Biblioteca de cintas modulares StorageTek SL150

Guía de seguridad

E40922-03

Junio de 2015

ORACLE

Biblioteca de cintas modulares StorageTek SL150
Guía de seguridad

E40922-03

Tabla de contenidos

Prefacio 7

Destinatarios 7
Accesibilidad a la documentación 7

1. Visión general 9

Visión general del producto 9
Seguridad 9
Principios generales de seguridad 9
Mantener el software actualizado 9
Restringir el acceso a la red 10
Manténgase actualizado sobre la información de seguridad más reciente 10

2. Instalación segura 11

Comprensión del entorno 11
¿Qué recursos necesitan protección? 11
¿De quién se protegen los recursos? 11
¿Qué sucede si falla la protección de los recursos estratégicos? 11
Protección de la biblioteca 11
Configuración de la instalación 12
Asignación de la contraseña del usuario (administrador) 12
Aplicación de la gestión de contraseñas 13
Autenticación de la interfaz de usuario de explorador 13

3. Funciones de seguridad 15

4. Reimplementación 17

A. Lista de comprobación de la implementación segura 19

B. Referencias 21

Lista de tablas

2.1. Puertos de red de SL150 11

Prólogo

En este documento, se describen las características de seguridad del sistema de biblioteca de cintas modular StorageTek SL150, de Oracle.

Destinatarios

Esta guía está destinada a cualquier persona que se encargue de la instalación y la configuración seguras de la biblioteca de cintas modular StorageTek SL150, de Oracle, y la utilización de sus características de seguridad.

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

Visión general

En esta sección, se brinda una visión general de la Biblioteca de cintas modular StorageTek SL150 de Oracle y se explican los principios generales de la seguridad de la biblioteca de cintas.

Visión general del producto

La biblioteca de cintas modular StorageTek SL150 es una biblioteca de cintas automatizada y modular montada en rack de 19 in de 3U a 21U de Oracle Corporation. Ofrece capacidad de almacenamiento de 30 a 300 cartuchos de cinta LTO, de 1 a 20 unidades de canal de fibra LTO o unidades de cinta SAS y una ruta de control de puertos SAS o de canal de fibra de unidad con puente por medio de una de las unidades de cinta instaladas.

Seguridad

Todos los productos de biblioteca de cintas están diseñados y documentados para utilizarse dentro de un entorno de servidor controlado sin acceso general a la red ni acceso de usuarios. Esto ofrece la mejor funcionalidad y protección contra el riesgo, tanto de Internet en general como de una entidad interna que utilice la biblioteca.

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. Las versiones de firmware de LS150 lanzadas desde abril de 2015 son las siguientes:

Junio de 2012 v1.00 (RTA 0.1.0.0.0)
Septiembre de 2012 v1.03 (RTA 0.1.0.3.0)
Octubre de 2012 v1.50 (RTA 0.1.5.0.0)
Enero de 2013 v1.82 (RTA 0.1.8.2.0)
Agosto de 2013 v2.0 (RTA 0.2.0.0.0)
Octubre de 2013 v2.01(RTA 0.2.0.1.0)
Abril de 2014 v2.25 (RTA 0.2.2.5.0)
Junio de 2015 v2.50 (RTA 0.2.5.0.0)

Restringir el acceso a la red

Mantenga la biblioteca protegida por un firewall de 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. Siempre que sea posible, se recomienda identificar los hosts que tienen permitido adjuntarse a la biblioteca y bloquear todos los otros.

Manténgase 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.

2

Instalación segura

En esta sección, se detallan los procesos de planificación para lograr una instalación segura, se describen varias topologías de implementación recomendadas para los sistemas y se explica cómo proteger la biblioteca.

Comprensión del entorno

Para comprender mejor las necesidades de seguridad, deben hacerse las siguientes preguntas.

¿Qué recursos necesitan protección?

Pueden protegerse varios recursos en el entorno de producción. Considere los recursos que necesitan protección al decidir el nivel de seguridad que debe proporcionar.

¿De quién se protegen los recursos?

La biblioteca debe estar protegida contra todos los usuarios de Internet y usuarios de intranet.

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

En algunos casos, un fallo en un esquema de seguridad se detecta fácilmente y se considera nada más que un inconveniente. En otros casos, un fallo podría causar un gran daño a la empresa o a los clientes individuales que usan la biblioteca. Comprender las ramificaciones de la seguridad de cada recurso ayudará a protegerlo correctamente.

Protección de la biblioteca

Por defecto, la biblioteca utiliza puertos detallados en la Tabla 2.1, “Puertos de red de SL150”. El firewall debe estar configurado para permitir que el tráfico utilice estos puertos y que se bloqueen todos los puertos no utilizados.

Tabla 2.1. Puertos de red de SL150

Puerto	Tipo	Descripción
22	TCP	Acceso SSH desde la CLI: entrante con estado Para prueba de desarrollo y depuración solamente; no disponible en el campo
25	TCP	SMTP sin autenticación

Puerto	Tipo	Descripción
67	DHCP	Cliente: saliente
68	DHCP	Cliente: entrante
80	HTTP	Puerto WebLogic para la interfaz de usuario remoto
123	NTP	Protocolo de hora de red (si está activado)
161	UDP	Solicitudes de agente de biblioteca de SNMP: entrante con estado
162	UDP	Notificaciones de información y capturas de SNMP de biblioteca: saliente sin estado para las capturas, saliente con estado para la información
465	TCP	SMTP con SSL o autenticación TLS
443	HTTPS	Puerto WebLogic para la interfaz de usuario remoto para HTTPS
546	DHCPv6	Cliente IPv6 DHCP: saliente
547	DHCPv6	Cliente IPv6 DHCP: entrante
33200-33500	TRACEROUTE	Uso del desarrollo del software

La selección del número de puerto válido para el uso de la biblioteca está reservada o recomendada según la tabla anterior. Los números de puerto legítimos comienzan con el valor numérico 1, ya que cero no es un puerto legítimo.

