StorageTek Enterprise Library Software

Guide de sécurité

E63466-01

Mars 2015

ORACLE

StorageTek Enterprise Library Software
Guide de sécurité

E63466-01

Table des matières

Préface

Ce document décrit les fonctions de sécurité du logiciel StorageTek Enterprise Library Software (ELS) d'Oracle.

Public

Ce guide s'adresse à toute personne impliquée dans l'utilisation des fonctions de sécurité et dans l'installation et la configuration sécurisée du logiciel StorageTek Enterprise Library Software (ELS).

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 contient une présentation de la suite logicielle ELS et explique les principes généraux de sécurité des applications.

1.1. Présentation du produit

ELS fournit une prise en charge de l'automatisation des bandes aux environnements de bande mainframe d'Oracle StorageTek pour les plates-formes suivantes :

- Plate-forme IBM z/OS. ELS prend en charge une architecture d'automatisation de bande client/serveur TCP/IP, ce qui permet au logiciel client SMC s'exécutant sur une partition LPAR z/OS de communiquer avec le logiciel serveur HSC/VTCS s'exécutant sur une partition LPAR z/OS différente.
- Plate-forme IBM z/VM. Le logiciel VM Client d'ELS pour les systèmes z/VM communique avec le serveur HSC/VTCS en cours d'exécution sur un LPAR z/OS pour automatiser la bande virtuelle et physique traitant z/VM.
- Plate-forme Fujitsu MSP/EX. Le composant SMC doit s'exécuter sur chaque hôte sur lequel un traitement de bande a lieu. Le composant serveur d'ELS (HSC/VTCS) peut s'exécuter sur le même hôte MSP/EX que le composant SMC. Il peut également s'exécuter sur un hôte distant différent. Si SMC et HSC/VTCS se trouvent sur des hôtes MSP/EX différents, le protocole TCP/IP est utilisé pour envoyer des demandes depuis l'hôte client vers l'hôte serveur. Pour permettre la réception de demandes HTTP d'un client SMC distant, le composant HTTP doit être activé sur le SMC s'exécutant sur l'hôte serveur.

Les communications client/serveur d'ELS sont utilisées pour envoyer des demandes de chemin de contrôle, principalement des demandes de montage/démontage, pour des volumes de bande virtuels et physiques. Les informations comprises dans ces demandes de chemin de contrôle sont les informations relatives à la configuration et la stratégie TapePlex, les adresses d'unité de transport de bande virtuel/physique et les numéros de série de volume de bande virtuel/physique. Il est important de noter que les communications client/serveur d'ELS ne contiennent pas de données client, lesquelles sont toujours acheminées via des interfaces de chemin de données IBM FICON/ESCON connectant des partitions LPAR de l'hôte aux transports de bande ou périphériques de bande virtuels VSM Oracle StorageTek.

Les informations contenues dans le présent guide de sécurité s'appliquent à toutes les versions d'ELS. Comme décrit dans la partie 3 de ce guide, il est possible de sécuriser les communications de chemin de contrôle client/serveur d'ELS si une protection de ce type est souhaitée ou nécessaire. Par ailleurs, ce document couvre tous les aspects de sécurité des diverses opérations d'installation et de postinstallation d'ELS.

1.2. Principes généraux de sécurité

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

1.2.1. 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. Le dernier bundle de maintenance cumulatif d'ELS, ainsi que les correctifs PTF individuels et les données HOLDDATA, sont tous disponibles sur My Oracle Support (MOS). Les bundles de maintenance cumulatifs sont mis à jour tous les mois de sorte à inclure tous les correctifs PTF du dernier cycle de test de régression mensuel d'ELS. Tous les correctifs PTF d'un bundle cumulatif ont été testés ensemble sous la forme d'un package complet. Il est possible de recevoir des notifications par e-mail de correctif PTF HIPER en s'abonnant aux documents d'alerte sur les sujets d'actualité MOS concernant les produits ELS. Les clients sont encouragés à conserver les niveaux de maintenance actuels, à maintenir les données HOLDDATA à jour et à s'abonner aux alertes sur les sujets d'actualité liés à HIPER.

