

StorageTek Enterprise Library Software

Guía de seguridad

E63465-01

Marzo de 2015

StorageTek Enterprise Library Software

Guía de seguridad

E63465-01

Copyright © 2015, 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. Descripción general	7
1.1. Descripción general del producto	7
1.2. Principios generales de seguridad	8
1.2.1. Mantenga el software actualizado	8
1.2.2. Restringir el acceso a la red	8
1.2.3. Manténgase actualizado acerca de la última información de seguridad	8
2. Instalación segura	9
2.1. Instalación de ELS	9
2.2. Configuración posterior a la instalación de ELS	9
3. Funciones de seguridad	11
3.1. Protección de ELS con AT-TLS (z/OS) únicamente	11
3.2. Uso de la función de seguridad de la XAPI de ELS	12
4. Consideraciones de seguridad para desarrolladores	13
A. Lista de comprobación de la implementación segura	15
B. Referencias	17

Prólogo

En este documento, se describen las funciones de seguridad de StorageTek Enterprise Library Software (ELS), 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 StorageTek Enterprise Library Software (ELS).

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>.

Descripción general

En esta sección, se brinda una descripción general del paquete de software ELS y se explican los principios generales de la seguridad de la aplicación.

1.1. Descripción general del producto

ELS brinda compatibilidad con la automatización de cintas para entornos de cinta de mainframe de StorageTek, de Oracle, para las siguientes plataformas:

- Plataforma de z/OS de IBM. ELS admite una arquitectura cliente/servidor TCP/IP de automatización de cintas que permite que el software SMC del cliente se ejecute en una LPAR de z/OS para comunicarse con el software del servidor de HSC/VTCS que se ejecuta en otra LPAR de z/OS.
- Plataforma de z/VM de IBM. El software cliente VM de ELS para sistemas z/VM se comunica con el software de servidor HSC/VTCS que se ejecuta en una LPAR de z/OS para automatizar el procesamiento de cintas físicas y virtuales para z/VM.
- La plataforma MSP/EX de Fujitsu. SMC debe ejecutarse en todos los hosts en los que se lleva a cabo procesamiento de cintas. El componente del servidor (HSC/VTCS) de ELS se puede ejecutar en el mismo host de MSP/EX, como el SMC, o se puede ejecutar en un host remoto independiente. Cuando SMC y HSC/VTCS residen en distintos hosts de MSP/EX, se usa TCP/IP para enviar solicitudes del host del cliente al host del servidor. Para recibir solicitudes de HTTP de un cliente remoto de SMC, el componente HTTP debe estar activado en el SMC que se ejecuta en el host del servidor.

La comunicación cliente/servidor de ELS se utiliza para emitir solicitudes de ruta de control, principalmente, solicitudes de montaje/desmontaje, para volúmenes de cinta física y virtual. La información incluida en estas solicitudes de ruta de control consta de números de serie de volúmenes de cinta virtual/física, direcciones de unidades de transporte de cinta virtual/física e información sobre políticas y configuración de TapePlex. Lo más importante es que la comunicación de cliente/servidor de ELS nunca contiene datos del cliente, los cuales siempre viajan por interfaces de rutas de datos FICON/ESCON de IBM que conectan las LPAR del host a los transportes de cinta StorageTek, de Oracle, o a dispositivos de cinta virtual VSM.

La información incluida en esta guía de seguridad se aplica a todas las versiones de ELS. Como se describe en la parte 3 de esta guía, es posible proteger las comunicaciones de la ruta de control de cliente/servidor de ELS cuando dicha protección es conveniente o necesaria. Además, en este documento se analizan aspectos de seguridad de diversas actividades que se deben realizar durante la instalación de ELS y después de esta.

1.2. Principios generales de seguridad

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

1.2.1. Mantenga 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. El paquete de mantenimiento acumulativo más reciente de ELS, junto con HOLDDATA y los PTF individuales, está disponible en My Oracle Support (MOS). Los paquetes de mantenimiento acumulativo se actualizan de forma mensual para que incluyan todos los PTF y el último ciclo de prueba de regresión mensual de ELS. Todos los PTF incluidos en un paquete acumulativo han sido sometidos a prueba de forma conjunta como un paquete completo. La notificación por correo electrónico de HIPER PTF está disponible mediante suscripción a los documentos de temas actuales de alerta de MOS para los productos ELS. Se alienta a los clientes a permanecer en sus niveles actuales de mantenimiento, mantener HOLDDATA actualizado y suscribirse a las notificaciones de temas actuales de alerta de HIPER.

