StorageTek T10000D

Guía de seguridad

E50320-04

Agosto de 2016

ORACLE

StorageTek T10000D
Guía de seguridad

E50320-04

Tabla de contenidos

Lista de tablas

Prefacio

En este documento, se describen las funciones de seguridad de StorageTek T10000D, 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 StorageTek T10000D.

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 unidad de cinta StorageTek T10000D y se explican los principios generales de la seguridad de las unidades de cinta.

Visión general del producto

La unidad de cinta empresarial T10000D es compatible con el protocolo SCSI mediante canal de fibra y el protocolo mainframe mediante FICON. La unidad de cinta T10000D transfiere datos a un host y desde él, y los almacena en un soporte magnético extraíble. La unidad de cinta T10000D tiene como objetivo principal proporcionar capacidades de copia de seguridad, archivo y procesamiento de datos de alta confiabilidad y capacidad para los clientes empresariales que exigen confiabilidad y un ciclo de tareas intenso. El producto ofrece cifrado de datos opcional. El cliente tiene la opción de activar la función de cifrado. El producto de unidad de cinta fue mejorado con respecto a la capacidad y a la velocidad nativa de cinta. Asimismo, también se agregaron funciones de administración de datos.

Capacidad y rendimiento de T10000D

La unidad de cinta T10000D tiene hasta 8,5 TB de capacidad y 252 MB por segundo de velocidad nativa de cinta.

Seguridad

La unidad de cinta T10000D está diseñada y documentada para su uso dentro de un entorno de hardware controlado. Las unidades de cinta siempre se ubican en un centro de datos controlado y, generalmente, están dentro de una biblioteca de cintas. En algunos casos, el cliente usará una versión de montaje en rack, pero es poco común. El centro de datos controlado también está dentro de un firewall protegido por las políticas de seguridad propias del cliente. Esto ofrecerá la mejor funcionalidad y protección contra el riesgo, tanto de Internet en general como de una entidad interna que utilice la unidad de cinta.

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 este documento, se asume el siguiente nivel de software:

T10000D 4.XX.1XX

Restringir el acceso a la red

Mantenga la unidad de cinta protegida por un 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 firewalls independientes. Siempre que sea posible, se recomienda identificar los hosts que tienen permitido conectarse a la unidad de cinta y bloquear todos los otros.

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.

2

Capítulo 2. Instalación segura

En esta sección, se detallan los procesos de planificación e implementación para lograr una instalación y una configuración seguras, y se describen varias topologías de implementación recomendadas para los sistemas. Además, se explica cómo proteger una biblioteca de cinta.

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.

¿Contra quién se protegen los recursos?

La unidad de cinta debe estar protegida contra todos los usuarios de Internet. Pero ¿debe protegerse la unidad de cinta contra los empleados de la intranet de su empresa?

¿Qué sucederá si fallan las protecciones 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 unidad de cinta. Comprender las ramificaciones de la seguridad de cada recurso ayudará a protegerlo correctamente.

Protección de la unidad de cinta

De forma predeterminada, la unidad de cinta usa los puertos detallados en la siguiente tabla. El firewall debe estar configurado para permitir que el tráfico utilice estos puertos y que se bloqueen todos los puertos no utilizados. Las unidades de cinta son compatibles con IPv6 e IPv4.

Tabla 2.1. Puertos de red utilizados

Puerto	T10000D
22 tcp - SSH VOP	X

Puerto	T10000D
22 tcp - SFTP	X
161 udp - Solicitudes de agente de unidad de cinta de SNMPV1 (entrante con estado)	X
162 udp - Notificaciones de información y capturas de SNMPV1 de unidad de cinta (saliente sin estado para las capturas, saliente con estado para la información)	X
23 tcp - TELNET	
21 tcp - FTP	
9842 tcp - EPT	
3331 OKM - Servicio CA de desafío y raíz	X
3332 OKM – Inscripción. La potencia cibernética es AES256	X
3334 OKM: Intercambio de claves de cifrado. La potencia cibernética es AES256	X
3335 OKM - Descubrimiento de cluster. La potencia cibernética es AES256	X

Para T10000D, los puertos 21 y 23 se desactivarán para nuestros clientes. Existe una opción de configuración de VOP disponible para el caso en que un cliente requiera acceso a una TELNET no segura y/o a un FTP no seguro.

Instalación de la aplicación del panel del operador virtual (VOP)

VOP solo debe instalarse en sistemas que se encuentren dentro de la misma infraestructura de red protegida que la unidad de cinta. Los controles de acceso del cliente deben aplicarse en los sistemas en los que VOP esté instalado para garantizar el acceso restringido a la unidad de cinta. Consulte Tabla 2.1, “Puertos de red utilizados” para obtener información acerca de los puertos utilizados por VOP.

Consulte la siguiente guía del usuario de VOP para iniciar por Web las instrucciones de instalación de VOP.

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

Configuración posterior a la instalación

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

Asignación de la contraseña del usuario (administrador)

El cliente debe cambiar la contraseña de la cuenta de administrador de cliente en el sitio, y esta contraseña le pertenecerá al cliente. La contraseña de seguridad debe cumplir con los estándares de Oracle. Una cantidad infinita de contraseñas está disponible para su uso durante

el ciclo de vida de la unidad de cinta. Si se olvida la contraseña de administrador, esta puede restablecerse. La primera contraseña es la predeterminada que se envía con la unidad de cinta.

Aplicación de la administración de contraseñas

Se deben aplicar las reglas de administración de contraseñas básicas, como longitud y complejidad de la contraseña, a la contraseña del administrador.

Las reglas de administración de contraseñas deben incluir al menos una de las siguientes reglas.

- Debe tener entre 8 y 16 caracteres de largo
- Minúsculas (a-z)
- Mayúsculas (A-Z)
- Dígito decimal (0-9)
- Caracteres especiales (.?;:"{}[]()!@#$%&, ...)

3

Capítulo 3. Funciones de seguridad

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

La unidad de cinta T10000D se comunica por un canal seguro con el Sistema de administración de claves de Oracle. La unidad de cinta T10000D comunicará SSH y SFTP al panel de operador virtual, y TELNET y FTP se desactivarán para nuestros clientes. Estas no deben ser las únicas líneas de seguridad para proteger la unidad de cinta. Se recomienda que las unidades de cinta se encuentren en un centro de datos físicamente protegido que también tenga una red segura que sólo permita el acceso desde los servidores que utilizan su funcionalidad. Estos servidores y las aplicaciones que se ejecutan en ellos también deben ser seguros. Además, el cliente tiene la opción de elevar la seguridad de la unidad de cinta a otro nivel. Una de las opciones es cifrar los datos.

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 unidad de cinta:

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 monitorearse el acceso al sistema.
   d. Deben comprobarse las direcciones IP de la red.
4. Póngase en contacto con Oracle Services, Oracle Tape Library Engineering o su representante de cuenta si encuentra vulnerabilidades en las unidades de cinta de Oracle.

Apéndice B

Apéndice B. Referencias

Puede acceder a la Guía del usuario de VOP desde:

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