

Oracle® Hierarchical Storage Manager et StorageTek QFS Software

Guide de sécurité

Version 6.0

E62075-01

Mars 2015

Oracle® Hierarchical Storage Manager et StorageTek QFS Software

Guide de sécurité

E62075-01

Copyright © 2015, Oracle et/ou ses affiliés. Tous droits réservés.

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

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

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

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

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

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

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

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

Table des matières

Préface	5
Public	5
Accessibilité de la documentation	5
Conventions typographiques	5
Invites de shell dans les exemples de commandes	6
1. Présentation	7
1.1. Présentation du produit	7
1.2. Principes de sécurité généraux	8
1.2.1. Garantir la mise à jour des logiciels	8
1.2.2. Limiter l'accès réseau à des services critiques	8
1.2.3. Suivre le principe du moindre privilège	8
1.2.4. Contrôle de l'activité du système	9
1.2.5. Assurer la mise à jour des informations de sécurité	9
2. Installation sécurisée	11
2.1. Compréhension de votre environnement	11
2.1.1. Quelles sont les ressources à protéger ?	11
2.1.2. De quels utilisateurs les ressources doivent-elles être protégées ?	12
2.1.3. Que se passera-t-il si la protection des ressources stratégiques échoue ?	12
2.2. Topologies de déploiement recommandées	12
2.2.1. Installation de SAM-Remote	13
2.2.2. Installation de l'interface utilisateur graphique (GUI) du Gestionnaire d'utilisateurs	14
2.2.3. Configuration post-installation	14
3. Fonctions de sécurité	15
3.1. Modèle de sécurité	15
3.1.1. Authentification	15
3.1.2. Contrôle d'accès	15
4. Considérations relatives à la sécurité pour les développeurs	17

A. Liste de contrôle du déploiement sécurisé 19

Préface

Le guide de sécurité de Oracle Hierarchical Storage Manager et StorageTek QFS Software inclut des informations sur les produits Oracle Hierarchical Storage Manager et QFS, et explique les principes généraux de sécurité de l'application.

Public

Ce guide s'adresse à toute personne pouvant être amenée à utiliser les fonctions de sécurité et à effectuer des opérations sécurisées d'installation et de configuration de Oracle Hierarchical Storage Manager et StorageTek QFS Software.

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Accès au support d'Oracle

Les clients Oracle ayant souscrit au support 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 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si vous êtes malentendant.

Conventions typographiques

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

Police de caractères	Signification	Exemple
<i>AaBbCc123</i>	Noms des commandes et affichage à l'écran	<i>Utilisez <code>ls -a</code> pour afficher la liste de tous les fichiers.</i>
AaBbCc123	Saisie utilisateur avec affichage sur l'écran de l'ordinateur	<i><code>nom_machine% su</code></i> <i>Mot de passe :</i>
<i>aabbcc123</i>	Paramètre fictif, à remplacer par un nom ou une valeur réel(le).	La commande permettant de supprimer un fichier est <i><code>rm nom_fichier</code></i> .
<i>AaBbCc123</i>	Titres de manuels, nouveaux termes et termes importants	Lisez le chapitre 6 du <i>Guide de l'utilisateur</i> . Un <i>cache</i> est une copie stockée localement. N'enregistrez pas le fichier. Remarque : en ligne, certains termes 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.

Shell	Invite
Bashshell, Kornshell et BourneShell	\$
Bashshell, Kornshell et BourneShell pour superutilisateur	#
Cshell	nom_machine%
Cshell pour superutilisateur	nom_machine#

Présentation

Ce chapitre offre une présentation de Oracle Hierarchical Storage Manager et StorageTek QFS Software et explique les principes généraux des applications de sécurité.

1.1. Présentation du produit

Oracle Hierarchical Storage Manager et StorageTek QFS Software est un système de fichiers partagé avec un gestionnaire de stockage hiérarchique. Le produit se compose des composants principaux suivants :

Package StorageTek QFS

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

Les packages d'installation QFS sont SUNWqfsr et SUNWqfsu. Ces packages ne comportent pas le composant Oracle Hierarchical Storage Manager (HSM).

