Oracle® Secure Global Desktop

Guide d'administration de Gateway version 4.7

E35903-01
Août 2012

Oracle® Secure Global Desktop: Guide d'administration de Gateway version 4.7

Résumé

Ce guide explique comment installer, configurer et utiliser le serveur Oracle Secure Global Desktop Gateway.

Document publié le : 2012-10-18 (revision: 1177)

Table des matières

Préface

Le manuel *Guide d'administration d'Oracle Secure Global Desktop Gateway version 4.7* fournit des instructions d'installation, de configuration et d'utilisation d'Oracle Secure Global Desktop (SGD Gateway). Ce document est destiné aux administrateurs système.

1. Public

Ce document s'adresse aux personnes qui utilisent le serveur SGD Gateway pour la première fois. Il est supposé que ce public maîtrise les technologies Web et les plates-formes Windows et UNIX.

2. Organisation de ce document

Ce document est organisé comme suit :

- Chapitre 1, *Installation du serveur SGD Gateway* explique comment installer le serveur SGD Gateway.
- Chapitre 2, *Configuration de la passerelle SGD Gateway* décrit comment configurer le serveur SGD Gateway pour votre réseau.
- Annexe A, *Présentation de l'architecture de SGD Gateway* présente l'architecture du serveur SGD Gateway.
- Annexe B, *Référence de ligne de commande* décrit comment configurer et contrôler le serveur SGD Gateway à partir de la ligne de commande.
- Annexe C, *Configuration avancée* traite de la configuration avancée du serveur SGD Gateway, et notamment de la configuration et de l'utilisation du service de réflexion du serveur SGD Gateway.
- Annexe D, *Dépannage de la passerelle SGD Gateway* comprend des informations de dépannage permettant de diagnostiquer et de résoudre les problèmes liés au serveur SGD Gateway.

3. Accessibilité de la documentation

Pour en savoir plus sur l'engagement d'Oracle en matière d'accessibilité, visitez le site Web du Programme d'accessibilité d'Oracle à l'adresse http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Accès au support Oracle

Les clients d'Oracle peuvent accéder à un support électronique via My Oracle Support. Pour plus d'informations, visitez le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info ou le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs si vous êtes malentendant.

4. Documents associés

La documentation de ce produit est disponible à l'adresse :

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

Pour plus d' informations, reportez-vous aux manuels suivants :

- *Oracle Secure Global Desktop Administration Guide for Release 4.7*
- *Guide d'installation d'Oracle Secure Global Desktop version 4.7*

- *Guide de l'utilisateur d'Oracle Secure Global Desktop version 4.7*
- *Oracle Secure Global Desktop Prise en charge des plates-formes et notes de version relatives à la version 4.7*
- *Oracle Secure Global Desktop Security Guide for Release 4.7*

5. Conventions

Les conventions suivantes sont utilisées dans ce document :

Convention	Signification
gras	Les caractères en gras indiquent des éléments de l'interface utilisateur graphique associés à une action, ou des termes définis dans le texte ou le glossaire.
italique	Les caractères en italique indiquent des titres de livres, la mise en valeur d'un concept ou des variables substituables pour lesquelles vous fournissez des valeurs particulières.
`Largeur fixe`	Le type largeur fixe indique des commandes au sein d'un paragraphe, des adresses URL, des exemples de code, du texte affiché à l'écran ou du texte que vous saisissez.

Chapitre 1. Installation du serveur SGD Gateway

Faisant suite d'une brève présentation du serveur Oracle Secure Global Desktop Gateway (SGD Gateway), ce chapitre décrit comment installer le logiciel SGD Gateway. Le chapitre inclut également des informations sur la configuration système requise pour SGD Gateway.

Ce chapitre comprend les rubriques suivantes :

1.1. A propos de la passerelle SGD Gateway

La passerelle SGD Gateway est un serveur proxy conçu pour être déployé à l'avant d'un groupe de serveurs SGD dans une zone démilitarisée (DMZ). Cela permet au groupe de serveurs SGD de se trouver dans le réseau interne d'une organisation. En outre, toutes les connexions peuvent être authentifiées dans DMZ avant d'établir des connexions avec les serveurs SGD du groupe.

L'utilisation de la passerelle SGD Gateway constitue une alternative à l'exécution des serveurs SGD en mode Firewall Traversal, appelée également transfert via pare-feu.

La passerelle SGD Gateway gère l'équilibrage de charge des connexions HTTP (Hypertext Transfer Protocol, protocole de transfert hypertexte), ce qui vous évite d'avoir à utiliser la page d'équilibrage de charge JavaServer Pages (JSP) fournie avec SGD.

1.2. Configuration système requise

Les plates-formes d'installation prises en charge pour l'hôte de la passerelle SGD Gateway sont indiquées dans le document *Oracle Secure Global Desktop Prise en charge des plates-formes et notes de version relatives à la version 4.7* disponible à l'adresse http://www.oracle.com/technetwork/documentation/sgd-193668.html .

La configuration suivante s'applique aux serveurs SGD utilisés avec la passerelle SGD Gateway :

- **Mode sécurisé.** Par défaut, la passerelle SGD Gateway utilise des connexions sécurisées vers les serveurs SGD. Les connexions sécurisées doivent être activées sur vos serveurs SGD. Le transfert via pare-feu ne doit pas être activé.

  Dans une installation classique, un serveur SGD est configuré automatiquement pour utiliser les connexions sécurisées. Reportez-vous à la section "Connexions sécurisées aux serveurs SGD" du chapitre 1 du *Oracle Secure Global Desktop Administration Guide for Release 4.7* pour plus d'informations sur la manière de sécuriser un serveur SGD.

- **SGD version.** Les serveurs SGD doivent exécuter au minimum la version 4.5 de SGD. Il est préférable d'utiliser la version 4.7 de la passerelle avec la version 4.7 de SGD.

- **Synchronisation d'horloge.** Il est important que les horloges système des serveurs SGD et de la passerelle SGD Gateway soient synchronisées. Utilisez le logiciel NTP (Network Time Protocol) ou la commande `rdate` pour vous en assurer.

Pour plus d'informations sur la configuration système requise du serveur SGD , reportez-vous au manuel *Oracle Secure Global Desktop Prise en charge des plates-formes et notes de version relatives à la version 4.7*.

1.2.1. Problèmes connus

Reportez-vous au manuel *Oracle Secure Global Desktop Prise en charge des plates-formes et notes de version relatives à la version 4.7* pour plus d'informations sur les problèmes connus relatifs à cette version de la passerelle SGD Gateway.

1.3. Réalisation de l'installation

Sur les plates-formes Oracle Solaris, installez la passerelle SGD Gateway à l'aide de la commande `pkgadd`.

Sur les plates-formes Linux, installez la passerelle SGD Gateway à l'aide de la commande `rpm`.

Par défaut, la passerelle SGD Gateway est installée dans le répertoire `/opt/SUNWsgdg`. Vous pouvez changer de répertoire d'installation en procédant comme suit :

- **Plates-formes Oracle Solaris** : vous devez indiquer le répertoire d'installation à l'installation du logiciel.
- **Plates-formes Linux** : pour modifier le répertoire d'installation, spécifiez l'option `--prefix` de la commande `rpm` à l'installation du logiciel.

1.3.1. Installation de la passerelle SGD Gateway

1. Enregistrez le package SGD Gateway dans un répertoire temporaire situé sur l'hôte.

   Si vous effectuez une installation à partir d'un média d'installation, vous trouverez le package dans le répertoire `gateway`.

   Vous pouvez également télécharger le programme d'installation d'un serveur Web SGD à l'adresse `https://`*`server.example.com`*, *`server.example.com`* représentant le nom d'un serveur SGD. Lorsque la page d'accueil du serveur Web SGD s'affiche, cliquez sur Installer Oracle Secure Global Desktop Gateway.

   Les fichiers du package sont les suivants :

   - `SUNWsgdg-`*`version`*`.sol-x86.pkg` pour Oracle Solaris sur les plates-formes x86
   - `SUNWsgdg-`*`version`*`.sol-sparc.pkg` pour Oracle Solaris sur les plates-formes SPARC
   - `SUNWsgdg-`*`version`*`.i386.rpm` sur les plates-formes Linux

   où *`version`* représente le numéro de version de SGD Gateway.
2. Connectez-vous à l'hôte en tant que superutilisateur (utilisateur root).
3. Installez SGD Gateway.

   Décompressez le fichier de package avant l'installation, le cas échéant.

   Installation d'Oracle Solaris sur les plates-formes x86 :

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

   Installation d'Oracle Solaris sur les plates-formes SPARC :

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

Note

Sur les plates-formes Oracle Solaris, si l'installation échoue sur un message d'erreur `pwd: cannot determine current directory!`, réessayez en indiquant le répertoire */tempdir* .

Installation sur les plates-formes Linux :

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

4. Vérifiez que le package SGD Gateway est enregistré dans la base de données de package.

   Sur les plates-formes Oracle Solaris :

   ```
   # pkginfo -x SUNWsgdg
   ```

   Sur les plates-formes Linux :

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

5. Exécutez le programme d'installation de SGD Gateway.

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

   Le programme d'installation de SGD Gateway présente les paramètres acceptables ou modifiables suivants :

   - **Paramètres de port SGD Gateway.** Interface et port que la passerelle SGD Gateway utilise pour les connexions entrantes. Par défaut, SGD Gateway écoute sur le port 443 dans toutes les interfaces.
   - **Point d'entrée réseau.** Adresse IP (Internet Protocol), ou nom DNS (Domain Name System), et port que les périphériques client utilisent pour se connecter à la passerelle SGD Gateway. Le point d'entrée ne correspond pas toujours à l'adresse de la passerelle SGD Gateway. Selon la configuration de votre réseau, il peut s'agir de l'adresse d'un équilibreur de charge ou d'un autre périphérique externe.

     Par exemple, si des utilisateurs se connectent directement à une passerelle SGD Gateway à l'adresse `gateway1.example.com`, saisissez `gateway1.example.com:443` comme point d'entrée pour le réseau.

     Si des utilisateurs se connectent à la passerelle SGD Gateway via un équilibreur de charge à l'adresse `lb.example.com`, saisissez `lb.example.com:443` comme point d'entrée du réseau.
   - **Connexions sécurisées.** Indiquez s'il faut sécuriser les connexions entre la passerelle SGD Gateway et les serveurs SGD du groupe. Par défaut, la passerelle SGD Gateway utilise des connexions sécurisées. Pour utiliser des connexions sécurisées, les serveurs SGD du groupe doivent s'exécuter en mode sécurisé.

     Reportez-vous à Section C.4, « Utilisation de connexions non chiffrées au groupe de serveurs SGD » pour plus d'informations sur l'utilisation des connexions non chiffrées aux serveurs SGD dans le groupe.

Note

Ces paramètres peuvent être modifiés ultérieurement, à l'aide de la commande `gateway config create`. Reportez-vous à la section Section 2.2.1.1, « Procédure de configuration des ports et des connexions à la passerelle SGD Gateway ».

Une fois que vous avez installé le logiciel, vous devez effectuer des étapes de configuration supplémentaires de la passerelle SGD Gateway. Reportez-vous au Chapitre 2, *Configuration de la passerelle SGD Gateway* pours plus d'informations sur les opérations requises.

1.4. Mise à niveau de SGD Gateway

Cette section décrit comment mettre à niveau SGD Gateway.

Lorsque vous mettez SGD Gateway à niveau, la plus grande partie de votre configuration initiale, notamment les fichiers de configuration de proxy de routage, est préservée. Cependant, le processus de la mise à niveau écrase les certificats auto-signés utilisés par la passerelle.

Après une mise à niveau, vous devez reconfigurer la passerelle SGD Gateway. Suivez les étapes de configuration standard pour autoriser une passerelle sur SGD, comme décrit dans la Section 2.2.2.2, « Procédure d'installation des certificats SGD Gateway dans le groupe SGD ».

Un journal de mise à niveau est créé à l'emplacement `/opt/SUNWsgdg/proxy/var/log/upgrade_`*`oldversion_newversion`*`.log`, *`oldversion`* représentant l'ancienne version de SGD Gateway et *`newversion`* la version mise à niveau de SGD.

Lors de la mise à niveau, le programme d'installation SGD Gateway sauvegarde tous les fichiers de serveur Web Apache personnalisés qu'il détecte et les répertorie dans le journal de mise à niveau. Le cas échéant, vous devez les mettre à niveau manuellement. Vous pouvez utiliser un utilitaire tel que `diff` pour comparer les fichiers et afficher les modifications effectuées.

1.4.1. Mise à niveau de SGD Gateway

1. Assurez-vous qu'aucune session utilisateur ou session d'application ne s'exécute par le biais de la passerelle SGD Gateway.

2. Installez la nouvelle version de SGD Gateway.

   Reportez-vous à Section 1.3.1, « Installation de la passerelle SGD Gateway ».

Chapitre 2. Configuration de la passerelle SGD Gateway

Ce chapitre décrit comment configurer la passerelle SGD Gateway (SGD Gateway) dans des scénarios de déploiement type. Il couvre également les procédures de démarrage et d'arrêt de la passerelle SGD Gateway et fournit des instructions de retrait du logiciel SGD Gateway.

Ce chapitre comprend les rubriques suivantes :

2.1. Déploiement de la passerelle SGD Gateway

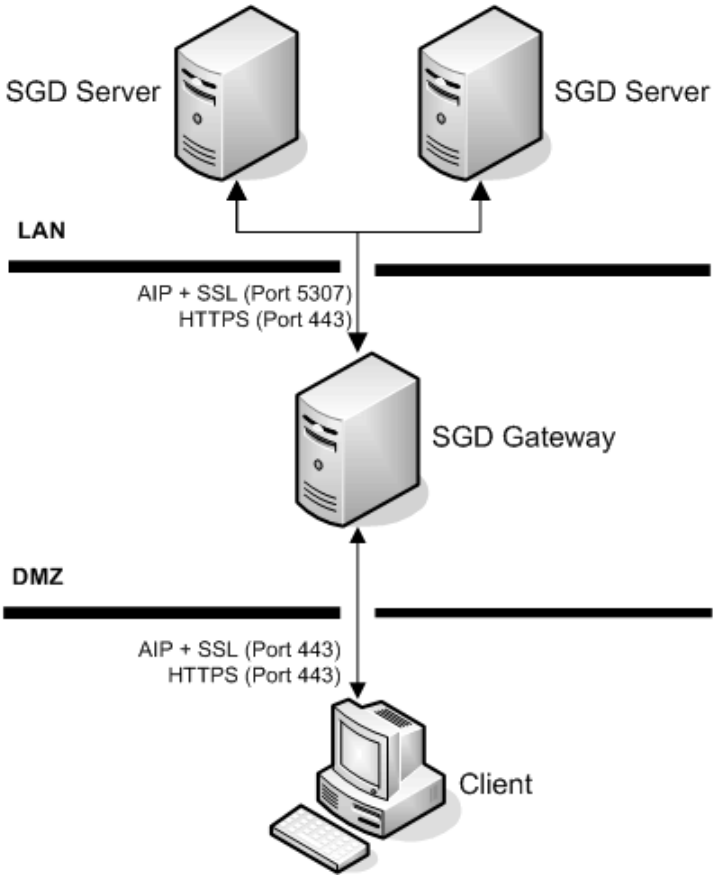
Cette section décrit les scénarios suivants de déploiement de la passerelle SGD Gateway :

2.1.1. Déploiement classique

Cette section décrit les tâches de configuration à effectuer dans le cadre d'un déploiement classique de la passerelle.

Dans un déploiement classique, une seule passerelle SGD Gateway est utilisée, comme l'illustre la Figure 2.1, « Déploiement classique avec une seule passerelle SGD Gateway ».

Figure 2.1. Déploiement classique avec une seule passerelle SGD Gateway



La configuration d'un déploiement classique implique de définir les connexions répertoriées dans le Tableau 2.1, « Connexions à configurer pour un déploiement classique de la passerelle SGD Gateway ».

Tableau 2.1. Connexions à configurer pour un déploiement classique de la passerelle SGD Gateway

Connexion	Procédure de configuration
Du périphérique client à la passerelle SGD Gateway	1. Configurez les ports et les connexions utilisés par la passerelle SGD Gateway. Vous avez configuré ces paramètres lors de l'installation de la passerelle. Reportez-vous à la section Section 2.2.1.1, « Procédure de configuration des ports et des connexions à la passerelle SGD Gateway » si vous souhaitez changer la configuration de la passerelle SGD Gateway. 2. Sur la passerelle SGD Gateway, installez un certificat SSL (Secure Sockets Layer) pour les connexions client. Reportez-vous à la section Section 2.2.1.2, « Procédure d'installation d'un certificat SSL pour les connexions client dans le keystore du client ».
De la passerelle SGD Gateway aux serveurs SGD	1. Activez les services de sécurité SGD pour le groupe.

