

Oracle® Secure Global Desktop

**Prise en charge des plates-formes et notes de version relatives
à la version 4.7**



E35905-01
Août 2012

Oracle® Secure Global Desktop: Prise en charge des plates-formes et notes de version relatives à la version 4.7

Copyright © 2012, Oracle et/ou ses affiliés. Tous droits réservés.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government. Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

Résumé

Ce document décrit les nouvelles fonctions et les modifications apportées aux fonctions existantes du produit Oracle Secure Global Desktop 4.7. Il dresse également une liste des éléments pris en charge et des bogues et problèmes recensés.

Document publié le : 2012-11-12 (revision: 1287)

Table des matières

Préface	v
1. Public	v
2. Organisation de ce document	v
3. Accessibilité de la documentation	v
4. Documents associés	v
5. Conventions	vi
1. Nouvelles fonctionnalités et modifications	1
1.1. Nouvelles fonctionnalités de la version 4.70	1
1.1.1. Installation sécurisée par défaut	1
1.1.2. Nouvelle implémentation du serveur X	1
1.1.3. Enregistrement audio pour les applications Windows	1
1.1.4. Prise en charge de l'authentification au niveau du réseau pour les applications Windows	2
1.1.5. Nouveau courtier de serveur virtuel pour Oracle VDI	2
1.2. Modifications dans la version 4.70	2
1.2.1. Modifications de l'installation du client SGD	2
1.2.2. Modifications de la méthode de connexion par défaut	3
1.2.3. Nouveaux paramètres du courtier SGD définis par l'utilisateur	3
1.2.4. Le lancement local n'est plus pris en charge	3
1.2.5. Pool de licence d'accès client retiré	3
1.2.6. Modifications des attributs d'affichage des objets d'application	4
1.2.7. Fonctionnalités retirées de cette version	4
1.2.8. Modifications dans la documentation	4
1.2.9. Modifications apportées aux environnements linguistiques pris en charge	4
2. Configuration système requise et compatibilité	7
2.1. Serveur SGD : configuration requise et compatibilité	7
2.1.1. Configuration matérielle requise pour SGD	7
2.1.2. Plates-formes d'installation prises en charge par SGD	7
2.1.3. Chemins de mise à niveau pris en charge	10
2.1.4. Version de la technologie Java	10
2.1.5. Utilisateurs et privilèges requis	10
2.1.6. Configuration réseau requise	11
2.1.7. Synchronisation d'horloge	12
2.1.8. Serveur Web SGD	12
2.1.9. Mécanismes d'authentification pris en charge	13
2.1.10. Prise en charge du chiffrement SSL	14
2.1.11. Prise en charge de l'impression	14
2.2. Périphériques client : configuration requise et compatibilité	15
2.2.1. Plates-formes client prises en charge	15
2.2.2. Serveurs proxy pris en charge	17
2.2.3. Prise en charge de l'impression PDF	18
2.2.4. Cartes à puce prises en charge	18
2.3. Passerelle SGD Gateway : configuration requise et compatibilité	18
2.3.1. Plates-formes d'installation prises en charge par la passerelle SGD Gateway	18
2.3.2. Configuration requise des serveurs SGD pour la passerelle SGD Gateway	19
2.3.3. Serveur Web Apache	20
2.3.4. Version de la technologie Java	20
2.3.5. Prise en charge du chiffrement SSL	20
2.4. Affichage d'applications : configuration requise et compatibilité	21
2.4.1. Applications prises en charge	21
2.4.2. Plates-formes d'installation prises en charge par le module d'enrichissement SGD	22

2.4.3. Microsoft Windows Services Remote Desktop	23
2.4.4. Applications X et à traitement de caractère	25
2.4.5. Infrastructure de bureaux virtuels (Virtual Desktop Infrastructure)	27
2.5. Fonctionnalités retirées	27
2.5.1. Modifications prévues dans la prochaine version de SGD	28
3. Problèmes connus, résolution de bogues et problèmes détectés dans la documentation	29
3.1. Bogues et problèmes connus	29
3.1.1. 2205237 : problèmes d'affichage dans une fenêtre transparente lors du redémarrage d'une session déconnectée	29
3.1.2. 6555834 : la technologie Java est activée pour le navigateur mais n'est pas installée sur le périphérique client	29
3.1.3. 6831480 : la commande de liste des serveurs principaux de sauvegarde renvoie un message d'erreur	29
3.1.4. 6863153 : l'application HyperTerminal se bloque à partir d'une session de bureau Windows	29
3.1.5. 6937146 : audio non disponible pour les applications X hébergées sur des serveurs d'applications Linux 64 bits	30
3.1.6. 6942981 : lenteur du démarrage de l'application sur Solaris Trusted Extensions	30
3.1.7. 6957820 : le client SGD se bloque lors de l'utilisation de l'authentification des cartes à puce pour les applications Windows	31
3.1.8. 6962970 : un périphérique client Windows utilise plusieurs CAL	31
3.1.9. 6970615 : échec de l'authentification SecurID pour les applications X	31
3.1.10. 7004887 : échec de l'impression dans un fichier pour les périphériques client Windows	31
3.1.11. 12300549 : le nom du serveur d'annuaires personnel de certains environnements linguistiques client est illisible	31
3.1.12. 13068287 : problèmes avec la couleur 16 bits dans les applications OpenGL	32
3.1.13. 13117149 : caractères accentués dans les noms d'utilisateur Active Directory	32
3.1.14. 13354844, 14032389, 13257432, 13117470 : problèmes d'affichage sur les périphériques client Ubuntu	32
3.1.15. 13360596 : problème d'authentification directe avec Oracle VDI	33
3.1.16. 13971245 : problèmes de retrait des packages dans Oracle Solaris 11	33
3.1.17. 14026511 : échec des connexions du courtier VDI après une mise à niveau d'Oracle VDI	34
3.1.18. 14021467 : problème de sélection de la langue sur le bureau Web	34
3.1.19. 14085800 : problème de gestion de l'ancien mot de passe d'Active Directory	35
3.1.20. 14147506 : échec de la résilience de groupe en cas de modification du serveur principal	35
3.1.21. 14221098 : échec du démarrage de l'application Konsole sur Oracle Linux	35
3.1.22. 14237565 : problème de taille de page lors de l'impression sur les périphériques client non Windows	36
3.1.23. 14287570 : applications Microsoft Windows Server 2003 limitées à une profondeur de couleur de 8 bits pour les résolutions grand écran	36
3.1.24. 14287730 : messages d'erreur X lors de la reproduction à partir de la ligne de commande	36
3.1.25. 14404371 : les caractères saisis par l'utilisateur dans la boîte de dialogue d'authentification sont illisibles	37
3.1.26. 14408025 : fermeture inattendue du client SGD sur Ubuntu Linux	37
3.1.27. 14472019 : SGD ne démarre pas au démarrage du système	37
3.2. Résolution de bogues dans la version 4.70	37
3.3. Problèmes détectés dans la documentation de la version 4.70	46
3.3.1. Problèmes détectés dans la documentation du courtier VDI hérité	46
3.4. Envoi de commentaires et signalement des problèmes	46
3.4.1. Communication avec le support spécialisé Oracle	47

Préface

Les *Oracle Secure Global Desktop Prise en charge des plates-formes et notes de version relatives à la version 4.7* fournissent des informations relatives à la configuration système requise, au support ainsi qu'aux nouvelles fonctionnalités et modifications de cette version d'Oracle Secure Global Desktop (SGD). Ce document est destiné aux administrateurs système.

1. Public

Ce document s'adresse aux personnes qui utilisent SGD 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 :

- Le [Chapitre 1, Nouvelles fonctionnalités et modifications](#) décrit les nouvelles fonctionnalités et modifications de cette version de Oracle Secure Global Desktop.
- Le [Chapitre 2, Configuration système requise et compatibilité](#) inclut les détails relatifs à la configuration système requise et aux plates-formes prises en charge pour cette version de Oracle Secure Global Desktop.
- Le [Chapitre 3, Problèmes connus, résolution de bogues et problèmes détectés dans la documentation](#) contient des informations relatives aux problèmes connus, correctifs et problèmes détectés dans la documentation pour cette version de Oracle Secure Global Desktop. Des informations sur l'envoi de commentaires et le signalement de bogues sont également fournies.

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 d'administration d'Oracle Secure Global Desktop Gateway version 4.7*
- *Guide de l'utilisateur d'Oracle Secure Global Desktop 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.
<i>italique</i>	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.
<code>Largeur fixe</code>	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. Nouvelles fonctionnalités et modifications

Ce chapitre décrit les nouvelles fonctionnalités et modifications de la version 4.70 de Oracle Secure Global Desktop (SGD).

1.1. Nouvelles fonctionnalités de la version 4.70

Cette section décrit les nouvelles fonctionnalités de la version 4.70 de SGD.

1.1.1. Installation sécurisée par défaut

Dans les versions précédentes de SGD, les connexions aux serveurs SGD ont été sécurisées comme une tâche de postinstallation. Dans cette version, les connexions au serveur SGD peuvent être sécurisées pendant l'installation. Il s'agit d'une installation en *mode sécurisé*.

L'installation en mode sécurisé utilise la commande `tarantella security enable` pour configurer et activer automatiquement les services de sécurité SGD. Au cours de l'installation, les utilisateurs peuvent choisir d'utiliser leurs propres certificats SSL (Secure Sockets Layer) pour sécuriser les connexions.

L'installation en mode sécurisé permet également de sécuriser les communications intragroupes pour le serveur SGD. Les connexions entre les serveurs SGD d'un groupe sont donc chiffrées.

L'installation de SGD sans utiliser des connexions sécurisées est toujours possible.

Reportez-vous à [Installation de SGD](#) pour plus d'informations sur l'installation en mode sécurisé.

1.1.2. Nouvelle implémentation du serveur X

Cette version intègre une nouvelle implémentation du moteur de protocoles X, en fonction de la version X11R7.6 du serveur X.Org Foundation.

Cette nouvelle implémentation offre une meilleure prise en charge des moniteurs multiples et du redimensionnement des sessions dynamiques. Ces fonctions sont activées grâce à l'utilisation des extensions RANDR et XINERAMA X.

De nouveaux attributs ont été introduits pour la configuration de la prise en charge de l'extension RANDR. L'attribut de l'extension RandR (`--array-xrandr-enabled`) active la prise en charge RANDR du groupe. L'option Taille de la fenêtre : Extension RandR (`--xrandr`) active la prise en charge RANDR pour un objet d'application.

SGD prend désormais en charge l'extension X de clavier (XKB). L'utilisation de XKB améliore la prise en charge de la globalisation, en fournissant une prise en charge intégrée de plusieurs environnements linguistiques. La configuration des claviers hérités et la configuration côté serveur ne sont plus requises pour traiter la saisie au clavier pour les applications X.

Reportez-vous à [Using the RANDR X Extension](#) pour plus d'informations sur la configuration des applications utilisant ces nouvelles fonctions.

1.1.3. Enregistrement audio pour les applications Windows

Cette version prend en charge l'enregistrement audio dans les applications Windows affichées via SGD.

L'attribut Entrée audio (`--array-audioin`) a été introduit pour activer l'entrée audio pour un groupe SGD.

Reportez-vous à [Enabling SGD Audio Services](#) pour plus d'informations sur la configuration de l'enregistrement audio pour les applications Windows.

1.1.4. Prise en charge de l'authentification au niveau du réseau pour les applications Windows

Cette version prend en charge l'authentification au niveau du réseau (NLA) à l'aide de CredSSP, pour l'authentification des utilisateurs de l'application Windows. L'utilisation de NLA permet aux utilisateurs de s'authentifier avant d'établir une session sur le serveur d'applications Windows.

L'attribut de sécurité réseau améliorée (`--enhancednetworksecurity`) a été introduit pour configurer NLA pour les applications Windows. Cet attribut est activé par défaut.

1.1.5. Nouveau courtier de serveur virtuel pour Oracle VDI

Pour offrir une meilleure intégration aux déploiements d'Oracle Virtual Desktop Infrastructure (VDI), un nouveau courtier de serveur virtuel a été introduit. Le nouveau courtier peut être utilisé avec la version 3.3 d'Oracle VDI et supérieures.

Le nouveau courtier utilise l'API des services Web d'Oracle VDI pour authentifier l'utilisateur, obtenir la liste des bureaux ainsi que démarrer et arrêter le bureau. Avec ce courtier, SGD et Oracle VDI peuvent être installés sur différents hôtes.

Ce nouveau courtier porte le nom de *courtier VDI*. Le courtier actuel pour les installations héritées Oracle VDI portait jusqu'à présent le nom de courtier VDI, et a été renommé dans cette version *Courtier VDI hérité*.

Le tableau suivant indique la compatibilité du courtier avec les versions d'Oracle VDI.

Tableau 1.1. Courtiers utilisés avec Oracle VDI

Nom du courtier	Version d'Oracle VDI
Courtier VDI	3.3.2 et 3.4.1
Courtier VDI hérité	3.2

Le courtier VDI offre d'autres fonctionnalités, telles que la prise en charge d'un hôte dédié au truststore de certificats, l'équilibrage de charge hôte et les délais d'expiration.

Reportez-vous à [VDI Broker](#) pour plus d'informations sur la configuration et l'utilisation du courtier VDI.

Reportez-vous à [Section 3.3.1, « Problèmes détectés dans la documentation du courtier VDI hérité »](#) pour plus d'informations sur les problèmes détectés dans la documentation relative au courtier VDI hérité.

1.2. Modifications dans la version 4.70

Cette section décrit les modifications apportées à la version 4.60 de SGD.

1.2.1. Modifications de l'installation du client SGD

Les modifications suivantes ont été apportées à l'installation du client SGD.

- **Installation automatique** Les répertoires d'installation par défaut ont été modifiés.

Reportez-vous à [Automatic Installation of the SGD Client](#) pour plus d'informations sur les modifications.

- **Installation manuelle.** Pour assurer la prise en charge des systèmes de fichiers partagés, les administrateurs peuvent à présent installer le client SGD à un emplacement pour l'ensemble du système.

SGD conserve une trace de l'emplacement de tous les clients SGD que vous avez installés manuellement.

L'installation manuelle est désormais prise en charge sur les plates-formes Mac OS X.

Les emplacements des fichiers par défaut ont été modifiés. Sur les plates-formes Windows, les sorties sont journalisées dans le dossier des données d'application de l'utilisateur. Sur les plates-formes UNIX, Linux et Mac OS X, les sorties sont désormais consignées au même emplacement que le journal du système.

1.2.2. Modifications de la méthode de connexion par défaut

L'attribut Méthode de connexion (`--method`) spécifie le mécanisme utilisé par le serveur SGD pour accéder à un serveur d'applications et démarrer une application.

Le paramètre de méthode de connexion par défaut est passé de `telnet` à `ssh`.

Le paramètre `rexec` n'est plus disponible.

1.2.3. Nouveaux paramètres du courtier SGD définis par l'utilisateur

Des nouveaux paramètres activant la configuration de la page de sélection ont été introduits pour le courtier SGD défini par l'utilisateur. Le courtier SGD défini par l'utilisateur est utilisé avec la fonctionnalité de lancement dynamique de SGD pour permettre aux utilisateurs de sélectionner ou d'indiquer le serveur d'applications au démarrage d'une application.

