StorageTek SL150 Modular Tape Library

Guide de sécurité

E40923-03

Juin 2015

ORACLE

StorageTek SL150 Modular Tape Library
Guide de sécurité

E40923-03

Copyright © 2012, 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

Liste des tableaux

Préface

Ce document décrit les fonctions de sécurité de la bibliothèque StorageTek SL150 Modular Tape Library d'Oracle.

Public

Ce guide s'adresse à toute personne pouvant être amenée à installer ou configurer la bibliothèque StorageTek SL150 Modular Tape Library d'Oracle de façon sécurisée et à utiliser ses fonctions de sécurité.

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

Présentation

Cette section fournit une présentation du système StorageTek SL150 Modular Tape Library d'Oracle et explique les principes généraux de sécurité de la bibliothèque de bandes.

Présentation du produit

Le système StorageTek SL150 Modular Tape Library est une bibliothèque de bandes modulaire automatisée montée en rack de 3U à 21U (19 pouces) d'Oracle Corporation. Il offre une capacité de stockage allant de 30 à 300 cartouches de bande LTO, de 1 à 20 lecteurs Fibre Channel LTO ou lecteurs de bande SAS et un chemin de contrôle du port du lecteur de bande passerelle Fibre ou SAS via l'un des lecteurs de bande installé.

Sécurité

Toutes les bibliothèques sont conçues et documentées pour une utilisation dans un environnement matériel contrôlé et aucun réseau général ou accès utilisateur. Grâce à un compromis entre Internet et l'entité interne qui fait fonctionner la bibliothèque, vous obtenez de meilleures fonctionnalités et un niveau de protection plus élevé.

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. Les versions du microprogramme SL150 disponibles depuis avril 2015 sont les suivantes :

Juin 2012 v1.00 (RTA 0.1.0.0.0)
Septembre 2012 v1.03 (RTA 0.1.0.3.0)
Octobre 2012 v1.50 (RTA 0.1.5.0.0)
Janvier 2013 v1.82 (RTA 0.1.8.2.0)
Août 2013 v2.0 (RTA 0.2.0.0.0)
Octobre 2013 v2.01(RTA 0.2.0.1.0)
Avril 2014 v2.25 (RTA 0.2.2.5.0)
Juin 2015 v2.50 (RTA 0.2.5.0.0)

Restriction d'accès au réseau

Placez la bibliothèque derrière un pare-feu du centre de données. Le pare-feu vous permet d'être certain que l'accès à ces systèmes 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. Nous vous recommandons d'identifier les hôtes autorisés à se connecter à la bibliothèque et, si possible, de bloquer tous les autres hôtes.

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.

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 et explique comment sécuriser la bibliothèque.

Présentation de votre environnement

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

Quelles sont les ressources à protéger ?

Vous pouvez protéger plusieurs types de ressources de l'environnement de production. Lorsque vous choisissez le niveau de sécurité à mettre en oeuvre, tenez compte des ressources qui nécessitent une protection.

De quels utilisateurs les ressources doivent-elles être protégées ?

Il faut interdire l'accès à la bibliothèque à toute personne connectée à Internet et aux utilisateurs d'intranet non autorisés.

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

Certains types de failles sont aisément détectés et ne sont considérés que comme un désagrément. Toutefois, ce type de faille peut avoir de lourdes conséquences pour les entreprises ou les clients qui utilisent la bibliothèque. Pour protéger correctement vos ressources, vous devez comprendre toutes les implications liées à la sécurité de chaque ressource.

Sécurisation de la bibliothèque

Par défaut, la bibliothèque utilise les ports répertoriés dans le Tableau 2.1, « Ports réseau SL150 ». Le pare-feu doit être configuré de sorte que ces ports puissent être utilisés par le trafic et que tous les ports non utilisés soient bloqués.

Tableau 2.1. Ports réseau SL150

Port	Type	Description
22	TCP	Accès à la CLI SSH - données entrantes avec état For development test and debug only, not available in the field
25	TCP	SMTP sans authentification
67	DHCP	Client - données sortantes
68	DHCP	Client - données entrantes
80	HTTP	Port WebLogic pour l'interface utilisateur distante
123	NTP	Network Time Protocol (s'il est activé)
161	UDP	Demandes de l'agent de bibliothèque SNMP - données entrantes avec état
162	UDP	Notifications d'informations et de déroutements SNMP - données sortantes sans état pour les déroutements, avec état pour les informations
465	TCP	SMTP avec authentification SSL ou TLS
443	HTTPS	Port WebLogic pour l'interface utilisateur distante pour HTTPS
546	DHCPv6	Client DHCP IPv6 - données sortantes
547	DHCPv6	Client DHCP IPv6 - données entrantes
33200-33500	TRACEROUTE	Utilisation du développement logiciel

La sélection d'un numéro de port valide pour l'utilisation de la bibliothèque est soit réservée soit recommandée par la liste de tableaux ci-dessus. Les numéros de port légitimes commencent à 1, car zéro n'est pas un numéro de port légitime.

Lorsque vous configurez SNMP, il est vivement recommandé d'utiliser le protocole SNMPv3 (et non SNMPv2c) en raison de ses fonctions de confidentialité, d'intégrité et d'authentification.

Lors de la configuration de SMTP, il est fortement recommandé de préférer l'utilisation de l'authentification TLS à SSL et aux options de non-authentification.

