Guía de seguridad de Oracle SuperCluster serie M7

Referencia: E69652-01
Febrero de 2016

Referencia: E69652-01

Accesibilidad a la documentación

Para obtener información acerca del 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 Oracle Support

Los clientes de Oracle que hayan adquirido servicios de soporte disponen de acceso a soporte electrónico a través de My Oracle Support.. Para obtener información, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` o `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si tiene problemas de audición.

Contenido

Uso de esta documentación

- **Visión general**: proporciona información acerca de la planificación, la configuración y el mantenimiento de un entorno seguro para los sistemas Oracle SuperCluster serie M7.
- **Destinatarios**: técnicos, administradores de sistemas y proveedores de servicio autorizados.
- **Conocimiento requerido**: experiencia avanzada en UNIX y administración de bases de datos.

Biblioteca de documentación del producto

La documentación y los recursos para este producto y los productos relacionados se encuentran disponibles en http://www.oracle.com/goto/sc-m7/docs.

Comentarios

Escriba sus comentarios sobre esta documentación en http://www.oracle.com/goto/docfeedback.

Descripción de los principios de seguridad

Esta guía proporciona información acerca de la planificación, la configuración y el mantenimiento de un entorno seguro para los sistemas Oracle SuperCluster serie M7.

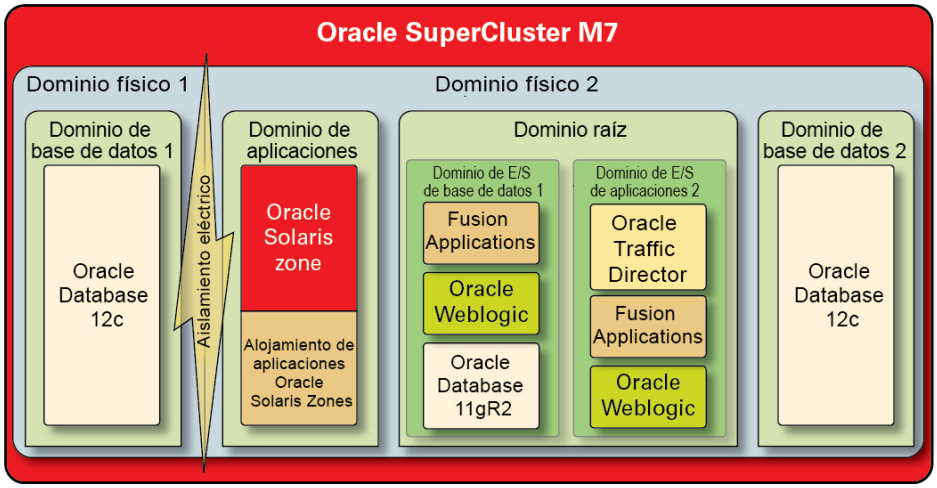
En esta sección, se incluyen los siguientes temas:

Aislamiento seguro

SuperCluster M7 admite una variedad de estrategias de aislamiento que los proveedores de la nube pueden seleccionar según sus requisitos de seguridad y garantía. Esta flexibilidad permite a los proveedores de la nube crear una arquitectura de varios inquilinos segura y personalizada para su empresa.

SuperCluster M7 admite una variedad de estrategias de aislamiento de carga de trabajo, con su propio juego exclusivo de capacidades. Si bien cada estrategia de implementación se puede usar de manera independiente, también se pueden usar en conjunto en un enfoque híbrido que permite a los proveedores de la nube implementar arquitecturas que pueden equilibrar su seguridad, rendimiento, necesidades de disponibilidad y otras necesidades de manera más eficaz.

FIGURA 1 Aislamiento seguro con configuración de inquilinos dinámica



Los proveedores de la nube pueden usar dominios físicos (también denominados PDomains) para situaciones en las que los hosts inquilinos están ejecutando aplicaciones y bases de datos que se deben aislar físicamente de otras cargas de trabajo. Es posible que los recursos físicos dedicados se requieran para un despliegue debido a su importancia para la organización, la confidencialidad de la información que contienen, los mandatos de conformidad o simplemente porque la carga de trabajo de la base de datos o la aplicación usará por completo los recursos de un sistema físico completo.

Para las organizaciones que requieren aislamiento mediado por hipervisor, los dominios de Oracle VM Server for SPARC, conocidos como dominios dedicados, se usan para crear entornos virtuales que aíslan instancias de bases de datos o aplicaciones. Los dominios dedicados se crean como parte de la instalación de SuperCluster y cada uno ejecuta su propia instancia única del sistema operativo Oracle Solaris. El acceso a los recursos físicos está mediado por los hipervisores asistidos por hardware desarrollados en los procesadores de SPARC.

Además, SuperCluster le permite crear dominios adicionales que se conocen como dominios raíz, que aprovechan la tecnología de virtualización de E/S de raíz simple (SR-IOV). Los dominios raíz tienen uno o dos HCA IB y 10 NIC GbE. Puede elegir crear dominios adicionales de forma dinámica, conocidos como dominios de E/S, en la parte superior de los dominios raíz. SuperCluster M7 incluye una herramienta basada en explorador para crearlos y gestionarlos.

Sin embargo, dentro de cada uno de estos dominios, los inquilinos consumidores de la nube pueden aprovechar la tecnología Oracle Solaris Zones para crear entornos aislados adicionales. Mediante el uso de zonas, es posible implementar instancias de base de datos o aplicación individuales o grupos de instancias de base de datos o aplicaciones en uno o más contenedores virtualizados que, en conjunto, se ejecutan sobre un único núcleo de sistema operativo. Este enfoque ligero a la virtualización se usa para crear un límite de seguridad más eficaz en los servicios implementados.

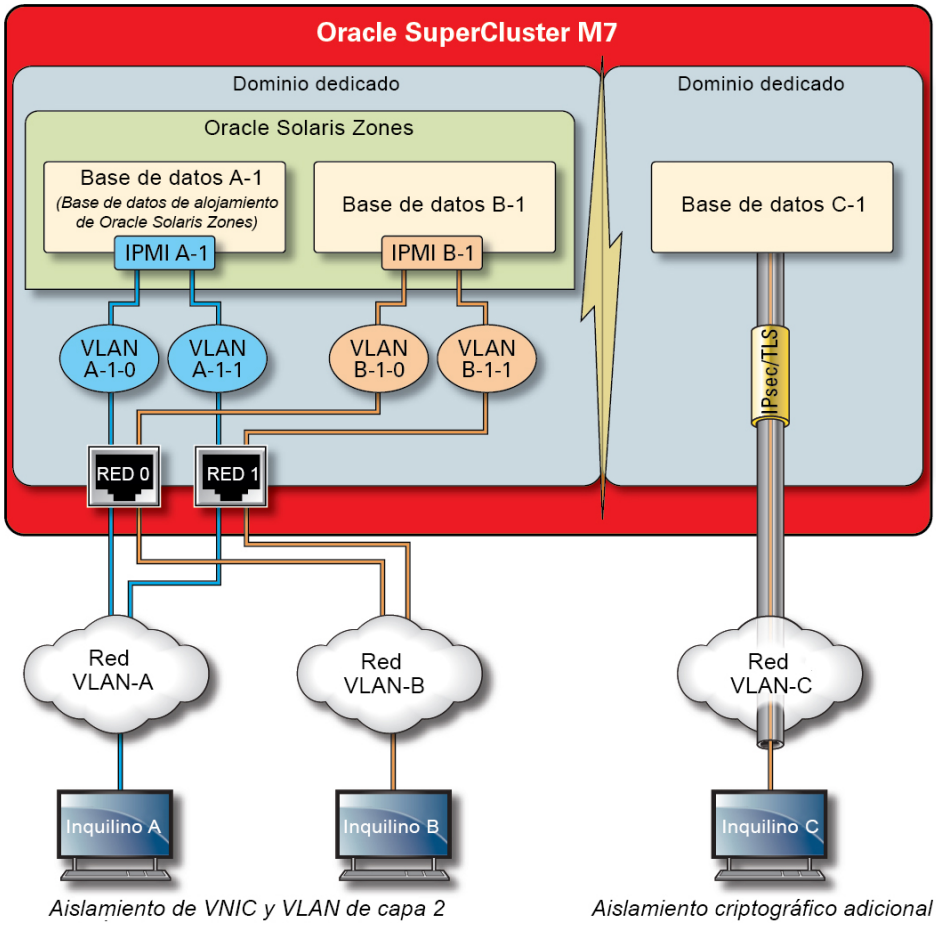
Los inquilinos que alojan varias aplicaciones o bases de datos en SuperCluster también pueden optar por implementar un enfoque híbrido, mediante una combinación de estrategias de aislamiento basadas en Oracle Solaris Zones, dominios de E/S y dominios dedicados para crear arquitecturas flexibles y resistentes que se alinean con sus necesidades de infraestructura de nube. Gracias a una variedad de opciones de virtualización, SuperCluster permite que los inquilinos alojados en nube se aíslen de manera segura en la capa de hardware y proporciona a Oracle Solaris Zones seguridad mejorada y mayor aislamiento en el entorno de tiempo de ejecución.

Garantizar que las aplicaciones, las bases de datos, los usuarios y los procesos individuales se aíslen correctamente en el sistema operativo del host es un primer buen paso. Sin embargo, es igualmente importante considerar las tres redes principales usadas en SuperCluster y la manera en la que la que se protegen las capacidades de aislamiento de red y las comunicaciones que fluyen por la red:

- Red de acceso de cliente de 10 GbE
- Red de servicio de IB privada
- Red de gestión

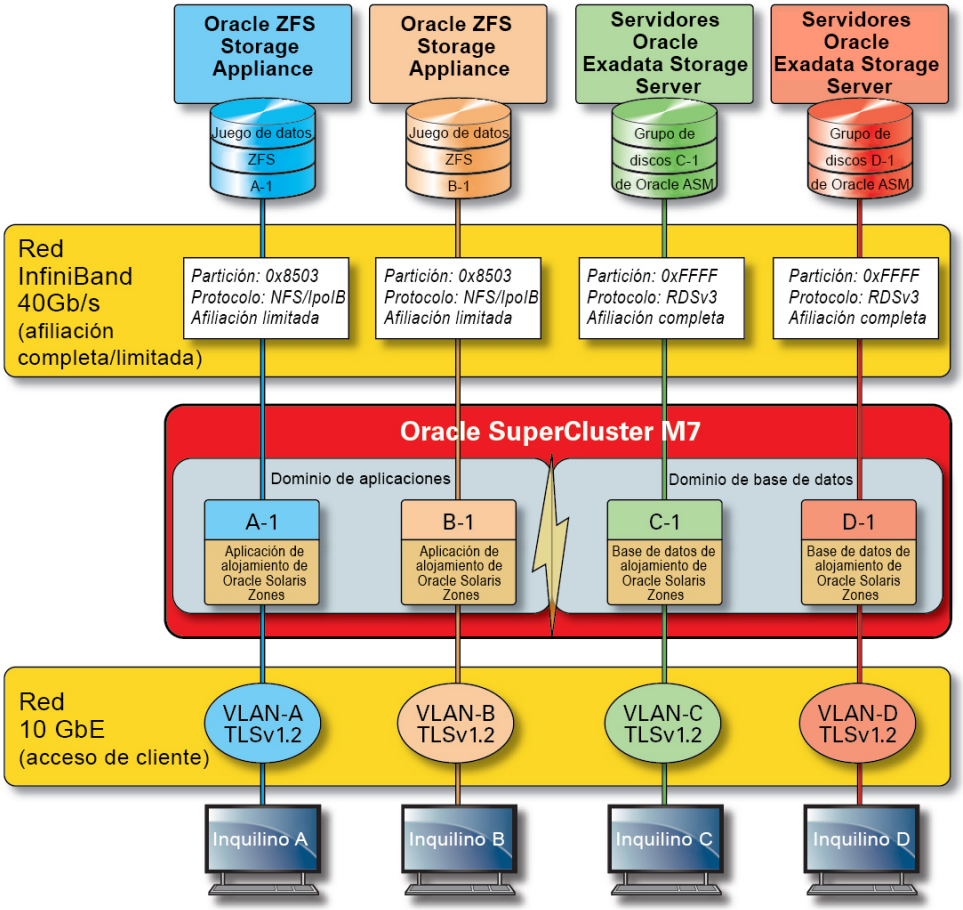
El tráfico de red que fluye en la red de acceso de cliente de SuperCluster se puede aislar mediante una variedad de técnicas. En esta figura, se muestra una configuración posible en la que se configuran cuatro instancias de base de datos para funcionar en LAN virtuales (VLAN) diferentes. Mediante la configuración de interfaces de red de SuperCluster para usar VLAN, el tráfico de red se puede aislar entre los dominios dedicados de Oracle VM Server for SPARC y entre Oracle Solaris Zones.

FIGURA 2 Protección del aislamiento de red mediante la red de acceso de cliente



SuperCluster incluye una red IB privada usada por las instancias de base de datos para acceder a la información almacenada en los servidores Exadata Storage Server y en ZFS Storage Appliance, y para llevar a cabo las comunicaciones internas necesarias para agrupación en clusters y alta disponibilidad. Esta ilustración muestra el aislamiento de red seguro en SuperCluster M7.

FIGURA 3 Aislamiento de red seguro en la red IB de 40 Gbs



Por defecto la red IB de SuperCluster está particionada en seis particiones diferentes durante la instalación y la configuración. Si bien no se pueden cambiar las particiones por defecto, Oracle no admite la creación y el uso de particiones dedicadas adicionales en situaciones donde se requiere una mayor segmentación de la red IB. Además, la red IB admite la noción de afiliación de partición limitada y completa. Los usuarios limitados se pueden comunicar solamente con miembros completos y los miembros completos se pueden comunicar con todos los nodos de la partición. Los dominios de E/S y Oracle Solaris 11 Zones se pueden configurar como miembros limitados de sus respectivas particiones de IB y garantizar que tienen la capacidad

de comunicarse solamente con ZFS Storage Appliance, que está configurado como miembro completo y no con otros nodos de afiliación que pueden existir en esa misma partición.

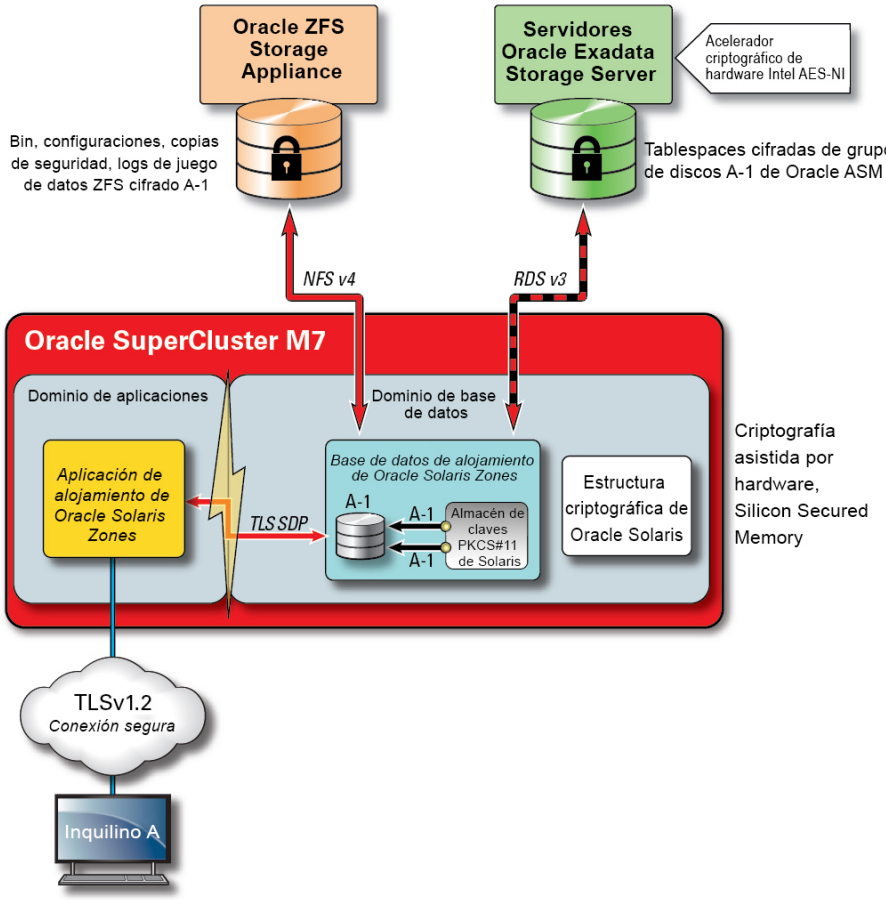
SuperCluster también incluye una red de gestión dedicada mediante la cual se pueden gestionar y supervisar todos los componentes principales. Esta estrategia mantiene las funciones de gestión y supervisión importantes asiladas de las rutas de red que se usan para procesar las solicitudes de cliente. Si se mantienen las funciones aisladas en esta red de gestión, SuperCluster puede reducir aún más la superficie de ataque de red que se expone mediante el acceso de cliente y las redes IB. Se recomienda que los proveedores de la nube sigan esta práctica recomendada y que aíslen las funciones de gestión y supervisión, y las funciones relacionadas, de modo que se pueda acceder a ellas solamente desde la red de gestión.

Protección de datos

Para los proveedores de la nube, la protección de datos es el aspecto central de la estrategia de seguridad. Dada la importancia de los mandatos de privacidad y conformidad, las organizaciones que consideran arquitecturas de varios inquilinos deben considerar el uso de la criptografía para proteger la información que fluye desde y hacia sus bases de datos. El uso de servicios criptográficos para protección de datos se aplica de manera sistemática para garantizar la confidencialidad y la integridad de la información a medida que fluye por la red y cuando reside en el disco.

El procesador SPARC M7 en SuperCluster facilita el cifrado asistido por hardware y de alto rendimiento para las necesidades de protección de datos de los entornos de TI donde la seguridad es importante. Le procesador SPARC M7 también cuenta con tecnología Silicon Secured Memory, que garantiza la prevención de ataques malintencionados de nivel de aplicación, como recortes de memoria, daños silenciosos de memoria, saturaciones de buffer y ataques relacionados.

FIGURA 4 Protección de datos proporcionada por la aceleración criptográfica asistida por hardware y la protección contra intrusiones de memoria



Para arquitecturas de varios inquilinos seguras, donde la protección de datos es importante en prácticamente todos los aspectos de una arquitectura, SuperCluster y el software de soporte permiten a las organizaciones alcanzar los objetivos de seguridad y conformidad sin necesidad de sacrificar el rendimiento. SuperCluster aprovecha las instrucciones criptográficas basadas en el núcleo y las capacidades de Silicon Secured Memory, que están diseñadas en el procesador SPARC M7 para acelerar las operaciones criptográficas y garantizar la protección de la intrusión de memoria sin un impacto en el rendimiento. Estas capacidades protegen el rendimiento criptográfico mejorado y proporcionan comprobación de intrusiones de memoria.

También mejoran el rendimiento general, ya que se pueden dedicar más recursos de cálculo a atender las cargas de trabajo de los inquilinos.

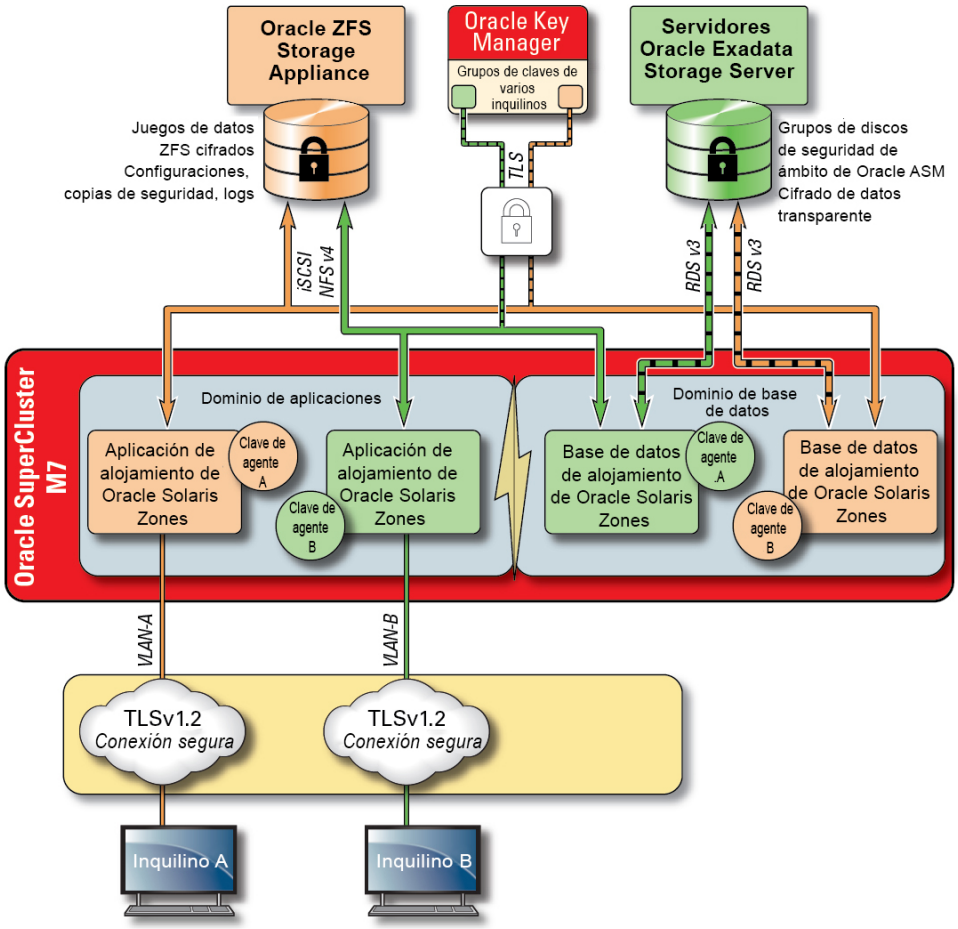
El procesador SPARC permite el soporte de la aceleración criptográfica asistida por hardware para más de 16 algoritmos criptográficos estándar del sector. En conjunto, estos algoritmos admiten las necesidades criptográficas más modernas, incluido el cifrado de claves públicas, el cifrado de claves simétricas, la generación de números aleatorios, y el cálculo y la verificación de firmas digitales y resúmenes de mensajes. Además, en el nivel del sistema operativo, la aceleración de hardware criptográfico está activada por defecto para la mayoría de los servicios principales, incluidos shell seguro IPSec/IKE y juegos de datos ZFS cifrados.

Oracle Database y Oracle Fusion Middleware identifican de manera automática el sistema operativo Oracle Solaris y el procesador SPARC usado por SuperCluster. Esto permite que la base de datos y el middleware usen automáticamente las capacidades de aceleración criptográfica de la plataforma para TLS, WS-Securit y operaciones de cifrado de tablespace. También les permite usar la función Silicon Secured Memory para garantizar la protección de memoria y garantiza la integridad de los datos de aplicación sin necesidad de configuración del usuario final. Para proteger la confidencialidad y la integridad de las comunicaciones entre zonas y específicas de un inquilino, basadas en IP, que fluyen por la red de IB, use IPSec (seguridad IP) e IKE (intercambio de claves de Internet).

Cualquier análisis de criptografía estaría incompleto sin el análisis de cómo se gestionan las claves de cifrado. La generación y la gestión de claves de cifrado, en especial para grandes colecciones de servicios, ha sido tradicionalmente un desafío mayor para las organizaciones y los desafíos aumentan aún más en el caso de un entorno de varios inquilinos basado en nube. En SuperCluster, el cifrado de juego de datos ZFS y el cifrado de datos transparentes de Oracle Database pueden aprovechar el almacén de claves PKCS#11 de Oracle Solaris para proteger correctamente la clave maestra. El uso del almacén de claves PKCS#11 de Oracle Solaris involucra de inmediato la aceleración criptográfica asistida por hardware de SPARC para las operaciones maestras clave. Esto permite a SuperCluster mejorar ampliamente el rendimiento de las operaciones de cifrado y descifrado asociadas con el cifrado de juegos de datos ZFS, el cifrado de tablespace de Oracle Database, las copias de seguridad de base de datos cifradas (mediante Oracle Recovery Manager [Oracle RMAN]), las exportaciones de base de datos cifradas (mediante la función Data Pump de Oracle Database) y los redo logs (mediante Oracle Active Data Guard).

Los inquilinos que usan un enfoque de cartera compartida pueden aprovechar el dispositivo de almacenamiento ZFS para crear un directorio que se pueda compartir en todos los nodos de un cluster. Mediante el uso de un almacén de claves centralizado y compartido, se puede ayudar a los inquilinos a gestionar, mantener y rotar mejor las claves en las arquitecturas de base de datos agrupadas, como Oracle Real Application Clusters (Oracle RAC), ya que las claves se pueden sincronizar en cada uno de los nodos del cluster.

FIGURA 5 Protección de datos mediante un escenario de gestión de claves de varios inquilinos mediante Oracle Key Manager



Para solucionar las complejidades y los problemas de gestión de claves asociados con varios hosts y aplicaciones en un entorno de varios inquilinos basado en la nube, use la Oracle Key Manager opcional como un dispositivo integrado a la red de gestión. Oracle Key Manager autoriza, protege y gestiona de manera central el acceso a claves de cifrado usadas por Oracle Database, aplicaciones de Oracle Fusion, Oracle Solaris y ZFS Storage Appliance. Oracle Key Manager también admite las unidades de cinta de cifrado de Oracle StorageTek. La política

de cifrado y la gestión de claves del juego de datos ZFS (sistema de archivos) permiten la supresión garantizada de sistemas de archivos de inquilinos mediante la destrucción de claves.

