Oracle® Secure Global Desktop

Gateway 发行版 4.7 管理指南

E35904-01
2012 年 8 月

Oracle® Secure Global Desktop: Gateway 发行版 4.7 管理指南

摘要

本指南介绍了如何安装、配置和操作 Oracle Secure Global Desktop Gateway。

文档生成日期： 2012-10-18 (revision: 1179)

目录

前言

《Oracle Secure Global Desktop Gateway 发行版 4.7 管理指南》提供了有关安装、配置和操作 Oracle Secure Global Desktop (SGD Gateway) 的说明。本文档是为系统管理员编写的。

1. 目标读者

本文档的目标读者是 SGD Gateway 的新用户。本文档假定读者熟悉 Web 技术，并对 Windows 和 UNIX 平台有一般性的了解。

2. 文档结构

本文档的结构如下所示：

- 第 1 章 安装 SGD Gateway介绍如何安装 SGD Gateway。
- 第 2 章 配置 SGD Gateway介绍如何为您的网络配置 SGD Gateway。
- 附录 A, SGD Gateway 体系结构概述介绍 SGD Gateway 的体系结构。
- 附录 B, 命令行参考介绍如何从命令行配置和控制 SGD Gateway。
- 附录 C, 高级配置介绍 SGD Gateway 的高级配置，包括如何配置和使用 SGD Gateway 的反射服务。
- 附录 D, SGD Gateway 故障排除包括故障排除信息，以帮助您诊断和修复 SGD Gateway 的问题。

3. 文档辅助功能

Oracle 致力于提高辅助功能，有关信息请访问 Oracle 辅助功能计划网站，网址为：http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc。

获取 Oracle 支持

Oracle 客户可通过 My Oracle Support 获取电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如有听力障碍，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

4. 相关文档

可从以下位置访问此产品的文档：

http://www.oracle.com/technetwork/documentation/sgd-193668.html

有关更多信息，请参见以下手册：

- 《Oracle Secure Global Desktop Administration Guide for Release 4.7》
- 《Oracle Secure Global Desktop 发行版 4.7 安装指南》
- 《Oracle Secure Global Desktop 发行版4.7 用户指南》
- 《Oracle Secure Global Desktop 发行版 4.7 平台支持和发行说明》
- 《Oracle Secure Global Desktop Security Guide for Release 4.7》

5. 约定

本文档中使用了以下文本约定。

约定	含义
粗体	粗体类型用于指示与操作相关的图形用户界面元素，或者在文本或词汇表中定义的术语。

约定	含义
斜体	斜体类型用于指示书名、重点内容或要为其提供特定值的占位符变量。
等宽字体	等宽字体类型用于指示段落、URL、示例中代码、屏幕显示文本或您输入的文本中的命令。

第 1 章 安装 SGD Gateway

以下是对 Oracle Secure Global Desktop Gateway (SGD Gateway) 的简要介绍，本章说明了如何安装 SGD Gateway 软件。本章还详细介绍了 SGD Gateway 的系统要求。

本章包括以下主题：

1.1. 关于 SGD Gateway

SGD Gateway 是一种代理服务器，用于部署在隔离区 (Demilitarized Zone, DMZ) 中 SGD 阵列的前端。这使得 SGD 阵列能够位于组织的内部网络中。此外，在与阵列中的 SGD 服务器建立连接之前，可以先在 DMZ 中对所有连接进行验证。

使用 SGD Gateway 可以代替运行 SGD 服务器搭配防火墙穿越（也称为防火墙转发）功能。

SGD Gateway 可管理 HTTP 连接的负载平衡，因此，您无需使用 SGD 随附的 JavaServer Pages (JSP) 技术负载平衡页面。

1.2. 系统要求

《Oracle Secure Global Desktop 发行版 4.7 平台支持和发行说明》中列出了支持的 SGD Gateway 主机安装平台，该文档位于 http://www.oracle.com/technetwork/documentation/sgd-193668.html。

对于与 SGD Gateway 配合使用的 SGD 服务器，需要满足以下要求：

- 安全模式。默认情况下，SGD Gateway 使用到 SGD 服务器的安全连接。SGD 服务器必须启用安全连接。绝对不要启用防火墙转发。

  在标准安装中，SGD 服务器将自动配置为使用安全连接。如果需要有关如何保护 SGD 服务器安全的信息，请参见《Oracle Secure Global Desktop Administration Guide for Release 4.7》第 1 章中的 "Secure Connections to SGD Servers"。

- SGD 版本。SGD 服务器必须至少运行 4.5 版的 SGD。最好将 4.7 版的 Gateway 与 4.7 版的 SGD 配合使用。

- 时钟同步。请务必使 SGD 服务器上的系统时钟与 SGD Gateway 上的系统时钟保持同步。使用网络时间协议 (Network Time Protocol, NTP) 软件或 rdate 命令来确保时钟同步。

有关 SGD 服务器系统要求的更多信息，请参见《Oracle Secure Global Desktop 发行版 4.7 平台支持和发行说明》。

1.2.1. 已知问题

有关此 SGD Gateway 发行版的已知问题的详细信息，请参见《Oracle Secure Global Desktop 发行版 4.7 平台支持和发行说明》。

1.3. 执行安装

在 Oracle Solaris 平台上，请使用 pkgadd 命令安装 SGD Gateway。

在 Linux 平台上，请使用 rpm 命令安装 SGD Gateway。

默认情况下，SGD Gateway 安装在 /opt/SUNWsgdg 目录中。您可以按如下方式更改安装目录：

- Oracle Solaris 平台 - 当您安装本软件时，安装程序会要求您指定安装目录。
- Linux 平台 - 当您安装本软件时，可使用带 --prefix 选项的 rpm 命令选择一个不同的安装目录。

1.3.1. 如何安装 SGD Gateway

1. 将 SGD Gateway 软件包保存到主机上的一个临时目录中。

   如果您是从安装介质进行安装，则软件包位于 gateway 目录中。

   或者，也可以通过 SGD Web 服务器从 https://server.example.com 下载安装程序，其中 server.example.com 是 SGD 服务器的名称。显示 SGD Web 服务器欢迎页后，单击 "Install the Oracle Secure Global Desktop Gateway"（安装 Oracle Secure Global Desktop Gateway）。

   软件包文件包括：

   - SUNWsgdg-version.sol-x86.pkg（适用于 x86 平台上的 Oracle Solaris）
   - SUNWsgdg-version.sol-sparc.pkg（适用于 SPARC 技术平台上的 Oracle Solaris）
   - SUNWsgdg-version.i386.rpm（适用于 Linux 平台）

   其中 version 是 SGD Gateway 的版本号。

2. 在主机上，以超级用户 (root) 身份登录。

3. 安装 SGD Gateway。

   如果软件包文件是压缩文件，则在安装之前必须先解压缩。

   在 x86 平台上的 Oracle Solaris 中安装：

   ```
   # pkgadd -d /tempdir/SUNWsgdg-version.sol-x86.pkg
   ```

   在 SPARC 技术平台上的 Solaris OS 中安装：

   ```
   # pkgadd -d /tempdir/SUNWsgdg-version.sol-sparc.pkg
   ```

   注意

   在 Oracle Solaris 平台上，如果安装失败，且错误消息为 "pwd: cannot determine current directory!"，请转至 /tempdir 目录并重试。

   在 Linux 平台上安装：

   ```
   # rpm -Uvh /tempdir/SUNWsgdg-version.i386.rpm
   ```

4. 检验是否已在软件包数据库中注册了 SGD Gateway 软件包。

   在 Oracle Solaris 平台上：

   ```
   # pkginfo -x SUNWsgdg
   ```

   在 Linux 平台上：

   ```
   # rpm -qa | grep -i SUNWsgdg
   ```

5. 运行 SGD Gateway 安装程序。

   ```
   # /opt/SUNWsgdg/bin/gateway setup
   ```

   SGD Gateway 安装程序会提供以下设置，您可以接受或更改它们：

   - SGD Gateway 端口设置。SGD Gateway 用于传入连接的接口和端口。默认情况下，SGD Gateway 侦听所有接口上的 443 端口。

- 网络入口点。客户端设备用于连接到 SGD Gateway 的 Internet 协议 (Internet Protocol, IP) 地址或域名系统 (Domain Name System, DNS) 名称和端口。它并非总是与 SGD Gateway 的地址相同。可以是负载平衡器的地址，也可以是其他外部设备的地址，具体取决于网络配置。

  例如，如果用户直接连接到位于 gateway1.example.com 处的 SGD Gateway，则为网络入口点键入 gateway1.example.com:443。

  如果用户通过位于 lb.example.com 处的负载平衡器连接到 SGD Gateway，则为网络入口点键入 lb.example.com:443。

- 安全连接。是否保护 SGD Gateway 与阵列中的 SGD 服务器之间的连接安全。默认情况下，SGD Gateway 使用安全连接。要使用安全连接，阵列中的 SGD 服务器必须在安全模式下运行。

  有关对阵列中的 SGD 服务器使用未加密连接的更多信息，请参见第 C.4 节 “使用未加密的 SGD 阵列连接”。

注意

以后可以通过使用 gateway config create 命令更改这些设置。请参见第 2.2.1.1 节 “如何配置 SGD Gateway 的端口和连接”。

安装本软件后，必须执行 SGD Gateway 的其他配置。有关所需执行的操作的详细信息，请参见第 2 章 配置 SGD Gateway。

1.4. 升级 SGD Gateway

本节介绍如何升级 SGD Gateway。

升级 SGD Gateway 时，将保留您的大部分初始配置，例如路由代理配置文件。不过，升级过程会覆盖 Gateway 使用的任何自签名证书。

升级后，您必须重新配置 SGD Gateway。请按照第 2.2.2.2 节 “如何在 SGD 阵列上安装 SGD Gateway 证书”中所述的标准配置步骤向 SGD 授权一个 Gateway。

升级日志是在 /opt/SUNWsgdg/proxy/var/log/upgrade_oldversion_newversion.log 中创建的，其中 oldversion 是旧版本的 SGD Gateway，newversion 是已升级版本的 SGD Gateway。

升级时，SGD Gateway 安装程序会备份其检测到的所有定制 Apache Web 服务器文件并将这些文件列在升级日志中。您必须手动升级这些文件。您可以使用 diff 之类的实用程序来比较这些文件并显示所做的更改。

1.4.1. 如何升级 SGD Gateway

1. 确保没有任何用户会话和应用程序会话正通过 SGD Gateway 运行。
2. 安装 SGD Gateway 的新版本。

   请参见第 1.3.1 节 “如何安装 SGD Gateway”。

第 2 章 配置 SGD Gateway

本章介绍如何针对典型部署方案配置 Oracle Secure Global Desktop Gateway (SGD Gateway)。本章还介绍了如何启动和停止 SGD Gateway 并说明了如何删除 SGD Gateway 软件。

