

Notes de version de Sun Secure Global Desktop 4.4

Sun Microsystems, Inc.
www.sun.com

Part No. 820-2810-10
Octobre 2007, révision 01

Adressez vos commentaires à l'adresse : <http://docs.sun.com/app/docs/form/comments>

Copyright 2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, États-Unis. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs aux technologies décrites dans le présent document. En particulier, et sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains répertoriés sur le site <http://www.sun.com/patents> et un ou plusieurs brevets supplémentaires ou dépôts de brevets en cours d'homologation aux États-Unis et dans d'autres pays.

Ce produit et ce document sont protégés par des licences qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses concédants de licence, le cas échéant.

Le logiciel tiers, y compris sa technologie relative aux polices de caractère, est protégé par un copyright et une licence des fournisseurs de Sun.

Des parties du produit peuvent être dérivées de systèmes Berkeley-BSD, sous licence de l'Université de Californie. UNIX est une marque déposée aux États-Unis et dans d'autres pays, sous licence exclusive de X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, JavaScript, SunSolve, JavaServer, JSP, JDK, JRE, Sun Ray et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux États-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux États-Unis et dans d'autres pays. Les produits portant les marques SPARC utilisent une architecture développée par Sun Microsystems, Inc.

Adobe est la marque déposée de Adobe Systems, Incorporated.

L'interface utilisateur graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et détenteurs de licence. Sun reconnaît le travail précurseur de Xerox en matière de recherche et de développement du concept d'interfaces utilisateur visuelles ou graphiques pour le secteur de l'informatique. Sun détient une licence Xerox non exclusive sur l'interface utilisateur graphique Xerox. Cette licence englobe également les détenteurs de licences Sun qui implémentent l'interface utilisateur graphique OPEN LOOK et qui, en outre, se conforment aux accords de licence écrits de Sun.

Droits du gouvernement américain - usage commercial. Les utilisateurs gouvernementaux sont soumis au contrat de licence standard de Sun Microsystems, Inc. et aux dispositions du Federal Acquisition Regulation (FAR, règlements des marchés publics fédéraux) et de leurs suppléments.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, REPRÉSENTATIONS ET GARANTIES EXPRESSES OU TACITES, Y COMPRIS TOUTE GARANTIE IMPLICITE RELATIVE À LA COMMERCIALISATION, L'ADÉQUATION À UN USAGE PARTICULIER OU LA NON-VIOLATION DE DROIT, SONT FORMELLEMENT EXCLUES. CETTE EXCLUSION DE GARANTIE NE S'APPLIQUERAIT PAS DANS LA MESURE OÙ ELLE SERAIT TENUE JURIDIQUEMENT NULLE ET NON AVENUE.



Please
Recycle



Adobe PostScript

Table des matières

Préface ix

1. Configuration système requise et éléments pris en charge 1

Matériel requis 2

Configuration requise du système d'exploitation 3

Modifications du système d'exploitation 3

Configuration de serveur Web requise 5

Configuration réseau requise 5

Configuration requise du client 7

Configuration requise du module d'enrichissement SGD 9

Types d'applications prises en charge 10

Protocoles pris en charge 10

Prise en charge de la sécurité 11

Prise en charge du serveur proxy 12

Méthodes d'authentification prises en charge 13

Authentification SecurID 13

Serveurs de répertoire LDAP pris en charge 13

Prise en charge de l'impression 14

Prise en charge des cartes à puce 15

2. Nouvelles fonctions et modifications 17

Nouvelles fonctions de la version 4.40 17

Console d'administration SGD 17

URL Desktop Direct 20

Prise en charge des profils utilisateur itinérant 21

Délai d'attente automatique pour les sessions utilisateur inactives 22

Filtres de masque de réseau pour la spécification d'adresses réseau 22

Touches de gestion des fenêtres 23

Prise en charge de SE Solaris 10 Trusted Extensions 23

Gestion globale des mots de passe et des jetons 24

Noms d'objet alternatifs pour les certificats de serveur 24

Attribut de fichier de mappage des fuseaux horaires 24

Nouvelles fonctions de la version 4.31 25

Prise en charge du format audio dans les applications X 25

Prise en charge du Bureau à distance de Microsoft Windows Vista 26

Paramètres clients SSH 26

Nouvelles fonctions de la version 4.30 27

Intégration au menu de démarrage du bureau 27

Connexion unique 28

Gestion des configurations client à l'aide de profils 28

Configuration du serveur proxy mobile 29

Amélioration de la ligne de commande pour le client SGD 30

Installation manuelle du client SGD 30

Nouveau serveur X 31

Nouvel attribut de l'extension de sécurité X 32

Impression de PDF pour les clients UNIX, Linux et Mac OS X 32

Mappage du disque client pour la plate-forme UNIX et les applications
LINUX 33

Prise en charge des ports série dans les applications Windows 34

Prise en charge du Bureau à distance de Microsoft Windows XP Professionnel	34
Prise en charge des connexions à la session de console avec les services de terminal Windows Server 2003	35
Connexion initiale sécurisée	35
Protection des clients contre les serveurs non autorisés	36
Contrôle des copier-coller	36
Prise en charge de SecurID pour l'authentification du serveur d'application	37
Interface utilisateur localisée	37
Documentation traduite	38
Prise en charge des langues dans les scripts Expect	38
Modifications dans la version 4.40	39
Modifications apportées aux plates-formes d'installation prises en charge	39
Retrait des clients classiques	39
Séquence de connexion et d'authentification	40
Certificats de serveur et noms DNS externes multiples	40
Modifications des services Web	40
Remise à niveau du cache Kerberos	44
Commande <code>tem status</code>	44
Java non pris en charge par le client SGD par défaut	45
Informations sur les fichiers journaux client SGD des périphériques client	45
Arguments de la ligne de commande renommés	46
Attribut Domaine Windows NT	46
Imprimantes PDF renommées	47
Avertissement de fermeture de la fenêtre	47
Proxy SOCKS supprimé du profil client	47
Outils d'administration supprimés du bureau Web de l'administrateur	48
Modifications du script de connexion	48
Activation des méthodes d'entrée pour les environnements linguistiques	49

Délais d'expiration de client SGD	49
Modifications dans la version 4.31	50
Authentification SecurID sur les plates-formes Solaris x86	50
Prise en charge de plusieurs serveurs SGD en mode intégré	50
Routage des baies	50
Scripts de démarrage de SGD	51
Message de connexion initiale non autorisée	51
Touche Windows désactivée	51
Modifications dans la version 4.30	52
Package d'installation unique	52
Démon SSL actif en permanence	52
Fichier de préférences utilisateur sur les périphériques client UNIX, Linux et Mac OS X	52
Attribut de fermeture de fenêtre (--windowclose)	52
Prise en charge de PAM pour l'authentification des utilisateurs UNIX	53
Impression de PDF	53
Certificats client pour l'authentification Active Directory	54
Magasin de certificats SGD	54
Octroi de licence	54
Méthodes de connexion aux applications	54
Attribut des connexions simultanées au bureau Web	55
Applications mainframe (3270)	55
3. Produits pris en charge, problèmes connus, résolution de bogues et problèmes détectés dans la documentation	57
Produits n'étant plus pris en charge	58
Problèmes et bogues connus	58
602423 : Problèmes liés à la touche retour et à la touche Entrée du pavé numérique	58
6443840 : échec de configuration automatique de scripts du serveur proxy	59

6448990 : problèmes avec les touches \ (backslash) et ¥ (Yen)	60
6456278 : le mode intégré ne fonctionne pas pour l'utilisateur root	61
6458111 : le menu principal Gnome s'arrête brutalement en cas d'utilisation du mode intégré	61
6461864 et 6476661 : échec de la connexion automatique et du mode intégré avec le bureau Gnome	62
6468716 : le clavier ne fonctionne pas pendant les sessions Gnome	62
6470197 : échec de la compilation du module serveur Web SGD	63
6476194 : aucun élément de menu de KDE Desktop pour le client SGD	63
6477187 : le mappage du disque client échoue sans le service Client pour les réseaux Microsoft	64
6481312 : la mise à niveau réinitialise les types de connexion disponibles	64
6482912 : le client SGD n'est pas installé automatiquement	65
6493374 : caractères non ASCII dans les fenêtres de méthode d'entrée	65
6542943 : Firefox échoue avec l'outil Sun Java Plug-in version 1.5	66
6555834 : Java est activé pour le navigateur mais n'est pas installé sur le périphérique client	66
6591516 : les transitions de pages du bureau Web ne fonctionnent pas dans Internet Explorer	67
6592560 : l'aide en ligne de la console d'administration n'est pas disponible avec le protocole HTTPS	67
6598048 : le clavier français (Canada) n'est pas correctement mappé pour les applications Windows	68
6605404 : le fichier de ressources Tomcat a changé d'emplacement	68
6609001 : il est impossible de séparer un serveur secondaire arrêté à l'aide de la console d'administration	69
6609518 : lien à la baie lorsque la console d'administration est en cours d'exécution à partir d'un serveur secondaire	69
6610760 : les paramètres personnalisés de l'imprimante PDF ne sont pas respectés dans les applications Windows	70
6611502 : des erreurs se produisent lors de la création ou de la modification d'objets à partir d'un serveur secondaire	70

Problèmes liés au clavier japonais Sun Type 7	71
Les éléments du menu Démarrer ne sont pas triés par ordre alphabétique	71
Absence d'entrées du menu de démarrage sur Sun Java Desktop System	72
Résolution de bogues dans la version 4.40	72
Résolution de bogues dans la version 4.31	74
Résolution de bogues dans la version 4.30	75
Outils d'administration	76
Échec de lancement	76
Clients et bureau Web	77
Émulation	78
Installation et mise à niveau	79
Internationalisation et localisation	79
Autre	80
Impression	81
Sécurité	81
Serveur	82
Authentification des utilisateurs	82
Services Web	83
Problèmes liés à la documentation dans la version 4.40	84
Modifications apportées à l'onglet Profils des utilisateurs assignés	84
Le fichier de ressources Tomcat a changé d'emplacement	84
Délai d'attente automatique pour les sessions utilisateur inactives	85
Options de la commande (<code>--displayusing</code>) de type de fenêtre	85
Des erreurs se produisent lors de la création ou de la modification d'objets à partir d'un serveur secondaire	86
Création d'entrées dans le cache des mots de passe	86
Corrections apportées à la page Sécurisation des connexions SOAP vers un serveur SGD	88

Préface

Les *Notes de version de Sun Secure Global Desktop 4.4* fournissent des informations relatives à la configuration système requise, à l'assistance, ainsi qu'aux nouvelles fonctions et modifications pour cette version du logiciel Sun Secure Global Desktop (SGD). Ce document est destiné aux administrateurs système.

Utilisation des commandes système

Ce document peut contenir des informations relatives aux commandes et procédures UNIX® de base, par exemple pour arrêter ou initialiser le système, ou pour configurer des périphériques. Pour obtenir les informations correspondantes, reportez-vous à la documentation du système. Cependant, ce document contient des informations relatives à certaines commandes SGD.

Invites de shell

Shell	Invite
C shell	<i>nom_machine%</i>
Superutilisateur de C shell	<i>nom_machine#</i>
Bourne shell et Korn shell	\$
Superutilisateur de Bourne shell et Korn shell	#

Conventions typographiques

Style*	Signification	Exemples
AaBbCc123	Noms de commandes, fichiers et répertoires ; sorties à l'écran	Modifiez le fichier <code>.login</code> . Exécutez la commande <code>ls -a</code> pour afficher la liste des fichiers. % You have mail.
AaBbCc123	Saisies utilisateur (pour les différencier des sorties à l'écran)	% su Mot de passe :
<i>AaBbCc123</i>	Titres de documents, mots ou termes nouveaux ; mise en évidence de mots dans le texte Remplacez les variables de ligne de commande par les valeurs ou noms adéquats.	Reportez-vous au chapitre 6 du <i>Guide de l'utilisateur</i> . Ce sont les <i>options de classe</i> . Pour supprimer un fichier, tapez rm <i>nomfichier</i> .

*. Dans votre navigateur, les paramètres peuvent être différents.

Documentation connexe

Les documents disponibles en ligne sont accessibles à partir de la page Web <http://docs.sun.com/app/docs/coll/170612>.

Application	Titre	Numéro de référence	Format	Emplacement
Installation	<i>Guide d'installation de Sun Secure Global Desktop 4.4</i>	820-2815-10	HTML	En ligne
			PDF	En ligne et CD du logiciel
Administration	<i>Sun Secure Global Desktop 4.4 Administration Guide</i>	820-2550	HTML	En ligne
Référence	<i>Sun Secure Global Desktop 4.4 Reference Manual</i>	820-2551	HTML	En ligne
			PDF	En ligne
Utilisateur	<i>Guide de l'utilisateur de Sun Secure Global Desktop 4.4</i>	820-2822-10	HTML	En ligne

Vos commentaires sont les bienvenus

Chez Sun, nous tenons à améliorer en permanence la documentation et nous sommes ravis de recevoir vos commentaires et suggestions. Pour nous les faire parvenir, envoyez un e-mail à l'adresse suivante : <http://docs.sun.com/app/docs/Form/comments>.

Veuillez inclure le titre du document et son numéro de référence (*Notes de version de Sun Secure Global Desktop 4.4*, numéro de référence 820-2810-10) dans l'objet de votre courrier électronique.

Configuration système requise et éléments pris en charge

Ce chapitre contient la configuration système requise pour l'installation et l'utilisation de SGD version 4.40.

Il est constitué des rubriques suivantes :

- [Matériel requis, page 2](#)
- [Configuration requise du système d'exploitation, page 3](#)
- [Configuration de serveur Web requise, page 5](#)
- [Configuration réseau requise, page 5](#)
- [Configuration requise du client, page 7](#)
- [Configuration requise du module d'enrichissement SGD, page 9](#)
- [Types d'applications prises en charge, page 10](#)
- [Protocoles pris en charge, page 10](#)
- [Prise en charge de la sécurité, page 11](#)
- [Prise en charge du serveur proxy, page 12](#)
- [Méthodes d'authentification prises en charge, page 13](#)
- [Prise en charge de l'impression, page 14](#)
- [Prise en charge des cartes à puce, page 15](#)

Matériel requis

Les données ci-dessous sont fournies à titre indicatif et votre matériel ne doit pas répondre strictement à cette configuration. Pour de plus amples informations sur le matériel requis, contactez un SGD sales office (<http://www.sun.com/secure/contact/>).

Pour connaître la configuration requise sur un serveur hébergeant SGD, vous devez estimer l'*ensemble* des besoins suivants :

- Installation et exécution de SGD
- Connexion utilisateur à SGD et exécution d'applications

La configuration requise pour installer et exécuter SGD est la suivante :

- 256 Mo d'espace disque disponible, 300 Mo de plus au moment de l'installation ;
- 256 Mo de mémoire vive (RAM, Random Access Memory) ;
- un processeur de 1 GHz ;
- une carte d'interface réseau (NIC, Network Interface Card).

Il s'agit d'éléments *supplémentaires* à la configuration requise pour le système d'exploitation, en partant du principe que le serveur est exclusivement utilisé pour SGD.

Pour se connecter à SGD et exécuter des applications, les utilisateurs doivent disposer de la configuration système suivante :

- 20 Mo minimum pour chaque utilisateur ;
- 15 MHz par utilisateur (plates-formes SPARC®) ;
- 20 MHz par utilisateur (plates-formes x86).



Attention – La mémoire et l'unité de calcul centrale (CPU, Central Processing Unit) requises dépendent considérablement des applications utilisées.

Configuration requise du système d'exploitation

Le tableau suivant donne la description des plates-formes d'installation prises en charge pour SGD.

Système d'exploitation	Versions prises en charge
Système d'exploitation Solaris™ (SE Solaris) sur plates-formes SPARC	8, 9, 10, 10 Trusted Extensions
SE Solaris sur plate-forme x86	10, 10 Trusted Extensions
Red Hat Enterprise Linux (Intel x86 32 bits)	4, 5
Fedora Linux (Intel x86 32 bits)	7
SUSE Linux Enterprise Server (Intel x86 32 bits)	9, 10

Modifications du système d'exploitation

Des modifications du système d'exploitation peuvent s'avérer nécessaires. Sans ces modifications, l'installation et le fonctionnement de SGD risquent d'être altérés.

Messages localisés lors de l'installation de SGD sur les plates-formes Linux

Lorsque vous installez SGD sur une plate-forme Linux, les messages localisés dans les langues prises en charge s'affichent uniquement si le package `gettext` a été installé au préalable. Dans le cas contraire, l'installation s'exécute en anglais.

Fedora 7

L'installation de SGD échoue si la bibliothèque `libXp.so.6` n'est pas disponible sur le serveur. Cette bibliothèque a été abandonnée dans Fedora Core 3. Cependant, le fichier reste disponible dans le package `libXp`.

Applications 5250 et 3270

La prise en charge des applications 5250 et 3270 requiert la bibliothèque `libXm.so.3`. Cette bibliothèque est disponible dans le package OpenMotif 2.2.

SUSE Linux Enterprise Server 9 avec Service Pack 2

L'installation de SGD échoue si la bibliothèque `libgdbm.so.2` n'est pas disponible sur le serveur. SUSE Linux Enterprise Server 9 avec Service Pack 2 contient la version 3 de la bibliothèque par défaut. Procurez-vous la version 2 de la bibliothèque et installez-la avant l'installation de SGD.

SUSE Linux Enterprise Server 10

L'installation de SGD échoue si les bibliothèques `libgdbm.so.2` et `libexpat.so.0` ne sont pas disponibles sur le serveur. Par défaut, SUSE Linux Enterprise Server 10 contient les versions 3 et 1 de ces bibliothèques. Obtenez et installez les versions requises de ces bibliothèques avant l'installation de SGD.

SE Solaris 8, 9 et 10

Installez au moins la distribution End User SE Solaris afin d'obtenir les bibliothèques requises par SGD. Sinon, SGD ne s'installera pas.

L'installation de SGD échoue si la bibliothèque `/usr/lib/libsendfile.so` n'est pas disponible sur le serveur. Cette bibliothèque peut être incluse dans le package Core Solaris Libraries (`SUNWcsl`). Dans le cas contraire, appliquez le patch 111297 pour l'obtenir.