Oracle Key Manager es un dispositivo completo de gestión de claves que admite operaciones de gestión de claves del ciclo de vida y almacenamiento de claves de confianza. Cuando se configura con una tarjeta PCIe Sun Crypto Accelerator 6000 de Oracle, Oracle Key Manager ofrece almacenamiento de claves certificado FIPS 140-2 nivel 3 de claves de cifrado AES de 256 bits, así como generación aleatoria de números que cumplen con FIPS 186-2. Dentro de SuperCluster, todos los dominios de base de datos y aplicación, incluidas las zonas globales y no globales, se pueden configurar para usar Oracle Key Manager para la gestión de claves asociadas con aplicaciones, bases de datos y juegos de datos ZFS cifrados. De hecho, Oracle Key Manager admite operaciones de gestión de claves asociadas con instancias de base de datos individuales o múltiples, Oracle RAC, Oracle Active Data Guard, Oracle RMAN y la función Data Pump de Oracle Database.

Finalmente, la separación de tareas, aplicada por Oracle Key Manager, permite que cada inquilino mantenga el control completo sobre las claves de cifrado, con una visibilidad coherente de las operaciones de gestión de claves. Dada la importancia de las claves para la protección de información, es crítico que los inquilinos implementen los niveles necesarios de control de acceso basado en roles y la auditoría para garantizar que las claves se protejan correctamente durante el ciclo de vida.

Información relacionada

- “Oracle Key Manager” [130]

Control de acceso

Para las organizaciones que adoptan una estrategia de entorno alojado en la nube, el control de acceso es uno de los desafíos más críticos para resolver. Los inquilinos deben poder confiar en que la información almacenada en la infraestructura compartida estará protegida y disponible solamente para hosts, servicios, individuos, grupos y roles autorizados. Los hosts, los individuos y los servicios autorizados se deben restringir aún más, según el principio del último privilegio, de modo que tengan solamente los derechos y los privilegios necesarios para una operación determinada.

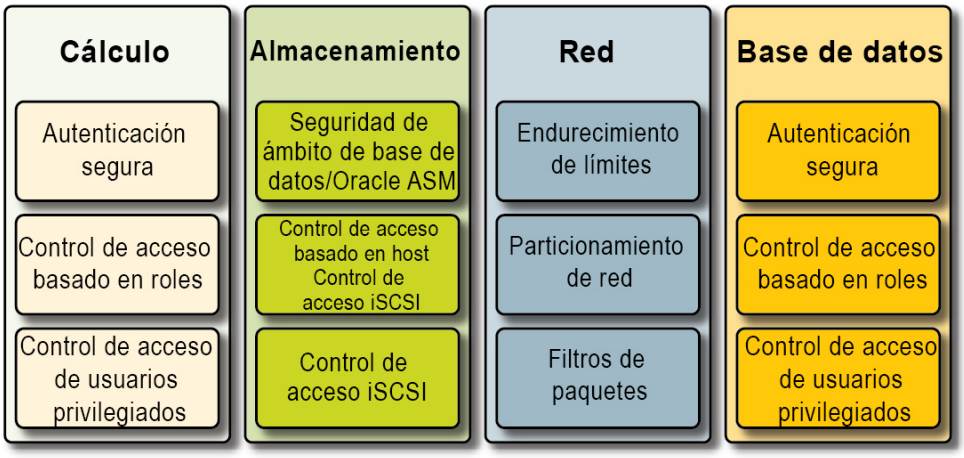
SuperCluster facilita una arquitectura de control de acceso en capas y flexible, que abarca todas las capas de la pila y admite una variedad de roles, incluidos los usuarios finales, los administradores de base de datos y los administradores del sistema. Esto permite a las

organizaciones definir políticas que protegen hosts, aplicaciones y bases de datos de manera individual y proteger el cálculo subyacente, el almacenamiento y la infraestructura de red en la que se ejecutan los servicios.

En las capas de virtualización y del sistema operativo, el control de acceso comienza con la reducción del número de servicios expuestos en la red. Esto ayuda a controlar el acceso a las consolas, los dominios y las zonas de Oracle VM Server for SPARC. Mediante la reducción de los puntos de entrada mediante los que se puede acceder a los sistemas, el número de políticas de control también se puede reducir y mantener con mayor facilidad durante la vida del sistema.

Dentro del sistema operativo Oracle Solaris, los controles de acceso se implementan mediante una combinación de permisos de POSIX junto con la utilidad de control de acceso basado en roles de Oracle Solaris (RBAC). Igualmente importante es la capacidad de proteger los hosts, las aplicaciones, las bases de datos y los servicios relacionados que se ejecutan en SuperCluster desde los ataques basados en la red. Para esto, los inquilinos primero deben verificar que solamente se ejecuten los servicios aprobados y se escuchen las conexiones de red entrantes. Una vez que se ha minimizado la superficie de ataque de red, los inquilinos configuran luego los servicios restantes, de modo que escuchen las conexiones entrantes solamente en las redes e interfaces aprobadas. Esta práctica simple ayudará a garantizar que los protocolos de gestión. como el shell seguro, no sean accesibles desde otro lugar que no sea la red de gestión.

FIGURA 6 Resumen de control de acceso de extremo a extremo



Además, los inquilinos también pueden elegir implementar un firewall basado en host, como el servicio de filtro IP de Oracle Solaris. Los firewalls basados en host son útiles porque

proporcionan a los hosts una manera de controlar el acceso a los servicios de red con funciones enriquecidas. En concreto, el filtro IP admite filtrado de paquetes con estado y puede filtrar paquetes por dirección IP, por puerto, por protocolo, por interfaz de red y por dirección de tráfico. Estas capacidades son importantes para plataformas como SuperCluster que operan diversas interfaces de red y admiten una variedad de comunicaciones de red entrantes y salientes.

En SuperCluster, el filtro IP se puede configurar dentro de un dominio Oracle VM Server for SPARC o se puede operar desde una instancia de Oracle Solaris Zone. Esto permite que se aplique la política de control de acceso de red en el mismo contenedor del sistema operativo en el que se ofrecen los servicios de la base de datos. En escenarios de varios inquilinos, la cantidad de actividad de red saliente será probablemente mínima y se podrá categorizar fácilmente de modo que se pueda crear una política que limite las comunicaciones a interfaces y destinos de red específicos. El resto del tráfico se deberá denegar y registrar como parte de una política de “denegación por defecto” para bloquear comunicaciones no autorizadas, entrantes y salientes.

La seguridad de usuario final de Oracle permite a los inquilinos integrar sus aplicaciones y bases de datos con los servicios de gestión de identidad existentes para admiten gestión de roles y usuarios centralizada y e inicio de sesión único (SSO). En especial, la seguridad de usuario final de Oracle ayuda mediante la centralización de (1) aprovisionamiento y desaprovisionamiento de usuarios y administradores de base de datos, (2) gestión de contraseñas y restablecimiento de contraseñas de autoservicio y (3) gestión de autorizaciones mediante roles de base de datos globales. Las organizaciones que requieren métodos de autenticación de varios factores, como Kerberos o PKI, pueden aprovechar Oracle Advanced Security.

La tecnología Oracle Exadata Storage Server admite un juego predefinido de cuentas de usuario, cada una con privilegios diferentes. Los administradores que realizan la administración de Oracle Exadata Storage Server deben usar uno de estos roles predefinidos para acceder al sistema. El dispositivo de almacenamiento ZFS, por otra parte, admite la creación de cuentas administrativas locales y remotas, y ambas son capaces de admitir la asignación individual de roles y privilegios.

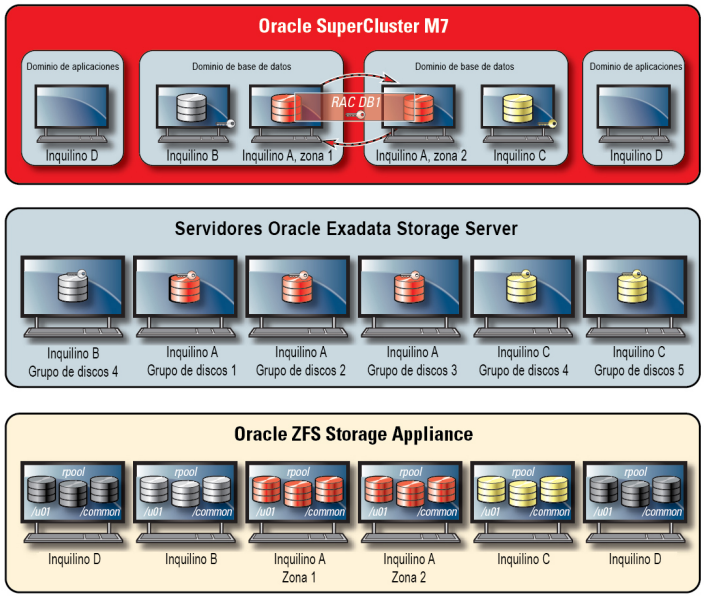
Por defecto, los dominios de base de datos acceden a los servidores de Oracle Exadata Storage Server usados en SuperCluster mediante la utilidad Oracle Automatic Storage Management. Esta instalación permite a los administradores de la nube crear grupos de disco diferentes para cada inquilino, que son capaces de satisfacer sus requisitos de capacidad, rendimiento y disponibilidad. En términos de control de acceso, Oracle Automatic Storage Management admite tres modos de control de acceso: seguridad abierta, seguridad con ámbito de Oracle Automatic Storage Management y seguridad con ámbito de base de datos.

En un escenario de varios inquilinos, se recomienda la seguridad con ámbito de base de datos, ya que ofrece el nivel de control de acceso más específico. En este modo, es posible

configurar grupos de discos, de modo que solamente una base de datos puede acceder a ellos. En especial, esto significa que se podrán limitar tanto los administradores como los usuarios para acceso a únicamente esos discos de cuadrícula para los que tienen privilegios de acceso. En los escenarios de consolidación de base de datos en los que es posible que las bases de datos admitan diferentes organizaciones o inquilinos, es importante que cada inquilino pueda acceder y manipular su propio almacenamiento. En particular, cuando se combina con las estrategias de aislamiento de base de datos y carga de trabajo analizadas anteriormente, es posible que los inquilinos compartimenten el acceso a bases de datos individuales.

La seguridad con ámbito de base de datos es una herramienta eficaz para limitar el acceso a los discos de cuadrícula de Oracle ASM. En esta figura, se muestra la seguridad con ámbito de Oracle ASM junto con la seguridad de ZFS. En situaciones en las que hay gran cantidad de instancias de Oracle Database implementadas en la plataforma de SuperCluster, es posible que una estrategia de seguridad de ámbito de Oracle ASM por inquilino tenga mayor sentido, ya que reduce ampliamente el número de claves que se deben crear, asignar y gestionar. Además, dado que la seguridad con ámbito de base de datos requiere grupos de discos separados para cada base de datos, este enfoque también reducirá ampliamente el número de discos de cuadrícula separados que se deben crear en un servidor Exadata Storage Server.

FIGURA 7 Seguridad con ámbito de Oracle ASM por inquilino



SuperCluster aprovecha la protección de enlace de datos de Oracle Solaris, que busca evitar daños potenciales que pueden ser causados por máquinas virtuales malintencionadas de inquilinos en la red. Esta función integrada de Oracle Solaris ofrece protección contra las siguientes amenazas básicas: falsificación de direcciones IP y MAC, y falsificación de marco L2 (por ejemplo, ataques de unidad de datos de protocolo de puente). La protección de enlace de datos de Oracle Solaris también se debe aplicar de forma individual a todas las zonas no globales de Oracle Solaris implementadas dentro del entorno de varios inquilinos.

Dado que los inquilinos individuales no deben requerir acceso administrativo o de nivel de host para los servidores Exadata Storage Server, se recomienda que el acceso sea restringido. Los servidores Exadata Storage Server se deben configurar para evitar el acceso directo para zonas no globales de inquilinos y dominios de E/S mientras se permite el acceso desde los dominios de base de datos de SuperCluster (que son operados por el proveedor de la nube). Esto garantiza que los servidores Exadata Storage Server se podrán gestionar solamente desde ubicaciones de confianza en la red de gestión.

Una vez que se ha definido e implementado la configuración de seguridad de los inquilinos, los proveedores de servicio pueden considerar el paso adicional de configuración de zonas globales y no globales específicas de inquilinos para ser inmutables como entornos de solo lectura. Las zonas inmutables crean un entorno de funcionamiento resistente y de alta integridad dentro del cual los inquilinos pueden operar sus propios servicios. Las zonas inmutables se desarrollan sobre las capacidades de seguridad inherentes de Oracle Solaris y garantizan que algunos (o todos) los directorios del sistema operativo se podrán cambiar sin intervención del proveedor de servicios de la nube. La aplicación de esta postura de solo lectura ayuda a evitar cambios no autorizados, promover procedimientos de gestión de cambios más eficaces y desalentar la inyección de malware basado en núcleo y usuario.

Supervisión y auditoría de conformidad

La supervisión preventiva y el registro en un entorno de nube son muy importantes y, en muchos casos, ayuda a mitigar los ataques que se originan desde orificios de bucles y vulnerabilidades. Ya sea para la generación de informes de conformidad o la respuesta de incidentes, la supervisión y la auditoría son funciones críticas para el proveedor de la nube y las organizaciones de inquilinos deben aplicar un registro bien definido y una política de auditoría para obtener una mayor visibilidad en el entorno de alojamiento. El grado en el que se emplea la supervisión y la auditoría a menudo se basa en el riesgo o la importancia del entorno que se protege.

La arquitectura de la nube de SuperCluster confía en el uso del subsistema de auditoría de Oracle Solaris para recopilar, almacenar y procesar la información de evento de auditoría. Cada zona no global específica de inquilinos generará registro de auditoría que se almacenan

de forma local para cada dominio dedicado de SuperCluster (zona global). Este enfoque garantizará que los inquilinos individuales no podrán alterar sus políticas de auditoría, configuraciones o datos registrados, dado que la responsabilidad pertenece al proveedor de servicios de la nube. La funcionalidad de auditoría de Oracle Solaris supervisa todas las acciones administrativas, las invocaciones de comandos y las llamadas al sistema de nivel de núcleo individual en ambas zonas y dominios de inquilino. Esta instalación tiene una gran capacidad de configuración y ofrece políticas de auditoría globales, por zona e incluso por usuario. Cuando se configuran para zonas de inquilinos, los registros de auditoría de cada zona se pueden almacenar en la zona global para protegerlos contra manipulación. Los dominios dedicados y los dominios de E/S también aprovechan la instalación de auditoría de Oracle Solaris para registrar las acciones y los eventos asociados con los eventos de virtualización y la administración de dominios.

Los servidores Exadata Storage Server y el dispositivo de almacenamiento ZFS admiten inicio de sesión, hardware y configuración de auditoría. Esto permite a las organizaciones determinar quién accedió a un dispositivo y qué acciones se tomaron. Si bien la auditoría no se expone directamente al usuario final, la auditoría de Oracle Solaris proporciona el contenido subyacente para la información presentada por el dispositivo de almacenamiento ZFS.

De manera similar, la auditoría de Exadata Storage Server es una recopilación completa de eventos del sistema que se pueden usar junto con la información de alertas de hardware y configuración proporcionadas por el software Exadata Storage Server. Con la capacidad de filtro IP de Oracle Solaris, el proveedor de la nube puede registrar de manera selectiva las comunicaciones de red entrantes y salientes, y la capacidad se puede aplicar en el nivel del dominio y de la zona no global. Esto ayuda a las organizaciones a segmentar las políticas de red y a verificar los registros de actividad. De manera opcional, el dispositivo de Oracle Audit Vault and Database Firewall se puede implementar para agregar y analizar información de auditoría de manera segura desde una variedad de bases de datos de Oracle y de bases de datos que no pertenecen a Oracle, además de información de auditoría de Oracle Solaris.

Mediante la integración con Oracle Enterprise Manager, SuperCluster puede admitir una variedad de operaciones de autoservicio en la nube. Los proveedores de la nube pueden definir agrupaciones de recursos, asignar agrupaciones y cuotas a inquilinos individuales, identificar y publicar catálogos de servicio y, en última instancia, admitir la supervisión y el registro de recursos de base de datos y aplicación.

Información relacionada

- Auditoría de conformidad [123]
- “Supervisión de seguridad” [133]

Recursos adicionales para mejores prácticas de seguridad de SuperCluster

Para obtener información adicional sobre la seguridad, la arquitectura y las mejores prácticas de SuperCluster, consulte los siguientes recursos:

- Oracle SuperCluster M7: capacidades y principios de seguridad de la plataforma

  http://www.oracle.com/us/products/servers-storage/servers/sparc-enterprise/supercluster/supercluster-t4-4/ssc-security-pac-1716580.pdf
- Oracle SuperCluster M7: arquitectura de nube privada segura

  http://www.oracle.com/technetwork/server-storage/engineered-systems/oracle-supercluster/documentation/supercluster-secure-multi-tenancy-2734706.pdf
- Protección de datos completa en Oracle SuperCluster

  https://community.oracle.com/docs/DOC-918251
- Consolidación de base de datos segura en Oracle SuperCluster

  http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-053-securedb-osc-t5-8-1990064.pdf
- Oracle SuperCluster y conformidad con PCI

  http://www.oracle.com/technetwork/server-storage/engineered-systems/sparc-supercluster/supercluster-pci-dss-compliance-2372543.pdf
- Oracle SuperCluster: validación y mejores prácticas de la Guía de implementación técnica de seguridad (STIG)

  http://www.oracle.com/technetwork/server-storage/hardware-solutions/stig-sparc-supercluster-1841833.pdf
- Guía del desarrollador para la seguridad de Oracle Solaris 11

  https://docs.oracle.com/cd/E36784_01/html/E36855/index.html
- Conformidad con Oracle Solaris 11 y PCI

  http://www.oracle.com/us/products/servers-storage/solaris/solaris11/solaris11-pci-dss-wp-1937938.pdf
- Inicio rápido de auditoría de Oracle Solaris 11

  http://www.oracle.com/technetwork/articles/servers-storage-admin/sol-audit-quick-start-1942928.html
- Directrices de seguridad de Oracle Solaris 11

  http://docs.oracle.com/cd/E53394_01/html/E54807/index.html
- Guía de seguridad de Oracle Database 12c versión 1 (12.1)

  https://docs.oracle.com/database/121/DBSEG/E48135-11.pdf

Revisión de la configuración de seguridad por defecto

En estos temas, se describe la configuración de seguridad por defecto para SuperCluster M7.

Configuración de seguridad por defecto

El software SuperCluster M7 está instalado con varios ajustes de seguridad por defecto. Siempre que es posible, use la configuración segura por defecto:

- Las políticas de contraseña aplican una complejidad de contraseña mínima.
- Los intentos de inicio de sesión fallidos causan un bloqueo después de un número definido de intentos fallidos.
- Todas las cuentas del sistema por defecto del sistema operativo están bloqueadas y tienen el inicio de sesión prohibido.
- Se configura una capacidad limitada para usar el comando `su`.
- Los módulos y los protocolos innecesarios están desactivados en el núcleo del sistema operativo.
- El cargador de inicio está protegido por contraseña.
- Todos los servicios del sistema innecesarios están desactivados, incluido `inetd` (daemon de servicio de Internet).
- El firewall del software está configurado en celdas de almacenamiento.
- Los permisos de archivo restrictivos están configurados en archivos de configuración relacionados con la seguridad y en archivos ejecutables.
- Los puertos de escucha SSH están restringidos a redes privadas y de gestión.
- SSH está limitado al protocolo v2.

- Los mecanismos de autenticación de SSH están desactivados.
- Los codificadores criptográficos están configurados.
- Los conmutadores están separados en el sistema del tráfico de datos en la red.

Cuentas de usuario y contraseñas por defecto

En esta tabla, se muestran las cuentas y contraseñas por defecto para SuperCluster M7. Se proporcionan instrucciones adicionales para cambio de las contraseñas por defecto en los capítulos siguientes para cada componente.

Componente	Nombre de usuario	Contraseña	Información sobre cuentas de usuario y contraseñas
Oracle ILOM en: ■ Servidores serie SPARC M7 ■ Servidores Exadata Storage Server ■ ZFS Storage Appliance	■ `root`	`welcome1`	Consulte Configuración y mantenimiento en la recopilación de documentación, disponible en: `http://docs.oracle.com/cd/E24707_01/html/E24528`.
Servidores serie SPARC M7	■ `root` ■ `oracle` ■ `grid`	`welcome1` `welcome1` `welcome1`	Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55]. Consulte también los siguientes recursos: ■ **Oracle Solaris 11**: consulte la documentación de seguridad de Oracle Solaris 11, disponible en: `http://www.oracle.com/goto/Solaris11/docs`. ■ **Oracle Solaris 10**: consulte *Administración de Oracle Solaris: administración básica*, disponible en: `http://docs.oracle.com/cd/E26505_01`.

Servidores Exadata Storage Server	■ `root`
	■ `celladmin`
	■ `cellmonitor`
		`welcome1`
		`welcome`
		`welcome`
			Consulte Cambio de contraseñas del servidor de almacenamiento [96].

Oracle ZFS Storage ZS3-ES	■ `root`	`welcome1`	Consulte Cambie la contraseña `root` de ZFS Storage Appliance [84]. Consulte también la sección Usuarios en la *Guía de administración de Oracle ZFS Storage Appliance*, disponible en: `http://www.oracle.com/goto/ZS3-ES/docs`.
Conmutadores InifiniBand	■ `root` ■ `nm2user`	`welcome1` changeme	Consulte Cambio de las contraseñas `root` y `nm2user` [113].

Componente	Nombre de usuario	Contraseña	Información sobre cuentas de usuario y contraseñas
			Consulte también Control del chasis en la *Recopilación de documentos HTML para la versión de firmware 2.1 de Sun Datacenter InfiniBand Switch 36*, disponible en: http://docs.oracle.com/cd/E36265_01.
InfiniBand Oracle ILOM	■ ilom-admin ■ ilom-operator	ilom-admin ilom-operator	Consulte Cambio de contraseñas de conmutador (IB Oracle ILOM) [114]. Consulte también la documentación de InfiniBand, disponible en: http://docs.oracle.com/cd/E36265_01.
Conmutador de gestión de Ethernet	■ admin	welcome1	Consulte Cambio de la contraseña de conmutador Ethernet [121].
Herramienta de creación de dominios de E/S de Oracle	■ admin	welcome1	Consulte la *Guía de administración de dominios de E/S de Oracle*, disponible en: http://www.oracle.com/goto/sc-m7/docs.
Oracle Engineered Systems Hardware Manager	■ admin ■ service	welcome1 welcome1	Consulte la *Guía del propietario Oracle SuperCluster serie M7: administración*, disponible en: http://www.oracle.com/goto/sc-m7/docs.

Nota - Si se cambia la contraseña `root` o `admin` para este componente, también se debe cambiar en Oracle Engineered Systems Hardware Manager. Para obtener instrucciones, consulte la *Guía del propietario de Oracle SuperCluster serie M7: administración*. Consulte también "Contraseñas conocidas por Oracle Engineered Systems Hardware Manager" [31].

Contraseñas conocidas por Oracle Engineered Systems Hardware Manager

Oracle Engineered Systems Hardware Manager debe estar configurado con las cuentas y las contraseñas para los componentes de esta tabla.

Nota - Oracle Engineered Systems Hardware Manager no necesita conocer las contraseñas de los dominios lógicos o de las zonas.

Componente	Cuenta
Todas las instancias de Oracle ILOM	`root`
Sistema operativo de los servidores Exadata Storage Server	`root`

Componente	Cuenta
Sistema operativo de los controladores de ZFS Storage	`root`
Conmutadores IB	`root`
Conmutador de gestión de Ethernet	`admin`
PDU	`admin`

Para obtener más información acerca de Oracle Engineered Systems Hardware Manager, consulte “Oracle Engineered Systems Hardware Manager” [131] y consulte la *Guía de administración de Oracle SuperCluster serie M7*, disponible en `http://www.oracle.com/goto/sc-m7/docs`.

Protección del hardware

En estas secciones, se describen las directrices de seguridad para proteger el hardware:

Restricciones de acceso

- Instale sistemas de Oracle SuperCluster serie M7 y los equipos relacionados en una habitación cerrada con llave y de acceso restringido.
- Cierre con llave las puertas del rack a menos que se debe realizar un mantenimiento en componentes del rack. Esto restringirá el acceso a los dispositivos conectables en caliente o intercambiables en caliente, y a los puertos USB, los puertos de red y las consolas del sistema.
- Almacene las unidades sustituibles en campo (FRU) o las unidades sustituibles por el cliente (CRU) de repuesto en un armario cerrado. Restrinja el acceso al armario cerrado a personal autorizado.
- Verifique periódicamente el estado y la integridad de las cerraduras del rack y el armario de repuestos para brindar protección contra la manipulación de cerraduras o puertas abiertas accidentalmente, o para detectar si esto ha sucedido.
- Almacene las llaves del armario en una ubicación segura con acceso limitado.
- Restrinja el acceso a consolas USB. Los dispositivos como los controladores del sistema, las unidades de distribución de energía (PDU) y los conmutadores de red pueden tener conexiones USB. La restricción del acceso físico es un método más seguro para acceder a un componente, ya que elimina la posibilidad de ataques basados en red.

Números de serie

- Registre los números de serie de los componentes en sistemas SuperCluster serie M7.
- Realice una marca de seguridad en todos los elementos importantes del hardware de la computadora, como las piezas de repuesto. Utilice plumas ultravioleta o etiquetas en relieve especiales.
- Mantenga los registros de las licencias y las claves de activación de hardware en una ubicación segura y de fácil acceso para el administrador del sistema en caso de emergencia del sistema. Los documentos impresos podrían ser su única prueba para demostrar la propiedad.
- Almacene de forma segura todas las hojas de información que se proporcionan con el sistema.

