Oracle® Key Manager 3

Guía de seguridad

Versión 3.1

E52200-02

Abril de 2016

ORACLE®

Oracle® Key Manager 3
Guía de seguridad

E52200-02

Tabla de contenidos

Lista de tablas

Prefacio

En este documento, se describen las funciones de seguridad de Oracle Key Manager 3 (OKM 3).

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 OKM 3.

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 del producto y se explican los principios generales de la seguridad de la aplicación.

1.1. Visión general del producto

Oracle Key Manager (OKM) crea, almacena y gestiona claves de cifrado. OKM consta de los siguientes componentes:

- Dispositivo de gestión de claves: una caja de seguridad endurecida que proporciona gestión de claves de ciclo de vida basada en políticas, autenticación, control de acceso y servicios de suministro de claves. Como autoridad de confianza para redes de almacenamiento, el dispositivo de gestión de claves garantiza que todos los dispositivos de almacenamiento estén registrados y autenticados, y que toda creación, suministro y supresión de claves de cifrado se lleve a cabo de conformidad con las políticas establecidas.
- GUI de Oracle Key Manager: una interfaz gráfica de usuario que se ejecuta en una estación de trabajo y se comunica con el dispositivo de gestión de claves mediante una red IP para configurar y gestionar el OKM. La GUI de Oracle Key Manager debe instalarse en una estación de trabajo proporcionada por el cliente.
- CLI de Oracle Key Manager: dos interfaces de línea de comandos que se ejecutan en una estación de trabajo y se comunican con el dispositivo de gestión de claves mediante una red IP para automatizar operaciones administrativas habituales. Las CLI de Oracle Key Manager deben instalarse en una estación de trabajo proporcionada por el cliente.
- Cluster de OKM: el conjunto completo de dispositivos de gestión de claves del sistema. Todos estos dispositivos de gestión de claves se reconocen entre sí y se replican información.
- Agente: un dispositivo o software que efectúa el cifrado mediante el uso de claves gestionadas por el cluster de OKM. Un ejemplo de un agente es una unidad de cinta de cifrado StorageTek. Los agentes se comunican con los dispositivos de gestión de claves mediante el protocolo de agentes KMS. La API de agente es un conjunto de interfaces de software que se incorpora en el software o hardware de agente.

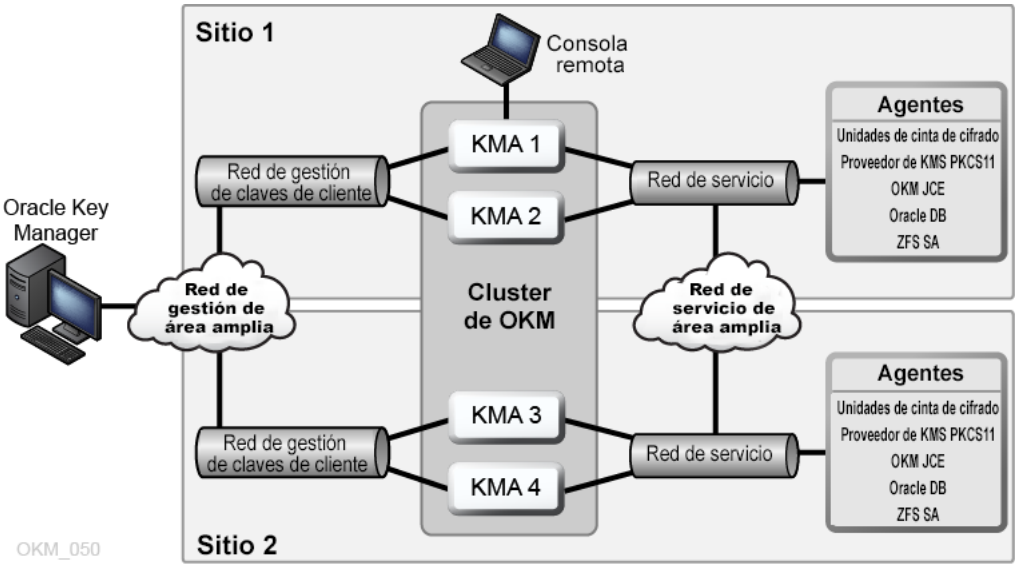
OKM usa redes TCP/IP para establecer conexiones entre los dispositivos de gestión de claves, los agentes y las estaciones de trabajo en las que se ejecutan las CLI y la GUI de Oracle Key Manager. Para establecer conexiones de redes flexibles, se proporcionan tres interfaces para las conexiones de redes en cada dispositivo de gestión de claves:

- Conexión de gestión: sirve para establecer la conexión con la red del cliente

- Conexión de servicio: sirve para establecer la conexión con los agentes
- Conexión ILOM/ELOM: sirve para establecer la conexión con el ILOM o ELOM del dispositivo de gestión de claves

En la siguiente imagen, se muestra un ejemplo:

Figura 1.1.



1.2. Principios generales de seguridad

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

1.2.1. 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. Los instaladores y paquetes de actualización de Oracle Key Manager más recientes están disponibles en el sitio web My Oracle Support: `http://support.oracle.com`.

1.2.2. Restringir el acceso de red a los servicios críticos

Proteja las aplicaciones empresariales con un firewall. 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.

1.2.3. Seguir el principio de privilegios mínimos

El principio de privilegio mínimo indica que los usuarios deben recibir la menor cantidad de privilegios para realizar sus trabajos. El otorgamiento excesivamente ambicioso de

responsabilidades, roles, permisos, etc., puede dejar vulnerable un sistema, en especial al comienzo del ciclo de vida de una organización, cuando hay pocas personas y el trabajo apremia. Los privilegios de usuario deben ser revisados con regularidad para determinar la relevancia en relación con las responsabilidades actuales de los puestos.

1.2.4. Supervisar 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. Cada componente dentro de un sistema tiene algún grado de capacidad de supervisión. Siga los consejos de auditoría de este documento y supervise los registros de auditoría de manera periódica.

1.2.5. Mantenerse actualizado sobre la información de seguridad más reciente

Oracle mejora continuamente su software y su documentación. Visite el sitio web My Oracle Support todos los años para obtener las revisiones.

