Système StorageTek Virtual Storage Manager

Guide de sécurité de la console VSM

E79954-01

Septembre 2016

ORACLE

Système StorageTek Virtual Storage Manager
Guide de sécurité de la console VSM

E79954-01

Table des matières

Préface 5

Public 5
Accessibilité de la documentation 5

1. Présentation 7

Présentation du produit 7
Principes généraux de sécurité 9
Mise à jour des logiciels 9
Limitation de l'accès réseau aux services critiques 9
Authentification 9
Application du principe du moindre privilège 9
Surveillance de l'activité du système 10
Consultation des dernières informations de sécurité 10

2. Installation sécurisée 11

3. Fonctions de sécurité 13

Préface

Ce document décrit les fonctions de sécurité de la console VSM de StorageTek Virtual Storage Manager.

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 la console VSM.

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.

1

Chapitre 1. Présentation

Cette section contient une présentation du produit et explique les principes généraux de sécurité de l'application.

Présentation du produit

La console Virtual Storage Manager (VSM) des systèmes StorageTek Virtual Storage Manager 6 et 7 fournit une plate-forme commune pour toutes les applications VSM dans les environnements ne comprenant pas de contrôleur zOS. Elles est composée d'éléments matériels et de logiciels Oracle. La console VSM est fournie sur un serveur T5-2 exécutant Solaris 11.3, appelé appareil, avec les applications Virtual Tape Control Software (VTCS), Automated Cartridge System Library Software (ACSLS) et VSM Graphical User Interface (GUI). Ces applications sont préinstallées et préconfigurées sur l'appareil hébergeant la console VSM, ce qui limite les opérations de configuration requises au niveau du site pour intégrer le produit dans l'environnement géré du client. L'appareil a été conçu de façon à limiter les opérations d'administration par le client.

Remarque :

Le personnel Oracle qualifié est seul autorisé à assurer la maintenance du système et à apporter des modifications à la configuration.

La console VSM n'est qu'un composant de la solution VSM.

Les principaux sous-systèmes sont les suivants :