Unidades

Por lo general, las unidades de disco duro y de estado sólido se usan para almacenar información confidencial. Para proteger esta información de la divulgación no autorizada, las unidades de deberían sanearse antes de ser reutilizadas, retiradas o desechadas.

- Use herramientas de borrado de disco duro, como el comando `format` (`1M`) de Oracle Solaris, para borrar por completo todos los datos de la unidad.
- Las organizaciones deberán consultar sus respectivas políticas de protección de datos para determinar el método más apropiado para sanear los discos duros.
- Si es necesario, aproveche el servicio de retención de dispositivos y datos de clientes de Oracle. Consulte el siguiente documento: `http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf`.

Atención - Debido a la manera en que se gestiona el acceso a los datos, quizá no sea posible suprimir algunos de los datos en unidades modernas con software de borrado de disco duro.

OBP

Por defecto, el OBP de SPARC serie M7 no está protegido por contraseña. Puede mejorar la seguridad del sistema mediante la restricción del acceso al OBP si realiza las siguientes acciones:

- Implementación de la protección con contraseña.
- Comprobación de inicios de sesión fallidos de OBP.
- Aprovisionamiento de un banner de encendido de OBP.

Recursos adicionales de hardware

Todos los principios de seguridad que se describen en la *Guía de seguridad de los servidores de sistemas SPARC serie M7* se aplican a los servidores SPARC M7 de SuperCluster. La guía de seguridad está disponible en: http://www.oracle.com/goto/M7/docs.

Protección de Oracle ILOM

Oracle ILOM proporciona hardware y software de procesador de servicio avanzado que se usa para gestionar y supervisar los componentes de Oracle SuperCluster, incluidos los servidores de cálculo, los servidores de almacenamiento, el dispositivo de almacenamiento ZFS y los conmutadores IB.

Oracle ILOM le permite gestionar y supervisar de forma activa los servidores y los dispositivos subyacentes, independientemente del estado del sistema operativo, y proporciona una capacidad de gestión de Lights Out confiable.

Para proteger completamente Oracle ILOM en SuperCluster M7, debe aplicar los ajustes de configuración en todos los componentes activados para Oracle ILOM de manera individual. Estos componentes tienen Oracle ILOM:

- Servidores de cálculo
- Servidores de almacenamiento
- ZFS Storage Appliance
- Conmutadores IB

Realice las siguientes tareas para proteger Oracle ILOM:

▼ Inicio de sesión en la CLI de Oracle ILOM

1. **En la red de gestión, inicie sesión en Oracle ILOM.**

En este ejemplo, sustituya *ILOM_SP_ipaddress* por la dirección IP de Oracle ILOM para el componente al que desea acceder:

- Servidores de cálculo
- Servidores de almacenamiento
- ZFS Storage Appliance
- Conmutadores IB

Las direcciones IP de la configuración se muestran en el resumen de despliegue proporcionado por el personal de Oracle.

```
% ssh root@ILOM_SP__ipaddress
```

2. **Escriba la contraseña de usuario root de Oracle ILOM.**

   Consulte "Cuentas y contraseñas por defecto (Oracle ILOM)" [40].

Determinación de la versión de Oracle ILOM

Para aprovechar las mejoras más recientes de funciones, capacidades y seguridad, actualice el software de Oracle ILOM con la versión admitida más reciente.

1. **En la red de gestión, inicie sesión en Oracle ILOM.**

   Consulte Inicio de sesión en la CLI de Oracle ILOM [37].

2. **Visualice la versión de Oracle ILOM.**

   En este ejemplo, el software Oracle ILOM es versión 3.2.4.1.b.

```
-> version
SP firmware 3.2.4.1.b
SP firmware build number: 94529
SP firmware date: Thu Nov 13 16:41:19 PST 2014
SP filesystem version: 0.2.10
```

Nota - Para actualizar la versión de Oracle ILOM en cualquiera de los componentes de SuperCluster, instale el parche de descarga de pila completa trimestral de SuperCluster disponible en My Oracle Support, en `https://support.oracle.com`.

Nota - Los sistemas de Oracle Engineered System, como SuperCluster están restringidos en las versiones de Oracle ILOM que se pueden usar y en la manera en la que se actualizan las versiones. Para obtener más información, póngase en contacto con el representante de Oracle.

Activación de operación que cumple con FIPS-140 (Oracle ILOM) (Si se requiere)

Se requiere el uso de la criptografía validada por FIPS 140 para los clientes del Gobierno Federal de los EE. UU.

Por defecto, Oracle ILOM no opera con la criptografía validada por FIPS 140. Sin embargo, si es necesario, se puede activar el uso de la criptografía validada por FIPS 140.

Algunas funciones y capacidades de Oracle ILOM no están disponibles cuando se configuran para operaciones que cumplen con FIPS 140. Se abarca una lista de esas funciones en la *Guía de seguridad de Oracle ILOM* en la sección titulada "Funciones no admitidas cuando está activado el modo de FIPS" (consulte “Recursos adicionales de Oracle ILOM” [52]).

Consulte también “Conformidad con FIPS-140-2 nivel 1” [126].

Atención - Esta tarea requiere el restablecimiento de Oracle ILOM. Un restablecimiento causa la pérdida de todos los ajustes de configuración del usuario. Por este motivo, debe activar la operación que cumple con FIPS 140 antes de que se realicen cambios adicionales específicos del sito en Oracle ILOM. Para sistemas en los que se han realizado cambios de configuración específicos del sitio, realice una copia de seguridad de Oracle ILOM de modo que se pueda restaurar después de que se haya restablecido Oracle ILOM. De lo contrario, se perderán los cambios de configuración.

1. **En la red de gestión, inicie sesión en Oracle ILOM.**

   Consulte Inicio de sesión en la CLI de Oracle ILOM [37].

2. **Determine si Oracle ILOM está configurado para operación que cumple con FIPS 140.**

```
-> show /SP/services/fips state status
/SP/services/fips
Properties:
state = enabled
status = enabled
```

   El modo que cumple con FIPS 140 en Oracle ILOM está representado por las propiedades `state` y `status`. La propiedad `state` representa el modo configurado en Oracle ILOM y la propiedad `status` representa el modo operativo en Oracle ILOM. Cuando la propiedad `state`de FIPS se modifica, el cambio no afecta la propiedad `status` de FIPS del modo operativo hasta el siguiente reinicio de Oracle ILOM.

3. **Active la operación que cumple con FIPS 140.**

```
-> set /SP/services/fips state=enabled
```

4. **Reinicie el procesador de servicio de Oracle ILOM.**

   Se debe reiniciar el SP de Oracle ILOM para que se aplique el cambio.

```
-> reset /SP
```

Cuentas y contraseñas por defecto (Oracle ILOM)

Cuenta	Tipo	Contraseña por defecto	Descripción
`root`	administrador	`welcome1`	Esta es la cuenta por defecto que se entrega y se activa para este componente. Esta cuenta se usa para realizar la configuración inicial y para permitir la creación de cuentas administrativas adicionales no compartidas. Para fines de seguridad, cambie la contraseña por defecto.

Servicios de red expuestos por defecto (Oracle ILOM)

En esta tabla, se muestran los servicios de red por defecto expuestos nuevamente por Oracle ILOM.

Para obtener información adicional acerca de estos servicios, consulte la *Guía de seguridad de Oracle ILOM* (consulte “Recursos adicionales de Oracle ILOM” [52]).

Nombre de servicio	Protocolo	Puerto	Descripción
SSH	TCP	22	Usado por el servicio de shell seguro integrado para permitir el acceso administrativo a Oracle ILOM mediante una interfaz de línea de comandos.
HTTP (BUI)	TCP	80	Usado por el servicio HTTP integrado para permitir el acceso administrativo a Oracle ILOM mediante una interfaz de explorador. Si bien TCP/80 generalmente se usa para acceso de texto no cifrado, por defecto, Oracle ILOM redirecciona automáticamente las solicitudes entrantes a la versión segura de este servicio que se ejecuta en TCP/443.
NTP	UDP	123	Usado por el servicio de protocolo de hora de red (NTP) (solo cliente) que se usa para sincronizar el reloj del sistema local con uno o más orígenes de hora externa.

Nombre de servicio	Protocolo	Puerto	Descripción
SNMP	UDP	161	Usado por el servicio SNMP integrado para proporcionar una interfaz de gestión para supervisar el estado de Oracle ILOM y supervisar las notificaciones de captura recibidas.
HTTPS (BUI)	TCP	443	Usado por el servicio HTTPS integrado para permitir el acceso administrativo a Oracle ILOM por un canal (SSL/TLS) cifrado mediante una interfaz de explorador.
IPMI	TCP	623	Usado por el servicio de interfaz de gestión de plataforma inteligente integrada (IPMI) para proporcionar una interfaz de computadora para varias funciones de supervisión y gestión. Este servicio no se debe desactivar, ya que lo usa Oracle Enterprise Manager Ops Center para recopilar datos de inventario de hardware, descripciones de FRU, información de sensores de hardware e información de estado de componentes del sistema.
KVMS remoto	TCP	5120 5121 5123 5555 5556 7578 7579	En conjunto, los puertos de KVMS remoto proporcionan un juego de protocolos que brindan capacidades de teclado, video, mouse y almacenamiento que se pueden usar con Oracle Integrated Lights Out Manager.
ServiceTag	TCP	6481	Usado por el servicio Oracle ServiceTag. Protocolo de detección de Oracle utilizado para identificar servidores y facilitar solicitudes de servicio. Este servicio es usado por productos como Oracle Enterprise Manager Ops Center para detectar software de Oracle ILOM y para integrarlo con otras soluciones de servicio automático de Oracle.
WS-Man sobre HTTPS	TCP	8888	Usado por el servicio WS-Man integrado para proporcionar una interfaz de servicios web basada en estándares, que se usa para gestionar Oracle ILOM mediante el protocolo HTTPS. La desactivación de este servicio evita que Oracle ILOM se gestione mediante este protocolo. Este servicio ya no se incluye como parte de Oracle ILOM versión 3.2.
WS-Man sobre HTTP	TCP	8889	Usado por el servicio WS-Man integrado para proporcionar una interfaz de servicios web basada en estándares, que se usa para gestionar Oracle ILOM mediante el protocolo HTTP. La desactivación de este servicio evitará que Oracle ILOM se gestione mediante este protocolo. Este servicio ya no se incluye como parte de Oracle ILOM versión 3.2.
Inicio de sesión único	TCP	11626	Este puerto es usado por la función Inicio de sesión único, que reduce el número de veces que un usuario debe introducir el nombre de usuario y la contraseña. La desactivación de este servicio evita el inicio de KVMS sin necesidad de volver a introducir una contraseña.

Endurecimiento de la configuración de seguridad de Oracle ILOM

En estos temas, se describe cómo proteger Oracle ILOM mediante varios ajustes de configuración.

▼ Desactivación de servicios innecesarios (Oracle ILOM)

Desactive los servicios que no se requieren para los requisitos operativos y de gestión de la plataforma.

Por defecto, Oracle ILOM emplea una configuración de red segura por defecto, donde los servicios no esenciales ya están desactivados. Sin embargo, según las políticas y los requisitos de seguridad, es posible que sea necesario desactivar servicios adicionales.

1. **En la red de gestión, inicie sesión en Oracle ILOM.**

   Consulte Inicio de sesión en la CLI de Oracle ILOM [37].

2. **Determine la lista de servicios admitidos por Oracle ILOM.**

   ```
   -> show /SP/services
   ```

3. **Determine si un servicio determinado está activado.**

   Sustituya *servicename* por el nombre del servicio identificado en Paso 2.

   ```
   -> show /SP/services/servicename servicestate
   ```

   Si bien la mayoría de los servicios reconocen y usan el parámetro `servicestate` para registrar si el servicio está activado o desactivado, hay unos pocos servicios, como `servicetag`, `ssh`, `sso` y `wsman`, que usan el parámetro denominado `state`. Independientemente del parámetro real usado,

un servicio está activado si el parámetro `servicestate` o `state` devuelve el valor `enabled`, como se muestra en los siguientes ejemplos:

```
-> show /SP/services/https servicestate
/SP/services/https
Properties:
servicestate = enabled
```

```
-> show /SP/services/ssh state
/SP/services/ssh
Properties:
state = enabled
```

4. **Para desactivar un servicio que no se requiere, configure el estado del servicio en `disabled`.**

```
-> set /SP/services/http servicestate=disabled
```

5. **Determine si se deberá desactivar alguno de estos servicios.**

   Según las herramientas y los métodos usados, estos servicios adicionales se pueden desactivar si no se requieren o no se usan:

   - **Para una interfaz administrativa de explorador (HTTP, HTTPS), escriba:**

     ```
     -> set /SP/services/http servicestate=disabled
     -> set /SP/services/http secureredirect=disabled
     -> set /SP/services/https servicestate=disabled
     ```

   - **Para un teclado, video, servicio de mouse (KVMS), escriba:**

     ```
     -> set /SP/services/kvms servicestate=disabled
     ```

   - **Para gestión de servicios web (WS-Man sobre HTTP/HTTPS), (Oracle ILOM versión 3.1 y posteriores), escriba:**:

     ```
     -> set /SP/services/wsman state=disabled
     ```

   - **Para servicios de inicio de sesión único (SSO), escriba:**

     ```
     -> set /SP/services/sso state=disabled
     ```

Configuración de redireccionamiento de HTTP a HTTPS (Oracle ILOM)

Por defecto, Oracle ILOM está configurado para redireccionar solicitudes de HTTP entrante al servicio HTTPS para garantizar que todas las comunicaciones basadas en explorador estén cifradas entre Oracle ILOM y el administrador.

1. **En la red de gestión, inicie sesión en Oracle ILOM.**

   Consulte Inicio de sesión en la CLI de Oracle ILOM [37].

2. **Compruebe que el redireccionamiento seguro esté activado.**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **Si el valor por defecto se ha modificado, puede activar el redireccionamiento seguro.**

```
-> set /SP/services/http secureredirect=enabled
```

4. **Para comprobar esta configuración, repita Paso 2.**

Desactivación de protocolos no aprobados

Use los siguientes temas para desactivar los protocolos no aprobados:

- Desactivación del protocolo SSLv2 para HTTPS [44]
- Desactivación del protocolo SSLv3 para HTTPS [45]

Desactivación del protocolo SSLv2 para HTTPS

Por defecto, se desactiva el protocolo SSLv2 para el servicio HTTPS.

Para fines de seguridad, es muy importante que SSLv2 esté desactivado.

1. **En la red de gestión, inicie sesión en Oracle ILOM.**

   Consulte Inicio de sesión en la CLI de Oracle ILOM [37].

2. **Determine si el protocolo SSLv2 está desactivado para el servicio HTTP.**

```
-> show /SP/services/https sslv2
/SP/services/https
Properties:
sslv2 = disabled
```

3. **Si el servicio está activado, desactive el protocolo SSLv2.**

```
-> set /SP/services/https sslv2=disabled
```

4. **Para comprobar esta configuración, repita Paso 2.**

Desactivación del protocolo SSLv3 para HTTPS

Por defecto, se activa el protocolo SSLv3 para el servicio HTTPS.

Para fines de seguridad, desactive el protocolo SSLv3.

1. **En la red de gestión, inicie sesión en Oracle ILOM.**
   Consulte Inicio de sesión en la CLI de Oracle ILOM [37].

2. **Determine si el protocolo SSLv3 está desactivado para el servicio HTTP.**

```
-> show /SP/services/https sslv3
/SP/services/https
Properties:
sslv3 = enabled
```

3. **Desactive el protocolo SSLv3.**

```
-> set /SP/services/https sslv3=disabled
```

4. **Para comprobar esta configuración, repita Paso 2.**

Desactivación de protocolos TLS no aprobados para HTTPS

Por defecto, los protocolos TLSv1.0, TLSv1.1 y TLSv1.2 están activados para el servicio HTTPS.

Puede desactivar una o más versiones del protocolo TLS que no cumplen con las políticas de seguridad.

Para fines de seguridad, use TLSv1.2 a menos que se requiera compatibilidad con versiones anteriores del protocolo TLS.

1. **En la red de gestión, inicie sesión en Oracle ILOM.**

   Consulte Inicio de sesión en la CLI de Oracle ILOM [37].

2. **Determine la lista de versiones de protocolo de TLS que están activadas para el servicio HTTPS.**

```
-> show /SP/services/https tlsv1 tlsv1_1 tlsv1_2
/SP/services/https
Properties:
tlsv1 = enabled
tlsv1_1 = enabled
tlsv1_2 = enabled
```

3. **Desactive TLSv1.0.**

```
-> set /SP/services/https tlsv1_0=disabled
```

4. **Desactive TLSv1.1.**

```
-> set /SP/services/https tlsv1_1=disabled
```

5. **Para comprobar esta configuración, repita Paso 2.**

▼ Desactivación de cifrados débiles y medios de SSL para HTTPS

Por defecto, Oracle ILOM desactiva el uso de cifrados débiles y medios para el servicio HTTPS.

1. **En la red de gestión, inicie sesión en Oracle ILOM.**

   Consulte Inicio de sesión en la CLI de Oracle ILOM [37].

2. **Determine si los cifrados débil y medio están desactivados.**

```
-> show /SP/services/https weak_ciphers
```

```
/SP/services/https
Properties:
weak_ciphers = disabled
```

3. **Si ha modificado el valor por defecto, puede desactivar el uso de los cifrados débil y medio.**

```
-> set /SP/services/https weak_ciphers=disabled
```

4. **Para comprobar esta configuración, repita Paso 2.**

▼ Desactivación de protocolos SNMP no aprobados (Oracle ILOM)

Por defecto, solamente el protocolo SNMPv3 está activado para el servicio SNMP que se usa para supervisar y gestionar Oracle ILOM. Asegúrese de que las versiones anteriores del protocolo SNMP permanezcan desactivadas a menos que se requiera lo contrario.

Algunos productos de Oracle y de terceros tienen soporte limitado para versiones de protocolo SNMP más recientes. Consulte la documentación del producto asociada con esos componentes para confirmar el soporte de versiones específicas del protocolo SNMP. Asegúrese de que Oracle ILOM esté configurado para admitir las versiones de protocolo requeridas por esos componentes.

Nota - La versión 3 del protocolo SNMP presentó compatibilidad con el modelo de seguridad basado en usuario (USM, User-based Security Model). Esta funcionalidad sustituye las cadenas de comunidad SNMP tradicionales por las cuentas de usuario reales que se pueden configurar con permisos específicos, autenticación, protocolos de privacidad y contraseñas. Por defecto, Oracle ILOM no incluye cuentas de USM. Configure cuentas de USM SNMPv3 según el tipo de requisitos de despliegue, gestión y supervisión.

---

1. **En la red de gestión, inicie sesión en Oracle ILOM.**

   Consulte Inicio de sesión en la CLI de Oracle ILOM [37].

2. **Determine el estado de cada uno de los protocolos SNMP.**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = disabled
v2c = disabled
v3 = enabled
```

3. **Si es necesario, desactive SNMPv1 y SNMPv2c.**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

4. **Para comprobar esta configuración, repita Paso 2.**

▼ Configuración de cadenas de comunidad SNMP v1 y v2c (Oracle ILOM)

Esta tarea solamente se aplica si SNMP v1 o SNMPv2c están activados y configurados para uso.

Para que SNMP funcione correctamente, el cliente y el servidor deben estar de acuerdo en la cadena comunitaria que se usa para autenticar el acceso. Por lo tanto, cuando cambie cadenas de comunidad SNMP, asegúrese de que la cadena nueva esté configurada en Oracle ILOM y para todos los componentes que intentarán conectarse con Oracle ILOM mediante el protocolo SNMP.

Dado que SNMP a menudo se usa para supervisar el estado del dispositivo, es importante que las cadenas de comunidad SNMP por defecto usadas por el dispositivo se sustituyan por valores definidos por el cliente.

1. **En la red de gestión, inicie sesión en Oracle ILOM.**

   Consulte Inicio de sesión en la CLI de Oracle ILOM [37].

2. **Cree una nueva cadena comunitaria SNMP.**

   En este ejemplo, sustituya estos elementos de la línea de comandos:

   - *string*: sustituya por un valor definido por el cliente que cumpla con los requisitos del Departamento de Defensa de los EE. UU. en relación con la composición de las cadenas de comunidad SNMP.
   - *access*: sustituya por `ro` o `rw`, según si es una cadena de acceso de solo lectura o solo escritura.

```
-> create /SP/services/snmp/communities/string permission=access
```

   Una vez que se hayan creado las cadenas de comunidad, se deberán eliminar las cadenas de comunidad por defecto.

3. **Elimine las cadenas de comunidad SNMP por defecto.**

```
-> delete /SP/services/snmp/communities/public
-> delete /SP/services/snmp/communities/private
```

4. **Compruebe las cadenas de comunidad SNMP.**

```
-> show /SP/services/snmp/communities
```

▼ Sustitución de los certificados autofirmados por defecto (Oracle ILOM)

Oracle ILOM usa certificados autofirmados para activar el uso integrado de los protocolos SSL y TLS. Siempre que sea posible, sustituya certificados autofirmados por certificados aprobados para uso en su entorno y firmados por una autoridad de certificación reconocida.

Oracle ILOM admite una variedad de métodos que se pueden usar para acceder al certificado digital y la clave privada, incluidos HTTPS, HTTP, SCP, FTP, TFTP, y pegar la información directamente en una interfaz de explorador web. Para obtener más información, consulte la *Guía de configuración y mantenimiento de Oracle ILOM* (consulte "Recursos adicionales de Oracle ILOM" [52]).

1. **Determine si Oracle ILOM está usando un certificado autofirmado por defecto.**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

2. **Instale el certificado de la organización.**

```
-> set /SP/services/https/ssl/custom_cert load_uri=URI_method
-> set /SP/services/https/ssl/custom_key load_uri=URI_method
```

▼ Configuración de timeout de inactividad de interfaz administrativa de explorador

Oracle ILOM admite la capacidad de desconectar y cerrar las sesiones administrativas que han estado inactivas durante más de un número predefinido de minutos. Por defecto, la sesión de la interfaz de explorador genera un timeout después de 15 minutos.

Los parámetros de timeout de la sesión asociados con los servicios HTTPS y HTTP se configuran y se gestionan de manera independiente. Asegúrese de configurar el parámetro `sessiontimeout` asociado con cada servicio.

1. **En la red de gestión, inicie sesión en Oracle ILOM.**

   Consulte Inicio de sesión en la CLI de Oracle ILOM [37].

2. **Compruebe el parámetro de timeout de inactividad asociado con el servicio HTTPS.**

```
-> show /SP/services/https sessiontimeout
/SP/services/https
Properties:
sessiontimeout = 15
```

3. **Configure el parámetro de timeout de inactividad.**

   Sustituya *n* por un valor especificado en minutos.

```
-> set /SP/services/https sessiontimeout=n
```

4. **Compruebe el parámetro de timeout de inactividad asociado con el servicio HTTP.**

```
-> show /SP/services/http sessiontimeout
/SP/services/http
Properties:
sessiontimeout = 15
```

5. **Configure el parámetro de timeout de inactividad.**

   Sustituya *n* por un valor especificado en minutos.

```
-> set /SP/services/http sessiontimeout=n
```

6. **Para comprobar esta configuración, repita Paso 2 y Paso 4.**

Configuración de timeout de interfaz administrativa (CLI de Oracle ILOM)

Oracle ILOM admite la capacidad de desconectar y cerrar las sesiones administrativas de la CLI que han estado inactivas durante más de un número predefinido de minutos.

Por defecto, la CLI de SSH no tiene un valor de timeout especificado y, por lo tanto, los usuarios administrativos que acceden a este servicio permanecen conectados de manera indefinida.

Por motivos de seguridad, configure este parámetro para que coincida con el valor asociado con la interfaz de usuario del explorador. Este valor podría ser 15 minutos u otro.

1. **En la red de gestión, inicie sesión en Oracle ILOM.**

   Consulte Inicio de sesión en la CLI de Oracle ILOM [37].

2. **Compruebe el parámetro de timeout de inactividad asociado con la CLI.**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **Configure el parámetro de timeout de inactividad.**

   Sustituya *n* por un valor especificado en minutos.

```
-> set /SP/cli timeout=n
```

4. **Para comprobar esta configuración, repita Paso 2.**

Configuración de banners de advertencia de inicio de sesión (Oracle ILOM)

Oracle ILOM admite la capacidad de mostrar mensajes específicos del cliente antes y después de que un administrador se haya conectado con el dispositivo.

El mensaje de conexión de Oracle ILOM se muestra antes de la autenticación, mientras que el mensaje de inicio de sesión se muestra después de la autenticación.

De manera opcional, puede configurar Oracle ILOM para que requiera la aceptación del mensaje de inicio de sesión antes de otorgar acceso a las funciones de Oracle ILOM. Los mensajes de conexión y de inicio de sesión, y los requisitos opcionales de aceptación, son implementados por las interfaces de acceso de línea de comandos y explorador.

Oracle ILOM admite mensajes de conexión e inicio de sesión de hasta un máximo de 1,000 caracteres.

1. **En la red de gestión, inicie sesión en Oracle ILOM.**
   Consulte Inicio de sesión en la CLI de Oracle ILOM [37].

2. **Determine si se han configurado los mensajes de conexión e inicio de sesión.**

```
-> show /SP/preferences/banner connect_message login_message
/SP/preferences/banner
Properties:
connect_message = (none)
login_message = (none)
```

3. **Configure un nuevo mensaje de conexión o inicio de sesión.**

```
-> set /SP/preferences/banner connect_message="Authorized Use Only"
-> set /SP/preferences/banner login_message="Authorized Use Only"
```

4. **Determine si la aceptación del mensaje de inicio de conexión está activada.**

```
-> show /SP/preferences/banner login_message_acceptance
/SP/preferences/banner
Properties:
login_message_acceptance = disabled
```

5. **(Opcional) Aplique la aceptación del mensaje de inicio de sesión.**

Atención - El requerimiento de la aceptación del mensaje de inicio de sesión podría inhibir el funcionamiento correcto de los procesos de gestión automatizada que usan SSH, ya que es posible que no puedan o no estén configurados para responder a la solicitud de aceptación. Como resultado, las conexiones se pueden bloquear o se puede alcanzar el timeout ya que Oracle ILOM no permitirá el uso de la CLI hasta que no se haya satisfecho el requisito de aceptación del mensaje.