本章包括以下主题：

2.1. 部署 SGD Gateway

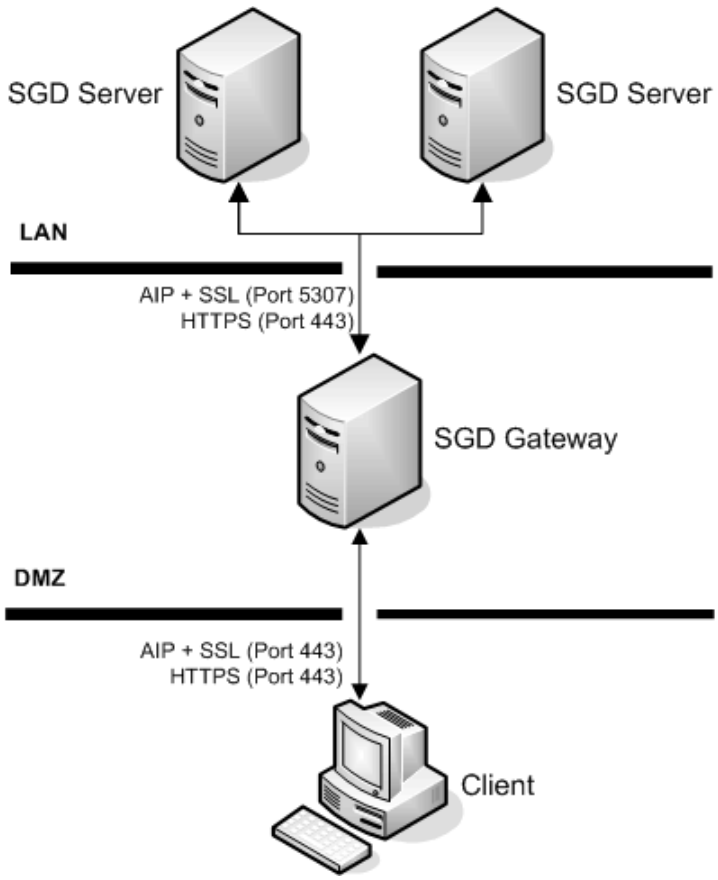
本节介绍以下 SGD Gateway 部署方案：

2.1.1. 基本部署

本节介绍适用于 SGD Gateway 基本部署的配置任务。

基本部署使用一个 SGD Gateway，如图 2.1 “使用一个 SGD Gateway 的基本部署”中所示。

图 2.1. 使用一个 SGD Gateway 的基本部署



配置基本部署涉及配置表 2.1 “用于 SGD Gateway 基本部署的连接”中所显示的连接。

表 2.1. 用于 SGD Gateway 基本部署的连接

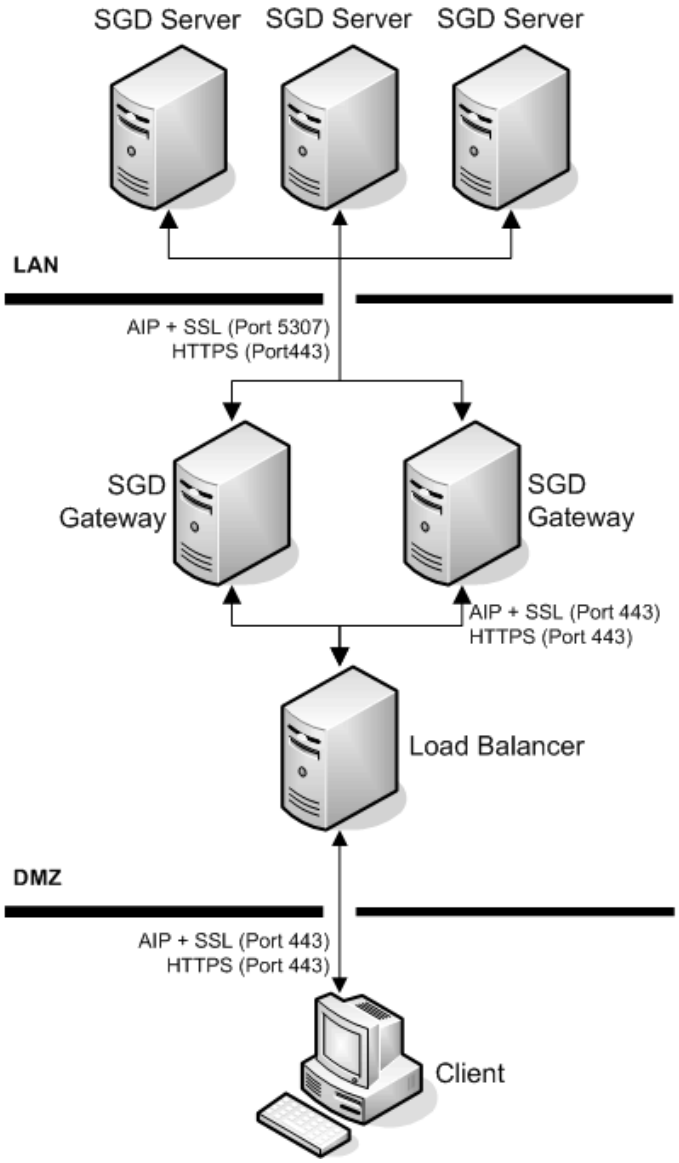
连接	配置步骤
客户端设备到 SGD Gateway	1. 配置 SGD Gateway 使用的端口和连接。 在安装 SGD Gateway 时已配置这些设置。 如果要更改 SGD Gateway 的配置，请参见第 2.2.1.1 节 “如何配置 SGD Gateway 的端口和连接”。 2. 在 SGD Gateway 上，安装用于客户端连接的安全套接字层 (Secure Sockets Layer, SSL) 证书。 请参见第 2.2.1.2 节 “如何将用于客户端连接的 SSL 证书安装到客户端密钥库中”。
SGD Gateway 到 SGD 服务器	1. 为阵列启用 SGD 安全服务。 SGD 服务器必须在安全模式下运行。绝对不要启用防火墙转发。 在标准安装中，SGD 服务器将自动配置为使用安全连接。如果需要有关如何保护 SGD 服务器安全的信息，请参见《Oracle Secure Global Desktop Administration Guide for Release 4.7》第 1 章中的 "Secure Connections to SGD Servers"。 2. 在 SGD Gateway 上，安装 SGD 服务器的安全证书。 使用 gateway server 命令将阵列中 SGD 服务器的 CA 证书和 SSL 证书导入到 SGD Gateway 密钥库中。 请参见第 2.2.2.1 节 “如何安装 SGD 服务器证书”。 3. 将阵列中的 SGD 服务器设置为使用 SGD Gateway。 在 SGD 阵列上安装 SGD Gateway 证书，并使用 tarantella gateway add 命令将 SGD Gateway 注册到 SGD 阵列中。 请参见第 2.2.2.2 节 “如何在 SGD 阵列上安装 SGD Gateway 证书”。 4. 配置哪些 SGD Client 连接可以使用 SGD Gateway。 请参见第 2.2.2.3 节 “如何配置 SGD Client 连接”。

2.1.2. 负载平衡部署

本节介绍适用于 SGD Gateway 负载平衡部署的配置任务。

负载平衡部署使用多个 SGD Gateway 和一个负载平衡器作为网络入口点，如图 2.2 “使用多个 SGD Gateway 和一个负载平衡器的网络部署”中所示。

图 2.2. 使用多个 SGD Gateway 和一个负载平衡器的网络部署



配置负载平衡部署涉及配置表 2.2 “用于 SGD Gateway 负载平衡部署的连接”中所显示的连接。

表 2.2. 用于 SGD Gateway 负载平衡部署的连接

连接	配置任务
客户端设备到负载平衡器	1. 启用来自客户端设备的传入连接。 通常，此操作使用 TCP 端口 443。 有关如何执行此操作的详细信息，请参见所用负载平衡器的文档。 2. （可选）在负载平衡器上，安装 SGD Gateway 用于客户端连接的 SSL 证书。 有关如何执行此操作的详细信息，请参见所用负载平衡器的文档。
负载平衡器到 SGD Gateway	1. 配置负载平衡器以将连接转发给 SGD Gateway。 有关如何执行此操作的详细信息，请参见所用负载平衡器的文档。

连接	配置任务
	2. 配置 SGD Gateway 使用的端口和连接。 将网络入口点设置为负载平衡器的地址。 在安装 SGD Gateway 时已配置这些设置。 如果要更改 SGD Gateway 的配置，请参见第 2.2.1.1 节 “如何配置 SGD Gateway 的端口和连接”。 3. 在每个 SGD Gateway 上，安装用于客户端连接的 SSL 证书。 请参见第 2.2.1.2 节 “如何将用于客户端连接的 SSL 证书安装到客户端密钥库中”。
SGD Gateway 到 SGD 服务器	1. 为 SGD 阵列启用 SGD 安全服务。 SGD 服务器必须在安全模式下运行。绝对不要启用防火墙转发。 在标准安装中，SGD 服务器将自动配置为使用安全连接。如果需要有关如何保护 SGD 服务器安全的信息，请参见《Oracle Secure Global Desktop Administration Guide for Release 4.7》第 1 章中的 "Secure Connections to SGD Servers"。 2. 在 SGD Gateway 上，安装 SGD 服务器的安全证书。 使用 gateway server 命令将阵列中 SGD 服务器的 CA 证书和 SSL 证书导入到 SGD Gateway 密钥库中。 请参见第 2.2.2.1 节 “如何安装 SGD 服务器证书”。 3. 将阵列中的 SGD 服务器设置为使用 SGD Gateway。 在 SGD 阵列上安装 SGD Gateway 证书，并使用 tarantella gateway add 命令将 SGD Gateway 注册到 SGD 阵列中。 请参见第 2.2.2.2 节 “如何在 SGD 阵列上安装 SGD Gateway 证书”。 4. 配置哪些 SGD Client 连接可以使用 SGD Gateway。 请参见第 2.2.2.3 节 “如何配置 SGD Client 连接”。

2.2. SGD Gateway 配置任务

本节说明如何配置 SGD Gateway 使用的连接。

介绍了以下配置任务：

- 第 2.2.1 节 “客户端设备到 SGD Gateway 的连接”
- 第 2.2.2 节 “SGD Gateway 到 SGD 服务器的连接”
- 第 2.2.3 节 “客户端设备到负载平衡器的连接”
- 第 2.2.4 节 “负载平衡器到 SGD Gateway 的连接”

2.2.1. 客户端设备到 SGD Gateway 的连接

配置客户端设备与 SGD Gateway 之间的连接涉及以下配置任务：

1. （可选）配置 SGD Gateway 使用的端口和连接。

   在安装 SGD Gateway 时配置了这些设置。

要更改这些设置，请参见第 2.2.1.1 节 “如何配置 SGD Gateway 的端口和连接”。

2. （可选）在 SGD Gateway 上，安装用于客户端连接的 SSL 证书。

   请参见第 2.2.1.2 节 “如何将用于客户端连接的 SSL 证书安装到客户端密钥库中”。

2.2.1.1. 如何配置 SGD Gateway 的端口和连接

仅当要更改安装 SGD Gateway 期间进行的设置时才需要执行此过程。

1. 在 SGD Gateway 主机上，以超级用户 (root) 身份登录。
2. 运行 gateway config create 命令。

```
# /opt/SUNWsgdg/bin/gateway config create
```

   回答屏幕上的问题以配置以下各项：

   - SGD Gateway 端口设置。SGD Gateway 用于传入连接的接口和端口。
   - 网络入口点。客户端设备用于连接到 SGD Gateway 的 IP 地址或 DNS 名称和端口。它并非总是与 SGD Gateway 的地址相同。可以是负载平衡器的地址，也可以是其他外部设备的地址，具体取决于网络配置。
   - 安全连接。是否保护 SGD Gateway 与阵列中的 SGD 服务器之间的连接安全。要使用安全连接，阵列中的 SGD 服务器必须在安全模式下运行。

3. 保存连接和端口设置。

   SGD Gateway 将使用输入的设置进行配置。

2.2.1.2. 如何将用于客户端连接的 SSL 证书安装到客户端密钥库中

SGD Gateway 用于客户端连接的 SSL 证书称为 SGD Gateway SSL 证书。SSL 证书存储在客户端密钥库 /opt/SUNWsgdg/proxy/etc/keystore.client 中。

默认情况下，SGD Gateway 使用自签名 SGD Gateway SSL 证书进行客户端连接，但是，您可以将自签名 SSL 证书替换为证书颁发结构 (Certificate Authority, CA) 签名的证书。

以下过程假定您拥有 CA 签名的 SSL 证书。

安装的私钥必须采用保密性增强的电子邮件 (Privacy Enhanced Mail, PEM) 格式。

1. 在 SGD Gateway 主机上，以超级用户 (root) 身份登录。
2. 将 SSL 证书和相应的私钥复制到 SGD Gateway 主机。
3. 将 SSL 证书和私钥导入到客户端密钥库中。

   按如下方式使用 gateway sslkey import 命令：

```
# /opt/SUNWsgdg/bin/gateway sslkey import \
--keyfile temp.key \
--keyalg RSA \
--certfile example.com.pem
```

   此时，证书文件 example.com.pem 和 RSA 编码的相应私钥 temp.key 将导入到客户端密钥库中。

   客户端密钥库中的现有自签名 SSL 证书将被覆盖。

4. （可选）重新启动 SGD Gateway。

小心

此步骤只能在不执行 SGD Gateway 初始配置时执行。如果在初始配置阶段重新启动 SGD Gateway，则会显示一条错误消息，因为 SGD Gateway 的初始配置尚未完成。

如果要替换已配置且正在运行的 SGD Gateway 上的 SSL 证书，请重新启动 SGD Gateway。

注意

重新启动 SGD Gateway 将断开正通过 SGD Gateway 运行的所有用户会话和应用程序会话的连接。

在 SGD Gateway 主机上，运行以下命令：

```
# /opt/SUNWsgdg/bin/gateway restart
```

2.2.2. SGD Gateway 到 SGD 服务器的连接

SGD Gateway 与阵列中的 SGD 服务器之间的连接使用证书进行相互授权。配置这些连接涉及以下配置任务：

1. 在 SGD Gateway 上安装 SGD 服务器证书。

   请参见第 2.2.2.1 节 “如何安装 SGD 服务器证书”。

2. 在 SGD 阵列上安装 SGD Gateway 证书。

   请参见第 2.2.2.2 节 “如何在 SGD 阵列上安装 SGD Gateway 证书”。

3. 配置 SGD Gateway 的 SGD Client 连接。

   请参见第 2.2.2.3 节 “如何配置 SGD Client 连接”。

2.2.2.1. 如何安装 SGD 服务器证书

要执行此过程，阵列中的 SGD 服务器必须在安全模式下运行。

在标准安装中，SGD 服务器将自动配置为使用安全连接。如果需要有关如何在 SGD 服务器上启用安全服务的更多信息，请参见《Oracle Secure Global Desktop Administration Guide for Release 4.7》第 1 章中的 “Secure Connections to SGD Servers”。

对阵列中的每个 SGD 服务器重复以下过程。

1. 在 SGD 主机上，以超级用户 (root) 身份登录。
2. 将 CA 证书从 SGD 服务器复制到 SGD Gateway 密钥库目录。

   SGD 服务器的 CA 证书位于 SGD 主机的 /opt/tarantella/var/info/certs/PeerCAcert.pem 中。

   注意

   此证书与 SGD 服务器用于阵列内安全通信的 CA 证书相同。

   SGD Gateway 密钥库目录为 /opt/SUNWsgdg/proxy/etc。

   复制 CA 证书时，最佳做法是重命名证书文件，以便您可以标识该文件所包含的内容及其所源自的 SGD 服务器。

3. 将 SSL 证书从 SGD 服务器复制到 SGD Gateway 密钥库目录。

   在安全模式下运行的 SGD 服务器的 SSL 证书位于 SGD 主机的 /opt/tarantella/var/tsp/cert.pem 中。

   SGD Gateway 密钥库目录为 /opt/SUNWsgdg/proxy/etc。

   复制 SSL 证书时，最佳做法是重命名证书文件，以便您可以标识该文件所包含的内容及其所源自的 SGD 服务器。

4. 在 SGD Gateway 主机上，以超级用户 (root) 身份登录。
5. 将证书导入到 SGD Gateway 密钥库中。

```
# /opt/SUNWsgdg/bin/gateway server add --server sgd-server1 \
--certfile /opt/SUNWsgdg/proxy/etc/PeerCAcert.pem --url https://sgd1.example.com \
--ssl-certfile /opt/SUNWsgdg/proxy/etc/cert.pem
```

--server 选项定义在密钥库中存储证书时使用的别名。在此示例中，使用 sgd-server1 别名存储 CA 证书，使用 sgd-server1-ssl 别名存储 SSL 证书。

https://sgd1.example.com 是 SGD Web 服务器的 URL。

6. 重新启动 SGD Gateway。

注意

重新启动 SGD Gateway 将断开正通过 SGD Gateway 运行的所有用户会话和应用程序会话的连接。

在 SGD Gateway 主机上，运行以下命令：

```
# /opt/SUNWsgdg/bin/gateway restart
```

2.2.2.2. 如何在 SGD 阵列上安装 SGD Gateway 证书

对每个 SGD Gateway 重复以下过程。

1. 导出 SGD Gateway 证书。
   a. 在 SGD Gateway 主机上，以超级用户 (root) 身份登录。
   b. 从 SGD Gateway 密钥库导出 SGD Gateway 证书。

      按如下方式使用 gateway cert export 命令：

      ```
      # /opt/SUNWsgdg/bin/gateway cert export --certfile gateway1.pem
      ```

      证书将导出至 gateway1.pem 文件中。
   c. 将证书复制到阵列中主 SGD 服务器的 /opt/tarantella/var/tsp 目录中。

      导出证书时，最佳做法是为证书文件指定合适的名称，以便您可以标识其所源自的 SGD Gateway。
   d. 更改 Gateway 证书的文件权限和所有权。

      ```
      # chmod 600 /opt/tarantella/var/tsp/gateway1.pem
      # chown ttasys:ttaserv /opt/tarantella/var/tsp/gateway1.pem
      ```
2. 将 SGD Gateway 注册到 SGD 阵列中。
   a. 在主 SGD 服务器上，以超级用户 (root) 身份登录。
   b. 导入 SGD Gateway 证书。

      ```
      # tarantella gateway add --name sgd-gateway1 \
      --certfile /opt/tarantella/var/tsp/gateway1.pem
      ```

      其中，sgd-gateway1 是 SGD 用于标识 SGD Gateway 的名称，gateway1.pem 是 SGD Gateway 证书的文件名。

      要同时注册多个 SGD Gateway，请使用带 --file 选项的 tarantella gateway add 命令。有关更多详细信息，请参见第 B.27 节 “tarantella gateway 命令”。

      使用 tarantella gateway add 所做的配置更改将复制到阵列中的其他 SGD 服务器。

2.2.2.3. 如何配置 SGD Client 连接

1. 配置使用 SGD Gateway 的 SGD Client 连接。

在主 SGD 服务器上，设置 --security-gateway 全局属性以基于 SGD Client 的 IP 地址或 DNS 名称定义哪些 SGD Client 可以使用 SGD Gateway。

要指定所有 SGD Client 连接都通过一个 SGD Gateway (gateway1.example.com) 的 TCP 端口 443 进行路由，请使用以下命令：

```
$ tarantella config edit --security-gateway \
"*:sgdg:gateway1.example.com:443"
```

要指定所有 SGD Client 连接都通过一个外部负载平衡器 (lb.example.com) 的 TCP 端口 443 进行路由，请使用以下命令：

```
$ tarantella config edit --security-gateway \
"*:sgdg:lb.example.com:443"
```

