Guide de sécurité de Sun QFS et Sun Storage Archive Manager 5.3

Référence : E35997
Juin 2012

ORACLE

120817@25097

Table des matières

Préface

Le guide *Guide de sécurité de Sun QFS et Sun Storage Archive Manager* inclut des informations sur le produit Sun QFS et Storage Archive Manager (SAM-QFS) et explique les principes généraux de sécurité de l'application.

Accès au support d'Oracle

Les clients Oracle ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` adapté aux utilisateurs malentendants.

Conventions typographiques

Le tableau suivant répertorie les conventions typographiques utilisées dans ce manuel.

TABLEAU P–1 Conventions typographiques

Type de caractères	Description	Exemple
`AaBbCc123`	Noms de commandes, fichiers et répertoires, ainsi que messages système	Modifiez le fichier `.login`. Utilisez `ls -a` pour afficher la liste des fichiers. `machine_name% Vous avez reçu du courrier.`
`AaBbCc123`	Ce que vous tapez, par opposition à l'affichage sur l'écran de l'ordinateur	`nom_machine%` **`su`** `Mot de passe :`
aabbcc123	Paramètre fictif : à remplacer par un nom ou une valeur réel(le)	La commande permettant de supprimer un fichier est `rm` *filename*.

TABLEAU P–1 Conventions typographiques *(Suite)*

Type de caractères	Description	Exemple
AaBbCc123	Titres de manuels, nouveaux termes et termes importants	Lisez le chapitre 6 du *Guide de l'utilisateur*. Un *cache* est une copie stockée localement. N'enregistrez *pas* le fichier. **Remarque :** en ligne, certains éléments mis en valeur s'affichent en gras.

Invites de shell dans les exemples de commandes

Le tableau suivant présente l'invite système UNIX par défaut et l'invite de superutilisateur pour les shells faisant partie du SE Oracle Solaris. Notez que l'invite système par défaut affichée dans les exemples de commandes varie en fonction de la version d'Oracle Solaris.

TABLEAU P–2 Invites de shell

Shell	Invite
Shell Bash, shell Korn et shell Bourne	`$`
Shell Bash, shell Korn et shell Bourne pour superutilisateur	`#`
Shell C	`nom_machine%`
Shell C pour superutilisateur	`nom_machine#`

◆ ◆ ◆ CHAPITRE 1

1 Présentation de Sun QFS et Sun Storage Archive Manager

Ce chapitre offre une présentation du produit Sun QFS et Storage Archive Manager (SAM-QFS) et explique les principes généraux des applications de sécurité.

Présentation du produit

SAM-QFS est un système de fichiers partagé avec un gestionnaire de stockage hiérarchique. SAM-QFS est constitué des principaux composants suivants :

- **Package Sun QFS :** inclut le système de fichiers Sun QFS haute performance qui peut être configuré de manière autonome ou partagée. Dans le cas d'une configuration autonome, Sun QFS est configuré sur un système unique et sans clients partagés. Sun QFS utilise les opérations vnode VFS standard pour créer une interface avec les systèmes d'exploitation Oracle Solaris et Linux.

  Les packages d'installation Sun QFS sont `SUNWqfsr` et `SUNWqfsu`. Ces packages n'incluent *pas* le composant SAM hiérarchique.

  La configuration d'un package Sun QFS autonome sans clients partagés réduit largement les risques de sécurité. Cette configuration n'exécute aucun démon et n'utilise aucune autre connexion à distance que la connexion Fibre Channel (FC)-disque. La configuration d'un QFS partagé inclut les connexions FC au disque et une connexion TCP/IP entre les clients et le serveur de métadonnées (MDS).
- **Package SAM-QFS :** inclut le système de fichiers Sun QFS et le code requis pour exécuter SAM.