```
-> set /SP/preferences/banner login_message_acceptance=enabled
```

6. **Para comprobar esta configuración, repita Paso 2 and Paso 4.**

Recursos adicionales de Oracle ILOM

Para obtener más información sobre los procedimientos de administración y seguridad de Oracle ILOM, consulte la biblioteca de documentación de Oracle ILOM que corresponde a la versión que se ejecuta en SuperCluster M7:

- *Guía de seguridad de Oracle ILOM, versiones de firmware 3.0, 3.1 y 3.2*:

http://docs.oracle.com/cd/E37444_01/html/E37451

- Oracle Integrated Lights Out Manager versión 3.2.*x*:

  http://docs.oracle.com/cd/E37444_01
- Oracle Integrated Lights Out Manager versión 3.1.*x*:

  http://docs.oracle.com/cd/E24707_01
- Oracle Integrated Lights Out Manager versión 3.0.*x*:

  http://docs.oracle.com/cd/E19860-01

Protección de servidores de cálculo

Se instalan uno o dos servidores SPARC M7 (servidores de cálculo) en SuperCluster M7. Cada servidor de cálculo está dividido en dos particiones de hardware (dos PDomains). Cada PDomain incluye la mitad de los posibles procesadores, memoria y ranuras de expansión PCIe en el chasis. Ambos PDomains funcionan como un servidor independiente dentro del mismo chasis. Un par de módulos de procesador de servicio redundantes (SPM) gestionan cada partición.

Debe proteger cada PDomain.

En esta sección, se proporciona un juego de controles de seguridad para los servidores de cálculo.

▼ Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto

Para acceder a un solo PDomain mediante Oracle ILOM, debe iniciar sesión en el SPM activo que controla dicho PDomain. Puede encender, reiniciar o gestionar una partición mientras la otra sigue funcionando normalmente.

Existen varios métodos para iniciar sesión en un servidor de cálculo SuperCluster. El método que se describe en esta tarea involucra el inicio de sesión en la interfaz de línea de comandos

del SPM del servidor de cálculo. Este método le permite acceder al servidor en cualquiera de estos estados:

- En modo de energía en espera
- El sistema está encendido, pero no en ejecución
- El sistema operativo se está iniciando
- Completamente encendido y con el sistema operativo en ejecución

1. **En la red de gestión, inicie sesión mediante el comando `ssh`.**

```
$ ssh root@compute_server_SPM_ILOM_IP-address
```

2. **Cuando se le solicite, introduzca la contraseña.**

   La contraseña por defecto de fábrica de `root` es `welcome1`.

   Si se le solicita que cambie la contraseña, hágalo.

   En este punto, puede realizar cualquiera de las tareas de seguridad que se llevan a cabo en Oracle ILOM en el servidor de cálculo.

3. **Si desea acceder a la consola de host del servidor de cálculo, inicie la consola del host.**

```
    -> start /Servers/PDomains/PDomain_0/HOST/console
Are you sure you want to start /Servers/PDomains/PDomain_0/HOST/console (y/n)? y

Serial console started.  To stop, type #.

root@system-identifier-pd0:~#
```

Nota - No verá la petición de datos de PDomain si no se está ejecutando el host.

Nota - Para volver a la petición de datos de Oracle ILOM, escriba los caracteres de escape (`#.` son los caracteres por defecto).

4. **Si es necesario, asuma un rol de superusuario.**

   Use el comando `su` para cambiar a un usuario que esté configurado con el rol `root`.

Cuentas y contraseñas por defecto (servidores de cálculo)

Cuenta	Contraseña por defecto	Descripción
`root`	`welcome1`	Oracle ILOM requiere que se cambie la contraseña por defecto de inmediato después del primer inicio de sesión correcto.
`oracle`	`welcome1`	
`grid`	`welcome1`	

▼ Determinación de la versión del software SuperCluster

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host.**

   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Escriba este comando.**

```
# svcprop -p configuration/build svc:/system/oes/id:default
```

   En la salida, los números anexados a `ssc` representan la versión de software.

   Para actualizar la versión del software SuperCluster, instale el parche de descarga de pila completa trimestral de SuperCluster disponible en My Oracle Support, en `https://support.oracle.com`.

Nota - Para SuperCluster, es posible que existan restricciones adicionales que limiten las versiones de software que se pueden usar y la manera en la que se actualizan las versiones. En estas situaciones, comuníquese con su representante de Oracle.

▼ Configuración del servicio de shell seguro

La realización de esta tarea mejora la configuración de seguridad de shell seguro implementada en Oracle SuperCluster.

El archivo `/etc/ssh/sshd_config` es un archivo de configuración del sistema, donde puede configurar parámetros para el servicio de shell seguro.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**

   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Edite el archivo `/etc/ssh/sshd_config`.**

3. **Configure el parámetro `ListenAddress` para garantizar que solamente se aceptarán las conexiones que se originen desde la red de acceso de cliente de SuperCluster.**

   Asegúrese de que la dirección IP `ListenAddress` esté configurada en la red del cliente.

   Esto garantiza que las conexiones de shell seguro no se podrán iniciar correctamente entre los componentes mediante redes de gestión o IB.

4. **Revise otros parámetros de `sshd_config` y configúrelos según los requisitos del sitio.**

   Estos ajustes protegen el servicio de shell seguro:

```
Protocol 2
Banner /etc/issue
PermitEmptyPasswords no
PermitRootLogin no
StrictModes yes
IgnoreRhosts yes
PrintLastLog yes
X11Forwarding no
ClientAliveInterval 600
ClientAliveCountMax 0
```

5. **Guarde el archivo `sshd_config`.**

6. **Reinicie el servicio.**

   Debe reiniciar el servicio para que se apliquen los cambios.

```
# svcadm restart ssh
```

▼ Verificación de que `root` es un rol

Por defecto, Oracle Solaris está configurado de modo que `root` es un rol y no una cuenta de usuario. Además, la configuración de SuperCluster no permite inicios de sesión de usuario `root` anónimos. En su lugar, todos los usuarios deben iniciar sesión como usuarios regulares antes de asumir el rol de usuario. Todas las operaciones de administración de SuperCluster se deben llevar a cabo mediante el uso de `root` como rol.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host.**

   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Verifique que los atributos de `root` estén configurados en `type=role`.**

```
# grep root /etc/user_attr
root::::type=role
```

3. **(Opcional) Asigne un usuario regular al rol `root`.**

```
# usermod -R root user_name
```

Servicios de red expuestos por defecto (servidores de cálculo)

En esta tabla, se muestran los servicios de red por defecto expuestos nuevamente en los servidores de cálculo.

Nombre de servicio	Protocolo	Puerto	Descripción
SSH	TCP	22	Usado por el servicio de shell seguro integrado para permitir el acceso administrativo a los servidores de cálculo mediante una interfaz de línea de comandos.
HTTP (BUI)	TCP	80	Usado por el servicio HTTP integrado para permitir el acceso administrativo a los servidores de cálculo mediante una interfaz de explorador.
HTTPS (BUI)	TCP	443	Usado por el servicio HTTPS integrado para permitir el acceso administrativo a los servidores de cálculo por un canal (SSL/TLS) cifrado mediante una interfaz de explorador.
SNMP	UDP	161	Usado por el servicio SNMP integrado para proporcionar una interfaz de gestión para supervisar el estado de los servidores de cálculo y supervisar las notificaciones de captura recibidas.

Endurecimiento de la configuración de seguridad del servidor de cálculo

En estos temas, se describe cómo configurar servidores de cálculo de manera segura.

- Activación del servicio `intrd` [60]

▼ Activación del servicio `intrd`

El servicio de equilibrador de interrupciones (`intrd`) supervisa las asignaciones entre interrupciones y CPU para garantizar un rendimiento óptimo. Para obtener más información, consulte la página del comando man `intrd(1M)`.

Este servicio solamente se ejecuta en la zona global.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**

   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Inicie el servicio.**

```
# svcadm enable intrd
```

Desactivación de servicios innecesarios (servidores de cálculo)

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**
   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Desactive el monitor de estado NFS si el sistema no está en servidor o un cliente NFS.**
   Este servicio interactúa con `lockd(1M)` para proporcionar las funciones de bloqueo y recuperación para los servicios de bloqueo en NFS.

```
# svcadm disable svc:/network/nfs/status
```

3. **Desactive el servicio de gestor de bloqueo de NFS si no está usando NFS o si está usando NFSv4.**
   El gestor de bloqueo de NFS admite operaciones de bloqueo de registro en archivos NFS de NFSv2 y NFSv3.

```
# svcadm disable svc:/network/nfs/nlockmgr
```

4. **Si el sistema no está montando archivos, puede desactivar el servicio de cliente NFS o desinstalar su paquete.**
   El servicio de cliente NFS solamente es necesario si el sistema está montando archivos desde un servidor NFS. Para obtener más información, consulte la página del comando man `mount_nfs(1M)`.

```
# svcadm disable svc:/network/nfs/client
```

5. **Desactive el servicio del servidor NFS en un sistema que no sea un servidor de archivos NFS.**
   El servicio de servidor NFS administra las solicitudes del sistema de archivos de cliente mediante NFS versión 2, 3 y 4. Si este sistema no es un servidor NFS, desactive el servicio.

```
# svcadm disable svc:/network/nfs/server
```

6. **Si no está usando FedFS para registros SRV de DNS o referencias basadas en LDAP, desactive el servicio.**

   El servicio de cliente del sistema de archivos federados (FedFS) gestiona los valores por defecto y la información de conexión para servidores LDAP que almacenan información de FedFS.

   ```
   # svcadm disable svc:/network/nfs/fedfs-client
   ```

7. **Desactive el servicio `rquota`.**

   El servidor de cuota `remote` devuelve cuotas para un usuario de un sistema local de archivos montado mediante NFS. El comando `quota(1M)` usa los resultados para mostrar las cuotas de usuario para sistemas de archivos remotos. El comando `inetd(1M)` generalmente invoca el daemon `rquotad(1M)`. El daemon proporciona información acerca de la red para usuarios potencialmente maliciosos.

   ```
   # svcadm disable svc:/network/nfs/rquota
   ```

8. **Desactive el servicio `cbd`.**

   El servicio `cbd` gestiona puntos finales de comunicación para el protocolo NFS versión 4. El daemon `nfs4cbd(1M)` ejecuta el cliente NFS versión 4 y crea un puerto de listener para devoluciones de llamadas.

   ```
   # svcadm disable svc:/network/nfs/cbd
   ```

9. **Desactive el servicio `mapid` si no está usando NFSv4.**

   El servicio de daemon de asignación de ID y usuario de NFS realiza asignaciones desde y hasta los atributos de identificación `owner` y `owner_group` de la versión 4 de NFS y los números de UID y GID local usados por el servidor y el cliente de la versión 4 de NFS.

   ```
   # svcadm disable svc:/network/nfs/mapid
   ```

10. **Desactive el servicio `ftp`.**

    El servicio FTP proporciona servicio de transferencia de archivos no cifrados y usa autenticación de texto sin formato. Use el programa de copia segura `scp(1)` en lugar de `ftp`, ya que proporciona autenticación cifrada y transferencia de archivos.

    ```
    # svcadm disable svc:/network/ftp:default
    ```

11. **Desactive el servicio de gestor de volumen remoto.**

    El gestor de volumen removible es un gestor de volumen que reconoce HAL que puede montar y desmontar automáticamente medios y almacenamiento conectable en caliente. Es posible que los usuarios importen programas malintencionados o transfieran datos confidenciales fuera del sistema. Para obtener más información, consulte la página del comando man `rmvolmgr(1M)`.

Este servicio solamente se ejecuta en la zona global.

```
# svcadm disable svc:/system/filesystem/rmvolmgr
```

12. Desactive el servicio `smserver`.

El servicio `smserver` se usa para acceder a los dispositivos de medios extraíbles.

```
# svcadm disable rpc/smserver:default
```

13. Especifique `pam_deny.so.1` como módulo para la pila de autenticación de los servicios de `r-protocol` en el directorio `/etc/pam.d`.

Por defecto, los servicios heredados, como `r-protocols`, `rlogin(1)` y `rsh(1),` no están instalados. Sin embargo, estos servicios se definen en `/etc/pam.d`. Si elimina las definiciones de servicio de `/etc/pam.d`, los servicios usan los demás servicios (por ejemplo, SSH) en caso de que los servicios heredados estén activados.

```
# cd /etc/pam.d
# cp rlogin rlogin.orig
# pfedit rlogin
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
# cp rsh rsh.orig
# pfedit rsh
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
```

14. Edite el archivo `/etc/default/keyserv` para cambiar el valor de `ENABLE_NOBODY_KEYS` a `NO`.

El servicio `keyserv` no puede usar la clave de usuario `nobody`. El valor de `ENABLE_NOBODY_KEYS` es `YES` por defecto.

```
# pfedit /etc/default/keyserv
. . .
ENABLE_NOBODY_KEYS=NO
```

15. Agregue usuarios al archivo `ftpusers` para restringir el acceso a `ftp`.

Las transferencias de archivos FTP no deben estar disponibles para todos los usuarios y deben requerir que los usuarios calificados suministren sus nombres y contraseñas. En general, los usuarios del sistema no deben tener permiso para usar FTP. Esta comprobación verifica que las cuentas del sistema se han incluido en el archivo `/etc/ftpd/ftpusers`, de modo que no tienen permiso para usar FTP.

El archivo `/etc/ftpd/ftpusers` se usa para prohibir a los usuarios que usen el servicio FTP. Como mínimo, incluya todos los usuarios del sistema, como `root`, `bin`, `adm`, etc.

```
# pfedit /etc/ftpd/ftpusers
....
root
daemon
bin
...
```

16. **Configure una máscara de creación de archivos por defecto segura mediante el servidor FTP.**

    El servidor FTP no necesariamente usa la máscara de creación de archivos del sistema del usuario. La configuración del comando umask del FTP garantiza que los archivos transmitidos mediante FTP usarán un comando umask de creación de archivos seguro.

    ```
    # pfedit /etc/proftpd.conf
    Umask          027
    ```

17. **Desactive las respuestas a las consultas de topología de red.**

    Es importante desactivar las respuestas a las solicitudes de eco. Las solicitudes de ICMP se gestionan mediante el comando `ipadm`.

    Estos ajustes impiden la difusión de información sobre la topología de la red.

    ```
    # ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
    # ipadm set-prop -p _respond_to_echo_broadcast=0 ip
    ```

18. **Desactive los mensajes de ICMP de redireccionamiento.**

    Los enrutadores utilizan los mensajes de redireccionamiento de ICMP para informar a los hosts sobre rutas más directas hacia un destino. Un mensaje de redireccionamiento de ICMP ilícito puede generar un ataque de tipo "man-in-the-middle".

    ```
    # ipadm set-prop -p _ignore_redirect=1 ipv4
    ```

19. **Desactive `mesg(1)` para evitar que `talk(1)` y `write(1)` accedan a las terminales remotas.**

    ```
    # mesg -n
    ```

20. **(Opcional) Revise y desactive la escucha de servicios innecesarios en la red.**

    Por defecto, `ssh(1)` es el único servicio de red que puede enviar y recibir paquetes de red.

    ```
    # svcadm disable FMRI_of_unneeded_service
    ```

▼ Activación de varios orígenes estrictos

Para los sistemas que son gateways a otros dominios, como un firewall o un nodo de VPN, se debe activar la función de varios orígenes estrictos. La propiedad `hostmodel` controla

el comportamiento de envío y recepción de paquetes IP en un sistema de varios orígenes. Configure la opción de varios orígenes en `1` de modo que los paquetes no se acepten en una interfaz diferente. El valor por defecto es `0`.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**

   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Configure la opción de varios orígenes estrictos en `1`.**

```
# ipadm set-prop -p _strict_dst_multihoming=1 ipv4
```

Activación de la ASLR

Nota - No active la ASLR en dominios de base de datos o en zonas de base de datos.

Oracle Solaris etiqueta muchos de sus datos binarios de usuarios de usuarios para activar la ejecución aleatoria de la disposición del espacio de direcciones (ASLR). La ASLR ejecuta aleatoriamente la dirección de inicio de partes clave de un espacio de direcciones. Este mecanismo de defensa de seguridad puede hacer que los ataques de la programación orientada al retorno (ROP) fallen cuando traten de explotar las vulnerabilidades de seguridad del software. Las zonas heredan esta disposición de ejecución aleatoria para sus procesos. Dado que es posible que el uso de la ASLR puede no sea óptimo para todos los datos binarios, la ASLR se puede configurar en el nivel de zona y en el nivel binario.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**

   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Active la ASLR.**

```
# sxadm delcust aslr
# sxadm info
EXTENSION    STATUS                CONFIGURATION
aslr         enabled (tagged-files) System default (default)
```

Configuración de conexiones de TCP

La configuración de las conexiones de TCP de apertura media máximas en 4096 por dirección IP y por puerto ayuda a protegerse contra los ataques de denegación de servicio de flujo SYN. La configuración del número máximo de conexiones TCP entrantes en cola a, por lo menos, 1024 ayuda a evitar ciertos ataques de denegación de servicio (DDoS) distribuidos.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**
   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Configure las conexiones TCP entrantes en cola y de apertura media máximas.**

```
# ipadm set-prop -p _conn_req_max_q0=9096 tcp
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

Configuración de logs de historial de contraseñas y políticas de contraseñas para conformidad con PCI

El parámetro `HISTORY` del archivo `/etc/default/passwd` evita que los usuarios usen contraseñas similares con el valor `HISTORY`.

Si `MINWEEKS` está configurado en `3` y `HISTORY` está configurado en `10`, las contraseñas no se podrán volver a usar durante 10 meses.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**
   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Edite el archivo `/etc/default/passwd` y configure los parámetros de contraseña.**

```
# pfedit /etc/default/passwd
. . .
#Compliance to the PCI-DSS benchmark is 10
#HISTORY=0
HISTORY=10
MINDIFF=4
MINDIGIT=1
```

```
MINUPPER=1
MINWEEKS=3
MAXWEEKS=13
```

3. **Edite el archivo `/etc/default/login` para incluir estos parámetros.**

```
# pfedit /etc/default/login
. . .
# Compliance edit
#PASSLENGTH=6
PASSLENGTH=14
. . .
```

Cómo garantizar que los directorios de inicio tengan los permisos adecuados

Los propietarios de los directorios de inicio deben poder escribir y buscar en ellos. Generalmente, otros usuarios no tienen derechos para modificar esos archivos o para agregar archivos al directorio de inicio del usuario. Para asegurarse de que este sea el caso, configure los permisos en el directorio del usuario.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**
   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Configure los permisos en un directorio del usuario.**

```
# chmod 750 /export/home/user_home_directory
```

Activación del firewall de filtro de IP

La función de filtro de IP es un firewall basado en host que proporciona un filtrado de paquetes con estado y la traducción de direcciones de red (NAT). Los filtros de paquetes ofrecen protección básica contra ataques de la red. El filtro de IP también incluye filtrado de paquetes sin estado y permite crear y gestionar agrupaciones de direcciones.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**
   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Active el firewall de filtro de IP.**

```
# svcadm svc:/network/ipfilter:default
```

Cómo garantizar que los servicios de nombres solamente usen archivos locales

El sistema operativo usa un número de bases de datos de información sobre hosts, `ipnodes`, usuarios (`passwd(4)`, `shadow(4)`, `user_attr(4)`) y `groups`. Los datos de estos elementos provienen de una variedad de orígenes. Por ejemplo, los nombres de host y las direcciones de host, se pueden encontrar en`/etc/hosts`, NIS, LDAP, DNS o DNS multidifusión. Los sistemas que se encuentran en entornos restringidos son más seguros si solamente se usan entradas de archivos locales para estos elementos.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**
   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Configure los servicios de nombres para usar solamente archivos locales.**

```
# svccfg -s name-service/switch setprop config/default = astring: "files"
# svccfg -s name-service/switch setprop config/host = astring: "files"
# svccfg -s name-service/switch setprop config/password = astring: "files"
# svccfg -s name-service/switch setprop config/group = astring: "files"
# svccfg -s name-service/switch:default refresh
```

Activación de Sendmail y servicios de NTP

El servicio de sendmail se debe estar ejecutando; de lo contrario, no se entregará el correo del sistema importante a `root`.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**
   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Active sendmail.**

```
# svcadm enable smtp:sendmail
```

3. **Si es necesario, instale el servicio de NTP.**

   El servicio `ntp` debe estar instalado en todos los sistemas donde se desea seguridad y conformidad.

```
# pkg install service/network/ntp
```

4. **Configure el servicio NTP como cliente y active el servicio.**

   El daemon Protocolo de hora de red se debe activar y configurar correctamente como cliente. El archivo `/etc/inet/ntp.conf` debe incluir al menos una definición de servidor. El archivo también debe contener la línea `restrict default ignore` para evitar que el cliente también actúe como servidor.

```
# vi /etc/inet/ntp.conf
. . .
server server_IP_address iburst
restrict default ignore ...
# svcadm enable ntp
```

Desactivación de GSS (a menos que se use Kerberos)

El servicio de seguridad genérico (`gss`) gestiona la generación y la validación de los tokens de seguridad de la Interfaz del programa de aplicación de servicios de seguridad genéricos (GSS-API). El daemon `gssd(1M)` funciona entre el núcleo `rpc` y GSS-API.

Nota - Kerberos usa este servicio. Desactive el servicio `rpc/gss` si Kerberos no está configurado y no está en uso.

---

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**

   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Active `rpc/gss`.**

```
# svcadm enable rpc/gss
```

3. **Defina un límite para `/tmpfs`.**

El tamaño del sistema de archivos `tmpfs` no está limitado por defecto. A fin de evitar un impacto en el rendimiento, puede limitar el tamaño de cada montaje de `tmpfs`. Para obtener más información, consulte las páginas del comando man `mount_tmpfs(1M)` y `vfstab(4)`.

```
# pfedit /etc/vfstab
...
swap - /tmp tmpfs - yes size=sz
```

4. **Reinicie el servidor de cálculo.**

```
# reboot
```

Configuración bits de permanencia para archivos con permiso general de escritura

El bit de permanencia de un directorio evita que cualquier persona, excepto el propietario del archivo o el rol `root`, pueda suprimir o mover el directorio con permiso general de escritura. Esto resulta útil en directorios que son comunes a varios usuarios, como el directorio `/tmp`.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**
   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Defina el bit de permanencia en `/tmp` y en el resto de los archivos con permiso general de escritura.**

```
# chmod 1777 /tmp
```

Protección de volcados de núcleo

Los volcados de núcleo pueden contener datos importantes. La protecciones pueden incluir permisos de archivos y registro de eventos de volcado de núcleo. Consulte las páginas del comando man `coreadm(1m)` y `chmod(1M)`.