注意

对 --security-gateway 属性的更改会影响阵列中的所有 SGD 服务器。更改仅应用于新用户会话。

有关如何使用 --security-gateway 属性定义多个 SGD Client 连接过滤器的更多详细信息，请参见第 B.31 节 “--security-gateway 属性”。

2.2.3. 客户端设备到负载平衡器的连接

配置客户端设备与外部负载平衡器之间的连接涉及以下配置任务：

1. 配置负载平衡器以接受来自客户端设备的连接。

   有关如何执行此操作的详细信息，请参见所用负载平衡器的文档。

2. （可选）将 SGD Gateway 的 SSL 证书安装到负载平衡器上。

   有关如何执行此操作的详细信息，请参见所用负载平衡器的文档。

2.2.4. 负载平衡器到 SGD Gateway 的连接

配置外部负载平衡器与 SGD Gateway 之间的连接涉及以下配置任务：

1. 配置 SGD Gateway 使用的端口和连接。

   请参见第 2.2.1.1 节 “如何配置 SGD Gateway 的端口和连接”。

2. （可选）在 SGD Gateway 上，安装用于传入客户端连接的 SSL 证书。

   请参见第 2.2.1.2 节 “如何将用于客户端连接的 SSL 证书安装到客户端密钥库中”。

2.3. 控制 SGD Gateway

本节介绍如何控制 SGD Gateway。介绍了以下任务：

- 启动 SGD Gateway
- 停止 SGD Gateway
- 重新启动 SGD Gateway

2.3.1. 启动 SGD Gateway

要启动 SGD Gateway，请使用以下命令：

```
# /opt/SUNWsgdg/bin/gateway start
```

2.3.2. 停止 SGD Gateway

小心

停止 SGD Gateway 将断开正通过 SGD Gateway 运行的所有用户会话和应用程序会话的连接。这意味着如果意外停止 SGD Gateway，应用程序数据可能会丢失。

要停止 SGD Gateway，请使用以下命令：

```
# /opt/SUNWsgdg/bin/gateway stop
```

在使用 gateway stop 命令时，会显示一条警告消息，提示您确认要停止 SGD Gateway。如果不希望显示此消息，请使用带 --force 选项的 gateway stop 命令。

注意

如果停止 SGD Gateway，网络外部的用户将无法使用 SGD Gateway 连接到 SGD。使用 --security-gateway 属性启用了不通过 SGD Gateway 直接访问 SGD 的客户端设备仍可以访问 SGD。请参见第 B.31 节 “--security-gateway 属性”。

2.3.3. 重新启动 SGD Gateway

小心

重新启动 SGD Gateway 将断开正通过 SGD Gateway 运行的所有用户会话和应用程序会话的连接。这意味着如果意外重新启动 SGD Gateway，应用程序数据可能会丢失。

要重新启动 SGD Gateway，请使用以下命令：

```
# /opt/SUNWsgdg/bin/gateway restart
```

在使用 gateway restart 命令时，会显示一条警告消息，提示您确认要停止 SGD Gateway。如果不希望显示此消息，请使用带 --force 选项的 gateway restart 命令。

2.4. 删除 SGD Gateway

要删除 SGD Gateway，请删除 SGD Gateway 主机上安装的软件。

2.4.1. 如何删除 SGD Gateway

1. 在 SGD Gateway 主机上，以超级用户 (root) 身份登录。
2. 更改 SGD 阵列的 SGD Client 路由配置。
   a. 在主 SGD 服务器上以超级用户 (root) 身份登录。
   b. 编辑 SGD 阵列的 --security-gateway 属性。

      对于使用一个 SGD Gateway 的基本部署，请运行以下命令：

      ```
      # tarantella config edit --security-gateway ""
      ```

      注意

      对于使用多个 SGD Gateway 和一个外部负载平衡器的负载平衡部署，无需编辑 --security gateway 属性。
3. 卸载 SGD Gateway。

   运行以下命令：

   ```
   # /opt/SUNWsgdg/bin/gateway uninstall
   ```

将显示一条警告消息，提示您确认要停止 SGD Gateway。

小心

gateway uninstall 命令是用于删除 SGD Gateway 的唯一受支持的方法。请不要直接使用 pkgrm 或 rpm 命令来删除 SGD Gateway。

4. （可选）从 SGD 阵列的注册 SGD Gateway 列表中删除 SGD Gateway。

   a. 显示 SGD 阵列的注册 SGD Gateway。

```
# tarantella gateway list
Installed gateway: gateway1.example.com
Issuer: CN=gateway1.example.com, OU=Marketing, O=Example, L=Boston,
ST=Massachusetts, C=US
Serial Number: 1208509056
Subject: CN=gateway2.example.com, OU=Marketing, O=Example, L=Boston,
ST=Massachusetts, C=US
Valid from Fri Sep 26 09:57:36 GMT 2008 to Thu Dec 25 09:57:36 GMT 2008
```

   b. 从 SGD 阵列的注册 SGD Gateway 列表中删除 SGD Gateway。

```
# tarantella gateway remove --name gateway1.example.com
```

附录 A. SGD Gateway 体系结构概述

本章介绍 Oracle Secure Global Desktop Gateway (SGD Gateway) 的体系结构及其主要组件。

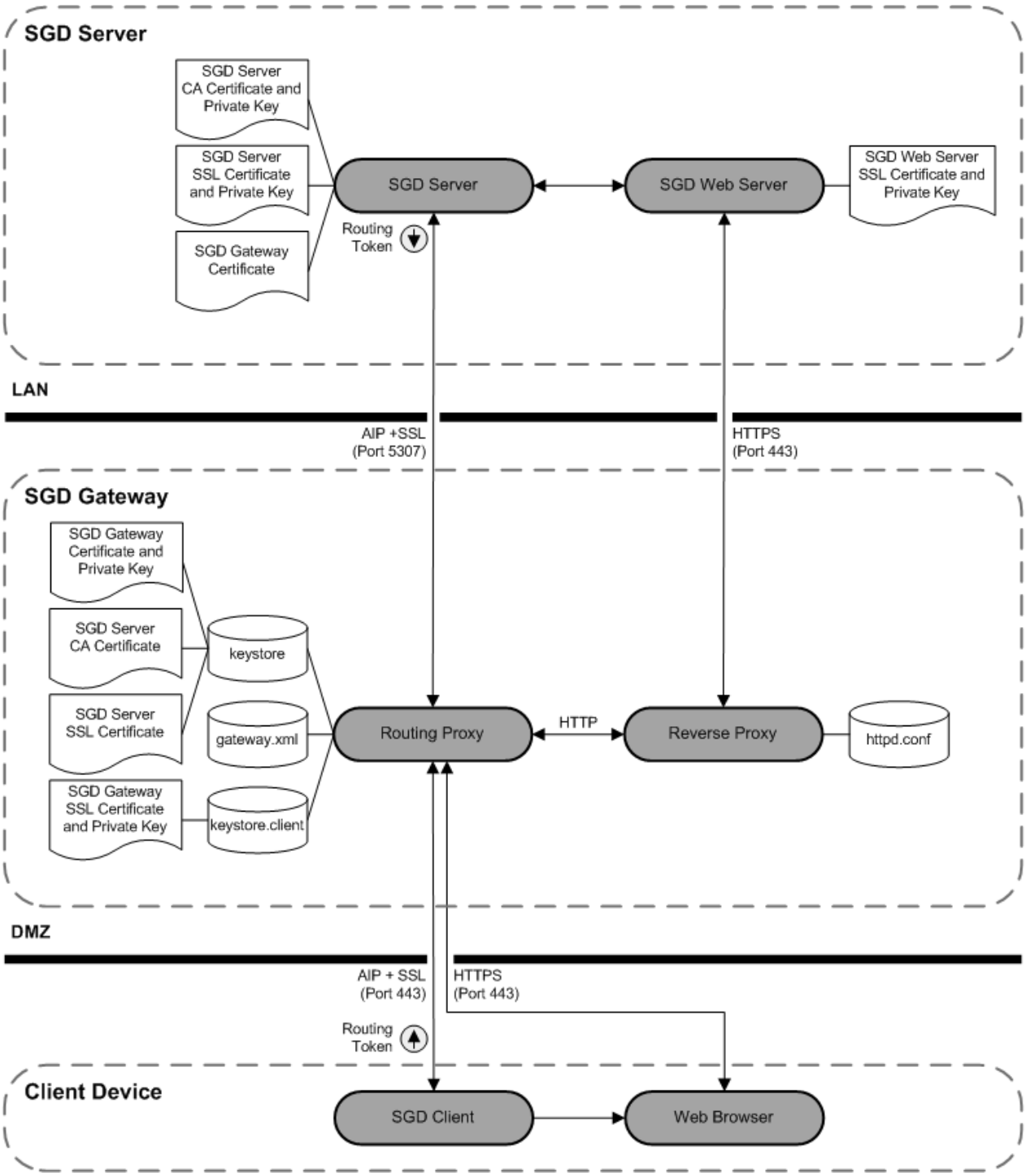
本章包括以下主题：

A.1. SGD Gateway 体系结构

本节探讨 SGD Gateway 的体系结构，并介绍有关通过 SGD Gateway 访问 SGD 时建立的连接。

图 A.1 “SGD Gateway 体系结构”显示了 SGD Gateway 的体系结构。

图 A.1. SGD Gateway 体系结构



以下步骤介绍了通过 SGD Gateway 访问 SGD 时建立的连接。这些步骤包含使用浏览器与 SGD 建立初始连接、登录 SGD，直至启动应用程序。

1. 客户端设备上的浏览器在 TCP 端口 443 上与 SGD Gateway 建立安全套接字层上的 HTTP (HTTP over Secure Sockets Layer, HTTPS) 连接。

   - 对于基本部署，用户可以通过转至 SGD Gateway 的 URL 来访问 SGD。

- TCP 端口 443 是 SGD Gateway 的默认端口。SGD Gateway 使用的端口是使用路由代理配置文件 gateway.xml 定义的。此文件在安装 SGD Gateway 期间自动创建，并在使用 gateway config 命令更改 SGD Gateway 配置时进行更新。
- SGD Gateway 提供 SSL 证书。该证书是 SGD Gateway 上 keystore.client 密钥库中的唯一一个条目。
- SGD Gateway 使用的密钥库的位置和密码是在路由代理配置文件 gateway.xml 中定义的。

2. 路由代理识别 HTTPS 连接，解密数据流，并将 HTTP 数据转发到 Apache 反向代理。
   - HTTP 数据在内部通过 TCP 端口 8080 以上的第一个空闲端口发送。
   - Apache 反向代理的配置是由 httpd.conf 文件定义的。该文件和相关反向代理配置文件在安装 SGD Gateway 期间自动创建。该文件在使用 gateway config 命令更改 SGD Gateway 配置时进行更新。
3. 反向代理使用 HTTP 负载平衡在阵列中选择 SGD Web 服务器。
   - 使用 HTTPS 在 TCP 端口 443 上建立反向代理和 SGD Web 服务器之间的连接，该连接安全可靠。
   - Apache 反向代理在浏览器中设置负载平衡 cookie。浏览器的所有后续 HTTP 请求都将使用同一个 SGD Web 服务器。
4. SGD Web 服务器将 HTML 传输到客户端设备上的浏览器。
   - 该 HTML 作为 HTTPS 数据通过在 SGD Gateway 的 TCP 端口 443 上建立的连接发送。
   - SGD Gateway 将 HTTPS 数据转发到浏览器。
5. 用户登录到 SGD。
   - SGD 服务器验证用户，选择 SGD 服务器来管理用户会话，并启动新的用户会话。
   - 在客户端设备上下载、安装并启动 SGD Client。
   - 在发送到浏览器的 HTML 中包含一个路由令牌。该路由令牌包含选择用于管理用户会话的 SGD 服务器的地址。此信息用于将自适应 Internet 协议 (Adaptive Internet Protocol, AIP) 数据路由到正确的 SGD 服务器。
   - 在 SGD 服务器上使用 SGD 服务器的私钥对该路由令牌签名，然后使用 SGD Gateway 证书对其加密。
   - 该路由令牌传送到 SGD Client。
   - 到客户端设备的连接使用 HTTPS。
6. SGD Client 在 TCP 端口 443 上与 SGD Gateway 建立连接。
   - SGD Client 和 SGD Gateway 之间的数据连接使用安全套接字层 (Secure Sockets Layer, SSL) 上的 AIP。
   - 为此连接提供 SGD Gateway 的 SSL 证书。
   - 路由代理识别传入的 SSL 上的 AIP 数据。
   - SSL 数据流被解密，并从 AIP 数据流提取路由令牌。
   - 使用 SGD Gateway 私钥解密路由令牌，然后使用 SGD 服务器的 CA 证书进行验证。
   - SGD Gateway 私钥和 SGD 服务器的 CA 证书存储在 SGD Gateway 密钥库 keystore 中。
   - 对路由令牌上的时间戳进行检查，以确保路由令牌有效。
   - AIP 数据流使用 SSL 进行重新加密。
7. SSL 上的 AIP 数据通过路由代理路由到路由令牌指示的 SGD 服务器。
   - SSL 上的 AIP 数据连接使用 TCP 端口 5307。

- 该路由令牌不包含在 AIP 数据流中。

8. 用户在 SGD Webtop 上启动应用程序。
   - 该应用程序启动请求通过 HTTPS 发送到 SGD Gateway。
   - 路由代理识别并解密 HTTPS 数据，并将 HTTP 通信转发到 Apache 反向代理。
   - 该反向代理检测负载平衡 cookie，并使用该 cookie 指示的 SGD Web 服务器。
   - SGD 应用程序会话负载平衡选择同一个 SGD 服务器来管理应用程序会话。
   - 在 SGD 服务器上创建一个新的路由令牌。该路由令牌用于将 AIP 数据路由到选择用于管理应用程序会话的 SGD 服务器。
   - SGD 服务器将路由令牌发送到 SGD Client。该路由令牌包含在现有 AIP 数据流中。
9. SGD Client 在 TCP 端口 443 上与 SGD Gateway 建立连接。
   - 为此连接提供 SGD Gateway 的 SSL 证书。
   - 路由代理识别传入的 SSL 上的 AIP 数据。
   - 对路由令牌进行解密、检验和验证。
   - SSL 上的 AIP 数据通过路由代理路由到路由令牌指示的 SGD 服务器。
   - 该路由令牌不包含在 AIP 数据流中。
10. SGD 服务器管理应用程序会话。
    - 该应用程序在位于局域网 (local area network, LAN) 中的应用程序服务器上运行。

A.2. SGD Gateway 的组件

SGD Gateway 包含以下组件：

- 路由代理。一种基于 Java 技术的应用程序，用于将 AIP 数据连接路由到 SGD 服务器。

  路由代理的主要组件有：

  - 路由令牌 - 请参见第 A.2.1 节 “关于路由令牌”
  - 密钥库 - 请参见第 A.2.2 节 “SGD Gateway 使用的密钥库”
  - 路由代理配置文件 - 请参见第 A.2.3 节 “路由代理配置文件”
- 反向代理。一种 Apache Web 服务器，配置为在反向代理模式下工作。反向代理还执行 HTTP 连接的负载平衡。

  反向代理的主要组件有：

  - 用于 Apache Web 服务器的配置文件 - 请参见第 A.2.4 节 “Apache Web 服务器配置文件”
  - 用于反向代理和 HTTP 负载平衡的 Apache 模块 - 请参见第 A.2.5 节 “SGD Gateway 使用的 Apache 模块”

