实施 IPv4 和 IPv6 协议栈。

混合双协议栈 IPv6/IPv4 实施支持特殊类地址，即 IPv4 映射的 IPv6 地址。此类地址的前 80 位设置为 0，接下来的 16 位设置为 1，最后 32 位设置为一个 IPv4 地址。这些地址通常采

用标准的 IPv6 格式表示，但是最后 32 位采用 IPv4 惯用的 IPv4 点分十进制表示法编写；例如：ffff:192.0.2.128 表示 IPv4 地址 192.0.2.128。

SA 将双协议栈概念用于 SA 核心和卫星端。SA 核心和卫星端均需要 IPv4 地址和 IPv6 地址；这些地址可以在单个网络接口卡 (NIC) 上，也可以在两个 NIC 上。原因是，仅 SA 网关组件启用 IPv6，所有其他 SA 核心和卫星端组件仅启用 IPv4（除代理直接访问的组件以外，例如 OGFS、NFS 和 Samba）。

HP SA 中的 IPv6 支持

当 SA 核心或卫星端启用 IPv6 时，托管服务器将能够使用 IPv6 地址注册到核心，并且使用 IPv6 协议与核心或卫星端通信。直接或间接与托管服务器通信的 SA 核心组件将能够识别托管服务器的 IPv6 地址并利用从核心到托管服务器的 IPv6 通信，反之亦然。

核心内部通过 IPv4 通信

代理和卫星端网关使用其 IPv6 地址公告其 IPv6 能力，但仍将使用 IPv4 地址完成大部分通信。

SA 代理安装

IPv4、IPv6 和双协议栈网络均支持 SA 代理。在安装代理期间，通过将 SA 网关地址指定为 IPv4 或 IPv6 地址（列表），可以选择托管服务器上代理的管理 IP。如果同时传递 IPv4 和 IPv6 地址并且以传递这些地址的顺序尝试它们，则第一个成功连接将确定管理 IP。

OS 配置

OS 配置支持 IPv4、IPv6 和双协议栈网络。

在 IPv6 网络中，只能通过路由器公告 (RA) 消息配置路由信息。要将 DHCPv6 用于地址和其他信息，必须将 RA 用于路由配置。

SA 托管服务器对等内容缓存

在之前的 SA 发布中，如果您的站点较小，没有足够数量的托管服务器对齐完整的 SA 核心安装，则 SA 提供卫星端安装。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，然后该卫星端主机可通过 SA 网关连接访问主核心的数据库和其他服务。

SA 还提供托管服务器对等内容缓存，其在无需安装卫星端组件的情况下，为少于 50 台托管服务器的设施提供软件数据库的缓存。

托管服务器对等内容缓存的一些优点是：

- 对等缓存使用现有 SA 托管服务器（无需额外的硬件基础结构）
- 无需 SA 卫星端安装
- 无需 SA 网关
- 对等缓存可在软件暂存期间减少 WAN 流量
- 对等缓存允许预先暂存软件包

- 远程站点不需要 SA 卫星端或网关
- 可以将软件手动加载到缓存中

要求

托管服务器对等内容缓存要求：

- 一台运行任意 SA 所支持操作系统的托管服务器以充当对等内容服务器。
- 必须使用自定义服务器特性将托管服务器配置为使用对等缓存。

安装对等缓存

1. 决定哪个或哪些托管服务器将充当对等缓存。
2. 将这些托管服务器上的代理升级到 SA 9.14（其他托管服务器代理不需要升级）。

备注： 按照《SA 用户指南：Server Automation》附录中“代理实用程序”的描述执行代理升级。

配置对等缓存和 SA 服务器

1. 为分支/远程站点中的每个托管服务器创建自定义特性。
    1. 例如，`peer_cache_dvc_id = 240001`，其中 `240001` 是充当对等缓存的服务器的设备 ID。
    2. 如果分支/远程站点以设备组的形式建模，则您可以使用脚本在设备组级别应用自定义特性。以后添加到设备组的托管服务器将自动继承此自定义特性。
2. 确保所有使用对等缓存的托管服务器都属于对等缓存的客户。
3. （可选）在充当对等缓存的托管服务器上创建下列自定义特性：
    1. `peer_cache_size` = <以兆字节为单位的值>

       默认值：1TB（但是限制为文件系统大小）
    2. `peer_cache_path` = <文件存储的位置>

备注： `sa_cache` 附加到您为路径指定的值。例如，Windows 的默认值为：

```
\Program Files\Common Files\Opsware\sa_cache
```

4. 默认情况下，托管服务器尝试使用缓存的主 IP 地址连接到对等缓存。不过，您可以使用自定义特性指定以下格式的其他 IP 地址：

   ```
   peer_cache_ip_field = < primary_ip | management_ip |
   ip:<addr>>
   ```

   其中：

`primary_ip` - （默认）是管理界面的 IP 地址。是本地配置的 IP 地址（不是 NAT 转换的地址）。

`management_ip` - 是 SA 用于和服务器通信的 IP 地址。这可以是 NAT 转换的地址。

`ip:<addr>` - 用于手动设置 IP 地址（例如，`ip:192.168.2.1`）

有关为托管服务器配置主 IP 地址和 NAT 的详细信息，请参见《SA 用户指南：Server Automation》。

在启用对等缓存的情况下修正

按照《SA 用户指南：软件管理》中所述开始修正。

如果启用了托管服务器对等内容缓存，则修正执行下列步骤：

1. 在暂存阶段，为托管服务器赋予缓存 IP 地址（从附加到服务器的 `peer_cache_dvc_id` 自定义特性派生）。
2. 托管服务器暂存分支/远程站点对等缓存中的数据包（请参见检索对等缓存中的对象）。

检索对等缓存中的对象

当检索对等缓存中的对象时，SA 执行下列任务：

1. 托管服务器上的暂存代码在配置对等缓存的 IP 地址上得以通过。
2. 暂存代码使用代理的 SA 安全证书安全连接到对等缓存服务器的代理端口上。
3. 对等缓存确认连接客户端已配置为使用该缓存并与该对等缓存同属一个客户。
4. 向对等缓存发出了暂存指定单元的请求。
5. 对等缓存服务器通过发送单元来响应该请求。
6. 在操作阶段中，针对软件数据库中相同对象的校验和来验证对象的校验和。

可能的错误

步骤 1：没有已配置的分支缓存，或者无法与缓存代理通信：

- 暂存在 WAN 中正常继续。

步骤 3：客户端无权使用对等缓存：

1. 缓存记录未经授权的尝试。
2. 缓存将 403 Forbidden 状态返回到客户端。
3. 暂存在 WAN 中正常继续。

步骤 5：缓存没有请求的对象。

1. 缓存将具有“稍后重试”值的 503 返回到客户端。
2. 缓存在 WAN 中从软件数据库请求对象。
3. 客户端在指定的时间后重试缓存，并检索文件。

步骤 5：缓存具有请求的单元，但是校验和与核心校验和不匹配：

1. SA 将该文件视为过时，当缓存已满时将该文件删除。
2. 继续步骤 5。

步骤 5：软件数据库没有请求的对象：

1. 在分析阶段这种情况应得到控制，如果没有则：
2. 缓存返回 404 文件未找到消息。

查看对等缓存状态页

1. 安装浏览器证书：`browser.p12`

   `browser.p12` 位于任何切分组件捆绑包主机上的以下目录：

   `/var/opt/opsware/crypto/spin/`

   中。根据浏览器导入证书的说明，将文件复制到本地计算机并将 `browser.p12` 导入到浏览器中。

2. 使用 Web 浏览器访问：

   `https://<peer_cache>:1002/oplets/peer_cache.py`

概念：SA 核心通信基础结构

SA 是分布式计算环境，在该环境中，各个组件通过 IP 网络彼此安全地进行通信。为此，SA 使用 SSL/TLS 和 X.509 证书确保这些组件之间通信的安全。

当 SA 核心组件必须与另一个组件通信时，它打开一个使用已知端口的安全通信通道（通常是 SSL/TLS）。每个 SA 核心组件都有一个公钥证书，此证书是在安装 SA 时生成的。当组件向另一个组件进行身份验证时，将使用此公钥证书。大部分进程间通信都经过了强健的身份验证（使用可用的最强密码进行了加密）和完整性检查。

SA 核心间的通信

如果通过多个数据中心运行 SA，则 SA 将自动同步所有 SA 托管的数据中心的数据。从广义上讲，SA 同步两种数据：服务器（包括所有硬件、软件和配置特性信息）和软件包的 SA 模型。

- 复制 SA 模型：SA 使用集成认证的消息来同步 SA 模型数据。SA 实现 SSL 来确保跨消息总线流动的消息的安全。这些消息描述必须对 SA 数据库（模型库）进行的 SQL 更改。
- 复制软件包：SA 按需复制软件包。也就是说，仅在需要时复制软件包。例如，当管理 New Jersey 数据中心服务器的管理员指示 SA 安装在 New Jersey 软件数据库不存在的软件包时，SA 会从其他数据中心请求该数据包。

  实际文件传输使用开放源实用程序 `rsync`，使用 SSH 确保通信通道的安全。卫星端和对等缓存软件数据库的该流程是类似的。

图 33 和**图 34** 显示带有卫星端的两个核心的安装，以及核心的组件如何使用网关进行通信。

图 33.主 SA 核心

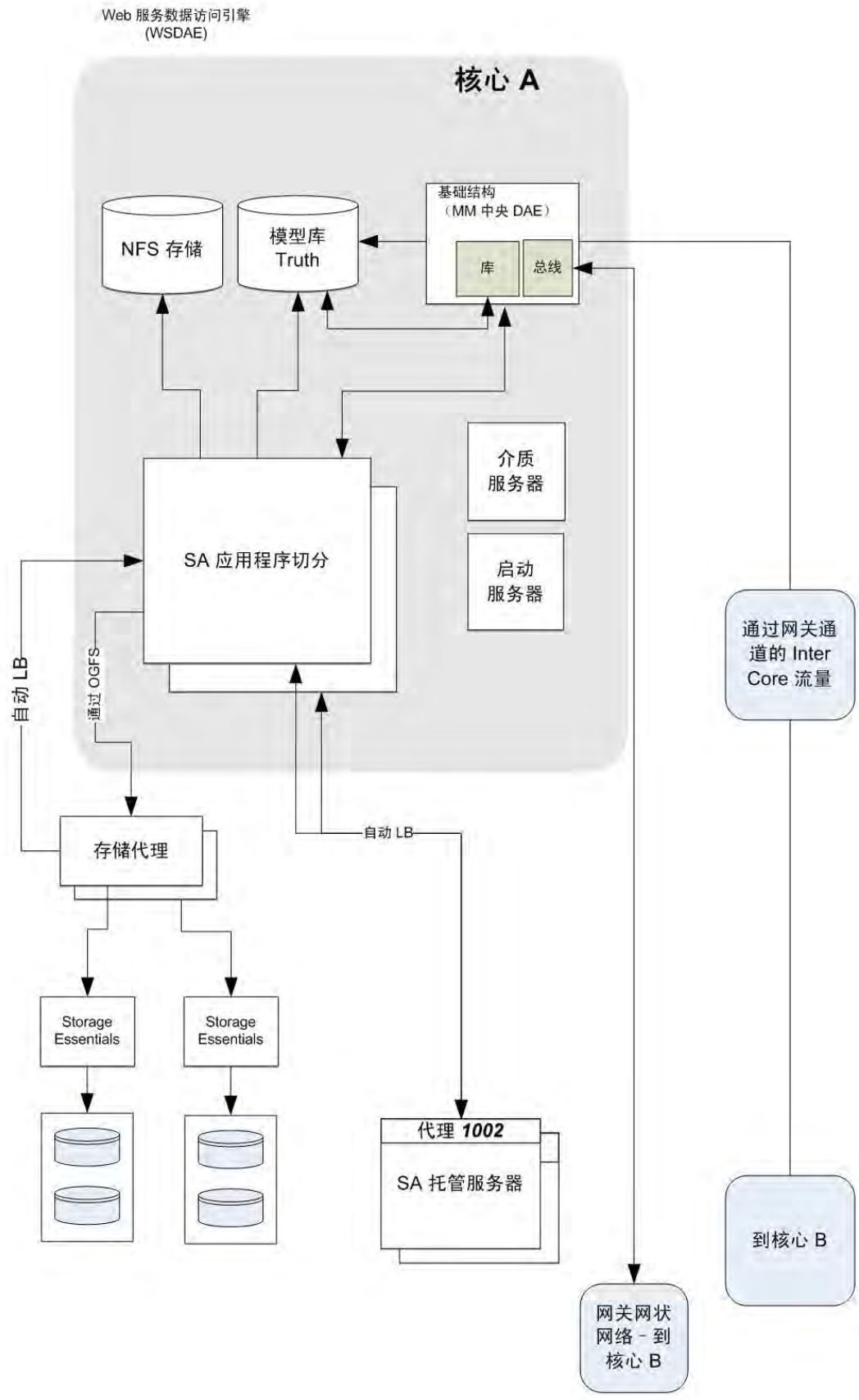
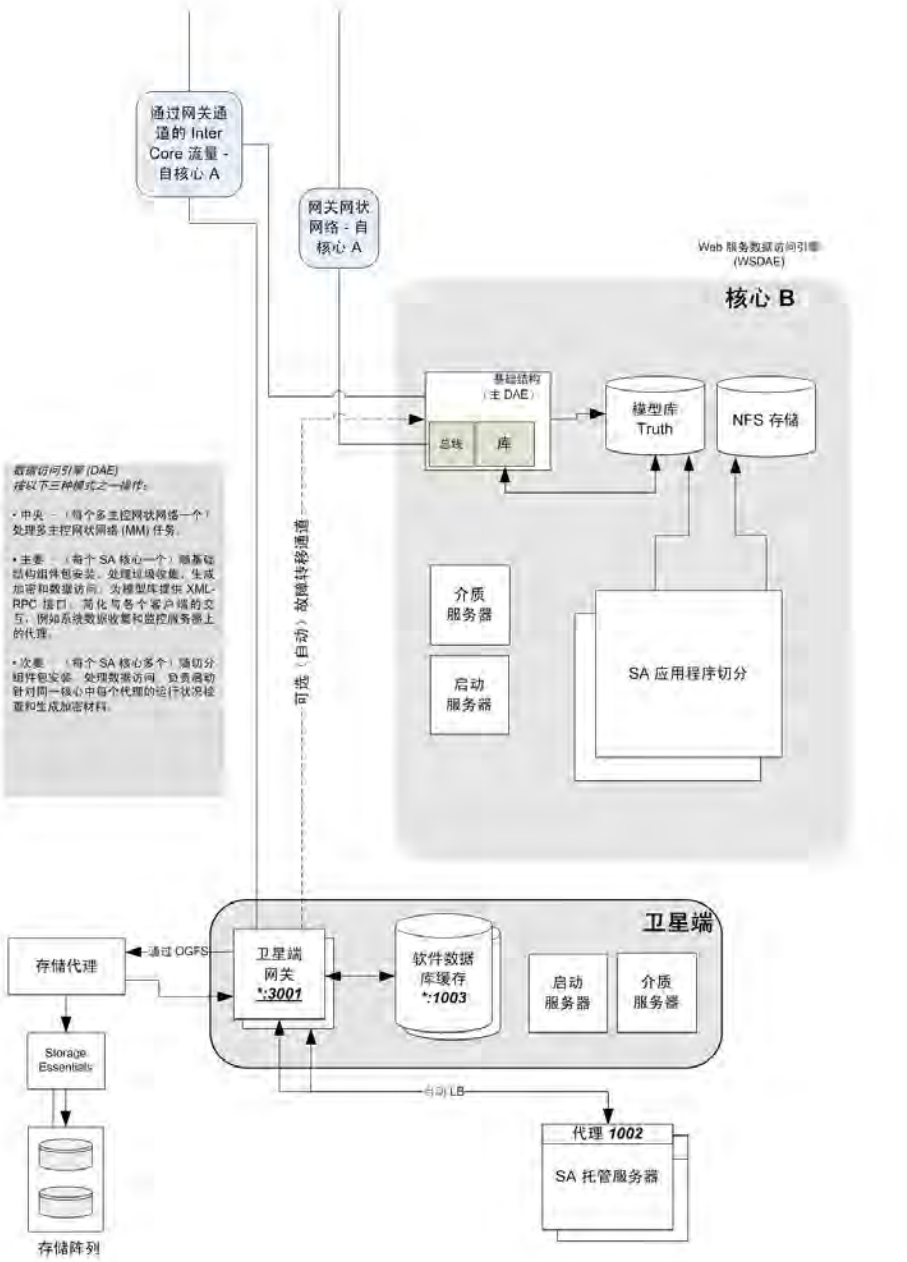

Web 服务数据访问引擎
(WSDAE)
核心 A
NFS 存储
模型库
Truth
基础结构
（MM 中央 DAE）
库
总线
介质
服务器
SA 应用程序切分
启动
服务器
通过网关通
道的 Inter
Core 流量
自动 LB
通过 OGFS
存储代理
自动 LB
Storage
Essentials
Storage
Essentials
代理 1002
SA 托管服务器
到核心 B
网关网状
网络 - 到
核心 B

图 34.次要核心和卫星端



高级：代理与 SA 核心组件之间的通信

安装在托管服务器上的 SA 代理也会参与进行强健的身份验证和加密 SSL/TLS 通信。另外，当代理被指示执行某服务器上的管理任务时，典型的控制消息流将有助于确保仅已授权用户执行这些操作。入侵者很难生成有效命令序列来指示代理执行未经授权的任务。

下面的序列描述典型的 SA 管理任务：在 SA 托管服务器上配置软件。托管服务器上的其他操作遵循相同的常规协议：

1. 数据访问引擎使用 SA 代理通过 HTTPS 打开通信通道,被指示执行管理任务。
2. SA 代理回调数据访问引擎，以检索有关要执行的任务的具体信息。要打开通信通道，代理必须提供其公钥证书，即 SA 核心将用于验证内部数据库是否映射证书本身到该计算机的 IP，它是安装此代理时 SA 生成的唯一计算机标识符。这一保护可防止用户将数字证书和相应密钥简单地复制到另一个想要假扮成原始托管服务器的计算机。

   成功打开通信通道后，SA 代理会收到要安装和删除的软件（以及任何要执行的脚本、软件安装顺序和配置过程期间何时重新启动）的准确列表。
3. SA 代理打开通向软件数据库的通信通道（也是通过 HTTPS）并对它需要安装的软件发出下载请求。在软件数据库启动下载之前，它会重新计算该包的 SHA 校验和以及它所知的密钥。只有当 SHA 校验和与上载数据包时生成的校验和相匹配时，SA 代理才会收到它请求的软件，但还有另一个安全保护措施。

   当 SA 核心不需要直接管理数以百计的同步代理操作时，已启动代理将异步调用 SA 核心为进度报告和长期运行操作提供可扩展支持。即使是在防火墙阻止代理启动 TCP 连接的网络环境中，SA 也支持这些从代理到核心的异步调用，这是因为 SA 网关基础结构可通过单向连接提供双向隧道连接。

代理/核心通信的其他技术详细信息包括：

- 连接是 SSL v3，则与 X.509 证书进行相互验证（服务器检查此客户端证书，反之亦然）。
- 核心和代理证书的私钥存储在只有 root 可读取的文件中。
- 所有证书都在安装时生成，由客户拥有，对于 HP 是未知的。
- 证书在安装 10 年后到期。SA 提供了重新认证工具，以便在证书到期之前重新认证核心和代理。
- 证书由 SA 内部自签名证书颁发机构签名。要避免在 Web 浏览器中出现 HTTPS 安全警告，客户可在 Apache SA 实例中安装外部签名的证书。

本节提供有关 SA 网关所使用的网关属性文件中的参数的参考信息。

SA 网关属性文件语法

网关属性文件中的条目控制网关在当前主机上的操作和配置。

SA 网关属性文件位于每个核心主机上的

```
/var/opt/OPSWgw/gwname/opswgw.properties
```

中。

SA 网关属性文件可以有下列条目：

备注: 不要修改这些条目，除非您确定知道修改对此核心产生的影响。

用法：`./opswgw-tc-70 [options]`

`--Gateway name`

（必需）设置 SA 网关的名称。此名称必须在网关网状网络中唯一。

`--Realm realm`

（必需）所有网关都在一个命名领域中运行。*领域*是一种 SA 构造，它涉及网关在该领域为其提供服务的一系列服务器。领域可支持可与其他领域重叠的 IPv4 地址空间。领域还用来定义针对 SA 函数的带宽使用限制。

`--Root true | false`

指定此网关将当作网关网状网络的 root。root 网状网络中的所有网关必须为 root 网关。

默认值：false。

`--Level int`

（*实验*）网关的路由级别。从 0 到 7 共有八个可能的级别。领域中的所有网关必须具有相同的级别。

默认值：0

`--GWAddress lhost`

设置本地主机地址（如果您为管理网关指定值，则仅使用 IP 地址；不使用主机名称。不过，对其他非管理网关您可以使用主机名），此网关使用该地址告诉其他组件如何与其联系。该值供核心用来发现新的核心端网关。也用于与活动的网关列表通信，这些网关列表通过 `X-OPSW-GWLIST` MIME 标头为代理客户端（如代理）的领域提供服务。

`--Daemon true | false`

守护进程。

默认值：false。

`--Watchdog true | false`

启动内部监视程序进程以在出现失败或信号时重新启动网关。发送到监视程序的 SIGTERM 将停止监视程序和网关进程。

默认值：false。

--User name

启动时切换到此用户。

--RunDir path

启动时切换到此目录。

--ChangeRoot true | false

如果为 true，则 chroot 到 RunDir。帮助器脚本可以使用它来构造居留位置。

默认值：false

--PreBind proto:ip:port, ...

出于安全考虑，运行已 chroot 为无权限使用的网关是非常有帮助的（只有 1024 以上的端口可用于任何侦听器）。如果您想用无权限用户*和*有权限侦听器端口，则可以使用 --PreBind 指令在进程是 root 时且放弃特权之前保留该端口。

--HardExitTimeout seconds

在重新启动或退出请求后，主线程在执行硬退出之前等待内部线程和队列静默的秒数。

--LogLevel INFO | DEBUG | TRACE

设置日志记录级别。请注意 DEBUG 和 TRACE 可产生大量输出，这些输出通常仅与开发人员有关且可对性能产生负面影响。

默认值：INFO.

--LogFile file

SA 日志文件的文件名。

--LogNum num

要保留的滚动日志文件的数量。

`--LogSize size`

每个日志文件的大小（以字节为单位）。

`--TunnelDst [lip1:]lport1[:crypto1],...`

如果已指定，则启动隧道目标侦听器。隧道侦听器可以侦听多个端口（逗号分隔的列表，无空格）。如果端口的前缀为 IP 地址，则侦听器将仅绑定到该 IP 地址。例如：`2001`，`10.0.0.2:2001`，`2001:/var/foo.pem`，`10.0.0.2:2001:/var/foo.pem`

`--TunnelSrc rhost1:rport1:cost1:bw1[:crypto1],...`

如果已指定，则在此网关与在 `rhost1:rport1` 处侦听的网关之间创建一个隧道。必须设置链接 `cost1` 和链接带宽 `bw1`。成本是 32 位无符号整数，带宽的单位为千位/秒（1 千位 = 1024 位）。（其他隧道由逗号分隔。）示例：`gw.foo.com:2001:1:0`，`gw.bar.com:2001:10:256:/var/foo.pem`

`--ProxyPort [lip1:]lport1,[lip2:]lport2,...`

HTTP CONNECT 代理侦听器端口。如果需要多个代理侦听器端口，则可以使用逗号分隔列表添加更多端口。可以通过将 IP 地址附加到端口前面，启用接口绑定。

`--ForwardTCP [lip1:]lport1:realm1:rhost1:rport1,...`

创建静态 TCP 端口转发。将本地端口 `lport(`*x*`)` 转发到 `realm(`*x*`)` 中的远程服务 `rhost(`*x*`):rport(`*x*`)`。空的 `realm`（例如 `lport::rhost:rport`）意味着路由到最近的 Root 领域。

`--ForwardTLS [lip1:]lport1:realm1:rhost1:rport1, ...`

创建 TLS 流量中专用的静态 TCP 端口转发。TLS 会话 ID 经过解析，发送到出口网关以在负载平衡算法中使用。在所有其他方面，此功能的行为类似于 ForwardTCP。

`--ForwardUDP [lip1:]lport1:realm1:rhost1:rport1,...`

创建静态 UDP 端口转发。将本地端口 `lport(`*x*`)` 转发到 `realm(`*x*`)` 中的远程服务 `rhost(`*x*`):rport(`*x*`)`。空的 `realm`（例如 `lport::rhost:rport`）意味着路由到最近的 Root 领域。（注意：某些 UDP 服务，如 DHCP，无法按此方法进行代理。）

`--IdentPort [lip:]lport`

在本地端口 `lport`（可以选择绑定到本地 IP `lip`）上启动 IDENT 服务侦听。

--AdminPort [lip:]lport[:crypto1]

在本地端口 lport（可以选择绑定到本地 IP lip）上启动管理界面侦听。如果您使用 crypto，则包括 crypto 规范文件名。

--ConnectionLimit int

为最大连接数指定软内存调整限制。

--OpenTimeout seconds

等待远程 CONNECT 调用建立远程连接的最大 seconds。

--ConnectTimeout seconds

等待 connect() 完成的最大 seconds。如果发生超时，则向客户端返回 HTTP 503 消息（通过入口网关）。如果 ConnectTimeout 加上网关网状网络转换延迟小于 OpenTimeout，则客户端将获取此消息。

--ReorderTimeout seconds

如果出现无序消息（对于 TCP 流），则限制等待重组所需的消息到达的时间量 (seconds)。无序消息的最常见原因是转换隧道失败而中途采用新路由。

--TunnelStreamPacketTimeout seconds

如果部分 TCP 流不能传送到端点，则 TCP 连接在 seconds 后断开。

--QueueWaitTimeout seconds

指定隧道消息在内部路由队列开头等待（等待恢复隧道时）的最大时间。

--KeepAliveRate seconds

在每个链接上每 *x* 秒发送一次链接 keepalive 消息。

--LsaPublishRateMultiple float

每 k*M 秒发布一次链接状态广告 (LSA)，其中 M 是网状网络中的网关数，k 是使用 --LsaPublishRateMultiple 指定的浮点常量。例如，如果网状网络中有 100 个网关，--LsaPublishRateMultiple 设置为 2.0，则大约每 200 秒发布一次 LSA（由于实现因素，实际延迟将介于 190 和 210 秒之间）。

--LsaTTLMultiple float

将 LSA 的 TTL 设置为 float 乘以 LsaPublishRate。示例：如果 LsaPublishRate 是 10 秒而 LsaTTLMultiple 是 3，则通过此网关发布的 LSA 的 TTL 将设为 30 秒。

--MaxRouteAge seconds

丢弃路由表中 seconds 内未刷新的路由。

--RouteRecalcDutyCycle percentage

如果计算 Dijkstra 的时间花费 tau 秒，则等待 tau*(1/RouteRecalcDutyCycle-1) 秒，直到可进行另一次重新计算。

--TunnelTimeoutMultiple float

此数字乘以 KeepAliveRate 将得出对隧道执行垃圾回收之前隧道处于空闲状态的最大时间。

--DoNotRouteService host1:port1,host2:port2,...

指定当本地客户端创建与 host:port 的代理连接时，不路由消息；而是在本地为其提供服务。使用此属性可确保在网关的当前领域中本地处理某些服务。

--ForceRouteService host1:port1:realm1,host2:port2:realm2,...

在本地客户端创建到 host:port 的代理连接时，强制将该消息路由到指定的领域。

--HijackService host1:port1,host2:port2,...

当本地网关通过隧道看到与 host:port 的连接，且源领域不是本地领域时，它必须为连接提供服务。如果连接来自本地领域，则网关必须允许消息继续前进到其目标。您可以使用此功能实现透明缓存。

--RouteMessages *true | false

如果指定为 true，则开启转换路由。如果为 false，则禁用转换路由。如果消息的目标*不是*本地网关，则默认情况下基于当前路由表来路由消息。如果不需要这种路由，则将此属性设为 false。

--EgressFilter proto:dsthost1:dstport1:srchost1:srcrealm1,...

当本地网关看到从 srchost1:srcrealm1 到 dsthost:dstport 的 TCP 连接尝试时，它必须允许该连接。暗含的默认值为拒绝所有连接。如果您要*允许*所有连接，请将出口

筛选器指定为 *:*:*:*:*。出口筛选器通常也仅允许来自 Root 领域的连接。这可以通过将 srcrealm 保留为空来表示。示例：tcp:10.0.0.5:22:172.16.0.5: 允许从 root 领域中的 172.16.0.5 到 10.0.0.5 端口 22 的 TCP 连接。

```
--IngressMap ip1:name,ip2:name,...
```

当发送开放消息（且 srcip 位于入口映射中）时，将 ip:name 映射（以元数据的形式）附加到该开放消息。这会允许远程出口筛选器将 name 用作 srchost 而不是 ip。此功能支持将服务器添加到场，无需将服务器单独添加到多个 EgressFilter 条目。

```
--LoadBalanceRule proto:thost:tport:mode:rhost1:rport1:
rhost2:rport2, ...
```

当收到 thost:tport 的新连接消息时，将对通过 rhost1:rport1、rhost2:rport2 等真实主机的连接执行负载平衡。负载平衡策略是通过 mode 定义的。

有六种负载平衡模式：

STICKY：根据源 IP 和源领域的哈希随机化的优先级列表，将连接发送到工作目标（可以通过输入 MIME 头 X-OPSW-LBSOURCE 覆盖哈希字符串）。

LC：使用最少数量的连接将连接发送到工作目标。

RR：以循环方式将连接发送到下一个工作目标。

TLS_STICKY：基于会话 ID 缓存，使用 SSLv3/TLSv1.0 会话 ID 将连接发送回上一个目标。如果目标出现错误，或者会话 ID 在缓存中丢失，退回到 STICKY 模式以进行新选择。

TLS_LC：与 TLS_STICKY 模式类似，但是退回到 LC 模式（最少的连接）。

TLS_RR：与 TLS_STICKY 模式类似，但是退回到 RR 模式（循环）。记住为 proto:thost:tport 添加出口筛选器。无需为目标添加出口筛选器。非 TLS 负载平衡模式 *可以* 用于 UDP 服务。

```
--LoadBalanceRetryWindow seconds
```

如果在使用负载平衡的目标（例如上面的 rhost1:rport1）时出错，则目标标记为 in-error。此属性控制网关在重试目标之前等待的秒数。如果目标缺失（如根据连接请求接收到 RST），则负载平衡器将尝试查找正常运行的目标。

在收获 sessionId 关联之前负载平衡的 SSLv3/TLS 客户端可能处于空闲的秒数。此属性影响 TLS 流的出口网关。

```
--SessionIdCacheLimit slots
```

对缓存可保存的 SSLv3/TLS 会话 ID 的数量进行的软限制。如果超出此限制，则垃圾回收器开始降低 SessionIdTimeout 值，以便达到 --SessionIdCacheLimit 所指定的缓存限制。

--MinIdleTime seconds

指定将连接视为收获之前在重载情况下连接处于空闲的最小 seconds 数。

--GCOverloadTrigger float

指定启动重载保护措施的 SoftConnectionLimit 的分数。当打开的连接数达到重载触发器点时，重载保护启动，通过 MinIdleTime 获得最空闲的连接。当连接计数小于重载触发器点时，重载保护停止。

--GCCloseOverload true | false

当客户端尝试在达到 ConnectionLimit 后打开连接时，此属性告知网关应当对新连接采取何种操作。true 值致使网关关闭新连接。false 值致使网关将新连接存放在内核的后备日志中，在重载情况平息后为新连接提供服务。适当的设置取决于应用程序。

默认值：false。

--VerifyRate seconds

当连接停止移动数据达到指定的 seconds 数时，将向远程网关发送一条连接验证消息，以验证该连接仍处于打开状态。此检查定期重复进行，如果已超过超时时间，则此检查无限重复。

--OutputQueueSize slots

指定隧道输出队列的大小。这些队列存储发往远程网关的消息。每个远程网关有一个输出队列。达到 MaxQueueIdleTime 后，队列被执行垃圾回收。

--MaxQueueIdleTime seconds

指定垃圾回收删除空闲输出队列之前保留该队列的最大时间。

--TunnelManagementQueueSize slots

指定用于管理隧道管理流量（如 LSA）的队列的大小。

--TunnelTCPBuffer bytes

指定 TCP SEND 和 RECV 缓冲区的大小（以 bytes 为单位）。操作系统必须配置为处理指定的值。您可以查看网关的日志文件以了解操作系统是否拒绝指定的值。

--DefaultChunkSize bytes

指定当封装 TCP 流时的默认（最大）IO 区块大小。此属性值只能应用于没有带宽限制的链接。

--LinkSaturationTime seconds

当链接有带宽限制时，根据两个参数计算区块大小 DefaultChunkSize。第一个参数是链接的带宽限制。第二个参数是带宽整形程序在链接上应使用完整、实际带宽的时间量。此参数控制带宽整形程序的作用周期。值越小，则带宽控制越平滑，开销成本越大，这是因为每个较小的 IO 区块都有一个标头。

--TunnelPreLoad slots

指定等待第一个 Ack 消息之前要使用的输出队列插槽的最大数量。这将允许对长粗型管道执行管道操作。随着队列数大幅递减，该值呈几何式下降到一。

--BandwidthAveWindow samples

指定带宽估计移动窗口的 IO 速率示例的最大数量。对此窗口中的示例进行平均以提供由隧道使用的低通带宽估计。由于筛选器窗口的边缘很陡，此估计具有高频率组件。

--BandwidthFilterPole float

指定用于删除移动窗口估计器的高频率组件的离散时间一阶平滑筛选器的极点。将该值设置为 0.0 可关闭此筛选器。

--StyleSheet URL

当呈现管理 UI 时将样式表链接添加到 URL。这对于将管理 UI 嵌入到另一个基于 Web 的 UI 中很有帮助。除了使用此属性控制默认样式表，还通过将变量 StyleSheet=<url>/style.css 添加到管理 UI URL 来支持动态样式表覆盖。

--ValidatePeerCN true | false

指定隧道握手操作期间是否针对对等配置验证对等 CN。在安装不可信网关时，必须关闭对等。

默认值：true。

--PropertiesCache file

可以通过借助隧道连接传递的 parametermodify 消息来控制链接成本和带宽。这些针对运行进程的实时调整写入到将覆盖属性文件或命令行参数的参数缓存中。

--PropertiesInclude file

指定要加载并与当前属性合并的包括文件。包括文件中的属性可以覆盖原始属性文件中的属性。可以从命令行指定此属性。如果是，它将覆盖*所有*属性，包括命令行覆盖。它不是递归性的，不支持列表。

```
--PropertiesFile file
```

将所有命令行参数放置在 opswgw 命名空间内的属性文件中。请注意，PropertiesFile 命令行参数本身在 opswgw 命名空间内*必须未*放置在属性文件中。

opswgw 命令行参数

可以将上一节中的所有参数指定为 `opswgw` 命令的选项。例如，网关属性文件中的 `opswgw.Gateway foo` 条目等同于以下命令行参数：

```
/opt/opsware/opswgw/bin/opswgw --Gateway foo
```

命令行参数覆盖网关属性文件中的相应条目。除在上一节列出的条目外，`opswgw` 命令可指定一个网关属性文件为参数；例如：

```
/opt/opsware/opswgw/bin/opswgw --PropertiesFile filename
```