1.2.2. Restringir el acceso a la red

A los efectos del rendimiento y la seguridad, dirija las comunicaciones de la ruta de control de ELS por una red aislada protegida por un firewall. El uso de un firewall garantiza que el acceso a los sistemas ELS esté restringido a una red conocida, que puede supervisarse y restringirse, en caso de ser necesario. El uso de una red dedicada para las comunicaciones de cliente/servidor de ELS elimina el conflicto de redes con otras aplicaciones y mejora el rendimiento del sistema de cinta.

1.2.3. Manténgase actualizado acerca de la última información de seguridad

Oracle mejora continuamente su software y su documentación. Consulte con regularidad las revisiones de esta guía de seguridad y la demás documentación de producto de ELS. Toda la documentación de ELS a la que se hace referencia en este documento está disponible en la sección Productos de almacenamiento en cinta de Oracle Technical Network.

Instalación segura

La utilidad de autorización del sistema (SAF, System Authorization Facility) del sistema operativo z/OS de IBM ofrece protección esencial para la mayoría de los aspectos de seguridad de ELS. SAF se implementa, generalmente, con el paquete RACF de IBM o uno equivalente. En esta sección, se describe el uso de un entorno SAF basado en RACF para instalar y configurar una instalación segura de ELS.

2.1. Instalación de ELS

En el documento de Oracle *StorageTek Enterprise Library Software: Instalación de ELS*, se describe cómo instalar y configurar su versión de ELS con la protección de RACF. Consulte este documento para obtener más información sobre los siguientes temas de instalación relacionados con la seguridad:

- Instalación del software básico y del último paquete de mantenimiento acumulativo
- Autorización de APF para biblioteca de carga de ELS
- Autorización de APF para biblioteca de salida de usuario de HSC
- Autorización de APF para biblioteca de carga de SMC JES3

2.2. Configuración posterior a la instalación de ELS

En estos documentos de Oracle se describen las tareas posteriores a la instalación para su versión de ELS:

- *StorageTek Enterprise Library Software: Configuración de HSC y VTCS*
- *StorageTek Enterprise Library Software: Configuración y gestión de SMC*
- *StorageTek Enterprise Library Software: Referencia de programación de ELS*

Consulte estos documentos para obtener más información sobre los siguientes temas posteriores a la instalación relacionados con la seguridad:

- Definición de la protección de RACF para la seguridad del conjunto de datos CDS
- Definición de la autoridad de comando y de la autoridad de interfaz de programación mediante la salida de usuario SLSUX15 de HSC
- Definición de la autoridad de acceso al volumen para montar y expulsar volúmenes mediante la salida de usuario SLSUX14 de HSC
- Definición de la autoridad VOLSER de subconjunto nuevo y de conjunto de MVC

- Definición de un segmento de RACF de SMC OMVS para comunicación con un subsistema HSC remoto
- Definición de un segmento de RACF de SMC OMVS para comunicación con un dispositivo VLE

Funciones de seguridad

En este capítulo, se describen los mecanismos de seguridad específicos que ofrece ELS.

3.1. Protección de ELS con AT-TLS (z/OS) únicamente

La utilidad de seguridad de la capa de transporte transparente de la aplicación (AT-TLS) de z/OS de IBM utiliza cifrado de datos de SSL para proteger las aplicaciones TCP/IP de z/OS. Para obtener más información sobre AT-TLS, consulte la publicación de IBM *z/OS Communications Server: IP Configuration Guide* (Servidor de comunicaciones de z/OS: Guía de configuración de IP), y consulte la información sobre el agente de políticas de AT-TLS en la publicación de IBM *z/OS Communications Server: IP Configuration Reference* (Servidor de comunicaciones de z/OS: Referencia de configuración de IP).

La protección de las comunicaciones de cliente/servidor de ELS entre SMC y HSC/VTCS se describe en la documentación técnica de Oracle *Using AT-TLS with HSC/SMC Client/Server z/OS Solution: Implementation Example* (Uso de AT-TLS con la solución de cliente/servidor HSC/SMC [z/OS]: Ejemplo de implementación). Esta documentación técnica está publicada en la sección Productos de almacenamiento en cinta de Oracle Technical Network. Consulte esta publicación para obtener información detallada sobre la configuración.

