StorageTek SL150 Modular Tape Library

セキュリティーガイド

E40924-03

2015 年 6 月

ORACLE

StorageTek SL150 Modular Tape Library
セキュリティーガイド

E40924-03

目次

表の一覧

はじめに

このドキュメントでは、オラクル社の StorageTek SL150 Modular Tape Library 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、オラクル社の StorageTek SL150 Modular Tape Library のセキュアなインストールと構成およびそのセキュリティー機能の使用に関与するすべてのユーザーを対象にしています。

ドキュメントのアクセシビリティについて

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、オラクル社の StorageTek SL150 Modular Tape Library の概要を説明し、テープライブラリのセキュリティーの一般原則について説明します。

製品の概要

StorageTek SL150 Modular Tape Library はオラクル社の 3U から 21U の 19 インチラックマウント型モジュラ自動テープライブラリです。これは、設置されたテープドライブのいずれかを通じて、30 から 300 の LTO テープカートリッジ、1 から 20 の LTO ファイバチャネルドライブまたは SAS テープドライブ、およびブリッジドライブファイバまたは SAS ポート制御パスのストレージ容量を提供します。

セキュリティー

すべてのテープライブラリ製品は、一般的なネットワークまたはユーザーアクセスのない制御されたサーバー環境内で使用するように設計され、ドキュメント化されています。これは、最高の機能を提供し、一般的なインターネットとライブラリを操作する内部エンティティーのどちらの危険からも保護します。

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。

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。2015 年 4 月以降にリリースされた SL150 ファームウェアバージョンは、次のとおりです。

2012 年 6 月 v1.00 (RTA 0.1.0.0.0)
2012 年 9 月 v1.03 (RTA 0.1.0.3.0)
2012 年 10 月 v1.50 (RTA 0.1.5.0.0)
2013 年 1 月 v1.82 (RTA 0.1.8.2.0)
2013 年 8 月 v2.0 (RTA 0.2.0.0.0)

2013年 10 月 v2.01(RTA 0.2.0.1.0)
2014 年 4 月 v2.25 (RTA 0.2.2.5.0)
2015 年 6 月 v2.50 (RTA 0.2.5.0.0)

ネットワークアクセスを制限する

ライブラリは、データセンターのファイアウォールの背後に置いてください。ファイアウォールにより、これらのシステムへのアクセスが、既知のネットワークルートに確実に制限され、必要に応じてモニターおよび制限されます。代わりとして、ファイアウォールルーターは複数の独立したファイアウォールに置き換わるものです。可能な場合、ライブラリに接続を許可されているホストを識別し、ほかのすべてのホストをブロックすることをお勧めします。

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。リリースごとにこのドキュメントのリビジョンを確認してください。

2

セキュアなインストール

このセクションでは、セキュアなインストールの計画プロセスについて説明し、システムの推奨される導入トポロジーをいくつか紹介して、ライブラリをセキュリティー保護する方法を説明します。

環境を理解する

セキュリティーニーズをよりよく理解するには、次の質問を尋ねる必要があります。

保護する必要があるリソースはどれか

本番環境の多くのリソースを保護できます。実現する必要があるセキュリティーのレベルを決定する際に、保護を必要とするリソースを考慮します。

だれからリソースを保護するか

ライブラリは、インターネット上のすべてのユーザーと権限のないイントラネットユーザーから保護する必要があります。

戦略的リソースの保護が失敗した場合に何が起こるか

場合によっては、セキュリティースキームの障害は簡単に検出され、不便なだけと見なされることがあります。あるいは、障害によって、ライブラリを使用する会社や個々のクライアントに多大な損害を与える可能性もあります。各リソースのセキュリティーの影響を理解することで、それらを正しく保護するために役立ちます。

ライブラリのセキュリティー保護

デフォルトで、ライブラリは表2.1「SL150 ネットワークポート」に示すポートを使用します。トラフィックでこれらのポートを使用することを許可し、未使用のすべてのポートをブロックするように、ファイアウォールを構成してください。

表2.1 SL150 ネットワークポート

ポート	種類	説明
22	TCP	SSH CLI アクセス – インバウンドステートフル

ポート	種類	説明
		開発テストおよびデバッグ専用、フィールドでは使用不可
25	TCP	認証なしの SMTP
67	DHCP	クライアント - アウトバウンド
68	DHCP	クライアント - インバウンド
80	HTTP	リモートユーザーインタフェース用 WebLogic ポート
123	NTP	Network Time Protocol (有効な場合)
161	UDP	SNMP ライブラリエージェントリクエスト - インバウンドステートフル
162	UDP	SNMP ライブラリの TRAP および INFORM 通知 - TRAP の場合アウトバウンドステートレス、INFORM の場合アウトバウンドステートフル
465	TCP	SSL または TLS 認証を用いた SMTP
443	HTTPS	リモートユーザーインタフェース用 WebLogic ポート (HTTPS)
546	DHCPv6	IPv6 DHCP クライアント - アウトバウンド
547	DHCPv6	IPv6 DHCP クライアント - インバウンド
33200 - 33500	traceroute	ソフトウェア開発で使用

上記の表に従って、ライブラリで使用するための有効なポート番号が予約または推奨されます。正当なポート番号は数値 1 から始まります (ゼロは正当なポート番号ではありません)。