第 6 章

SA 维护

SA 启动/停止脚本

SA 提供多功能脚本用于启动、停止和获取 SA 状态：

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

您可以使用该脚本显示安装在服务器上的所有 SA 组件，启动、停止或重新启动所有核心组件，启动、停止或重新启动特定 SA 组件（除 Oracle 数据库之外的组件）。

有关启动和停止 Oracle 数据库的信息，请参见启动 Oracle 数据库（模型库）。

当在核心组件主机上运行该脚本时，该脚本针对本地系统上安装的每个组件执行必要的先决条件检查。

备注： 如果 SA 核心的组件跨多个服务器分布，则启动/停止脚本无法直接与远程服务器交互来启动或停止远程组件。不过，该脚本可以连接到远程服务器以确定本地启动依赖组件之前是否符合先决条件。

当为在远程服务器上运行的组件检查先决条件时，该脚本通过使用超时值允许服务器之间的启动时间差异和速度差异。如果任何先决条件检查失败，则脚本终止，并显示错误。

启动/停止脚本的依赖关系检查

启动/停止脚本识别 SA 组件的依赖关系，并按正确的顺序启动 SA 组件。先决条件在脚本启动给定组件之前检查验证依赖关系是否满足，从而确保安装在多个服务器上的 SA 组件按正确地顺序启动。

例如，如果您尝试启动的组件要求另一个组件运行，则脚本验证：

- 所要求的组件的主机名是否可解析
- 运行所要求的组件的主机是否正在侦听给定的端口

启动/停止脚本日志

启动/停止脚本写入以下日志：

启动/停止脚本日志记录

日志	备注
`/var/log/opsware/startup`	当服务器引导时，该脚本记录本地系统上安装的所有 SA 组件的启动进程的全文（发送到 `stdout` 的所有文本）。

日志	备注
stdout	当从命令行调用时，该脚本显示组件的启动进程的全文。
syslog	当服务器引导时，该脚本以后台进程形式运行，并将状态消息发送到系统事件记录器。

启动/停止脚本语法

SA 启动/停止脚本具有以下语法：

```
/etc/init.d/opsware-sas [options] [component1] [component2]...
```

当指定特定组件启动、停止或重新启动时，这些组件必须安装在本地系统中，且您必须输入与它们通过 `list` 选项显示的完全一致的名称。表 24 列出 SA 启动/停止脚本的选项。要查看也使用 `opsware-sas` 调用的运行状况检查监控器 (HCM) 的选项，请参见**表 28**。

表 24.SA 启动/停止脚本的选项

选项	描述
list	显示本地系统上安装的且受脚本管理的所有组件。该脚本按组件的启动顺序显示组件。
start	按正确顺序启动本地系统上安装的所有组件。当使用 `start` 选项启动特定组件时，脚本先执行必要的先决条件检查，然后再启动该组件。 `start` 选项不启动 Oracle 数据库（模型库），在 SA 组件启动之前，Oracle 数据库必须启动并运行。 某些 SA 组件（例如 Web 服务数据访问引擎 (twist)）会花费较长时间启动。对于这些组件，您可以使用 `start` 选项来运行该脚本，以便该脚本在本地系统上作为后台进程运行，并将错误和失败的检查组件记录到组件的日志文件中。 **备注:** 注意：当使用 `start` 选项启动服务器上安装的多个组件时，该脚本将始终运行带有 `startsync` 选项的 `/etc/init.d/opsware-sas` 命令。
startsync	`startsync` 选项以同步模式启动本地系统上安装的所有组件。 当您使用 `startsync` 选项时，该脚本在前台运行，并将其进度的摘要消息显示到 `stdout`。
restart	以同步模式停止并启动本地系统上安装的所有组件。脚本先按相反顺序停止所有本地组件，然后再执行 `startsync` 选项按正确顺序重新启动这些组件。
stop	按正确顺序停止本地系统上安装的所有组件。 此选项不停止 Oracle 数据库。

启动 Oracle 数据库（模型库）

SA 启动/停止脚本无法启动（模型库所需的）Oracle 数据库，在 SA 组件运行之前，Oracle 数据库必须启动并运行。在您启动 SA 组件之前，请确保通过输入以下命令启动 Oracle 侦听器和数据库：

```
/etc/init.d/opsware-oracle start
```

启动独立 SA 核心

要启动单一服务器上已安装的核心，请执行下列步骤：

1. 以 `root` 身份登录核心服务器。
2. 启动模型库的 Oracle 侦听器和数据库：

   ```
   /etc/init.d/opsware-oracle start
   ```

3. 启动所有核心组件：

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

启动多服务器 SA 核心

SA 核心启动顺序受多个因素影响。本节描述如何在多主控网状网络配置中启动 SA 核心。

核心组件主机开机

如果在整个网状网络停止的情况下将主机开机，则必须先启动主核心，然后启动每个次要核心。必须一次启动一个次要核心。

请执行下列步骤：

主核心

1. 如有必要，确定托管核心组件的服务器。以 root 身份登录模型库主机并调用以下命令：

   ```
   /etc/init.d/opsware-sas list
   ```

2. 以 `root` 身份登录主核心的模型库主机，启动 Oracle 侦听器和数据库：

   ```
   /etc/init.d/opsware-oracle start
   ```

3. 数据库和侦听器成功启动后，按以下顺序，在下列核心组件主机上运行 SA 启动脚本，一次一个服务器：
   - 基础结构组件捆绑包主机
   - 切分组件捆绑包（初始切分）（如果没有与基础结构组件捆绑包安装在同一个主机上）
   - 后续切分组件捆绑包主机
   - OS 配置组件捆绑包主机
   - 与核心关联的卫星端主机

   在每个主机上使用下列命令调用 SA 启动脚本：

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

您在下一个服务器上调用启动脚本之前，启动脚本必须完全成功启动每个主机上的所有核心组件。

次要核心

其启动顺序与上面所述一致，但必须在主核心组件成功启动后才能被执行。必须一次仅在一个次要核心上启动核心组件。

核心组件主机关机

核心组件主机关机后，主机的开启也会启动 SA；因此必须按以下顺序启动主机：

- 基础结构组件捆绑包主机
- 切分组件捆绑包 (Slice0)（如果没有与基础结构组件捆绑包安装在同一个主机上）
- 其他切分组件捆绑包（Slice1 到 Slice n），一次打开一个
- OS 配置组件捆绑包主机
- 与核心关联的卫星端主机，一次打开一个

主机必须一次一个地开机，SA 核心组件必须成功启动才能将下一个服务器开机。您可以在 `/var/opt/opsware/log/startup` 中的最近创建的日志文件中使用 tail 命令以确定每个主机上组件的启动状态。

启动单个 SA 核心组件

如果这些组件在本地系统上运行，则可指定一个或多个组件启动。您必须严格按照 `opsware-sas` 命令的 `list` 选项的显示来输入组件名称。

要启动 SA 核心的单个组件，请执行下列步骤：

1. 以 `root` 身份登录具有您要启动的组件的服务器。
2. （可选）要列出服务器上安装的 SA 组件，请输入以下命令：

   ```
   /etc/init.d/opsware-sas list
   ```

3. 输入以下命令，其中 *component* 是 `list` 选项显示的名称：

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

   例如，如果 `list` 选项显示 `buildmgr`，则输入以下命令启动 OS 配置构建管理器：

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

提示： 另外，可以在服务器上启动组件时输入 `startsync` 选项。有关 `startsync` 选项的描述，请参见本章中的表 24.SA 启动/停止脚本的选项。

单个 SA 核心组件的启动顺序

SA 启动脚本按下列顺序启动主机上安装的核心组件。当该脚本停止主机上安装的组件时，它按与启动顺序相反的顺序停止这些组件。

1. opswgw-mgw：SA 主核心主网关
2. opswgw-cgws0-<facility>：运行核心的设施的核心端网关
3. opswgw-cgws：网状网络中的其他网关
4. vaultdaemon：模型库多主控组件
5. dhcpd：OS 配置功能的组件
6. pxe：PXE 引导环境
7. memcached：与软件数据库加速器 (tsunami) 组件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。
8. spin：数据访问引擎
9. mm_wordbot：软件数据库的组件
10. tsunami：软件数据库加速器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。
11. waybot：命令引擎
12. smb：OS 配置功能的组件
13. twist：Web 服务数据访问引擎
14. buildmgr：OS 配置构建管理器
15. opswgw-agw0-<facility>：运行核心的设施的代理端网关
16. opswgw-agws：代理网关
17. hub：全局文件系统的组件
18. sshd：全局文件系统的组件
19. apxproxy：自动化平台扩展 (APX) 代理
20. spoke：全局文件系统的组件
21. agentcache：全局文件系统的组件
22. occ.server：SA Web 客户端的组件
23. httpsProxy：SA Web 客户端的组件
24. da：应用程序部署组件
25. opsware-agent：服务器代理

停止具有多个主机的 SA 核心

当关闭网状网络时，每个核心必须按与启动顺序相反的顺序关闭，核心中的每个主机必须按与启动顺序相反的顺序关机。必须一次一个地关闭每个次要核心，最后关闭主核心。

在每个核心（主要或次要）中，/etc/init.d/opsware-sas stop 需要按以下顺序在服务器上运行：

- 与核心关联的卫星端主机，一次关闭一个
- OS 配置组件捆绑包主机
- 其他切分组件捆绑包（Slice1 到 Slice n），一次关闭一个
- 切分组件捆绑包 (Slice0)（如果没有与基础结构组件捆绑包安装在同一个主机上）

- 基础结构组件捆绑包主机
- 数据库/模型库主机

要在主机上停止核心组件，请调用以下命令：

```
/etc/init.d/opsware-oracle stop
```

多个数据访问引擎

本节将讨论下列主题：

- 多个数据访问引擎概述
- 将数据访问引擎重新分配给次要角色
- 指定多主控中心数据访问引擎

多个数据访问引擎概述

在具有多个数据访问引擎实例的核心中，可以按下列方法之一指定每个实例：

1. 主数据访问引擎：每个设施只有一个*主* 数据访问引擎。此数据访问引擎定期检查托管服务器以确定 SA 是否可以与它们通信。如果一个设施具有多个主数据访问引擎，则竞争的可达性检查可能相互干扰。
2. 次级数据访问引擎：如果一个设施安装了多个数据访问引擎（用于实现可扩展性），则可以将非主数据访问引擎指定为次级数据访问引擎。将安装的第一个数据访问引擎指定为主数据访问引擎或多主控中心数据访问引擎。次级数据访问引擎不检查托管服务器以确定它们是否可达。它只与模型库进行通信来写入或读取数据。
3. 多主控中心数据访问引擎：一个 SA 主控网状网络有多个核心因此也有多个数据访问引擎。应当将一个核心的主数据访问引擎指定为*多主控中心数据访问引擎*。虽然任何核心都可能具有多个数据访问引擎，但是只能有一个网状网络是中心数据访问引擎。

将数据访问引擎重新分配给次要角色

如果您安装了其他数据访问引擎，则必须执行下列步骤以将新的数据访问引擎重新分配给次要角色：

1. 以 SA Administrators 组成员用户身份登录 SA 客户端。将显示 SA 客户端主页。
2. 从“导航”面板，单击“管理”>“Opsware 软件”。将显示“软件”页。
3. 单击“spin”链接。将显示“Opsware 软件 | spin”页。
4. 选择“成员”选项卡。将显示托管数据访问引擎的托管服务器的列表。
5. 选中“其他数据访问引擎服务器”的复选框。
6. 从“任务”菜单，选择“重新分配节点”。
7. 选择“服务级别 | Opsware | spin 节点”的选项。

8. 单击“选择”。
9. 通过单击下列节点导航节点层次结构：
   - Opsware
   - spin
   - Secondary
10. 单击“重新分配”。
11. 在终端窗口，以 `root` 身份登录到运行其他数据访问引擎的服务器，然后输入以下命令重新启动数据访问引擎：

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

指定多主控中心数据访问引擎

HP BSA 安装程序自动分配多主控中心数据访问引擎。

警告： 大多数情况下，在安装之后无需对多主控中心数据访问引擎进行更改。否则会导致将 SA 核心升级到新版本时出现问题。按照本节中的步骤操作之前，请联系 HP 专业服务人员。

执行下列步骤指定多主控中心数据访问引擎：

1. 以 SA System Administrators 组成员用户身份登录 SA 客户端。
2. 在导航面板中，单击“管理”下面的“Opsware 软件”。将显示“Opsware 软件”页。
3. 单击“spin”链接。
4. 选择“服务器”选项卡。
5. 选中新核心的数据访问引擎服务器的复选框。
6. 从“服务器”菜单，选择“重新分配节点”。
7. 选择“服务级别 | Opsware | spin | 节点”的选项。
8. 单击“选择”。
9. 通过单击每个节点导航节点层次结构：“Opsware | Spin | 多主控中心”。
10. 单击“重新分配”。
11. 重新启动多主控中心数据访问引擎。

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

计划审核结果和快照删除

因为审核结果和快照（快照规范的结果）可随着时间进行积累，按重复计划运行时尤其如此，所以您可以对 SA 核心进行配置，这样审核结果和快照将在指定天数后从该核心删除。

请注意，此设置仅适用于尚未存档的审核结果和快照。存档结果只能从 SA 客户端中手动删除。

另外，在下列两种情况下，审核结果*或*快照将无法通过这些设置删除：

- 如果快照正在用作审核的目标
- 如果审核结果*或*快照*是*审核或快照规范的唯一结果

配置审核结果和快照删除

1. 在 SA 客户端中选择“管理”选项卡。
2. 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。
3. 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。
4. 查找并修改下列系统配置参数：
   - 查找 `spin.cronbot.delete_audits.cleanup_days` 参数。直接输入新值，或者选择新值按钮  ，输入删除所有非存档审核结果之前必须经过的天数。如果您选择“默认值”，将不删除任何审核。
   - 查找 `spin.cronbot.delete_snapshots.cleanup_day` 参数。直接输入新值，或者选择新值按钮  ，输入删除所有非存档快照之前必须经过的天数。如果您选择“默认值”，将不删除任何快照。
5. 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。

Web 服务数据访问引擎配置参数

本节将讨论如果使用 SA 客户端或通过编辑配置文件更改 Web 服务数据访问引擎系统配置参数。

备注：在更改任何系统配置参数后，必须重新启动 Web 服务数据访问引擎。

更改系统配置参数

本节描述了如何使用 SA 客户端更改一些系统配置参数。其他参数只能通过编辑配置文件（如Web 服务数据访问引擎配置文件所述）来更改。

要在 SA 客户端中更改 Web 服务数据访问引擎的系统配置参数，请执行以下步骤：

1. 在 SA 客户端中选择“管理”选项卡。
2. 在导航面板中选择“系统配置”。将显示包含系统配置参数的 SA 组件、设施和领域。
3. 在 SA 组件列表中，选择“Web 服务数据访问引擎”。将显示此组件的系统配置参数。
4. 查找并修改要更改的系统配置参数。
5. 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。
6. 使用以下命令重新启动 Web 服务数据访问引擎：

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

Web 服务数据访问引擎配置文件

Web 服务数据访问引擎配置文件包括影响 SA Web 服务 API 2.2 的服务器端的属性。（这些属性未显示在 SA 客户端中）。完全合格的配置文件名称如下：

```
/etc/opt/opsware/twist/twist.conf
```

备注： 在 SA 升级期间，将替换 `twist.conf` 文件，但是保留 `twist_custom.conf` 文件。当您升级到新 SA 版本以保留配置设置时，必须编辑 twist_custom.conf 文件。`twist_custom.conf` 中的属性覆盖 `twist.conf` 中指定的属性。UNIX `twist` 用户必须有 `twist_custom.conf` 文件的写入访问权限。

更改配置文件中定义的属性：

1. 使用文本编辑器打开 `twist.conf` 文件。
2. 保存更改的文件。
3. 在服务器上重新启动 Web 服务数据访问引擎。

备注： 您必须属于 Administrators 组 (admin) 才能修改 `twist.conf` 文件。一旦文件已更改，必须重新启动 Web 服务数据访问引擎才能应用更改。

下表列出影响 SA Web 服务 API 2.2 的配置文件的属性。这些属性中的一些属性与服务器事件的缓存（滑动窗口）相关。SA 维护事件的滑动窗口（默认大小为两个小时），用于描述对 SA 对象的更改。此窗口使软件开发人员不必检索所有对象，即可更新对象的客户端缓存。有关详细信息，请参见 `EventCacheService` 的 API 文档。

Configuration File for SA Web Services API 2.2

属性	默认值	描述
`twist.webservices.debug.level`	1	一个为服务器端的 SA Web 服务 API 设置调试级别的整数值。允许的值： 0 - 基本信息 1 - 详细信息 2 - 堆栈跟踪 3 - 当某个项添加到缓存时，用于打印服务器事件缓存条目。
`twist.webservices.locale.country`	US	Localizer 实用程序的国家/地区国际化参数。当前仅支持 US 代码。

属性	默认值	描述
twist.webservices.locale.language	en	Localizer 实用程序的语言国际化参数。当前仅支持 en 代码。
twist.webservices.caching.windowsize	120	维护服务器事件缓存的滑动窗口的大小（以分钟为单位）。
twist.webservices.caching.windowslide	15	维护服务器事件缓存的窗口的滑动范围（以分钟为单位）。
twist.webservices.caching.safetybuffer	5	维护服务器事件缓存的滑动窗口的安全缓冲区（以分钟为单位）。
twist.webservices.caching.minwindowsize	30	维护服务器事件缓存的滑动窗口的最小大小（以分钟为单位）。
twist.webservices.caching.maxwindowsize	240	维护服务器事件缓存的滑动窗口的最大大小（以分钟为单位）。

增加 Web 服务数据访问引擎最大堆内存分配

当多主控网状网络中的数据增长时，您可能会发现您必须增大 Web 服务数据访问引擎的最大堆内存分配 (twist)。默认值为 1280Mb。为此，请执行下列任务：

1. 使用文本编辑器，打开文件：

   /etc/opt/opsware/twist/twist_custom.conf

2. 请修改所需分配的以下条目：

   twist.mxMem=<memory size>

   其中，内存大小对应于 -Xmx<memory size>。

   例如：

   twist.mxMem=2048m

   将给予 Web 服务数据访问引擎一个最大值为 2048 兆字节的堆内存。即使在升级后，该更改也会保留。如果将此 twist_custom.conf 参数留空，则使用 twist.sh 中指定的默认值 (1280m)。

更改软件数据库镜像参数

软件数据库镜像可使多主控网状网络中的软件数据库保持冗余和灾难恢复的同步。本节描述如何更改软件数据库镜像配置参数。有关详细信息，请参见软件数据库监控。

更改系统配置参数

本节描述了如何使用 SA 客户端更改一些系统配置参数。其他参数只能通过编辑配置文件（如Web 服务数据访问引擎配置文件所述）来更改。

要在 SA 客户端中更改 Web 服务数据访问引擎的系统配置参数，请执行以下步骤：

1. 在 SA 客户端中选择“管理”选项卡。
2. 在导航面板中选择“系统配置”。将显示包含系统配置参数的 SA 组件、设施和领域。
3. 在 SA 组件列表中，选择“Web 服务数据访问引擎”。将显示此组件的系统配置参数。
4. 查找并修改要更改的系统配置参数。
5. 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。
6. 使用以下命令重新启动 Web 服务数据访问引擎：

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

软件数据库镜像配置参数

您可以通过修改下列配置参数，启用软件数据库镜像和设置镜像作业的运行频率。软件数据库镜像作业在软件数据库之间复制数据，以使它们都保持同步。有关详细信息，请参见软件数据库监控。

软件数据库镜像参数

参数	类型	允许的值	默认值	描述
word.enable_content_mirroring	布尔标记	0 或 1	0	将此值设置为 1 将启用软件数据库镜像。将此值设置为 0 将禁用它。
word.mirror_job_period	分钟	任何正整数	60	此值指定软件数据库镜像作业的运行频率。

第 7 章

监控 SA 核心组件

您需要时常监控 SA 内部组件以进行故障排除并调整组件行为。

SA 监控概述

SA 在 SA 客户端中提供系统诊断测试以诊断下列 SA 组件的功能：

- 数据访问引擎
- 软件数据库
- 命令引擎
- Web 服务数据访问引擎
- 多主控基础结构组件（在 SA 文档中称作模型库多主控组件）

本节提供有关对上述组件和下列附加 SA 组件执行基本监控的信息：

- 服务器代理
- 代理缓存
- SA 客户端
- 模型库
- 轮辐
- 网关
- OS 构建管理器
- OS 启动服务器
- OS 介质服务器

当由于 SA 客户端无法运行而无法使用系统诊断测试时，或者当托管环境已设置进行自动监控时，使用此信息。在这种情况下，您可以使用这些命令自动执行系统诊断和监控 SA。

该监控包括：

- 确认特定组件进程正在运行的命令，以及期望输出的示例
- 组件和操作系统所提供的命令
- 组件特定的端口、日志和管理 URL

备注： 此文档中显示的命令必须都输入到一行中。不过，为了确保命令和生成的输出可读，已经用空格、空行和换行符或反斜杠 (\) 对它们进行修改，以指示命令在下一行的何处继续。另外，显示的输出仅作为示例。您的服务器上的输出将有所不同。

有关本文中提及的每个 SA 组件的描述，请参见《SA 概述和体系结构》指南。

代理监控

服务器代理是在 SA 管理的每个服务器上运行的软件模块。无论何时需要更改托管服务器时，服务器代理都会代理请求。

有关服务器代理的详细信息，请参见《SA 用户指南：Server Automation》。

要使用 SA 客户端来测试 SA 核心与托管服务器上运行的服务器代理之间的通信，请参见《SA 用户指南：Server Automation》中的以下章节：

- 代理可达性通信测试
- 通信测试故障排除

代理端口

服务器代理使用端口 1002。

监控代理的进程

在 Windows 上的“开始”菜单中，选择“运行”。在“运行”对话框中，输入 `taskmgr`。在“Windows 任务管理器”对话框中，单击“进程”选项卡，查找称为 `watchdog.exe` 和 `python.exe` 的进程。

在 UNIX（Solaris、Linux、AIX 和 HP-UX）上，服务器代理有两个运行进程。

在 Solaris 上，执行以下命令：

```
# ps -flg `awk -F= '($1=="pgrp") {print $2}'
/var/opt/opsware/agent/daemonbot.pid`
```

运行此命令应当生成类似如下的输出：

```
F S  UID  PID  PPID  C  PRI
NI  ADDR  SZ  WCHAN  STIME  TTY  TIME  CMD

8 S  root 9541 9539  0  41  20  ?    1768 ?     Aug
08  ?    1:23 /opt

/opsware/agent/bin/python
/opt/opsware/agent/pylibs/shadowbot/daemonbot.pyc --conf
/etc/opt/opsware/agent/agent.args

8 S  root  9539   1  0  99  20  ?    398  ?     Aug
08  ?    0:00 /opt

/opsware/agent/bin/python
/opt/opsware/agent/pylibs/shadowbot/daemonbot.pyc --conf
/etc/opt/opsware/agent/agent.args
```

在 Linux 上，执行以下命令：

```
# ps -flg `awk -F= '($1=="pgrp") {print $2}'
/var/opt/opsware/agent/daemonbot.pid`
```

运行此命令应当生成类似如下的输出：

```
F S  UID  PID  PPID  C  PRI
NI  ADDR  SZ  WCHAN  STIME  TTY  TIME  CMD

1 S  root 2538 1     0  85  0   -    3184 wait4  Sep11  ?
00:00:00

/opt/opsware/agent/bin/python
/opt/opsware/agent/pylibs/shadowbot/daemonbot.pyc --conf
/etc/opt/opsware/agent/agent.args

5 S  root 2539 2538  0  75  0   -   30890 schedu Sep11  ?
0:02:56

/opt/opsware/agent/bin/python
/opt/opsware/agent/pylibs/shadowbot/daemonbot.pyc --conf
/etc/opt/opsware/agent/agent.args
```

守护程序监控器是 PPID 为 1 的进程。其他是服务器或监控器线程。

在 AIX 上，执行以下命令：

```
# ps -flg `awk -F= '($1=="pgrp") {print $2}'
/var/opt/opsware/agent/daemonbot.pid`
```

运行此命令应当生成类似如下的输出：

```
F    S UID  PID  PPID  C  PRI
NI  ADDR  SZ  WCHAN  STIME  TTY  TIME  CMD

40001 A root 110600 168026 0 60 20 2000d018 16208 * Sep 05 -
7:15 /opt/

opsware/agent/bin/python
/opt/opsware/agent/pylibs/shadowbot/daemonbot.pyc --conf
/etc/opt/opsware/agent/agent.args

40001 A root 168026 1  0  60 20 2000f25c 1352       Sep 05 -
0:02 /opt/

opsware/agent/bin/python
/opt/opsware/agent/pylibs/shadowbot/daemonbot.pyc --conf
/etc/opt/opsware/agent/agent.args
```

在 HP-UX 上，执行以下命令：

```
# ps -flg `awk -F= '($1=="pgrp") {print $2}'
/var/opt/opsware/agent/daemonbot.pid`
```

运行此命令应当生成类似如下的输出：

```
F  S  UID  PID  PPID  C  PRI  NI     ADDR  SZ  WCHAN  STIME TTY
TIME COMD
```

```
1  R root 10009  1    0  152 20 437eb1c0 266      - Sep 22 ?0:00
/opt/

opsware/agent/bin/python
/opt/opsware/agent/pylibs/shadowbot/daemonbot.pyc --conf
/etc/opt/opsware/agent/agent.args

1  R root 10010 10009 0  152 20 434fb440 2190    - Sep 22  ?3:29
/opt/

opsware/agent/bin/python
/opt/opsware/agent/pylibs/shadowbot/daemonbot.pyc --conf
/etc/opt/opsware/agent/agent.args
```

代理日志

服务器代理在托管服务器上创建下列日志文件。

Windows:

- `%ProgramFiles%Common Files\opsware\log\agent\agent.log*`
- `%ProgramFiles%Common Files\opsware\log\agent\agent.err*`

UNIX:

- `/var/log/opsware/agent/agent.log*`
- `/var/log/opsware/agent/agent.err*`

监控UNIX日志的条件:

- 包含"Traceback"的字符串
- 包含"OpswareError"的字符串

代理日志

服务器代理在托管服务器上创建下列日志文件。

Windows:

- `%ProgramFiles%Common Files\opsware\log\agent\agent.log*`
- `%ProgramFiles%Common Files\opsware\log\agent\agent.err*`

UNIX:

- /var/log/opsware/agent/agent.log*
- /var/log/opsware/agent/agent.err*

监控 UNIX 日志的条件：

- 包含“Traceback”的字符串
- 包含“OpswareError”的字符串

代理缓存监控

代理缓存是在代理部署过程中为服务器代理安装文件提供服务的组件。代理缓存组件缓存最新版本的 SA 代理。当 SA 在服务器上安装代理以对其进行管理时，它包含代理缓存组件中的代理安装二进制文件。

监控代理缓存的进程

在所有配置中，代理缓存组件都有一个运行进程。

在 Solaris 或 Linux 上，在运行网关的服务器（位于 SA 核心和卫星中）上执行以下命令：

```
# ps auxwww | grep -v grep | grep agentcache
```

运行此命令应当生成类似如下的输出：

```
root  22288  0.5  0.1  15920  4464  ?S  19:55  0:08  /opt/opsware-
/bin/

python /opt/opsware/agentcache/AgentCache.pyc -d
/var/opt/opsware/agent_installers -p 8081 -b
```

代理缓存日志

代理缓存日志位于以下文件中：

- /var/log/opsware/agentcache/agentcache.log
- /var/log/opsware/agentcache/agentcache.err

日志中要监控的情况：

- 包含“Error downloading agent”的字符串
- 包含“Another process is listening on port”的字符串

命令中心监控

命令中心是基于 Web 的 SA 用户界面。使用 SA 客户端可进入命令中心。

SA 用户通过 Apache HTTPS 代理（由带有命令中心组件的 HP BSA 安装程序安装）连接到命令中心组件。

命令中心端口

HTTPS 代理使用端口 443 (HTTPS) 和端口 80，将连接指向命令中心组件，命令中心组件使用端口 1031（Web 服务端口）。

监控命令中心的进程

在 Linux 上，在运行命令中心组件的服务器上执行以下命令：

```
# ps -eaf | grep -v grep | grep java | grep occ
```

运行此命令应当生成类似如下的输出：

```
occ  17373  1  6  19:46  ?00:02:35  /opt/opsware/j2sdk1.4.2_
10/bin/

java -server -Xms256m -Xmx384m -XX:NewRatio=3 -
Docc.home=/opt/opsware/occ -Docc.cfg.dir=/etc/opt/opsware/occ -
Dopsware.deploy.urls=,/opt/opsware/occ/deploy/ -
Djboss.server.name=occ -
Djboss.server.home.dir=/opt/opsware/occ/occ -Djboss.server.
```

提示: 要监控命令中心组件，还可以设置自动监控进程以将 URL 查询（使用 Wget 等工具）发送到命令中心 URL。如果命令中心组件返回其登录页，则说明 Apache HTTPS 代理和命令中心进程都运行正常。

命令中心日志

命令中心不生成其自己的日志。命令中心使用 JBoss 服务器，JBoss 服务器写入下列日志文件：

- `/var/log/opsware/occ/server.log*`
- `/var/log/opsware/httpsProxy/*log*`

日志中要监控的情况：

- `java.net.ConnectionException`
- `java.net.SocketException`
- `java.lang.NullPointerException`

负载平衡网关监控

负载平衡网关在 SA 核心中提供高可用性和横向扩展。

当您运行 HP BSA 安装程序时，它安装带有命令中心组件的负载平衡网关。

负载平衡网关端口

默认情况下，负载平衡网关使用端口 8080。

监控负载平衡网关的进程

在所有的配置中，负载平衡网关组件有两个运行进程 - 网关进程本身和其监视程序进程。

在 Solaris 或 Linux 上，在运行命令中心组件的服务器上执行以下命令：

```
# ps -eaf | grep -v grep | grep opswgw | grep lb
```

运行此命令应当生成类似如下的输出：

```
root  32149  1  0  Sep27  ?00:00:00  [opswgw-watchdog-2.1.1: lb]
--PropertiesFile /etc/opt/opsware/opswgw-lb/opswgw.properties --
BinPath /opt/opsware/opswgw/bin/opswgw
root  32156  32149  0  Sep27  ?00:24:31  [opswgw-gateway-2.1.1:
lb]
--PropertiesFile /etc/opt/opsware/opswgw-lb/opswgw.properties --
BinPath /opt/opsware/opswgw/bin/opswgw --Child true
```

负载平衡网关日志

负载平衡网关日志位于以下文件中：

- `/var/log/opsware/gateway-name/opswgw.log*`

日志中要监控的情况：

- 字符串包含“ERROR”
- 字符串包含“FATAL”（表示进程将终止）

数据访问引擎监控

数据访问引擎简化了与 SA 中的各种客户端（如命令中心、系统数据收集和服务器上的监控代理）的交互。

数据访问引擎端口

数据访问引擎对外部使用端口 1004 (HTTPS)，对于同一服务器上安装的 SA 组件，则使用端口 1007（回路接口）。

多主控中心数据访问引擎端口转发

网状网络中的多主控中心数据访问引擎与该网状网络中其他 SA 核心中的模型库之间的 SQLnet 流量通过 SA 网关网状网络进行路由。

运行多主控中心数据访问引擎的服务器上的 tnsnames.ora 文件指向其他 SA 核心中每个核心端网关上的指定端口。运行多主控中心数据访问引擎的核心中的核心端网关将连接转发到每个其他核心中的核心端网关，这些网关接下来又将连接转发到其他核心中的模型库。

核心端网关上的端口号计算为 20000 + data_center_id。例如，如果多主控网状网络有两个设施（设施 ID 为 1 的设施 A 和设施 ID 为 2 的设施 B），则设施 A 中的多主控中心数据访问引擎需要连接到运行网关的服务器上的端口 20002，才能访问设施 B 中的模型库。

有关多主控中心数据访问引擎的信息，请参见多个数据访问引擎。

有关网关网状网络拓扑的信息，请参见《SA 概述和体系结构》指南。

监控数据访问引擎的进程

在 Linux 上，在运行数据访问引擎组件的服务器上执行以下命令：

```
# ps auxwww | grep -v grep | grep spin | grep -v java
```

运行此命令应当生成类似如下的输出：

```
root  30202  0.0  0.0  13592  1500  ?S  Sep11 0:01
/opt/opsware/bin/

python /opt/opsware/pylibs/shadowbot/daemonbot.pyc --conf
/etc/opt/opsware/spin/spin.args

root  30204  1.3  0.6  154928  25316  ?S  Sep11  411:15
/opt/opsware/

bin/python /opt/opsware/pylibs/shadowbot/daemonbot.pyc
--conf /etc/opt/opsware/spin/spin.args

root  30256  0.1  0.3  28500  13024  ?S  Sep11  50:35
/opt/opsware/

bin/python /opt/opsware/spin/certgenmain.pyc --start
--conf /etc/opt/opsware/spin/spin.args
```

数据访问引擎 URL

- https://spin.<data_center>:1004

  要访问数据访问引擎 (spin) UI，需要浏览器证书 browser.p12。

  browser.p12 位于任何切分组件捆绑包主机上的以下目录：

  /var/opt/opsware/crypto/spin/

  中。根据浏览器导入证书的说明，将文件复制到本地计算机并将 browser.p12 导入到浏览器中。
- https://spin.<data_center>:1004/ObjectBrowser.py?cls=Account&id=0

  当模型库组件未运行时，访问第二个 URL 将失败。

- `https://spin.<data_center>:1004/sys/dbstatus.py`

  访问此 URL 将在 HTML 页中显示数据库连接状态。您的自动监控系统可以使用正则表达式提取活动数据库连接数。

数据访问引擎日志

数据访问引擎日志位于以下文件中：

- `/var/log/opsware/spin/spin.err*`（主数据访问引擎错误文件）
- `/var/log/opsware/spin/spin.log*`（主数据访问引擎日志文件）
- `/var/log/opsware/spin/spin_db.log`
- `/var/log/opsware/spin/daemonbot.out`（应用程序服务器的输出）

在具有多个数据访问引擎的核心中，每个运行数据访问引擎的服务器都有一组上述日志文件。

Web 服务数据访问引擎监控

Web 服务数据访问引擎为其他 SA 组件提供更好的性能。

Web 服务数据访问引擎组件作为切分组件捆绑包的一部分进行安装。

Web 服务数据访问引擎端口

Web 服务数据访问引擎使用端口 1032。

命令中心组件通过端口 1026（专用回路端口）与 Web 服务数据访问引擎进行通信。

监控 Web 服务数据访问引擎的进程

在 Linux 上，在运行命令中心组件的服务器上和运行切分组件捆绑包的服务器上执行以下命令：

ps auxwww | grep -v grep | grep \/opt\/opsware\/twist

运行此命令应当生成类似如下的输出：

twist 4039 0.2 11.3 2058528 458816 ?S Sep11 80:51 /opt/opsware/

j2sdk1.4.2_10/bin/java -server -Xms256m -Xmx1280m -XX:MaxPermSize=192m -Dorg.apache.commons.logging.Log=org.apache.commons.logging.impl.Jdk14Logger .....

twist 4704 0.0 0.0 4236 1124 ?S Sep11 1:28 /bin/sh /opt/

opsware/twist/watchdog.sh start 60'

twist 4743 0.0 0.6 376224 27160 ?S Sep11 18:31 /opt/opsware/

j2sdk1.4.2_10/bin/java -server -Xms16m -Xmx128m -Dtwist.port=1026 .....-classpath /opt/opsware/j2sdk1.4.2_10/jre/.....