Pseudopériphérique `/dev/random` de SE Solaris 8

Les utilisateurs risquent de ne pas pouvoir se connecter à SGD sur les plates-formes SE Solaris 8 si le pseudopériphérique `/dev/random` est absent du serveur. Vous devrez éventuellement installer le patch 112438 pour obtenir ce périphérique.

Configuration de serveur Web requise

Le serveur Web constitue un élément essentiel de l'installation SGD et ils sont installés simultanément. Le serveur Web SGD est un serveur Web Apache préconfiguré pour l'utilisation avec SGD. Il comprend les éléments répertoriés dans le tableau suivant.

Composant	Versio n
Apache HTTP Server	1.3.36
mod_ssl	2.8.27
OpenSSL	0.9.8d
mod_jk	1.2.15
Apache Jakarta Tomcat	5.0.28
Apache Axis	1.2

Vous pouvez utiliser votre propre serveur Web avec SGD. Pour savoir comment procéder, reportez-vous au *Guide d'administration de Sun Secure Global Desktop 4.4*.

Configuration réseau requise

Vous devez configurer votre réseau en vue d'une utilisation avec SGD.
Vous trouverez ci-après les exigences principales :

- Les serveurs SGD doivent présenter des entrées DNS (Domaine Name System, système de noms de domaine) résolubles par chacun des clients.
- La recherche DNS (normale ou inverse) d'un serveur SGD ne doit jamais échouer.
- Tous les périphériques client doivent utiliser DNS.
- Les périphériques client doivent pouvoir établir des connexions TCP/IP (Transmission Control Protocol/Internet Protocol, protocole de contrôle de transmission/protocole Internet) vers SGD, via les ports TCP suivants :
 - **80** : port dédié aux connexions HTTP (Hypertext Transfer Protocol, protocole de transfert hypertexte) entre les périphériques client et le serveur Web SGD. Le numéro de port peut varier selon le port sélectionné à l'installation.

- **443** : port dédié aux connexions HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer, protocole de transfert hypertexte sécurisé) entre les périphériques client et le serveur Web SGD.
- **3144** : port dédié aux connexions standard (non chiffrées) entre les périphériques client et SGD.
- **5307** : port dédié aux connexions sécurisées entre les périphériques client et SGD. Les connexions sécurisées utilisent le protocole SSL (Secure Sockets Layer, couche de sockets sécurisée).

Remarque – La connexion initiale entre un périphérique client et SGD est *toujours* sécurisée. Une fois l'utilisateur connecté à SGD, la connexion devient une connexion standard. Lors de la première installation de SGD, les ports TCP 3144 et 5307 doivent être ouverts pour assurer la connexion à SGD. Vous pouvez configurer SGD de manière à toujours utiliser des connexions sécurisées.

- Pour exécuter des applications, SGD doit être à même d'établir des connexions TCP/IP vers des serveurs d'application. Les types d'application à exécuter déterminent les ports TCP à ouvrir. Par exemple :
 - **22** : port dédié aux applications X et aux applications à traitement de caractères utilisant SSH (Secure Shell, shell sécurisé) ;
 - **23** : port dédié aux applications X et Windows et aux applications à traitement de caractères utilisant Telnet ;
 - **3389** : port dédié aux applications Windows utilisant les services Terminal Server de Windows ;
 - **6010 et supérieur** : port dédié aux applications X.

Le *Guide d'administration de Sun Secure Global Desktop 4.4* contient des informations détaillées sur les ports utilisés par SGD et sur l'utilisation de SGD avec des pare-feu.

Configuration requise du client

Pour utiliser le bureau Web à l'adresse `http://exemple.serveur.com/sgd`, où *exemple.serveur.com* correspond au nom d'un serveur SGD, vous devez disposer du client SGD et d'un navigateur Web pris en charge.

Le client SGD peut fonctionner en deux modes :

- **Mode bureau Web** : le client SGD affiche les commandes de SGD dans une page Web spéciale (bureau Web). C'est le mode par défaut.
- **Mode intégré** : le client SGD affiche les commandes de SGD dans le menu de démarrage du bureau. D'autres facteurs de configuration peuvent contribuer à l'utilisation d'un navigateur Web pour l'authentification initiale et la recherche des paramètres de serveur proxy.

Les plates-formes client, les navigateurs Web et les systèmes de menu pris en charge lorsque le client SGD fonctionne en mode intégré sont répertoriés dans le tableau suivant :

Plates-formes client prises en charge	Navigateurs client pris en charge	Prise en charge du mode intégré
Microsoft Windows Vista	Internet Explorer 7.0+ Mozilla 1.5+ Mozilla Firefox 2.0+	Menu Démarrer de Microsoft Windows
Microsoft Windows XP Professionnel	Internet Explorer 6.0+, 7.0+ Mozilla 1.5+ Mozilla Firefox 2.0+	Menu Démarrer de Microsoft Windows
Microsoft Windows 2000 Professionnel	Internet Explorer 6.0+, 7.0+ Mozilla 1.5+ Mozilla Firefox 2.0+	Menu Démarrer de Microsoft Windows
SE Solaris 8+ sur plate-forme SPARC	Mozilla 1.5+ Mozilla Firefox 2.0+	Menu de démarrage de Sun Java Desktop System
SE Solaris 10 Trusted Extensions sur plate-forme SPARC	Mozilla 1.5+ Mozilla Firefox 2.0+	Non pris en charge
SE Solaris 10 sur plate-forme x86	Mozilla 1.5+ Mozilla Firefox 2.0+	Menu de démarrage de Sun Java Desktop System
Mac OS X 10.4+	Safari 2.0+ Mozilla Firefox 2.0+	Non pris en charge
Fedora Linux 7 (Intel x86 32 bits)	Mozilla 1.5+ Mozilla Firefox 2.0+	Menu Démarrer de Gnome ou de KDE

Plates-formes client prises en charge	Navigateurs client pris en charge	Prise en charge du mode intégré
Red Hat Desktop version 4	Mozilla 1.5+ Mozilla Firefox 2.0+	Menu Démarrer de Gnome ou de KDE
SUSE Linux Enterprise Desktop 10	Mozilla 1.5+ Mozilla Firefox 2.0+	Menu Démarrer de Gnome ou de KDE
Ubuntu 7.04	Mozilla 1.5+ Mozilla Firefox 2.0+	Menu Démarrer de Gnome

Les versions Bêta et les versions précédentes des navigateurs Web ne sont pas prises en charge.

JavaScript™ doit être activé pour les navigateurs Web.

De même, la technologie Java doit être activée pour leur permettre :

- de télécharger et d'installer automatiquement le client SGD ;
- de déterminer les paramètres du serveur proxy à partir du navigateur Web par défaut de l'utilisateur.

Si la technologie Java n'est pas disponible, le client SGD peut être téléchargé et installé manuellement.

Les plug-ins pris en charge pour la technologie Java sont les suivants :

- outil Sun Java Plug-in version 1.6.0.
- outil Sun Java Plug-in version 1.5.0.

Remarque – Les plates-formes Microsoft Windows Vista ne prennent en charge *que* l'outil Sun Java Plug-in version 1.6.0.

Lorsque les utilisateurs démarrent plusieurs sessions utilisateur à l'aide du même périphérique et du même navigateur Web, les sessions utilisateur se lient. En d'autres termes, l'ouverture de la nouvelle session ne ferme pas la session existante. Pour que les sessions se lient ainsi, le navigateur Web doit être configuré afin d'autoriser les cookies permanents. Dans le cas contraire, les sessions utilisateur sont toujours fermées et cela peut entraîner la fermeture des fenêtres d'application.

Pour des résultats optimaux, configurez les périphériques client en 256 couleurs minimum.

Le mappage de port série n'est pris en charge que sur les plates-formes UNIX, Linux et Microsoft Windows.

Configuration requise du module d'enrichissement SGD

Le module d'enrichissement SGD est un composant logiciel à installer sur un serveur d'application afin de doter SGD des fonctionnalités suivantes :

- équilibrage de charge avancé ;
- mappage de disque client (CDM, Client Drive Mapping) ;
- fenêtres transparentes (plates-formes Windows uniquement) ;
- audio (plates-formes UNIX ou Linux uniquement).

Les plates-formes d'installation prises en charge par le module d'enrichissement SGD sont les suivantes :

Système d'exploitation	Versions prises en charge
Microsoft Windows	Windows Server 2003 Windows 2000 Server Microsoft Windows XP Professionnel* Microsoft Windows Vista Edition intégrale* Microsoft Windows Vista Professionnel*
SE Solaris sur plate-forme SPARC	8, 9, 10, 10 Trusted Extensions\
SE Solaris sur plate-forme x86	10, 10 Trusted Extensions\
Red Hat Enterprise Linux (Intel x86 32 bits)	4, 5
Fedora Linux (Intel x86 32 bits)	7
SUSE Linux Enterprise Server (Intel x86 32 bits)	9, 10

* Les plates-formes Microsoft Windows XP Professionnel et Microsoft Windows Vista prennent uniquement en charge le mappage du disque client. Les fenêtres transparentes et la fonction avancée d'équilibrage de charge ne sont pas prises en charge. Seules les sessions de bureau Windows complètes sont prises en charge, pas les applications.

\ Sur les plates-formes SE Solaris 10 Trusted Extensions, l'audio et le mappage du disque client ne sont pas pris en charge.

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

Types d'applications prises en charge

SGD permet d'accéder aux applications suivantes :

- Microsoft Windows ;
- applications à traitement de caractères s'exécutant sur SE Solaris, Linux, HP-UX et AIX ;
- applications X s'exécutant sur SE Solaris, Linux, HP-UX et AIX ;
- IBM mainframe et AS/400 ;
- applications Web (utilisant HTML et la technologie Java).

Protocoles pris en charge

SGD assure la prise en charge des protocoles suivants :

- Microsoft RDP (Remote Desktop Protocol, protocole de bureau distant) version 5.2 ;
- X11 ;
- HTTP ;
- HTTPS ;
- SSH version 2 ou ultérieure ;
- ICA (Citrix Independent Computing Architecture, architecture de programmation indépendante) ;
- Telnet VT, ANSI (American National Standards Institute, institut américain des normes nationales) ;
- TN3270E ;
- TN5250.

Prise en charge de la sécurité

SGD assure la prise en charge des connexions sécurisées en provenance de clients utilisant les protocoles suivants :

- SSL version 3.0
- TLS (Transport Layer Security, sécurité des couches de transport) version 1.0.

Les suites de chiffrement suivantes sont prises en charge :

- 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 .

SGD assure la prise en charge des certificats X.509 au format PEM utilisant le codage en base 64, signés par l'un des certificats d'autorités de certification (ou certificats racine) suivants :

- Baltimore CyberTrust Code Signing Root ;
- Baltimore CyberTrust Root ;
- Entrust.net CA ;
- Entrust.net Client CA 1 ;
- Entrust.net Client CA 2 ;
- Entrust.net Server CA 1 ;
- Entrust.net Server CA 2 ;
- Equifax Secure CA ;
- Equifax Secure eBusiness CA 1 ;
- Equifax Secure eBusiness CA 2 ;
- Equifax Secure Global eBusiness CA ;
- GeoTrust Global CA ;
- The Go Daddy Group, Inc. Class 2 CA ;
- GTE CyberTrust Root ;
- GTE CyberTrust Global Root ;
- GTE CyberTrust Root 5 ;
- Starfield Technologies, Inc. Class 2 CA ;
- Thawte Personal Basic CA ;

- Thawte Personal Freemail CA ;
- Thawte Personal Premium CA ;
- Thawte Premium CA ;
- Thawte Server CA ;
- <http://www.valicert.com> ;
- VeriSign Class 1 Public Primary CA - G1 ;
- VeriSign Class 1 Public Primary CA - G2 ;
- VeriSign Class 1 Public Primary CA - G3 ;
- VeriSign Class 2 Public Primary CA - G1 ;
- VeriSign Class 2 Public Primary CA - G2 ;
- VeriSign Class 2 Public Primary CA - G3 ;
- VeriSign Class 3 Public Primary CA - G1 ;
- VeriSign Class 3 Public Primary CA - G2 ;
- VeriSign Class 3 Public Primary CA - G3 ;
- VeriSign Class 4 Public Primary CA - G2 ;
- VeriSign Class 4 Public Primary CA - G3 ;
- VeriSign/RSA Secure Server.

D'autres types de certificat peuvent être pris en charge via l'installation du certificat d'autorité de certification (le certificat racine) pour cette autorité de certification (AC).

Prise en charge du serveur proxy

Si vous souhaitez utiliser SGD avec un serveur proxy, celui-ci doit assurer la prise en charge de la mise sous tunnel.

Pour le bureau Web, vous avez le choix entre les serveurs proxy HTTP, Secure (SSL) et SOCKS v5.

Pour les serveurs proxy SOCKS v5, SGD prend en charge deux méthodes d'authentification : authentification de base et aucune authentification requise.

Méthodes d'authentification prises en charge

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

- LDAP (Lightweight Directory Access Protocol, protocole léger d'accès aux répertoires) version 3 ;
- Microsoft Active Directory ;
- NIS (Network Information Service, service d'informations réseau) ;
- Microsoft Windows Domains ;
- RSA SecurID ;
- authentification de serveur Web (authentification HTTP/HTTPS de base), avec les certificats de client de PKI (Public Key Infrastructure, infrastructure de clé publique).

Authentification SecurID

SGD fonctionne avec les versions 4, 5 et 6 du RSA Authentication Manager (précédemment nommé RSA ACE/Server).

Serveurs de répertoire LDAP pris en charge

SGD assure la prise en charge de la version 3 du protocole standard LDAP. Vous pouvez utiliser l'authentification LDAP et les méthodes de recherche LDAP pour l'authentification de tiers, quel que soit le serveur de répertoire utilisé (compatible avec LDAP version 3-). SGD prend en charge cette fonctionnalité sur les serveurs de répertoire suivants :

- Sun Java&trade ; System Directory Server version 4.1+ (appelé auparavant Sun ONE, Netscape™ ou iPlanet Directory Server) ;
- Microsoft Active Directory.

D'autres serveurs de répertoire sont également susceptibles de fonctionner, mais ne sont pas pris en charge.

L'authentification Active Directory n'est prise en charge que sur les serveurs Microsoft Active Directory.

La fonctionnalité d'intégration des services d'annuaire (parfois appelée génération de bureau Web) est prise en charge sur les serveurs de répertoire suivants :

- Sun Java™ System Directory Server version 4.1+ (appelé auparavant Sun ONE, Netscape ou iPlanet Directory Server) ;
- Microsoft Active Directory.

D'autres serveurs de répertoire sont également susceptibles de fonctionner, mais ne sont pas pris en charge.

Prise en charge de l'impression

SGD prend en charge l'impression vers PostScript, PCL (Printer Command Language, langage de commande d'impression) et les imprimantes texte connectées au périphérique client de l'utilisateur.

Le script SGD `tta_print_convert` effectue les conversions requises pour formater les travaux d'impression en fonction de l'imprimante client. Pour la conversion de Postscript à PCL, Ghostscript doit être installé sur le serveur SGD.

Vous devez installer Ghostscript 6.52 ou une version plus récente sur le serveur SGD afin d'assurer la prise en charge de l'impression PDF (Portable Document Format) SGD. La distribution Ghostscript doit inclure le programme `ps2pdf`. Les périphériques client Microsoft Windows doivent disposer d'Adobe Reader version 4.0 ou plus récente.

SGD assure la prise en charge de l'impression avec CUPS (Common Unix Printing System, système d'impression Unix commun). Vous devez installer CUPS (version 1.1.19 minimum) sur le serveur SGD. Il faut également procéder à d'autres opérations de configuration.

Lors de l'impression à partir d'une application Windows faisant appel au protocole Microsoft RDP, Secure Global Desktop prend en charge les mêmes imprimantes que le serveur d'application Microsoft Windows.

Prise en charge des cartes à puce

SGD permet aux utilisateurs d'accéder à un lecteur de cartes à puce connecté à leur périphérique client à partir d'applications s'exécutant sur un serveur d'application Windows Server 2003. Les utilisateurs peuvent :

- se connecter à un serveur Windows Server 2003 à l'aide d'une carte à puce ;
- accéder aux données résidant sur une carte à puce tout en utilisant une application s'exécutant sur un serveur Windows 2003, par exemple afin d'utiliser un certificat pour la signature ou le chiffrement d'un e-mail.

SGD fonctionne avec tout type de lecteur et de carte à puce compatibles PCSC (Personal Computer/Smart Card, ordinateur personnel/carte à puce).

La connexion à un serveur d'application Windows Server 2003 à l'aide d'une carte à puce a été testée pour les cartes à puce répertoriées dans le tableau suivant :

Système d'exécution client et bibliothèques	Carte à puce
Microsoft Windows XP Vista	ActivCard 64K CryptoFlex 32K GemPlus GPK16000
Microsoft Windows XP Professionnel	ActivCard 64K CryptoFlex 32K GemPlus GPK16000
Microsoft Windows 2000 Professionnel	ActivCard 64K CryptoFlex 32K GemPlus GPK16000
SE Solaris avec package PCSC Bypass client léger Sun Ray™ (SUNWsrcbp)	ActivCard 64K CryptoFlex 32K
Fedora Linux avec pcsc-lite 1.2.0	ActivCard 64K CryptoFlex 32K GemPlus GPK16000

Nouvelles fonctions et modifications

Ce chapitre décrit les nouvelles fonctions et modifications apportées aux versions 4.40, 4.31 et 4.30 de Secure Global Desktop.

Il est constitué des rubriques suivantes :

- [Nouvelles fonctions de la version 4.40, page 17](#)
- [Nouvelles fonctions de la version 4.31, page 25](#)
- [Nouvelles fonctions de la version 4.30, page 27](#)
- [Modifications dans la version 4.40, page 39](#)
- [Modifications dans la version 4.31, page 50](#)
- [Modifications dans la version 4.30, page 52](#)

Nouvelles fonctions de la version 4.40

Cette section décrit les nouvelles fonctions intégrées au logiciel Sun Secure Global Desktop version 4.40.

Console d'administration SGD

Le gestionnaire d'objets, le gestionnaire de baies, l'assistant de configuration et le gestionnaire de sessions, utilisés par SGD en tant qu'outils d'administration, ont été remplacés par la console d'administration SGD. La console d'administration SGD est une application Web à la disposition des administrateurs SGD pour la configuration de SGD.