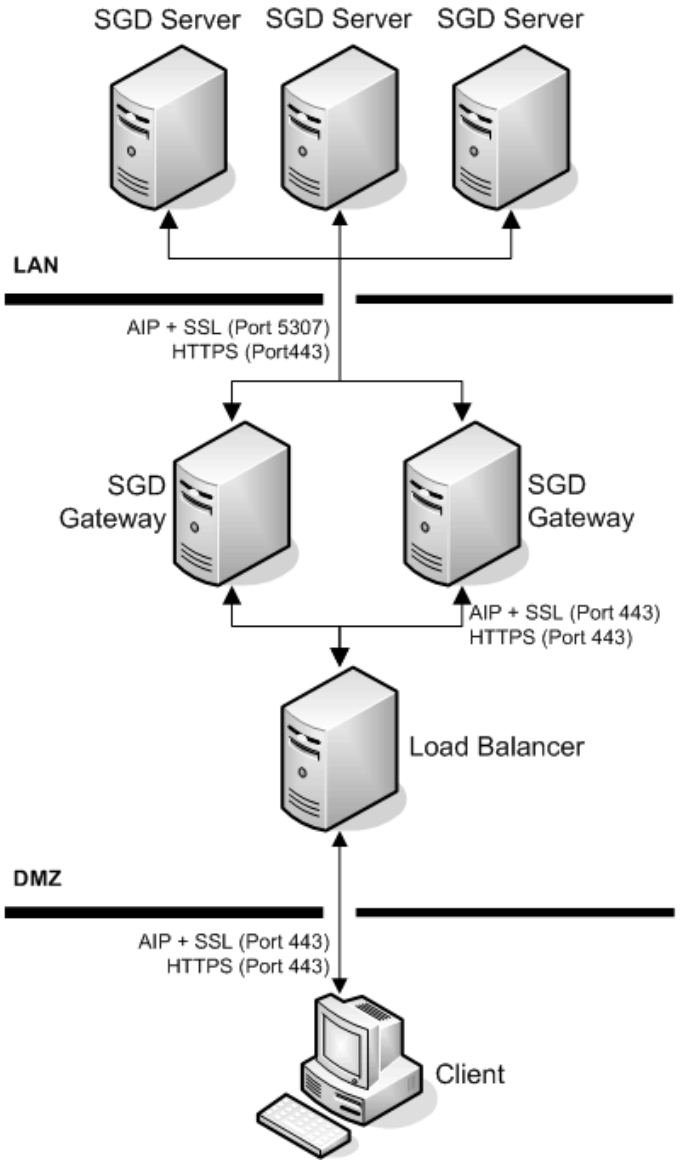
Connexion	Procédure de configuration
	Les serveurs SGD doivent s'exécuter en mode sécurisé. Le transfert via pare-feu ne doit pas être activé. Dans une installation classique, un serveur SGD est configuré automatiquement pour utiliser les connexions sécurisées. Reportez-vous à la section "Connexions sécurisées aux serveurs SGD" du chapitre 1 du *Oracle Secure Global Desktop Administration Guide for Release 4.7* pour plus d'informations sur la manière de sécuriser un serveur SGD. 2. Sur la passerelle SGD Gateway, installez les certificats de sécurité des serveurs SGD. Utilisez la commande `gateway server` pour importer les certificats CA et les certificats SSL des serveurs SGD dans le groupe dans le keystore de la passerelle SGD Gateway. Reportez-vous à la section Section 2.2.2.1, « Procédure d'installation des certificats de serveur SGD ». 3. Configurez les serveurs SGD du groupe de sorte qu'ils utilisent la passerelle SGD Gateway. Installez le certificat SGD Gateway dans le groupe SGD et utilisez la commande `tarantella gateway add` pour enregistrer la passerelle SGD Gateway auprès du groupe SGD. Reportez-vous à la section Section 2.2.2.2, « Procédure d'installation des certificats SGD Gateway dans le groupe SGD ». 4. Configurez les connexions client SGD que la passerelle SGD Gateway peut utiliser. Reportez-vous à la section Section 2.2.2.3, « Procédure de configuration des connexions client SGD ».

2.1.2. Déploiement avec équilibrage de charge

Cette section décrit les tâches de configuration à effectuer dans le cadre d'un déploiement de la passerelle avec équilibrage de charge.

Un déploiement avec équilibrage de charge utilise plusieurs passerelles SGD et un équilibreur de charge come point d'entrée du réseau, comme illustré à la Figure 2.2, « Déploiement réseau avec plusieurs passerelles SGD et un équilibreur de charge ».

Figure 2.2. Déploiement réseau avec plusieurs passerelles SGD et un équilibreur de charge



La configuration d'un déploiement avec équilibrage de charge implique de définir les connexions répertoriées dans le Tableau 2.2, « Connexions à configurer pour un déploiement de la passerelle SGD Gateway avec équilibrage de charge ».

Tableau 2.2. Connexions à configurer pour un déploiement de la passerelle SGD Gateway avec équilibrage de charge

Connexion	Tâches de configuration
Du périphérique client à l'équilibreur de charge	1. Activez les connexions entrantes provenant de périphériques client. En général, cette connexion utilise le port TCP 443. Pour plus d'informations sur la procédure à suivre, reportez-vous à la documentation de votre équilibreur de charge.

Connexion	Tâches de configuration
	2. (Facultatif) Sur l'équilibreur de charge, installez le certificat SSL que les passerelles SGD utilisent pour les connexions client. Pour plus d'informations sur la procédure à suivre, reportez-vous à la documentation de votre équilibreur de charge.
De l'équilibreur de charge à la passerelle SGD Gateway	1. Configurez votre équilibreur de charge pour transférer des connexions à la passerelle SGD Gateway. Pour plus d'informations sur la procédure à suivre, reportez-vous à la documentation de votre équilibreur de charge. 2. Configurez les ports et les connexions utilisés par la passerelle SGD Gateway. Spécifiez l'adresse de l'équilibreur de charge comme point d'entrée du réseau. Vous avez configuré ces paramètres lors de l'installation de la passerelle. Reportez-vous à la section Section 2.2.1.1, « Procédure de configuration des ports et des connexions à la passerelle SGD Gateway » si vous souhaitez changer la configuration de la passerelle SGD Gateway. 3. Sur chaque passerelle SGD Gateway, installez un certificat SSL des connexions client. Reportez-vous à la section Section 2.2.1.2, « Procédure d'installation d'un certificat SSL pour les connexions client dans le keystore du client ».
De la passerelle SGD Gateway aux serveurs SGD	1. Activez les services de sécurité SGD pour le groupe SGD. Les serveurs SGD doivent s'exécuter en mode sécurisé. Le transfert via pare-feu ne doit pas être activé. Dans une installation classique, un serveur SGD est configuré automatiquement pour utiliser les connexions sécurisées. Reportez-vous à la section "Connexions sécurisées aux serveurs SGD" du chapitre 1 du *Oracle Secure Global Desktop Administration Guide for Release 4.7* pour plus d'informations sur la manière de sécuriser un serveur SGD. 2. Sur la passerelle SGD Gateway, installez les certificats de sécurité des serveurs SGD. Utilisez la commande `gateway server` pour importer les certificats CA et les certificats SSL des serveurs SGD dans le groupe dans le keystore de la passerelle SGD Gateway. Reportez-vous à la section Section 2.2.2.1, « Procédure d'installation des certificats de serveur SGD ».

Connexion	Tâches de configuration
	3. Configurez les serveurs SGD du groupe de sorte qu'ils utilisent les passerelles SGD Gateway. Installez les certificats SGD Gateway dans le groupe SGD et utilisez la commande `tarantella gateway add` pour enregistrer les passerelles SGD Gateway auprès du groupe SGD. Reportez-vous à la section Section 2.2.2.2, « Procédure d'installation des certificats SGD Gateway dans le groupe SGD ». 4. Configurez les connexions client SGD que les passerelles SGD Gateway peuvent utiliser. Reportez-vous à la section Section 2.2.2.3, « Procédure de configuration des connexions client SGD ».

2.2. Tâches de configuration de SGD Gateway

Cette section inclut des instructions permettant de configurer les connections utilisées par la passerelle SGD Gateway.

Les tâches de configuration suivantes sont décrites :

- Section 2.2.1, « Connexions entre le périphérique client et la passerelle SGD Gateway »
- Section 2.2.2, « Connexions entre la passerelle SGD Gateway et le serveur SGD »
- Section 2.2.3, « Connexions entre le périphérique client et l'équilibreur de charge »
- Section 2.2.4, « Connexions entre l'équilibreur de charge et la passerelle SGD Gateway »

2.2.1. Connexions entre le périphérique client et la passerelle SGD Gateway

La configuration des connexions entre le périphérique client et une passerelle SGD Gateway suppose d'effectuer les tâches de configuration suivantes :

1. (Facultatif) Configurez les ports et les connexions utilisés par la passerelle SGD Gateway.

   Vous avez configuré ces paramètres lors de l'installation de la passerelle.

   Pour modifier ces paramètres, reportez-vous à la section Section 2.2.1.1, « Procédure de configuration des ports et des connexions à la passerelle SGD Gateway ».

2. (Facultatif) Sur la passerelle SGD Gateway, installez un certificat SSL pour les connexions client.

   Reportez-vous à la section Section 2.2.1.2, « Procédure d'installation d'un certificat SSL pour les connexions client dans le keystore du client ».

2.2.1.1. Procédure de configuration des ports et des connexions à la passerelle SGD Gateway

Vous pouvez conserver cette procédure si vous souhaitez modifier les paramètres spécifiés lors de l'installation de la passerelle SGD Gateway.

1. Connectez-vous à l'hôte en tant que superutilisateur (utilisateur root) à l'hôte SGD Gateway.

2. Exécutez la commande `gateway config create`.

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

   Répondez aux questions qui s'affichent pour configurer les éléments suivants :

   - **Paramètres de port SGD Gateway.** Interface et port que la passerelle SGD Gateway utilise pour les connexions entrantes.
   - **Point d'entrée réseau.** Adresse IP, ou nom DNS, et port que les périphériques client utilisent pour se connecter à la passerelle SGD Gateway. Le point d'entrée ne correspond pas toujours à l'adresse de la passerelle SGD Gateway. Selon la configuration de votre réseau, il peut s'agir de l'adresse d'un équilibreur de charge ou d'un autre périphérique externe.
   - **Connexions sécurisées.** Indiquez s'il faut sécuriser les connexions entre la passerelle SGD Gateway et les serveurs SGD du groupe. Pour utiliser des connexions sécurisées, les serveurs SGD du groupe doivent s'exécuter en mode sécurisé.

3. Enregistrez les paramètres de connexion et de port.

   La passerelle SGD Gateway est alors configurée selon les paramètres spécifiés.

2.2.1.2. Procédure d'installation d'un certificat SSL pour les connexions client dans le keystore du client

Le certificat SSL que la passerelle SGD Gateway utilise pour les connexions client est appelé le certificat SSL SGD Gateway. Le certificat SSL est enregistré dans le keystore du client, `/opt/SUNWsgdg/proxy/etc/keystore.client`.

Par défaut, la passerelle SGD Gateway utilise un certificat SSL SGD Gateway *auto-signé* pour les connexions client. Vous pouvez toutefois remplacer le certificat SSL auto-signé par un certificat signé par une autorité de certification (AC).

La procédure suivante suppose que vous disposez d'un certificat SSL signé par une AC.

La clé privée que vous installez doit être au format PEM (Privacy Enhanced Mail).

1. Connectez-vous à l'hôte en tant que superutilisateur (utilisateur root) à l'hôte SGD Gateway.
2. Copiez le certificat SSL et la clé privée correspondante sur l'hôte SGD Gateway.
3. Importez le certificat SSL et la clé privée dans le keystore du client.

   Utilisez la commande `gateway sslkey import`, comme suit :

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

   Ici, le fichier de certificat *`example.com.pem`* et la clé privée codée RSA correspondante, *`temp.key`*, sont importées dans le keystore du client.

   Le certificat SSL auto-signé existant dans le keystore du client est écrasé.

4. (Facultatif) Redémarrez la passerelle SGD Gateway.

Attention

Appliquez cette étape uniquement si vous n'avez pas effectué de configuration initiale de la passerelle SGD Gateway. Le redémarrage de la passerelle SGD Gateway à ce stade de la configuration initiale entraîne l'affichage d'un message d'erreur, car la configuration initiale de la passerelle n'est pas finalisée.

Redémarrez la passerelle SGD Gateway si vous remplacez le certificat SSL sur une passerelle SGD Gateway qui est déjà configurée et en cours d'exécution.

Note

Le redémarrage de la passerelle SGD Gateway déconnecte toutes les sessions utilisateur et les sessions d'application qui s'exécutent via la passerelle SGD Gateway.

Sur l'hôte SGD Gateway, exécutez la commande suivante :

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

2.2.2. Connexions entre la passerelle SGD Gateway et le serveur SGD

Les connexions entre une passerelle SGD Gateway et les serveurs SGD du groupe sont basés sur des certificats qui leur permettent de s'octroyer des autorisations mutuelles. La définition de ces connexions suppose d'effectuer les tâches de configuration suivantes :

1. Installez les certificats de serveur SGD sur la passerelle SGD Gateway.

   Reportez-vous à la section Section 2.2.2.1, « Procédure d'installation des certificats de serveur SGD ».

2. Installez le certificat SGD Gateway dans le groupe SGD.

   Reportez-vous à la section Section 2.2.2.2, « Procédure d'installation des certificats SGD Gateway dans le groupe SGD ».

3. Configurez les connexions client SGD pour la passerelle SGD Gateway.

   Reportez-vous à la section Section 2.2.2.3, « Procédure de configuration des connexions client SGD ».

2.2.2.1. Procédure d'installation des certificats de serveur SGD

Pour utiliser cette procédure, les serveurs SGD du groupe doivent s'exécuter en mode sécurisé.

Dans une installation classique, un serveur SGD est configuré automatiquement pour utiliser les connexions sécurisées. Reportez-vous à la section "Connexions sécurisées aux serveurs SGD" du chapitre 1 du *Oracle Secure Global Desktop Administration Guide for Release 4.7* pour plus d'informations sur l'activation des services de sécurité sur un serveur SGD.

Répétez la procédure suivante pour chaque serveur SGD du groupe.

1. Connectez-vous à l'hôte en tant que superutilisateur (utilisateur root) à l'hôte SGD.

2. Copiez le certificat AC du serveur SGD dans le répertoire du keystore de la passerelle SGD Gateway.

   Le certificat AC d'un serveur SGD se trouve à l'emplacement `/opt/tarantella/var/info/certs/PeerCAcert.pem` sur l'hôte SGD.

Note

Il s'agit du même certificat AC que le serveur SGD utilise pour sécuriser les communications intragroupes.

Le répertoire du keystore de la passerelle SGD Gateway est le suivant : `/opt/SUNWsgdg/proxy/etc`.

Lorsque vous copiez le certificat AC, il est recommandé de renommer le fichier de certificat pour faciliter l'identification du contenu du fichier et du serveur SGD auquel il est associé.

3. Copiez le certificat SSL issu du serveur SGD dans le répertoire du keystore de la passerelle SGD Gateway.

   Le certificat SSL d'un serveur SGD qui s'exécute en mode sécurisé se trouve à l'emplacement `/opt/tarantella/var/tsp/cert.pem` sur l'hôte SGD.

   Le répertoire du keystore de la passerelle SGD Gateway est le suivant : `/opt/SUNWsgdg/proxy/etc`.

   Lorsque vous copiez le certificat SSL, il est recommandé de renommer le fichier de certificat pour faciliter l'identification du contenu du fichier et du serveur SGD auquel il est associé.

4. Connectez-vous à l'hôte en tant que superutilisateur (utilisateur root) à l'hôte SGD Gateway.

5. Importez les certificats dans le keystore de la passerelle SGD Gateway.

```
# /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
```

   L'option `--server` définit les noms utilisés lors du stockage des certificats dans le keystore. Dans cet exemple, le certificat AC est stocké sous l'alias *`sgd-server1`* et le certificat SSL sous l'alias *`sgd-server1-ssl`*.

   `https://sgd1.example.com` est l'URL du serveur Web SGD.

6. Redémarrez la passerelle SGD Gateway.

Note

Le redémarrage de la passerelle SGD Gateway déconnecte toutes les sessions utilisateur et les sessions d'application qui s'exécutent via la passerelle SGD Gateway.

   Sur l'hôte SGD Gateway, exécutez la commande suivante :

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

2.2.2.2. Procédure d'installation des certificats SGD Gateway dans le groupe SGD

Répétez la procédure suivante pour chaque passerelle SGD Gateway.

1. Exportez le certificat SGD Gateway.

   a. Connectez-vous à l'hôte en tant que superutilisateur (utilisateur root) à l'hôte SGD Gateway.

   b. Exportez le certificat SGD Gateway du keystore de la passerelle SGD Gateway.

Utilisez la commande `gateway cert export` comme suit :

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

Le certificat est exporté dans le fichier *`gateway1.pem`*.

c. Copiez le certificat dans le répertoire `/opt/tarantella/var/tsp` du serveur SGD principal du groupe.

Lorsque vous exportez le certificat, il est recommandé de nommer le fichier de certificat de sorte à faciliter l'identification de la passerelle SGD Gateway dont il est issu.

d. Modifiez les autorisations de fichier et la propriété du certificat de la passerelle.

