# GUI de StorageTek Virtual Storage Manager

Guía de seguridad

**E79974-01**

**Julio de 2016**

ORACLE

**GUI de StorageTek Virtual Storage Manager**
Guía de seguridad

**E79974-01**

# Tabla de contenidos

# Prefacio

En este documento, se describen las características de seguridad de la GUI de StorageTek Virtual Storage Manager, de Oracle.

## Destinatarios

Esta guía está destinada a cualquier persona que se encargue de la utilización de funciones de seguridad y de la instalación y la configuración seguras de la GUI de VSM.

## Accesibilidad a la documentación

Para obtener información sobre el compromiso de Oracle con la accesibilidad, visite el sitio web del Programa de Accesibilidad de Oracle en http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

**Acceso a My Oracle Support**
Los clientes de Oracle que hayan contratado servicios de soporte electrónico pueden acceder a ellos mediante My Oracle Support. Para obtener información, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info o, si tiene alguna discapacidad auditiva, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs.

# 1

# Capítulo 1. Visión general

En esta sección, se brinda una visión general de la GUI de StorageTek Virtual Storage Manager (VSM) y se explican los principios generales de su seguridad.

## Visión general del producto

La GUI de StorageTek VSM es un producto de software de Oracle que proporciona a los clientes informes y control de cinta virtual para supervisar y gestionar de manera eficaz y preventiva las operaciones de cinta virtual del centro de datos.

La GUI de VSM admite clientes de cinta de Enterprise MVS Virtual Storage Manager (VSM). La GUI de VSM admite clientes con todas las generaciones admitidas de productos VSM.

## Seguridad

**Seguridad física**
La GUI de VSM se debe instalar en una máquina virtual en un servidor Oracle VM o VMware del cliente dentro del centro de datos de la organización. El acceso físico al servidor estará establecido en la política de la empresa del cliente.

**Seguridad de red**
Se requiere que la GUI de VSM esté incorporada o configurada en una red interna del cliente protegida por firewall. Esta red requiere acceso TCP/IP a todas las instancias del servidor HTTP del SMC que se informan en recursos virtuales de cinta.

**Seguridad de acceso de usuarios**
El acceso a la aplicación de la GUI de VSM está controlado por la autenticación de nombre de usuario y contraseña. La autenticación de nombre de usuario y contraseña se realizan configurando la aplicación en el servicio LDAP del usuario.

## Principios generales de seguridad

Los siguientes principios son fundamentales para usar cualquier producto de manera segura.

### Mantener el software actualizado

Uno de los principios de una buena práctica de seguridad es mantener todas las versiones y todos los parches de software actualizados. En todo este documento, asumimos un nivel de software de:

GUI de VSM versión 1.1; julio de 2016

**Nota:**

La GUI de VSM admite ELS 7.1, ELS 7.2 y ELS 7.3, y requiere que se apliquen las actualizaciones de mantenimiento más recientes.

## Restringir el acceso a la red

Mantenga el servidor host de la GUI de VSM protegido por el firewall del centro de datos. El firewall garantiza que el acceso a esos sistemas esté restringido a una ruta de red conocida, que puede supervisarse y restringirse, en caso de ser necesario. Como alternativa, un enrutador de firewall sustituye varios firewall independientes.

## Mantenerse actualizado sobre la información de seguridad más reciente

Oracle mejora continuamente su software y su documentación. Consulte este documento con cada versión para ver las revisiones. En las notas de la versión también se puede incluir información acerca de cuestiones de seguridad específicas.

2

# Capítulo 2. Instalación segura

En esta sección, se detallan los procesos de planificación para lograr una instalación segura y se describen varias topologías de implementación recomendadas para los sistemas. La Guía del usuario de la GUI de VSM 1.0 cubre detalladamente la instalación, la configuración y la administración.

## Comprensión del entorno

Para comprender mejor las necesidades de seguridad, debe hacerse las siguientes preguntas:

### ¿Qué recursos necesitan protección?

Para la GUI de VSM, el servidor host y la red asociada deben estar protegidos contra el acceso no autorizado

### ¿De quién se protegen los recursos?

La GUI de VSM debe protegerse contra todos los usuarios de Internet, los usuarios externos y los usuarios internos no autorizados.

### ¿Qué sucede si falla la protección de los recursos estratégicos?

Dado que la GUI de VSM es una aplicación de uso y supervisión de recursos de almacenamiento virtual, el acceso no autorizado a la GUI de VSM puede afectar la disponibilidad de los recursos de VSM. Se puede afectar el estado de un recurso, pero los datos que residen en los recursos de almacenamiento no se verán afectados.

## Instalación de la GUI de StorageTek VSM

La GUI de VSM solo se debe instalar en sistemas que están dentro de la misma infraestructura de red protegida (con firewall) que los recursos virtuales supervisados (es decir, VTCS y HSC). Se deben aplicar controles de acceso del cliente en los sistemas en los que la GUI de VSM esté instalada para garantizar el acceso restringido a la aplicación.

Consulte la *Guía del usuario de la GUI de VSM* para obtener instrucciones de instalación.

# Configuración posterior a la instalación

No hay cambios de seguridad para la configuración posterior a la instalación. El cliente realiza la configuración durante la instalación.

## Asignación de la contraseña del usuario (administrador)

El cliente configura la contraseña de la cuenta de administración del cliente durante la instalación.

## Aplicar la administración de contraseñas

Se deben aplicar las reglas de gestión de contraseñas corporativas del cliente, como longitud, historial y complejidad de la contraseña, a la contraseña del administrador.

3

# Capítulo 3. Funciones de seguridad

En esta sección, se describen los mecanismos de seguridad específicos que ofrece el producto. La aplicación de la GUI de VSM proporciona a los usuarios roles de contraseña cifrada para protegerse. Esta no es la única línea de seguridad para proteger la aplicación. La aplicación debe encontrarse en un centro de datos físicamente seguro que también cuente con una red protegida que permita el acceso solo a usuarios autorizados.

# Apéndice A

## Apéndice A. Lista de comprobación de la implementación segura

La siguiente lista de comprobación de seguridad incluye pautas que ayudan a proteger la biblioteca:

1. Aplicar la administración de contraseñas.
2. Aplicar controles de acceso.
3. Restringir el acceso a la red.
    a. Debe implementarse un firewall.
    b. El firewall no debe estar comprometido.
    c. Debe supervisarse el acceso al sistema.
    d. Deben comprobarse las direcciones IP de la red.
4. Comunicarse con el departamento de productos de seguridad de Oracle en caso de encontrar vulnerabilidades en la GUI de VSM.

# Apéndice B

## Apéndice B. Referencias

*Guía del usuario de la GUI de VSM*