Use el comando `coreadm` para ver y definir la configuración actual.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**

Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Visualice la configuración actual.**

```
# coreadm
global core file pattern: /var/share/cores/core.%f.%p
global core file content: default
init core file pattern: core
init core file content: default
global core dumps: enabled
per-process core dumps: enabled
global setid core dumps: disabled
per-process setid core dumps: disabled
global core dump logging: enabled
```

3. **Configure los archivos de núcleo y proteja el directorio de volcado de núcleo.**

```
# coreadm -g /var/cores/core_%n_%f_%u_%g_%t_%p \
          -e log -e global -e global-setid \
          -d process -d proc-setid
```

4. **Compruebe los permisos.**

```
# ls -ld /var/share/cores
drwx------ 2 root root 2 Aug 2 2015 cores/
```

5. **Configure los permisos correctamente en el directorio.**

```
# chmod 700 /var/share/cores
```

Aplicación de pilas no ejecutables

La activación de pilas no ejecutables es una técnica muy útil para impedir determinados tipos de ataques de desbordamiento de buffer. Si `nxstack` de Oracle Solaris está activado, el segmento de memoria de la pila del proceso se marca como no ejecutable. Esta extensión defiende contra los ataques que se basan en la inyección de código malintencionado y en su ejecución en la pila.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**

   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Active `nxstack`.**

```
# sxadm set model=all nxstack
```

3. **Verifique la configuración.**

```
# sxadm get all nxstack
EXTENSION     PROPERTY     VALUE
nxstack         model        all
```

Activación del espacio de intercambio cifrado

Cifre el espacio de intercambio, ya sea si es un volumen ZFS o un dispositivo raw. El cifrado garantiza que los datos importantes, como las contraseñas de usuario, estarán protegidos si el sistema necesita intercambiar esas páginas con el disco.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**
   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Edite el archivo `/etc/vfstab` y configure `swap` en `encrypted`.**

```
# pfedit /etc/vfstab
...
/dev/zvol/dsk/rpool/swap - - swap - no encrypted
```

3. **Cree e inicialice un almacén de claves PKCS #11.**

```
# pktool setpin keystore=pkcs11
Enter token passphrase: changeme
Create new passphrase: welcome1
Re-enter new passphrase: welcome1
```

4. **Genere una clave simétrica y almacénela en un almacén de claves PKCS #11.**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=globalzone-key
```

Activación de la auditoría

Asegúrese de que los logs de auditoría capturen todas las acciones administrativas, incluidos los comandos con argumentos.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**

   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Configure la instalación de auditoría.**

```
# auditconfig -setpolicy +argv
# auditconfig -setflags lo,ad,ex >& /dev/null
# auditconfig -setpolicy +zonename
```

Activación de protección de enlace de datos (falsificación) en zonas globales

La protección de enlace de datos de Oracle Solaris evita posibles daños causados por máquinas virtuales malintencionadas en la red.

La activación de la configuración de corrección de búsqueda mejora el rendimiento de la red, ya que permite que el tráfico de red del entorno virtual sea aislado del tráfico mayor recibido o enviado por el sistema host. La protección de enlace evita los daños que pueden ser causados por posibles máquinas virtuales malintencionadas en la red. La función ofrece protección contra las siguientes amenazas básicas:

- Falsificación de IP y MAC
- Falsificación de marco L2, como los ataques de unidad de datos del protocolo de puente (BPDU)

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**

   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Configure la protección de enlaces.**

```
# dladm set-linkprop -p protection=mac-nospoof,restricted,ip-nospoof,dhcp-nospoof net0
```

3. **Confirme la configuración.**

```
# dladm show-linkprop -p protection net0
LINK         PROPERTY     PERM     VALUE         EFFECTIVE         DEFAULT     POSSIBLE
net0         protection     rw     mac-nospoof   mac-nospoof        --         mac-nospoof,
                                   restricted    restricted         --         restricted,
```

```
                                    ip-nospoof    ip-nospoof        --        ip-nospoof,
                                    dhcp-nospoof  dhcp-nospoof      --        dhcp-nospoof
```

4. **Defina las IP permitidas en el enlace.**

```
# dladm set-linkprop -p allowed-ips=10.0.0.1,10.0.0.2 net0
```

Activación de protección de enlace de datos (falsificación) en zonas no globales

La protección de enlace de datos de Oracle Solaris también se puede aplicar de forma individual a todas las zonas no globales de Oracle Solaris implementadas dentro del entorno de SuperCluster.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**

   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Aplique la protección de enlace de datos en una interfaz de red determinada mediante el comando `zonecfg(1M)`.**

   Asegúrese de que la lista de direcciones IP permitidas sea precisa y esté completa. La lista debe incluir las direcciones IP virtuales usadas por IPMP de Oracle Solaris, Oracle Real Application Clusters, etc. Además, tenga en cuenta que los cambios realizados en la configuración de la zona no global de SuperCluster no se aplican hasta que no se reinicia la zona no global.

```
# zonecfg –z zonename
zonecfg:zonename> select anet linkname=network-link-name
zonecfg:zonename:anet> set allowed-address="list_of_allowed_IP_addresses"
zonecfg:zonename:anet>  set link-protection=mac-nospoof,ip-nospoof,restricted
zonecfg:zonename:anet>  set configure-allowed-address=false
zonecfg:zonename:anet>  end
zonecfg:zonename>  commit
zonecfg:zonename>  exit
```

Creación de juegos de datos ZFS

Las organizaciones que requieren la protección *data-at-rest* pueden optar por proteger aún más las aplicaciones implementadas en la zona y la información mediante los juegos de datos ZFS

cifrados. Para garantizar que todas las zonas no globales se puedan iniciar sin intervención del administrador, los juegos de datos ZFS cifrados se configuran para acceder a las claves de cifrado de ZFS que se almacenan de manera local dentro de la base de datos individual o del dominio de la aplicación.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**

   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Cree claves de cifrado ZFS.**

   Una manera simple de crear la clave requerida consiste en usar comandos similares a estos:

```
# zfs create zfs_pool_name/zfskeystore
$ chown root:root /zfs_pool_name/zfskeystore
$ chmod 700 /zfs_pool_name/zfskeystore
$ pktool genkey keystore=file keytype=aes keylen=256 \
outkey=/zfs_pool_name/zfskeystore/zone_name.key
```

3. **Cree el juego de datos ZFS cifrado.**

```
# zfs create -o encryption=aes-256-ccm -o \
keysource=raw,file:///zfs_pool_name/zone_name.key \
zfs_pool_name/zone_name
```

4. **Cifre u01 y los juegos de datos comunes.**

   Este mismo enfoque se puede usar para cifrar u01 y los juegos de datos comunes, mediante la misma clave (específica de SuperCluster) o mediante una clave única por juego de datos, según los requisitos y las políticas específicas del sitio. En este ejemplo, el juego de datos comunes se crea mediante la misma clave creada en Paso 3. Tenga en cuenta que los parámetros de configuración de ZFS adicionales, como la compresión, también se pueden definir durante la creación de estos juegos de datos adicionales.

```
# zfs create -o compression=on -o encryption=aes-256-ccm -o \
keysource=raw,file:///zfs_pool_name/zfskeystore/zone_name.key \zfs_pool_name/u01
```

▼ (Opcional) Configuración de frase de contraseña para acceso del almacén de claves

La tarea anterior,Creación de juegos de datos ZFS [74], usa un archivo de clave (raw) definido de manera local que se debe almacenar directamente en un sistema de archivos. Otra técnica de almacenamiento de claves aprovecha un almacén de claves PKCS#11 protegido por

frase de contraseña, denominado *Softtoken de Sun Software PKCS#11*. Para usar este método, realice esta tarea.

El almacén de claves PKCS#11 se debe desbloquear manualmente antes de que la clave se ponga a disposición de ZFS. En última instancia, esto significa que la intervención administrativa manual se requiere para montar el juego de datos ZFS cifrado (y para iniciar la zona no global si la zona también usa un juego de datos ZFS cifrado). Para obtener más información sobre otras estrategias de almacenamiento de claves, consulte la página del manual `zfs_encrypt(1M)`.

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**
   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Defina un PIN (frase de contraseña) que se requerirá para acceder al almacén de claves.**
   El PIN por defecto asociado con un nuevo almacén de claves PKCS#11 es `changeme`. Use esta frase de contraseña en la primera petición de datos de este ejemplo.

```
# pktool setpin keystore=pkcs11
Enter token passphrase:
Create new passphrase:
Re-enter new passphrase:
```

3. **Defina una variable de entorno `${SOFTTOKEN}` para almacenar la clave en una ubicación diferente.**
   El material de clave usado por el softtoken PKCS#11 se almacena por defecto en el directorio `/var/user/ ${USERNAME}/pkcs11_softtoken`. La variable de entorno `${SOFTTOKEN}` se puede definir para almacenar el material de la clave en una ubicación diferente. Puede usar esta capacidad para activar el almacenamiento específico de SuperCluster para este material de clave protegida por contraseña.

```
# export SOFTTOKEN=/<zfs_pool_name>/zfskeystore
# pktool setpin keystore=pkcs11
Enter token passphrase:
Create new passphrase:
Re-enter new passphrase:
```

4. **Cree una clave.**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=zone_name_rpool
Enter PIN for Sun Software PKCS#11 softtoken:
```

5. **Cree el juego de datos de ZFS cifrado; para ello, consulte la clave creada en el paso anterior.**

```
# zfs create -o encryption=aes-256-ccm -o keysource=raw,pkcs11:
object=<zone_name>_rpool zfs_pool_name/zone_name
Enter PKCS#11 token PIN for 'zfs_pool_name/zone_name':
```

Creación de zonas globales inmutables

La protección contra alteraciones mediante inmutabilidad permite a las zonas globales y no globales crear un entorno de funcionamiento resistente y de alta integridad dentro del cual los servidores de cálculo de SuperCluster operan sus propios servicios. Las zonas inmutables se basan en las capacidades de seguridad inherentes de las zonas globales y no globales de Oracle Solaris, y garantizan que (algunos o todos) los directorios y los archivos del sistema operativo no se podrán cambiar (sin intervención del administrador). La aplicación de esta postura de solo lectura ayuda a evitar cambios no autorizados, promueve procedimientos de gestión de cambios más eficaces y desalienta la inyección de malware basada en núcleo y usuario.

Nota - Una vez que se ha configurado la zona inmutable, no se puede actualizar de otra manera que no sea mediante el inicio de sesión en la ruta de confianza o cuando el sistema se reinicia mediante el modo de escritura con el comando `reboot -- -w`.

Si bien siempre debe confirmar que el software de la aplicación funciona de manera esperada en un entorno inmutable, tenga en cuenta que la ejecución correcta de las instancias de Oracle Database y los clusters de Oracle RAC se verifica dentro de las zonas no globales inmutables de Oracle Solaris.

1. **Inicie sesión en la zona global de Oracle Solaris (dominio dedicado, dominio raíz o dominio de E/S) como superusuario.**
   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Modifique la configuración de la zona global de Oracle Solaris mediante el ajuste de la propiedad `file-mac-profile`.**

   ```
   # zonecfg -z global set file-mac-profile=fixed-configuration
   zonecfg:global> commit
   ```

3. **Reinicie la zona global de Oracle Solaris para que se apliquen los cambios. Inicie sesión en el dominio mediante la consola de ILOM.**

4. **Inicie la consola de la ruta de confianza de la zona global inmutable.**
   Cuando se configura la zona global inmutable, es importante introducir el inicio de sesión de la consola mediante una de estas secuencias de salto:

- **Consola gráfica**: F1-A
- **Consola serie**: <Break> o la secuencia de salto alternativa (CR~ Ctrl-b)

```
trusted path console login:
```

5. **Inicie sesión en la zona global del dominio de E/S y asuma el rol `root` para llevar a cabo actualizaciones específicas en el sistema, a continuación reinicie el sistema para regresarlo al modo de solo lectura.**

```
# reboot
```

▼ Configuración de zonas no globales inmutables

Para configurar una zona no global de Oracle Solaris para que sea inmutable, realice esta tarea.

Nota - El sistema operativo Oracle Solaris 11 admite ajustes de configuración de zonas inmutables adicionales más allá del ajuste identificado en esta tarea (configuración fija). Para obtener más información sobre estas opciones, consulte la página del manual `zonecfg(1M)`. Sin embargo, solamente se probó la opción de configuración fija como parte de la arquitectura de SuperCluster.

Atención - La agregación, modificación o supresión de cuentas y contraseñas de usuario de zona no se puede llevar a cabo una vez que se ha activado la inmutabilidad de zonas no globales de Oracle Solaris, como se describe en esta tarea. Sin embargo, este problema se puede resolver mediante la implementación de un directorio de LDAP para contener información específica de la zona, como usuarios, roles, grupos, perfiles de derechos, etc.

Atención - La funcionalidad de la zona inmutable de Oracle Solaris está limitada a esos juegos de datos ZFS que se implementan por defecto en una zona no global de Oracle Solaris. Los sistemas de archivos, las agrupaciones o los juegos de datos adicionales no están sujetos a la política de zona inmutable, aunque el acceso a esos elementos de archivo se puede controlar mediante otros medios, como el uso de montajes de bucle de retorno de solo lectura.

---

1. **Inicie sesión en uno de los servidores de cálculo y acceda a la consola del host como superusuario.**

   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Asegúrese de que la zona no global de Oracle Solaris esté apagada.**

   Si este comando devuelve un valor, entonces se está ejecutando la zona no global de Oracle Solaris y deberá apagarla.

   Nota - Si bien la zona se puede detener mediante el comando `zoneadm(1M)`, siga los procedimientos de apagado correspondientes que ha establecido su organización para evitar el potencial de interrupción de servicio y pérdida de datos.

   ```
   # zoneadm list | grep -w "zone_name"
   ```

3. **Ajuste la configuración de la zona no global de Oracle Solaris mediante la configuración de la propiedad de configuración de zona `file-mac-profile`.**

   ```
   # zonecfg -z zone_name set file-mac-profile=fixed-configuration
   ```

4. **Si es necesario, desactive la configuración inmutable de la zona no global.**

   ```
   # zonecfg -z zone_name set file-mac-profile=none
   ```

5. **Reinicie la zona no global de Oracle Solaris para que se apliquen los cambios.**

   ```
   # zoneadm -z zone_name boot
   ```

▼ Activación del inicio verificado seguro (CLI de Oracle ILOM)

Use esta tarea para activar el inicio verificado seguro mediante la CLI de Oracle ILOM. De manera alternativa, puede usar la interfaz web de Oracle ILOM. Consulte “Inicio verificado seguro (interfaz web de Oracle ILOM)” [81].

El inicio verificado consulta la verificación de los módulos de objeto antes de la ejecución mediante firmas digitales. Oracle Solaris protege contra la carga de módulos de núcleo peligrosos. El inicio verificado aumenta la seguridad y la solidez de Oracle Solaris mediante la verificación de los módulos del núcleo antes de la ejecución.

Si está activado, el inicio verificado de Oracle Solaris comprueba la firma de fábrica en un módulo de núcleo antes de cargar y ejecutar el módulo. Esta comprobación detecta la modificación accidental o malintencionada de un módulo. La acción realizada se puede configurar y, si está activada, imprimirá un mensaje de advertencia y continuará cargando y ejecutando el módulo, o fallará y no cargará ni ejecutará el módulo.

1. **Acceda a Oracle ILOM en el servidor de cálculo.**

   Consulte Inicio de sesión en un servidor de cálculo y cambio de la contraseña por defecto [55].

2. **Active el inicio verificado.**

```
-> set /HOST/verified_boot/ module_policy=enforce
Set 'module_policy' to 'enforce'
```

3. **Acceda al certificado proporcionado por Oracle y visualícelo.**

   Se proporciona un archivo de certificado de inicio verificado preinstalado, `/etc/certs/ORCLS11SE`, como parte de Oracle ILOM.

```
# more /etc/certs/ORCLS11SE
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----
```

4. **Inicie la carga del certificado.**

```
-> set /HOST/verified_boot/user_certs/1 load_uri=console
```

5. **Copie el contenido del archivo `/etc/certs/ORCLS11SE` y péguelo en la consola de Oracle ILOM.**

   Introduzca Ctrl-z para guardar y procesar la información.

   Introduzca Ctrl-c para salir y desechar los cambios.

```
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----^Z
Load successful.
```

6. **Verifique el certificado.**

```
-> show /HOST/verified_boot/user_certs/1/
/HOST/verified_boot/user_certs/1
Targets:
Properties:
clear_action = (Cannot show property)
issuer = /C=US/O=Oracle Corporation/OU=VeriSign Trust Network/OU=Class 2 Managed PKI
 Individual
Subscriber CA/CN=Object Signing CA
```

```
load_uri = (Cannot show property)
subject = /O=Oracle Corporation/OU=Corporate Object Signing/OU=Solaris Signed Execution/
CN=Solaris 11
valid_from = Mar 1 00:00:00 2012 GMT
valid_until = Mar 1 23:59:59 2015 GMT
Commands:
cd
load
reset
show
->
```

7. **Verifique que el parámetro `use-nvram` de OBP esté configurado en `false`.**

   Cuando usa el inicio verificado, el parámetro `use-nvram` de OBP debe estar configurado en `false`. Esto evita que se modifique OBP para desactivar la funcionalidad de inicio verificado. El valor por defecto es false. Inicie sesión en Oracle Solaris y escriba:

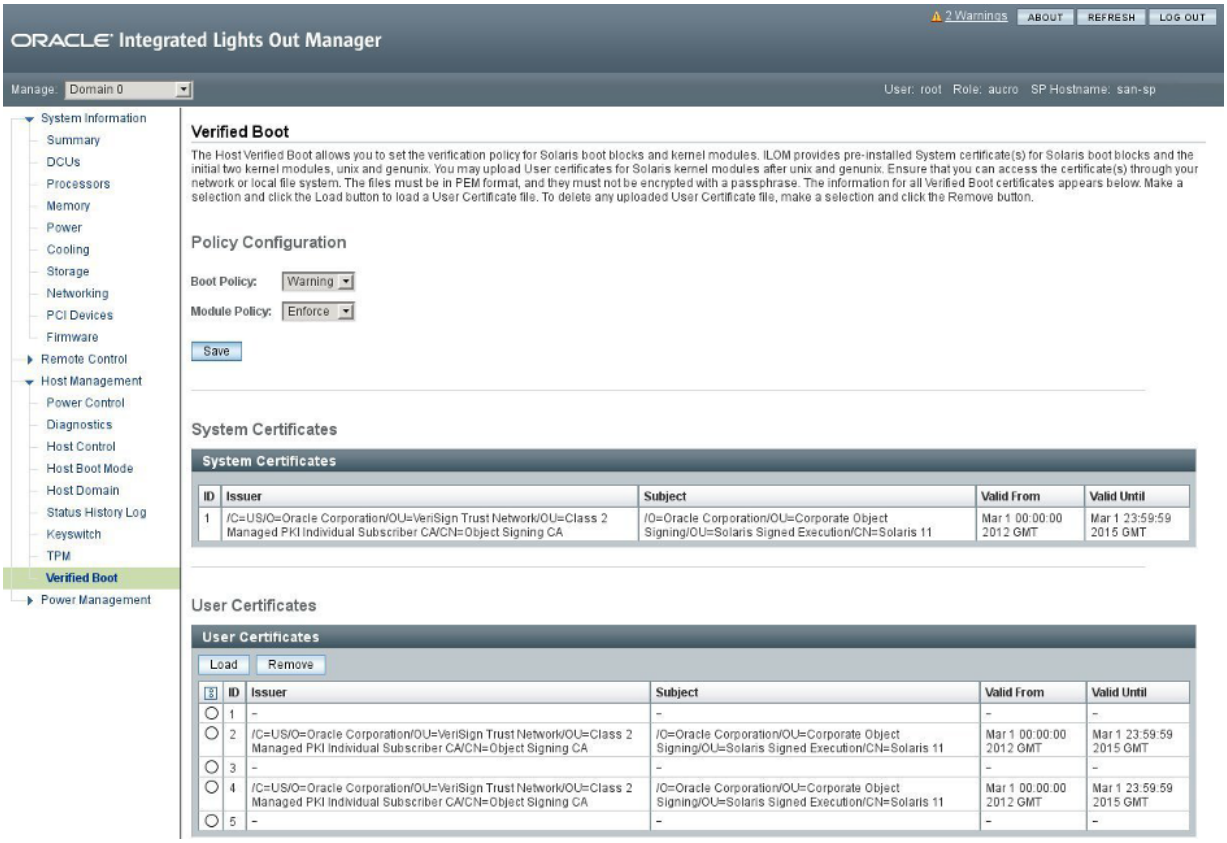
```
$ /usr/sbin/eeprom/eeprom use-nvramrc?

use-nvramrc?=false
```

Inicio verificado seguro (interfaz web de Oracle ILOM)

La interfaz web de Oracle ILOM también admite la configuración de variables de política de inicio verificado y la gestión de archivos de certificado, y proporciona la misma funcionalidad que la CLI. Navegue hasta el enlace Inicio verificado del menú de navegación Gestión de hosts.

Por ejemplo:



Recursos de servidor de cálculo adicionales

Para el sistema operativo Oracle Solaris y las guías de seguridad de Oracle Solaris Cluster, consulte la biblioteca de documentación que corresponde a su versión del sistema operativo. Las bibliotecas están disponibles en `http:/docs.oracle.com/en/operating-systems`.

Para obtener información de seguridad sobre Oracle VM Server for SPARC, consulte la guía de seguridad en `http://docs.oracle.com/cd/E62357_01`.

Para obtener más información de seguridad sobre el hardware del servidor de cálculo, consulte la guía de seguridad de `http://docs.oracle.com/cd/E55211_01`.

Protección de ZFS Storage Appliance

ZFS Storage Appliance es uno de los componentes de SuperCluster que admiten la consolidación de almacenamiento en una variedad de cargas de trabajo demandantes, que incluye inteligencia empresarial, almacenamiento de datos, virtualización, desarrollo y prueba y protección de datos.

ZFS Storage Appliance incluye dos controladores de almacenamiento ZFS redundantes. Debe proteger ambos controladores.

En estas secciones, se describen las directrices y las funciones de seguridad de ZFS Storage Appliance:

▼ Inicio de sesión en ZFS Storage Appliance

Para llevar a cabo las tareas de seguridad de esta sección, inicie sesión en ZFS Storage Appliance mediante la red de gestión.

En esta tarea, se describe cómo iniciar sesión mediante la CLI. Para obtener instrucciones equivalentes para iniciar sesión en la interfaz web de Oracle ILOM, consulte la *Guía de administración de Oracle ZFS*. Consulte “Recursos adicionales de ZFS Storage Appliance” [93].

1. **En la red de gestión, use SSH para conectarse a ZFS Storage Appliance.**
   Si no tiene configurados otros usuarios para administrar el dispositivo, deberá iniciar sesión como `root`.

```
% ssh root@ZFS_Storage_App_IPaddress_or_hostname
Password:
Last login: Mon Oct 13 15:43:05 2015
hostname:>
```

2. **Si es necesario, acceda a la ayuda de la CLI.**

   El comando `help` proporciona ayuda específica según el contexto. Para obtener ayuda sobre un tema en particular, especifique el tema como argumento de `help`. Para ver los temas disponibles, finalice con tabulación el comando help o escriba `help topics`.

Determinación de la versión de software de ZFS Storage Appliance

Use este procedimiento para determinar la versión de software en ZFS Storage Appliance.

1. **Inicie sesión en ZFS Storage Appliance.**

   Consulte Inicio de sesión en ZFS Storage Appliance [83].

2. **Visualice la versión de software.**

```
hostname:> configuration version show
[...]
Appliance Product: Sun ZFS Storage 7320
Appliance Type: Sun ZFS Storage 7320
Appliance Version: 2013.06.05.2.10,1-2.1.1.1
[...]
```

En este ejemplo, la versión del software ZFS Storage Appliance es `2013.06.05.2.10`.

Para actualizar la versión del software ZFS Storage Appliance, instale el parche de descarga de pila completa trimestral de SuperCluster disponible en My Oracle Support, en `https://support.oracle.com`.

Nota - Para SuperCluster, es posible que existan restricciones adicionales que limiten las versiones del software ZFS Storage Appliance que se pueden usar y la manera en la que se actualizan las versiones. En estas situaciones, comuníquese con su representante de Oracle.

Cambie la contraseña `root` de ZFS Storage Appliance

ZFS Storage Appliance no está configurado con una contraseña `root` por defecto. La configuración inicial de ZFS Storage Appliance se lleva a cabo mediante una sesión de consola

desde la instancia de Oracle ILOM incrustada. La contraseña de usuario `root` del dispositivo se configura durante la sesión de configuración inicial.

Cuando accede por primera vez a la consola del dispositivo, aparece una pantalla de configuración de interfaz de shell. Compruebe la información que se muestra en la pantalla e introduzca los valores requeridos. La contraseña de usuario `root` de ZFS Storage Appliance se configura durante este proceso.

Nota - La instancia de Oracle ILOM para el dispositivo no tiene una cuenta y una contraseña de usuario `root` por defecto de `welcome1`. Consulte Protección de Oracle ILOM [37].

Una vez que tenga una cuenta de usuario `root`, podrá cambiar la contraseña en cualquier momento, como se describe en esta tarea.

Nota - Si se cambia una contraseña para un componente de SuperCluster que gestiona Oracle Engineered Systems Hardware Manager (como el sistema operativo del controlador de almacenamiento AFS), también deberá actualizar la contraseña en Oracle Engineered Systems Hardware Manager. Para obtener más información, consulte la *Guía de administración de Oracle SuperCluster serie M7*.

---

1. **Inicie sesión en ZFS Storage Appliance.**

   Consulte Inicio de sesión en ZFS Storage Appliance [83].

2. **Cambie la contraseña de usuario `root`.**

   En este ejemplo, sustituya *password* por una contraseña que cumpla con las políticas de complejidad de contraseñas del Departamento de Defensa de los EE. UU.

```
hostname:> configuration users select root set initial_password=password initial_password = ************
hostname:configuration users> done
```

Para obtener más información sobre la instalación inicial y la configuración de ZFS Storage Appliance, consulte la *Guía de instalación del Oracle ZFS Storage Appliance*. Consulte “Recursos adicionales de ZFS Storage Appliance” [93].

Servicios de red expuestos por defecto (ZFS Storage Appliance)

En esta tabla, se muestran los servicios de red por defecto expuestos por ZFS Storage Appliance.

Servicio	Protocolo	Puerto	Descripción
SSH	TCP	22	Usado por el servicio de shell seguro para permitir el acceso administrativo a ZFS Storage Appliance mediante una interfaz de línea de comandos.
PORTMAP	TCP/UDP	111	Usado por el daemon de asignación de puertos de llamada a procedimiento remoto (RPC) (conocido como `rpcbind` o `portmap`). Este servicio se requiere para compatibilidad con NFS versión 3.
NTP	UDP	123	Usado por el servicio de protocolo de hora de red (NTP) (solo cliente)para sincronizar el reloj del sistema local con uno o más orígenes de hora externa.
HTTPS (BUI)	TCP	215	Usado por el servicio HTTPS integrado para permitir el acceso administrativo a ZFS Storage Appliance por un canal (SSL/TLS) cifrado mediante una interfaz de explorador.
Replicación remota	TCP	216	Usado por el servicio de replicación de datos remotos. La replicación de datos remotos duplica y sincroniza proyectos y los comparte entre los dispositivos ZFS Storage Appliance mediante un canal (SSL/TLS) cifrado.
NFS	TCP/UDP	2049 4045 varios	Usado por el servicio del sistema de archivos de red (NFS). NFS proporciona el servicio de uso compartido de archivos de red. El número real de puertos depende de cuál versión del protocolo NFS se use. La versión 3 de NFS confía en el daemon de asignación de puertos RPC (que se muestra arriba) y en los puertos asignados de forma dinámica para proporcionar montaje, estado, cuota y servicios relacionados. Sin embargo, la versión 4 de NFS confía en TCP/2049. El servicio de bloqueo NFS usa TCP/4045.
iSCSI / iSNS	TCP	3260	Usado por el servicio iSCSI que proporciona un protocolo de red de almacenamiento basado en IP para enlace de utilidades de almacenamiento de datos. ZFS Storage Appliance se puede configurar para compartir dispositivos iSCSI (denominados LUN) con clientes en red.
Etiquetas de servicio	TCP	6481	Usado por el servicio Oracle ServiceTag. Protocolo de detección de Oracle utilizado para identificar servidores y facilitar solicitudes de servicio. Este servicio es usado por productos como Oracle Enterprise Manager Ops Center para detectar software de ZFS Storage Appliance y para integrarlo con otras soluciones de servicio automático de Oracle.
NDMP	TCP	10000	Usado por el servicio de protocolo de gestión de datos de red (NDMP) que permite que ZFS Storage Appliance participe en copias de seguridad coordinadas de manera remota.