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

2. Enregistrez la passerelle SGD Gateway auprès du groupe SGD.

a. Sur le serveur SGD principal, connectez-vous en tant que superutilisateur (utilisateur root).

b. Importez le certificat SGD Gateway.

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

`sgd-gateway1` correspondant au nom utilisé par SGD pour identifier la passerelle SGD Gateway et *`gateway1.pem`* le nom du fichier de certificat SGD Gateway.

Pour enregistrer plusieurs passerelles SGD Gateway en même temps, utilisez l'option `--file` de la commande `tarantella gateway add`. Reportez-vous à la section Section B.27, « La commande tarantella gateway » pour plus d'informations.

Les modifications apportées à la configuration à l'aide de la commande `tarantella gateway add` sont répliquées sur les autres serveurs SGD du groupe.

2.2.2.3. Procédure de configuration des connexions client SGD

1. Configurez les connexions client SGD qui utilisent la passerelle SGD Gateway.

Sur le serveur SGD principal, définissez l'attribut global `--security-gateway` pour spécifier les clients SGD qui peuvent utiliser la passerelle SGD Gateway, en fonction de leur adresse IP ou nom DNS.

Pour indiquer que toutes les connexions client SGD doivent être acheminées via le port TCP 443 d'une passerelle SGD Gateway `gateway1.example.com`, utilisez la commande suivante :

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

Pour indiquer que toutes les connexions client SGD doivent être acheminées via le port TCP 443 d'un équilibreur de charge externe, `lb.example.com`, utilisez la commande suivante :

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

Note

Les modifications apportées à l'attribut `--security-gateway` s'appliquent à tous les serveurs SGD du groupe. Les modifications s'appliquent uniquement aux nouvelles sessions utilisateur.

Reportez-vous à la section Section B.31, « L'attribut --security-gateway » pour plus d'informations sur l'utilisation de l'attribut `--security-gateway` afin de définir plusieurs filtres de connexion client SGD.

2.2.3. Connexions entre le périphérique client et l'équilibreur de charge

La configuration des connexions entre le périphérique client et un équilibreur de charge suppose d'effectuer les tâches de configuration suivantes :

1. Configurez l'équilibrage de charge de sorte qu'il accepte les connexions provenant des périphériques client.

   Pour plus d'informations sur la procédure à suivre, reportez-vous à la documentation de votre équilibreur de charge.

2. (Facultatif) Installez le certificat SSL de la passerelle SGD Gateway sur l'équilibreur de charge.

   Pour plus d'informations sur la procédure à suivre, reportez-vous à la documentation de votre équilibreur de charge.

2.2.4. Connexions entre l'équilibreur de charge et la passerelle SGD Gateway

La configuration des connexions entre un équilibreur de charge et la passerelle SGD Gateway suppose d'effectuer les tâches de configuration suivantes :

1. Configurez les ports et les connexions utilisés par la passerelle SGD Gateway.

   Reportez-vous à la section Section 2.2.1.1, « Procédure de configuration des ports et des connexions à la passerelle SGD Gateway ».

2. (Facultatif) Sur la passerelle SGD Gateway, installez un certificat SSL pour les connexions client entrantes.

   Reportez-vous à la section Section 2.2.1.2, « Procédure d'installation d'un certificat SSL pour les connexions client dans le keystore du client ».

2.3. Contrôle de la passerelle SGD Gateway

Cette section décrit comment contrôler la passerelle SGD Gateway. Les tâches suivantes sont décrites :

- Démarrage de la passerelle SGD Gateway
- Arrêt de la passerelle SGD Gateway
- Redémarrage de la passerelle SGD Gateway

2.3.1. Démarrage de la passerelle SGD Gateway

Pour démarrer la passerelle SGD Gateway, utilisez la commande suivante :

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

2.3.2. Arrêt de la passerelle SGD Gateway

Attention

L'arrêt de la passerelle SGD Gateway déconnecte toutes les sessions utilisateur et les sessions d'application qui s'exécutent via la passerelle. Cela signifie que des données d'application peuvent être perdues si la passerelle SGD Gateway est arrêtée de manière inattendue.

Pour arrêter la passerelle SGD Gateway, utilisez la commande suivante :

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

Quand vous utilisez la commande `gateway stop`, un message d'avertissement s'affiche, vous demandant de confirmer que vous souhaitez l'arrêt de la passerelle SGD Gateway. Utilisez l'option `--force` de la commande `gateway stop` si vous ne souhaitez pas que ce message s'affiche.

Note

En cas d'arrêt de la passerelle SGD Gateway, les utilisateurs qui se trouvent hors du réseau ne peuvent pas se connecter à SGD via la passerelle SGD Gateway. Les périphériques client qui ont été activés à l'aide de l'attribut `--security-gateway` pour accéder directement à SGD sans passer par la passerelle SGD Gateway, peuvent toujours accéder à SGD. Reportez-vous à la section Section B.31, « L'attribut --security-gateway ».

2.3.3. Redémarrage de la passerelle SGD Gateway

Attention

Le redémarrage de la passerelle SGD Gateway déconnecte toutes les sessions utilisateur et les sessions d'application qui s'exécutent via la passerelle SGD Gateway. Cela signifie que des données d'application peuvent être perdues si la passerelle SGD Gateway est redémarrée de manière inattendue.

Pour redémarrer la passerelle SGD Gateway, utilisez la commande suivante :

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

Quand vous utilisez la commande `gateway restart`, un message d'avertissement s'affiche, vous demandant de confirmer que vous souhaitez l'arrêt de la passerelle SGD Gateway. Utilisez l'option `--force` de la commande `gateway restart` si vous ne souhaitez pas que ce message s'affiche.

2.4. Retrait de la passerelle SGD Gateway

Pour retirer la passerelle SGD Gateway, il vous faut retirer le logiciel installé sur l'hôte SGD Gateway.

2.4.1. Procédure de retrait de SGD Gateway

1. Connectez-vous à l'hôte en tant que superutilisateur (utilisateur root) à l'hôte SGD Gateway.
2. Modifiez la configuration de routage des clients SGD du groupe SGD.
   a. Connectez-vous au serveur SGD principal en tant que superutilisateur (utilisateur root).
   b. Modifiez l'attribut `--security-gateway` du groupe SGD.

Dans un déploiement classique basé sur une seule passerelle SGD Gateway, exécutez la commande suivante :

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

Note

Dans le cas d'un déploiement avec équilibrage de charge basé sur plusieurs passerelles SGD Gateway et sur un équilibreur de charge, vous ne pouvez pas modifier l'attribut `--security gateway`.

3. Désinstallez la passerelle SGD Gateway.

   Exécutez la commande suivante :

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

   Un message d'avertissement apparaît, vous invitant à confirmer l'arrêt de la passerelle SGD Gateway.

Attention

La commande `gateway uninstall` est la seule méthode prise en charge pour retirer la passerelle SGD Gateway. N'utilisez pas les commandes `pkgrm` et `rpm` directement pour retirer la passerelle SGD Gateway.

4. (Facultatif) Retirez la passerelle SGD Gateway de la liste des passerelles SGD Gateway enregistrées pour le groupe SGD.

   a. Affichez les passerelles SGD Gateway SGD enregistrées pour le groupe SGD.

