

StorageTek Linear Tape File System, Library Edition

Sicherheitshandbuch

Version 1

E40934-02

Juli 2016

StorageTek Linear Tape File System, Library Edition
Sicherheitshandbuch

E40934-02

Copyright © 2013, 2016, Oracle und/oder verbundene Unternehmen. Alle Rechte vorbehalten.

Diese Software und zugehörige Dokumentation werden im Rahmen eines Lizenzvertrages zur Verfügung gestellt, der Einschränkungen hinsichtlich Nutzung und Offenlegung enthält und durch Gesetze zum Schutz geistigen Eigentums geschützt ist. Sofern nicht ausdrücklich in Ihrem Lizenzvertrag vereinbart oder gesetzlich geregelt, darf diese Software weder ganz noch teilweise in irgendeiner Form oder durch irgendein Mittel zu irgendeinem Zweck kopiert, reproduziert, übersetzt, gesendet, verändert, lizenziert, übertragen, verteilt, ausgestellt, ausgeführt, veröffentlicht oder angezeigt werden. Reverse Engineering, Disassemblierung oder Dekompilierung der Software ist verboten, es sei denn, dies ist erforderlich, um die gesetzlich vorgesehene Interoperabilität mit anderer Software zu ermöglichen.

Die hier angegebenen Informationen können jederzeit und ohne vorherige Ankündigung geändert werden. Wir übernehmen keine Gewähr für deren Richtigkeit. Sollten Sie Fehler oder Unstimmigkeiten finden, bitten wir Sie, uns diese schriftlich mitzuteilen.

Wird diese Software oder zugehörige Dokumentation an die Regierung der Vereinigten Staaten von Amerika bzw. einen Lizenznehmer im Auftrag der Regierung der Vereinigten Staaten von Amerika geliefert, dann gilt Folgendes:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Diese Software oder Hardware ist für die allgemeine Anwendung in verschiedenen Informationsmanagementanwendungen konzipiert. Sie ist nicht für den Einsatz in potenziell gefährlichen Anwendungen bzw. Anwendungen mit einem potenziellen Risiko von Personenschäden geeignet. Falls die Software oder Hardware für solche Zwecke verwendet wird, verpflichtet sich der Lizenznehmer, sämtliche erforderlichen Maßnahmen wie Fail Safe, Backups und Redundancy zu ergreifen, um den sicheren Einsatz dieser Software oder Hardware zu gewährleisten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keinerlei Haftung für Schäden, die beim Einsatz dieser Software oder Hardware in gefährlichen Anwendungen entstehen.

Oracle und Java sind eingetragene Marken von Oracle und/oder ihren verbundenen Unternehmen. Andere Namen und Bezeichnungen können Marken ihrer jeweiligen Inhaber sein.

Intel und Intel Xeon sind Marken oder eingetragene Marken der Intel Corporation. Intel und Intel Xeon sind Marken oder eingetragene Marken der Intel Corporation. Alle SPARC-Marken werden in Lizenz verwendet und sind Marken oder eingetragene Marken der SPARC International, Inc. UNIX ist eine eingetragene Marke von The Open Group.

Diese Software oder Hardware und die Dokumentation können Zugriffsmöglichkeiten auf oder Informationen über Inhalte, Produkte und Serviceleistungen von Dritten enthalten. Sofern nicht ausdrücklich in einem Vertrag mit Oracle vereinbart, übernehmen die Oracle Corporation und ihre verbundenen Unternehmen keine Verantwortung für Inhalte, Produkte und Serviceleistungen von Dritten und lehnen ausdrücklich jegliche Art von Gewährleistung diesbezüglich ab. Sofern nicht ausdrücklich in einem Vertrag mit Oracle vereinbart, übernehmen die Oracle Corporation und ihre verbundenen Unternehmen keine Verantwortung für Verluste, Kosten oder Schäden, die aufgrund des Zugriffs oder der Verwendung von Inhalten, Produkten und Serviceleistungen von Dritten entstehen.

