

StorageTek Virtual Storage Manager System

Guía de seguridad de la consola VSM

E79960-01

Septiembre de 2016

StorageTek Virtual Storage Manager System

Guía de seguridad de la consola VSM

E79960-01

Copyright © 2016, Oracle y/o sus filiales. Todos los derechos reservados.

Este software y la documentación relacionada están sujetos a un contrato de licencia que incluye restricciones de uso y revelación, y se encuentran protegidos por la legislación sobre la propiedad intelectual. A menos que figure explícitamente en el contrato de licencia o esté permitido por la ley, no se podrá utilizar, copiar, reproducir, traducir, emitir, modificar, conceder licencias, transmitir, distribuir, exhibir, representar, publicar ni mostrar ninguna parte, de ninguna forma, por ningún medio. Queda prohibida la ingeniería inversa, desensamblaje o descompilación de este software, excepto en la medida en que sean necesarios para conseguir interoperabilidad según lo especificado por la legislación aplicable.

La información contenida en este documento puede someterse a modificaciones sin previo aviso y no se garantiza que se encuentre exenta de errores. Si detecta algún error, le agradeceremos que nos lo comunique por escrito.

Si este software o la documentación relacionada se entrega al Gobierno de EE.UU. o a cualquier entidad que adquiera las licencias en nombre del Gobierno de EE.UU. entonces aplicará la siguiente disposición:

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.

Este software o hardware se ha desarrollado para uso general en diversas aplicaciones de gestión de la información. No se ha diseñado ni está destinado para utilizarse en aplicaciones de riesgo inherente, incluidas las aplicaciones que pueden causar daños personales. Si utiliza este software o hardware en aplicaciones de riesgo, usted será responsable de tomar todas las medidas apropiadas de prevención de fallos, copia de seguridad, redundancia o de cualquier otro tipo para garantizar la seguridad en el uso de este software o hardware. Oracle Corporation y sus filiales declinan toda responsabilidad derivada de los daños causados por el uso de este software o hardware en aplicaciones de riesgo.

Oracle y Java son marcas comerciales registradas de Oracle y/o sus filiales. Todos los demás nombres pueden ser marcas comerciales de sus respectivos propietarios.

Intel e Intel Xeon son marcas comerciales o marcas comerciales registradas de Intel Corporation. Todas las marcas comerciales de SPARC se utilizan con licencia y son marcas comerciales o marcas comerciales registradas de SPARC International, Inc. AMD, Opteron, el logotipo de AMD y el logotipo de AMD Opteron son marcas comerciales o marcas comerciales registradas de Advanced Micro Devices. UNIX es una marca comercial registrada de The Open Group.

Este software o hardware y la documentación pueden proporcionar acceso a, o información sobre contenidos, productos o servicios de terceros. Oracle Corporation o sus filiales no son responsables y por ende desconocen cualquier tipo de garantía sobre el contenido, los productos o los servicios de terceros a menos que se indique otra cosa en un acuerdo en vigor formalizado entre Ud. y Oracle. Oracle Corporation y sus filiales no serán responsables frente a cualesquiera pérdidas, costos o daños en los que se incurra como consecuencia de su acceso o su uso de contenidos, productos o servicios de terceros a menos que se indique otra cosa en un acuerdo en vigor formalizado entre Ud. y Oracle.

Tabla de contenidos

Prefacio	5
Destinatarios	5
Accesibilidad a la documentación	5
1. Visión general	7
Visión general del producto	7
Principios generales de seguridad	9
Mantener el software actualizado	9
Restricción del acceso de red a los servicios críticos	9
Autenticación	9
Seguir el principio de privilegios mínimos	9
Supervisión de la actividad del sistema	10
Cómo mantenerse actualizado sobre la información de seguridad más reciente	10
2. Instalación segura	11
3. Funciones de seguridad	13

Prefacio

En este documento, se describen las características de seguridad de la consola VSM 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 consola 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>.

Capítulo 1. Visión general

En esta sección, se brinda una visión general del producto y se explican los principios generales de la seguridad de la aplicación.

Visión general del producto

La consola Virtual Storage Manager (consola VSM) de StorageTek Virtual Storage Manager (VSM) System 6 y 7 proporciona una plataforma común para que todas las aplicaciones de VSM residan donde no hay un sistema controlador de zOS. La consola VSM consta de una pila de hardware y software de Oracle. La consola VSM se entrega en un servidor T5-2 como un dispositivo que se ejecuta en Solaris 11.3, con aplicaciones que incluyen el software de control de cinta virtual (VTCS), Automated Cartridge System Library Software (ACSL) y la interfaz gráfica de usuario (GUI) de VSM personalizados. El dispositivo de la consola VSM incluye aplicaciones preinstaladas y preconfiguradas, de modo que se requiere una configuración limitada en el nivel del sitio para integrar el producto en el entorno de cinta gestionada del cliente. El dispositivo está diseñado para evitar la necesidad de que el cliente deba administrar el sistema.