   ```
   # 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. Retirez la passerelle SGD Gateway de la liste des passerelles SGD Gateway enregistrées pour le groupe SGD.

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

Annexe A. Présentation de l'architecture de SGD Gateway

Ce chapitre décrit l'architecture et les principaux composants de Oracle Secure Global Desktop Gateway (SGD Gateway).

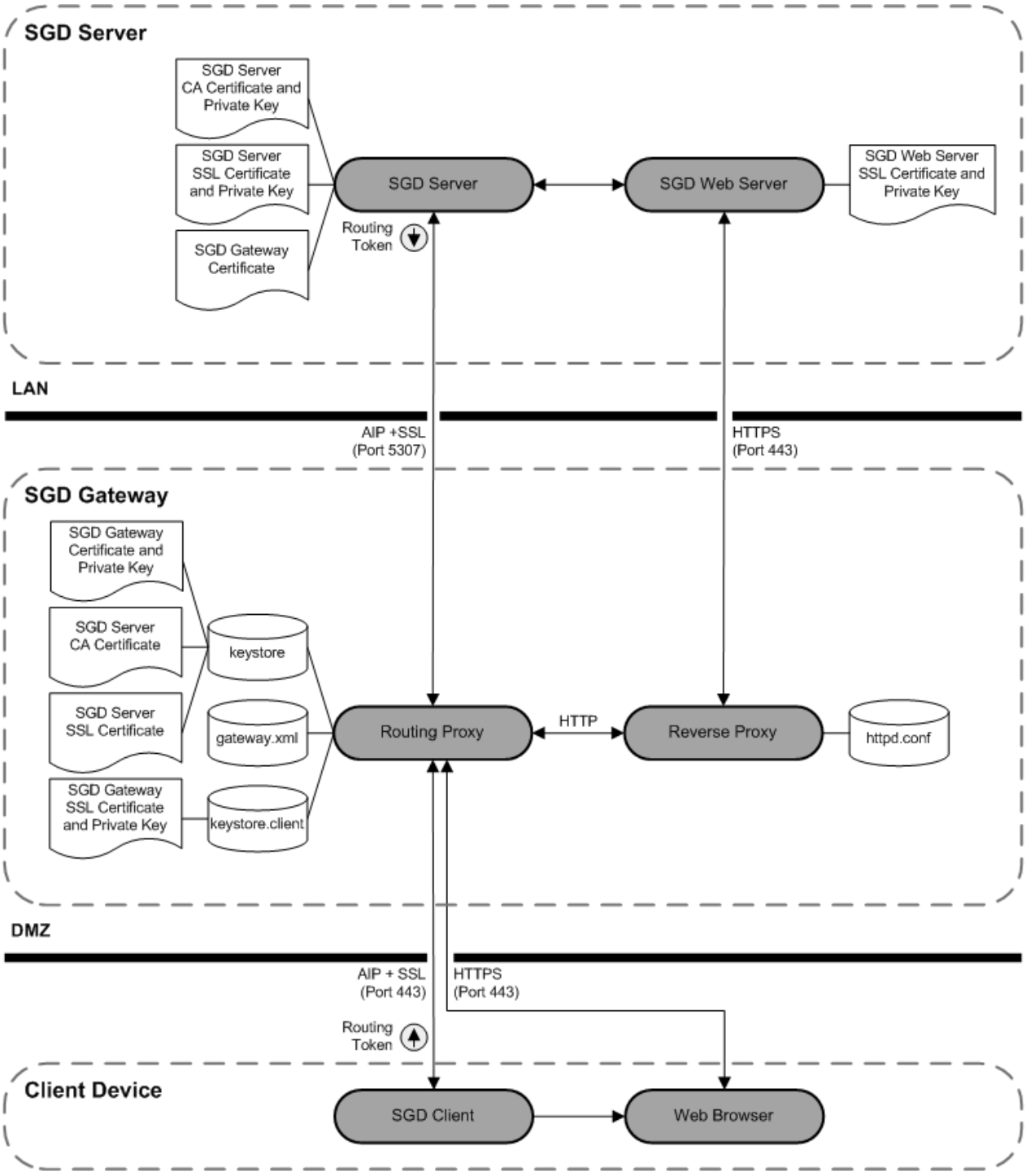
Ce chapitre comprend les rubriques suivantes :

A.1. Architecture de SGD Gateway

Cette section aborde l'architecture de SGD Gateway et comprend une description des connexions établies lorsque vous accédez à SGD via la passerelle SGD Gateway.

La Figure A.1, « Architecture de SGD Gateway » présente l'architecture de la passerelle SGD Gateway.

Figure A.1. Architecture de SGD Gateway



La procédure suivante décrit les connexions établies lorsque vous accédez à SGD via la passerelle SGD Gateway. Les étapes couvertes vont de la connexion initiale à SGD depuis un navigateur, la connexion à SGD, jusqu'au démarrage d'une application.

1. Le navigateur du périphérique client opère une connexion HTTPS (HTTP over Secure Sockets Layer) à la passerelle SGD Gateway sur le port TCP 443.

- Dans le cas d'un déploiement classique, les utilisateurs peuvent accéder à SGD en saisissant l'URL de la passerelle SGD Gateway.
- Le port TCP 443 est le port par défaut de la passerelle SGD Gateway. Les ports utilisés par la passerelle SGD Gateway sont définis dans le fichier de configuration du proxy de routage, `gateway.xml`. Ce fichier est créé automatiquement lors de l'installation de la passerelle SGD Gateway. Il est mis à jour lorsque la commande `gateway config` est utilisée pour modifier la configuration de la passerelle SGD Gateway.
- La passerelle SGD Gateway présente une certificat SSL. Ce certificat est la seule entrée contenue dans le keystore `keystore.client` stocké sur la passerelle SGD Gateway.
- L'emplacement et les mots de passes des keystores utilisés par la passerelle SGD Gateway sont définis dans le fichier de configuration du proxy de routage, `gateway.xml`.

2. Le proxy de routage reconnaît une connexion HTTPS, déchiffre le flux de données et transfère les données HTTP sur le proxy inverse Apache.
   - Les données HTTP sont envoyées en interne sur le premier port disponible au delà du port TCP 8080.
   - La configuration du proxy inverse Apache est définie par le fichier `httpd.conf`. Ce fichier et les fichiers de configuration du proxy inverse associés sont créés automatiquement lors de l'installation de la passerelle SGD Gateway. Les fichiers sont mis à jour lorsque la commande `gateway config` est utilisée pour modifier la configuration de la passerelle SGD Gateway.
3. Le proxy inverse se base sur l'équilibrage de charge HTTP pour sélectionner un serveur Web SGD dans le groupe de serveurs.
   - Les connexions entre le proxy inverse et le serveur Web SGD sont sécurisées via HTTPS sur le port TCP 443.
   - Le proxy inverse Apache définit un cookie d'équilibrage de charge dans le navigateur. Par la suite, toutes les demandes HTTP envoyées par le navigateur utiliseront ce serveur Web.
4. Le serveur Web SGD fournit du contenu HTML au navigateur Web sur le périphérique client.
   - Le contenu HTML est envoyé sous forme de données HTTPS sur la connexion établie au port TCP 443 sur la passerelle SGD Gateway.
   - La passerelle SGD Gateway transfère les données HTTPS au navigateur.
5. L'utilisateur se connecte à SGD.
   - Le serveur SGD authentifie l'utilisateur, sélectionne un serveur SGD pour gérer la session utilisateur et démarre une nouvelle session.
   - Le client SGD est téléchargé, installé et démarré sur le périphérique client.
   - Un jeton de routage est inclus dans le contenu HTML envoyé au navigateur Web. Le jeton de routage contient l'adresse du serveur SGD sélectionné pour gérer la session utilisateur. Ces informations sont utilisées pour acheminer les données AIP (Adaptive Internet Protocol) vers le bon serveur SGD.
   - Le jeton de routage est signé à l'aide de la clé privée du serveur SGD. Il est ensuite chiffré à l'aide du certificat SGD Gateway sur le serveur SGD.

- Le jeton de routage est transmis au client SGD.
- Les connexions au périphérique client sont basées sur le protocole HTTPS.

6. Le client SGD se connecte à la passerelle SGD Gateway sur le port TCP 443.
   - La connexion de données entre le client SGD et la passerelle SGD Gateway est basée sur le protocole AIP sur SSL (Secure Sockets Layer).
   - Le certificat SSL de la passerelle SGD Gateway est présentée pour établir la connexion.
   - Le proxy de routage reconnaît les données AIP sur SSL entrantes.
   - Le flux de données SSL est déchiffré et le jeton de routage est extrait du flux de données AIP.
   - Le jeton de routage est déchiffré avec la clé privée de SGD Gateway, puis vérifié à l'aide du certificat AC du serveur SGD.
   - La clé privée de la passerelle SGD Gateway et le certificat AC du serveur SGD sont stockés dans le keystore SGD Gateway, `keystore`.
   - L'horodatage du jeton de routage fait l'objet d'une vérification ayant pour but de confirmer sa validité.
   - Le flux de données AIP est rechiffré à l'aide du protocole SSL.
7. Les données AIP sur SSL sont acheminées via le proxy de routage vers le serveur SGD indiqué par le jeton de routage.
   - La connexion de données AIP sur SSL utilise le port TCP 5307.
   - Le jeton de routage AIP n'est pas inclus dans le flux de données AIP.
8. L'utilisateur démarre une application sur le bureau Web de SGD.
   - La demande de lancement d'application est envoyée à la passerelle SGD Gateway via le protocole HTTPS.
   - Le proxy de routage reconnaît et déchiffre les données HTTPS et transfère le trafic HTTP au proxy inverse Apache.
   - Le proxy de routage détecte le cookie d'équilibrage de charge et utilise le serveur Web SGD indiqué par le cookie.
   - L'équilibrage de charge des sessions de l'application SGD sélectionne le même serveur SGD pour gérer la session d'application.
   - Un nouveau jeton de routage est créé sur le serveur SGD. Le jeton de routage est utilisé pour acheminer les données AIP vers le serveur SGD sélectionné pour gérer la session d'application.
   - Le serveur SGD envoie le jeton de routage au client SGD. Le jeton de routage est inclus avec le flux de données AIP existant.
9. Le client SGD se connecte à la passerelle SGD Gateway sur le port TCP 443.
   - Le certificat SSL de la passerelle SGD Gateway est présentée pour établir la connexion.
   - Le proxy de routage reconnaît les données AIP sur SSL entrantes.

- Le jeton de routage est déchiffré, vérifié et validé.
- Les données AIP sur SSL sont acheminées via le proxy de routage vers le serveur SGD indiqué par le jeton de routage.
- Le jeton de routage AIP n'est pas inclus dans le flux de données AIP.

10. Le serveur SGD gère la session d'application.
    - L'application exécute un serveur d'applications situé sur le réseau local.

A.2. Composants de la passerelle SGD Gateway

La passerelle SGD Gateway comporte les composants suivants :

- **Proxy de routage**. Une application basée sur Java qui achemine les connexions de données AIP vers un serveur SGD.

  Les composants principaux du proxy de routage sont les suivants :

  - Jetons de routage : reportez-vous à la Section A.2.1, « A propos des jetons de routage »
  - Keystores : reportez-vous à la Section A.2.2, « Keystores utilisés par la passerelle SGD Gateway »
  - Fichier de configuration de proxy de routage : reportez-vous à la section Section A.2.3, « Fichier de configuration de proxy de routage »

- **Proxy inverse.** Serveur Web Apache configuré pour fonctionner en mode proxy inverse. Le proxy inverse effectue également l'équilibrage de charge des connexions HTTP.

  Les principaux composants du proxy inverse sont les suivants :

  - Fichiers de configuration du serveur Web Apache : reportez-vous à la Section A.2.4, « Fichiers de configuration du serveur Web Apache »
  - Modules Apache pour les opérations de proxy inverse et d'équilibrage de charge HTTP : reportez-vous à la Section A.2.5, « Modules Apache utilisés par la passerelle SGD Gateway »

A.2.1. A propos des jetons de routage

La passerelle SGD Gateway utilise un *jeton de routage* pour gérer une connexion AIP. Un jeton de routage est un message chiffré et signé qui permet d'identifier les serveurs SGD d'origine et de destination pour une route. Le jeton de routage inclut un horodatage, lequel permettra de limiter la durée de vie du jeton.

Les jetons de routage sortants subissent les opérations suivantes :

- Signature sur le serveur SGD à l'aide de la clé privée du serveur SGD.
- Chiffrement sur le serveur SGD à l'aide du certificat SGD Gateway.
- Envoi au client SGD sur le périphérique client.

Les jetons de routage entrants subissent les opérations suivantes :

- Déchiffrement sur la passerelle SGD Gateway à l'aide de la clé privée de la passerelle.
- Vérification sur la passerelle SGD Gateway à l'aide du certificat AC du serveur SGD d'origine.

- Suppression sur la passerelle SGD Gateway. La connexion présentant le jeton de routage est dirigée vers le serveur SGD de destination.

A.2.2. Keystores utilisés par la passerelle SGD Gateway

La passerelle SGD Gateway utilise des clés privées et des certificats pour signer et vérifier les jetons de routage, pour sécuriser les connexions aux serveurs SGD du groupe, pour sécuriser les connexions client à la passerelle SGD Gateway, et pour autoriser l'accès au service de réflexion.

Les certificats et les clés privées utilisés par la passerelle SGD Gateway sont stockés dans des keystores situés dans le répertoire `/opt/SUNWsgdg/proxy/etc`.

Ce répertoire contient les keystores suivants :

- **Keystore de la passerelle SGD Gateway.** Le keystore de la passerelle SGD Gateway, `keystore`, contient le certificat et la clé privée de la passerelle SGD Gateway, les certificats AC des serveurs SGD du groupe et les certificats SSL du serveur SGD permettant de sécuriser les connexions aux serveurs SGD du groupe.

  Pour ajouter, retirer et répertorier les entrées du keystore de la passerelle SGD Gateway, utilisez la commande `gateway`.

- **Keystore du client.** Le keystore du client, `keystore.client`, contient un seul certificat SSL de la passerelle SGD Gateway et la clé privée utilisée pour sécuriser les connexions entre le périphérique client et la passerelle SGD Gateway. Par défaut, ce keystore contient un certificat auto-signé. Vous pouvez remplacer ce certificat par un certificat signé par une autorité de certification.

- **Keystore du service de réflexion.** Le keystore du service de réflexion, `keystore.reflection`, contient un certificat et une clé privée utilisés pour autoriser l'accès au service de réflexion sur la passerelle SGD Gateway. Par défaut, ce keystore contient un certificat auto-signé et une clé privée.

Les keystores sont créés automatiquement lors de l'exécution de la commande `gateway setup` après avoir installé la passerelle SGD Gateway.

Note

Tous les keystores utilisent le même mot de passe, lequel est défini dans le fichier `/opt/SUNWsgdg/etc/password`. Le mot de passe est un mot de passe aléatoire créé automatiquement lors de la création initiale des keystores. Le fichier de mot de passe peut uniquement être lu par un superutilisateur (utilisateur root).

A.2.3. Fichier de configuration de proxy de routage

Le fichier de configuration du proxy de routage est le suivant : `/opt/SUNWsgdg/etc/gateway.xml`. Il s'agit d'un fichier XML qui permet de configurer les routes, en fonction du type de protocole des données. Le fichier configure également les emplacements de keystore et les mots de passe nécessaires pour le routage et les protocoles SSL.

Le fichier de configuration du proxy de routage est créé automatiquement lorsque vous installez la passerelle SGD Gateway. Il est mis à jour lorsque vous utilisez la commande `gateway config` pour modifier le fichier de configuration de la passerelle SGD Gateway.

Attention

Utilisez les commandes `gateway config` pour configurer la passerelle.
Si possible, évitez de modifier le fichier `gateway.xml` de façon manuelle.

Toute configuration incorrecte du fichier `gateway.xml` peut entraîner un dysfonctionnement de la passerelle SGD Gateway.

Le fichier de configuration du proxy de routage par défaut utilise le mot de passe indiqué dans le fichier `/opt/SUNWsgdg/etc/password` pour accéder aux keystores utilisés par la passerelle SGD Gateway. Si vous ne souhaitez pas enregistrer ce mot de passe sur disque, prenez note de la valeur du mot de passe. Ensuite, supprimez le fichier de mot de passe, ainsi que les entrées `password` de tous les éléments `<keystore>` figurant dans le fichier `gateway.xml`. Au prochain démarrage de la passerelle SGD Gateway, vous devrez donc saisir le mot de passe du keystore.

Pour modifier le mot de passe d'un keystore utilisé par la passerelle SGD Gateway, utilisez l'option `-storepasswd` de la commande `keytool`. Par exemple, pour modifier le mot de passe du keystore `keystore.client`, exécutez la commande suivante :

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

Reportez-vous à la documentation relative aux outils et utilitaires JDK pour plus d'informations sur le fonctionnement de l'application `keytool`.

Note

Le répertoire `/opt/SUNWsgdg/etc` contient également des fichiers de type `.xml` et `.template`. Ces fichiers sont utilisés en interne par la commande `gateway config` pour mettre à jour le fichier `gateway.xml`. Il est fortement déconseillé de modifier ces fichiers manuellement.

A.2.4. Fichiers de configuration du serveur Web Apache

Les fichiers de configuration pour le serveur Web Apache configurés pour être utilisés avec la passerelle SGD Gateway se trouvent dans le répertoire `/opt/SUNWsgdg/httpd/`*`apache-version`*`/conf`.

Les fichiers de configuration situés dans ce répertoire permettent de configurer le fonctionnement du proxy inverse et l'équilibrage de charge pour le serveur Web Apache.

A.2.4.1. Configuration du fonctionnement du proxy inverse et de l'équilibrage de charge

Les fichiers permettant de configurer le fonctionnement du proxy inverse et l'équilibrage de charge sont situés dans le sous-répertoire `extra/gateway`. Ces fichiers sont activés par la directive `Include` suivante dans le fichier `httpd.conf` :

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

Le fichier `httpd-gateway.conf` configure le fonctionnement du proxy inverse et l'équilibrage de charge pour le serveur Web Apache. Les membres du groupe d'équilibrage de charge sont définis à l'aide d'une directive `Include` indiquée dans le fichier `httpd-gateway.conf`, comme suit :

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

Le répertoire `extra/gateway/servers` contient des fichiers de configuration pour chacun des serveurs Web SGD du groupe d'équilibrage de charge. Les fichiers de configuration sont nommés *`server-name`*`.conf`, *`server-name`* correspondant au nom de serveur utilisé dans la commande `gateway server add`. Reportez-vous à la Section B.12, « gateway server add » pour plus d'infos sur cette commande.

La passerelle SGD Gateway utilise un équilibrage de charge HTTP de type *session persistante*. Cela signifie que le proxy inverse Apache définit un cookie dans le navigateur du client qui permettra de rediriger systématiquement le navigateur vers le serveur Web SGD qui a été choisi par l'équilibrage de charge. Le cookie expire à la fin de la session utilisateur.

Les cookies des sessions persistantes sont activés par la directive `Header add Set-Cookie` indiquée dans le fichier `httpd-gateway.conf`, comme suit :

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

`BALANCEID` correspondant au nom du cookie, et `BALANCER_WORKER_ROUTE` et `BALANCER_ROUTE_CHANGED` à des variables d'environnement exportées par le module `mod_proxy_balancer` d'Apache. Reportez-vous à la documentation relative au module mod_proxy_balancer d'Apache pour plus d'informations sur ces variables d'environnement.

A.2.5. Modules Apache utilisés par la passerelle SGD Gateway

Le serveur Web Apache fourni avec la passerelle SGD Gateway utilise les modules Apache standard pour les opérations de proxy inverse et d'équilibrage de charge. Les modules sont installés en tant que modules DSO (Dynamic Shared Object).

Les modules sont activés par les directives `LoadModule` du fichier de configuration Apache `httpd.conf`, à l'adresse `/opt/SUNWsgdg/httpd/`*`apache-version`*`/conf/httpd.conf`.

Annexe B. Référence de ligne de commande

Ce chapitre décrit comment gérer, contrôler et modifier la configuration de la passerelle SGD Gateway (SGD Gateway) à partir de la ligne de commande.

Les commandes fournies permettent d'effectuer des tâches telles que la configuration des keystores et des certificats, la définition des ports utilisés par la passerelle SGD Gateway et la configuration de l'équilibrage de charge pour les serveurs SGD du groupe.

Ce chapitre comprend les rubriques suivantes :

B.1. La commande gateway

La commande `gateway` permet de configurer et de contrôler la passerelle SGD Gateway.

Note

Le chemin d'accès complet de la commande `gateway` est `/opt/SUNWsgdg/bin/gateway`.

Syntaxe

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

Description

Les commandes `gateway` disponibles sont présentées dans le tableau suivant.

Commande	Description	Informations supplémentaires
`gateway start`	Démarre la passerelle SGD Gateway	Section B.22, « gateway start »
`gateway stop`	Arrête la passerelle SGD Gateway	Section B.24, « gateway stop »
`gateway restart`	Arrête puis redémarre la passerelle SGD Gateway	Section B.10, « gateway restart »
`gateway config`	Configure la passerelle SGD Gateway et met à jour les fichiers de configuration du proxy inverse Apache	Section B.3, « gateway config »
`gateway server`	Installe les certificats de sécurité de serveur SGD et configure l'équilibrage de charge pour le groupe SGD	Section B.11, « gateway server »
`gateway status`	Affiche l'état actuel de la passerelle SGD Gateway	Section B.23, « gateway status »
`gateway version`	Affiche le numéro de version de la passerelle SGD Gateway	Section B.26, « gateway version »

Commande	Description	Informations supplémentaires
`gateway sslcert`	Exporte et imprime le certificat SSL (Secure Sockets Layer) dans le keystore du client	Section B.16, « gateway sslcert »
`gateway sslkey`	Gère la clé privée et le certificat dans le keystore du client	Section B.19, « gateway sslkey »
`gateway cert export`	Exporte le certificat SGD Gateway du keystore de la passerelle SGD Gateway	Section B.2, « gateway cert export »
`gateway key import`	Importe une clé privée et un certificat dans le keystore de la passerelle SGD Gateway	Section B.9, « gateway key import »
`gateway setup`	Exécute le programme d'installation de SGD Gateway	Section B.15, « gateway setup »
`gateway uninstall`	Désinstalle le logiciel SGD Gateway	Section B.25, « gateway uninstall »

Note

Toutes les commandes `gateway` incluent une option `--help`. Vous pouvez utiliser cette option pour afficher l'aide relative à la commande.

Exemples

La ligne suivante permet de démarrer la passerelle SGD Gateway.

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

La ligne suivante signifie que le serveur SGD `server.example.com` ne sera pas autorisé à utiliser la passerelle SGD Gateway.

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

B.2. gateway cert export

Exporte le certificat SGD Gateway du keystore de la passerelle SGD Gateway

Syntaxe

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

Description

Exporte le certificat SGD Gateway du keystore de la passerelle SGD Gateway, à l'emplacement `/opt/SUNWsgdg/proxy/etc/keystore`. Le certificat est enregistré dans le fichier indiqué par l'option `--certfile`.

Pour accéder au keystore de la passerelle SGD Gateway, cette commande utilise le mot de passe figurant dans le fichier `/opt/SUNWsgdg/etc/password`. Si ce fichier n'est pas présent, la commande vous invite à saisir un mot de passe.

Exemples

La ligne suivante permet de récupérer le certificat SGD Gateway à partir du keystore de la passerelle SGD Gateway et de l'exporter dans le fichier `gateway1.pem`.

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

B.3. gateway config

Configure la passerelle SGD Gateway. La commande `gateway config` configure les connexions sécurisées, les ports et les paramètres du proxy inverse pour la passerelle SGD Gateway.

Syntaxe

```
gateway config create | show
```

Description

Le tableau suivant présente les sous-commandes disponibles pour cette commande.

Sous-commande	Description	Informations supplémentaires
`create`	Crée une configuration pour la passerelle SGD Gateway	Section B.4, « gateway config create »
`list`	Affiche la configuration actuelle de la passerelle SGD Gateway sous forme de liste	Section B.8, « gateway config list »
`edit`	Permet de modifier la configuration actuelle de la passerelle SGD Gateway	Section B.6, « gateway config edit »
`enable`	Active un service SGD Gateway	Section B.7, « gateway config enable »
`disable`	Désactive un service SGD Gateway	Section B.5, « gateway config disable »

Exemples

La ligne suivante permet d'afficher la configuration actuelle de la passerelle SGD Gateway sous forme de liste.

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

B.4. gateway config create

Crée une configuration pour la passerelle SGD Gateway, en écrasant la configuration actuelle.

Syntaxe

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

Description

Le tableau suivant présente les options disponibles pour cette commande.

Option	Description
`--interface`	Interface et port sur lesquels la passerelle SGD Gateway écoute les connexions proxy entrantes. La valeur par défaut est le port TCP 443, sur toutes les interfaces.

Option	Description
`--entry-point`	Point d'entrée du réseau. Il s'agit de l'adresse IP (Internet Protocol) et du port que les clients utilisent pour se connecter à la passerelle SGD Gateway. Vous pouvez indiquer une adresse DNS (Domain Name System) plutôt qu'une adresse IP.
`--out`	Format du trafic sortant issu de la passerelle SGD Gateway à destination des serveurs SGD du groupe. Si vous utilisez des connexions sécurisées, choisissez `ssl`.
`--file`	Spécifie un fichier contenant des paramètres de configuration.

Note

Si aucune option n'est spécifiée pour la commande `gateway config create`, une série d'invites en ligne s'affiche, vous permettant de saisir les paramètres requis.

Si vous utilisez l'option `--file` avec la commande `gateway config create`, le fichier spécifié doit présenter le même format que le fichier `/opt/SUNWsgdg/etc/gatewayconfig.xml`. Ce fichier est créé au cours de la première configuration de la passerelle SGD Gateway, comme spécifié à la Section 2.2.1.1, « Procédure de configuration des ports et des connexions à la passerelle SGD Gateway ».

Exemples

La ligne suivante permet de configurer une passerelle SGD Gateway pour écouter sur le port TCP 443 les connexions issues du point d'entrée du réseau, ici 192.168.0.1. Des connexions sécurisées sont utilisées entre la passerelle SGD Gateway et les serveurs SGD du groupe.

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

B.5. gateway config disable

Désactive un ou plusieurs des services SGD Gateway.

Syntaxe

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

Description

Les options de ligne de commande permettent de désactiver des services SGD Gateway spécifiques. Vous devez indiquer au moins une option de ligne de commande.

Note

Après avoir utilisé cette commande pour désactiver un service, vous devez redémarrer la passerelle SGD Gateway pour arrêter le service.

Le tableau suivant présente les options disponibles pour cette commande.

Option	Description
`--services-reflection`	Désactive l'accès non authentifié au service de réflexion de la passerelle SGD Gateway.

Option	Description
	Par défaut, ce service est désactivé. Reportez-vous à la Section C.9, « Service de réflexion » pour plus d'informations sur le service de réflexion de la passerelle SGD Gateway.
`--services-reflection-auth`	Désactive l'accès authentifié au service de réflexion de la passerelle SGD Gateway. Par défaut, ce service est désactivé. Reportez-vous à la Section C.9, « Service de réflexion » pour plus d'informations sur le service de réflexion de la passerelle SGD Gateway.
`--routes-http-redirect`	Désactive le service de redirection HTTP. Par défaut, ce service est désactivé.

Exemples

La ligne suivante permet de désactiver l'accès authentifié au service de réflexion de la passerelle SGD Gateway.

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

B.6. gateway config edit

Permet de modifier la configuration actuelle de la passerelle SGD Gateway.

Syntaxe

