StorageTek SL150 Modular Tape Library

Sicherheitshandbuch

E40927-03

Juni 2015

ORACLE

StorageTek SL150 Modular Tape Library
Sicherheitshandbuch

E40927-03

Inhalt

Tabellen

Vorwort

In diesem Dokument werden die Sicherheitsfunktionen von StorageTek SL150 Modular Tape Library von Oracle beschrieben.

Zielgruppe

Dieses Handbuch richtet sich an Personen, die an der sicheren Installation und Konfiguration von StorageTek SL150 Modular Tape Library von Oracle und der Verwendung der Sicherheitsfunktionen 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

Überblick

Dieser Abschnitt enthält einen Überblick über die StorageTek SL150 Modular Tape Library von Oracle und erläutert die allgemeinen Grundsätze der Sicherheit von Bandbibliotheken.

Produktüberblick

Die StorageTek SL150 Modular Tape Library ist eine in 19-Zoll-Racks montierte modulare automatisierte Bandbibliothek mit 3 bis 21 Höheneinheiten von Oracle Corporation. Sie hat eine Speicherkapazität von 30 bis 300 LTO-Bandkassetten, unterstützt 1 bis 20 LTO-Fibre Channel-Laufwerke oder SAS-Bandlaufwerke und über eines der installierten Bandlaufwerke einen Fibre- oder SAS-Portkontrollpfad für ein Laufwerk mit Brücke.

Sicherheit

Alle Bandlaufwerke sind zur Verwendung in einer kontrollierten Serverumgebung ohne allgemeinen Netzwerk- oder Benutzerzugriff konzipiert und dokumentiert. Dies gewährleistet optimale Funktionalität und Schutz vor Gefährdung sowohl aus dem Internet im Allgemeinen als auch von der internen Entity, die die Bibliothek betreibt.

Allgemeine Sicherheitsgrundsätze

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

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. Folgende SL150-Firmwareversionen wurden seit April 2015 herausgegeben:

Juni 2012 v1.00 (RTA 0.1.0.0.0)
September 2012 v1.03 (RTA 0.1.0.3.0)
Oktober 2012 v1.50 (RTA 0.1.5.0.0)
Januar 2013 v1.82 (RTA 0.1.8.2.0)
August 2013 v2.0 (RTA 0.2.0.0.0)
Oktober 2013 v2.01(RTA 0.2.0.1.0)
April 2014 v2.25 (RTA 0.2.2.5.0)
Juni 2015 v2.50 (RTA 0.2.5.0.0)

Einschränkung des Netzwerkzugriffs

Die Bibliothek 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, wenn möglich die Hosts zu identifizieren, die auf die Bibliothek zugreifen können, und alle anderen Hosts zu blockieren.

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

Sichere Installation

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

Ihre Umgebung

Damit Sie die Sicherheitsanforderungen besser verstehen, müssen die folgenden Fragen gestellt werden.

Welche Ressourcen müssen geschützt werden?

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

Vor wem müssen die Ressourcen geschützt werden?

Die Bibliothek muss vor jedem Benutzer im Internet und nicht befugten Intranetbenutzern 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 die Bibliothek verwenden. Wenn Sie die Sicherheitsauswirkungen jeder Ressource kennen, können Sie diese richtig schützen.

Sichern der Bibliothek

Standardmäßig verwendet die Bibliothek Ports, die in Tabelle 2.1, „SL150-Netzwerkports“ aufgeführt werden. Die Firewall muss so konfiguriert sein, dass der Datenverkehr diese Ports verwenden kann und dass alle nicht verwendeten Ports blockiert sind.

Tabelle 2.1. SL150-Netzwerkports

Port	Typ	Beschreibung
22	TCP	SSH-CLI-Zugriff - eingehend, zustandsbehaftet

Port	Typ	Beschreibung
		Nur für Tests und Debugging in der Entwicklung, im normalen Betrieb nicht verfügbar
25	TCP	SMTP ohne Authentifizierung
67	DHCP	Client - ausgehend
68	DHCP	Client - eingehend
80	HTTP	WebLogic-Port für Remote-Benutzerschnittstelle
123	NTP	Network Time Protocol (wenn aktiviert)
161	UDP	Anforderungen von SNMP-Bibliotheks-Agent - eingehend, zustandsbehaftet
162	UDP	SNMP-Bibliotheks-Traps und Benachrichtigungen zur Information - ausgehend, zustandslos für Traps, ausgehend, zustandsbehaftet für Informationen
465	TCP	SMTP mit SSL- oder TLS-Authentifizierung
443	HTTPS	WebLogic-Port für Remote-Benutzerschnittstelle für HTTPS
546	DHCPv6	IPv6 DHCP-Client - ausgehend
547	DHCPv6	IPv6 DHCP-Client - eingehend
33200-33500	TRACEROUTE	Verwendung bei Softwareentwicklung

Für die Bibliothek können entweder reservierte oder in der obigen Liste empfohlene Portnummern ausgewählt werden. Gültige Portnummern beginnen bei der Zahl 1, da 0 (null) keine gültige Portnummer ist.

Bei der Konfiguration von SNMP wird unbedingt empfohlen, SNMPv3 wegen seiner Vertraulichkeits-, Integritäts- und Authentifizierungsmöglichkeiten und nicht SNMPv2c zu verwenden.

Bei der Konfiguration von SMTP wird unbedingt empfohlen, TLS-Authentifizierung und nicht SSL oder keine Authentifizierung zu verwenden.

