Oracle® Secure Global Desktop

Gateway 管理者ガイド (リリース 4.7 用)

E35250-01
2012 年 8 月

Oracle® Secure Global Desktop: Gateway 管理者ガイド (リリース 4.7 用)

概要

このガイドでは、オラクル Secure Global Desktop Gateway をインストール、構成、および操作する方法について説明します。

ドキュメント作成日: 2013-01-04 (revision: 1406)

目次

はじめに v
1. 対象ユーザー v
2. ドキュメントの構成 v
3. ドキュメントのアクセシビリティー v
4. 関連ドキュメント v
5. 表記規則 v
1. SGD Gateway のインストール 1
1.1. SGD Gateway について 1
1.2. システム要件 1
1.2.1. 既知の問題 1
1.3. インストールの実行 1
1.3.1. SGD Gateway をインストールする方法 2
1.4. SGD Gateway のアップグレード 3
1.4.1. SGD Gateway をアップグレードする方法 3
2. SGD Gateway の構成 5
2.1. SGD Gateway の配備 5
2.1.1. 基本的な配備 5
2.1.2. 負荷分散された配備 7
2.2. SGD Gateway の構成タスク 9
2.2.1. クライアントデバイスから SGD Gateway への接続 10
2.2.2. SGD Gateway から SGD サーバーへの接続 11
2.2.3. クライアントデバイスからロードバランサへの接続 13
2.2.4. ロードバランサから SGD Gateway への接続 13
2.3. SGD Gateway の制御 14
2.3.1. SGD Gateway の起動 14
2.3.2. SGD Gateway の停止 14
2.3.3. SGD Gateway の再起動 14
2.4. SGD Gateway の削除 14
2.4.1. SGD Gateway を削除する方法 15
A. SGD Gateway のアーキテクチャーの概要 17
A.1. SGD Gateway のアーキテクチャー 17
A.2. SGD Gateway のコンポーネント 20
A.2.1. ルーティングトークンについて 21
A.2.2. SGD Gateway で使用されるキーストア 21
A.2.3. ルーティングプロキシ構成ファイル 22
A.2.4. Apache Web サーバーの設定ファイル 22
A.2.5. SGD Gateway で使用される Apache モジュール 23
B. コマンド行リファレンス 25
B.1. gateway コマンド 25
B.2. gateway cert export 26
B.3. gateway config 26
B.4. gateway config create 27
B.5. gateway config disable 27
B.6. gateway config edit 28
B.7. gateway config enable 29
B.8. gateway config list 30
B.9. gateway key import 31
B.10. gateway restart 32
B.11. gateway server 32
B.12. gateway server add 32
B.13. gateway server list 33
B.14. gateway server remove 34
B.15. gateway setup 34
B.16. gateway sslcert 34
B.17. gateway sslcert export 35
B.18. gateway sslcert print 35
B.19. gateway sslkey 36

B.20. gateway sslkey export 36
B.21. gateway sslkey import 36
B.22. gateway start 37
B.23. gateway status 38
B.24. gateway stop 38
B.25. gateway uninstall 38
B.26. gateway version 39
B.27. tarantella gateway コマンド 39
B.28. tarantella gateway add 40
B.29. tarantella gateway list 40
B.30. tarantella gateway remove 41
B.31. --security-gateway 属性 41
C. 詳細構成 45
C.1. SGD Gateway の調整 45
C.1.1. AIP 接続の最大数の変更 45
C.1.2. HTTP 接続の最大数の変更 46
C.1.3. JVM のメモリーサイズの変更 46
C.2. HTTP リダイレクトの構成 47
C.3. SGD Gateway のバインディングポートの変更 47
C.4. SGD アレイに対する非暗号化接続の使用 47
C.4.1. SGD アレイへの非暗号化接続を使用するための Gateway の構成 48
C.5. 外部 SSL アクセラレータの使用 48
C.5.1. 外部 SSL アクセラレータのサポートを有効にする方法 49
C.6. SGD Gateway 暗号化方式の構成 49
C.6.1. Gateway の暗号化方式を構成する方法 49
C.7. SGD Gateway でのクライアント証明書の使用 50
C.7.1. クライアント証明書が使用されるように SGD Gateway を構成する方法 50
C.7.2. クライアント証明書の CSR を生成する方法 51
C.8. Balancer Manager アプリケーションの有効化 51
C.9. リフレクションサービス 52
C.9.1. リフレクションサービスの有効化 52
C.9.2. リフレクションサービスの使用 54
D. SGD Gateway のトラブルシューティング 57
D.1. ロギングと診断 57
D.1.1. SGD Gateway の口ギングについて 57
D.1.2. SGD Gateway のプロセス情報の表示 58
D.1.3. コマンド行からの設定の確認 58
D.2. SGD サーバーのピア DNS 名の変更 58
D.3. SGD Gateway のエラーメッセージ 59

はじめに

『オラクル Secure Global Desktop Gateway 管理者ガイド (リリース 4.7 用)』では、オラクル Secure Global Desktop (SGD Gateway) のインストール、構成、および操作の手順について説明します。このドキュメントはシステム管理者向けに記述されています。

1. 対象ユーザー

このドキュメントは、SGD Gateway の新規ユーザーを対象としています。Web 関連のテクノロジに関する知識と、Windows および UNIX のプラットフォームに関する一般的な知識が必要となります。

2. ドキュメントの構成

このドキュメントは次のように構成されています。

- 1章SGD Gateway のインストールでは、SGD Gateway をインストールする方法について説明します。
- 2章SGD Gateway の構成では、SGD Gateway をネットワーク用に構成する方法について説明します。
- 付録A SGD Gateway のアーキテクチャーの概要では、SGD Gateway のアーキテクチャーについて説明します。
- 付録B コマンド行リファレンスでは、SGD Gateway をコマンド行から構成および制御する方法について説明します。
- 付録C 詳細構成では、SGD Gateway のリフレクションサービスを構成および使用する方法など、SGD Gateway の高度な構成について説明します。
- 付録D SGD Gateway のトラブルシューティングでは、SGD Gateway の問題の診断と解決に役立つ、トラブルシューティング関連の情報について説明します。

3. ドキュメントのアクセシビリティー

アクセシビリティーに対するオラクルのコミットメントについては、オラクルのアクセシビリティープログラム の Web サイト (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc) を参照してください。

Oracle Support へのアクセス

お客様は、My Oracle Support を通じてオンラインでのサポートをご利用いただけます。詳細については、http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info (聴覚障害をお持ちの方は http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs) を参照してください。

4. 関連ドキュメント

この製品のドキュメントは、次のサイトで入手できます。

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

追加情報については、次のマニュアルを参照してください。

- オラクル Secure Global Desktop 管理者ガイド (リリース 4.7 用)
- オラクル Secure Global Desktop インストールガイド (リリース 4.7 用)
- オラクル Secure Global Desktop ユーザーガイド (リリース 4.7 用)
- オラクル Secure Global Desktop のプラットフォームサポートおよびリリースノート (リリース 4.7 用)
- オラクル Secure Global Desktop Security Guide for Release 4.7

5. 表記規則

このドキュメントでは、次のような表記規則を使用しています。

表記規則	意味
ボールド体	ボールド体の個所は、アクションに関連するグラフィカルユーザーインタフェース要素、テキストや用語集で定義された用語などを表しています。
イタリック体	イタリック体の個所は、書名、強調語句、特定の値が指定されるプレースホルダ変数などを表しています。
モノスペース体	モノスペース体の個所は、パラグラフ内のコマンド、URL、例示されているコード、画面上に表示されるテキスト、ユーザーが入力するテキストなどを表しています。

第1章 SGD Gateway のインストール

この章では、オラクル Secure Global Desktop Gateway (SGD Gateway) の簡単な紹介に続き、SGD Gateway ソフトウェアをインストールする方法について説明します。この章では、SGD Gateway のシステム要件の詳細についても説明します。

この章の内容は、次のとおりです。

- 「SGD Gateway について」
- 「システム要件」
- 「インストールの実行」
- 「SGD Gateway のアップグレード」

1.1. SGD Gateway について

SGD Gateway は、非武装ゾーン (DMZ) で SGD アレイの前に配備されるように設計されたプロキシサーバーです。これにより、組織の内部ネットワーク上に SGD アレイを配置できるようになります。また、アレイ内の SGD サーバーに接続する前に、すべての接続を DMZ で認証できます。

ファイアウォール越え (ファイアウォール転送とも呼ばれる) を使用して SGD サーバーを実行する代わりに、SGD Gateway を使用できます。

SGD Gateway は HTTP 接続の負荷分散を管理するため、SGD に含まれている JavaServer Pages (JSP) テクノロジの負荷分散ページを使用する必要はありません。

1.2. システム要件

SGD Gateway ホストでサポートされるインストールプラットフォームは、http://www.oracle.com/technetwork/jp/index.html/documentation/sgd-193668.html で参照可能な『オラクル Secure Global Desktop のプラットフォームサポートおよびリリースノート (リリース 4.7 用)』に一覧表示されています。

SGD Gateway とともに使用される SGD サーバーには、次の要件が適用されます。

- セキュアモード。デフォルトでは、SGD Gateway では SGD サーバーへのセキュア接続が使用されます。SGD サーバーのセキュア接続が有効になっている必要があります。ファイアウォールの転送が無効になっている必要があります。

  標準インストールでは、SGD サーバーはセキュア接続を使用するように自動的に構成されます。SGD サーバーをセキュリティー保護する方法についての情報が必要な場合は、『オラクル Secure Global Desktop 管理者ガイド (リリース 4.7 用)』の、SGD サーバーへのセキュア接続に関する第 1 章を参照してください。
- SGD のバージョン。SGD サーバーでは SGD のバージョン 4.5 以降が実行されている必要があります。SGD バージョン 4.7 で Gateway バージョン 4.7 を使用することをお勧めします。
- クロックの同期。SGD サーバーと SGD Gateway のシステムクロックが同期していることが重要です。時間情報プロトコル (NTP) ソフトウェアまたは rdate コマンドを使用して、クロックが同期していることを確認してください。

SGD サーバーのシステム要件の詳細については、『オラクル Secure Global Desktop のプラットフォームサポートおよびリリースノート (リリース 4.7 用)』を参照してください。

1.2.1. 既知の問題

SGD Gateway のこのリリースでの既知の問題の詳細については、『オラクル Secure Global Desktop のプラットフォームサポートおよびリリースノート (リリース 4.7 用)』を参照してください。

1.3. インストールの実行

Oracle Solaris プラットフォームでは、pkgadd コマンドを使用して SGD Gateway をインストールします。

Linux プラットフォームでは、rpm コマンドを使用して SGD Gateway をインストールします。

デフォルトでは、SGD Gateway は /opt/SUNWsgdg ディレクトリにインストールされます。インストールディレクトリは、次のようにして変更できます。

- Oracle Solaris プラットフォーム – ソフトウェアのインストール時に、インストールプログラムによってインストールディレクトリの指定が求められます。
- Linux プラットフォーム – ソフトウェアのインストール時に rpm コマンドに --prefix オプションを使用することで、別のインストールディレクトリを選択できます

1.3.1. SGD Gateway をインストールする方法

1. ホスト上の一時ディレクトリに SGD Gateway パッケージを保存します。

   インストールメディアからインストールする場合、パッケージは gateway ディレクトリにあります。

   または、インストールプログラムを SGD Web サーバー https://server.example.com からダウンロードします。ここで、server.example.com は SGD サーバーの名前です。SGD Web サーバーの開始画面が表示されたら、「オラクル Secure Global Desktop のインストール」をクリックします。

   パッケージファイルは次のとおりです。

   - SUNWsgdg-version.sol-x86.pkg (x86 プラットフォーム版 Oracle Solaris)
   - SUNWsgdg-version.sol-sparc.pkg (SPARC テクノロジプラットフォーム版 Oracle Solaris)
   - SUNWsgdg-version.i386.rpm (Linux プラットフォーム)

   ここで、version は SGD Gateway のバージョン番号です。

2. ホストにスーパーユーザー (root) としてログインします。
3. SGD Gateway をインストールします。

   パッケージファイルが圧縮されている場合、インストール前にファイルを解凍する必要があります。

   x86 プラットフォーム版 Oracle Solaris にインストールする場合:

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

   SPARC テクノロジプラットフォーム版 Oracle Solaris にインストールする場合:

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

   注記

   Oracle Solaris プラットフォームでは、pwd: cannot determine current directory! というエラーメッセージが表示されてインストールが失敗した場合は、/tempdir ディレクトリに移動して、インストールを再度実行してください。

   Linux プラットフォームにインストールする場合:

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

4. SGD Gateway パッケージがパッケージデータベースに登録されていることを確認します。

   Oracle Solaris プラットフォームの場合:

   ```
   # pkginfo -x SUNWsgdg
   ```

   Linux プラットフォームの場合:

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

5. SGD Gateway のセットアッププログラムを実行します。

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

SGD Gateway のセットアッププログラムは次の設定を提示し、ユーザーは、それを受け入れることも変更することもできます。

- SGD Gateway ポート設定。SGD Gateway で着信接続に使用されるインタフェースとポートです。デフォルトでは、SGD Gateway はすべてのインタフェースのポート 443 で待機します。
- ネットワークエントリポイント。クライアントデバイスが SGD Gateway に接続するために使用するインターネットプロトコル (IP) アドレスまたはドメインネームシステム (DNS) 名、およびポートです。これは、SGD Gateway のアドレスと常に同じであるとは限りません。ネットワークの構成によっては、ロードバランサなどの外部デバイスのアドレスになることがあります。

  たとえば、ユーザーが SGD Gateway gateway1.example.com に直接接続する場合は、ネットワークエントリポイントとして gateway1.example.com:443 を入力します。

  ユーザーがロードバランサ lb.example.com を介して SGD Gateway に接続する場合は、ネットワークエントリポイントとして lb.example.com:443 を入力します。
- セキュア接続。SGD Gateway とアレイ内の SGD サーバーとの接続をセキュリティー保護するかどうか。デフォルトでは、SGD Gateway はセキュア接続を使用します。セキュア接続を使用するには、アレイ内の SGD サーバーがセキュアモードで稼働している必要があります。

  アレイ内の SGD サーバーに対して暗号化されていない接続を使用することについての詳細は、「SGD アレイに対する非暗号化接続の使用」を参照してください。

注記

これらの設定は、あとで gateway config create コマンドを使用して変更できます。「SGD Gateway のポートと接続を構成する方法」を参照してください。

ソフトウェアをインストールしたあと、SGD Gateway の追加の構成を実行する必要があります。実行する必要のある作業の詳細については、2章SGD Gateway の構成を参照してください。

1.4. SGD Gateway のアップグレード

このセクションでは、SGD Gateway のアップグレード方法について説明します。

SGD Gateway をアップグレードしても、ルーティングプロキシ構成ファイルなど、元の構成はほとんど保持されます。ただし、アップグレード処理によって、Gateway で使用される自己署名証明書はすべて上書きされます。

アップグレード後、SGD Gateway を再構成する必要があります。「SGD Gateway の証明書を SGD アレイにインストールする方法」で説明されているように、SGD に対して Gateway を認証するための標準の構成手順を実行してください。

アップグレードログは、/opt/SUNWsgdg/proxy/var/log/upgrade_oldversion_newversion.log に作成されます。ここで、oldversion は SGD Gateway の古いバージョンで、newversion は SGD Gateway のアップグレードされたバージョンです。

