StorageTek Enterprise Library Software

Sicherheitshandbuch

E63464-01

März 2015

ORACLE

StorageTek Enterprise Library Software
Sicherheitshandbuch

E63464-01

Inhalt

Vorwort

In diesem Dokument werden die Sicherheitsfunktionen von StorageTek Enterprise Library Software (ELS) von Oracle beschrieben.

Zielgruppe

Das Handbuch richtet sich an alle, die Sicherheitsfeatures und sichere Installationen und Konfigurationen von StorageTek Enterprise Library Software (ELS) verwenden.

Barrierefreie Dokumentation

Informationen über Eingabehilfen für die Dokumentation finden Sie auf der Oracle Accessibility Program-Webseite unter http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Zugang zum Oracle-Support
Oracle-Kunden mit einem gültigen Oracle-Supportvertrag haben Zugriff auf elektronischem Support über My Oracle Support. Weitere Informationen erhalten Sie unter http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info oder unter http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs, falls Sie eine Hörbehinderung haben.

1

Überblick

Dieser Abschnitt gibt einen Überblick über die ELS-Software-Suite und erläutert die allgemeinen Grundsätze der Anwendungssicherheit.

1.1. Produktüberblick

ELS bietet Unterstützung für die Bandautomatisierung von Oracle StorageTek-Mainframe-Bandumgebungen auf den folgenden Plattformen:

- IBM z/OS-Plattform. ELS unterstützt eine Architektur der TCP/IP-Client/Server-Bandautomatisierung, bei der die auf einer z/OS-LPAR ausgeführte SMC-Clientsoftware mit der HSC/VTCS-Serversoftware kommuniziert, die auf einer anderen z/OS-LPAR ausgeführt wird.
- IBM z/VM-Plattform. Die ELS-VM-Clientsoftware für z/VM-Systeme kommuniziert mit der HSC/VTCS-Serversoftware, die auf einer z/OS-LPAR ausgeführt wird, um eine virtuelle und physische Bandverarbeitung für z/VM zu automatisieren.
- Fujitsu MSP/EX-Plattform. SMC muss auf allen Hosts ausgeführt werden, auf denen Bandverarbeitung stattfindet. Die ELS-Serverkomponente (HSC/VTCS) kann auf demselben MSP/EX-Host wie SMC oder auf einem separaten Remotehost ausgeführt werden. Wenn sich SMC und HSC/VTCS auf unterschiedlichen MSP/EX-Hosts befinden, senden Sie mit TCP/IP Anforderungen vom Clienthost an den Serverhost. Um HTTP-Anforderungen von einem SMC-Remoteclient zu empfangen, muss die HTTP-Komponente auf der SMC aktiviert werden, die auf dem Serverhost ausgeführt wird.

Mithilfe der ELS-Client/Server-Kommunikation werden Kontrollpfadanforderungen abgesetzt. Das sind in erster Linie Anforderungen für das Laden/Entnehmen von virtuellen und physischen Band-Volumes. In diesen Kontrollpfadanforderungen sind Informationen zur TapePlex-Konfiguration und Policy, Adressen von virtuellen/physischen Bandtransporteinheiten und Seriennummern von virtuellen/physischen Band-Volumes enthalten. Noch wichtiger: ELS-Client/Server-Kommunikation enthält niemals Kundendaten. Kundendaten werden immer über IBM-FICON/ESCON-Datenpfadschnittstellen geleitet, die Host-LPARs mit Oracle StorageTek-Bandtransportsystemen oder virtuellen VSM-Bandgeräten verbinden.

Die Informationen in diesem Sicherheitshandbuch gelten für alle ELS-Releases. Wie in Teil 3 dieses Handbuchs erörtert, können ELS-Client/Server-Kontrollpfadkommunikationen gesichert werden, wenn ein solcher Schutz wünschenswert oder erforderlich ist. Darüber hinaus werden in diesem Dokument Sicherheitsaspekte verschiedener ELS-Aktivitäten während und nach der Installation erörtert.

1.2. Allgemeine Sicherheitsgrundsätze

Die folgenden Grundsätze sind für die sichere Verwendung jedes Produkts von wesentlicher Bedeutung.

1.2.1. Software muss immer auf dem neuesten Stand sein

Einer der Grundsätze für einen sicheren Betrieb besteht darin, alle Softwareversionen und Patches auf dem neuesten Stand zu halten. Das neueste kumulierte ELS-Wartungs-Bundle sowie einzelne PTFs und HOLDDATA sind unter My Oracle Support (MOS) verfügbar. Kumulierte Wartungs-Bundle werden monatlich aktualisiert, sodass sie alle PTFs aus dem aktuellen monatlichen ELS-Regressionstestzyklus enthalten. Alle PTFs in einem kumulierten Bundle wurden zusammen als Komplettpaket getestet. Die HIPER PTF-E-Mail-Benachrichtigung ist verfügbar, wenn Sie für die ELS-Produkte Dokumente mit MOS Hot Topics Alerts abonnieren. Kunden wird empfohlen, die aktuellen Wartungsebenen beizubehalten, HOLDDATA auf dem aktuellen Stand zu halten und Hot Topics Alerts für HIPER-Benachrichtigungen zu abonnieren.