ZFS Storage Appliance también admite una variedad de otros servicios que están desactivados por defecto, incluidos `HTTP`, `FTP`, `SFTP`, `TFTP`, `WebDAV`, etc. Es posible que se expongan puertos de red adicionales si los servicios están activados después de la instalación.

Endurecimiento de la configuración de seguridad de ZFS Storage Appliance

En estos temas, se describe cómo fortalecer la seguridad de ZFS Storage Appliance:

- Implementación de endurecimiento de la configuración de seguridad de Oracle ILOM [87]

Implementación de endurecimiento de la configuración de seguridad de Oracle ILOM

ZFS Storage Appliance incluye una instancia de Oracle ILOM incrustada como parte del producto. Al igual que con otras implementaciones de Oracle ILOM, hay cambios de configuración de seguridad relevantes que se pueden implementar para mejorar la configuración de seguridad por defecto del dispositivo.

- **Para proteger la interfaz de Oracle ILOM de ZFS Storage Appliance, realice los procedimientos de Protección de Oracle ILOM [37].**

Desactivación de servicios innecesarios (ZFS Storage Appliance)

Desactive los servicios que no se requieren para los requisitos operativos y de gestión de la plataforma.

Por defecto, ZFS Storage Appliance emplea una configuración de red *segura por defecto*, donde los servicios no esenciales ya están desactivados. Sin embargo, según las políticas y los requisitos de seguridad, es posible que sea necesario activar o desactivar servicios adicionales.

1. **Inicie sesión en ZFS Storage Appliance.**

   Consulte Inicio de sesión en ZFS Storage Appliance [83].

2. **Visualice la lista de servicios admitidos por ZFS Storage Appliance.**

```
hostname:> configuration services
```

3. **Determine si un servicio determinado está activado.**

   Sustituya *servicename* por el nombre del servicio identificado en Paso 2.

   ```
   hostname:> configuration services servicename get <status>
   ```

   Un servicio está activado si el parámetro de estado del servicio devuelve el valor `enabled`. Por ejemplo:

   ```
   hostname:> configuration services iscsi get <status>
   <status> = online
   ```

4. **Desactive un servicio que ya no sea necesario.**

   Configure el estado del servicio esté desactivado. Por ejemplo:

   ```
   hostname:> configuration services iscsi disable
   ```

▼ Desactivación de enrutamiento dinámico

ZFS Storage Appliance se configura para ejecutar el protocolo de enrutamiento dinámico por defecto.

Antes de desactivar el servicio de enrutamiento dinámico, asegúrese de que ZFS Storage Appliance esté conectado a una red con la que se deba comunicar o asegúrese de que se haya configurado para usar enrutamiento estático o una ruta por defecto. Este paso es necesario para garantizar que no haya pérdida de conectividad una vez que se haya desactivado el enrutamiento dinámico.

1. **Inicie sesión en ZFS Storage Appliance.**

   Consulte Inicio de sesión en ZFS Storage Appliance [83].

2. **Desactive el enrutamiento dinámico.**

   ```
   hostname:> configuration services dynrouting disable
   ```

3. **Para determinar si el enrutamiento dinámico está activado, escriba:**

   ```
   hostname:> configuration services dynrouting get <status>
   ```

Restricción del acceso remoto a root mediante el shell seguro

Por defecto, ZFS Storage Appliance está configurado para permitir acceso administrativo remoto a la cuenta root mediante el servicio de shell seguro (SSH).

Use este procedimiento para desactivar el acceso remoto a root mediante SSH.

Una vez que se haya llevado a cabo este cambio de configuración, la cuenta root ya no estará disponible para acceder al sistema mediante SSH. Sin embargo, la cuentaroot puede acceder al sistema mediante la interfaz administrativa de HTTPS.

1. **Inicie sesión en ZFS Storage Appliance.**

   Consulte Inicio de sesión en ZFS Storage Appliance [83].

2. **Desactive el acceso remoto a root.**

   ```
   hostname:> configuration services ssh set permit_root_login=false
   ```

3. **Compruebe que la cuenta root ya no se permita para acceder al sistema mediante SSH.**

   ```
   hostname:> configuration services ssh get permit_root_login
   ```

4. **Si se requiere el acceso administrativo a SSH, cree al menos una cuenta que no sea root.**

   Para obtener instrucciones, consulte la *Guía de administración de Oracle ZFS Storage Appliance* que corresponde a la versión que se ejecuta en ZFS Storage Appliance. Consulte "Recursos adicionales de ZFS Storage Appliance" [93].

Configuración del timeout de inactividad de la interfaz de administración (HTTPS)

ZFS Storage Appliance admite la capacidad de desconectar y cerrar las sesiones administrativas que han estado inactivas durante más de un número predefinido de minutos. Por defecto, la sesión de la interfaz de usuario de explorador (HTTPS) genera un timeout después de 15 minutos.

Nota - Ningún parámetro equivalente aplica un timeout de inactividad en la interfaz de línea de comandos SSH de ZFS Storage Appliance.

Use este procedimiento para configurar el parámetro de timeout de inactividad en un valor personalizado.

1. **Inicie sesión en ZFS Storage Appliance.**

   Consulte Inicio de sesión en ZFS Storage Appliance [83].

2. **Visualice el parámetro de timeout de inactividad actual que está asociado con la interfaz de explorador.**

```
hostname:> configuration preferences get session_timeout
session_timeout = 15
```

3. **Configure el parámetro de timeout.**

   El valor `session_timeout` se especifica en minutos (10 minutos en este ejemplo).

```
hostname:> configuration preferences set session_timeout=10
session_timeout = 10
```

4. **Para comprobar el parámetro de timeout, repita Paso 2.**

▼ Desactivación de protocolos SNMP no aprobados

Por defecto, SNMPv1 y SNMPv2c están activados en ZFS Storage Appliance. ZFS Storage Appliance admite SNMPv1/v2c en todas las versiones admitidas del producto. A partir de la versión 2013.1.2, ZFS Storage Appliance también admite SNMPv3.

Nota - La versión 3 del protocolo SNMP presentó compatibilidad con el modelo de seguridad basado en usuario (USM, User-based Security Model). Esta funcionalidad sustituye las cadenas de comunidad SNMP tradicionales por las cuentas de usuario reales que se pueden configurar con permisos específicos, autenticación, protocolos de privacidad y contraseñas. Por defecto, ZFS Storage Appliance no incluye un nombre de usuario o contraseña para la cuenta USM integrada (solo lectura). Para fines de seguridad, configure las credenciales y los protocolos de USM según los requisitos de despliegue, gestión y supervisión.

Asegúrese de que las versiones no usadas o anteriores del protocolo SNMP estén desactivadas, a menos que se requiera lo contrario.

1. **Inicie sesión en ZFS Storage Appliance.**

   Consulte Inicio de sesión en ZFS Storage Appliance [83].

2. **Determine cuál sesión del protocolo SNMP usa el dispositivo.**

```
hostname:> configuration services snmp get version
version = v2
```

3. **Active el uso de SNMPv3 (si está disponible).**

   El uso de SNMPv1/v2c y SNMPv3 es mutuamente excluyente, de modo que cuando active SNMPv3, SNMPv1/v2c estarán desactivados.

```
hostname:> configuration services snmp set version=v3
version = v3
```

4. **Compruebe la versión de SNMP.**

```
hostname:> configuration services snmp get version
version = v3
```

▼ Configuración de cadenas de comunidad SNMP

Solamente realice esta tarea si ZFS Storage Appliance está configurado para usar SNMPv1 o v2.

Dado que SNMP a menudo se usa para supervisar el estado del dispositivo, es importante que la cadena comunitaria SNMP por defecto usada por el dispositivo se cambie por un valor definido por el cliente.

1. **Inicie sesión en ZFS Storage Appliance.**

   Consulte Inicio de sesión en ZFS Storage Appliance [83].

2. **Cambie la cadena comunitaria SNMP.**

   En este ejemplo, sustituya *string* por un valor que cumpla con los requisitos del Departamento de Defensa de los EE. UU. en relación con la composición de las cadenas de comunidad SNMP.

```
hostname:> configuration services snmp set community=string
community = value
```

3. **Compruebe la cadena comunitaria SNMP.**

```
hostname:> configuration services snmp get community
```

Configuración de redes autorizadas por SNMP

Solamente realice esta tarea si ZFS Storage Appliance está configurado para usar SNMPv1 o v2.

Para minimizar la divulgación de la información de configuración del sistema, las consultas de SNMP solamente se deben aceptar desde orígenes de red o host aprobados.

1. **Inicie sesión en ZFS Storage Appliance.**
   Consulte Inicio de sesión en ZFS Storage Appliance [83].

2. **Configure el parámetro de red autorizado por SNMP.**

```
hostname:> configuration services snmp set network=127.0.0.1/8
network = 127.0.0.1/8
```

3. **Compruebe el valor del parámetro de red autorizado por SNMP.**
   En este ejemplo, la configuración del parámetro de red en `127.0.0.1/8` bloquea de manera eficaz todas las consultas de SNMP basadas en red. Este valor se debe ajustar según sea necesario para permitir hosts y redes aprobados.

   El valor `0.0.0.0/0` permite realizar consultas desde cualquier ubicación de red.

```
hostname:> configuration services snmp get network
network = 127.0.0.1/8
```

Restricción del acceso a la red de gestión

Además de estos procedimientos de endurecimiento de seguridad, las interfaces de gestión expuestas por ZFS Storage Appliance se deben implementar en una red de gestión dedicada y aislada. Este paso ayuda a proteger ZFS Storage Appliance contra tráfico de red administrativa no autorizado o no deseado. Debe restringir estrictamente el acceso de control a la red de gestión con acceso garantizado solamente a los administradores que requieren este nivel de acceso.

Además, ZFS Storage Appliance se puede configurar para activar o desactivar el acceso administrativo (gestión) en interfaces de red específicas. Este cambio se puede implementar mediante este procedimiento.

1. **Inicie sesión en ZFS Storage Appliance.**

   Consulte Inicio de sesión en ZFS Storage Appliance [83].

2. **Configure las interfaces de red de gestión.**

   En este ejemplo, sustituya el valor *interface* por el nombre de la interfaz de red real para la que se aplica esta configuración.

   ```
   hostname:> configuration net interfaces select interface set admin=false
   ```

Recursos adicionales de ZFS Storage Appliance

Para obtener directrices de seguridad adicionales para ZFS Storage Appliance, consulte la guía de seguridad que corresponde a la versión que se ejecuta en ZFS Storage Appliance. Consulte Determinación de la versión de software de ZFS Storage Appliance [84].

Estas guías proporcionan información adicional sobre las funciones de seguridad del producto, las capacidades y las opciones de configuración:

- *Guía de seguridad de la versión de Oracle ZFS Storage Appliance* (versión 2013.1.4.0)

  http://docs.oracle.com//cd/E56047_01
- *Guía de seguridad de la versión de Oracle ZFS Storage Appliance* (versión 2013.1.3.0)

  http://docs.oracle.com/cd/E56021_01
- *Guía de seguridad de la versión de Oracle ZFS Storage Appliance* (versión 2013.1.2.0)

  http://docs.oracle.com/cd/E51475_01

Protección de servidores Exadata Storage Server

Los servidores Exadata Storage Server (servidores de almacenamiento) son el bloque de generación de almacenamiento de SuperCluster. Todos los servidores de almacenamiento se entregan preinstalados e integrados como parte de SuperCluster M7 con todos los componentes de cálculo, almacenamiento y software necesarios.

Nota - Solamente se permite realizar cambios en la configuración mediante la aplicación de métodos, parches o actualizaciones aprobados. Este software de servidor de almacenamiento no se podrá alterar de ninguna otra manera.

SuperCluster M7 tiene un mínimo de tres servidores de almacenamiento. Se pueden instalar servidores de almacenamiento adicionales en el rack principal de SuperCluster y en los racks de expansión opcionales. Deberá proteger cada servidor de almacenamiento individual.

En estos temas, se describe cómo proteger los servidores de almacenamiento:

▼ Inicio de sesión en el sistema operativo del servidor de almacenamiento

- **En la red de gestión, inicie sesión en uno de los servidores de almacenamiento como `celladmin`.**

Para la contraseña por defecto, consulte “Usuarios y contraseñas por defecto” [96].

```
# ssh celladmin@Storage_Server_IP_address
```

Usuarios y contraseñas por defecto

Tabla que muestra las contraseñas y las cuentas por defecto de los servidores de almacenamiento.

Nombre de cuenta	Tipo	Contraseña por defecto	Descripción
`root`	Administrador	`welcome1`	Se usa para acceder al sistema operativo del servidor de almacenamiento para realizar acciones administrativas generales y para actualizar el software del servidor de almacenamiento.
`celladmin`	Administrador de celdas	`welcome`	Se usa para llevar a cabo la instalación y la configuración del servidor de almacenamiento. Además, todos los servicios de almacenamiento de la plataforma funcionan con esta cuenta.
`cellmonitor`	Supervisor	`welcome`	Se usa solamente para fines de supervisión. Esta cuenta aprovecha un shell restringido para asegurar que la configuración y los objetos que residen en el servidor de almacenamiento no se podrán modificar desde esta cuenta.

▼ Cambio de contraseñas del servidor de almacenamiento

Para obtener una lista de cuentas y contraseñas por defecto, consulte “Usuarios y contraseñas por defecto” [96].

Nota - Si se cambia una contraseña para un componente de SuperCluster que gestiona Oracle Engineered Systems Hardware Manager (como el sistema operativo del servidor Exadata Storage Server), también deberá actualizar la contraseña en Oracle Engineered Systems Hardware Manager. Para obtener más información, consulte la *Guía de administración de Oracle SuperCluster serie M7*.

1. **Inicie sesión en el servidor como `celladmin`.**

   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].

2. **Cambie una contraseña por defecto mediante uno de estos métodos.**

- **Cambie la contraseña por una cuenta en el servidor en la que haya iniciado sesión.**

  ```
  # passwd account_name
  ```

- **Cambie una contraseña de cuenta en todos los servidores de almacenamiento.**

  El comando `cell_group` es un simple archivo de texto que muestra los nombres de host de todos los servidores de almacenamiento (uno por línea).

  En este ejemplo, sustituya estos elementos de la línea de comandos:

  - *new_password*: sustitúyalo por la nueva contraseña que cumple con las políticas del sitio.
  - *account_name*: sustitúyalo por el nombre de la cuenta de Oracle Linux.

  ```
  # dcli -g cell_group -l root "echo new_password | passwd --stdin account_name"
  ```

Determinación de la versión del software Exadata Storage Server

1. **Inicie sesión en uno de los servidores de almacenamiento.**

   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].

2. **Escriba este comando.**

   En este ejemplo, la versión de software del servidor de almacenamiento es 12.1.2.1.1.150316.2.

   ```
   # imageinfo -ver
   12.1.2.1.1.150316.2
   ```

   Para actualizar la versión del software, instale el parche de descarga de pila completa trimestral de SuperCluster disponible en My Oracle Support, en `https://support.oracle.com`.

   Nota - Para SuperCluster, es posible que existan restricciones adicionales que limiten las versiones de software que se pueden usar y la manera en la que se actualizan las versiones. En estas situaciones, comuníquese con su representante de Oracle.

Servicios de red expuestos por defecto (servidores de almacenamiento)

Nombre de servicio	Protocolo	Puerto	Descripción
SSH	TCP	22	Usado por el servicio de shell seguro, que está integrado en el software del servidor de almacenamiento para proporcionar acceso administrativo al sistema mediante una CLI. Por defecto, el servidor de shell seguro está configurado para responder a solicitudes de conexión solamente en las redes de gestión (NET 0) e IB (BONDIB0).

Este servidor de almacenamiento también se comunica con los dominios de Oracle Database en SuperCluster mediante el protocolo de sockets de datagrama seguros (RDSv3) mediante interfaces de acceso de memoria directa remota (RDMA). Esta comunicación punto a punto no usa TCP/IP y está limitada a la partición de red IB interna en la que residen ambos dominios de Oracle Database en SuperCluster y los servidores de almacenamiento.

Endurecimiento de la configuración de seguridad del servidor de almacenamiento

Nota - El servidor de almacenamiento incluye una instancia de Oracle ILOM incrustada como parte del producto. Al igual que con otras implementaciones de Oracle ILOM, hay cambios de configuración de seguridad relevantes que se pueden implementar para mejorar la configuración de seguridad por defecto del dispositivo. Para obtener más información, consulte Protección de Oracle ILOM [37].

En estos temas, se describe cómo fortalecer la seguridad de los servidores de almacenamiento:

Restricciones de la configuración de seguridad

La utilidad `host_access_control` es el único método permitido y admitido para implementar cambios de configuración de seguridad en los servidores de almacenamiento. No tiene permiso para realizar cambios manuales en la configuración de estos dispositivos de acuerdo con el aviso de Oracle Support 1068804.1. Además, antes de usar esta herramienta, primero debe obtener la aprobación explícita del soporte de Oracle SuperCluster para cambiar la configuración de los servidores de almacenamiento. Para solicitar esta aprobación, abra una solicitud de servicio con el soporte de Oracle.

El comando `host_access_control`, disponible a partir de la versión del software Exadata 11.2.3.3.0, se usa para implementar un juego limitado de ajustes de configuración de acceso y seguridad:

- Restricción del acceso raíz remoto.
- Restricción del acceso de red a determinadas cuentas.
- Implementación de caducidad de contraseña y políticas de complejidad.
- Implementación de banners de advertencia de inicio de sesión.
- Definición de políticas de timeout de sesión y bloqueo de cuentas.

▼ Visualización de ajustes de configuración de seguridad disponibles con `host_access_control`

Para ver qué está disponible en la utilidad `host_access_control`, realice estos pasos.

1. **Inicio de sesión en el sistema operativo del servidor de almacenamiento.**
   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].

2. **(Opcional) Visualice la ayuda de `host_access_control` para obtener más información.**

```
# /opt/oracle.cellos/host_access_control --help
```

Configuración de una contraseña de cargador de inicio del sistema

Puede configurar los servidores de almacenamiento para requerir una contraseña de cargador de inicio del sistema cada vez que un administrador intente acceder al editor del cargador de inicio (GRUB) o la interfaz de comandos.

1. **Inicie sesión en el servidor como `celladmin`.**

   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].

2. **Configure una contraseña de cargador de inicio del sistema.**

```
# /opt/oracle.cellos/host_access_control grub-password
New GRUB password: password
Retype new GRUB password: password
[...]
```

3. **Compruebe la configuración.**

   Si el comando devuelve un valor similar al de este ejemplo, se instalará una contraseña de cargador de inicio.

```
# grep "^password" /etc/grub.conf
password --md5 $1$Hdner/$Q2VoiZeTJwmNQsFnH9oFy.
```

Desactivación del acceso a la consola del sistema Oracle ILOM

Cada uno de los servidores de almacenamiento incluye una instancia incrustada de Oracle ILOM para activar la supervisión y la gestión remotas. Oracle ILOM también se puede usar para proporcionar acceso remoto a la consola del sistema del servidor de almacenamiento.

Lleve a cabo este procedimiento si desea desactivar el acceso al servidor de almacenamiento mediante Oracle ILOM.

1. **Inicie sesión en el servidor como `celladmin`.**
   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].
2. **Desactive el acceso a la consola del sistema Oracle ILOM.**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --lock
```

3. **Compruebe la configuración.**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --status
```

Restricción del acceso a `root` mediante SSH

Por defecto, el usuario de `root` tiene permiso para acceder de manera remota a los servidores de almacenamiento.

1. **Inicie sesión en el servidor como `celladmin`.**
   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].
2. **Desactive el acceso a `root` mediante SSH.**

```
# /opt/oracle.cellos/host_access_control rootssh --lock
```

3. **Compruebe la configuración.**

```
# /opt/oracle.cellos/host_access_control rootssh --status
```

Configuración de bloqueo de cuenta del sistema

Por defecto, los servidores de almacenamiento se configuran para bloquear las cuentas del sistema después de cinco intentos de autenticación fallida consecutivos.

Para cambiar este umbral, realice este procedimiento.

1. **Inicie sesión en el servidor como `celladmin`.**
   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].
2. **Cambie el umbral.**

Para cumplir con los requisitos de seguridad del Departamento de Defensa de los EE. UU., especifique el valor `3`. Si es necesario, sustituya ese valor por uno que cumpla con la política local del sitio.

```
# /opt/oracle.cellos/host_access_control pam-auth --deny 3
```

3. **Compruebe la configuración.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep deny=
```

▼ Configuración de reglas de complejidad de contraseña

Por defecto, los servidores de almacenamiento no implementan restricciones importantes que rigen la complejidad de las contraseñas de la cuenta del sistema.

1. **Inicie sesión en el servidor como `celladmin`.**

   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].

2. **Defina una política de complejidad de contraseña.**

   Sintaxis:

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc N0,N1,N2,N3,N4
```

   Sustituya *N0,N1,N2,N3,N4* por un juego de cinco valores separados por comas. Estos cinco valores definen en conjunto la política de complejidad de contraseña del sistema real. Estos son los valores (también se muestran en la página del comando man `passwdqc.conf(5)`):

   - *N0*: se usa para contraseñas compuestas por solamente una clase de carácter (dígitos, caracteres en minúsculas, caracteres en mayúsculas y caracteres especiales). En general, este parámetro se configura en `disabled` ya que las contraseñas simples no son seguras.
   - *N1*: se usa para contraseñas que consisten de dos clases de caracteres que no cumplen con los requisitos de una frase de contraseña. Para que se aplique esta regla, la contraseña debe tener al menos N1 caracteres de longitud.
   - *N2*: se usa para contraseñas que consisten de una frase de contraseña. Para que se aplique esta regla, la contraseña debe tener al menos N2 caracteres de longitud y debe cumplir con los requisitos de frase de contraseña.
   - *N3*: se usa para contraseñas que consisten de al menos tres clases de caracteres. Para que se aplique esta regla, la contraseña debe tener al menos N3 caracteres de longitud.

- *N4*: se usa para contraseñas que consisten de al menos cuatro clases de caracteres. Para que se aplique esta regla, la contraseña debe tener al menos *N4* caracteres de longitud.

Para cumplir con los requisitos de seguridad del Departamento de Defensa de los EE. UU., configure los parámetros *N0*,*N1*,*N2*,*N3*,*N4* en `disabled,disabled,disabled,disabled,15`. Esto garantiza que solamente las contraseñas que se aceptan consisten de al menos cuatro clases de caracteres (mayúsculas, minúsculas, numéricos, especiales) y de al menos 15 caracteres de longitud.

Nota - Las letras en mayúsculas al comienzo de la contraseña y los dígitos al final de la contraseña no se cuentan cuando se calcula el número de clases de caracteres.

Por ejemplo, para configurar la complejidad de la contraseña que cumple con los requisitos del Departamento de Defensa de los EE. UU., escriba:

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc disabled,disabled,disabled,disabled,15
```

3. **Compruebe el estado actual de esta configuración.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep min=
```

▼ Configuración de una política de historial de contraseñas

Por defecto, los servidores de almacenamiento definen una política de historial de contraseñas que evita que los usuarios reutilicen las últimas (10) contraseñas.

1. **Inicie sesión en el servidor como `celladmin`.**

   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].

2. **Visualice la configuración actual.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep remember=
```

3. **Cambie el historial de contraseñas.**

   Para cumplir con los requisitos de seguridad del Departamento de Defensa de los EE. UU. y con los requisitos de PCI-DSS, configure la política del historial de contraseñas en `5`. Esto garantiza que una cuenta no podrá reutilizar ninguna de las cinco contraseñas anteriores asignadas a la

cuenta. Si es necesario, sustituya ese valor por uno que cumpla con las políticas locales del sitio.

```
# /opt/oracle.cellos/host_access_control pam-auth --remember 5
```

4. **Para comprobar esta configuración, repita Paso 2.**

Configuración de retraso de bloqueo de autenticación fallida

Por defecto, los servidores de almacenamiento implementan una política donde una cuenta del sistema se bloquea durante 10 minutos después de un único intento de autenticación fallida.

Para cambiar este umbral, realice este procedimiento.

1. **Inicie sesión en el servidor como `celladmin`.**
   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].

2. **Visualice la configuración actual.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep lock_time=
```

3. **Cambie el umbral.**
   Para cumplir con los requisitos de seguridad del Departamento de Defensa de los EE. UU., configure el valor en 4 (segundos). Si es necesario, sustituya ese valor por uno que cumpla con las políticas locales del sitio.

```
# /opt/oracle.cellos/host_access_control pam-auth --lock 4
```

4. **Para comprobar esta configuración, repita Paso 2.**

Configuración de las políticas de control de antigüedad de contraseñas

Los servidores de almacenamiento admiten una variedad de controles de antigüedad de contraseñas, incluidos parámetros para controlar el número máximo de días que se usará una contraseña, el número mínimo de días entre cambios de contraseñas y el número de días por adelantado que se advierte al usuario sobre la caducidad de la contraseña.