La configuration autonome de QFS sans client partagé présente l'exposition la moindre en termes de sécurité. Cette configuration n'exécute aucun démon, et ne dispose d'aucune connexion distante autre que la connexion Fibre Channel (FC) aux disques. 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 Oracle HSM

Comporte le système de fichiers QFS et le code requis pour l'exécution de Oracle HSM. Les packages d'installation Oracle HSM sont les packages SUNWsamfsr et SUNWsamfsu. Si vous n'avez pas besoin de gestion hiérarchique du stockage, installez *uniquement* le package StorageTek QFS.

SAM-Remote

Permet d'accéder aux bibliothèques de bande et aux lecteurs à distance via les connexions réseau WAN TCP/IP. StorageTek SAM-Remote fournit une forme de récupération après sinistre en localisant à distance des installations de bandes. Vous pouvez installer SAM-Remote avec les packages QFS ou SAM-QFS, mais vous devez activer et configurer SAM-Remote séparément. Pour plus d'informations sur SAM-Remote, reportez-vous à la *Bibliothèque de documentation client de Oracle Hierarchical Storage Manager et StorageTek QFS Software version 6.0* à l'adresse suivante : <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

Interface utilisateur graphique du Gestionnaire d'utilisateurs

L'interface utilisateur graphique (GUI) du Gestionnaire d'utilisateurs, fsmgr, s'exécute sur le serveur MDS, et son accès se fait 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 utilisateur. Pour plus d'informations sur l'installation et la configuration de l'interface utilisateur graphique du Gestionnaire d'utilisateurs, reportez-vous à la *Bibliothèque de documentation client de Oracle Hierarchical Storage Manager et StorageTek QFS Software version 6.0* à l'adresse suivante : <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

1.2. Principes de sécurité généraux

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

1.2.1. Garantir la mise à jour des logiciels

Restez au fait de la version de Oracle HSM que vous exécutez. Vous pouvez trouver les versions actuelles du logiciel à télécharger sur Oracle Software Delivery Cloud (<https://edelivery.oracle.com/>).

1.2.2. Limiter l'accès réseau à des services critiques

Oracle HSM utilise les ports TCP/IP suivants :

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

Remarque:

Pour le trafic client MDS bidirectionnel, 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.

1.2.3. Suivre le principe du moindre privilège

Affectez à l'utilisateur ou l'administrateur le moindre privilège requis pour accomplir la tâche à effectuer. L'interface utilisateur graphique (GUI) du Gestionnaire de profils possède plusieurs rôles pouvant être attribués aux utilisateurs. Ces rôles attribuent des types et quantités de privilèges variables. L'exécution de tâches d'administration à partir de la ligne de commande requiert une autorisation root.

Pour plus d'informations sur l'utilisation de l'interface utilisateur graphique (GUI) du Gestionnaire d'utilisateurs, reportez-vous à la *Bibliothèque de documentation client de Oracle Hierarchical Storage Manager et StorageTek QFS Software version 6.0* à l'adresse suivante : <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

1.2.4. Contrôle de l'activité du système

Contrôlez l'activité du système afin de déterminer si Oracle HSM 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/*

1.2.5. 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 https://communities.oracle.com/portal/server.pt/community/sam_qfs_storage_archive_manager_and_sun_qfs/401. La meilleure manière de rester à jour en termes de sécurité est d'exécuter la version la plus récente du logiciel Oracle HSM.

Installation sécurisée

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

2.1. Compréhension de votre environnement

Les réponses aux questions suivantes peuvent vous aider à comprendre les exigences de sécurité :

2.1.1. Quelles sont les ressources à protéger ?

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 Oracle HSM, protégez les ressources suivantes :

Métadonnées et disque de données principal

Ces ressources disque permettent de créer des systèmes de fichiers Oracle HSM. Elles sont généralement connectées par Fibre Channel (FC). L'accès indépendant à ces disques (par un autre moyen que Oracle HSM) présente un risque de sécurité car les autorisations normales d'accès aux répertoires et fichiers Oracle HSM 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 Oracle HSM

Accès indépendant aux bandes, généralement dans une bibliothèque de bandes, où les données de fichier sont écrites lorsque le déplacement d'un système de fichiers Oracle HSM constitue un risque de sécurité.