Nota:

Solo se permite que personal calificado de Oracle mantenga el sistema y administre los cambios de configuración.

La consola VSM es solo un componente de una solución de VSM.

Los subsistemas principales incluyen:

Software y hardware de VTSS

VSM 6 y VSM 7 VTSS admiten conectividad de cinta emulada mediante interfaces FICON a hosts IBM MVS, VM y zLinux, y, además, conexión FICON a unidades de cinta reales (RTD) y conexión TCP/IP a otros VTSS y VLE. FICON es un estándar de IBM para el protocolo de canal entre CPU (zOS) y dispositivos.

Enterprise Library Software (ELS) y software de control de cinta virtual (VTCS)

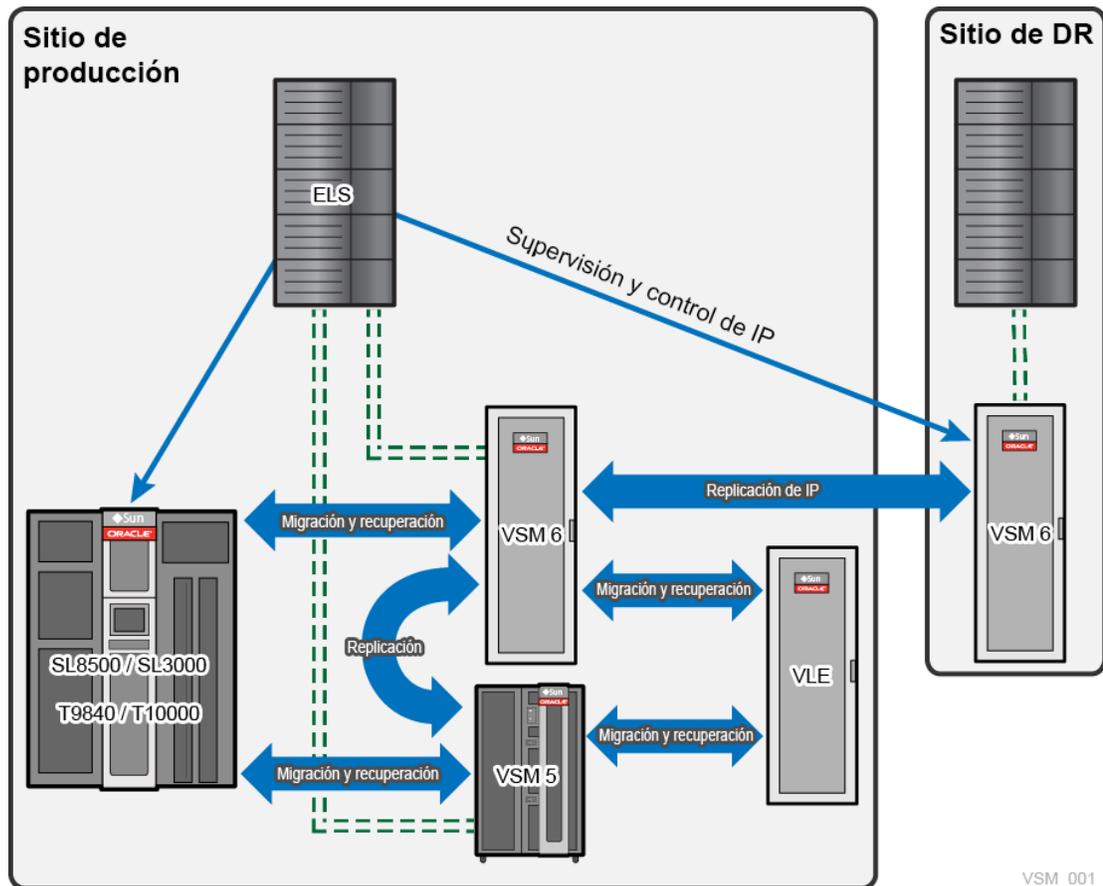
ELS es el conjunto consolidado de software de mainframe de StorageTek que activa y gestiona el VTSS. Cuando se utiliza un sistema MVS, el software ELS base está formado por el componente de software de host (HSC), el componente de gestión de almacenamiento (SMC), el servidor HTTP y el software de control de cinta virtual (VTCS).