Les nouveaux paramètres sont les suivants :

- `hideAppservers`. La liste des serveurs d'applications n'est pas affichée dans la page de sélection.
- `checkAppserver`. Pour les serveurs d'applications spécifiés par l'utilisateur, SGD vérifie que le serveur d'applications a été affecté à l'objet d'application. Si le serveur d'applications n'est pas affecté à l'objet d'application, un message d'erreur s'affiche.

1.2.4. Le lancement local n'est plus pris en charge

L'exécution d'une application sur les périphériques client Windows (le "lancement local") n'est plus prise en charge. L'attribut Local Client Launch (`--trylocal`) a été abandonné.

Le paramètre Serveur X local (`localx`) ne prend plus en charge l'attribut Type de fenêtre (`--displayusing`).

Le paramètre de profil Rechercher le serveur X local n'est plus disponible.

1.2.5. Pool de licence d'accès client retiré

Les CAL (Client Access Licenses) pour les autres périphériques client non Windows ne sont plus stockées dans un pool de licences sur le serveur SGD. Les CAL sont maintenant stockées à un emplacement situé sur le périphérique client.

La commande `tarantella tscal` de gestion du pool de licences n'est plus disponible.



Note

Lorsque vous mettez à niveau un serveur SGD, toutes les CAL stockées dans le pool de licences sont retirées. Les périphériques client non Windows peuvent utiliser des CAL temporaires émises par l'hôte Hôte de session Remote Desktop jusqu'à ce que les CAL correctes soient stockées sur le périphérique.

Reportez-vous à la documentation Microsoft Services Remote Desktop pour plus d'informations sur la gestion des CAL.

1.2.6. Modifications des attributs d'affichage des objets d'application

En raison de la nouvelle implémentation XPE introduite dans cette version, les attributs d'affichage suivants ne sont plus pris en charge :

- Base de données RVB (`--xpe-rgbdatabase`). XPE prend désormais en charge les noms de couleurs X11.
- Symbole de l'euro (`--euro`). Le symbole de l'euro est désormais pris en charge par défaut.
- Configuration du clavier : Verrouillé (`--lockkeymap`).
- Configuration du clavier (`--xpe-keymap`). L'extension XKB est désormais utilisée pour les configurations du clavier.
- Configuration du clavier (`--keymap`). L'extension XKB est désormais utilisée pour les configurations du clavier.

1.2.7. Fonctionnalités retirées de cette version

Reportez-vous à [Section 2.5, « Fonctionnalités retirées »](#) pour obtenir la liste des fonctionnalités retirées dans la version 4.70.

1.2.8. Modifications dans la documentation

Les modifications suivantes ont été apportées à la documentation dans cette version :

- **Guide de sécurité.** Un nouveau manuel, *Oracle Secure Global Desktop Security Guide for Release 4.7*, a été introduit pour aider les administrateurs à déployer SGD en toute sécurité.
- **Documentation traduite.** La documentation traduite est désormais disponible dans les langues suivantes :
 - Français
 - Japonais
 - Chinois (simplifié)

1.2.9. Modifications apportées aux environnements linguistiques pris en charge

Pour cette version, le client et le bureau Web SGD sont disponibles dans les langues prises en charge suivantes :

- Anglais

- Français
- Allemand
- Italien
- Japonais
- Coréen
- Portugais (Brésil)
- Espagnol
- Chinois (simplifié)
- Chinois (traditionnel)

Chapitre 2. Configuration système requise et compatibilité

Ce chapitre inclut des informations relatives à la configuration système requise et aux plates-formes prises en charge par Oracle Secure Global Desktop (SGD) version 4.70.

2.1. Serveur SGD : configuration requise et compatibilité

Cette section décrit les plates-formes prises en charge et la configuration requise pour installer des serveurs SGD.

2.1.1. Configuration matérielle requise pour SGD

Les indications de configuration matérielle suivantes sont fournies à titre indicatif et non restrictif. Pour obtenir une aide supplémentaire au sujet de la configuration matérielle requise, contactez un [bureau des ventes Oracle](#).

Le calcul de la configuration requise pour un serveur hébergeant SGD doit prendre en compte l'intégralité des points suivants :

- Configuration nécessaire pour installer et exécuter SGD
- Configuration nécessaire pour chaque utilisateur qui se connecte à SGD sur l'hôte et exécute des applications

La configuration suivante est requise pour l'installation et l'exécution de SGD :

- 2 Go d'espace disque libre
- 2 Go de RAM
- Processeur 1 GHz
- Carte d'interface réseau

Ces éléments viennent *s'ajouter* à la configuration nécessaire pour le système d'exploitation lui-même et supposent que l'utilisation du serveur est dédiée à SGD.

La configuration suivante est requise pour prendre en charge les utilisateurs qui se connectent à SGD et exécutent des applications :

- 50 Mo minimum pour chaque utilisateur
- 50 MHz pour chaque utilisateur



Attention

La configuration réelle requise pour la CPU et la mémoire varie considérablement selon les applications utilisées.

2.1.2. Plates-formes d'installation prises en charge par SGD

Le tableau suivant répertorie les plates-formes d'installation prises en charge par SGD.

Système d'exploitation	Versions prises en charge
Oracle Solaris sur plates-formes SPARC	Solaris 10 8/11 (mise à jour 10)

Système d'exploitation	Versions prises en charge
	Solaris 11 Solaris 10 8/11 (mise à jour 10) Trusted Extensions Solaris 11 Trusted Extensions
Oracle Solaris sur plates-formes x86	Solaris 10 8/11 (mise à jour 10) Solaris 11 Solaris 10 8/11 (mise à jour 10) Trusted Extensions Solaris 11 Trusted Extensions
Oracle Linux (32 bits et 64 bits)	5.7 5.8 6.2 6.3

Les produits Oracle certifiés sur Oracle Linux sont également certifiés et pris en charge sur Red Hat Enterprise Linux en raison de la compatibilité implicite entre les deux distributions. Oracle n'exécute pas de test supplémentaire sur les produits Red Hat Enterprise Linux.

2.1.2.1. Modifications du système d'exploitation

Vous pouvez être amené à apporter des modifications aux systèmes d'exploitation. Sans ces modifications, il est possible que SGD ne s'installe pas correctement ou ne fonctionne pas correctement.

2.1.2.1.1. Oracle Solaris

Pour les plates-formes Oracle Solaris, voici les modifications qu'il peut être nécessaire d'apporter aux systèmes d'exploitation :

- Vous devez installer au minimum la distribution Oracle Solaris utilisateur final afin d'obtenir les bibliothèques nécessaires à SGD. Sans cela, SGD ne peut pas être installé.
- La fonction TCP Fusion d'Oracle Solaris risque de poser des problèmes avec certaines connexions de socket locales utilisées par SGD. Désactivez la fonction TCP Fusion avant d'installer SGD, comme suit :

1. Ajoutez la ligne suivante à la fin du fichier `/etc/system`.

```
set ip:do_tcp_fusion = 0x0
```

2. Redémarrez le serveur.

- Sur les plates-formes Oracle Solaris 11, SGD affecte des privilèges d'administration à la première entrée du fichier `/etc/user_attr` qui possède l'attribut `roles=root`. Assurez-vous de connaître les données d'identification de cet utilisateur Oracle Solaris.

Après l'installation, l'administrateur SGD peut être configuré à l'aide de la commande suivante :

```
# tarantella object edit --name "o=Tarantella System Objects/cn=Administrator" \
--user user-name --surname family-name
```

2.1.2.1.2. Oracle Linux

Pour les plates-formes Oracle Linux, voici les modifications qu'il peut falloir apporter aux systèmes d'exploitation :

- Le fichier `/etc/hosts` pour Oracle Linux contient une seule entrée, qui fait correspondre à tort le nom d'hôte de l'hôte SGD à l'adresse loopback locale, `127.0.0.1`.

Modifiez le fichier `/etc/hosts` de sorte à retirer ce mappage et ajoutez une entrée qui mappe le nom de l'hôte SGD à l'adresse IP réseau de l'hôte SGD. Le nom d'hôte de SGD ne doit pas être mappé à l'adresse IP de loopback locale.

- Lors de l'installation sur les plates-formes Oracle Linux 6, choisissez le groupe de paquetages Desktop ou Software Development Workstation. Cela permet de s'assurer que les paquetages requis pour le bureau Web SGD par défaut sont installés. Les paquetages requis incluent des outils d'administration graphiques et des clients X tels que `xterm` et `gnome-terminal`.

Vous pouvez également choisir un autre groupe de paquetages lors de l'installation et sélectionnez l'option Personnaliser maintenant pour ajouter les paquetages requis dans la catégorie Environnements de bureau.

2.1.2.1.3. Applications 5250 et 3270

Les modifications suivantes sont nécessaires à la prise en charge des applications 5250 et 3270 :

- **Plates-formes Linux.** La bibliothèque `libXm.so.3` est requise. Cette bibliothèque est disponible dans le paquetage OpenMotif 2.2.
- **Plates-formes Solaris 11.** Installez le paquetage `motif` comme suit :

```
# pkg install motif
```

2.1.2.2. Prise en charge de la virtualisation

Les plates-formes d'installation de SGD sont prises en charge sur un hyperviseur Type 1 (sans système d'exploitation) ou un hyperviseur Type 2 (hébergé), par exemple Oracle VM VirtualBox, VMWare ou Oracle VM Server pour SPARC (anciennement connu sous le nom Sun Logical Domains ou LDoms).

L'installation dans les zones est prise en charge pour les plates-formes Oracle Solaris. SGD peut être installé dans la zone globale ou dans une ou plusieurs zones non globales. L'installation aussi bien dans la zone globale que dans une zone non globale n'est pas prise en charge.

Sur les plates-formes Oracle Solaris Trusted Extensions, vous devez installer SGD dans une zone étiquetée. N'installez pas SGD dans la zone globale.

2.1.2.3. Déclassés des plates-formes d'installation SGD prises en charge

Le tableau suivant répertorie les plates-formes d'installation SGD qui ont été déclassées.

Version de SGD	Plates-formes qui ne sont plus prises en charge
4.70	Red Hat Enterprise Linux 5.5 et 5.6
	Oracle Enterprise Linux 5.5 et 5.6
	D'Oracle Solaris 10 jusqu'à Solaris 10 9/10 (mise à jour 9) compris
4.60	OpenSolaris (toutes versions)

Version de SGD	Plates-formes qui ne sont plus prises en charge
	Red Hat Enterprise Linux version 5.0 à 5.4
	De l'O/S Solaris 10 jusqu'à Solaris 10 5/09 (mise à jour 7) compris
	SUSE Linux Enterprise Server 10

2.1.3. Chemins de mise à niveau pris en charge

Les mises à niveau vers la version 4.70 de SGD sont uniquement prises en charge à partir des versions suivantes :

- Oracle Secure Global Desktop Software version 4.62.913
- Oracle Secure Global Desktop Software version 4.61.915
- Oracle Secure Global Desktop Software version 4.60.911

Si vous souhaitez effectuer une mise à niveau à partir d'une autre version de SGD, contactez le support Oracle.

2.1.4. Version de la technologie Java

Le tableau suivant indique les versions JDK fournies avec SGD.

Version de SGD	Version de JDK
4.70	1.6.0_33
4.62	1.6.0_29
4.61	1.6.0_24
4.60	1.6.0_21

2.1.5. Utilisateurs et privilèges requis

Pour installer SGD, vous devez disposer des privilèges superutilisateur (root).

Le système doit compter des utilisateurs `ttaserv` et `ttasys` et un groupe `ttaserv` avant que SGD puisse être installé.

L'utilisateur `ttasys` possède tous les fichiers et les processus utilisés par le serveur SGD. L'utilisateur `ttaserv` possède tous les fichiers et les processus utilisés par le serveur Web SGD.

L'exécution du serveur SGD ne nécessite pas de privilèges superutilisateur (root). Le serveur SGD démarre avec le compte utilisateur root avant de passer au compte utilisateur `ttasys`.

Si vous tentez d'installer le logiciel alors que les utilisateurs et le groupe requis ne sont pas mis en place, le programme d'installation s'interrompt. Aucune modification n'est apportée au système et un message indique la procédure à suivre. Le message indique les informations détaillées d'un script d'installation que vous pouvez exécuter pour créer les utilisateurs et le groupe requis.

Si vous devez créer manuellement les utilisateurs et le groupe requis, voici les conditions nécessaires :

- Les noms d'utilisateur doivent être `ttaserv` et `ttasys`.
- Le nom de groupe doit être `ttaserv`.

- Vous pouvez utiliser n'importe quel numéro d'identification utilisateur (**UID**) ou ID de groupe (**GID**). Les numéros **UID** et **GID** peuvent être différents.
- Le groupe **ttaserv** doit constituer le groupe principal des deux utilisateurs.
- Les deux utilisateurs doivent posséder un shell valide, par exemple **/bin/sh**.
- Les deux utilisateurs doivent posséder un répertoire personnel *inscriptible*.
- Pour des raisons de sécurité, verrouillez ces comptes, par exemple à l'aide de la commande **passwd -l**.

Créez ces utilisateurs à l'aide des commandes **useradd** et **groupadd**. Par exemple :

```
# groupadd ttaserv
# useradd -g ttaserv -s /bin/sh -d /home/ttasy -m ttasy
# useradd -g ttaserv -s /bin/sh -d /home/ttaserv -m ttaserv
# passwd -l ttasy
# passwd -l ttaserv
```

Pour vérifier si les comptes utilisateur **ttasy** et **ttaserv** sont correctement configurés sur votre système, exécutez les commandes suivantes.

```
# su ttasy -c "/usr/bin/id -a"
# su ttaserv -c "/usr/bin/id -a"
```

Si le système est configuré correctement, la sortie de la commande doit être proche des exemples suivants :

```
uid=1002(ttaserv) gid=1000(ttaserv) groups=1000(ttaserv)
uid=1003(ttasy) gid=1000(ttaserv) groups=1000(ttaserv)
```

2.1.6. Configuration réseau requise

Vous devez configurer votre réseau en vue d'une utilisation avec SGD. Voici les principaux éléments de la configuration requise :

- Les hôtes doivent disposer d'entrées DNS (Domain Name System) pouvant être résolues par chacun des clients.
- Les recherches DNS et les recherches inverses d'un hôte ne doivent jamais échouer.
- Tous les périphériques client doivent utiliser DNS.
- Lors de l'installation de SGD, une invite vous demande le nom DNS à utiliser pour le serveur SGD. Le nom DNS doit répondre aux exigences suivantes :
 - Dans un réseau comprenant un pare-feu, utilisez le nom DNS sous lequel l'hôte SGD est connu à l'intérieur du pare-feu.
 - Veillez à toujours utiliser des noms DNS complets pour l'hôte SGD. Par exemple, **boston.example.com**.

Le manuel *Oracle Secure Global Desktop Administration Guide for Release 4.7* possède des informations détaillées sur les ports utilisés par SGD et sur le fonctionnement de SGD avec des pare-feu. La liste ci-dessous répertorie les ports les plus couramment utilisés.

