StorageTek T10000D

Sicherheitshandbuch

E50326-04

August 2016

ORACLE

StorageTek T10000D
Sicherheitshandbuch

E50326-04

Inhalt

Tabellen

Vorwort

In diesem Dokument werden die Sicherheitsfunktionen des StorageTek T10000D von Oracle beschrieben.

Zielgruppe

Dieses Handbuch richtet sich an Personen, die an der Verwendung der Sicherheitsfunktionen und der sicheren Installation und Konfiguration von StorageTek T10000D beteiligt sind.

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

Kapitel 1. Überblick

Dieser Abschnitt enthält einen Überblick über die StorageTek T10000D-Bandlaufwerke und erläutert die allgemeinen Grundsätze der Bandlaufwerkssicherheit.

Produktüberblick

Das T10000D Enterprise-Bandlaufwerk kann sowohl über das Open-Systems-SCSI-over-Fibre-Channel-Protokoll als auch über Mainframe-over-FICON-Protokoll angeschlossen werden. Das T10000D-Bandlaufwerk überträgt Daten an einen und von einem Host und speichert diese auf einem magnetischen Wechselmedium. Das T10000D-Bandlaufwerk soll in erster Linie hohe Verlässlichkeit, Backup mit hoher Kapazität, Archivierungs- und Datenverarbeitungsmöglichkeiten für Firmenkunden bereitstellen, die Arbeitszyklen mit hoher Einschaltdauer und Verlässlichkeit benötigen. Das Produkt bietet optionale Datenverschlüsselung. Der Kunde hat die Möglichkeit, die Verschlüsselungsfunktion zu aktivieren. Das Bandlaufwerk wurde im Hinblick auf Kapazität und native Bandgeschwindigkeit verbessert. Außerdem wurden Funktionen zur Datenverwaltung hinzugefügt.

Speicherkapazität und Leistungspotential des T10000D

Das T10000D-Bandlaufwerk verfügt über eine Speicherkapazität bis zu 8,5 TB und eine native Bandgeschwindigkeit von 252 MB pro Sekunde.

Sicherheit

Das T10000D-Bandlaufwerk ist zur Verwendung innerhalb einer kontrollierten Hardwareumgebung konzipiert und dokumentiert. Bandlaufwerke befinden sich immer in einem kontrollierten Data Center und im Allgemeinen innerhalb einer Bandbibliothek. In einigen Fällen verwenden Kunden eine rackmontierte Version, dies ist jedoch selten. Das kontrollierte Data Center befindet sich ebenfalls innerhalb einer Firewall, die mit den eigenen Sicherheitsrichtlinien des Kunden geschützt wird. Dies bietet optimale Funktionalität und Schutz vor Gefährdung sowohl aus dem Internet im Allgemeinen als auch von der internen Entity, die das Bandlaufwerk betreibt.

Allgemeine Sicherheitsgrundsätze

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

Software immer auf dem neuesten Stand halten

Einer der Grundsätze für einen sicheren Betrieb besteht darin, alle Softwareversionen und Patches auf dem neuesten Stand zu halten. Im ganzen Dokument wird von folgenden Softwareebenen ausgegangen:

T10000D 4.XX.1XX

Netzwerkzugriff einschränken

Das Bandlaufwerk muss sich hinter einer Data Center-Firewall befinden. Die Firewall bietet die Gewähr, dass der Zugriff auf diese Systeme auf eine bekannte Netzwerkroute beschränkt ist, die gegebenenfalls überwacht und eingeschränkt werden kann. Als Alternative kann ein Firewallrouter anstelle von mehreren, unabhängigen Firewalls verwendet werden. Es wird empfohlen, die Hosts zu identifizieren, die auf das Bandlaufwerk zugreifen können, und alle anderen Hosts zu blockieren, sofern dies möglich ist.

Sicherheitsinformationen immer auf dem neuesten Stand halten

Oracle nimmt fortwährend Verbesserungen an Software und Dokumentation vor. Prüfen Sie dieses Dokument mit jeder neuen Version auf Änderungen.

2

Kapitel 2. Sichere Installation

In diesem Abschnitt werden die Schritte bei der Planung und Implementierung einer sicheren Installation und Konfiguration aufgeführt. Außerdem werden verschiedene empfohlene Deployment-Topologien für die Systeme beschrieben und wird erläutert, wie Sie eine Bandbibliothek sichern.

Ihre Umgebung

Zum besseren Verständnis der Sicherheitsanforderungen müssen die folgenden Fragen gestellt werden:

Welche Ressourcen müssen geschützt werden?

Viele Ressourcen in der Produktionsumgebung können geschützt werden. Bedenken Sie, welche Ressourcen geschützt werden müssen, wenn Sie die erforderliche Sicherheitsstufe festlegen.

Vor wem müssen die Ressourcen geschützt werden?

Das Bandlaufwerk muss vor jedem Benutzer im Internet geschützt werden. Muss das Bandlaufwerk jedoch auch vor den Mitarbeitern im Intranet Ihres Unternehmens geschützt werden?

Was geschieht, wenn der Schutz bei strategischen Ressourcen versagt?

In einigen Fällen kann ein Fehler im Sicherheitsschema einfach entdeckt und nur als eine Unannehmlichkeit eingestuft werden. In anderen Fällen kann ein Fehler großen Schaden für Unternehmen oder einzelne Kunden anrichten, die das Bandlaufwerk verwenden. Wenn Sie die Sicherheitsauswirkungen jeder Ressource kennen, können Sie diese richtig schützen.

Sichern des Bandlaufwerks

Standardmäßig verwendet das Bandlaufwerk die in der folgenden Tabelle aufgeführten Ports. Die Firewall muss so konfiguriert sein, dass diese Ports zum Datenaustausch verwendet

werden können, und dass alle nicht verwendeten Ports blockiert sind. Die Bandlaufwerke unterstützen IPv6 und IPv4.