アップグレード時には、SGD Gateway のインストールプログラムによって、検出されてアップグレードログに一覧表示された、カスタマイズ済みの Apache Web サーバーファイルがバックアップされます。これらのファイルは手動でアップグレードする必要があります。diff などのユーティリティーを使用して、ファイルを比較したり、加えられた変更を示したりすることができます。

1.4.1. SGD Gateway をアップグレードする方法

1. SGD Gateway を介して実行されているユーザーセッションやアプリケーションセッションがないことを確認します。
2. 新しいバージョンの SGD Gateway をインストールします。

   「SGD Gateway をインストールする方法」を参照してください。

第2章 SGD Gateway の構成

この章では、通常の配備シナリオで オラクル Secure Global Desktop Gateway (SGD Gateway) を構成する方法について説明します。SGD Gateway を起動および停止する方法と、SGD Gateway ソフトウェアを削除する方法についてもこの章で説明します。

この章の内容は、次のとおりです。

- 「SGD Gateway の配備」
- 「SGD Gateway の構成タスク」
- 「SGD Gateway の制御」
- 「SGD Gateway の削除」

2.1. SGD Gateway の配備

このセクションでは、次に示す SGD Gateway の配備シナリオについて説明します。

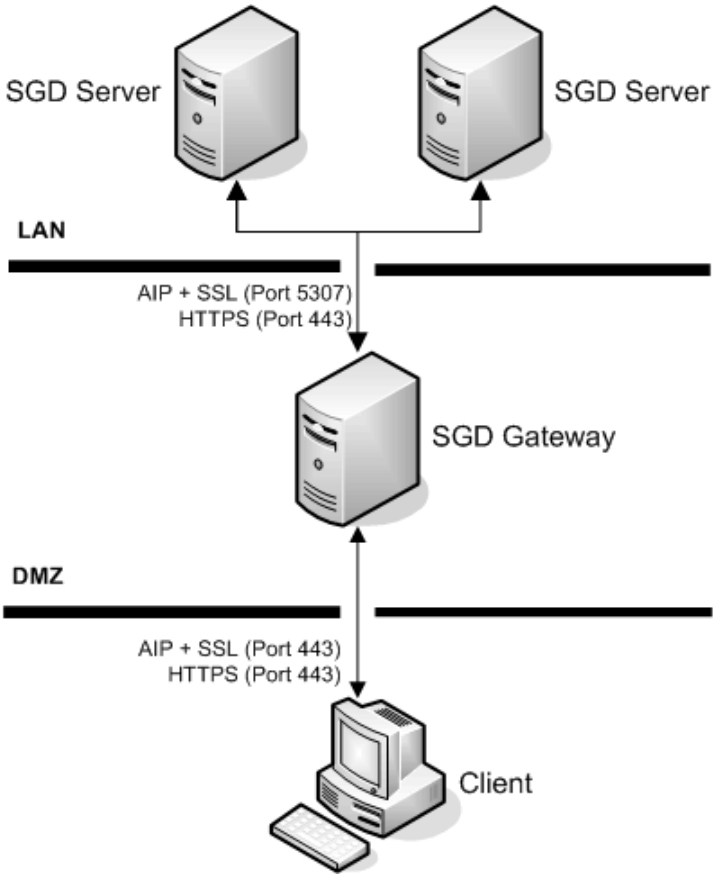
- 「基本的な配備」
- 「負荷分散された配備」

2.1.1. 基本的な配備

このセクションでは、SGD Gateway の基本的な配備の構成タスクについて説明します。

基本的な配備では、図2.1「単一の SGD Gateway を使用した基本的な配備」に示すように単一の SGD Gateway を使用します。

図2.1 単一の SGD Gateway を使用した基本的な配備



基本的な配備を構成するには、表2.1「SGD Gateway の基本的な配備のための接続」 に示す接続の構成を行います。

表2.1 SGD Gateway の基本的な配備のための接続

接続	構成手順
クライアントデバイスから SGD Gateway	1. SGD Gateway で使用するポートと接続を構成します。 これらの構成は、SGD Gateway のインストール時に行いました。 SGD Gateway の構成を変更する場合は、「SGD Gateway のポートと接続を構成する方法」を参照してください。 2. SGD Gateway に、クライアント接続用の Secure Sockets Layer (SSL) 証明書をインストールします。 「クライアント接続用の SSL 証明書をクライアントキーストアにインストールする方法」を参照してください。
SGD Gateway から SGD サーバー	1. アレイに対して SGD セキュリティーサービスを有効にします。 SGD サーバーはセキュアモードで稼働している必要があります。ファイアウォールの転送が無効になっている必要があります。 標準インストールでは、SGD サーバーはセキュア接続を使用するように自動的に構成されます。SGD サーバーをセキュリティー保護する方法についての情報が必要な場合は、『オラクル Secure Global Desktop 管理者ガイド (リリース 4.7 用)』の、SGD サーバーへのセキュア接続に関する第 1 章を参照してください。

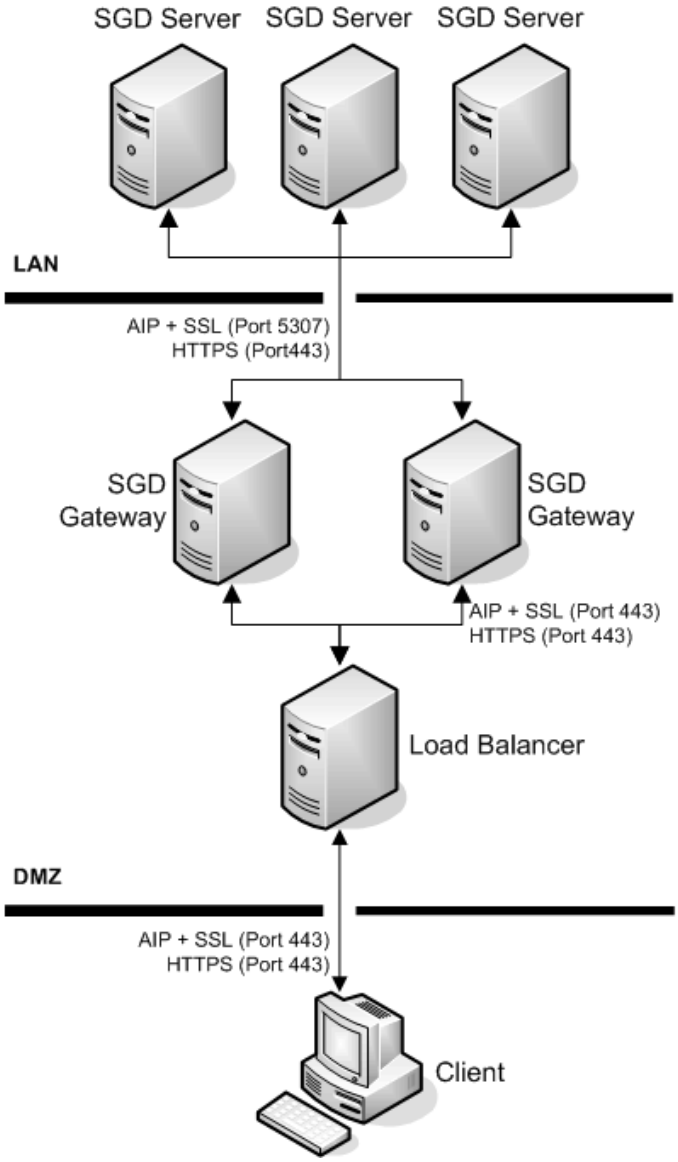
接続	構成手順
	2. SGD Gateway に、SGD サーバーのセキュリティー証明書をインストールします。 gateway server コマンドを使用して、アレイ内の SGD サーバーの CA 証明書と SSL 証明書を SGD Gateway キーストアにインポートします。 「SGD サーバーの証明書をインストールする方法」を参照してください。 3. SGD Gateway を使用するようにアレイ内の SGD サーバーを設定します。 SGD Gateway の証明書を SGD アレイにインストールし、tarantella gateway add コマンドを使用して SGD Gateway を SGD アレイに登録します。 「SGD Gateway の証明書を SGD アレイにインストールする方法」を参照してください。 4. どの SGD Client 接続で SGD Gateway を使用できるかを構成します。 「SGD Client 接続を構成する方法」を参照してください。

2.1.2. 負荷分散された配備

このセクションでは、SGD Gateway の負荷分散された配備の構成タスクについて説明します。

負荷分散された配備では、複数の SGD Gateway とネットワークエントリポイントとなるロードバランサを、図 2.2「複数の SGD Gateway とロードバランサを使用したネットワーク配備」のように使用します。

図2.2 複数の SGD Gateway とロードバランサを使用したネットワーク配備



負荷分散された配備を構成するには、表2.2「SGD Gateway の負荷分散された配備で使用する接続」 に示す接続の構成を行います。

表2.2 SGD Gateway の負荷分散された配備で使用する接続

接続	構成タスク
クライアントデバイスからロードバランサ	1. クライアントデバイスからの着信接続を有効にします。 通常、これは TCP ポート 443 を使用します。 この方法の詳細については、ロードバランサのドキュメントを参照してください。 2. (オプション) ロードバランサに、SGD Gateway でクライアント接続に使用される SSL 証明書をインストールします。 この方法の詳細については、ロードバランサのドキュメントを参照してください。

接続	構成タスク
ロードバランサから SGD Gateway	1. 接続を SGD Gateway に転送するようにロードバランサを構成します。 この方法の詳細については、ロードバランサのドキュメントを参照してください。 2. SGD Gateway で使用するポートと接続を構成します。 ネットワークエントリポイントをロードバランサのアドレスに設定します。 これらの構成は、SGD Gateway のインストール時に行いました。 SGD Gateway の構成を変更する場合は、「SGD Gateway のポートと接続を構成する方法」を参照してください。 3. 各 SGD Gateway に、クライアント接続用の SSL 証明書をインストールします。 「クライアント接続用の SSL 証明書をクライアントキーストアにインストールする方法」を参照してください。
SGD Gateway から SGD サーバー	1. SGD アレイに対して SGD セキュリティーサービスを有効にします。 SGD サーバーはセキュアモードで稼働している必要があります。ファイアウォールの転送が無効になっている必要があります。 標準インストールでは、SGD サーバーはセキュア接続を使用するように自動的に構成されます。SGD サーバーをセキュリティー保護する方法についての情報が必要な場合は、『オラクル Secure Global Desktop 管理者ガイド (リリース 4.7 用)』の、SGD サーバーへのセキュア接続に関する第 1 章を参照してください。 2. SGD Gateway に、SGD サーバーのセキュリティー証明書をインストールします。 gateway server コマンドを使用して、アレイ内の SGD サーバーの CA 証明書と SSL 証明書を SGD Gateway キーストアにインポートします。 「SGD サーバーの証明書をインストールする方法」を参照してください。 3. SGD Gateway を使用するようにアレイ内の SGD サーバーを設定します。 SGD Gateway の証明書を SGD アレイにインストールし、tarantella gateway add コマンドを使用して SGD Gateway を SGD アレイに登録します。 「SGD Gateway の証明書を SGD アレイにインストールする方法」を参照してください。 4. どの SGD Client 接続で SGD Gateway を使用できるかを構成します。 「SGD Client 接続を構成する方法」を参照してください。

2.2. SGD Gateway の構成タスク

このセクションでは、SGD Gateway で使用する接続を構成する手順について説明します。

説明する構成タスクは次のとおりです。

- 「クライアントデバイスから SGD Gateway への接続」
- 「SGD Gateway から SGD サーバーへの接続」
- 「クライアントデバイスからロードバランサへの接続」

- 「ロードバランサから SGD Gateway への接続」

2.2.1. クライアントデバイスから SGD Gateway への接続

クライアントデバイスと SGD Gateway の間の接続を構成するには、次の構成タスクを行います。

1. (オプション) SGD Gateway で使用するポートと接続を構成します。

   これらの構成は、SGD Gateway のインストール時に行います。

   これらの設定を変更する場合は、「SGD Gateway のポートと接続を構成する方法」を参照してください。

2. (オプション) SGD Gateway に、クライアント接続用の SSL 証明書をインストールします。

   「クライアント接続用の SSL 証明書をクライアントキーストアにインストールする方法」を参照してください。

2.2.1.1. SGD Gateway のポートと接続を構成する方法

この手順を使用する必要があるのは、SGD Gateway のインストール時に行なった設定を変更する場合のみです。

1. SGD Gateway ホストにスーパーユーザー (root) としてログインします。
2. gateway config create コマンドを実行します。

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

   画面上の質問に回答して次の項目を構成します。

   - SGD Gateway ポート設定。SGD Gateway で着信接続に使用されるインタフェースとポートです。
   - ネットワークエントリポイント。クライアントデバイスが SGD Gateway に接続するために使用する IP アドレスまたは DNS 名、およびポートです。これは、SGD Gateway のアドレスと常に同じであるとは限りません。ネットワークの構成によっては、ロードバランサなどの外部デバイスのアドレスになることがあります。
   - セキュア接続。SGD Gateway とアレイ内の SGD サーバーとの接続をセキュリティー保護するかどうか。セキュア接続を使用するには、アレイ内の SGD サーバーがセキュアモードで稼働している必要があります。

3. 接続とポートの設定を保存します。

   入力した設定を使用して SGD Gateway が構成されます。

2.2.1.2. クライアント接続用の SSL 証明書をクライアントキーストアにインストールする方法

SGD Gateway でクライアント接続に使用される SSL 証明書は、SGD Gateway SSL 証明書と呼ばれます。SSL 証明書はクライアントキーストア /opt/SUNWsgdg/proxy/etc/keystore.client に保存されます。

デフォルトでは、SGD Gateway は自己署名付き SGD Gateway SSL 証明書をクライアント接続に使用しますが、この自己署名付き SSL 証明書を認証局 (CA) によって署名された証明書で置き換えることができます。

次の手順では、CA によって署名された SSL 証明書があることを前提としています。

インストールする非公開鍵は Privacy Enhanced Mail (PEM) 形式で作成されている必要があります。

1. SGD Gateway ホストにスーパーユーザー (root) としてログインします。
2. SSL 証明書とそれに対応する非公開鍵を SGD Gateway ホストにコピーします。
3. SSL 証明書と非公開鍵をクライアントキーストアにインポートします。

   gateway sslkey import コマンドを次のように使用します。

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

```
--certfile example.com.pem
```

ここでは、証明書ファイル example.com.pem と、それに対応する RSA で符号化された非公開鍵 temp.key がクライアントキーストアにインポートされます。

クライアントキーストア内の既存の自己署名付き SSL 証明書は上書きされます。

4. (オプション) SGD Gateway を再起動します。

注意

この手順は、SGD Gateway の初期構成を実行しない場合にのみ使用してください。初期構成のこの段階で SGD Gateway を再起動すると、SGD Gateway の初期構成が完了していないため、エラーメッセージが表示されます。