Web 服务数据访问引擎 URL

https://occ.<data_center>:1032

Web 服务数据访问引擎日志

Web 服务数据访问引擎日志位于下列文件中：

- /var/log/opsware/twist/stdout.log*
- /var/log/opsware/twist/twist.log
- /var/log/opsware/twist/access.log
- /var/log/opsware/twist/server.log*（应用程序级别日志记录）
- /var/log/opsware/twist/boot.log
- /var/log/opsware/twist/watchdog.log

stdout.log 文件包含 stdout 和 stderr，并记录任何 System.out.println()、System.err.println() 和 e.printStackTrace() 消息的输出；不过，只有某些异常将显示在这些日志中。可以通过 twist.conf 配置文件数和每个文件的大小。当达到指定的最大文件大小时，将创建附加日志。stdout.log 是最新文件，stdout.log.1 到 stdout.log.5 渐增的早期文件。该文件还会在启动时轮循。

twist.log 文件包含 WebLogic 特定消息和 WebLogic 级别异常。这些文件在启动时轮循。监控 twist.log 文件中是否显示指示 Web 服务数据访问引擎 (Twist) 组件无法正确启动的异常。如果在模型库 (Truth) 连接设置期间出现问题，则错误记录在 twist.log 文件中；例如，您可能看到以下错误消息：

```
####<Oct 14, 2006 1:37:43 AM UTC> <Error> <JDBC>
<localhost.localdomain> <twist> <main> <<WLS Kernel>> <> <BEA-
001150> <Connection Pool "TruthPool" deployment failed with the
following error:

<Specific message, such as Oracle error codes and tracebacks>
```

access.log 文件包含普通日志格式的访问信息。当该文件达到 5MB 大小时，这些文件将轮循。

server.log 文件包含从 Web 服务数据访问引擎生成的应用程序级别异常和调试消息。server.log 文件还将包含由模型库 (Truth) 连接设置问题导致的错误。调试消息受 twist.conf 文件中的包或类级别设置的日志级别控制。可以通过 twist.conf 配置文件数和每个文件的大小。server.log.0 始终是当前文件，而 erver.log.9 是最旧的文件。

boot.log 文件包含有关当 Web 服务数据访问引擎启动时生成的初始 stdout 和 stderr 消息的信息。此外，boot.log 文件还包含 Kill －QUIT 命令的输出。

watchdog.log 文件每分钟记录一次 Web 服务数据访问引擎的状态。

命令引擎监控

分布式程序（例如服务器代理）借助命令引擎跨多个服务器运行。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。

命令引擎端口

命令引擎使用端口 1018。

监控命令引擎的进程

在 Linux 上，在运行命令引擎组件的服务器上执行以下命令：

```
# ps auxwww | egrep '(COMMAND$|waybot)' | grep -v grep
```

运行此命令应当生成类似如下的输出：

```
USER   PID   %CPU   %MEM   VSZ   RSS   TTY   STAT   START   TIME   COMMAND

root   412   0.0    0.0 13600 1472    ?    S     Sep11    0:00
/opt/opsware/

bin/python /opt/opsware/pylibs/shadowbot/daemonbot.pyc
--conf /etc/opt/opsware/waybot/waybot.args
```

在运行内核 2.4 或更高版本的 Linux 服务器上，命令引擎有一个进程。

命令引擎日志

命令引擎日志位于以下文件中：

- /var/log/opsware/waybot/waybot.err*
- /var/log/opsware/waybot/waybot.log*
- /var/log/opsware/waybot/daemonbot.out*

软件数据库监控

软件数据库是 SA 核心的组件，它是存储 SA 所管理的所有软件的位置。软件数据库是 SA 库的一部分。每个核心有一个或多个软件数据库。本节描述如何监控您的核心中的软件数据库。

软件数据库镜像可使多主控网状网络中的软件数据库保持冗余和灾难恢复的同步。例如，如果您将软件包上载到网状网络中的一个核心，则软件数据库镜像作业将该软件包复制到网状网络中的所有其他软件数据库。

要启用或禁用软件数据库镜像或者更改软件数据库镜像作业的运行频率，请参见更改软件数据库镜像参数。

软件数据库端口

软件数据库使用下列端口：

- 1003（加密）
- 1006（明文）
- 1005（复制器管理用户界面）
- 5679（多主控软件数据库）

监控软件数据库的进程 - Linux

要检查 Linux 上的软件数据库进程，请在运行软件数据库组件的服务器上运行以下命令：

```
#ps auxwwww | grep -v grep | grep mm_wordbot
```

此命令生成类似如下的输出：

```
root  31006  0.0  0.0  13612  1492  ?S  Sep11  0:00
/opt/opsware/bin/

python /opt/opsware/pylibs/shadowbot/daemonbot.pyc --conf
/etc/opt/opsware/mm_wordbot/mm_wordbot.args

root  31007  0.0  0.1  103548  7688  ?S  Sep11  7:33
/opt/opsware/bin/

python /opt/opsware/pylibs/shadowbot/daemonbot.pyc --conf
/etc/opt/opsware/mm_wordbot/mm_wordbot.args

root  31092  0.0  0.0  13608  1480  ?S  Sep11  0:00
/opt/opsware/bin/

python /opt/opsware/pylibs/shadowbot/daemonbot.pyc --conf
/etc/opt/opsware/mm_wordbot/mm_wordbot-clear.args

root  31093  0.0  0.1  70172  6424  ?S  Sep11  2:11
/opt/opsware/bin/

python /opt/opsware/pylibs/shadowbot/daemonbot.pyc --conf
/etc/opt/opsware/mm_wordbot/mm_wordbot-clear.args
```

在 Linux 上，软件数据库有多个运行进程（大多数为线程），分别用于加密的软件数据库和明文软件数据库。

软件数据库日志

软件数据库日志位于下列文件中：

- /var/log/opsware/mm_wordbot/wordbot.err*
- /var/log/opsware/mm_wordbot/wordbot.log*
- /var/log/opsware/mm_wordbot-clear/wordbot-clear.err*
- /var/log/opsware/mm_wordbot-clear/wordbot-clear.log*

软件数据库监控 - SA 客户端

软件数据库镜像可使所有软件数据库保持冗余和灾难恢复的同步。如果一个软件数据库失败，则其他软件数据库可以继续为软件请求服务。要启用软件数据库监控，请参见更改软件数据库镜像参数。

如果已启用软件数据库镜像，则可以按如下方式查看和监控软件数据库镜像的状态：

1. 以拥有多控制工具权限的用户身份登录 SA 客户端。有关权限的详细信息，请参见权限参考。
2. 选择“管理”选项卡。
3. 在导航面板中，选择“软件存储库镜像”。此屏幕显示多主控网状网络中的软件数据库镜像的状态。显示的信息包括：
   - **网状网络中的文件数**：这是每个完全同步的软件数据库中的总文件数。
   - **使用的总磁盘空间：**这是完全同步的软件数据库所需的大致总磁盘空间。
   - **状态**：显示哪些软件数据库具有所有所需的文件（绿色）、哪些需要文件（黄色）、哪些禁用了镜像（灰色）。
     - **绿色**：所有所需的文件都在设施的软件数据库中存在。丢失的文件数为零。
     - **黄色**：设施的软件数据库中缺少一个或多个文件，因此需要更新。这些设施将在镜像作业下一次运行时更新。镜像作业按镜像作业运行周期的定义定期运行。
     - **灰色**：设施中禁用软件数据库监控。
   - **设施**：显示运行软件数据库的 SA 设施。
   - **文件**：主机软件数据库中当前的文件数。
   - **大小**：软件数据库文件当前使用的大致总磁盘空间。
   - **缺失**：需要由设施的软件数据库镜像但尚未进行复制的文件的数量。

要更改软件数据库镜像作业的运行频率，请参见更改软件数据库镜像参数。

图 35 显示软件数据库镜像的状态以及名为 Bangalore、London 和 New York 的三个 SA 核心。软件包上载到 London 核心。黄色状态指示器显示 Bangalore 和 New York 核心未同步 - 此软件包尚未复制到这两个核心中。

图 35.软件数据库镜像状态 - 未同步

图 36 显示的是在运行镜像作业并复制软件包到所有核心后的软件数据库镜像状态。绿色状态指示器表示所有核心已同步。

图 36.软件数据库镜像状态 - 已同步

模型库监控

模型库是一个包含基本信息的 Oracle 数据库，这些基本信息是构建、运行和维护一系列托管服务器、其硬件、其配置、操作系统以及所有其他应用程序所需要的。

有关模型库的详细信息（包括有关监控模型库的详细信息），请参见《SA Installation Guide》中的“附录 A：模型库的 Oracle 设置”。

模型库端口

模型库的默认端口是 1521；但是此端口有可能已被安装此模型库的数据库管理员修改。

监控模型库的进程

监控 Oracle 数据库进程。如果找不到进程，则数据库已失败或无法启动。

在 Linux 上，在运行 Oracle 的服务器上执行以下命令：

```
# ps -fu oracle | grep pmon
```

运行此命令应当生成类似如下的输出：

```
oracle 2112 1 0 21:22 ?    00:00:00 ora_pmon_truth
```

（进程名称可能包括数据库 SID truth，如此示例中所示）。

如果找不到进程，则侦听器已失败或无法启动。

在 Linux 上，使用此命令监控 Oracle 侦听器进程：

```
# ps -fu oracle | grep tnslsnr
```

运行此命令应当生成类似如下的输出：

```
oracle 2021 1 0 21:22 ?    00:00:01
/u01/app/oracle/product/11.2.0/db_2/bin/tnslsnr LISTENER -
inherit
```

模型库日志

模型库的日志文件由 Oracle 数据库产生，它们的位置是特定于安装的。

默认情况下，SA 对模型库日志的每个 SID（在本例中为 truth）使用一个目录。（根据 Oracle 的安装方式，这会有所不同。）

/u01/app/oracle/admin/truth/bdump/alter_truth.log

要监控的情况：

并非所有错误都表示数据库有问题。某些错误可能是由应用程序导致。

在这些示例中，如果命令有以下输出，则说明有问题。

```
grep ORA- /u01/app/oracle/admin/truth/bdump/alter_truth.log
ORA-00600: internal error code, arguments:[729], [480], [space
leak], [], [], [], [], []
ORA-07445: exception encountered: core dump [lxmcpen()+0]
[SIGSEGV] [Address not mapped to object] ...
```

表空间使用情况

应当针对阈值监控表空间使用情况，通常以严重性增加来表示（例如超过 80% 为警告，超过 90% 为错误，超过 95% 为严重错误）。

监控表空间使用情况有很多方法。有关为了检测表空间可用磁盘空间是否充足而需要运行的 SQL 查询，请参见《SA Installation Guide》中的“附录 A：模型库的 Oracle 设置”。必须以拥有权限的数据库用户的身份来执行安装指南中提供的 SQL 查询。

多主控冲突

通过以任何 SA 数据库用户的身份运行以下 SQL 查询，可以找出任何模型库中有冲突事务的数量。

```
select count(*) from transaction_conflicts where resolved = 'N';
```

可以分阶段监控多主控冲突，冲突数量的增长会导致升级级别的提升。用于阶段的值取决于使用模式。

SA 管理员应当记录某段时间（可能是一个星期）的冲突数，并使用该信息确定监控系统发出警报的级别。

模型库多主控组件监控

模型库多主控组件是一个 Java 程序，它负责保持多个模型库同步和将原始模型库的更改传播到所有其他模型库数据库。

模型库多主控组件端口

模型库多主控组件使用端口 5678。

监控模型库多主控组件的进程

在 Linux 上，在安装基础结构组件捆绑包的服务器上执行以下命令：

```
# ps auxwww | grep -v grep | grep vault | grep -v twist
```

运行此命令将产生类似以下内容的输出：

```
root  28662  0.0  0.0  2284  532  ?S  Sep27  0:00
/opt/opsware//bin/

python /opt/opsware//pylibs/shadowbot/etc/daemonizer.pyc
--runpath /var/opt/opsware/vault --cmd /opt/opsware/j2sdk1.4.2_
10/bin/java -classpath
/opt/opsware/vault/classes:/opt/opsware/vault ......-ms120m -
mx1024m
-DCONF=/etc/opt/opsware/vault/
-DHOSTNAME=m234.dev.opsware.com com.loudcloud.vault.Vault

root  28663  0.0  6.3  1285800  130896  ?S  Sep27  5:32
/opt/opsware/

j2sdk1.4.2_10/bin/java -classpath
/opt/opsware/vault/classes:/opt/opsware/vault ......-ms120m -
mx1024m
-DCONF=/etc/opt/opsware/vault/
-DHOSTNAME=m234.dev.opsware.com com.loudcloud.vault.Vault
```

模型库多主控组件日志

模型库多主控组件日志位于以下文件中：

- /var/log/opsware/vault/vault.*n*.log

要配置日志文件名称、日志文件大小或日志记录级别，请执行下列步骤。

1. 在 SA 客户端中选择“管理”选项卡。
2. 在导航面板中选择“系统配置”。将显示包含系统配置参数的 SA 组件、设施和领域。

3. 在 SA 组件列表中，选择“模型库，多主控组件”。将显示该组件的系统配置。
4. 根据需要，查找并修改 `log`、`logLevel` 或 `logsize` 配置参数。
5. 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。

全局文件系统监控

全局 Shell 功能是作为任何切分组件捆绑包的一部分安装的。它动态地构建了全局文件系统 (OGFS) 虚拟文件系统。

全局 Shell 可连接到服务器代理以打开托管服务器上的 UNIX Shell 或 Windows 远程桌面连接。

有关使用全局 Shell 的信息，请参见《SA 用户指南：Server Automation》中的“全局 Shell”一章和附录。

全局文件系统组件由以下程序组成：

- **集线器**：是一个与托管服务器上其他核心组件和代理交互作用组成文件系统视图的 Java 程序。
- **适配器**：Linux 上的一种 C 程序，它在 FUSE（内核中的模块）和集线器之间传输文件系统请求和回复，并使用 FUSE 用户空间库与 FUSE 内核模块进行通信。
- **代理的代理服务器**：一种 Python 程序，它为集线器提供与托管服务器上运行的代理的 SSL 连接。
- **FUSE**（*仅限 Linux*）：用户空间 (FUSE)（GNU GPL 许可证管理的软件）中的文件系统，它向适配器提供文件系统请求的内核内分派。

集线器的进程组 ID 文件位于以下目录中：

- `/var/opt/opsware/hub/hub.pgrp`

所有全局文件系统程序（集线器、适配器、代理的代理服务器及其日志轮循器）都在此进程组中运行。

监控全局文件系统的进程

在 Solaris 上，在运行切分组件捆绑包的服务器上执行以下命令：

```
# ptree $(ps -g $(cat /var/opt/opsware/hub/hub.pgrp) -o pid=)
```

运行此命令将产生类似以下内容的输出：

```
7594 /opt/opsware/bin/python /opt/opsware/hub/bin/rotator.py
/opt/

opsware/j2sdk1.4.2......

 7598 /opt/opsware/j2sdk1.4.2_10/bin/java -server -Xms64m -
Xmx1024m
```

```
-Dhub.kernel=SunO......

  7613 /opt/opsware/bin/python
/opt/opsware/adapter/SunOS/bin/rotator.py

/opt/opsware/......

    7617 /opt/opsware/ogfsutils/bin/python2.4
/opt/opsware/adapter/

SunOS/lib/adapter.py......

     7618 /opt/opsware/adapter/SunOS/bin/mount -o hostpath=

/hostpath,nosuid /dev/ogdrv /v......

 7619 /opt/opsware/bin/python
/opt/opsware/agentproxy/bin/rotator.pyc

/opt/opsware/bi......

  7625 /opt/opsware/bin/python /opt/opsware/agentproxy/lib/

main.pyc......
```

在 Solaris 上，OGFS（尤其是程序集线器、适配器和代理的代理服务器）有七个运行进程。

在 Linux 上，在运行切分组件捆绑包的服务器上执行以下命令。

```
# ps u -g $(cat /var/opt/opsware/hub/hub.pgrp)
```

运行此命令将产生类似以下内容的输出：

```
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND

root 8862 0.0 0.0 2436 1356 ?S Sep29 0:00 /opt/opsware/bin/python
/opt/opsware/hub/bin/rotator.py /opt/opsware/j2sdk1.4.2_
10/b......

root 8868 0.1 1.8 1256536 76672 ?S Sep29 35:51
/opt/opsware/j2sdk1.4.2_

10/bin/java -server -Xms64m -Xmx1024m -Dhub.kernel=Linux -
Dh......

root 8906 0.0 0.0 2412 1304 ?S Sep29 0:28 /opt/opsware/bin/python
/opt/

opsware/adapter/bin/adapter......

root 8908 0.0 0.0 13088 684 ?S Sep29 0:10
/opt/opsware/adapter/Linux/

bin/adapter.bin /var/opt/opsware/ogfs/mnt/ogfs -f -o none......

root 8913 0.0 0.0 2308 1132 ?S Sep29 0:00 /opt/opsware/bin/python
/opt/

opsware/agentproxy/bin/rotator.pyc /opt/opsware/bin/pyt......
```

```
root 8923 0.0 0.1 153120 6544 ?S Sep29 5:56
/opt/opsware/bin/python

/opt/opsware/agentproxy/lib/main.pyc......
```

在 Linux 上，OGFS（尤其是程序集线器、适配器和代理的代理服务器）有六个运行进程。

全局文件系统还支持将 `status` 选项添加到 Linux 和 Solaris 上的 `init` 脚本。

在 Linux 或 Solaris 上，在运行切分组件捆绑包的服务器上执行以下命令以运行此 `status` 选项：

```
# /etc/opt/opsware/startup/hub status
```

运行此命令将产生类似以下内容的输出：

```
Testing for presence of Hub process group file
(/var/opt/opsware/hub/hub.pgrp) ...OK

Testing that processes are running in Hub process group (8862)
...OK

Testing that OGFS is mounted ...OK

Testing that the OGFS authenticate file is present ...OK

OGFS is running
```

全局文件系统日志

集线器日志位于以下文件中：

- `/var/log/opsware/hub/hub.log*`
- `/var/log/opsware/hub/hub.out*`

  集线器日志中要监控的情况：
  - 包含“Can’t establish twist connection”的字符串

适配器日志位于以下文件中：

- `/var/log/opsware/adapter/adapter.err*`

代理的代理服务器日志位于以下文件中：

- `/var/log/opsware/agentproxy/agentproxy.err*`

监控 FUSE 的进程（仅限 Linux）

在 Linux 上，在运行切分组件捆绑包的服务器上执行以下命令：

```
# lsmod | grep -v grep | grep fuse
```

运行此命令将产生类似以下内容的输出：

```
fuse       31196 2
```

FUSE 将消息记录在以下文件中：

- /var/log/messages

监控 SunOS 内核模块的进程

在 Solaris 上，OGFS 功能依赖于 SunOS 内核模块。

在运行切分组件捆绑包的服务器上执行以下命令：

```
# modinfo | grep -i opsware
```

运行此命令将产生类似以下内容的输出：

```
137 1322cd8 43a9 272 1 ogdrv (Opsware GFS driver v1.13)
138 13ac227 338df 18 1 ogfs (Opsware Global Filesystem v1.14)
```

全局文件系统将与 SunOS 内核模块相关的消息记录在以下文件中：

- /var/adm/messages

轮辐监控

轮辐是 SA 客户端的后端组件。轮辐作为一个 Java RMI 服务器将提供对 OGFS 中文件的访问权以及在 OGFS 会话内部运行命令的权利。

轮辐端口

轮辐使用端口 8020。

监控轮辐的进程

在 Linux 上，在运行切分组件捆绑包的服务器上执行以下命令：

```
# ps -ef | grep -v grep | grep spoke
```

运行此命令将产生类似以下内容的输出：

```
root  29191  1  0  Aug28  ?01:12:11  /opt/opsware/j2sdk1.4.2_
10/bin/

java -server -Xms32m -Xmx256m -Dbea.home=/opt/opsware/spoke/etc -
Dspoke.home=/opt/opsware/spoke
-Dspoke.cryptodir=/var/opt/opsware/crypto/spoke
-Dspoke.logdir=/var/log/opsware/spoke
-Djava.util.logging.config.file=/opt/opsware/spoke/etc/logg
```

在 Linux 上，Spoke 组件具有单一的 Java 运行进程。

轮辐日志

轮辐日志位于以下文件中：

- /var/log/opsware/spoke/spoke-*.log
- /var/log/opsware/spoke/stdout.log

网关监控

SA 管理和核心网关允许 SA 核心管理位于一个或多个 NAT 设备或防火墙后的服务器。网关之间的连接借助通过网关实例之间的永久 TCP 通道路由消息来进行维护。

有关配置网关的信息，请参见《SA 概述和体系结构》指南。

有关维护卫星网关的信息，请参见卫星端管理。

网关端口

默认情况下，网关使用以下端口：

- 2001—管理网关侦听器端口
- 2001—切分组件核心网关侦听器端口
- 3001—代理网关端口
- 3001—卫星端网关端口

监控网关的进程

在所有的配置中，网关组件有两个运行进程 - 网关进程本身和其监视程序进程。

在 Solaris 或 Linux 上，在运行网关组件的服务器上执行以下命令：

```
# ps -eaf | grep -v grep | grep opswgw | grep cgw
```

运行此命令将产生类似以下内容的输出：

```
root  17092  1  0  Sep21  ?00:00:00  [opswgw-watchdog-2.1.1:
cgw0-C43]

--PropertiesFile /etc/opt/opsware/opswgw-cgw0-
C43/opswgw.properties --BinPath /opt/opsware/opswgw/bin/opswgw

root  17094  17092  0  Sep21  ?02:23:21  [opswgw-gateway-2.1.1:
cgw0-

C43] --PropertiesFile /etc/opt/opsware/opswgw-cgw0-
C43/opswgw.properties --BinPath /opt/opsware/opswgw/bin/opswgw --
Child true
```

```
# ps -eaf | grep -v grep | grep opswgw | grep agw
```

运行此命令将产生类似以下内容的输出：

```
root  17207  1  0  Sep21  ?00:00:00  [opswgw-watchdog-2.1.1:
agw0-C43]
```

```
--PropertiesFile /etc/opt/opsware/opswgw-agw0-
C43/opswgw.properties --BinPath /opt/opsware/opswgw/bin/opswgw

root  17208  17207  0  Sep21  ?01:18:54  [opswgw-gateway-2.1.1:
agw0-

C43] --PropertiesFile /etc/opt/opsware/opswgw-agw0-
C43/opswgw.properties --BinPath /opt/opsware/opswgw/bin/opswgw --
Child true
```

在 Solaris 或 Linux 上，在运行卫星网关组件的服务器上执行以下命令：

```
# ps -eaf | grep -v grep | grep opswgw | grep <gateway-name>
```

其中，此例中的 <gateway-name> 为 `Sat1`**。**

运行此命令将产生类似以下内容的输出：

```
root  17092  1  0  Sep21  ?00:00:00  [opswgw-watchdog-2.1.1:Sat1]

--PropertiesFile /etc/opt/opsware/opswgw-Sat1/opswgw.properties -
-BinPath /opt/opsware/opswgw/bin/opswgw

root  17094  17092  0  Sep21  ?02:23:21  [opswgw-gateway-
2.1.1:Sat1]

--PropertiesFile /etc/opt/opsware/opswgw-Sat1/opswgw.properties -
-BinPath /opt/opsware/opswgw/bin/opswgw --Child true
```

网关 URL

登录到 SA 客户端 UI，然后在导航窗格的“管理”下选择“网关”。

```
https://occ.<data_center>/com.opsware.occ.gwadmin/index.jsp
```

网关日志

网关日志位于以下文件中：

- `/var/log/opsware/gateway-name/opswgw.log*`

日志中要监控的情况：

- **字符串包含“ERROR”**
- **字符串包含“FATAL”（表明进程将很快结束）**

OS 构建管理器监控

OS 构建管理器组件帮助 OS 构建代理和命令引擎进行通信。它从命令引擎接受 OS 配置命令，然后为特定于平台的内部版本脚本提供运行时环境，以执行 OS 配置过程。

OS 构建管理器端口

OS 构建管理器使用下列端口：

- 1012 (HTTPS)
- 1017（SA 构建代理）

监控 OS 构建管理器的进程

在所有配置中，OS 构建管理器组件都有一个运行进程。

在 Linux 上，在运行 OS 构建管理器组件的服务器上执行以下命令：

```
# ps -eaf | grep -v grep | grep buildmgr
```

运行此命令将产生类似以下内容的输出：

```
root 2174 1 0 Sep27 ?0:13:54 /opt/opsware/j2sdk1.4.2_10/bin/
      java -Xmx256m -Dbuildmgr -
      Djava.security.properties=/opt/opsware/buildmgr/etc/java.secur
      ity -DDEBUG -DDEBUG_VERBOSE=1 -DLOG_OPTIONS=tTN -DLOG_FILE_
      THRESHOLD=10485760 -DLOG_FILE_RETAIN_COUNT=7 -DLOG_
      CLASSES=com.opsware.buildmgr.OutputStreamLo
```

OS 构建管理器 URL

```
https://buildmgr.<data_center>:1012
```

OS 构建管理器 UI 是只读的，该 UI 的端口 1012 是可配置的。

OS 构建管理器日志

OS 构建管理器日志位于以下文件中：

- `/var/log/opsware/buildmgr/buildmgr.log`（构建代理活动、OS 配置活动）
- `/var/log/opsware/buildmgr/*.request.log`（Web 服务器日志；每天一个文件；最多 90 个日志）
- `/var/log/opsware/buildmgr/console.log`
- `/var/log/opsware/buildmgr/servers/<IP_address or machine_ID or MAC_address>`（每个连接日志一个）

日志中要监控的情况：字符串“Traceback”

OS 启动服务器监控

OS 启动服务器属于 OS 配置构建功能，支持分别配备 inetboot 和 PXE 的 Sun 和 x86 系统的网络启动。用于提供此支持的进程是 Internet Software Consortium DHCP 服务器。

这些应用程序由 SA 安装程序安装，但不是特定于 SA 的。可以通过对这些应用程序使用标准系统管理最佳实践来监控它们。

OS 启动服务器端口

OS 启动服务器使用下列端口：

- 67 (UDP)（DHCP 服务）
- 69 (UDP)（TFTP 服务）

OS 启动服务器日志

OS 启动服务器不生成其自己的日志。OS 启动服务器使用下列服务：带有 INETD 的 TFTP、NFS 服务器和 ISC DHCPD。所有这些服务都使用 syslog 进行日志记录。有关详细信息，请参考供应商文档。另请参见 `syslog.conf` 文件，该文件用来配置 OS 启动服务器以确定如何为此组件配置日志记录。

OS 介质服务器监控

OS 介质服务器是 OS 配置功能的一部分，负责提供针对 OS 配置期间使用的供应商提供的介质的网络访问。用于提供此支持的进程包括 Samba SMB 服务器和 Sun Solaris NFS。

这些应用程序由 HP BSA 安装程序安装，但不是特定于 SA 的。尤其是，SA 提供了客户可用来安装 OS 介质服务器的适用于 Linux 和 Solaris 的 Samba 包。NFS 服务由操作系统提供。使用 HP BSA 安装程序安装 OS 介质服务器会在 Linux 和 Solaris 上配置 NFS。

可以通过对 Sun Solaris NFS 应用程序使用标准系统管理最佳实践来监控 Samba SMB 服务器和这些应用程序。

OS 介质服务器端口

OS 介质服务器使用下列端口：

- NFS 使用的 portmapper 是端口 111。
- Samba SMB 使用端口 137、138、139 和 445。

OS 介质服务器日志

OS 介质服务器日志位于以下文件中：

- `/var/log/opsware/samba/log.smbd`
- `/var/log/opsware/samba/log.nmbd`

Solaris 和 Linux OS 配置使用供应商提供的服务，例如 NFSD。这些服务通常通过 syslog 进行日志记录。有关这些日志文件的详细信息，请参考供应商文档。

第 8 章

SA 故障排除 - 诊断测试

本节描述：

- **核心运行状况检查监控器**，对单个 SA 组件的运行状况进行检查。请参见核心运行状况检查监控器 (HCM)。
- **系统诊断**工具，对 SA 核心总体运行状况进行检查。请参见运行系统诊断。

可以使用这些工具来诊断维护 SA 时可能遇到的下列问题类型：

- **运行问题**：进程（例如，数据访问引擎、命令引擎或软件数据库）失败或者变得无响应
- **SA 核心组件失败**：导致其他组件失败。

  以下示例描述某些核心组件失败的影响：
  - 如果数据访问引擎失败，则 SA 客户端、命令引擎以及软件数据库组件将失败。
  - 如果软件数据库无法与数据访问引擎联系，则无法从软件数据库下载。
  - 如果模型库失败，则数据访问引擎失败。
  - 如果软件数据库没有正常运行的 DNS 或正确配置的 /etc/hosts 文件，则无法与数据访问引擎联系。
  - 如果托管环境中存在无法访问的服务器，则通信中断。

备注: 一次只能在一个设施上运行系统诊断。

SA 核心组件内部名称

为了能与旧版兼容，本文使用内部名称来称呼 SA 核心组件。**表 27** 显示了 SA 组件的内部和外部名称。

表 27.内部和外部组件名称

内部名称	外部名称
agentcache	全局文件系统的组件
buildmgr	OS 配置构建管理器
hub	全局文件系统的组件
mm_wordbot	软件数据库的组件
occ	SA 命令中心

内部名称	外部名称
opswgw-agw0	代理网关
opswgw-mgws0	主网关
spin	数据访问引擎
spoke	全局文件系统的组件
truth	模型库
twist	Web 服务数据访问引擎
vault/vaultdaemon	模型库多主控组件
way/waybot	命令引擎
word	软件数据库

核心运行状况检查监控器 (HCM)

运行状况检查监控器 (HCM) 包括一套用于检查 SA 核心状态的测试。HCM 中的脚本通过 SA 安装程序安装。HCM 与系统诊断测试中所述的系统诊断工具之间有一些功能重叠。

HCM 提供两种类型的测试：

- **本地测试**：逐组件验证核心的运行状况。
- **全局测试**：整体验证核心的运行状况。

HCM 本地测试概述

HCM 本地测试对 *单个核心组件* 进行验证。本地测试与它们验证的组件驻留在相同的服务器上。通过运行 SA 启动脚本 (`/etc/init.d/opsware-sas`) 并指定测试模式参数和可选的组件名称，运行本地测试。

测试模式指定要运行的测试集（您不能指定单个测试）。即使您指定了多个需要相同测试的组件，每个测试也只能运行一次。测试结果显示在 `stdout` 中。

备注: 运行状况检查监控器不能从卫星端主机运行。

HCM 本地测试脚本的语法

HCM 本地测试使用下列语法：

```
/etc/init.d/opsware-sas <mode> [<component>[<component>...]]
[<name>=<value>[<name>=<value>]...]
```

运行 HCM 本地测试

要运行本地测试，请执行以下步骤：

1. 以 root 身份登录运行要测试的 SA 核心组件的服务器。
2. 使用 status 参数或指定 mode（测试类别）参数以及一个或多个组件（请参见下一节的命令选项）运行 SA 启动脚本。例如，下面的命令验证 Web 服务数据访问引擎是否可用：

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

表 28 描述了 HCM 命令行参数。有关用于启动和停止核心的 opsware-sas 选项的描述，请参见表 24.SA 启动/停止脚本的选项。

表 28.HCM 本地测试脚本的选项

选项	描述
mode	要运行的测试集。mode 可以是下列字符串之一： status：运行对指定组件可用性进行验证的测试。例如，测试验证组件是否正在侦听正确的端口和响应基本查询。 verify_post：与 status 相同。 verify_pre：运行对指定组件正常工作所需的条件进行验证的测试。 verify_functionality：运行与 status 模式所运行的测试类似的测试；不过，它们的运行可能花费更长时间。因此，您可以选择跳过这些测试以节省时间。 health：运行 status、verify_pre 和 verify_functionality 模式的测试，并提供指定的组件的总体状态概述。
component	核心组件的内部名称。如果未指定此选项，则验证所有组件。要查看本地服务器上安装的组件的内部名称，请输入以下命令： /etc/init.d/opsware-sas list
name=value	控制测试运行方式的选项。允许的值： terse=[true|false]：如果为 true，则将每个组件的所有成功测试结果汇总在一条成功消息中；但是，将单独显示失败测试的结果。默认情况下，此选项设置为 false。（此选项传递到单个测试。） parsable=[true|false]：如果为 true，则使用单一“成功”或“失败”消息汇总每个组件的所有测试结果。默认情况下，此选项设置为 false。（此选项传递到单个测试。）

选项	描述
	verify_filter=<regex>：仅运行其文件名与您输入的正则表达式匹配的测试。例如，如果指定 verify_filter="OPSW"，则仅运行文件名包含字符串 OPSW 的测试（例如 100_OPSWcheck_host_spin.sh）。默认情况下，此选项未定义。（此选项不传递到单个测试。） 如果给定测试是另一个文件的符号链接，则根据符号链接的目标（而不是符号链接的名称）来评估筛选器。如果测试是符号链接，则 verify_filter 使用它指向的文件的文件名，以进行比较。

备注: 您可以在SA 核心组件内部名称中找到用于某些核心组件的内部名称及其标准名称的列表。

HCM 全局测试概述

全局 HCM 测试检查整个 SA 核心。通过在以下主机上执行 run_all_probes.sh 脚本运行这些测试：

- **切分配置** — 托管核心管理网关和/或基础结构组件（在典型安装中，管理网关安装在托管基础结构组件的主机上）的服务器。
- **非切分配置** — 托管要验证核心的主模型库多主控组件的服务器。

测试结果显示在 stdout 中。全局测试无法检查多主控网状网络中其他核心的状态。

在多主控核心中，全局测试使用 SSH 连接到其他核心服务器。所有连接都以 root 身份生成。通过在命令行中指定 root 密码或密钥文件来执行身份验证。如果同时指定了二者，则使用 root 密码。必须指定这些身份验证方法之一，除非服务器是本地主机。

运行 HCM 全局测试

要运行 HCM 全局测试，请执行以下步骤：

1. 以 root 身份登录托管模型库多主控组件和/或基础结构组件的服务器。
2. 执行带有 run 选项（有关该选项的详细信息请参见下一节）的 run_all_probes.sh 脚本。例如，要检查模型库的 Oracle 数据库中表空间的使用情况，请输入以下命令：

```
/opt/opsware/oi_util/bin/run_all_probes.sh run \
check_database_tables
```

HCM 全局测试脚本的语法

运行 HCM 全局测试的脚本具有以下语法：

```
/opt/opsware/oi_util/bin/run_all_probes.sh run|list
[<test> [<test>...]
[hosts="<system>[:<password>] [<system>[:<password>]]..."
[keyfile=<keyfiletype>:<keyfile>[:<passphrase>]]
```