Para cumplir con los requisitos de seguridad del Departamento de Defensa de los EE. UU. y de PCI-DSS, use los valores del Departamento de Defensa de la siguiente tabla:

Política	Valor de Oracle por defecto	Valor del Departamento de Defensa
Duración máxima de contraseña	90 días	60 días
Duración mínima de contraseña	1 día	1 día
Longitud mínima de contraseña	8 caracteres	15 caracteres
Advertencia de caducidad de contraseña	7 días	7 días

Para cambiar cualquiera de estos parámetros, lleve a cabo el siguiente procedimiento.

1. **Inicie sesión en el servidor como `celladmin`.**

   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].

2. **Visualice la configuración actual.**

   ```
   # /opt/oracle.cellos/host_access_control password-policy --status
   ```

3. **Configure estas políticas según las políticas de contraseña del sitio.**

   - **Para cambiar el parámetro de duración máxima de contraseña, escriba:**

     ```
     # /opt/oracle.cellos/host_access_control password-policy --PASS_MAX_DAYS 60
     ```

   - **Para cambiar el parámetro de duración mínima de contraseña, escriba:**

     ```
     # /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_DAYS 1
     ```

   - **Para cambiar el parámetro de longitud mínima de contraseña, escriba:**

     ```
     # /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_LEN 15
     ```

   - **Para cambiar el parámetro de advertencia de caducidad de contraseña, escriba:**

     ```
     # /opt/oracle.cellos/host_access_control password-policy --PASS_WARN_AGE 7
     ```

4. **Para comprobar esta configuración, repita Paso 2.**

Configuración del timeout de inactividad de la interfaz de administración (shell de inicio de sesión)

El servidor de almacenamiento admite la capacidad de finalizar sesiones administrativas que están inactivas durante más de un número predefinido de segundos.

Para definir el timeout de inactividad de la interfaz administrativa para un shell de inicio de sesión de cuenta del sistema, realice el siguiente procedimiento.

1. **Inicie sesión en el servidor como `celladmin`.**

   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].

2. **Visualice la configuración actual.**

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --status | grep Shell
   ```

3. **Defina el timeout de inactividad de la interfaz administrativa.**

   Para cumplir con los requisitos de seguridad del Departamento de Defensa de los EE. UU. y de PCI-DSS, especifique el valor `900` (segundos). Si es necesario, sustituya ese valor por uno que cumpla con la política local del sitio.

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --shell 900
   ```

4. **Para comprobar esta configuración, repita Paso 2.**

Configuración del timeout de inactividad de la interfaz de administración (shell seguro)

El servidor de almacenamiento admite la capacidad de finalizar sesiones administrativas de SSH que han estado inactivas durante más de un número predefinido de segundos.

Para definir el timeout de inactividad de interfaz administrativa de una sesión de SSH, realice el siguiente procedimiento.

1. **Inicie sesión en el servidor como `celladmin`.**

   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].

2. **Visualice la configuración actual.**

```
# /opt/oracle.cellos/host_access_control idle-timeout --status | grep SSH
```

3. **Defina el timeout de inactividad de la interfaz administrativa para una sesión de SSH.**

   Para cumplir con los requisitos de seguridad del Departamento de Defensa de los EE. UU., especifique el valor `900` (segundos). Si es necesario, sustituya ese valor por uno que cumpla con la política local del sitio.

```
# /opt/oracle.cellos/host_access_control idle-timeout --client 900
```

4. **Para comprobar esta configuración, repita Paso 2.**

Configuración de un banner de advertencia de inicio de sesión (servidor de almacenamiento)

El servidor de almacenamiento admite la capacidad de mostrar mensajes específicos del cliente antes de que un usuario se autentique correctamente en el sistema.

Para definir un banner de advertencia de inicio de sesión antes de la autenticación, siga este procedimiento.

1. **Inicie sesión en el servidor como `celladmin`.**

   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].

2. **Determine la configuración actual.**

```
# /opt/oracle.cellos/host_access_control banner --status
```

3. **Cree un archivo de texto que contenga el mensaje de banner de advertencia de inicio de sesión aprobado.**

4. **Defina un banner de advertencia de inicio de sesión previo a la autenticación.**

   Para cumplir con los requisitos de seguridad del Departamento de Defensa de los EE. UU., sustituya *filename* por la ruta y el nombre de un archivo que contiene el mensaje de banner de advertencia de inicio de sesión aprobado.

```
# /opt/oracle.cellos/host_access_control banner --file filename
```

5. **Para comprobar esta configuración, repita Paso 2.**

Limitación del acceso de red remoto

Puede limitar el acceso de red remoto entrante a los servidores de almacenamiento mediante la implementación de un juego de reglas de filtrado. También puede ajustar el acceso de red mediante la definición de un juego de reglas personalizado.

Use los siguientes procedimientos para limitar el acceso remoto.

- "Aislamiento de red de gestión de servidor de almacenamiento" [108]
- Limitación del acceso de red remoto [108]

Aislamiento de red de gestión de servidor de almacenamiento

El servidor de almacenamiento se implementa en una red de gestión dedicada y aislada. Esto ayuda a proteger el servidor de almacenamiento contra tráfico de red no autorizado o no deseado. El acceso a la red de gestión se debe controlar estrictamente con acceso garantizado solamente a los administradores que requieren este nivel de acceso.

▼ Limitación del acceso de red remoto

Hay varias maneras en las que puede limitar el acceso de red remoto en servidores de almacenamiento. Puede restringir el acceso de red entrante al servidor de almacenamiento mediante la implementación de un juego de reglas de filtrado desde arriba hacia abajo, que define el acceso por cuenta de usuario y origen. También puede definir un juego de reglas personalizado o denegar el acceso, según los requisitos del Departamento de Defensa de los EE. UU. y de PCI-DSS.

Atención - Tenga cuidado cuando implementa políticas que no son política por defecto para garantizar que no se interrumpa el acceso al sistema. Cuando agregue reglas individuales nuevas, los cambios se aplicarán de inmediato.

Para implementar un juego de reglas, realice este procedimiento.

1. **Inicie sesión en el servidor como `celladmin`.**

   Consulte Inicio de sesión en el sistema operativo del servidor de almacenamiento [95].

2. **Examine el juego de reglas activas.**

   ```
   # /opt/oracle.cellos/host_access_control access --status
   ```

3. **Exporte el juego de reglas actual a un archivo y guárdelo como copia de seguridad.**

   Este comando exporta el juego de reglas a un archivo de texto ASCII:

   ```
   # /opt/oracle.cellos/host_access_control access-export --file filename
   ```

4. **Configure el juego de reglas mediante uno o más de estos comandos, según el método que desea usar para crear el juego de reglas:**

   - **Para implementar un juego de reglas abierto que elimine las restricciones de la red entrante, escriba:**

     ```
     # /opt/oracle.cellos/host_access_control access --open
     ```

   - **Para implementar un juego de reglas cerrado que solamente permita acceso entrante mediante SSH, escriba:**

     ```
     # /opt/oracle.cellos/host_access_control access --close
     ```

   - **Para modificar un juego de reglas existentes, escriba:**

     Exporte el juego de reglas actuales a un archivo de texto ASCII:

     ```
     # /opt/oracle.cellos/host_access_control access-export --file filename
     ```

     Use un editor para editar el archivo de texto y configurar el juego de reglas.

     Importe el juego de reglas del archivo de texto y sustituya el juego de reglas existente:

     ```
     # /opt/oracle.cellos/host_access_control access-import --file filename
     ```

   - **Para agregar reglas específicas de forma individual:**

     Este método incluye el permiso y la denegación del acceso según estos parámetros:

- **Nombre de usuario**: los valores válidos incluyen la palabra clave `all` o uno o más nombres de usuario de cuenta local válidos.
- **Origen**: los valores válidos incluyen la palabra clave `all` o entradas individuales que describen el origen del acceso del sistema, incluidos la consola, la consola virtual, Oracle ILOM, la dirección IP, la dirección de red, el nombre de host o el dominio DNS.

En este ejemplo, el acceso al servidor de almacenamiento se otorga al usuario de `celladmin` cuando se inicia la conexión desde el host `trusted.example.org` o desde cualquier host dentro del dominio `.trusted.domain.com`.

```
# /opt/oracle.cellos/host_access_control access --add --user celladmin \
--origins trustedhost.example.org,.trusted.domain.com
```

Recursos de servidor de almacenamiento adicionales

Consulte la Guía de seguridad de Exadata Database Machine Security en http://docs.oracle.com/cd/E50790_01/welcome.html.

Protección de conmutadores IB y Ethernet

El conmutador Oracle Sun Data Center InfiniBand Switch 36 usado por SuperCluster proporciona la base de red para un alto rendimiento, alta escalabilidad y plano posterior completamente redundante en todos los componentes internos.

Los conmutadores IB se conectan a los servidores de cálculo, a las celdas de almacenamiento y a ZFS Storage Appliance. Los conmutadores IB incorporan Oracle ILOM incrustado para proporcionar capacidades de gestión y supervisión avanzadas. En especial, Oracle ILOM permite la supervisión y el control de los usuarios, el hardware, los servicios, los protocolos y otros parámetros de configuración.

SuperCluster M7 tiene un mínimo de dos conmutadores IB, con conmutadores IB adicionales instalados según sea necesario para configuraciones más grandes. Deberá proteger cada conmutador IB adicional.

En estos temas, se describe cómo proteger los conmutadores IB en SuperCluster M7:

▼ Inicio de sesión en un conmutador IB

En esta tarea, se describe cómo iniciar sesión en la interfaz de Oracle ILOM en el conmutador, donde se llevan a cabo la mayoría de las tareas administrativas.

- **En la gestión de red, inicie sesión en Oracle ILOM en el conmutador IB como `ilom-admin`.**

  Para las contraseñas por defecto, consulte "Cuentas y contraseñas por defecto (conmutador IB)" [113].

```
% ssh ilom-admin@IB_Switch_ILOM_IPaddress
->
```

Determinación de la versión de firmware del conmutador IB

Para aprovechar las funciones, las capacidades y las mejoras de seguridad más recientes, asegúrese de que el conmutador IB esté actualizado con la versión de firmware admitido más reciente.

1. **Inicie sesión en un conmutador IB como `ilom-admin`.**

   Consulte Inicio de sesión en un conmutador IB [111].

2. **Visualice la versión de firmware.**

   En este ejemplo, el firmware del conmutador es versión `2.1.5-1`.

```
-> version
SP firmware 2.1.5-1
SP firmware build number: 47111
SP firmware date: Sat Aug 24 16:59:14 IST 2013
SP filesystem version: 0.1.22
```

   Para actualizar la versión del firmware del conmutador IB instale el parche de descarga de pila completa trimestral de SuperCluster más reciente disponible en My Oracle Support, en `https://support.oracle.com`.

Nota - Para SuperCluster M7, es posible que haya restricciones adicionales que limiten el software de conmutador IB que se puede usar. Las restricciones también indican la manera en la que se actualiza el firmware. En estas situaciones, comuníquese con su representante de Oracle.

Cuentas y contraseñas por defecto (conmutador IB)

Nombre de cuenta	Tipo	Contraseña por defecto	Descripción
`root`	Administrador	`welcome1`	Se usa para acceder al sistema operativo del conmutador IB. Esta cuenta generalmente no se usa para `ilom-admin`, `ilom-operator` o cuentas definidas por el cliente.
`ilom-admin`	Administrador	`ilom-admin`	Se usa para llevar a cabo funciones administrativas en el Oracle ILOM incrustado, para realizar actualizaciones de software, para configurar usuarios y servicios, y para realizar funciones de diagnóstico de conmutador IB y gestión de tejido.
`ilom-operator`	Operador	`ilom-operator`	Se usa para las funciones de supervisión de Oracle ILOM y diagnóstico de tejido IB.
`nm2user`	Solo lectura	`changeme`	Esta cuenta tiene privilegios de solo lectura en la interfaz administrativa de la línea de comandos del conmutador IB. Esta cuenta a menudo es usada por Oracle Enterprise Manager para admitir la supervisión del hardware y el software del conmutador.

▼ Cambio de las contraseñas `root` y `nm2user`

El conmutador IB mantiene las cuentas del sistema en dos ubicaciones. El sistema operativo subyacente del conmutador configura y expone las cuentas `root` y `nm2user`. En esta capa no se admite la agregación, la eliminación ni el cambio de cuentas, pero debe cambiar las contraseñas por defecto.

Para otras cuentas y contraseñas, consulte Cambio de contraseñas de conmutador (IB Oracle ILOM) [114].

El conmutador IB no tiene la capacidad de definir ni aplicar complejidad, antigüedad, historia u otras reglas. Debe asegurarse de que las contraseñas asignadas cumplan con los requisitos de complejidad de contraseñas del Departamento de Defensa de los EE. UU. y que los procesos se implementen para garantizar que las contraseñas se actualizarán según la política del Departamento de Defensa de los EE. UU.

Para obtener más información sobre la gestión de cuentas IB, incluida la manera en la que se crean cuentas nuevas, asignan permisos a cuentas existentes o eliminan cuentas, consulte la *Guía de seguridad de hardware de Oracle Sun Data Center InfiniBand Switch 36* y el *Suplemento de Oracle Integrated Lights Out Manager para Oracle Sun Data Center InfiniBand Switch 36*. Consulte “Recursos de conmutador IB adicionales” [121].

Nota - Si se cambia una contraseña para un componente de SuperCluster que gestiona Oracle Engineered Systems Hardware Manager (como los conmutadores IB), también deberá actualizar la contraseña en Oracle Engineered Systems Hardware Manager. Para obtener más información, consulte la *Guía de administración de Oracle SuperCluster serie M7*.

1. **Inicie sesión en un conmutador IB como `root`.**

```
# ssh root@IB_Switch_IP_address
```

Para las contraseñas por defecto, consulte "Cuentas y contraseñas por defecto (conmutador IB)" [113].

2. **Cambie la contraseña de usuario `root`.**

```
$ passwd root
```

3. **Cambie la contraseña `nm2user`.**

```
$ passwd nm2user
```

▼ Cambio de contraseñas de conmutador (IB Oracle ILOM)

El conmutador IB mantiene las cuentas del sistema en dos ubicaciones. En esta sección, se describe cómo cambiar contraseñas en la interfaz de Oracle ILOM del conmutador IB. Para otras cuentas y contraseñas, consulte Cambio de las contraseñas `root` y `nm2user` [113].

Las cuentas de conmutador IB por defecto y las cuentas definidas por el cliente se gestionan mediante la instancia de Oracle ILOM incrustada en los conmutadores IB.

Para ver las cuentas y cambiar las contraseñas, realice este procedimiento.

1. **Inicie sesión en un conmutador IB como `ilom-admin`.**

Consulte Inicio de sesión en un conmutador IB [111].

Para las contraseñas por defecto, consulte "Cuentas y contraseñas por defecto (conmutador IB)" [113].

2. **Visualice las cuentas de Oracle ILOM configuradas en el conmutador IB.**

```
-> show /SP/users
```

3. **Cambie la contraseña para la cuenta `ilom-admin`.**

```
-> set /SP/users/ilom-admin password=password
```

Aislamiento de red del conmutador IB

La interfaz de gestión del conmutador IB se implementa en una red de gestión dedicada y aislada. Esto protege el conmutador IB contra tráfico de red no autorizado o no deseado.

El acceso a esta red de gestión se debe controlar estrictamente con acceso garantizado solamente a los administradores que requieren este nivel de acceso.

Servicios de red expuestos por defecto (conmutador IB)

Nombre de servicio	Protocolo	Puerto	Descripción
SSH	TCP	22	Usado por el servicio de shell seguro integrado para permitir el acceso administrativo al conmutador IB mediante una interfaz de línea de comandos.
HTTP (BUI)	TCP	80	Usado por el servicio HTTP integrado para permitir el acceso administrativo al conmutador IB mediante una interfaz de explorador. Si bien TCP/80 generalmente se usa para acceso de texto no cifrado, por defecto, el conmutador redirecciona automáticamente las solicitudes entrantes a la versión segura de este servicio que se ejecuta en TCP/443.
NTP	UDP	123	Usado por el servicio de protocolo de hora de red (NTP) (solo cliente) que se usa para sincronizar el reloj del sistema local con uno o más orígenes de hora externa.
SNMP	UDP	161	Usado por el servicio SNMP integrado para proporcionar una interfaz de gestión para supervisar el estado de los conmutadores IB y supervisar las notificaciones de captura recibidas.
HTTPS (BUI)	TCP	443	Usado por el servicio HTTPS integrado para permitir el acceso administrativo a los conmutadores IB por un canal (SSL/TLS) cifrado mediante una interfaz de explorador.
IPMI	TCP	623	Usado por el servicio de interfaz de gestión de plataforma inteligente integrada (IPMI) para proporcionar una interfaz de computadora para varias funciones de supervisión y gestión. No desactive este servicio, ya que lo usa Oracle Enterprise Manager Ops Center para recopilar datos de inventario de hardware, descripciones de unidades sustituibles en el campo, información de sensores de hardware e información de estado de componentes de hardware.
ServiceTag	TCP	6481	Usado por el servicio Oracle ServiceTag. Protocolo de detección de Oracle utilizado para identificar servidores y facilitar solicitudes de servicio. Este servicio es usado por productos como Oracle Enterprise Manager Ops Center para detectar

Nombre de servicio	Protocolo	Puerto	Descripción
			software de conmutadores IB y para integrarlo con otras soluciones de servicio automático de Oracle.

Endurecimiento de la configuración del conmutador IB

En estos temas, se describe cómo proteger el conmutador IB mediante varios ajustes de configuración.

▼ Desactivación de servicios innecesarios (conmutador IB)

Desactive los servicios que no se requieren para los requisitos operativos y de gestión de la plataforma. Por defecto, el conmutador IB emplea una configuración de red segura por defecto, donde los servicios no esenciales ya están desactivados. Sin embargo, según las políticas y los requisitos de seguridad del cliente, es posible que sea necesario desactivar servicios adicionales.

1. **Inicie sesión en un conmutador IB como `ilom-admin`.**
   Consulte Inicio de sesión en un conmutador IB [111].

2. **Determine la lista de servicios admitidos por el conmutador IB.**

   ```
   -> show /SP/services
   ```

3. **Determine si un servicio determinado está activado.**
   Sustituya *servicename* por el nombre del servicio identificado en Paso 2.

   ```
   -> show /SP/services/servicename servicestate
   ```

   Si bien la mayoría de los servicios reconocen y usan el parámetro `servicestate` para registrar si el servicio está activado o desactivado, hay unos pocos servicios, como `servicetag`, `ssh`, `sso` y

`wsman`, que usan el parámetro denominado `state`. Independientemente del parámetro real usado, un servicio está activado si el parámetro de estado devuelve el valor `enabled`, como se muestra en los siguientes ejemplos:

```
-> show /SP/services/https servicestate
/SP/services/https
Properties:
servicestate = enabled
```

```
-> show /SP/services/ssh state
/SP/services/ssh
Properties:
state = enabled
```

4. **Para desactivar un servicio que ya no se requiere, configure el estado del servicio en `disabled`.**

```
-> set /SP/services/http servicestate=disabled
```

5. **Determine si se deberá desactivar alguno de estos servicios.**

Según las herramientas y los métodos usados, los servicios de explorador HTTP y HTTPS se pueden desactivar si no se requieren o no se usan. Escriba:

```
-> set /SP/services/http servicestate=disabled
-> set /SP/services/http secureredirect=disabled
-> set /SP/services/https servicestate=disabled
```

- Interfaz administrativa de explorador (HTTP, HTTPS):
  - -> **set /SP/services/http servicestate=disabled**
  - -> **set /SP/services/http secureredirect=disabled**
  - -> **set /SP/services/https servicestate=disabled**

▼ Configuración de redireccionamiento de HTTP a HTTPS (conmutador IB)

Por defecto, el conmutador IB está configurado para redireccionar solicitudes de HTTP entrantes al servicio de HTTPS para garantizar que todas las comunicaciones basadas en explorador estén cifradas entre el conmutador y el administrador.

1. **Inicie sesión en un conmutador IB como `ilom-admin`.**

Consulte Inicio de sesión en un conmutador IB [111].

2. **Compruebe que el redireccionamiento seguro esté activado.**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **Si el valor por defecto se ha modificado, puede activar el redireccionamiento seguro.**

```
-> set /SP/services/http secureredirect=enabled
```

Desactivación de protocolos SNMP no aprobados (conmutador IB)

Por defecto, SNMPv1, SNMPv2c y SNMPv3 están activados para el servicio SNMP que se usa para supervisar y gestionar el conmutador IB. Asegúrese de que las versiones anteriores del protocolo SNMP permanezcan desactivadas a menos que se requiera lo contrario.

Nota - La versión 3 del protocolo SNMP presentó compatibilidad con el modelo de seguridad basado en usuario (USM, User-based Security Model). Esta funcionalidad sustituye las cadenas de comunidad SNMP tradicionales por las cuentas de usuario reales que se pueden configurar con permisos específicos, autenticación, protocolos de privacidad y contraseñas. Por defecto, el conmutador IB no incluye cuentas de USM. Configure cuentas de USM SNMPv3 según el tipo de requisitos de despliegue, gestión y supervisión.

---

1. **Inicie sesión en un conmutador IB como `ilom-admin`.**

   Consulte Inicio de sesión en un conmutador IB [111].

2. **Determine el estado de cada uno de los protocolos SNMP.**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = enabled
v2c = enabled
v3 = enabled
```

3. **Si es necesario, desactive SNMPv1 y SNMPv2c.**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

Configuración de cadenas de comunidad SNMP (conmutador IB)

Esta tarea solamente se aplica si SNMP v1 o SNMPv2c están activados y configurados para uso.

Dado que SNMP a menudo se usa para supervisar el estado del dispositivo, es importante que las cadenas de comunidad SNMP por defecto usadas por el dispositivo se sustituyan por valores definidos por el cliente.

1. **Inicie sesión en un conmutador IB como `ilom-admin`.**

   Consulte Inicio de sesión en un conmutador IB [111].

2. **Cree una nueva cadena comunitaria SNMP.**

   En este ejemplo, sustituya estos elementos de la línea de comandos:

   - *string*: sustituya por un valor definido por el cliente que cumpla con los requisitos del Departamento de Defensa de los EE. UU. en relación con la composición de las cadenas de comunidad SNMP.
   - *access*: sustituya por `ro` o `rw`, según si es una cadena de acceso de solo lectura o solo escritura.

   ```
   -> create /SP/services/snmp/communities/string permission=access
   ```

   Una vez que se hayan creado las cadenas de comunidad, se deberán eliminar las cadenas de comunidad por defecto.

3. **Elimine las cadenas de comunidad SNMP por defecto.**

   ```
   -> delete /SP/services/snmp/communities/public
   -> delete /SP/services/snmp/communities/private
   ```

4. **Compruebe las cadenas de comunidad SNMP.**

   ```
   -> show /SP/services/snmp/communities
   ```

Sustitución de los certificados autofirmados por defecto (conmutador IB)

Los conmutadores IB usan certificados autofirmados para activar el uso integrado del protocolo HTTPS. Como una de las mejores prácticas, sustituya certificados autofirmados por certificados aprobados para uso en su entorno y firmados por una autoridad de certificación reconocida.

El conmutador IB admite una variedad de métodos que se pueden usar para acceder al certificado SSL/TLS y la clave privada, incluidos HTTPS, HTTP, SCP, FTP, TFTP, y pegar la información directamente en una interfaz de explorador web. Para obtener más información, consulte el documento *Suplemento de Oracle Integrated Lights Out Manager para Oracle Sun Data Center InfiniBand Switch 36*. Consulte "Recursos de conmutador IB adicionales" [121].

1. **Inicie sesión en un conmutador IB como `ilom-admin`.**

   Consulte Inicio de sesión en un conmutador IB [111].

2. **Determine si el conmutador IB está usando un certificado autofirmado por defecto.**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

3. **Instale el certificado de la organización.**

```
-> load -source URI /SP/services/https/ssl/custom_cert
-> load -source URI /SP/services/https/ssl/custom_key
```

Configuración de timeout de sesión de la CLI administrativa (conmutador IB)

Los conmutadores IB admiten la capacidad de desconectar y cerrar las sesiones administrativas de la CLI que han estado inactivas durante más de un número predefinido de minutos.

Por defecto, el valor del timeout de la CLI es de 15 minutos.

1. **Inicie sesión en un conmutador IB como `ilom-admin`.**

   Consulte Inicio de sesión en un conmutador IB [111].

2. **Compruebe el parámetro de timeout de inactividad asociado con la CLI.**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **Configure el parámetro de timeout de inactividad.**

   Sustituya *n* por un valor especificado en minutos.

```
-> set /SP/cli timeout=n
```

Recursos de conmutador IB adicionales

Para obtener información sobre la administración de conmutadores IB y los procedimientos de seguridad, consulte la biblioteca de documentación de Sun Datacenter InfiniBand Switch 36 en http://docs.oracle.com/cd/E36265_01.

▼ Cambio de la contraseña de conmutador Ethernet

Nota - Si se cambia una contraseña para un componente de SuperCluster que gestiona Oracle Engineered Systems Hardware Manager (como el conmutador Ethernet), también deberá actualizar la contraseña en Oracle Engineered Systems Hardware Manager. Para obtener más información, consulte la *Guía de administración de Oracle SuperCluster serie M7*.

1. **Conecte un cable serie desde la consola de conmutador Ethernet a una PC portátil o un dispositivo similar.**

   La velocidad del puerto serie por defecto es de 9600 baudios, 8 bits, sin paridad, 1 bit de parada y ningún establecimiento de comunicación.