2

Capítulo 2. Configuración e instalación seguras

En esta sección, se detallan los procesos de planificación para lograr una instalación segura y se describen varias topologías de despliegue recomendadas para los sistemas.

2.1. Comprensión del entorno

Para comprender mejor sus necesidades de seguridad, hágase las siguientes preguntas:

2.1.1. ¿Qué recursos estoy protegiendo?

Pueden protegerse varios recursos en el entorno de producción. Tenga en cuenta los recursos que desea proteger cuando decida qué nivel de seguridad debe proporcionar.

En general, los recursos que se deben proteger primero son los datos. Los demás recursos se detallan aquí porque se asocian con la gestión y la protección de datos. Varias preocupaciones se relacionan con la protección de datos; por ejemplo, perder los datos (es decir, que los datos no estén disponibles) o que los datos se pongan en riesgo o se divulguen a partes no autorizadas.

Las claves criptográficas se usan habitualmente para proteger los datos contra la divulgación no autorizada. Por lo tanto, son otro recurso que hay que proteger. La gestión de claves de alta confiabilidad resulta esencial para mantener la alta disponibilidad de los datos. Otro grupo de recursos que debe protegerse incluye los activos que se encuentran en el cluster de Oracle Key Manager, incluidos los dispositivos de gestión de claves.

2.1.2. ¿De quién estoy protegiendo los recursos?

Estos recursos deben protegerse de todos los que no tengan autoridad para acceder a ellos. Deben protegerse de manera física. Tenga en cuenta cuales de sus empleados necesitan tener acceso a estos recursos. Luego, identifique qué tipos de operaciones debe poder ejecutar cada empleado en el entorno de Oracle Key Manager.

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

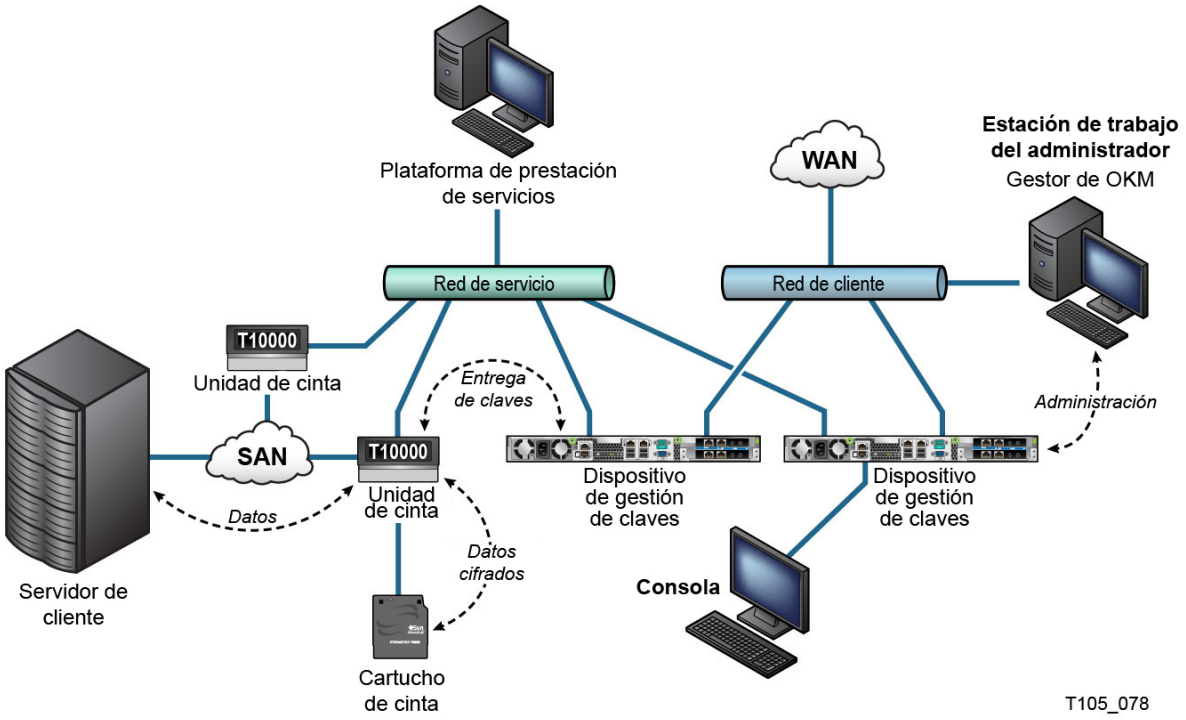
En algunos casos, un fallo en un esquema de seguridad se detecta fácilmente y se considera nada más que un inconveniente. En otros casos, un fallo podría causar un gran daño a las

empresas o a los clientes individuales que usan los recursos. Comprender las ramificaciones de la seguridad de cada recurso ayudará a protegerlo correctamente.

2.2. Topologías de despliegue recomendadas

En la siguiente figura, se muestra un despliegue típico de una solución para Oracle Key Manager.

Figura 2.1. Despliegue típico de una solución OKM



2.3. Instalación de un dispositivo de gestión de claves

En esta sección, se describe cómo instalar y configurar un dispositivo de gestión de claves de OKM de manera segura.

Los dispositivos de gestión de claves se fabrican como dispositivos endurecidos y ya traen disponible la funcionalidad de Oracle Key Manager.

Para instalar y configurar los dispositivos de gestión de claves en un cluster de OKM, se deben seguir estos pasos:

1. Instalar cada dispositivo de gestión de claves en un rack.
2. Para cada dispositivo de gestión de claves, proteger la instancia de ILOM correspondiente.
3. Configurar el primer dispositivo de gestión de claves en el cluster de OKM.

4. Agregar dispositivos de gestión de claves adicionales al cluster de OKM.

En la *Guía de visión general y planificación* de OKM se incluye más información acerca de la planificación del despliegue de un cluster de OKM.