すでに構成済みで稼働している SGD Gateway の SSL 証明書を置き換える場合は、SGD Gateway を再起動します。

注記

SGD Gateway を再起動すると、SGD Gateway を介して実行されているユーザーセッションとアプリケーションセッションはすべて切断されます。

SGD Gateway ホストで、次のコマンドを実行します。

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

2.2.2. SGD Gateway から SGD サーバーへの接続

SGD Gateway とアレイ内の SGD サーバーとの接続では、相互承認のために証明書が使用されます。これらの接続を構成するには、次の構成タスクを行います。

1. SGD サーバーの証明書を SGD Gateway にインストールします。

   「SGD サーバーの証明書をインストールする方法」を参照してください。

2. SGD Gateway の証明書を SGD アレイにインストールします。

   「SGD Gateway の証明書を SGD アレイにインストールする方法」を参照してください。

3. SGD Gateway に対する SGD Client 接続を構成します。

   「SGD Client 接続を構成する方法」を参照してください。

2.2.2.1. SGD サーバーの証明書をインストールする方法

この手順を使用するには、アレイ内の SGD サーバーがセキュアモードで稼働している必要があります。

標準インストールでは、SGD サーバーはセキュア接続を使用するように自動的に構成されます。SGD サーバーに対してセキュリティーサービスを有効にする方法については、『オラクル Secure Global Desktop 管理者ガイド (リリース 4.7 用)』の、SGD サーバーへのセキュア接続に関する第 1 章を参照してください。

アレイ内の各 SGD サーバーで、次の手順を繰り返します。

1. SGD ホスト上でスーパーユーザー (root) としてログインします。

2. SGD サーバーから SGD Gateway キーストアディレクトリに CA 証明書をコピーします。

   SGD サーバーの CA 証明書は、SGD ホストの /opt/tarantella/var/info/certs/PeerCAcert.pem にあります。

注記

この CA 証明書は、SGD サーバーがアレイ内のセキュア通信に使用するものと同じです。

SGD Gateway キーストアディレクトリは /opt/SUNWsgdg/proxy/etc です。

CA 証明書をコピーするときは、ファイルの内容や証明書ファイルがあった SGD サーバーを特定できるように、証明書ファイルの名前を変更することをお勧めします。

3. SGD サーバーから SGD Gateway キーストアディレクトリに SSL 証明書をコピーします。

   セキュアモードで稼働している SGD サーバーの SSL 証明書は、SGD ホストの /opt/tarantella/var/tsp/cert.pem にあります。

   SGD Gateway キーストアディレクトリは /opt/SUNWsgdg/proxy/etc です。

   SSL 証明書をコピーするときは、ファイルの内容や証明書ファイルがあった SGD サーバーを特定できるように、証明書ファイルの名前を変更することをお勧めします。

4. SGD Gateway ホストにスーパーユーザー (root) としてログインします。

5. SGD Gateway キーストアに証明書をインポートします。

```
# /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 オプションは、証明書をキーストアに保存するときに使用する別名を定義します。この例では、CA 証明書は sgd-server1 という別名を使用して保存され、SSL 証明書は sgd-server1-ssl という別名を使用して保存されます。

   https://sgd1.example.com は、SGD Web サーバーの URL です。

6. SGD Gateway を再起動します。

   注記

   SGD Gateway を再起動すると、SGD Gateway を介して実行されているユーザーセッションとアプリケーションセッションはすべて切断されます。

   SGD Gateway ホストで、次のコマンドを実行します。

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

2.2.2.2. SGD Gateway の証明書を SGD アレイにインストールする方法

各 SGD Gateway で、次の手順を繰り返します。

1. SGD Gateway の証明書をエクスポートします。

   a. SGD Gateway ホストにスーパーユーザー (root) としてログインします。

   b. SGD Gateway キーストアから SGD Gateway の証明書をエクスポートします。

      gateway cert export コマンドを次のように使用します。

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

      証明書がファイル gateway1.pem にエクスポートされます。

   c. アレイのプライマリ SGD サーバーの /opt/tarantella/var/tsp ディレクトリに証明書をコピーします。

      証明書をエクスポートするときは、証明書ファイルがあった SGD Gateway を特定できるように、証明書ファイルの名前を変更することをお勧めします。

   d. Gateway の証明書でファイルへのアクセス権および所有権を変更します。