La console d'administration est localisée dans les langues prises en charge par SGD : anglais, français, japonais, coréen, chinois simplifié et chinois traditionnel.

Pour utiliser la console d'administration, vous devez avoir activé JavaScript sur votre navigateur.

Dans la mesure du possible, exécutez la console d'administration sur le serveur principal dans la baie SGD. Il est préférable d'exécuter certaines opérations, comme la création d'objets ou la modification d'attributs d'objet, sur le serveur principal. Si vous effectuez ces opérations sur un serveur secondaire lorsque le serveur principal n'est pas en cours d'exécution, les modifications ne seront pas implémentées.

Remarque – La distribution SGD comprend un fichier archive Web (WAR, Web Archive) pour la console d'administration : `sgdadmin.war`. L'utilisation de ce fichier pour déployer la console d'administration sur un autre serveur d'application Web n'est pas prise en charge.

Pour lancer la console d'administration, suivez l'une des méthodes ci-dessous :

- Cliquez sur le lien de la console d'administration sur le bureau Web d'un administrateur SGD.
- Cliquez sur le lien Lancer la console d'administration Sun Secure Global Desktop sur la page de bienvenue du serveur Web SGD à l'adresse : `http://exemple.serveur.com`, où `exemple.serveur.com` correspond au nom d'un serveur SGD.
- Allez à l'adresse `http://exemple.serveur.com/sgdadmin`, où `exemple.serveur.com` correspond au nom d'un serveur SGD.

Pour plus de détails sur la console d'administration, reportez-vous au *Guide d'administration de Sun Secure Global Desktop 4.4* et au *Manuel de référence de Sun Secure Global Desktop 4.4*.

Modification de la terminologie

La terminologie de la console d'administration est différente de celle des versions précédentes de SGD.

Les termes habituels de la version 4.31 sont récapitulés dans le tableau suivant, avec leur équivalent dans la console d'administration.

SGD version 4.31	Console d'administration
membre de la baie	serveur SGD
bureau Web du navigateur	bureau Web
session de l'émulateur	session d'application
ENS (Enterprise Naming Scheme, schéma d'attribution de nom d'entreprise)	référentiel local
nom équivalent d'ENS	profil utilisateur
nom complet	identité de l'utilisateur
hôte	serveur d'application
routage des baies intelligent	groupe d'équilibrage de charge
autorité de connexion	authentification système
profil de connexion	profil utilisateur
personne	objet de profil utilisateur
TFN (Tarantella Federated Naming, attribution de nom Tarantella fédérée)	<i>inutilisé</i>
session de bureau Web	session utilisateur

Modifications de nom d'attribut

Certains attributs ont été renommés dans la console d'administration. Le *Manuel de référence de Secure Global Desktop 4.4* comprend les noms d'attribut utilisés dans la console d'administration, ainsi que leur équivalent dans le gestionnaire d'objets et le gestionnaire de baies.

URL Desktop Direct

L'URL (Uniform Resource Locator, localisateur de ressource uniforme) Desktop Direct permet aux utilisateurs de se connecter et d'afficher un bureau plein écran sans afficher un bureau Web.

L'utilisation de l'URL Direct Desktop requiert l'assignation d'un objet d'application appelé Mon bureau (`nc=Mon bureau`) à l'utilisateur. Cet objet est automatiquement créé lors de l'installation de SGD. L'objet est configuré par défaut pour exécuter l'application de bureau par défaut disponible sur le serveur SGD (Sun Java Desktop System par exemple). Vous avez la possibilité de reconfigurer cet objet pour qu'il exécute toute application ; vous obtiendrez cependant de meilleures performances avec des applications de bureau plein écran. Si les utilisateurs requièrent différentes applications de bureau, vous pouvez créer des objets Mon bureau supplémentaires. Cependant, chaque utilisateur ne peut disposer que d'une seule application Mon bureau.

Remarque – Un nombre illimité d'applications peut être assigné aux utilisateurs, mais l'URL Desktop Direct ne leur donne accès qu'à l'application Mon bureau.

L'URL Desktop Direct est habituellement `http://exemple.serveur.com/sgd/mydesktop`, où *exemple.serveur.com* correspond au nom d'un serveur SGD. La page de connexion SGD s'affiche aussitôt. Une fois l'utilisateur connecté, la session de bureau s'affiche et il peut fermer le navigateur Web.

Remarque – Il n'existe pas de commande pour suspendre ou reprendre l'application de bureau. Les utilisateurs doivent se déconnecter de l'application de bureau comme d'habitude.

Prise en charge des profils utilisateur itinérant

Les utilisateurs de périphériques client Microsoft Windows peuvent posséder un profil utilisateur itinérant. Grâce à ce profil utilisateur itinérant, ils disposent du même environnement de travail, quel que soit l'ordinateur Microsoft Windows utilisé. Si un utilisateur Microsoft Windows possède un profil utilisateur itinérant, son profil client SGD est automatiquement modifié pour permettre cette fonctionnalité :

- Les paramètres spécifiques au périphérique client de l'utilisateur (la configuration de serveur proxy par exemple) sont stockés sur le périphérique.

Par défaut, il s'agit de *disque_personnel\Documents and Settings\nom_utilisateur\Local Settings\Application Data\Sun\SSGD\profile.xml*

Les paramètres spécifiques à l'utilisateur (la langue préférée par exemple) sont stockés dans le répertoire du profil utilisateur itinérant.

- Il s'agit habituellement de *disque_personnel\Documents and Settings\nom_utilisateur\Application Data\Sun\SSGD\profile.xml*

Remarque – Cet emplacement contient également les fichiers `hostsvisited` et `certstore.pem` de l'utilisateur.

Les paramètres suivants du profil client SGD sont stockés dans le répertoire du profil utilisateur itinérant :

Paramètre de profil client	Entrée de profil itinérant
URL de connexion	<url>
Ajout d'applications au menu Démarrer	<mode>
Connexion client automatique	<autologin> <AT>
Connexion en même temps qu'au système	<autostart>
Échec de la connexion	<reconnect mode> <reconnect_attempts> <reconnect_interval>

Délai d'attente automatique pour les sessions utilisateur inactives

Les administrateurs SGD ont à présent la possibilité de configurer un délai d'attente automatique pour les sessions utilisateur inactives.

Ce délai d'attente permet de suspendre les sessions utilisateur si aucune activité dans la session d'application ou sur le bureau Web n'a été relevée pendant un certain laps de temps. Le délai d'attente s'applique à tous les serveurs SGD de la baie.

Le délai d'attente peut être uniquement configuré depuis la ligne de commande. Vous ne pouvez pas le modifier depuis la console d'administration.

Configurez-le à l'aide de la commande suivante :

```
$tarantella config edit \  
--tarantella-config-array-webtopsessionidletimeout secondes
```

Remplacez *secondes* par le délai d'attente, en secondes.

Lorsque ce paramètre est défini sur 0, la fonctionnalité de délai d'attente pour les sessions utilisateur inactives est désactivée. Il s'agit de la valeur par défaut.

Dans l'exemple suivant, les sessions utilisateur sont suspendues après 1 800 secondes (30 minutes) d'inactivité.

```
$tarantella config edit \  
--tarantella-config-array-webtopsessionidletimeout 1800
```

Filtres de masque de réseau pour la spécification d'adresses réseau

Vous pouvez à présent spécifier un filtre de masque de réseau lors de la définition des attributs suivants :

- noms DNS externes (--server-dns-external) ;
- routages de baie
(--tarantella-config-array-netservice-proxy-routes).

Le format du filtre de masque de réseau est le suivant : v.w.x.y/z. Les filtres précédents de type générique sont toujours pris en charge.

L'exemple suivant utilise un filtre de masque de réseau pour spécifier les noms DNS externes.

```
$tarantella config edit --server-dns-external \  
"192.168.55.0/24:boston.indigo-insurance.com"
```

Touches de gestion des fenêtres

Un nouvel attribut de touches de gestion des fenêtres (`--remotewindowkeys`) est disponible pour les types d'objet suivants :

- application Windows ;
- application X.

Avec cet attribut, les raccourcis clavier associés à la gestion des fenêtres peuvent être envoyés à la session distante ou utilisés localement. Ce paramètre n'est disponible que pour les applications dont le paramètre Type de fenêtre est défini sur Mode kiosque.

Pour quitter le mode kiosque lorsque cet attribut est activé, utilisez la combinaison de touches ALT+CTRL+MAJ+ESPACE. Cette opération minimise la session kiosque sur le bureau local.

Prise en charge de SE Solaris 10 Trusted Extensions

SGD s'exécute sur SE Solaris 10 Trusted Extensions avec les restrictions connues suivantes :

- SGD doit être installé sur une zone avec libellé. Reportez-vous au *Guide d'installation de Sun Secure Global Desktop 4.4* pour plus de détails sur l'installation de SGD sur SE Solaris 10 Trusted Extensions.
- Le disque client n'est pas pris en charge par les périphériques client UNIX [6610354].
- L'audio n'est pas pris en charge par les plates-formes UNIX [6610352].
- Le mode intégré n'est pas pris en charge par les plates-formes client SE Solaris 10 Trusted Extensions [6610371].
- Le mode kiosque ne fournit pas les meilleurs résultats sur les plates-formes client SE Solaris 10 Trusted Extensions [6594795].

Gestion globale des mots de passe et des jetons

La console d'administration sert à la gestion globale des mots de passe et des jetons pour tous les utilisateurs SGD.

Vous pouvez à présent gérer les mots de passe et les jetons selon l'identité de l'utilisateur ou son profil. Auparavant, le gestionnaire d'objets ne pouvait gérer les mots de passe et les jetons que par profil utilisateur.

Noms d'objet alternatifs pour les certificats de serveur

Si, par exemple, un serveur SGD possède plusieurs noms DNS, il est alors connu sous différents noms à l'intérieur et à l'extérieur d'un pare-feu. Vous pouvez spécifier les noms DNS supplémentaires en tant que *noms d'objet alternatifs* lors de la génération d'une CSR (Certificate Signing Request, demande de signature de certificat). Cette opération permet d'associer plusieurs noms DNS à un certificat de serveur.

La commande `tarantella security certrequest` vous invite à saisir les noms d'objet alternatifs lors de la génération d'une CSR.

La commande `tarantella security certinfo` permet d'afficher les noms d'objet alternatifs associés à un certificat.

Attribut de fichier de mappage des fuseaux horaires

Vous disposez d'un nouvel attribut de fichier de mappage des fuseaux horaires (`--xpe-tzmapfile`).

Cet attribut permet de spécifier un fichier contenant les mappages entre le périphérique client UNIX et les noms de fuseau horaire du serveur de l'application Windows. Il s'applique à tous les serveurs SGD de la baie.

Nouvelles fonctions de la version 4.31

Cette section décrit les nouvelles fonctions du logiciel Sun Secure Global Desktop version 4.31.

Prise en charge du format audio dans les applications X

Les administrateurs SGD peuvent à présent activer le son dans les applications X dont l'accès s'effectue en utilisant SGD.

L'activation du son dans les applications X requiert les conditions suivantes :

- Le périphérique client doit pouvoir effectuer de la lecture audio.
- Le client SGD doit être utilisé pour la connexion à SGD.
- Le module audio UNIX du module d'enrichissement SGD doit être installé et en cours d'exécution sur le serveur d'application.
- L'application X doit utiliser OSS (Open Sound System) pour la sortie son. Si votre système utilise ALSA (Advanced Linux Sound Architecture), il est possible que vous deviez activer les modules d'émulation ALSA OSS dans le noyau.
- Le service audio SGD UNIX doit être activé dans la console d'administration.
Ce service est désactivé par défaut.

Le module audio UNIX contient un émulateur de pilote audio OSS. L'émulateur de pilote audio est installé sur le noyau lors de l'installation du module audio UNIX du module d'enrichissement SGD.

Remarque – Dans la mesure où le module audio UNIX inclut un émulateur de pilote audio, il n'est pas nécessaire que le serveur d'application dispose lui-même d'une carte son.

Certaines applications X utilisent du code permanent lorsqu'elles font appel à des périphériques `/dev/audio` ou `/dev/dsp` pour la sortie son. Un nouvel attribut pour les objets d'application X, la bibliothèque de redirection audio (`--unixaudiopreload`), permet à une bibliothèque de redirection audio SGD de forcer l'application X à utiliser le périphérique audio SGD.

Prise en charge du Bureau à distance de Microsoft Windows Vista

Le Bureau à distance de Microsoft Windows Vista permet d'accéder à un ordinateur distant à l'aide du protocole Microsoft RDP (Remote Desktop Protocol).

Vous pouvez maintenant utiliser cette fonction avec SGD afin de permettre, par exemple, à un utilisateur d'accéder à distance à son PC lorsqu'il est en déplacement. Seules les sessions de bureau Windows complètes sont prises en charge.

Vous pouvez également installer le module d'enrichissement SGD sur les périphériques client Microsoft Windows Vista pour la prise en charge du mappage du disque client. La fonction avancée d'équilibrage de charge et les fenêtres transparentes ne sont pas prises en charge.

Paramètres clients SSH

Un nouvel attribut d'arguments SSH (`--ssharguments`) est disponible pour les types d'objet suivants :

- Application X
- Application à traitement de caractère
- Application 3270
- Application 5250

Cet attribut permet de spécifier les arguments de ligne de commande pour le client SSH lorsque SSH constitue la méthode de connexion pour une application.

Nouvelles fonctions de la version 4.30

Cette section décrit les nouvelles fonctions intégrées au logiciel Sun Secure Global Desktop version 4.30.

Intégration au menu de démarrage du bureau

Le client SGD peut à présent fonctionner dans l'un des modes suivants :

- **Mode bureau Web** : le bureau Web s'affiche avec le navigateur Web, de la même manière que dans les versions précédentes. C'est le mode par défaut.
- **Mode intégré** : le contenu du bureau Web (les liens pour démarrer les applications) s'affiche dans le menu de démarrage du bureau. Ainsi les utilisateurs peuvent exécuter les applications à distance, tout comme ils exécutent les applications locales. L'utilisation d'un navigateur Web n'est pas toujours nécessaire. Elle dépend du mode de configuration de l'intégration au menu de démarrage.

Remarque – Utilisez le mode intégré si votre entreprise préfère ne pas utiliser la technologie Java sur le périphérique client.

Pour accéder au mode intégré, vous devez vous connecter à SGD en cliquant sur le lien de connexion du menu de démarrage du bureau. Le mode intégré n'est pas accessible si vous vous connectez à partir d'un navigateur Web.

Le travail en mode intégré simplifie la gestion des sessions. À la différence du bureau Web, ce mode n'offre aucune commande de suspension ou de reprise d'applications. Lorsque vous vous déconnectez, le client suspend ou arrête automatiquement toutes les sessions d'application en cours d'exécution. Après reconnexion, le client reprend automatiquement toutes les sessions suspendues.

L'impression est également simplifiée. Les travaux d'impression peuvent être lancés en permanence et ils sont directement dirigés vers l'imprimante sélectionnée. En revanche, la gestion individuelle des travaux d'impression n'est pas prise en charge.

Si vous souhaitez accéder au bureau Web, par exemple pour relancer une application suspendue ou gérer les impressions, cliquez sur le lien correspondant dans le menu de démarrage. Le bureau Web s'affiche dans le navigateur Web par défaut.

Si vous avez configuré le contenu du bureau Web pour qu'il soit organisé en groupes, ces groupes s'affichent également dans le menu de démarrage. Si vous avez paramétré le masquage du contenu du bureau Web d'un groupe, ces informations ne s'affichent pas dans le menu de démarrage.

Pour vous déconnecter de SGD, cliquez sur le lien correspondant dans le menu de démarrage.

Pour obtenir des informations sur les systèmes de bureau qu'il est possible d'utiliser en mode intégré, consultez la section [Configuration requise du client, page 7](#).

Connexion unique

Vous pouvez à présent configurer le client SGD pour qu'il démarre automatiquement lorsqu'un utilisateur se connecte au périphérique client. Le client SGD peut également mettre un jeton d'authentification en mémoire cache, ce qui permet d'ouvrir une session utilisateur de manière automatique. Avec ce type de configuration, les utilisateurs bénéficient des avantages d'une connexion unique.

La connexion automatique s'établit par authentification de jeton. Si le client SGD présente un jeton d'authentification valide, SGD authentifie automatiquement l'utilisateur. Pour obtenir un jeton d'authentification, l'utilisateur doit se connecter à l'aide d'un navigateur Web, puis générer le jeton manuellement en modifiant son profil. Chaque serveur de connexion à SGD requiert un jeton différent.

Gestion des configurations client à l'aide de profils

Les fonctions du menu de démarrage du bureau et de connexion unique impliquent de configurer le client SGD en vue d'une connexion à SGD. En outre, la configuration requise peut varier en fonction des situations (travail au bureau ou travail à domicile, par exemple). La version 4.3 permet de gérer plusieurs configurations client par le biais de profils, une méthode de stockage de groupes de paramètres client. Chaque profil client permet de configurer les éléments suivants :

- l'URL de connexion à SGD ;
- le mode de fonctionnement du client SGD, à savoir le mode bureau Web ou le mode intégré ;
- l'activation des connexions automatiques ;
- le démarrage automatique du client SGD lorsque l'utilisateur se connecte au périphérique client ;

- le type de configuration du serveur proxy, à savoir manuelle, par le biais du profil, ou automatique, d'après les paramètres du navigateur Web ;
- les paramètres de reconnexion qui définissent le comportement du client suite à une perte de connexion à SGD ;
- les paramètres de connexion qui définissent les données écrites dans le fichier journal client SGD ;
- le chemin d'accès au visionneur PDF configuré pour l'impression de fichiers PDF sur les clients SE Solaris, Linux et Mac OS X.

Les administrateurs SGD disposent du contrôle total des profils clients grâce à l'éditeur de profils, nouvel outil d'administration, se trouvant sur leur bureau Web. Ils peuvent créer et modifier les profils clients pour les objets d'une organisation ou d'une unité d'organisation (UO) ainsi que pour les objets de profil de l'organisation d'objets système Tarantella. En définissant des profils clients pour ces objets, les administrateurs peuvent déployer des configurations client SGD par défaut courantes pour les utilisateurs.

