StorageTek Virtual Storage Manager GUI

Sicherheitshandbuch

Version 1.0

E72343-01

April 2015

ORACLE

StorageTek Virtual Storage Manager GUI
Sicherheitshandbuch

E72343-01

Inhalt

Vorwort

In diesem Dokument werden die Sicherheitsfunktionen von Oracle StorageTek Virtual Storage Manager GUI beschrieben.

Zielgruppe

Dieses Handbuch richtet sich an Personen, die an der Verwendung der Sicherheitsfunktionen und der sicheren Installation und Konfiguration von VSM GUI 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 StorageTek Virtual Storage Manager (VSM) GUI und erläutert die allgemeinen Grundsätze für dessen Sicherheit.

Produktüberblick

StorageTek VSM GUI ist ein Oracle-Softwareprodukt, das Kunden Kontrollen und Berichte für virtuelle Bänder bietet, mit denen die Vorgänge im Zusammenhang mit virtuellen Bändern ihrer Data Centers effizient und proaktiv überwacht und verwaltet werden können.

VSM GUI unterstützt Enterprise MVS Virtual Storage Manager-(VSM-)Bandkunden. VSM GUI unterstützt Kunden mit allen unterstützten Generationen von VSM-Produkten.

Sicherheit

Physisch
VSM GUI muss auf einer virtuellen Maschine auf dem Oracle VM- oder VMware-Server eines Kunden im Data Center einer Organisation installiert werden. Der physische Zugriff auf den Server unterliegt den Unternehmensrichtlinien des Kunden.

Netzwerk
VSM GUI muss in einem internen, durch Firewall geschützten Netzwerk des Kunden hinzugefügt oder konfiguriert werden. Dieses Netzwerk benötigt TCP/IP-Zugriff auf alle Instanzen von SMC-HTTP-Server, die Berichte zu virtuellen Bandressourcen erstellen.

Benutzerzugriff
Der Zugriff auf die VSM GUI-Anwendung wird durch Benutzername- und Passwortauthentifizierung kontrolliert. Die Benutzernamen- und Passwortauthentifizierung erfolgt, indem Sie die Anwendung für den LDAP-Service des Benutzers konfigurieren.

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. Im ganzen Dokument wird von folgenden Softwareebenen ausgegangen:

VSM GUI Version 1.0; Mai 2015

Hinweis:

VSM GUI unterstützt ELS7.1 und ELS7.2 und erfordert, dass die aktuellsten Wartungsupdates eingespielt werden.

Einschränkung des Netzwerkzugriffs

Der VSM GUI-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.

Sicherheitsinformationen müssen immer auf dem neuesten Stand sein

Oracle nimmt fortwährend Verbesserungen an Software und Dokumentation vor. Prüfen Sie dieses Dokument mit jeder neuen Version auf Änderungen. Besondere Sicherheitsfragen werden möglicherweise auch in den Versionshinweisen angesprochen.

2

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 VSM GUI-Benutzerhandbuch 1.0 werden die Installation, Konfiguration und Administration ausführlich erläutert.

Umgebung analysieren

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

Welche Ressourcen müssen geschützt werden?

Bei VSM GUI müssen der Hostserver und das zugehörige Netzwerk vor unbefugtem Zugriff geschützt werden

Vor wem werden die Ressourcen geschützt?

VSM GUI muss vor jedem Benutzer im Internet, externen Benutzern und nicht befugten internen Benutzern geschützt werden.

Was geschieht, wenn der Schutz bei strategischen Ressourcen versagt?

Das VSM GUI eine Ressourcenüberwachungs- und -nutzungsanwendung für virtuelle Speicher ist, kann der unbefugte Zugriff auf VSM GUI sich auf die Verfügbarkeit von VSM-Ressourcen auswirken. Der Status einer Ressource kann betroffen sein, aber die Daten auf den Speicherressourcen sind nicht betroffen.

StorageTek VSM GUI installieren

VSM GUI darf nur auf Systemen installiert werden, die sich innerhalb derselben (per Firewall) geschützten Netzwerkinfrastruktur wie die überwachten virtuellen Ressourcen befinden (also VTCS und HSC). Kundenzugriffskontrolle muss für die Systeme erzwungen werden, auf denen VSM GUI installiert ist, um den eingeschränkten Zugriff auf die Anwendung zu gewährleisten.

Installationsanleitungen finden Sie im *VSM GUI-Benutzerhandbuch*.

Konfiguration nach Abschluss der Installation

Nach Abschluss der Installation können keine Änderungen an der Konfigurationssicherheit vorgenommen werden. Die Konfiguration wird vom Kunden 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 auf das Administratorpasswort angewendet werden.

3

Kapitel 3. Sicherheitsfunktionen

In diesem Abschnitt werden die spezifischen Sicherheitsverfahren beschrieben, die das Produkt bietet. Die VSM GUI-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

Anhang A. Prüfliste für sicheres Deployment

Die folgende Sicherheitsprüfliste enthält Richtlinien, mit denen Sie die Bibliothek 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. Wenden Sie sich an Oracle Security Products, wenn Sie Sicherheitslücken bei VSM GUI entdecken.

Anhang B

Anhang B. Referenzen

VSM GUI-Benutzerhandbuch