

# **StorageTek Virtual Storage Manager System**

VSM 7 – Sicherheitshandbuch

**E74281-01**

**März 2016**

---

## StorageTek Virtual Storage Manager System

VSM 7 – Sicherheitshandbuch

### E74281-01

Copyright © 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

---

<b>Vorwort</b> .....	5
Zielgruppe .....	5
Barrierefreie Dokumentation .....	5
<b>1. Überblick</b> .....	7
Produktüberblick .....	7
Wichtige Sicherheitsgrundlagen .....	8
Software muss immer auf dem neuesten Stand sein .....	8
Netzwerkzugriff muss auf kritische Services begrenzt sein. ....	8
Authentifizierung .....	9
Prinzip der geringsten Rechte .....	9
Überwachen der Systemaktivität .....	9
Sicherheitsinformationen immer auf dem neuesten Stand halten .....	9
<b>2. Sichere Installation</b> .....	11
<b>3. Sicherheitsfunktionen</b> .....	13
<b>A. Prüfliste für sicheres Deployment</b> .....	15



# Vorwort

---

In diesem Dokument werden die Sicherheitsfunktionen des Oracle StorageTek Virtual Storage Manager System 7 Virtual Tape Storage Subsystems (VSM 7 VTSS) beschrieben.

## Zielgruppe

Dieses Handbuch richtet sich an Personen, die an der Verwendung der Sicherheitsfunktionen und der sicheren Installation und Konfiguration von VSM 7 VTSS 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 das Produkt und erläutert die allgemeinen Grundsätze der Appliance-Sicherheit.

### Produktüberblick

Das Oracle StorageTek Virtual Storage Manager System 7 Virtual Tape Storage Subsystem (VSM 7 VTSS) ist als vorgefertigtes System in einem Package integriert, das auf vorhandenen Oracle-Server- und Speicherungsplattformen aufbaut. Die Server, der Datenträgerspeicher und das Standardrack werden als in einem Package integriertes System oder als Appliance geliefert. Die VTSS-Appliance umfasst eine vorinstallierte, vordefinierte Software für die VTSS-Funktionalität, sodass eine begrenzte Konfiguration auf Standortebene erforderlich ist, um das Produkt in der verwalteten Bandumgebung des Kunden zu integrieren. Die Appliance ist so ausgelegt, dass keine Kundenadministration des Systems erforderlich ist.

---

#### Hinweis:

Nur qualifizierte Oracle-Mitarbeiter dürfen das System warten und Konfigurationsänderungen verwalten.

---

Das VTSS ist nur eine Komponente einer VSM-Lösung.

Weitere wichtige Subsysteme umfassen:

#### **VTSS-Hardware und -Software**

VSM 7 VTSS unterstützt emulierte Bandkonnektivität über FICON-Schnittstellen zu IBM MVS-, VM- und zLinux-Hosts und auch FICON-Anschluss zu Real Tape Drives (RTDs) und TCP/IP-Anschluss zu anderen VTSSs und VLEs. FICON ist ein IBM-gesteuerter Standard für Kanalprotokolle zwischen CPU (zOS) und Geräten.

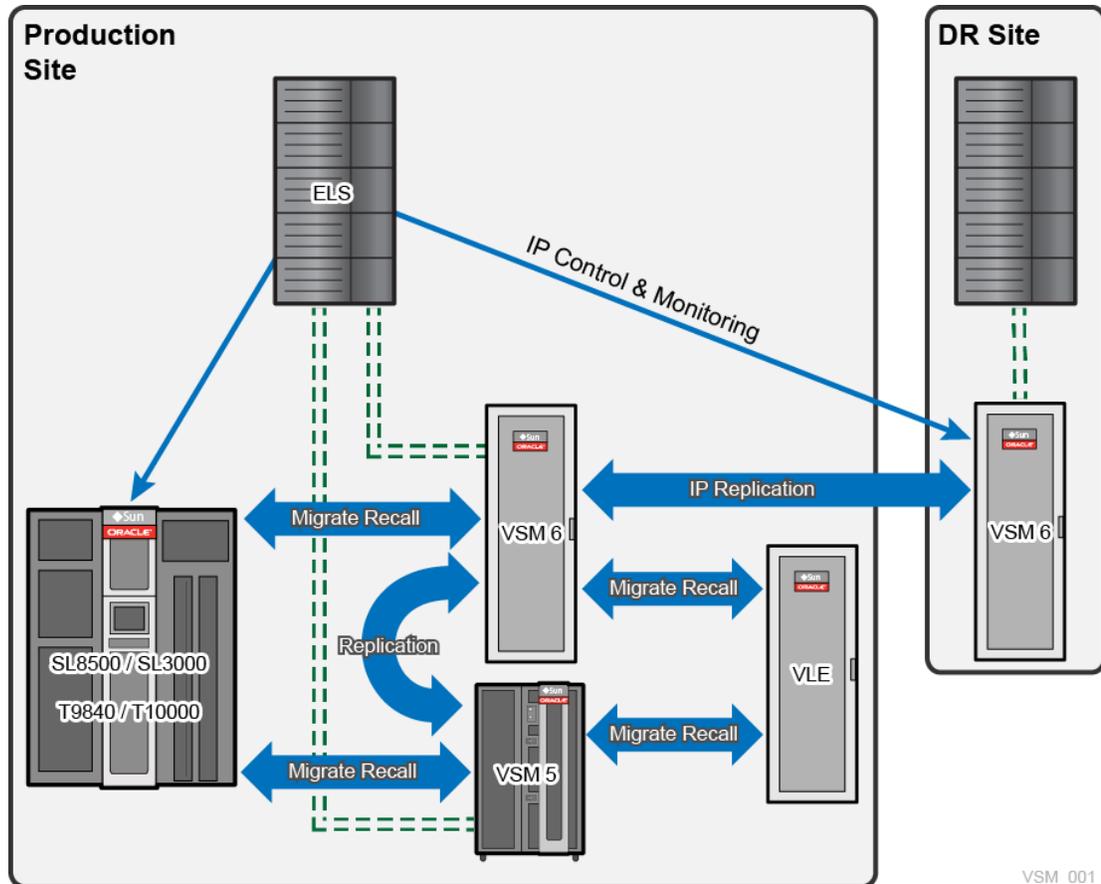
#### **Enterprise Library Software (ELS) und Virtual Tape Control Software (VTCS)**