  Les packages d'installation SAM-QFS sont `SUNWsamfsr` et `SUNWsamfsu`. Si le SAM n'est pas requis, installez *uniquement* le package Sun QFS.
- **Sun SAM-Remote :** permet d'accéder aux bibliothèques de bande et aux lecteurs à distance via les connexions réseau WAN TCP/IP. Sun SAM-Remote fournit une forme de reprise sur sinistre en localisant à distance des installations de bandes. Vous pouvez installer Sun SAM-Remote avec les packages Sun QFS ou SAM-QFS, mais vous devez activer et

configurer Sun SAM-Remote séparément. Pour plus d'informations sur Sun SAM-Remote, reportez-vous au Chapitre 18, “Utilisation du logiciel Sun SAM-Remote” du manuel *Guide de configuration et d'administration de Sun Storage Archive Manager 5.3*.

- **Package d'outils SAM-QFS :** installe les outils et pages de manuel dans le répertoire `/opt/SUNWsamfs/tools`. Aucun de ces outils ne dispose de privilèges particuliers, mais l'accès root est requis pour l'utilisation. Le package d'installation est `SUNWsamtp`.
- **SAM-QFS Manager :** SAM-QFS Manager, `fsmgr`, s'exécute sur le MDS et est accessible à distance via un navigateur Web. L'accès est accordé via le port 6789 (`https://`*hostname*`:6789`).

  Pour utiliser `fsmgr`, vous devez vous connecter en tant qu'utilisateur valide sur le MDS et ajouter certains rôles au compte d'utilisateur. Pour plus d'informations sur l'installation et la configuration de SAM-QFS Manager, reportez-vous au Chapitre 6, “Installation et configuration de SAM-QFS Manager” du manuel *Guide d'installation de Sun QFS et Sun Storage Archive Manager 5.3*.

Principes généraux de sécurité

Les sections suivantes décrivent les principes fondamentaux nécessaires pour utiliser toutes les applications en toute sécurité.

Garantir la mise à jour des logiciels

Assurez-vous de toujours exécuter la dernière version de SAM-QFS. Vous pouvez trouver les versions actuelles du logiciel à télécharger sur Oracle Software Delivery Cloud (`https://edelivery.oracle.com/`).

Limiter l'accès réseau aux services critiques

SAM-QFS utilise les ports TCP/IP :

- `tcp/7105` est utilisé pour le trafic de métadonnées entre le client et le MDS
- `tcp/1000` est utilisé pour Sun SAM-Remote
- `tcp/6789` est le port HTTPS utilisé pour qu'un navigateur contacte `fsmgr`
- `tcp/5012` est utilisé pour `sam-rpcd`

Remarque – Pour le trafic client MDS, envisagez de configurer un réseau séparé qui n'est pas interconnecté au WAN externe. Cette configuration empêche l'exposition aux menaces externes et assure également que le trafic externe ne limite pas les performances MDS.

Suivre le principe du moindre privilège

Affectez à l'utilisateur ou à l'administrateur le moindre privilège requis pour accomplir la tâche à effectuer. SAM-QFS Manager possède plusieurs rôles pouvant être affectés aux utilisateurs. Ces rôles attribuent des types et quantités de privilèges variables. L'exécution de tâches d'administration SAM-QFS à partir de la ligne de commande requiert des autorisations root.

Pour plus d'informations sur l'utilisation de SAM-QFS Manager, reportez-vous au Chapitre 6, "Installation et configuration de SAM-QFS Manager" du manuel *Guide d'installation de Sun QFS et Sun Storage Archive Manager 5.3*.

