StorageTek Enterprise Library Software

セキュリティーガイド

E63468-01

2015 年 3 月

ORACLE

StorageTek Enterprise Library Software
セキュリティーガイド

E63468-01

目次

はじめに

このドキュメントでは、Oracle の StorageTek Enterprise Library Software (ELS) のセキュリティー機能について説明します。

対象読者

このガイドは、StorageTek Enterprise Library Software (ELS) のセキュリティー機能およびセキュアなインストールおよび構成を使用するすべての人を対象としています。

ドキュメントのアクセシビリティー

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility Program の Web サイト (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc) を参照してください。

Oracle Support へのアクセス
サポートをご契約のお客様には、My Oracle Support を通して電子支援サービスを提供しています。詳細情報は (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info) か、聴覚に障害のあるお客様は (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs) を参照してください。

1

概要

このセクションでは、ELS ソフトウェアスイートの概要を示し、アプリケーションセキュリティーの一般原則について説明します。

1.1. 製品の概要

ELS では、次のプラットフォームの Oracle StorageTek メインフレームテープ環境のテープ自動化サポートを提供します。

- IBM z/OS プラットフォーム。ELS では TCP/IP クライアント/サーバーのテープ自動化アーキテクチャーをサポートし、1 つの z/OS LPAR で実行している SMC クライアントソフトウェアが別の z/OS LPAR で実行している HSC/VTCS サーバーソフトウェアと通信できるようにします。
- IBM z/VM プラットフォーム。z/VM システムの ELS VM クライアントソフトウェアは、z/OS LPAR で実行している HSC/VTCS サーバーソフトウェアと通信し、z/VM の仮想および物理テープ処理を自動化します。
- 富士通 MSP/EX プラットフォーム。SMC は、テープ処理が発生しているすべてのホストで実行される必要があります。ELS サーバーコンポーネント (HSC/VTCS) は SMC と同じ MSP/EX ホストで実行することも、個別のリモートホストで実行することもできます。SMC と HSC/VTCS が別々の MSP/EX ホスト上にある場合、クライアントホストからサーバーホストへの要求の送信には TCP/IP が使用されます。リモートの SMC クライアントからの HTTP 要求を受信するためには、サーバーホストで実行されている SMC で HTTP コンポーネントをアクティブ化する必要があります。

ELS クライアント/サーバー通信は、仮想および物理テープボリュームの制御パス要求 (主にマウント/マウント解除要求) を発行するために使用されます。これらの制御パス要求に含まれる情報は、TapePlex 構成とポリシー情報、仮想/物理テープトランスポートユニットのアドレス、および仮想/物理テープボリュームのシリアル番号で構成されます。もっとも重要なことですが、ELS クライアント/サーバー通信に顧客データが含まれることはなく、それらはホスト LPAR を Oracle StorageTek テープトランスポートまたは VSM 仮想テープデバイスに接続する IBM FICON/ESCON データパスインタフェース上を常に伝送します。

このセキュリティーガイドの情報は、すべての ELS リリースに適用されます。このガイドのパート 3 で説明するように、ELS クライアント/サーバーの制御パス通信をセキュリティー保護することが望ましい場合または必要な場合は、そのような保護が可能です。また、このドキュメントでは、さまざまな ELS インストールおよびインストール後アクティビティーのセキュリティー面について説明します。

1.2. 一般的なセキュリティー原則

すべての製品をセキュアに使うために、次の原則が重要になります。

1.2.1. ソフトウェアを最新に維持する

優れたセキュリティー実践の原則の 1 つは、すべてのソフトウェアバージョンとパッチを最新に維持することです。最新の ELS 累積メンテナンスバンドルと個々の PTF および HOLDDATA は、My Oracle Support (MOS) からすべて入手できます。累積メンテナンスバンドルは、最新の ELS 月次レグレッションテストサイクルからのすべての PTF が含まれるように毎月更新されます。累積バンドル内のすべての PTF は、完全なパッケージとしてまとめてテストされています。MOS で ELS 製品のホットトピックのアラートドキュメントにサブスクライブすると、HIPER PTF 電子メール通知を利用できます。顧客は、現在のメンテナンスレベルを維持し、HOLDDATA を最新の状態にし、HIPER 通知のホットトピックのアラートにサブスクライブすることをお勧めします。