表 29 描述了此语法的选项。

表 29.HCM 全局测试脚本的选项

选项	描述
`list`	列出可用测试。
`run`	运行指定的测试。
`test`	要运行的测试的名称。如果未指定任何测试，则运行所有测试。该脚本在交付时包括下列测试： · `check_opsware_services`：通过在每个核心服务器上远程运行以下命令，在所有指定的服务器上运行本地测试：`/etc/init.d/opsware-sas health` · `check_MM_state`：对于多主控源核心，检查核心的多主控状态。 · `check_time`：在多主控核心中，验证核心服务器的系统时钟是否同步。 · `check_opsware_version`：验证核心中所有组件的版本是否是相同版本。 · `check_database_tables`：验证模型库表空间的使用情况是否在可接受的限制内。有关表空间的详细信息，请参见《SA Installation Guide》中的“模型库的 Oracle 设置”。 · `check_OS_resources`：验证 SA 分区中的虚拟内存和磁盘空间是否在可接受的阈值内。 · `check_fully_functional`：验证所有 SA 组件的完整功能。有关从 SA 客户端运行系统诊断综合测试的其他方式，请参见系统诊断测试。
`system:password`	指定远程核心服务器（主机名或 IP 地址）和服务器的可选 `root` 密码。
`keyfiletype`	指定要使用的密钥文件类型。允许值包括： · `rsa_key_file` · `dsa_key_file`。
`keyfile`	指定含有当前服务器 SSH 私钥的文件。
`passphrase`	指定用于对 SSH 私钥加密的密码。

设置全局测试的无密码 SSH

全局测试通过 SSH 守护程序访问核心中的远程服务器。这些测试要求您提供 `root` 密码或使用 SSH 公钥/私钥。

要使用 `ssh-keygen` 生成的公钥/私钥设置身份验证，请执行下列步骤：

1. 在可信服务器上运行下列命令并接受默认值。对于 Linux 和 Solaris，这些命令有所不同。

   Linux:

   ```
   cd /root/.ssh
   ssh-keygen -t dsa
   ```

   Solaris:

   ```
   cd /.ssh
   ssh-keygen -t dsa
   ```

2. 通过将 `id_dsa.pub` 文件复制到客户端服务器的 `.ssh` 目录中，然后将其重命名为 `authorized_keys` 来更新该客户端服务器。下面是适用于 Linux 和 Solaris 的一些示例命令：

   Linux:

   ```
   scp id_dsa.pub <host>:/.ssh/authorized_keys
   /root/.ssh/authorized_keys
   ```

   Solaris:

   ```
   scp id_dsa.pub <host>:/.ssh/authorized_keys
   /.ssh/authorized_keys
   ```

3. 验证可信服务器。运行下列命令以验证可信服务器是否可以在没有密码的情况下连接到客户端服务器：

   ```
   ssh -l root <host>
   ```

扩展运行状况检查监控器

本节的目标读者是具有 UNIX Shell 编程和 SA 管理经验的高级系统管理员。

HCM 作为在核心服务器上执行本地或全局测试的一系列 UNIX Shell 脚本执行。这些脚本符合特定命名约定，驻留在预定义的目录中。您可以通过编写自己的脚本并将它们复制到 `/opt/opsware/oi_util` 下的正确目录中来扩展 HCM。

HCM 本地测试扩展的要求

HCM 本地测试是一种通过 /etc/init.d/opsware-sas 脚本运行的脚本（请参见运行 HCM 本地测试）。本地测试脚本必须符合下列要求：

- **UNIX Shell 脚本**：是以 root 身份运行的 UNIX Shell 脚本。
- **组件服务器**：脚本在脚本验证的组件的服务器上驻留并运行。例如，如果脚本验证数据访问引擎 (spin)，则它驻留在运行数据访问引擎的服务器上。
- **可执行文件**：脚本是可执行文件 (chmod u+x)。
- **文件名**：脚本的文件名具有以下语法：

  <int><test>.sh

  在此语法中，int 是指定测试执行顺序的整数值，test 是测试的名称。请注意，随 SA 提供的 HCM 脚本在脚本文件名中包含 OPSW，例如 100_OPSWportping.sh。
- **目录**：脚本驻留在下列目录中：

  /opt/opsware/oi_util/local_probes/<component>/[verify_pre | verify_post | verify_functionality]/

  在此路径中，component 是核心组件的内部名称，例如 spin 或 twist。component 目录下的目录匹配测试的类别。例如，如果测试在核心组件上执行运行时验证，则脚本驻留在 verify_functionality 子目录中。有关详细信息，请参见类别和本地测试目录。

  将 component 目录下的目录映射到 /etc/init.d/opsware-sas 命令的 mode 选项。例如，如果您将某个脚本保存到 verify_pre 子目录中，则当您运行具有 verify_pre 选项的 opsware-sas 时，将执行该脚本。如果您指定 opsware-sas 的 health 选项，则执行全部三个目录中的脚本。**表 30** 描述了目录名称和模式选项之间的映射。

表 30.opsware-sas 的模式和本地测试脚本的子目录

命令行的模式选项	此选项的脚本运行的子目录
health	verify_pre verify_post verify_functionality
status	verify_post
verify_functionality	verify_functionality
verify_post	verify_post
verify_pre	verify_pre

- **退出代码**：脚本返回退出代码 0 指示成功或非 0 指示失败。/etc/init.d/opsware-sas 命令使用退出代码确定测试的状态。

- **显示的结果**：脚本将测试结果显示在 `stdout` 中。
- **本地前言脚本**：测试脚本运行 `local_probe_preamble.sh` 脚本，如HCM 本地测试示例所述。`local_probe_preamble.sh` 脚本包含 `/etc/init.d/opsware-sas` 命令使用的库和 Shell 变量的超集。

  `local_probe_preamble.sh` 脚本执行下列任务：
  - 设置本地测试使用的 Shell 变量。例如，它设置 `$PYTHON`（指向 Python 解释程序）和 `$UTILS_DIR`（指向可用于测试的实用程序的目录）。
  - 解析命令行，评估所有 `name=value` 对，并设置 shell 变量。例如，如果您在运行 `/etc/init.d/opsware-sas` 时在命令行中指定 `timeout=60`，则 `local_probe_preamble.sh` 脚本将变量 `$timeout` 设置为值 `60`。
  - 提供有用函数的访问权限，例如 `retry`，该函数多次执行命令，直到它成功或超过指定的超时。
- **Shell 变量**：测试脚本将命令行中 `name=value` 选项指定的变量考虑在内。有关预定义名称列表，请参见表 28.HCM 本地测试脚本的选项中的 `name=value` 选项。

类别和本地测试目录

`/opt/opsware/oi_util` 目录具有下列子目录。

local_probes/<component>/verify_pre

此目录包括每个组件的先决条件测试。这些测试验证组件正常工作所需的条件是否存在。例如，目录 `twist/verify_pre` 包含测试脚本 `10check_localhost_spin.sh`，这是因为数据访问引擎组件必须可用，才能让 Web 服务数据访问引擎组件正常运行。

local_probes/<component>/verify_post

此目录包括每个组件的验证测试。这些测试验证给定的组件是否可用。例如，目录 `spin/verify_post` 包含测试脚本 `10check_primary_spin.sh` 以验证数据访问引擎组件是否正在侦听端口 1004 和响应基本查询。

local_probes/<component>/verify_functionality

此目录包括每个组件的运行时验证测试。这些测试验证组件是否可完全正常运行。它们类似于 `verify_post` 测试；但是运行它们需要更长的时间。您可以选择跳过这些测试以节省时间。

HCM 本地测试的目录布局

下列目录布局显示了本地测试驻留的位置：

```
/opt/opsware/oi_util/
 |
```

```
|_lib
| |_local_probe_preamble.sh
|
|_local_probes
  |
  |_COMMON
  | |_<test>
  | |_ ...
  |
  |_<component>
  | |
  | |_verify_pre
  | | |_ <int><test> (can be symlink to ../../COMMON/<test>)
  | | |_ ...
  | |
  | |_verify_post
  | | |_ <int><test> (can be symlink to ../../COMMON/<test>)
  | | |_ ...
  | |
  | |_verify_functionality
  | |_<int><test> (can be symlink to ../../COMMON/<test>)
  | |_...
  |
  |_<component>
    ...
```

HCM 本地测试示例

以下脚本验证 `cron` 实用程序是否在本地服务器上运行：

```
#!/bin/sh
# Verify that cron is running
# Read in our libraries / standard variable settings and parse
# the command line.
```

```
/opt/opsware/oi_util/lib/local_probe_preamble.sh
printf "Verify \"cron\" is running:"
process_running=`ps -eo fname | egrep '^cron$' | head -1`
if [ -z "$process_running" ]; then
echo "FAILURE (cron does not exist in the process table)"
exit 1
else
echo "SUCCESS"
exit 0
fi
```

HCM 全局测试扩展的要求

HCM 全局测试是由 `run_global_probes.sh` 命令调用的脚本（请参见运行 HCM 全局测试）。全局测试脚本必须符合下列要求：

- **UNIX Shell 脚本**：是以 `root` 身份运行的 UNIX Shell 脚本。
- **模型库服务器**：该脚本位于模型库服务器，但它可在任意核心服务器上远程运行。
- **可执行文件**：脚本是可执行文件 (`chmod u+x`)。
- **文件名**：脚本的文件名具有以下语法：

  ```
  <int><test>.sh[.remote]
  ```

  在此语法中，`int` 是指定测试执行顺序的整数值，`test` 是在命令行中指定的测试的名称。请注意使用 SA 提供的 HCM 脚本在脚本文件名称中含有 `OPSW`，例如 `300_OPSWcheck_time.sh`。
- **远程执行**：如果测试脚本在HCM 全局测试概述中所述的核心服务器之外的其他核心服务器上运行，则文件名必须包含 `.remote` 扩展名。当您执行 `run_all_probes.sh` 并指定此类测试时，脚本自动复制到所有指定服务器，并使用 SSH 协议远程执行。

  对于在模型库所在的服务器上运行的测试，不需要 `.remote` 文件扩展名。多主控组件（在非切分安装中）或管理网关/基础结构组件（在切分安装中）。这些测试的示例便是对模型库完整性和多主控冲突性的检查。如果脚本没有 `.remote` 扩展名且需要与远程服务器通信，则脚本必须使用 SSH。全局前言脚本包括帮助程序函数，以使用 SSH 处理远程通信。
- **目录**：脚本驻留在下列目录中：

  ```
  /opt/opsware/oi_util/global_probes/[verify_pre | verify_post ]/
  ```

  有关详细信息，请参见HCM 全局测试目录。

- **退出代码**：脚本返回退出代码 0 指示成功或非 0 指示失败。`run_global_probes.sh` 命令使用退出代码确定测试的状态。
- **显示的结果**：脚本将测试结果显示在 `stdout` 中。
- **全局前言脚本**：测试脚本运行 `global_probe_preamble.sh` 脚本，如 HCM 全局测试示例所述。`global_probe_preamble.sh` 脚本包含 HCM 全局测试使用的库和 Shell 变量的超集。

  `global_probe_preamble.sh` 脚本执行下列任务：
  - 设置测试使用的 Shell 变量。
  - 解析命令行，评估所有 `name=value` 对，并将它们设置为 Shell 变量。例如，如果您使用 `run_all_probes.sh` 在命令行中指定 `hosts="sys1:pw1 sys2:pw2"`，则 `global_probe_preamble.sh` 脚本将变量 `$hosts` 设置为值 `"sys1:pw1 sys2:pw2"`。
  - 提供下列函数的访问权限：
    - `copy_and_run_on_multiple_hosts`：在多个远程服务器上复制并执行 Shell 脚本。
    - `copy_from_remote`：从远程服务器复制文件。
    - `copy_to_remote`：将文件复制到远程服务器。
    - `run_on_multiple_hosts`：在多个服务器上运行现有命令。
    - `run_on_single_host`：在单一服务器上运行现有命令。
- **Shell 变量**：测试脚本将命令行中 `name=value` 选项指定的 Shell 变量考虑在内。
- **身份验证**：脚本设置身份验证或公钥/私钥生成。请参见设置全局测试的无密码 SSH。

HCM 全局测试示例

以下脚本检查 SA 使用的文件系统的可用磁盘空间。此脚本在通过 `run_all_probes.sh` 命令的 `hosts` 选项指定的核心服务器上运行：

```
# Check for freespace percentage on Opsware SA filesystems
# Read in our libraries, standard variable settings, and parse
# the command line.
/opt/opsware/oi_util/lib/global_probe_preamble.sh
MAX_PERCENTAGE=80
for filesystem in /opt/opsware /var/opt/opsware \
/var/log/opsware; do
#  The leading and trailing spaces in the following printf
#  are to improve readability.
printf " Checking $filesystem:"
```

```
percent_free=`df -k $filesystem 2> /dev/null | \
grep -v Filesystem | \
awk '{print $5}' | \
sed 's/%//'`
if [ $percent_free -ge $MAX_PERCENTAGE ] ; then
echo "FAILURE (percent freespace > $MAX_PERCENTAGE)"
exit_code=1
else
echo "SUCCESS"
exit_code=0
fi
done
exit $exit_code
```

HCM 全局测试的目录布局

以下目录布局显示了全局测试的所在位置:

```
/opt/opsware/oi_util/
 |_bin
 | |_run_all_probes.sh
 | |_remote_host.py
 | |_<support_utility>
 | |_...
 | |_lib
 | |_global_probe_preamble
 |
 |_global_probes
   |
   |_verify_pre
   | |_<int><probe>.remote
   |
   |_verify_post
     |_int<probe>[.remote]
```

```
|_ ...
```

HCM 全局测试目录

`/opt/opsware/oi_util` 目录具有以下子目录：

global_probes/verify_pre

此目录包括确定指定的服务器是否是核心服务器的测试。当此类别的全局测试确定服务器未运行 SA 组件或者服务器不可访问时，将不对该服务器运行进一步的测试。

`verify_pre` 目录下仅允许具有 `.remote` 扩展名的测试。

global_probes/verify_post

此目录包括用于确定整个核心的特定方面状态的测试。例如，目录包括 `600_OPSWcheck_OS_resources.sh.remote` 脚本，检查如虚拟内存和磁盘空间等资源。

运行系统诊断

下面描述如何运行一组系统诊断。有关单个诊断测试的详细信息，请参见系统诊断测试。

要运行系统诊断测试，必须具有系统诊断操作权限。有关权限的详细信息，请参见权限参考。

在运行诊断测试之前，建议您先运行运行状况检查监控器。有关说明，请参见核心运行状况检查监控器 (HCM)、运行 HCM 本地测试和运行 HCM 全局测试。

要运行系统诊断测试，请执行以下步骤：

1. 在 SA 客户端中，在导航窗格中选择“管理”选项卡。
2. 在导航窗格中选择“设施”节点。这会显示您的所有 SA 设施。
3. 选择要运行诊断测试的设施。
4. 选择“操作”菜单或右键单击并选择“运行系统诊断”。这将显示“运行程序扩展”窗口，其中显示了系统诊断扩展。
5. **程序属性**：选择“下一步”以显示“选项”窗口。
6. **选项**：设置下列选项，然后选择“下一步”。或者要接受其余默认值并运行测试，则选择“启动作业”。
    1. 验证或更改要运行诊断测试的设施。
    2. 选择要运行的测试。有关测试的详细信息，请参见系统诊断测试。
    3. 验证或设置作业超时。如果作业未在指定时间完成，它将中止。
7. **计划**：选择希望系统诊断作业何时运行，然后选择“下一步”。
8. **通知**：输入当作业完成时接收通知的电子邮件地址。选择所需的通知类型。可以选择输入要与作业关联的工单标识符，然后单击“下一步”。
9. **作业状态**：选择“启动作业”或“计划作业”按钮。这将运行作业或计划在将来运行作业并在窗口标题中显示作业 ID 号。您可以在“作业和会话”选项卡

下使用作业 ID 号查找作业。

当作业运行时，它运行诊断测试并显示结果。

10. 选择作业状态中的任何行可查看运行的每个诊断测试的详细信息。
11. 按 Ctrl-F 可显示搜索栏。
12. 选择“导出所有结果”可创建包含结果的文件以进行进一步分析。可将结果保存为 zip 文件、文本文件或逗号隔开值文件。

有关每个诊断测试的详细信息，请参见系统诊断测试。

系统诊断测试

系统诊断工具检查 SA 核心组件的功能以及托管服务器与 SA 核心交互的能力。您可以使用 SA 诊断工具解决 SA 核心中出现的大多数错误。

系统诊断工具首先测试 SA 核心组件，然后可以选择测试您指定的托管环境中的任何服务器。系统诊断工具执行核心组件功能性的集中测试：

- **独立测试**：在不使用其他 SA 组件的情况下，尽可能多地测试某个组件的功能。独立测试验证基层功能和组件响应 XML-RPC 调用的能力。
- **全面测试**：测试所有核心组件的全部功能。

  在全面测试完成时，系统诊断工具显示每个测试是成功还是失败、测试结果和任何失败测试的错误信息。

核心组件不按特定顺序进行测试；不过，测试通常按以下顺序进行：

- 组件独立测试
- 组件全面测试

系统诊断工具测试的核心组件

组件测试模拟所有组件功能。除了错误，测试还验证每个组件是否在特定条件下能够正常工作（例如，数据库连接数是否在数据访问引擎上接近最大值）。

系统诊断工具测试下列组件：

- 模型库
- 数据访问引擎
- 软件数据库（和字存储）
- 命令引擎
- SA 核心服务器上的服务器代理
- OS 构建管理器
- 模型库多主控组件
- Web 服务数据访问引擎

数据访问引擎测试

下节描述数据访问引擎诊断测试期间发生的测试。

独立测试

- 检查当前数据访问引擎版本。
- 检查当前模型库数据库版本。
- 验证所有 Oracle 对象是否有效。
- 获取设备对象。
- 获取 MegaDevice 对象。
- 验证高级查询功能。
- 验证设备对象。
- 获取设施列表。
- 获取数据访问引擎 cronbot 作业的名称。
- 检查数据库连接的使用是否在可接受的级别下。
- 检查任何数据库连接是否已打开 600 秒以上。
- 检查数据访问引擎和模型库是否在同一设施中。
- 验证当模型库在多主控模式下运行时所有模型库垃圾回收器是否正在运行。
- 如果数据访问引擎已配置为中心多主控数据访问引擎:
    - 检查是否正在发布多主控事务。
    - 检查远程设施中是否显示了多主控事务。
    - 检查是否有多主控事务冲突。

全面测试

- 在配置的端口上测试与模型库的连接。
- 在配置的端口上测试与命令引擎的连接。
- 在配置的端口上测试与软件数据库的连接。

附加数据库权限导致的错误

如果已手动添加了 Oracle 数据库（模型库）的附加权限，则会显示下列错误消息:

```
Test Results:The following tables differ between the Data Access
Engine and the Model Repository:facilities.
```

要解决此问题，请调用数据库授权。有关说明，请参见《SA Installation Guide》中的“Troubleshooting System Diagnosis Errors”。

软件数据库测试

下节描述软件数据库诊断测试期间发生的测试。

独立测试

无。

全面测试

- 测试非程序包的文件是否可以上载到为加密文件提供服务的软件数据库进程。此测试验证该文件是否在软件数据库文件系统中存在，文件大小是否与源匹配。
- 验证是否可以从软件数据库中下载文件。
- 验证为非加密文件提供服务的软件数据库进程是否正在运行和正在服务于文件。
- 尝试在不加密的情况下下载文件。
- 验证程序包是否可以上载到软件数据库，程序包是否向模型库进行了注册。
- 验证程序包是否可以从软件数据库中删除，以及是否可以从模型库中移除。

Web 服务数据访问测试

下节描述 Web 服务数据访问诊断测试期间发生的测试。

独立测试

- 连接到 Web 服务数据访问引擎，并检索其版本信息。

全面测试

- 连接到 Web 服务数据访问引擎。
- 从模型库读取服务器记录，因而检查与模型库的连接。

命令引擎测试

下节描述命令引擎诊断测试期间发生的测试。

独立测试

- 检查计算机的状态。
- 检查会话表。
- 检查锁定状态。
- 检查是否有签名失败。
- 检查命令和服务表。
- 检查设施缓存。

全面测试

- 检查数据访问引擎连接。
- 检查安全签名。
- 检查锁定操作。
- 运行内部脚本。
- 运行外部脚本。

模型库多主控组件测试

下节描述模型库多主控组件诊断测试期间发生的测试。

独立测试

- 通过检查分类账文件，检查分类账状态。
- 报告已发送消息总数、仍在分类账文件中的消息数（例如所有侦听程序未确认的消息）以及每个侦听程序确认的最后一条消息的序列号。
- 通过检查出站模型库多主控组件的状态，检查发送方运行状况。
- 通过检查入站模型库多主控组件的状态，检查接收方运行状况。

全面测试

无。

第 9 章

SA 故障排除 - 日志文件

SA 组件将事件记录在日志文件中。这些组件日志文件是解决 SA 问题的最有价值工具之一。理解 SA 组件以及这些组件日志信息可帮您快速故障排除和解决问题的方式。当您提出支持请求时，HP 支持可能要求您发送一个或多个日志文件或会话数据文件。

本节描述日志文件、日志文件所在位置，以及您如何使用它们来解决问题。它还描述了如何创建会话数据文件。

有关 SA 内部组件名称的列表，请参见SA 核心组件内部名称。

查看日志文件

要在终端窗口中查看日志文件，请登录运行组件的服务器，使用命令行实用程序，例如 `more`、`less`、`grep` 或 `vi`。有关特定 SA 组件的日志文件请参见接下来的章节。

备注: 组件的日志文件驻留在安装组件的服务器上。

日志文件的存储位置

大部分 SA 日志文件存储在 `/var/log/opsware` 中。但是一些组件或者记录到它们自己的目录（如 Oracle），或者使用系统日志（如 NFS 和 DHCPD）。**表 31** 列出了 SA 组件以及它们的日志目录。这些信息可帮您决定哪些组件或日志文件可能有助于您解决特定问题。

表 31.SA 日志文件

产品区域	SA 组件	日志文件目录
数据库	模型库（truth 或 Oracle 数据库）	`/u01/app/oracle` 下的各种目录，或根据配置
数据访问、API	数据访问引擎 (spin)	`/var/log/opsware/spin`
	Web 服务数据访问引擎 (twist)	`/var/log/opsware/twist`
对象存储	软件数据库（字/字缓存）	`/var/log/opsware/mm_wordbot`
	Tsunami	`/var/log/opsware/tsunami`
	Memcached	`/var/log/opsware/memcached`

产品区域	SA 组件	日志文件目录
作业和会话管理	命令引擎 (way)	/var/log/opsware/waybot
全局 Shell、APX	全局文件系统、OGFS（集线器）	/var/log/opsware/hub
	全局文件系统、OGFS（轮辐）	/var/log/opsware/spoke
	APX 代理	/var/log/opsware/apxproxy
	其他	/var/log/opsware/adapter /var/log/opsware/ogfs /var/log/opsware/agentproxy /var/log (opswsshd)
网状网络通信	代理网关	/var/log/opsware/opswgw-agwsN-FACILITY
	核心网关	/var/log/opsware/opswgw-cgwsN-FACILITY
	管理网关	/var/log/opsware/opswgw-mgwsN-FACILITY
前端	SA Web 客户端 (occ)	/var/log/opsware/occ
	HTTPS 代理	/var/log/opsware/httpsProxy
网状网络复制	模型库多主控组件 (vault/OMB)	/var/log/opsware/vault
OS 配置	构建管理器	/var/log/opsware/buildmgr
	DHCPD	/var/log，或按 syslog 配置
	Samba	/var/log/samba
	NFS	/var/log，或按 syslog 配置
代理部署	代理缓存	/var/log/opsware/agentcache
启动	SA 初始脚本	/var/log/opsware/startup
SA 代理	SA 代理	/var/log/opsware/agent

产品区域和相关组件日志文件

了解**表 31** 中列出的每个组件的功能用途可帮助您确定在解决问题时从哪些组件和日志入手。在许多情况下，问题上下文（包括错误消息或回溯）有助于您了解要检查的日志。

例如，当解决代理通信问题时，关键的一步是识别所有网状网络通信中所涉及的一个或多个网关以及是否某网关关闭或不能正常起作用，网状网络通信将受影响。

表 32 列出了当解决问题时要检查的 SA 产品区域和日志文件。

表 32.产品区域和相关组件日志文件

产品区域	数据库日志	数据访问日志	对象存储日志	作业管理日志	全局 Shell 日志	网状网络通信日志	代理日志
代理部署	X	X	X		X	X	X
审核与符合性	X	X	X	X	X	X	X
软件管理的修正	X	X	X	X		X	X
安装修补程序	X	X	X	X		X	X
运行脚本	X	X		X	X	X	X
应用程序配置	X	X		X		X	X
OS 配置	X	X		X	X	X	X
全局 Shell、APX	X	X			X	X	X
临时设备管理	X	X			X	X	X

关于日志文件大小

日志文件的默认最大大小为 10 MB。当达到指定的最大文件大小时，将创建附加日志文件。

如果提高任何组件的日志级别，则通常日志文件增长地将显著快于默认日志级别。非常重要的一点是您仅可在短期内提高日志级别，时间足够收集您正解决的问题的日志信息即可，然后再将调试级别设回默认值。

关于组件日志级别

默认情况下，大部分 SA 组件被设置为仅记录错误和警告。临时提高个别组件上的日志级别可显示更多详细消息，这有助于您了解特定组件出了什么问题。

提高日志级别可能会引起其他开销和性能损失，所以请不要长期保持高日志级别。仅在主动诊断问题时将其提高，然后在您结束时将其恢复。

更改日志级别之前，请保存原始日志级别以便在结束时方便复原。在编辑原始配置文件之前对其备份，然后在您结束时将其恢复。

日志级别通常遵循一个常用的命名格式：

- 跟踪
- 调试
- 信息
- 警告
- 错误
- 致命
- 最佳

日志级别命名可因组件而异，但大部分遵循标准化的命名

更改组件日志级别

本节描述如何为支持日志级别的各种 SA 组件更改日志级别。因为网状网络中可能存在多个组件实例，所以可能需要在多个服务器（如 SA 切分或 SA 卫星端）上执行这些步骤。

启动服务器日志

启动服务器不生成其自己的日志。启动服务器使用下列服务：带有 INETD 的 TFTP、NFS 服务器和 ISC DHCPD。所有这些服务都使用 `syslog` 进行日志记录。有关详细信息，请参考供应商文档。另请参见 `syslog.conf` 文件，该文件用来配置启动服务器以确定如何为此组件配置日志记录。

构建管理器日志

这些日志位于以下文件中：

```
/var/log/opsware/buildmgr/buildmgr.log
```

命令引擎日志

这些日志位于以下文件中：

```
/var/log/opsware/waybot/waybot.err*
/var/log/opsware/waybot/waybot.log*
```

更改日志级别

要更改命令引擎的日志级别，请编辑文件 /etc/opt/opsware/waybot/waybot.args，并添加具有所需日志级别的以下行：

```
loglevel:DEBUG
```

您必须重新启动命令引擎才能使此更改生效。

数据访问引擎日志

这些日志位于以下文件中：

```
/var/log/opsware/spin/spin.err*
/var/log/opsware/spin/spin.log*
```

备注: 在具有多个数据访问引擎的核心中，每个运行引擎的服务器都有一组上述日志文件。

HP Live Network (HPLN) 日志

这些日志位于以下位置：

```
/var/log/opsware/hpln
```

介质服务器日志

这些日志位于以下文件中：

```
/var/log/opsware/samba/log.smbd
/var/log/opsware/samba/log.nmbd
```

Solaris 和 Linux OS 配置使用供应商提供的服务，例如 NFSD。这些服务通常通过 `syslog` 进行日志记录。有关这些日志文件的详细信息，请参考供应商文档。

模型库日志

模型库是 Oracle 数据库。数据库日志的位置特定于您的安装。有关详细信息，请参见《SA Installation Guide》中的“Monitoring Oracle Log Files”一节。

模型库多主控组件日志

这些日志位于以下文件中：

```
/var/log/opsware/vault/err*
```

```
/var/log/opsware/vault/vault.n.log
```

更改日志记录

要配置模型库多主控组件的日志文件名称、日志文件大小或日志记录级别，请在 SA 客户端中选择“管理”选项卡，在导航面板中选择“系统配置”，然后选择“模型库多主控组件”。这将显示可用于模型库多主控组件的日志文件、日志级别和日志大小系统配置参数。设置所需的值后，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。

另外，要更改模型库多主控组件的日志级别，请编辑文件 `/etc/opt/opsware/vault/logging.properties` 并更改以下行。

```
.level=INFO
```

默认日志级别值为 INFO。

您必须重新启动模型库多主控组件才能使此更改生效。有关说明，请参见启动单个 SA 核心组件。

代理日志

代理在托管服务器上创建以下日志文件：

UNIX：

```
/var/log/opsware/agent/agent.log*
/var/log/opsware/agent/agent.err*
```

Windows：

```
%ProgramFiles%Common Files\opsware\log\agent\agent.log*
%ProgramFiles%Common Files\opsware\log\agent\agent.err*
```

SA 客户端日志

SA 客户端不生成其自身日志。SA 客户端使用 JBoss 服务器，该服务器写入以下日志文件：

```
/var/log/opsware/occ/server.log*
/var/log/opsware/httpsProxy/*log*
```

更改日志级别

要更改 SA 客户端的日志级别，请编辑 `/opt/opsware/occ/occ/conf/log4j.xml` 文件并更改所需命名空间的 `org.jboss.logging.XLevel` 特性值。默认值为 INFO。

要使此次更改生效必须重新启动 SA 客户端。

软件数据库日志

这些日志位于以下文件中：

```
/var/log/opsware/mm_wordbot/wordbot.err*
/var/log/opsware/mm_wordbot/wordbot.log*
```

更改日志级别

要更改软件数据库的日志级别，请编辑文件 `/etc/opt/opsware/mm_wordbot/mm_wordbot.args`，并将下列属性更改为所需的日志级别：

```
logLevel: logging.Level.INFO
```

例如，要将日志记录设置为调试，请将此值设置为下列值：

```
logLevel: logging.Level.DEBUG
```

您必须重新启动软件数据库才能使此更改生效。有关说明，请参见启动单个 SA 核心组件。

Web 服务数据访问引擎日志

Web 服务数据访问引擎包含下列日志文件：

```
/var/log/opsware/twist/stdout.log*
/var/log/opsware/twist/twist.log
/var/log/opsware/twist/access.log
/var/log/opsware/twist/server.log*
/var/log/opsware/twist/boot.log
/var/log/opsware/twist/watchdog.log
```

`stdout.log` 文件包含服务器生成的每个异常的调试输出和日志记录。该文件不符合特定格式。* 表示文件为 1og.1、log.2、log.3 等等。文件数量和每个文件的大小都可使用 twist.conf 进行配置。当达到指定的最大文件大小时，将创建附加日志。stdout.log 是最新文件，stdout.log.1 到 stdout.log.5 是渐增的早期文件。该文件还会在启动时轮循。此文件也包含任何 System.out.println()、System.err.println() 和 e.printStackTrace() 声明的输出。

`twist.log` 文件包含 JBoss 特定的错误或参考消息和 Weblogic 特定的消息。这些文件在启动时轮循。

`access.log` 文件包含普通日志格式的访问信息。当该文件达到 5MB 大小时，这些文件将轮循。

server.log 文件包含从 Web 服务数据访问引擎生成的调试消息。调试消息受 twist.conf 文件中的包或类级别设置的日志级别控制。* 表示文件为 1og.1、log.2、log.3 等等。可以通过 twist.conf 配置文件数和每个文件的大小。server.log.0 始终是当前文件，而 erver.log.9 是最旧的文件。

boot.log 文件包含有关当启动 Web 服务数据访问引擎时生成的初始此外，boot.log 文件还包含 Kill – QUIT 命令的输出。

watchdog.log 文件每分钟记录一次 Web 服务数据访问引擎的状态。

更改日志级别

要更改 Web 服务数据访问引擎的日志级别，请编辑文件 `/etc/opt/opsware/twist/twist.conf`。将日志级别从“警告”更改为“最佳”或默认日志级别的另一个值或您感兴趣的另一个记录器命名空间的值。此文件中有多个命名空间。您可更改所有命名空间或单个命名空间的日志级别。

网关日志

这些日志位于以下文件中：

/var/log/opsware/<*gateway-name*>/opswgw.log*

其中 <gateway-name> 是指定网关组件的目录。

更改日志级别

要更改任何网关组件的日志级别，请创建或编辑文件 /etc/opt/opsware/<*gateway-name*>/opswgw.custom 并在下列行中设置日志级别。

```
opswgw.LogLevel=INFO
```

必须在更改日志级别后重新启动网关。有关说明，请参见重新启动或停止网关进程。

全局文件系统日志

OGFS 日志文件位于以下文件中：

```
/var/log/opsware/hub/OPSWhub.log*
/var/log/opsware/ogfs/ogsh.err*
/var/log/opsware/adapter/adapter.err*
/var/log/opsware/agentcache/agentcache.log
/var/log/opsware/spoke/spoke-*.log
/var/log/opsware/spoke/stdout.log
```

更改日志级别 - OGFS 集线器组件

要更改 OGFS 集线器组件的日志级别，请执行以下步骤：

1. 以管理用户的身份登录全局 Shell (OGSH)。有关说明，请参见《SA 用户指南：Server Automation》。
2. 要确定当前日志级别，请检查文件 /opsw/sys/hub/loglevel。例如，运行以下 OGFS 命令：

   ```
   more /opsw/sys/hub/loglevel
   ```

3. 要更改日志级别，请输入以下 OGSH 命令：

   ```
   echo "MESSAGE ON" > /opsw/sys/hub/loglevel
   ```

   ```
   echo "LEVEL FINE" > /opsw/sys/hub/loglevel
   ```

默认值是“MESSAGE OFF”和“LEVEL INFO”。

更改日志级别 - OGFS 轮辐组件

要更改 OGFS 轮辐组件的日志级别，请编辑文件 /etc/opt/opsware/spoke/spoke_custom.conf。修改以下行或者将以下行添加到此文件，并设置所需的日志级别：

```
.level=INFO
```

更改日志级别后必须重新启动 OGFS 轮辐组件。有关说明，请参见启动单个 SA 核心组件。

HTTPS 服务器代理日志

这些日志位于：

```
/cust/apache/servers/https-Proxy/logs
```

备注: 日志文件 `ssl_request_log` 可能增长得很大，如果您担心磁盘空间可用性，则应当检查此日志文件。

APX 代理日志

APX 代理日志文件位于 `/var/log/opsware/apxproxy/`。

更改日志级别

要更改 APX 代理组件的日志级别，请创建或编辑文件 `/etc/opt/opsware/apxproxy/apxProxyOverides.conf`。添加或修改下列行，并设置所需的日志级别：

```
.level = INFO

com.opsware.level=INFO

com.opsware.apxproxy.level=CONFIG
```

更改日志级别后必须重新启动 APX 代理。有关说明，请参见启动单个 SA 核心组件。

`/etc/opt/opsware/apxproxy/apxProxy.conf` 文件中列出了这些属性的可能值。

SSHD 日志

SSHD 日志文件位于 syslog 配置的位置，通常为 `/var/log`。

更改日志级别

要更改 SSHD 组件的日志级别，请编辑文件 `/etc/opt/opsware/sshd/sshd_conf`。修改以下行，并设置所需的日志级别：

```
LogLevel INFO
```

更改日志级别后必须重新启动 SSHD。有关说明，请参见启动单个 SA 核心组件。

全局 Shell 审核日志

当用户使用全局 Shell 功能访问或修改托管服务器时，SA 将事件记录在审核日志中。全局 Shell 审核日志包含有关下列事件的信息：

- 使用全局 Shell 和远程终端会话进行登录和注销
- 全局 Shell 和远程终端会话中输入的命令
- 托管服务器上的文件系统操作（例如创建和删除）
- 通过远程 Shell (`rosh`) 在托管服务器上运行的命令和脚本