```
# chmod 600 /opt/tarantella/var/tsp/gateway1.pem
# chown ttasys:ttaserv /opt/tarantella/var/tsp/gateway1.pem
```

2. SGD Gateway を SGD アレイに登録します。

   a. プライマリ SGD サーバーにスーパーユーザー (root) としてログインします。

   b. SGD Gateway の証明書をインポートします。

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

   ここで、sgd-gateway1 は SGD が SGD Gateway の識別に使用する名前、gateway1.pem は SGD Gateway の証明書ファイル名です。

   複数の SGD Gateway を同時に登録するには、tarantella gateway add コマンドの --file オプションを使用します。詳細については、「tarantella gateway コマンド」を参照してください。

   tarantella gateway add を使用して行なった構成変更は、アレイ内のほかの SGD サーバーに複製されます。

2.2.2.3. SGD Client 接続を構成する方法

1. SGD Gateway を使用する SGD Client 接続を構成します。

   プライマリ SGD サーバーで --security-gateway グローバル属性を設定して、どの SGD Client が SGD Gateway を使用できるかをクライアントの IP アドレスまたは DNS 名に基づいて定義します。

   単一の SGD Gateway gateway1.example.com の TCP ポート 443 を介してすべての SGD Client 接続をルーティングするように指定するには、次のコマンドを使用します。

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

   外部ロードバランサ lb.example.com の TCP ポート 443 を介してすべての SGD Client 接続をルーティングするように指定するには、次のコマンドを使用します。

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

注記

--security-gateway 属性に加えた変更は、アレイ内のすべての SGD サーバーに適用されます。変更が反映されるのは、新規ユーザーセッションだけです。

   --security-gateway 属性を使用して複数の SGD Client 接続フィルタを定義する方法については、「--security-gateway 属性」を参照してください。

2.2.3. クライアントデバイスからロードバランサへの接続

クライアントデバイスと外部ロードバランサの間の接続を構成するには、次の構成タスクを行います。

1. クライアントデバイスからの接続を受け入れるようにロードバランサを構成します。

   この方法の詳細については、ロードバランサのドキュメントを参照してください。

2. (オプション) SGD Gateway の SSL 証明書をロードバランサにインストールします。

   この方法の詳細については、ロードバランサのドキュメントを参照してください。

2.2.4. ロードバランサから SGD Gateway への接続

外部ロードバランサと SGD Gateway の間の接続を構成するには、次の構成タスクを行います。

1. SGD Gateway で使用するポートと接続を構成します。

   「SGD Gateway のポートと接続を構成する方法」を参照してください。

2. (オプション) SGD Gateway に、着信クライアント接続用の SSL 証明書をインストールします。

「クライアント接続用の SSL 証明書をクライアントキーストアにインストールする方法」を参照してください。

2.3. SGD Gateway の制御

このセクションでは、SGD Gateway を制御する方法について説明します。説明するタスクは次のとおりです。

- SGD Gateway の起動
- SGD Gateway の停止
- SGD Gateway の再起動

2.3.1. SGD Gateway の起動

SGD Gateway を起動するには、次のコマンドを使用します。

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

2.3.2. SGD Gateway の停止

注意

SGD Gateway を停止すると、SGD Gateway を介して実行されているユーザーセッションとアプリケーションセッションはすべて切断されます。つまり、SGD Gateway が予期せず停止された場合は、アプリケーションデータが失われる可能性があります。

SGD Gateway を停止するには、次のコマンドを使用します。

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

gateway stop コマンドを使用すると、SGD Gateway を停止するかどうかの確認を求める警告メッセージが表示されます。このメッセージを表示しないようにするには、gateway stop コマンドの --force オプションを使用してください。

注記

SGD Gateway が停止している場合、ネットワークの外部のユーザーが SGD Gateway を使用して SGD に接続することはできません。--security-gateway 属性を使用して、クライアントデバイスが SGD Gateway を経由せずに直接 SGD にアクセスできるようにした場合、このようなクライアントデバイスは引き続き SGD にアクセスできます。「--security-gateway 属性」を参照してください。

2.3.3. SGD Gateway の再起動

注意

SGD Gateway を再起動すると、SGD Gateway を介して実行されているユーザーセッションとアプリケーションセッションはすべて切断されます。つまり、SGD Gateway が予期せず再起動された場合は、アプリケーションデータが失われる可能性があります。

SGD Gateway を再起動するには、次のコマンドを使用します。

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

gateway restart コマンドを使用すると、SGD Gateway を停止するかどうかの確認を求める警告メッセージが表示されます。このメッセージを表示しないようにするには、gateway restart コマンドの --force オプションを使用してください。

2.4. SGD Gateway の削除

SGD Gateway を削除するには、SGD Gateway ホストにインストールされているソフトウェアを削除します。

2.4.1. SGD Gateway を削除する方法

1. SGD Gateway ホストにスーパーユーザー (root) としてログインします。
2. SGD アレイの SGD Client のルーティング構成を変更します。
   a. プライマリ SGD サーバーにスーパーユーザー (root) としてログインします。
   b. SGD アレイの --security-gateway 属性を編集します。

      単一の SGD Gateway を使用した基本的な配備の場合は、次のコマンドを実行します。

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

      注記

      複数の SGD Gateway と外部ロードバランサを使用した負荷分散された配備の場合、--security gateway 属性を編集する必要はありません。
3. SGD Gateway をアンインストールします。

   次のコマンドを実行します。

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

   SGD Gateway を停止するかどうかの確認を求める警告メッセージが表示されます。

   注意

   SGD Gateway の削除方法としてサポートされているのは、gateway uninstall コマンドだけです。pkgrm コマンドや rpm コマンドを使用して SGD Gateway を直接削除しないでください。
4. (オプション) SGD アレイに登録されている SGD Gateway のリストから、この SGD Gateway を削除します。
   a. SGD アレイに登録されている SGD Gateway を表示します。

      ```
      # 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. SGD アレイに登録されている SGD Gateway のリストから、この SGD Gateway を削除します。

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

付録A SGD Gateway のアーキテクチャーの概要

この章では、オラクル Secure Global Desktop Gateway (SGD Gateway) のアーキテクチャーと主要コンポーネントについて説明します。

この章の内容は、次のとおりです。

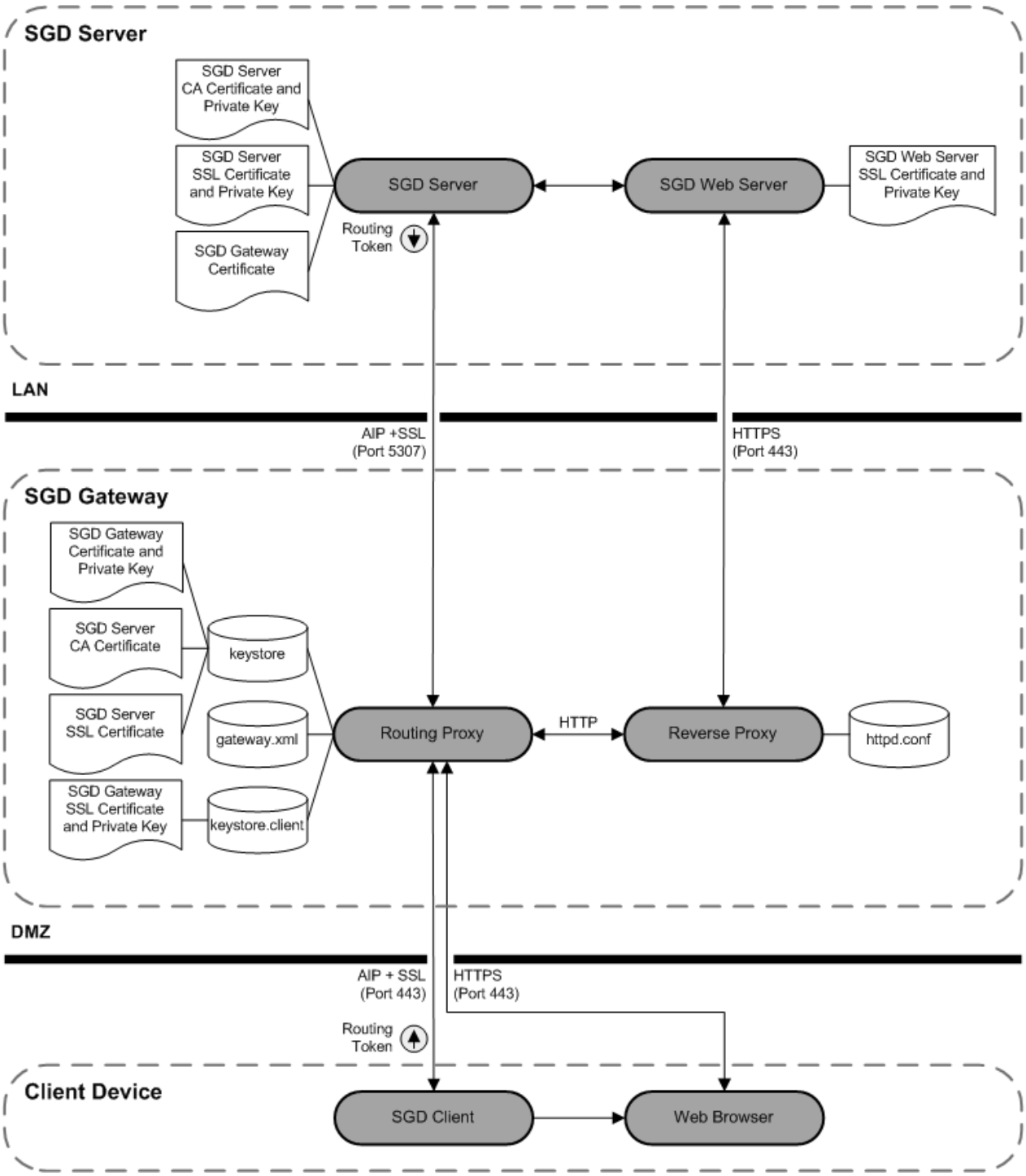
- 「SGD Gateway のアーキテクチャー」
- 「SGD Gateway のコンポーネント」

A.1. SGD Gateway のアーキテクチャー

このセクションでは、SGD Gateway のアーキテクチャーを示し、SGD Gateway を介して SGD にアクセスするときに確立される接続について説明します。

図A.1「SGD Gateway のアーキテクチャー」 に、SGD Gateway のアーキテクチャーを示します。

図A.1 SGD Gateway のアーキテクチャー



次の手順では、SGD Gateway を介して SGD にアクセスするときに確立される接続について説明します。この手順では、ブラウザを使用した SGD への初期接続、SGD へのログオン、さらにアプリケーションの起動までが示されています。

1. クライアントデバイスのブラウザが SGD Gateway に対して TCP ポート 443 で HTTPS (HTTP over Secure Sockets Layer) 接続を行います。

- 基本的な配備の場合、ユーザーは SGD Gateway の URL にアクセスすることによって SGD にアクセスできます。
- TCP ポート 443 は SGD Gateway のデフォルトポートです。SGD Gateway が使用するポートは、ルーティングプロキシ構成ファイル gateway.xml で定義されます。このファイルは、SGD Gateway のインストール時に自動的に作成され、gateway config コマンドを使用して SGD Gateway の構成を変更したときに更新されます。
- SGD Gateway は SSL 証明書を提示します。この証明書は、SGD Gateway の keystore.client キーストアにある唯一のエントリです。
- SGD Gateway が使用するキーストアの場所とパスワードは、ルーティングプロキシ構成ファイル gateway.xml で定義されます。

2. ルーティングプロキシは HTTPS 接続を認識し、データストリームを復号化し、HTTP データを Apache 逆プロキシに転送します。
   - HTTP データは、TCP ポート 8080 より上の最初の空きポートに内部で送信されます。
   - Apache 逆プロキシの構成は httpd.conf ファイルで定義されます。このファイルとそれに関連する逆プロキシ構成ファイルは、SGD Gateway のインストール時に自動的に作成されます。これらのファイルは、gateway config コマンドを使用して SGD Gateway の構成を変更したときに更新されます。
3. 逆プロキシは HTTP 負荷分散を使用して、アレイ内の SGD Web サーバーを選択します。
   - 逆プロキシと SGD Web サーバーの間の接続は、TCP ポート 443 で HTTPS を使用してセキュリティー保護されます。
   - Apache 逆プロキシはブラウザに負荷分散 Cookie を設定します。これ以降、ブラウザによるすべての HTTP リクエストで同じ SGD Web サーバーが使用されます。
4. SGD Web サーバーはクライアントデバイスのブラウザに HTML を配信します。
   - HTML は、SGD Gateway の TCP ポート 443 に確立された接続上で、HTTPS データとして送信されます。
   - SGD Gateway は HTTPS データをブラウザに転送します。
5. ユーザーが SGD にログインします。
   - SGD サーバーはユーザーを認証し、ユーザーセッションを管理する SGD サーバーを選択し、新しいユーザーセッションを開始します。
   - クライアントデバイスに SGD Client がダウンロードおよびインストールされ、起動されます。
   - ブラウザに送信された HTML にルーティングトークンが含まれています。ルーティングトークンには、ユーザーセッションを管理するように選択された SGD サーバーのアドレスが含まれています。この情報は、AIP (Adaptive Internet Protocol) データを正しい SGD サーバーにルーティングするために使用されます。
   - ルーティングトークンは、SGD サーバーの非公開鍵を使用して署名されたあと、SGD サーバーにある SGD Gateway の証明書を使用して暗号化されます。
   - ルーティングトークンは SGD Client に渡されます。
   - クライアントデバイスへの接続では HTTPS が使用されます。
6. SGD Client は SGD Gateway に TCP ポート 443 で接続します。
   - SGD Client と SGD Gateway の間のデータ接続では、AIP over Secure Sockets Layer (SSL) が使用されます。
   - SGD Gateway の SSL 証明書が接続のために提示されます。
   - ルーティングプロキシは AIP over SSL 着信データを認識します。
   - SSL データストリームが復号化され、AIP データストリームからルーティングトークンが抽出されます。

- ルーティングトークンは、SGD Gateway の非公開鍵を使用して復号化されたあと、SGD サーバーの CA 証明書を使用して確認されます。
- SGD Gateway の非公開鍵と SGD サーバーの CA 証明書は、SGD Gateway キーストア keystore に保存されています。
- ルーティングトークンが有効であることを確認するために、ルーティングトークンのタイムスタンプが検査されます。
- SSL を使用して AIP データストリームが再度暗号化されます。

7. AIP over SSL データはルーティングプロキシを介して、ルーティングトークンで指定されている SGD サーバーに転送されます。
   - AIP over SSL データ接続では TCP ポート 5307 が使用されます。
   - AIP データストリームにはルーティングトークンは含まれていません。
8. ユーザーが SGD Webtop でアプリケーションを起動します。
   - アプリケーションの起動リクエストは HTTPS を使用して SGD Gateway に送信されます。
   - ルーティングプロキシは HTTPS データを認識して復号化し、HTTP トラフィックを Apache 逆プロキシに転送します。
   - 逆プロキシは負荷分散 Cookie を検出し、Cookie で指定されている SGD Web サーバーを使用します。
   - SGD アプリケーションセッションの負荷分散では、アプリケーションセッションを管理するために同じ SGD サーバーが選択されます。
   - SGD サーバー上で新しいルーティングトークンが作成されます。ルーティングトークンは、アプリケーションセッションを管理するように選択された SGD サーバーに AIP データをルーティングするために使用されます。
   - SGD サーバーはルーティングトークンを SGD Client に送信します。既存の AIP データストリームにはルーティングトークンが含まれています。
9. SGD Client は SGD Gateway に TCP ポート 443 で接続します。
   - SGD Gateway の SSL 証明書が接続のために提示されます。
   - ルーティングプロキシは AIP over SSL 着信データを認識します。
   - ルーティングトークンの復号化、確認、および検証が行われます。
   - AIP over SSL データはルーティングプロキシを介して、ルーティングトークンで指定されている SGD サーバーに転送されます。
   - AIP データストリームにはルーティングトークンは含まれていません。
10. SGD サーバーはアプリケーションセッションを管理します。
    - アプリケーションは、ローカルエリアネットワーク (LAN) に配置されたアプリケーションサーバー上で実行されます。

A.2. SGD Gateway のコンポーネント

SGD Gateway は次のコンポーネントで構成されます。

- ルーティングプロキシ。AIP データ接続を SGD サーバーにルーティングする、Java テクノロジベースのアプリケーションです。

  ルーティングプロキシの主要コンポーネントは次のとおりです。

- ルーティングトークン – 「ルーティングトークンについて」を参照
- キーストア – 「SGD Gateway で使用されるキーストア」を参照
- ルーティングプロキシ構成ファイル – 「ルーティングプロキシ構成ファイル」を参照

- 逆プロキシ。逆プロキシモードで動作するように構成された Apache Web サーバーです。逆プロキシは HTTP 接続の負荷分散も実行します。

  逆プロキシの主要コンポーネントは次のとおりです。

  - Apache Web サーバーの構成ファイル – 「Apache Web サーバーの設定ファイル」を参照
  - 逆プロキシ用および HTTP 負荷分散用の Apache モジュール – 「SGD Gateway で使用される Apache モジュール」を参照

A.2.1. ルーティングトークンについて

SGD Gateway はルーティングトークンを使用して AIP 接続を管理します。ルーティングトークンは、経路の送信元および送信先の SGD サーバーを識別する、署名され暗号化されたメッセージです。ルーティングトークンにはタイムスタンプが含まれており、トークンの寿命を制限するために使用されます。

発信ルーティングトークンは次のようになります。

- SGD サーバーの非公開鍵を使用して SGD サーバー上で署名されます。
- SGD Gateway の証明書を使用して SGD サーバー上で暗号化されます。
- クライアントデバイスの SGD Client に送信されます。

着信ルーティングトークンは次のようになります。

- SGD Gateway の非公開鍵を使用して SGD Gateway 上で復号化されます。
- 送信元 SGD サーバーの CA 証明書を使用して SGD Gateway 上で確認されます。
- SGD Gateway 上で破棄されます。ルーティングトークンを提示している接続は、送信先 SGD サーバーにルーティングされます。

A.2.2. SGD Gateway で使用されるキーストア

SGD Gateway は非公開鍵と証明書を使用して、ルーティングトークンへのデジタル署名、ルーティングトークンの確認、アレイ内の SGD サーバーに対する接続のセキュリティー保護、SGD Gateway へのクライアント接続のセキュリティー保護、およびリフレクションサービスへのアクセスの承認を行います。

SGD Gateway で使用される証明書と非公開鍵は、/opt/SUNWsgdg/proxy/etc ディレクトリのキーストアに保存されています。

このディレクトリには次のキーストアがあります。

- SGD Gateway キーストア。SGD Gateway キーストア keystore には、SGD Gateway の証明書と非公開鍵、アレイ内の SGD サーバーの CA 証明書、および SGD サーバーの SSL 証明書があり、アレイ内の SGD サーバーに対するセキュア接続に使用されます。

  SGD Gateway キーストアのエントリを追加、削除、および一覧表示するには、gateway コマンドを使用します。

- クライアントキーストア。クライアントキーストア keystore.client には、単一の SGD Gateway SSL 証明書と非公開鍵があり、クライアントデバイスと SGD Gateway の間の接続をセキュリティー保護するために使用されます。デフォルトでは、このキーストアには自己署名付き証明書が入っています。この証明書を認証局 (CA) によって署名された証明書で置き換えることができます。

- リフレクションサービスキーストア。リフレクションサービスキーストア keystore.reflection には、SGD Gateway でリフレクションサービスへのアクセスの承認に使用される証明書と非公開鍵が含まれています。デフォルトでは、このキーストアには自己署名付き証明書と非公開鍵が入っています。

キーストアは、SGD Gateway のインストール後に gateway setup コマンドを実行したときに自動的に作成されます。

注記

すべてのキーストアで同じパスワードが使用され、パスワードは /opt/SUNWsgdg/etc/password ファイルで定義されます。このパスワードは、キーストアの最初の作成時に自動的に作成されるランダムなパスワードです。パスワードファイルを読み取ることができるのはスーパーユーザー (root) だけです。

A.2.3. ルーティングプロキシ構成ファイル

ルーティングプロキシ構成ファイルは /opt/SUNWsgdg/etc/gateway.xml です。これは、データプロトコルの種類に応じて経路を構成する XML ファイルです。ルーティングおよび SSL プロトコルに必要なキーストアの場所とパスワードも、このファイルで構成されます。

ルーティングプロキシ構成ファイルは、SGD Gateway のインストール時に自動的に作成され、gateway config コマンドを使用して SGD Gateway の構成を変更したときに更新されます。

注意

gateway config コマンドは、Gateway の構成に使用します。可能なかぎり、gateway.xml ファイルを手動で編集しないでください。gateway.xml ファイルの構成が間違っていると、SGD Gateway の動作が停止することがあります。

デフォルトのルーティングプロキシ構成ファイルは /opt/SUNWsgdg/etc/password ファイル内のパスワードを使用して、SGD Gateway が使用するキーストアにアクセスします。このパスワードをディスクに保存したくない場合は、パスワードファイル内のエントリを書きとめます。パスワードファイルを削除し、gateway.xml ファイルからすべての <keystore> 要素の password エントリを削除します。次に SGD Gateway を起動するとき、キーストアパスワードの入力を求められます。

SGD Gateway が使用するキーストアのパスワードを変更するには、keytool コマンドの -storepasswd オプションを使用します。たとえば、keystore.client キーストアのパスワードを変更するには、次のコマンドを実行します。

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

keytool アプリケーションを使用する方法の詳細については、JDK Tools and Utilities のドキュメントを参照してください。

注記

/opt/SUNWsgdg/etc ディレクトリには、ほかの .xml および .template ファイルもあります。これらのファイルは、gateway config コマンドで gateway.xml ファイルを更新するために内部的に使用されます。これらのファイルを手動で編集しないでください。

A.2.4. Apache Web サーバーの設定ファイル

SGD Gateway で使用するために構成された Apache Web サーバーの構成ファイルは、/opt/SUNWsgdg/httpd/apache-version/conf ディレクトリにあります。

このディレクトリにある設定ファイルは、Apache Web サーバーの逆プロキシ処理と負荷分散を設定するために使用されます。

A.2.4.1. 逆プロキシと負荷分散の設定

逆プロキシ処理と負荷分散を構成するためのファイルは、extra/gateway サブディレクトリにあります。これらのファイルは、メインの httpd.conf ファイルで次の Include 指令によって有効にされます。

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

httpd-gateway.conf ファイルは、Apache Web サーバーの逆プロキシと負荷分散を構成します。負荷分散グループのメンバーは、httpd-gateway.conf ファイルで次のように Include 指令を使用して定義されます。

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

extra/gateway/servers ディレクトリには、負荷分散グループの各 SGD Web サーバーの構成ファイルがあります。構成ファイルには server-name.conf という名前が付けられます。ここで、server-name は gateway server add コマンドで使用されたサーバー名です。このコマンドの詳細については、「gateway server add」を参照してください。

SGD Gateway ではスティッキーセッション HTTP 負荷分散が使用されます。つまり、Apache 逆プロキシはクライアントのブラウザに Cookie を設定することによって、ブラウザが必ず負荷分散で選択された SGD Web サーバーに戻るようにします。ユーザーセッションの終了時に Cookie は期限切れになります。

スティッキーセッションの Cookie は、httpd-gateway.conf ファイルで次のように Header add Set-Cookie 指令によって有効にされます。

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

ここで、BALANCEID は Cookie の名前、BALANCER_WORKER_ROUTE と BALANCER_ROUTE_CHANGED は Apache mod_proxy_balancer モジュールによってエクスポートされた環境変数です。これらの環境変数については、Apache mod_proxy_balancer のドキュメントを参照してください。

A.2.5. SGD Gateway で使用される Apache モジュール

SGD Gateway に付属の Apache Web サーバーでは、逆プロキシと負荷分散のために標準の Apache モジュールが使用されます。モジュールは DSO (Dynamic Shared Object) モジュールとしてインストールされます。

これらのモジュールは、
/opt/SUNWsgdg/httpd/apache-version/conf/httpd.conf にある Apache 構成ファイル httpd.conf で、LoadModule 指令によって有効にされます。

付録B コマンド行リファレンス

この章では、オラクル Secure Global Desktop Gateway (SGD Gateway) の構成を、コマンド行から管理、制御、および変更する方法について説明します。

キーストアと証明書の設定、SGD Gateway で使用するポートの構成、アレイ内の SGD サーバーに対する負荷分散の構成といったタスクのためのコマンドが提供されています。

この章の内容は、次のとおりです。

- 「gateway コマンド」
- 「tarantella gateway コマンド」
- 「--security-gateway 属性」

B.1. gateway コマンド

gateway コマンドは、SGD Gateway の構成と制御に使用します。

注記

gateway コマンドのフルパスは、/opt/SUNWsgdg/bin/gateway です。

構文

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

説明

使用可能な gateway コマンドを次の表に示します。

コマンド	説明	詳細情報
gateway start	SGD Gateway を起動します	「gateway start」
gateway stop	SGD Gateway を停止します	「gateway stop」
gateway restart	SGD Gateway を停止してから再起動します	「gateway restart」
gateway config	SGD Gateway を構成し、Apache 逆プロキシ構成ファイルを更新します	「gateway config」
gateway server	SGD サーバーのセキュリティー証明書をインストールし、SGD アレイの負荷分散を構成します	「gateway server」
gateway status	SGD Gateway の現在のステータスを表示します	「gateway status」
gateway version	SGD Gateway のバージョン番号を表示します	「gateway version」
gateway sslcert	クライアントキーストア内の Secure Sockets Layer (SSL) 証明書をエクスポートし、出力します	「gateway sslcert」
gateway sslkey	クライアントキーストア内の非公開鍵と証明書を管理します	「gateway sslkey」
gateway cert export	SGD Gateway キーストアから SGD Gateway の証明書をエクスポートします	「gateway cert export」
gateway key import	非公開鍵と証明書を SGD Gateway キーストアにインポートします	「gateway key import」
gateway setup	SGD Gateway のセットアッププログラムを実行します	「gateway setup」

コマンド	説明	詳細情報
gateway uninstall	SGD Gateway ソフトウェアをアンインストールします	「gateway uninstall」

注記

すべての gateway コマンドに --help オプションがあります。このオプションを使用すると、コマンドのヘルプを表示できます。

例

次の例では、SGD Gateway を起動します。

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

次の例は、SGD サーバー server.example.com が、SGD Gateway の使用を承認されていないことを意味します。

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

B.2. gateway cert export

SGD Gateway キーストアから SGD Gateway の証明書をエクスポートします。

構文

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

説明

SGD Gateway キーストア /opt/SUNWsgdg/proxy/etc/keystore から SGD Gateway の証明書をエクスポートします。証明書は、--certfile オプションで指定されたファイルに書き出されます。

このコマンドは、/opt/SUNWsgdg/etc/password 内のパスワードを使用して SGD Gateway キーストアにアクセスします。このファイルが存在しない場合、パスワードの入力が求められます。

例

次の例では、SGD Gateway キーストアから SGD Gateway の証明書をファイル gateway1.pem にエクスポートします。

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

B.3. gateway config

SGD Gateway を構成します。gateway config コマンドは、SGD Gateway のセキュア接続、ポート、および逆プロキシサーバー設定を構成します。

構文

