StorageTek T10000D

セキュリティーガイド

E50322-04

2016 年 8 月

ORACLE

StorageTek T10000D
セキュリティーガイド

E50322-04

目次

表の一覧

はじめに

このドキュメントでは、Oracle の StorageTek T10000D 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 T10000D のセキュリティー機能の使用およびセキュアなインストールと構成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

第1章 概要

このセクションでは、StorageTek T10000D テープドライブの概要を説明し、テープドライブ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

T10000D エンタープライズテープドライブは、ファイバーチャネルプロトコル経由でオープンシステム SCSI に、また FICON プロトコル経由でメインフレームに接続されます。T10000D テープドライブはホストとの間でデータを転送し、それをリムーバブル磁気メディア上に格納します。T10000D テープドライブは主に、高いデューティーサイクルと信頼性を要求する企業の顧客向けに、高い信頼性、大容量のバックアップ、アーカイブ、およびデータ処理機能を提供することを目的にしています。この製品は、オプションのデータ暗号化を提供します。顧客には、暗号化機能を有効にするオプションがあります。このテープドライブ製品は、容量およびネイティブテープ速度が拡張されています。さらに、それとともにデータ管理機能も追加されました。

T10000D の容量および性能

T10000D テープドライブは、最大 8.5T バイトの容量と 252M バイト/秒のネイティブテープ速度を備えています。

セキュリティー

T10000D テープドライブは、制御されたハードウェア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。テープドライブは常に制御されたデータセンター内に置き、一般にテープライブラリの内部に置きます。場合によっては顧客はラックマウントバージョンを使用しますが、これはまれです。制御されたデータセンターも、顧客の独自のセキュリティーポリシーによって保護されているファイアウォール内に置きます。これにより、最適な機能、および一般的なインターネットとテープドライブを操作する内部のエンティティーの両方の危険からの保護が提供されます。

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。このドキュメント全体にわたって、次のソフトウェアレベルを想定しています。

T10000D 4.XX.1XX

ネットワークアクセスを制限する

テープドライブは、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経路に制限されることが保証され、これは必要に応じてモニターおよび制限できます。単一のファイアウォールルーターを複数の独立したファイアウォールの代わりに使用することもできます。可能な場合は、テープドライブへの接続が許可されているホストを識別し、その他のすべてのホストをブロックすることをお勧めします。

最新のセキュリティー情報を維持する

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

第2章 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と構成の計画および実装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、テープ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何ですか。

本稼動環境の多くのリソースを保護できます。提供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しますか。

テープドライブは、インターネット上のすべてのユーザーから保護する必要があります。ただし、企業のイントラネット上の従業員からテープドライブを保護すべきですか。

戦略的リソースの保護が失敗した場合、何が起こりますか。

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、障害によって会社やテープドライブを使用する個々のクライアントに多大な損害を与える可能性がある場合もあります。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。

テープドライブをセキュリティー保護する

デフォルトで、テープドライブは次の表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。テープドライブは、IPv6 と IPv4 をサポートします。

表2.1 使用されるネットワークポート

ポート	T10000D
22 TCP - SSH VOP	X
22 TCP - SFTP	X
161 UDP - SNMPV1 テープドライブエージェントリクエスト - インバウンドステートフル	X
162 UDP - SNMPV1 テープドライブの 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	X
23 TCP - TELNET	
21 TCP - FTP	
9842 TCP - EPT	
3331 OKM - チャレンジおよびルート CA サービス	X
3332 OKM – 登録。サイバー強度は AES256	X
3334 OKM – 暗号化鍵交換。サイバー強度は AES256	X
3335 OKM – クラスター検出。サイバー強度は AES256	X

ポート 21 および 23 は、T10000D の顧客には無効化されます。顧客がセキュアでない TELNET やセキュアでない FTP、またはその両方にアクセスする必要がある場合は、VOP 構成オプションを使用できます。

Virtual Operator Panel (VOP) アプリケーションのインストール

VOP は、テープドライブと同じ保護されているネットワークインフラストラクチャー内にあるシステムにのみインストールしてください。VOP がインストールされているシステムには、テープドライブへの制限されたアクセスを保証するために、顧客アクセス制御を適用してください。VOP で使用されるポートについては、表2.1「使用されるネットワークポート」 を参照してください。

Web 起動の VOP インストール手順については、次の VOP ユーザーガイドを参照してください。

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

インストール後の構成

このセクションでは、インストール後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ます。

お客様の admin アカウントパスワードは、サイトでお客様が変更する必要があり、お客様が所有します。パスワードのセキュリティーは Oracle の標準を満たします。テープドライブの寿命を通じて、無限の数のパスワードを使用できます。admin パスワードを忘れた場合は、リセットできます。最初のパスワードは、テープドライブと一緒に発送されたデフォルトのパスワードです。

パスワード管理を適用する

パスワード長や複雑さなどの基本的なパスワード管理規則を管理者パスワードに適用する必要があります。

パスワード管理規則には、次の各規則の少なくとも 1 つが必要です。

- 8 文字から 16 文字の長さにする
- 小文字 (a から z)
- 大文字 (A から Z)
- 10 進数 (0 から 9)
- 特殊文字 (.?;:"{}[]()!@#$%&, ...)

3

第3章 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。

T10000D テープドライブはセキュアなチャネルで、Oracle 鍵管理システムと通信します。T10000D は Virtual Operator Panel に SSH および SFTP を通知するため、顧客の TELNET および FTP は無効になります。これらをテープドライブ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。理想的には、テープドライブは、その機能を利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のある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てください。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。さらに、顧客にはテープドライブのセキュリティーレベルをほかのレベルに高めるオプションもあります。オプションの 1 つは、データを暗号化することです。

付録A

付録A セキュアな導入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、テープドライブ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. パスワード管理を適用します。
2. 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てはいけません。
   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。
4. Oracle テープドライブの脆弱性に遭遇した場合は、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。

付録B

付録B 参照情報

VOP ユーザーガイドは次からアクセスできます。

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