Les périphériques client doivent pouvoir établir des connexions TCP/IP (Transmission Control Protocol/Internet Protocol) avec SGD sur les ports TCP suivants :

- **80** - Pour les connexions HTTP entre des périphériques client et le serveur Web SGD. Le numéro de port peut varier selon le choix effectué lors de l'installation.
- **443** - Pour les connexions HTTPS (HTTP over Secure Sockets Layer) entre des périphériques client et le serveur Web SGD.
- **3144** - Pour les connexions standard (non chiffrées) entre le client SGD et le serveur SGD.
- **5307** - Pour les connexions sécurisées entre le client SGD et le serveur SGD. Les connexions sécurisées utilisent le chiffrement SSL (Secure Sockets Layer).



Note

Pour une installation par défaut en mode sécurisé dans laquelle vous activez les services de sécurité SGD et utilisez le protocole HTTPS, seuls les ports 443 et 5307 doivent être ouverts dans le pare-feu.

Pour une installation en mode standard dans laquelle les connexions ne sont pas sécurisées, les ports 80, 3144 et 5307 doivent être ouverts dans le pare-feu. En effet, le client SGD établit initialement une connexion sécurisée sur le port 5307. Une fois la connexion établie, celle-ci redevient une connexion standard sur le port 3144.

Pour exécuter des applications, SGD doit pouvoir établir des connexions TCP/IP avec les serveurs d'applications. Le type d'application à exécuter détermine quel port TCP ouvrir, par exemple :

- **22** – Pour les applications X et à traitement de caractère qui utilisent le protocole SSH (Secure Shell)
- **23** – Pour les applications Windows, X et à traitement de caractère qui utilisent Telnet
- **3389** – Pour les applications Windows qui utilisent Windows Services Remote Desktop
- **6010** et au-delà – Pour les applications X

2.1.7. Synchronisation d'horloge

Dans SGD, un groupe se définit comme un ensemble de serveurs SGD qui partagent des informations de configuration. Etant donné que les serveurs SGD d'un groupe partagent les informations relatives aux sessions utilisateur et aux sessions d'application, il est important de synchroniser les horloges des hôtes SGD. Pour vérifier que les horloges de tous les hôtes SGD sont synchronisées, utilisez le logiciel Network Time Protocol (NTP) ou la commande `rdate`.

2.1.8. Serveur Web SGD

Le serveur Web SGD est composé d'un serveur Web Apache et d'un conteneur de technologie JavaServer Pages (JSP) Tomcat préconfiguré pour être utilisé avec SGD.

Le serveur Web SGD est composé de plusieurs éléments. Le tableau suivant répertorie les versions des composants du serveur Web correspondant aux éditions récentes de SGD.

Nom du composant	Version de SGD 4.70	Version de SGD 4.62	Version de SGD 4.61	Version de SGD 4.60
Serveur HTTP Apache	2.2.22	2.2.21	2.2.17	2.2.16
OpenSSL	1.0.0.j	1.0.0.e	1.0.0.d	1.0.0a

Nom du composant	Version de SGD 4.70	Version de SGD 4.62	Version de SGD 4.61	Version de SGD 4.60
<code>mod_jk</code>	1.2.37	1.2.32	1.2.31	1.2.27
Apache Jakarta Tomcat	7.0.29	6.0.33	6.0.32	6.0.29
Apache Axis	1.4	1.4	1.4	1.4

Le serveur Web Apache comprend tous les modules Apache standard sous forme d'objets partagés.

La taille minimale du segment de mémoire logicielle de JVM (Java Virtual Machine) du conteneur de technologie JSP Tomcat est de 256 méga-octets.

2.1.9. Mécanismes d'authentification pris en charge

Les mécanismes suivants sont pris en charge pour l'authentification d'utilisateurs dans SGD :

- LDAP (Lightweight Directory Access Protocol) version 3
- Microsoft Active Directory
- NIS (Network Information Service)
- RSA SecurID
- Authentification du serveur Web (authentification de base HTTP/HTTPS), y compris les certificats client PKI (Public Key Infrastructure)

2.1.9.1. Versions prises en charge d'Active Directory

L'authentification Active Directory et l'authentification LDAP sont prises en charge dans les versions suivantes d'Active Directory :

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

2.1.9.2. Annuaire LDAP pris en charge

SGD prend en charge la version 3 du protocole LDAP standard. Vous pouvez utiliser l'authentification LDAP avec n'importe quel serveur d'annuaire compatible avec LDAP version 3. Toutefois, SGD prend uniquement en charge les serveurs d'annuaire suivants :

- Oracle Internet Directory 11gR1 (toutes les éditions 11.1.1.x.0)
- Oracle Directory Server Enterprise Edition version 11gR1
- Microsoft Active Directory, comme indiqué dans la section [Section 2.1.9.1, « Versions prises en charge d'Active Directory »](#)
- Sun Directory Server version 6.3 ou ultérieure

Il est possible que d'autres serveurs d'annuaire fonctionnent sans être officiellement pris en charge.

Novell eDirectory ne fait plus partie des serveurs d'annuaire LDAP pris en charge.

2.1.9.3. Versions prises en charge de SecurID

SGD fonctionne avec les versions 4, 5, 6 et 7 de RSA Authentication Manager (anciennement connu sous le nom ACE/Server).

SGD prend en charge les codes PIN générés par le système et les codes PIN créés par l'utilisateur.

2.1.10. Prise en charge du chiffrement SSL

SGD prend en charge TLS version 1.0 et SSL version 3.0.

SGD prend en charge les certificats X.509 codés en base 64 PEM (Privacy Enhanced Mail). Ces certificats possèdent la structure suivante :

```
-----BEGIN CERTIFICATE-----  
...certificate...  
-----END CERTIFICATE-----
```

SGD prend en charge l'extension Autre nom de l'objet ([subjectAltName](#)) pour les certificats SSL. SGD prend également en charge l'utilisation du caractère générique * dans la première partie du nom de domaine, par exemple *.[example.com](#).

SGD inclut la prise en charge de plusieurs autorités de certification (AC). Le fichier [/opt/tarantella/etc/data/cacerts.txt](#) contient les noms distinctifs (DN) X.500 et les signatures MD5 de tous les certificats AC pris en charge par SGD. Un paramétrage supplémentaire est requis pour assurer la prise en charge des certificats SSL signés par une autorité de certification non prise en charge. Les AC intermédiaires sont prises en charge, mais des étapes de configuration supplémentaires peuvent être nécessaires si l'un des certificats de la chaîne est signé par une AC non prise en charge.

SGD prend en charge l'utilisation des accélérateurs SSL matériels externes à l'aide de paramétrages appropriés.

SGD prend en charge les suites de chiffrement suivantes :

- RSA_WITH_AES_256_CBC_SHA
- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_3DES_EDE_CBC_SHA
- RSA_WITH_RC4_128_SHA
- RSA_WITH_RC4_128_MD5
- RSA_WITH_DES_CBC_SHA

2.1.11. Prise en charge de l'impression

SGD prend en charge deux types d'impression : l'impression PDF et l'impression Printer-Direct.

Pour l'impression PDF, SGD utilise [Ghostscript](#) pour convertir les travaux d'impression en fichiers PDF (Portable Document Format). Votre distribution Ghostscript doit inclure le programme [ps2pdf](#). Pour de meilleurs résultats, installez la dernière version de Ghostscript sur l'hôte SGD.

SGD prend en charge l'impression Printer-Direct sur les imprimantes PostScript, PCL (Printer Command Language) et texte seul connectées au périphérique client de l'utilisateur. Le script SGD `tta_print_converter` effectue toutes les conversions nécessaires en vue de formater les travaux d'impression correctement pour l'imprimante client. Le script `tta_print_converter` utilise Ghostscript pour convertir du format Postscript à PCL. Pour prendre en charge cette conversion, Ghostscript doit être installé sur le serveur SGD. Pour de meilleurs résultats, téléchargez et installez des polices supplémentaires.

Ghostscript n'est pas inclus dans le logiciel SGD.

2.2. Périphériques client : configuration requise et compatibilité

Cette section décrit les plates-formes prises en charge et la configuration requise pour les périphériques client.

2.2.1. Plates-formes client prises en charge

Le tableau suivant répertorie les plates-formes client et les navigateurs pris en charge par le client SGD.



Attention

La plate-forme du client SGD doit être un système d'exploitation de bureau. Une application individuelle, tel qu'un navigateur, ne constitue pas une plate-forme client prise en charge.

Plates-formes client prises en charge	Navigateurs pris en charge
Microsoft Windows 7 (32 bits et 64 bits) ^a	Internet Explorer 8 Internet Explorer 9 Mozilla Firefox 3.6, 10.0.3:ESR, 11 Chrome 17
Microsoft Windows XP Professionnel SP3 (32 bits)	Internet Explorer 7 Internet Explorer 8 Mozilla Firefox 3.6, 10.0.3:ESR, 11 Chrome 17
Oracle Solaris sur plates-formes SPARC	Mozilla Firefox 3.6, 10.0.3:ESR, 11
Solaris 10 8/11 (mise à jour 10), Solaris 11	Chrome 17
Oracle Solaris sur plates-formes x86	Mozilla Firefox 3.6, 10.0.3:ESR, 11
Solaris 10 8/11 (mise à jour 10), Solaris 11	Chrome 17
Oracle Solaris Trusted Extensions sur plates-formes SPARC	Mozilla Firefox 3.6, 10.0.3:ESR, 11
Solaris 10 8/11 (mise à jour 10), Solaris 11	Chrome 17
Oracle Solaris Trusted Extensions sur plates-formes x86	Mozilla Firefox 3.6, 10.0.3:ESR, 11
Solaris 10 8/11 (mise à jour 10), Solaris 11	Chrome 17

Plates-formes client prises en charge	Navigateurs pris en charge
Mac OS X 10.6 (version la plus récente) et 10.7 ^b	Safari 5 Mozilla Firefox 3.6, 10.0.3:ESR, 11 Chrome 17
Oracle Linux 5.7, 5.8, 6.2 et 6.3 (32 bits et 64 bits)	Mozilla Firefox 3.6, 10.0.3:ESR, 11 Chrome 17
Ubuntu 10.04, 12.04 (32 bits et 64 bits)	Mozilla Firefox 3.6, 10.0.3:ESR, 11 Chrome 17

^a Sur les plates-formes client 64 bits, les versions 32 bits et 64 bits d'Internet Explorer sont prises en charge.

^b Mac OS X 10.8 ne fait pas partie des plates-formes client prises en charge.

Les produits Oracle certifiés sur Oracle Linux sont également certifiés et pris en charge sur Red Hat Enterprise Linux en raison de la compatibilité implicite entre les deux distributions. Oracle n'exécute pas de test supplémentaire sur les produits Red Hat Enterprise Linux.

La console d'administration SGD n'est pas prise en charge sur les navigateurs Safari.

Les versions bêta et les versions préliminaires des navigateurs ne sont pas prises en charge.

Le langage de programmation JavaScript doit être activé dans les navigateurs.

Pour prendre en charge les fonctions suivantes, les navigateurs doivent disposer de la technologie Java :

- Téléchargement et installation automatiques du client SGD
- Recherche des paramètres de serveur proxy à partir du navigateur par défaut de l'utilisateur

Si la technologie Java n'est pas disponible, le client SGD peut être téléchargé et installé manuellement. L'installation manuelle est disponible sur toutes les plates-formes client prises en charge.

Seul le logiciel Java Plug-in version 1.6 est pris en charge en tant que plug-in de technologie Java.



Attention

En raison de problèmes connus, le logiciel Java Plug-in version 1.7 n'est pas pris en charge dans cette édition. Assurez-vous que les problèmes que vous signalez au support Oracle sont reproductibles avec le logiciel Java Plug-in version 1.6.

Pour des résultats optimaux, configurez les périphériques client sur le paramètre Milliers de couleurs au minimum.

Le client SGD et son bureau Web sont disponibles dans les langues suivantes :

- Anglais
- Français
- Allemand
- Italien
- Japonais

- Coréen
- Portugais (Brésil)
- Espagnol
- Chinois (simplifié)
- Chinois (traditionnel)

2.2.1.1. Prise en charge de la virtualisation

Les plates-formes client de SGD sont prises en charge sur un hyperviseur Type 1 (sans système d'exploitation) ou un hyperviseur Type 2 (hébergé), par exemple Oracle VM VirtualBox, VMWare ou Oracle VM Server pour SPARC (anciennement connu sous le nom Sun Logical Domains ou LDOMs).

2.2.1.2. Déclassissements des plates-formes client prises en charge

Le tableau suivant présente les plates-formes d'installation SGD, les navigateurs et les outils Java Plugin qui ont fait l'objet d'un déclassissement.

Version de SGD	Plates-formes qui ne sont plus prises en charge
4.70	<p>Microsoft Windows Vista</p> <p>Red Hat Enterprise Linux 5.5 Desktop</p> <p>D'Oracle Solaris 10 jusqu'à Solaris 10 9/10 (mise à jour 9) compris</p> <p>Safari 4</p>
4.60	<p>Mac OS X 10.5</p> <p>OpenSolaris (toutes versions)</p> <p>Red Hat Enterprise Linux Desktop 5.0 à 5.4</p> <p>De l'O/S Solaris 10 jusqu'à Solaris 10 5/09 (mise à jour 7) compris</p> <p>Ubuntu 8</p> <p>Firefox 2</p> <p>Internet Explorer 6</p> <p>Safari 2</p> <p>Safari 3</p> <p>Outil Java Plugin version 1.5</p>

2.2.2. Serveurs proxy pris en charge

Pour vous connecter à SGD, via un serveur proxy, celui-ci doit prendre en charge la mise en tunnel. Vous pouvez utiliser des serveurs proxy HTTP, Secure (SSL) ou SOCKS version 5.

Dans le cas de serveurs proxy SOCKS version 5, SGD prend en charge les méthodes de type Authentification de base et Aucune authentification requise. Aucune configuration côté serveur n'est requise.

2.2.3. Prise en charge de l'impression PDF

Afin de pouvoir utiliser l'impression PDF, il est nécessaire qu'un visionneur PDF soit installée sur le périphérique client. SGD prend en charge les visionneurs PDF suivants par défaut.

Plate-forme client	Visionneur PDF par défaut
Plates-formes Microsoft Windows	Adobe Reader version 4.0. ou supérieure
Oracle Solaris sur plates-formes SPARC	Visionneur PDF de GNOME (gpdf) Adobe Reader (acroread)
Oracle Solaris sur plates-formes x86	Visionneur PDF de GNOME (gpdf)
Oracle Linux	Visionneur PDF de GNOME (gpdf) Visionneur de documents d'Evince (evince) X PDF Reader (xpdf)
Mac OS X	Preview App (/Applications/Preview.app)



Note

Le visionneur de PDF Adobe Reader doit prendre en charge l'option de commande `-openInNewWindow`. Le visionneur de PDF Preview App doit prendre en charge l'option de commande `open -a`.