VTCS es el componente de ELS que controla la creación, la supresión, la replicación y la migración de cintas virtuales y la recuperación de imágenes de cinta virtual en el subsistema de VTSS, y, además, captura información de informes del subsistema de VTSS.

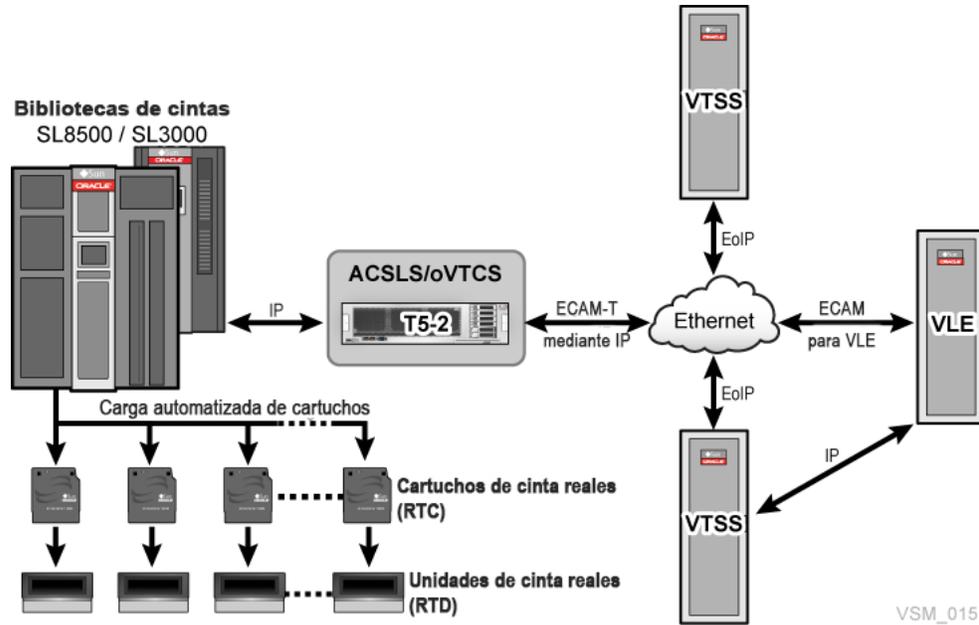
Ahora, VTCS se puede ejecutar en un sistema z/os del cliente o puede estar incrustado en la consola VSM.

Hardware y software de Virtual Library Extended (VLE)

El subsistema de Virtual Library Extended (VLE) funciona como almacenamiento secundario de VTSS para migración y recuperación de copias de volúmenes de cinta virtual (VTV). VLE está conectado por IP con VTSS.



Cuando no hay ningún sistema MVS presente, se utiliza la solución de la consola VSM. Una aplicación interna de ACSLS reemplaza el componente HSC, y se utiliza el puerto de la consola VSM de la aplicación VTCS.



Principios generales de seguridad

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

Mantener el software actualizado

Las actualizaciones del sistema y del software de la aplicación serán instaladas por personal calificado de Oracle.

Restricción del acceso de red a los servicios críticos

Los dispositivos deben instalarse en ubicaciones físicas seguras con acceso limitado a empleados o agentes del cliente y personal de servicio de asistencia de Oracle. El sistema debe tener un firewall conectado.

Autenticación

Asegúrese de que solo personal autorizado pueda acceder al sistema. Las contraseñas deben cambiarse cuando se realiza la implementación en el sitio del cliente.

Seguir el principio de privilegios mínimos

No se permiten cuentas de usuarios que no sean de VTSS. Sólo se usan cuentas preexistentes para el mantenimiento y la administración del sistema.

Supervisión de la actividad del sistema

La seguridad del sistema depende de tres pilares: buenos protocolos de seguridad, configuración del sistema correcta y supervisión del sistema. Las auditorías y la revisión de los registros de auditoría son útiles para cumplir con este último requisito.

Cómo mantenerse actualizado sobre la información de seguridad más reciente

Oracle mejora continuamente su software y su documentación. Consulte esta nota anual sobre la versión para ver las revisiones.

Capítulo 2. Instalación segura

Todo el código de la aplicación está preinstalado en el dispositivo de la consola VSM.

Todos los datos del cliente se comprimen y se envían en un formato exclusivo que incluye predominancia de intercomunicación con los sistemas heredados que están actualmente instalados en los entornos del cliente. Las comunicaciones IP deben realizarse en una red privada y dedicada con cifrado incorporado en la infraestructura IP.

Capítulo 3. Funciones de seguridad

En el dispositivo de la consola VSM no se ofrecen características de seguridad configurables.

