Guía de seguridad de Oracle MiniCluster S7-2

Referencia: E78271-02
Octubre de 2016

Referencia: E78271-02

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 MiniCluster S7-2.
- **Destinatarios:** técnicos, administradores de sistemas y proveedores de servicios 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 están disponibles en http://www.oracle.com/goto/minicluster-s7-2/docs.

Comentarios

Envíenos comentarios acerca de esta documentación mediante http://www.oracle.com/goto/docfeedback.

Descripción de los principios de seguridad

En esta guía, se proporciona información acerca de la planificación, la configuración y el mantenimiento de un entorno seguro para los sistemas Oracle MiniCluster S7-2.

En esta sección, se incluyen los siguientes temas:

Tareas de seguridad mínimas necesarias

Como sistema de ingeniería, MiniCluster viene configurado como un sistema altamente seguro de fábrica por defecto y proporciona las siguientes funciones de seguridad:

- Viene preconfigurado con controles de seguridad completamente automatizados para todas las máquinas virtuales (VM).
- El cifrado está activado por defecto, lo cual garantiza que los datos inactivos y en tránsito estén seguros.
- Las máquinas virtuales se configuran automáticamente con un sistema operativo endurecido y minimizado con firewalls basados en host.
- El control de acceso requiere un acceso basado en roles con la menor cantidad de privilegios.
- Todas las máquinas virtuales usan almacenamiento ZFS cifrado.
- Hay una utilidad de gestión de claves centralizada, que utiliza PKCS#11, y se admite FIPS.
- El sistema incluye una política de auditoría completa con logs de auditoría centralizados.
- El sistema y todas las máquinas virtuales se configuran para un perfil de seguridad PCI-DSS, equivalente a CIS o DISA-STIG. Nota: Este último perfil está actualmente en

etapa de revisión. Solo utilice el perfil DISA-STIG para uso experimental en entornos no productivos.

- Hay un panel de control de conformidad fácil de ver que admite referencias de conformidad fáciles de ejecutar.

Inmediatamente después de la instalación de MiniCluster, el administrador de seguridad debe realizar dos tareas:

- Cambiar la contraseña de usuario root de Oracle ILOM. Consulte Cambio de las contraseñas de usuario `root` por defecto de Oracle ILOM [27].

Además, debe revisar la información de seguridad de esta guía para comprender y verificar las funciones de seguridad de MiniCluster.

