

StorageTek Virtual Storage Manager GUI

Guide de sécurité

E79968-01

Juillet 2016

StorageTek Virtual Storage Manager GUI

Guide de sécurité

E79968-01

Copyright © 2016, 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
1. Présentation	7
Présentation du produit	7
Sécurité	7
Principes généraux de sécurité	7
Mise à jour du logiciel	7
Restriction de l'accès au réseau	8
Consultation des dernières informations de sécurité	8
2. Installation sécurisée	9
Analyse de votre environnement	9
Quelles sont les ressources à protéger ?	9
De quels utilisateurs les ressources doivent-elles être protégées ?	9
Que peut-il se passer en cas de défaillance de la protection des ressources stratégiques ?	9
Installation de StorageTek VSM GUI	9
Configuration post-intallation	10
Attribution du mot de passe utilisateur (admin)	10
Application de la gestion des mots de passe	10
3. Fonctions de sécurité	11
A. Liste de contrôle du déploiement sécurisé	13
B. Références	15

Préface

Ce document décrit les fonctions de sécurité du logiciel StorageTek Virtual Storage Manager GUI d'Oracle.

Public

Ce guide s'adresse à toute personne pouvant être amenée à utiliser les fonctions de sécurité et à effectuer des opérations d'installation et de configuration de VSM GUI.

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 aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de 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 le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si vous êtes malentendant.

Chapitre 1. Présentation

Cette section contient une présentation de StorageTek Virtual Storage Manager (VSM) GUI et explique les principes généraux de sécurité à mettre en oeuvre.

Présentation du produit

StorageTek VSM GUI est un logiciel Oracle qui fournit aux clients des fonctions de contrôle et de production de rapports pour surveiller et gérer de façon efficace et proactive les opérations sur bandes virtuelles de leurs centres de données.

VSM GUI prend en charge Enterprise MVS Virtual Storage Manager. Il admet également toutes les générations prises en charge de produits VSM.

Sécurité

Accès physique

VSM GUI doit être installé sur une machine virtuelle définie sur un serveur Oracle VM ou VMware du client dans le centre de données de l'organisation. L'accès physique au serveur est régi par la politique de l'entreprise du client.

Réseau

VSM GUI doit être ajouté ou configuré au sein d'un réseau interne du client protégé par un pare-feu. Ce réseau doit pouvoir accéder par TCP/IP à toutes les instances de serveur SMC HTTP utilisant les ressources de bande virtuelles.

Accès des utilisateurs

L'accès à l'application VSM est contrôlé grâce à l'authentification du nom de l'utilisateur et de son mot de passe. Cette authentification nécessite la configuration du service LDAP de l'utilisateur dans l'application.

Principes généraux de sécurité

Les principes suivants sont essentiels pour une utilisation sécurisée des produits.

Mise à jour du logiciel

L'un des principes fondamentaux d'une utilisation sécurisée est l'installation régulière des dernières versions et patches du logiciel. Dans ce document, il est supposé que vous utilisez la version logicielle suivante :

VSM GUI version 1.1; juillet 2016

Remarque :

VSM GUI prend en charge ELS7.1, ELS 7.2 et ELS 7.3. Il nécessite l'installation des dernières mises à jour de maintenance.

Restriction de l'accès au réseau

Placez le serveur hôte VSM GUI derrière un pare-feu du centre de données. Le pare-feu vous permet d'être certain que l'accès au système est limité à une route réseau définie, qui peut être surveillée et restreinte le cas échéant. Un routeur peut éventuellement remplacer plusieurs pare-feux indépendants.

Consultation des dernières informations de sécurité

Oracle s'efforce d'améliorer continuellement les logiciels et la documentation. Consultez ce document à chaque nouvelle version logicielle. Les problèmes de sécurité spécifiques peuvent aussi être traités dans les notes de version.

Chapitre 2. Installation sécurisée

Cette section vous indique le processus de planification pour une installation sécurisée. Il décrit également plusieurs topologies de déploiement recommandées pour ces systèmes. Le guide de l'utilisateur de VSM GUI 1.0 décrit en détail l'installation, la configuration et l'administration du produit.

Analyse de votre environnement

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

Quelles sont les ressources à protéger ?

Pour VSM GUI, il est nécessaire de protéger le serveur hôte et le réseau associé contre les accès non autorisés.

De quels utilisateurs les ressources doivent-elles être protégées ?

Il faut protéger VSM GUI contre l'accès de personnes connectées par Internet, d'utilisateurs externes et d'utilisateurs internes non autorisés.

Que peut-il se passer en cas de défaillance de la protection des ressources stratégiques ?

VSM GUI est une application de surveillance et de gestion de ressources de stockage virtuelles. Les accès non autorisés peuvent avoir une incidence sur la disponibilité des ressources VSM. Il se peut que l'état d'une ressource soit modifié, mais les données qu'elle contient ne sont pas affectées.

Installation de StorageTek VSM GUI

VSM GUI ne peut être installé que sur des systèmes se trouvant dans la même infrastructure réseau protégée (au moyen d'un pare-feu) que les ressources virtuelles surveillées (VTCS et HSC). Il faut mettre en place des contrôles d'accès client sur les systèmes où VSM GUI est installé pour garantir un accès restreint à l'application.

Reportez-vous au *Guide de l'utilisateur de VSM GUI* pour les instructions relatives à l'installation.

Configuration post-intallation

Il n'y a aucune modification de sécurité à apporter après l'installation. La configuration est effectuée par le client au moment de l'installation.

Attribution du mot de passe utilisateur (admin)

Le mot de passe du compte d'administration est défini par le client au cours de l'installation.

Application de la gestion des mots de passe

Les règles de gestion des mots de passe définies dans l'entreprise du client (comme la longueur, l'historique et la complexité) doivent être appliquées au mot de passe administrateur.

Chapitre 3. Fonctions de sécurité

Cette section décrit les mécanismes de sécurité spécifiques qu'offre le produit. L'application VSM GUI attribue aux utilisateurs des rôles avec mots de passe chiffrés pour une meilleure protection. Mais la sécurité ne se limite pas à cela. L'application doit se trouver dans un centre de données physiquement sécurisé, également doté d'un réseau sécurisé accessible uniquement aux utilisateurs autorisés.

Annexe A. Liste de contrôle du déploiement sécurisé

La liste de contrôle de sécurité suivante inclut les directives permettant de sécuriser la bibliothèque :

1. Activez la gestion des mots de passe.
2. Mettez en oeuvre des contrôles d'accès.
3. Limitez l'accès au réseau.
 - a. Il convient d'implémenter un pare-feu.
 - b. Ce pare-feu ne doit pas être compromis.
 - c. L'accès au système doit faire l'objet d'une surveillance.
 - d. Les adresses IP du réseau doivent être vérifiées.
4. Contactez le service Oracle Security Products si vous détectez des failles de sécurité dans VSM GUI.

Annexe B

Annexe B. Références

Guide de l'utilisateur de VSM GUI