1.2.2. Einschränkung des Netzwerkzugriffs

Aus Performance- und Sicherheitsgründen sollten Sie ELS-Kontrollpfadkommunikationen über ein isoliertes Netzwerk leiten, dem eine Firewall vorgeschaltet ist. Die Firewall bietet die Gewähr, dass der Zugriff auf ELS-Systeme auf ein bekanntes Netzwerk beschränkt ist, das gegebenenfalls überwacht und eingeschränkt werden kann. Ein dediziertes Netzwerk für ELS-Client/Server-Kommunikationen vermeidet Netzwerkkonflikte mit anderen Anwendungen und verbessert die Performance von Bandsystemen.

1.2.3. Sicherheitsinformationen immer auf dem neuesten Stand halten

Oracle nimmt fortwährend Verbesserungen an Software und Dokumentation vor. Prüfen Sie regelmäßig, ob neue Fassungen von diesem Sicherheitshandbuch und allen anderen ELS-Produktdokumentationen vorhanden sind. Alle in diesem Dokument referenzierten ELS-Dokumentationen sind im Oracle Technical Network im Abschnitt "Tape Storage Products" verfügbar.

2

Sichere Installation

Das System Authorization Facility (SAF) für IBM z/OS bietet grundlegenden Schutz für die meisten Sicherheitsaspekte von ELS. SAF wird in der Regel mit dem RACF-Package von IBM oder einer vergleichbaren Lösung implementiert. In diesem Abschnitt wird erläutert, wie Sie mit einer auf RACF basierenden SAF-Umgebung eine sichere ELS-Installation durchführen und konfigurieren.

2.1. Installation von ELS

Im Oracle-Dokument *StorageTek Enterprise Library Software: Installing ELS* wird beschrieben, wie Sie Ihre Version von ELS mit RACF-Schutz installieren und konfigurieren. In diesem Dokument erhalten Sie weitere Informationen zu den folgenden sicherheitsbezogenen Installationsthemen:

- Installation der Basissoftware und des neuesten kumulierten Wartungs-Bundles
- APF-Autorisierung ELS-Lastbibliothek
- APF-Autorisierung HSC User Exit-Bibliothek
- APF-Autorisierung SMC-JES3-Lastbibliothek

2.2. ELS-Konfiguration nach der Installation

In diesen Oracle-Dokumenten werden Konfigurationsaufgaben beschrieben, die für Ihre Version von ELS nach der Installation ausgeführt werden:

- *StorageTek Enterprise Library Software: Configuring HSC and VTCS*
- *StorageTek Enterprise Library Software: Configuring and Managing SMC*
- *StorageTek Enterprise Library Software: ELS Programming Reference*

In diesen Dokumenten erhalten Sie weitere Informationen zu den folgenden Sicherheitsthemen, die nach der Installation relevant sind:

- RACF-Schutz für CDS-Dataset-Sicherheit definieren
- Befehlsautorität und Autorität der programmatischen Schnittstelle mit HSC User Exit SLSUX15 definieren
- Volume-Zugriffsautorität für das Laden und Entnehmen von Volumes mit dem HSC User Exit SLSUX14 definieren
- MVC-Pool- und Scratch-Subpool-Volser-Autorität definieren

- SMC-OMVS-RACF-Segment für die Kommunikation mit einem Remote-HSC-Subsystem definieren
- SMC-OMVS-RACF-Segment für die Kommunikation mit einer VLE-Appliance definieren

3

Sicherheitsfunktionen

In diesem Kapitel werden die spezifischen Sicherheitsverfahren bei ELS beschrieben.

3.1. ELS mit AT-TLS sichern – nur z/OS

Die Application Transparent Transport Layer Security (AT-TLS) von IBM z/OS sichert z/OS-TCP/IP-Anwendungen mit SSL-Datenverschlüsselung. Weitere Informationen zu AT-TLS finden Sie im Dokument *IBM publication z/OS Communications Server: IP Configuration Guide*. Weitere Informationen zum AT-TLS Policy Agent finden Sie im Dokument *IBM publication z/OS Communications Server: IP Configuration Reference*.

Das Sichern von ELS-Client/Server-Kommunikationen zwischen SMC und HSC/VTCS wird im Oracle Whitepaper *Using AT-TLS with HSC/SMC Client/Server z/OS Solution: Implementation Example* beschrieben. Dieses Whitepaper wird im Oracle Technical Network im Abschnitt "Tape Storage Products" veröffentlicht. Detaillierte Informationen zur Konfiguration finden Sie in dieser Publikation.