1.2.2. Restriction d'accès au réseau

Dans un souci de performances et de sécurité, acheminez les communications de chemin de contrôle d'ELS via un réseau isolé protégé par un pare-feu. L'utilisation d'un pare-feu vous permet d'être certain que l'accès aux systèmes ELS est limité à un réseau défini, qui peut être surveillé et restreint le cas échéant. L'utilisation d'un réseau dédié aux communications client/serveur d'ELS élimine les conflits d'utilisation avec d'autres applications et améliore les performances des systèmes de bande.

1.2.3. Consultation des dernières informations de sécurité

Oracle s'efforce d'améliorer continuellement les logiciels et la documentation. Recherchez régulièrement des révisions éventuelles du présent guide de sécurité et de toute autre documentation produit d'ELS. Toutes les guides référencés dans ce document sont disponibles sur le site Oracle Technical Network dans la section Tape Storage Products.

2

Installation sécurisée

La fonction SAF (System Authorization Facility) d'IBM z/OS fournit une protection essentielle sur la plupart des aspects de sécurité d'ELS. La fonction SAF est généralement implémentée avec le package RACF d'IBM ou un équivalent. Cette section décrit l'utilisation d'un environnement SAF basé sur RACF en vue d'installer et de configurer une installation ELS sécurisée.

2.1. Installation d'ELS

Le document Oracle *StorageTek Enterprise Library Software: Installation d'ELS* décrit comment installer et configurer votre version d'ELS en utilisant la protection RACF. Reportez-vous à ce document pour plus d'informations sur les sujets d'installation suivants liés à la sécurité :

- Installation du logiciel de base et du dernier bundle de maintenance cumulatif
- Autorisation APF de bibliothèque de chargement ELS
- Autorisation APF de bibliothèque d'exits utilisateur HSC
- Autorisation APF de bibliothèque de chargement SMC JES3

2.2. Configuration d'ELS suivant l'installation

Les documents Oracle nommés ci-dessous décrivent les tâches de configuration suivant l'installation pour votre version d'ELS :

- *StorageTek Enterprise Library Software: Gestion du HSC et du VTCS*
- *StorageTek Enterprise Library Software : Configuration et gestion du SMC*
- *StorageTek Enterprise Library Software: ELS Programming Reference*

Reportez-vous à ces documents pour plus d'informations sur les sujets de postinstallation suivants liés à la sécurité :

- Définition d'une protection RACF pour la sécurité du jeu de données CDS
- Définition d'une autorité de commande et d'une autorité d'interface de programmation à l'aide de l'exit utilisateur HSC SLSUX15
- Définition d'une autorité d'accès au volume pour le montage et l'éjection des volumes à l'aide de l'exit utilisateur HSC SLSUX14
- Définition d'une autorité VOLSER des pools MVC et des sous-pools de travail vides

- Définition d'un segment OMVS RACF de SMC pour les communications avec un sous-système HSC distant
- Définition d'un segment OMVS RACF de SMC pour les communications avec un appareil VLE

3

Fonctions de sécurité

Ce chapitre décrit les mécanismes de sécurité spécifiques qu'offre ELS.

3.1. Sécurisation d'ELS à l'aide du protocole AT-TLS - z/OS uniquement

Le protocole AT-TLS (Application Transparent Transport Layer Security) d'IBM z/OS utilise le chiffrement de données SSL pour sécuriser les applications TCP/IP z/OS. Pour plus d'informations sur le protocole AT-TLS, reportez-vous à la publication *IBM z/OS Communications Server: IP Configuration Guide* et consultez les informations sur l'agent de stratégie AT-TLS disponibles dans la publication *IBM z/OS Communications Server: IP Configuration Reference*.

La sécurisation des communications client/serveur ELS entre le composant SMC et le composant HSC/VTCS est décrite dans le livre blanc Oracle *Using AT-TLS with HSC/SMC Client/Server z/OS Solution: Implementation Example*. Ce livre blanc est publié sur le site Oracle Technical Network dans la section Tape Storage Products. Reportez-vous à cette publication pour obtenir des informations de configuration détaillées.