1.2.2. ネットワークアクセスを制限する

パフォーマンスおよびセキュリティーのため、ELS 制御パス通信はファイアウォールの背後にある孤立したネットワークにルーティングしてください。ファイアウォールを使用すると、ELS システムへのアクセスが、既知のネットワークに確実に制限され、必要に応じてモニターおよび制限できます。ELS クライアント/サーバー通信に専用のネットワークを使用すると、ほかのアプリケーションとのネットワーク競合が減り、テープシステムのパフォーマンスが向上します。

1.2.3. セキュリティー情報を最新に維持する

Oracle では、ソフトウェアおよびドキュメントを絶えず改善しています。このセキュリティーガイドおよびその他すべての ELS 製品ドキュメントのリビジョンを定期的に確認してください。このドキュメントで参照されているすべての ELS ドキュメントは、Oracle Technical Network のテープストレージ製品のセクションから入手可能です。

2

セキュアなインストール

IBM z/OS の System Authorization Facility (SAF) では、ELS のほとんどのセキュリティー面に不可欠な保護を提供します。一般に、SAF は IBM RACF パッケージまたは同等の機能を使用して実装されます。このセクションでは、RACF ベースの SAF 環境を使用してセキュアな ELS インストールをインストールおよび構成する方法について概要を説明します。

2.1. ELS のインストール

Oracle ドキュメントの *StorageTek Enterprise Library Software の ELS インストール*では、RACF 保護を使用して使用中のバージョンの ELS のインストールおよび構成の方法について説明しています。次のセキュリティー関連のインストールトピックの詳細については、このドキュメントを参照してください。

- 基本ソフトウェアおよび最新の累積メンテナンスバンドルのインストール
- ELS ロードライブラリの APF 許可
- HSC ユーザー出口ライブラリの APF 許可
- SMC JES3 ロードライブラリの APF 許可

2.2. ELS のインストール後の構成

これらの Oracle ドキュメントでは、使用中の ELS バージョンのインストール後構成タスクについて説明します。

- *StorageTek Enterprise Library Software の HSC および VTCS の構成*
- *StorageTek Enterprise Library Software の SMC の構成および管理*
- *StorageTek Enterprise Library Software の ELS プログラミングリファレンス*

次のセキュリティー関連のインストール後トピックの詳細については、これらのドキュメントを参照してください。

- CDS データセットセキュリティーの RACF 保護を定義する
- HSC ユーザー出口 SLSUX15 を使用してコマンド権限およびプログラミングインタフェース権限を定義する

- HSC ユーザー出口 SLSUX14 を使用してボリュームのマウントおよび取り出しのボリュームアクセス権限を定義する
- MVC プールおよびスクラッチサブプール volser 権限を定義する
- リモート HSC サブシステムとの通信の SMC OMVS RACF セグメントを定義する
- VLE アプライアンスとの通信の SMC OMVS RACF セグメントを定義する

3

セキュリティー機能

この章では、ELS で提供される個別のセキュリティーメカニズムについて説明します。

3.1. AT-TLS による ELS のセキュリティー保護 – z/OS のみ

IBM z/OS Application Transparent Transport Layer Security (AT-TLS) 機能は、SSL データ暗号化を使用して z/OS TCP/IP アプリケーションをセキュリティー保護します。AT-TLS の詳細については、IBM の資料『*z/OS Communications Server: IP 構成ガイド*』を参照し、IBM の資料『*z/OS Communications Server: IP 構成解説書*』で AT-TLS ポリシーエージェントに関する情報を参照してください。

SMC と HSC/VTCS の間の ELS クライアント/サーバー通信のセキュリティー保護については、*HSC/SMC クライアント/サーバー z/OS ソリューションにおける AT-TLS の使用の実装例*に関する Oracle のホワイトペーパーで説明されています。このホワイトペーパーは、Oracle Technical Network のテープストレージ製品のセクションで公開されています。詳細な構成情報については、この資料を参照してください。