```
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 ]
```

Description

Les options de ligne de commande permettent de modifier des paramètres de configuration spécifiques. Vous devez indiquer au moins une option de ligne de commande.

La configuration actuelle de la passerelle SGD Gateway est stockée dans le fichier `/opt/SUNWsgdg/etc/gatewayconfig.xml`.

Vous devez redémarrer la passerelle pour que les modifications prennent effet.

Le tableau suivant présente les options disponibles pour cette commande.

Option	Description
`--binding`	Interface et port sur lesquels la passerelle SGD Gateway écoute les connexions proxy entrantes. La valeur par défaut est le port TCP 443, sur toutes les interfaces.

Option	Description
`--routes-http-maxcon`	Nombre maximum de connexions HTTP. La valeur par défaut est configurée au moment de l'installation et dépend des ressources mémoire disponibles sur la passerelle SGD Gateway. Reportez-vous à la Section C.1, « Réglage de la passerelle SGD Gateway ».
`--routes-aip-maxcon`	Nombre maximum de connexions AIP. La valeur par défaut est configurée au moment de l'installation et dépend des ressources mémoire disponibles sur la passerelle SGD Gateway. Reportez-vous à la Section C.1, « Réglage de la passerelle SGD Gateway ».
`--routes-reverseproxy-redirect`	Port de redirection HTTP. La valeur par défaut est le port TCP 8080.
`--services-reflection-binding`	Interface et port utilisés pour l'accès non authentifié au service de réflexion de la passerelle SGD Gateway. La valeur par défaut est le port TCP 81, sur l'interface localhost loopback.
`--services-reflection-auth-binding`	Interface et port utilisés pour l'accès authentifié au service de réflexion de la passerelle SGD Gateway. La valeur par défaut est le port TCP 82, sur toutes les interfaces.

Exemples

La ligne suivante permet de modifier le nombre maximum de connexions HTTP et AIP de la passerelle SGD Gateway.

```
# /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

Active un ou plusieurs services SGD Gateway.

Syntaxe

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

Description

Les options de ligne de commande permettent d'activer des services SGD Gateway spécifiques. Vous devez indiquer au moins une option de ligne de commande.

Note

Après avoir utilisé cette commande pour activer un service, vous devez redémarrer la passerelle SGD Gateway pour démarrer le service.

Le tableau suivant présente les options disponibles pour cette commande.

Option	Description
`--services-reflection`	Active l'accès non authentifié au service de réflexion de la passerelle SGD Gateway.

Option	Description
	Par défaut, ce service est désactivé. Reportez-vous à la Section C.9, « Service de réflexion » pour plus d'informations sur le service de réflexion de la passerelle SGD Gateway.
`--services-reflection-auth`	Active l'accès authentifié au service de réflexion de la passerelle SGD Gateway. Par défaut, ce service est désactivé. Reportez-vous à la Section C.9, « Service de réflexion » pour plus d'informations sur le service de réflexion de la passerelle SGD Gateway.
`--routes-http-redirect`	Active le service de redirection HTTP. Par défaut, ce service est désactivé.

Exemples

La ligne suivante permet d'activer l'accès authentifié au service de réflexion de la passerelle SGD Gateway.

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

B.8. gateway config list

Affiche la configuration actuelle de la passerelle SGD Gateway sous forme de liste.

Syntaxe

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

Description

Les options de ligne de commande permettent d'afficher des paramètres de configuration spécifiques sous forme de liste. Si aucune option n'est spécifiée, l'intégralité des informations relatives à la configuration de la passerelle SGD Gateway est affichée.

La configuration actuelle de la passerelle SGD Gateway est stockée dans le fichier `/opt/SUNWsgdg/etc/gatewayconfig.xml`.

Le tableau suivant présente les options disponibles pour cette commande.

Option	Description
`--binding`	Interface et port sur lesquels la passerelle SGD Gateway écoute les connexions proxy entrantes.
`--routes-http-maxcon`	Nombre maximum de connexions HTTP.

Option	Description
`--routes-aip-maxcon`	Nombre maximum de connexions AIP (Adaptive Internet Protocol).
`--routes-reverseproxy-redirect`	Port de redirection HTTP.
`--services-reflection-binding`	Interface et port utilisés pour l'accès non authentifié au service de réflexion de la passerelle SGD Gateway.
`--services-reflection-auth-binding`	Interface et port utilisés pour l'accès authentifié au service de réflexion de la passerelle SGD Gateway.

Exemples

La ligne suivante permet d'afficher la configuration d'authentification et le nombre maximum de connexions AIP de la passerelle SGD Gateway.

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

La ligne suivante permet d'afficher l'intégralité des informations relatives à la configuration de la passerelle SGD Gateway.

```
# /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

Importe une clé et un certificat SGD Gateway dans le keystore de la passerelle SGD Gateway.

Syntaxe

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

Description

Importe une clé privée, ainsi que le certificat de clé publique correspondant, dans le keystore de la passerelle SGD Gateway, à l'emplacement `/opt/SUNWsgdg/proxy/etc/keystore`.

Si le keystore possède déjà une entrée de clé SGD Gateway, celle-ci sera écrasée. Par défaut, une invite de confirmation s'affiche.

Pour accéder au keystore de la passerelle SGD Gateway, cette commande utilise le mot de passe figurant dans le fichier `/opt/SUNWsgdg/etc/password`. Si ce fichier n'est pas présent, la commande vous invite à saisir un mot de passe.

Le tableau suivant présente les options disponibles pour cette commande.

Option	Description
`--keyfile`	Fichier contenant la clé privée. La clé doit être au format PEM.
`--keyalg`	Algorithme de codage utilisé par la clé privée. Les options possibles sont RSA et DSA. Par défaut, l'option RSA est sélectionnée.
`--certfile`	Fichier de certificat SSL.
`--cacertfile`	Fichier de certificat AC ou racine.
`--alwaysoverwrite`	Ne pas demander confirmation avant d'écraser une entrée du keystore.

Pour importer une chaîne de certificat, utilisez l'option `--cacertfile` et spécifiez un certificat AC intermédiaire. Tous les certificats de la chaîne doivent être au format PEM.

Si une chaîne de certificat utilise plusieurs certificats AC, combinez tous les certificats AC de la chaîne dans un seul et même fichier. Le certificat AC utilisé pour signer le certificat de serveur *doit y figurer en premier*. Voici un exemple :

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

Exemples

La ligne suivante permet d'importer une clé privée codée RSA, `gateway1.key`, ainsi que le certificat de clé publique correspondant, `gateway1.pem`, dans le keystore de la passerelle SGD Gateway.

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

La ligne suivante permet d'importer une clé privée et une chaîne de certificats dans le keystore de la passerelle SGD Gateway. Le certificat AC intermédiaire est `gateway1-ca.pem`.

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

B.10. gateway restart

Arrête puis redémarre la passerelle SGD Gateway.

Syntaxe

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

Description

Arrête puis redémarre la passerelle SGD Gateway. Avant d'arrêter la passerelle SGD Gateway, le système demande confirmation à l'utilisateur.

L'option `--force` permet d'arrêter la passerelle SGD Gateway, sans qu'un message de confirmation s'affiche.

Exemples

La ligne suivante permet d'arrêter et de redémarrer la passerelle SGD Gateway avec un message de confirmation.

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

B.11. gateway server

Permet d'autoriser les serveurs SGD à utiliser la passerelle SGD Gateway.

Syntaxe

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

Description

Le tableau suivant présente les sous-commandes disponibles pour cette commande.

Sous-commande	Description	Informations supplémentaires
`add`	Autorise les serveurs SGD à utiliser la passerelle SGD Gateway	Section B.12, « gateway server add »
`remove`	Retire l'autorisation d'utiliser la passerelle SGD Gateway accordée aux serveurs SGD	Section B.14, « gateway server remove »
`list`	Permet d'afficher une liste des serveurs SGD autorisés à utiliser la passerelle SGD Gateway.	Section B.13, « gateway server list »

Exemples

La ligne suivante permet de retirer l'autorisation d'utiliser la passerelle SGD Gateway accordée au serveur `sgd.example.com`.

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

B.12. gateway server add

Permet d'autoriser un serveur SGD à utiliser la passerelle SGD Gateway.

Syntaxe

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

Description

Le tableau suivant présente les options disponibles pour cette commande.

Option	Description
`--server`	Nom DNS du serveur SGD
`--cert-file`	Certificat de l'autorité de certification (AC) du serveur SGD

Option	Description
`--url`	URL du serveur Web SGD
`--ssl-certfile`	Certificat SSL du serveur SGD

La commande `gateway server add` effectue les opérations suivantes :

- Importe le certificat AC du serveur SGD dans le keystore de la passerelle SGD Gateway, à l'emplacement `/opt/SUNWsgdg/proxy/etc/keystore`. Le certificat AC est stocké dans le keystore sous un alias identique au nom du serveur SGD spécifié par l'option `--server`.
- Importe le certificat SSL du serveur SGD dans le keystore de la passerelle SGD Gateway, à l'emplacement `/opt/SUNWsgdg/proxy/etc/keystore`. Le certificat SSL est enregistré dans le keystore à l'aide d'un alias composé du suffixe `-ssl` et du nom du serveur SGD spécifié par l'option `--server`.
- Ajoute le serveur SGD au groupe d'équilibrage de charge utilisé par le serveur de proxy inverse Apache

Note

Après avoir utilisé la commande `gateway server add`, vous devez redémarrer la passerelle SGD Gateway pour que les modifications prennent effet.

Exemples

La ligne suivante permet d'ajouter le certificat AC `PeerCAcert.pem` au keystore de la passerelle SGD Gateway à l'aide de l'alias `sgd.example.com`. Le certificat SSL `cert.pem` est également ajouté au keystore, avec l'alias `sgd.example.com-ssl`.

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

Dans cet exemple, l'URL du serveur Web SGD, `https://sgd.example.com`, est ajouté au groupe d'équilibrage de charge du proxy inverse et un fichier de configuration est créé à l'emplacement `/opt/SUNWsgdg/httpd/`*`apache-version`*`/conf/extra/gateway/servers/conf/sgd.example.com.conf`.

B.13. gateway server list

Affiche les informations relatives aux serveurs SGD autorisés à utiliser la passerelle SGD Gateway.

Syntaxe

```
gateway server list
```

Description

Cette commande permet d'afficher les informations de certificat et les URL des serveurs SGD autorisés à utiliser la passerelle SGD Gateway.

Exemples

La ligne suivante affiche les informations relatives aux serveurs SGD autorisés à utiliser la passerelle SGD Gateway.

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

B.14. gateway server remove

Retire l'autorisation d'utiliser la passerelle SGD Gateway accordée aux serveurs SGD.

Syntaxe

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

Description

Le certificat AC et le certificat SSL du serveur SGD sont retirés du keystore de la passerelle SGD Gateway.

Note

Après avoir utilisé la commande `gateway server remove`, vous devez redémarrer la passerelle SGD Gateway pour que les modifications prennent effet.

Exemples

Dans l'exemple suivant, l'autorisation d'utiliser la passerelle SGD Gateway accordée au serveur SGD `sgd.example.com` est retirée.

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

B.15. gateway setup

Exécute le programme d'installation de SGD Gateway;.

Syntaxe

```
gateway setup
```

Description

Répondez aux questions qui s'affichent pour configurer les ports, les interfaces et les paramètres de sécurité qui seront utilisés par la passerelle SGD Gateway.

Exemples

La ligne suivante permet d'exécuter le programme d'installation de SGD Gateway.

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

B.16. gateway sslcert

Permet d'imprimer ou d'exporter le certificat SSL de la passerelle SGD Gateway stocké dans le keystore du client.

Syntaxe

```
gateway sslcert export | print
```

Description

Le tableau suivant présente les sous-commandes disponibles pour cette commande.

Sous-commande	Description	Informations supplémentaires
`export`	Exporte le certificat SSL de la passerelle SGD Gateway à partir du keystore du client	Section B.17, « gateway sslcert export »
`print`	Imprime le certificat SSL de la passerelle SGD Gateway stocké dans le keystore du client	Section B.18, « gateway sslcert print »

Exemples

La ligne suivante permet d'imprimer le certificat SSL SGD Gateway stocké dans le keystore du client.

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

B.17. gateway sslcert export

Permet d'exporter le certificat SSL de la passerelle SGD Gateway à partir du keystore du client.

Syntaxe

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

Description

Permet d'exporter le certificat SSL de la passerelle SGD Gateway à partir du keystore du client, à l'emplacement `/opt/SUNWsgdg/proxy/etc/keystore.client`. Le certificat est enregistré dans le fichier indiqué par l'option `--certfile`.

Pour accéder au keystore du client, cette commande utilise le mot de passe spécifié dans le fichier `/opt/SUNWsgdg/etc/password`. Si ce fichier n'est pas présent, la commande vous invite à saisir un mot de passe.

Exemples

La ligne suivante permet de récupérer le certificat SSL de la passerelle SGD Gateway à partir du keystore du client et de l'exporter dans le fichier `gateway-ssl.pem`.

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

B.18. gateway sslcert print

Imprime le certificat SSL de la passerelle SGD Gateway.

Syntaxe

```
gateway sslcert print
```

Description

Imprime le certificat SSL de la passerelle SGD Gateway stocké dans le keystore du client, à l'emplacement `/opt/SUNWsgdg/proxy/etc/keystore.client`.

La commande affiche les informations du certificat dans la fenêtre de terminal.

Pour accéder au keystore du client, cette commande utilise le mot de passe spécifié dans le fichier `/opt/SUNWsgdg/etc/password`. Si ce fichier n'est pas présent, la commande vous invite à saisir un mot de passe.

Exemples

La ligne suivante permet d'imprimer le certificat SSL SGD Gateway stocké dans le keystore du client.

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

B.19. gateway sslkey

Permet de gérer les entrées de clé privée et de certificat SSL dans le keystore du client.

Syntaxe

```
gateway sslkey import | export
```

Description

Le tableau suivant présente les sous-commandes disponibles pour cette commande.

Sous-commande	Description	Informations supplémentaires
`import`	Importe une clé privée et un certificat dans le keystore du client	Section B.21, « gateway sslkey import »
`export`	Exporte une clé privée du keystore du client	Section B.20, « gateway sslkey export »

Exemples

La ligne suivante permet d'exporter le certificat SSL de la passerelle SGD Gateway stocké dans le keystore du client.

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

B.20. gateway sslkey export

Permet d'exporter la clé privée SSL de la passerelle SGD Gateway du keystore du client.

Syntaxe

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

Description

Permet d'exporter la clé privée SSL de la passerelle SGD Gateway à partir du keystore du client, à l'emplacement `/opt/SUNWsgdg/proxy/etc/keystore.client`. La clé privée est enregistrée dans le fichier spécifié par l'option `--keyfile`.

Il est possible de spécifier un mot de passe pour la clé privée à l'aide de l'option `--keypass`. Par défaut, le mot de passe spécifié dans le fichier `/opt/SUNWsgdg/etc/password` est utilisé.

Exemples

La ligne suivante permet de récupérer la clé privée SSL de la passerelle SGD Gateway à partir du keystore du client et de l'exporter dans le fichier `gateway-ssl.key`.

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

B.21. gateway sslkey import

Importe une clé et un certificat SSL dans le keystore du client.

Syntaxe

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

Description

Importe une clé privée SSL ainsi que le certificat SSL correspondant dans le keystore du client, plus précisément dans le fichier `/opt/SUNWsgdg/proxy/etc/keystore.client`. Par défaut, ce keystore contient un seul certificat auto-signé.

Si le keystore possède déjà une entrée, cette commande la remplacera par la nouvelle. Par défaut, un message s'affiche pour demander de confirmer le remplacement de l'entrée du keystore.

Pour accéder au keystore du client, cette commande utilise le mot de passe spécifié dans le fichier `/opt/SUNWsgdg/etc/password`. Si ce fichier n'est pas présent, la commande vous invite à saisir un mot de passe.

Le tableau suivant présente les options disponibles pour cette commande.

Option	Description
`--keyfile`	Fichier contenant la clé privée SSL. La clé doit être au format PEM (Privacy Enhanced Mail).
`--keyalg`	Algorithme de codage utilisé par la clé privée. Les options disponibles sont RSA et DSA (Digital Signature Algorithm). Par défaut, l'option RSA est sélectionnée.
`--certfile`	Fichier de certificat SSL.
`--cacertfile`	Fichier de certificat AC ou racine.
`--alwaysoverwrite`	Ne pas demander confirmation avant d'écraser l'entrée du keystore du client.

Pour importer une chaîne de certificat, utilisez l'option `--cacertfile` et spécifiez le certificat AC intermédiaire. Tous les certificats de la chaîne doivent être au format PEM.

Si une chaîne de certificat utilise plusieurs certificats AC, combinez tous les certificats AC de la chaîne dans un seul et même fichier. Le certificat AC utilisé pour signer le certificat de serveur *doit y figurer en premier*. Voici un exemple :

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