Zur Sicherung von ELS mit AT-TLS empfiehlt Oracle die Verwendung der folgenden SSL-Verschlüsselungsalgorithmen:

- SHA-2-Familie (SHA-256, SHA-384, SHA-512)
- AES >= 128 Bit
- RSA >= 2048 Bit
- Diffie-Hellman (DH) >= 2048 Bit
- ECC >= 256 Bit

Andere SSL-Verschlüsselungsalgorithmen bieten einen schwächeren Schutz und sollten nicht mit ELS verwendet werden.

Hinweis:

Die Appliance StorageTek Virtual Library Extension (VLE) für VSM unterstützt gegenwärtig keine AT-TLS-Kommunikationen. Sichern Sie ELS-VLE-Kommunikationen nicht mit AT-TLS.

3.2. Verwendung der ELS-XAPI-Sicherheitsfunktion

ELS 7.3 führt eine neue XAPI-Sicherheitsfunktion für die Kommunikation zwischen Client und Server ein, die standardmäßig auf dem SMC-HTTP-Server aktiviert ist. Die XAPI-Sicherheitsfunktion bietet zusätzliche Möglichkeiten der Benutzerauthentifizierung als

Teil des XAPI-Protokolls. Diese Möglichkeiten sind integraler Bestandteil und vollständig in ELS enthalten. Wenn Sie die XAPI-Sicherheitsfunktion verwenden möchten, müssen Sie Sicherheitszugangsdaten (Benutzer-IDs und Kennwörter) für ELS-Clients und -Server festlegen. ELS 7.3 TapePlex-Vorgänge verwenden diese Sicherheitszugangsdaten zum Sichern von XAPI-Transaktionen (Laden, Entnehmen, Volume-Lookup, Scratch usw.). Die Verwendung von XAPI-Sicherheitszugangsdaten ist vollständig transparent und erfordert keine weiteren Eingriffe durch den Benutzer oder den Operator. Weitere Informationen zum Konfigurieren der XAPI-Sicherheitsfunktion finden Sie unter *Configuring and Managing SMC 7.3*.

Die bevorzugte Methode zum Sichern von XAPI-Transaktionen für TapePlexes, auf denen nur ELS-Clientanwendungen (SMC- und VM-Client) gehostet werden, ist die Verwendung von AT/TLS-Funktionen, wie unter Abschnitt 3.1, „ELS mit AT-TLS sichern – nur z/OS“ beschrieben. AT/TLS ist eine Transportschichtfunktion, die für ELS extern und transparent ist.

Verwenden Sie die ELS 7.3 XAPI-Sicherheitsfunktion, um TapePlexes zu sichern, auf denen Nicht-ELS-Clients (Clients für offene Systeme) oder eine Kombination aus ELS-Clients (SMC- und VM-Client) und Nicht-ELS-Clients gehostet sind. AT-TLS kann in diesen Umgebungen zusätzlich zur ELS 7.3 XAPI-Sicherheitsfunktion verwendet werden, allerdings sichert AT-TLS keine XAPI-Transaktionen für Nicht-ELS-Clients.

4

Überlegungen zur Sicherheit für Entwickler

Im Oracle-Dokument *StorageTek Enterprise Library Software: ELS Programming Reference* werden die ELS-APIs beschrieben, die Anwendungsentwicklern zur Verfügung stehen. Die programmatische Schnittstelle zu ELS verwendet die Unified User Interface (UUI). Diese verwaltet mit dem Sicherheitsausgang SLSUX15 des HSC-Befehls den Zugriff auf die Funktionen auf Basis der RACF- (oder einer vergleichbaren) Autorisierung. Weitere Informationen zum Schutz von SLSUX15 mit RACF finden Sie unter Abschnitt 2.2, „ELS-Konfiguration nach der Installation“.

Anhang A

Prüfliste für sicheres Deployment

1. Verwenden Sie RACF-Schutz (oder einen vergleichbaren Schutz), wie in diesem Sicherheitshandbuch beschrieben.
2. Schränken Sie den Netzwerkzugriff ein. ELS und die verwalteten Bandbibliotheken müssen sich hinter einer Unternehmensfirewall befinden.
3. Schützen Sie den ELS-Netzwerkverkehr gegebenenfalls mit der AT-TLS-Funktion von IBM oder der ELS-XAPI-Sicherheitsfunktion.
4. Wenden Sie alle ELS-PTFs und HOLDDATA an.
5. Kontaktieren Sie den Oracle-Softwaresupport unter `http://www.myoraclesupport.com/`, wenn Sie auf Sicherheitslücken in der Oracle ELS-Software stoßen.

Anhang B

Referenzen

Die ELS-Dokumentation wird aufgeschlüsselt nach ELS-Releases in Bibliotheken gespeichert. Rufen Sie diese auf der Seite "Tape Storage Documentation" auf.

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