Installationskonfiguration

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

Zuweisen des Benutzer-(Admin-)Passworts

Beim ersten Einschalten wird automatisch ein Setupassistent im lokalen Bedienfeld ausgeführt, um grundlegende Konfigurationsinformationen abzurufen. Dazu gehören Benutzername und Kennwort des Administratorkontos, Netzwerkeinstellungen sowie andere grundlegende Einstellungen.

Die Bibliothek ist erst betriebsbereit, nachdem der Setupassistent abgeschlossen ist.

Ein Anmeldekonto wird mit der Produktlieferung bereitgestellt, das als erster Schritt in der Routine des Setupassistenten eingegeben werden muss. Der Benutzer muss dann ein neues Passwort eingeben, bevor der Setupassistent abgeschlossen wird.

Sobald der Assistent für das anfängliche Setup abgeschlossen wurde und die Bibliothek vollständig eingeschaltet ist, können weitere Änderungen an der Bibliothekskonfiguration über die Browserbenutzeroberfläche (Browser Unser Interface, BUI) für alle Bibliothekseinstellungen vorgenommen werden.

Durchsetzen der Passwortverwaltung

Grundlegende Regeln zur Passwortverwaltung, wie Passwortlänge, Historie und Komplexität müssen für alle Passwörter angewendet werden. SL150-Kennwörter müssen zwischen 8 und 128 Zeichen lang sein und mindestens eine Zahl oder ein Sonderzeichen enthalten. Das Standardpasswort muss während der Installation geändert werden und kann nicht wieder verwendet werden.

Hinweis:

Die Anzahl der maskiert angezeigten Zeichen gibt nicht die genaue Anzahl der eingegebenen Zeichen wieder.

Authentifizierung der Browserbenutzeroberfläche

Begrenzen Sie die Browsereinstellungen, die für den Zugriff auf die Remote-Benutzeroberfläche verwendet werden, auf TLS 1.0 oder höher, um CVE-2014-3566 für Firmware unter Version 2.50 herabzusetzen. Die Bibliotheksfirmware wird in Version 2.50 nicht selbstständig auf SSLv3 herabgesetzt.

3

Sicherheitsfunktionen

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

Die Bibliothek enthält eine interne Firewall zur ihrem eigenen Schutz. Dies sollte jedoch nicht die einzige Sicherheitsmaßnahme zum Schutz der Bibliothek sein. Es wird empfohlen, dass die Bibliothek in einem physisch gesicherten Data Center in einem gesicherten Netzwerk enthalten ist, auf das nur von Servern zugegriffen werden kann, die diese Funktionalität verwenden. Diese Server und die auf ihnen ausgeführten Anwendungen müssen ebenfalls gesichert sein.

Es sollte nicht für alle Benutzer die Rolle *Admin* vergeben werden, sondern Benutzerkonten sollten auf die Rollenebene *Operator* beschränkt sein. Die Benutzerrolle *Service* muss ebenfalls ordnungsgemäß verwendet werden. Erstellen, aktivieren oder deaktivieren Sie *Service*-Benutzerrollenkonten nach Bedarf. Servicerollen haben mehr Berechtigungen als *Operator*. Tatsächlich entsprechen sie nahezu der Rolle *Admin*.

Wenn zu Untersuchungszwecken eine Historie der Bibliotheksaktivität erforderlich ist, kann das Aktivitätslog geprüft und zur weiteren Analyse exportiert werden. Anhand des Aktivitätslogs auf der Benutzeroberfläche können Benutzeranmeldungen sowie von Host oder Benutzeroberfläche initiierte Aktionen nachvollzogen werden.

4

Erneutes Deployment

In diesem Abschnitt wird beschrieben, wie die Bibliothek in einen werkseitigen Standardstatus zurückversetzt wird, um alle Kundendaten zu löschen.

Falls ein Kunde eine Bibliothek außer Betrieb setzen muss, gibt es eine Prozedur, die alle benutzerdefinierten Konfigurationsinformationen und alle Logdateien entfernt und die Bibliothek wieder in einen werkseitigen Standardstatus versetzt. Diese Prozedur wird aufgerufen, indem die Bibliothek in einen "locate"-Modus versetzt wird und die vorderen und rückwärtigen Locate-Tasten dann gleichzeitig länger als 10 Sekunden gedrückt gehalten werden. Anschließend beide Tasten loslassen.

Wenn die Locate-Taste lange genug gedrückt wurde, wird dies dadurch angezeigt, dass die LED-Lampe nicht mehr langsam, sondern schnell blinkt.

Anhang A

Prüfliste für sicheres Deployment

Die folgende Sicherheitsprüfliste enthält Richtlinien, mit denen Sie die Bibliothek sichern können:

1. Setzen Sie die Kennwortverwaltung für alle Benutzerkonten durch.
2. Setzen Sie Zugriffskontrollen durch, und zwar sowohl physische Näherungskontrollen als auch über Schnittstellen wie SCSI, UI, SNMP usw.
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.
   e. Services verfügen möglicherweise über Tools, für die ordnungsgemäße Kennwörter oder Zugriffskontrollen überwacht werden müssen (Beispiel: SDP-2, um das automatische Herunterladen von Loginformationen oder andere Zugriffe zu ermöglichen)
4. Wenn Sie Sicherheitslücken in Bandbibliotheken 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.
5. Für SMTP muss TLS verwendet werden und nicht ein schwächeres Protokoll wie SSL oder gar kein Protokoll.
6. SNMP muss mit V3 statt mit V2C oder einer geringeren Schutzstufe eingerichtet werden.

Anhang B

Referenzen

SL150-Benutzerhandbuch in:

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

Die gesamte Dokumentation zu SL150 finden Sie im Online-Dokumentationsset mit der Teilenummer E35103-07.