Ils peuvent également autoriser les utilisateurs à créer et modifier leurs propres profils clients. La modification du profil utilisateur peut être activée à l'échelle globale, pour une organisation, une UO ou des utilisateurs individuels. Cette fonctionnalité est activée par défaut. Les profils sont créés et modifiés à partir du bouton Éditer du bureau Web.

Le profil par défaut configuré sur le système SGD offre aux utilisateurs le même bureau Web standard que dans les versions précédentes. Les administrateurs peuvent modifier ce profil.

Lorsque le client SGD se connecte à SGD, le profil configuré pour l'utilisateur est copié à partir de SGD vers le périphérique client. Si un utilisateur modifie son profil, les modifications sont stockées *uniquement* sur le périphérique client.

Configuration du serveur proxy mobile

Le client SGD nécessite différents paramètres de serveur proxy en fonction de l'emplacement à partir duquel s'effectue la connexion à SGD. Il peut donc s'avérer difficile de s'assurer que chaque utilisateur dispose des paramètres de proxy adéquats. La version 4.3 propose la configuration de serveur proxy mobile. Grâce à la configuration de serveur proxy mobile, le client SGD utilise les paramètres dans le profil client pour définir les paramètres de serveur proxy. Les paramètres de serveur proxy peuvent être spécifiés comme suit :

- **manuellement** : les paramètres du proxy sont stockés au sein même du profil client ;
- **automatiquement** : les paramètres du proxy sont obtenus à partir du navigateur Web par défaut de l'utilisateur.

Si le client SGD fonctionne en mode intégré et s'il est configuré pour utiliser les paramètres du navigateur, il obtient les paramètres du proxy en chargeant l'URL spécifié dans le profil utilisateur du navigateur par défaut. Une fois les paramètres obtenus mis en cache, le client SGD peut les utiliser de façon à ce que le navigateur par défaut de l'utilisateur n'ait besoin d'être démarré qu'une fois.

Remarque – Pour déterminer les paramètres du proxy à partir d'un navigateur Web, la technologie Java doit être activée sur ce dernier.

Amélioration de la ligne de commande pour le client SGD

La ligne de commande du client SGD a été améliorée sur l'ensemble des plates-formes afin d'assurer la prise en charge des profils clients. Vous pouvez utiliser des arguments pour spécifier ce qui suit :

- le profil à utiliser ;
- l'URL de connexion à SGD (remplace l'URL dans le profil spécifié) ;
- la langue à utiliser.

Grâce aux améliorations apportées à la ligne de commande, vous pouvez créer vos propres scripts de démarrage du client SGD et d'exécution d'applications.

Installation manuelle du client SGD

Il est à présent possible de charger et d'installer manuellement le client SGD. Ce dernier peut ainsi être exécuté en mode intégré ou dans des environnements dans lesquels les navigateurs Web ne fonctionnent pas avec la technologie Java. Vous pouvez télécharger le client SGD à partir d'un serveur SGD sur le site Web <http://exemple.serveur.com>, où *exemple.serveur.com* correspond au nom d'un serveur SGD. Cliquez sur Installer le client Sun SGD pour installer le client SGD.

Nouveau serveur X

Cette version comporte un nouveau serveur X basé sur X11R6.8.2. Par rapport à la version 4.2, les performances du nouveau serveur X démontrent des améliorations significatives en matière de vitesse et de bande passante.

Ce nouveau serveur prend en charge les extensions X suivantes :

- 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.

Le nouveau serveur X prend également en charge d'autres polices X. La police Speedo n'est plus disponible.

Nouvel attribut de l'extension de sécurité X

Les objets d'application X disposent d'un nouvel attribut de l'extension de sécurité X (`--securityextension`) qui active l'extension de sécurité X pour une application. Activez cet attribut pour exécuter une application X sur un serveur d'application non sécurisé. Ainsi, vous pourrez exécuter l'application en mode non sécurisé. Ce mode limite les opérations de l'application X dans le serveur X et protège l'affichage. La sécurité X ne fonctionne qu'avec les versions de SSH assurant la prise en charge de l'option `-Y`. Pour OpenSSH, il s'agit de la version 3.8 et des versions ultérieures.

Impression de PDF pour les clients UNIX, Linux et Mac OS X

Le client SGD prend maintenant en charge l'impression de PDF sur les périphériques client UNIX, Linux et Mac OS X. Sur ces clients, le document à imprimer s'affiche dans un visionneur PDF à partir duquel il peut être enregistré et/ou imprimé sur une imprimante PDF SGD. Par défaut, SGD assure la prise en charge des visionneurs PDF suivants.

Plate-forme client	Visionneur PDF par défaut
SE Solaris sur plate-forme SPARC	Adobe Reader (<code>acroread</code>)
SE Solaris sur plate-forme x86	Visionneur de PDF GNOME (<code>gpdf</code>)
Linux	Visionneur de PDF GNOME (<code>gpdf</code>)
Mac OS X	Preview.app

Pour utiliser un visionneur par défaut, l'application doit résider dans le CHEMIN utilisateur.

Pour utiliser un autre visionneur PDF, spécifiez le *chemin complet* de ce dernier dans le profil utilisé par le client SGD.

Remarque – Lorsque vous spécifiez une imprimante PDF sur les périphériques client UNIX, Linux et Mac OS X, l'imprimante PDF universel et les visionneurs PDF universel ne présentent aucune différence, puisque le document s'affiche toujours dans un visionneur PDF.

L'impression de PDF sur les périphériques client Microsoft Windows est inchangée.

Mappage du disque client pour la plate-forme UNIX et les applications LINUX

Le mappage du disque client (CDM, Client Drive Mapping) est maintenant disponible sous UNIX et pour les applications Linux.

Une fois le mappage du disque client activé dans la console d'administration, il est activé pour les applications UNIX, Linux et Windows.

Les attributs de gestion des droits d'accès aux disques client des organisations, unités d'organisation ou objets de profil utilisateur ne s'appliquent qu'aux périphériques client Windows, qu'ils soient associés à Windows, à la plate-forme UNIX ou à des applications Linux.

Pour gérer les disques mappés pour les périphériques client de la plate-forme UNIX, de Linux ou de Mac OS X il suffit de vérifier les entrées du fichier de configuration de l'utilisateur `$HOME/.tarantella/native-cdm-config`.

Les conditions suivantes sont nécessaires pour rendre disponible le mappage de disque client aux applications UNIX et Linux :

- Le module d'enrichissement SGD doit être installé et en cours d'exécution sur le serveur d'application UNIX ou Linux. Actuellement, le service de mappage du disque client doit être démarré manuellement à l'aide de la commande `/opt/tta_tem/bin/tem startcdm`.
- Un serveur NFS (Network File System) doit être installé et en cours d'exécution sur le serveur d'application. Le serveur NFS doit exporter un répertoire nécessaire au mappage du disque client. Par défaut, il s'agit du répertoire `/smb`. Il est possible de spécifier un répertoire différent dans le fichier `/opt/tta_tem/etc/client.prf`. L'entrée de ce fichier doit être au format `NFS_server/mount/mountpoint`.
- Le mappage du disque client doit être activé dans la baie.
- Le service de mappage du disque client de SGD doit être démarré dans la baie à l'aide de la commande `tarantella start cdm`.
- Les droits d'accès aux disques client doivent être configurés à l'aide de la console d'administration (pour les clients Windows) et dans le fichier de configuration de l'utilisateur (clients UNIX, Linux et Mac OS X).

Lorsque le mappage du disque client est activé, les disques ou systèmes de fichiers clients de l'utilisateur sont accessibles par défaut dans son répertoire personnel, `My SGD drives`. Le répertoire `My SGD drives` est un lien symbolique vers le répertoire NFS partagé nécessaire au mappage du disque client.

Prise en charge des ports série dans les applications Windows

Les utilisateurs qui exécutent des applications Windows sur Windows Terminal Server ont maintenant accès aux ports série sur leur périphérique client.

Pour accéder à un port série, les conditions suivantes doivent être remplies :

- Le mappage de port COM doit être activé dans la configuration de services de terminal (option par défaut).
- Le mappage de port série doit être activé dans le panneau Paramètres globaux ⇒ Périphérique client de la console d'administration (option par défaut).
- L'accès aux ports série doit être activé pour les organisations, unités d'organisation ou objets de profil utilisateur. Les droits d'accès doivent être transférables.
- Les clients SGD doivent être en mesure d'énumérer les ports série des périphériques client. Pour de plus amples informations sur le mappage des ports série, reportez-vous au *Guide d'administration de Sun Secure Global Desktop 4.4*.

Les utilisateurs doivent avoir un accès en lecture et en écriture sur les ports série auxquels ils veulent accéder.

Le mappage de port série est accessible au client SGD qui s'exécute sur les périphériques client Windows, plate-forme Solaris et Linux.

Prise en charge du Bureau à distance de Microsoft Windows XP Professionnel

Le Bureau à distance de Microsoft Windows XP Professionnel permet d'accéder à un ordinateur distant à l'aide du protocole Microsoft RDP (Remote Desktop Protocol). Vous pouvez maintenant utiliser cette fonction avec SGD afin de permettre, par exemple, à un utilisateur d'accéder à distance à son PC lorsqu'il est en déplacement. Seules les sessions de bureau Windows complètes sont prises en charge.

Vous pouvez également installer le module d'enrichissement SGD sur les périphériques client Microsoft Windows XP Professionnel pour la prise en charge du mappage du disque client. La fonction avancée d'équilibrage de charge et les fenêtres transparentes ne sont pas prises en charge.

Prise en charge des connexions à la session de console avec les services de terminal Windows Server 2003

Le client des services de terminal SGD (`ttatssc`) assure désormais la prise en charge d'une option supplémentaire, `-console`, qui permet la connexion à la session de console avec les services de terminal de Windows Server 2003.

Cette option peut être définie dans l'attribut d'arguments de protocole (`--protoargs`) de l'objet d'application Windows.

Connexion initiale sécurisée

La connexion initiale entre un client SGD et un serveur SGD est sécurisée avec SSL. Toutefois, une fois l'utilisateur connecté, la connexion redevient standard. Si vous souhaitez utiliser SSL de façon permanente pour les connexions à SGD, vous devez activer les services de sécurité SGD.

Les connexions SSL entre les clients SGD et SGD utilisent le port TCP 5307. L'ouverture de ce port pourrait devoir s'effectuer dans votre pare-feu afin de permettre aux clients SGD de se connecter.

SGD dispose d'une fonction de routage des baies permettant de configurer les serveurs proxy SOCKS côté serveur. Les commandes suivantes permettent de configurer le routage des baies :

```
$ tarantella config edit \  
----tarantella-config-array-netservice-proxy-routes route...
```

Si un routage inclut l'option `:ssl`, vous devrez configurer le démon SGD SSL pour qu'il accepte les connexions non chiffrées à l'aide de l'attribut Prise en charge de l'accélérateur SSL situé dans l'onglet Paramètres de serveur Secure Global Desktop ⇒ Sécurité de la console d'administration ou à l'aide de la commande suivante :

```
$ tarantella config edit --security-acceptplaintext 1
```

Protection des clients contre les serveurs non autorisés

Avec l'automatisation du démarrage et de la connexion du client SGD, il est essentiel de pouvoir vérifier la fiabilité des connexions. Cette version permet désormais à l'utilisateur d'autoriser explicitement la connexion à SGD.

Lors de sa première connexion à SGD, l'utilisateur reçoit un message de connexion initiale non autorisée qui l'invite à confirmer la connexion au serveur SGD. Ce message affiche le nom d'hôte et l'empreinte du certificat de sécurité du serveur auquel il se connecte. Il est important de vérifier ces informations *avant* de cliquer sur Oui. Si l'utilisateur accepte la connexion, le message ne s'affichera plus qu'en cas de problème.

Pour assurer la fiabilité des connexions utilisateur aux serveurs SGD, les administrateurs doivent :

- fournir aux utilisateurs une liste des noms d'hôtes et empreintes des serveurs de confiance (liste obtenue à l'aide de la commande `tarantella security fingerprint` sur chaque membre de la baie) ;
- expliquer aux utilisateurs les implications de sécurité liées à la connexion au serveur.

Sur une nouvelle installation, chaque serveur SGD possède son propre certificat de sécurité autosigné. Les administrateurs doivent installer un certificat X.509 valide pour chaque serveur SGD.

Contrôle des copier-coller

Les administrateurs SGD peuvent désormais contrôler les opérations de copier-coller dans les sessions d'application Windows et X. Les copier-coller peuvent être configurés de la manière suivante :

- La fonction copier-coller peut être activée ou désactivée pour l'ensemble de SGD.
- La fonction copier-coller peut être activée ou désactivée pour des organisations, des unités d'organisation ou des objets de profil utilisateur. L'administrateur peut ainsi définir les utilisateurs autorisés à copier-coller.
- Un niveau de sécurité peut être assigné au presse-papiers des applications. Les données ne peuvent être copiées que si le presse-papiers de l'application cible (l'application *recevant* les données) possède un niveau de sécurité identique ou supérieur à celui de l'application source. L'administrateur peut ainsi sécuriser les données accessibles à travers certaines applications.

- Vous pouvez assigner un niveau de sécurité au presse-papiers du client SGD. Les données ne peuvent être copiées sur des applications du périphérique client que si le presse-papiers du client SGD possède un niveau de sécurité identique ou supérieur à celui de l'application source. L'administrateur peut ainsi sécuriser le flux de données à l'extérieur de SGD.

Si un utilisateur tente une opération de copier-coller non autorisée (en raison de niveaux de sécurité différents, par exemple), le message suivant est collé à la place des données copiées :

```
Logiciel Sun SGD : Copied data not available to this  
application (Données copiées non disponibles pour cette  
application)
```

Prise en charge de SecurID pour l'authentification du serveur d'application

De même que l'on peut utiliser RSA SecurID pour authentifier les utilisateurs de SGD, il est possible d'utiliser SecurID pour authentifier le serveur d'application lors du lancement d'applications X et à traitement de caractères.

Avant d'utiliser l'authentification SecurID sur SGD, assurez-vous que les utilisateurs peuvent se connecter au serveur d'application à l'aide de SecurID. Après cette vérification, configurez l'application de sorte qu'elle utilise le script de connexion `securid.exp`.

Interface utilisateur localisée

La version 4.3 propose des interfaces utilisateur localisées en :

- Français
- Japonais
- Coréen
- Chinois simplifié
- Chinois traditionnel

Les utilisateurs peuvent choisir la langue du bureau Web en visitant une page différente ou en sélectionnant une langue sur la page de bienvenue du serveur SGD (<http://exemple.serveur.com>, où *exemple.serveur.com* correspond au nom d'un serveur SGD). Le client SGD peut également être démarré dans la langue de votre choix.

La console d'administration est localisée dans les langues de l'interface utilisateur.

Documentation traduite

Le tableau suivant répertorie les traductions de la documentation SGD disponibles.

Langue	Notes de version	Guide d'installation	Guide d'administration	Manuel de référence	Guide de l'utilisateur
Français	Oui	Oui	Non	Non	Oui
Japonais	Oui	Oui	Oui	Oui	Oui
Coréen	Oui	Oui	Non	Non	Oui
Chinois simplifié	Oui	Oui	Non	Non	Oui
Chinois traditionnel	Oui	Oui	Non	Non	Oui

Prise en charge des langues dans les scripts Expect

Les scripts Expect servant au démarrage des applications sur les serveurs d'application ont également été améliorés afin d'assurer la prise en charge des invites système en plusieurs langues. Par défaut, ces langues sont celles prises en charge par SGD.

Pour permettre aux scripts Expect de fonctionner avec des invites système en plusieurs langues, les objets de serveur d'application disposent d'un nouvel attribut de demande d'environnement linguistique (`--hostlocale`) qui permet de spécifier la version localisée du serveur d'application.

Modifications dans la version 4.40

Cette section décrit les modifications apportées par rapport au logiciel Sun Secure Global Desktop version 4.31.

Modifications apportées aux plates-formes d'installation prises en charge

Pour cette version, les modifications suivantes ont été apportées aux plates-formes d'installation prises en charge pour SGD :

- SE Solaris 10 Trusted Extensions sur les plates-formes SPARC et x86 est dorénavant pris en charge. Reportez-vous à la rubrique [Prise en charge de SE Solaris 10 Trusted Extensions, page 23](#) pour plus d'informations.
- Fedora Linux 7 (Intel x86 32 bits) est dorénavant pris en charge. La plate-forme Fedora Core 6 n'est plus pris en charge.

Reportez-vous à la rubrique [Chapitre 1](#) pour plus d'informations sur les plates-formes prises en charge dans cette version.

Retrait des clients classiques

SGD version 4.31 était la dernière version contenant les clients Java, les clients natifs SGD et le bureau Web classique. La version 4.40 ne contient pas ces clients.

Par conséquent, pour cette version de SGD, vous ne pouvez plus configurer les applications pour qu'elles s'affichent dans une fenêtre de navigateur Web. Les options `webtop` et `newbrowser` de l'attribut Type de fenêtre (`--displayusing`) ont été supprimées.

Séquence de connexion et d'authentification

Par mesure de sécurité pour éviter les attaques par saturation, la séquence des événements de connexion à SGD a été modifiée de la manière suivante :

- Dans SGD version 4.31, le client SGD démarrait *avant* l'affichage de l'écran de connexion.
- Dans SGD version 4.40, le client SGD démarre uniquement *après* l'authentification réussie de l'utilisateur sur l'écran de connexion.

Une icône sur la barre des tâches du bureau indique le démarrage du client SGD. Reportez-vous au *Guide d'installation de Sun Secure Global Desktop 4.4* pour plus de détails sur la connexion à SGD.

À présent, vous ne pouvez plus refuser une connexion à SGD en fonction de l'adresse IP du client.

Certificats de serveur et noms DNS externes multiples

Dans les versions précédentes, l'attribut `--tarantella-config-ssldaemon-certificates` servait à associer un certificat X.509 avec un nom DNS externe pour un serveur SGD.

Cet attribut n'est plus pris en charge. Dans cette version, vous pouvez spécifier des noms DNS externes en tant que noms d'objet alternatifs lors de la génération d'une CSR.