备注: 全局 Shell 审核日志位于安装 OGFS 的服务器上。

要查看日志文件，请打开终端窗口，登录运行 OGFS 的服务器，使用命令行实用程序，例如 `more`、`grep` 或 `tail`。有关使用 `tail` 命令的示例，请参见监控全局 Shell 审核日志的示例。

全局 Shell 审核日志由三组日志文件组成：

- Shell 事件日志
- Shell 流日志
- Shell 脚本日志

Shell 事件日志

shell 事件日志包含有关用户使用全局 Shell 在托管服务器上执行的操作的信息。这些日志位于以下目录中（其中 *ogfs-host* 是运行 OGFS 的服务器的名称）：

`/var/opt/opsware/ogfs/mnt/audit/event/`***ogfs-host***

日志文件名具有下列语法（其中 *n* 是日志轮循编号）：

`audit.log.`***n***

对于每个事件，SA 将单行写入到事件日志文件中。日志文件中的每行包含有关事件的下列信息：

- 事件的唯一 ID
- 父事件的唯一 ID
- 操作日期
- 执行操作的 SA 用户的 ID
- 执行操作的 SA 用户的名称
- 生成审核事件的组件的名称
- 生成审核事件的 SA 组件的版本
- 生成审核事件的 SA 功能的名称
- 操作的名称
- 详细级别
- 事件的退出状态
- 托管服务器的 ID
- 托管服务器的名称
- 事件的详细信息

下面的示例显示了审核事件日志文件中的单行：

```
jdoe@m185:051202182224813:13 jdoe@m185:051202182224790:12
2006/01/28-12:40:19.622 User.Id=2610003 User.Name=jdoe
```

```
Hub:1.1 GlobalShell AgentRunTrustedScript 1 OK
Device.Id=10003 Device.Name=m192.dev.opsware.com
ConnectMethod=PUSH RemotePath= RemoteUser=root
ScriptName=__global__.sc_snapshot.sh
ScriptVersion=30b.2.1572 ChangeTime=1128971572
RemoteErrorName=
```

在此示例中，第一个字段是事件的 ID：

```
jdoe@m185:051202182224813:13
```

该 ID 字段具有以下语法：

opsware-user@*ogfs-host*:*YYMMDDHHmmssSSS*:*n*

该 ID 字段结尾的 *n* 是会话中生成的审核事件的序列号。该 ID 字段与 Shell 流日志文件的名称相匹配。

Shell 流日志

Shell 流日志包含从全局 Shell 运行的脚本的 `stdout`。这些日志位于以下目录中（其中 *ogfs-host* 是运行 OGFS 的服务器的名称）：

`/var/opt/opsware/ogfs/mnt/audit/streams/`***ogfs-host***

日志文件名具有下列语法：

opsware-user@*ogfs-host*:*YYMMDDHHmmssSSS*:*n*

日志文件名与 Shell 事件日志中的 ID 字段相匹配。日志文件中的标题行包含文件名、字符集、版本和 SA 用户名。如果脚本的 `stdout` 包含控制字符，则 Shell 流日志将包含同样的控制字符。

Shell 脚本日志

Shell 脚本日志包含从全局 Shell 运行的脚本的内容。这些日志位于以下目录中（其中 *ogfs-host* 是运行 OGFS 的服务器的名称）：

`/var/opt/opsware/ogfs/mnt/audit/scripts/`***ogfs-host***

日志文件的名称是基于此脚本内容的哈希字符串，例如：

```
23f1d546cc657137fa012f78d0adfdd56095c3b5
```

日志文件中的标题行包含文件名、字符集、版本和 SA 用户名。

监控全局 Shell 审核日志的示例

以下示例监控由登录到带有远程终端会话的托管服务器的最终用户输入的命令：

1. 在终端窗口中，以 `root` 身份登录运行 OGFS 的核心服务器。以下步骤中涉及的窗口是指“审核窗口”。
2. 在审核窗口中，转到 `audit/event` 目录：

   ```
   cd /var/opt/opsware/ogfs/mnt/audit/event/ogfs-host
   ```

3. 在 SA 客户端，打开到 UNIX 托管服务器的远程终端。
4. 在审核窗口中，检查 audit.log 文件的最后一行：

   ```
   tail -1 audit.log.n
   ```

   例如，audit.log 文件中的下列条目表示 SA 用户 jdoe 打开了主机 (Device.Name) 的远程终端 toro.example.com。事件 ID 为 jdoe@m235:060413184452579:59。

   ```
   jdoe@m235:060413184452595:60 jdoe@m235:060413184452579:59
   2006/04/13-18:44:52.728 User.Id=6220044 User.Name=jdoe
   Hub:1.1 GlobalShellAgentLogin 1 OK Device.Id=840044
   Device.Name=toro.example.com ConnectMethod=JUMP RemotePath=
   RemoteUser=root
   ```

5. 在审核窗口中，转到 audit/streams 目录：

   ```
   cd /var/opt/opsware/ogfs/mnt/audit/streams/ogfs-host
   ```

6. 在审核窗口中，使用 tail -f 命令监控对应于远程终端会话的文件。文件名与事件 ID 相同。例如，如果事件 ID 为 jdoe@m235:060413184452579:59，则您需要输入下列命令：

   ```
   tail -f jdoe*59
   ```

7. 在远程终端窗口，输入 UNIX 命令，如 pwd 和 ls。
8. 观察审核窗口。远程终端会话中的命令（及其输出）写入 audit/streams 目录中的文件。

全局 Shell 审核日志中的数字签名

Shell 流和脚本日志文件包含数字签名和指纹，它们是使用 RSA-SHA1 算法生成的。要验证日志文件的签名和指纹，请打开终端窗口，登录 OGFS，输入下列命令：

```
/opt/opsware/agentproxy/bin/auditverify stream_file_name \
rsa_key_path
```

这是 bash 中的示例：

```
STREAMDIR=/var/opt/opsware/ogfs/mnt/audit/streams/acct.opsw.com

STREAMFILE=jdoe@somehost:051210003000111:61

RSAKEYPATH=/var/opt/opsware/crypto/waybot/waybot.srv

/opt/opsware/agentproxy/bin/auditverify $STREAMDIR/$STREAMFILE \
$RSAKEYPATH
```

如果日志文件未被修改，则 auditverify 将显示以下信息：

```
[AuditVerify]:Verification Result:Valid Signature
```

默认情况下，日志使用下列文件中的私钥进行签名：

```
/var/opt/opsware/crypto/agent/agent.srv
```

要更改用于签名的密钥文件，请按照配置全局 Shell 审核日志中所述修改 `audit.signature.key_path` 系统配置参数。

全局 Shell 审核日志的存储管理

通过定期删除 Shell 流和脚本日志文件，SA 阻止这些文件填满可用磁盘空间。SA 提供用于确定何时删除日志文件的系统配置参数。通过这些参数，您可以根据文件的寿命 (archive_days) 或文件使用的磁盘空间量 (archive_size) 来指定日志文件的删除。

下列参数指定要删除的文件的寿命：

`audit.stream.archive_days`

`audit.script.archive_days`

下列参数指定删除文件之前文件可以占据的磁盘空间量：

`audit.stream.archive_size`

`audit.script.archive_size`

有关这些参数的详细信息，请参见**表 33**。有关修改这些系统配置的说明，请参见配置全局 Shell 审核日志。

表 33.全局 Shell 审核日志配置的参数

参数	描述	默认值
`audit.script.archive_days`	将删除比该值早（以天计）的审核脚本文件。0 表示从未删除文件。	100
`audit.script.archive_size`	所有审核脚本文件使用的最	100

参数	描述	默认值
	大磁盘空间量（以 MB 计）-。首先删除较早的文件。0 表示没有最大值。	
audit.signature.algorithm	当对审核流签名时要使用的签名算法。	RSA-SHA1
audit.signature.key_path	当对审核流签名时使用的私钥的位置。	/var/opt/opsware/crypto/waybot/waybot.srv
audit.stream.archive_days	将删除比该值早（以天计）的审	10

参数	描述	默认值
	核流文件。0 表示从未删除文件。	
audit.stream.archive_size	所有审核流文件使用的最大磁盘空间量（以 MB 计）-。首先删除较早的文件。0 表示没有最大值。	1000
audit.stream.file_keep	轮循审核流文件的最大数量。	50
audit.stream.file_size	审核流的最大文件大	10

参数	描述	默认值
	小。以 MB 为单位进行指定。最大允许值为 50M-B。	

配置全局 Shell 审核日志

您可以更改全局 Shell 审核日志的某些系统配置参数，例如最大日志文件大小。有关可以更改的参数的列表，请参见**表 33**。要配置参数，请执行以下步骤：

1. 在 SA 客户端中选择“管理”选项卡。
2. 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。
3. 在 SA 组件列表中，选择“集线器”。将显示此组件的系统配置参数。
4. 按**表 33** 所列，查找并修改要更改的系统配置参数。
5. 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。

提取会话数据

SA 保存有关作业的上下文和其他信息，也称之为“方式会话”或简化为“会话”。默认情况下，此会话数据在被回收重用空间之前可保存七天。此数据对于解决作业和会话问题十分有用。您还可能要保存有效会话数据以便与出现问题的情况进行比较。

可以使用 dump_session 工具提取和保存此信息。dump_session 工具生成一个压缩包文件，将会话数据包含在一个名为 `Session<job_ID>.pkl.gz` 的文件中。

本节描述 dump_session 工具以及如何使用它来提取会话数据。

要捕获 SA 作业的会话数据，请执行以下步骤：

1. 确定有问题的作业或命令的数字作业 ID。对于作业，请在 SA 客户端中选择“作业和会话”选项卡，查找所需的作业。“作业 ID”列中列出了作业 ID。
2. 登录 SA 核心服务器。
3. 运行 dump_session 工具，将作业 ID 作为第一个参数提供。例如：

   ```
   # /opt/opsware/bin/dump_session <job_ID>
   ```

4. 保存会话输出，它是位于当前工作目录中的名为 `Session<ID>.pkl.gz` 的

压缩包。
5. 如果 HP 支持人员请求，请将该压缩包附加到问题的支持事件。

列出最近的会话

可以通过运行带有 -l 选项的 dump_session 并指定要查看的作业数，列出最近的作业集。例如，下列命令列出最近 25 个作业：

```
# /opt/opsware/bin/dump_session -l 25
```

使用 -l 列出的默认作业数为十。

以下是五个会话的输出示例：

```
# /opt/opsware/bin/dump_session -l 5

Session ID | Start Date | Session Desc

26000001 | 20100902T12:00:01 | 'Automated Communications Test for core 1'

25980001 | 20100902T15:00:00 | 'opsware.patch_compliance'

26030001 | 20100902T17:51:57 | 'Communication Test'

25990001 | 20100903T00:00:00 | 'Automated Hypervisor Scan for core:1'

26010001 | 20100903T00:00:01 | 'Automated Communications Test for core 1'
```

示例输出

下面显示了示例 dump_session 命令和 SA 作业 ID 1870001 的示例输出：

```
# /opt/opsware/bin/dump_session 1870001

Dumping session to 'Session1870001.pkl.gz'

Session:1870001

MegaServiceInstance:20001

WayScriptVersion:1830001

SecurityUser:60001

Realm:0

Device:10001

WayScript:1830001
```

dump_session 命令参考

本节描述 dump_session 命令语法和选项。dump_session 命令位于 /opt/opsware/bin/dump_session。它从 SA 数据库提取 SA 会话和相关命令，并对它们进行

格式化。

语法

```
dump_session [<session_id> ...][<session_file> ...][-h] [-l <num>] [-d<num>]
```

选项

表 34 列出了 dump_session 命令的选项。

表 34. dump_session 选项

选项	描述
<*session_id*>	指定一个或多个 SA 作业 ID。有关这些作业的信息将从 SA 数据库复制到当前工作目录中名为“<*session_id*>.pkl.gz”的压缩集合文件中。
<*session_file*>	指定一个或多个以前保存的 <session_id>.pkl.gz 文件。这些文件将被处理并转换为类似 waybot 后端 Web UI 的静态 HTML 目录结构。
-h	显示帮助信息。
-l <*num*>	将网状网络中每个核心上执行的最后 <*num*> 个 SA 作业显示到 stdout。如果忽略 <*num*>，则假设为 10 个。只有当 -l 是命令行中的最后一个参数时，才可以忽略 <*num*>。
-d<*num*>	将调试级别设置为指定的数字。

第 10 章

SA 通知配置

本节描述用户可定义的配置参数，您可以使用这些参数修改 SA 客户端帮助中的联系信息，配置核心邮件服务器，设置核心电子邮件警报地址等。

配置参数通常是在 SA 核心安装采访过程中指定的。有关详细信息，请参见《SA Installation Guide》。

警告: 各种系统配置参数的许多默认值都不得更改，除非您的技术支持代表或顾问明确指示要这样做。

备注: 服务器代理仅在安装时读取系统配置值。如果您更改任何配置值，则必须手动更新所有代理的配置。若要获得关于进行这些更改或在 SA 系统配置中进行任何其他更改的帮助，请与 HP Server Automation 支持代表联系。

配置 SA 帮助中的 SA 管理员联系信息

要配置 Server Automation 帮助页中显示的 SA 管理员联系信息，请执行下列任务：

1. 以 root 用户身份登录到运行核心命令中心 (OCC) 的服务器。
2. 切换到以下目录：

   ```
   /etc/opt/opsware/occ
   ```

3. 在文本编辑器中打开 `psrvr.properties` 文件。
4. 更改下列字段中的值，以指定 SA 客户端帮助中的联系信息：

   ```
   pref.occ.support.href
   ```

   ```
   pref.occ.support.tex
   ```

5. 保存文件，并退出编辑器。
6. 通过输入以下命令，重新启动 OCC：

   ```
   /etc/init.d/opsware-sas restart occ.server
   ```

为设施配置邮件服务器

SA 核心组件使用系统配置参数 `opsware.mailserver` 来确定用于电子邮件通知的邮件服务器地址。默认情况下，`opsware.mailserver` 的值为 `smtp`，如果未指定任何值，则使用该值。大多数系统可成功使用该值。

但是，如果您需要为 `opsware.mailserver` 指定其他值，请执行下列步骤：

1. 在 SA 客户端中选择“管理”选项卡。
2. 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。
3. 在 SA 组件列表中，选择设施。将显示该设施的系统配置参数。
4. 查找参数 opsware.mailserver。
5. 在值列中，直接输入新值，或者选择新值按钮  ，然后输入邮件服务器的主机名。
6. 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。

配置命令引擎通知电子邮件

1. 在 SA 客户端中选择“管理”选项卡。
2. 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。
3. 在 SA 组件列表中，选择“命令引擎”。将显示此组件的系统配置参数。
4. 查找参数 way.notification.email.fromAddr。
5. 在值列中，直接输入新值，或者选择新值按钮  ，然后输入命令引擎为了向用户通知计划作业而将要发送的电子邮件的“发件人”电子邮件地址。
6. 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。
7. 使用以下命令重新启动命令引擎组件：

   ```
   /etc/init.d/opsware-sas restart occ.server
   ```

8. 如果 SA 在多主控模式下运行，则重新启动模型库多主控组件。

   当重新启动多个 SA 组件时，必须按正确的顺序重新启动它们。请参见启动独立 SA 核心。

配置 SA 核心的电子邮件警报地址

要求: 服务器代理仅在安装时读取系统配置值。如果您更改任何配置值，则必须手动更新所有代理的配置。若要获得关于进行这些更改或在 SA 系统配置中进行任何其他更改的帮助，请与 HP SA 支持代表联系。

执行下列任务以配置电子邮件通知地址。SA 核心安装使用这些参数的默认值 (`EMAIL_ADDR`)。

1. 在 SA 客户端中选择“管理”选项卡。
2. 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。
3. 在 SA 组件列表中，选择“SA 代理”。将显示此组件的系统配置参数。

4. 根据需要，查找并修改下列参数：
   - 在参数 `CronbotMailAlertsEnabled` 中，指定值 `1` 以启用 cronbot 电子邮件警报。要禁用 cronbot 电子邮件警报，请指定值 `0`。
   - 在参数 `CronbotAlertAddress` 中，输入服务器代理用来向收件人通知失败的计划作业的电子邮件地址。
5. 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。

配置多主控网状网络的电子邮件警报地址

执行下列任务以配置多主控网状网络的电子邮件通知地址。SA 核心安装使用这些参数的默认值 `EMAIL_ADDR`。

1. 在 SA 客户端中选择“管理”选项卡。
2. 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。
3. 在 SA 组件列表中，选择“模型库，多主控组件”。将显示此组件的系统配置参数。
4. 根据需要，查找并修改下列参数。
   - 在字段 `sendMMErrorsTo` 中，输入多主控冲突将发送到的电子邮件地址。
   - 在字段 `sendMMErrorsFrom` 中，输入 SA 将用作多主控冲突警报电子邮件“发件人”地址的电子邮件地址。
5. 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。

重新启动多主控网状网络中的所有 SA 核心中的模型库多主控组件。请参见启动单个 SA 核心组件。

第 11 章

全局 Shell：Windows 子身份验证包

在 Microsoft® Windows 下，如果不提供用户帐户的密码，则程序（服务或应用程序）无法获取该用户帐户的登录会话句柄。如果没有用户名和密码，则运行的程序无法模拟或充当该程序当前用其身份运行的用户之外的其他用户。

此限制也适用于 SA 代理。SA 代理安装后运行在 LocalSystem 安全上下文中。LocalSystem 登录会话是一个特别的、受信任的且已授权的安全上下文，此安全上下文在每个运行 Windows Server 2003、2008 和 2012 操作系统的 Windows 服务器上的启动时间创建。但是，如果 SA 代理需要在另一个用户的安全上下文（如 *<DOMAIN>\<username>*）中运行子进程，则它需要该用户帐户的密码。用户名、密码和子程序名称都传送到 Win32 API `LogonUser()`。

SA 代理代表 SA 全局 Shell 功能在托管服务器上执行操作。SA 用户可以使用全局 Shell 功能和 SA 代理在托管服务器上执行注册表读取操作、文件创建和浏览操作。如果 SA 用户想要以 LocalSystem 用户身份执行操作，则 SA 代理只需要创建一个在代理本身的安全上下文中运行的子进程。如果 SA 想要以非 LocalSystem 用户身份执行全局 Shell 操作，则代理不能使用 Win32 API `LogonUser()`，因为它需要用户帐户密码。有关全局 Shell 操作的详细信息，请参见《SA 用户指南：Server Automation》。

Microsoft Windows 身份验证过程

Microsoft Windows 身份验证是验证用户是否有权访问系统的过程。在此验证过程中，用户提供哈希加密的密码。此哈希值然后与存储值进行比较。

Windows 提供一个支持其他身份验证形式的子系统。此子系统称为 Microsoft® Windows 本地安全机构子系统 (LSASS)，采用在 Windows 服务器上运行 lsass.exe 应用程序的进程形式。

LSASS 的设计允许 Windows 支持多个身份验证包。这些身份验证包对密码、Kerberos 标记、指纹、视网膜图案等进行验证。

在标准 Windows NT4 安装中，LSASS 有一个称为 MSV1_0 的身份验证包。MSV1_0 是实现 NT4 域身份验证的身份验证包。任何时候您登录 Windows NT4 服务器，提供用户名、密码和域名时，或者任何时候您在 Windows NT4 服务器上安装共享时，您都在与 MSV1_0 身份验证包交互。在 Windows 2000 服务器上，标准身份验证包集合由 MSV1_0 和 Kerberos 组成。取决于域配置，任何登录尝试将让用户与这些身份验证包之一进行交互。MSV1_0 和 Kerberos 还可用作 Windows Server 2003、2008 和 2012 上的身份验证包。

Microsoft Windows 子身份验证包

所有主 Microsoft Windows 身份验证包都支持将凭据检查委托给称为子身份验证包的代码。子身份验证包是一个 DLL，它对主身份验证包使用的身份验证和验证标准进行补充或替换其中的一部分。

MSV1_0 身份验证包可以（在客户端的请求下）将用户名和密码的验证转给以前注册的子身份验证包。默认情况下，MSV1_0 使用其自己的内部用户名和密码检查软件。只有当 Windows 客户端（如 SA 代理）请求特定子身份验证模块（MSV1_0 将该特定模块委托给已标识的模块）时。

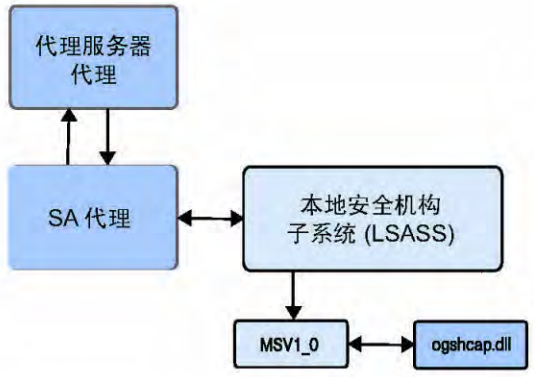
SA 子身份验证包

SA 提供 MSV1_0 子身份验证包，当 SA 代理对必须以其身份运行全局 Shell 操作（例如子进程）的用户进行身份验证时会请求该子身份验证包。该子身份验证包是名为 *ogshcap.dll* 的 DLL（其中 *ogshcap* 代表全局 Shell 自定义身份验证和子身份验证包）。

客户端应用程序将提供给 Windows 的凭据传递到 ogshcap.dll 文件。该 DLL 在所有受支持的 Windows 操作系统（Windows Server 2003、2008 和 2012）中使用，在每个操作系统中的使用方式相同。

图 37 演示了 SA 中的子身份验证过程。

图 37.子身份验证过程流



就 SA 代理而言，该代理在调用特殊 Windows API 以请求 SA 子身份验证包 (ogshcap.dll) 进行的子身份验证时，会随用户名传递 NULL 密码。Windows API 然后调用 MSV1_0 身份验证包，该包继而将凭据（包括 NULL 密码）传递给请求的子身份验证包。

SA 子身份验证包执行检查，以验证用户帐户未被锁定或禁用，且调用客户端为 SA 代理。DLL 忽略密码字段，该字段留空 (NULL)。通过其验证步骤后，DLL 会将成功状态返回到 MSV1_0，MSV1_0 创建一个随后传递到 LSASS 的登录会话。接下来，LSASS 将此登录会话的句柄传递到 SA 代理。此登录会话句柄然后由 SA 代理传递到对 Win32 API `CreateProcessAsUser()` 的调用，以便以非 LocalSystem 的用户身份运行子进程。

Windows 被请求使用 ogshcap.dll 文件执行单一子身份验证操作后，Windows 会打开此文件，并保持打开，直到服务器下次重新启动为止。这意味着，在下次重新启动之前不能删除 ogshcap.dll，也不能在代理安装或升级期间未重新启动的情况下覆盖它。

备注: 对于所有 Windows 操作系统，要进行身份验证的安全主体的用户名必须是本地服务器上 Administrators 组的成员，或者是服务器所属主域的 Domain Admins 组的成员。

SA 代理安装更改

在所有 Windows 操作系统上安装 SA 代理期间，会创建下列注册表项的新 Windows 注册表值（如果它尚不存在）：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0

该新注册表值属于 REG_SZ 类型，包含：

- **名称**：Auth155
- **值**：ogshcap

SA 代理安装程序包含 ogshcap.dll 文件。在代理安装期间，ogshcap.dll 文件复制到下列源位置：

```
%SystemDrive%:\Program Files\Opsware\bin\ogshcap.dll
```

在此位置创建该 DLL 文件后，代理安装程序尝试将其复制到下列目标位置：

```
%SystemRoot%\system32\ogshcap.dll
```

如果此类文件在目标位置当前不存在，则复制成功。如果由于该文件已打开和正在使用而导致复制失败，代理安装程序会计算源文件和目标文件的加密哈希。如果源文件和目标文件的哈希不同，则代理安装程序调用 `Win32 API MoveFileEx()`，其将创建 Windows 内部的注册表项。该注册表项通知 Windows 必须在下次重新启动时将目标文件替换为源文件。

如果无法计算这两个或其中一个 DLL 文件的哈希，代理安装程序将假设 DLL 的替换是需要保证的。例如，如果代理安装程序无法加载 Microsoft 加密模块，则无法计算哈希。代理安装程序则假设必须替换 DLL。

可以通过在代理安装程序命令行上指定安装程序选项 (`--reboot`)，在代理安装后启动安装后重新启动。

备注: 当需要安装后重新启动以获取最新版本的 DLL 时，重新启动执行移动操作，将源位置中的 DLL 移动到目标位置。因此，源 DLL 文件覆盖目标 DLL。

如果必须替换操作系统上的现有 ogshcap.dll 且需要重新启动才能完成此操作，代理安装程序（默认情况下）不启动重新启动。只有当执行安装的人员将 `--reboot` 指定为命令行选项时，才发生重新启动。

所有操作系统上的代理安装程序都接受 `--reboot` 选项；不过，它只在 Windows 操作系统上执行。例如，如果
在 Linux 7.2 操作系统上代理安装期间指定了 `--reboot` 选项，则代理安装程序将不执行重新启动。相比之下，如果
在 Windows 2000 操作系统上代理安装期间指定了 `--reboot` 选项，则代理安装程序将执行重新启动。

如果已计算哈希，且源文件和目标文件验证为相同，则不尝试覆盖已打开的 ogshcap.dll 文件。

代理始终执行 ogshcap.dll 的首次安装，或者分析是否应当使用代理安装程序负载中的 DLL 版本覆盖现有 DLL。在这种情况下，无法阻止代理安装程序安装此 DLL。

如果代理安装程序指示需要重新启动，但是代理安装后未发生重新启动，则 SA 代理将使用 DLL 的过时版本，直到发生重新启动为止。这意味着，SA 代理将不使用新 DLL 中的任何缺陷修补程序或经过修改的功能，直到重新启动为止。不过，旧 DLL 代表 SA 代理进行的 Windows 身份验证仍将成功，甚至在该 DLL 标记为将被更新的 DLL 替换时也是这样。

下列代理安装程序日志示例取自 ogshcap.dll 的安装。在此案例中，不需要替换操作系统上的现有 DLL。

```
[08/Jun/2005 20:59:18] [INFO] Install CAP file if differing
checksum between new and existing file.

[08/Jun/2005 20:59:18] [TRACE] NeedToReplaceOGSHCAPDLL()

[08/Jun/2005 20:59:18] [INFO] Testing CAP file existence:

C:\WINDOWS\system32\ogshcap.dll

[08/Jun/2005 20:59:18] [INFO] C:\WINDOWS\system32\ogshcap.dll CAP
file exists

[08/Jun/2005 20:59:18] [TRACE] GenerateKeyToFile()

[08/Jun/2005 20:59:18] [TRACE] Successfully called CreateFile
(C:\Program

Files\Common Files\Opsware\cogbot\hmac.key)

[08/Jun/2005 20:59:18] [TRACE] Key file already exists

[08/Jun/2005 20:59:18] [TRACE] C:\Program Files\Common

Files\Opsware\cogbot\hmac.key size:36 bytes

[08/Jun/2005 20:59:18] [TRACE] Successfully called CloseHandle
(C:\Program

Files\Common Files\Opsware\cogbot\hmac.key)

[08/Jun/2005 20:59:18] [TRACE] GenerateKeyToFile() = 1

[08/Jun/2005 20:59:18] [INFO] Calculate MAC for File:

C:\WINDOWS\system32\ogshcap.dll
```

```
[08/Jun/2005 20:59:18] [TRACE] C:\WINDOWS\system32\ogshcap.dll
size:40960 bytes

[08/Jun/2005 20:59:18] [TRACE] C:\Program Files\Common

Files\Opsware\cogbot\hmac.key size:36 bytes

[08/Jun/2005 20:59:18] [TRACE] Successfully called
CreateFileMapping() for

C:\WINDOWS\system32\ogshcap.dll

[08/Jun/2005 20:59:18] [TRACE] Successfully called
CreateFileMapping() for

C:\Program Files\Common Files\Opsware\cogbot\hmac.key

[08/Jun/2005 20:59:18] [TRACE] CalculateMAC()

[08/Jun/2005 20:59:18] [TRACE] PrintHexBytes()

[08/Jun/2005 20:59:18] [TRACE] HMAC for
C:\WINDOWS\system32\ogshcap.dll:0x02

0x95 0x2B 0x03 0x51 0x02 0x9F 0x6D 0x58 0xF6 0xF1 0x5E 0x1C 0xFC
0x2A 0x72 0x5D

0x7E 0x5F 0xDA

[08/Jun/2005 20:59:18] [TRACE] CalculateMACFromFile() = 1

[08/Jun/2005 20:59:18] [INFO] Calculate MAC for File:C:\Program

Files\Opsware\bin\ogshcap.dll

[08/Jun/2005 20:59:18] [TRACE] C:\Program
Files\Opsware\agent\bin\ogshcap.dll size:

40960 bytes

[08/Jun/2005 20:59:18] [TRACE] C:\Program Files\Common

Files\Opsware\cogbot\hmac.key size:36 bytes

[08/Jun/2005 20:59:18] [TRACE] Successfully called
CreateFileMapping() for

C:\Program Files\Opsware\agent\bin\ogshcap.dll

[08/Jun/2005 20:59:18] [TRACE] Successfully called
CreateFileMapping() for

C:\Program Files\Common Files\Opsware\cogbot\hmac.key

[08/Jun/2005 20:59:18] [TRACE] CalculateMAC()

[08/Jun/2005 20:59:18] [TRACE] PrintHexBytes()

[08/Jun/2005 20:59:18] [TRACE] HMAC for C:\Program
```

```
Files\Opsware\agent\bin\ogshcap.dll:0x02 0x95 0x2B 0x03 0x51 0x02
0x9F 0x6D 0x58

0xF6 0xF1 0x5E 0x1C 0xFC 0x2A 0x72 0x5D 0x7E 0x5F 0xDA

[08/Jun/2005 20:59:18] [TRACE] CalculateMACFromFile() = 1

[08/Jun/2005 20:59:18] [INFO] C:\WINDOWS\system32\ogshcap.dll CAP
file does not

need to be replaced

[08/Jun/2005 20:59:18] [TRACE] NeedToReplaceOGSHCAPDLL() = 0

[08/Jun/2005 20:59:18] [TRACE] UpdateCAPRegistrySetting()

[08/Jun/2005 20:59:18] [INFO] Update SubAuthentication Package
Registry key

[08/Jun/2005 20:59:18] [TRACE] Successfully opened registry key

SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0.

[08/Jun/2005 20:59:18] [TRACE] Successfully found registry
value:'Auth255' at

this key, retrieved value 'ogshcap' (8) bytes.

[08/Jun/2005 20:59:18] [TRACE] Existing registry value matches
expected value:

'ogshcap'

[08/Jun/2005 20:59:18] [TRACE] UpdateCAPRegistrySetting() = 1

[08/Jun/2005 20:59:18] [INFO] UpdateCapRegistrySetting() was
successful

[08/Jun/2005 20:59:18] [TRACE] Win32InstallN() = 1

[08/Jun/2005 20:59:18] [INFO] Installation completed
successfully.

[08/Jun/2005 20:59:18] [INFO] An Agent install time reboot is NOT
needed.
```

SA 代理卸载更改

在 SA 代理卸载期间，Windows 卸载程序尝试删除下列文件：

```
%SystemRoot%\system32\ogshcap.dll
```

如果删除失败（由于该文件已打开且正被 Windows 使用），则卸载程序调用 `MoveFileEx()`，指示 Windows 在下次重新启动时删除该文件。如果尝试删除文件失败，卸载程序将提示用户是否应当立即执行重新启动。

卸载程序还删除代理安装时创建的特殊子身份验证注册表项值。有关详细信息，请参见SA 代理卸载更改。

附录 A

权限参考

此附录列出了使用 SA 执行任务所需的权限。有关权限的详细信息，请参见用户和用户组设置及安全性。

服务器对象权限

表 35 指定了服务器对象（例如已注册软件、Internet Information Server、本地安全设置、运行时状态、用户和组以及 .Net Framework 配置）所需的权限。

表 35：服务器对象权限

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
浏览服务器对象	管理服务器模块：读取和写入 允许执行服务器模块：是	N/A	N/A
添加到库（从服务器浏览器）	管理服务器模块：读取和写入 允许执行服务器模块：是 管理程序包：读取和写入		写入
添加到软件策略	管理服务器模块：读取和写入 允许执行服务器模块：是 管理程序包：读取和写入 管理软件策略：读取和写入	N/A	写入

服务器属性和重新启动权限

表 36 指定了用户修改服务器属性、重启服务器和停用 SA 代理所需的权限。对于安全管理员，此表回答了这样一个问题：要执行特定操作，用户需要具有什么权限？

表 36.用户操作所需的服务器属性和重新启动权限

用户操作	操作权限	服务器权限（客户、设施、设备组）
停用 SA 代理	停用：是	读取和写入
修改属性服务器名称或描述	N/A	读取和写入
重新启动服务器	重新启动服务器：是	读取和写入

设备组权限

要使用 SA 客户端中的设备组，您必须具有**表 37** 中所述的权限。有关需要“建立公用设备组模型”权限的任务的列表，请参见**表 45**。

表 37.设备组操作权限

用户操作	操作权限
创建公用静态设备组	管理公用设备组：是
创建公用动态设备组	管理公用设备组：是
向公用静态设备组添加服务器	管理公用设备组：是
向公用动态设备组添加服务器	管理公用设备组：是
从公用静态设备组删除服务器	管理公用设备组：是
从公用动态设备组删除服务器	管理公用设备组：是
移动公用设备组	管理公用设备组：是
复制公用设备组	管理公用设备组：是
删除公用设备组	管理公用设备组：是
向正用作访问控制组的设备组中添加设备	管理公用设备组和超级管理员

服务器代理部署权限

要在使用 SA 客户端的服务器上安装服务器代理，您必须拥有**表 38** 中所述的权限。

表 38.代理操作权限

用户操作	操作权限
在服务器上安装 SA 代理	允许安装代理：是
扫描网络中的无代理服务器	允许扫描网络：是
查看运行代理和设备组的服务器	托管的服务器和组：是
修改设施	设施：是

除了**表 38** 所列的操作权限，还需要下列服务器资源：

- 您将在其中扫描服务器和管理服务器的设施的读取访问权限。
- 客户 Opsware 和您将向其分配服务器的客户的读取访问权限。

虚拟化服务管理权限

要管理虚拟化服务 (VS)、虚拟机 (VM) 和虚拟机模板，您必须具有**表 39** 中所列的操作权限。

如果用户没有特定操作权限（权限设置为“否”），则相应的菜单项将不会出现在 SA 客户端“操作”菜单中。

表 39.虚拟化操作权限

操作权限	描述
查看虚拟化库存	还需要将“托管的服务器和组”权限设置为“是”。允许您查看虚拟化库存（通过支持的技术），并执行“重新加载数据”操作以查看最新虚拟化信息。如果此权限设置为“否”，则 SA 客户端中的“虚拟化”选项卡和“Oracle Solaris 区域”视图不显示。
管理虚拟机生命周期：克隆虚拟机	克隆虚拟机并执行兼容性检查。自定义来宾也需要“自定义来宾 OS”。
管理虚拟机生命周期：创建虚拟机	创建虚拟机并执行兼容性检查。当从“创建虚拟机”作业运行 OS 构建计划时，还需要**表 42** 中列出的“运行 OS 构建计划”权限。
管理虚拟机生命周期：自定义来宾 OS	允许在“克隆虚拟机”或“从虚拟机模板部署虚拟机”期间自定义来宾 OS。
管理虚拟机生命周期：删除虚拟机	删除虚拟机。
管理虚拟机生命周期：从虚	从虚拟机模板部署虚拟机并执行兼容性检查。自定义来