Contrôler l'activité du système

Contrôlez l'activité du système afin de déterminer si SAM-QFS fonctionne correctement et si une activité anormale est détectée. Consultez les fichiers journaux suivants :

- `/var/adm/messages`
- `/var/opt/SUNWsamfs/sam-log`
- `/var/opt/SUNWsamfs/archiver.log`, voir `/etc/opt/SUNWsamfs/archiver.cmd`
- `/var/opt/SUNWsamfs/recycler.log`, voir `/etc/opt/SUNWsamfs/recycler.cmd`
- `/var/opt/SUNWsamfs/releaser.log`, voir `/etc/opt/SUNWsamfs/releaser.cmd`
- `/var/opt/SUNWsamfs/stager.log`, voir `/etc/opt/SUNWsamfs/stager.cmd`
- `/var/opt/SUNWsamfs/trace/*`

Assurer la mise à jour des informations de sécurité

Vous pouvez accéder à plusieurs sources d'informations de sécurité. Pour obtenir des informations de sécurité et des alertes pour toute une gamme de produits logiciels, reportez-vous à la page `http://www.us-cert.gov`. Pour des informations spécifiques à SAM-QFS, reportez-vous à la page `http://mail.opensolaris.org/mailman/listinfo/sam-qfs-discuss`. La meilleure manière de rester à jour en termes de sécurité est d'exécuter la version la plus récente du logiciel SAM-QFS.

◆ ◆ ◆ CHAPITRE 2

Installation et configuration sécurisées

Ce chapitre décrit le processus de planification pour une installation sécurisée et décrit plusieurs des topologies de déploiement recommandées pour les systèmes.

Présentation de l'installation

Comprendre votre environnement

Pour mieux comprendre vos besoins en matière de sécurité, posez-vous les questions suivantes :

- **Quelles sont les ressources que je protège ?**

  Vous pouvez protéger un grand nombre de ressources dans l'environnement de production. Tenez compte du type de ressources que vous souhaitez protéger lors de la détermination du niveau de sécurité à fournir.

  Lors de l'utilisation de SAM-QFS, protégez les ressources suivantes :

  - **Métadonnées et disque de données principal :** ces ressources de disque sont utilisées pour créer les systèmes de fichiers SAM-QFS. Elles sont généralement connectées par Fibre Channel (FC). L'accès indépendant à ces disques (par un autre moyen que SAM-QFS) présente un risque de sécurité car les autorisations normales d'accès aux fichiers et répertoires SAM-QFS sont ignorées. Ce type d'accès externe peut provenir d'un système non fiable qui lit ou écrit sur les disques FC, ou d'un système interne qui fournit par accident un accès non-root à des fichiers de périphérique brut.
  - **Bandes SAM :** accès indépendant aux bandes, généralement dans une bibliothèque de bandes, où les données de fichier sont écrites lorsque le déplacement d'un fichier SAM constitue un risque de sécurité.

- **Fichiers de vidage SAM-QFS :** les vidages de système de fichiers créés à partir de `samfsdump` contiennent des données et métadonnées. Ces données et métadonnées doivent être protégées contre l'accès autre que par l'administrateur système au cours d'un vidage de routine ou d'une activité de restauration.
- **Serveur de métadonnées (MDS) SAM-QFS :** les clients SAM-QFS requièrent un accès TCP/IP au MDS. Cependant, assurez-vous que les clients sont protégés d'un accès WAN externe.
- **Fichiers et paramètres de configuration :** les paramètres de configuration de SAM-QFS *doivent* être protégés de l'accès par des non-administrateurs. En général, ces paramètres sont protégés automatiquement par SAM-QFS lorsque vous utilisez SAM-QFS Manager. Notez que rendre les fichiers de configuration accessibles en écriture à des utilisateurs non administratifs présente un risque de sécurité.

- **Contre qui les ressources doivent-elles être protégées ?**

  En général, les ressources décrites dans la section précédente *doivent* être protégées contre l'accès par des utilisateurs non-root ou non-administrateur sur un système configuré, ou contre un système externe non fiable qui peut accéder à ces ressources via le WAN ou le Fabric FC.

- **Que se passera-t-il si la protection des ressources stratégiques échoue ?**

  Les échecs de la protection contre les ressources stratégiques peuvent aller d'un accès inapproprié (accès à des données en dehors de l'autorisation d'accès aux fichiers POSIX SAM-QFS) à la corruption des données (écriture sur le disque ou la bande en dehors des autorisations normales).