Reportez-vous à la rubrique [Noms d'objet alternatifs pour les certificats de serveur, page 24](#) pour plus d'informations.

Modifications des services Web

Les modifications suivantes ont été apportées aux services Web de cette version :

- Modifications du modèle d'authentification
- Nouveaux noms de méthode
- Nouvelles opérations de service Web
- Codage de messages SOAP documents/littéraux
- Requêtes sur les données de périphérique

Modifications du modèle d'authentification

Dans la version 4.31, les méthodes `startSession` et `authenticateSession` servaient à authentifier une session utilisateur.

Dans la version 4.40, la création et l'authentification ont été fusionnées en une seule méthode : `authenticate`.

Les méthodes `startSession` et `authenticateSession` ne sont plus disponibles dans la version 4.40.

Nouveaux noms de méthode

La version 4.31 contenait des méthodes surchargées. Celles-ci se distinguaient par la quantité et le type de leurs paramètres. Toutes ces méthodes surchargées ont été renommées dans la version 4.40. De plus, les paramètres obligatoires pour la méthode `setSessionIdentity` ont été modifiés dans la version 4.40.

Les nouveaux noms de méthode dans cette version sont répertoriés dans le tableau suivant.

Nom de l'interface	Nom de la méthode dans la version 4.31	Nom de la méthode dans la version 4.40
ITarantellaDatastore	<code>modify(String, String, String[])</code>	<code>modifyReplace(String, String, String[])</code>
ITarantellaEvent	<code>adminSendClientSideMessage(String, String, String, String, String)</code>	<code>adminBroadcastClientSideMessage(String, String, String, String, String)</code>
ITarantellaExternalAuth	<code>setSessionIdentity(String, String)</code>	<code>setSessionIdentity(String, String, String)</code>
ITarantellaPrint	<code>printJobs(String)</code>	<code>printAllJobs(String)</code>
ITarantellaWebtopSession	<code>authenticateSession(String, String, String)</code>	<code>authenticate(String, String, String, String)</code>
ITarantellaWebtopSession	<code>authenticateSession(String, String, String, Item[], Item[])</code>	<code>authenticateExt(String, String, String, String, Item[], Item[])</code>
ITarantellaWebtopSession	<code>setTCCConfiguration(String, String, String, String, String, Item[])</code>	<code>setTCCConfigurationOverrides(String, String, String, String, String, Item[])</code>
ITarantellaWebtopSession	<code>startSession(*)</code>	Aucun équivalent

Nouvelles opérations de service Web

Le tableau suivant récapitule les nouvelles opérations de service Web.

Nom de l'interface	Nom de la méthode	Description
ITarantellaDatastore	deleteObjects	Supprime plusieurs objets du magasin de données SGD.
	searchStart	Nettoie les ressources côté serveur pour une recherche donnée.
	searchNext	Extrait le sous-ensemble de résultats de recherche suivant.
	searchEnd	Lance une recherche de magasin de données avec retour d'un sous-ensemble de résultats.
ITarantellaEmulatorSession	adminCount	Compte le nombre de sessions d'application correspondant à une recherche donnée.
	adminSearchEnd	Nettoie les ressources côté serveur pour une recherche donnée.
	adminSearchNext	Extrait le sous-ensemble de résultats de recherche suivant.
	adminSearchStart	Lance une recherche avec retour d'un sous-ensemble de résultats.
	endSessions	Termine diverses sessions d'application.
ITarantellaPrint	adminCount	Compte le nombre de travaux d'impression correspondant à une recherche donnée.
	adminSearchEnd	Nettoie les ressources côté serveur pour une recherche donnée.
	adminSearchNext	Extrait le sous-ensemble de résultats de recherche suivant.
	adminSearchStart	Lance une recherche avec retour d'un sous-ensemble de résultats.

Nom de l'interface	Nom de la méthode	Description
ITarantellaWebtopSession	associateTCC	Associe une session utilisateur à une connexion TCC existante.
	authenticate	Authentifie une session utilisateur.
	authenticateExt	Authentifie une session utilisateur.
	createView	Crée un nouvel affichage pour une session utilisateur existante.
	adminEndSessions	Termine diverses sessions utilisateur.
	adminCount	Compte le nombre de sessions utilisateur correspondant à une recherche donnée.
	adminSearchEnd	Nettoie les ressources côté serveur pour une recherche donnée.
	adminSearchNext	Extrait le sous-ensemble de résultats de recherche suivant.
	adminSearchStart	Lance une recherche avec retour d'un sous-ensemble de résultats.
ITarantellaUtility	SearchEnd	Nettoie les ressources côté serveur pour une recherche donnée.
	SearchNext	Extrait le sous-ensemble de résultats de recherche suivant.
	SearchStart	Lance une recherche avec retour d'un sous-ensemble de résultats.

Codage de messages SOAP documents/littéraux

Le format de codage de messages SOAP utilisé pour les services Web SGD a été remplacé par le format RPC/Codage en documents/littéraux.

Pour afficher la liste des services Web SGD, allez à l'adresse <http://exemple.serveur.com/axis/services>, où *exemple.serveur.com* correspond au nom d'un serveur SGD. Cliquez sur le lien wsdl pour afficher la liste WSDL (Web Services Description Language, langage de description de services Web) correspondant à un service Web SGD.

Les listes WSDL pour les versions RPC/Codage de services Web sont toujours incluses sur cette page. N'utilisez pas les versions RPC/Codage pour le développement de vos propres applications. Ces versions de services Web seront abandonnées dans les prochaines versions.

Requêtes sur les données de périphérique

L'opération `adminLookupSession` renvoie à présent des informations sur les périphériques. Cette opération permet de soumettre des requêtes sur les attributs de données de périphérique `--scotttarawdevicedata` et `--scottdeviceaccessibledata`.

Les informations sur les périphériques renvoyées peuvent servir d'outil de diagnostic.

Remise à niveau du cache Kerberos

Un nouveau paramètre pour la commande `tarantella cache` permet d'actualiser les paramètres de configuration de Kerberos pour un serveur SGD.

Cette nouvelle option, `krb5config`, s'utilise de la manière suivante :

```
$ tarantella cache --flush krb5config
```

Ce paramètre permet de mettre à jour la configuration de Kerberos pour un serveur SGD sans avoir à le redémarrer. Cette fonctionnalité est uniquement disponible pour l'authentification Active Directory.

Commande `tem status`

Une nouvelle commande est disponible pour les utilisateurs du module d'enrichissement SGD.

La commande `tem status` fournit des informations d'état sur l'équilibrage de charge, l'audio UNIX et les services de mappage du disque client pour la baie SGD. Cette commande répertorie les modules installés et indique s'ils sont en cours d'exécution ou non.

Java non pris en charge par le client SGD par défaut

Vous pouvez démarrer le client SGD à partir de la ligne de commande via la commande `tcc` sur les plates-formes client Microsoft Windows ou la commande `ttatcc` sur les plates-formes client UNIX, Linux ou Mac OS X.

Dans cette version, lorsque vous démarrez le client SGD à partir de la ligne de commande ou en mode intégré, le client SGD suppose par défaut que Java n'est pas activé sur le périphérique client. Un nouvel argument `-use-java` pour les commandes `tcc` et `ttatcc` configure le client SGD afin qu'il utilise Java.

Dans les versions précédentes, le client SGD considérait par défaut que Java était activé. L'argument `-no-java` des commandes `tcc` et `ttatcc` permettait d'ignorer ce comportement. Cet argument a été abandonné dans cette version.

Les arguments disponibles pour les commandes `tcc` et `ttatcc` sont décrits dans le *Guide d'administration de Sun Secure Global Desktop 4.4*.

Informations sur les fichiers journaux client SGD des périphériques client

Le client SGD consigne à présent les informations sur les périphériques client. Les données d'accès aux périphériques et les messages d'erreur sont consignés pour l'impression, le port série, le mappage du disque client et les périphériques audio et à cartes à puce.

Les informations sur les périphériques client sont inscrites dans le fichier journal client SGD et sont affichées sur la page Diagnostics détaillés du bureau Web.

Arguments de la ligne de commande renommés

Plusieurs attributs ont été renommés pour leur donner des noms plus courts. Cela évite les éventuelles erreurs lors de la saisie du nom de ces attributs dans la ligne de commande.

Les attributs modifiés sont récapitulés dans le tableau suivant.

Nom de l'attribut dans la version 4.31	Nom de l'attribut dans la version 4.40
--tarantella-config-login-thirdparty-searchens	--login-thirdparty-ens
--tarantella-config-login-thirdparty-allownonens	--login-thirdparty-nonens
--tarantella-config-ldap-thirdpartyldapcandidate-us eens	--login-ldap-thirdparty-ens
--tarantella-config-ldap-thirdpartyldapcandidate-us eprofile	--login-ldap-thirdparty-profile
--tarantella-config-xpeconfig-timezonemapfile	--xpe-tzmapfile

Attribut Domaine Windows NT

L'attribut Domaine Windows NT a été renommé Nom de domaine. Cet attribut spécifie le domaine à utiliser au cours de la procédure d'authentification du serveur d'application.

Cet attribut est disponible pour les objets suivants :

- serveur d'application ;
- application Windows ;
- profil utilisateur.

Imprimantes PDF renommées

Les noms des imprimantes PDF SGD ont été modifiés, comme indiqué dans le tableau suivant.

Nom de l'imprimante dans la version 4.31	Nom de l'imprimante dans la version 4.4
PDF universel	Imprimante PDF universel
Imprimante de fichier PDF locale	Visionneur PDF universel

Avertissement de fermeture de la fenêtre

Pour les objets d'application dont le paramètre Type de fenêtre est défini sur Fenêtre indépendante, une boîte de dialogue d'avertissement s'affiche lorsque la fenêtre de l'application est fermée. La boîte de dialogue vous permet de confirmer ou d'annuler la fermeture de la session d'application.

Proxy SOCKS supprimé du profil client

Vous ne pouvez plus configurer les serveurs proxy SOCKS via le profil client SGD.

Vous pouvez toujours configurer les serveurs proxy SOCKS via la fonctionnalité de routage des baies. Exécutez la commande ci-dessous :

```
$ tarantella config edit \  
--tarantella-config-array-netservice-proxy-routes \  
"192.168.10.*:CTSOCKS:taurus.indigo-insurance.com:8080"
```

Avec cette configuration, les clients dont les adresses IP commencent par 192.168.10 se connectent à l'aide du serveur proxy SOCKS taurus.indigo-insurance.com sur le port TCP 8080.

Outils d'administration supprimés du bureau Web de l'administrateur

Le gestionnaire d'objets, le gestionnaire de baies, l'assistant de configuration et le gestionnaire de sessions, auparavant utilisés en tant qu'outils d'administration, ne s'affichent plus sur le bureau Web de l'administrateur. Ils ont été remplacés par un outil d'administration unique basée sur navigateur appelé la console d'administration. Reportez-vous à la rubrique [Console d'administration SGD](#), [page 17](#) pour plus d'informations.

L'assistant de configuration reste inclus dans la distribution SGD en tant qu'exemple d'application Web. Pour afficher l'assistant de configuration, rendez-vous à l'adresse `http://exemple.serveur.com/sgd/admin/configmgr/index.jsp`, où *exemple.serveur.com* correspond au nom d'un serveur SGD.

Le gestionnaire de sessions est toujours inclus dans la distribution SGD en tant qu'exemple d'application Web. Pour afficher le gestionnaire de sessions, allez à l'adresse `http://exemple.serveur.com/sgd/admin/sessmgr/index.jsp`, où *exemple.serveur.com* correspond au nom d'un serveur SGD.

Modifications du script de connexion

Les scripts de connexion dans le répertoire `/rép-install/var/serverresources/expect` ont été normalisés. Certains scripts ont été renommés, d'autres ont été fusionnés.

Si vous utilisez SecurID pour l'authentification du serveur d'application, les objets utilisent le script `securid.exp` plutôt que le script `securid/unix.exp`. Pour une compatibilité ascendante, un lien existe maintenant entre `securid/unix.exp` et le nouveau script `securid.exp`.

Activation des méthodes d'entrée pour les environnements linguistiques

Une méthode d'entrée (IM, Input Method) est un composant de programme ou de système d'exploitation qui permet de saisir des caractères et des symboles absents du clavier. Pour les plates-formes Microsoft Windows, une méthode d'entrée s'appelle un éditeur de méthode de saisie (IME, Input Method Editor).

Lors de l'exécution d'une application, SGD active une méthode d'entrée lorsque les variables d'environnement `TTA_PREFERREDLOCALE`, `TTA_HOSTLOCALE` ou `LANG` (redéfinition de l'environnement de l'application) sont définies sur un environnement linguistique qui en requiert une. Ces environnements linguistiques sont contrôlés par la variable `IM_localeList` définie dans le script de connexion `vars.exp`.

Une méthode d'entrée est activée par défaut pour les environnements linguistiques japonais, coréen et chinois. Vous pouvez en activer une dans d'autres environnements linguistiques en modifiant la variable `vars.exp` et en ajoutant l'environnement concerné à la variable `IM_localeList`.

Délais d'expiration de client SGD

Lorsqu'une application est interrompue à cause de la fermeture inattendue du client SGD, les délais d'attente suivants sont rallongés de 20 minutes :

- **Délai d'attente avant la possibilité de reprise d'une session utilisateur** : pour les applications autorisant les reprises de session utilisateur.
- **Délai d'attente avant une possibilité de reprise générale** : pour les applications autorisant l'ensemble des reprises.

Modifications dans la version 4.31

Cette section décrit les modifications réalisées par rapport au logiciel Sun Secure Global Desktop 4.30.

Authentification SecurID sur les plates-formes Solaris x86

Dans la version 4.31, vous pouvez utiliser l'authentification SecurID lorsque SGD est installé sur les plates-formes Solaris x86.

Prise en charge de plusieurs serveurs SGD en mode intégré

Dans la version 4.30, il est possible de se connecter uniquement à un serveur SGD lorsque le client SGD est en mode intégré. Dans la version 4.31, il est possible d'utiliser le mode intégré avec plusieurs serveurs SGD. Un lien de connexion est disponible dans le menu de démarrage du bureau pour chaque serveur SGD.

Routage des baies

SGD dispose d'une fonction de routage des baies permettant de configurer les serveurs proxy SOCKS côté serveur. Les commandes suivantes permettent de configurer le routage des baies :

```
$ tarantella config edit \  
--tarantella-config-array-netservice-proxy-routes route...
```

Les routages de baie ont été améliorés afin de permettre la configuration d'un type de connexion directe. Utilisez CTDIRECT en tant que type de connexion pour spécifier les clients que vous pourrez connecter sans utiliser un serveur proxy.

Vous trouverez ci-après un exemple de configuration de routage de baie :

```
$ tarantella config edit \  
--tarantella-config-array-netservice-proxy-routes route...
```

```
--tarantella-config-array-netservice-proxy-routes \  
"192.168.5.*:CTDIRECT:" \  
"192.168.10.*:CTSOCKS:taurus.indigo-insurance.com:8080"
```

Cette configuration permet aux clients dont l'adresse IP commence par 192.168.5 d'avoir une connexion directe. Les clients dont les adresses IP commencent par 192.168.10 se connectent à l'aide du serveur proxy SOCKS taurus.indigo-insurance.com sur le port TCP 8080.

Scripts de démarrage de SGD

Dans la version 4.31, les scripts de démarrage assurant le démarrage et l'interruption des services SGD lors du redémarrage d'un serveur SGD ont été renommés et restructurés. Les scripts `*Tarantella` et `*TarantellaWebserver` ont été remplacés par un script unique nommé `*sun.com-sgd-base`. Le script `*tem` pour le module d'enrichissement SGD se nomme désormais `*sun.com-sgd-em`.

Message de connexion initiale non autorisée

Le message de connexion initiale non autorisée qui s'affiche lorsque les utilisateurs se connectent initialement à un serveur SGD a été amélioré. Les utilisateurs peuvent désormais visualiser le certificat de sécurité du serveur à partir de ce message.

Touche Windows désactivée

La touche Windows est désormais désactivée par défaut dans les sessions de services de terminal Windows SGD. La touche Windows est prise en compte uniquement dans les sessions locales Windows. La combinaison de touches `Alt+ORIGINE` permet d'afficher le menu de démarrage Windows dans une session de services de terminal SGD.

Le client des services de terminal SGD (`ttatsc`) prend désormais en charge une option supplémentaire, `-windowskey on|off`, qui permet d'activer la prise en charge de la touche Windows. Cette option peut être définie dans l'attribut d'arguments de protocole (`--protoargs`) de l'objet d'application Windows.

Modifications dans la version 4.30

Cette section décrit les modifications réalisées par rapport au logiciel Sun Secure Global Desktop version 4.20.

Package d'installation unique

La version 4.3 propose un package d'installation unique pour SGD. Il permet d'installer simultanément tous les packages qui devaient auparavant être installés séparément (notamment les packages de polices). Les clés de licence installées dans la baie contrôlent les composants SGD qui peuvent être utilisés.

Démon SSL actif en permanence

La connexion initiale à SGD étant désormais sécurisée en permanence, cela signifie que le démon SGD SSL est actif en permanence, même si les services de sécurité ne le sont pas.

Fichier de préférences utilisateur sur les périphériques client UNIX, Linux et Mac OS X

Dans les versions précédentes, la configuration du client SGD sur les périphériques client UNIX, Linux et Mac OS X s'effectuait à l'aide d'un fichier de préférences utilisateur. Avec l'introduction des profils, ce fichier n'est plus utilisé.

Attribut de fermeture de fenêtre (`--windowclose`)

Dans les versions précédentes, l'attribut de fermeture de fenêtre (`--windowclose`) n'était accessible qu'aux applications X dont l'affichage dépendait du système de gestion de fenêtres client. L'utilisation de cet attribut a été étendue aux applications X, Windows et à traitement de caractères, configurées pour s'afficher dans une fenêtre indépendante.

Dès lors, l'utilisateur peut arrêter ou suspendre la session de l'application en fermant une fenêtre indépendante. Par défaut, la fermeture d'une fenêtre ferme la session.