操作权限	描述
拟机模板部署虚拟机	宾也需要“自定义来宾 OS”。
管理虚拟机生命周期：迁移虚拟机	迁移虚拟机（仅主机、仅存储或主机和存储）并执行兼容性检查。
管理虚拟机生命周期：修改虚拟机	修改虚拟机配置。
管理虚拟机电源状态	针对虚拟机执行电源控制操作的能力（例如启动电源、关闭电源、暂停、挂起、重置、重新启动来宾和关闭来宾）。
管理虚拟机模板：将虚拟机转换成虚拟机模板	将虚拟机转换成虚拟机模板。
管理虚拟机模板：删除虚拟机模板	删除虚拟机模板。
管理虚拟化服务	注册、修改和删除虚拟化服务。
将主机添加到虚拟化服务	将虚拟机监控程序添加到虚拟化服务以便得到托管。

虚拟化容器权限和服务器资源权限

除了操作权限，执行所有虚拟化操作还需要虚拟化容器权限。虚拟化容器权限为您提供虚拟化容器（如数据中心、虚拟机监控程序、主机组、群集、资源池、文件夹、项目以及它们的子容器）的访问权。

访问控制列表 (ACL) 继承规则将定义哪些用户组会自动被授权访问任何新添加或新发现的虚拟化容器，该规则基于用户组具有的该父容器的 ACL 内容。

权限选项包括 L（“列表”）、“读取”、“写入”、X（“执行”）和 PM（“编辑权限”）。如果想要将组设置为使用 X 或 PM 继承 ACL，则使用“X,PM”。此规则的路径位于下方：Administration/System Configuration/Server Automation/Web Services Data Access Engine/Twist.v12n.inventory.inheritance.acl。

默认的 PM 选项为最严谨的选项，适合用于多租户控制。PM 需要具有“编辑”权限的用户（通常为虚拟化管理员）手动向其他组分配访问权。仅已具有新添加或新发现容器的父容器的 PM 的用户组可获得访问权。

“列表”选项是最宽容的。如果用户组具有父容器的“列表”权限，则自动将该用户组添加到新容器中时该组具有相同权限。例如，对数据中心 1，组 A 具有“列表”和“读取”权限，组 B 具有“列表”、“读取”、“写入”和“执行”权限。在数据中心 1 中添加一个新群集。则组 A 现在具有新群集的“列表”和“读取”权限，组 B 具有新群集的“列表”、“读取”、“写入”和“执行”权限。

除了操作权限和虚拟化容器权限外，服务器在虚拟化服务中运行还需要服务器资源权限。服务器资源权限是通过设施、客户和设备组授予的。

有关虚拟化权限和服务器资源权限的详细信息，请参见《SA 用户指南：虚拟化管理》。

表 39 仅列出了操作权限，**表 40** 列出了用户可执行的任务以及执行每个用户操作所需的整套操作权限、虚拟化容器权限、服务器资源权限和某些情况下的文件夹权限。

虚拟化任务和所需的权限

表 40 列出在虚拟化库存中执行每个任务所需的权限。此表中的任务用在 VMware vCenter 和 Microsoft SCVMM 中。有关这些任务的详细信息，请参见《SA 用户指南：虚拟化管理》。

表 40.vCenter 和 SCVMM 的虚拟化任务和所需权限

用户操作	所需的操作权限	所需的虚拟化容器权限	所需的服务器资源权限（设施、客户、设备组）
查看 SA 客户端中的“虚拟化”选项卡	查看虚拟化库存：是 托管的服务器和组：是	VS：列出 和 在 VS 下，每个容器所需的单独权限 数据中心：读取（用于对基础数据存储的访问） 在虚拟机和模板的父容器上：读取	VS 服务器：读取
添加 VS	管理虚拟化服务：是 查看虚拟化库存：是 托管的服务器和组：是	不需要。	VS 服务器：读取
编辑 VS，删除 VS	管理虚拟化服务：是 查看虚拟化库存：是 托管的服务器和组：是	VS：写入	VS 服务器：读取
在 VS 下为 VS 或容器重新加载数据。	查看虚拟化库存：是 托管的服务器	VS 或 VS 下的容器：读取	不需要

用户操作	所需的操作权限 和组：是	所需的虚拟化容器权限	所需的服务器资源权限（设施、客户、设备组）
将主机添加到虚拟化服务	将主机添加到虚拟化服务：是 查看虚拟化库存：是 托管的服务器和组：是	添加虚拟机监控程序到其中的容器：写入 或 如果未指定容器则 VS 容器：写入	添加的服务器（虚拟机监控程序）：读取
虚拟机电源控制 - 启动、停止、重新启动来宾、关闭来宾、挂起和暂停虚拟机	查看虚拟化库存：是 管理虚拟机电源状态：是 托管的服务器和组：是	虚拟机驻留的容器：读取	
创建虚拟机	查看虚拟化库存：是 管理虚拟机生命周期：创建虚拟机：是 托管的服务器和组：是 允许执行 OS 构建计划：是（如果指定 OSBP）。 管理程序包：读取，对于非 PXE，使用 OSBP 创建虚拟机。	虚拟机将驻留的目标容器（虚拟机监控程序、群集或资源池）：写入 虚拟机将驻留的 vCenter VS 库中的文件夹：写入	新创建虚拟机的服务器写入 注意 - 包含所选 OS 构建计划的 SA 库文件夹中还需要执行权限。 对于非 PXE，使用 OSBP 创建虚拟机：在 `Opsware/Tools/OS Provisioning/WinPE` 文件夹 (Windows) 上读取 在 `Opsware/Tools/OS Provisioning` 文件夹 (Linux) 上读取
修改虚拟机	查看虚拟化库存：是 管理虚拟机生命周期：修改虚拟机：是 托管的服务器	虚拟机驻留的容器：写入 和 虚拟机所在的虚拟机监控程序（仅限	虚拟机服务器：写入

用户操作	所需的操作权限 和组：是	所需的虚拟化容器权限 vCenter）：列出	所需的服务器资源权限（设施、客户、设备组）
迁移虚拟机	查看虚拟化库存：是 管理虚拟机生命周期：迁移虚拟机：是 托管的服务器和组：是	虚拟机驻留的容器：写入 其他： 用于迁移存储 - 虚拟机监控程序：列出 用于迁移主机或主机和存储 - 虚拟机将驻留的目标容器（虚拟机监控程序、群集或资源池）：写入	虚拟机服务器：读取
克隆虚拟机（仅限 vCenter）	查看虚拟化库存：是 管理虚拟机生命周期：克隆虚拟机：是 托管的服务器和组：是	虚拟机驻留的容器：读取 新虚拟机将驻留的目标容器（虚拟机监控程序、群集或资源池）：写入 新虚拟机将驻留的 vCenter VS 库存中的文件夹：写入	源虚拟机服务器：读取 新虚拟机服务器：写入
自定义来宾 OS - 当作为“克隆虚拟机”操作或“从虚拟机模板部署虚拟机”操作的一部分执行时	当作为克隆虚拟机操作的一部分执行时与“克隆虚拟机”相同。 当作为部署虚拟机操作的一部分执行时与“从虚拟机模板部署虚拟	当作为克隆虚拟机操作的一部分执行时与“克隆虚拟机”相同。 当作为部署虚拟机操作的一部分执行时与“从虚拟机模板部署虚拟	当作为克隆虚拟机操作的一部分执行时与“克隆虚拟机”相同。 当作为部署虚拟机操作的一部分执行时与“从虚拟机模板部署虚拟机”相同。 对于 Linux 自定义设置，请在 `Opsware/Tools/Build Plans/Virtualization/Guest Customization/Linux` 文件夹上执行。

用户操作	所需的操作权限	所需的虚拟化容器权限	所需的服务器资源权限（设施、客户、设备组）
	机”相同。 管理虚拟机生命周期：自定义来宾 OS：是 允许执行 OS 构建计划：是	机”相同。	对于 Windows 自定义设置，请在 `Opsware/Tools/Build Plans/Virtualization/Guest Customization/Windows` 文件夹上执行。
删除虚拟机	查看虚拟化库存：是 管理虚拟机生命周期：删除虚拟机：是 托管的服务器和组：是	虚拟机驻留的容器：写入	虚拟机服务器：写入
从虚拟机模板部署虚拟机	查看虚拟化库存：是 管理虚拟机生命周期：从虚拟机模板部署虚拟机：是 托管的服务器和组：是	虚拟机模板驻留的容器：执行 新虚拟机将驻留的目标容器（虚拟机监控程序、群集或资源池）：写入 新虚拟机将驻留的 vCenter VS 库存中的文件夹：写入	虚拟机模板服务器：读取 新虚拟机服务器：写入
将虚拟机转换成虚拟机模板	查看虚拟化库存：是 管理虚拟机模板：将虚拟机转换成虚拟机模板：是 托管的服务器和组：是	虚拟机驻留的容器：写入 SCVMM 库中的虚拟机模板文件夹：写入	虚拟机服务器：读取
删除虚拟机模板	查看虚拟化库存：是	虚拟机模板驻留的容器：写入	虚拟机服务器：写入

用户操作	所需的操作权限 管理虚拟机模板：删除 虚拟机模板：是 托管的服务器和组：是	所需的虚拟化容器权限	所需的服务器资源权限（设施、客户、设备组）
合并服务器	查看虚拟化库存：是（用于将虚拟化服务器和其他服务器合并） 合并服务器：是 托管的服务器和组：是	虚拟机或模板驻留的容器：写入 或 虚拟机监控程序：写入	要合并的两个服务器的服务器写入

Solaris 虚拟化权限

表 41 列出了管理 Oracle Solaris 区域所需的权限。有关详细信息，请参见《SA 用户指南：虚拟化管理》。

表 41.Solaris 虚拟化权限

用户操作	所需的操作权限	必需 服务器资源权限（设施、客户、设备组）
创建区域	管理虚拟机生命周期：创建虚拟机 查看虚拟化库存：是 托管的服务器和组：是	虚拟机监控程序服务器：读取 新虚拟机分配到的客户：写入
重新加载数据	查看虚拟化库存：是 托管的服务器和组：是	虚拟机监控程序服务器：读取 虚拟机服务器：读取
修改	管理虚拟机生命周期：修改虚拟机 查看虚拟化库存：是 托管的服务器和组：是	虚拟机监控程序服务器：读取 虚拟机服务器：写入
删除	管理虚拟机生命周期：删除虚拟机 查看虚拟化库存：是 托管的服务器和组：是	虚拟机监控程序服务器：读取 虚拟机服务器：读取
启动、停止	管理虚拟机电源状态：是 查看虚拟化库存：是 托管的服务器和组：是	虚拟机监控程序服务器：读取 虚拟机服务器：写入

OS 配置权限

本节描述 OS 配置所需的权限。对于安全管理员，**表 42** 回答了这样一个问题：要执行特定操作，用户需要具有什么权限？

在**表 42** 中，“服务器权限”列针对的是 OS 序列或安装配置文件所引用的服务器。服务器权限由 SA Web 客户端中的客户、设施和设备组权限指定。要创建 OS 序列并将其保存到文件夹中，您将需要该文件夹的写入权限。

表 42.用户操作所需的 OS 配置权限

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
OS 构建计划			
创建 OS 构建计划	管理 OS 构建计划：读取和写入	无	写入
查看 OS 构建计划	管理 OS 构建计划：读取	无	读取
编辑 OS 构建计划	管理 OS 构建计划：读取和写入	无	写入
删除 OS 构建计划	管理 OS 构建计划：读取和写入	无	写入
将设备组添加到 OS 构建计划	下列任何权限组合都是有效的： 1) 管理服务器和组 + 管理 OS 构建计划：读取和写入，或者 2) 管理公用	无	包含 OS 构建计划的文件夹：写入

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
	设备组（在“客户端功能”选项卡中的“服务器”部分）+ 管理 OS 构建计划：读取和写入，或者 3) 管理公用设备组（SA Web 客户端）（从“其他”选项卡中的“服务器和设备组权限”部分）+ 管理 OS 构建计划：读取和写入		
将 OGFS 脚本添加到 OS 构建计划	管理 OGFS 脚本：读取 + 管理 OS 构建计划：读取和写入	无	包含 OGFS 脚本的文件夹：读取 + 包含 OS 构建计划的文件夹：写入
将服务器脚本添加到 OS 构建计划	管理服务器脚本：读取 + 管理 OS 构建计划：读取和写入	无	包含服务器脚本的文件夹：读取 + 包含 OS 构建计划的文件夹：写入
将 ZIP 包添加到 OS 构建计划	管理程序包：读取 + 管理 OS 构建计划：读取和写入	无	包含程序包的文件夹：读取 + 包含 OS 构建计划的文件夹：写入

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
将软件策略附加到 OS 构建计划	管理软件策略：读取 + 管理 OS 构建计划：读取和写入	无	包含软件策略的文件夹：读取 + 包含 OS 构建计划的文件夹：写入
将 Windows 修补程序策略附加到 OS 构建计划	管理 Windows 修补程序：策略 + 管理 OS 构建计划：读取和写入	无	包含 OS 构建计划的文件夹：写入
运行 OS 构建计划（从服务器或从 OS 构建计划节点）	托管服务器和组 + 管理 OS 构建计划：允许执行 OS 构建计划：是	读取和写入	包含 OS 构建计划的文件夹：执行
运行 OS 构建计划（针对 VMware ESXi 4.1）	管理服务器和组 + 管理 OS 构建计划：读取 + 允许执行 OS 构建计划：是 + 允许管理服务器 + 查看虚拟服务器 + 管理虚拟服务器	读取和写入	文件夹 (`/Opsware Tools/OS Provisioning`) 包含运行 OS 构建计划 Web 扩展：执行 + 包含 OS 构建计划的文件夹：`/Opsware/Tools/Virtualization Programs/Hypervisor Scanner` 文件夹的执行 + 列出和执行文件夹权限
OS 序列			
创建 OS 序列	管理 OS 序列：读取和写入 + 操作系统 + 向导：准备	**注意**：要使用分配给客户的 OS 安装	写入

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
	OS	配置文件创建 OS 序列，用户必须至少拥有该客户的读取权限 **注意**：要使用客户独立 OS 安装配置文件创建 OS 序列，则不需要客户权限。	
查看 OS 序列	管理 OS 序列： 读取	无	读取
编辑 OS 序列	管理 OS 序列： 读取和写入	无	写入
删除 OS 序列	管理 OS 序列： 读取和写入	无	写入
运行 OS 序列 （从服务器或从 OS 序列）	管理 OS 序列： 读取 和 允许执行 OS 序列： 是	读取和写入	读取

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
查看未配置的服务器	SA Web 客户端权限：服务器池	读取	N/A
附加软件策略	管理软件策略：读取 + 管理 OS 序列：读取和写入	NA	包含软件策略的文件夹：读取 + 包含 OS 序列的文件夹：写入
附加 Windows 修补程序策略	管理 Windows 修补程序：策略 + 管理 OS 序列：读取和写入	NA	包含 OS 序列的文件夹：写入
附加 Solaris 修补程序策略	管理软件策略：读取 + 管理 OS 序列：读取和写入	NA	包含 Solaris 修补程序策略的文件夹：读取 + 包含 OS 序列的文件夹：写入
OS 安装配置文件			
创建、编辑、删除 OS 安装配置文件	操作系统 + 向导：准备 OS	**注意**：要使用分配给客户的 OS 安装配置文件创建 OS 序列，客户必须拥有读取和写入权限。 **注意**：	N/A

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
		要使用客户独立 OS 安装配置文件创建 OS 序列，则不需要客户权限。	
未配置的服务器列表			
查看未配置的服务器列表中的服务器	服务器池	N/A	N/A
管理启动客户端			
执行托管启动客户端 Web 应用程序	允许配置网络启动 + 托管的服务器和组 + 管理客户 + 服务器池	设施和客户的读取/写入 + 未分配的客户的读取/写入	列出并执行 `/Opsware /Tools/OS Provisioning/Manage Boot Clients` 文件夹

表 43 列出了用户可以对各 OS 配置权限执行的操作。**表 43** 包含的数据与**表 42** 相同，但是按操作权限排序。

对于安全管理员，**表 43** 回答了这样一个问题：如果向用户授予了特定操作权限，那么用户可以执行何种操作？

表 43.SA 客户端中 OS 配置权限允许的用户操作

操作权限	用户操作	服务器权限（客户、设施、设备组）	文件夹
管理 OS 序列：读取	查看 OS 序列	读取	读取
管理 OS 序列：读取和写入 +	创建 OS 序列	读取	写入

操作权限	用户操作	服务器权限（客户、设施、设备组）	文件夹
操作系统 + 向导：准备 OS			
允许执行 OS 序列：是	运行 OS 序列	写入	读取
管理 OS 序列：读取 允许执行 OS 序列：是	运行 OS 序列	写入	读取
管理 OS 序列：读取 允许执行 OS 序列：否	查看 OS 序列	读取	读取
管理 OS 序列：写入 允许执行 OS 序列：是	运行 OS 序列 编辑 OS 序列	写入	写入
管理 OS 序列：写入 允许执行 OS 序列：否	编辑 OS 序列	读取	写入
操作系统 + 向导：准备 OS	创建、编辑、删除 OS 安装配置文件	读取和写入， N/A， N/A	N/A
服务器池	查看未配置的服务器列表中的服务器	读取	N/A

管理启动客户端权限

以下部分描述使用 OS 配置的管理启动客户端 (MBC) 实用程序所需的权限。

表 44.管理启动客户端实用程序权限

操作权限	用户操作	服务器权限（客户、设施、设备组）	文件夹
允许执行 OS 构建计划	运行 OS 构建计划	写入	读取
允许执行 OS 序列	运行 OS 序列	写入	读取
管理服务器和组	管理服务器和组	写入	读取
管理客户	创建、编辑客户	写入	读取
服务器池	访问服务器池	写入	读取
未分配的客户的读取和写入权限	访问分配给未分配客户的服务器	写入	读取

操作权限	用户操作	服务器权限（客户、设施、设备组）	文件夹
允许配置网络启动	配置网络启动	写入	读取

软件管理权限

表 45 指定了用户在 SA 客户端中执行特定操作所需的软件管理权限。对于安全管理员，此表回答了这样一个问题：要执行特定操作，用户需要具有什么权限？

如果将客户分配到文件夹，则客户约束可能限制可与该文件夹中包含的软件策略关联的对象。有关受这些约束影响的任务的列表，请参见文件夹、客户约束和软件策略。

要安装软件，您必须是具有安装软件权限的用户组的成员。此用户组还必须具有您要安装的软件的文件夹权限。

表 45.用户操作所需的软件管理权限

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
软件策略			
创建软件策略	管理软件策略：读取和写入	N/A	写入
删除软件策略	管理软件策略：读取和写入	N/A	写入
打开软件策略（查看）	管理软件策略：读取	N/A	读取
编辑软件策略属性	管理软件策略：读取和写入	N/A	写入
添加程序包	管理软件策略：读取和写入 管理程序包：读取	N/A	包含软件策略的文件夹：写入
添加 RPM 包	管理软件策略：读取和写入 管理程序包：读取	N/A	包含软件策略的文件夹：写入
添加修补程序	管理软件策略：读取和写入	N/A	包含软件策略的文件夹：写入

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
	管理修补程序：读取		
添加应用程序配置	管理软件策略：读取和写入 管理应用程序配置：读取	N/A	包含软件策略的文件夹：写入
添加脚本	管理软件策略：读取和写入 管理服务器脚本：读取	N/A	包含软件策略的文件夹：写入
添加服务器对象	管理软件策略：读取和写入 管理程序包：读取	N/A	包含软件策略的文件夹：写入
添加软件策略	管理软件策略：读取和写入	N/A	包含软件策略的文件夹：写入
删除程序包	管理软件策略：读取和写入	N/A	写入
删除 RPM 包	管理软件策略：读取和写入	N/A	写入
删除修补程序	管理软件策略：读取和写入	N/A	写入
删除应用程序配置	管理软件策略：读取和写入	N/A	写入
删除软件策略	管理软件策略：读取和写入	N/A	写入
删除脚本	管理软件策略：读取和写入	N/A	写入
删除服务器对象	管理软件策略：读取和写入	N/A	写入
安装/卸载软件	管理软件策略：读取 允许附加/分离软件策略：是 允许安装/卸载软件：是 建立公用设备组模型：是	读取和写入	读取

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
	（如果您修正公用设备组，则需要此权限）		
附加软件策略	管理软件策略：读取 允许附加/分离软件策略：是 建立公用设备组模型：是（如果您将软件策略附加到公用设备组，则需要此权限）	读取和写入	读取
分离软件策略	管理软件策略：读取 允许附加/分离软件策略：是 建立公用设备组模型：是（如果您将软件策略附加到公用设备组，则需要此权限）	读取和写入	读取
修正	管理软件策略：读取 允许修正服务器：是 建立公用设备组模型：是（如果您修正公用设备组，则需要此权限）	读取和写入	读取
运行 ISM 控制	管理软件策略：读取 允许运行 ISM 控制：是 建立公用设备组模型：是（如果您在公用设备组上运行 ISM 控制，则需要此权限）	读取和写入	读取
复制 Zip 包	管理软件策略：读取和写入	N/A	写入
编辑 ZIP 安装目录	管理软件策略：读取和写入	N/A	写入
扫描软件符合性	N/A	读取	N/A

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
重命名软件策略	管理软件策略：读取和写入	N/A	写入
剪切软件策略	管理软件策略：读取和写入	N/A	写入
复制软件策略	管理软件策略：读取	N/A	读取
粘贴软件策略	管理软件策略：读取和写入	N/A	源文件夹：读取（对于复制和粘贴） 源文件夹：写入（对于剪切和粘贴） 目标文件夹：写入
移动软件策略	管理软件策略：读取和写入	N/A	源文件夹：写入 目标文件夹：写入
文件夹			
创建文件夹	N/A	N/A	写入
删除文件夹	N/A	N/A	写入
打开文件夹	N/A	N/A	读取
查看文件夹属性	N/A	N/A	读取
编辑文件夹属性	N/A	N/A	写入
管理文件夹权限	N/A	N/A	编辑文件夹权限
剪切文件夹	N/A	N/A	写入
复制文件夹	N/A	N/A	读取
粘贴文件夹	N/A	N/A	源文件夹：读取（对于复制和粘贴） 源文件夹：写入（对于剪切和粘

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
			贴） 目标文件夹：写入
移动文件夹	N/A	N/A	源文件夹：写入 目标文件夹：写入
重命名文件夹	N/A	N/A	写入
程序包			
导入程序包	管理程序包：读取和写入	N/A	写入
导出程序包	管理程序包：读取	N/A	读取
打开程序包（查看）	管理程序包：读取	N/A	读取
编辑程序包属性	管理程序包：读取和写入	N/A	读取
删除程序包	管理程序包：读取和写入	N/A	写入
重命名程序包	管理程序包：读取和写入	N/A	写入
剪切程序包	管理程序包：读取和写入	N/A	写入
粘贴程序包	管理程序包：读取和写入	N/A	源文件夹：读取（对于复制和粘贴） 源文件夹：写入（对于剪切和粘贴） 目标文件夹：写入
移动程序包	管理程序包：读取和写入	N/A	源文件夹：写入 目标文件夹：写入

表 46 列出了用户可以对各软件管理权限执行的操作。**表 46** 包含的数据与**表 45** 相同，但是按操作权限排序。对于安全管理员，**表 46** 回答了这样一个问题：如果向用户授予了特定操作权限，那么用户可以执行何种操作？

表 46.软件管理权限允许的用户操作

操作权限	用户操作	服务器权限（客户、设施、设备组）	文件夹权限
管理软件策略：读取和写入	创建软件策略	N/A	写入
	删除软件策略	N/A	写入
	编辑软件策略	N/A	写入
	重命名软件策略	N/A	写入
	剪切软件策略	N/A	写入
	粘贴软件策略	N/A	写入
	移动软件策略	N/A	写入
	删除程序包	N/A	写入
	删除修补程序	N/A	写入
	删除应用程序配置	N/A	写入
	删除脚本	N/A	写入
	删除服务器对象	N/A	写入
	删除软件策略	N/A	写入
	复制 Zip 包	N/A	写入
管理软件策略：读取	打开软件策略（查看）	N/A	读取
	复制软件策略属性	N/A	读取
管理软件策略：读取和写入 和 管理程序包：读取	添加程序包 添加 RPM 包	N/A	包含软件策略的文件夹：写入 包含程序包的文件夹：读取
管理软件策略：读取和写入 和 管理修补程序：读取	添加修补程序	N/A	包含软件策略的文件夹：写入 包含修补程序的文件夹：读取
管理软件策略：读取和写入	添加应用程序配置	N/A	包含软件策略的文件夹：写入

操作权限	用户操作	服务器权限（客户、设施、设备组）	文件夹权限
和 管理应用程序配置：读取			包含应用程序配置的文件夹：读取
管理软件策略：读取和写入	添加软件策略	N/A	包含软件策略的文件夹：写入 包含要添加到另一个软件策略的软件策略的文件夹：读取
管理软件策略：读取和写入 和 管理服务器脚本：读取	添加脚本	N/A	包含软件策略的文件夹：写入 包含脚本的文件夹：读取
管理软件策略：读取和写入 和 管理程序包：读取	添加服务器对象	N/A	包含软件策略的文件夹：写入 包含服务器对象的文件夹：读取
管理软件策略：读取和写入	删除程序包	N/A	写入
	删除 RPM 包	N/A	写入
	删除修补程序	N/A	写入
	删除应用程序配置	N/A	写入
	删除脚本	N/A	写入
	删除服务器对象	N/A	写入
	删除软件策略	N/A	写入
管理软件策略：读取 和 允许附加/分离软件策略：是 和	附加软件策略	读取和写入	读取

操作权限	用户操作	服务器权限（客户、设施、设备组）	文件夹权限
建立公用设备组模型：是（如果您将软件策略附加到公用设备组，则需要此权限）			
	分离软件策略	读取和写入	读取
管理软件策略：读取 和 允许修正服务器：是 和 建立公用设备组模型：是（如果您修正公用设备组，则需要此权限）	修正	读取和写入	读取
管理软件策略：读取 和 允许附加/分离软件策略：是 和 允许安装/卸载软件：是 和 建立公用设备组模型：是（如果您修正公用设备组，则需要此权限）	安装/卸载软件	读取和写入	读取
管理软件策略：读取 和 允许运行 ISM 控制：是 和 建立公用设备组模型：是（如果您在公用设备组上运行 ISM	运行 ISM 控制	读取和写入	读取

操作权限	用户操作	服务器权限（客户、设施、设备组）	文件夹权限
控制，则需要此权限）			
管理程序包：读取和写入	导入程序包	N/A	写入
	删除程序包	N/A	写入
	重命名程序包	N/A	写入
	剪切程序包	N/A	写入
	粘贴程序包	N/A	写入
	移动程序包	N/A	写入
管理程序包：读取和写入	编辑程序包属性	N/A	读取
管理程序包：读取	导出程序包	N/A	读取
	打开程序包（查看）	N/A	读取

Chef Cookbook 管理权限

本节指定了用户在 SA 客户端中执行特定操作所需的 Chef Cookbook 管理权限。对于安全管理员，此表回答了这样一个问题：要执行特定操作，用户需要具有什么权限？

备注: 除了列出的操作权限以外，每个用户操作还需要“托管的服务器和组”权限。

从不包含依赖关系的 Cookbook 运行 Chef Recipe 的权限

从不包含依赖关系的 Cookbook 运行 Chef Recipe 需要以下权限：

- 这些**操作权限**控制您可以执行的 Chef 任务。

权限	设置	已启用的任务
运行 Chef Recipe	是	可启动或计划特定运行 Chef Recipe 作业。
管理程序包	读取（或更强）	可在运行 Chef Recipe 作业中使用 Cookbook（一种 SA 程序包类型）。

  执行运行 Chef Recipe 作业运行的用户必须属于具有*运行 Chef Recipe* 和*管理程序包*权限的用户组。

- **文件夹权限**控制对 Cookbook 所在的 SA 库文件夹的访问权限。

  执行运行 Chef Recipe 作业运行的用户必须属于具有 Cookbook 所在文件夹的*读取*权限的用户组。

- **资源权限**控制当前用户对 SA 中的托管服务器的访问权限。

  执行运行 Chef Recipe 作业运行的用户必须属于对服务器的设施、客户和至少一个设备组具有*读取和写入* 权限的用户组。

  有关设置资源权限的详细信息，请参见关于资源权限。

- **文件夹客户约束**确定可以成为运行 Chef Recipe 作业目标的服务器。由于每个服务器都分配给一个*客户*，因此 Cookbook 文件夹的客户约束必须包含目标服务器的客户。

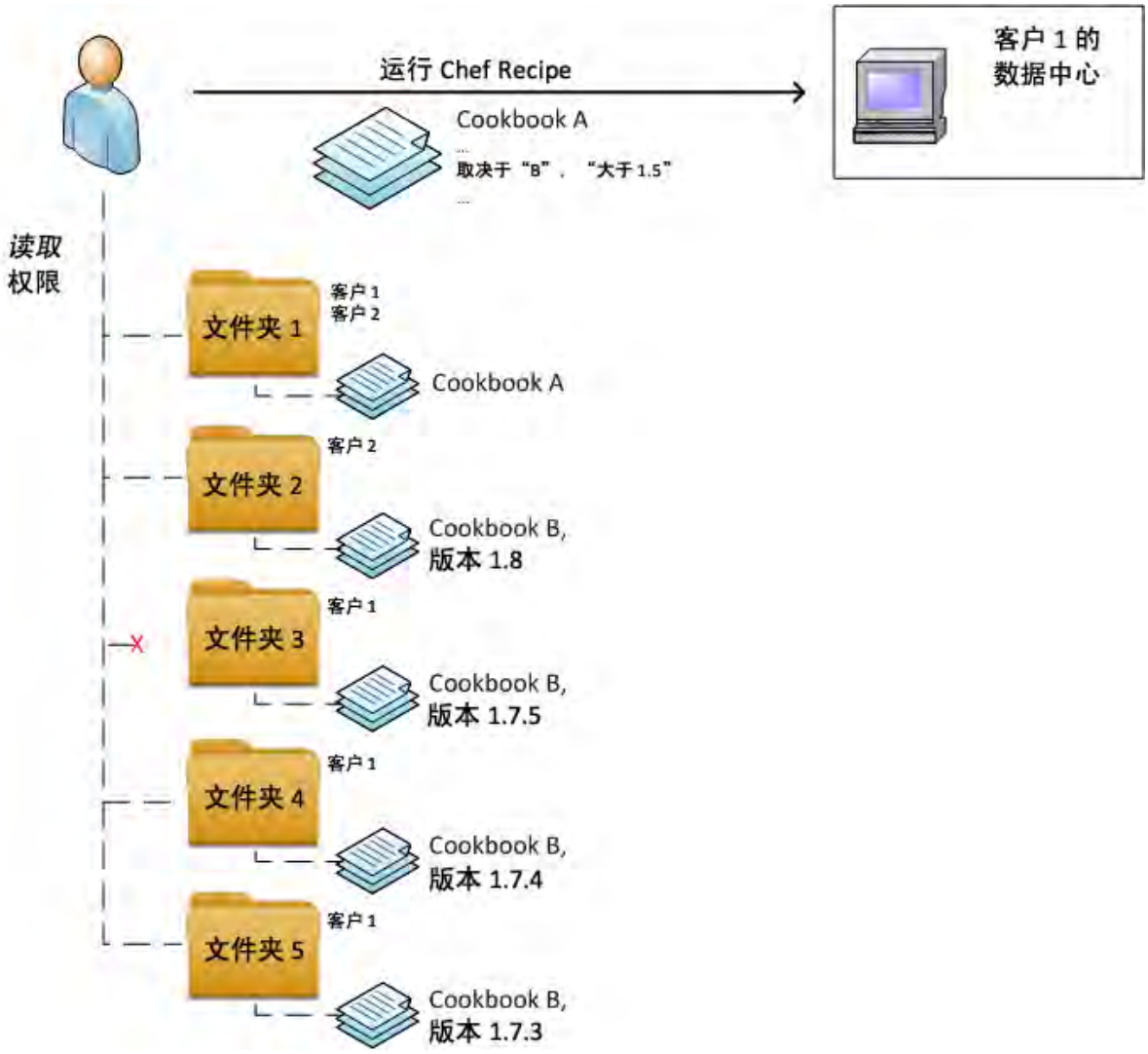
  或者，您可以通过将*独立于客户* 客户分配给 Cookbook 文件夹， 完全忽略文件夹客户权限。

  有关设置文件夹权限的详细信息，请参见关于文件夹权限。

包含依赖关系的 Cookbook 的权限管理

Cookbook 的依赖关系必须满足的权限要求与主 Cookbook 相同：读取文件夹权限和相应文件夹客户约束。如果依赖 Cookbook 存在多个版本，则 SA 将使用整个依赖关系图满足全部所需权限的依赖 Cookbook 的最新版本。

例如：在以下安装中，当用户尝试从 Cookbook A 运行 Recipe 时， SA 将它与 Cookbook B 的依赖关系解析到版本 1.7.4。

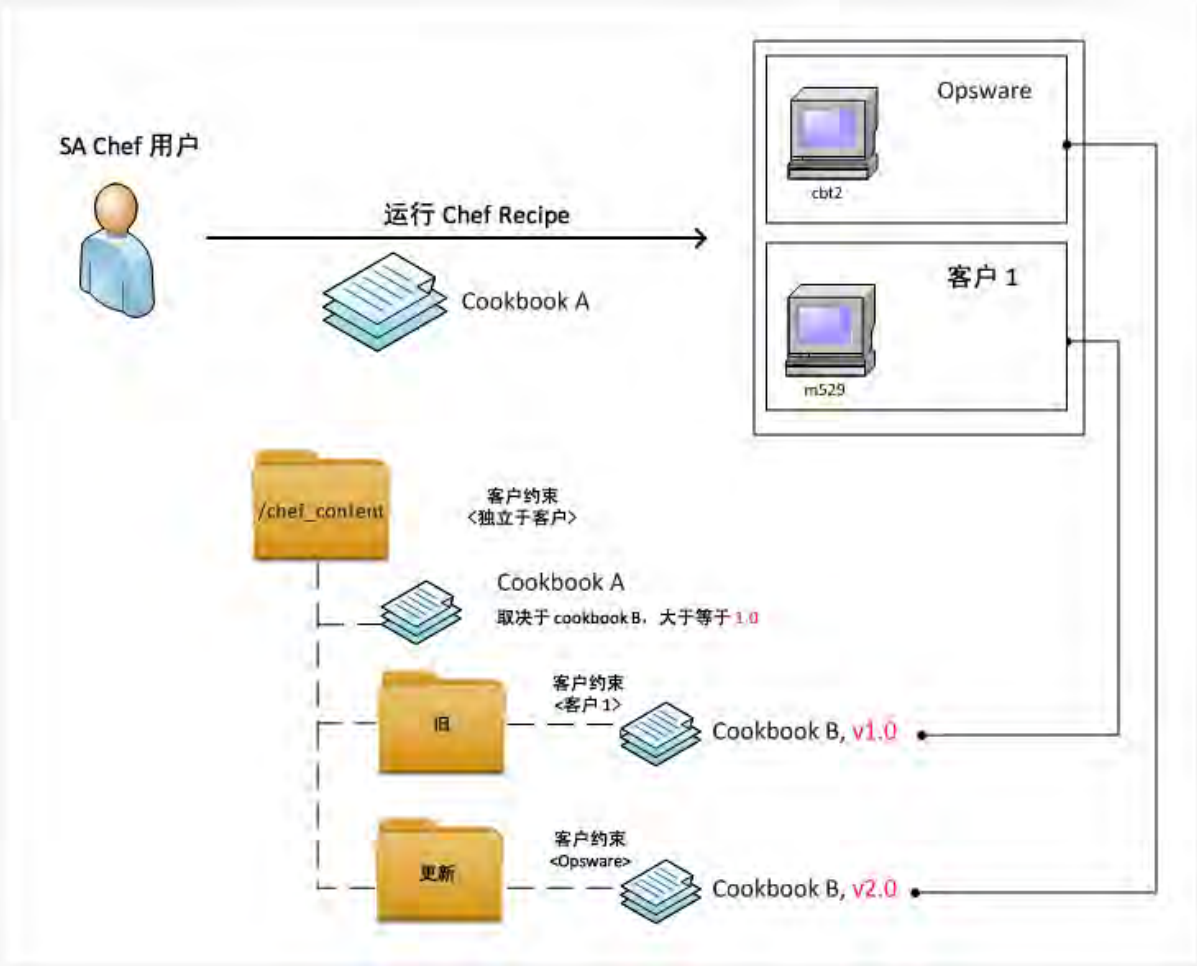


进一步说明，不能使用 Cookbook B 版本 1.8，因为 folder2 未关联到 customer1（目标服务器的客户）。不能使用 Cookbook B 版本 1.7.5，因为用户不具有 folder3 的任何权限。版本 1.7.4 和 1.7.3 均可访问，SA 将选择较高的版本，因此为 1.7.4。