Pour permettre l'utilisation d'un visionneur de PDF pris en charge, l'application doit être installée sous le chemin [PATH](#) de l'utilisateur.

La prise en charge d'autres visionneurs de PDF peut être configurée dans le profil client de l'utilisateur.

2.2.4. Cartes à puce prises en charge

SGD fonctionne avec n'importe quelle carte à puce et lecteur de cartes compatibles PC/SC (Ordinateur personnel/Carte à puce) et pris en charge par les services Microsoft Remote Desktop.

2.3. Passerelle SGD Gateway : configuration requise et compatibilité

Cette section décrit les plates-formes prises en charge par la passerelle SGD Gateway et la configuration requise pour l'installer.

2.3.1. Plates-formes d'installation prises en charge par la passerelle SGD Gateway

Les plates-formes d'installation prises en charge par l'hôte *SGD Gateway* sont présentées dans le tableau suivant.

Système d'exploitation	Versions prises en charge
Oracle Solaris sur plates-formes SPARC	Solaris 10 8/11 (mise à jour 10) Solaris 11
Oracle Solaris sur plates-formes x86	Solaris 10 8/11 (mise à jour 10)

Système d'exploitation	Versions prises en charge
	Solaris 11
Oracle Linux (32 bits et 64 bits)	5.7
	5.8
	6.2
	6.3

Les produits Oracle certifiés sur Oracle Linux sont également certifiés et pris en charge sur Red Hat Enterprise Linux en raison de la compatibilité implicite entre les deux distributions. Oracle n'exécute pas de test supplémentaire sur les produits Red Hat Enterprise Linux.

Par défaut, la passerelle SGD Gateway est configurée de sorte à prendre en charge un maximum de 100 connexions HTTP simultanées et 512 connexions AIP (Adaptive Internet Protocol) simultanées. La taille de la mémoire JVM est optimisée pour assurer le nombre de connexions défini. L'annexe C du manuel *Guide d'administration d'Oracle Secure Global Desktop Gateway version 4.7* donne des informations sur la définition des paramètres de la passerelle pour un nombre d'utilisateurs donné.

2.3.1.1. Prise en charge de la virtualisation

Les plates-formes d'installation de la passerelle SGD Gateway sont prises en charge sur un hyperviseur Type 1 (sans système d'exploitation) ou un hyperviseur Type 2 (hébergé), par exemple Oracle VM VirtualBox, VMWare ou Oracle VM Server pour SPARC (anciennement connu sous le nom Sun Logical Domains ou LDoms).

Sur les plates-formes Oracle Solaris, l'installation en zones est prise en charge. La passerelle SGD Gateway peut être installée sur la zone globale, ou dans une ou plusieurs zones non globales. L'installation aussi bien dans la zone globale que dans une zone non globale n'est pas prise en charge.

2.3.1.2. Déclassés des plates-formes d'installation prises en charge par la passerelle

Le tableau suivant répertorie les plates-formes d'installation de SGD Gateway qui ont été déclassées.

Version de SGD	Plates-formes qui ne sont plus prises en charge
4.70	D'Oracle Solaris 10 jusqu'à Solaris 10 9/10 (mise à jour 9) compris Red Hat Enterprise Linux 5.5 Oracle Enterprise Linux 5.5
4.60	OpenSolaris (toutes versions) Red Hat Enterprise Linux version 5.0 à 5.4 De l'O/S Solaris 10 jusqu'à Solaris 10 5/09 (mise à jour 7) compris SUSE Linux Enterprise Server 10

2.3.2. Configuration requise des serveurs SGD pour la passerelle SGD Gateway

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. Vous devez activer les connexions sécurisées 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.

- **Version de SGD.** 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 Gateway.
- **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.

2.3.3. Serveur Web Apache

La version du serveur Web Apache fourni avec la passerelle SGD Gateway est 2.2.22. Ce serveur inclut les modules Apache standard pour réaliser les opérations de proxy inverse et d'équilibrage de charge. Les modules sont installés en tant que modules DSO (Dynamic Shared Object).

2.3.4. Version de la technologie Java

La passerelle SGD Gateway inclut Java Runtime Environment (JRE) version 1.6.0_33.

2.3.5. Prise en charge du chiffrement SSL

La prise en charge du chiffrement SSL pour la passerelle SGD Gateway est disponible grâce à l'environnement Java Runtime Environment (JRE) fourni par la passerelle Gateway. Reportez-vous à la [documentation de la plate-forme Java](#) pour plus d'informations.

La passerelle SGD Gateway prend en charge les certificats X.509 codés en base 64 PEM (Privacy Enhanced Mail). Ces certificats possèdent la structure suivante :

```
-----BEGIN CERTIFICATE-----  
...certificate...  
-----END CERTIFICATE-----
```

La passerelle SGD Gateway prend en charge l'utilisation des accélérateurs SSL matériels externes à l'aide de paramétrages appropriés.

Par défaut, la passerelle SGD Gateway est configurée de sorte à prendre en charge les suites de chiffrement haute qualité suivantes pour les connexions SSL :

- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA

- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

Les suites de chiffrement suivantes sont également prises en charge, mais doivent être configurées par l'utilisateur comme indiqué dans le manuel *Guide d'administration d'Oracle Secure Global Desktop Gateway version 4.7*.

- SSL_RSA_WITH_DES_CBC_SHA
- SSL_DHE_RSA_WITH_DES_CBC_SHA
- SSL_DHE_DSS_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA

2.4. Affichage d'applications : configuration requise et compatibilité

Cette section décrit les plates-formes prises en charge et la configuration requise pour afficher des applications via SGD.

2.4.1. Applications prises en charge

Vous pouvez utiliser SGD pour accéder aux types d'application suivants :

- Microsoft Windows
- Applications X s'exécutant sur les serveurs d'applications Oracle Solaris, Linux, HP-UX et AIX
- Applications à traitement de caractère s'exécutant sur les serveurs d'applications Oracle Solaris, Linux, HP-UX et AIX
- Applications s'exécutant sur les systèmes mainframe et AS/400 d'IBM
- Applications Web basées sur le HTML et la technologie Java

SGD prend en charge les protocoles suivants :

- Microsoft RDP (Remote Desktop Protocol) version 5.2 ou supérieure
- X11
- HTTP
- HTTPS
- SSH version 2 ou supérieure
- Telnet VT, ANSI (American National Standards Institute)

- TN3270E
- TN5250

2.4.2. Plates-formes d'installation prises en charge par le module d'enrichissement SGD

Le module d'enrichissement SGD est un composant logiciel pouvant être installé sur un serveur d'applications pour bénéficier des fonctions suivantes lors de l'utilisation des applications affichées via SGD :

- Equilibrage de charge avancé
- Mappage du disque client (plates-formes UNIX ou Linux uniquement)
- Fenêtres transparentes (plates-formes Windows uniquement)
- Audio (plates-formes UNIX ou Linux uniquement)

Le tableau suivant répertorie les plates-formes d'installation prises en charge par le module d'enrichissement SGD.

Système d'exploitation	Versions prises en charge
Microsoft Windows (64 bits)	Windows Server 2008 R2
Microsoft Windows (32 bits et 64 bits)	Windows Server 2008
	Windows Server 2003 R2
	Windows Server 2003
Oracle Solaris sur plates-formes SPARC	Solaris 8, 9, 10 et 11
	Solaris Trusted Extensions 10 et 11
Oracle Solaris sur plates-formes x86	Solaris 10 et 11
	Solaris Trusted Extensions 10 et 11
Oracle Linux (32 bits et 64 bits)	5, 6
SUSE Linux Enterprise Server (32 bits et 64 bits)	10, 11

Les produits Oracle certifiés sur Oracle Linux sont également certifiés et pris en charge sur Red Hat Enterprise Linux en raison de la compatibilité implicite entre les deux distributions. Oracle n'exécute pas de test supplémentaire sur les produits Red Hat Enterprise Linux.

Sur les plates-formes Oracle Solaris Trusted Extensions, seule la fonction avancée d'équilibrage de charge est prise en charge. Les fonctions audio et CDM *ne sont pas prises en charge*.

Les serveurs d'applications qui ne font pas partie des plates-formes prises en charge par le module d'enrichissement SGD peuvent être utilisés avec SGD pour accéder à une application compatible, via un des protocoles pris en charge.

2.4.2.1. Prise en charge de la virtualisation

Les plates-formes d'installation compatibles avec le module d'enrichissement SGD Gateway sont prises en charge sur un hyperviseur Type 1 (sans système d'exploitation) ou un hyperviseur Type 2 (hébergé), par

exemple Oracle VM VirtualBox, VMWare ou Oracle VM Server pour SPARC (anciennement connu sous le nom Sun Logical Domains ou LDom).

L'installation dans les zones est prise en charge pour les plates-formes Oracle Solaris. SGD peut être installé dans la zone globale ou dans une ou plusieurs zones non globales. L'installation aussi bien dans la zone globale que dans une zone non globale *n'est pas prise en charge*.

Sur les plates-formes Oracle Solaris Trusted Extensions, vous devez installer SGD dans une zone étiquetée. N'installez pas SGD dans la zone globale.

2.4.2.2. Déclasser les plates-formes d'installation prises en charge par le module d'enrichissement SGD

Le tableau suivant présente les plates-formes d'installation du module d'enrichissement SGD qui ont fait l'objet d'un déclasser.

Version de SGD	Plates-formes qui ne sont plus prises en charge
4.70	Red Hat Enterprise Linux 5
4.60	OpenSolaris (toutes versions) Windows Vista Professionnel Windows Vista Professionnel Windows XP Professionnel



Note

Le module d'enrichissement SGD ne fournit plus de fonctions prises en charge sur les plates-formes Windows 7 et Windows XP. Ces plates-formes font toujours partie des plates-formes de serveur d'applications prises en charge. Reportez-vous à la section [Section 2.4.3, « Microsoft Windows Services Remote Desktop »](#).

2.4.3. Microsoft Windows Services Remote Desktop

SGD n'inclut pas de licences pour Microsoft Windows Services Remote Desktop. Si vous accédez à la fonctionnalité Services Remote Desktop disponible avec les systèmes d'exploitation Microsoft, vous devez vous procurer des licences supplémentaires pour utiliser ces produits. Consultez les contrats de licence de vos systèmes d'exploitation Microsoft afin d'identifier les licences à acquérir.



Note

Auparavant, Microsoft Windows Server 2008 R2 Remote Desktop Services s'appelait Terminal Services.

SGD prend en charge les connexions RDP avec les versions suivantes de Microsoft Windows :

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003
- Windows 7 SP1

- Windows XP Professionnel SP3

Sur les plates-formes Windows XP et Windows 7, seules les sessions ouvertes Windows complètes sont prises en charge. L'exécution d'applications individuelles n'est pas prise en charge. Les fenêtres transparentes ne sont pas prises en charge.

Les fonctions prises en charge par SGD varient selon que vous vous connectez via le protocole RDP ou Oracle VRDP (VM VirtualBox RDP), comme indiqué dans le tableau suivant.

Tableau 2.1. Comparaison des fonctions prises en charge par SGD lors de l'utilisation de RDP et VRDP

Fonction	RDP	VRDP
Enregistrement audio (entrée audio)	✓	✓
Redirection audio	✓	✓
Redirection du presse-papiers	✓	✓
Mappage des ports COM	✓	X
Compression	✓	X
Redirection des lecteurs (mappage des lecteurs des clients)	✓	X
Multi-moniteurs	✓	X
Sécurité du réseau (niveau de chiffrement)	✓	✓
Annuaire de sessions	✓	X
Redirection des cartes à puce	✓	X
Redirection des fuseaux horaires	✓	X
Mappage des imprimantes Windows (impression au niveau des clients)	✓	X

2.4.3.1. Qualité audio

Windows Server 2008 R2 et Windows 7 prennent en charge un taux d'échantillonnage audio pouvant atteindre 44,1 kHz. Par défaut, SGD prend en charge un taux d'échantillonnage pouvant atteindre 22,05 khz. Pour prendre en charge un taux d'échantillonnage pouvant atteindre 44,1 khz, dans la console d'administration, accédez à l'onglet Paramètres globaux, Périphérique client et sélectionnez l'option Audio windows : Qualité optimale.

2.4.3.2. Redirection de l'enregistrement audio

La redirection de l'enregistrement audio est prise en charge par les serveurs d'applications Microsoft Windows Server 2008 R2 et Microsoft Windows 7.

Pour enregistrer du son dans une session Windows Services Remote Desktop, la redirection de l'enregistrement audio doit être activée sur le serveur d'applications. Par défaut, la redirection de l'enregistrement audio est désactivée.

Pour activer l'enregistrement audio sur les serveurs d'applications Microsoft Windows 7 Enterprise, vous devez également ajouter l'entrée de registre suivante à la clé `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp`.

```
"fDisableAudioCapture"=dword:00000000
```

2.4.3.3. Profondeur des couleurs

SGD prend en charge les profondeurs de couleurs 8 bits, 16 bits, 24 bits et 32 bits dans une session Windows Services Remote Desktop.

La profondeur de couleurs 32 bits est disponible sur les plates-formes Windows Server 2008, Windows Server 2008 r2 et Windows 7. Pour afficher des couleurs 32 bits, le périphérique client doit être capable d'afficher des couleurs 32 bits.

La profondeur de couleurs 15 bits n'est pas prise en charge. Si la profondeur de couleurs est spécifiée sur l'hôte Hôte de session Remote Desktop, SGD règle automatiquement la profondeur de couleur sur 8 bits.

2.4.3.4. Niveau de chiffrement

Vous pouvez uniquement utiliser les niveaux de chiffrement Faible, Compatible client et Elevé avec SGD. SGD ne prend pas en charge le niveau de chiffrement FIPS (Federal Information Processing Standards).

2.4.3.5. Transport Layer Security

A partir de Microsoft Windows Server 2003, vous pouvez utiliser TLS (Transport Layer Security) à des fins d'authentification serveur et de chiffrement des communications de l'hôte Hôte de session Remote Desktop.

2.4.3.6. Authentification au niveau du réseau

Si l'hôte Hôte de session Remote Desktop prend en charge l'authentification au niveau du réseau (NLA) à l'aide de CredSSP, vous pouvez utiliser NLA pour l'authentification serveur.

2.4.4. Applications X et à traitement de caractère

Pour exécuter des applications X et à traitement de caractère, SGD doit pouvoir se connecter au serveur d'applications qui héberge l'application. SGD prend en charge les méthodes de connexion SSH et Telnet. Il est conseillé d'utiliser le protocole SSH pour une sécurité optimale.

SGD fonctionne avec SSH version 2 ou ultérieure. Pour pallier les problèmes de compatibilité de versions SSH, utilisez la même version majeure de SSH, à savoir la version 2 ou 3, sur tous les hôtes et les serveurs d'applications SGD.

Si vous utilisez SSH pour vous connecter aux applications X, activez la fonction de transfert X11. Pour cela, accédez à la configuration SSH ou configurez l'application dans SGD. Le manuel *Oracle Secure Global Desktop Administration Guide for Release 4.7* offre des informations détaillées sur l'utilisation de SSH avec SGD.