```
gateway config create | show
```

説明

次の表は、このコマンドで使用可能なサブコマンドを示しています。

サブコマンド	説明	詳細情報
create	SGD Gateway の新しい構成を作成します	「gateway config create」
list	SGD Gateway の現在の構成を一覧表示します	「gateway config list」
edit	SGD Gateway の現在の構成を編集します	「gateway config edit」

サブコマンド	説明	詳細情報
enable	SGD Gateway のサービスを有効にします	「gateway config enable」
disable	SGD Gateway のサービスを無効にします	「gateway config disable」

例

次の例では、SGD Gateway の現在の構成を一覧表示します。

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

B.4. gateway config create

SGD Gateway, の新しい構成を作成し、現在の構成を上書きします。

構文

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

説明

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
--interface	SGD Gateway が着信プロキシ接続を待機するインタフェースとポート。デフォルトは、すべてのインタフェースの TTCP ポート 443 です。
--entry-point	ネットワークのエントリポイント。これは、クライアントが SGD Gateway に接続するために使用するインターネットプロトコル (IP) アドレスとポートです。IP アドレスの代わりにドメインネームシステム (DNS) アドレスを指定することもできます。
--out	SGD Gateway からアレイ内の SGD サーバーへの発信トラフィックの形式。セキュア接続を使用している場合は、ssl を選択してください。
--file	構成設定を含んでいるファイルを指定します。

注記

gateway config create コマンドにオプションを指定しない場合、一連のオンラインプロンプトが表示されるので、必要な設定を入力できます。

gateway config create に --file オプションを使用する場合、指定するファイルは /opt/SUNWsgdg/etc/gatewayconfig.xml ファイルと同じ形式でなければいけません。「SGD Gateway のポートと接続を構成する方法」で説明されているように、このファイルは SGD Gateway の初期構成時に作成されます。

例

次の例では、192.168.0.1 で、ネットワークエントリポイントからの接続を TCP ポート 443 で待機するように SGD Gateway を構成します。セキュア接続は、SGD Gateway とアレイ内の SGD サーバーの間で使用されます。

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

B.5. gateway config disable

1 つ以上の SGD Gateway サービスを無効にします。

構文

```
gateway config disable [ --services-reflection ]
```

```
[ --services-reflection-auth ]
[ --routes-http-redirect ]
```

説明

特定の SGD Gateway サービスを無効にするには、コマンド行オプションを使用します。少なくとも 1 つのコマンド行オプションを指定する必要があります。

注記

このコマンドを使用してサービスを無効にしたあと、SGD Gateway を再起動してサービスを停止する必要があります。

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
--services-reflection	SGD Gateway リフレクションサービスに対する無認証アクセスを無効にします。 デフォルトでは、このサービスは無効になっています。 SGD Gateway リフレクションサービスの詳細については、「リフレクションサービス」を参照してください。
--services-reflection-auth	SGD Gateway リフレクションサービスに対する認証アクセスを無効にします。 デフォルトでは、このサービスは無効になっています。 SGD Gateway リフレクションサービスの詳細については、「リフレクションサービス」を参照してください。
--routes-http-redirect	HTTP リダイレクトサービスを無効にします。 デフォルトでは、このサービスは無効になっています。

例

次の例では、SGD Gateway リフレクションサービスに対する認証アクセスを無効にします。

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

B.6. gateway config edit

SGD Gateway の現在の構成を編集します。

構文

```
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 ]
```

説明

コマンド行オプションを使用すると、特定の構成設定を編集できます。少なくとも 1 つのコマンド行オプションを指定する必要があります。

SGD Gateway の現在の構成は、/opt/SUNWsgdg/etc/gatewayconfig.xml ファイルに保存されています。

構成に加えた変更を有効にするには、SGD Gateway を再起動する必要があります。

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
--binding	SGD Gateway が着信プロキシ接続を待機するインタフェースとポート。デフォルトは、すべてのインタフェースの TCP ポート 443 です。
--routes-http-maxcon	HTTP 接続の最大数。デフォルト値は、SGD Gateway で使用可能なメモリーリソースに応じてインストール時に構成されます。「SGD Gateway の調整」を参照してください。
--routes-aip-maxcon	AIP 接続の最大数。デフォルト値は、SGD Gateway で使用可能なメモリーリソースに応じてインストール時に構成されます。「SGD Gateway の調整」を参照してください。
--routes-reverseproxy-redirect	HTTP リダイレクトポート。デフォルトの TCP ポートは 8080 です。
--services-reflection-binding	SGD Gateway リフレクションサービスに対する無認証アクセスに使用されるインタフェースとポート。デフォルトは、localhost ループバックインタフェースの TCP ポート 81 です。
--services-reflection-auth-binding	SGD Gateway リフレクションサービスに対する認証アクセスに使用されるインタフェースとポート。デフォルトは、すべてのインタフェースの TCP ポート 82 です。

例

次の例では、SGD Gateway の HTTP 接続と AIP 接続の最大数を変更します。

```
# /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

1 つ以上の SGD Gateway サービスを有効にします。

構文

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

説明

特定の SGD Gateway サービスを有効にするには、コマンド行オプションを使用します。少なくとも 1 つのコマンド行オプションを指定する必要があります。

注記

このコマンドを使用してサービスを有効にしたあと、SGD Gateway を再起動してサービスを起動する必要があります。

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
--services-reflection	SGD Gateway リフレクションサービスに対する無認証アクセスを有効にします。 デフォルトでは、このサービスは無効になっています。 SGD Gateway リフレクションサービスの詳細については、「リフレクションサービス」を参照してください。

オプション	説明
--services-reflection-auth	SGD Gateway リフレクションサービスに対する認証アクセスを有効にします。 デフォルトでは、このサービスは無効になっています。 SGD Gateway リフレクションサービスの詳細については、「リフレクションサービス」を参照してください。
--routes-http-redirect	HTTP リダイレクトサービスを有効にします。 デフォルトでは、このサービスは無効になっています。

例

次の例では、SGD Gateway リフレクションサービスに対する認証アクセスを有効にします。

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

B.8. gateway config list

SGD Gateway の現在の構成を一覧表示します。

構文

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

説明

コマンド行オプションを使用すると、特定の構成設定を一覧表示できます。オプションを指定しないと、SGD Gateway の構成の詳細がすべて表示されます。

SGD Gateway の現在の構成は、/opt/SUNWsgdg/etc/gatewayconfig.xml ファイルに保存されています。

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
--binding	SGD Gateway が着信プロキシ接続を待機するインタフェースとポート
--routes-http-maxcon	HTTP 接続の最大数
--routes-aip-maxcon	Adaptive Internet Protocol (AIP) 接続の最大数
--routes-reverseproxy-redirect	HTTP リダイレクトポート
--services-reflection-binding	SGD Gateway リフレクションサービスに対する無認証アクセスに使用されるインタフェースとポート
--services-reflection-auth-binding	SGD Gateway リフレクションサービスに対する認証アクセスに使用されるインタフェースとポート

例

次の例では、SGD Gateway のバインディング構成と AIP 接続の最大数を表示します。

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

次の例では、SGD Gateway の現在の構成の詳細をすべて表示します。

```
# /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

SGD Gateway の鍵と SGD Gateway の証明書を SGD Gateway キーストアにインポートします。

構文

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

説明

非公開鍵とそれに対応する公開鍵証明書を、SGD Gateway キーストア /opt/SUNWsgdg/proxy/etc/keystore にインポートします。

キーストアにすでに SGD Gateway の鍵のエントリが存在する場合、そのエントリは上書きされます。デフォルトでは、確認を求めるメッセージが表示されます。

このコマンドは、/opt/SUNWsgdg/etc/password 内のパスワードを使用して SGD Gateway キーストアにアクセスします。このファイルが存在しない場合、パスワードの入力が求められます。

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
--keyfile	非公開鍵を含んでいるファイル。鍵は PEM 形式で作成されている必要があります。
--keyalg	非公開鍵で使用するエンコーディングアルゴリズム。オプションは RSA および DSA です。デフォルトでは、RSA が選択されます。
--certfile	SSL 証明書ファイル。
--cacertfile	CA またはルート証明書ファイル。
--alwaysoverwrite	確認を求めずにキーストアのエントリを上書きします。

証明書チェーンをインポートするには、--cacertfile オプションを使用して中間 CA の証明書を指定します。チェーン内の証明書はすべて PEM 形式で作成されている必要があります。

証明書チェーンで複数の CA 証明書が使用されている場合は、チェーン内のすべての CA 証明書を結合して 1 つのファイルにします。サーバー証明書の署名に使用される CA 証明書が最初に表示される必要があり、次に例を示します。

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

例

次の例では、RSA でエンコードされた非公開鍵 gateway1.key と、それに対応する公開鍵証明書 gateway1.pem を、SGD Gateway キーストアにインポートします。

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

次の例では、非公開鍵と証明書チェーンを SGD Gateway キーストアにインポートします。中間 CA の証明書は gateway1-ca.pem です。

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

B.10. gateway restart

SGD Gateway を停止してから再起動します。

構文

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

説明

SGD Gateway を停止してから再起動します。SGD Gateway を停止する前に、ユーザーに確認を求めます。

--force オプションは、確認を求めずに SGD Gateway を停止します。

例

次の例では、ユーザーに確認を求めてから SGD Gateway を停止し、再起動します。

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

B.11. gateway server

SGD サーバーに SGD Gateway の使用を承認します。

構文

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

説明

次の表は、このコマンドで使用可能なサブコマンドを示しています。

サブコマンド	説明	詳細情報
add	SGD サーバーに SGD Gateway の使用を承認します	「gateway server add」
remove	SGD サーバーに対して SGD Gateway の使用の承認を削除します	「gateway server remove」
list	SGD Gateway の使用を承認されている SGD サーバーを一覧表示します	「gateway server list」

例

次の例では、SGD サーバー sgd.example.com に対して、SGD Gateway の使用の承認を削除します。

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

B.12. gateway server add

SGD サーバーに SGD Gateway の使用を承認します。

構文

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

説明

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
--server	SGD サーバーの DNS 名
--cert-file	SGD サーバーの認証局 (CA) 証明書
--url	SGD Web サーバーの URL
--ssl-certfile	SGD サーバーの SSL 証明書

gateway server add コマンドは次のことを実行します。

- SGD サーバーの CA 証明書を SGD Gateway キーストア /opt/SUNWsgdg/proxy/etc/keystore にインポートします。CA 証明書は、--server オプションで指定された SGD サーバーと同じ名前の別名でキーストアに保存されます。
- SGD サーバーの SSL 証明書を SGD Gateway キーストア /opt/SUNWsgdg/proxy/etc/keystore にインポートします。SSL 証明書は、--server オプションで指定された SGD サーバーの名前に -ssl を付加した別名でキーストアに保存されます。
- Apache 逆プロキシサーバーで使用される負荷分散グループに SGD サーバーを追加します

注記

gateway server add を使用したあと、変更を有効にするには SGD Gateway を再起動する必要があります。

例

次の例では、CA 証明書 PeerCAcert.pem を、sgd.example.com という別名を使用して SGD Gateway キーストアに追加します。SSL 証明書 cert.pem も sgd.example.com-ssl という別名を使用してキーストアに追加されます。

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

この例では、SGD Web サーバーの URL https://sgd.example.com を逆プロキシの負荷分散グループに追加し、/opt/SUNWsgdg/httpd/apache-version/conf/extra/gateway/servers/conf/sgd.example.com.conf に構成ファイルを作成します。

B.13. gateway server list

SGD Gateway の使用を承認されている SGD サーバーの詳細を表示します。

構文

```
gateway server list
```

説明

このコマンドは、SGD Gateway の使用を承認されている SGD サーバーの証明書の詳細と URL を表示します。

例

次の例では、SGD Gateway の使用を承認されている SGD サーバーの詳細を一覧表示します。

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

B.14. gateway server remove

SGD サーバーに対して SGD Gateway の使用の承認を削除します。

構文

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

説明

SGD サーバーの CA 証明書と SSL 証明書を SGD Gateway キーストアから削除します。

注記

gateway server remove を使用したあと、変更を有効にするには SGD Gateway を再起動する必要があります。

例

次の例では、SGD サーバー sgd.example.com に対して、SGD Gateway の使用の承認を削除します。

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

B.15. gateway setup

SGD Gateway のセットアッププログラムを実行します。

構文

```
gateway setup
```

説明

画面上の質問に回答して、SGD Gateway で使用するポート、インタフェース、およびセキュリティーを構成します。

例

次の例では、SGD Gateway のセットアッププログラムを実行します。

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

B.16. gateway sslcert

クライアントキーストアに保存されている SGD Gateway の SSL 証明書を出力またはエクスポートします。

構文

```
gateway sslcert export | print
```

説明

次の表は、このコマンドで使用可能なサブコマンドを示しています。

サブコマンド	説明	詳細情報
export	クライアントキーストアから SGD Gateway の SSL 証明書をエクスポートします	「gateway sslcert export」
print	クライアントキーストアに保存されている SGD Gateway の SSL 証明書を出力します。	「gateway sslcert print」

例

次の例では、クライアントキーストアに保存されている SGD Gateway の SSL 証明書を出力します。

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

B.17. gateway sslcert export

クライアントキーストアから SGD Gateway の SSL 証明書をエクスポートします。

構文

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

説明

クライアントキーストア /opt/SUNWsgdg/proxy/etc/keystore.client から SGD Gateway の SSL 証明書をエクスポートします。証明書は、--certfile オプションで指定されたファイルに書き出されます。

このコマンドは、/opt/SUNWsgdg/etc/password 内のパスワードを使用してクライアントキーストアにアクセスします。このファイルが存在しない場合、パスワードの入力が求められます。

例

次の例では、クライアントキーストアから SGD Gateway の SSL 証明書をファイル gateway-ssl.pem にエクスポートします。

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

B.18. gateway sslcert print

SGD Gateway の SSL 証明書を出力します。

構文

```
gateway sslcert print
```

説明

クライアントキーストア /opt/SUNWsgdg/proxy/etc/keystore.client に保存されている SGD Gateway の SSL 証明書を出力します。

このコマンドは、証明書の詳細を端末ウィンドウに書き出します。

このコマンドは、/opt/SUNWsgdg/etc/password 内のパスワードを使用してクライアントキーストアにアクセスします。このファイルが存在しない場合、パスワードの入力が求められます。

例

次の例では、クライアントキーストアに保存されている SGD Gateway の SSL 証明書を出力します。

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

B.19. gateway sslkey

クライアントキーストア内の SSL 鍵および証明書のエントリを管理します。

構文