A.2.1. 关于路由令牌

SGD Gateway 使用路由令牌来管理 AIP 连接。路由令牌是经过签名的加密消息，用于标识路由的源 SGD 服务器和目标 SGD 服务器。该路由令牌包含用于限制令牌生命周期的时间戳。

传出的路由令牌：

- 使用 SGD 服务器的私钥在 SGD 服务器上签名。

- 使用 SGD Gateway 证书在 SGD 服务器上加密。
- 发送到客户端设备上的 SGD Client。

传入路由令牌：

- 使用 SGD Gateway 私钥在 SGD Gateway 上解密。
- 使用源 SGD 服务器的 CA 证书在 SGD Gateway 上进行验证。
- 在 SGD Gateway 上被丢弃。提供路由令牌的连接将路由到目标 SGD 服务器。

A.2.2. SGD Gateway 使用的密钥库

SGD Gateway 使用私钥和证书来对路由令牌进行数字签名和验证，保护与阵列中的 SGD 服务器的连接安全，保护与 SGD Gateway 的连接安全，并对反射服务访问进行授权。

©SGD Gateway 使用的证书和私钥存储在 /opt/SUNWsgdg/proxy/etc 目录下的密钥库中。

该目录包含以下密钥库：

- SGD Gateway 密钥库。SGD Gateway 密钥库 keystore 包含 SGD Gateway 证书和私钥、阵列中 SGD 服务器的 CA 证书以及用于与阵列中 SGD 服务器建立安全连接的 SGD 服务器 SSL 证书。

  要添加、删除和列出 SGD Gateway 密钥库中的条目，请使用 gateway 命令。

- 客户端密钥库。客户端密钥库 keystore.client 包含一个 SGD Gateway SSL 证书和私钥，用于保护客户端设备和 SGD Gateway 之间的连接安全。默认情况下，该密钥库包含自签名证书。您可以将该证书替换为由证书颁发机构 (Certificate Authority, CA) 签名的证书。

- 反射服务密钥库。反射服务密钥库 keystore.reflection 包含一个证书和私钥，用于在 SGD Gateway 上对反射服务访问进行授权。默认情况下，该密钥库包含自签名证书和私钥。

如果在安装 SGD Gateway 后运行 gateway setup 命令，将自动创建密钥库。

注意

所有密钥库都使用 /opt/SUNWsgdg/etc/password 文件中定义的同一个密码。该密码是首次创建密钥库时自动创建的随机密码。该密码文件只能由超级用户 (root) 读取。

A.2.3. 路由代理配置文件

该路由代理配置文件为 /opt/SUNWsgdg/etc/gateway.xml。这是一个 XML 文件，用于根据数据协议类型配置路由。该文件还配置路由和 SSL 协议所需的密钥库位置和密码。

该路由代理配置文件在安装 SGD Gateway 时自动创建，并在使用 gateway config 命令更改 SGD Gateway 的配置时进行更新。

小心

使用 gateway config 命令来配置 Gateway。如有可能，避免手动编辑 gateway.xml 文件。gateway.xml 文件中的错误配置可能导致 SGD Gateway 停止运行。

默认路由代理配置文件使用 /opt/SUNWsgdg/etc/password 文件中的密码来访问 SGD Gateway 使用的密钥库。如果您不希望将该密码存储在磁盘上，请记录密码文件中的条目。删除该密码文件，并删除 gateway.xml 文件中所有 <keystore> 元素的 password 条目。当您下次启动 SGD Gateway 时，会提示您输入密钥库密码。

要更改 SGD Gateway 使用的密钥库密码，请使用带 -storepasswd 选项的 keytool 命令。例如，要更改 keystore.client 密钥库的密码，请运行以下命令：

```
# /opt/SUNWsgdg/java/default/bin/keytool -storepasswd \
-keystore /opt/SUNWsgdg/proxy/etc/keystore.client
```

有关如何使用 keytool 应用程序的详细信息，请参见 JDK Tools and Utilities（JDK 工具和实用程序）文档。

注意

/opt/SUNWsgdg/etc 目录还包含其他 .xml 和 .template 文件。gateway config 命令在内部使用这些文件来更新 gateway.xml 文件。请不要手动编辑这些文件。

A.2.4. Apache Web 服务器配置文件

配置用于 SGD Gateway 的 Apache Web 服务器的配置文件位于 /opt/SUNWsgdg/httpd/apache-version/conf 目录中。

此目录中的配置文件用于为 Apache Web 服务器配置反向代理操作和负载平衡。

A.2.4.1. 配置反向代理和负载平衡

用于配置反向代理操作和负载平衡的文件位于 extra/gateway 子目录中。这些文件由主要 httpd.conf 文件中的以下 Include 指令启用：

```
# SGD Reverse Proxy/Load Balance settings
Include conf/extra/gateway/httpd-gateway.conf
```

httpd-gateway.conf 文件为 Apache Web 服务器配置反向代理和负载平衡。负载平衡组的成员是使用 httpd-gateway.conf 文件中的 Include 指令定义的，如下所示：

```
<Proxy Balancer://mysgdservers/>
Include conf/extra/gateway/servers/*.conf
</Proxy>
```

extra/gateway/servers 目录包含负载平衡组中每个 SGD Web 服务器的配置文件。配置文件命名为 server-name.conf，其中 server-name 是 gateway server add 命令中使用的服务器名称。有关此命令的更多详细信息，请参见第 B.12 节 “gateway server add”。

SGD Gateway 使用粘性会话 HTTP 负载平衡。这意味着 Apache 反向代理在客户端浏览器中设置 cookie，以确保浏览器始终返回负载平衡选择的 SGD Web 服务器。cookie 在用户会话结束时过期。

粘性会话 cookie 由 httpd-gateway.conf 文件中的 Header add Set-Cookie 指令启用，如下所示：

```
Header add Set-Cookie "BALANCEID=balanceworker.%{BALANCER_WORKER_ROUTE}e; path=/" \
env=BALANCER_ROUTE_CHANGED
```

其中 BALANCEID 是 cookie 的名称，BALANCER_WORKER_ROUTE 和 BALANCER_ROUTE_CHANGED 是 Apache mod_proxy_balancer 模块导出的环境变量。有关这些环境变量的更多信息，请参见 Apache mod_proxy_balancer 文档。

A.2.5. SGD Gateway 使用的 Apache 模块

随 SGD Gateway 提供的 Apache Web 服务器使用标准 Apache 模块进行反向代理和负载平衡。这些模块是作为动态共享对象 (Dynamic Shared Object, DSO) 模块安装的。

这些模块由 httpd.conf Apache 配置文件（位于 /opt/SUNWsgdg/httpd/apache-version/conf/httpd.conf）中的 LoadModule 指令启用。

附录 B. 命令行参考

本章介绍如何从命令行管理、控制和更改 Oracle Secure Global Desktop Gateway (SGD Gateway) 的配置。

为许多任务提供了执行命令，例如：设置密钥库和证书、配置 SGD Gateway 使用的端口以及为阵列中的 SGD 服务器配置负载平衡。

本章包括以下主题：

B.1. gateway 命令

可使用 gateway 命令来配置和控制 SGD Gateway。

注意

gateway 命令的完整路径为 /opt/SUNWsgdg/bin/gateway。

语法

```
gateway start | stop | restart | config | server | status | setup | version | sslcert |
sslkey | cert | key | setup | uninstall
```

描述

下表显示了可用的 gateway 命令。

命令	描述	更多信息
gateway start	启动 SGD Gateway	第 B.22 节 “gateway start”
gateway stop	停止 SGD Gateway	第 B.24 节 “gateway stop”
gateway restart	停止然后重新启动 SGD Gateway	第 B.10 节 “gateway restart”
gateway config	配置 SGD Gateway，然后更新 Apache 反向代理配置文件	第 B.3 节 “gateway config”
gateway server	为 SGD 阵列安装 SGD 服务器安全证书并配置负载平衡	第 B.11 节 “gateway server”
gateway status	显示 SGD Gateway 的当前状态	第 B.23 节 “gateway status”
gateway version	显示 SGD Gateway 的版本号	第 B.26 节 “gateway version”
gateway sslcert	导出并输出客户端密钥库中的安全套接字层 (Secure Sockets Layer, SSL) 证书	第 B.16 节 “gateway sslcert”
gateway sslkey	管理客户端密钥库中的私钥和证书	第 B.19 节 “gateway sslkey”
gateway cert export	从 SGD Gateway 密钥库导出 SGD Gateway 证书	第 B.2 节 “gateway cert export”
gateway key import	将私钥和证书导入 SGD Gateway 密钥库	第 B.9 节 “gateway key import”
gateway setup	运行 SGD Gateway 安装程序	第 B.15 节 “gateway setup”
gateway uninstall	卸载 SGD Gateway 软件	第 B.25 节 “gateway uninstall”

注意

所有 gateway 命令都包含 --help 选项。您可以使用此选项来显示相关命令的帮助信息。

示例

以下示例启动 SGD Gateway。

```
# /opt/SUNWsgdg/bin/gateway start
```

以下示例表示未授权 SGD 服务器 server.example.com 使用 SGD Gateway。

```
# /opt/SUNWsgdg/bin/gateway server remove --server server.example.com
```

B.2. gateway cert export

从 SGD Gateway 密钥库导出 SGD Gateway 证书。

语法

```
gateway cert export --certfile file-name
```

描述

从位于 /opt/SUNWsgdg/proxy/etc/keystore 的 SGD Gateway 密钥库导出 SGD Gateway 证书。该证书写入由 --certfile 选项指定的文件。

为访问 SGD Gateway 密钥库，此命令使用 /opt/SUNWsgdg/etc/password 中的密码。如果未提供此文件，则该命令会提示输入密码。

示例

下列示例将 SGD Gateway 证书从 SGD Gateway 密钥库导出到文件 gateway1.pem 中。

```
# /opt/SUNWsgdg/bin/gateway cert export --certfile gateway1.pem
```

B.3. gateway config

配置 SGD Gateway。gateway config 命令为 SGD Gateway 配置安全连接、端口和反向代理服务器设置。

语法

```
gateway config create | show
```

描述

下表显示了此命令的可用子命令。

子命令	描述	更多信息
create	创建 SGD Gateway 的新配置	第 B.4 节 “gateway config create”
list	列出 SGD Gateway 的当前配置	第 B.8 节 “gateway config list”
edit	编辑 SGD Gateway 的当前配置	第 B.6 节 “gateway config edit”
enable	启用 SGD Gateway 服务	第 B.7 节 “gateway config enable”
disable	禁用 SGD Gateway 服务	第 B.5 节 “gateway config disable”

示例

以下示例列出 SGD Gateway 的当前配置。

```
# /opt/SUNWsgdg/bin/gateway config list
```

B.4. gateway config create

为 SGD Gateway 创建新配置来覆盖当前配置。

语法

```
gateway config create { [ --interface interface:port ]
                        [ --entry-point ip-address:port ]
                        [ --out plaintext | ssl ]
                      } | --file file
```

描述

下表显示了此命令的可用选项。

选项	描述
--interface	SGD Gateway 侦听传入代理连接所使用的接口和端口。默认为所有接口上的 TCP 端口 443。
--entry-point	网络的入口点。这是客户端用于连接 SGD Gateway 的 Internet 协议 (Internet Protocol, IP) 地址和端口。您可以指定域名系统 (Domain Name System, DNS) 地址来代替 IP 地址。
--out	从 SGD Gateway 到阵列中的 SGD 服务器的传出通信格式。如果您要使用安全连接，请选择 ssl。
--file	指定包含配置设置的文件。

注意

如果没有为 gateway config create 命令指定选项，则将显示一系列联机提示，使您能够键入所需设置。

如果在 gateway config create 中使用 --file 选项，则指定的文件必须与 /opt/SUNWsgdg/etc/gatewayconfig.xml 文件格式相同。此文件在 SGD Gateway 的初始配置期间创建，如第 2.2.1.1 节 “如何配置 SGD Gateway 的端口和连接”中所述。

示例

以下示例将 SGD Gateway 配置为在 TCP 端口 443 上侦听来自位于 192.168.0.1 的网络入口点的连接。SGD Gateway 和阵列中的 SGD 服务器之间使用安全连接。

```
# /opt/SUNWsgdg/bin/gateway config create --interface *:443 \
--entry-point 192.168.0.1:443 --out ssl
```

B.5. gateway config disable

禁用一个或多个 SGD Gateway 服务。

语法

```
gateway config disable [ --services-reflection ]
                       [ --services-reflection-auth ]
                       [ --routes-http-redirect ]
```

描述

使用命令行选项来禁用特定的 SGD Gateway 服务。您必须至少指定一个命令行选项。

注意

使用此命令禁用服务后，您必须重新启动 SGD Gateway 来停止该服务。

下表显示了此命令的可用选项。

选项	描述
--services-reflection	禁用对 SGD Gateway 反射服务进行未经验证的访问。 默认情况下，该服务处于禁用状态。 有关 SGD Gateway 反射服务的更多详细信息，请参见第 C.9 节 “反射服务”。
--services-reflection-auth	禁用对 SGD Gateway 反射服务进行经过验证的访问。 默认情况下，该服务处于禁用状态。 有关 SGD Gateway 反射服务的更多详细信息，请参见第 C.9 节 “反射服务”。
--routes-http-redirect	禁用 HTTP 重定向服务。 默认情况下，该服务处于禁用状态。

示例

以下示例禁用对 SGD Gateway 反射服务进行经过验证的访问。

```
# /opt/SUNWsgdg/bin/gateway config disable --services-reflection-auth
```

B.6. gateway config edit

编辑 SGD Gateway 的当前配置。

语法

```
gateway config edit [ --binding int:port ]
                    [ --routes-http-maxcon num ]
                    [ --routes-aip-maxcon num ]
                    [ --routes-reverseproxy-redirect port ]
                    [ --services-reflection-binding int:port ]
                    [ --services-reflection-auth-binding int:port ]
```

描述

这些命令行选项使您能够编辑特定的配置设置。您必须至少指定一个命令行选项。

SGD Gateway 的当前配置存储在 /opt/SUNWsgdg/etc/gatewayconfig.xml 文件中。

您必须重新启动 SGD Gateway 来启用您执行的任何配置更改。

下表显示了此命令的可用选项。

选项	描述
--binding	SGD Gateway 侦听传入代理连接所使用的接口和端口。默认为所有接口上的 TCP 端口 443。
--routes-http-maxcon	HTTP 连接的最大数量。默认值在安装时配置，并取决于 SGD Gateway 上可用的内存资源。请参见第 C.1 节 “调整 SGD Gateway”。
--routes-aip-maxcon	AIP 连接的最大数量。默认值在安装时配置，并取决于 SGD Gateway 上可用的内存资源。请参见第 C.1 节 “调整 SGD Gateway”。
--routes-reverseproxy-redirect	HTTP 重定向端口。默认为 TCP 端口 8080。
--services-reflection-binding	用于对 SGD Gateway 反射服务进行未经验证的访问的接口和端口。默认为本地主机回送接口上的 TCP 端口 81。
--services-reflection-auth-binding	用于对 SGD Gateway 反射服务进行经过验证的访问的接口和端口。默认为所有接口上的 TCP 端口 82。

