StorageTek T10000D

Guide de sécurité

E50321-04

Août 2016

StorageTek T10000D
Guide de sécurité

E50321-04

Table des matières

Liste des tableaux

Préface

Ce document décrit les fonctions de sécurité du système StorageTek T10000D 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 du système StorageTek T10000D.

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 fournit une vue d'ensemble du lecteur de bande T10000D et explique les principes généraux de sécurité pour ce produit.

Présentation du produit

Le lecteur de bande d'entreprise T10000Dse connecte à l'interface SCSI des systèmes ouverts via le protocole Fibre Channel et aux mainframes via le protocole FICON. Le lecteur de bande T10000D transfère les données vers et depuis un hôte et les stocke sur un support magnétique amovible. L'objectif principal du lecteur de bande T10000D est de fournir d'importantes capacités de sauvegarde, d'archivage et de traitement des données mais aussi d'assurer une grande fiabilité aux clients d'entreprise qui exigent un cycle de service de qualité et un niveau élevé de fiabilité. Ce produit fournit une fonction de chiffrement des données en option. Le client peut activer cette fonction. Les capacités et la rapidité des bandes natives de ce lecteur de bande ont été améliorées. En outre, des fonctions de gestion des données ont été ajoutées.

Capacité et performances du T10000D

Le lecteur de bande T10000D a une capacité de 8,5 To et une vitesse de bande native de 252 Mo/seconde.

Sécurité

Le lecteur de bande T10000D est conçu et documenté pour une utilisation dans un environnement matériel contrôlé. Les lecteurs de bande sont toujours situés dans un centre de données contrôlé et sont généralement installés à l'intérieur d'une bibliothèque de bandes. Il arrive que les clients utilisent une version en rack, mais c'est peu fréquent. Le centre de données contrôlé est également situé derrière un pare-feu protégé par les stratégies de sécurité du client. Grâce à un compromis entre Internet et l'entité interne qui fait fonctionner le lecteur de bande, 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 du produit.

Mise à jour des logiciels

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

T10000D 4.XX.1XX

Restriction de l'accès au réseau

Conservez le lecteur de bande derrière un pare-feu du centre de données. Le pare-feu permet de garantir que l'accès aux 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. Il est recommandé d'identifier les hôtes autorisés à se connecter au lecteur de bande 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

Chapitre 2. Installation sécurisée

Cette section vous indique les processus de planification et d'implémentation pour une installation et une configuration sécurisées. Il décrit également plusieurs topologies de déploiement recommandées pour ces systèmes et explique comment sécuriser un lecteur de bande.

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 au lecteur de bande à toute personne connectée à Internet. Faut-il également interdire l'accès au lecteur de bande aux employés qui utilisent l'intranet de votre entreprise ?

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

Il peut arriver qu'une faille dans le schéma de sécurité soit détectée et considérée uniquement comme un désagrément. Toutefois, ce type de faille peut avoir des conséquences lourdes pour les entreprises ou les clients qui utilisent le lecteur de bande. Pour protéger correctement vos ressources, vous devez comprendre toutes les implications liées à la sécurité de chaque ressource.

Sécurisation du lecteur de bande

Par défaut, le lecteur de bande utilise les ports répertoriés dans le tableau suivant. Il faut configurer le pare-feu de sorte que ces ports puissent être utilisés par le trafic et que tous les

ports non utilisés soient bloqués. Les lecteurs de bande prennent en charge les protocoles IPv6 et IPv4.

Tableau 2.1. Ports réseau utilisés

Port	T10000D
Port TCP : 22 - SSH VOP	X
Port TCP : 22 - SFTP	X
Port UDP : 161 - SNMPV1 Demandes de l'agent de lecteur de bande - données entrantes avec état	X
Port UDP : 162 - Notifications d'informations et de déroutements de lecteur de bande SNMPV1 - données sortantes sans état pour les déroutements, avec état pour les informations	X
TCP :23 - TELNET	
TCP : 21 - FTP	
TCP : 9842 - EPT	
3331 OKM - Service CA des serveurs Root et Challenge	X
3332 OKM – Inscription. Niveau de chiffrement : AES256	X
3334 OKM – Echange de clé de chiffrement. Niveau de chiffrement : AES256	X
3335 OKM – Détection du cluster. Niveau de chiffrement : AES256	X

Les ports 21 et 23 seront désactivés pour les utilisateurs du lecteur de bande T10000D. Une option de configuration VOP est à la disposition des clients ayant besoin d'un accès TELNET et/ou FTP non sécurisés.

Installation de l'application Virtual Operator Panel (VOP)

VOP doit être installé uniquement sur les systèmes qui se trouvent dans la même infrastructure réseau protégée que le lecteur de bande. Il faut mettre en place des contrôles d'accès client sur les systèmes où VOP est installé pour garantir un accès restreint au lecteur de bande. Reportez-vous au Tableau 2.1, « Ports réseau utilisés » pour connaître les ports utilisés par VOP.

Reportez-vous au guide d'utilisation VOP pour consulter les instructions d'installation de VOP sur Internet.

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

Configuration postintallation

Cette section documente les modifications de configuration de la sécurité à effectuer une fois l'installation terminée.

Attribution du mot de passe utilisateur (admin)

Le client du site doit modifier le mot de passe du compte admin et ce dernier appartiendra au client. La sécurité du mot de passe doit être conforme aux normes Oracle. Il existe un nombre infini de mots de passe que vous pouvez utiliser tout au long du cycle de vie du lecteur de bande. Si le mot de passe admin a été oublié, il est possible de le réinitialiser. Le premier mot de passe correspond au mot de passe par défaut envoyé avec le lecteur de bande.

Application de la gestion des mots de passe

Les règles élémentaires de gestion des mots de passe (comme la longueur et la complexité) doivent être appliquées au mot de passe administrateur.

Le mot de passe doit comporter au moins un des éléments de chacune des règles suivantes.

- Le mot de passe doit comprendre entre 8 et 16 caractères.
- Minuscules (a-z)
- Majuscules (A-Z)
- Chiffre décimal (0-9)
- Caractères spéciaux (.?;:"{}[]()!@#$%&, ...)

3

Chapitre 3. Fonctions de sécurité

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

Le lecteur de bande T10000D communique par le biais d'un canal sécurisé avec Oracle Key Management System. Le T10000D communique par SSH et SFTP avec Virtual Operator Panel ; TELNET et FTP seront désactivés pour nos clients. Toutefois, cela ne doit pas constituer la seule ligne de sécurité du lecteur de bande. Idéalement, les lecteurs de bande doivent se trouver dans un centre de données physiquement sécurisé, également doté d'un réseau sécurisé dont l'accès est réservé aux serveurs qui utilisent ses fonctionnalités. Les serveurs et les applications exécutés sur les lecteurs de bande doivent également être sécurisés. En outre, l'utilisateur peut élever le niveau de sécurité du lecteur de bande à un niveau supérieur. L'une des possibilités dont il dispose pour cela est le chiffrement des données.

Annexe A. Liste de contrôle du déploiement sécurisé

La liste de contrôle de sécurité suivante inclut les directives permettant de sécuriser le lecteur de bande :

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. Il faut surveiller l'accès au système.
   d. Il faut vérifier les adresses IP du réseau.
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 des failles de sécurité dans des lecteurs de bande Oracle.

Annexe B

Annexe B. Références

Vous pouvez accéder au guide de l'utilisateur VOP à l'adresse :

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