```
gateway sslkey import | export
```

説明

次の表は、このコマンドで使用可能なサブコマンドを示しています。

サブコマンド	説明	詳細情報
import	非公開鍵と証明書をクライアントキーストアにインポートします	「gateway sslkey import」
export	クライアントキーストアから非公開鍵をエクスポートします	「gateway sslkey export」

例

次の例では、クライアントキーストアに保存されている SGD Gateway の SSL 証明書をエクスポートします。

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

B.20. gateway sslkey export

クライアントキーストアから SGD Gateway の SSL 非公開鍵をエクスポートします。

構文

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

説明

クライアントキーストア /opt/SUNWsgdg/proxy/etc/keystore.client から SGD Gateway の SSL 非公開鍵をエクスポートします。非公開鍵は、--keyfile オプションで指定されたファイルに書き出されます。

--keypass オプションを使用すると非公開鍵のパスワードを指定できます。デフォルトでは、/opt/SUNWsgdg/etc/password にあるパスワードが使用されます。

例

次の例では、クライアントキーストアから SGD Gateway の SSL 非公開鍵をファイル gateway-ssl.key にエクスポートします。

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

B.21. gateway sslkey import

SSL 鍵と証明書をクライアントキーストアにインポートします。

構文

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

説明

SSL 非公開鍵とそれに対応する SSL 証明書を、クライアントキーストア /opt/SUNWsgdg/proxy/etc/keystore.client にインポートします。デフォルトでは、このキーストアには自己署名付き証明書が 1 つ入っています。

クライアントキーストアにすでにエントリが存在する場合、このコマンドによって上書きされます。デフォルトでは、キーストアのエントリを上書きする前に確認を求めるメッセージが表示されます。

このコマンドは、/opt/SUNWsgdg/etc/password 内のパスワードを使用してクライアントキーストアにアクセスします。このファイルが存在しない場合、パスワードの入力が求められます。

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
--keyfile	SSL 非公開鍵を含んでいるファイル。この鍵は Privacy Enhanced Mail (PEM) 形式で作成されている必要があります。
--keyalg	非公開鍵で使用するエンコーディングアルゴリズム。オプションは RSA およびデジタル署名アルゴリズム (DSA) です。デフォルトでは、RSA が選択されます。
--certfile	SSL 証明書ファイル。
--cacertfile	CA 証明書またはルート証明書ファイル。
--alwaysoverwrite	確認を求めずにクライアントキーストアのエントリを上書きします。

証明書チェーンをインポートするには、--cacertfile オプションを使用して中間 CA の証明書を指定します。チェーン内の証明書はすべて PEM 形式で作成されている必要があります。

証明書チェーンで複数の CA 証明書が使用されている場合は、チェーン内のすべての CA 証明書を結合して 1 つのファイルにします。サーバー証明書の署名に使用される CA 証明書が最初に表示される必要があり、次に例を示します。

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

例

次の例では、RSA でエンコードされた SSL 非公開鍵 gateway1-ssl.key とそれに対応する SSL 証明書 gateway1-ssl.pem をクライアントキーストアにインポートします。

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

次の例では、RSA でエンコードされた SSL 非公開鍵と SSL 証明書チェーンをクライアントキーストアにインポートします。中間 CA の証明書は gateway1-ca.pem です。

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

B.22. gateway start

SGD Gateway を起動します。

構文

```
gateway start
```

説明

SGD Gateway を起動します。

例

次の例では、SGD Gateway を起動します。

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

B.23. gateway status

SGD Gateway の現在のステータスを表示します。

構文

```
gateway status
```

説明

このコマンドは、SGD Gateway が起動しているか停止しているか、あるいは問題が発生しているかを示します。

例

次の例では、SGD Gateway のステータス情報を表示します。この例で、SGD Gateway は停止しています。

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

B.24. gateway stop

SGD Gateway を停止します。

構文

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

説明

ユーザーに確認を求めてから SGD Gateway を停止します。

--force オプションは、確認を求めずに SGD Gateway を停止します。

例

次の例では、ユーザーに確認を求めてから SGD Gateway を停止します。

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

B.25. gateway uninstall

SGD Gateway ソフトウェアをアンインストールします。

構文

```
gateway uninstall
```

説明

SGD Gateway を停止し、すべての構成情報も含めて SGD Gateway ソフトウェアを削除します。

SGD Gateway を停止する前に、このコマンドはユーザーに確認を求めます。

例

次の例では、コマンドを実行するホストから SGD Gateway ソフトウェアをアンインストールします。

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

B.26. gateway version

SGD Gateway ソフトウェアのバージョン番号を表示します。

構文

```
gateway version
```

説明

SGD Gateway のバージョン番号を表示します。

例

次の例では、コマンドを実行するホストにインストールされている SGD Gateway のバージョンを表示します。

```
# /opt/SUNWsgdg/bin/gateway version
オラクル Secure Global Desktop Gateway 4.50.301
```

B.27. tarantella gateway コマンド

tarantella gateway コマンドは、SGD アレイの承認済みゲートウェイを構成するために使用します。

構文

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

説明

tarantella gateway コマンドを使用すると、SGD アレイのゲートウェイを追加、削除、および一覧表示できます。

tarantella gateway コマンドは、アレイ内の任意の SGD サーバー上で使用できます。加えた変更は、ほかのアレイメンバーに自動的に複製されます。

SGD サーバーがアレイに追加されると、プライマリ SGD サーバー上で定義されているゲートウェイセットがこの新しいアレイメンバーにコピーされ、承認済みゲートウェイがすでに存在している場合、それらはすべて上書きされます。SGD サーバーをアレイから切り離しても、登録済みゲートウェイがそこから削除されることはありません。

使用可能な tarantella gateway コマンドのサブコマンドを次の表に示します。

サブコマンド	説明	詳細情報
add	SGD アレイの SGD Gateway を追加します	「tarantella gateway add」
list	SGD アレイの SGD Gateway を一覧表示します	「tarantella gateway list」

サブコマンド	説明	詳細情報
remove	SGD アレイの SGD Gateway を削除します	「tarantella gateway remove」

注記

すべての tarantella gateway サブコマンドに --help オプションがあります。このオプションを使用すると、サブコマンドのヘルプを表示できます。

例

次の例では、SGD アレイの登録済みゲートウェイのリストに gateway1.example.com を追加します。

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

B.28. tarantella gateway add

SGD Gateway を SGD アレイに登録します。

構文

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

説明

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
--name	登録する SGD Gateway の名前。
--certfile	SGD サーバーで使用する SGD Gateway の証明書。Definite Encoding Rules (DER) 形式または PEM 形式の証明書を使用できます。
--file	複数の SGD Gateway の構成設定を含んでいるバッチファイル。

例

次の例では、SGD アレイの登録済みゲートウェイのリストに gateway1.example.com を追加します。

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

次の例では、tarantella gateway add の --file オプションを使用して、複数のゲートウェイを同時に登録します。

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

--file オプションでバッチファイル gateways.list を指定しており、このファイルには、次のように各ゲートウェイの設定の行が含まれています。

```
--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

SGD アレイに登録されている SGD Gateway を一覧表示します。

構文

```
tarantella gateway list
```

説明

tarantella gateway add コマンドを使用して SGD アレイに登録された SGD Gateway の詳細を表示します。

例

次の例では、SGD アレイの登録済みゲートウェイを一覧表示します。

```
$ tarantella gateway list
```

B.30. tarantella gateway remove

SGD アレイの登録済みゲートウェイのリストから、SGD Gateway を削除します。

構文

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

説明

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
--name	登録の詳細を削除する SGD Gateway の名前
--file	複数の SGD Gateway の構成設定を含んでいるバッチファイル

例

次の例では、SGD アレイの登録済みゲートウェイのリストから、SGD Gateway gateway1.example.com を削除します。

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

B.31. --security-gateway 属性

説明

--security-gateway 属性は、SGD アレイで SGD Gateway を使用できるようにするために使用します。この属性は、次のものを定義します。

- SGD Gateway にアクセスできる SGD Client を、クライアントの IP アドレスまたは DNS 名に基づいて定義します。
- クライアントデバイスが SGD Gateway に接続するために使用するアドレス。

注記

--security-gateway 属性は、AIP 接続でのみ使用されます。HTTP 接続のルーティングは、Gateway の Apache 逆プロキシコンポーネント上の HTTP 負荷分散サービスによって処理されます。

--security-gateway 属性に加えた変更は、アレイ内のすべての SGD サーバーに適用されます。

構文

--security-gateway 属性の構文は次のとおりです。

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

この filter-spec は、次のタイプのフィルタ仕様で置き換えます。

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

- client-ip-address は、SGD Client の IP アドレスです。SGD Gateway 経由の接続の場合、これは SGD Gateway がアレイ内の SGD サーバーに接続するために使用するインタフェースです。

  単一アスタリスク * は、すべての IP アドレスを表します。

  クライアント IP アドレス文字列は * および ? のワイルドカードを含むことができ、* は複数の文字に一致し、? は単一の文字に一致します。次に例を示します。

  192.169.10.* は、192.169.10 ネットワーク上のすべてのアドレスに一致します。

  192.169.10.12? は、192.169.10.120 から 192.169.10.129 までのアドレス範囲に一致します。

  注記

  SGD Gateway とともに外部ロードバランサを使用している場合、client-ip-address にはロードバランサのアドレスを入力します。

- gateway protocol は、SGD Gateway 経由の接続の場合は sgdg で、SGD Gateway を経由せずに SGD アレイに直接接続する SGD Client の場合は direct です。
- gateway-address は SGD Gateway または外部ロードバランサ (使用している場合) の外部アドレスです。クライアントデバイスはこのアドレスを使用して SGD Gateway に接続します。

  SGD への direct 接続の場合、アレイのプライマリサーバーのアドレスを指定します。
- gateway-port は、クライアントデバイスが SGD Gateway または外部ロードバランサ (使用している場合) に接続するために使用する TCP ポートです。

  SGD への direct 接続の場合、アレイのプライマリサーバーのポートを指定します。

複数の filter-spec エントリはコンマで区切り、文字列全体を二重引用符 (" ") で囲みます。B.31項「 複数のフィルタの使用 」を参照してください。

例

次の例では、すべての SGD Client が SGD Gateway gateway1.example.com の TCP ポート 443 を使用して接続できるようにします。

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

次の例では、すべての SGD Client が外部ロードバランサ lb.example.com を使用して接続できるようにします。

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

次の例では、すべての SGD Client が SGD Gateway を経由せずに SGD アレイに直接接続できるようにします。アレイのプライマリサーバーは sgd1.example.com です。

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

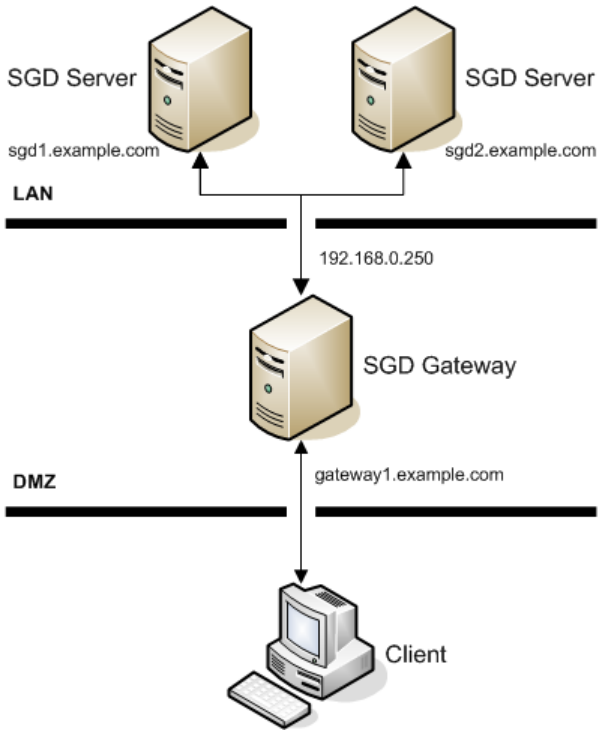
複数のフィルタの使用

次に例に示すように、複数のフィルタ仕様を使用できます。

図B.1「複数のフィルタ仕様の使用」 に示す基本的な配備について考えましょう。この配備では、単一の SGD Gateway gateway1.example.com と、2 つの SGD サーバー sgd1.example.com および sgd2.example.com を含む SGD アレイが使用されます。アレイのプライマリサーバーは sgd1.example.com です。

内部ネットワーク上の SGD Gateway のアドレスは 192.168.0.250 です。

図B.1 複数のフィルタ仕様の使用



この例には、次のようなフィルタ仕様を使用できます。

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

この構成により、次の内容が適用されます。

- アレイ内の SGD サーバーへの接続は、SGD Gateway の IP アドレス 192.168.0.250 から許可されます。組織外部の SGD Client は、SGD Gateway gateway1.example.com の TCP ポート 443 を使用して接続します。
- ローカルエリアネットワーク (LAN) 上にあるものなど、その他すべての SGD Client は、プライマリ SGD サーバー sgd1.example.com の TCP ポート 80 に直接接続します。これらの接続では SGD Gateway は使用されません。
- フィルタの順番は重要です。フィルタの順番を逆にすると、すべての SGD Client が SGD サーバー sgd1.example.com に直接接続するようになります。

付録C 詳細構成

この章では、オラクル Secure Global Desktop Gateway (SGD Gateway) の拡張機能を構成および使用することについて説明します。

この章の内容は、次のとおりです。

- 「SGD Gateway の調整」
- 「HTTP リダイレクトの構成」
- 「SGD Gateway のバインディングポートの変更」
- 「SGD アレイに対する非暗号化接続の使用」
- 「外部 SSL アクセラレータの使用」
- 「SGD Gateway 暗号化方式の構成」
- 「SGD Gateway でのクライアント証明書の使用」
- 「Balancer Manager アプリケーションの有効化」
- 「リフレクションサービス」

C.1. SGD Gateway の調整

SGD Gateway のインストール時に、SGD Gateway ホストで使用可能なメモリーに応じて、Adaptive Internet Protocol (AIP) および HTTP の同時接続の最大数が自動的に構成されます。SGD Gateway の Java 仮想マシン (JVM) に割り当てられるメモリーサイズも、この接続数に応じて最適化されます。

SGD Gateway のインストール後に、見込まれる SGD ユーザー数およびこれらのユーザーが実行するアプリケーションの数に応じて、デフォルトの設定を調整できます。その際は、JVM のメモリーサイズも調整する必要があります。この処理は、SGD Gateway の調整と呼ばれます。

注意

見込まれる接続数に対して JVM のメモリーサイズが不足すると、SGD Gateway が動作しなくなり、それ以降の接続をすべて拒否する場合があります。この場合は、十分な JVM メモリーが使用できるように SGD Gateway を調整する必要があります。SGD Gateway で java.lang.OutOfMemoryError のエラーメッセージが表示された場合は、調整が必要な可能性があります。

SGD Gateway を調整するには、次の作業を実行します。

- AIP 接続の最大数を変更します。「AIP 接続の最大数の変更」を参照してください。
- HTTP 接続の最大数を変更します。「HTTP 接続の最大数の変更」を参照してください。
- JVM のメモリーサイズを変更します。「JVM のメモリーサイズの変更」を参照してください。

C.1.1. AIP 接続の最大数の変更

AIP 接続の最大数はインストール時に構成されます。デフォルトの設定は、SGD Gateway ホストで使用可能なメモリーリソースによって異なります。

使用している配備に応じて、この設定をより適した値に変更できます。SGD Gateway で使用される AIP 接続の最大数を計算する方法の詳細については、「AIP 接続数の計算」を参照してください。