```
...CA root certificate...
-----END CERTIFICATE-----
```

Exemples

La ligne suivante permet d'importer une clé privée SSL codée RSA, `gateway1-ssl.key`, ainsi que le certificat SSL correspondant, `gateway1.pem`, dans le keystore du client.

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

La ligne suivante permet d'importer une clé privée SSL codée RSA et une chaîne de certificats SSL dans le keystore du client. Le certificat AC intermédiaire est `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

Démarre la passerelle SGD Gateway.

Syntaxe

```
gateway start
```

Description

Démarre la passerelle SGD Gateway.

Exemples

La ligne suivante permet de démarrer la passerelle SGD Gateway.

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

B.23. gateway status

Affiche l'état actuel de la passerelle SGD Gateway.

Syntaxe

```
gateway status
```

Description

Cette commande indique si la passerelle SGD Gateway est à l'état démarré, arrêté ou si un problème a été rencontré.

Exemples

La ligne suivante permet d'afficher les informations d'état de la passerelle SGD Gateway. Dans cet exemple, la passerelle SGD Gateway est arrêtée.

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

B.24. gateway stop

Arrête la passerelle SGD Gateway.

Syntaxe

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

Description

Arrête la passerelle SGD Gateway sur confirmation de l'utilisateur.

L'option `--force` permet d'arrêter la passerelle SGD Gateway, sans qu'un message de confirmation s'affiche.

Exemples

La ligne suivante permet d'arrêter la passerelle SGD Gateway en affichant une invite de confirmation.

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

B.25. gateway uninstall

Désinstalle le logiciel SGD Gateway.

Syntaxe

```
gateway uninstall
```

Description

Arrête la passerelle SGD Gateway et retire le logiciel SGD Gateway, y compris toutes les informations de configuration.

Avant d'arrêter la passerelle SGD Gateway, la commande demande confirmation à l'utilisateur.

Exemples

La ligne suivante permet de désinstaller le logiciel SGD Gateway de l'hôte sur lequel la commande est exécutée.

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

B.26. gateway version

Affiche le numéro de version de la passerelle SGD Gateway.

Syntaxe

```
gateway version
```

Description

Affiche le numéro de version de la passerelle SGD Gateway.

Exemples

La ligne suivante permet d'afficher la version de SGD Gateway installée sur l'hôte sur lequel la commande est exécutée.

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

B.27. La commande tarantella gateway

Utilisez la commande `tarantella gateway` pour configurer les passerelles autorisées d'un groupe SGD.

Syntaxe

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

Description

A l'aide de la commande `tarantella gateway`, vous pouvez ajouter, retirer et répertorier les passerelles d'un groupe SGD.

La commande `tarantella gateway` peut être utilisée sur n'importe quel serveur SGD du groupe. Toutes les modifications effectuées sont automatiquement répliquées sur les autres membres du groupe.

Lorsqu'un serveur SGD rejoint un groupe, le jeu de passerelles défini sur le serveur SGD principal est copié sur le nouveau membre du groupe. Si celui-ci contenait déjà des passerelles autorisées, elles sont écrasées. Les passerelles enregistrées ne sont pas supprimées d'un serveur SGD lorsque celui-ci est séparé d'un groupe.

Les sous-commandes disponibles pour la commande `tarantella gateway` sont présentées dans le tableau suivant.

Sous-commande	Description	Informations supplémentaires
`add`	Ajoute une passerelle SGD Gateway pour un groupe SGD	Section B.28, « tarantella gateway add »
`list`	Affiche la liste des passerelles SGD Gateway d'un groupe SGD	Section B.29, « tarantella gateway list »
`remove`	Retire une passerelle SGD Gateway d'un groupe SGD	Section B.30, « tarantella gateway remove »

Note

Toutes les commandes `tarantella gateway` incluent une option `--help`. Vous pouvez utiliser cette option pour afficher l'aide relative à la sous-commande.

Exemples

Dans l'exemple suivant, `gateway1.example.com` est ajouté à la liste des passerelles du groupe SGD.

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

B.28. tarantella gateway add

Permet d'enregistrer une passerelle SGD Gateway auprès d'un groupe SGD.

Syntaxe

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

Description

Le tableau suivant présente les options disponibles pour cette commande.

Option	Description
`--name`	Nom de la passerelle SGD Gateway à enregistrer.
`--certfile`	Certificat de la passerelle SGD Gateway utilisé par le serveur SGD. Le certificat peut être au format DER (Definite Encoding Rules) ou PEM.
`--file`	Fichier batch contenant les paramètres de configuration de plusieurs passerelles SGD Gateway.

Exemples

Dans l'exemple suivant, `gateway1.example.com` est ajouté à la liste des passerelles du groupe SGD.

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

Dans l'exemple suivant, l'option `--file` de la commande `tarantella gateway add` permet d'enregistrer plusieurs passerelles à la fois.

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

L'option `--file` spécifie un fichier batch, `gateways.list`, qui contient une ligne de paramètres pour chaque passerelle, comme suit :

```
--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

Affiche la liste des passerelles SGD Gateway enregistrées pour un groupe SGD.

Syntaxe

```
tarantella gateway list
```

Description

Affiche les informations des passerelles SGD Gateway qui ont été enregistrées pour un groupe SGD à l'aide de la commande `tarantella gateway add`.

Exemples

La ligne suivante permet d'afficher la liste des passerelles enregistrées pour le groupe SGD.

```
$ tarantella gateway list
```

B.30. tarantella gateway remove

Retire une passerelle SGD Gateway de la liste des passerelles enregistrées d'un groupe SGD.

Syntaxe

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

Description

Le tableau suivant présente les options disponibles pour cette commande.

Option	Description
`--name`	Nom de la passerelle SGD Gateway dont les informations d'enregistrement doivent être retirées
`--file`	Fichier batch contenant les paramètres de configuration de plusieurs passerelles SGD Gateway

Exemples

Dans l'exemple suivant, la passerelle SGD Gateway `gateway1.example.com` est retirée de la liste des passerelles enregistrées du groupe SGD.

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

B.31. L'attribut --security-gateway

Description

L'attribut `--security-gateway` permet d'activer l'utilisation de la passerelle SGD Gateway pour le groupe SGD. L'attribut définit les éléments suivants :

- Les clients SGD qui peuvent accéder à une passerelle SGD Gateway selon leur adresse IP ou leur nom DNS.
- L'adresse utilisées par les périphériques client pour contacter la passerelle SGD Gateway.

Note

L'utilisation de l'attribut `--security-gateway` est réservée aux connexions AIP. Le routage des connexions HTTP est géré par le service d'équilibrage de charge HTTP sur le composant de proxy inverse Apache de la passerelle.

Les modifications apportées à l'attribut `--security-gateway` s'appliquent à tous les serveurs SGD du groupe.

Syntaxe

La syntaxe de l'attribut `--security-gateway` est la suivante :

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

Remplacez *`filter-spec`* par une spécification de filtre du type :

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

- La valeur *`client-ip-address`* correspond à l'adresse IP du client SGD. Pour les connexions via la passerelle SGD Gateway, il s'agit de l'interface utilisée par la passerelle SGD Gateway pour se connecter aux serveurs SGD du groupe.

  Un astérisque simple, `*`, représente toutes les adresses IP.

  La chaîne de l'adresse IP du client peut contenir les caractères génériques `*` et `?`, `*` pouvant correspondre à un groupe de caractères et `?` à un seul caractère. Par exemple :

  `192.169.10.*` correspond à toutes les adresses du réseau `192.169.10`.

  `192.169.10.12?` correspond à la plage d'adresses allant de `192.169.10.120` à `192.169.10.129`.

  Note

  Si vous utilisez un équilibreur de charge externe avec la passerelle SGD Gateway, saisissez l'adresse de l'équilibreur de charge en tant que *`client-ip-address`*.

- La valeur *`gateway protocol`* est `sgdg` pour les connexions via la passerelle SGD Gateway, ou `direct` pour les clients SGD qui se connectent directement à un groupe SGD, sans passer par la passerelle SGD Gateway.
- La valeur *`gateway-address`* est l'adresse externe de la passerelle SGD Gateway, ou d'un équilibreur de charge externe, le cas échéant. Il s'agit de l'adresse utilisée par les périphériques client pour contacter la passerelle SGD Gateway.

  Pour les connexions `direct` à un groupe SGD, spécifiez l'adresse du serveur principal dans le groupe.
- La valeur *`gateway-port`* correspond au port TCP que les périphériques client utilisent pour se connecter à la passerelle SGD Gateway, ou à un équilibreur de charge externe, le cas échéant.

  Pour les connexions `direct` à un groupe SGD, spécifiez le port du serveur principal du groupe.

Séparez les entrées *`filter-spec`* multiples par une virgule et placez la chaîne entière entre guillemets (`" "`). Reportez-vous à la Section B.31, « Utilisation de plusieurs filtres ».

Exemples

La ligne suivante permet à tous les clients SGD de se connecter via le port TCP 443 de la passerelle SGD Gateway `gateway1.example.com`.

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

La ligne suivante permet à tous les clients SGD de se connecter via un équilibreur de charge externe, `lb.example.com`.

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

La ligne suivante permet à tous les clients SGD de se connecter directement à un groupe SGD, sans passer par la passerelle SGD Gateway. Le serveur principal du groupe est `sgd1.example.com`.

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

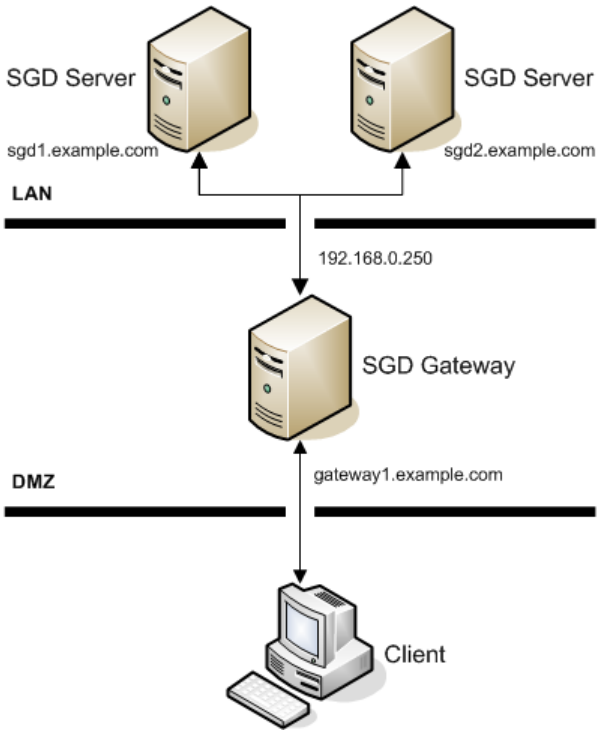
Utilisation de plusieurs filtres

Vous pouvez utiliser plusieurs spécifications de filtre, comme indiqué dans l'exemple suivant.

Envisagez un déploiement classique, présenté à la Figure B.1, « Utilisation de plusieurs spécifications de filtre ». Le déploiement est basé sur une seule passerelle SGD Gateway, `gateway1.example.com`, et sur un groupe SGD contenant deux serveurs SGD, `sgd1.example.com` et `sgd2.example.com`. Le serveur principal du groupe est `sgd1.example.com`.

L'adresse de la passerelle SGD Gateway sur le réseau interne est `192.168.0.250`.

Figure B.1. Utilisation de plusieurs spécifications de filtre



La spécification de filtre suivante peut être utilisée dans cet exemple :

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

Dans une configuration de ce type, les conditions suivantes s'appliquent :

- Les connexions aux serveurs SGD du groupe sont autorisées de l'adresse IP de la passerelle SGD Gateway, `192.168.0.250`. Les clients SGD en dehors de l'entreprise se connectent via le port TCP 443 de la passerelle SGD Gateway, `gateway1.example.com`.
- Tous les autres clients SGD, par exemple ceux situés dans le réseau LAN, se connectent directement au port TCP 80 sur le serveur SGD principal, `sgd1.example.com`. Ces connexions n'utilisent pas la passerelle SGD Gateway.
- L'ordre des filtres est important. Si l'ordre des filtres est inversé, tous les clients SGD se connectent directement au serveur SGD, `sgd1.example.com`.

Annexe C. Configuration avancée

Ce chapitre contient des informations sur la configuration et l'utilisation des fonctionnalités avancées de la passerelle Oracle Secure Global Desktop Gateway (SGD Gateway).

Ce chapitre comprend les rubriques suivantes :

C.1. Réglage de la passerelle SGD Gateway

Lors de l'installation de la passerelle SGD Gateway, les valeurs par défaut du nombre maximum de connexions simultanées AIP (Adaptive Internet Protocol) et HTTP sont configurées automatiquement en fonction de la mémoire disponible sur l'hôte SGD Gateway. Le volume de mémoire alloué à la machine virtuelle Java (JVM) de la passerelle SGD Gateway est également optimisé pour ce nombre de connexions.

Après avoir installé SGD Gateway, vous pouvez changer les paramètres par défaut en fonction du nombre d'utilisateurs SGD prévu et le nombre d'applications qu'ils exécuteront. Au cours de cette opération, vous pouvez être amené à changer également la taille de la mémoire JVM. On appelle cela *régler* la passerelle SGD Gateway.

Attention

Si la taille de la mémoire JVM est trop faible pour le nombre de connexions prévu, il est possible que la passerelle SGD Gateway cesse de fonctionner et rejette toutes les connexions ultérieures. Dans ce cas, vous devez régler la passerelle SGD Gateway de façon à garder suffisamment de mémoire JVM disponible. Le message d'erreur `java.lang.OutOfMemoryError` qui s'affiche sur la passerelle SGD Gateway indique qu'un réglage peut être nécessaire.

Pour régler la passerelle SGD Gateway, procédez comme suit :

- Modifiez le nombre maximum de connexions AIP. Reportez-vous à la Section C.1.1, « Modification du nombre maximum de connexions AIP ».
- Modifiez le nombre maximum de connexions HTTP. Reportez-vous à la Section C.1.2, « Modification du nombre maximum des connexions HTTP ».
- Modifiez la taille de la mémoire JVM. Reportez-vous à la Section C.1.3, « Modification de la taille de la mémoire JVM ».

C.1.1. Modification du nombre maximum de connexions AIP

Le nombre maximum de connexions AIP est configuré lors de la phase d'installation. Le paramètre par défaut dépend des ressources disponibles sur l'hôte SGD Gateway.

Vous pouvez remplacer ce paramètre par une valeur personnalisée, mieux adaptée à votre déploiement. Reportez-vous à la Section C.1.1.1, « Calcul du nombre de connexions AIP » pour plus d'informations sur le calcul du nombre maximum de connexions AIP utilisées par une passerelle SGD Gateway.

Pour modifier le nombre maximum des connexions AIP, utilisez l'option `--routes-aip-maxcon` de la commande `gateway config edit`. Par exemple, pour passer le nombre maximum de connexions AIP à 3 000, exécutez la commande suivante :

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

Vous devez redémarrer la passerelle SGD Gateway pour que les modifications effectuées prennent effet.

C.1.1.1. Calcul du nombre de connexions AIP

Le nombre de connexions AIP utilisées par une passerelle SGD Gateway dépend du nombre d'utilisateurs SGD simultanés, et du nombre d'applications qu'ils exécutent, comme suit :

Nombre de connexions AIP = (*nombre d'applications* + 3) x *nombre d'utilisateurs SGD*

Par exemple, une passerelle SGD Gateway traitant 1 000 utilisateurs SGD, exécutant chacun quatre applications, nécessite le nombre maximum suivant de connexions AIP simultanées :

(4 + 3) x 1000 = 7000 connexions AIP

C.1.2. Modification du nombre maximum des connexions HTTP

La configuration du nombre maximum des connexions HTTP se fait lors de l'installation. Ce paramètre définit le nombre maximum d'utilisateurs simultanés. La valeur par défaut est 100.

Pour modifier le nombre maximum de connexions HTTP, utilisez l'option `--routes-http-maxcon` de la commande `gateway config edit`. Par exemple, pour modifier le nombre maximum des connexions HTTP sur 200, exécutez la commande suivante :

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

Vous devez redémarrer la passerelle SGD Gateway pour que les modifications effectuées prennent effet.