Topologies de déploiement recommandées

Installation de SAM-QFS

Cette section décrit l'installation et la configuration sécurisées d'un composant d'infrastructure.

Pour plus d'informations sur l'installation de SAM-QFS, reportez-vous au Chapitre 5, “Installation de Sun QFS et SAM-QFS” du manuel *Guide d'installation de Sun QFS et Sun Storage Archive Manager 5.3*.

Tenez compte des points suivants lors de l'installation et de la configuration de SAM-QFS :

- **Réseau de métadonnées distinct :** pour connecter les clients SAM-QFS aux serveurs MDS, fournissez un réseau TCP/IP séparé et un matériel du commutateur qui n'est connecté à aucun WAN. Le trafic des métadonnées étant mis en œuvre à l'aide de TCP/IP, une attaque externe sur ce trafic est théoriquement possible. La configuration d'un réseau de métadonnées séparé limite ce risque et permet également une performance améliorée. Les performances améliorées sont obtenues en fournissant un chemin d'accès garanti aux métadonnées. S'il est impossible de réaliser un réseau de métadonnées distinct, réduisez au moins le trafic sur les ports SAM-QFS à partir du WAN externe et de tous les hôtes non autorisés sur le réseau. Reportez-vous à la section "Limiter l'accès réseau aux services critiques" à la page 8.
- **Zonage FC :** utilisez le zonage FC pour refuser l'accès aux disques SAM-QFS à partir d'un serveur qui ne requiert pas d'accès aux disques. Utilisez de préférence un commutateur FC séparé pour *uniquement* connecter physiquement aux serveurs qui requièrent l'accès.
- **Protégez l'accès à la configuration des disques SAN :** les disques SAN RAID sont généralement accessibles à des fins d'administration via le protocole TCP/IP ou plus généralement le protocole HTTP. Vous devez protéger les disques d'un accès externe en limitant l'accès administratif aux disques SAN RAID pour les systèmes uniquement au sein d'un domaine de confiance. D'autre part, modifiez le mot de passe par défaut sur des baies de stockage.
- **Installation du package SAM-QFS :** tout d'abord, installez uniquement les packages dont vous avez besoin. Par exemple, si vous n'envisagez pas d'exécuter SAM, installez *uniquement* les packages QFS.

  Les autorisations d'accès aux fichiers et répertoires SAM-QFS par défaut et les propriétaires ne doivent *pas* être modifiés sans envisager les implications en termes de sécurité de telles modifications.
- **Accès au client :** si vous envisagez de configurer des clients partagés, déterminez les clients qui doivent avoir accès au système de fichiers dans le fichier `host`. Reportez-vous à la page de manuel `hosts.fs(4)`. Configurez *uniquement* les hôtes qui requièrent l'accès au système de fichiers particulier en cours de configuration.
- **Renforcement du serveur de métadonnées Oracle Solaris :** pour plus d'informations sur le renforcement du SE Oracle Solaris, reportez-vous aux *Directives de sécurité d'Oracle Solaris 10* et aux *Directives de sécurité d'Oracle Solaris 11*. Choisissez au minimum un bon mot de passe root, installez une version à jour du SE Oracle Solaris, et restez à jour au niveau des patchs, particulièrement les patchs de sécurité.
- **Renforcement des clients Linux :** consultez la documentation Linux pour savoir comment sécuriser les clients Linux. Choisissez au minimum un bon mot de passe root, installez une version à jour du système d'exploitation Linux, et restez à jour au niveau des patchs, particulièrement les patchs de sécurité.