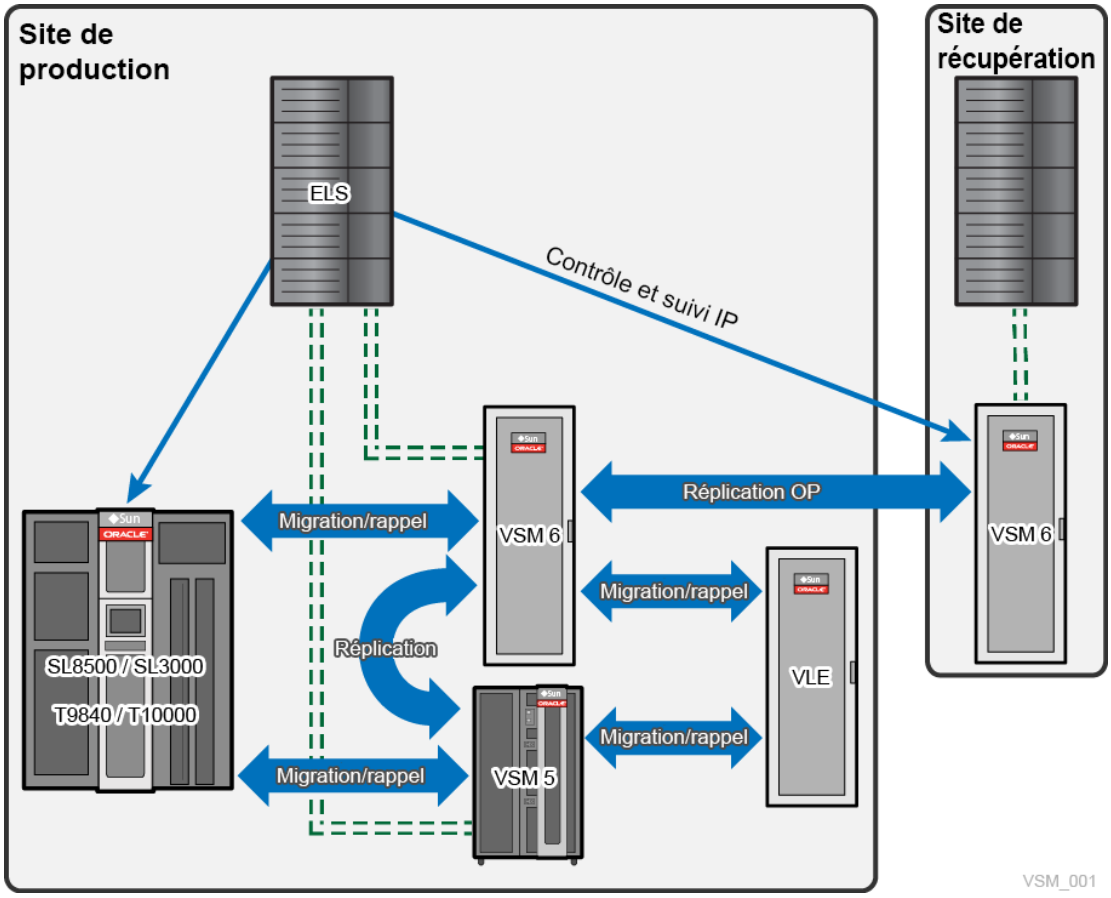
Composants matériels et logiciels VTSS
Les sous-systèmes VTSS VSM 6 et VSM 7 prennent en charge la connectivité émulée de bandes à des hôtes IBM MVS, VM et zLinux par le biais d'interfaces FICON, ainsi que la connexion FICON à des lecteurs RTD (Real Tape Drives, lecteurs de bandes réels) et la connexion TCP/IP à d'autres appareils VTSS et VLE. FICON est une norme développée par IBM désignant un protocole de canal pour le raccordement d'une CPU (zOS) et de périphériques.

Enterprise Library Software (ELS) et Virtual Tape Control Software (VTCS)
ELS est la suite logicielle StorageTek pour mainframe qui permet de gérer le sous-système VTSS. Si un système MVS est utilisé, le logiciel de base ELS comprend Host Software Component (HSC), Storage Management Component (SMC), HTTP Server et Virtual Tape Control Software (VTCS).

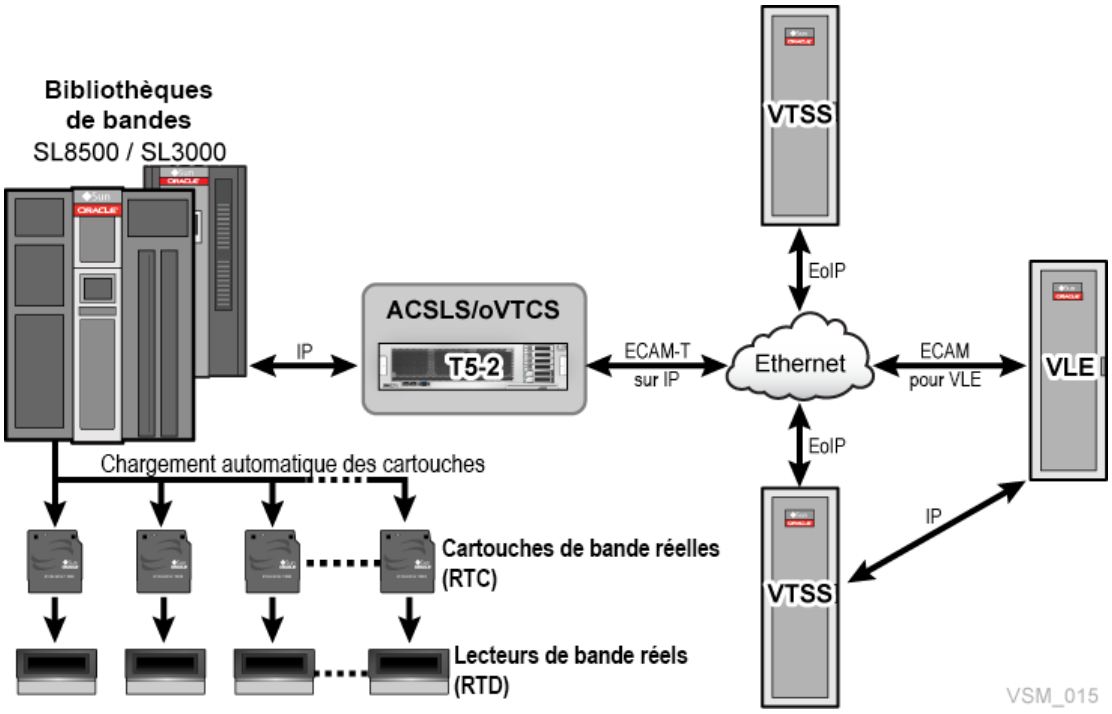
VTCS est le composant d'ELS qui contrôle la création, la suppression, la réplication, la migration de bandes virtuelles ainsi que le rappel d'images de bandes virtuelles sur le sous-système VTSS ; il capture également les informations de rapports provenant du sous-système VTSS.