Bandes de vidage Oracle HSM

Les vidages de système de fichiers créés à partir de samfsdump contiennent des données et des 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.

Seueur de métadonnées (MDS) Oracle HSM

Les clients Oracle HSM 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 Oracle HSM doivent être protégés contre l'accès par des non-administrateurs. En général, ces paramètres sont protégés automatiquement par Oracle HSM lorsque vous utilisez l'interface utilisateur graphique (GUI) du Gestionnaire d'utilisateurs. Notez que rendre les fichiers de configuration accessibles en écriture à des utilisateurs non administratifs présente un risque de sécurité.

2.1.2. De quels utilisateurs 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.

2.1.3. 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 Oracle HSM) à l'altération des données (écriture sur le disque ou la bande en dehors des autorisations normales).

2.2. Topologies de déploiement recommandées

Cette section décrit l'installation et la configuration sécurisées d'un composant d'infrastructure. Pour plus d'informations sur l'installation de Oracle HSM, reportez-vous à la *Bibliothèque de documentation client de Oracle Hierarchical Storage Manager Software version 6.0* à l'adresse suivante : <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

Tenez compte des points suivants lors de l'installation et de la configuration de Oracle HSM :

Réseau de métadonnées séparé

Pour connecter les clients Oracle HSM aux serveurs MDS, fournissez un réseau TCP/IP séparé et un matériel de commutateur qui n'est connecté à aucun WAN. Le trafic des métadonnées étant mis en oeuvre 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, interdisez au moins le trafic sur les ports Oracle HSM à partir du WAN externe et de tous les hôtes non autorisés sur le réseau. Voir la [Section 1.2.2, « Limiter l'accès réseau à des services critiques » \[8\]](#).

Zonage FC

Utilisez le zonage FC pour refuser l'accès aux disques Oracle HSM à partir d'un serveur qui ne requiert pas d'accès aux disques. Utilisez de préférence un commutateur FC séparé pour uniquement établir une connexion physique aux serveurs qui requièrent l'accès.

Protection de 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 disques.

Installation du package Oracle HSM

Tout d'abord, installez uniquement les packages dont vous avez besoin. Si vous n'utilisez pas la gestion de stockage hiérarchique, par exemple, installez uniquement les packages QFS. Les autorisations d'accès aux fichiers et répertoires Oracle HSM par défaut et les propriétaires ne doivent pas être modifiés après l'installation sans envisager les implications en termes de sécurité de telles modifications.

Accès client

Si vous envisagez de configurer des clients partagés, déterminez les clients qui doivent avoir accès au système de fichiers dans le fichier des hôtes. 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 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 patches, particulièrement les patches 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 patches, particulièrement les patches de sécurité.

Sécurité des bandes Oracle HSM

Empêchez l'accès externe aux bandes Oracle HSM depuis l'extérieur de Oracle HSM, ou limitez l'accès aux administrateurs uniquement. Utilisez le zonage FC pour limiter l'accès aux lecteurs de bande uniquement aux MDS (ou aux MDS potentiels si un MDS de sauvegarde est configuré). L'accès aux lecteurs de bande sera requis pour les clients Solaris configurés pour utiliser les E/S distribuées. En outre, limitez l'accès au fichier de périphérique de bande en attribuant des autorisations root uniquement. L'accès non autorisé aux bandes Oracle HSM peut compromettre ou détruire les données d'utilisateur.

Sauvegardes

Définissez et exécutez des sauvegardes des données Oracle HSM à l'aide de la commande `samfsdump` ou `qfsdump`. Limitez l'accès aux bandes de vidage comme cela est recommandé pour les bandes Oracle HSM.