```
sscsw-adm0 con0 is now available
Press RETURN to get started.
```

2. **Coloque el conmutador en el modo activado.**

```
sscsw-adm0> enable
```

3. **Configure la contraseña.**

```
sscsw-adm0# configure terminal
Enter configuration commands,one per line.End with CNTL/Z.
sscsw-adm0(config)# enable password *******
sscsw-adm0(config)# enable secret *******
sscsw-adm0(config)# end
sscsw-adm0# write memory
*Apr 24 14:25:05.893:%SYS-5-CONFIG_I:Configured from console by
console
Building configuration...
Compressed configuration from 2502 bytes to 1085 bytes [OK ]
```

4. **Guarde la configuración.**

```
sscsw-adm0# copy running-config startup-config
```

5. **Salga de la sesión.**

```
sscsw-adm0# exit
```

6. **Desconecte la PC portátil del conmutador Ethernet.**

Auditoría de conformidad

Use la utilidad de conformidad de Oracle Solaris para acceder a la conformidad de un sistema e informarlo a una referencia conocida.

El comando `compliance` de Oracle Solaris asigna los requisitos de una referencia al código, el archivo o la salida del comando que comprueba la compatibilidad con un requisito específico. Oracle SuperCluster actualmente admite dos perfiles de referencia de conformidad de seguridad:

- **Recomendado**: perfil basado en la referencia del Centro de seguridad e Internet.
- **PCI-DSS**: perfil que comprueba los requisitos de conformidad del estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS, Card Industry Data Security Standard).

Estas herramientas de análisis de perfiles asignan controles de seguridad a los requisitos de conformidad y los informes de conformidad resultantes pueden reducir considerablemente el tiempo de auditoría. Además, la función de conformidad proporciona guías que contienen la lógica para cada comprobación de seguridad y los pasos para solucionar una comprobación fallida. Las guías pueden ser útiles para llevar a cabo capacitaciones y como directrices para pruebas futuras. Por defecto, en el momento de la instalación, se crean guías para cada perfil de seguridad. El administrador de SuperCluster Solaris puede agregar o cambiar una referencia y crear una guía nueva.

En estos temas, se describe cómo ejecutar informes de complimiento y se describe la conformidad con FIPS-140:

▼ Generación de una evaluación de conformidad

Para realizar esta tarea, debe tener asignado el perfil de derechos de instalación de software para agregar paquetes al sistema. Debe tener asignados derechos de administración para la mayoría de los comandos de conformidad.

1. **Instale el paquete de conformidad.**

```
# pkg install compliance
```

Este mensaje indica que el paquete está instalado:

```
No updates necessary for this image.
```

Para obtener más información, consulte la página del comando man `pkg(1)`.

Nota - Instale el paquete en cada zona en la que pretenda ejecutar pruebas de conformidad.

2. **Muestre las referencias, los perfiles y las evaluaciones anteriores.**

En este ejemplo, hay dos referencias.

- **`pci-dss`**: incluye un perfil denominado `Solaris_PCI-DSS`
- **`solaris`**: incluye dos perfiles denominados `Baseliine` y `Recommended`

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
solaris: Baseline, Recommended
Assessments:
No assessments available
```

3. **Genere una evaluación de conformidad.**

Ejecute el comando `compliance` con esta sintaxis:

`compliance assess -b` *benchmark* `-p` *profile*

`-b`	Especifica una referencia determinada. Si no se especifica, el valor que se usa por defecto es `solaris`.
`-p`	Especifica el perfil. El nombre de perfil distingue entre mayúsculas y minúsculas. Si no se especifica, se usa por defecto el valor del primer perfil.

Ejemplos:

- Uso del perfil `Recommended`.

```
# compliance assess -b solaris -p Recommended
```

El comando crea un directorio en `/var/share/compliance/assessments` que contiene la evaluación en tres archivos: un archivo log, un archivo XML y un archivo HTML.

- Uso del perfil PCI-DSS:

```
# compliance assess -b pci-dss
```

Nota - La referencia `pci-dss` solamente tiene un perfil, de modo que la opción de perfil (`-p`) no se requiere en la línea de comandos.

4. Compruebe que se hayan creado los archivos de conformidad.

```
# cd /var/share/compliance/assessments/filename_timestamp
# ls
recommended.html
recommended.txt
recommended.xml
```

Nota - Si ejecuta el mismo comando `compliance` nuevamente, los archivos no se sustituyen. Debe eliminar los archivos antes de reutilizar un directorio de evaluación.

5. (Opcional) Cree un informe personalizado.

Puede ejecutar informes personalizados de manera repetida. Sin embargo, puede ejecutar una evaluación solo una vez en el directorio original.

En este ejemplo, se usa la opción `-s` para seleccionar los tipos de resultados que deberán aparecer en el informe.

Por defecto, todos los tipos de resultados aparecen en el informe, excepto `notselected` o `notapplicable`. Los tipos de resultados se especifican como una lista separada por comas para mostrar además de los valores por defecto. Los tipos de resultados individuales se pueden suprimir si se los antecede con un signo `-`; si se inicia la lista con un signo `=`, se especifica exactamente cuáles tipos de resultados se deberán incluir. Los tipos de resultados son: `pass`, `fixed`, `notchecked`, `notapplicable`, `notselected`, `informational`, `unknown`, `error` o `fail`.

```
# compliance report -s -pass,fail,notselected
/var/share/compliance/assessments/filename_timestamp/report_A.html
```

Este comando crea un informe que contiene los elementos en formato HTML que hayan fallado o que no se hayan seleccionado. El informe se ejecuta en relación con la evaluación más reciente.

6. Vea el informe completo.

Puede ver el archivo log en un editor de texto, ver el archivo HTML en un explorador o ver el archivo XML en un visor de XML. Por ejemplo, para ver el informe personalizado en HTML del paso anterior, escriba la siguiente entrada en el explorador:

```
file:///var/share/compliance/assessments/filename_timestamp/report_A.html
```

7. Corrija los fallos que la política de seguridad requiera para pasar la prueba.

Si la corrección incluye reiniciar el sistema, reinicie el sistema antes de ejecutar la evaluación de nuevo.

8. **Repita la evaluación hasta que no haya fallos.**

▼ (Opcional) Ejecución de informes de conformidad con un trabajo `cron`

- **Como superusuario, use el comando `crontab -e` para agregar la entrada adecuada para el archivo `crontab`.**

  En esta lista, se proporcionan ejemplos de entradas de `crontab`:

  - Ejecuta evaluaciones de conformidad diarias a las 2:30 a. m.

    ```
    30 2 * * * /usr/bin/compliance assess -b solaris -p Baseline
    ```

  - Ejecuta evaluaciones de conformidad semanales los domingos a las 1:15 a. m.

    ```
    15 1 * * 0 /usr/bin/compliance assess -b solaris -p Recommended
    ```

  - Ejecuta evaluaciones mensuales el primer día del mes a las 4:00 a. m.

    ```
    0 4 1 * * /usr/bin/compliance assess -b pci-dss
    ```

  - Ejecuta evaluaciones el primer lunes del mes a las 3:45 a. m.

    ```
    45 3 1,2,3,4,5,6,7 * 1 /usr/bin/compliance assess
    ```

Conformidad con FIPS-140-2 nivel 1

Las aplicaciones criptográficas alojadas en SuperCluster confían en la función de estructura criptográfica de Oracle Solaris, que está validada para conformidad con FIPS 140-2 nivel 1. La estructura criptográfica de Oracle Solaris es el almacén criptográfico central de Oracle Solaris y proporciona dos módulos verificados por FIPS 140 que admiten los procesos de espacio de usuario y nivel de núcleo. Estos módulos de biblioteca proporcionan funciones de cifrado, descifrado, método de hashing, generación y verificación de firmas y certificados, y autenticación de mensajes para aplicaciones. Las aplicaciones de nivel de usuario que llaman a estos módulos se ejecutan en el modo FIPS 140.

Además de la estructura criptográfica de Oracle Solaris, el módulo de objeto OpenSSL incluido en Oracle Solaris está validado para conformidad con FIPS 140-2 nivel 1, que admite la criptografía para aplicaciones basadas en los protocolos TLS y de shell seguro. El proveedor de servicios de la nube puede elegir activar los hosts de inquilinos mediante modos que cumplen con FIPS 140. Si Oracle Solaris y OpenSSL se ejecutan en modos que cumplen con FIPS 140, que son proveedores de FIPS 140-2, aplique el uso de algoritmos criptográficos validados por FIPS 140.

Consulte también Activación de operación que cumple con FIPS-140 (Oracle ILOM) (Si se requiere) [39].

En esta tabla, se muestra los algoritmos aprobados por FIPS que son admitidos por Oracle Solaris en SuperCluster M7.

Clave o CSP	Número de certificado	
	v1.0	**v1.1**
Clave simétrica		
AES: modos ECB, CBC, CFB-128, CCM, GMAC, GCM y CTR para tamaños de butes de 128 bits, 192 bits y 256 bits	#2311	#2574
AES: modo XTS para tamaños de claves de 256 bits y 512 bits	#2311	#2574
TripleDES: modo CBC y ECB para opción de claves 1	#1458	#1560
Clave asimétrica		
Generación/verificación de firmas RSA PKCS #1.5: 1024 bits, 2048 bits (con SHA-1, SHA-256, SHA-384, SHA-512)	#1194	#1321
Generación/verificación de firmas ECDSA: P-192, -224, -256, -384, -521; K-163, -233, -283, -409, -571; B-163, -233, -283, -409, -571	#376	#446
Estándar de hashing seguro (SHS)		
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	#1425	#1596
Autenticación de mensajes basados en hash (con claves)		
HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	#1425	#1596
Generación de números aleatorios		
Generación de números aleatorios FIPS 186-2 swrand	#1154	#1222
Generación de números aleatorios FIPS 186-2 n2rng	#1152	#1226

Oracle Solaris ofrece dos proveedores de algoritmos criptográficos validados para el nivel 1 de FIPS 140-2.

- La función de estructura criptográfica de Oracle Solaris es el almacén criptográfico central de un sistema Oracle Solaris y proporciona dos módulos FIPS 140. El módulo de espacio de usuario proporciona criptografía para las aplicaciones que se ejecutan en el espacio de usuario, y el módulo de núcleo proporciona criptografía para los procesos en el nivel de núcleo. Estos módulos de biblioteca proporcionan funciones de cifrado, descifrado, método de hashing, generación y verificación de firmas y certificados, y autenticación de mensajes para aplicaciones. Las aplicaciones de nivel de usuario que llaman a estos módulos se ejecutan en el modo FIPS 140, por ejemplo, el comando `passwd` e IKEv2. Los consumidores en el nivel del núcleo, por ejemplo, Kerberos e IPsec, utilizan API patentadas para llamar a la estructura criptográfica del núcleo.

- El módulo del objeto OpenSSL proporciona criptografía para SSH y aplicaciones web. OpenSSL es el kit de herramientas de código abierto para los protocolos de capa de conexión segura (SSL) y seguridad de capa de transporte (TLS), y proporciona una biblioteca de criptografía. En Oracle Solaris, SSH y el servidor web Apache son consumidores del módulo FIPS 140 de OpenSSL. Oracle Solaris envía una versión FIPS 140 de OpenSSL con Oracle Solaris 11.2 que está disponible para todos los consumidores, pero la versión que se envía con Oracle Solaris 11.1 está disponible solamente para Solaris SSH. Debido a que los módulos del proveedor FIPS 140-2 hacen un uso intensivo de la CPU, no están activados por defecto. Como administrador, es responsable de la activación de los proveedores en el modo FIPS 140 y de la configuración de los consumidores.

Para obtener más información sobre cómo activar los proveedores FIPS-140 en Oracle Solaris, consulte el documento titulado *Uso de un sistema activado para FIPS 140 en Oracle Solaris 11.2*, disponible en la cabecera Protección del sistema operativo Oracle Solaris 11 en: `http://docs.oracle.com/cd/E36784_01`.

Cómo mantener la seguridad de los sistemas SuperCluster serie M7

En estos temas, se describen las funciones de SuperCluster serie M7 que puede usar para mantener la seguridad durante la vida del sistema:

Gestión de la seguridad de SuperCluster

SuperCluster M7 aprovecha las capacidades de gestión de seguridad de una variedad de productos, incluidos Oracle ILOM, Oracle Enterprise Manager Ops Center, Oracle Enterprise Manager e Identity Management Suite de Oracle. En estas secciones, se describen los detalles:

Oracle ILOM para gestión segura

Oracle ILOM es un proveedor de servicios incrustado en varios componentes de SuperCluster M7. Use Oracle ILOM para realizar estas actividades de gestión fuera de banda:

- Proporcionar acceso seguro para realizar la gestión segura de Lights Out fuera de los componentes de SuperCluster. El acceso incluye acceso basado en web protegido por SSL, acceso de línea de comandos mediante shell seguro, y los protocolos IPMI v2.0 y SNMPv3.
- Separar los requisitos de tareas mediante un modelo RBAC. Asignar usuarios individuales a roles específicos que limiten las funciones que pueden realizar.
- Proporcionar un registro de auditoría de todas las conexiones y los cambios de configuración. Cada entrada del log de auditoría muestra el usuario que realizó la acción y un registro de hora. Esta capacidad le permite detectar actividades o cambios no autorizados y atribuir esas acciones a usuarios específicos.

Para obtener más información, consulte la documentación de Oracle Integrated Lights Out Manager en: http://docs.oracle.com/en/hardware/?tab=4.

Oracle Identity Management Suite

Oracle Identity Management Suite gestiona el ciclo de vida completo de las identidades y las cuentas de una organización. Este conjunto incluye soporte de control de acceso basado en web mediante inicio de sesión único, control de acceso basado en web, seguridad de servicios web, administración de identidades, autenticación segura, y control de identidad y acceso.

Oracle Identity Management puede proporcionar un único punto para gestión de identidades y acceso no solamente a aplicaciones y servicios que se ejecutan en Oracle SuperCluster, sino también para la infraestructura y los servicios subyacentes que lo gestionan.

Para obtener más información, consulte la documentación de Oracle Identity Management disponible en:

http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

Oracle Key Manager

Oracle Key Manager es un sistema de gestión de claves (KMS) completo que simplifica la gestión y la supervisión de claves de cifrado que protegen la información almacenada.

Oracle Key Manager admite entornos empresariales con una arquitectura altamente escalable y disponible que puede gestionar cientos de dispositivos y millones de claves. Esta función opera en un entorno operativo fortalecido, aplica control de acceso eficaz y separación de roles para operaciones de gestión y supervisión de claves y, de manera opcional, admite el almacenamiento de claves en la tarjeta Sun Crypto Accelerator 6000 PCIe Card de Oracle, un módulo seguro de hardware con FIPS 140-2.

En el contexto de SuperCluster, Oracle Key Manager puede autorizar, proteger y gestionar el acceso a claves de cifrado usadas por las unidades de cinta de cifrado Oracle StorageTek, bases de datos de Oracle cifradas que usan cifrado de datos transparente y sistemas de archivos ZFS cifrados disponibles en el sistema operativo Oracle Solaris 11.

Para obtener más información, consulte la documentación de Oracle Key Manager disponible en:

http://docs.oracle.com/cd/E26076_02

Oracle Engineered Systems Hardware Manager

Oracle Engineered Systems Hardware Manager es una herramienta de gestión de hardware de nivel de rack basada en interfaz de usuario de explorador, destinada al uso del personal del servicio de asistencia de Oracle. Para obtener más información, consulte la *Guía del propietario de Oracle SuperCluster serie M7: administración*.

Oracle Engineered Systems Hardware Manager incluye dos conjuntos de información de autenticación:

- **Contraseñas de componentes de SuperCluster M7**

  Oracle Engineered Systems Hardware Manager mantiene el almacenamiento seguro de contraseñas para todas las cuentas de fábrica para todo el hardware de SuperCluster M7. El software usa estas contraseñas para gestionar los componentes de SuperCluster M7.

  Si alguna de estas contraseñas cambia, debe actualizar la aplicación Oracle Engineered Systems Hardware Manager con las contraseñas nuevas.
- **Autenticación Local**

  Oracle Engineered Systems Hardware Manager tiene dos cuentas de usuario locales. Una cuenta es usada por los clientes para personalizar Oracle Engineered Systems Hardware Manager para su entorno y para gestionar la cuenta de servicio. La otra cuenta es usada por el personal de Oracle Service para configurar y brindar servicio y soporte para el hardware SuperCluster M7.

Oracle Engineered Systems Hardware Manager proporciona los siguientes recursos de gestión local.

- **Política de contraseñas**: la capacidad de configurar las contraseñas de aplicación según las políticas empresariales garantizar que las contraseñas cumplirán con los estándares empresariales.

Nota - Consulte a la persona responsable de la seguridad de la empresa acerca de la política de contraseñas.

- **Certificados**: Oracle Engineered Systems Hardware Manager usa certificados para proteger la comunicación entre los servidores de cálculo y el servidor de Oracle Engineered Systems Hardware Manager y la BUI. Estos certificados se crean automáticamente durante la instalación y son exclusivos de cada instancia; sin embargo, se pueden sustituir por certificados y claves proporcionados por el cliente.
- **Puertos**: los puertos de red usados por Oracle Engineered Systems Hardware Manager se configuran en caso de que haya un conflicto con la política empresarial. Se usan los puertos 8001 hasta 8004 (inclusive).

Para obtener instrucciones sobre configuración, consulte la *Guía del propietario de Oracle SuperCluster serie M7: administración*.

Oracle Enterprise Manager

El conjunto Oracle Enterprise Manager es una solución de gestión de nubes completa a integrada que se concentra en la gestión del ciclo de vida de aplicaciones, middleware, bases de datos e infraestructura física y virtual (mediante Oracle Enterprise Manager Ops Center). Oracle Enterprise Manager proporciona las siguientes tecnologías de gestión:

- Admite supervisión detallada, notificación de eventos, aplicación de parches, gestión de cambios, configuración continua, gestión de conformidad y generación de informes para la aplicación, el middleware y la base de datos.
- Permite mantener los ajustes de configuración de manera central y acceder a las políticas de control y auditoría para grupos de bases de datos. El acceso a estas funciones se puede limitar a individuos autorizados, lo que garantiza que el acceso de gestión admitirá los mandatos de conformidad para separación de tareas, menor privilegio y responsabilidad.
- Admite la autenticación segura mediante una variedad de métodos, controles de acceso específicos y auditoría completa, lo que garantiza que la gestión del entorno de SuperCluster se podrá lograr de manera segura.

Para obtener más información, consulte la documentación de Oracle Enterprise Manager disponible en: http://www.oracle.com/technetwork/oem/grid-control/documentation/oem-091904.html

Oracle Enterprise Manager Ops Center (Opcional)

Oracle Enterprise Manager Ops Center es una tecnología opcional que puede usar para gestionar algunos aspectos de seguridad de Oracle SuperCluster.

Oracle Enterprise Manager Ops Center es parte del conjunto Oracle Enterprise Manager y es una solución de gestión de hardware convergente que proporciona una única interfaz administrativa para servidores, sistemas operativos, firmware, máquinas virtuales, zonas, almacenamiento y tejidos de red.

Puede usar Oracle Enterprise Manager Ops Center para asignar acceso administrativo a recopilaciones de sistemas físicos y virtuales, supervisar actividad de administrador, detectar fallas, y configurar y gestionar alertas. Oracle Enterprise Manager Ops Center admite una variedad de informes que permiten comparar sistemas con bases de configuración conocidas, niveles de parches y vulnerabilidades de seguridad.

Para obtener más información, consulte la documentación de Oracle Enterprise Manager Ops Center disponible en: `http://docs.oracle.com/cd/E27363_01/index.htm`.

Nota - Para versiones anteriores de Oracle Enterprise Manager Ops Center, se instaló el software Ops Center y se ejecuta desde el sistema SuperCluster. A partir de la versión 2 de Oracle Enterprise Manager Ops Center 12c (12.2.0.0.0), el software Ops Center se debe instalar y ejecutar en un sistema externo al sistema SuperCluster.

Supervisión de seguridad

Si para la generación de informes de conformidad o la respuesta de incidentes, la supervisión y la auditoría son funciones críticas que debe usar para obtener mayor visibilidad en el entorno de TI. El grado en el que se emplea la supervisión y la auditoría a menudo se basa en el riesgo o la importancia de la naturaleza del entorno.

Los sistemas SuperCluster serie M7 proporcionan funcionalidades de supervisión y auditoría completas en el servidor, la red, la base de datos y las capas de almacenamiento, lo que garantiza que la información podrá estar disponible según los requisitos de auditoría y conformidad.

En estas secciones, se describen la supervisión y la auditoría de la carga de trabajo y la base de datos:

- “Supervisión de carga de trabajo” [134]
- “Supervisión y auditoría de la actividad de base de datos” [134]

Supervisión de carga de trabajo

El sistema operativo Oracle Solaris tiene una utilidad de auditoría completa que puede supervisar acciones administrativas, invocaciones de línea de comandos e incluso llamadas del sistema de nivel de núcleo. Esta instalación tiene una gran capacidad de configuración y ofrece políticas de auditoría globales, por zona e incluso por usuario.

Cuando se configura el sistema para usar Oracle Solaris Zones, los registros de auditoría de cada zona se pueden almacenar en la zona global para protegerlos contra manipulación.

La auditoría de Oracle Solaris proporciona la capacidad de enviar registros de auditoría para puntos de recopilación remotos mediante la utilidad de log del sistema (`syslog`). Muchos servicios de detección y prevención de intrusión comercial pueden usar los registros de auditoría de Oracle Solaris como punto adicional para análisis y generación de informes.

Oracle VM Server for SPARC aprovecha la utilidad de auditoría de Oracle Solaris para registrar acciones y eventos asociados con eventos de virtualización y administración de dominios.

Para obtener más información, consulte la sección Supervisión y mantenimiento de la seguridad de Oracle Solaris en las directrices de seguridad de Oracle Solaris, disponibles en:

`http://docs.oracle.com/cd/E26502_01`

Supervisión y auditoría de la actividad de base de datos

La compatibilidad de Oracle Database con auditoría específica permite establecer políticas que determinan de manera selectiva cuándo se generan los registros. Esta capacidad le permite concentrarse en otras actividades de base de datos y reduce la carga a menudo asociada con las actividades de auditoría.

Oracle Audit Vault and Database Firewall centraliza la gestión de la configuración de auditoría de base de datos y automatiza la consolidación de los datos de auditoría en un repositorio seguro. Este software incluye la generación de informes integrada para supervisar una variedad de actividades, incluida la actividad de usuario privilegiado y los cambios en estructuras de base de datos. Los informes generados por Oracle Audit Vault and Database Firewall proporcionan visibilidad en varias actividades de base de datos administrativas y de aplicación, y proporcionan información detallada para admitir la responsabilidad de acciones.

Oracle Audit Vault and Database Firewall permite la detección proactiva y la generación de alertas de actividades que pueden indicar intentos de acceso no autorizado o abuso de privilegios del sistema. Estas alertas pueden incluir eventos y condiciones definidos por el usuario y por el sistema, como la creación de cuentas de usuarios privilegiados o la modificación de tablas que contienen información importante.

El monitor remoto de Oracle Audit Vault and Database Firewall puede proporcionar supervisión de seguridad de base de datos en tiempo real. Esta función consulta las conexiones de la base de datos para detectar tráfico malintencionado, como omisión de aplicaciones, actividad no autorizada, inyección de SQL u otras amenazas. Mediante el uso de un enfoque preciso basado en gramática, este software ayuda a identificar rápidamente actividad de base de datos sospechosa.

Para obtener más información, consulte la documentación de Oracle Audit Vault and Database Firewall en http://docs.oracle.com/cd/E37100_01/index.htm.

Supervisión de red

Una vez que las redes se configuraron según las directrices de seguridad, es necesario realizar una revisión y un mantenimiento periódicos.

Siga estas directrices para garantizar la seguridad del acceso local y remoto al sistema:

- Revise los logs para detectar posibles incidentes y archívelos de acuerdo con las políticas de seguridad de la organización.
- Realice revisiones periódicas de la red de acceso de cliente para garantizar que la configuración del host y de Oracle ILOM permanecerá intacta.

Para obtener más información, consulte las guías de seguridad del sistema operativo Oracle Solaris:

- Sistema operativo Oracle Solaris 11: http://www.oracle.com/goto/Solaris11/docs
- Sistema operativo Oracle Solaris 10: http://www.oracle.com/goto/Solaris10/docs

Actualización de firmware y software

Las actualizaciones del sistema SuperCluster serie M7 ser proporcionan en QFSDP. Mediante la instalación de QFSDP se actualizan todos los componentes al mismo tiempo. Esta práctica

garantiza que todos los componentes se sigan ejecutando en una combinación de versiones de software que han sido probadas íntegramente en conjunto por Oracle.

Obtenga el QFSDP más reciente de My Oracle Support en: `http://support.oracle.com`

Para obtener información acerca del software y el firmware admitidos, consulte las *Notas del producto de Oracle SuperCluster serie M7*. En la nota 1605591.1 de MOS, se proporcionan instrucciones para acceder a las Notas del producto.

Nota - Únicamente cambie la versión, actualice o aplique parches en componentes aislados para mantenimiento reactivo bajo la supervisión del soporte de Oracle.

Índice

R

S

U

V

Z