SGD prend en charge l'extension de sécurité X. L'extension de sécurité X ne fonctionne qu'avec les versions de SSH qui prennent en charge l'option `-Y`. Pour OpenSSH, il s'agit de la version 3.8 ou ultérieure.

2.4.4.1. Logiciel X11

SGD comprend l'implémentation d'un moteur de protocoles X (XPE) basée sur X.Org Foundation X Server version X11R7.6.

L'implémentation de XPE est basée sur les sources X.org Foundation suivantes :

- [xorg-server 1.9.3](#)
- [xrandr 1.3](#)

- [xkeyboard-config 2.1](#)

Les versions suivantes des dépendances X.org sont utilisées :

- [Mesa 7.9.2](#)
- [pixman 0.20.2](#)

2.4.4.2. Extensions X prises en charge

SGD prend en charge les extensions X suivantes pour les applications X :

- BIG-REQUESTS
- BLINK
- DAMAGE
- DEC-XTRAP
- DOUBLE-BUFFER
- Extended-Visual-Information
- GLX
- MIT-SCREEN-SAVER
- MIT-SHM
- MIT-SUNDRY-NONSTANDARD
- NATIVE-WND
- RDP
- RECORD
- RENDER
- SCO-MISC
- SECURITY
- SGI-GLX
- SHAPE
- SYNC
- TOG-CUP
- X-Resource
- XC-APPGROUP
- XC-MISC
- XFIXES

- XFree86-Bigfont
- XTEST
- XTTDEV
- KEYBOARD
- RANDR
- XINERAMA

L'extension X suivante *n'est pas* prise en charge :

- XVIDEO

2.4.4.3. Applications à traitement de caractère

SGD prend en charge les applications à traitement de caractère VT420, Wyse 60 ou SCO Console.

2.4.5. Infrastructure de bureaux virtuels (Virtual Desktop Infrastructure)

SGD utilise un type d'objet appelé un *serveur d'applications dynamique* pour représenter un courtier de serveur virtuel (VSB). SGD utilise le VSB pour obtenir une liste des serveurs d'applications qui peuvent exécuter une application.

SGD inclut des courtiers qui vous permettent d'octroyer aux utilisateurs un accès aux bureaux fournis par un serveur Oracle VDI (Virtual Desktop Infrastructure).

L'intégration à Oracle VDI est également prise en charge par le biais de la configuration d'un objet d'application Windows, comme indiqué dans le manuel *Oracle Secure Global Desktop Administration Guide for Release 4.7*.

Cette version de SGD prend en charge les versions suivantes d'Oracle VDI :

- Oracle VDI 3.4.1
- Oracle VDI 3.3.2

2.5. Fonctionnalités retirées

Les fonctionnalités suivantes ont été retirées de la version 4.70 :

- **Pool de licences CAL.** Les CAL (Client Access Licenses) pour les autres périphériques client non Windows ne sont plus stockées dans un pool de licences sur le serveur SGD. La commande `tarantella tscal` de gestion du pool de licences n'est plus disponible.
- **Lancement local.** L'exécution d'une application sur les périphériques client Windows (le "lancement local") n'est plus prise en charge. L'attribut Local Client Launch (`--trylocal`) a été abandonné.

Le paramètre `localx` n'est plus pris en charge pour l'attribut Type de fenêtre (`--displayusing`).

Le paramètre de profil Rechercher le serveur X local n'est plus disponible.

- **Authentification de domaine Windows.** L'authentification de domaine Windows ne fait plus partie des méthodes prises en charge d'authentification des utilisateurs de SGD. L'attribut Contrôleur de domaine Windows (`--login-nt`) a été abandonné.

Il est possible d'utiliser l'authentification Active Directory à la place de l'authentification de domaine Windows.

- **Utilisation de la commande `rexec` pour démarrer des applications.** La commande `rexec` ne fait plus partie des options prises en charge pour l'attribut Méthode de connexion (`--method`).
- **Attributs d'affichage.** Les attributs XPE (X Protocol Engine) et d'affichage X suivantes ont été abandonnés :
 - Base de données RVB (`--xpe-rgbdatabase`). XPE prend désormais en charge les noms de couleurs X11.
 - Symbole de l'euro (`--euro`). Le symbole de l'euro est désormais pris en charge par défaut.
 - Configuration du clavier : Verrouillé (`--lockkeymap`). L'extension XKB est désormais utilisée pour la prise en charge des claviers.
 - Configuration du clavier (`--xpe-keymap`). L'extension XKB est désormais utilisée pour la prise en charge des claviers.
 - Configuration du clavier (`--keymap`). Cet attribut est désormais disponible depuis la ligne de commande uniquement.

2.5.1. Modifications prévues dans la prochaine version de SGD

Les fonctionnalités SGD suivantes ne seront peut-être plus disponibles dans la prochaine version de SGD :

- Plates-formes client et navigateurs pris en charge : Ubuntu Linux 10.04 et Mac OS X 10.6 ne feront peut-être plus partie des plates-formes client prises en charge. La prise en charge de Mac OS X 10.8 sera disponible dans la prochaine version.

Pour ce qui est des navigateurs, Internet Explorer 7 ne sera peut-être plus pris en charge.

- Serveurs d'annuaire LDAP : Sun Directory Server ne sera peut-être plus pris en charge.
- JSP d'équilibrage de charge de SGD (`swcd.jsp`) : la passerelle SGD Gateway fournit une solution plus efficace pour les déploiements avec équilibrage de charge.
- Utilisation facultative des cookies de navigateur lors de l'accès à SGD.
- Authentification SecurID : utilisez RSA Authentication Agent avec une authentification tierce à la place.
- Mode intégré pour le client SGD.
- Commande `tarantella cache`.

Chapitre 3. Problèmes connus, résolution de bogues et problèmes détectés dans la documentation

Ce chapitre contient des informations relatives aux problèmes connus, à la résolution de bogues et aux problèmes détectés dans la documentation pour Oracle Secure Global Desktop (SGD). Des informations sur l'envoi de commentaires et le signalement de bogues sont également fournies.

3.1. Bogues et problèmes connus

Cette section répertorie les bogues et problèmes connus pour la version 4.70 de SGD.

3.1.1. 2205237 : problèmes d'affichage dans une fenêtre transparente lors du redémarrage d'une session déconnectée

Problème : le redémarrage d'une application Windows par l'utilisateur après sa fermeture peut entraîner des problèmes avec les fenêtres transparentes. Ce problème se produit lorsque l'application est hébergée sur un serveur Windows Server 2008 R2.

Cause : un problème connu avec certaines versions du module d'enrichissement SGD.

Solution : vérifiez que la version du module d'enrichissement SGD exécutée sur le serveur d'applications Windows est identique à la version du serveur SGD.

3.1.2. 6555834 : la technologie Java est activée pour le navigateur mais n'est pas installée sur le périphérique client

Problème : si la technologie est activée dans vos paramètres de navigateur mais que le plug-in Java n'est pas installé sur le périphérique client, le bureau Web SGD ne s'affiche pas. Le processus de connexion s'arrête au niveau de l'écran de démarrage.

Cause : SGD utilise les paramètres de navigateur afin de déterminer si la technologie Java doit être utilisée.

Solution : installez le plug-in Java et créez un lien symbolique entre le répertoire de plug-ins du navigateur et l'emplacement du logiciel Java Virtual Machine (JVM). Reportez-vous à la documentation du navigateur pour plus d'informations.

3.1.3. 6831480 : la commande de liste des serveurs principaux de sauvegarde renvoie un message d'erreur

Problème : l'utilisation de la commande `tarantella array list_backup primaries` sur un serveur SGD arrêté puis déconnecté d'un groupe renvoie le message d'erreur "Echec de la connexion".

Cause : un problème connu.

Solution : redémarrez le serveur SGD déconnecté avant d'utiliser la commande `tarantella array list_backup primaries`.

3.1.4. 6863153 : l'application HyperTerminal se bloque à partir d'une session de bureau Windows

Problème : les utilisateurs exécutant l'application HyperTerminal dans une session de bureau Windows rencontrent des problèmes lorsqu'ils tentent de rouvrir une session de bureau à partir d'un autre périphérique client. L'application HyperTerminal ne répond pas et ne peut pas être fermée.

Cause : un problème connu avec HyperTerminal lors de la reprise de session de bureau Windows à partir d'un autre périphérique client (également appelé "capture de session").

Solution : fermez l'application HyperTerminal avant de reprendre une session de bureau Windows à partir d'un autre périphérique client.

3.1.5. 6937146 : audio non disponible pour les applications X hébergées sur des serveurs d'applications Linux 64 bits

Problème : le son n'est pas disponible dans les applications X hébergées sur les serveurs d'applications Linux 64 bits. Ce problème se produit dans les applications X codées en dur de façon à utiliser le périphérique `/dev/dsp` ou `/dev/audio`, et l'attribut Bibliothèque de redirection audio (`--unixaudiopreload`) est activé.

Cause : un problème connu. Une bibliothèque de redirection audio 64 bits SGD n'est pas incluse dans le module d'enrichissement SGD.

Solution : aucune solution connue à ce jour.

3.1.6. 6942981 : lenteur du démarrage de l'application sur Solaris Trusted Extensions

Problème : sur les plates-formes Oracle Solaris Trusted Extensions, le temps de démarrage des applications Windows et X peut être plus long que prévu.

Cause : par défaut, le moteur de protocoles X tente de se connecter au port d'affichage X 10. Ce port n'est pas disponible lors de l'utilisation de Solaris Trusted Extensions. Après un certain délai, le moteur de protocoles X se connecte à un autre port d'affichage X et l'application démarre.

Solution : effectuez l'une des opérations suivantes :

- Modifiez le port d'affichage minimal utilisé par défaut par le serveur SGD.

Sur le serveur SGD, configurez le paramètre suivant dans le fichier `xpe.properties` du répertoire `/opt/tarantella/var/serverconfig/local` :

```
tarantella.config.xpeconfig.defaultmindisplay=11
```

Redémarrez le serveur SGD une fois la modification terminée.

- Excluez le port indisponible des ports utilisables par le moteur de protocoles X.

Dans la console d'administration, accédez à l'onglet Moteurs de protocoles X pour chaque serveur SGD du groupe et saisissez `-xport portnum` dans le champ Arguments de la ligne de commande, où `portnum` correspond au numéro de port TCP à exclure.

Vous pouvez également utiliser la commande suivante :

```
$ tarantella config edit --xpe-args "-xport portnum"
```

Par exemple, pour exclure le port d'affichage X 10 des ports utilisés par le moteur de protocoles X :

```
$ tarantella config edit --xpe-args "-xport 6010"
```

Les modifications apportées s'appliquent uniquement aux nouveaux moteurs de protocoles X. Les moteurs de protocoles X existants ne sont pas affectés.

3.1.7. 6957820 : le client SGD se bloque lors de l'utilisation de l'authentification des cartes à puce pour les applications Windows

Problème : lorsque vous utilisez une carte à puce pour vous connecter à une session d'application Windows depuis un périphérique client Ubuntu Linux 10.04, le client SGD se bloque une fois que l'utilisateur a quitté la session d'application authentifiée. L'utilisateur peut se trouver dans l'impossibilité de démarrer d'autres applications ou de se déconnecter de SGD.

Cause : un problème connu avec la version 1.5.3 de PCSC-Lite sur les plates-formes client Ubuntu.

Solution : mettez votre version à jour vers la dernière version de PCSC-Lite sur le périphérique client.

3.1.8. 6962970 : un périphérique client Windows utilise plusieurs CAL

Problème : plusieurs licences d'accès client (CAL) sont affectées à un périphérique client Windows. Une CAL est affectée par erreur à chaque démarrage d'une application Windows.

Cause : problème connu si la clé ou l'une des sous-clés `HKEY_LOCAL_MACHINE\Software\Microsoft\MSLicensing` ne sont pas présentes dans le registre Windows sur un périphérique client. Ce problème concerne les plates-formes Microsoft Windows 7.

Solution : recréez les clés manquantes en lançant la connexion Bureau à distance avec des privilèges d'administrateur. Voir l'article 187614 de la base de connaissances Microsoft pour plus d'informations.

3.1.9. 6970615 : échec de l'authentification SecurID pour les applications X

Problème : l'authentification SecurID pour les applications X échoue en cas d'utilisation de l'agent d'authentification RSA pour PAM. Ce problème concerne les applications X configurées pour utiliser telnet comme méthode de connexion.

Cause : un problème connu en cas d'utilisation de l'agent d'authentification RSA pour PAM.

Solution : configurez l'objet d'application X de façon à utiliser SSH comme méthode de connexion.

3.1.10. 7004887 : échec de l'impression dans un fichier pour les périphériques client Windows

Problème : lorsqu'un utilisateur sélectionne l'option Imprimer dans un fichier dans une application Windows affichée via SGD, le travail d'impression est mis en attente dans la file d'impression sur le périphérique client. Ce problème concerne les périphériques client exécutant Windows Vista et Windows 7.

Cause : un problème connu avec certaines versions de Windows.

Solution : une solution de contournement pour Windows Vista est décrite dans l'article 2022748 de la base de connaissances de Microsoft.

3.1.11. 12300549 : le nom du serveur d'annuaires personnel de certains environnements linguistiques client est illisible

Problème : lors du mappage du disque client dans SGD, le nom de l'annuaire personnel de l'utilisateur peut comporter des caractères illisibles. Par défaut, l'annuaire personnel de l'utilisateur est mappé au disque "My Home".

Ce problème concerne les périphériques client non Windows configurés avec un environnement linguistique client non anglais, tel que `ja_JP.UTF-8`.

Cause : un problème connu pour certains environnements linguistiques client.

Solution : aucune solution connue à ce jour.

3.1.12. 13068287 : problèmes avec la couleur 16 bits dans les applications OpenGL

Problème : les applications OpenGL, telles que les programmes graphiques en 3D, ne démarrent pas ou ne s'affichent pas correctement lorsqu'elles sont affichées via SGD. Ce problème survient lorsque le paramètre de profondeur des couleurs de l'objet d'application est défini sur 16 bits.

Cause : problème connu lors de l'affichage d'applications Open GL utilisant une couleur 16 bits.

Solution : il est possible d'afficher l'application en réglant le paramètre de profondeur des couleurs sur 24 bits.

3.1.13. 13117149 : caractères accentués dans les noms d'utilisateur Active Directory

Problème : l'authentification Active Directory échoue pour les noms d'utilisateur contenant des caractères accentués, tels que le caractère allemand umlaut (ü). Ce problème a été constaté lors de l'utilisation de Windows Server 2003 R2.

L'erreur suivante est indiquée dans la sortie du journal lors de l'utilisation du filtre du journal `server/login/info` :

```
javax.security.auth.login.LoginException: Integrity check on decrypted field failed (31)
```

Cause : l'authentification Active Directory utilise le protocole d'authentification Kerberos. Ce problème a été constaté lorsque l'authentification Kerberos est configurée pour utiliser le chiffrement DES.

Solution : il est possible de désactiver l'utilisation du chiffrement DES dans le fichier de configuration Kerberos `krb5.conf` sur le serveur SGD.