Inhalt

Vorwort	5
Zielgruppe	5
Barrierefreie Dokumentation	5
1. Überblick	7
Produktüberblick	7
Sicherheit	7
Physisch	8
Netzwerk	8
Benutzerzugriff	8
Allgemeine Sicherheitsgrundsätze	8
Software immer auf dem neuesten Stand halten	8
Einschränkung des Netzwerkzugriffs	8
Sicherheitsinformationen immer auf dem neuesten Stand halten	9
2. Sichere Installation	11
Ihre Umgebung	11
Welche Ressourcen müssen geschützt werden?	11
Vor wem müssen die Ressourcen geschützt werden?	11
Was geschieht, wenn der Schutz bei strategischen Ressourcen versagt?	11
Installieren von Linear Tape File System – Library Edition (LTFS-LE)	11
Konfiguration nach Abschluss der Installation	12
Zuweisen des Benutzer-(Admin-)Passworts	12
Durchsetzen der Passwortverwaltung	12
3. Sicherheitsfunktionen	13
A. Prüfliste für sicheres Deployment	15
B. Referenzen	17

Vorwort

In diesem Dokument werden die Sicherheitsfunktionen von StorageTek Linear Tape File System, Library Edition (LTFS-LE) von Oracle beschrieben.

Zielgruppe

Dieses Handbuch richtet sich an Personen, die an der Verwendung von Sicherheitsfunktionen und der sicheren Installation und Konfiguration von LTFS-LE 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.

Kapitel 1. Überblick

Dieser Abschnitt enthält einen Überblick über LTFS-LE und erläutert die allgemeinen Grundsätze für dessen Sicherheit.

Produktüberblick

Heute besteht bei Bandspeichern die Gefahr, dass sie vollständig dem Backup- und Archivierungsmarkt untergeordnet werden, selbst wenn Kunden eine kostenwirksamere Speicherplattform fordern, die für die Nearline-Speicherung verwendet werden könnte, weil Probleme bei Verwendbarkeit und Performance festgestellt wurden. Die Pionierarbeit der StorageTek- und Sun-Entwickler zur Abwehr dieses Angriffs der Datenträgerhersteller hat schließlich 2010 zur Einführung von Linear Tape File System (LTFS) für einzelne Bandlaufwerke geführt. Zuerst als Open Source-Spezifikation von IBM und dem LTO-Konsortium freigegeben, lässt LTFS zu, dass ein einzelnes Laufwerk wie ein USB-Stick oder Speicherstick behandelt werden kann. Diese neue Darstellung hat die Schwierigkeiten der Bandspeicherung abstrahiert und sie benutzerfreundlicher gestaltet. Außerdem hat sie neue Möglichkeiten geschaffen, den Wert des Bandes zu verbessern, weil Branchen, bei denen der Speicher portierbar sein muss, jetzt über eine kostengünstige Speicherplattform verfügen.

Oracle hat die Spezifikation mit ihrem T10000C-Bandlaufwerk übernommen. LTFS für ein einzelnes Laufwerk ist jedoch nur von begrenztem Wert sowohl für den Kunden als auch für Oracle. Wenn LTFS auf eine ganze Bibliothek erweitert wird, können Kunden im Wesentlichen tausende von USB-Sticks verwenden. Sie können Datenmengen im Petabyte-Bereich in ihrer Bibliothek nur mit einer Explorer-Basisbenutzeroberfläche verwalten. Dadurch wird das Band nicht nur benutzerfreundlicher, sondern Benutzer können auch beruhigt sein, weil alle Inhalte in einem offenen Format geschrieben werden. Kunden sind nicht auf ihre Backupanwendung oder andere proprietäre Formate angewiesen. Außerdem werden die Vorteile der Portabilität wesentlich erweitert. Schließlich ermöglicht LTFS – Library Edition (LTFS-LE), dass zukünftige Oracle-Anwendungen und -Middleware das Band als Speicherformat verwenden, indem ein einzelner, einfacher Zugriffspunkt bereitgestellt wird.

Sicherheit

Es gibt drei Aspekte für die LTFS-LE-Sicherheit: Physisch, Netzwerk und Benutzerzugriff.

Physisch

LTFS-LE muss auf einem Standalone-Server im Data Center eines Unternehmens installiert sein. Der physische Zugriff auf den Server unterliegt den Unternehmensrichtlinien des Kunden.