多租户

文件夹客户约束提供的机制支持多租户，允许对不同客户应用不同内容。

在下面的示例中，对两个托管服务器（cbt2 和 m529）的组应用 Cookbook A 将导致对服务器 m529 应用 Cookbook B 版本 1.0 版本而对服务器 cbt2 应用 Cookbook B 版本 2.0。



应用程序配置管理权限

用户操作所需的应用程序配置管理权限 指定了用户在 SA 客户端中使用应用程序配置执行特定操作所需的权限。对于安全管理员，此表回答了这样一个问题：要执行特定操作，用户需要具有什么权限？

备注: 除了 用户操作所需的应用程序配置管理权限 中列出的操作权限以外，每个用户操作还需要“托管的服务器和组”权限。

在 用户操作所需的应用程序配置管理权限 中，“服务器权限”列针对的是应用程序配置或配置模板所引用的服务器。服务器权限由 SA Web 客户端中的客户、设施和设备组权限指定。在 用户操作所需的应用程序配置管理权限 中，“文件夹权限”列针对的是包含应用程序配置和配置模板的 SA 库中的文件夹。

用户需要一些权限才能执行操作。例如，要将应用程序配置附加到服务器，用户必须具有下列权限：

- 管理应用程序配置：读取
- 管理配置模板：读取
- 管理在服务器上安装的配置和备份：读取和写入
- 托管的服务器和组
- 服务器的设施、设备组和客户的读取和写入权限
- 包含应用程序配置或模板的 SA 库中的文件夹的读取权限。

用户操作所需的应用程序配置管理权限

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限（应用程序配置、应用程序配置模板）
应用程序配置			
创建应用程序配置	管理应用程序配置：读取和写入 和管理配置模板：读取	无	读取和写入
查看应用程序配置	管理应用程序配置：读取和写入 和管理配置模板：读取	无	读取
编辑应用程序配置	管理应用程序配置：读取和写入 和管理配置模板：读取	无	读取和写入
删除应用程序配置	管理应用程序配置：读取和写入 和管理配置模板：读取	无	读取和写入
指定模板顺序	管理应用程序配置：读取和写入 和管理配置模板：读取	无	读取和写入
将应用程序配置附加到服务器	管理应用程序配置：读取 和管理配置模板：读取 和管理在服务器上安装的配置和备份：	读取和写入	读取

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限（应用程序配置、应用程序配置模板）
	读取和写入		
将应用程序配置附加到设备组	管理应用程序配置： 读取 和管理配置模板： 读取 和管理在服务器上安装的配置和备份： 读取和写入 和管理公用设备组：是 和建立公用设备组模型：是	读取和写入	读取
设置服务器上的应用程序配置值	管理应用程序配置： 读取 和管理配置模板： 读取 和管理在服务器上安装的配置和备份： 读取和写入	读取和写入	读取
将应用程序配置推送到服务器	管理应用程序配置： 读取 和管理配置模板： 读取 和管理在服务器上安装的配置和备份： 读取和写入	读取和写入	读取
计划应用程序配置推送	管理应用程序配置： 读取 和管理配置模板： 读取 和管理在服务器上安装的配置和备份： 读取和写入	读取和写入	读取
扫描配置符合性	允许配置符合性扫描： 是 和管理应用程序配置： 读取 和管理配置模板：	读取	读取

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限（应用程序配置、应用程序配置模板）
	读取		
计划应用程序配置审核	允许配置符合性扫描： 是 和管理应用程序配置： 读取 和管理配置模板： 读取	读取	读取
回滚（还原）应用程序配置推送	管理应用程序配置： 读取 和管理配置模板： 读取 和管理在服务器上安装的配置和备份： 读取和写入	读取和写入	读取
应用程序配置模板			
创建应用程序配置模板	管理配置模板： 读取和写入	无	读取和写入
查看应用程序配置模板	管理配置模板： 读取和写入	无	读取
编辑应用程序配置模板	管理配置模板： 读取和写入	无	读取和写入
删除应用程序配置模板	管理配置模板： 读取和写入	无	读取和写入
加载（导入）应用程序配置模板	管理应用程序配置： 读取和写入 和管理配置模板： 读取和写入	无	读取和写入
将应用程序配置模板设置为以脚本运行	管理配置模板： 读取和写入	无	读取和写入
比较两个应用程序配置模板	管理配置模板： 读取	无	读取
针对实际配置文件比较应用程序配置模板（预览）	管理应用程序配置： 读取	读取	读取

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限（应用程序配置、应用程序配置模板）
	和管理配置模板： 读取 和管理在服务器上安装的配置和备份： 读取		

应用程序配置管理权限允许的用户操作 列出了用户可以对每个权限的应用程序配置执行的操作。应用程序配置管理权限允许的用户操作包含的数据与 用户操作所需的应用程序配置管理权限相同，但是按权限排序。尽管应用程序配置管理权限允许的用户操作中未指明，但是所有 OS 配置操作都需要“托管的服务器和组”权限。

对于安全管理员，应用程序配置管理权限允许的用户操作回答了这样一个问题：如果向用户授予了特定权限，那么用户可以执行何种操作？

应用程序配置管理权限允许的用户操作

操作权限	用户操作	服务器权限（客户、设施、设备组）	文件夹权限（应用程序配置、应用程序配置模板）
允许配置符合性扫描：是 和管理应用程序配置： 读取 和管理配置模板： 读取	扫描配置符合性	读取	读取
	计划应用程序配置审核	读取	读取
管理应用程序配置： 读取和写入 和管理配置模板： 读取	创建应用程序配置	无	读取和写入
	删除应用程序配置	无	读取和写入
	编辑应用程序配置	无	读取和写入
	指定模板顺序	无	读取和写入
	查看应用程序配置	无	读取
管理应用程序配置： 读取和写入 和管理配置模板： 读取和写入	加载（导入）应用程序配置模板	无	读取和写入

操作权限	用户操作	服务器权限（客户、设施、设备组）	文件夹权限（应用程序配置、应用程序配置模板）
管理应用程序配置： 读取 和管理配置模板： 读取 和管理在服务器上安装的配置和备份： 读取	针对实际配置文件比较应用程序配置模板（预览）	读取	读取
管理应用程序配置： 读取 和管理配置模板： 读取 和管理在服务器上安装的配置和备份： 读取和写入	将应用程序配置附加到服务器	读取和写入	读取
	将应用程序配置推送到服务器	读取和写入	读取
	回滚（还原）应用程序配置推送	读取和写入	读取
	计划应用程序配置推送	读取和写入	读取
	设置服务器上的应用程序配置值	读取和写入	读取
管理应用程序配置： 读取 和管理配置模板： 读取 和管理在服务器上安装的配置和备份： 读取和写入 和管理公用设备组：是 和建立公用设备组模型：是	将应用程序配置附加到设备组	读取和写入	读取
管理配置模板： 读取	比较两个应用程序配置模板	无	读取
管理配置模板： 读取和写入	创建应用程序配置模板	无	读取和写入
	删除应用程序配置模板	无	读取和写入
	编辑应用程序配置模板	无	读取和写入
管理配置模板： 读取和写入（继续）	将应用程序配置模板设置为以脚本运行	无	读取和写入
	查看应用程序配置模板	无	读取

Windows 修补程序管理权限

表 49 指定了用户在 SA 客户端中执行特定操作所需的 Windows 修补程序管理权限。对于安全管理员，此表回答了这样一个问题：要执行特定操作，用户需要具有什么权限？

备注: 除了**表 49** 中列出的权限以外，每个用户操作还需要“托管的服务器和组”权限。

在**表 49** 中，“用户操作”列中的大多数条目对应于 SA 客户端中的菜单项。除了操作权限以外，受修补操作影响的托管服务器需要具有服务器权限。

备注: 如果“允许安装修补程序”权限设置为“是”，则“管理修补程序”和“管理 Windows 修补程序策略”权限自动设置为“读取”。

表 49.用户操作所需的 Windows 修补程序管理权限

用户操作	操作权限	服务器权限（客户、设施、设备组）
修补程序		
安装修补程序（可用）	允许安装修补程序：是 管理修补程序：读取	读取和写入
卸载修补程序（可用）	允许卸载修补程序：是 和管理修补程序：读取	读取和写入
安装修补程序（有限的可用性）	允许安装修补程序：是 管理修补程序：读取和写入	读取和写入
卸载修补程序（有限的可用性）	允许卸载修补程序：是 和管理修补程序：读取和写入	读取和写入
打开修补程序（查看修补程序）	管理修补程序：读取	N/A
更改修补程序属性	管理修补程序：读取和写入	N/A
导入修补程序	管理修补程序：读取和写入 和程序包	N/A
导入修补程序数据库	管理修补程序：读取和写入	N/A
导出修补程序	管理修补程序：读取 和程序包	N/A
导出修补程序	或允许安装修补程序：是	N/A

用户操作	操作权限	服务器权限（客户、设施、设备组）
	和程序包：是	
导出修补程序	或允许卸载修补程序：是 和程序包	N/A
导出修补程序	或管理策略：读取 和程序包	N/A
删除修补程序	管理修补程序：读取和写入	N/A
修补程序策略和例外		
修正策略	允许安装修补程序：是	读取和写入
打开修补程序策略（查看）	管理 Windows 修补程序策略：读取	N/A
向修补程序策略添加修补程序	管理修补程序：读取 和管理 Windows 修补程序策略：读取和写入	N/A
从修补程序策略删除修补程序	管理 Windows 修补程序策略：读取和写入	N/A
设置异常	允许安装修补程序：是	读取和写入
设置异常	或允许卸载修补程序：是	读取和写入
复制异常	允许安装修补程序：是	读取和写入
复制异常	或允许卸载修补程序：是	读取和写入
将修补程序策略附加到服务器（或设备组）	管理 Windows 修补程序策略：读取	读取和写入
从服务器（或设备组）分离修补程序策略	管理 Windows 修补程序策略：读取	读取和写入
创建修补程序策略	管理 Windows 修补程序策略：读取和写入	N/A
删除修补程序策略	管理 Windows 修补程序策略：读取和写入	N/A
更改修补程序策略属性	管理 Windows 修补程序策略：读取和写入	N/A

用户操作	操作权限	服务器权限（客户、设施、设备组）
修补程序符合性规则		
编辑修补程序产品（“修补程序配置”窗口）	管理修补程序符合性规则：是	N/A
扫描修补程序符合性	管理 Windows 修补程序策略：读取	N/A
计划修补程序策略扫描	管理修补程序符合性规则：是	N/A
更改默认修补程序可用性	管理修补程序符合性规则：是	N/A
更改修补程序策略符合性规则	管理修补程序符合性规则：是	N/A
查看修补程序策略符合性规则	管理 Windows 修补程序策略：是	N/A

表 50 列出了用户可以对各修补程序管理权限执行的操作。**表 50** 包含的数据与**表 49** 相同，但是按操作权限排序。尽管**表 50** 中未指明，但是所有“修补程序管理”操作都需要“托管的服务器和组”权限。

对于安全管理员，**表 50** 回答了这样一个问题：如果向用户授予了特定操作权限，那么用户可以执行何种操作？

表 50.Windows 修补程序管理权限允许的用户操作

操作权限	用户操作	服务器权限（客户、设施、设备组）
允许安装修补程序：是	复制异常	读取和写入
	修正策略	读取和写入
	设置异常	读取和写入
允许安装修补程序：是 和管理修补程序：读取	安装修补程序（可用）	读取和写入
	卸载修补程序（可用）	读取和写入
允许安装修补程序：是 和管理修补程序：读取和写入	安装修补程序（有限的可用性）	读取和写入
	卸载修补程序（有限的可用性）	读取和写入
允许安装修补程序：是 和程序包：是	导出修补程序	N/A

操作权限	用户操作	服务器权限（客户、设施、设备组）
允许卸载修补程序：是	复制异常	读取和写入
	设置异常	读取和写入
允许卸载修补程序：是 和程序包	导出修补程序	N/A
允许卸载修补程序：是 和管理修补程序：读取	卸载修补程序	读取和写入
管理修补程序符合性规则：是	更改默认修补程序可用性	N/A
	更改修补程序策略符合性规则	N/A
	编辑修补程序产品（“修补程序配置”窗口）	N/A
	计划修补程序策略扫描	N/A
管理 Windows 修补程序策略：读取	将修补程序策略附加到服务器（或设备组）	读取和写入
	从服务器（或设备组）分离修补程序策略	读取和写入
	打开修补程序策略（查看）	N/A
管理 Windows 修补程序策略：读取和写入	更改修补程序策略属性	N/A
	创建修补程序策略	N/A
	删除修补程序策略	N/A
	从修补程序策略删除修补程序	N/A
管理 Windows 修补程序策略：是	查看修补程序策略符合性规则	N/A
管理修补程序：读取	打开修补程序（查看修补程序） 扫描修补程序符合性	N/A
管理修补程序：读取和写入	更改修补程序属性	N/A
	删除修补程序	N/A
	导入修补程序数据库	N/A
管理修补程序：读取和写入 和程序包	导入修补程序	N/A

操作权限	用户操作	服务器权限（客户、设施、设备组）
管理修补程序：读取 和管理 Windows 修补程序策略： 读取和写入	向修补程序策略添加修补程序	N/A
管理修补程序：读取 和程序包	导出修补程序	N/A
管理策略：读取 和程序包	导出修补程序	N/A

Ubuntu 修补程序管理权限

在 Ubuntu 修补程序管理中，合并了所有用户角色，这意味着单个用户可以执行所有修补程序管理操作。Ubuntu 预置的设置为用户提供以下用户组角色：

- Patch Policy Setter
- Patch Deployer
- Software Policy Setter
- Policy Deployer

此外，还必须满足下列条件：

- 要配置 Ubuntu 修补程序策略：
  - 用户必须同时属于 Patch Policy Setters 和 Software Policy Setters 用户组。
  - 用户必须对服务器所属的客户具有资源的读取和写入权限。
  - 必须为以上两个组添加数据中心。
- 要部署 Ubuntu 修补程序策略：
  - 用户必须同时属于 Patch Deployers 和 Software Deployers 用户组。
  - 用户必须对服务器所属的客户具有资源的读取和写入权限。
  - 必须为以上两个组添加数据中心。
- 要向 Ubuntu 服务器附加 Ubuntu 修补程序策略：
  - 用户必须对目标修补程序策略驻留的文件夹具有读取和写入权限。
  - 要导入 Debian 程序包，用户必须对 Opsware 客户具有资源的读取和写入权限。

备注： 有关标准的修补操作权限，请参见Windows 修补程序管理权限。

要使管理服务器的设施中用户组角色所含的用户具有正确的权限来使用 Ubuntu 修补程序，他们必须具有**表 51** 中显示的文件夹权限。

表 51.Ubuntu 用户组角色的文件夹权限

文件夹	用户组角色	权限
/Opsware	Patch Policy Setter	读取和写入
/Opsware	Software Policy Setter	读取和写入
/Opsware	Patch Policy Deployer	读取
/Opsware	Software Policy Deployer	读取
/Opsware	Superuser	读取和写入
/Opsware	Opsware System Administrator	读取和写入
/Opsware/Patching/Tools	Patch Policy Setter	读取、列出、执行
/Opsware/Patching/Tools	Software Policy Setter	读取、列出、执行
/Opsware/Patching/Tools	Patch Policy Deployer	读取、列出、执行
/Opsware/Patching/Tools	Software Policy Deployer	读取、列出、执行
/Opsware/Patching/Tools	Superuser	读取、列出、执行
/Opsware/Patching/Tools	Opsware System Administrator	读取、列出、执行
/Opsware/Patching/Tools	Command-Line Administrator	读取、列出、执行

Solaris 修补程序管理权限

本节描述在 Solaris 系统上管理修补程序所需的权限。有关其他 UNIX 系统上的修补程序信息，请参见其他 UNIX 修补程序管理权限。有关 Solaris 修补程序策略的权限，请参见 Solaris 修补程序策略管理权限。

表 52 指定了用户在 SA 客户端中执行特定操作所需的修补程序管理权限。对于安全管理员，此表回答了这样一个问题：要执行特定操作，用户需要具有什么权限？

备注: 除了**表 52** 中列出的权限以外，每个用户操作还需要“托管的服务器和组”权限。

在**表 52** 中，“用户操作”列中的大多数条目对应于 SA 客户端中的菜单项。除了操作权限以外，受修补操作影响的托管服务器需要具有服务器权限。

备注: 如果“允许安装修补程序”权限设置为“是”，则“管理修补程序”权限自动设置为“读取”。如果您打算使用 Solaris 修补程序策略，还应当将“管理软件策略”设置为“读取”或“读取和写入”。有关详细信息，请参见Solaris 修补程序策略管理权限。

表 52.用户操作所需的 Solaris 修补程序管理权限

用户操作	操作权限	服务器权限（客户、设施、设备组）
修补程序		
安装修补程序（可用）	允许安装修补程序：是 管理修补程序：读取	读取和写入
卸载修补程序（可用）	允许卸载修补程序：是 管理修补程序：读取	读取和写入
安装修补程序（有限的可用性）	允许安装修补程序：是 管理修补程序：读取和写入	读取和写入
卸载修补程序（有限的可用性）	允许卸载修补程序：是 管理修补程序：读取和写入	读取和写入
打开修补程序（查看修补程序）	管理修补程序：读取	N/A
更改修补程序属性	管理修补程序：读取和写入	N/A
导入修补程序	管理修补程序：读取和写入	N/A
导出修补程序	管理修补程序：读取 允许安装修补程序：是（可选） 允许卸载修补程序：是（可选） 管理软件策略：读取（可选）	N/A
删除修补程序	管理修补程序：读取和写入	N/A

表 53 列出了用户可以对各 Solaris 修补程序管理权限执行的操作。**表 53** 包含的数据与**表 52** 相同，但是按操作权限排序。尽管**表 53** 中未指明，但是所有“修补程序管理”操作都需要“托管的服务器和组”权限。

对于安全管理员，**表 53** 回答了这样一个问题：如果向用户授予了特定操作权限，那么用户可以执行何种操作？

表 53.Solaris 修补程序管理权限允许的用户操作

操作权限	用户操作	服务器权限（客户、设施、设备组）
允许安装修补程序：是	修正策略	读取和写入

操作权限	用户操作	服务器权限（客户、设施、设备组）
允许安装修补程序：是 管理修补程序：读取	安装修补程序（可用）	读取和写入
	卸载修补程序（可用）	读取和写入
允许安装修补程序：是 管理修补程序：读取和写入	安装修补程序（有限的可用性）	读取和写入
	卸载修补程序（有限的可用性）	读取和写入
允许安装修补程序：是 （还要将“管理修补程序”设置为：读取）	导出修补程序	N/A
允许卸载修补程序：是 （还要将“管理修补程序”设置为：读取）	导出修补程序	N/A
允许卸载修补程序：是 （还要将“管理修补程序”设置为：读取）	卸载修补程序	读取和写入
管理修补程序：读取	打开修补程序（查看修补程序）	N/A
	导出修补程序	N/A
管理修补程序：读取和写入	更改修补程序属性	N/A
	删除修补程序	N/A
	导入修补程序	N/A

Solaris 修补程序策略管理权限

表 54 指定了用户在 SA 客户端中执行特定操作所需的 Solaris 修补程序策略管理权限。对于安全管理员，此表回答了这样一个问题：要执行特定操作，用户需要具有什么权限？

如果将客户分配到文件夹，则客户约束可能限制可与该文件夹中包含的 Solaris 修补程序策略关联的对象。有关受这些约束影响的任务的列表，请参见文件夹、客户约束和软件策略。

表 54.用户操作所需的 Solaris 修补程序策略管理权限

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
Solaris 修补程序策略			
创建 Solaris 修补程序策略	管理软件策略：读取和写入	N/A	写入
删除 Solaris 修补程序策略	管理软件策略：读取和写入	N/A	写入
打开 Solaris 修补程序策略（查看）	管理软件策略：读取	N/A	读取
编辑 Solaris 修补程序策略属性	管理软件策略：读取和写入	N/A	写入
添加修补程序	管理软件策略：读取和写入 管理修补程序：读取	N/A	包含软件策略的文件夹：写入
添加脚本	管理软件策略：读取和写入 管理服务器脚本：读取	N/A	包含软件策略的文件夹：写入
删除修补程序	管理软件策略：读取和写入	N/A	写入
删除脚本	管理软件策略：读取和写入	N/A	写入
附加 Solaris 修补程序策略	管理软件策略：读取 允许附加/分离软件策略：是 建立公用设备组模型：是（如果您将 Solaris 修补程序策略附加到公用设备组，则需要此权限。）	读取和写入	读取
分离 Solaris 修补程序策略	管理软件策略：读取 允许附加/分离软件策略：是 建立公用设备组模型：是（如果您将 Solaris 修补程	读取和写入	读取

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
	序策略附加到公用设备组，则需要此权限。）		
修正	管理软件策略：读取 允许修正服务器：是 建立公用设备组模型：是（如果您修正公用设备组，则需要此权限。）	读取和写入	读取
扫描 Solaris 修补程序符合性	N/A	读取	N/A
重命名 Solaris 修补程序策略	管理软件策略：读取和写入	N/A	写入
剪切 Solaris 修补程序策略	管理软件策略：读取和写入	N/A	写入
复制 Solaris 修补程序策略	管理软件策略：读取	N/A	读取
粘贴 Solaris 修补程序策略	管理软件策略：读取和写入	N/A	源文件夹：读取（对于复制和粘贴） 源文件夹：写入（对于剪切和粘贴） 目标文件夹：写入
移动 Solaris 修补程序策略	管理软件策略：读取和写入	N/A	源文件夹：写入 目标文件夹：写入

其他 UNIX 修补程序管理权限

本节描述在 Solaris 之外的 UNIX 系统上管理修补程序所需的权限。有关 Solaris 信息，请参见Solaris 修补程序管理权限。您可以将软件策略用于 UNIX 修补程序。有关详细信息，请参见软件管理权限。

表 55 指定了用户在 SA 客户端中执行特定操作所需的修补程序管理权限。对于安全管理员，此表回答了这样一个问题：要执行特定操作，用户需要具有什么权限？

备注: 除了**表 55** 中列出的权限以外，每个用户操作还需要“托管的服务器和组”权限。

在**表 55** 中，“用户操作”列中的大多数条目对应于 SA 客户端中的菜单项。除了操作权限以外，受修补操作影响的托管服务器需要具有服务器权限。

备注: 如果“允许安装修补程序”权限设置为“是”，则“管理修补程序”权限自动设置为“读取”。如果您打算使用策略，还应当将“管理软件策略”设置为“读取”或“读取和写入”。

表 55.用户操作所需的 UNIX 修补程序管理权限

用户操作	操作权限	服务器权限（客户、设施、设备组）
修补程序		
安装修补程序（可用）	允许安装修补程序：是 管理修补程序：读取	读取和写入
卸载修补程序（可用）	允许卸载修补程序：是 和管理修补程序：读取	读取和写入
安装修补程序（有限的可用性）	允许安装修补程序：是 管理修补程序：读取和写入	读取和写入
卸载修补程序（有限的可用性）	允许卸载修补程序：是 和管理修补程序：读取和写入	读取和写入
打开修补程序（查看修补程序）	管理修补程序：读取	N/A
更改修补程序属性	管理修补程序：读取和写入	N/A
导出修补程序	管理修补程序：读取 和程序包	N/A
导出修补程序	或允许安装修补程序：是 和程序包：是	N/A
导出修补程序	或允许卸载修补程序：是 和程序包	N/A
导出修补程序	或管理策略：读取 和程序包	N/A
删除修补程序	管理修补程序：读取和写入	N/A

表 56 列出了用户可以对各修补程序管理权限执行的操作。**表 56** 包含的数据与**表 55** 相同，但是按操作权限排序。尽管**表 56** 中未指明，但是所有“修补程序管理”操作都需要“托管的服务器和组”权限。

对于安全管理员，**表 56** 回答了这样一个问题：如果向用户授予了特定操作权限，那么用户可以执行何种操作？

表 56.UNIX 修补程序管理权限允许的用户操作

操作权限	用户操作	服务器权限（客户、设施、设备组）
允许安装修补程序：是	复制异常	读取和写入
	修正策略	读取和写入
	设置异常	读取和写入
允许安装修补程序：是 和管理修补程序：读取	安装修补程序（可用）	读取和写入
	卸载修补程序（可用）	读取和写入
允许安装修补程序：是 和管理修补程序：读取和写入	安装修补程序（有限的可用性）	读取和写入
	卸载修补程序（有限的可用性）	读取和写入
允许安装修补程序：是 和程序包：是	导出修补程序	N/A
允许卸载修补程序：是	复制异常	读取和写入
	设置异常	读取和写入
允许卸载修补程序：是 和程序包	导出修补程序	N/A
管理修补程序：读取	打开修补程序（查看修补程序）	N/A
管理修补程序：读取和写入	更改修补程序属性	N/A
	删除修补程序	N/A
	导入修补程序数据库	N/A
管理修补程序：读取和写入 和程序包	导入修补程序	N/A
管理修补程序：读取 和管理策略：读取和写入	向策略添加修补程序	N/A
管理修补程序：读取 和程序包	导出修补程序	N/A

操作权限	用户操作	服务器权限（客户、设施、设备组）
管理策略：读取和程序包	导出修补程序	N/A

审核和修正权限

表 57 指定了用户在 SA 客户端中执行特定操作所需的审核和修正权限。对于安全管理员，此表回答了这样一个问题：要执行特定操作，用户需要具有什么权限？

备注: 除了**表 57** 中列出的权限以外，每个用户操作还需要“托管的服务器和组”权限。

审核和修正的服务器权限

审核和修正操作需要操作权限和服务器权限。例如，“创建审核”操作需要操作权限“管理审核：读取和写入”和“托管的服务器和组”权限。此操作还需要在审核引用的服务器上具有读取权限。在**表 57** 中，“服务器权限”列针对的是审核或快照规范所引用的服务器 - 取决于操作。服务器权限由 SA Web 客户端中的客户、设施和设备组权限指定。

如果审核和修正对象（例如快照规范）引用多个服务器，则所有引用的服务器至少需要读取权限。否则，无法查看或修改该对象。

审核和修正对象不直接与客户和设施关联。客户和设施权限控制审核和修正对象（例如快照规范和审核）所引用的服务器的访问权限。

审核和修正的“允许创建特定于任务的策略权限”

作为最佳实践，*不要* 启用此权限 — *不要* 将此权限设置为“是”。默认情况下，禁用此权限 - 已将其设置为“否”。建议您在审核策略中创建审核规则，然后将审核任务和快照规范链接到该审核策略。

审核和修正的 OGFS 权限

对于访问托管服务器的文件系统的操作，需要“OGFS 读取服务器文件系统”权限。例如，需要“读取服务器文件系统”权限，才能创建具有包含托管服务器文件的规则的快照规范。此类规则包含应用程序配置、自定义脚本、COM+ 对象、文件系统、IIS 元数据库条目和 Windows 注册表。

其他类型的选择条件需要相应的 OGFS 权限：

- 读取服务器注册表
- 读取 COM+ 数据库
- 读取 IIS 元数据库

审核和修正用户操作权限

下表列出了典型审核和修正用户操作和执行它们所需的权限。

表 57.执行用户操作所需的审核和修正权限

用户操作	操作权限	OGFS 权限	服务器权限（客户、设施、设备组）
快照规范			
查看快照规范的内容	管理快照规范：读取	N/A	读取
计划和运行快照规范	管理快照规范：读取	N/A	读取
创建快照规范	管理快照规范：读取和写入	N/A	读取和写入
创建应用程序配置规则	管理快照规范：读取和写入	写入服务器文件系统	读取和写入
创建 COM+ 规则	管理快照规范：读取和写入	读取 COM+ 数据库	读取和写入
创建自定义脚本规则	管理快照规范：读取和写入 允许创建自定义脚本策略规则：是。	写入服务器文件系统	读取和写入
创建文件	管理快照规范：读取和写入	写入服务器文件系统	读取和写入
创建 IIS 元数据库规则	管理快照规范：读取和写入	读取 IIS 元数据库	读取和写入
创建注册表规则	管理快照规范：读取和写入	读取服务器注册表	读取和写入
将审核策略链接到快照规范	管理快照规范：读取和写入 管理审核策略：读取 库文件夹：读取	N/A	读取和写入
将审核策略导入快照规范	管理快照规范：读取和写入 管理审核策略：读取 库文件夹：读取	N/A	读取和写入

用户操作	操作权限	OGFS 权限	服务器权限（客户、设施、设备组）
另存为审核策略	管理快照规范：读取和写入 管理审核策略：读取和写入 库文件夹：读取和写入	N/A	读取和写入
快照			
查看、列出快照的内容	管理快照：读取 管理快照规范：读取	N/A	读取
从快照创建审核	管理快照：读取 管理快照规范：读取 管理审核：读取	N/A	读取
查看存档的快照	管理快照：读取	N/A	读取
从存档的快照创建审核	管理快照：读取 管理审核：读取	N/A	读取
删除快照结果	管理快照： 读取和写入	N/A	读取和写入
从服务器分离快照	允许常规快照管理：是 管理快照：读取和写入 管理快照规范：读取	N/A	读取
修正快照结果	管理快照：读取 管理快照规范：读取 允许修正审核/快照结果：是	N/A	读取和写入
修正快照结果：应用程序配置	管理快照：读取 允许修正审核/快照结果：是 管理快照规范：读取	写入服务器文件系统	读取和写入
修正快照结果：COM+	管理快照：读取	读取 COM+ 数据库	读取和写入

用户操作	操作权限	OGFS 权限	服务器权限（客户、设施、设备组）
	允许修正审核/快照结果：是 管理快照规范：读取		
修正快照结果：自定义脚本	管理快照：读取 允许修正审核/快照结果：是 管理快照规范：读取	写入服务器文件系统	读取和写入
修正快照结果：文件系统	管理快照：读取 允许修正审核/快照结果：是 管理快照规范：读取	写入服务器文件系统	读取和写入
修正快照结果：元数据库	管理快照：读取 允许修正审核/快照结果：是 管理快照规范：读取	读取 IIS 元数据库	读取和写入
修正快照结果：注册表	管理快照：读取 允许修正审核/快照结果：是 管理快照规范：读取	读取服务器注册表	读取和写入
审核			
查看审核	管理审核：读取	N/A	读取
运行审核	管理审核结果：读取	N/A	读取
计划审核	管理审核结果：读取和写入	N/A	读取
创建审核	管理审核：读取和写入	N/A	读取
创建应用程序配置规则	管理审核：读取和写入	写入服务器文件系统	读取和写入
创建 COM+ 规则	管理审核：读取和写入	读取 COM+ 数据库	读取和写入

用户操作	操作权限	OGFS 权限	服务器权限（客户、设施、设备组）
创建自定义脚本规则	管理审核：读取和写入 允许创建自定义脚本策略规则：是	写入服务器文件系统	读取和写入
创建发现的软件规则	管理审核：读取和写入 管理服务器模块：读取	N/A	读取和写入
创建文件规则	管理审核：读取和写入	写入服务器文件系统	读取和写入
创建硬件规则	管理审核：读取和写入	N/A	读取和写入
创建 IIS 元数据库规则	管理审核：读取和写入	读取 IIS 元数据库	读取和写入
创建 Internet Information Server 规则	管理审核：读取和写入	N/A	读取和写入
创建已注册的软件规则	管理审核：读取和写入 管理服务器模块：读取	N/A	读取和写入
创建软件规则	管理审核：读取和写入	N/A	读取和写入
创建存储规则	管理审核：读取和写入 管理服务器模块：读取	N/A	读取和写入
创建 Weblogic 规则	管理审核：读取和写入 管理服务器模块：读取	N/A	读取和写入
创建 .NET Framework 配置规则	管理审核：读取和写入 管理服务器模块：读取	N/A	读取和写入
创建 Windows 注册表规则	管理审核：读取和写入	读取服务器注册表	读取和写入
创建 Windows 服务规则	管理审核：读取和写入	N/A	读取和写入
创建 Windows/UNIX 用户和组规则	管理审核：读取和写入 管理服务器模块：读取	N/A	读取和写入
将审核策略链接到审核	管理审核：读取和写入 管理审核策略：读取	N/A	读取和写入

用户操作	操作权限	OGFS 权限	服务器权限（客户、设施、设备组）
	SA 客户端库文件夹：读取		
将审核策略导入审核	管理审核：读取和写入 管理审核策略：读取 库文件夹：读取	N/A	读取和写入
另存为审核策略	管理审核：读取和写入 管理审核策略：读取和写入 库文件夹：读取和写入	N/A	读取和写入
审核结果			
查看审核结果	管理审核结果：读取 管理审核：读取	N/A	读取
查看存档的审核结果	管理审核：读取	N/A	读取
删除审核结果	管理审核结果：读取和写入	N/A	读取和写入
修正审核结果	管理审核：读取 管理审核结果：读取和写入 允许修正审核/快照结果：是	N/A	读取和写入
修正审核结果：应用程序配置	管理审核：读取 管理审核结果：读取和写入 允许修正审核/快照结果：是	写入服务器文件系统	读取和写入
修正审核结果：COM+	管理审核：读取 管理审核结果：读取和写入 允许修正审核/快照结果：是	读取 COM+ 数据库	读取和写入

用户操作	操作权限	OGFS 权限	服务器权限（客户、设施、设备组）
修正审核结果：自定义脚本规则	管理审核：读取 管理审核结果：读取和写入 允许修正审核/快照结果：是	写入服务器文件系统	读取和写入
修正审核结果：发现的软件	管理审核：读取 管理审核结果：读取和写入 允许修正审核/快照结果：是 管理服务器模块：读取 允许执行服务器模块：是	N/A	读取和写入
修正审核结果：文件	管理审核：读取 管理审核结果：读取和写入 允许修正审核/快照结果：是	写入服务器文件系统	读取和写入
修正审核结果：IIS 元数据库	管理审核：读取 管理审核结果：读取和写入 允许修正审核/快照结果：是	读取 IIS 元数据库	读取和写入
修正审核结果：修正 Internet Information Server	管理审核：读取 管理审核结果：读取和写入 允许修正审核/快照结果：是	读取 IIS 元数据库	读取和写入
修正审核结果：修正发现的软件	管理审核：读取 管理审核结果：读取和写入 允许修正审核/快照结果：	N/A	读取和写入