Prise en charge de PAM pour l'authentification des utilisateurs UNIX

SGD prend désormais en charge les PAM (Pluggable Authentication Modules, modules d'authentification enfichables) pour l'authentification des utilisateurs UNIX. Cette modification se répercute sur les mécanismes d'authentification UNIX :

- recherche de l'ID Unix dans le référentiel local (ENS) ;
- utilisation du profil utilisateur par défaut (utilisateur UNIX) ;
- recherche de l'ID du groupe Unix dans le référentiel local (groupe UNIX).

SGD utilise les PAM pour l'authentification des utilisateurs ainsi que pour les opérations de compte et de mot de passe.

Lorsque vous installez SGD sur une plate-forme Linux, le programme d'installation crée automatiquement des entrées de configuration PAM pour SGD en copiant la configuration actuelle pour le programme `passwd` et en créant le fichier `/etc/pam.d/tarantella`. Sur les plates-formes SE Solaris, vous pouvez, si nécessaire, ajouter une nouvelle entrée pour SGD (`tarantella`) dans le fichier `/etc/pam.conf`.

L'utilisation de PAM offre aux administrateurs SGD davantage de flexibilité et un contrôle accru sur l'authentification des utilisateurs UNIX en leur permettant, par exemple, d'ajouter des tests de connexion, des limites de compte ou des contrôles de mot de passe.

Impression de PDF

La version actuelle propose une nouvelle prise en charge de l'impression de fichiers PDF sur les périphériques client UNIX, Linux et Mac OS X. De ce fait, l'attribut de la boîte de dialogue d'affichage de l'impression Adobe Reader (`--pdfprompt`) a été supprimé.

Dorénavant, lorsque l'utilisateur d'un client Windows lance une impression sur l'imprimante de type PDF universel, le travail d'impression est automatiquement envoyé à l'imprimante par défaut du client. Pour envoyer le travail vers une autre imprimante, sélectionnez l'imprimante Visionneur PDF universel.

Certificats client pour l'authentification Active Directory

Lors d'une authentification Active Directory, l'option Certificats client est disponible dans l'assistant d'authentification. Elle évite à l'utilisateur de spécifier un nom d'utilisateur et un mot de passe d'utilisateur privilégié, à condition qu'un certificat client ait été créé et installé pour SGD et qu'Active Directory utilise les certificats client.

Magasin de certificats SGD

Le mot de passe utilisé pour le magasin de certificats de SGD (*/rép-install/var/info/certs/sslkeystore*) n'utilise plus le code permanent 123456. Chaque magasin dispose à présent d'un mot de passe aléatoire stocké dans */rép-install/var/info/key*. Utilisez ce mot de passe avec les options `-storepass` et `-keypass` lorsque vous utilisez `keytool`.

Octroi de licence

Les modifications suivantes ont été apportées au contrat de licence de la version 4.2 :

- L'activation des clés de licence n'est plus nécessaire pour activer une baie.
- L'octroi d'une licence de manière nominative n'est plus disponible.
- Les clés de licence pour la maintenance et le droit de mise à niveau n'existent plus.

La mise à niveau à partir d'une version antérieure entraîne automatiquement la conversion des clés de licence existantes et la suppression des clés de licence obsolètes.

Méthodes de connexion aux applications

Depuis la version 4.1, SGD ne prend plus en charge les méthodes de connexion `rlogin` et `rcmd` pour le démarrage des applications. Pour mettre à niveau à partir d'une version antérieure, vous devez modifier la méthode de connexion de toutes les applications qui utilisent ces méthodes.

Attribut des connexions simultanées au bureau Web

Depuis la version 4.1, SGD utilise un attribut différent pour le paramétrage du nombre maximal de sessions utilisateur simultanées (`--tuning-maxconnections`). La configuration par défaut de cet attribut s'applique au logiciel mis à niveau à partir d'une version antérieure.

Applications mainframe (3270)

Depuis la version 4.0, SGD utilise un émulateur différent pour les applications mainframe (3270). Les objets des applications X 3270 et de celles à traitement de caractères 3270 ne sont plus disponibles et ont été remplacés par un seul objet d'application 3270. Le nouvel objet d'application 3270 ayant plusieurs attributs, il est possible de mettre à niveau les objets d'application 3270 existants. La mise à niveau à partir d'une version antérieure entraîne la suppression automatique des applications X 3270 et à traitement de caractères 3270. Vous devez donc les reconfigurer.

Produits pris en charge, problèmes connus, résolution de bogues et problèmes détectés dans la documentation

Ce chapitre contient des informations à propos des produits pris en charge par SGD.

Il est constitué des rubriques suivantes :

- [Produits n'étant plus pris en charge, page 58](#)
- [Problèmes et bogues connus, page 58](#)
- [Résolution de bogues dans la version 4.40, page 72](#)
- [Résolution de bogues dans la version 4.31, page 74](#)
- [Résolution de bogues dans la version 4.30, page 75](#)
- [Problèmes liés à la documentation dans la version 4.40, page 84](#)

Produits n'étant plus pris en charge

Le tableau suivant dresse la liste des dates de fin de prise en charge pour les produits SGD.

Logiciel et version	Fin de prise en charge	Fin de prise en charge limitée	Fin de durée de vie
Logiciel Sun Secure Global Desktop 4,3	29.04.09	29.04.13	29.04.13
Logiciel Sun Secure Global Desktop 4.2	08.11.08	08.11.12	08.11.12
Secure Global Desktop Enterprise Edition 4.1			31 mars 2007
Secure Global Desktop Enterprise Edition 4.0			31 mars 2007
Secure Global Desktop Software Appliance 4.0			31 mars 2007
Secure Global Desktop Enterprise Edition 3.44*			31.12.07
Secure Global Desktop Enterprise Edition 3.42			31 mars 2007
Tarantella Enterprise 3 (TASP compris)			31 mars 2007

* Japonais uniquement

Pour obtenir des informations à propos de la politique de fin de vie Sun (EOSL, End of Service Life), consultez <http://www.sun.com/service/eosl/>.

Les clients en possession d'un accord de prise en charge valide peuvent mettre leur logiciel SGD à niveau vers la version la plus récente, sans frais supplémentaires.

Problèmes et bogues connus

Cette section répertorie les bogues et problèmes connus de SGD version 4.40.

602423 : Problèmes liés à la touche retour et à la touche Entrée du pavé numérique

Problème : les émulateurs de caractères et SGD ne font pas la différence entre la touche retour et la touche Entrée du pavé numérique sur le clavier client de l'utilisateur.

Cause : un problème connu.

Solution : par défaut, le client SGD mappe la touche Entrée du pavé numérique tant pour revenir à la session X que pour revenir à la session d'application de caractères. Il est possible de modifier ce comportement à l'aide de paramètres appropriés.

Pour modifier le comportement de la touche Entrée du pavé numérique dans une session d'*application à traitement de caractères*, définissez un mappage pour l'objet d'application à traitement de caractères (`--keymap`) et ajoutez un mappage pour `KPENTER`, comme ci-dessous :

```
KPENTER="hello"
```

Pour modifier le comportement de la touche Entrée dans une session *Windows* ou d'*application X*, modifiez le mappage X (par exemple, `xuniversal.txt`) et ajoutez un mappage pour la touche `KP_Enter`, par exemple :

```
92 KP_Enter KP_Enter NoSymbol NoSymbol 0x801c
```

Attention – Le mappage X constituant une ressource utilisateur globale, chacune des applications de cet utilisateur est susceptible d'être affectée par cette modification. Si l'une de ces applications ne gère pas `KP_Enter`, vous devrez peut-être demander de l'aide au fournisseur de l'application Windows/X.

6443840 : échec de configuration automatique de scripts du serveur proxy

Problème : les scripts de configuration automatique de serveur proxy peuvent spécifier une liste de serveurs proxy à essayer. Si le premier sur la liste n'est pas disponible, le navigateur essaie les serveurs suivants jusqu'à ce qu'il en trouve un qui soit disponible.

Si vous utilisez Microsoft Internet Explorer avec l'outil Sun Java Plug-in version 1.5.0, seul le premier serveur proxy de la liste est utilisé. Si ce serveur proxy n'est pas disponible, la connexion échoue.

Cause : un problème connu.

Solution : utilisez l'outil Sun Java Plug-in version 1.6.0.

6448990 : problèmes avec les touches \ (backslash) et ¥ (Yen)

Problème : les touches \ (backslash) et ¥ (Yen) des claviers japonais PC 106 et Sun Type 7 produisent le même résultat avec les applications Windows qui fonctionnent dans SGD.

Cause : problème connu lié à la gestion des touches.

Solution : modifiez les tables de touches Xsun ou Xorg sur le périphérique client.

Par exemple, modifiez le fichier `/usr/openwin/etc/keytables/Japan7.kt` comme suit :

```
...
#137      RN      XK_backslash  XK_bar  XK_prolongedsound
137      RN      XK_yen          XK_bar  XK_prolongedsound
...
#39       RN      XK_0      XK_asciitilde  XK_kana_WA      XK_kana_WO
39       RN      XK_0      XK_0          XK_kana_WA      XK_kana_WO
...
```

Par exemple, modifiez le fichier `/usr/X11/lib/X11/xkb/symbols/sun/jp` comme suit :

```
...
# key <AE13> { [ backslash, bar      ], [ prolongedsound  ]      };
  key <AE13> { [ yen, bar          ], [ prolongedsound    ]      };
...
# key <AE10> { [ 0, asciitilde      ], [ kana_WA, kana_WO  ]      };
  key <AE10> { [ 0, 0], [ kana_WA, kana_WO  ]      };
...
```

Après ces modifications, redémarrez `dtlogin` :

```
# /etc/init.d/dtlogin stop
# /etc/init.d/dtlogin start
```


6456278 : le mode intégré ne fonctionne pas pour l'utilisateur root

Problème : lors des connexions en tant qu'utilisateur `root` sur les plates-formes Solaris 10x86, aucune application ne vient s'ajouter au menu de démarrage de Solaris 10 bien que le mode intégré soit activé. De surcroît, l'avertissement suivant s'affiche :

```
gnome-vfs-modules-WARNING **: Error writing vfolder configuration
file "///.gnome2/vfolders/applications.vfolder-info": File not found.
```

Cause : problème connu lié au système de fichiers virtuel (VFS) de Gnome.

Solution : aucune solution n'est actuellement disponible.

6458111 : le menu principal Gnome s'arrête brutalement en cas d'utilisation du mode intégré

Problème : sur les périphériques client exécutant SUSE Linux Enterprise Server 10, le menu principal Gnome s'arrête brutalement en cas d'utilisation du client SGD en mode intégré. L'arrêt se produit généralement à la connexion ou à la déconnexion.

Cause : ce comportement est dû à un problème connu avec l'applet du menu principal Gnome sur SUSE Linux Enterprise Server 10 (bogue Novell, référence 186555).

Solution : installez la dernière version du package `gnome-main-menu.rpm` pour SUSE Linux Enterprise Server 10.

Vous pouvez aussi désactiver la fonctionnalité Dernières applications utilisées : le menu principal Gnome sera alors plus stable. Exécutez les commandes suivantes sur le périphérique client :

```
$ gconftool-2 --set --type=list --list-type=int \  
/desktop/gnome/applications/main-menu/lock-down/showable_file_types [0,2]  
$ pkill main-menu  
$ pkill application-browser
```

6461864 et 6476661 : échec de la connexion automatique et du mode intégré avec le bureau Gnome

Problème : une fois la connexion client automatique ou le mode intégré activés, le client SGD ne démarre pas automatiquement lorsque vous vous connectez au bureau Gnome et le menu Démarrer n'est pas mis à jour avec les contenus du bureau Web lorsque vous vous connectez à SGD. Ce problème touche SUSE Linux Enterprise Server 9 et Red Hat Enterprise Linux 4.

Cause : comme les répertoires contenant les fichiers `.menu` ne sont pas contrôlés, la détection des modifications dans le menu Démarrer est impossible.

Solution : exécutez la commande `kill gnome-panel` pour redémarrer le panneau Gnome et collecter les nouvelles informations du menu.

Remarque – Vous devez exécuter la commande `kill gnome-panel` pour mettre le menu à jour à *chaque* modification de ce dernier.

6468716 : le clavier ne fonctionne pas pendant les sessions Gnome

Problème : une fois la session Gnome démarrée sur SE Solaris 10 sur plates-formes SPARC, il est impossible de saisir quoi que ce soit au clavier. Cependant, la souris fonctionne toujours.

Cause : un bogue connu lié aux sessions Gnome. La référence du bogue Sun Microsystems est 6239595.

Solution : ce problème spécifique a été résolu par le patch 119542. Ce patch a également été inclus à un patch cumulé (ID de patch : 122212) pour Gnome Desktop.

Pour résoudre ce problème, créez un fichier de configuration Gnome `/etc/gconf/gconf.xml.defaults/apps/gnome_settings_daemon/keybindings/%gconf.xml` avec le contenu suivant :

```
<?xml version="1.0"?>
<gconf>
<entry name="volume_up" mtime="1110896708" type="string">
<stringvalue></stringvalue>
</entry>
<entry name="volume_mute" mtime="1110896705" type="string">
<stringvalue></stringvalue>
```

```

</entry>
<entry name="volume_down" mtime="1110896702" type="string">
<stringvalue></stringvalue>
</entry>
<entry name="help" mtime="1110896698" type="string">
<stringvalue></stringvalue>
</entry>
</gconf>

```

6470197 : échec de la compilation du module serveur Web SGD

Problème : lorsque vous compilez les modules Apache pour les utiliser avec un serveur Web SGD, la compilation échoue en raison de l'absence du compilateur egcc.

Cause : le fichier de configuration de l'outil Apache eXtenSion (apxs) servant à construire les modules d'extension du serveur Web SGD a recours au compilateur egcc alors que celui-ci n'est peut-être pas disponible sur le système.

Solution : spécifiez un compilateur disponible sur le système dans le fichier de configuration apxs ou créez un lien symbolique entre le compilateur egcc et le compilateur disponible sur le système. Le fichier de configuration apxs se trouve dans `/rép-install/webserver/apache/version/bin/apxs`.

6476194 : aucun élément de menu de KDE Desktop pour le client SGD

Problème : les raccourcis vers le client SGD ne s'affichent pas dans le menu de KDE Desktop sur SUSE Linux Enterprise Server 10.

Cause : dans une configuration SUSE du système de menu KDE, c'est l'application qui figure dans un menu, et non le menu lui-même, qui est utilisée dans le menu principal (sous réserve que le menu en question ne contienne qu'une seule entrée). Si cette entrée de menu est un sous-menu, celui-ci ne s'affiche pas. Par conséquent, le menu de connexion pour le client SGD en mode intégré ne s'affiche pas.

Solution : pour résoudre ce problème, ajoutez la ligne suivante à la section [menus] du fichier `$HOME/.kde/share/config/kickerrc` :

```
ReduceMenuDepth=false
```

Exécutez ensuite la commande ci-dessous pour que le panneau KDE applique immédiatement ces modifications :

```
# dcop kicker kicker restart
```

Toutes les sessions KDE utiliseront automatiquement ce paramètre.

6477187 : le mappage du disque client échoue sans le service Client pour les réseaux Microsoft

Problème : le mappage du disque client échoue si le service Client pour les réseaux Microsoft n'est pas activé sur un serveur d'application Windows.

Cause : le service Client pour les réseaux Microsoft doit être activé pour que le système puisse accéder à distance aux fichiers et dossiers.

Solution : activez le service Client pour les réseaux Microsoft.

▼ Activation du client pour les réseaux Microsoft

1. Dans le Panneau de configuration, double-cliquez sur Connexions réseau.
2. Cliquez avec le bouton droit de la souris sur la carte réseau et sélectionnez Propriétés.
3. Dans l'onglet Général, cochez la case en regard de Client pour les réseaux Microsoft.
4. Cliquez sur OK.

6481312 : la mise à niveau réinitialise les types de connexion disponibles

Problème : après la mise à niveau vers la version 4,40, un serveur configuré pour accepter uniquement les connexions sécurisées accepte également les connexions standard.

Cause : un problème connu.

Solution : reconfigurez le serveur pour qu'il accepte uniquement les connexions sécurisées. Dans la console d'administration, affichez l'onglet Sécurité des serveurs Secure Global Desktop ⇒ pour le serveur SGD et désactivez l'option Standard dans le champ Types de connexion. Vous pouvez aussi exécuter la commande ci-dessous :

```
$ tarantella config edit --security-connectiontypes ssl
```

6482912 : le client SGD n'est pas installé automatiquement

Problème : lorsque Internet Explorer 7 est utilisé sur les plates-formes Microsoft Windows Vista, le téléchargement et l'installation automatique du client SGD sont impossibles. Le client SGD peut être installé soit manuellement, soit automatiquement à l'aide d'un autre navigateur, par exemple Firefox.

Cause : Internet Explorer propose un mode Protégé qui empêche le téléchargement et l'installation automatique du client.

Solution : ajoutez le serveur SGD à la liste des sites de confiance dans les paramètres de sécurité d'Internet Explorer.

6493374 : caractères non ASCII dans les fenêtres de méthode d'entrée

Problème : dans les environnements linguistiques chinois (simplifié et traditionnel), les caractères non ASCII ne s'affichent pas dans les fenêtres de candidature et de statut de la méthode d'entrée lors de l'exécution d'applications sur un serveur d'applications SE Solaris. Ce problème se produit sur les plates-formes SE Solaris 8, 9, 10 et 10u1.

Cause : le chemin de la police n'est pas configuré sur le serveur SGD.

Solution : si le serveur d'application est en cours d'exécution sur Solaris10 ou Solaris10u1, effectuez l'une des opérations suivantes :

- Pour les plates-formes SPARC, installez les patches 120410,120412 et 120414.
- Pour les plates-formes x86, installez les patches 120411,120413 et 12041.
- Effectuez une mise à niveau vers Solaris 10u2 ou une version ultérieure.

Si le serveur d'application est en cours d'exécution sur Solaris 8 ou Solaris 9, effectuez l'une des opérations suivantes :

- **Chinois simplifié** : définissez les variables d'environnement sur "LANG=zh;LC_ALL=zh" dans l'onglet Applications ⇒ Démarrer de la console d'administration.
- **Chinois traditionnel** : définissez les variables d'environnement comme suit "LANG=zh_TW;LC_ALL=zh_TW" dans l'onglet Applications ⇒ Démarrer de la console d'administration.