C.1.3. Modification de la taille de la mémoire JVM

Si vous modifiez le nombre maximum de connexions AIP et HTTP, il vous faudra peut-être également changer le volume de mémoire alloué à la JVM de la passerelle SGD Gateway. Pour ce faire, modifiez les paramètres suivants dans le fichier `/opt/SUNWsgdg/proxy/etc/tuning_parameters` :

- `-Xms` : taille initiale de la mémoire JVM, en octets
- `-Xmx` : taille maximale de la mémoire JVM, en octets

Astuce

Vous pouvez joindre les modificateurs `K` (kilo) et `M` (méga) à ces paramètres. Par exemple : 960K = 960 kilo-octets et 512M = 512 méga-octets.

Reportez-vous à la Section C.1.3.1, « Calcul de la taille de la mémoire JVM » pour plus d'informations sur le calcul des valeurs de taille de la mémoire JVM.

Note

Assurez-vous que le système dispose de suffisamment de mémoire pour supporter les paramètres JVM définis.

Vous devez redémarrer la passerelle SGD Gateway pour que les modifications effectuées prennent effet.

C.1.3.1. Calcul de la taille de la mémoire JVM

La quantité de mémoire JVM utilisée par la passerelle SGD Gateway dépend du nombre de connexions AIP et HTTP simultanées.

Etant donné que chaque connexion de passerelle SGD Gateway nécessite environ 300 kilo-octets de mémoire JVM, le calcul de la mémoire JVM peut être exprimé ainsi :

(*nombre de connexions AIP + nombre de connexions HTTP*) x 300 kilo-octets

Par exemple, prenons une passerelle SGD Gateway traitant 500 utilisateurs SGD, exécutant chacun deux applications. Le nombre maximum de connexions AIP serait de :

(2 + 3) x 500 = 2 500 connexions AIP

La passerelle SGD Gateway doit également gérer suffisamment de connexions HTTP simultanées sur le serveur Web SGD. Dans cet exemple, le nombre maximum de connexions HTTP est le suivant :

250 connexions HTTP

Ainsi, la quantité de mémoire JVM requise est de :

(2500 + 250) x 300 kilo-octets = environ 806 méga-octets.

Note

Dans le fichier `/opt/SUNWsgdg/proxy/etc/tuning_parameters`, définissez `-Xms` et `-Xmx` sur la valeur de mémoire JVM calculée. Les paramètres `-Xms` et `-Xmx` sont généralement définis sur la même valeur pour optimiser les performances.

C.2. Configuration de la redirection HTTP

Par défaut, la passerelle SGD Gateway refuse les connexions HTTP sur le port TCP 80.

Pour autoriser les connexions sur le port TCP 80, utilisez la commande `gateway config enable` pour activer le service de redirection HTTP, comme suit :

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

Vous devez redémarrer la passerelle SGD Gateway pour que les modifications effectuées prennent effet.

C.3. Changement du port d'authentification de la passerelle SGD Gateway

L'interface et le port que la passerelle SGD Gateway utilise pour les connexions entrantes sont appelés *port d'authentification*. Par défaut, la passerelle SGD Gateway utilise le port TCP 443 comme port d'authentification sur toutes les interfaces.

Pour changer le port d'authentification, utilisez l'option `--binding` de la commande `gateway config edit`. Par exemple, pour modifier le port d'authentification au port TCP 4443, exécutez la commande suivante :

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

Vous pouvez également modifier le port d'authentification en exécutant la commande `/opt/SUNWsgdg/bin/gateway config create` sur l'hôte SGD Gateway. Cette commande vous invite à indiquer une interface et le port à utiliser pour les connexions proxy entrantes.

Note

La commande `gateway config create` commande entraîne la création d'une configuration et remplace tous les paramètres de configuration que vous avez définis.

Vous devez redémarrer la passerelle SGD Gateway pour que les modifications effectuées prennent effet.

C.4. Utilisation de connexions non chiffrées au groupe de serveurs SGD

Par défaut, les connexions entre la passerelle SGD Gateway et les serveurs SGD du groupe sont sécurisées à l'aide du protocole SSL (Secure Sockets Layer). Cela signifie que les données AIP sur SSL utilisent le port TCP 5307 et que les données HTTPS utilisent le port TCP 443.

Pour utiliser des connexions non chiffrées entre la passerelle SGD Gateway et les serveurs SGD du groupe, reportez-vous à la Section C.4.1, « Configuration de la passerelle de sorte à utiliser des connexions non chiffrées avec le groupe SGD ».

Pour les connexions non chiffrées, les données AIP utilisent le port TCP 3144 et les données HTTP utilisent le port TCP 80.

C.4.1. Configuration de la passerelle de sorte à utiliser des connexions non chiffrées avec le groupe SGD

Cette procédure décrit les étapes à suivre pour reconfigurer un déploiement de passerelle de sorte à utiliser des connexions non chiffrées.

1. Modifiez la configuration de la passerelle de sorte à utiliser des connexions non chiffrées avec le groupe SGD.

   ```
   # gateway config create
   ```

   Note

   Cette commande remplace la configuration actuelle de la passerelle.

   Au moment d'indiquer si vous souhaitez sécuriser les connexions entre la passerelle et les serveurs SGD du groupe, entrez `n`.

2. Retirez tout serveur SGD préalablement enregistré auprès de la passerelle.

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

   où *`sgd.example.com`* est le nom du serveur SGD.

   Le certificat AC et le certificat SSL du serveur SGD sont retirés du keystore de la passerelle.

3. Assurez-vous que les serveurs SGD du groupe sont configurés pour utiliser des connexions standard non chiffrées.

Exécutez la commande suivante sur chaque serveur SGD du groupe pour désactiver les services de sécurité SGD.

```
# tarantella security disable
```

4. Enregistrez les serveurs SGD du groupe auprès de la passerelle.

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

La ligne suivante permet d'ajouter le certificat AC `PeerCAcert.pem` au keystore de la passerelle SGD Gateway à l'aide de l'alias *`sgd.example.com`*. L'URL du serveur Web SGD est *`http://sgd.example.com`*.

5. Redémarrez la passerelle.

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

C.5. Utilisation d'accélérateurs SSL externes

Par défaut, la passerelle SGD Gateway est configurée pour fonctionner avec des connexions de données HTTP et AIP entrantes, lesquelles sont sécurisées à l'aide du protocole SSL. La passerelle prend également en charge l'utilisation des accélérateurs SSL externes pour gérer le traitement SSL.

Pour utiliser un accélérateur SSL externe avec la passerelle, effectuez les opérations suivantes :

- Configurez l'accélérateur SSL externe pour déchiffrer les connexions SSL et redirigez ces dernières en clair vers la passerelle.
- Activez la prise en charge de l'accélérateur SSL externe sur la passerelle.

  Cela permet à la passerelle d'accepter les connexions non chiffrées sur le port sécurisé. Reportez-vous à la Section C.5.1, « Procédure d'activation de la prise en charge d'un accélérateur SSL externe ».
- Assurez-vous que les périphériques client utilisent l'accélérateur SSL comme point d' entrée du réseau.

  En général, l'accélérateur SSL est également un équilibreur de charge. Configurez les serveurs SGD et passerelles SGD Gateway pour permettre un déploiement avec équilibrage de charge selon la description de la Section 2.1.2, « Déploiement avec équilibrage de charge ».

C.5.1. Procédure d'activation de la prise en charge d'un accélérateur SSL externe

Assurez-vous qu'aucun utilisateur n'est connecté à SGD via la passerelle.

1. Connectez-vous à l'hôte en tant que superutilisateur (utilisateur root) à l'hôte SGD Gateway.
2. Activez la prise en charge des connexions entrantes non chiffrées.

   Changez le lien symbolique du fichier `gateway.xml` de façon à ce qu'il renvoie au fichier `gateway-plaintext.xml` au lieu de `gateway-ssl.xml` (paramètre par défaut).

   Exécutez la commande suivante :

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

3. (Facultatif) Modifiez le port d'authentification de la passerelle.

Selon votre configuration réseau, vous serez peut-être amené à modifier également le port d'authentification de la passerelle SGD Gateway.

Reportez-vous à la Section C.3, « Changement du port d'authentification de la passerelle SGD Gateway ».

4. Redémarrez la passerelle SGD Gateway.

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

C.6. Configuration des chiffrements pour la passerelle SGD Gateway

La passerelle prend en charge une large gamme de mécanismes de chiffrement pour les connexions SSL. Reportez-vous au manuel *Oracle Secure Global Desktop Prise en charge des plates-formes et notes de version relatives à la version 4.7* pour obtenir une liste des mécanismes de chiffrement pris en charge.

Au cours de l'installation, la passerelle est configurée pour utiliser un jeu de chiffrements composé uniquement de chiffrements haute qualité. Cela signifie que les connexions à la passerelle SSL utilisent toujours un niveau de sécurité optimisé. Si nécessaire, vous pouvez configurer la passerelle de façon à ce qu'elle utilise un autre jeu de chiffrements.

C.6.1. Procédure de configuration des chiffrements pour la passerelle

1. Arrêtez la passerelle.

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

2. Configurez les chiffrements requis.

   Dans le répertoire `/opt/SUNWsgdg/etc`, modifiez le fichier `ciphersuites.xml`.

   Par défaut, le fichier `ciphersuites.xml` contient les entrées suivantes, correspondant aux chiffrements haute qualité.

```
<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. Vérifiez que l'entrée suivante figure dans le fichier `opt/SUNWsgdg/etc/gateway.xml`, de sorte à inclure le fichier `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. Redémarrez la passerelle.

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

C.7. Utilisation de certificats client avec la passerelle SGD Gateway

Vous pouvez utiliser des *certificats client* pour augmenter le niveau de sécurité de la passerelle SGD Gateway, en limitant l'accès aux utilisateurs disposant d'un certificat valide.

Un certificat client est un certificat SSL installé dans le navigateur sur le périphérique client. Reportez-vous à la documentation de votre navigateur pour plus d'informations sur la procédure d'installation d'un certificat client.

Reportez-vous à la Section C.7.2, « Procédure de génération d'une demande de signature de certificat pour un certificat client » si vous avez besoin de générer une demande de signature de certificat (CSR) pour obtenir un nouveau certificat client.

Les procédures suivantes font appel à l'application `keytool`. Reportez-vous à la documentation relative aux outils et utilitaires JDK pour plus d'informations sur le fonctionnement de l'application `keytool`.

C.7.1. Procédure de configuration de la passerelle SGD Gateway en vue de l'utilisation des certificats client

1. Connectez-vous à l'hôte en tant que superutilisateur (utilisateur root) à l'hôte SGD Gateway.
2. Arrêtez la passerelle SGD Gateway.

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

3. Configurez la passerelle SGD Gateway afin qu'ils utilisent des certificats client pour les connexions client HTTPS.

   Ajoutez une entrée `<needClientAuth>` au fichier `/opt/SUNWsgdg/etc/gateway.xml`, comme suit :

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

4. (Facultatif) Importez le certificat client dans le keystore du client SGD Gateway.

Note

Vous n'avez pas besoin d'effectuer cette étape si le certificat client est signé par une autorité de certification sécurisée.

   Utilisez la commande `keytool`, comme suit :

```
# /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‘
```

Dans cet exemple, le certificat client `mycert.crt` est importé dans le keystore client de SGD Gateway. Le certificat client est enregistré sous l'alias `mycert`.

5. Démarrez la passerelle SGD Gateway.

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

C.7.2. Procédure de génération d'une demande de signature de certificat pour un certificat client

Pour obtenir un certificat client que vous pouvez utiliser avec la passerelle, vous devez d'abord générer une demande de signature de certificat. Vous envoyez ensuite la demande de signature de certificat à une autorité de certification (AC) pour signature.

Note

Cette procédure explique comment utiliser l'application `keytool` sur l'hôte Gateway pour générer une demande de signature de certificat. Toutefois, vous n'êtes pas obligé de suivre les étapes décrites dans cette procédure. Vous pouvez tout à fait utiliser votre outil de gestion des certificats préféré pour générer la demande de signature de certificat.

1. Connectez-vous à l'hôte en tant que superutilisateur (utilisateur root) à l'hôte SGD Gateway.
2. Générez un certificat auto-signé et une clé privée correspondante.

   Utilisez la commande `keytool`, comme suit :

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

   Dans cet exemple, un certificat auto-signé et une clé privée sont créés et enregistrés dans un keystore appelé `keystore.mycert`. La paire de clés est enregistrée sous un alias `mycert`.

3. Générez une demande de signature de certificat pour le certificat auto-signé.

   Utilisez la commande `keytool`, comme suit :

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

   Dans cet exemple, une demande de signature de certificat est générée et enregistrée dans le fichier `/tmp/`*`gateway-name`*`.csr`, *`gateway-name`* correspondant au nom de la passerelle.

C.8. Activation de l'application Balancer Manager

Le proxy inverse Apache inclut une application Web appelée Balancer Manager. Balancer Manager vous permet de gérer les serveurs Web SGD dans le groupe d'équilibrage de charge utilisé par le proxy inverse.

A l'aide de Balancer Manager, vous pouvez effectuer les opérations suivantes :

- Afficher des informations d'état sur les serveurs Web SGD compris dans le groupe d'équilibrage de charge
- Visualiser et changer les routes d'équilibrage de charge des serveurs Web SGD
- Retirer les serveurs Web SGD du groupe d'équilibrage de charge

Pour activer Balancer Manager, retirez les commentaires du fichier de configuration de proxy inverse, `/opt/SUNWsgdg/httpd/apache-version/conf/extra/gateway/httpd-gateway.conf`, qui désactivent l'application.

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

Vous devez redémarrer la passerelle pour que les modifications prennent effet.

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

Pour accéder Balancer Manager, démarrez un navigateur et rendez-vous sur le site `https://gateway.example.com/balancer-manager`, *`gateway.example.com`* correspondant à l'hôte SGD Gateway.

Pour plus d'informations sur la configuration de Balancer Manager, reportez-vous à la Apache mod_proxy_balancer documentation.

C.9. Service de réflexion

Le *service de réflexion* est une série de services Web RESTful utilisés par le proxy de routage de la passerelle SGD Gateway. A l'aide du service de réflexion, l'administrateur d'une passerelle SGD Gateway peut configurer des routes, des services, des niveaux de journalisation et des connexions, et afficher des informations d'état sur le proxy de routage.

Cette section comprend les rubriques suivantes relatives au service de réflexion :

- Section C.9.1, « Activation du service de réflexion »
- Section C.9.2, « Utilisation du service de réflexion »

C.9.1. Activation du service de réflexion

Par défaut, le service de réflexion n'est pas activé pour la passerelle SGD Gateway.

Vous pouvez activer le service de réflexion pour une ou plusieurs des méthodes d'accès suivantes :

- **Accès non autorisé** : les utilisateurs n'ont pas besoin de s'authentifier.

  Par défaut, l'accès non autorisé sera uniquement disponible depuis l'hôte SGD Gateway.

  Reportez-vous à la Section C.9.1.1, « Procédure d'activation de l'accès non autorisé au service de réflexion » pour plus d'informations sur l'activation d'un accès non autorisé.

- **Accès autorisé** : les utilisateurs doivent s'authentifier avant d'accéder au service de réflexion.

  Reportez-vous à la Section C.9.1.2, « Procédure d'activation de l'accès autorisé au service de réflexion » pour plus d'informations sur l'activation d'un accès autorisé.

C.9.1.1. Procédure d'activation de l'accès non autorisé au service de réflexion

1. Connectez-vous à l'hôte en tant que superutilisateur (utilisateur root) à l'hôte SGD Gateway.
2. Activez l'accès non autorisé au service de réflexion.

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

3. (Facultatif) Changez l'interface utilisée par le service de réflexion.

Attention

Par défaut, l'accès non autorisé au service de réflexion est uniquement disponible depuis l'hôte SGD Gateway. L'activation de l'accès non authentifié sur d'autres interfaces peut engendrer un risque pour la sécurité.

L'interface par défaut utilisée pour accéder au service de réflexion de manière non autorisée est l'interface loopback `localhost`. L'exemple suivant indique comment activer l'accès non autorisé sur toutes les interfaces :

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

4. (Facultatif) Modifiez le port utilisé par le service de réflexion.

   Le port par défaut utilisé pour accéder de façon non autorisée au service de réflexion est le port TCP 81. Vous pouvez le remplacer par un port inutilisé, comme suit :

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

   portnum correspondant au numéro de port utilisé par le service de réflexion.

5. Redémarrez la passerelle SGD Gateway.

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

6. Accédez au service de réflexion.

   Sur l'hôte SGD Gateway, vous pouvez démarrer un navigateur et vous rendre sur le site `http://localhost:81`.

   La page d'accueil du service de réflexion s'affiche.

C.9.1.2. Procédure d'activation de l'accès autorisé au service de réflexion

1. Sur l'hôte SGD Gateway, connectez-vous à l'hôte en tant que superutilisateur (utilisateur root).
2. Exportez le certificat et la clé privée du service de réflexion.

   Le certificat et la clé privée du service de réflexion sont enregistrées dans le keystore du service de réflexion, à l'emplacement suivant : `/opt/SUNWsgdg/proxy/etc/keystore.reflection`. Ce keystore est créé automatiquement au cours de l'installation de SGD Gateway.

   Par défaut, le keystore du service de réflexion contient un certificat auto-signé unique et une paire de clés.

   a. Exportez le certificat du service de réflexion.