Netzwerk

LTFS-LE muss in einem internen, durch Firewall geschützten Netzwerk des Kunden hinzugefügt oder konfiguriert werden. Dieses Netzwerk benötigt SSH- und SNMP-Zugriff auf Bibliotheken, in denen auf Daten zugegriffen wird.

Benutzerzugriff

Der Zugriff auf die LTFS-LE-Anwendung wird durch Benutzername- und Passwortauthentifizierung kontrolliert. Diese Authentifizierung wird bei der Erstinstallation vom Kunden eingerichtet. Die Passwörter müssen den Oracle-Standardanforderungen entsprechen.

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. Dieses Dokument ist für die folgende Softwareebene ausgelegt:

LTFS-LE Version 1.0 oder höher

Hinweis:

Es wird außerdem erwartet, dass Bibliotheken, Bibliothekssoftware und Laufwerke den mindestens erforderlichen Firmwareversionsebenen entsprechen, die für die LTFS-LE-Anwendung gelten. Diese Firmwareebenen werden in den LTFS-LE-Versionshinweisen aufgeführt.

Einschränkung des Netzwerkzugriffs

Der LTFS-LE-Hostserver 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.

Kapitel 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. Im Folgenden werden die Installation, Konfiguration und Administration der LTFS-LE-Anwendung nicht im Einzelnen beschrieben. Installation, Konfiguration und Administration werden im LTFS-LE-Installations- und Administrationshandbuch 1.0 abgedeckt.

Ihre Umgebung

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

Welche Ressourcen müssen geschützt werden?

Bei LTFS-LE müssen der Hostserver und das zugehörige Netzwerk vor unbefugtem Zugriff geschützt werden

Vor wem müssen die Ressourcen geschützt werden?

LTFS-LE muss vor jedem Benutzer im Internet, externen Benutzern und nicht befugten internen Benutzern geschützt werden.

Was geschieht, wenn der Schutz bei strategischen Ressourcen versagt?

Jemand könnte böswillig einen Datenverlust im Bandspeicher verursachen, indem er sich unbefugt Zugriff auf LTFS-LE verschafft.

Installieren von Linear Tape File System – Library Edition (LTFS-LE)

LTFS-LE darf nur in Systemen installiert werden, die sich innerhalb derselben (durch Firewall) geschützten Netzwerkinfrastruktur befinden wie die überwachten Geräte. Kundenzugriffskontrolle muss für die Systeme erzwungen werden, auf denen LTFS-LE installiert ist, um den eingeschränkten Zugriff auf die Anwendung zu gewährleisten.

Anweisungen zur Installation finden Sie in den folgenden LTFS-LE-Benutzerhandbüchern.

Oracle LTFS-LE - Planung und Installation

Konfiguration nach Abschluss der Installation

Nach Abschluss der Installation können keine Änderungen an der Sicherheit der Konfiguration vorgenommen werden. Die Konfiguration wird vom Benutzer während der Installation festgelegt.

Zuweisen des Benutzer-(Admin-)Passworts

Das Passwort für das Kundenadministrationskonto wird vom Kunden während der Installation festgelegt.

Durchsetzen der Passwortverwaltung

Im Unternehmen des Kunden gültige Regeln zur Passwortverwaltung, wie Passwortlänge, Historie und Komplexität müssen für das Administratorpasswort angewendet werden.

Kapitel 3. Sicherheitsfunktionen

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

Die LTFS-LE-Anwendung stellt dem Benutzer verschlüsselte Passwortrollen zum Schutz bereit. Dies ist nicht die einzige Sicherheitsmaßnahme, mit der die Anwendung geschützt wird. Die Anwendung muss in einem physisch gesicherten Data Center verwendet werden, das über ein gesichertes Netzwerk verfügt, das nur autorisierten Benutzern den Zugriff ermöglicht.

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 LTFS-LE oder Bandbibliotheken von Oracle befürchten, wenden Sie sich an Oracle Services, Oracle Tape Library Engineering oder den für Ihr Konto verantwortlichen Mitarbeiter.

Anhang B

Anhang B. Referenzen

Oracle LTFS-LE - Planung und Installation