6542943 : Firefox échoue avec l'outil Sun Java Plug-in version 1.5

Problème : le navigateur Web Firefox s'interrompt de façon inattendue lorsque l'outil Sun Java Plug-in version 1.5.0 est utilisé.

Cause : le chemin de la machine virtuelle Java (JVM) a été modifié dans la version 1.5.0 de l'outil Sun Java Plug-in.

Solution : assurez-vous qu'il existe un lien symbolique entre le répertoire des plug-ins Firefox et l'emplacement de la JVM, `/usr/local/jre-version/plugin/i386/ns7/libjavaplugin_oji.so`, où *jre-version* correspond à la version de Java Runtime Environment (JRE™).

6555834 : Java est activé pour le navigateur mais n'est pas installé sur le périphérique client

Problème : lorsque Java est activé dans les paramètres du navigateur Web, mais qu'aucun outil Sun Java Plug-in n'est 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 connexion.

Cause : SGD utilise les paramètres du navigateur Web pour déterminer si Java sera utilisé.

Solution : installez l'outil Sun Java Plug-in et créez un lien symbolique entre le répertoire des plug-ins du navigateur Web et l'emplacement de JVM. Pour obtenir plus d'informations, reportez-vous à la documentation du navigateur Web.

6591516 : les transitions de pages du bureau Web ne fonctionnent pas dans Internet Explorer

Problème : avec certaines versions du pare-feu client Symantec, telles que la version 8.7.4.79, des problèmes de connexion peuvent se produire lors de l'utilisation d'Internet Explorer. Le processus de connexion s'arrête au niveau de l'écran de connexion et le bureau Web SGD ne s'affiche pas.

Cause : le pare-feu intercepte certaines opérations JavaScript.

Solution : définissez le serveur SGD en tant qu'hôte fiable. Pour obtenir plus d'informations, reportez-vous à la documentation Symantec.

6592560 : l'aide en ligne de la console d'administration n'est pas disponible avec le protocole HTTPS

Problème : l'aide en ligne de la console d'administration est désactivée lorsque les connexions HTTPS au serveur Web SGD sont activées.

Cause : la console d'administration utilise le logiciel JavaHelp™ pour afficher l'aide en ligne. L'exécution de JavaHelp avec une connexion HTTPS requiert des paramètres supplémentaires.

Solution : importez le certificat utilisé pour sécuriser le serveur Web SGD dans le keystore du logiciel JDK™. Utilisez l'application `keytool` du logiciel Java de la manière suivante :

```
$ keytool -import -keystore -storepass changeit \  
/rép-install/bin/version-jdk/jre/lib/security/cacerts \  
-file /rép-install/var/tsp/ca.pem
```

changeit correspond au mot de passe du keystore et *version-jdk* à la version de JDK installée sur le serveur SGD.

Si vous possédez plusieurs certificats dans le fichier `ca.pem`, séparez les certificats et ajoutez-les individuellement.

6598048 : le clavier français (Canada) n'est pas correctement mappé pour les applications Windows

Problème : lorsque vous utilisez une disposition de clavier (hérité) français (Canada) avec des applications Windows, certains caractères français ne s'impriment pas correctement.

Cause : problème connu lié à la disposition du clavier (hérité) français (Canada).

Solution : aucune solution connue. À l'heure actuelle, aucun fichier de mappage clavier compatible n'est fourni avec SGD.

6605404 : le fichier de ressources Tomcat a changé d'emplacement

Problème : après une mise à niveau vers la version 4.40, vous pouvez rencontrer des problèmes lors de la configuration de connexions SOAP sécurisées.

Cause : le fichier de ressources `Resources.properties` a été transféré vers un autre emplacement dans cette version. Il est requis lors de la sécurisation de connexions SOAP dans le conteneur JSP Tomcat. Son emplacement était, dans la version 4.31:

```
/rép-install/webserver/tomcat/version/webapps/sgd/WEB-INF/classes/com/tarantella/tta/webservices/client/apis/Resources.properties
```

L'emplacement de ce fichier dans la version 4.40 est le suivant :

```
/rép-install/webserver/tomcat/version/shared/classes/com/tarantella/tta/webservices/client/apis/Resources.properties
```

Solution : localisez et modifiez le fichier `Resources.properties`. Redémarrez le conteneur JSP Tomcat.

6609001 : il est impossible de séparer un serveur secondaire arrêté à l'aide de la console d'administration

Problème : lorsqu'un serveur est hors service, il est impossible de le supprimer de la baie SGD via la console d'administration. Les opérations de séparation à l'aide de la commande `tarantella array detach` ne sont pas affectées.

Cause : dans cette version, la séparation d'un serveur secondaire hors service à l'aide de la console d'administration n'est pas prise en charge.

Solution : redémarrez le serveur hors service et utilisez la console d'administration pour le séparer de la baie SGD. Vous pouvez aussi utiliser la commande `tarantella array detach` pour supprimer le serveur secondaire hors service.

6609518 : lien à la baie lorsque la console d'administration est en cours d'exécution à partir d'un serveur secondaire

Problème : vous ne pouvez pas ajouter un nouveau serveur secondaire à une baie SGD lorsque la console d'administration est en cours d'exécution sur un serveur secondaire existant.

Cause : dans cette version, il est impossible de fournir des informations d'authentification pour plusieurs serveurs secondaires.

Solution : exécutez la console d'administration à partir du serveur principal ou du serveur à relier à la baie.

6610760 : les paramètres personnalisés de l'imprimante PDF ne sont pas respectés dans les applications Windows

Problème : les paramètres personnalisés de l'imprimante PDF ne sont pas respectés lorsque vous imprimez depuis une application Windows.

Par exemple : vous *activez* l'imprimante PDF universel SGD et le visionneur PDF universel pour une unité d'organisation. Ensuite, vous ignorez les paramètres des unités parentes et *désactivez* l'imprimante PDF universel et le visionneur PDF universel pour un utilisateur dans l'unité d'organisation. Les paramètres d'impression personnalisés ne sont pas définis en fonction de l'utilisateur.

Cause : problème connu lié à la transmission des paramètres de l'imprimante PDF universel.

Solution : aucune solution connue. Définissez les paramètres de l'imprimante PDF de préférence au niveau de l'organisation ou de l'unité d'organisation lorsque cela est possible.

6611502 : des erreurs se produisent lors de la création ou de la modification d'objets à partir d'un serveur secondaire

Problème : la création ou la modification d'objets lorsque la console d'administration est en cours d'exécution à partir d'un serveur secondaire SGD génère le message d'erreur suivant : Impossible de créer l'objet.

Cause : l'objet est créé ou modifié correctement, mais la console d'administration procède au chargement avant que les données répliquées ne soient renvoyées du serveur principal.

Solution : attendez quelques secondes, puis répétez l'opération.

Problèmes liés au clavier japonais Sun Type 7

Problème : les utilisateurs possédant des claviers japonais Sun Type 7 ne peuvent pas saisir correctement les caractères dans SGD.

Cause : il manque une table de touches SE Solaris sur le périphérique client.

Solution : installez le patch nécessaire à l'installation de la table de touches sur le périphérique client :

Plate-forme	Patch
SE Solaris 10 sur plate-forme SPARC	121868
SE Solaris 9 sur plate-forme SPARC	113764
SE Solaris 8 sur plate-forme SPARC	111075
SE Solaris 10 sur plate-forme x86	121869
SE Solaris 9 sur plate-forme x86	113765
SE Solaris 8 sur plate-forme x86	114539

Les éléments du menu Démarrer ne sont pas triés par ordre alphabétique

Problème : les utilisateurs du client SGD en mode intégré sur les périphériques client Microsoft Windows ont remarqué que les entrées du menu Démarrer n'étaient pas classées par ordre alphabétique.

Cause : sous Windows, les ajouts sont insérés en fin de la liste et non pas dans l'ordre alphabétique.

Solution : consultez Microsoft KB article 177482 pour obtenir des informations.

Absence d'entrées du menu de démarrage sur Sun Java Desktop System

Problème : sur Sun Java Desktop System, aucune entrée du menu de démarrage n'est créée pour Secure Global Desktop, bien que le mode intégré soit activé. Ces entrées sont ajoutées après déconnexion, puis reconnexion.

Cause : problème connu lié au panneau Gnome.

Solution : installez les patchs suivants :

- 119906 pour SE Solaris sur plate-forme SPARC ;
- 119907 pour SE Solaris sur plate-forme x86.

Pour contourner le problème, déconnectez-vous du bureau puis reconnectez-vous.

Résolution de bogues dans la version 4.40

Le tableau suivant répertorie les principales corrections de bogues apportées à la version 4.40.

Référence	Description
2144612	L'authentification Active Directory ne bascule pas vers le catalogue global suivant.
2147536	La commande <code>ttaxpe</code> ne ferme pas lorsqu'un mot de passe incorrect a été saisi.
2148699	Le mappage du disque client échoue avec des noms DNS externes multiples.
2148700	Le client SGD échoue lorsqu'une application X s'ouvre dans une fenêtre spécifique.
2148811	Les préférences d'impression dans les services de terminal ne sont pas définies de façon permanente pour une imprimante de code zébré.
2149630	Le clavier coréen ne fonctionne pas correctement avec SSD 4.30.915.
2150849	Des problèmes se produisent occasionnellement au niveau de la redirection d'un port COM (série).
2151274	Les caractères accentués ne s'affichent pas dans les fenêtres de l'environnement linguistique français.
6469935	Le client SGD devrait pouvoir associer le nom d'hôte à l'élément DNS dans l'extension <code>subjectAltName</code> du certificat.

Référence	Description
6478585	Élimination de la clé SSL de la machine virtuelle Java et du magasin de certificats à la mise à niveau.
6520742	La commande <code>tarantella security peerca --show</code> échoue sur le serveur SGD principal.
6525004	Extension de la connexion au périphérique client dans le client SGD.
6527507	Meilleur signalement des erreurs pour les échecs de service Web.
6532425	Le mappage du disque client UNIX échoue lorsque la commande <code>ttattem</code> n'est pas installée dans un répertoire standard.
6532764	Le basculement LDAP n'est pas continu lorsque plusieurs serveurs LDAP sont configurés.
6537643	Le client SGD s'arrête brutalement lorsque l'utilisateur quitte l'application quand une boîte de dialogue est ouverte.
6541478	La session SGD se bloque lorsque l'audio a été lu depuis SGD tandis que l'audio local est lu sur le client Sun Ray.
6541914	Le mappage du disque client ne fonctionne pas dans certains scénarios sous Windows Vista.
6542533	Le bureau Web ne se met pas à jour pour afficher les applications ouvertes dans Safari sous Mac OS X 10.4.9.
6544350	Les commandes d'impression du bureau Web ne sont pas stables dans une baie.
6546840	Le mode intégré n'est pas activé sur SUSE Linux Enterprise Server 9.
6547337	L'option <code>-preferredlanguage</code> de la commande <code>ttatcc</code> n'ouvre pas la page dans l'environnement linguistique approprié.
6550172	Le démarrage échoue lorsqu'un serveur hors ligne est sélectionné dans un groupe équilibré.
6552038	Améliorations apportées à la journalisation du débogage de <code>ttaxpe</code> .
6553252	Le client SGD se ferme avec un défaut de segmentation et est interrompu par l'application Electric Fence.
6558691	Les licences secondaires sont supprimées en cas d'arrêt des licences principales ou de déconnexion de la baie.
6561306	Vérification de la version <code>ssh</code> avant la mise à jour des arguments <code>ssh</code> .
6563481	Amélioration des messages d'erreur dans les fichiers journaux <code>execpe</code> .
6571826	La ligne de commande pour la création d'objets 3270 et 5250 n'accepte pas correctement tous les arguments.
6574469 6574471	Mise à jour de la plate-forme Java, de Standard Edition vers la version 1.6.0_01 ou une version ultérieure (tiers) pour les plates-formes Solaris et Linux.
6583316	Le mappage du disque client ne peut pas être désactivé d'un client à l'autre pour les clients SGD.

Référence	Description
6583333	Le démarrage de <code>ssh</code> échoue lorsque <code>sshhelper</code> est défini sur <code>setuid</code> et que l'utilisateur SGD ne possède pas de répertoire de base.
6597576	Le module d'enrichissement SGD pour les plates-formes Linux ne s'installe pas sur un chemin d'accès différent du chemin par défaut.
6598686	Le titre de l'application est récupéré dans les environnements linguistiques.
6601084	En mode intégré, le dossier spécifié dans le champ Démarrer dans n'est pas valide.

Résolution de bogues dans la version 4.31

Le tableau suivant répertorie les principales corrections de bogues apportées à la version 4.31.

Référence	Description
2140625	La fonction de redirection de fuseau horaire a été corrigée pour les clients sur les plates-formes UNIX.
2145026	Les informations de licence ne sont plus copiées sur l'ensemble des serveurs secondaires tant qu'un redémarrage n'a pas eu lieu.
2145602	Le lancement d'application X est lent ou expire. Possibilité d'une erreur dans la gestion de méthode d'entrée dans le script <code>procs.exp</code> .
2145932	La fonctionnalité de la touche Windows est retenue lorsque vous revenez à une session SGD.
2146043	Si vous utilisez le mappage de disques clients, vous ne pouvez pas écraser un fichier de taille supérieure.
2146285	Tomcat échoue et les icônes ne s'affichent pas sur le bureau Web.
6440254	La boîte de dialogue de l'authentification du serveur proxy ne contient pas les informations de domaine.
6443192	La mise à niveau à l'aide de la commande <code>pkgadd</code> sur le SE Solaris rapporte des centaines de conflits de fichiers.
6443840	Le client SGD ne comprend pas le basculement de proxy à partir de fichiers de configuration de serveur proxy (PAC).
6474180	La limite <code>HARD_SERVER_LIMIT</code> du serveur Web SGD passe à 1 024.
6480225	En mode intégré, les applications ne parviennent pas à reprendre sur les plates-formes client UNIX.

Référence	Description
6494450	Le mappage de disque client ne peut pas gérer des fichiers dont la taille dépasse 2 Go.
6499639	Une requête récursive de répertoire entraîne une erreur de segmentation lors de l'utilisation du mappage de disque client sur les plates-formes UNIX et Linux.
6503627	Le fichier de mappage de clavier <code>xfrbelgian.txt</code> contient une erreur.
6518152	Le menu Démarrer n'est pas mis à jour en utilisant le mode intégré sur les périphériques client Microsoft Windows Vista.
6518638	La commande <code>tarantella print cancel</code> supprime toutes les impressions et non pas l'impression sélectionnée.
6525384	XRDP ne fonctionne pas avec SGD.
6528037	Page introuvable s'affiche sur le bureau Web lorsqu'un groupe contenant des hôtes est déployé par erreur sur un bureau Web.
6506222	Le fichier <code>.xdefaults</code> d'un utilisateur n'est pas utilisé lors du lancement d'une application.

Résolution de bogues dans la version 4.30

Cette section répertorie les principales corrections de bogues apportées à la version 4.30. Les corrections de bogues sont classées selon les catégories suivantes :

- [Outils d'administration, page 76](#)
- [Échec de lancement, page 76](#)
- [Clients et bureau Web, page 77](#)
- [Émulation, page 78](#)
- [Installation et mise à niveau, page 79](#)
- [Internationalisation et localisation, page 79](#)
- [Autre, page 80](#)
- [Impression, page 81](#)
- [Sécurité, page 81](#)
- [Serveur, page 82](#)
- [Authentification des utilisateurs, page 82](#)
- [Services Web, page 83](#)

Outils d'administration

Les bogues suivants des outils d'administration SGD ont été corrigés.

Référence	Description
6433525	Le propriétaire de <code>/usr/bin</code> devient utilisateur <code>ttasys</code> au démarrage.
6436735	La commande <code>tarantella object new_xapp</code> n'accepte pas l'argument <code>--accel</code> .
6437203	Le gestionnaire d'objets affiche un message d'avertissement lorsque vous renommez un objet ENS.
6445405	Si l'utilisateur tente de prendre le contrôle à distance via la ligne de commande, l'ID de session utilisé n'est pas valide.
6447937	Les cookies d'autorité X ne doivent pas être transmis via l'environnement.
6450323	Les attributs ne peuvent pas être spécifiés à la création d'un objet mais peuvent être définis lors de sa modification.
6451537	Les commandes <code>tarantella license</code> et le gestionnaire de baies affichent des composants logiciels obsolètes.

Échec de lancement

Les bogues de lancement d'application suivants ont été corrigés.

Référence	Description
6357003	Le client natif ne peut pas lancer un navigateur Web sur SE Solaris.
6357022	Le client natif décale vers le haut le bureau Web en plein écran sur Java Desktop System.
6392279	Un problème d'autorisation X entraîne l'échec du lancement.
6401949	Lorsque <code>optimizelaunch</code> est activé dans le script de connexion <code>unix.exp</code> , le gestionnaire de mots de passe expirés ne fonctionne pas.
6405808	Le script de filtrage (<code>runsubscript.exp</code>) n'est pas appelé lors du processus de lancement.
6416951	Un message d'erreur s'affiche lorsque l'utilisateur ferme une application dans la fenêtre du navigateur en cliquant sur le bouton en forme de croix.
6419574	La boîte de dialogue d'authentification renvoie des données défectueuses si le mot de passe contient plus de huit caractères.
6427189	Un échec du lancement se produit lorsque SSH ne connaît pas l'hôte.

Référence	Description
6434660	La gestion de l'expiration de mot de passe au lancement de l'application est interrompue.
6447551	Un seul processus ttacpe devrait être créé par session de bureau Web.
6455378	Échec du lancement lorsque SSH est utilisé via su pour une application s'exécutant sur l'hôte SGD.
6464809	Si la bannière de connexion du système contient un caractère #, le processus de lancement automatique échoue.
6470173	Ajout de la prise en charge de l'agent SecurID ACE pour PAM.
6475303	Les certificats d'autorité de certification personnalisés ne sont pas reconnus et génèrent une invite lors du lancement d'applications sur place.
6476180	La fenêtre racine reste affichée après la déconnexion d'une session Gnome de kiosque.

Clients et bureau Web

Les bogues suivants des clients SGD et du bureau Web ont été corrigés.