ELS ist die konsolidierte Suite von StorageTek-Mainframesoftware, die VTSS aktiviert und verwaltet. Die ELS-Basissoftware besteht aus Hostsoftwarekomponente (HSC), Speicherverwaltungskomponente (SMC), HTTP-Server und Virtual Tape Control-Software (VTCS).

VTCS ist die ELS-Komponente, die Erstellen, Löschen, Replizieren, Migrieren und Wiederaufrufen von virtuellen Bandimages auf dem VTSS-Subsystem kontrolliert und außerdem Informationen zur Berichterstellung aus dem VTSS-Subsystem erfasst.

### Virtual Library Extended-(VLE-)Hardware und -Software

Das Virtual Library Extended-(VLE-)Subsystem wird als Migrations- und Wiederaufrufziel für virtuelle Bandvolumes (VTVs) von VTSS verwendet. Das VLE ist über IP an VTSS angeschlossen.



## Wichtige Sicherheitsgrundlagen

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

### Software muss immer auf dem neuesten Stand sein

Patches und Systemupdates werden von qualifizierten Oracle-Mitarbeitern installiert

### Netzwerkzugriff muss auf kritische Services begrenzt sein.

Appliances müssen an sicheren physischen Standorten installiert werden. Der Zugang muss auf autorisierte Mitarbeiter oder Beauftragte des Kunden und auf Oracle-Servicemitarbeiter

beschränkt sein. Das System muss hinter einer Firewall vernetzt sein. Nur Oracle-Servicemitarbeiter dürfen das System verwalten.

## **Authentifizierung**

Es muss gewährleistet sein, dass nur autorisierte Mitarbeiter Zugang zu dem System haben. Passwörter müssen beim Deployment am Standort des Kunden geändert werden.

## **Prinzip der geringsten Rechte**

Nicht-VTSS-Benutzerkonten sind nicht zulässig. Nur bereits vorhandene Konten werden zur Systemwartung und -verwaltung verwendet.

## **Überwachen der Systemaktivität**

Systemsicherheit steht auf drei Beinen: gute Sicherheitsprotokolle, richtige Systemkonfiguration und Systemüberwachung. Diese dritte Anforderung wird durch Auditing und Prüfung von Auditdatensätzen erfüllt.

## **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

Die gesamte Software ist bereits in der VTSS-Appliance vorinstalliert. Zur Sicherung des Systems müssen Sie nur das Passwort des VSM-Administratorkontos ändern.

Daten werden komprimiert und in einem herstellereigenen Format gesendet. Dabei ist die Interkommunikation mit älteren Systemen vorrangig, die aktuell in der Kundenumgebung installiert sind. Die IP-Kommunikation muss über ein privates, dediziertes Netzwerk erfolgen, das eine in der IP-Infrastruktur integrierte Verschlüsselung bereitstellt.



## **Kapitel 3. Sicherheitsfunktionen**

Die VTSS-Appliance enthält keine konfigurierbaren Sicherheitsfunktionen.



## Anhang A. Prüfliste für sicheres Deployment

Die folgende Sicherheitsprüfliste enthält Richtlinien, mit denen Sie die VTSS-Appliance sichern können:

1. Setzen Sie das VSM-Administratorkonto zurück, wenn Sie die Appliance das erste Mal einschalten.

---