AIP 接続の最大数を変更するには、gateway config edit コマンドの --routes-aip-maxcon オプションを使用します。たとえば、AIP 接続の最大数を 3000 に変更するには、次のコマンドを実行します。

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

実行した変更を有効にするには、SGD Gateway を再起動する必要があります。

C.1.1.1. AIP 接続数の計算

SGD Gateway で使用される AIP 接続の数は、同時に接続する SGD ユーザーの数およびこれらのユーザーが実行するアプリケーションの数によって異なります。

AIP 接続数 = (アプリケーションの数 + 3) x SGD ユーザーの数

たとえば、SGD Gateway で 1000 人の SGD ユーザーがそれぞれ 4 つのアプリケーションを実行する場合、必要な AIP 同時接続の最大数は次のようになります。

(4 + 3) x 1000 = 7000 AIP 接続

C.1.2. HTTP 接続の最大数の変更

HTTP 接続の最大数はインストール時に構成されます。この設定は、同時ユーザーの最大数を定義します。デフォルト値は 100 です。

HTTP 接続の最大数を変更するには、gateway config edit コマンドの --routes-http-maxcon オプションを使用します。たとえば、HTTP 接続の最大数を 200 に変更するには、次のコマンドを実行します。

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

実行した変更を有効にするには、SGD Gateway を再起動する必要があります。

C.1.3. JVM のメモリーサイズの変更

HTTP 接続と AIP 接続の最大数を変更する場合は、SGD Gateway の JVM に割り当てられているメモリーサイズの変更も必要になることがあります。これを行うには、/opt/SUNWsgdg/proxy/etc/tuning_parameters ファイルで次の設定を編集します。

- -Xms – JVM の初期メモリーサイズ (バイト単位)
- -Xmx – JVM の最大メモリーサイズ (バイト単位)

ヒント

これらの設定では、K (キロ) および M (メガ) 修飾子を使用できます。たとえば、960K = 960K バイト、512M = 512M バイトです。

JVM メモリーサイズの値を計算する方法の詳細については、「JVM のメモリーサイズの計算」を参照してください。

注記

JVM の設定に対して十分なメモリーリソースがシステムに設定されていることを確認してください。

実行した変更を有効にするには、SGD Gateway を再起動する必要があります。

C.1.3.1. JVM のメモリーサイズの計算

SGD Gateway で使用される JVM メモリーの量は、AIP および HTTP の同時接続数によって異なります。

各 SGD Gateway 接続に約 300K バイトの JVM メモリーが必要なので、必要な JVM メモリーは次のように求められます。

(AIP 接続数 + HTTP 接続数) x 300K バイト

たとえば、SGD Gateway で 500 人の SGD ユーザーがそれぞれ 2 つのアプリケーションを実行するとします。AIP 同時接続の最大数は次のようになります。

(2 + 3) x 500 = 2500 AIP 接続

SGD Gateway では、SGD Web サーバーに対する十分な数の HTTP 同時接続も処理する必要があります。この例では、HTTP 接続の最大数は次のとおりです。

250 HTTP 接続

したがって、必要な JVM メモリーは次のようになります。

(2500 + 250) x 300K バイト = 約 806M バイト

注記

/opt/SUNWsgdg/proxy/etc/tuning_parameters ファイル内で、-Xms および -Xmx パラメータを、計算された JVM 値に設定します。-Xms および -Xmx は通常、パフォーマンス上の理由で同じ値に設定されます。

C.2. HTTP リダイレクトの構成

デフォルトでは、SGD Gateway は TCP ポート 80 での HTTP 接続を拒否します。

TCP ポート 80 での接続を有効にするには、次のように gateway config enable コマンドを使用して HTTP リダイレクトサービスを有効にします。

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

実行した変更を有効にするには、SGD Gateway を再起動する必要があります。

C.3. SGD Gateway のバインディングポートの変更

SGD Gateway で着信接続に使用されるインタフェースとポートは、バインディングポートと呼ばれます。デフォルトでは、SGD Gateway はすべてのインタフェースで TCP ポート 443 をバインディングポートとして使用します。

バインディングポートを変更するには、gateway config edit コマンドの --binding オプションを使用します。たとえば、バインディングポートを TCP ポート 4443 に変更するには、次のコマンドを実行します。

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

または、SGD Gateway ホストで /opt/SUNWsgdg/bin/gateway config create コマンドを実行することによっても、バインディングポートを変更できます。このコマンドでは、着信プロキシ接続に使用するインタフェースとポートの入力が求められます。

注記

gateway config create コマンドを使用すると新しい構成が作成され、それまでに行なった設定はすべて上書きされます。

実行した変更を有効にするには、SGD Gateway を再起動する必要があります。

C.4. SGD アレイに対する非暗号化接続の使用

デフォルトでは、SGD Gateway とアレイ内の SGD サーバーの間の接続は、Secure Sockets Layer (SSL) を使用してセキュリティー保護されます。つまり、AIP over SSL データでは TCP ポート 5307 が使用され、HTTPS データでは TCP ポート 443 が使用されます。

SGD Gateway とアレイ内の SGD サーバーの間で非暗号化接続を使用するには、「SGD アレイへの非暗号化接続を使用するための Gateway の構成」を参照してください。

非暗号化接続の場合、AIP データでは TCP ポート 3144 が使用され、HTTP データでは TCP ポート 80 が使用されます。

C.4.1. SGD アレイへの非暗号化接続を使用するための Gateway の構成

この手順では、非暗号化接続を使用するために Gateway の配備を再構成する方法について説明します。

1. SGD アレイへの非暗号化接続を使用するように Gateway 構成を変更します。

```
# gateway config create
```

注記

このコマンドは Gateway の現在の構成を上書きします。

Gateway とアレイ内の SGD サーバーの間の接続をセキュリティー保護するかどうかをたずねるプロンプトが表示されたら、n と入力します。

2. Gateway に対して以前登録された SGD サーバーを削除します。

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

ここで、sgd.example.com は SGD サーバーの名前です。

SGD サーバーの CA 証明書と SSL 証明書が Gateway キーストアから削除されます。

3. アレイ内の SGD サーバーが標準の非暗号化接続を使用するように構成されるようにします。

アレイ内の各 SGD サーバーについて次のコマンドを実行し、SGD セキュリティーサービスをオフにします。

```
# tarantella security disable
```

4. アレイ内の SGD サーバーを Gateway に登録します。

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

この例では、CA 証明書 PeerCAcert.pem を、sgd.example.com という別名を使用して SGD Gateway キーストアに追加します。SGD Web サーバーの URL は http://sgd.example.com です。

5. Gateway を再起動します。

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

C.5. 外部 SSL アクセラレータの使用

デフォルトでは、SGD Gateway は、SSL を使用してセキュリティー保護された HTTP および AIP の着信データ接続で動作するように構成されています。Gateway では、SSL の処理を行うために外部 SSL アクセラレータの使用もサポートされています。

Gateway で外部 SSL アクセラレータを使用するには、次の手順を実行します。

- SSL 接続を復号化し、それらを暗号化されていない接続として Gateway に転送するように外部 SSL アクセラレータを構成します。
- Gateway で外部 SSL アクセラレータのサポートを有効にします。

  これにより、セキュリティー保護されたポートで Gateway が暗号化されていない接続を受け入れることができるようになります。「外部 SSL アクセラレータのサポートを有効にする方法」を参照してください。
- クライアントデバイスで SSL アクセラレータがネットワークのエントリポイントとして使用されていることを確認します。

  通常、SSL アクセラレータはロードバランサでもあります。「負荷分散された配備」で説明されている負荷分散された配備に対して SGD サーバーと Gateway を構成します。

C.5.1. 外部 SSL アクセラレータのサポートを有効にする方法

Gateway を経由して SGD に接続されているユーザーがいないことを確認します。

1. SGD Gateway ホストにスーパーユーザー (root) としてログインします。
2. 暗号化されていない着信接続のサポートを有効にします。

   gateway.xml ファイルのシンボリックリンクを変更して、デフォルトの gateway-ssl.xml ではなく、gateway-plaintext.xml ファイルにリンクするようにします。

   次のコマンドを実行します。

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

3. (オプション) Gateway のバインディングポートを変更します。

   ネットワークの構成によっては、SGD Gateway のバインディングポートを変更する必要がある場合もあります。

   「SGD Gateway のバインディングポートの変更」を参照してください。

4. SGD Gateway を再起動します。

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

C.6. SGD Gateway 暗号化方式の構成

Gateway では、広い範囲にわたる SSL 接続用の暗号化方式群がサポートされています。サポートされる暗号化方式群のリストについては、『オラクル Secure Global Desktop のプラットフォームサポートおよびリリースノート (リリース 4.7 用)』を参照してください。

インストール中、Gateway は、ハイグレードの暗号化方式のみで構成される暗号化方式のセットを使用するように構成されます。つまり、Gateway への SSL 接続では、常に強化されたセキュリティーが使用されるということを意味します。必要な場合、別の暗号化方式のセットを使用するように Gateway を構成できます。

C.6.1. Gateway の暗号化方式を構成する方法

1. Gateway を停止します。

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

2. 必要な暗号化方式を構成します。

   /opt/SUNWsgdg/etc ディレクトリで、ciphersuites.xml ファイルを編集します。

   デフォルトでは、ciphersuites.xml ファイルには、ハイグレード暗号化方式のための次のエントリが含まれています。

   ```
   <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. /opt/SUNWsgdg/etc/gateway.xml ファイル内に次のエントリが存在し、ciphersuites.xml が含まれていることを確認します。

   ```
   <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. Gateway を再起動します。

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

C.7. SGD Gateway でのクライアント証明書の使用

クライアント証明書を使用して、有効な証明書を持っているユーザーにアクセスを制限することによって、SGD Gateway のセキュリティーを強化できます。

クライアント証明書とは、クライアントデバイスのブラウザにインストールされる SSL 証明書です。クライアント証明書のインストール方法については、ブラウザのオンラインドキュメントを参照してください。

新しいクライアント証明書の証明書発行リクエスト (CSR) を生成する必要がある場合は、「クライアント証明書の CSR を生成する方法」を参照してください。

次の手順では、keytool アプリケーションが使用されています。keytool アプリケーションを使用する方法の詳細については、JDK Tools and Utilities のドキュメントを参照してください。

C.7.1. クライアント証明書が使用されるように SGD Gateway を構成する方法

1. SGD Gateway ホストにスーパーユーザー (root) としてログインします。
2. SGD Gateway を停止します。

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

3. HTTPS クライアント接続にクライアント証明書が使用されるように、SGD Gateway を構成します。

   次のように、<needClientAuth> エントリを /opt/SUNWsgdg/etc/gateway.xml ファイルに追加します。

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

4. (オプション) クライアント証明書を SGD Gateway クライアントキーストアにインポートします。

注記

クライアント証明書が、信頼された認証局 (CA) によって署名されている場合、このステップを実行する必要はありません。

keytool コマンドを次のように使用します。

```
# /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‘
```

この例では、クライアント証明書 mycert.crt が SGD Gateway クライアントキーストアにインポートされます。クライアント証明書は、mycert の別名で保存されます。

5. SGD Gateway を起動します。

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

C.7.2. クライアント証明書の CSR を生成する方法

Gateway で使用できるクライアント証明書を取得するには、最初に CSR を生成する必要があります。次に、CSR を認証局 (CA) に送信して署名を受けます。

注記

この手順では、Gateway ホスト上で keytool アプリケーションを使用して CSR を生成する方法を示します。ただし、この手順に記載するステップを使用する必要はありません。その代わりに、使い慣れた証明書管理ツールを使用して CSR を生成できます。

1. SGD Gateway ホストにスーパーユーザー (root) としてログインします。
2. 自己署名付き証明書および対応する非公開鍵を生成します。

   keytool コマンドを次のように使用します。

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

   この例では、自己署名付き証明書と非公開鍵は、keystore.mycert と呼ばれるキーストア内で作成および保管されます。鍵ペアは、mycert の別名で保存されます。
3. 自己署名付き証明書の CSR を生成します。

   keytool コマンドを次のように使用します。

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

   この例では、CSR は /tmp/gateway-name.csr というファイル内に生成および保管され、ここで gateway-name は Gateway の名前です。

C.8. Balancer Manager アプリケーションの有効化

Apache 逆プロキシには Balancer Manager という Web アプリケーションが含まれています。Balancer Manager では、逆プロキシで使用される負荷分散グループの SGD Web サーバーを管理できます。

Balancer Manager を使用すると、次の作業を実行できます。

- 負荷分散グループの SGD Web サーバーのステータス情報を表示します
- SGD Web サーバーの負荷分散の経路を表示および変更します
- 負荷分散グループから SGD Web サーバーを削除します

Balancer Manager を有効にするには、逆プロキシ構成ファイル /opt/SUNWsgdg/httpd/apache-version/conf/extra/gateway/httpd-gateway.conf 内で、アプリケーションを無効にしているコメントを削除します。

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

加えた変更を有効にするには、Gateway を再起動する必要があります。

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

Balancer Manager にアクセスするには、ブラウザを起動して、https://gateway.example.com/balancer-manager にアクセスします。ここで、gateway.example.com は SGD Gateway ホストです。

Balancer Manager の構成の詳細については、Apache mod_proxy_balancer のドキュメント を参照してください。

C.9. リフレクションサービス

リフレクションサービスとは、SGD Gateway のルーティングプロキシコンポーネントで使用される RESTful Web サービスの集まりです。SGD Gateway 管理者はリフレクションサービスを使用すると、ルーティングプロキシの経路、サービス、ロギングレベル、および接続を構成したり、ステータス情報を表示したりできます。

このセクションでは、次に示すリフレクションサービス関連のトピックについて説明します。

- 「リフレクションサービスの有効化」
- 「リフレクションサービスの使用」

C.9.1. リフレクションサービスの有効化

デフォルトでは、SGD Gateway のリフレクションサービスは無効になっています。

次のアクセス方法の 1 つ以上に対してリフレクションサービスを有効にします。

- 無認証アクセス – ユーザーは認証を受ける必要がありません。

  デフォルトでは、無認証アクセスを使用できるのは SGD Gateway ホストからだけです。

  無認証アクセスを有効にする方法の詳細については、「リフレクションサービスに対する無認証アクセスを有効にする方法」を参照してください。

- 認証アクセス – ユーザーはリフレクションサービスにアクセスする前に認証を受ける必要があります。

  認証アクセスを有効にする方法の詳細については、「リフレクションサービスに対する認証アクセスを有効にする方法」を参照してください。

C.9.1.1. リフレクションサービスに対する無認証アクセスを有効にする方法

1. SGD Gateway ホストにスーパーユーザー (root) としてログインします。
2. リフレクションサービスに対する無認証アクセスを有効にします。

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

3. (オプション) リフレクションサービスで使用するインタフェースを変更します。

注意

デフォルトでは、リフレクションサービスに対する無認証アクセスを使用できるのは SGD Gateway ホストからだけです。ほかのインタフェースで無認証アクセスを有効にすると、セキュリティーリスクが発生する可能性があります。

リフレクションサービスに対する無認証アクセスに使用されるデフォルトのインタフェースは、localhost ループバックインタフェースです。次の例は、すべてのインタフェースで無認証アクセスを有効にする方法を示しています。