2.3.1. Instalación de un dispositivo de gestión de claves en un rack

Un técnico del servicio al cliente de Oracle instala el dispositivo de gestión de claves en un rack siguiendo los procedimientos que se describen en el *Manual de servicio e instalación de Oracle Key Manager*. El personal del servicio de asistencia de Oracle puede consultar dicho manual para obtener información más detallada.

2.3.2. Protección del ILOM de un dispositivo de gestión de claves

Los dispositivos de gestión de claves de Oracle Key Manager se fabrican con las versiones más recientes de firmware de ILOM. El cliente o un técnico del servicio al cliente de Oracle deben proteger el ILOM del dispositivo de gestión de claves. El ILOM también debe protegerse después de actualizar el firmware de ILOM.

La protección del ILOM implica definir una configuración particular de ILOM, de modo que no se permita realizar cambios en ILOM que pongan en riesgo la seguridad. Para obtener instrucciones, consulte "Endurecimiento de la seguridad de ILOM" en el apéndice Procedimientos del procesador de servicio de la *Guía de administración* de OKM.

2.3.3. Configuración del primer dispositivo de gestión de claves en el cluster de OKM

Antes de configurar el primer dispositivo de gestión de claves, primero identifique las credenciales de división de claves y los ID de usuario y las frases de contraseña que se definirán en este cluster de OKM. Puede usar una hoja de trabajo para hacerlo, como la que se incluye en el *Manual de instalación y servicio* de OKM (solo para uso interno). Consulte con el representante de soporte de Oracle.

Proporcione estas credenciales de división de claves y los ID de usuario y las frases de contraseña al personal correspondiente. Consulte "Protección por quórum" más adelante en este documento para obtener más información.

Nota:

Retenga y proteja estas credenciales de división de claves y los ID de usuario y las frases de contraseña.

Abra un explorador web, inicie la consola remota y, luego, inicie la utilidad QuickStart de OKM dentro de la consola remota. Para inicializar el cluster de OKM en este dispositivo

de gestión de claves, siga el procedimiento de inicialización del cluster que se describe en la *Guía de administración de Oracle Key Manager* que se incluye en las bibliotecas de documentación de Oracle Key Manager.

Durante este procedimiento se definen las credenciales de división de claves y un usuario con privilegios de responsable de la seguridad. Una vez que se completa el procedimiento de QuickStart, el responsable de la seguridad debe iniciar sesión en el dispositivo de gestión de claves y definir usuarios adicionales de OKM.

2.3.4. Consideraciones para definir las credenciales de división de claves

Es más conveniente definir menos frases de contraseña e ID de usuario de división de claves y un umbral inferior, pero es menos seguro. Definir más frases de contraseña e ID de usuario de división de claves y un umbral superior es menos conveniente, pero es más seguro.

2.3.5. Consideraciones para definir usuarios adicionales de OKM

Es más conveniente definir menos usuarios de OKM, de los cuales algunos tengan varios roles asignados, pero es menos seguro. Definir más usuarios de OKM, de los cuales la mayoría tenga solo un rol asignado, es menos conveniente, pero es más seguro, ya que facilita el seguimiento de las operaciones realizadas por un usuario determinado de OKM.

2.3.6. Agregación de dispositivos de gestión de claves adicionales al cluster de OKM

Abra un explorador web, inicie la consola remota y, luego, inicie la utilidad QuickStart de OKM dentro de la consola remota. Para agregar este dispositivo de gestión de claves al cluster de OKM, siga el procedimiento descrito en "Incorporación al cluster" en la *Guía de administración de Oracle Key Manager*, disponible en:

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

2.3.7. Consideraciones para agregar dispositivos de gestión de claves adicionales

Oracle Key Manager ofrece una opción conveniente de desbloqueo autónomo para cada dispositivo de gestión de claves. Esta opción se define durante el procedimiento de QuickStart para el primer dispositivo de gestión de claves y para los adicionales en un cluster, pero el responsable de la seguridad puede modificarla más adelante.

Si el desbloqueo autónomo está activado, el dispositivo de gestión de claves se bloquea automáticamente al inicio y queda listo para proporcionar claves sin necesidad de aprobación

de quórum. Si el desbloqueo autónomo se desactiva, el dispositivo de gestión de claves permanece bloqueado al inicio y no proporciona claves hasta que el responsable de la seguridad emite una solicitud de desbloqueo y un quórum la aprueba.

Para mantener una seguridad máxima, Oracle no recomienda la activación del desbloqueo autónomo. Para obtener más información sobre la opción de desbloqueo autónomo, consulte *Documentación técnica de autenticación y seguridad de Oracle Key Manager versión 2.x* en el siguiente enlace:

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf

2.3.8. Características de los dispositivos de gestión de claves endurecidos

Como se explicó anteriormente, los dispositivos de gestión de claves se fabrican como dispositivos endurecidos y ya traen disponible la funcionalidad de Oracle Key Manager. Como dispositivos endurecidos, tienen las siguientes características:

- Los paquetes de Solaris que no son necesarios no se incluyen en la imagen de Solaris. Por ejemplo, las utilidades y los servicios de ftp y telnet no aparecen en la imagen de Solaris.
- Los dispositivos de gestión de claves no producen archivos principales.
- La utilidad estándar de Solaris login(1) se ha reemplazado con la consola de OKM. Por lo tanto, los usuarios no pueden iniciar sesión en la consola de Solaris.
- El servicio ssh está desactivado por defecto. En los casos de soporte al cliente, el responsable de la seguridad puede activar el servicio ssh y definir una cuenta de soporte durante un período limitado. Esta cuenta de soporte es la única cuenta disponible y tiene permisos y acceso limitados. A continuación, se mencionan comandos de seguimiento de auditoría de Solaris que invoca la cuenta de soporte:
- La cuenta root está desactivada y configurada como rol.
- Los dispositivos de gestión de claves no se equipan con una unidad de DVD.
- Los puertos USB se desactivan correctamente.
- Los puertos de red sin usar se cierran.
- Las pilas no ejecutables están activadas.
- La ejecución aleatoria de consultas en el espacio de direcciones está configurada.
- Los montones no ejecutables están activados.
- Se usa el cifrado de ZFS para los sistemas de archivo confidenciales de seguridad.
- Solaris está configurado de manera de cumplir con la referencia PCI-DSS de SCAP.
- Los servicios de SMF innecesarios están desactivados.
- El inicio verificado de Oracle Solaris se puede configurar en los dispositivos de gestión de claves basados en SPARC T7-1 para proteger el proceso de inicio del sistema, lo cual, a su vez, protege contra el daño de los módulos del núcleo, la inserción de rootkits y otros programas maliciosos.