Pour sécuriser le logiciel ELS à l'aide du protocole AT-TLS, Oracle recommande l'emploi d'un des algorithmes de chiffrement SSL suivants :

- Famille SHA-2 (SHA-256, SHA-384, SHA-512)
- AES >= 128 bits
- RSA >= 2 048 bits
- Diffie-Hellman (DH) >= 2 048 bits
- ECC >= 256 bits

Les autres algorithmes de chiffrement SSL offrent une protection plus faible et ne doivent pas être utilisés avec ELS.

Remarque:

Actuellement, l'appareil StorageTek Virtual Library Extension (VLE) pour VSM ne prend pas en charge les communications AT-TLS. Ne choisissez donc pas le protocole AT-TLS pour sécuriser les communications VLE d'ELS.

3.2. Utilisation de la fonction de sécurité XAPI d'ELS

ELS 7.3 introduit une nouvelle fonction de sécurité XAPI pour les communications client/serveur. Elle est activée par défaut sur le serveur HTTP SMC. Elle offre des fonctionnalités d'authentification d'utilisateur supplémentaires issues du protocole XAPI qui sont entièrement contenues dans ELS. Pour utiliser la fonction de sécurité XAPI, vous devez définir les informations d'identification de sécurité (codes utilisateur et mots de passe) des clients et des serveurs ELS. Les opérations TapePlex d'ELS 7.3 utilisent ces informations d'identification pour sécuriser les transactions XAPI (montage, démontage, consultation de volume, ajout au pool de travail). L'utilisation des informations d'identification de sécurité XAPI est totalement transparente et ne requiert pas l'intervention d'un utilisateur ou d'un opérateur. Reportez-vous au document *Configuration et gestion du SMC version 7.3* pour plus d'informations sur la configuration de la fonction de sécurité XAPI.

Le meilleur moyen de sécuriser les transactions XAPI des TapePlex qui hébergent uniquement des applications client ELS (SMC et VM) est d'utiliser les fonctions AT/TLS décrites dans Section 3.1, « Sécurisation d'ELS à l'aide du protocole AT-TLS - z/OS uniquement ». AT/TLS est une fonction de couche transport externe et transparente pour ELS.

Utilisez la fonction de sécurité XAPI d'ELS 7.3 pour sécuriser les TapePlex qui hébergent des clients hors ELS (clients de systèmes ouverts) ou une combinaison de clients ELS (SMC et VM) et de clients hors ELS. Dans ces environnements, la fonction AT-TLS peut être associée à la fonction de sécurité XAPI d'ELS 7.3 mais elle ne permet pas de sécuriser les transactions XAPI des clients hors ELS.

4

Considérations de sécurité pour les développeurs

Le document Oracle *StorageTek Enterprise Library Software: ELS Programming Reference* décrit les API ELS mises à la disposition des développeurs d'applications. L'interface de programmation d'ELS est basée sur l'interface UUI (Unified User Interface), laquelle utilise l'exit de sécurité de commande HSC SLSUX15 pour gérer l'accès à ses fonctions sur la base d'une autorisation RACF (ou équivalent). Reportez-vous à la section Section 2.2, « Configuration d'ELS suivant l'installation » pour plus d'informations sur la sécurisation de SLSUX15 à l'aide de RACF.

Annexe A

Liste de contrôle du déploiement sécurisé

1. Utilisez la protection RACF (ou équivalent) comme l'explique le présent guide de sécurité.
2. Limitez l'accès au réseau. Le logiciel ELS et les bibliothèques de bandes qu'il gère doivent se trouver derrière le pare-feu de l'entreprise.
3. Si nécessaire, protégez le trafic réseau d'ELS à l'aide du protocole AT-TLS d'IBM ou de la fonction de sécurité XAPI d'ELS.
4. Appliquez tous les correctifs PTF et les données HOLDDATA d'ELS.
5. Contactez l'équipe de support logiciel d'Oracle sur le site `http://www.myoraclesupport.com/` si vous constatez des vulnérabilités dans le logiciel ELS d'Oracle.

Annexe B

Références

La documentation ELS est enregistrée dans des bibliothèques organisées selon la version d'ELS. Vous pouvez y accéder à la partir de la page de documentation des produits de stockage sur bande.

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