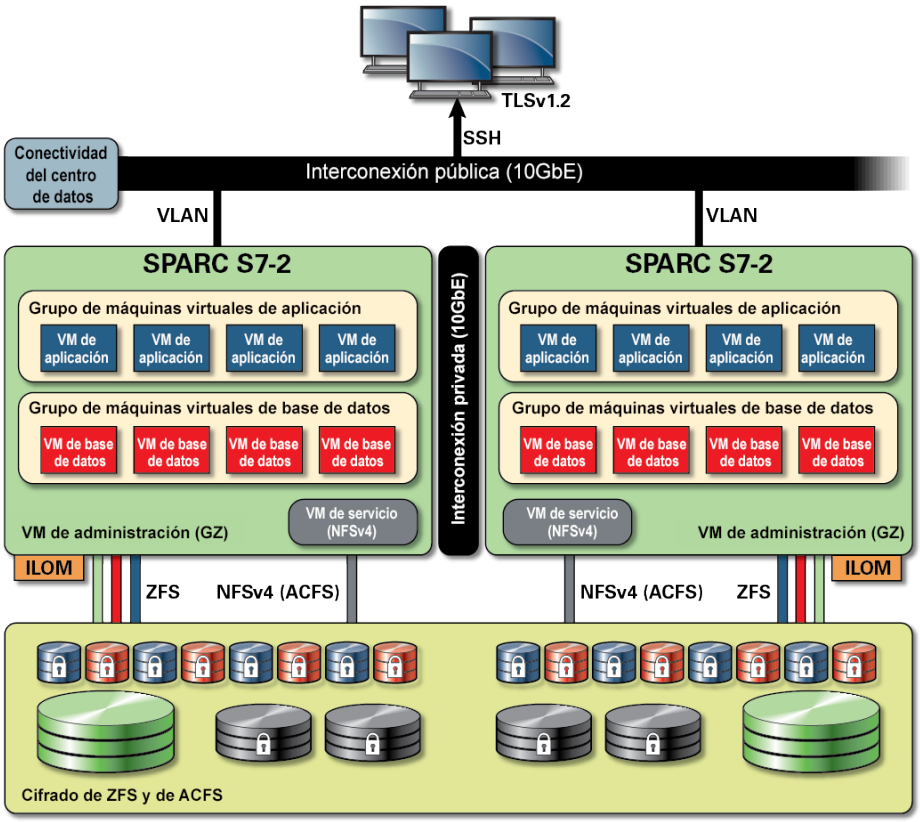
Principios de seguridad principales

MiniCluster es una plataforma de infraestructura de nube segura para la consolidación de aplicaciones y bases de datos y es apropiada para proporcionar servicios de nube dedicados basados en la infraestructura de cálculo como servicio (IaaS). Dado que está desarrollado como un sistema de ingeniería de varios usos, combina la potencia de cálculo del procesador SPARC S7 de Oracle, las capacidades de virtualización eficaces de Solaris SPARC y el rendimiento optimizado de la base de datos Oracle integrada con almacenamiento dedicado. Además, se emplea una red 10GbE, que les permite a los clientes acceder a los servicios que se están ejecutando en MiniCluster. Por último, otra red 10GbE proporciona un conducto que permite la comunicación entre el entorno de máquina virtual de los servidores SPARC S7 y las aplicaciones alojadas.

El procesador SPARC S7 presenta una funcionalidad criptográfica asistida por hardware que siempre está activada, la cual ayuda a las entidades alojadas en MiniCluster a proteger la información con una protección de datos de alto rendimiento, para datos inactivos, en uso y en tránsito. El procesador también presenta la capacidad Silicon Secured Memory, que detecta y evita ataques relacionados con daños en los datos de la memoria y recortes de memoria, lo cual garantiza la integridad de los datos de aplicación.

Por defecto, MiniCluster viene preconfigurado con más de 250 controles de seguridad listos para usar que reducen la superficie de ataque del sistema mediante la desactivación de los servicios, los puertos y los protocolos que no son absolutamente necesarios y mediante la configuración de los servicios expuestos para que acepten solo conexiones confiables.

El sistema admite una variedad de opciones de configuración y despliegue. En esta figura, se ilustra un despliegue típico que consolida las cargas de trabajo de las aplicaciones y de Oracle Database.



Máquinas virtuales seguras

La seguridad se proporciona en varios niveles dentro de los nodos de cálculo de MiniCluster. Comienza con un inicio verificado seguro de los nodos de cálculo, un sistema operativo endurecido y minimizado que se ejecuta como máquinas virtuales aisladas para evitar que usuarios y sistemas no autorizados accedan a los datos y a las cargas de trabajo. La tecnología de zonas de Oracle Solaris se usa de la misma manera que las máquinas virtuales en MiniCluster, para alojar entornos de cálculo aislados y crear de manera eficaz sandboxes de diferentes aplicaciones que se están ejecutando en el mismo sistema operativo, para protegerlas de actividades maliciosas o involuntarias que se produzcan en otras máquinas virtuales. A pesar de que se ejecutan en el mismo núcleo, cada zona de Solaris tiene su propia identidad y su propio aislamiento de recursos, de espacios de nombres y de procesos. En esencia, las zonas de Solaris proporcionan virtualización incorporada con controles de recursos flexibles y aislamiento eficaz en un espacio de memoria y de CPU más pequeño que las máquinas virtuales tradicionales que se ejecutan en hipervisores de tipo 1. Cada máquina virtual se configura con un perfil de seguridad que define un conjunto completo de políticas y controles de seguridad

que se aplican automáticamente durante el proceso de instalación. Los juegos de datos y las agrupaciones ZFS permiten delimitar y aislar el almacenamiento en unidades más granulares para las máquinas virtuales y pueden tener sus propias políticas de seguridad.