- Los dispositivos de gestión de claves más nuevos basados en los servidores SPARC T7-1 y Netra SPARC T4-1, dan prueba de alteraciones (fallo de ILOM) si se accede a la puerta del chasis cuando está activo el suministro de energía.
- El firmware de ILOM 3.2 ahora cuenta con la certificación FIPS 140-2 nivel 1 y se lo puede configurar en el modo FIPS.
- La herramienta básica de creación de informes y auditoría se ejecuta periódicamente para facilitar el análisis. Estos informes se incluyen en volcados de sistema de OKM.
- La estructura de seguridad criptográfica de Solaris se configura en función de las políticas de seguridad de FIPS 140-2 nivel 1 (documentado para Solaris 11.1) en presencia o ausencia de un módulo de seguridad de hardware.

2.4. Conexiones TCP/IP y el dispositivo de gestión de claves

Si existe un firewall entre las entidades (OKM Manager, agentes y otros dispositivos de gestión de claves en el mismo cluster) y el dispositivo de gestión de claves, el firewall debe permitir que la entidad establezca conexiones TCP/IP con el dispositivo de gestión de claves en los siguientes puertos:

- La comunicación de OKM Manager a dispositivo de gestión de claves requiere los puertos 3331, 3332, 3333, 3335.
- La comunicación de agente a dispositivo de gestión de claves requiere los puertos 3331, 3332, 3334, 3335.
- La comunicación de dispositivo de gestión de claves a dispositivo de gestión de claves requiere los puertos 3331, 3332, 3336.

Nota:

Para los usuarios que configuran los dispositivos de gestión de claves para usar direcciones IPv6, configure firewalls de borde basados en IPv4 para eliminar los 41 paquetes de IPv4 de salida y los 3544 paquetes de puerto UDP a fin de evitar que los host de Internet utilicen el tráfico de túnel IPv6 sobre IPv4 para llegar a los hosts internos.

Consulte la documentación de configuración de firewall para obtener detalles. En la Tabla 2.1, “Conexiones de puertos de los dispositivos de gestión de claves ” se muestran los puertos explícitamente utilizados por los dispositivos de gestión de claves o los puertos en los que los dispositivos de gestión de claves prestan servicio.

Tabla 2.1. Conexiones de puertos de los dispositivos de gestión de claves

Número de puerto	Protocolo	Dirección	Descripción
22	TCP	Recepción	SSH (únicamente cuando el soporte técnico está activado)
123	TCP/UDP	Recepción	NTP
3331	TCP	Recepción	Servicio CA de OKM
3332	TCP	Recepción	Servicio de certificado de OKM
3333	TCP	Recepción	Servicio de gestión de OKM
3334	TCP	Recepción	Servicio de agente de OKM

Número de puerto	Protocolo	Dirección	Descripción
3335	TCP	Recepción	Servicio de detección de OKM
3336	TCP	Recepción	Servicio de replicación de OKM

En la Tabla 2.2, “Otros servicios ” se muestran otros servicios con recepción en puertos que posiblemente no se utilicen.

Tabla 2.2. Otros servicios

Número de puerto	Protocolo	Dirección	Descripción
53	TCP/UDP	Conexión	DNS (únicamente cuando el dispositivo de gestión de claves está configurado para usar DNS)
68	UDP	Conexión	DHCP (únicamente cuando el dispositivo de gestión de claves está configurado para usar DHCP)
111	TCP/UDP	Recepción	RPC (los dispositivos de gestión de claves responden a consultas rpcinfo); este puerto está abierto a solicitudes externas únicamente en KMS 2.1 y versiones anteriores
161	UDP	Conexión	SNMP (únicamente cuando se definen gestores de SNMP)
161	UDP	Recepción	SNMP (solo si Hardware Management Pack está activado)
514	TCP	Conexión	Syslog remoto (solo si hay servidores de syslog remoto definidos y configurados para usar TCP sin cifrado)
546	UDP	Conexión	DHCPv6 (únicamente cuando el dispositivo de gestión de claves está configurado para usar DHCP e IPv6)
4045	TCP/UDP	Recepción	Daemon de boqueo de NFS (KMS 2.0 únicamente)
6514	TLS mediante TCP	Conexión	Syslog remoto (solo si hay servidores de syslog remoto definidos y configurados para usar TLS)

Nota:

El puerto 443 debe estar abierto para permitir que los clientes accedan a la interfaz web del procesador de servicio y a la consola de OKM a través del firewall. Consulte el *Manual de servicio e instalación de Oracle Key Manager* (solo interno) para ver los puertos ELOM e ILOM.

En la Tabla 2.3, “Puertos de ELOM/ILOM ” se muestran los puertos ELOM/ILOM del dispositivo de gestión de claves. Estos puertos se pueden activar si se requiriere acceso a ELOM/ILOM desde fuera del firewall; de lo contrario, no es necesario activarlos para la dirección IP de ELOM/ILOM:

Tabla 2.3. Puertos de ELOM/ILOM

Número de puerto	Protocolo	Dirección	Descripción
22	TCP	Recepción	SSH (para interfaz de línea de comandos de ELOM/ILOM)