- **Sécurité de bande SAM-QFS :** empêchez l'accès externe aux bandes SAM depuis l'extérieur du SAM, ou limitez l'accès aux administrateurs uniquement. Utilisez le zonage FC pour limiter l'accès aux lecteurs de bandes uniquement aux MDS (ou aux MDS potentiels si un MDS de sauvegarde est configuré). En outre, limitez l'accès au fichier de périphérique de bande en attribuant des autorisations root uniquement. L'accès non autorisé aux bandes SAM peut compromettre ou détruire les données d'utilisateur.
- **Sauvegarde :** définissez et exécutez des sauvegardes des données SAM-QFS à l'aide de la commande `samfsdump` ou `qfsdump`. Limitez l'accès aux fichiers de vidage comme cela est recommandé pour les bandes SAM.

Installation de Sun SAM-Remote

Pour plus d'informations sur l'installation sécurisée du logiciel Sun SAM-Remote, reportez-vous au Chapitre 18, “Utilisation du logiciel Sun SAM-Remote” du manuel *Guide de configuration et d'administration de Sun Storage Archive Manager 5.3*.

Installation de SAM-QFS Manager

Pour plus d'informations sur l'installation sécurisée de SAM-QFS Manager, reportez-vous au Chapitre 6, “Installation et configuration de SAM-QFS Manager” du manuel *Guide d'installation de Sun QFS et Sun Storage Archive Manager 5.3*.

Configuration post-installation

Après avoir installé l'un des packages SAM-QFS, commencez par lire la liste de contrôle dans l'Annexe A, “Liste de contrôle pour un déploiement sécurisé”.

◆ ◆ ◆ CHAPITRE 3

Fonctions de sécurité de Sun QFS et Sun Storage Archive Manager

Pour éviter les menaces de sécurité potentielles, les clients utilisant un système de fichiers partagé doivent faire attention aux éléments suivants :

- Divulgation des données du système de fichiers non conforme à la stratégie
- Perte de données
- Modification non détectée de données

Ces menaces de sécurité peuvent être réduites grâce à une configuration adéquate et en suivant la liste de contrôle post-installation de l'Annexe A, “Liste de contrôle pour un déploiement sécurisé”.

Modèle de sécurité

Les fonctionnalités de sécurité critiques suivantes protègent contre les menaces de sécurité :

- **Authentification :** garantit que seules les personnes autorisées peuvent accéder au système et aux données.
- **Autorisations :** contrôlent l'accès aux privilèges système et aux données. Cette fonctionnalité repose sur l'authentification afin de garantir que les personnes disposent uniquement de l'accès dont elles ont besoin.
- **Audit :** permet aux administrateurs de détecter les violations tentées du mécanisme d'authentification, ainsi que les violations tentées ou réelles du contrôle d'accès.

Authentification

SAM-QFS utilise l'authentification des utilisateurs basée sur les hôtes afin de contrôler les personnes pouvant effectuer les tâches d'administration. L'administration à l'aide de SAM-QFS Manager est principalement contrôlée par des rôles affectés à plusieurs utilisateurs. L'administration à l'aide des lignes de commande est limitée à l'utilisateur root.

Contrôle d'accès

Le contrôle d'accès dans SAM-QFS est divisé en deux parties :

- **Contrôle d'accès administratif** : contrôle les personnes autorisées à effectuer des actions d'administration pour SAM-QFS. Les contrôles sont basés sur les rôles affectés aux utilisateurs via SAM-QFS Manager. Pour les opérations de ligne de commande, les contrôles sont basés sur les autorisations root. Pour plus d'informations sur SAM-QFS Manager, reportez-vous au Chapitre 6, “Installation et configuration de SAM-QFS Manager” du manuel *Guide d'installation de Sun QFS et Sun Storage Archive Manager 5.3*.
- **Contrôle d'accès aux fichiers/répertoires** : SAM-QFS implémente un système de fichiers compatible POSIX disposant d'un riche ensemble de contrôles d'accès. Pour en savoir plus, reportez-vous à la documentation de SAM-QFS.