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

4. (オプション) リフレクションサービスで使用するポートを変更します。

   リフレクションサービスに対する無認証アクセスに使用されるデフォルトのポートは、TCP ポート 81 です。これを別の未使用のポートに次の手順で変更できます。

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

   ここで、portnum はリフレクションサービスで使用するポート番号です。

5. SGD Gateway を再起動します。

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

6. リフレクションサービスにアクセスします。

   SGD Gateway ホストで、ブラウザを起動して http://localhost:81 にアクセスします。

   リフレクションサービスのホームページが表示されます。

C.9.1.2. リフレクションサービスに対する認証アクセスを有効にする方法

1. SGD Gateway ホストにスーパーユーザー (root) としてログインします。
2. リフレクションサービスの証明書と非公開鍵をエクスポートします。

   リフレクションサービスの証明書と非公開鍵は、リフレクションサービスキーストア /opt/SUNWsgdg/proxy/etc/keystore.reflection に保存されています。このキーストアは、SGD Gateway のインストール時に自動的に作成されます。

   デフォルトでは、リフレクションサービスキーストアには自己署名付き証明書と鍵のペアが 1 つ入っています。

   a. リフレクションサービスの証明書をエクスポートします。

```
# /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
```

      ここで、server-name はリフレクションキーストアでリフレクションサービスの証明書に使用されている別名、client.pem はエクスポートした証明書のファイル名です。

      keytool アプリケーションを使用する方法の詳細については、JDK Tools and Utilities のドキュメントを参照してください。

   b. リフレクションサービスの非公開鍵をエクスポートします。

      SGD Gateway に組み込まれている KeyManager アプリケーションを使用します。

```
# /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)"
```

      ここで、alias-name はリフレクションキーストアでリフレクションサービスの鍵に使用されている別名、client.key はエクスポートした鍵のファイル名です。

3. 証明書と非公開鍵をクライアントデバイスにインストールします。

   証明書と非公開鍵は、リフレクションサービスに対する承認を得るためにクライアントデバイスで使用されます。

   証明書と鍵をブラウザの証明書ストアにインポートするには、最初に証明書と鍵を PKCS12 形式のファイルに変換する必要があります。次に例を示します。

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

   このコマンドは、証明書ファイル mycert.crt および関連付けられた非公開鍵 mycert_key.pem を、PKCS12 形式の証明書ファイル mycert.p12 に変換します。

   PKCS12 形式の証明書をブラウザにインポートする方法の詳細については、ブラウザのオンラインドキュメントを参照してください。

4. リフレクションサービスに対する認証アクセスを有効にします。

SGD Gateway ホストで、次のコマンドを実行します。

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

5. (オプション) リフレクションサービスで使用するインタフェースとポートを変更します。

   リフレクションサービスに対する認証アクセスに使用されるデフォルトのバインディングは、すべてのインタフェースの TCP ポート 82 です。これを別のインタフェースの未使用のポートに次の手順で変更できます。

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

   ここで、int はインタフェース、portnum はリフレクションサービスで使用するポート番号です。

6. SGD Gateway を再起動します。

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

7. 証明書と非公開鍵を使用して、クライアントデバイスからリフレクションサービスに接続します。

   - curl コマンドを使用する場合:

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

     この例では、curl コマンドを使用してリフレクションサービスのホームページ https://gateway.example.com:82 にアクセスします。ここで、gateway.example.com は SGD Gateway の名前です。リフレクションサービスの証明書と非公開鍵は、client.pem と client.key です。

   - ブラウザを使用する場合:

     https://gateway.example.com:82 に移動します。ここで、gateway.example.com は SGD Gateway の名前です。

     リフレクションサービスのホームページが表示されます。

C.9.2. リフレクションサービスの使用

リフレクションサービスによって提供されている RESTful Web サービスにアクセスするには、クライアントアプリケーションを使用します。適切なクライアントアプリケーションには次のようなものがあります。

- ブラウザ。リフレクションサービスにアクセスするもっとも簡単な方法は、ブラウザを使用することです。ただし、ブラウザでサポートされるのは HTTP GET リクエストだけなので、情報を取り出す RESTful Web サービスにしかアクセスできません。実際、ブラウザを使用すると、ルーティングプロキシのステータス情報を表示したり、経路とサービスを一覧表示したりするタスクに役立ちます。
- curl。これは UNIX および Linux プラットフォーム用のコマンド行ツールで、HTTP GET、PUT、POST、および DELETE リクエストをサポートしています。したがって、リフレクションサービスの全種類の RESTful Web サービスを使用できます。このツールの出力をファイルや別のプログラムにリダイレクトして、さらに処理することもできます。

または、RESTful Web サービスをサポートするユーザー独自のクライアントアプリケーションを持っている場合は、それを使用してリフレクションサービスにアクセスできます。

注記

リフレクションサービスを使用してルーティングプロキシの構成を変更する場合、SGD Gateway を再起動する必要はありません。

リフレクションサービスからは次の出力形式でデータが返されることがあります。

- ASCII。これはデフォルトの出力形式です。データはタブで区切られた ASCII 形式で返されます。この出力形式は、あとでデータに構文解析などの処理を行う場合に役立ちます。
- HTML。データは、ブラウザでの表示に適した HTML 形式で返されます。HTML 出力で返すには、Web サービスの URI (Uniform Resource Identifier) の末尾に /html を付加します。

C.9.2.1. RESTful Web サービスについて

表C.1「SGD Gateway リフレクションサービスの RESTful Web サービス」 に、SGD Gateway リフレクションサービスの RESTful Web サービスの一覧を示します。

表C.1 SGD Gateway リフレクションサービスの RESTful Web サービス

相対 URI	HTTP リクエストメソッド	説明
/	GET	ルーティングプロキシに関する稼働時間などの概要情報を表示します。
/service	GET	使用可能なサービスを一覧表示します。 サービスは、ルーティングプロキシが着信接続を行うエントリポイントです。
/service/Service-Id	GET	Service-Id で指定されたサービスの情報を一覧表示します。
/service/Service-Id	PUT	Service-Id で指定されたサービスを起動します。
/service/Service-Id	DELETE	Service-Id で指定されたサービスを停止します。
/client	GET	使用可能なクライアントを一覧表示します。 クライアントは、ルーティングプロキシが発信接続を行う出口ポイントです。
/client/Client-Id	GET	Client-Id で指定されたクライアントの情報を一覧表示します。
/route	GET	使用可能な経路を一覧表示します。 経路は、サービス経由の着信接続から、クライアント経由の発信接続までの、ルーティングプロキシを通る経路です。
/route/Route-Id	GET	Route-Id で指定された経路の情報を一覧表示します。
/route/Route-Id	PUT	Route-Id で指定された経路を起動します。
/route/Route-Id	DELETE	Route-Id で指定された経路を停止します。
/route/Route-Id/connection	GET	Route-Id で指定された特定の経路の接続を一覧表示します。
/route/Route-Id/connection/Connection-Id	DELETE	Connection-Id で指定された接続を終了します。
/connection	GET	すべての経路について、現在実行中の接続を一覧表示します。
/logging/level	GET	グローバルなロギングレベルを表示します。
/logging/level/Log-Level	PUT	ルーティングプロキシのグローバルなロギングレベルを設定します。
/logging/Package/level	GET	ルーティングプロキシの特定のコンポーネントのロギングレベルを表示します。
/logging/Package/level/Log-Level	PUT	ルーティングプロキシの特定のコンポーネントのロギングレベルを設定します。

RESTful Web サービスにアクセスするには、リフレクションサービスの URL に Web サービスの相対 URI を付加します。

たとえば、SGD Gateway gateway.example.com の使用可能な経路を一覧表示するには、次のようにリフレクションサービスの URL に /route を付加します。

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

ここで、client.pem と client.key は、リフレクションサービスの証明書と非公開鍵です。この例では、クライアントはリフレクションサービスにアクセスする前に認証を受けます。

C.9.2.2. リフレクションサービスの使用例

次の例ではいずれも、リフレクションサービスにアクセスするためのクライアントアプリケーションとして curl コマンドを使用します。

これらの例では、gateway.example.com という SGD Gateway のリフレクションサービスに対して認証アクセスを使用します。クライアントは、証明書 client.pem および非公開鍵 client.key を使用して認証されます。

SGD Gateway の使用可能なサービスを一覧表示するには:

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

経路を停止するには、リフレクションサービスでその経路に使用されている Route Id を指定します:

```
$ 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
```

グローバルなロギングレベルを FINER に設定するには:

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

付録D SGD Gateway のトラブルシューティング

この章には、オラクル Secure Global Desktop Gateway (SGD Gateway) の問題を診断して修正するために役立つトラブルシューティングのトピックが含まれています。

この章の内容は、次のとおりです。

- 「ロギングと診断」
- 「SGD サーバーのピア DNS 名の変更」
- 「SGD Gateway のエラーメッセージ」

D.1. ロギングと診断

このセクションでは、SGD Gateway のロギング機能と診断機能について説明します。

このセクションの内容は、次のとおりです。

- 「SGD Gateway のロギングについて」
- 「SGD Gateway のプロセス情報の表示」
- 「コマンド行からの設定の確認」

D.1.1. SGD Gateway のロギングについて

SGD Gateway のロギングでは、Java Logging アプリケーションプログラミングインタフェース (API) が使用されます。Java でのロギングの実装については、http://download.oracle.com/javase/6/docs/technotes/guides/logging/overview.html を参照してください。

D.1.1.1. ロギングレベルの変更

SGD Gateway ではロギングプロパティー構成ファイル logging.properties が提供されています。このファイルは /opt/SUNWsgdg/proxy/etc ディレクトリにあります。

logging.properties ファイルを編集して、デフォルトのロギングレベルを変更したり、特定の SGD Gateway サービスのロギングレベルを構成したりできます。logging.properties ファイルでは、各 SGD Gateway サービスは async.channel エントリで表されます。

たとえば、TCP の着信接続と発信接続のロギングレベルを上げるには、TCP サービスのロギングレベルを FINEST に設定します。logging.properties ファイルで、次の行のコメントを解除します。

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

FileHandler クラスのドキュメントに、logging.properties ファイルで使用できるロギングレベルパラメータが記載されています。

logging.properties ファイルを編集してロギングレベルを変更した場合、変更を有効にするには SGD Gateway を再起動する必要があります。

注記

SGD Gateway リフレクションサービスを使用してロギングレベルを変更することもできます。リフレクションサービスの構成と使用については、「リフレクションサービス」を参照してください。

D.1.1.2. ログファイルの場所

SGD Gateway に問題が発生した場合は、次のログファイルを調べてください。

- ルーティングプロキシのログファイル。これらのログファイルの場所と名前は、logging.properties ファイルで設定されます。デフォルトでは、SGD Gateway はルーティングプロキシのログファイルを SGD Gateway ホストの /opt/SUNWsgdg/proxy/var/log ディレクトリに作成します。
- 逆プロキシのログファイル。HTTP 接続および HTTPS 接続の負荷分散およびプロキシサーバーのアクティビティーの詳細は、SGD Gateway ホストの /opt/SUNWsgdg/httpd/apache-version/logs ディレクトリの Apache ログファイルに記録されます。
- SGD サーバーのログファイル。アレイ内の各 SGD サーバーは、SGD サーバーホストの /opt/tarantella/var/log ディレクトリのログファイルにエラーメッセージを書き込みます。SGD サーバーのロギングの構成についての詳細は、『オラクル Secure Global Desktop 管理者ガイド (リリース 4.7 用)』の、監視およびロギングに関する第 6 章を参照してください。

D.1.2. SGD Gateway のプロセス情報の表示

SGD Gateway の起動時に、ルーティングプロキシのプロセス ID が SGD Gateway ホスト上の /opt/SUNWsgdg/proxy/var/run/proxy.pid ファイルに保存されます。

逆プロキシのプロセス ID は /opt/SUNWsgdg/httpd/apache-version/logs/httpd.pid ファイルに保存されます。このファイルの場所は、httpd.conf Apache 設定ファイルの PidFile 指令を使用して変更できます。

実行中の SGD Gateway プロセスを表示するには、SGD Gateway ホストで次のコマンドを使用します。

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

D.1.3. コマンド行からの設定の確認

次のコマンドを使用すると、SGD Gateway の構成を確認できます。

- gateway status – SGD Gateway のステータス情報を表示します。

  SGD Gateway ホストで次のコマンドを実行します。

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

  このコマンドの詳細については、「gateway status」も参照してください。

- tarantella gateway list – SGD アレイで使用することを承認されている SGD Gateway のリストを表示します。

  アレイ内の任意の SGD サーバーで次のコマンドを実行します。

  ```
  $ tarantella gateway list
  ```

  tarantella gateway コマンドの使用方法の詳細については、「tarantella gateway コマンド」を参照してください。

- tarantella config list – SGD アレイのグローバル設定を表示します。

  任意の SGD サーバーで次のコマンドを実行して、--security-gateway 属性の設定を表示します。この属性により、SGD Gateway の使用を許可される SGD Client が決まります。

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

  この属性の詳細については、「--security-gateway 属性」を参照してください。

D.2. SGD サーバーのピア DNS 名の変更

ピア DNS 名とは、SGD サーバーが、アレイ内のほかの SGD サーバーから自分自身を識別するために使用する DNS 名です。たとえば、boston.example.com です。

SGD サーバーのピア DNS 名を変更すると、Gateway がそのサーバーに接続できなくなることがあります。これは、Gateway によって使用されている証明書に、新しい DNS 名が含まれていないためです。

次のようにして、Gateway の配備を再構成することが必要な場合もあります。

1. (オプション) 新しい SGD サーバー SSL 証明書をインストールします。「SGD サーバーの証明書をインストールする方法」を参照してください。

   この手順は、SGD サーバーによって使用されている SSL 証明書に新しいピア DNS 名が含まれていない場合に必要です。SGD サーバー上の SSL 証明書を置き換えて、新しい SSL 証明書を各 Gateway にインストールする必要があります。

2. (オプション) SGD サーバーの新しい CA 証明書をインストールします。「SGD サーバーの証明書をインストールする方法」を参照してください。

   この手順は、アレイ内のプライマリサーバーのピア DNS 名を変更した場合に必要です。アレイ内のセキュリティー保護された通信に使用される証明書を再生成して、新しい CA 証明書を各 Gateway にインストールする必要があります。

SGD サーバーのピア DNS 名を変更する方法の詳細については、『オラクル Secure Global Desktop 管理者ガイド (リリース 4.7 用)』の第 1 章の、ピア DNS 名に関するセクションを参照してください。

D.3. SGD Gateway のエラーメッセージ

SGD Gateway のエラーメッセージは、SGD Gateway ホストの /opt/SUNWsgdg/proxy/var/log ディレクトリにあるルーティングプロキシのログファイルに報告されます。

SGD Gateway の代表的なエラーメッセージのいくつかを、その推定原因の説明とともに表D.1「SGD Gateway のエラーメッセージ」に示します。

表D.1 SGD Gateway のエラーメッセージ

エラーメッセージ	推定原因
トークンの検証に失敗しました: トークンはまだ有効になっていません	SGD Gateway とアレイ内の SGD サーバーのクロックが同期していません
トークンの復号化に失敗しました: 信頼できる署名が見つかりません	SGD サーバーの CA 証明書が SGD Gateway にインストールされていません
トークンの検証に失敗しました: トークンを復号化できる受信者がありません	SGD Gateway の証明書が SGD アレイにインストールされていません
SSL error: プロキシの SSL キーストアに有効な信頼できる証明書があることを確認してください	SGD サーバーの SSL 証明書が SGD Gateway にインストールされていません