2.2.1. Installation de SAM-Remote

Pour plus d'informations sur l'installation sécurisée du logiciel SAM-Remote, reportez-vous à la *Bibliothèque de documentation client de Oracle Hierarchical Storage Manager*

et StorageTek QFS Software version 6.0 à l'adresse suivante : <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

2.2.2. Installation de l'interface utilisateur graphique (GUI) du Gestionnaire d'utilisateurs

Pour plus d'informations sur l'installation sécurisée de l'interface utilisateur graphique (GUI) du Gestionnaire d'utilisateurs, reportez-vous à la *Bibliothèque de documentation client de Oracle Hierarchical Storage Manager and StorageTek QFS Software version 6.0* à l'adresse suivante : <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

2.2.3. Configuration post-installation

Une fois que vous avez installé l'un des packages Oracle HSM, commencez par lire la liste de contrôle de sécurité dans l'[Annexe A, Liste de contrôle du déploiement sécurisé \[19\]](#).

Fonctions de sécurité

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

- Divulcation des données du système de fichiers non conforme à la politique
- 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 du déploiement sécurisé](#) [19].

3.1. 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.

3.1.1. Authentification

Oracle HSM utilise l'authentification des utilisateurs basée sur les hôtes afin de contrôler les personnes pouvant effectuer les tâches administratives. L'administration à l'aide de l'interface utilisateur graphique (GUI) du Gestionnaire d'utilisateurs 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.

3.1.2. Contrôle d'accès

Le contrôle d'accès de Oracle HSM se divise en deux parties :

- Contrôle d'accès administratif : contrôle les personnes autorisées à effectuer des actions d'administration pour Oracle HSM. Les contrôles sont basés sur les rôles affectés aux

utilisateurs via l'interface utilisateur graphique (GUI) du Gestionnaire d'utilisateurs. Pour les opérations de ligne de commande, les contrôles sont basés sur les autorisations root. Pour plus d'informations sur l'interface utilisateur graphique (GUI) du Gestionnaire d'utilisateurs, reportez-vous à la *Bibliothèque de documentation client de Oracle Hierarchical Storage Manager et StorageTek QFS Software version 6.0* à l'adresse suivante : <http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs>

- Contrôle d'accès aux fichiers/répertoires : Oracle HSM implémente un système de fichiers compatible POSIX disposant d'un riche ensemble de contrôles d'accès. Pour plus de détails, reportez-vous à la documentation d'aide d'Oracle HSM.

Considérations relatives à la sécurité pour les développeurs

Les développeurs n'utilisent généralement pas directement Oracle HSM. 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)*.

Liste de contrôle du déploiement sécurisé

Cette liste de contrôle de sécurité inclut des directives pouvant aider à sécuriser votre base de données.

1. Définissez des mots de passe forts pour le compte root et les autres comptes auxquels un rôle Oracle HSM est affecté. Ces directives incluent :
 - Tous les comptes auxquels l'interface utilisateur graphique (GUI) du Gestionnaire d'utilisateurs a affecté un rôle d'administration.
 - Les ID utilisateur *acsss*, *acsdb* et *acssa* (le cas échéant).
 - Tout compte d'administration de baie de disques.
2. Si vous utilisez l'utilisateur *samadmin* par défaut avec l'interface utilisateur graphique (GUI) du Gestionnaire d'utilisateurs, remplacez immédiatement le mot de passe installé par défaut par un mot de passe fort. N'utilisez pas le compte root avec l'interface utilisateur graphique (GUI) du Gestionnaire d'utilisateurs, mais affectez les rôles selon les besoins à d'autres comptes utilisateur. Protégez également d'autres comptes avec des mots de passe forts.
3. Installez le filtrage de port sur les routeurs de périphérie WAN pour éviter que le trafic sur les ports répertoriés dans la [Section 1.2, « Principes de sécurité généraux » \[8\]](#) n'atteigne le MDS ou les clients, sauf comme requis pour SAM-Remote.
4. 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 de l'écrasement d'une bande ou d'un disque.
5. Sélectionnez */dev* pour vous assurer que les fichiers de périphérie sur disque ou bande ne sont pas accessibles aux utilisateurs autres que root. Cette pratique permet d'éviter l'accès inapproprié aux données Oracle HSM ou leur destruction.
6. Oracle HSM est un système de fichiers POSIX, qui fournit un riche 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 d'Oracle HSM.
7. Configurez un ensemble approprié de vidages de sauvegarde en fonction d'une politique 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 politiques lors du transport vers un emplacement hors site. Les sauvegardes doivent être protégées au même niveau que les bandes et disques Oracle HSM.