VTCS peut désormais s'exécuter sur un système z/os du client ou être intégré dans la console VSM.

Composants matériels et logiciels Virtual Library Extended (VLE)
Le sous-système Virtual Library Extended (VLE) sert d'espace de stockage secondaire pour les volumes VTSS de bandes virtuelles (VTV, Virtual Tape Volume) de migration et de rappel. Le sous-système VLE est raccordé par IP au sous-système VTSS.



En l'absence de système MVS, la solution avec console VSM est utilisée. L'application ACSLS interne remplace le composant HSC, et le port de console VSM de l'application VTCS est utilisé.



Principes généraux de sécurité

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

Mise à jour des logiciels

Les mises à jour des applications et du système sont installées par le personnel Oracle qualifié.

Limitation de l'accès réseau aux services critiques

Les sous-systèmes doivent être installés à des emplacements sécurisés accessibles uniquement aux salariés et agents autorisés du client ainsi qu'au personnel de maintenance Oracle. Le système doit être intégré à un réseau protégé par un pare-feu.

Authentification

Assurez-vous que le système est uniquement accessible au personnel autorisé. Il est recommandé de modifier les mots de passe lors du déploiement sur le site du client.

Application du principe du moindre privilège

Les comptes utilisateur non spécifiques à VTSS ne sont pas autorisés. La maintenance et l'administration du système sont uniquement assurées par le biais de comptes préexistants.

Surveillance de l'activité du système

La sécurité du système repose sur trois fondements : des protocoles de sécurité efficaces, la configuration correcte du système et la surveillance du système. Cette troisième exigence est satisfaite par la réalisation d'audits et l'examen des enregistrements d'audit.

Consultation des dernières informations de sécurité

Oracle s'efforce d'améliorer continuellement ses logiciels et la documentation associée. Consultez ce document chaque année pour prendre connaissance des révisions éventuelles.

2

Chapitre 2. Installation sécurisée

Tout le code des applications est préinstallé sur l'appareil hébergeant la console VSM.

Toutes les données de client sont compressées et envoyées dans un format propriétaire prenant en compte la prédominance de l'intercommunication avec les systèmes hérités actuellement installés dans les environnements des clients. Les communications IP doivent s'effectuer au sein d'un réseau privé dédié assurant un chiffrement intégré à l'infrastructure IP.

3

Chapitre 3. Fonctions de sécurité

L'appareil hébergeant la console VSM n'offre aucune fonction de sécurité configurable.