```
# /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
```

server-name correspondant à l'alias utilisé pour le certificat du service de réflexion dans le keystore de réflexion et *client.pem* correspondant au nom de fichier du certificat exporté.

Reportez-vous à la documentation relative aux outils et utilitaires JDK pour plus d'informations sur le fonctionnement de l'application `keytool`.

b. Exportez la clé privée du service de réflexion.

Utilisez l'application KeyManager fournie avec SGD Gateway.

```
# /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)"
```

alias-name correspondant à l'alias utilisé pour la clé du service de réflexion dans le keystore de réflexion *client.key* correspondant au nom de fichier de la clé exportée.

3. Installez le certificat et la clé privée sur le périphérique client.

Le certificat et la clé privée sont utilisés par le périphérique client de façon à autoriser l'accès au service de réflexion.

Pour importer le certificat et la clé dans la banque de certificats d'un navigateur, vous devez d'abord convertir ceux-ci en un fichier au format PKCS12. Par exemple :

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

Cette commande convertit le fichier de certificat `mycert.crt` et la clé privée associée `mycert_key.pem` en un fichier de certificat `mycert.p12` au format PKCS12.

Pour plus d'informations sur l'importation d'un certificat au format PKCS12 dans votre navigateur, reportez-vous à la documentation en ligne pour votre navigateur.

4. Activez l'accès autorisé au service de réflexion.

Sur l'hôte SGD Gateway, exécutez la commande suivante :

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

5. (Facultatif) Modifiez l'interface et le port utilisé par le service de réflexion.

Le port d'authentification utilisé par défaut pour l'accès autorisé au service de réflexion est le port TCP 82 sur toutes les interfaces. Vous pouvez le remplacer par une autre interface et un port inutilisé, comme suit :

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

int correspondant à l'interface et *portnum* au numéro de port utilisé par le service de réflexion.

6. Redémarrez la passerelle SGD Gateway.

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

7. Connectez-vous au service de réflexion à partir du périphérique client, à l'aide du certificat et de la clé privée.

   - Utilisation de la commande `curl` :

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

     Dans cet exemple, la commande `curl` permet d'accéder à la page d'accueil du service de réflexion à l'adresse `https://gateway.example.com:82`, *`gateway.example.com`* correspondant au nom de la passerelle SGD Gateway. Le certificat et la clé privée du service de réflexion sont *`client.pem`* et *`client.key`*.

   - A l'aide d'un navigateur :

     Accédez à l'adresse `https://gateway.example.com:82`, *`gateway.example.com`* correspondant au nom de la passerelle SGD Gateway.

     La page d'accueil du service de réflexion s'affiche.

C.9.2. Utilisation du service de réflexion

Utilisez une application client pour accéder aux services Web RESTful fournis par le service de réflexion. Voici des exemples d'applications client appropriées :

- **Navigateur.** L'utilisation d'un navigateur est la méthode la plus simple pour accéder au service de réflexion. Toutefois, un navigateur prend également en charge les demandes `GET` HTTP et donc limite l'accès aux services Web RESTful qui récupèrent les informations. En pratique, l'utilisation d'un navigateur est utile par exemple lors de d'affichage d'informations d'état ou de listes des routes et des services pour le proxy de routage.
- **curl.** Il s'agit d'un outil de ligne de commande pour les plates-formes UNIX et Linux qui prennent en charge les demandes HTTP `GET`, `PUT`, `POST` et `DELETE`. Cela signifie que la gamme complète des services Web RESTful du service de réflexion peut être utilisée. La sortie de cet outil peut être redirigée dans un fichier, ou dans un autre programme pour subir d'autres étapes de traitement.

Par ailleurs, si vous possédez votre propre application client qui prend en charge les services Web RESTful, vous pouvez l'utiliser pour accéder au service de réflexion.

Note

Il est inutile de redémarrer la passerelle SGD Gateway lorsque vous utilisez le service de réflexion pour modifier la configuration d'un proxy de routage.

Les données peuvent être renvoyées par le service de la réflexion dans les formats suivants :

- **ASCII.** Il s'agit du format de sortie par défaut. Les données sont renvoyées au format ASCII délimité par des tabulations. Ce format de sortie est utile si les données doivent passer par un autre processus, par exemple une analyse.
- **HTML.** Les données sont renvoyées au format HTML, ce qui permet de les afficher dans un navigateur Web. Pour obtenir une sortie HTML, ajoutez `/html` à la fin de l'URI (Uniform Resource Identifier) du service Web.

C.9.2.1. A propos des services Web RESTful

Le Tableau C.1, « Services Web RESTful du service de réflexion de la passerelle SGD Gateway » répertorie les services Web RESTful du service de réflexion de la passerelle SGD Gateway.

Tableau C.1. Services Web RESTful du service de réflexion de la passerelle SGD Gateway

URI relatif	Méthode de demande HTTP	Description
`/`	`GET`	Indique des informations générales sur le proxy de routage, tel que le temps de fonctionnement.
`/service`	`GET`	Répertorie les services disponibles. Un service représente un point d'entrée à partir duquel le proxy de routage crée des connexions entrantes.
`/service/`*`Service-Id`*	`GET`	Répertorie des informations sur un service, identifié par *`Service-Id`*.
`/service/`*`Service-Id`*	`PUT`	Démarre un service, identifié par *`Service-Id`*.
`/service/`*`Service-Id`*	`DELETE`	Arrête un service, identifié par *`Service-Id`*.
`/client`	`GET`	Répertorie les clients disponibles. Un client représente un point de sortie sur lequel le proxy de routage crée des connexions sortantes.
`/client/`*`Client-Id`*	`GET`	Répertorie des informations sur un client, identifié par *`Client-Id`*.
`/route`	`GET`	Répertorie les routes disponibles. Une route représente un itinéraire dans le proxy de routage, partant des connexions entrantes via les services, jusqu'aux connexions sortantes via les clients.
`/route/`*`Route-Id`*	`GET`	Répertorie des informations sur une route, identifié par *`Route-Id`*.
`/route/`*`Route-Id`*	`PUT`	Démarre une route, identifiée par *`Route-Id`*.
`/route/`*`Route-Id`*	`DELETE`	Arrête une route, identifiée par *`Route-Id`*.
`/route/`*`Route-Id`*`/connection`	`GET`	Répertorie les connexions d'une route spécifique, identifiée par *`Route-Id`*.
`/route/`*`Route-Id`*`/connection/`*`Connection-Id`*	`DELETE`	Interrompt une connexion, identifiée par *`Connection-Id`*.
`/connection`	`GET`	Répertorie toutes les connexions en cours d'exécution, pour toutes les routes.
`/logging/level`	`GET`	Indique le niveau de journalisation global.
`/logging/level/`*`Log-Level`*	`PUT`	Indique le niveau de journalisation global du proxy de routage.
`/logging/`*`Package`*`/level`	`GET`	Indique le niveau de journalisation pour un composant spécifique du proxy de routage.
`/logging/`*`Package`*`/level/`*`Log-Level`*	`PUT`	Définit le niveau de journalisation pour un composant spécifique du proxy de routage.

Pour accéder à un service Web RESTful, ajoutez-les URI relatifs du service Web à l'URL du service de réflexion.

Par exemple, pour répertorier les routes disponibles pour une passerelle SGD Gateway, *gateway.example.com*, ajoutez `/route` à l'URL du service de réflexion de la façon suivante :

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

client.pem et *client.key* correspondant au certificat et à la clé privée du service de réflexion. Dans cet exemple, le client reçoit l'autorisation avant d'accéder au service de réflexion.

C.9.2.2. Exemples d'utilisation du service de réflexion

Tous les exemples suivants utilisent la commande `curl` en tant qu'application cliente pour accéder au service de réflexion.

Les exemples utilisent un accès authentifié au service de réflexion sur une passerelle SGD Gateway appelée *gateway.example.com*. Le client est autorisé à l'aide d'un certificat, *client.pem*, et d'une clé privée, *client.key*.

Pour répertorier les différents services disponibles pour la passerelle SGD Gateway :

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

Pour arrêter une route, indiquez l'ID de route utilisé par le service de réflexion pour la route en question :

```
$ 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
```

Pour définir le niveau de journalisation global sur FINER (plus détaillé) :

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

Annexe D. Dépannage de la passerelle SGD Gateway

Ce chapitre contient des rubriques de dépannage permettant de diagnostiquer et de résoudre les problèmes rencontrés avec Oracle Secure Global Desktop Gateway (SGD Gateway).

Ce chapitre comprend les rubriques suivantes :

- Section D.1, « Journalisation et diagnostic »
- Section D.2, « Modification du nom DNS pair d'un serveur SGD »
- Section D.3, « Messages d'erreur de SGD Gateway »

D.1. Journalisation et diagnostic

Cette section décrit les fonctions de journalisation et de diagnostic de la passerelle SGD Gateway.

Cette section comprend les rubriques suivantes :

- Section D.1.1, « A propos de la journalisation de SGD Gateway »
- Section D.1.2, « Affichage des informations sur le processus SGD Gateway »
- Section D.1.3, « Contrôle de la configuration dans la ligne de commande »

D.1.1. A propos de la journalisation de SGD Gateway

La journalisation de SGD utilise une interface API de journalisation Java. Pour plus d'informations sur l'implémentation de la journalisation dans Java, reportez-vous au lien http://download.oracle.com/javase/6/docs/technotes/guides/logging/overview.html.

D.1.1.1. Modification du niveau de journalisation

Un fichier de configuration des propriétés de journalisation, `logging.properties`, est fourni avec la passerelle SGD Gateway. Ce fichier est situé dans le répertoire `/opt/SUNWsgdg/proxy/etc`.

Vous pouvez modifier le fichier `logging.properties` de sorte à définir un niveau de journalisation autre que celui par défaut, et pour configurer le niveau de journalisation spécifique à chaque service SGD Gateway. Chaque service SGD Gateway est représenté par une entrée `async.channel` dans le fichier `logging.properties`.

Par exemple, si vous souhaitez configurer une journalisation plus détaillée pour les connexions TCP entrantes et sortantes, définissez le niveau de journalisation du service TCP sur `FINEST` (le plus détaillé). Dans le fichier `logging.properties`, supprimez le commentaire de la ligne suivante :

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

La documentation de la classe `FileHandler` décrit les paramètres de niveau de journalisation que vous pouvez utiliser dans un fichier `logging.properties`.

Vous devez redémarrer la passerelle SGD Gateway pour que les modifications effectuées dans le fichier `logging.properties` prennent effet.

Note

Vous pouvez également utiliser le service de réflexion de la passerelle SGD Gateway pour modifier les niveaux de journalisation. Reportez-vous à la Section C.9, « Service de réflexion » pour plus d'informations sur la configuration et l'utilisation du service de réflexion.

D.1.1.2. Emplacements des fichiers journaux

Si vous rencontrez des problèmes avec la passerelle SGD Gateway, consultez les fichiers journaux suivants :

- **Fichiers journaux du proxy de routage.** L'emplacement et les noms de ces fichiers journaux sont définis dans le fichier `logging.properties`. Par défaut, la passerelle SGD Gateway crée des fichiers journaux de proxy de routage dans le répertoire `/opt/SUNWsgdg/proxy/var/log` situé sur l'hôte SGD Gateway.
- **Fichiers journaux du proxy inverse.** Les détails relatifs à l'équilibrage de charge et à l'activité du serveur proxy pour les connexions HTTP et HTTPS sont consignés dans les fichiers journaux Apache situés dans le répertoire `/opt/SUNWsgdg/httpd/`*`apache-version`*`/logs` sur l'hôte SGD Gateway.
- **Fichiers journaux du serveur SGD.** Chaque serveur SGD du groupe enregistre les messages d'erreur dans des fichiers journaux situés dans le répertoire `/opt/tarantella/var/log` sur l'hôte du serveur SGD. Reportez-vous à la section "Contrôle et journalisation" du chapitre 6 du manuel *Oracle Secure Global Desktop Administration Guide for Release 4.7* pour plus d'informations sur la configuration de la journalisation pour les serveurs SGD.

D.1.2. Affichage des informations sur le processus SGD Gateway

Au démarrage de la passerelle SGD Gateway, l'ID de processus du proxy de routage est enregistré dans le fichier `/opt/SUNWsgdg/proxy/var/run/proxy.pid` sur l'hôte SGD Gateway.

L'ID de processus du proxy inverse est enregistré dans le fichier `/opt/SUNWsgdg/httpd/`*`apache-version`*`/logs/httpd.pid`. L'emplacement de ce fichier peut être modifié à l'aide de la directive `PidFile` dans le fichier de configuration Apache `httpd.conf`.

Pour afficher les processus SGD Gateway en cours d'exécution, utilisez la commande suivante sur l'hôte SGD Gateway :

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

D.1.3. Contrôle de la configuration dans la ligne de commande

Vous pouvez utiliser les commandes suivantes pour vérifier la configuration de votre passerelle SGD Gateway.

- `gateway status` : affiche des informations d'état pour la passerelle SGD Gateway.

  Exécutez la commande suivante sur l'hôte SGD Gateway :

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

  Reportez-vous également à la Section B.23, « gateway status » pour plus d'informations sur cette commande.

- `tarantella gateway list` : affiche une liste des passerelles SGD Gateway qui sont autorisées à être utilisées par le groupe SGD.

  Exécutez la commande suivante sur un des serveurs SGD du groupe :

  ```
  $ tarantella gateway list
  ```

  Reportez-vous à la Section B.27, « La commande tarantella gateway » pour plus d'informations sur l'utilisation de la commande `tarantella gateway`.

- `tarantella config list` : affiche les paramètres globaux du groupe SGD.

  Exécutez la commande suivante sur l'un des serveurs SGD pour afficher le paramètre de l'attribut `--security-gateway`. Cet attribut identifie les clients SGD qui seront autorisés à utiliser la passerelle SGD Gateway.

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

  Reportez-vous à la Section B.31, « L'attribut --security-gateway » pour plus d'informations sur cet attribut.

D.2. Modification du nom DNS pair d'un serveur SGD

Le *nom DNS pair* est le nom DNS qu'un serveur SGD utilise pour s'identifier auprès d'autres serveurs SGD du groupe. Par exemple, `boston.example.com`.

Lorsque vous modifiez le nom DNS pair d'un serveur SGD, la passerelle ne sera plus en mesure de se connecter au serveur. En effet, les certificats utilisés par la passerelle ne contiennent pas le nouveau nom DNS.

Vous devrez peut-être reconfigurer le déploiement de votre passerelle comme suit :

1. (Facultatif) Installez le nouveau certificat SSL du serveur SGD. Reportez-vous à la section Section 2.2.2.1, « Procédure d'installation des certificats de serveur SGD ».

   Cette étape est nécessaire si le nouveau nom DNS pair n'est pas inclus dans le certificat SSL utilisé par le serveur SGD. Vous devez remplacer le certificat SSL sur le serveur SGD et installer le nouveau certificat SSL sur chaque passerelle.

2. (Facultatif) Installez le nouveau certificat AC du serveur SGD. Reportez-vous à la section Section 2.2.2.1, « Procédure d'installation des certificats de serveur SGD ».

   Cette étape est nécessaire si vous changez le nom DNS pair du serveur principal du groupe. Vous devez régénérer les certificats utilisés pour les communications intragroupes sécurisées et installer le nouveau certificat AC sur chaque passerelle.

Reportez-vous à la section "Noms DNS pairs" du chapitre 1 du manuel *Oracle Secure Global Desktop Administration Guide for Release 4.7* pour plus d'informations sur la modification du nom DNS pair d'un serveur SGD.

D.3. Messages d'erreur de SGD Gateway

Les messages d'erreur de SGD Gateway sont consignés dans les fichiers journaux du proxy de routage, situés dans le répertoire `/opt/SUNWsgdg/proxy/var/log` sur l'hôte SGD Gateway.

Certains messages d'erreur courants de SGD Gateway, accompagnés d'une description de l'origine probable du problème, sont répertoriés dans le Tableau D.1, « Messages d'erreur de SGD Gateway ».

Tableau D.1. Messages d'erreur de SGD Gateway

Message d'erreur	Cause probable

`Failed to validate token:`
 	
`Token time not yet valid`
	Les horloges de la passerelle SGD Gateway et des serveurs SGD du groupe ne sont pas synchronisées.

`Failed to decode token:`	Le certificat AC du serveur SGD n'a pas été installé sur la passerelle SGD Gateway.

Message d'erreur	Cause probable
`No trusted signature found`	

`Failed to validate token:`
 	
`No recipient available to decrypt token`
	Le certificat SGD Gateway n'a pas été installé dans le groupe SGD

`SSL error:`
 	
`Check the proxy SSL keystore has valid trusted certificates`
	Le certificat SSL du serveur SGD n'a pas été installé sur la passerelle SGD Gateway