用户操作	操作权限	OGFS 权限	服务器权限（客户、设施、设备组）
	是 管理服务器模块：读取 允许执行服务器模块：是		
修正审核结果：修正软件	管理审核：读取 管理审核结果：读取和写入	N/A	读取和写入
修正审核结果：修正存储	管理审核：读取 管理审核结果：读取和写入 允许修正审核/快照结果：是 管理服务器模块：读取 允许执行服务器模块：是	N/A	读取和写入
修正审核结果：修正 Weblogic	管理审核：读取 管理审核结果：读取和写入 允许修正审核/快照结果：是 管理服务器模块：读取 允许执行服务器模块：是	N/A	读取和写入
修正审核结果：修正 Windows .NET Framework 配置	管理审核：读取 管理审核结果：读取和写入 允许修正审核/快照结果：是 管理服务器模块：读取 允许执行服务器模块：是	N/A	读取和写入
修正审核结果：Windows 注册表	管理审核：读取 管理审核结果：读取和写入	读取服务器注册表	读取和写入

用户操作	操作权限	OGFS 权限	服务器权限（客户、设施、设备组）
	允许修正审核/快照结果：是		
修正审核结果：Windows 服务	管理审核：读取 管理审核结果：读取和写入 允许修正审核/快照结果：是	N/A	读取和写入
修正审核结果：修正 Windows/UNIX 用户和组	管理审核：读取 管理审核结果：读取和写入 允许修正审核/快照结果：是 管理服务器模块：读取 允许执行服务器模块：是	N/A	读取和写入

表 58 列出了用户可以对审核和修正权限执行的操作。**表 58** 包含的数据与**表 57** 相同，但是按操作权限排序。尽管**表 58** 中未指明，但是所有审核和修正操作都需要“托管的服务器和组”权限。

对于安全管理员，**表 58** 回答了这样一个问题：如果向用户授予了特定操作审核和修正权限，那么用户可以执行何种操作？

表 58.审核和修正权限允许的用户操作

操作权限	用户操作	OGFS 权限	服务器权限（客户、设施、设备组）
允许创建自定义脚本规则策略：否 和 管理审核：读取	查看自定义脚本规则：审核	N/A	读取
允许创建自定义脚本规则策略：是 和	创建自定义脚本规则：审核	写入服务器文件系统	读取和写入

操作权限	用户操作	OGFS 权限	服务器权限（客户、设施、设备组）
管理审核：读取和写入			
允许创建自定义脚本规则策略：否 和 管理快照：读取和写入	查看自定义脚本规则：快照	N/A	读取
允许创建自定义脚本规则策略：是 和 管理快照：读取和写入	创建自定义脚本规则：快照	写入服务器文件系统	读取和写入
允许常规 快照管理：是	从服务器分离快照	N/A	读取
管理快照规范：读取 和 允许修正审核/快照结果：否 和 管理审核或管理快照：读取	查看审核或快照，不修正	N/A	读取
管理快照规范：读取 和 允许修正审核/快照结果：是 和 管理审核或管理快照：读取和写入	修正审核/快照结果	N/A	读取和写入
管理快照规范：读取 和 允许修正审核/快照结果：是 和	修正应用程序配置规则	写入服务器文件系统	读取和写入

操作权限	用户操作	OGFS 权限	服务器权限（客户、设施、设备组）
管理审核或管理快照结果：读取和写入			
	修正 COM+ 规则	读取 COM+ 数据库	读取和写入
	修正自定义脚本规则注册表规则	写入服务器文件系统	读取和写入
	修正文件系统规则	读取 IIS 元数据库	读取和写入
	修正 IIS 元数据库规则	读取服务器注册表	读取和写入
	修正 Windows 注册表规则	写入服务器文件系统	读取和写入
管理审核：读取	查看、计划、运行审核	N/A	读取
管理审核：读取和写入	创建、编辑、删除审核	N/A	读取和写入
	将审核另存为审核策略	N/A	读取和写入
	将审核策略链接到审核	N/A	读取和写入
	创建应用程序配置规则	写入服务器文件系统	读取和写入
	创建 COM+ 规则	读取 COM+ 数据库	读取和写入
	创建文件系统规则	写入服务器文件系统	读取和写入
	创建 IIS 元数据库规则	读取 IIS 元数据库	读取和写入
	创建 Windows 注册表规则	读取服务器注册表	读取和写入
管理审核：读取和写入 和 允许创建自定义脚本策略规则：是	创建自定义脚本规则	写入服务器文件系统	读取和写入
管理审核：读取和写入	创建下列审核规则： · 发现的软件	N/A	读取和写入

操作权限	用户操作	OGFS 权限	服务器权限（客户、设施、设备组）
和 管理服务器模块：读取	· 已注册软件 · 存储 · Weblogic · Windows .NET Framework 配置 · Windows 用户和组		
管理审核结果：读取	查看审核结果	N/A	读取
管理审核结果：读取和写入	删除审核结果	N/A	读取和写入
管理快照规范：读取和写入	查看、计划、运行快照规范	N/A	读取
管理快照规范：读取和写入	创建、编辑和删除快照规范	N/A	
	将快照规范另存为审核策略 （此操作需要策略所在的库文件夹的读取和写入权限。）	N/A	
	将审核策略链接到审核	N/A	读取和写入
	创建应用程序配置规则	写入服务器文件系统	读取和写入
	创建 COM+ 规则	读取 COM+ 数据库	读取和写入
	创建发现的软件		
	创建文件系统规则	写入服务器文件系统	读取和写入
	创建 IIS 元数据库规则	读取 IIS 元数据库	读取和写入
	创建 Windows 注册表规则	读取服务器注册表	读取和写入
管理快照规范：读取和写	创建下列快照规则：	N/A	读取和写入

操作权限	用户操作	OGFS 权限	服务器权限（客户、设施、设备组）
入 和 管理服务器模块：读取	· 发现的软件 · 已注册软件 · 存储 · Weblogic · Windows .NET Framework 配置 · Windows 用户和组		
管理快照规范：读取和写入 和 创建自定义脚本策略规则	创建快照规范的自定义规则	写入服务器文件系统	读取和写入
管理快照：读取	查看快照的内容	N/A	读取
管理快照： 读取和写入	删除快照结果	N/A	读取和写入
管理审核策略：读取	查看审核和快照规范的内容	N/A	读取
管理审核策略： 读取和写入	创建、编辑审核策略	N/A	读取和写入
	创建应用程序配置规则	写入服务器文件系统	读取和写入
	创建 COM+ 规则	读取 COM+ 数据库	读取和写入
	创建文件系统规则	写入服务器文件系统	读取和写入
	创建 IIS 元数据库规则	读取 IIS 元数据库	读取和写入
	创建 Windows 注册表规则	读取服务器注册表	读取和写入
管理审核策略：读取和写入 管理服务器模块：读取	创建下列快照规则： · 发现的软件 · 已注册软件 · 存储	N/A	读取和写入

操作权限	用户操作	OGFS 权限	服务器权限（客户、设施、设备组）
	· Weblogic · Windows .NET Framework 配置 · Windows 用户和组		
管理审核策略： 读取和写入 和 允许创建自定义脚本策略规则	创建自定义脚本规则	写入服务器文件系统	读取和写入

符合性视图权限

下节描述用户在 SA 客户端中执行特定操作所需的符合性视图权限。对于安全管理员，下表回答了这样一个问题：要执行特定操作，用户需要具有什么权限？

表 59.用户操作所需的符合性视图权限

用户操作	操作权限	服务器权限（客户、设施、设备组）
审核		
查看详细信息	管理审核结果：读取	读取
运行审核	管理审核：读取 管理审核结果：读取和写入	读取和写入
修正	允许修正审核/快照结果：是 有关修正特定审核规则所需的其他权限，请参见审核和修正用户操作权限和表 58.审核和修正权限允许的用户操作。	读取和写入
软件		
修正	管理软件策略：读取 允许修正服务器：是	读取和写入

用户操作	操作权限	服务器权限（客户、设施、设备组）
扫描设备	管理软件策略：读取 或 允许附加/分离软件策略：是 或 允许安装/卸载软件：是 或 允许修正服务器：是	读取和写入
修补程序		
修正	管理修补程序策略：读取 安装修补程序：是	读取和写入
扫描设备	管理修补程序：读取 或 管理修补程序策略：读取 或 允许安装修补程序：是 或 允许卸载修补程序：是 或 允许安装/卸载软件 或 允许修正服务器	读取和写入
应用程序配置		
查看详细信息	管理应用程序配置：读取	读取
扫描设备	允许配置符合性扫描：是	读取
特定应用程序配置修正	有关修正应用程序配置所需的权限，请参见应用程序配置管理权限。	读取和写入

作业权限

要管理 SA 客户端中的作业，您必须具有**表 60** 中所述的权限。当您选择“编辑或取消任何作业”权限时，会自动选择“查看所有作业”权限。

要在 SA 客户端中查看任何作业，您必须拥有运行或执行该作业的权限。例如，如果对于“管理应用程序配置”等操作，您有设置为“读取”的权限，但是没有该操作的“写入”权限，则您将无法在 SA 客户端中看到任何“应用程序配置推送”作业。

表 60.作业管理权限

用户操作	操作权限
启用批准集成	管理批准集成
设置需要批准的作业类型	管理批准集成
调用 JobService API 方法来管理已阻止的（待批准）作业 （此操作由后端自定义软件执行，而非登录到 SA 客户端的最终用户执行。）	编辑或取消任何作业 查看所有作业
结束（取消）作业	编辑或取消任何作业 查看所有作业
删除计划	编辑或取消任何作业 查看所有作业

脚本执行权限

表 61 指定了用户在 SA 客户端中执行特定操作所需的脚本执行权限。对于安全管理员，此表回答了这样一个问题：要执行特定操作，用户需要具有什么权限？

如果将客户分配到文件夹，则客户约束可能限制可与该文件夹中包含的软件策略关联的对象。有关受这些约束影响的任务的列表，请参见文件夹、客户约束和软件策略。

表 61.用户操作所需的脚本执行权限

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
创建非超级用户服务器脚本	管理服务器脚本：读取和写入	N/A	写入
创建超级用户服务器脚本	管理服务器脚本：读取和写入	N/A	写入

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
	允许控制超级用户的服务器脚本：是		
创建 OGFS 脚本	管理 OGFS 脚本：读取和写入	N/A	写入
打开非超级用户服务器脚本（查看除脚本内容之外的所有脚本属性）	管理服务器脚本：读取	N/A	执行
打开非超级用户服务器脚本（查看包括脚本内容在内的所有脚本属性）	管理服务器脚本：读取	N/A	
打开超级用户服务器脚本（查看除脚本内容之外的所有脚本属性）	管理服务器脚本：读取 允许控制超级用户的服务器脚本：是	N/A	
打开超级用户服务器脚本（查看包括脚本内容在内的所有脚本属性）	管理服务器脚本：读取 允许控制超级用户的服务器脚本：是	N/A	
打开 OGFS 脚本（查看除脚本内容之外的所有脚本属性）	管理 OGFS 脚本：读取	N/A	执行
打开 OGFS 脚本（查看包括脚本内容在内的所有脚本属性）	管理 OGFS 脚本：读取	N/A	读取
编辑非超级用户服务器脚本属性	管理服务器脚本：读取和写入 注意：需要“允许控制超级用户的服务器脚本：是”权限才能编辑脚本属性“可以作为超级用户运行”。	N/A	写入
编辑超级用户服务器脚本	管理服务器脚本：读取和写入	N/A	写入

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
	允许控制超级用户的服务器脚本：是		
编辑 OGFS 脚本属性	管理 OGFS 脚本：读取和写入	N/A	写入
在文件夹中查找服务器脚本	管理服务器脚本：读取	N/A	读取
在文件夹中查找 OGFS 脚本	管理 OGFS 脚本：读取	N/A	读取
导出服务器脚本	管理服务器脚本：读取	N/A	读取
导出 OGFS 脚本	管理 OGFS 脚本：读取	N/A	读取
重命名服务器脚本	管理服务器脚本：读取和写入	N/A	写入
重命名超级用户服务器脚本	管理服务器脚本：读取和写入 允许控制超级用户的服务器脚本：是	N/A	写入
重命名 OGFS 脚本	管理 OGFS 脚本：读取和写入	N/A	写入
删除服务器脚本	管理服务器脚本：读取和写入	N/A	写入
删除超级用户服务器脚本	管理服务器脚本：读取和写入 允许控制超级用户的服务器脚本：是	N/A	写入
删除 OGFS 脚本	管理 OGFS 脚本：读取和写入	N/A	写入
以超级用户身份运行服务器脚本	托管的服务器和组：是	读取和写入	执行
以超级用户身份运行服务器脚本（通过从另一个脚本复制脚本内容）	管理服务器脚本：读取 运行临时脚本：是 以超级用户身份运行临时	读取和写入	读取

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
	的和源码可见的服务器脚本：是 托管的服务器和组：是		
以指定用户身份运行服务器脚本	托管的服务器和组：是	读取和写入	执行
以指定用户身份运行服务器脚本（通过从另一个脚本复制脚本内容）	管理服务器脚本：读取 运行临时脚本：是 托管的服务器和组：是	读取和写入	读取
运行临时脚本	运行临时脚本：是 托管的服务器和组：是	读取和写入	N/A
运行临时脚本 （以超级用户身份）	运行临时脚本：是 以超级用户身份运行临时的和源码可见的服务器脚本：是 托管的服务器和组：是	读取和写入	N/A
运行 OGFS 脚本	N/A	N/A	执行

表 62 列出了用户可以对每个脚本执行权限执行的操作。**表 62** 包含的数据与**表 61** 相同，但是按操作权限排序。对于安全管理员，**表 62** 回答了这样一个问题：如果向用户授予了特定操作权限，那么用户可以执行何种操作？

表 62.脚本执行权限允许的用户操作

操作权限	用户操作	服务器权限（客户、设施、设备组）	文件夹权限
管理服务器脚本：读取和写入	创建非超级用户服务器脚本	N/A	写入
	编辑非超级用户服务器脚本属性	N/A	写入
	删除非超级用户服务器脚本	N/A	写入

操作权限	用户操作	服务器权限（客户、设施、设备组）	文件夹权限
	重命名非超级用户服务器脚本	N/A	写入
管理服务器脚本：读取	打开非超级用户服务器脚本（查看包括脚本内容在内的所有脚本属性） 打开超级用户服务器脚本（查看包括脚本内容在内的所有脚本属性）	N/A	读取
	在文件夹中查找服务器脚本	N/A	读取
	导出服务器脚本	N/A	读取
管理服务器脚本：读取	打开非超级用户服务器脚本（查看除脚本内容之外的所有脚本属性） 打开超级用户服务器脚本（查看除脚本内容之外的所有脚本属性）		执行
管理服务器脚本：读取和写入 和 允许控制超级用户的服务器脚本：是	创建超级用户服务器脚本	N/A	写入
	编辑超级用户服务器脚本属性 编辑非超级用户服务器脚本属性	N/A	写入
	重命名超级用户服务器脚本 重命名非超级用户服务器脚本	N/A	写入
	删除超级用户服务器脚本 删除非超级用户服务器脚本	N/A	写入

操作权限	用户操作	服务器权限（客户、设施、设备组）	文件夹权限
管理 OGFS：读取和写入	创建 OGFS 脚本	N/A	写入
	编辑 OGFS 脚本属性	N/A	写入
	删除 OGFS 脚本	N/A	写入
	重命名 OGFS 脚本	N/A	写入
管理 OGFS 脚本：读取	打开 OGFS 脚本（查看包括脚本内容在内的所有 OGFS 脚本属性）	N/A	读取
	在文件夹中查找 OGFS	N/A	读取
	导出 OGFS 脚本	N/A	读取
管理 OGFS 脚本：读取	打开 OGFS 脚本（查看除脚本内容之外的所有 OGFS 脚本属性）	N/A	执行
运行临时脚本	运行临时脚本	读取和写入	N/A
以超级用户身份运行临时的和源码可见的服务器脚本	以超级用户身份运行临时脚本	读取和写入	N/A
N/A	运行非超级用户服务器脚本	读取和写入	执行
N/A	运行专用脚本	读取和写入	执行（在主文件夹中）
N/A	运行 OGFS 脚本	N/A	执行

下表列出使用软件策略运行脚本所需的脚本执行权限。

表 63.软件管理所需的脚本执行权限

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
将服务器脚本添加到软件策略	管理服务器脚本：读取	N/A	读取

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
将服务器脚本添加到“修正”窗口中的“选项”步骤	N/A	N/A	执行
将服务器脚本添加到“修正”窗口中的“选项”步骤（复制脚本内容）	管理服务器脚本：读取 运行临时脚本：是	N/A	读取
将超级用户服务器脚本添加到“修正”窗口中的“选项”步骤	管理服务器脚本：读取 运行临时脚本：是 以超级用户身份运行临时的和源码可见的服务器脚本：是	N/A	读取
将临时脚本指定到“修正”窗口中的“选项”步骤	运行临时脚本：是	N/A	N/A
将超级用户临时脚本指定到“修正”窗口中的“选项”步骤	运行临时脚本：是 以超级用户身份运行临时的和源码可见的服务器脚本：是	N/A	N/A
将服务器脚本添加到“安装软件”窗口中的“选项”步骤	N/A	N/A	执行
将服务器脚本添加到“安装软件”窗口中的“选项”步骤（复制脚本内容）	管理服务器脚本：读取 运行临时脚本：是	N/A	读取
将超级用户服务器脚本添加到“安装软件”窗口中的“选项”步骤	管理服务器脚本：读取 运行临时脚本：是 以超级用户身份运行临时的和源码可见的服务器脚本：是	N/A	读取
将临时脚本指定到“安装软件”窗口中的“选项”步骤	运行临时脚本：是	N/A	N/A

用户操作	操作权限	服务器权限（客户、设施、设备组）	文件夹权限
将超级用户临时脚本指定到“安装软件”窗口中的“选项”步骤	运行临时脚本：是 以超级用户身份运行临时的和源码可见的服务器脚本：是	N/A	N/A

流权限 - HP Operations Orchestration

在 SA 中管理流或运行流需要下列权限：

表 64.流相关权限

用户操作	权限
配置 SA-OO 集成	管理流集成
以 SA 用户身份在 SA 客户端中运行流	运行流

Service Automation Visualizer 权限

表 65 指定了在 SA 客户端中执行特定操作所需的 Service Automation Visualizer (SAV) 权限。对于安全管理员，此表回答了这样一个问题：要执行特定操作，用户需要具有什么权限？

在**表 65** 中，“用户操作”列中的大多数条目对应于 SA 客户端中的菜单项。除了操作权限，受分析操作影响的托管服务器上还需要服务器读取权限，例如从 Service Automation Visualizer 打开远程终端或远程桌面客户端、打开设备浏览器和打开全局 Shell 会话的权限。

备注: 扫描服务器所需的 SAV 权限对于物理服务器和虚拟服务器而言是相同的。

有关完整信息，请参见《SA 用户指南：Service Automation Visualizer》。

表 65.执行用户操作所需的 SAV 权限

用户操作	操作权限	源服务器权限（客户、设施）	文件夹权限
仅 SAV 操作			
启动 Service Automation Visualizer	允许分析：是	读取	N/A
生成扫描或刷新快照 - 常规或虚拟服务器	允许分析：是	读取	N/A
生成快照或编辑计划的快照	允许分析：是 管理业务应用程序：读取和写入	读取	N/A
启动、停止、暂停、重新启动 SAV 中的虚拟服务器（仅暂停 VMware 的虚拟机 — 不能暂停 Solaris 本地区域）	管理虚拟服务器：是	读取	N/A
SA 客户端操作			
运行脚本（以非超级用户身份）	运行临时脚本：是	读取和写入	N/A
运行脚本（以超级用户身份）	以超级用户身份运行临时的和源码可见的服务器脚本：是	读取和写入	N/A
执行 OGFS 脚本	管理 OGFS 脚本：是	读取和写入	N/A
存储操作（启用 SE 的核心）			
查看 SAN 阵列或 NAS 文件管理器数据（包括关系）。	查看存储系统：是	读取	N/A
查看任何 SAN 交换机数据（包括关系）	查看存储系统：是	读取	N/A
SA 客户端文件夹操作			
从文件夹打开业务应用程序	N/A	N/A	在文件夹中读取对象
创建业务应用程序并保存到文件夹	管理业务应用程序：是	N/A	在文件夹中写入对象

用户操作	操作权限	源服务器权限（客户、设施）	文件夹权限
在文件夹中重命名业务应用程序	N/A	N/A	在文件夹中写入对象
从文件夹删除业务应用程序	N/A	N/A	在文件夹中写入对象
在文件夹中剪切、复制或粘贴业务应用程序	N/A	N/A	在文件夹中写入对象

备注: 为了将业务应用程序保存到库中用户自己的主目录，例如 `/home/username`，此用户的专用用户组还需要将“管理业务应用程序”权限设置为“是”。有关详细信息，请参见《SA 管理指南》中的“用户组和设置”一章。

查看 SAV 中的存储和 SA 权限

即使用户属于没有权限查看 SAN 网络结构、阵列等存储设备的组，也仍有可能查看 SAV 快照中某些类型的存储信息。

具体而言，如果用户所在的一个或多个组具有权限*管理业务应用程序：读取和写入*，则用户将能够查看 SAV 快照中的设备和对象，例如网络结构（交换机）、存储阵列、网络设备，以及 SAV 快照中的虚拟机信息，即使组没有获得查看这些设备和对象的各个权限也是如此。

如果用户所在的一个或多个组没有*管理业务应用程序：读取和写入*，则仅当组获得各个权限时，用户才能查看 SAN 网络结构（交换机）、存储阵列、网络设备，以及 SAV 快照中的虚拟机信息。

例如，如果用户所在的一个或多个组具有以下权限：*管理业务应用程序：读取和写入*，但具有“管理网络结构：无”，则用户将仍可以查看 SAV 快照中的网络结构（和 SAN 交换机）。

存储可见性与自动化权限

您必须具有特定权限才能使用“存储可见性与自动化”执行操作。有关这些权限的描述，请参见《存储可见性与自动化安装和管理指南》。

SA Web 客户端所需的权限

下表根据可使用 SA Web 客户端执行的任务列出操作/功能权限。

任务 66.SA Web 客户端任务所需的权限

任务	操作/功能权限
OS 配置	
准备 OS	向导：准备 OS
编辑 OS 节点	操作系统
查看服务器池中的服务器	服务器池
服务器管理	
编辑服务器属性	托管的服务器和组
编辑服务器网络属性	托管的服务器和组
编辑服务器自定义特性	托管的服务器和组
停用服务器（代理）	停用
删除服务器	托管的服务器和组
重新分配客户	托管的服务器和组
查看服务器（只读访问权限）	托管的服务器和组
运行服务器通信测试	托管的服务器和组
锁定服务器	托管的服务器和组
设置计划作业以刷新服务器列表	允许运行刷新作业
报告	
创建或查看报告	数据中心智能报告
管理环境	
创建或编辑客户	客户
创建或编辑设施	设施
系统配置	
管理用户和组	（仅 Administrators 组）
定义服务器特性	服务器特性
运行系统诊断工具	系统诊断
管理 SA 系统配置	配置 SA
运行 SA 多控制工具	多主控

任务	操作/功能权限
网关管理	管理网关
其他任务	
运行自定义扩展	向导：自定义扩展
管理流	管理流集成
运行流	运行流

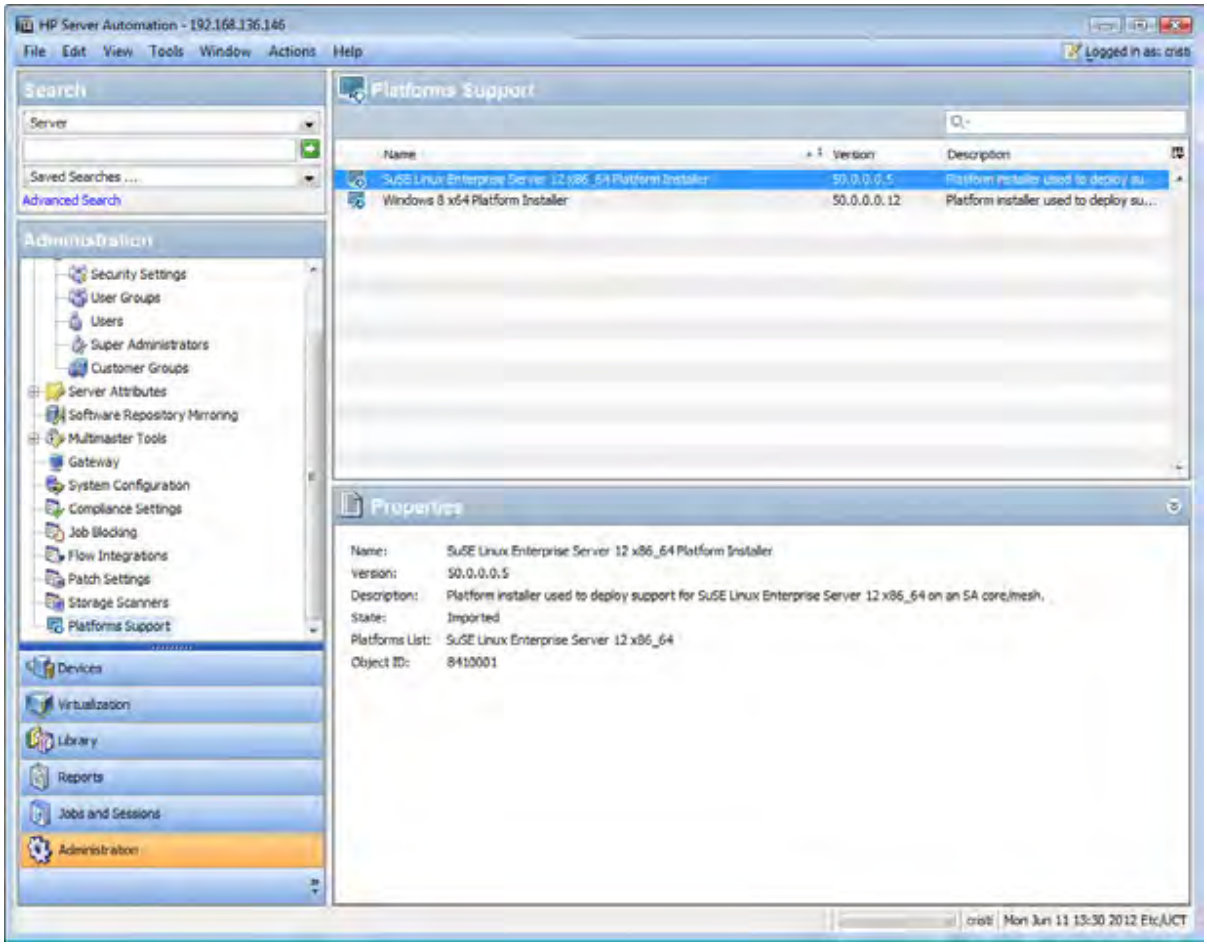
附录 B

托管平台支持

托管平台支持提供了一种向 SA 添加平台的简单方式。托管平台支持允许您自动对整个 SA 核心执行更改，并且降低了重新启动核心组件的需要。

对于每个新的托管平台，HP Live Network (HPLN) 均将提供一个名为平台安装程序的程序 APX。此平台安装程序将对 SA 核心执行必要的操作，以便为每个新的平台添加支持。**图 40** 显示整个新平台程序包的内容：

图 40.托管平台支持的新平台程序包



此附录描述如何导入新的平台程序包并在 SA 核心上部署新平台。

备注: 有关产品支持和兼容性信息，请参见相关产品发布的支持列表。您可以从 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://h20230.www2.hp.com/selfsolve/manuals。

导入新的平台程序包

您可以从 HPLN 单独下载平台程序包并将其导入 SA 核心。

1. 请输入以下 URL，进入 HPLN 门户：

   ```
   https://hpln.hp.com/group/managed-platform-content-server-automation
   ```

2. 此时将显示安装程序列表。将一个安装程序下载到 SA 核心文件系统。
3. 由于安装程序是一个 APX，请使用以下命令将其导入 SA 核心：

   ```
   /opt/opsware/bin/apxtool import <Platform Installer Filename>
   ```

4. 运行平台安装程序。

备注：将平台安装程序导入 SA 核心不会为新平台自动部署支持。平台安装程序必须由 SA 用户运行才能实施更新的信息和更改。下节将描述为新安装的平台部署支持。

为新平台部署支持

本节描述部署新导入的平台所必须执行的操作。

所需的托管的平台权限

要查看 SA 客户端平台支持功能及其平台安装程序列表并运行其中一个安装程序，SA 用户组必须具有“托管的平台”权限。

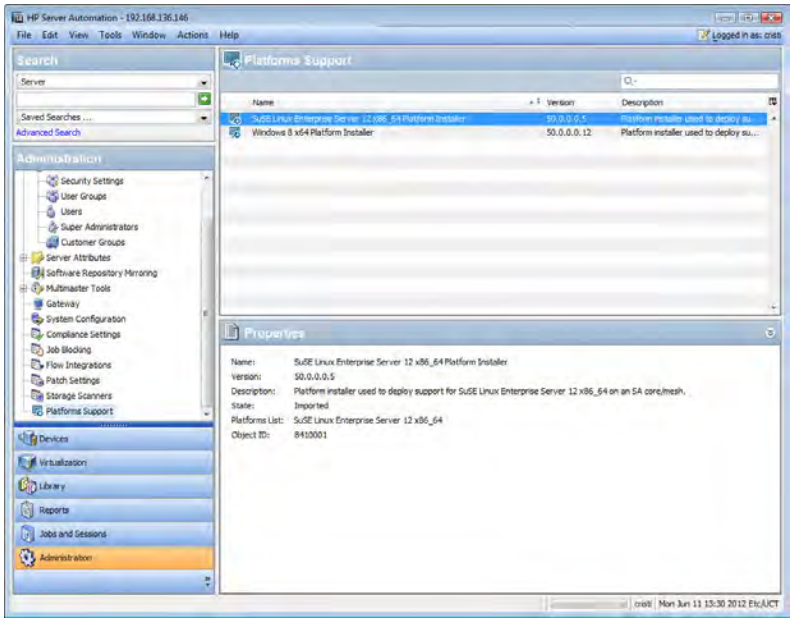
要将此权限分配给某个 SA 用户组，请执行以下操作：

1. 在 SA 客户端中打开此用户组并转到“操作权限”节点。
2. 在右侧面板的“系统管理”类别下，搜索“托管的平台”。
3. 将“托管的平台”设置为“是”，然后保存。

使用平台安装程序

具有“托管的平台”权限后，SA 客户端的“管理”选项卡下将显示“平台支持”条目（请参见**图 42**）。

图 42.平台支持窗口



此窗口列出了 SA 核心上导入的平台安装程序。每个安装程序具有以下特性：

- 名称
- 描述
- 版本
- 将部署的平台列表
- 状态

  平台安装程序的状态，如下：

  - NOT RUN - 安装程序已导入 SA 核心但尚未运行，因此，针对该 OS 的支持不可用。
  - FAILED - 安装程序已导入 SA 核心并且运行，但是运行失败。在这种情况下，仅部分部署对新 OS 的支持，并且在成功运行此安装程序之前，新的 OS 无法使用。
  - INSTALLED - 安装程序已导入 SA 核心并成功运行。同时成功部署对新 OS 的支持，SA 可以使用新的平台。
  - UNKNOWN - 安装程序状态无法确定。

运行平台安装程序

要运行安装程序，您可以执行以下操作：

- 右键单击安装程序并选择“运行...”或
- 选择一个安装程序并从主菜单中选择“操作”>“运行...”。

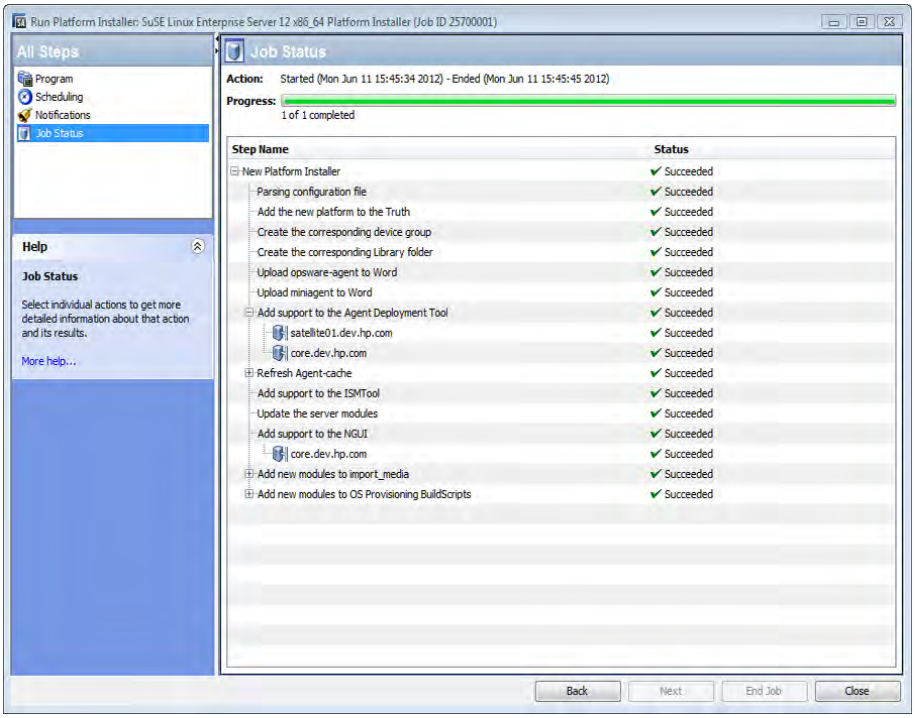
  此时将显示“运行平台安装程序”作业窗口。此窗口提供的选项可用于计划任务在指定时间且无重复周期运行以及设置电子邮件通知。

启动作业后，安装程序将确定网状网络中必须发生的更改并创建一系列步骤（请参见**图 42**）。

某些步骤只能执行一次（例如，“Add the new platform to the Truth”），其他步骤必须在网状网络/核心配置中的多台计算机上运行（例如，“Add support to the Agent Deployment Tool”）。

- 选择每个步骤时，将可以查看捕获的 **stdout** 和 **stderr** 文件。如果一个步骤必须在多台计算机上运行，则其在作业结果窗口中的对应节点将针对每台计算机具有一个子节点。
- 选择该子节点时，将可以查看在该特定计算机上运行此步骤而生成的 **stdout** 和 **stderr** 文件。

图 42.运行平台安装程序作业状态窗口



删除平台安装程序

要删除安装程序，您可以执行以下操作：

- 右键单击安装程序并选择“删除”或
- 选择一个安装程序并从主菜单中选择“操作”>“删除”。

删除安装程序并不意味着删除对该 OS 的支持（如果已在 SA 核心中部署该支持）。因此，在导入并运行平台安装程序后，可以安全地删除该安装程序，不会丢失 SA 中对该新 OS 的支持。

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：

《SA 管理指南》(Server Automation 10.2) 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 sa-docs@hp.com。

我们感谢您提出宝贵的意见！