示例

以下示例更改 SGD Gateway 的 HTTP 和 AIP 连接的最大数量。

```
# /opt/SUNWsgdg/bin/gateway config edit --routes-http-maxcon 200
# /opt/SUNWsgdg/bin/gateway config edit --routes-aip-maxcon 3000
```

B.7. gateway config enable

启用一个或多个 SGD Gateway 服务。

语法

```
gateway config enable [ --services-reflection ]
                      [ --services-reflection-auth ]
                      [ --routes-http-redirect ]
```

描述

使用命令行选项来启用特定的 SGD Gateway 服务。您必须至少指定一个命令行选项。

注意

使用此命令启用服务后，您必须重新启动 SGD Gateway 来启动该服务。

下表显示了此命令的可用选项。

选项	描述
--services-reflection	启用对 SGD Gateway 反射服务进行未经验证的访问。 默认情况下，该服务处于禁用状态。 有关 SGD Gateway 反射服务的更多详细信息，请参见第 C.9 节 “反射服务”。
--services-reflection-auth	启用对 SGD Gateway 反射服务进行经过验证的访问。 默认情况下，该服务处于禁用状态。 有关 SGD Gateway 反射服务的更多详细信息，请参见第 C.9 节 “反射服务”。
--routes-http-redirect	启用 HTTP 重定向服务。 默认情况下，该服务处于禁用状态。

示例

以下示例启用对 SGD Gateway 反射服务进行经过验证的访问。

```
# /opt/SUNWsgdg/bin/gateway config enable --services-reflection-auth
```

B.8. gateway config list

列出 SGD Gateway 的当前配置。

语法

```
gateway config list [ --binding ]
```

```
        [ --routes-http-maxcon ]
        [ --routes-aip-maxcon ]
        [ --routes-reverseproxy-redirect ]
        [ --services-reflection-binding ]
        [ --services-reflection-auth-binding ]
```

描述

这些命令行选项使您能够列出特定的配置设置。如果未指定选项，则将显示 SGD Gateway 的完整配置详细信息。

SGD Gateway 的当前配置存储在 /opt/SUNWsgdg/etc/gatewayconfig.xml 文件中。

下表显示了此命令的可用选项。

选项	描述
--binding	SGD Gateway 侦听传入代理连接所使用的接口和端口
--routes-http-maxcon	HTTP 连接的最大数量
--routes-aip-maxcon	自适应 Internet 协议 (Adaptive Internet Protocol, AIP) 连接的最大数量
--routes-reverseproxy-redirect	HTTP 重定向端口
--services-reflection-binding	用于对 SGD Gateway 反射服务进行未经验证的访问的接口和端口
--services-reflection-auth-binding	用于对 SGD Gateway 反射服务进行经过验证的访问的接口和端口

示例

以下示例显示 SGD Gateway 的绑定配置和 AIP 连接的最大数量。

```
# /opt/SUNWsgdg/bin/gateway config list --binding --routes-aip-maxcon
binding: *:443
routes-aip-maxcon: 2920
```

以下示例显示 SGD Gateway 当前配置的完整详细信息。

```
# /opt/SUNWsgdg/bin/gateway config list
binding: *:443
routes-http-maxcon: 100
routes-aip-maxcon: 2920
routes-reverseproxy-redirect: null
services-reflection-binding: localhost:81
services-reflection-auth-binding: *:82
```

B.9. gateway key import

将 SGD Gateway 密钥和 SGD Gateway 证书导入 SGD Gateway 密钥库。

语法

```
gateway key import --keyfile key-file
        [ --keyalg RSA|DSA ]
        { --certfile cert-file |
          --certfile cert-file.. [ --cacertfile ca-cert-file ] }
        [ --alwaysoverwrite ]
```

描述

将私钥和相应的公钥证书导入位于 /opt/SUNWsgdg/proxy/etc/keystore 的 SGD Gateway 密钥库。

如果该密钥库已有 SGD Gateway 密钥条目，则它将被覆盖。默认情况下，将显示确认提示。

为访问 SGD Gateway 密钥库，此命令使用 /opt/SUNWsgdg/etc/password 中的密码。如果未提供此文件，则该命令会提示输入密码。

下表显示了此命令的可用选项。

选项	描述
--keyfile	包含私钥的文件。该密钥必须是 PEM 格式。
--keyalg	私钥使用的编码算法。选项为 RSA 和 DSA。默认情况下，选择 RSA。
--certfile	SSL 证书文件。
--cacertfile	CA 或根证书文件。
--alwaysoverwrite	在覆盖密钥库中的条目之前不进行提示。

要导入证书链，请使用 --cacertfile 选项来指定中间 CA 证书。链中的所有证书都必须是 PEM 格式。

如果证书链使用多个 CA 证书，将链中的所有 CA 证书整合到一个文件中。用于对服务器证书进行签名的 CA 证书必须首先出现，例如：

```
-----BEGIN CERTIFICATE-----
...Intermediate CA's certificate...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
...CA root certificate...
-----END CERTIFICATE-----
```

示例

以下示例将 RSA 编码的私钥 gateway1.key 和相应的公钥证书 gateway1.pem 导入 SGD Gateway 密钥库。

```
# /opt/SUNWsgdg/bin/gateway key import \
--keyfile gateway1.key \
--certfile gateway1.pem
```

以下示例将私钥和证书链导入 SGD Gateway 密钥库。中间 CA 证书为 gateway1-ca.pem。

```
# /opt/SUNWsgdg/bin/gateway key import \
--keyfile gateway1.key \
--certfile gateway1.pem \
--cacertfile gateway1-ca.pem
```

B.10. gateway restart

停止然后重新启动 SGD Gateway。

语法

```
gateway restart [--force]
```

描述

停止然后重新启动 SGD Gateway。在停止 SGD Gateway 之前，将提示用户进行确认。

--force 选项会在不要求确认的情况下停止 SGD Gateway。

示例

以下示例在提示用户进行确认后停止然后重新启动 SGD Gateway。

```
# /opt/SUNWsgdg/bin/gateway restart
```

B.11. gateway server

授权 SGD 服务器使用 SGD Gateway。

语法

```
gateway server add | remove | list
```

描述

下表显示了此命令的可用子命令。

子命令	描述	更多信息
add	授权 SGD 服务器使用 SGD Gateway	第 B.12 节 “gateway server add”
remove	删除 SGD 服务器使用 SGD Gateway 的授权	第 B.14 节 “gateway server remove”
list	列出授权使用 SGD Gateway 的 SGD 服务器	第 B.13 节 “gateway server list”

示例

以下示例删除 SGD 服务器 sgd.example.com 使用 SGD Gateway 的授权。

```
# /opt/SUNWsgdg/bin/gateway server remove --server sgd.example.com
```

B.12. gateway server add

授权 SGD 服务器使用 SGD Gateway。

语法

```
gateway server add --server server-name
                   --certfile cert-file
                   --url server-url
                 [ --ssl-certfile ssl-cert ]
```

描述

下表显示了此命令的可用选项。

选项	描述
--server	SGD 服务器的 DNS 名称
--cert-file	SGD 服务器的证书颁发机构 (Certificate Authority, CA) 证书
--url	SGD Web 服务器的 URL
--ssl-certfile	SGD 服务器的 SSL 证书

gateway server add 命令执行以下操作：

- 将 SGD 服务器的 CA 证书导入位于 /opt/SUNWsgdg/proxy/etc/keystore 的 SGD Gateway 密钥库。CA 证书使用别名存储在密钥库中，该别名与 --server 选项指定的 SGD 服务器名称相同。
- 将 SGD 服务器的 SSL 证书导入位于 /opt/SUNWsgdg/proxy/etc/keystore 的 SGD Gateway 密钥库。使用别名将 SSL 证书存储到密钥库中，该别名是通过将 -ssl 附加到由 --server 选项指定的 SGD 服务器名称而构成的。
- 将 SGD 服务器添加到 Apache 反向代理服务器使用的负载平衡组

注意

使用 gateway server add 后，您必须重新启动 SGD Gateway 才能使任何更改生效。

示例

以下示例使用别名 sgd.example.com 将 CA 证书 PeerCAcert.pem 添加到 SGD Gateway 密钥库。还使用别名 sgd.example.com-ssl 将SSL 证书 cert.pem 添加到密钥库。

```
# /opt/SUNWsgdg/bin/gateway server add --server sgd.example.com \
--certfile PeerCAcert.pem \
--url https://sgd.example.com \
--ssl-certfile cert.pem
```

在该示例中，SGD Web 服务器的 URL https://sgd.example.com 添加到反向代理负载平衡组，并在 /opt/SUNWsgdg/httpd/apache-version/conf/extra/gateway/servers/conf/sgd.example.com.conf 中创建配置文件。

B.13. gateway server list

显示授权使用 SGD Gateway 的 SGD 服务器的详细信息。

语法

```
gateway server list
```

描述

此命令显示授权使用 SGD Gateway 的 SGD 服务器的证书详细信息和 URL。

示例

以下示例列出 SGD Gateway 的授权 SGD 服务器的详细信息。

```
# /opt/SUNWsgdg/bin/gateway server list
```

B.14. gateway server remove

删除 SGD 服务器使用 SGD Gateway 的授权。

语法

```
gateway server remove --server server-name
```

描述

将 SGD 服务器的 CA 证书和 SSL 证书从 SGD Gateway 密钥库中删除。

注意

使用 gateway server remove 后，您必须重新启动 SGD Gateway 才能使任何更改生效。

示例

以下示例删除 SGD 服务器 sgd.example.com 使用 SGD Gateway 的授权。

```
# /opt/SUNWsgdg/bin/gateway server remove --server sgd.example.com
```

B.15. gateway setup

运行 SGD Gateway 的安装程序。

语法

```
gateway setup
```

描述

回答屏幕上的问题来配置 SGD Gateway 使用的端口、接口和安全设置。

示例

以下示例运行 SGD Gateway 安装程序。

```
# /opt/SUNWsgdg/bin/gateway setup
```

B.16. gateway sslcert

输出或导出存储在客户端密钥库中的 SGD Gateway SSL 证书。

语法

```
gateway sslcert export | print
```

描述

下表显示了此命令的可用子命令。

子命令	描述	更多信息
export	从客户端密钥库导出 SGD Gateway SSL 证书	第 B.17 节 “gateway sslcert export”
print	输出存储在客户端密钥库中的 SGD Gateway SSL 证书	第 B.18 节 “gateway sslcert print”

示例

以下示例输出存储在客户端密钥库中的 SGD Gateway SSL 证书。

```
# /opt/SUNWsgdg/bin/gateway sslcert print
```

B.17. gateway sslcert export

从客户端密钥库导出 SGD Gateway SSL 证书。

语法

```
gateway sslcert export --certfile cert-file
```

描述

从位于 /opt/SUNWsgdg/proxy/etc/keystore.client 的客户端密钥库导出 SGD Gateway SSL 证书。该证书写入由 --certfile 选项指定的文件。

为访问客户端密钥库，此命令使用 /opt/SUNWsgdg/etc/password 中的密码。如果未提供此文件，则该命令会提示输入密码。

示例

以下示例将 SGD Gateway SSL 证书从客户端密钥库导出到文件 gateway-ssl.pem 中。

```
# /opt/SUNWsgdg/bin/gateway sslcert export --certfile gateway-ssl.pem
```

B.18. gateway sslcert print

输出 SGD Gateway SSL 证书。

语法

```
gateway sslcert print
```

描述

输出存储在位于 /opt/SUNWsgdg/proxy/etc/keystore.client 的客户端密钥库中的 SGD Gateway SSL 证书。

此命令将证书的详细信息写入终端窗口。

为访问客户端密钥库，此命令使用 /opt/SUNWsgdg/etc/password 中的密码。如果未提供此文件，则该命令会提示输入密码。

示例

以下示例输出存储在客户端密钥库中的 SGD Gateway SSL 证书。

```
# /opt/SUNWsgdg/bin/gateway sslcert print
```

B.19. gateway sslkey

管理客户端密钥库中的 SSL 密钥和证书条目。

语法

```
gateway sslkey import | export
```

描述

下表显示了此命令的可用子命令。

子命令	描述	更多信息
import	将私钥和证书导入客户端密钥库	第 B.21 节 “gateway sslkey import”
export	从客户端密钥库导出私钥	第 B.20 节 “gateway sslkey export”

示例

以下示例导出存储在客户端密钥库中的 SGD Gateway SSL 证书。

```
# /opt/SUNWsgdg/bin/gateway sslkey export --keyfile gateway-ssl.key
```

B.20. gateway sslkey export

从客户端密钥库导出 SGD Gateway SSL 私钥。

语法

```
gateway sslkey export --keyfile key-file [ --keypass passwd ]
```

描述

从位于 /opt/SUNWsgdg/proxy/etc/keystore.client 的客户端密钥库导出 SGD Gateway SSL 私钥。该私钥写入由 --keyfile 选项指定的文件。

可使用 --keypass 选项指定私钥的密码。默认情况下，使用来自 /opt/SUNWsgdg/etc/password 的密码。

示例

以下示例将 SGD Gateway SSL 私钥从客户端密钥库导出到文件 gateway-ssl.key 中。

```
# /opt/SUNWsgdg/bin/gateway sslkey export --keyfile gateway-ssl.key
```

B.21. gateway sslkey import

将 SSL 密钥和证书导入客户端密钥库。

语法

```
gateway sslkey import --keyfile key-file
                [ --keyalg RSA|DSA ]
                { --certfile cert-file |
                  --certfile cert-file.. [ --cacertfile ca-cert-file ] }
                [ --alwaysoverwrite ]
```

描述

将 SSL 私钥和相应的 SSL 证书导入位于 /opt/SUNWsgdg/proxy/etc/keystore.client 的客户端密钥库。默认情况下，该密钥库包含一个自签名证书。

如果客户端密钥库已有一个条目，此命令将覆盖该条目。默认情况下，在覆盖密钥库条目之前将显示确认提示。

为访问客户端密钥库，此命令使用 /opt/SUNWsgdg/etc/password 中的密码。如果未提供此文件，则该命令会提示输入密码。

下表显示了此命令的可用选项。

选项	描述
--keyfile	包含 SSL 私钥的文件。该密钥必须为保密性增强的电子邮件 (Privacy Enhanced Mail, PEM) 格式。
--keyalg	私钥使用的编码算法。选项为 RSA 和数字签名算法 (Digital Signature Algorithm, DSA)。默认情况下，选择 RSA。
--certfile	SSL 证书文件。
--cacertfile	CA 证书或根证书文件。
--alwaysoverwrite	在覆盖客户端密钥库中的条目之前不进行提示。

要导入证书链，请使用 --cacertfile 选项来指定中间 CA 证书。链中的所有证书都必须是 PEM 格式。

如果证书链使用多个 CA 证书，将链中的所有 CA 证书整合到一个文件中。用于对服务器证书进行签名的 CA 证书必须首先出现，例如：

```
-----BEGIN CERTIFICATE-----
...Intermediate CA's certificate...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
...CA root certificate...
-----END CERTIFICATE-----
```

示例

以下示例将 RSA 编码的 SSL 私钥 gateway1-ssl.key 和相应的 SSL 证书 gateway1-ssl.pem 导入客户端密钥库。

```
# /opt/SUNWsgdg/bin/gateway sslkey import \
--keyfile gateway1-ssl.key \
--certfile gateway1-ssl.pem
```