Al configurar SNMP, se recomienda especialmente el uso de SNMPv3 mediante SNMPv2c debido a sus capacidades de confidencialidad, integridad y autenticación.

Al configurar SMTP, se recomienda especialmente el uso de la autenticación TLS mediante SSL o la opción de no autenticación.

Configuración de la instalación

En esta sección, se documentan los cambios en la configuración de seguridad que deben realizarse durante la instalación.

Asignación de la contraseña del usuario (administrador)

En el primer encendido, un asistente de instalación se ejecuta automáticamente en el panel del operador local a fin de obtener información de configuración básica. Esto incluye el nombre de usuario y contraseña de la cuenta de administrador, la configuración de red, y otros valores de configuración básicos.

Se evita que la biblioteca se vuelva operacional hasta que se complete el asistente de instalación.

Con el envío del producto, se proporciona una cuenta de inicio de sesión en la que el instalador debe ingresar como primer paso de la rutina del asistente de instalación. Luego, el usuario debe introducir una nueva contraseña antes de que se complete el asistente de instalación.

Una vez que el asistente de configuración inicial se ha completado y la biblioteca esté completamente encendida, se pueden efectuar modificaciones adicionales a la configuración de la biblioteca mediante la interfaz de usuario basada en explorador (BUI) para todos los valores de configuración de la biblioteca.

Aplicación de la gestión de contraseñas

Se deben aplicar las reglas de administración de contraseñas básicas, como longitud, historial y complejidad de la contraseña, a todas las contraseñas. Las contraseñas de SL150 deben tener entre 8 y 128 caracteres y deben contener al menos un carácter numérico o especial. La contraseña por defecto debe modificarse durante la instalación y no debe volver a usarse.

Nota:

El número de caracteres que se muestra enmascarado no indica el número exacto de caracteres introducidos.

Autenticación de la interfaz de usuario de explorador

Mantenga la configuración del explorador que se utiliza para acceder a la interfaz del usuario remoto en TLS 1.0 o posterior para mitigar CVE-2014-3566 para niveles de firmware anteriores a la versión 2.50. El firmware de la biblioteca no negociará automáticamente SSLv3 en la versión 2.50.

3

Funciones de seguridad

En esta sección, se describen los mecanismos de seguridad específicos que ofrece el producto.

La biblioteca proporciona un firewall interno para protegerse. Esta no debe ser la única línea de seguridad para proteger la biblioteca. Se recomienda que la biblioteca se encuentre en un centro de datos físicamente protegido en una red segura que solo permita el acceso desde servidores que utilizan su funcionalidad. Estos servidores y las aplicaciones que se ejecutan en ellos también deben ser seguros.

Las cuentas de usuarios deben limitarse al nivel de rol *operador* en lugar de otorgar a todos los usuarios el nivel de rol de *administrador*. Debe practicarse el uso correcto del rol de usuario de *servicio*. Cree, active o desactive las cuentas del rol de usuario de *servicio* según sea necesario. Los roles de servicio tienen mayor privilegio que el rol de *operador* y casi la misma autorización que el rol de *administrador*.

Si se necesita un historial de la actividad de la biblioteca con fines de investigación, se puede revisar el "Log de actividad" y exportarlo para un mayor análisis. El log de actividad de la interfaz de usuario puede mostrar los inicios de sesión de usuarios, host o acciones iniciadas en la interfaz de usuario para rastreabilidad.

4

Reimplementación

En esta sección, se describe cómo se devuelve la biblioteca al estado por defecto de fábrica para borrar los datos del cliente.

En el caso de que el cliente necesite retirar una biblioteca, se proporciona un procedimiento que elimina toda la información de configuración del cliente y todos los archivos de log, y devuelve la biblioteca a su estado por defecto de fábrica. Para invocar este procedimiento se debe colocar la biblioteca en un modo “localizar”, luego, mantener presionados simultáneamente los botones de localización frontal y trasero durante más de diez segundos y, por último, soltar ambos botones.

Cuando se cumpla el tiempo suficiente presionando el botón de localización, el ritmo del parpadeo del indicador LED aumenta.

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. Aplique la administración de contraseñas para todas las cuentas de usuario.
2. Aplique controles de acceso, de proximidad física y mediante interfaces, como SCSI, UI, SNP, etc.
3. Restrinja 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.
   e. Es posible que los servicios dispongan de herramientas que necesitan una contraseña adecuada o controles de acceso supervisados (por ejemplo, SDP-2 para permitir la descarga de información del log u otro acceso).
4. Póngase en contacto con Oracle Services, Oracle Tape Library Engineering o su representante de cuenta si encuentra vulnerabilidades en las bibliotecas de cintas de Oracle.
5. SMTP debe utilizar TLS en lugar de protocolos anteriores, como SSL, o no debe utilizar ninguno.
6. SNMP debe configurarse con el nivel V3 en lugar de V2C o funciones anteriores.

Apéndice B

Referencias

Guía del usuario de SL150 ubicada en:

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#libraries

Toda la documentación relacionada con SL150 se encuentra en el documento en línea con número de referencia E35103-07.