Número de puerto	Protocolo	Dirección	Descripción
53	TCP/UDP	Conexión	DNS (solo se necesita si se configuró DNS)
68	UDP	Conexión	Si se necesita DHCP para ELOM/ILOM. **Nota**: No hay documentación disponible para DHCP y ELOM/ILOM, auque se admiten.
80	TCP	Recepción	HTTP (para la interfaz web de ELOM/ILOM) Si se necesita HTTP; de lo contrario, los usuarios pueden consultar instrucciones para conectarse a la consola remota en los siguientes enlaces: ELOM: http://docs.oracle.com/cd/E19121-01/sf.x2100m2/819-6588-14/819-6588-14.pdf ILOM: http://docs.oracle.com/cd/E19860-01/index.html
161	UDP	Recepción/ Conexión	SNMPv3 (configurable, es el puerto por defecto)
443	TCP /TLS	Recepción	Embedded/Integrated Lights Out Manager Servicios web de Desktop Management Task Force (DMTF) para protocolo de gestión (WS-Man) mediante seguridad de capa de transporte (TLS)
623	UDP	Recepción	interfaz inteligente de gestión de plataformas (IPMI)

3

Capítulo 3. Funciones de seguridad

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

3.1. Amenazas potenciales

Los clientes que tienen agentes con cifrado activado se preocupan fundamentalmente por lo siguiente:

- Divulgación de información por incumplimiento de políticas
- Pérdida o destrucción de datos
- Demora inaceptable en la restauración de los datos en caso de fallo catastrófico (por ejemplo, en un sitio donde la continuidad comercial se vea afectada)
- Modificación de datos no detectada

3.2. Objetivos de las funciones de seguridad

Los objetivos de las funciones de seguridad de Oracle Key Manager son los siguientes:

- Proteger datos cifrados contra la divulgación.
- Minimizar la exposición a ataques.
- Proporcionar suficiente fiabilidad y disponibilidad.

3.3. El modelo de seguridad

En esta sección de la guía de seguridad, se intenta ofrecer una visión general de las amenazas contra las que el sistema está diseñado para proteger y del modo en que se combinan las funciones de seguridad individuales para evitar ataques.

Las funciones de seguridad críticas que brindan estas protecciones son:

- Autenticación: garantiza que solo las personas autorizadas puedan acceder al sistema y a los datos.
- Autorización: privilegios y datos de control de acceso al sistema; este control de acceso complementa la autenticación para garantizar que solo las personas adecuadas tengan acceso.

- Auditoría: permite a los administradores detectar los intentos de violación del mecanismo de autenticación y los intentos de violación o las violaciones del control de acceso.

Para obtener más información sobre cuestiones de autenticación y seguridad relativas a Oracle Key Manager, consulte *Documentación técnica de autenticación y seguridad de Oracle Key Manager versión 2.x* en:

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf

3.4. Autenticación

La arquitectura de Oracle Key Manager proporciona autenticación mutua entre todos los elementos del sistema: de dispositivo de gestión de claves a dispositivo de gestión de claves, de agente a dispositivo de gestión de claves y de la CLI o la GUI de Oracle Key Manager al dispositivo de gestión de claves para las operaciones de usuario.

Cada elemento del sistema (por ejemplo, un nuevo agente de cifrado) se incorpora al sistema mediante la creación de un ID y una frase de contraseña en el OKM que, luego, se introduce en el elemento que se va a agregar. Por ejemplo, cuando se agrega una unidad de cinta al sistema, el agente y el dispositivo de gestión de claves ejecutan automáticamente un protocolo de desafío/respuesta que se basa en la frase de contraseña compartida y permite que el agente obtenga el certificado de autoridad de certificación root y un nuevo par de claves junto con un certificado firmado para el agente. Con el certificado de autoridad de certificación root, el certificado de agente y el par de claves en su lugar, el agente puede ejecutar el protocolo de seguridad de capa de transporte (TLS) para todas las comunicaciones subsiguientes con los dispositivos de gestión de claves. Todos los certificados son certificados X.509.

OKM actúa como autoridad de certificación root para generar un certificado root que los dispositivos de gestión de claves usan cuando es necesario para derivar (autofirmar) los certificados empleados por los agentes, los usuarios y los nuevos dispositivos de gestión de claves.

3.5. Control de acceso

El control de acceso puede ser de los siguientes tipos:

- Control de acceso basado en roles y usuarios
- Protección por quórum

3.5.1. Control de acceso basado en roles y usuarios

Oracle Key Manager proporciona la capacidad de definir varios usuarios, cada uno con un ID de usuario y una frase de contraseña. A cada usuario se le otorga uno o más roles predefinidos. Estos roles determinan qué operaciones puede realizar un usuario en un sistema de Oracle Key Manager. Estos roles son los siguientes:

- Responsable de la seguridad: gestión y configuración de Oracle Key Manager
- Operador: configuración de agentes y operaciones diarias
- Responsable de conformidad: definición de grupos de claves y control de acceso de agentes a grupos de claves
- Operado de copias de seguridad: ejecución de operaciones relativas a las copias de seguridad
- Auditor: supervisión de pistas de auditoría del sistema
- Miembro del quórum: supervisión y aprobación de operaciones de quórum pendientes

El responsable de la seguridad se define durante el proceso de QuickStart, donde se configura un dispositivo de gestión de claves en un cluster de OKM. Luego, un usuario debe iniciar sesión en el cluster como responsable de la seguridad mediante la GUI de Oracle Key Manager a fin de crear usuarios adicionales. El responsable de la seguridad puede optar por asignar varios roles a un usuario en particular, o bien puede asignar un rol en particular a varios usuarios.

Para obtener más información acerca de las operaciones permitidas por cada rol y el modo en que un responsable de seguridad crea usuarios y les asigna roles, consulte la *Guía de administración de Oracle Key Manager* que se incluye en las bibliotecas de documentación de Oracle Key Manager en el siguiente enlace:

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

Este control de acceso basado en roles admite los roles operativos de la publicación especial 800-60 del National Institute of Standards and Technology (NIST) para separar funciones operativas.

3.5.2. Protección por quórum

Algunas operaciones son tan críticas que requieren un nivel de seguridad adicional. Entre estas operaciones, se incluye la agregación de un dispositivo de gestión de claves a un cluster de OKM, el desbloqueo de un dispositivo de gestión de claves, la creación de usuarios y la agregación de roles a usuarios. Para implementar esta seguridad, el sistema usa un conjunto de credenciales de división de claves, además del acceso basado en roles descrito anteriormente.