以下示例将 RSA 编码的 SSL 私钥和 SSL 证书链导入客户端密钥库。中间 CA 证书为 gateway1-ca.pem。

```
# /opt/SUNWsgdg/bin/gateway sslkey import \
--keyfile gateway1-ssl.key \
--certfile gateway1-ssl.pem \
--cafile gateway1-ca.pem
```

B.22. gateway start

启动 SGD Gateway。

语法

```
gateway start
```

描述

启动 SGD Gateway。

示例

以下示例启动 SGD Gateway。

```
# /opt/SUNWsgdg/bin/gateway start
SGD Gateway started successfully
```

B.23. gateway status

显示 SGD Gateway 的当前状态。

语法

```
gateway status
```

描述

此命令指示 SGD Gateway 是启动、停止还是出现问题。

示例

以下示例显示 SGD Gateway 的状态信息。在本示例中，SGD Gateway 停止。

```
# /opt/SUNWsgdg/bin/gateway status
SGD Gateway status: STOPPED
```

B.24. gateway stop

停止 SGD Gateway。

语法

```
gateway stop [--force]
```

描述

提示用户进行确认后，停止 SGD Gateway。

--force 选项会在不要求确认的情况下停止 SGD Gateway。

示例

以下示例在提示用户进行确认后停止 SGD Gateway。

```
# /opt/SUNWsgdg/bin/gateway stop
```

B.25. gateway uninstall

卸载 SGD Gateway 软件。

语法

```
gateway uninstall
```

描述

停止 SGD Gateway 并删除 SGD Gateway 软件，其中包括所有配置信息。

在停止 SGD Gateway 之前，此命令将提示用户进行确认。

示例

以下示例从运行命令的主机卸载 SGD Gateway 软件。

```
# /opt/SUNWsgdg/bin/gateway uninstall
```

B.26. gateway version

显示 SGD Gateway 软件的版本号。

语法

```
gateway version
```

描述

显示 SGD Gateway 的版本号。

示例

以下示例显示在运行命令的主机上安装的 SGD Gateway 版本。

```
# /opt/SUNWsgdg/bin/gateway version
Oracle Secure Global Desktop Gateway 4.50.301
```

B.27. tarantella gateway 命令

使用 tarantella gateway 命令可为 SGD 阵列配置授权网关。

语法

```
tarantella gateway add | list | remove
```

描述

使用 tarantella gateway 命令，您可以添加、删除并列出 SGD 阵列的网关。

可以对阵列中的任何 SGD 服务器使用 tarantella gateway 命令。所做的任何更改都将自动复制到其他阵列成员中。

当某个 SGD 服务器加入阵列后，在主 SGD 服务器上定义的一组网关将被复制到新的阵列成员，覆盖已提供的任何授权网关。当 SGD 服务器从阵列中分离时，不会从该服务器中删除已注册的网关。

下表显示了 tarantella gateway 命令的可用子命令。

子命令	描述	更多信息
add	为 SGD 阵列添加 SGD Gateway	第 B.28 节 “tarantella gateway add”
list	列出 SGD 阵列的 SGD Gateway	第 B.29 节 “tarantella gateway list”
remove	删除 SGD 阵列的 SGD Gateway	第 B.30 节 “tarantella gateway remove”

注意

所有 tarantella gateway 子命令都包含 --help 选项。您可以使用此选项来显示相关子命令的帮助信息。

示例

以下示例将 gateway1.example.com 添加到 SGD 阵列的注册网关列表。

```
$ tarantella gateway add --name gateway1.example.com \
--certfile /opt/gateway1_cert_file.pem
```

B.28. tarantella gateway add

向 SGD 阵列注册 SGD Gateway。

语法

```
tarantella gateway add {
                --name server-name
                --certfile cert-file
                } | --file file
```

描述

下表显示了此命令的可用选项。

选项	描述
--name	要注册的 SGD Gateway 名称。
--certfile	SGD 服务器使用的 SGD Gateway 证书。该证书可以是确定性编码规则 (Definite Encoding Rules, DER) 格式或 PEM 格式。
--file	包含多个 SGD Gateway 的配置设置的批处理文件。

示例

以下示例将 gateway1.example.com 添加到 SGD 阵列的注册网关列表。

```
$ tarantella gateway add --name gateway1.example.com \
--certfile /opt/gateway1_cert_file.pem
```

以下示例使用带 --file 选项的 tarantella gateway add 来同时注册多个网关。

```
$ tarantella gateway add --file gateways.list
```

--file 选项指定一个批处理文件 gateways.list，其中包含每个网关的一系列设置，如下所示：

```
--name gateway1.example.com --certfile /opt/gateway1_cert_file.pem
--name gateway2.example.com --certfile /opt/gateway2_cert_file.pem
```

B.29. tarantella gateway list

列出 SGD 阵列的注册 SGD Gateway。

语法

```
tarantella gateway list
```

描述

显示使用 tarantella gateway add 向 SGD 阵列注册的 SGD Gateway 的详细信息。

示例

以下示例列出 SGD 阵列的注册网关。

```
$ tarantella gateway list
```

B.30. tarantella gateway remove

从 SGD 阵列的注册网关列表中删除 SGD Gateway。

语法

```
tarantella gateway remove --name server-name | --file file
```

描述

下表显示了此命令的可用选项。

选项	描述
--name	将删除其注册详细信息的 SGD Gateway 的名称
--file	包含多个 SGD Gateway 的配置设置的批处理文件

示例

以下示例将 SGD Gateway gateway1.example.com 从 SGD 阵列的注册网关列表中删除。

```
$ tarantella gateway remove --name gateway1.example.com
```

B.31. --security-gateway 属性

描述

可以使用 --security-gateway 属性为 SGD 阵列设置 SGD Gateway 的用法。该属性定义以下内容：

- 可访问 SGD Gateway 的 SGD Client，基于其 IP 地址或 DNS 名称定义。
- 客户端设备用于联系 SGD Gateway 的地址。

注意

--security-gateway 属性仅适用于 AIP 连接。HTTP 连接的路由是由 Gateway 的 Apache 反向代理组件上的 HTTP 负载平衡服务处理的。

对 --security-gateway 属性所做的更改将应用于阵列中的所有 SGD 服务器。

语法

--security-gateway 属性的语法如下所示：

```
--security-gateway filter-spec...
```

将 filter-spec 替换为以下类型的过滤器规范：

```
client-ip-address|*:gateway protocol:gateway-address:gateway-port
```

- client-ip-address 是 SGD Client 的 IP 地址。对于通过 SGD Gateway 的连接，这是 SGD Gateway 用于连接阵列中的 SGD 服务器的接口。

  一个星号 * 表示所有 IP 地址。

  客户端 IP 地址字符串可以包含 * 和 ? 通配符，其中 * 匹配多个字符，? 匹配单个字符。例如：

  192.169.10.* 匹配 192.169.10 网络上的所有地址。

  192.169.10.12? 匹配范围从 192.169.10.120 到 192.169.10.129 的地址。

  注意

  如果要将外部负载平衡器用于 SGD Gateway，请为 client-ip-address 键入负载平衡器的地址。

- 对于通过 SGD Gateway 的连接，gateway protocol 是 sgdg，对于直接连接 SGD 阵列（不通过 SGD Gateway）的 SGD Client，则是 direct。
- gateway-address 是 SGD Gateway 或外部负载平衡器（如果使用）的外部地址。这是客户端设备用于联系 SGD Gateway 的地址。

  对于到 SGD 阵列的 direct（直接）连接，请指定阵列中主服务器的地址。
- gateway-port 是客户端设备用于连接 SGD Gateway 或外部负载平衡器（如果使用）的 TCP 端口。

  对于到 SGD 阵列的 direct（直接）连接，请指定阵列中主服务器的端口。

使用逗号分隔多个 filter-spec 条目，并使用双引号 (" ") 将整个字符串括起。请参见第 B.31 节 “ 使用多个过滤器 ”。

示例

以下示例使所有 SGD Client 使用 SGD Gateway gateway1.example.com 的 TCP 端口 443 进行连接。

```
$ tarantella config edit --security-gateway "*:sgdg:gateway1.example.com:443"
```

以下示例使所有 SGD Client 使用外部负载平衡器 lb.example.com 进行连接。

```
$ tarantella config edit --security-gateway "*:sgdg:lb.example.com:443"
```

以下示例使所有 SGD Client 直接连接 SGD 阵列，而不通过 SGD Gateway。阵列中的主服务器为 sgd1.example.com。

```
$ tarantella config edit --security-gateway "*:direct:sgd1.example.com:443"
```

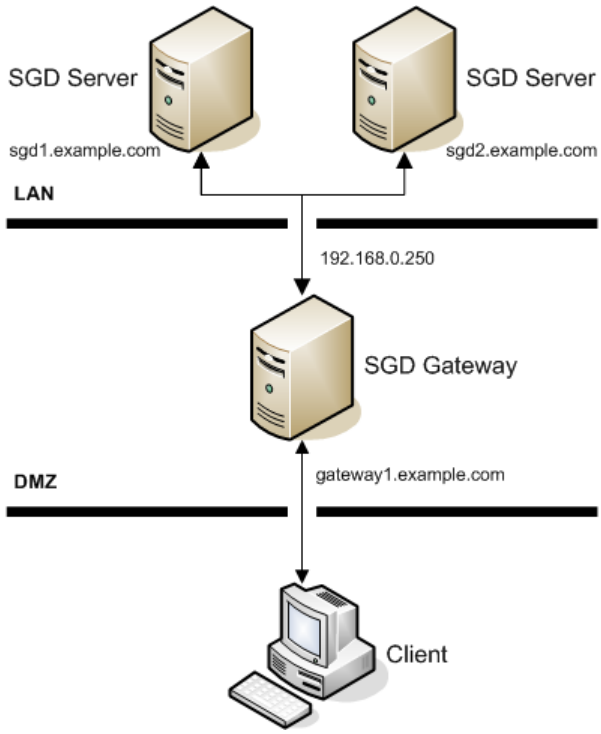
使用多个过滤器

您可以使用多个过滤器规范，如以下示例中所示。

请考虑图 B.1 “使用多个过滤器规范”中所示的基本部署。该部署使用一个 SGD Gateway gateway1.example.com 和包含两个 SGD 服务器（sgd1.example.com 和 sgd2.example.com）的 SGD 阵列。阵列中的主服务器为 sgd1.example.com。

内部网络上的 SGD Gateway 地址为 192.168.0.250。

图 B.1. 使用多个过滤器规范



以下过滤器规范可用于本示例：

```
"192.168.0.250:sgdg:gateway1.example.com:443,*:direct:sgd1.example.com:80"
```

使用此配置时，遵循以下方式：

- 允许从 SGD Gateway IP 地址 192.168.0.250 建立到阵列中 SGD 服务器的连接。组织外的 SGD Client 使用 SGD Gateway gateway1.example.com 的 TCP 端口 443 进行连接。
- 所有其他 SGD Client（如局域网 (local area network, LAN) 上的 SGD Client）直接连接到主 SGD 服务器 sgd1.example.com 上的 TCP 端口 80。这些连接不使用 SGD Gateway。
- 过滤器的顺序很重要。如果过滤器的顺序相反，则所有 SGD Client 将直接连接 SGD 服务器 sgd1.example.com。

附录 C. 高级配置

本章包含有关配置和使用 Oracle Secure Global Desktop Gateway (SGD Gateway) 高级功能的信息。

本章包括以下主题：

C.1. 调整 SGD Gateway

安装 SGD Gateway 时，系统会基于 SGD Gateway 主机上的可用内存自动配置并发自适应 Internet 协议 (Adaptive Internet Protocol, AIP) 和 HTTP 连接最大数量的默认值。同时还将针对此连接数量优化分配给 SGD Gateway 的 Java 虚拟机 (Java Virtual Machine, JVM) 的内存大小。

安装 SGD Gateway 之后，可以根据预期的 SGD 用户数以及他们将运行的应用程序数调整默认设置。执行此操作时，可能还需要调整 JVM 内存大小。此过程称为调整 SGD Gateway。

小心

如果 JVM 内存大小对于预期的连接数来说过低，SGD Gateway 可能会停止工作并拒绝后续的所有连接。在这种情况下，您需要调整 SGD Gateway，以便有足够的 JVM 内存可用。SGD Gateway 显示 java.lang.OutOfMemoryError 错误消息表示可能需要进行调整。

要调整 SGD Gateway，您需要执行以下操作：

- 更改 AIP 最大连接数。请参见第 C.1.1 节 “更改 AIP 最大连接数”。
- 更改 HTTP 最大连接数。请参见第 C.1.2 节 “更改 HTTP 最大连接数”。
- 更改 JVM 内存大小。请参见第 C.1.3 节 “更改 JVM 内存大小”。

C.1.1. 更改 AIP 最大连接数

AIP 最大连接数在安装时配置。默认设置取决于 SGD Gateway 主机上可用的内存资源。

可以将此设置改为更适合您的部署的值。有关如何计算 SGD Gateway 使用的 AIP 最大连接数的详细信息，请参见第 C.1.1.1 节 “计算 AIP 连接数”。

要更改 AIP 最大连接数，请使用带 --routes-aip-maxcon 选项的 gateway config edit 命令。例如，要将 AIP 最大连接数更改为 3000，请运行以下命令：

```
# /opt/SUNWsgdg/bin/gateway config edit --routes-aip-maxcon 3000
```

必须重新启动 SGD Gateway 才能启用所做的任何更改。

C.1.1.1. 计算 AIP 连接数

SGD Gateway 使用的 AIP 连接数取决于 SGD 并发用户数以及他们运行的应用程序数，具体如下：

AIP 连接数 = (应用程序数 + 3) x SGD 用户数

例如，如果 SGD Gateway 具有 1000 个 SGD 用户，每个用户运行四个应用程序，则需要的并发 AIP 最大连接数如下：

(4 + 3) x 1000 = 7000 个 AIP 连接

C.1.2. 更改 HTTP 最大连接数

HTTP 最大连接数在安装时配置。此设置定义最大并发用户数。默认值为 100。

要更改 HTTP 最大连接数，请使用带 --routes-http-maxcon 选项的 gateway config edit 命令。例如，要将 HTTP 最大连接数更改为 200，请运行以下命令：

```
# /opt/SUNWsgdg/bin/gateway config edit --routes-http-maxcon 200
```

必须重新启动 SGD Gateway 才能启用所做的任何更改。

C.1.3. 更改 JVM 内存大小

更改 AIP 和 HTTP 最大连接数时，可能需要更改分配给 SGD Gateway 的 JVM 的内存大小。为此，请编辑 /opt/SUNWsgdg/proxy/etc/tuning_parameters 文件中的以下设置：