AT-TLS を使用して ELS をセキュリティー保護する場合、これらの SSL 暗号アルゴリズムのいずれかを使用することをお勧めします。

- SHA-2 ファミリ (SHA-256、SHA-384、SHA-512)
- AES (128 ビット以上)
- RSA (2048 ビット以上)
- Diffie-Hellman (DH) (2048 ビット以上)
- ECC (256 ビット以上)

その他のどの SSL 暗号アルゴリズムも保護が弱いため、ELS では使用しないようにしてください。

注:

VSM 用の StorageTek Virtual Library Extension (VLE) アプライアンスでは、AT-TLS 通信を現在サポートしていません。ELS VLE 通信は AT-TLS を使用してセキュリティー保護しないでください。

3.2. ELS XAPI セキュリティー機能の使用

ELS 7.3 にはクライアント/サーバー通信のための新しい XAPI セキュリティー機能が導入されており、SMC HTTP サーバーではデフォルトとして有効になります。XAPI セキュリティー機能は、XAPI プロトコルの一部として、ELS の内部のみで使用される追加のユーザー認証機能を提供します。XAPI セキュリティー機能を使用するには、ELS クライアントおよびサーバーのセキュリティー資格証明 (ユーザー ID とパスワード) を定義する必要があります。ELS 7.3 TapePlex の操作では、これらのセキュリティー資格証明を使用して XAPI トランザクション (マウント、マウント解除、ボリューム検索、スクラッチなど) をセキュリティー保護します。XAPI セキュリティー資格証明の使用は完全に透過的であり、ユーザーやオペレータがほかに操作を行う必要はありません。XAPI セキュリティー機能の構成の詳細については、『*SMC 7.3 の構成および管理*』を参照してください。

ELS クライアントアプリケーションだけ (SMC および VM クライアント) をホストしている TapePlex の XAPI トランザクションをセキュリティー保護するための望ましい方法は、「AT-TLS による ELS のセキュリティー保護 – z/OS のみ」の説明に従って AT/TLS 機能を使用することです。AT/TLS は、ELS にとって外部にある透過的なトランスポートレイヤー機能です。

ELS 以外のクライアント (オープンシステムクライアント)、または ELS クライアント (SMC および VM クライアント) と ELS 以外のクライアントの混合をホストしている TapePlex をセキュリティー保護するには、ELS 7.3 XAPI セキュリティー機能を使用します。ELS 7.3 XAPI セキュリティー機能のほかに、AT-TLS もこのような環境で使用できますが、ELS 以外のクライアントの XAPI トランザクションはセキュリティー保護されません。

4

開発者のセキュリティーに関する考慮事項

Oracle ドキュメントの *StorageTek Enterprise Library Software の ELS プログラミングリファレンス*では、アプリケーション開発者が使用可能な ELS API について説明しています。ELS のプログラミングインタフェースでは、HSC コマンドセキュリティー出口 SLSUX15 を使用して RACF 許可 (または同等の機能) に基づいて機能へのアクセスを管理する、統合ユーザーインタフェース (UUI) を使用します。RACF を使用して SLSUX15 をセキュリティー保護する詳細については、「ELS のインストール後の構成」を参照してください。

付録A

セキュアな導入のためのチェックリスト

1. このセキュリティーガイドで説明しているとおり、RACF 保護 (または同等の機能) を使用してください。
2. ネットワークアクセスを制限します。ELS および管理対象のテープライブラリは、企業ファイアウォールの内側に配備するようにしてください。
3. 必要に応じて、IBM AT-TLS 機能または ELS XAPI セキュリティー機能を使用して ELS ネットワークトラフィックをセキュリティー保護してください。
4. すべての ELS PTF および HOLDDATA を適用してください。
5. Oracle ELS ソフトウェアの脆弱性を発見した場合は、Oracle ソフトウェアサポート http://www.myoraclesupport.com/ に問い合わせてください。

付録B

参照情報

ELS のドキュメントは、ELS のリリース別に整理されたライブラリに保存されています。テープストレージドキュメントのページから、これにアクセスしてください。

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