Configuration de l'installation

Cette section documente les modifications de configuration de la sécurité à effectuer au cours de l'installation.

Attribution du mot de passe utilisateur (admin)

Lors de la première mise sous tension, un assistant de configuration s'affiche automatiquement sur le panneau opérateur local pour fournir les informations de configuration de base. Celles-ci incluent le nom d'utilisateur et le mot de passe du compte administrateur, les paramètres du réseau et d'autres paramètres de base.

La bibliothèque n'est pas opérationnelle tant que toutes ces informations ne sont pas renseignées dans l'assistant de configuration.

Un compte de connexion est fourni à la livraison du produit. L'installateur doit entrer les informations relatives à ce compte au cours de la première étape de l'assistant de configuration. L'utilisateur doit ensuite saisir un nouveau mot de passe.

Après avoir suivi les étapes de l'assistant de configuration initiale et une fois la bibliothèque entièrement mise sous tension, les modifications supplémentaires apportées à la configuration de la bibliothèque peuvent être effectuées via l'interface utilisateur de navigateur (BUI) pour tous les paramètres de la bibliothèque.

Appliquez la gestion des mots de passe

Les règles élémentaires de gestion des mots de passe (comme la longueur, l'historique et la complexité) doivent être appliquées à tous les mots de passe. Les mots de passe de la bibliothèque SL150 doivent contenir de 8 à 128 caractères dont au moins un caractère alphanumérique ou un caractère spécial. Il faut modifier le mot de passe par défaut au cours de l'installation et ne jamais le réutiliser.

Remarque:

Le nombre de caractères masqués affichés ne correspond pas au nombre exact de caractères entrés.

Authentification de l'interface utilisateur de navigateur

Limitez les paramètres de navigateur utilisés pour accéder à l'interface utilisateur distante à TLS 1.0 ou supérieur, afin de réduire les niveaux de microprogramme du CVE-2014-3566 en dessous de la version 2.50. Le microprogramme de la bibliothèque n'adoptera pas automatiquement SSLv3 avec la version 2.50.

3

Fonctions de sécurité

Cette section décrit les mécanismes de sécurité spécifiques qu'offre ce produit.

Cette bibliothèque contient un pare-feu interne pour se protéger. Toutefois, cela ne doit pas constituer la seule ligne de sécurité de la bibliothèque. Idéalement, la bibliothèque doit se trouver dans un centre de données physiquement sécurisé, sur un réseau sécurisé dont l'accès est réservé aux serveurs qui utilisent ses fonctionnalités. Les serveurs et les applications exécutés sur les bibliothèques doivent également être sécurisés.

Les comptes utilisateur devraient se limiter au rôle *Operator* plutôt que d'accorder le rôle *Admin* à tous les utilisateurs.. L'utilisation du rôle d'utilisateur *Service* devrait faire l'objet d'un apprentissage. Créez, activez ou désactivez les comptes auxquels le rôle d'utilisateur *Service* a été accordé en fonction de vos besoins. Le rôle Service concède davantage de privilège que le rôle *Operator*, voire presqu'autant que le rôle *Admin*.

Si un historique des activités de la bibliothèque est requis pour des motifs d'investigation, le "Journal des activités" peut être consulté et exporté afin d'être analysé. Le Journal des activités accessible depuis l'interface utilisateur peut afficher les connexions d'utilisateur et les actions initiées par l'hôte ou l'interface utilisateur afin de garantir la traçabilité.

4

Redéploiement

Cette section décrit comment rétablir l'état par défaut d'usine de la bibliothèque pour effacer toutes les données de client.

Une procédure est fournie pour supprimer toutes les informations de configuration du client et tous les fichiers journaux, puis rétablir l'état par défaut du système (usine) dans l'hypothèse où le client aurait besoin de supprimer une bibliothèque. Pour appeler cette procédure, vous devez placer la bibliothèque en mode "locate", maintenir les boutons de localisation avant et arrière enfoncés pendant un peu plus de 10 secondes, puis relâcher les deux boutons.

L'accélération du clignotement de la LED indique que vous pouvez relâcher le bouton "Locate".

Annexe A

Liste de contrôle du déploiement sécurisé

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

1. Appliquez la gestion des mots de passe à tous les comptes.
2. Appliquez des contrôles d'accès, à la fois de proximité physique et via des interfaces, telles que SCSI, UI, SNMP, etc.
3. Limitez l'accès au réseau.
   a. Il convient d'implémenter un pare-feu.
   b. Ce pare-feu ne doit pas être compromis.
   c. Il faut surveiller l'accès au système.
   d. Il faut vérifier les adresses IP du réseau.
   e. Les services peuvent être dotés d'outils requérant un mot de passe approprié ou des contrôles d'accès surveillés (par exemple, SDP-2 pour permettre le téléchargement automatique des informations du journal ou d'autres accès)
4. Contactez le service de support Oracle, le service Oracle en charge des bibliothèques de bandes ou le responsable de votre compte si vous constatez une faille de sécurité dans des bibliothèques de bandes Oracle.
5. SMTP devrait utiliser TLS plutôt que des protocoles inférieurs, tels que SSL, ou qu'aucun protocole.
6. SNMP doit être configuré avec le niveau V3 plutôt que le niveau V2C ou tout niveau inférieur.

Annexe B

Références

Guide de l'utilisateur SL150 disponible à l'adresse :

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#libraries

Toute la documentation du SL150 est disponible parmi les documents en ligne sous la référence E35103-07.