Las credenciales de división de claves son un conjunto de pares de ID de usuario y frases de contraseña más la cantidad mínima necesaria de estos pares para que el sistema active la compleción de ciertas operaciones. A las credenciales de división de claves también se las llama "quórum" y a la cantidad mínima, "umbral de quórum".

Oracle Key Manager permite hasta diez pares de ID de usuario y frase de contraseña de división de claves, y un umbral que debe definirse. Estos se definen durante el proceso de QuickStart, cuando se configura el primer dispositivo de gestión de claves en un cluster de

OKM. Los ID de usuario y las frases de contraseña de división de claves difieren de los ID de usuario y las frases de contraseña que se usan para iniciar sesión en el sistema. Cuando un usuario intenta realizar una operación que requiere la aprobación del quórum, el umbral definido de ID de usuario y frases de contraseña de división de claves debe aprobar dicha operación antes de que el sistema la ejecute.

3.6. Auditorías

Cada dispositivo de gestión de claves registra los eventos de auditoría para las operaciones que realiza, incluidas las emitidas por agentes, usuarios y dispositivos de gestión de claves pares en el cluster de OKM. Los dispositivos de gestión de claves también registran eventos de auditoría cuando un agente, un usuario o un dispositivo de gestión de claves par no logra autoautenticarse. Se registran los eventos de auditoría que indican una infracción de seguridad. El fallo de autenticación es un ejemplo de un evento de auditoría que indica una infracción de seguridad. Si los agentes SNMP se identifican en el cluster de OKM, los dispositivos de gestión de claves también envían el comando SNMP INFORM a los agentes SNMP si detectan una infracción de seguridad. Si syslog remoto está configurado, el dispositivo de gestión de claves también envía estos mensajes de auditoría a servidores configurados. Consulte "*Syslog remoto* ".

El usuario debe iniciar sesión correctamente en el cluster de OKM y debe tener un rol asignado antes de que se le permita ver los eventos de auditoría.

Los dispositivos de gestión de claves gestionan sus eventos de auditoría. Los dispositivos de gestión de claves eliminan eventos de auditoría antiguos en función de los límites y los términos de retención (recuentos). El responsable de la seguridad puede modificar estos límites y términos de retención según sea necesario.

3.7. Otras funciones de seguridad

Oracle Key Manager proporciona otras funciones de seguridad. Para obtener más información sobre estas y otras funciones de OKM, consulte *Visión general de Oracle Key Manager* en el siguiente enlace:

`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf`

3.7.1. Comunicación segura

El protocolo de comunicación entre un agente y un dispositivo de gestión de claves, un usuario y un dispositivo de gestión de claves y un dispositivo de gestión de claves y un dispositivo de gestión de claves par es el mismo. En cada caso, el sistema usa una frase de contraseña para la entidad que inicia la comunicación para ejecutar un protocolo de desafío/respuesta. Si el proceso se realiza correctamente, la entidad obtiene un certificado y la clave privada correspondiente. Este certificado y la clave privada pueden establecer un canal de seguridad de capa de transporte (TLS) (sockets seguros). Se efectúa la autenticación mutua, y

cada punto final de cualquier conexión autentica a la otra parte. En OKM 3.1 con dispositivos de gestión de claves, siempre se usa TLS 1.2 para el tráfico de replicación entre pares.

3.7.2. Módulo de seguridad de hardware

Los dispositivos de gestión de claves tienen un módulo de seguridad de hardware disponible, el cual se pide por separado. Este módulo de seguridad de hardware, que es una tarjeta Sun Cryptographic Accelerator (SCA) 6000, obtuvo la certificación FIPS 140-2 nivel 3 y proporciona claves de cifrado del estándar de cifrado avanzado (AES) de 256 bits (este certificado caducó el 31 de diciembre de 2015 y no se renovará, se proporcionará un módulo de seguridad de hardware alternativo en una versión posterior). La tarjeta SCA 6000 admite un modo operativo de FIPS 140-2, nivel 3, y OKM usa siempre la tarjeta en este modo. Cuando el cluster de OKM opera en un modo que cumple con FIPS, las claves de cifrado no dejan el límite criptográfico de la tarjeta SCA 6000 en modo no encapsulado. La tarjeta SCA 6000 usa un generador de números aleatorios aprobado por FIPS, según lo especificado en el estándar DSA de generador de números aleatorios FIPS 186-2 mediante el uso de SHA-1 para generar claves de cifrado.

Cuando un dispositivo de gestión de claves no se configura con una tarjeta SCA 6000, la criptografía se realiza con un token variable de PKCS#11 de la estructura criptográfica de Solaris (SCF). La SCF se configura en el modo FIPS 140, según se describe en las políticas de seguridad FIPS 140-2 de Solaris más recientes.

3.7.3. Encapsulado de clave de AES

Oracle Key Manager usa el encapsulado de claves de AES (RFC 3994) con claves de cifrado de clave de 256 bits para proteger las claves simétricas cuando se crean, se almacenan en el dispositivo de gestión de claves, se transmiten a agentes o entre archivos de transferencia de claves.

3.7.4. Replicación de claves

Cuando el primer dispositivo de gestión de claves de un cluster de OKM se inicia, el dispositivo de gestión de claves genera una gran agrupación de claves. Cuando se agregan dispositivos de gestión de claves adicionales al cluster, las claves se replican en los nuevos dispositivos de gestión de claves y así quedan listos para usar para cifrar datos. Cada dispositivo de gestión de claves que se agrega al cluster genera una agrupación de claves y las replica en dispositivos de gestión de claves pares en el cluster. Todos los dispositivos de gestión de claves generan nuevas claves en la medida de lo necesario para mantener el tamaño de la agrupación de claves, de modo que las claves listas estén siempre disponibles para los agentes. Cuando un agente requiere una nueva clave, el agente contacta con un dispositivo de gestión de claves en el cluster y solicita una nueva clave. El dispositivo de gestión de claves toma una clave lista de la agrupación de claves y la asigna al grupo de claves por defecto del agente y a la unidad de datos. Luego, el dispositivo de gestión de claves replica las actualizaciones de bases de datos en toda la red para los demás dispositivos de gestión de claves del cluster. Más adelante, el agente puede contactar con otro dispositivo

de gestión de claves en el cluster para recuperar la clave. En ningún momento se transmite ningún material de clave de texto no cifrado en la red.