SNMP を構成する場合、機密性、整合性、および認証機能のため、SNMPv2c より SNMPv3 を使用することを強くお勧めします。

SMTP を構成する場合、SSL や認証なしのオプションではなく、TLS 認証を使用することを強くお勧めします。

インストール構成

このセクションでは、インストール時に実行する必要があるセキュリティー構成の変更について説明します。

ユーザー (admin) パスワードを割り当てる

最初の電源投入時に、ローカルオペレーターパネルでセットアップウィザードが自動的に実行され、基本構成情報が取得されます。これには管理者アカウントのユーザー名とパスワード、ネットワーク設定、およびその他の基本設定が含まれます。

セットアップウィザードが完了するまで、ライブラリは動作可能になりません。

インストールする人がセットアップウィザードルーチンの最初のステップとして入力する必要のあるログインアカウントが、製品出荷とともに提供されています。セットアップウィザードを完了する前に、ユーザーは新しいパスワードを入力する必要があります。

初期セットアップウィザードが完了し、ライブラリの電源が完全に投入されたら、すべてのライブラリ設定について、ブラウザユーザーインタフェース (BUI) からライブラリ構成を追加で変更できます。

パスワード管理を適用する

パスワード長、履歴、複雑さなどの基本的なパスワード管理規則をすべてのパスワードに適用する必要があります。SL150 のパスワードは 8 - 128 文字で、少なくとも 1 つの数字または特殊文字を含む必要があります。デフォルトのパスワードを再利用せず、インストール時に変更してください。

注記:

マスクされた状態で表示される文字の数は、入力された文字の数を正確に示しているわけではありません。

ブラウザ UI 認証

バージョン 2.50 より下位のファームウェアレベルでの CVE-2014-3566 を軽減するために、リモートユーザーインタフェースへのアクセスに使用するブラウザ設定は TLS 1.0 以上に保つように制限してください。バージョン 2.50 のライブラリファームウェアは、SSLv3 に自動ネゴシエーションされません。

3

セキュリティー機能

このセクションでは、製品に備えられている特定のセキュリティーメカニズムについて説明します。

ライブラリはそれ自体を保護するための内部ファイアウォールを備えています。これをライブラリを保護するための唯一のセキュリティー対策にしないでください。ライブラリは、その機能を使用するサーバーからのアクセスのみを許可するセキュリティー保護されたネットワーク上の物理的にセキュリティー保護されたデータセンターに配置します。これらで実行するサーバーとアプリケーションもセキュリティー保護してください。

すべてのユーザーに *Admin* 役割レベルを付与するのではなく、ユーザーアカウントを *operator* 役割レベルに制限するようにしてください。*service* ユーザー役割を適切に使用するようにしてください。必要に応じて *service* ユーザー役割アカウントを作成、有効化、または無効化してください。service の役割には、*admin* の役割と同程度の、*operator* よりも大きな特権があります。

調査のためにライブラリアクティビティーの履歴が必要な場合は、「アクティビティーログ」を確認し、さらに詳しく分析するためにエクスポートすることもできます。ユーザーインタフェースに関するアクティビティーログには、追跡調査のためにユーザーログイン、ホスト、または UI によって開始されたアクションが表示されることもあります。

4

再展開

このセクションでは、顧客データをすべてクリアするためにライブラリを出荷時のデフォルト状態に戻す方法について説明します。

お客様がライブラリを使用停止にする必要がある場合、すべてのお客様の構成情報を削除し、ライブラリを出荷時のデフォルト状態に戻す手順が用意されています。この手順を呼び出すには、ライブラリを「locate」モードにし、前面と背面の位置特定ボタンを 10 秒より長く同時に押し続けたあと、両方のボタンを放します。

位置特定ボタンを押し続けた時間が十分かどうかは、LED の点滅速度がゆっくりした点滅からすばやい点滅に変わることで判断できます。

付録A

セキュアな配備のためのチェックリスト

次のセキュリティーチェックリストに、ライブラリのセキュリティー保護に役立つガイドラインを示します。

1. すべてのユーザーアカウントについてパスワード管理を適用します。
2. 物理的に近接する接続と、SCSI、UI、SNMP などのインタフェース経由の両方にアクセス制御を適用します。
3. ネットワークアクセスを制限します。
   a. ファイアウォールを実装してください。
   b. ファイアウォールが危害を受けないようにしてください。
   c. システムアクセスをモニターしてください。
   d. ネットワーク IP アドレスをチェックしてください。
   e. サービスには、適切なパスワードを必要とする、またはアクセス制御がモニターされるツール (たとえば、ログ情報の自動ダウンロードやその他のアクセスを許可する SDP-2) が含まれている場合があります。
4. Oracle Tape Library の脆弱性を見つけた場合は、Oracle サービス、Oracle Tape Library エンジニアリング、またはアカウント担当者に問い合わせてください。
5. SMTP では SSL のような安全性の低いプロトコルを使ったり、認証なしにしたりする代わりに TLS を使用するようにしてください。
6. SNMP は、V2C 以下の機能ではなく、V3 レベルで設定するようにしてください。

付録B

参照情報

『*SL150 ユーザーズガイド*』は次の場所にあります。

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

SL150 に関連するすべてのドキュメントは、部品番号 E35103-07 のオンラインドキュメントセットに含まれています。