Incluez les lignes suivantes dans la section `[libdefaults]` du fichier `krb5.conf`.

```
[libdefaults]
    default_tgs_enctypes = rc4-hmac des3-cbc-sha1 aes128-cts aes256-cts
    default_tkt_enctypes = rc4-hmac des3-cbc-sha1 aes128-cts aes256-cts
```

3.1.14. 13354844, 14032389, 13257432, 13117470 : problèmes d'affichage sur les périphériques client Ubuntu

Problème : les problèmes d'affichage suivants peuvent se produire sur les périphériques client exécutant Ubuntu Linux.

- Le bouton de réduction du mode Kiosk ne fonctionne pas si vous n'utilisez pas de gestionnaire de fenêtres ou si vous utilisez un gestionnaire de fenêtres minimaliste, tel que `evilwm`.
- Le bouton de basculement du mode Kiosk à l'affichage de fenêtre intégré ne fonctionne pas.
- L'icône de la barre des tâches du client SGD ne s'affiche pas lors de l'utilisation du bureau Unity.
- Une application de fenêtres transparentes affichable sur plusieurs moniteurs est remplacée par des barres de défilement sur un seul moniteur.

Cause : un problème connu lors de l'utilisation d'un périphérique client Ubuntu Linux.

Solution : utilisez l'une des solutions de contournement suivantes.

- Pour utiliser la fenêtre du mode Kiosk, le gestionnaire de fenêtres doit implémenter le protocole d'état de modification de Normal à Icône. Vérifiez que vous exécutez un gestionnaire de fenêtres approprié.
- Utilisez le raccourci Ctrl+Alt+Attn pour passer du mode Kiosk à l'affichage de fenêtre intégré.
- Pour afficher l'icône de la barre des tâches du client SGD, ajoutez l'application du client SGD à la liste blanche du bureau Unity.

Démarrez l'utilitaire `dconf-editor` et accédez à la boîte de dialogue Desktop → Unity → Panel. Ajoutez `Oracle Secure Global Desktop` à la liste des applications.

- Il n'existe aucune solution connue pour le problème d'affichage des fenêtres transparentes sur plusieurs moniteurs.

3.1.15. 13360596 : problème d'authentification directe avec Oracle VDI

Problème : lors de l'utilisation du courtier VDI avec Oracle VDI, un message d'erreur s'affiche lors de l'authentification au bureau Windows. Les utilisateurs doivent saisir leur mot de passe à chaque démarrage du bureau.

Cause : un problème connu avec la mise en cache par SGD des données d'identification de l'utilisateur pour certaines configuration d'Oracle VDI.

Solution : sur le serveur SGD server, modifiez le script de lancement de l'application dans `/opt/tarantella/webserver/tomcat/tomcat-version/webapps/sgd/applicationLaunch/appLaunch.jsp`.

Localisez l'instruction suivante, à la ligne 484 dans `appLaunch.jsp` :

```
if (chosenCandidate.getUsername() == null)
```

Modifiez l'instruction de la manière suivante :

```
if (chosenCandidate.getUsername() == null || chosenCandidate.getPassword() == null)
```

3.1.16. 13971245 : problèmes de retrait des packages dans Oracle Solaris 11

Problème : SGD peut ne pas être désinstallé correctement sur les plates-formes Oracle Solaris 11. Une fois SGD désinstallé, les entrées pour les packages SGD sont toujours présentes dans la base de données du package Solaris.

Cause : un problème connu lors de l'utilisation d'Image Packaging System (IPS) inclus dans Oracle Solaris 11 et de la suppression de SGD.

Solution : la solution de contournement consiste à utiliser le script de réparation de la base de données du package SGD `pkgdbfix.sh` une fois SGD désinstallé. Ce script est inclus dans le répertoire `/opt/tarantella/etc/data` sur un serveur SGD.

Connectez-vous en tant que superutilisateur (racine) et effectuez l'une des opérations suivantes :

- Désinstallez SGD et recherchez les entrées de package SGD dans la base de données Solaris.

```
# pkgchk -l tta
# pkgchk -l tta.2
```

- Si toutes les entrées de package sont déclarées à l'aide d'une des commandes précédentes, réparez la base de données des packages.

```
# sh pkgdbfix.sh package-instance
```


où `package-instance` correspond à l'instance de package déclarée, soit `tta` ou `tta.2`.

3.1.17. 14026511 : échec des connexions du courtier VDI après une mise à niveau d'Oracle VDI

Problème : après la mise à niveau ou la reconfiguration d'un hôte Oracle VDI, il se peut que les utilisateurs ne puissent plus connecter leurs bureaux Oracle VDI avec le courtier VDI.

Cause : lors de l'utilisation du courtier VDI, les connexions à l'hôte Oracle VDI sont sécurisées à l'aide d'un certificat SSL auto-signé pour l'API des services Web.

Lorsque vous reconfigurez ou mettez à niveau Oracle VDI sur un hôte, le certificat auto-signé des services Web est renouvelé et le certificat SSL actuel n'est pas conservé. En outre, lors de la mise à niveau, le nom d'hôte (sujet) utilisé dans le certificat SSL des services Web peut être modifié.

Solution : utilisez l'une des solutions de contournement suivantes :

- Sauvegardez le keystore de certificats de services Web sur l'hôte Oracle VDI avant la mise à niveau ou la reconfiguration. Restaurez le keystore à partir de la sauvegarde une fois l'installation d'Oracle VDI modifiée.

Ce processus est décrit dans la documentation Oracle VDI.

- Reconfigurez le courtier VDI de la manière suivante :
 - Importez le certificat SSL des services Web pour *chaque hôte Oracle VDI* dans le truststore de certificats sur *chaque serveur SGD*. En fonction de votre configuration, le truststore peut être un truststore de certificats AC ou un truststore dédié.
 - Reconfigurez le courtier VDI de manière à utiliser les noms d'hôte des certificats SSL des services Web.

Modifiez les paramètres `preferredhosts` et `failoverhosts` pour utiliser les nouveaux noms d'hôte.

3.1.18. 14021467 : problème de sélection de la langue sur le bureau Web

Problème : en général, les utilisateurs peuvent sélectionner leur langue principale dans la liste sur la page d'accueil de SGD. Ils cliquent ensuite sur Connexion pour accéder à un bureau Web dans cette langue.

Après avoir sélectionné une langue sur la page d'accueil SGD, il se peut que les utilisateurs ne puissent pas sélectionner d'autres langues pour les connexions suivantes.

Cause : un problème connu avec la mise en cache de la sélection de la langue principale.

Solution : utilisez l'une des solutions de contournement suivantes :

- Effacez le cache du navigateur avant de sélectionner une autre langue.
- Localisez le texte suivant, à la ligne 66 dans le fichier `localeutils.jsp` :

```
prefLang = (String) pageContext.getAttribute(PREF_LANG, PageContext.SESSION_SCOPE);
```

Le fichier `localeutils.jsp` se trouve dans le répertoire `/opt/tarantella/webserver/tomcat/tomcat-version/webapps/sgd/resources/jsp` sur le serveur SGD.

- Modifiez le fichier de la manière suivante :


```
if (HttpServletRequest.getParameter(LANG_SELECTED) == null)
    prefLang = (String) pageContext.getAttribute(PREF_LANG, PageContext.SESSION_SCOPE);
```

3.1.19. 14085800 : problème de gestion de l'ancien mot de passe d'Active Directory

Problème : après expiration de leur mot de passe Active Directory, les utilisateurs peuvent mettre à jour leur mot de passe à l'invite de SGD. Toutefois, le mot de passe mis à jour n'est pas toujours stocké correctement dans le cache des mots de passe.

Cela signifie que certains utilisateurs peuvent être invités à s'authentifier chaque fois qu'ils démarrent une application hébergée sur un serveur d'applications Windows.

Ce problème survient dans les cas suivants :

- SGD est configuré pour saisir automatiquement le mot de passe de l'utilisateur lorsque celui-ci se connecte à un serveur d'applications, si le mot de passe a été mis en cache. Cette option est configurée par défaut sur SGD
- Le paramètre d'expiration du mot de passe de l'objet Service d'Active Directory (`--check-pwd-policy`) est activé.

Cause : un problème connu avec la gestion des anciens mots de passe pour Active Directory par SGD.

Solution : utilisez la solution de contournement suivante.

- Désactivez la fonction d'expiration du mot de passe pour l'objet Service. Par exemple :

```
$ tarantella service edit --name adl-east --check-pwd-policy 0
```

- Configurez l'attribut de nom de domaine pour l'objet d'application Windows. Par exemple :

```
$ tarantella object edit --name obj --ntdomain east.example.com
```

3.1.20. 14147506 : échec de la résilience de groupe en cas de modification du serveur principal

Problème : la résilience de groupe peut échouer si vous modifiez le serveur principal alors que le groupe est en cours de réparation. Le groupe est réparé à la fin du basculement.

Après le basculement de la résilience de groupe, lorsque les serveurs non joignables sont ajoutés au groupe, les communications avec les autres membres du groupe peuvent ne pas fonctionner.

Ce problème survient lorsque les communications intragroupe sécurisées sont activées pour le groupe.

Cause : un problème connu avec la résilience de groupe lorsque les communications intragroupes sécurisées sont activées. Par défaut, les communications intragroupes sécurisées sont activées dans un serveur SGD.

Solution : aucune solution connue. Si possible, évitez de modifier la structure du groupe pendant le processus de résilience de groupe.

3.1.21. 14221098 : échec du démarrage de l'application Konsole sur Oracle Linux

Problème : l'application d'émulation de terminal KDE `Konsole` échoue à démarrer lorsqu'elle est configurée en tant qu'objet d'application X dans SGD.

Ce problème survient lorsque l'application est hébergée sur une plate-forme Oracle Linux 6.

Cause : un problème connu lors de l'exécution de [Konsole](#) sur Oracle Linux 6. Ce problème est lié au lancement du processus de l'application au démarrage.

Solution : la solution de contournement consiste à utiliser l'option de commande `--nofork` au démarrage de [Konsole](#).

Dans la console d'administration, accédez à l'onglet de lancement pour l'objet d'application X et saisissez `--nofork` dans le champ Arguments de commande.

3.1.22. 14237565 : problème de taille de page lors de l'impression sur les périphériques client non Windows

Problème : les travaux d'impression ne sont pas envoyés à l'imprimante client au bon format de page. Par exemple, une tâche d'impression d'un document au format A4 est envoyée à l'imprimante client au format Lettre. En fonction de la configuration de l'imprimante client, cela peut entraîner l'échec du travail d'impression.

Ce problème se produit sur les périphériques client Linux et Mac OS X.

Cause : un problème connu d'impression sur des périphériques client non Windows.

Solution : certaines imprimantes client peuvent être configurées de manière à ignorer le format de page.

Pour contourner le problème, utilisez l'impression PDF lorsque vous imprimez à partir de SGD.

3.1.23. 14287570 : applications Microsoft Windows Server 2003 limitées à une profondeur de couleur de 8 bits pour les résolutions grand écran

Problème : pour les applications Microsoft Windows Server 2003, la profondeur des couleurs d'affichage sur les périphériques client est limitée à 8 bits pour les résolutions grand écran. Ce problème se présente avec les résolutions d'écran supérieures à 1 600 x 1 200 pixels.

Cause : un problème connu avec certaines sessions Windows Server 2003 Services Remote Desktop.

Solution : voir le correctif logiciel Microsoft 942610 pour plus d'informations sur l'augmentation de la profondeur des couleurs à 16 bits.

3.1.24. 14287730 : messages d'erreur X lors de la reproduction à partir de la ligne de commande

Problème : des messages d'erreur similaires au message ci-dessous s'affichent lors de la reproduction d'une session d'application à partir de la ligne de commande à l'aide de la commande `tarantella emulatorsession shadow`.

```
X Error: BadImplementation
Request Major code 152 (RANDR)
Request Minor code 8 ()
Error Serial #209
Current Serial #209
```

La reproduction fonctionne comme prévu malgré les messages d'erreur.

Cause : un problème connu si le serveur X n'implémente pas le redimensionnement de la session sur le périphérique client.

Solution : ces erreurs sont sans importance et peuvent être ignorées.

3.1.25. 14404371 : les caractères saisis par l'utilisateur dans la boîte de dialogue d'authentification sont illisibles

Problème : lorsqu'un utilisateur tente de saisir ses données d'identification à l'aide de la boîte de dialogue SGD certains caractères saisis peuvent être illisibles. Ce problème se produit sur les périphériques client non Windows, lorsque les données d'authentification de l'utilisateur contiennent des caractères multi-octets, tels que les caractères de langue européenne.

La boîte de dialogue d'authentification SGD s'affiche lorsque l'utilisateur maintient la touche Maj. enfoncée en cliquant sur le lien d'une application sur le bureau Web.

Cause : un problème connu avec la configuration de la liste des polices sur certains périphériques client par SGD.

Solution : utilisez la solution de contournement suivante.

- Sur le périphérique client, créez un fichier de spécification des polices avec le contenu suivant :

```
*XmTextField*fontList: -*-medium-r-normal-**-120-**-***-*
```

- Mettez les polices à disposition sur le périphérique client.

```
# xrdp -merge filename
```

où *filename* correspond au nom du fichier de spécification des polices.

Vous pouvez également ajouter la spécification des polices dans un fichier `.Xresources` dans votre annuaire personnel.

3.1.26. 14408025 : fermeture inattendue du client SGD sur Ubuntu Linux

Problème : sur les périphériques client Ubuntu Linux 12, le client SGD peut se fermer de manière inattendue. En d'autres termes, les utilisateurs doivent reprendre ou redémarrer les applications.

Cause : ce problème est lié à une bibliothèque Enlightened Sound Daemon (ESD) manquante, [libesd.so](#).

Solution : installez la bibliothèque manquante sur le périphérique client de la manière suivante :

```
# apt-get install libesd0
```

3.1.27. 14472019 : SGD ne démarre pas au démarrage du système

Problème : sur les plates-formes Oracle Linux 6, SGD ne démarre pas automatiquement au démarrage de l'hôte.

Lors de l'arrêt de l'hôte SGD, les services & ne sont pas arrêtés correctement.

Cause : le problème est lié à une modification de l'architecture de démarrage du système introduite dans Oracle Linux 6. Cela signifie que les liens symboliques requis ne sont pas créés automatiquement lors de l'installation de SGD.

Solution : ajoutez un lien symbolique de la manière suivante :

```
# ln -s /etc/init.d/sun.com-sgd-base /etc/rc3.d/S90sun.com-sgd-base
```

3.2. Résolution de bogues dans la version 4.70

Le tableau suivant répertorie les principales corrections de bogues apportées à la version 4.70.