3.7.5. Políticas de seguridad FIPS 140-2 de Solaris

En diciembre de 2013, el Instituto Nacional de Normas y Tecnología (NIST, National Institute of Standards and Technology) otorgó el certificado de validación FIPS 140-2 nivel 1 N.º 2061 al módulo de estructura criptográfica de núcleo de Oracle Solaris en Solaris 11. En enero de 2014, el NIST otorgó el certificado de validación FIPS 140-2 nivel 1 N.º 2076 a la estructura criptográfica de espacio de usuario de Oracle Solaris con SPARC T4 y SPARC T5. El dispositivo de gestión de claves Oracle Key Manager 3.1.0 ahora se basa en Solaris 11 .3, que todavía se está sometiendo a las pruebas de validación de FIPS 140-2. La estructura criptográfica de núcleo de Oracle Solaris de un dispositivo de gestión de claves Oracle Key Manager 3.1.0 se configura según lo detallado en *Política de seguridad de estructura criptográfica de núcleo de Oracle*. Asimismo, el dispositivo de gestión de claves también se configura según lo detallado en *Política de seguridad de estructura criptográfica de espacio de usuario de Oracle Solaris con SPARC T4 y T5*. OKM se actualizará con políticas de seguridad más recientes de Solaris a medida que dichas políticas estén disponibles.

3.7.6. Actualizaciones de software

Todos los paquetes de actualización de software de los dispositivos de gestión de claves tienen firma digital para evitar la carga de software peligroso de fuentes no aprobadas.

4

Capítulo 4. Puntos finales

OKM admite una variedad de puntos finales de cifrado. Los siguientes son los puntos finales admitidos:

- Unidades de cinta con capacidad de cifrado
- Cifrado de base de datos transparente (TDE) 11g de Oracle, y superiores
- Oracle ZFS Storage Appliance
- Sistemas de archivos Oracle Solaris 11 ZFS

Asimismo, hay herramientas de punto final disponibles para desarrolladores de aplicaciones o, en el caso de PKCS#11, para uso con el cifrado de base de datos transparente (TDE) de la base de datos de Oracle.

4.1. Proveedor de KMS PKCS#11 para Linux

Hay un proveedor de KMS PKCS#11 para Linux disponible para los clientes que deseen comunicarse con OKM mediante PKCS#11. El administrador puede descargar el proveedor de KMS PKCS#11 para Linux desde el sitio web My Oracle Support e instalarlo en el servidor Oracle Enterprise Linux. El proveedor de KMS PKCS#11 para Linux tiene las mismas características de seguridad y se autentica con los dispositivos de Oracle Key Manager de igual modo que los otros agentes. El proveedor de KMS PKCS#11 para Linux almacena un archivo log e información de perfil en el directorio `/var/opt/kms/username`. El usuario y el administrador deben gestionar el archivo log manualmente o mediante una utilidad como logrotate. El control del acceso al directorio `/var/opt/kms/username` debe restringirse mediante los permisos adecuados. En el directorio del perfil, las credenciales de autenticación del agente se retienen en un archivo PKCS#12. El archivo PKCS#12 se protege con una contraseña. Para obtener más información sobre el proveedor de KMS PKCS#11 para Linux, consulte la *Guía de administración de Oracle Key Manager*, incluida en las bibliotecas de documentación de Oracle Key Manager que se encuentran en el siguiente enlace:

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

4.2. Proveedor de KMS PKCS#11 para Solaris

Hay un proveedor de KMS PKCS#11 análogo disponible con Solaris 10 y Solaris 11.

4.3. Proveedor de KMS JCE

Hay un proveedor de Java Cryptographic Environment disponible para desarrolladores que deseen implementar aplicaciones de cliente de Java que puedan obtener claves de OKM. Este producto se integró con diversos productos de Oracle y está disponible en Oracle Technology Network.

4.4. Plugin de OKM para Oracle Enterprise Manager

El plugin del dispositivo de Oracle Key Manager (OKM) para Oracle Enterprise Manager (OEM) Cloud Control proporciona supervisión para clusters de OKM. Cada dispositivo de gestión de claves que pertenece a un cluster se supervisa mediante el plugin. Se proporciona una guía de seguridad para esta herramienta.

5

Capítulo 5. Syslog remoto

Oracle Key Manager admite syslog remoto. Los dispositivos de gestión de claves se pueden configurar para enviar mensajes en formato RFC 3164 o RFC 5424 a un servidor de syslog remoto mediante TCP sin cifrar o seguridad de capa de transporte (TLS). Tenga en cuenta que RFC 5425 describe el uso de TLS para proporcionar una conexión segura para el transporte de mensajes de syslog en formato RFC 5424.

Un responsable de seguridad puede configurar un dispositivo de gestión de claves para enviar mensajes por medio de TCP sin cifrar o TLS. Es más seguro usar TLS para autenticar y cifrar las comunicaciones entre el dispositivo de gestión de claves y un servidor de syslog remoto. El dispositivo de gestión de claves autentica el servidor de syslog remoto mediante la solicitud del certificado y la clave pública correspondientes. De manera opcional, el servidor de syslog remoto se puede configurar para usar autenticación mutua. La autenticación mutua garantiza que el servidor de syslog remoto acepte mensajes solo de clientes autorizados (como los dispositivos de gestión de claves). Si se lo configura para usar autenticación mutua, el servidor de syslog remoto solicita un certificado al dispositivo de gestión de claves para verificar la identidad del dispositivo de gestión de claves.

6

Capítulo 6. Hardware Management Pack

Oracle Key Manager es compatible con Oracle Hardware Management Pack (HMP) en los dispositivos de gestión de claves SPARC T7-1, Netra SPARC T4-1 y Sun Fire X4170 M2. El producto HMP pertenece al grupo de gestión de sistemas únicos de Oracle al igual que ILOM. Un responsable de seguridad puede activar HMP en un dispositivo de gestión de claves para usar un agente de gestión en Solaris para activar la supervisión en banda del dispositivo de gestión de claves por medio de SNMP. El software de HMP viene preinstalado pero desactivado en la configuración de agente de SNMP. En consecuencia, el puerto de recepción del agente de SNMP no se abre hasta que se activa HMP. HMP está desactivado por defecto.