Considérations relatives à la sécurité pour les développeurs

Les développeurs n'utilisent généralement pas directement SAM-QFS. Les deux seules exceptions sont l'API `libsam` et l'API `libsamrpc`. Ces deux API offrent les mêmes fonctionnalités. `libsam` s'applique à une machine locale uniquement, tandis que `libsamrpc` communique avec le MDS via `rpc(3)` pour implémenter les actions requises. L'authentification des requêtes effectuées via l'une de ces deux méthodes est basée sur l'UID et le GID du processus appelant. Elles possèdent les mêmes autorisations que les requêtes effectuées via la ligne de commande. Assurez-vous de disposer d'un espace UID et GID commun pour le MDS et les systèmes client.

Pour plus d'informations, reportez-vous aux pages de manuel `intro_libsam(3)` et `intro_libsamrpc`(3) dans *Sun QFS and Sun Storage Archive Manager 5.3 Reference Manual*.

◆ ◆ ◆ ANNEXE A

Liste de contrôle pour un déploiement sécurisé

Utilisez la liste de contrôle dans cette annexe comme aide-mémoire pour déployer le logiciel SAM-QFS en toute sécurité.

Liste de contrôle de déploiement

Cette liste de contrôle de sécurité inclut des instructions pour la sécurisation de votre base de données.

- Définissez des mots de passe forts pour le compte root et les autres comptes auxquels un rôle SAM-QFS est affecté. Ces instructions incluent :
  - Tous les comptes auxquels SAM-QFS Manager a affecté un rôle d'administration.
  - ID utilisateur `acsss`, `acsdb` et `acssa` (le cas échéant).
  - Tout compte d'administration de baie de stockage.
- Si vous utilisez l'utilisateur `samadmin` par défaut avec SAM-QFS Manager, remplacez immédiatement le mot de passe installé par défaut par un mot de passe fort. N'utilisez pas le compte root avec SAM-QFS Manager, mais affectez les rôles selon les besoins à d'autres comptes utilisateur. Protégez également ces comptes par des mots de passe forts.
- Installez le filtrage de port sur les routeurs de périphérie WAN pour éviter que le trafic sur les ports répertoriés dans les "Principes généraux de sécurité" à la page 8 n'atteigne le MDS ou les clients, sauf comme requis pour Sun SAM-Remote.
- Séparez les disques FC et les bandes physiquement ou via le zonage FC de sorte que les disques soient accessibles uniquement à partir du MDS et des clients, et les bandes uniquement à partir du MDS et du MDS potentiel. Cette pratique de sécurité aide à éviter les pertes de données accidentelles résultant du remplacement involontaire du contenu d'une bande ou d'un disque.
- Sélectionnez `/dev` pour vous assurer que les fichiers de périphérique sur disque ou bande ne sont pas accessibles aux utilisateurs autres que root. Cette pratique permet d'éviter l'accès inapproprié aux données SAM-QFS ou leur destruction.

- SAM-QFS est un système de fichiers POSIX fournissant un vaste ensemble d'autorisations d'accès aux fichiers/répertoires, dont des listes de contrôle d'accès (ACL). Utilisez-les selon les besoins pour protéger les données d'utilisateur sur le système de fichiers. Pour plus d'informations, reportez-vous à la documentation de SAM-QFS.
- Configurez un ensemble approprié de vidages de sauvegarde en fonction d'une stratégie locale. Les sauvegardes font partie de la sécurité et fournissent un moyen de restaurer des données perdues accidentellement ou en raison d'une faille. Votre sauvegarde doit inclure des stratégies lors du transport vers un emplacement hors site. Les sauvegardes doivent être protégées au même niveau que les bandes et disques SAM-QFS.

Références

- *Guide d'installation de Sun QFS et Sun Storage Archive Manager 5.3*
- *Guide de configuration et d'administration du système de fichiers Sun QFS 5.3*
- *Guide de configuration et d'administration de Sun Storage Archive Manager 5.3*
- *Sun QFS and Sun Storage Archive Manager 5.3 Reference Manual*