Tabelle 2.1. Verwendete Netzwerkports

Port	T10000D
22 tcp - SSH VOP	X
22 tcp - SFTP	X
161 udp - SNMPV1 Anforderungen des Bandlaufwerk-Agents - eingehend, zustandsbehaftet	X
162 udp - SNMPV1 Bandlaufwerk-Traps und Benachrichtigungen zur Information - ausgehend, zustandslos für Traps, ausgehend, zustandsbehaftet für Informationen	X
23 tcp - TELNET	
21 tcp - FTP	
9842 tcp - EPT	
3331 OKM - Challenge- und Root-CA-Service	X
3332 OKM – Enrollment. Cyber-Sicherheit ist AES256	X
3334 OKM – Verschlüsselungsschlüsselaustausch. Cyber-Sicherheit ist AES256	X
3335 OKM – Cluster-Discovery. Cyber-Sicherheit ist AES256	X

Die Ports 21 und 23 werden für T10000D-Kunden deaktiviert. Für Kunden, die Zugriff auf eine nicht sichere TELNET-Verbindung, einen nicht sicheren FTP-Server oder beides benötigen, besteht die Möglichkeit einer Konfiguration als Virtual Operator Panel (VOP).

Installieren der Virtual Operator Panel-(VOP-)Anwendung

VOP darf nur in Systemen installiert werden, die sich innerhalb derselben (durch eine Firewall) geschützten Netzwerkinfrastruktur befinden wie das Bandlaufwerk. Kundenzugriffskontrolle muss für die Systeme erzwungen werden, auf denen VOP installiert ist, um den eingeschränkten Zugriff auf das Bandlaufwerk zu gewährleisten. Informationen zu Ports, die von VOP verwendet werden, finden Sie unter Tabelle 2.1, „Verwendete Netzwerkports“.

In dem folgenden VOP-Benutzerhandbuch finden Sie Anweisungen zum Starten der VOP-Installation im Web.

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

Konfiguration nach Abschluss der Installation

In diesem Abschnitt werden die Änderungen an der Sicherheitskonfiguration dokumentiert, die nach der Installation vorgenommen werden müssen.

Zuweisen des Benutzer-(Admin-)Passworts

Das Passwort des benutzerdefinierten Admin-Kontos muss vom Kunden in der Site vorgenommen werden. Es gehört dem Kunden. Die Passwortsicherheit entspricht den Oracle-Standards. Eine unbegrenzte Anzahl von Passwörtern ist zur Verwendung während des Lebenszyklus des Bandlaufwerks verfügbar. Ein vergessenes Admin-Passwort kann zurückgesetzt werden. Das erste Passwort ist das Standardpasswort, das mit dem Bandlaufwerk verschickt wird.

Durchsetzen der Passwortverwaltung

Grundlegende Regeln zur Passwortverwaltung, wie Passwortlänge und Komplexität müssen für das Administratorpasswort angewendet werden.

Unter den Regeln für die Passwortverwaltung muss mindestens eine der folgenden Regeln beachtet werden.

- Es muss eine Länge zwischen 8 und 16 Zeichen haben.
- Kleinbuchstaben (a-z)
- Großbuchstaben (A-Z)
- Dezimalziffer (0-9)
- Sonderzeichen (.?;:"{}[]()!@#$%&, ...)

3

Kapitel 3. Sicherheitsfunktionen

In diesem Abschnitt werden die spezifischen Sicherheitsverfahren beschrieben, die das Produkt bietet.

Das T10000D-Bandlaufwerk tauscht über einen sicheren Kanal mit dem Oracle Key Management System Daten aus. Das T10000D sendet über SSH- und SFTP-Verbindungen Daten an das Virtual Operator Panel (VOP). Verbindungen über TELNET und FTP-Server werden für unsere Kunden deaktiviert. Dies sollte jedoch nicht die einzige Sicherheitsmaßnahme zum Schutz des Bandlaufwerks sein. Im Idealfall sollten sich alle Bandlaufwerke in einem physisch gesicherten Data Center befinden, das auch über ein gesichertes Netzwerk verfügt, auf das nur von den Servern zugegriffen werden kann, die diese Funktionalität nutzen. Diese Server und die auf ihnen ausgeführten Anwendungen müssen ebenfalls gesichert sein. Darüber hinaus ist es dem Kunden möglich, die Sicherheit des Bandlaufwerks um eine weitere Stufe zu erhöhen. Eine Möglichkeit besteht darin, alle Daten zu verschlüsseln.

Anhang A

Anhang A. Prüfliste für sicheres Deployment

Die folgende Sicherheitsprüfliste enthält Richtlinien, mit denen Sie Ihr Bandlaufwerk besser sichern können:

1. Setzen Sie die Passwortverwaltung durch.
2. Setzen Sie Zugriffskontrollen durch.
3. Schränken Sie den Netzwerkzugriff ein.
   a. Implementieren Sie eine Firewall.
   b. Die Firewall darf nicht gefährdet sein.
   c. Der Systemzugriff muss überwacht werden.
   d. Netzwerk-IP-Adressen müssen geprüft werden.
4. Wenn Sie Sicherheitslücken in Bandlaufwerken von Oracle feststellen, wenden Sie sich an Ihren Vertreter von Oracle Services, Ihren Vertreter der Engineering-Abteilung der Bandbibliothek von Oracle oder den Oracle-Vertreter für Ihr Benutzerkonto.

Anhang B

Anhang B. Referenzen

Sie erhalten das VOP-Benutzerhandbuch unter folgender Adresse:

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