StorageTek Virtual Storage Manager System

VSM 7 – Sicherheitshandbuch

E74281-01

März 2016

ORACLE

StorageTek Virtual Storage Manager System
VSM 7 – Sicherheitshandbuch

E74281-01

Inhalt

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.

1

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.

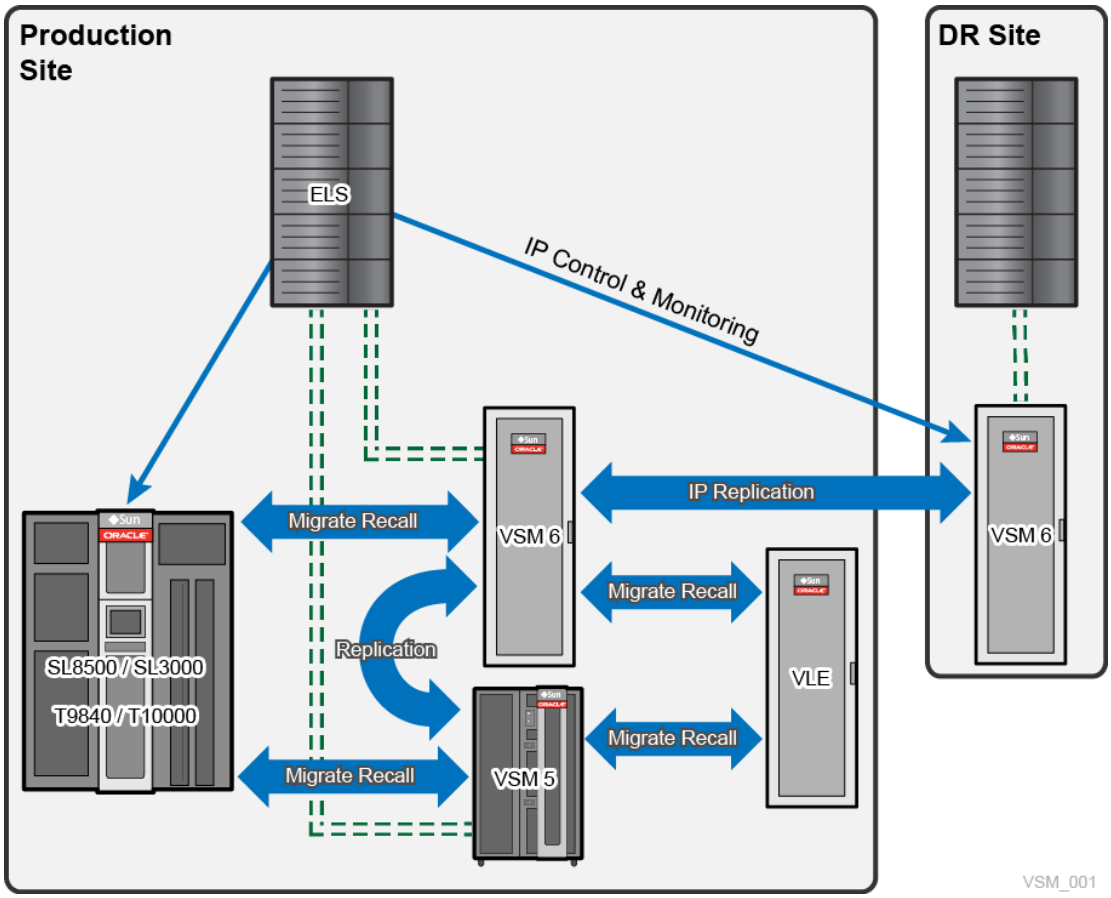
Weitere wichtige Subsysteme umfassen:

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 Berichtserstellung 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.

2

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.

3

Kapitel 3. Sicherheitsfunktionen

Die VTSS-Appliance enthält keine konfigurierbaren Sicherheitsfunktionen.

Anhang A

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.