Para proteger ELS con AT-TLS, Oracle recomienda usar cualquiera de estos algoritmos criptográficos de SSL:

- Familia de SHA-2 (SHA-256, SHA-384, SHA-512)
- AES \geq 128 bits
- RSA \geq 2048 bits
- Diffie-Hellman (DH) \geq 2048 bits
- ECC \geq 256 bits

Cualquier otro algoritmo criptográfico de SSL ofrece una protección más débil y no se debe usar con ELS.

Nota:

El dispositivo StorageTek Virtual Library Extension (VLE) para VSM no admite actualmente las comunicaciones de AT-TLS. No proteja las comunicaciones de VLE de ELS con AT-TLS.

3.2. Uso de la función de seguridad de la XAPI de ELS

ELS 7.3 presenta una nueva función de seguridad de XAPI para la comunicación cliente-servidor, que está activada como opción predeterminada en el servidor HTTP de SMC. La función de seguridad de la XAPI proporciona utilidades de autenticación de usuario adicionales como parte del protocolo de la XAPI, que son internas del ELS y están íntegramente contenidas en este. Para usar la función de seguridad de la XAPI, debe definir credenciales de seguridad (ID de usuario y contraseñas) para los clientes y los servidores de ELS. Las operaciones del ELS 7.3 TapePlex utilizan estas credenciales de seguridad para proteger las transacciones de la XAPI (montaje, desmontaje, consulta de volúmenes, volúmenes nuevos, etc.). El uso de credenciales de seguridad de la XAPI es completamente transparente y no requiere la intervención adicional del usuario ni del operador. Consulte *Configuración y gestión de SMC 7.3* para obtener más información acerca de la configuración de la función de seguridad de la XAPI.

El método preferido para proteger las transacciones de la XAPI en TapePlexes que alojan aplicaciones cliente del ELS solamente (SMC y cliente de VM) es usar las utilidades de AT/TLS como se describe en [Sección 3.1, “Protección de ELS con AT-TLS \(z/OS\) únicamente”](#). AT/TLS es una utilidad de la capa de transporte que es externa y transparente para ELS.

Use la función de seguridad de la XAPI de ELS 7.3 para proteger TapePlexes que alojen clientes que no sean de ELS (clientes de sistemas abiertos) o una combinación de clientes de ELS (SMC y cliente de VM) y clientes que no sean de ELS. AT-TLS se puede usar en estos entornos en combinación con la función de seguridad de la XAPI de ELS 7.3, pero no protegerá las transacciones de la XAPI para los clientes que no sean de ELS.

Consideraciones de seguridad para desarrolladores

En el documento de Oracle *StorageTek Enterprise Library Software: Referencia de programación de ELS*, se describen las interfaces de programación de aplicaciones (API, Application Programming Interface) de ELS disponibles para desarrolladores de aplicaciones. La interfaz de programación de ELS utiliza la interfaz unificada de usuario (UUI, Unified User Interface), que usa la salida de seguridad SLSUX15 del comando HSC para gestionar el acceso a sus funciones sobre la base de la autorización de RACF (o equivalente). Consulte [Sección 2.2, “Configuración posterior a la instalación de ELS”](#), para obtener más información sobre la protección de SLSUX15 con RACF.

Apéndice A

Lista de comprobación de la implementación segura

1. Utilice la protección de la utilidad de control de acceso a recursos (RACF, Resource Access Control Facility) (o equivalente) según se indica en esta guía de seguridad.
2. Restringir el acceso a la red. ELS y las bibliotecas de cintas que gestiona deberían estar protegidos por el firewall corporativo.
3. Proteja el tráfico de red de ELS con la utilidad AT-TLS de IBM o la función de seguridad de la XAPI de ELS si es necesario.
4. Aplique todos los HOLDDATA y los PTF de ELS.
5. Póngase en contacto con la asistencia técnica de Oracle en <http://www.myoraclesupport.com/> si encuentra vulnerabilidades en el software ELS de Oracle.

Apéndice B

Referencias

La documentación de ELS se guarda en bibliotecas organizadas por versión de ELS. Puede acceder a ellas desde la página de documentación de almacenamiento en cinta:

<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html>