- -Xms - JVM 的初始内存大小（以字节为单位）
- -Xmx - JVM 的最大内存大小（以字节为单位）

提示

可以将 K（kilo，千）和 M（mega，兆）修饰符用于这些设置。例如：960K = 960 千字节，512M = 512 兆字节。

有关如何计算 JVM 内存大小值的详细信息，请参见第 C.1.3.1 节 “计算 JVM 内存大小”。

注意

确保系统配置有足够的内存资源来支持您所做的 JVM 设置。

必须重新启动 SGD Gateway 才能启用所做的任何更改。

C.1.3.1. 计算 JVM 内存大小

SGD Gateway 使用的 JVM 内存量取决于并发 AIP 连接和 HTTP 连接数。

由于每个 SGD Gateway 连接大约需要 300 千字节的 JVM 内存，因此所需的 JVM 内存的计算公式为：

(AIP 连接数 + HTTP 连接数) x 300 千字节

例如，如果 SGD Gateway 具有 500 个 SGD 用户，每个用户运行两个应用程序。并发 AIP 最大连接数为：

(2 + 3) x 500 = 2500 个 AIP 连接

SGD Gateway 还必须能处理足够的 SGD Web 服务器并发 HTTP 连接。对于此示例，HTTP 最大连接数为：

250 个 HTTP 连接

因此，所需的 JVM 内存为：

(2500 + 250) x 300 千字节 = 806 兆字节（大约）。

注意

在 /opt/SUNWsgdg/proxy/etc/tuning_parameters 文件中，将 -Xms 和 -Xmx 参数设置为计算的 JVM 内存值。出于性能原因，-Xms 和 -Xmx 通常设置为同一值。

C.2. 配置 HTTP 重定向

默认情况下，SGD Gateway 会拒绝 TCP 端口 80 上的 HTTP 连接。

要启用 TCP 端口 80 上的连接，请使用 gateway config enable 命令来启用 HTTP 重定向服务，如下所示：

```
# /opt/SUNWsgdg/bin/gateway config enable --routes-http-redirect
```

必须重新启动 SGD Gateway 才能启用所做的任何更改。

C.3. 更改 SGD Gateway 的绑定端口

SGD Gateway 用于传入连接的接口和端口称为绑定端口。默认情况下，SGD Gateway 使用所有接口上的 TCP 端口 443 作为绑定端口。

要更改绑定端口，请使用带 --binding 选项的 gateway config edit 命令。例如，要将绑定端口更改为 TCP 端口 4443，请运行以下命令：

```
# /opt/SUNWsgdg/bin/gateway config edit --binding *:4443
```

或者，也可以通过在 SGD Gateway 主机上运行 /opt/SUNWsgdg/bin/gateway config create 命令来更改绑定端口。此命令提示您指定用于传入代理连接的接口和端口。

注意

gateway config create 命令将创建新配置并覆盖您以前所做的任何配置设置。

必须重新启动 SGD Gateway 才能启用所做的任何更改。

C.4. 使用未加密的 SGD 阵列连接

默认情况下，SGD Gateway 与阵列中 SGD 服务器之间的连接使用安全套接字层 (Secure Sockets Layer, SSL) 进行安全保护。这意味着 SSL 上的 AIP 数据使用 TCP 端口 5307，HTTPS 数据使用 TCP 端口 443。

要在 SGD Gateway 与阵列中的 SGD 服务器之间使用未加密连接，请参见第 C.4.1 节 “配置 Gateway 以使用未加密的 SGD 阵列连接”。

对于未加密连接，AIP 数据使用 TCP 端口 3144，HTTP 数据使用 TCP 端口 80。

C.4.1. 配置 Gateway 以使用未加密的 SGD 阵列连接

此过程介绍了如何重新配置 Gateway 部署以使用未加密连接。

1. 修改 Gateway 配置以使用未加密的 SGD 阵列连接。

   ```
   # gateway config create
   ```

   注意

   此命令将覆盖 Gateway 的当前配置。

   提示是否保护 Gateway 与阵列中的 SGD 服务器之间的连接安全时，请输入 n。

2. 删除 Gateway 的任何以前注册的 SGD 服务器。

   ```
   # /opt/SUNWsgdg/bin/gateway server remove --server sgd.example.com
   ```

   其中，sgd.example.com 是 SGD 服务器的名称。

   将从 Gateway 密钥库中删除 SGD 服务器的 CA 证书和 SSL 证书。

3. 确保将阵列中的 SGD 服务器配置为使用标准的未加密连接。

   针对阵列中的每个 SGD 服务器运行以下命令以关闭 SGD 安全服务。

```
# tarantella security disable
```

4. 向 Gateway 注册阵列中的 SGD 服务器。

```
# /opt/SUNWsgdg/bin/gateway server add --server sgd.example.com \
--certfile PeerCAcert.pem \
--url http://sgd.example.com
```

此示例使用别名 sgd.example.com 将 CA 证书 PeerCAcert.pem 添加到 SGD Gateway 密钥库。SGD Web 服务器的 URL 是 http://sgd.example.com。

5. 重新启动 Gateway。

```
# /opt/SUNWsgdg/bin/gateway restart
```

C.5. 使用外部 SSL 加速器

默认情况下，SGD Gateway 配置为使用通过 SSL 进行安全保护的传入 HTTP 和 AIP 数据连接。Gateway 也支持使用外部 SSL 加速器进行 SSL 处理。

要将外部 SSL 加速器与 Gateway 结合使用，请执行以下操作：

- 配置外部 SSL 加速器来解密 SSL 连接并将其作为未加密的连接转发给 Gateway。
- 在 Gateway 上启用外部 SSL 加速器支持。

  这将使 Gateway 能够在安全端口上接受未加密连接。请参见第 C.5.1 节 “如何启用外部 SSL 加速器支持”。
- 确保客户端设备将 SSL 加速器用作网络入口点。

  通常，SSL 加速器同时还是负载平衡器。要配置 SGD 服务器和 Gateway 实现负载平衡部署，请参见第 2.1.2 节 “负载平衡部署”中的说明。

C.5.1. 如何启用外部 SSL 加速器支持

确保没有任何用户通过 Gateway 连接到 SGD。

1. 在 SGD Gateway 主机上，以超级用户 (root) 身份登录。
2. 启用对未加密传入连接的支持。

   更改 gateway.xml 文件的符号链接，以便其链接到 gateway-plaintext.xml 文件，而不是默认设置 gateway-ssl.xml。

   运行以下命令：

```
# ln -fs /opt/SUNWsgdg/etc/gateway-plaintext.xml /opt/SUNWsgdg/etc/gateway.xml
```

3. （可选）更改 Gateway 的绑定端口。

   根据您的网络配置，您可能还需要更改 SGD Gateway 的绑定端口。

   请参见第 C.3 节 “更改 SGD Gateway 的绑定端口”。

4. 重新启动 SGD Gateway。

```
# /opt/SUNWsgdg/bin/gateway restart
```

C.6. 配置 SGD Gateway 的密码

对于 SSL 连接，Gateway 支持众多密码套件。有关支持的密码套件的列表，请参见《Oracle Secure Global Desktop 发行版 4.7 平台支持和发行说明》。

在安装期间，会将 Gateway 配置为使用只包含高级密码的密码集。这意味着到 Gateway 的 SSL 连接将始终使用增强的安全性。如果需要，可以将 Gateway 配置为使用其他密码集。

C.6.1. 如何为 Gateway 配置密码

1. 停止 Gateway。

```
# /opt/SUNWsgdg/bin/gateway stop
```

2. 配置所需的密码。

   在 /opt/SUNWsgdg/etc 目录中，编辑 ciphersuites.xml 文件。

   默认情况下，ciphersuites.xml 文件包含以下高级密码条目。

```
<ciphersuites>
 <cipher>SSL_RSA_WITH_RC4_128_MD5</cipher>
 <cipher>SSL_RSA_WITH_RC4_128_SHA</cipher>
 <cipher>TLS_RSA_WITH_AES_128_CBC_SHA</cipher>
 <cipher>TLS_RSA_WITH_AES_256_CBC_SHA</cipher>
 <cipher>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</cipher>
 <cipher>TLS_DHE_RSA_WITH_AES_256_CBC_SHA</cipher>
 <cipher>TLS_DHE_DSS_WITH_AES_128_CBC_SHA</cipher>
 <cipher>TLS_DHE_DSS_WITH_AES_256_CBC_SHA</cipher>
 <cipher>SSL_RSA_WITH_3DES_EDE_CBC_SHA</cipher>
 <cipher>SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA</cipher>
 <cipher>SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA</cipher>
</ciphersuites>
```

3. 检查以下条目是否存在于 /opt/SUNWsgdg/etc/gateway.xml 文件中，以便包含 ciphersuites.xml。

```
<service id="sgd-ssl-service" class="SSL">
              ...
  <keystore file="/opt/SUNWsgdg/proxy/etc/keystore.client"
   password="/opt/SUNWsgdg/etc/password"/>
   <xi:include href="ciphersuites.xml" parse="xml"/>
</service>
               ...
<service id="http-ssl-service" class="SSL">
              ...
  <keystore file="/opt/SUNWsgdg/proxy/etc/keystore.client"
   password="/opt/SUNWsgdg/etc/password"/>
  <xi:include href="ciphersuites.xml" parse="xml"/>
</service>
```

4. 重新启动 Gateway。

```
# /opt/SUNWsgdg/bin/gateway start
```

C.7. 将客户端证书用于 SGD Gateway

可以使用客户端证书来增强 SGD Gateway 的安全性，客户端证书会将访问限定在具有有效证书的用户内。

客户端证书是指安装在客户端设备上的浏览器中的 SSL 证书。有关如何安装客户端证书的详细信息，请参见所用浏览器的联机文档。

如果需要为新的客户端证书生成证书签名请求 (certificate signing request, CSR)，请参见第 C.7.2 节 “如何为客户端证书生成 CSR”。

以下过程使用 keytool 应用程序。有关如何使用 keytool 应用程序的详细信息，请参见 JDK Tools and Utilities（JDK 工具和实用程序）文档。

C.7.1. 如何将 SGD Gateway 配置为使用客户端证书

1. 在 SGD Gateway 主机上，以超级用户 (root) 身份登录。
2. 停止 SGD Gateway。

```
# /opt/SUNWsgdg/bin/gateway stop
```

3. 将 SGD Gateway 配置为使用客户端证书进行 HTTPS 客户端连接。

将 <needClientAuth> 条目添加到 /opt/SUNWsgdg/etc/gateway.xml 文件中，如下所示：

```
<service id="http-ssl-service" class="SSL">
   <needClientAuth>true</needClientAuth>
      <!-- Decrypts HTTPS traffic -->
      <subService id="ssl-splitter">
         <binding>*</binding>
      </subService>
```

4. （可选）将客户端证书导入到 SGD Gateway 客户端密钥库中。

注意

如果客户端证书是由受信任的证书颁发机构 (Certificate Authority, CA) 签名的，则无需执行此步骤。

按如下方式使用 keytool 命令：

```
# /opt/SUNWsgdg/java/default/bin/keytool -importcert \
-alias mycert -keystore /opt/SUNWsgdg/proxy/etc/keystore.client \
-file mycert.crt -storepass ‘cat /opt/SUNWsgdg/etc/password‘
```

在此示例中，客户端证书 mycert.crt 导入到 SGD Gateway 客户端密钥库中。客户端证书使用 mycert 别名存储。

5. 启动 SGD Gateway。

```
# /opt/SUNWsgdg/bin/gateway start
```

C.7.2. 如何为客户端证书生成 CSR

要获取可用于 Gateway 的客户端证书，首先需要生成 CSR。随后将 CSR 发送给证书颁发机构 (Certificate Authority, CA) 进行签名。

注意

以下过程介绍了如何使用 Gateway 主机上的 keytool 应用程序生成 CSR。但是，不一定要使用此过程中介绍的步骤。您可以改用自己喜欢的证书管理工具来生成 CSR。

1. 在 SGD Gateway 主机上，以超级用户 (root) 身份登录。
2. 生成自签名证书和相应的私钥。

   按如下方式使用 keytool 命令：

   ```
   # /opt/SUNWsgdg/java/default/bin/keytool -genkeypair -keyalg RSA \
   -alias mycert -keystore keystore.mycert -storepass letmein
   ```

   在此示例中，将创建自签名证书和私钥并将其存储在名为 keystore.mycert 的密钥库中。密钥对使用 mycert 别名存储。

3. 为自签名证书生成 CSR。

   按如下方式使用 keytool 命令：

   ```
   # /opt/SUNWsgdg/java/default/bin/keytool -certreq  \
   -alias mycert -keystore keystore.mycert -storepass letmein \
   -file /tmp/gateway-name.csr
   ```

   在此示例中，生成了 CSR 并将其存储在 /tmp/gateway-name.csr 文件中，其中 gateway-name 是 Gateway 的名称。

C.8. 启用 Balancer Manager 应用程序

Apache 反向代理包括名为 Balancer Manager 的 Web 应用程序。通过 Balancer Manager，可以管理反向代理使用的负载平衡组中的 SGD Web 服务器。

使用 Balancer Manager，可以执行以下操作：

- 查看负载平衡组中 SGD Web 服务器的状态信息
- 查看和更改 SGD Web 服务器的负载平衡路由
- 从负载平衡组中删除 SGD Web 服务器

要启用 Balancer Manager，请删除反向代理配置文件 /opt/SUNWsgdg/httpd/apache-version/conf/extra/gateway/httpd-gateway.conf 中用于禁用该应用程序的注释。

```
# Allows the configuration of load balancing parameters
#
#   <Location /balancer-manager>
#       SetHandler balancer-manager
#       Order Deny,Allow
#       Deny from all
#       Allow from all
#   </Location>
```

必须重新启动 Gateway 才能启用所做的任何更改。

```
# /opt/SUNWsgdg/bin/gateway restart
```

要访问 Balancer Manager，请启动浏览器并转至 https://gateway.example.com/balancer-manager，其中 gateway.example.com 为 SGD Gateway 主机。

有关配置 Balancer Manager 的更多详细信息，请参见 Apache mod_proxy_balancer 文档。

C.9. 反射服务

反射服务是 SGD Gateway 路由代理组件使用的一组 RESTful Web 服务。使用反射服务，SGD Gateway 管理员可以配置路由、服务、日志记录级别以及连接，并显示路由代理的状态信息。

本节包括以下反射服务主题：

- 第 C.9.1 节 “启用反射服务”
- 第 C.9.2 节 “使用反射服务”

C.9.1. 启用反射服务

默认情况下，不会为 SGD Gateway 启用反射服务。

可以为反射服务启用下面的一种或两种访问方法：

- 未授权访问 - 用户无需进行验证。

  默认情况下，仅可以从 SGD Gateway 主机进行未授权访问。

  有关如何启用未授权访问的详细信息，请参见第 C.9.1.1 节 “如何对反射服务启用未授权访问”。

- 授权访问 - 用户必须进行验证才能访问反射服务。

  有关如何启用授权访问的详细信息，请参见第 C.9.1.2 节 “如何对反射服务启用授权访问”。

C.9.1.1. 如何对反射服务启用未授权访问

1. 在 SGD Gateway 主机上，以超级用户 (root) 身份登录。
2. 对反射服务启用未授权访问。

   ```
   # /opt/SUNWsgdg/bin/gateway config enable --services-reflection
   ```

3. （可选）更改反射服务使用的接口。

小心

默认情况下，仅可以从 SGD Gateway 主机对反射服务进行未经验证的访问。在其他接口上启用未经验证的访问可能会带来安全风险。

对反射服务进行未授权访问的默认接口为 localhost 回送接口。以下示例显示了如何在所有接口上启用未授权访问：

```
# /opt/SUNWsgdg/bin/gateway config edit \
--services-reflection-binding *:81
```

4. （可选）更改反射服务使用的端口。

   对反射服务进行未授权访问的默认端口为 TCP 端口 81。您可以将此端口更改为其他未使用的端口，如下所示：

   ```
   # /opt/SUNWsgdg/bin/gateway config edit \
   --services-reflection-binding localhost:portnum
   ```