Tableau 3.1. Bogues corrigés dans la version 4.70

Référence	Description
14399820	APPLICATION LAUNCHES FAIL WHEN USING SECURID ON APPLICATION SERVER
14377391	SGD CLIENT IN ORACLE LINUX 5.8 SUN RAY SESSION CRASHES ON START UP
14375562	TTATCC DOES NOT INTEGRATE WITH SUN RAY LICENSE STORE
14360939	CLIENT WINDOWS MANAGEMENT FOCUS IS NOT SET CORRECTLY WHEN A WINDOW IS CLOSED
14341167	WARNING MESSAGES SEEN WHEN RESTARTING TARANTELLA ON SOLARIS SPARC SGD SERVER
14324111	NULL POINTER EXCEPTION IN PROXY.CONNECTION.START
14309113	SEAMLESS WINDOWS APPLICATION, MENUS NOT SHOWN PROPERLY ON MULTI MONITOR
14303042	TTATSC CRASHES WHEN VIEWING CERTAIN URLS WITH WIN 7 APPLICATION SERVER (PORT OF 14097708)
14282154	WE SHOULD DOCUMENT HOW TO ENABLE SECURE COOKIES WITH PLAIN TEXT CONNECTIONS
14273752	SGD CLIENT SEGMENTATION FAULTS WHEN LAUNCHING A SEAMLESS WINDOWS APP FROM A UBUNTU 11.10 CLIENT
14272631	REPAINT ISSUE WHEN GRABBING A SESSION TO WINDOWS FROM UBUNTU LINUX
14225437	DOCUMENT VERSIONS OF X11 SOFTWARE
14221098	PROBLEMS RUNNING KONSOLE ON OEL 6.2
14215152	LOGIN BUTTON ON MAIN ENTRY PAGE IS NOT LOCALIZED
14213904	OVERRIDE PROXY SETTING DOES NOT WORK
14203183	LD.SO.1: TTAXTEXTCONV: FATAL: LIBICONV.SO.2: OPEN FAILED
14202226	WINDOWS APPLICATION EXITS WHEN SCREEN SAVER APPEARS IN THE APPLICATION
14202097	CLASSROOM OBJECT FAILS TO LAUNCH WHEN X AUTHORIZATION FOR X DISPLAY IS ENABLED
14194633	COMMAND NOT FOUND ERROR ON TRYING TO SHADOW A CHARACTER OR SUSPENDED APPLICATION FROM CLI
14194487	SEGMENTATION FAULT IS SEEN ON CLOSING A SHADOWED SESSION LAUNCHED WITH --SILENT OPTION
14174406	CLIENTSESSIONOBJECT.FORWARDREQUEST DROPS ONE CONNECTION, TWO IF PEER SSL ENABLED
14169371	JDEVELOPER CRASHES THE TTAXPE
14169009	MAC OS X CLIENT SEGMENTATION FAULT ON CHANGING PROFILE SETTINGS
14151185	SETUP LOG ERROR FOR 3270 AND 5250 APPLICATIONS CREATED WITH LOCKKEYMAP ARGUMENT
14128209	VARIOUS SEAMLESS WINDOWS TOGGLE PROBLEMS UNDER UNIX
14124560	SGD CLIENT CORE DUMP FOR COMMAND LINE START UP
14124146	ORACLE SGD BANNER IS MISALIGNED

Référence	Description
14123398	SGD CLIENT NOSTARTIMMEDIATE FLAG NOT WORKING
14119028	TTATSC USES 100% CPU
14101871	DOC CORRECTION REQUIRED FOR TARANTELLA OBJECT NEW_GROUP
14101499	4.7 PORT OF 13947409 AND REMOVAL OF INSTRUMENTATION
14101480	CAPS LOCK STATE SYNC WHEN KEYBOARD IS JAPANESE PC ON SERVER
14080078	SOLARIS 11: 3270 AND 5250 WILL NOT RUN BECAUSE OF MOTIF DEPENDANCY
14079220	PRTINSTALL MESSAGE MENTIONS CONFIG FILES THAT MIGHT NOT EXIST
14068868	SGD CLIENT CRASHES WHEN DEFAULT URL IS INVALID AND NO PROMPT/ PROFILE/URL ARGS
14064173	PRINTING FROM GNOME EDIT FAILS
14062558	TTATCC DOES NOT LAUNCH ON SOLARIS 11 CLIENT
14058535	DIRECTORY SERVICE UNAVAILABLE ERROR WHEN NO PASSWORD SUPPLIED
14058517	PORT OF 13968262: DUPLICATE SESSION/APP START ISSUES FOR SOME USERS
14053610	UNSAFE DOWNGRADE OF ALL INTERNET EXPLORER TRAFFIC TO HTTP1.0/TLS1.0
14053578	DEFAULT CHARACTER APPLICATION DOES NOT LAUNCH
14051828	APPARENT PROBLEM WITH WIDTH/HEIGHT RETURNED IN EXTENSION EVENT (RANDR)
14042478	SEAMLESS WINDOWS APPLICATION IS REPRESENTED IN TASKBAR USING APP ICON WHEN COLOR DEPTH IS 16/8
14032389	MAXIMISE BACK TO KIOSK MODE NOT WORKING VERY WELL
14032229	UNLOCALIZED MESSAGES IN PROFILE EDIT PAGE
14027702	CLIENTS MAXIMUM SIZE FEATURE IS BROKEN
14025219	SGD NOT PRESERVING APACHE PORT NUMBER ON UPGRADE
14021791	TTWEBTOP WINDOW: CALCULATING FRAME INSETS... MESSAGE IS DISPLAYED ON UBUNTU 12.04
14021492	MISSING ZH_TW TAIWAN KEYBOARD ENTRY IN USER PROFILE
14019019	FILES SHOULD BE OWNED BY ROOT OR BIN NOT TTASERV
14018841	SGDAUDIO DAEMON DOES NOT RUN ON SOLARIS SPARC
14018564	LDAP PASSWORD EXPIRY CHANGE DOES NOT WORK
14006086	RDP SHORTCUT KEYS FOR SCREEN COPY BEHAVIOR ARE INVERTED
14005396	ARRAY IS NOT REPAIRING WHEN PRIMARY IS OUT OF NETWORK
14004321	SEAMLESS WINDOWS PAINT APPLICATION CANNOT BE MOVED TO RIGHT AFTER RESUMING IT ON MULTI MONITOR SETUP
14002030	WINDOWS LAUNCHES TO A 2008 R2, RDPSEC LAYER, FIPS COMPLIANT FAIL - NO ERROR
14000588	UNLOCALIZED MESSAGES DISPLAYED
13999334	GLOBAL GRAB BY AN APPLICATION CAN LOCK ALL APPLICATION SESSIONS THAT SHARE AN XPE
13997556	NLA ALWAYS ON, EVEN WHEN DISABLED FOR OBJECT
13997183	TTATSC SEGMENTATION FAULTS ON SESSION DIRECTORY REDIRECT

Référence	Description
13996950	CANNOT RUN TTATSC MANUALLY WITHOUT LD_LIBRARY_PATH BEING SET
13996443	AN APPLICATION USING RANDR DOES NOT INFLUENCE THE SIZE OF THE SHADOW SESSION
13995625	EXCEPTIONS SEEN WITH MYDESKTOP/AUTOLOGOUT FUNCTIONALITY
13995357	INPUT METHOD IS NOT INVOKED
13991896	TTASHADOW SHOULD BE ROBUST WHEN HAVING A WRONG FONT IN THE DEFAULT FONT PATH
13974978	ESC - NEED A 4.62 REPLACEMENT FOR 4.50 GROUP MATCHES FEATURE
13969843	TTATCC SEGMENTATION FAULTS ON LOG OUT
13969017	LDAP AND AD USERS WITHIN THEIR DN SEE AN EMPTY WEBTOP
13943954	REINSTALL OF SGD THROWS WARNING AFTER UNINSTALL WITHOUT PURGE
13943594	3270 APPLICATION LAUNCHED THROUGH SGD SERVERS GIVES JUNK CHARACTERS
13943378	ADMINISTRATION GUIDE MESSAGE SHOULD BE REMOVED
13943130	ON SILENT SHADOWING, MESSAGES SHOULD BE GIVEN TO ADMIN ON THE STATUS OF THE USER APPLICATION
13940099	SGD CLIENT NOT COMPATIBLE ERROR ON RESTARTING TARANTELLA
13939571	CWM X APPLICATION EXITS ON CLICKING THE SHADOWING WINDOW
13933608	ENHANCEMENT MODULE INSTALLATION THROWS AN ERROR OF NO SUCH FILE OR DIRECTORY
13931179	VDI BROKER ALWAYS DISPLAYS GUEST POOLS
13924905	SGD, LD_LIBRARY_PATH AND SETUID
13920661	ON SUN RAY CHOOSE ZH_TW BIG5 - THE SGD CLIENT CRASHES IN DDPSCINIT()
13920424	UNINSTALLATION OF SGD FAILS ON ORACLE LINUX BECAUSE OF YUM INSTALL DEPENDENCIES
13920127	GETTING WRONG MESSAGE DURING CONFIGURATION OF SGD SERVER ON SOLARIS 11
13919290	CGI SCRIPTS ARE MISSING EXECUTE PERMISSIONS ON SOLARIS
13918324	SOME ES/IT/PT_BR WEB PAGES ARE INCOMPLETELY LOCALIZED
13896960	XPE MMAP() MEMORY ALLOCATION STILL NEEDED ON SOLARIS
13887082	SGD DIRECTORY SERVICES INTEGRATION USER ATTRIBUTE AUTHENTICATION CACHE BROKEN
13871529	KIOSK UI CAN APPEAR ON THE WRONG MONITOR
13854955	CLASSROOM OBJECT FAILS TO LAUNCH
13852504	GATEWAY FAILS AND DENIES LOGINS
13849967	SUN RAY REMOTE SCREEN CAPTURE KEY SEQUENCE LOSES EVENTS
13843469	KIOSK APP SPANS ONLY ONE SCREEN AFTER CHANGING THE RESOLUTION OF ONE IN MULTI MONITOR SETUP
13829872	MAC CLIENT GETS POLISH KEYBOARD LOADED FOR FRENCH INPUT
13829754	ALLOW ACCESS TO XKBSETIGNORELOCKMODS FOR MOTIF ACCELERATOR BUGS

Référence	Description
13829264	BASIC AUTHENTICATION THIRD PARTY LOG IN DOES NOT WORK WITH TOMCAT 7
13813121	AGED PASSWORD HANDLER TRANSPORT DOES NOT VARY WITH APPLICATION
13810458	CLIENT KEYBOARD LAYOUT OVERRIDE DOES NOT DISPLAY CORRECT TERRITORY
13808564	ADDITIONAL TTAXPE INSTANCE IS STARTED ON LAUNCHING A SHAREABLE APPLICATION
13793464	VDI BROKER LOGS SHOULD INDICATE WHEN THE VDA.CREDENTIAL PROPERTY WAS RECEIVED
13783709	KIOSK DROP DOWN CONTROL IS TOO SLOW
13777898	CORRECT LOGGING AND MAKE IT MORE INFORMATIVE
13768869	TTACPE DUMP CORE PERIODICALLY
13741660	UPGRADE SCRIPTS CANNOT GREP OR COPY OLD PROPERTIES FILE
13721719	REVIEW THE 12296158 CPE FIX
13720573	HTTP STATUS 500 ERROR SEEN WHEN LC_ VARIABLES ARE SET TO C
13707502	TABBING ORDER OF THE UI ELEMENTS OF THE TTATCC PROMPT IS NOT CORRECT
13703100	APPLE KEYBOARD ISSUES
13702339	VDI BROKER: USERS ARE NOT PROMPTED FOR CREDENTIALS WHEN AUTHENTICATION IS DISABLED ON VDI SERVER
13696359	CHANGING THE PREFERRED LANGUAGE TO DE REPLACES EN WITH DE
13680486	SGD CLIENT INSTALLATION WINDOW DOES NOT SHOW THE CONTENTS IN THE PREFERRED LANGUAGE
13635728	AT INSTALL TIME THE SCRIPT CHECKS PORT 80 IS FREE - CHECK 443 AS WELL OR INSTEAD
13635716	CLEAN UP THE END OF INSTALL TEXT
13634040	VDI BROKER DOES NOT DETECT EXPIRED CERTIFICATES UNLESS SEPARATE TRUSTSTORE IS CONFIGURED
13630575	RDP LICENSE POOL: PROFILE SETTING REFERS TO SSGD
13618869	WEBTOP SESSION IDLE TIMEOUT CAN FAIL IN AN ARRAY
13603137	OEL6 SELINUX CONFIGURATION ISSUE CAUSES PROBLEM FOR SGD PRINTING
13596466	ESC: SGD (VDI) SESSION APPEARS TO CRASH WHEN USING PARTICULAR SPREADSHEETS
13596303	ESC: SGD TTATSC (VDI) SESSION APPEARS TO CRASH WHEN USING PIVOT TABLE IN MICROSOFT EXCEL
13583751	KEYSTORE GEN SCRIPT TEST FAILS ON SERVERRENAME OF EXISTING NODE
13582025	SGD BROKER LISTS APPLICATION SERVERS WHICH ARE DISABLED AS LAUNCH CANDIDATES
13525046	ENSURE ALL WINDOWS 2008 R2 AUDIO AND SESSION DIRECTORY CHANGES ARE IN 4.62
13524320	PORT 13422037 TO 4.7 (AGED PASSWORD HANDLER FAILS IN 4.6)

Référence	Description
13520731	CANNOT USE THE SAME BROKER (CONFIGURED DIFFERENTLY) BETWEEN DYNAMIC APP SERVERS
13510249	TARANTELLA PASSCACHE LIST FAILS IN SOME CIRCUMSTANCES WHEN SERVER IS RUNNING
13505639	REMOVE LOCAL LAUNCH
13496613	NUMEROUS TR: WARNING: AN UNESCAPED BACKSLASH MESSAGES INSTALLING SGD ON OEL 6.1
13485736	LDAP SEARCHES FROM THE ADMIN CONSOLE ARE NOT CONFIGURABLE
13474437	MAKE DEVICESTERVICE MORE ROBUST
13465649	REMOVE REXEC AND RCMD TRANSPORTS
13465645	NTLA IS DEPRECATED
13457415	SOLARIS 11: CHANGE ADMINISTRATOR PROFILE TO USE A LOGIN NAME WITH A ROOT ROLE
13451793	PORT 13442124 ADMIN CONSOLE FIX TO 4.7
13451320	PORT TTASHADOW LAUNCH FIXES TO 4.7
13441204	PORT OF 13255477 TO 4.7
13432087	MAC MANUAL INSTALLER WILL REPLACE ANY EXISTING SGD CLIENTS
13424293	LICENSE POOL REMOVAL ON UPGRADE TO 4.7
13414544	RFE: NEW BROKER FOR ACCESSING A TARGET PLATFORM AT LAUNCH TIME
13408097	UNIX SGD CLIENT DIALOG BOXES SHOULD BE CENTRED ON THE PRIMARY MONITOR NOT AT 0,0
13407638	WINDOW COLOR PRESENTATION ATTRIBUTE NEEDS REVIEWING
13403026	AUDIO DEVICE DOES NOT BUILD WITH ORACLE LINUX UEK HEADERS
13390651	AUDIO RECORD AND PLAYBACK IS CHOPPY OVER VPN, BETTER WITH COMPRESSION
13386831	VDI 3.3 BROKER DOES NOT PROMPT FOR CREDENTIALS AGAIN WHEN SESSION HAS EXPIRED
13386823	REMOVE ONLINE HELP FROM THE ADMIN CONSOLE
13386804	REMOVE DOCUMENTATION FROM INSTALLATION PACKAGES
13375588	MAKE DEFAULT XCLOCK APPLICATION SCALABLE
13359188	ALLOW READ TIMEOUTS TO BE CONFIGURED IN THE VDI 3.3 BROKER
13359119	VDI 3.3 BROKER SHOULD LOG TO A SEPARATE FILE BY DEFAULT
13354844	KIOSK MINIMISE BUTTON NOT WORKING
13341364	DO NOT GET LOCKED OUT ERROR AFTER EXHAUSTING FAILED LOGIN ATTEMPTS
13257432	NO SGD CLIENT PANEL CONTROL IN UNITY DESKTOP ON UBUNTU 11.10
13257339	MAC OS X CLIENT UNNECESSARILY VERBOSE ABOUT THE INPUT SERVICE STATE
13248823	TTASHADOW SEGMENTATION VIOLATION
13118977	SEAMLESS WINDOWS: SHOW DESKTOP CAUSING OCCASIONAL VISUAL DEFECTS