Référence	Description
6408157	Impossible de lancer une application de serveur X local à partir du bureau Web JSP.
6417140	Le cadre du bureau Web est vide après le lancement d'une application.
6417575	Client natif UNIX utilisant un serveur proxy : en cas de connexion, déconnexion puis reconnexion, le client natif se bloque.
6417631	Client natif UNIX : problèmes de retraçage avec les applications de kiosque.
6424776	Si l'utilisateur se déconnecte du bureau Web, le client SGD génère des erreurs et se ferme.
6432133	Le client natif SGD génère une erreur de segmentation si l'utilisateur ferme la fenêtre de progression de la connexion.
6465959	Lors du redémarrage de SGD, le client SGD s'exécute en boucle et envoie des centaines de paquets.
6468173	Sur les clients légers Sun Ray, le curseur d'attente n'est désormais plus défini de façon permanente.

Émulation

Les bogues d'émulation suivants ont été corrigés.

Référence	Description
6381531	Fichier <code>colormap.txt</code> modifié parfois ignoré lorsque la sécurité est activée.
6386091	Client natif SGD pour Windows et client Citrix ICA X : incompatibilité potentielle des événements liés aux touches du clavier.
6415498	Fermeture inattendue d'une session de terminal à traitement de caractère en cas d'utilisation des touches de fonction.
6417698	Les applications à fenêtre de taille variable ne basculent pas lorsque l'utilisateur appuie sur la touche arrêt défilement.
6426355	<code>ttaxpe</code> sort avec un défaut de segmentation.
6427789	En cas de copie (<code>ctrl+insert</code>), les applications X se bloquent.
6433273	Lorsque le client natif est utilisé sur SE Solaris, l'affichage du mode kiosque est incorrect.
6435437	Des fenêtres enfant s'affiche parfois sous leur fenêtre parent via des fenêtres transparentes.
6435489	Améliorations des performances pour les applications Windows.
6435527	Erreur de segmentation dans <code>ttaxpe</code> lors de l'exécution de l'outil de contrôle HP.
6445467	Les touches de logo Windows ne fonctionnent pas dans une session de services de terminal.
6446469	Problèmes relatifs au mappage et à l'environnement linguistique français.
6467368	Lettre répétée dans une session Remote Desktop Protocol.
6471395	La fonction de redirection de fuseau horaire ne parvient pas à définir l'heure exacte lors du passage à l'heure d'été. L'heure définie est toujours décalée d'une heure.
6472959	L'utilisation de la combinaison de touches Échap+Verr.num via un client SE Solaris ou un client léger SunRay entraîne un comportement inattendu.

Installation et mise à niveau

Les bogues d'installation et de mise à niveau suivants ont été corrigés.

Référence	Description
6355269	La configuration par défaut d'une session Java Desktop System perd des paramètres de configuration importants.
6368390	La mise à niveau de la version 4.20.909 vers les versions plus récentes requiert une opération de maintenance ou l'octroi d'un droit de mise à niveau de la licence.
6368675	Les certificats racine des serveurs LDAP sécurisés ne sont pas conservés en cas de mise à niveau.
6396629	L'installation échoue lors de la création de bean et le serveur ne démarre pas.
6407985	À l'installation, SGD ne gère pas correctement les grands volumes d'espace disque disponible.
6430913	Le fichier de configuration du serveur Web (<code>httpd.conf</code>) n'a pas été mis à niveau correctement.
6446020	La désinstallation de SGD ne s'exécute pas si le nom DNS externe est incorrect.
6453638	Connexion impossible à un serveur SGD après la mise à niveau.
6462429	SGD est désinstallé même si l'utilisateur sélectionne Non.

Internationalisation et localisation

Les bogues de localisation et d'internationalisation ont été corrigés.

Référence	Description
6354105	Dans l'assistant de configuration, la liste des applications affiche des chaînes défectueuses avec des caractères multioctets.
6355226	La boîte de dialogue Progression de la connexion ne peut pas afficher les caractères multioctets.
6357040	Impossible de copier et coller de Microsoft Windows vers SE Solaris.
6357075	Impossible de copier et coller de Microsoft Windows vers Microsoft Windows.
6357606	Impossible de copier et coller de Java Desktop System vers Common Desktop Environment.
6362374	Le mappage de disque client s'arrête brutalement si un fichier <code>native-cdm-config</code> localisé est utilisé.

Référence	Description
6419511	Les applications Windows doivent utiliser Unicode par défaut pour le symbole de l'euro.
6419523	L'environnement LANG du serveur écrase les paramètres de version localisée du client.
6447594	L'accès au mode fenêtre du client doit s'effectuer à l'aide d'une adresse IP et non d'un socket UNIX.
6450008	Impossible de générer une apostrophe avec un clavier suédois.

Autre

Les bogues divers suivants ont été corrigés.

Référence	Description
6375600	L'authentification échoue avec la carte à puce ActivCard - Cyberflex 64k (également bogue 607218).
6384746	Possibilité de lire des fichiers Common Gateway Interface (.cgi) avec un navigateur Web.
6390126	Si de nombreux utilisateurs se connectent à la suite de façon rapprochée, le serveur SGD se bloque.
6393623	Une nouvelle fenêtre de navigateur s'ouvre lors du lancement d'applications dans des fenêtres de navigateur à l'aide de la touche Ctrl.
6407855	Le serveur SGD se ferme en générant le code d'erreur 129, signal 0.
6408159	Une nouvelle fenêtre de navigateur vide s'ouvre lorsque l'utilisateur ferme l'application ouverte dans le mode de nouvelle fenêtre de navigateur.
6409117	Il semble que le module d'enrichissement de SGD pour SE Solaris sur plate-forme x86 échoue.
6409765	Erreur lors de la copie de fichiers volumineux du client vers le serveur via une connexion réseau lente dans les sessions RDP.
6410161	Si la connexion au port 1023 de l'hôte local s'effectue via telnet, le gestionnaire de moteur de protocoles utilise la CPU à 100 %.
6416384	La lecture de la sortie audio RDP s'arrête en cas d'utilisation d'un client léger SunRay.
6418965	Les applications du gestionnaire de fenêtres client affichent des boutons Réduire et Agrandir absents de l'application d'origine.
6430243	SGD Apache inclut des configurations et chemins privés de développement.

Référence	Description
6430396	Impossible de copier et coller d'une session WCP IWM vers le bureau Web classique et vice versa.
6436155	Si le paramètre de connexion persistante est défini sur 0, des connexions persistantes sont envoyées en permanence.
6442142	Si l'utilisateur ferme une session Gnome, ttaxe utilise la CPU à 100 %.
6446271	Le serveur Web SGD démarre mais reste connecté à la console.
6466415	Le LDAP sécurisé ne fonctionne pas si les licences de sécurité ne sont pas installées.

Impression

Les bogues d'impression suivants ont été corrigés.

Référence	Description
6376221	Les propriétés de l'imprimante (telles que la taille du papier) ne semblent pas être stockées entre les session RDP.
6406292	Le nom du pilote est dupliqué si l'impression est configurée au niveau utilisateur et OU.
6421283	Le client natif Windows détecte <code>DEFAULT_PRINTER_UNKNOWN</code> si aucune imprimante n'est configurée sur le périphérique client.
6427852	Délai de connexion dû à une imprimante réseau inaccessible connectée au périphérique client.

Sécurité

Les bogues de sécurité suivants ont été corrigés.

Référence	Description
6419520	Les recherches LDAP de Active Directory contactent les serveurs AD des autres zones pour obtenir des informations.
6446338	L'invite de modification du mot de passe ne s'affiche pas après l'expiration du mot de passe.
6446437	Impossible de créer une baie une fois les connexions SSL activées entre les membres de la baie.

Référence	Description
6457984	Validation des entrées utilisateur dans la fenêtre de connexion pour éviter les attaques de script d'un site à l'autre.
6468699	Core dumps générés par le démon SSL en raison de <code>sigsegv</code> , signal 11.
6469123	L'application du patch de sécurité OpenSSL <code>secadv_20060905.txt</code> est nécessaire.
6476728	L'application du patch de sécurité OpenSSL <code>secadv_20060928.txt</code> est nécessaire.
6478735	Correction d'une vulnérabilité des feuilles de style en cascade SGD.

Serveur

Les bogues suivants des serveurs SGD ont été corrigés.

Référence	Description
6379743	Le résultat de la commande <code>tarantella status</code> est incorrect lorsque les connexions SSL entre les membres de la baie sont activées.
6392365	La baie présente des problèmes lorsque l'un des membres de la baie n'est pas contactable.
6393745	Impossible de définir un serveur secondaire comme serveur principal si le serveur principal est hors service.
6445200	Comportement de la baie lors de la jonction et de la séparation des membres d'une baie sous licence.

Authentification des utilisateurs

Les bogues d'authentification d'utilisateur suivants ont été corrigés.

Référence	Description
6383417	Si le fichier <code>krb5.conf</code> comporte des erreurs, la connexion utilisateur se bloque et le serveur ajoute indéfiniment des exceptions dans le fichier <code>jserver.log</code> .
6400123	Les connexions ambiguës ne sont pas autorisées si les données d'identification indiquées la première fois ne sont pas valides.
6415709	L'authentification Active Directory échoue si un arbre d'une forêt n'est pas configuré dans le fichier <code>krb5.conf</code> .

Référence	Description
6439688	Le client natif SGD pour Windows n'affiche pas de message d'erreur en cas d'échec de la modification d'un mot de passe Active Directory.
6454261	Script mis à jour attendu pour les applications SE Solaris en allemand.
6460263	La carte Oberthur AuthentIC n'est pas reconnue lorsque SGD est utilisé (résolu pour les clients Windows uniquement).
6465569	L'infrastructure Active Directory PKI ne bascule pas vers le serveur de catalogue global suivant.
6471877	L'autorité des connexions SecurID ne fonctionne pas correctement.

Services Web

Les bogues suivants des services Web SGD ont été corrigés.

Référence	Description
6391262	Les utilisateurs anonymes peuvent créer et modifier les groupes de bureau Web. Cette information est alors stockée sur un disque et n'est pas nettoyée.
6427185	Le serveur Web SGD affiche trop d'informations.

Problèmes liés à la documentation dans la version 4.40

Cette section répertorie les problèmes connus de SGD version 4.40.

Modifications apportées à l'onglet Profils des utilisateurs assignés

Les tableaux de l'onglet Applications ⇒ Profils des utilisateurs assignés de la console d'administration ont été modifiés de la manière suivante :

- **Tableau des profils des utilisateurs effectifs** : la colonne Référentiel de ce tableau a été supprimée. Les profils utilisateur du référentiel local sont répertoriés dans la zone Assignations locales de ce tableau. Les utilisateurs et les groupes d'un référentiel LDAP sont répertoriés dans la zone Assignations LDPA de ce tableau. Cette zone n'apparaît que si le paramètre Local + LDAP est sélectionné dans le champ Référentiel de l'onglet Profils utilisateur. Cliquez sur le lien Charger les assignations LDAP pour actualiser cette zone du tableau.
- **Tableau des assignations modifiables** : la colonne Référentiel de ce tableau a été renommée et s'intitule dorénavant Type d'assignation.

La section Assigned User Profiles Tab, page 119 du *Sun Secure Global Desktop 4.4 Reference Manual*, ne traite pas de ces modifications.

Le fichier de ressources Tomcat a changé d'emplacement

Le fichier de ressources `Resources.properties` a été transféré vers un autre emplacement dans la version 4.40. Ce fichier est requis lors de la sécurisation de connexions SOAP dans le conteneur JSP Tomcat.

Dans la version 4.40, ce fichier se trouve à l'emplacement suivant :

```
/rép-install/webserver/tomcat/version/shared/classes/com/tarantella/  
tta/webservices/client/apis/Resources.properties
```

La documentation publiée ne contient pas de détails concernant la modification de l'emplacement du fichier.

Délai d'attente automatique pour les sessions utilisateur inactives

La documentation publiée ne contient pas de détails concernant la configuration du délai d'attente pour les sessions inactives.

Cet attribut permet d'attribuer une valeur au délai d'attente automatique pour les sessions utilisateur inactives. Les sessions utilisateur sont suspendues si aucune activité dans la session d'application ou sur le bureau Web n'a été relevée pendant un certain laps de temps.

Vous pouvez spécifier cet attribut à l'aide de la commande suivante :

```
$tarantella config edit \  
--tarantella-config-array-webtopsessionidletimeout secondes
```

Remplacez *secondes* par le délai d'attente, en secondes.

Lorsque ce paramètre est défini sur 0 (valeur par défaut), la fonctionnalité de délai d'attente pour les sessions utilisateur inactives est désactivée.

Options de la commande (`--displayusing`) de type de fenêtre

Le *Manuel de référence de Sun Secure Global Desktop 4.4* (page 214) indique à tort que les options de ligne de commande suivantes sont disponibles lors de la spécification de l'attribut Type de fenêtre (`--displayusing`) :

- webtop
- newbrowser

Ces options ont été abandonnées dans la version 4.40.

Des erreurs se produisent lors de la création ou de la modification d'objets à partir d'un serveur secondaire

Des problèmes peuvent se produire lors de la création ou de la modification d'objets, si la console d'administration est exécutée depuis un serveur SGD secondaire. En effet, la console d'administration n'attend pas assez longtemps pour récupérer les données répliquées du serveur principal et procède au chargement.

Vous pouvez configurer la console de façon à ce qu'elle attende un certain temps après la création ou la modification d'un objet. La durée de cette attente est définie par le paramètre `com.sun.tta.confmgr.ArraySyncPeriod` dans le fichier de configuration `web.xml` de la console d'administration. Le fichier `web.xml` se trouve dans le répertoire `/rep-install/webserver/tomcat/version/webapps/sgdadmin/WEB-INF/` du serveur SGD.

La documentation publiée ne contient pas de détails sur ce paramètre.

Création d'entrées dans le cache des mots de passe

La documentation publiée ne contient pas les informations suivantes sur la création d'entrées dans le cache des mots de passe à l'aide de la console d'administration.

L'onglet Paramètres globaux ⇒ Caches ⇒ Mots de passe permet de gérer les entrées de cache des mots de passe. Vous pouvez aussi ajouter des entrées de cache des mots de passe dans cet onglet via la page Créer une entrée dans le cache des mots de passe. Cette opération revient à utiliser la commande `tarantella passcache new`.

Il est important que vous entriez un nom valide dans les champs Identité de l'utilisateur ou Serveur de la page Créer une entrée dans le cache des mots de passe. Pour entrer un nom dans le champ Identité de l'utilisateur ou Serveur, vous avez le choix entre plusieurs méthodes :

- **Bouton Parcourir** : si le paramètre Type d'identité de l'utilisateur est défini sur Local ou LDAP/Active Directory, cliquez sur le bouton Parcourir à côté du champ Identité de l'utilisateur ou Serveur pour rechercher le nom de l'objet. En utilisant ce bouton, vous évitez les erreurs de frappe lorsque vous entrez des noms d'objet.

- **Nom complet** : saisissez le *nom complet* dans le champ. Par exemple, vous pouvez saisir le nom complet d'un serveur d'application à partir du référentiel local de la façon suivante :

```
.../_ens/o=appservers/cn=boston
```

- **Nom partiel** : saisissez le *nom partiel*, sans le préfixe d'espace de noms, dans le champ. En fonction de l'option Type d'identité de l'utilisateur sélectionnée, la console d'administration ajoute le préfixe d'espace de noms approprié lorsque l'entrée de cache des mots de passe est sauvegardée. Par exemple, vous pouvez saisir le nom partiel d'une identité d'utilisateur à partir du référentiel UNIX de la façon suivante :

```
o=organization/cn=indigo-jones
```

La console d'administration ajoute le préfixe d'espace de noms `.../_user` lorsque le cache des mots de passe est enregistré.

Le tableau suivant récapitule les préfixes d'espace de noms que la console d'administration ajoute en fonction de l'option Type d'identité de l'utilisateur sélectionnée.

Type d'identité de l'utilisateur	Préfixe d'espace de noms
Local	<code>.../_ens</code>
UNIX (Utilisateur/Groupe)	<code>.../_user</code>
Contrôleur de domaine Windows	<code>.../_wns</code>
LDAP/Active Directory	<code>.../service/sco/tta/ldapcache</code>
SecurID	<code>.../service/sco/tta/secuid</code>
Anonyme	Aucune
Tiers	<code>.../service/sco/tta/thirdparty</code>

Si vous spécifiez un nom partiel dans le champ Serveur, la console d'administration ajoute le préfixe d'espace de noms `.../_ens/o=appservers` lorsque le cache des mots de passe est enregistré.

Les noms LDAP doivent être saisis au format d'attribution de nom SGD. Le nom partiel de l'exemple suivant correspondant à une identité d'utilisateur dans le référentiel LDAP :

```
dc=com/dc=example/cn=indigo-jones
```

Ce nom est converti au format LDAP adéquat lorsque l'entrée de cache des mots de passe est enregistrée, comme indiqué ci-dessous :

```
.../_service/sco/tta/ldapcache/cn=indigo-jones,dc=example,dc=com
```

Corrections apportées à la page Sécurisation des connexions SOAP vers un serveur SGD

La page Sécurisation des connexions SOAP vers un serveur SGD du *Guide d'administration de Sun Secure Global Desktop 4.4* contient des erreurs.

Dans l'étape 2, le paragraphe suivant est incorrect :

« Vous devez ajouter le certificat X.509 pour chaque serveur SGD de la baie. Les certificats des serveurs sont stockés dans `/opt/tarantella/var/tsp/cert.pem`. »

Voici le paragraphe corrigé :

« Vous devez ajouter les certificats X.509 pour activer le serveur SGD afin de réaliser une chaîne de certification de confiance. La chaîne de certification de chaque serveur est stockée dans `/opt/tarantella/var/tsp/ca.pem`. »

Le paragraphe décrivant la commande `keytool` est incorrect. Voici le paragraphe corrigé :

```
$ keytool -import -keystore -storepass changeit \  
/rép-install/bin/jdk-version/jre/lib/security/cacerts \  
-file /rép-install/var/tsp/ca.pem -alias hostname
```

changeit correspond au mot de passe du keystore, *jdk-version* à la version de JDK installée sur le serveur SGD et *hostname* au nom d'identification du certificat.

Si vous possédez plusieurs certificats dans le fichier `ca.pem`, séparez chaque certificat et ajoutez-les individuellement.