   其中，portnum 是反射服务使用的端口号。

5. 重新启动 SGD Gateway。

   ```
   # /opt/SUNWsgdg/bin/gateway restart
   ```

6. 访问反射服务。

   在 SGD Gateway 主机上，可以启动浏览器并转至 http://localhost:81。

   此时将显示反射服务的主页。

C.9.1.2. 如何对反射服务启用授权访问

1. 在 SGD Gateway 主机上，以超级用户 (root) 身份登录。
2. 导出反射服务的证书和私钥。

   反射服务的证书和私钥存储在反射服务密钥库中，位于 /opt/SUNWsgdg/proxy/etc/keystore.reflection。此密钥库是在安装 SGD Gateway 期间自动创建的。

   默认情况下，反射服务密钥库包含一个自签名证书和一个密钥对。

   a. 导出反射服务的证书。

      ```
      # /opt/SUNWsgdg/java/default/bin/keytool -exportcert \
      -alias server-name -rfc \
      -keystore /opt/SUNWsgdg/proxy/etc/keystore.reflection \
      -storepass "$(cat /opt/SUNWsgdg/etc/password)" \
      -file client.pem
      ```

      其中，server-name 是反射密钥库中反射服务证书的别名，client.pem 是导出的证书的文件名。

      有关如何使用 keytool 应用程序的详细信息，请参见 JDK Tools and Utilities（JDK 工具和实用程序）文档。

   b. 导出反射服务的私钥。

      使用 SGD Gateway 随附的 KeyManager 应用程序。

      ```
      # /opt/SUNWsgdg/java/default/bin/java \
      -jar /opt/SUNWsgdg/proxy/KeyManager.jar export \
      --keyfile client.key \
      --keystore /opt/SUNWsgdg/proxy/etc/keystore.reflection \
      --keyalias alias-name \
      --keypass "$(cat /opt/SUNWsgdg/etc/password)" \
      --storepass "$(cat /opt/SUNWsgdg/etc/password)"
      ```

      其中，alias-name 是反射密钥库中反射服务密钥的别名，client.key 是导出的密钥的文件名。

3. 在客户端设备上安装证书和私钥。

证书和私钥供客户端设备用来对反射服务进行授权。

要将证书和密钥导入到浏览器证书库中，必须先将证书和密钥转换为 PKCS12 格式的文件。例如：

```
# openssl pkcs12 -export -in mycert.crt -inkey mycert_key.pem -out mycert.p12
```

此命令将证书文件 mycert.crt 和关联的私钥 mycert_key.pem 转换为 PKCS12 格式的证书文件 mycert.p12。

有关如何将 PKCS12 格式的证书导入到浏览器中的更多详细信息，请参见所用浏览器的联机文档。

4. 对反射服务启用授权访问。

   在 SGD Gateway 主机上，运行以下命令：

   ```
   # /opt/SUNWsgdg/bin/gateway config enable --services-reflection-auth
   ```

5. （可选）更改反射服务使用的接口和端口。

   用于对反射服务进行授权访问的默认绑定为所有接口上的 TCP 端口 82。您可以将其更改为其他未使用的接口和端口，如下所示：

   ```
   # /opt/SUNWsgdg/bin/gateway config edit \
   --services-reflection-binding int:portnum
   ```

   其中，int 和 portnum 分别为反射服务使用的接口和端口号。

6. 重新启动 SGD Gateway。

   ```
   # /opt/SUNWsgdg/bin/gateway restart
   ```

7. 使用证书和私钥从客户端设备连接到反射服务。

   - 使用 curl 命令：

     ```
     $ curl --cert client.pem --key client.key -k -X GET https://gateway.example.com:82
     ```

     在此示例中，curl 命令用于访问反射服务的主页，网址为：https://gateway.example.com:82，其中 gateway.example.com 为 SGD Gateway 的名称。反射服务的证书和私钥分别为 client.pem 和 client.key。

   - 使用浏览器：

     转至 https://gateway.example.com:82，其中 gateway.example.com 为 SGD Gateway 的名称。

     此时将显示反射服务的主页。

C.9.2. 使用反射服务

使用客户端应用程序访问反射服务提供的 RESTful Web 服务。以下列举了一些合适的客户端应用程序：

- 浏览器。 使用浏览器是访问反射服务的最简单方法。但是，浏览器仅支持 HTTP GET 请求，因此只能用于访问检索信息的 RESTful Web 服务。实际上，浏览器适用于显示状态信息和列出路由代理的路由和服务等任务。
- curl。 curl 是 UNIX 和 Linux 平台的命令行工具，支持 HTTP GET、PUT、POST 以及 DELETE 请求。这意味着可以使用反射服务提供的全部 RESTful Web 服务。该工具的输出可以重定向到某个文件或其他程序做进一步处理。

如果您自己有支持 RESTful Web 服务的客户端应用程序，也可以使用该应用程序来访问反射服务。

注意

使用反射服务来更改路由代理的配置时，无需重新启动 SGD Gateway。

反射服务返回的数据可按以下格式输出：

- ASCII。 这是默认输出格式。返回的数据采用制表符分隔的 ASCII 格式。如果要进一步处理数据（例如解析），此输出格式很有用。

- HTML。 返回的数据采用 HTML 格式，适用于在浏览器中显示。要返回 HTML 格式的输出，请将 /html 附加到 Web 服务统一资源标识符 (Uniform Resource Identifier, URI) 的末尾。

C.9.2.1. 关于 RESTful Web 服务

表 C.1 “SGD Gateway 反射服务的 RESTful Web 服务”列出了 SGD Gateway 反射服务的 RESTful Web 服务。

表 C.1. SGD Gateway 反射服务的 RESTful Web 服务

相对 URI	HTTP 请求方法	描述
/	GET	显示路由代理的高级信息，例如运行时间。
/service	GET	列出可用的服务。 服务代表路由代理创建传入连接的入口点。
/service/Service-Id	GET	列出由 Service-Id 标识的服务的信息。
/service/Service-Id	PUT	启动由 Service-Id 标识的服务。
/service/Service-Id	DELETE	停止由 Service-Id 标识的服务。
/client	GET	列出可用的客户端。 客户端代表路由代理构建传出连接的出口点。
/client/Client-Id	GET	列出由 Client-Id 标识的客户端的信息。
/route	GET	列出可用的路由。 路由代表一条通过路由代理的路径，从服务的传入连接到客户端的传出连接。
/route/Route-Id	GET	列出由 Route-Id 标识的路由的信息。
/route/Route-Id	PUT	启动由 Route-Id 标识的路由。
/route/Route-Id	DELETE	停止由 Route-Id 标识的路由。
/route/Route-Id/connection	GET	列出由 Route-Id 标识的特定路由的连接。
/route/Route-Id/connection/Connection-Id	DELETE	终止由 Connection-Id 标识的连接。
/connection	GET	列出当前运行的所有连接（所有路由）。
/logging/level	GET	显示全局日志记录级别。
/logging/level/Log-Level	PUT	设置路由代理的全局日志记录级别。
/logging/Package/level	GET	显示路由代理的特定组件的日志记录级别。
/logging/Package/level/Log-Level	PUT	设置路由代理的特定组件的日志记录级别。

要访问某个 RESTful Web 服务，请将该 Web 服务的相对 URI 附加到反射服务的 URL。

例如，要列出 SGD Gateway gateway.example.com 的可用路由，请将 /route 附加到反射服务的 URL，如下所示：

```
$ curl --cert client.pem --key client.key -k -X GET https://gateway.example.com:82/route
```

其中，client.pem 和 client.key 分别是反射服务的证书和私钥。在此示例中，客户端需要先获得授权，然后才能访问反射服务。

C.9.2.2. 使用反射服务的示例

以下所有示例均使用 curl 命令作为访问反射服务的客户端应用程序。

这些示例对名为 gateway.example.com 的 SGD Gateway 上的反射服务使用经过验证的访问。客户端使用证书 client.pem 和私钥 client.key 来授权。

要列出 SGD Gateway 的可用服务，请运行以下命令：

```
$ curl --cert client.pem --key client.key -k \
-X GET https://gateway.example.com:82/service
```

要停止路由，请指定反射服务对该路由使用的路由 ID：

```
$ curl --cert client.pem --key client.key -k \
-X GET https://gateway.example.com:82/route
Route Id  Route Uptime   Service Id  ...
0         21h18m20s743m  ssgd-route-service  ...
1         21h18m20s736m  shttp-ssl-service   ...
$ curl --cert client.pem --key client.key -k \
-X DELETE https://gateway.example.com:82/route/1
```

要将全局日志记录级别设置为 FINER，请运行以下命令：

```
$ curl --cert client.pem --key client.key -k \
-X PUT https://gateway.example.com:82/logging/level/FINER
```

附录 D. SGD Gateway 故障排除

本章包括有关故障排除的主题，用于帮助您诊断和修复 Oracle Secure Global Desktop Gateway (SGD Gateway) 的问题。

本章包括以下主题：

D.1. 日志记录和诊断

本节介绍 SGD Gateway 的日志记录和诊断功能。

本节包括以下主题：

D.1.1. 关于 SGD Gateway 日志记录

SGD Gateway 日志记录使用 Java 日志记录应用程序编程接口 (application programming interface, API)。有关 Java 中如何实现日志记录的更多详细信息，请参见 http://download.oracle.com/javase/6/docs/technotes/guides/logging/overview.html。

D.1.1.1. 更改日志记录级别

SGD Gateway 随附了一个日志记录属性配置文件 logging.properties。此文件位于 /opt/SUNWsgdg/proxy/etc 目录中。

您可以编辑 logging.properties 文件以更改默认日志记录级别，以及配置特定 SGD Gateway 服务的日志记录级别。每个 SGD Gateway 服务均由 logging.properties 文件中的一个 async.channel 条目表示。

例如，如果要增加传入和传出 TCP 连接的日志记录级别，请将 TCP 服务日志记录级别设置为 FINEST。取消 logging.properties 文件中以下行的注释：

```
# async.channel.tcp.level=FINEST
```

FileHandler 类文档介绍了可在 logging.properties 文件中使用的日志记录级别参数。

必须重新启动 SGD Gateway 才能启用通过编辑 logging.properties 文件所做的任何日志记录级别更改。

注意

还可以使用 SGD Gateway 反射服务更改日志记录级别。有关配置和使用反射服务的信息，请参见第 C.9 节 “反射服务”。

D.1.1.2. 日志文件位置

如果您有 SGD Gateway 方面的问题，请查看以下日志文件：

- 路由代理日志文件。这些日志文件的位置和名称在 logging.properties 文件中设置。默认情况下，SGD Gateway 在 SGD Gateway 主机的 /opt/SUNWsgdg/proxy/var/log 目录中创建路由代理日志文件。
- 反向代理日志文件。有关 HTTP 和 HTTPS 连接的负载平衡和代理服务器活动的详细信息均记录到 SGD Gateway 主机的 /opt/SUNWsgdg/httpd/apache-version/logs 目录中的 Apache 日志文件。

- SGD 服务器日志文件。阵列中的每个 SGD 服务器均会将错误消息写入 SGD 服务器主机的 /opt/tarantella/var/log 目录中的日志文件。有关配置 SGD 服务器的日志记录的更多详细信息，请参见《Oracle Secure Global Desktop Administration Guide for Release 4.7》第 6 章中的 “Monitoring and Logging”。

D.1.2. 显示 SGD Gateway 进程信息

启动 SGD Gateway 后，路由代理的进程 ID 将存储到 SGD Gateway 主机的 /opt/SUNWsgdg/proxy/var/run/proxy.pid 文件中。

反向代理的进程 ID 将存储到 /opt/SUNWsgdg/httpd/apache-version/logs/httpd.pid 文件中。在 httpd.conf Apache 配置文件中使用 PidFile 指令可以更改此文件位置。

要显示正在运行的 SGD Gateway 进程，请在 SGD Gateway 主机上运行以下命令：

```
# ps -ef| grep SUNWsgdg
```

D.1.3. 从命令行检查配置

您可以使用以下命令检查 SGD Gateway 配置。

- gateway status - 显示 SGD Gateway 的状态信息。

  在 SGD Gateway 主机上运行以下命令：

  ```
  # /opt/SUNWsgdg/bin/gateway status
  ```

  有关此命令的更多信息，另请参见第 B.23 节 “gateway status”。

- tarantella gateway list - 显示授权 SGD 阵列使用的 SGD Gateway 的列表。

  在阵列中的任意 SGD 服务器上运行以下命令：

  ```
  $ tarantella gateway list
  ```

  有关使用 tarantella gateway 命令的更多详细信息，请参见第 B.27 节 “tarantella gateway 命令”。

- tarantella config list - 显示 SGD 阵列的全局设置。

  在任意 SGD 服务器上运行以下命令以显示 --security-gateway 属性设置。此属性确定允许哪些 SGD Client 使用 SGD Gateway。

  ```
  $ tarantella config list --security-gateway
  ```

  有关此属性的更多详细信息，请参见第 B.31 节 “--security-gateway 属性”。

D.2. 更改 SGD 服务器的对等 DNS 名称

对等 DNS 名称是 SGD 服务器用于向阵列中的其他 SGD 服务器标识自身的 DNS 名称。例如，boston.example.com。

更改 SGD 服务器的对等 DNS 名称后，Gateway 可能无法再连接到该服务器。这是因为 Gateway 使用的证书不包含新的 DNS 名称。

您可能必须按如下所述重新配置 Gateway 部署：

1. （可选）安装新的 SGD 服务器 SSL 证书。请参见第 2.2.2.1 节 “如何安装 SGD 服务器证书”。

   如果新的对等 DNS 名称未包含在 SGD 服务器使用的 SSL 证书中，则需要执行此步骤。必须替换 SGD 服务器上的 SSL 证书并在每个 Gateway 上安装新的 SSL 证书。

2. （可选）安装 SGD 服务器的新 CA 证书。请参见第 2.2.2.1 节 “如何安装 SGD 服务器证书”。

   如果更改阵列中主服务器的对等 DNS 名称，则需要执行此步骤。必须重新生成用于阵列内安全通信的证书并在每个 Gateway 上安装新的 CA 证书。

有关如何更改 SGD 服务器的对等 DNS 名称的更多信息，请参见《Oracle Secure Global Desktop Administration Guide for Release 4.7》第 1 章中的 "Peer DNS Names" 一节。

D.3. SGD Gateway 错误消息

SGD Gateway 错误消息会报告给路由代理日志文件（位于 SGD Gateway 主机的 /opt/SUNWsgdg/proxy/var/log 目录中）。

表 D.1 “SGD Gateway 的错误消息”中列出了一些典型的 SGD Gateway 错误消息以及可能原因的解释。

表 D.1. SGD Gateway 的错误消息

错误消息	可能原因
Failed to validate token: Token time not yet valid	SGD Gateway 上的时钟与阵列中 SGD 服务器上的时钟不同步。
Failed to decode token: No trusted signature found	SGD Gateway 上尚未安装 SGD 服务器的 CA 证书
Failed to validate token: No recipient available to decrypt token	SGD 阵列上尚未安装 SGD Gateway 证书
SSL error: Check the proxy SSL keystore has valid trusted certificates	SGD Gateway 上尚未安装 SGD 服务器的 SSL 证书