La activación de HMP proporciona lo siguiente:

- Notificación de eventos de problemas de hardware antes de que aparezcan como notificaciones de SNMP específicas de Oracle Key Manager o como interrupción de dispositivos de gestión de claves.
- Posibilidad de activar HMP en cualquiera de los dispositivos de gestión de claves admitidos en un cluster de OKM, o en todos ellos.
- Posibilidad de usar operaciones get de SNMP de solo lectura para MIB de SNMP en el dispositivo de gestión de claves, incluidas MIB-II, SUN-HW-MONITORING-MIB y SUN-STORAGE-MIB.
- Integración de Oracle Red Stack con Oracle Enterprise Manager por medio de receivelets de SNMP y fetchlets de SNMP.

Debe tener presentes las siguientes consideraciones de seguridad al decidir activar HMP en un dispositivo de gestión de claves. Cuando está activado, HMP:

- Aprovecha los gestores del protocolo v2c SNMP activados configurados en el cluster de Oracle Key Manager. El protocolo SNMP v2c no tiene las mejoras de seguridad que aparecen en el protocolo SNMP v3.
- Se activa el agente de gestión de SNMP en el dispositivo de gestión de claves, lo que permite el acceso de red de solo lectura a la información de MIB de SNMP en este dispositivo de gestión de claves.
- Los riesgos de seguridad identificados en la *Guía de seguridad de Oracle Hardware Management Pack (HMP)* (`http://docs.oracle.com/cd/E20451_01/pdf/E27799.pdf`) se mitigan mediante lo siguiente:

- "Los productos de gestión del sistema pueden usarse para obtener un entorno raíz de inicio”: el endurecimiento de los dispositivos de gestión de claves desactiva el acceso root para los usuarios del sistema. SNMP se configura para acceso de solo lectura. Por lo tanto, se rechazan las operaciones put de SNMP.
- "Los productos de gestión del sistema incluyen potentes herramientas que requieren privilegios de usuario root o administrador para la ejecución”: el acceso root a los dispositivos de gestión de claves está desactivado. Por lo tanto, los usuarios del sistema no pueden ejecutar estas herramientas.

Apéndice A

Apéndice A. Lista de comprobación de despliegue seguro

En la siguiente lista de comprobación de seguridad se incluyen directrices que lo ayudan a proteger el sistema de gestión de claves:

1. Instale cada dispositivo de gestión de claves en un entorno físicamente seguro.
2. Proteja OpenBoot PROM o el BIOS en cada dispositivo de gestión de claves.
3. Proteja Lights Out Manager en cada dispositivo de gestión de claves.
4. Defina la configuración de división de claves para este cluster de Oracle Key Manager.
5. Defina la configuración de desbloqueo autónomo para cada dispositivo de gestión de claves, según corresponda.
6. Defina los usuarios de Oracle Key Manager y sus roles asociados.
7. Guíese por el principio del menor privilegio.
   a. Otorgue a cada usuario de Oracle Key Manager solamente los roles necesarios.
8. Supervise la actividad en el cluster de Oracle Key Manager.
   a. Investigue cualquier error que se registre en el log de auditoría de Oracle Key Manager, especialmente las infracciones de la seguridad.
9. Realice una copia de seguridad básica cuando se defina inicialmente la configuración de división de claves y cada vez que esta se modifique.
10. Realice copias de seguridad de Oracle Key Manager con regularidad.
11. Almacene los archivos de copias de seguridad básica y los archivos de copias de seguridad de Oracle Key Manager en una ubicación segura.

Apéndice B

Apéndice B. Referencias

- Documentación para clientes de Oracle Key Manager

  http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto
- *Guía de seguridad de Oracle Enterprise Manager System Monitoring Plug-in for Oracle Key Manager*
- *Manual de instalación y servicio de Oracle Key Manager* (solo interno)
- *Visión general de Oracle Key Manager*

  http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf
- *Documentación técnica de autenticación y seguridad de Oracle Key Manager versión 2.X*

  http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf
- Documentación de Oracle Integrated Lights Out Manager (ILOM)

  http://docs.oracle.com/cd/E37444_01/
- Documentación del servidor SPARC T7-1 https://docs.oracle.com/cd/E54976_01/
- Documentación del servidor Netra SPARC T4-1

  http://docs.oracle.com/cd/E23203_01/
- Documentación de Oracle Hardware Management Pack
  - Biblioteca de documentación de Oracle Hardware Management Pack

    http://docs.oracle.com/cd/E20451_01/
  - Gestión de sistemas únicos de Oracle

    http://www.oracle.com/technetwork/server-storage/servermgmt/overview/index.html
- Documentación de NIST:
  - *Publicación especial 800-60, volumen I, revisión 1, de National Institute of Standards and Technology*

    http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

- Documentación de política de seguridad para productos de Oracle:
  - *Política de seguridad de estructura criptográfica de núcleo de Oracle Solaris*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2061.pdf
  - *Política de seguridad de estructura criptográfica de núcleo de Oracle Solaris con SPARC T4 y T5*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2060.pdf
  - *Política de seguridad de Sun Cryptographic Accelerator 6000 FIPS 140-2*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1050.pdf
  - *Política de seguridad de unidad de cinta Oracle StorageTek T10000D*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2254.pdf
  - *Política de seguridad de unidad de cinta Oracle StorageTek T10000C*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1561.pdf
  - *Política de seguridad de unidad de cinta Oracle StorageTek T10000B*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1156.pdf
  - *Política de seguridad de unidad de cinta Oracle StorageTek T10000A*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1157.pdf
  - *Política de seguridad de unidad de cinta Oracle StorageTek T9480D*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1288.pdf
- Certificados de validación de FIPS para productos Oracle:
  - Sun Crypto Accelerator 6000: certificado N.º 1026 (caducado)

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1026.pdf