Référence	Description
13117053	WINDOWS APPLICATION SESSION IS ENDED ON SGD SERVER BUT IS STILL ALIVE AS AN RDP SESSION
13117046	KIOSK APPLICATION APPEARS IN STRANGE POSITIONS ON A DUAL MONITOR SYSTEM (UBUNTU)
13109118	AD USER IS PROMPTED INCORRECTLY BY SGD TO CHANGE PASSWORD
13097388	PORT OF BUG 12310050
13096064	LOAD BALANCED LAUNCHES ASSIGNED INCORRECT PROFILE FOR LDAP/AD USERS
13087707	INSTALLED SGD CLIENT DOES NOT REMEMBER LOCALE
13065305	RANDR: CAUSES PROBLEMS UNDER COMPIZ
13063591	ESC: VDI BROKER TO WINDOWS 7 VRDP PASSTHROUGH AUTHENTICATION FAILS WITH NON UPN USERNAME
13059922	UNABLE TO LIST CONTENTS OF LIGHT DIRECTORIES FROM COMMAND LINE
13038949	CONFIGURED LDAP OPERATION TIMEOUTS ARE NOT WORKING
13028776	ERROR MESSAGE: THE SGD SERVER URL IS INVALID
13013449	UNNECESSARY LIBXPM DEPENDENCY IN TTATSC
13009764	SGD PRINTING SUBSYSTEM DECLARES PCL PRINTER TO BE POSTSCRIPT PRINTER
12967239	LDAP SEARCHES THAT RETURN SIZE LIMIT EXCEEDED ERROR ARE NOT HANDLED CORRECTLY
12961980	CANNOT INSTALL SGD WINDOWS CLIENT AS A NON-ADMIN USER WITHOUT ADMIN PRIVILEGES
12903943	ADMIN CONSOLE LDAP USER SEARCH FILTER DOES NOT WORK WHEN USING OPENLDAP SERVER.
12863967	TTASHADOW REVIEW
12826145	UNIX CDM FAILS FOR USERS WITH UPPER CASE CHARACTERS
12768524	CREATE A MANUAL INSTALLER FOR THE MAC CLIENT
12768473	UPDATE THE WINDOWS CLIENT'S MANUAL INSTALLER
12768449	UPDATE THE UNIX CLIENT'S MANUAL INSTALLATION SCRIPT
12768390	ALLOW CHOICE OF SGD SERVER WHEN THE SGD CLIENT IS STARTED MANUALLY
12768347	SGD CLIENT HELPER SHOULD MAKE USE OF INSTALLED CLIENTS WHERE POSSIBLE.
12755593	SGD INCORRECTLY REQUIRES GATEWAY NAME TO BE A FULLY-QUALIFIED HOSTNAME
12708195	ESC: ENABLING BILLING SERVICES CAUSES STATUS COMMAND ERROR
12691786	SGD DOCUMENTATION DOES NOT EXPLICITLY STATE SUPPORTED CLIENT REQUIREMENTS
12687906	INCORRECT MESSAGE LOGGED REGARDING ROUTING TOKEN VALIDITY
12667391	CLIENT DRIVE MAPPING: MISLEADING OUT OF MEMORY ERROR MESSAGES WHEN TRYING TO SAVE FILES

Référence	Description
12636349	USER NOT PROMPTED FOR AUTHORIZATION IF NLA FAILS
12633214	SGD FAILS TO HANDLE LDAP USER NAMES WITH SPACES AT THE END OF THEIR DNS
12551476	GATEWAY LOGGING DOCUMENTATION IMPROVEMENTS
12542375	CREATE A VIRTUAL SERVER BROKER COMPATIBLE WITH VDI 3.3
12425312	ESC: AUTHENTICATION CONFIGURATION WIZARD: UNABLE TO CREATE A SERVICE OBJECT
12312532	NULL POINTER EXCEPTION WITHIN EXCEPTION HANDLING
12311743	NULL POINTER EXCEPTION WITH FAST LOGIN/LOGOUT CYCLE.
12310344	SUNBT7032412 POTENTIAL INFINITE LOOP IN DYNAMIC LAUNCH
12310034	SUNBT7031082 ESC: APPLICATION MENUS ARE NOT WORKING AS EXPECTED IN SEAMLESS WINDOWS
12309878	SUNBT7030194 ERROR ON DYNAMIC LAUNCH WHEN CREATING A PERMANENT ENS OBJECT
12309725	SUNBT2207875 ESC: X11 APPLICATIONS DO NOT REDRAW CORRECTLY
12309559	SUNBT7028247 JAVA NOT DETECTED CORRECTLY IN INTERNET EXPLORER 9 (WINDOWS 7)
12309384	SUNBT2207614 ESC: SGD 4.50 GATEWAY PROTOCOL TRANSLATION FAILS FROM HTTPS TO HTTP
12309088	SUNBT2207339 ERROR WHEN BUILDING AUDIO DRIVE ON 64-BIT SUSE 11
12308958	SUNBT7024633 ESC: PRINTING FAILS ON SOLARIS WHEN THE USER CN/DN EXCEEDS 149 CHARACTERS
12308892	SUNBT7024122 TARANTELLA STATUS REPORTS INCORRECT SECURITY STATUS
12308632	SUNBT7022398 90-METER SMART CARD STRING BUFFER SIZE AND AUTO-ALLOCATION FIXES
12308362	SUNBT7020722 ESC: UNABLE TO BROWSE AN AD SERVER VIA THE ADMIN CONSOLE
12308030	SUNBT7018972 ESC: OPENSSEAL COMMAND IN SECURE GLOBAL DESKTOP CANNOT LOAD CONFIG
12307930	SUNBT7018525 SOAP PEER CONNECTIONS ARE NOT ALARMED
12307553	SUNBT7016632 ESC: SGD INSTALLATION FAILS WITH A PERMISSION DENIED ERROR
12307459	SUNBT7016280 DOC: STATEMENT ON ARRAY RECOVER AFTER FAILOVER IS INCORRECT
12307455	SUNBT7016266 DOC: PATH TO SGD WEBSERVICES.JAR IS INCORRECT
12305483	SUNBT7007439 UTTSC CANNOT USE THE CAL STORED BY SGD
12305187	SUNBT7006408 OBSOLETE CLI STILL AVAILABLE
12305168	SUNBT7006334 INCORRECT SECTION LABEL ON PRESENTATION TAB FOR CHARACTER APPLICATIONS
12305011	SUNBT7005437 AUTOMATIC LOGOUT CAN FAIL WHEN AN APPLICATION IS SUSPENDED/RESUMED

Référence	Description
12304276	SUNBT7002124 GATEWAY DOCS NEED CORRECTING FOR CONFIG EDIT COMMANDS THAT ARE A LIST
12304039	SUNBT7000901 PRINTERS AND DRIVES NOT MAPPED FOR WINDOWS APPS
12303980	SUNBT7000586 MULTIPLE DEPENDENCY PROBLEMS WHEN INSTALLING 4.6 ON RHEL 6
12303665	SUNBT2202272 ESC: SINCE UPGRADE TO 4.5, PRINT JOBS INTERMITTENTLY STAY IN PRINT
12303609	SUNBT6998552 USING WEB SERVICES TO CREATE A DYNAMIC APPLICATION SERVER WITH A VSB
12303546	SUNBT2202151 IMPROVE SGD 4.50 COMPATIBILITY WITH WINDOWS SERVER 2008 AND 2008 R2
12302189	SUNBT6990599 LDAP URL FILTER WITHOUT A SEARCH FILTER DOES NOT WORK
12301942	SUNBT6989595 SEPARATOR BARS FOR WEBTOP GROUPS NEED REDUCING IN SIZE
12301940	SUNBT6989592 UPDATE DOCS FOR SPAN MULTIPLE MONITORS OPTION
12301668	SUNBT6988236 WEB.XML FOR ADMINISTRATION CONSOLE STILL REFERS TO SUN
12301484	SUNBT6987242 ACTIVE DIRECTORY CONFIGURATION WRONG AFTER AN UPGRADE
12300978	SUNBT2198455 ESC: RFE: SUPPORT FOR SECURE GLOBAL DESKTOP ENHANCEMENT MODULE
12300864	SUNBT6983054 DYNAMIC DRIVE MAPPING WARNING MESSAGES ONLY IN ENGLISH
12300298	SUNBT6979454 REVIEW DOCUMENTED GHOSTSCRIPT MINIMUM VERSION REQUIREMENTS
12299999	SUNBT6977961 A RUNTIME ERROR HAS OCCURRED WHILE CLICKING ON VERSION
12299915	SUNBT2197077 REVIEW /OPT/TARANTELLA/ETC/DATA/CACERTS.TXT
12299530	SUNBT6975570 CHANGE DEFAULT COLOR DEPTH TO 24/32 FOR WINDOWS APPLICATIONS
12299506	SUNBT6975287 UPGRADE LOG REFERS TO LEGACY TARANTELLA DOCS
12299354	SUNBT6974464 KIOSK APPLICATIONS ON UBUNTU HAVE OS TOOLBARS OVER THE TOP
12298702	SUNBT6971208 DOC NEEDS CORRECTING FOR WINDOWS AUDIO AND SUPPORT FOR HIGHER BITRATES
12298004	SUNBT2195462 TERMINAL SERVICES CALS NOT STORED IN REGISTRY ON WINDOWS 7/VISTA FOR NON-ADMIN USER
12297905	SUNBT6967170 APPLICATION SESSION RESUMABILITY TIMEOUTS NEED CLARIFICATION
12297901	SUNBT6967158 CDE DOES NOT COME UP FOR SOME LOCALIZED ENVIRONMENT FROM SGD
12297796	SUNBT2195370 SECURITY ENABLE WITH A THAWTE TEST CERT FAILS TO ACCEPT ROOT OR INTERMEDIATE CERTIFICATE

Référence	Description
12297749	SUNBT2195328 ESC: AUDIO CANNOT BE HEARD WITH WIN2008 R2 AS THE APPLICATION SERVER
12296804	SUNBT6961989 NON-ASCII CHARACTERS ARE NOT RETURNED TO THE LOGIN BOX
12296679	SUNBT6961333 SGD CLIENT INSTALL DIRECTORY: ORACLE REBRANDING NEEDED
12296343	SUNBT2194331 CAPSLOCK ON FRENCH KEYBOARD GIVES CAPITALISED ACCENTED CHRS
12294323	SUNBT2192822 ESC: DISABLE AUTOCOMPLETE ON LOGIN PAGE TO PREVENT BROWSER CREDENTIALS CACHING
12292967	SUNBT6945810 INTEGRATING SGD WITH ORACLE INTERNET DIRECTORY AS AN LDAP BACKEND
12291675	SUNBT6941088 PRINTING TROUBLESHOOTER NEEDS TO COVER RDP SETTINGS
12261595	SUNBT6802404 GATEWAY DOES NOT REPORT IF PORTS ARE IN USE
12260830	SUNBT6799048 CLOCK SKEWING ON GATEWAY SERVERS CAUSES SESSION LAUNCH FAIL
12218812	SUNBT6632783 MAC OS X SGD CLIENT FAILS TO RUN FROM COMMAND LINE

3.3. Problèmes détectés dans la documentation de la version 4.70

Cette section répertorie les problèmes connus de la version 4.70.

3.3.1. Problèmes détectés dans la documentation du courtier VDI hérité

Le courtier VDI hérité est un courtier de services virtuels permettant à SGD de demander un bureau à partir d'une installation locale Oracle VDI 3.2.

Etant donné que la version 4.70 de SGD ne prend pas en charge la version 3.2 d'Oracle VDI, la description et les procédures de configuration pour le courtier VDI hérité incluses dans la documentation publiée ne sont pas applicables pour cette version de SGD.

3.4. Envoi de commentaires et signalement des problèmes

Cette section indique comment envoyer des commentaires et contacter le support du produit Oracle Secure Global Desktop.

Si vous souhaitez signaler un bogue logiciel ou poser une question, contactez le forum [Secure Global Desktop Software Team and Community Forum](#). La publication sur le forum Secure Global Desktop Software Team and Community Forum ne garantit pas qu'une réponse vous sera envoyée. Si vous avez besoin d'un correctif pour un bogue et que vous avez souscrit un contrat de support Oracle Premier, il est recommandé d'ouvrir un cas auprès du support technique Oracle à l'adresse <https://support.oracle.com>.

Si vous signalez un bogue, renseignez les informations suivantes, le cas échéant :

- Description du problème, en précisant les conditions dans lesquelles il se produit et sa répercussion sur l'opération effectuée.
- Type de l'ordinateur, version du système d'exploitation, type et version du navigateur, environnement linguistique et version du produit, en précisant les patches appliqués, et les autres logiciels ayant éventuellement un impact sur le problème.

- Etapes détaillées de la procédure utilisée, afin de reproduire le problème.
- Les journaux des erreurs ou les dumps noyau éventuels.

3.4.1. Communication avec le support spécialisé Oracle

Si vous disposez d'un numéro CSI Oracle, essayez tout d'abord de résoudre votre problème en utilisant My Oracle Support à l'adresse <https://support.oracle.com>. Votre numéro CSI Oracle Premier Support ne couvre pas le support en cas de personnalisations, de logiciels tiers ou de matériel tiers.

Si vous n'arrivez pas à résoudre le problème, ouvrez un cas auprès de l'équipe de support spécialisé Oracle pour obtenir une assistance technique sur les problèmes de dépannage de la production. L'ingénieur du support technique qui vous répondra aura besoin des informations suivantes pour commencer :

- Votre numéro CSI Oracle.
- Le produit au sujet duquel vous appelez.
- Une brève description du problème pour lequel vous souhaitez obtenir de l'aide.

Si votre numéro CSI est inconnu, trouvez le service d'assistance clientèle pour votre pays (<http://www.oracle.com/us/support/contact-068555.html>), puis contactez les services Oracle pour soumettre une demande de service (SR) non technique pour obtenir votre numéro CSI. Une fois que vous disposez d'un numéro CSI, vous pouvez poursuivre et ouvrir un cas via My Oracle support.