Control de acceso

Para proteger los datos de las aplicaciones, las cargas de trabajo y la infraestructura subyacente en la que funciona todo el sistema, MiniCluster ofrece capacidades de control de acceso completas y flexibles para los usuarios y para los administradores. MiniCluster utiliza Oracle Solaris para una variedad de métodos de control de acceso para los usuarios y las aplicaciones que acceden a los servicios del sistema. Aunque los pares tradicionales de nombre de usuario y contraseña todavía se usan ampliamente, es posible integrar métodos de autenticación más seguros de manera sencilla por medio de la arquitectura de módulos de autenticación conectables (PAM) de Oracle Solaris, que permiten el uso de LDAP, Kerberos y la autenticación de clave pública. El entorno de cálculo de MiniCluster se basa en una utilidad de control de acceso basado en roles (RBAC) completa que permite a las organizaciones tener la flexibilidad de delegar el acceso de usuario o de administrador según sea necesario. Dado que elimina la noción de un superusuario omnipotente, la capacidad RBAC de Oracle Solaris permite la separación de tareas y admite la noción de roles administrativos, autorizaciones, privilegios más específicos y perfiles de derechos, que se usan en conjunto para asignar derechos a usuarios y administradores. RBAC está integrado con otros servicios principales de Oracle Solaris, incluidas la utilidad de gestión de servicios (SMF) de Oracle Solaris y las máquinas virtuales, para proporcionar una arquitectura coherente que permite satisfacer todas las necesidades de control de acceso en el nivel de sistema operativo. MiniCluster utiliza la capacidad RBAC de Oracle Solaris como base para la arquitectura de control de acceso, lo que permite a las organizaciones gestionar, controlar y auditar el acceso al sistema operativo y a la gestión de la virtualización desde una autoridad centralizada. Todas las operaciones esenciales se realizan con un principio de separación de tareas respaldado por un flujo de trabajo de autorización de varias personas. El sistema requiere que dos o más personas aprueben cada operación que conlleve riesgos para la seguridad. De manera colectiva, estas capacidades se pueden usar para proporcionar un alto grado de seguridad con respecto a la identidad de los usuarios y a su manejo de las operaciones comerciales críticas.

Todos los dispositivos del sistema MiniCluster incluyen la capacidad de limitar el acceso de red a los servicios por medio de métodos de arquitectura (por ejemplo, aislamiento de redes) o por medio de listas de control de acceso o filtros de paquetes para limitar la comunicación entre los dispositivos físicos y virtuales, además de los servicios expuestos por el sistema. MiniCluster despliega una postura seguridad por defecto, por medio de la cual ningún servicio, excepto el shell seguro (SSH), puede aceptar tráfico de red entrante. Otros servicios de red activados reciben internamente las solicitudes del sistema operativo Oracle Solaris (zona o máquina virtual). Esto garantiza que todos los servicios de red estén desactivados por defecto o se configuren para recibir solo comunicaciones del sistema local. Las organizaciones tienen la libertad de personalizar esta configuración según sus requisitos. MiniCluster viene preconfigurado con filtros de paquetes de capa de red y de transporte (con estado) que usan la

función de filtro IP de Oracle Solaris. El filtro IP ofrece una matriz amplia de capacidades de red basadas en host, incluidos los filtros de paquetes con estado, la traducción de direcciones de red y la traducción de direcciones de puertos.

Protección de datos

El procesador SPARC S7 de MiniCluster 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. El procesador SPARC M7 también cuenta con tecnología Silicon Secured Memory, que garantiza la prevención de ataques malintencionados en el nivel de aplicación, como recortes de memoria, daños silenciosos de memoria, saturaciones de buffer y ataques relacionados.

El procesador SPARC permite la compatibilidad con 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 criptográfica de hardware está activada por defecto para la mayoría de los servicios principales, incluidos el shell seguro, IPSec/IKE y los juegos de datos ZFS cifrados.

Oracle Database y Oracle Fusion Middleware identifican de manera automática el sistema operativo Oracle Solaris y el procesador SPARC que utiliza MiniCluster. Esto permite que la base de datos y el middleware usen automáticamente las capacidades de aceleración criptográfica de hardware de la plataforma para TLS, WS-Security 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. MiniCluster admite el uso de IPSec (seguridad IP) y se recomienda el intercambio de claves de Internet (IKE) para proteger la confidencialidad y la integridad de las comunicaciones específicas de máquinas virtuales y entre máquinas virtuales que fluyen en las redes públicas y privadas.

En MiniCluster, el cifrado de juegos de datos ZFS utiliza un almacén de claves PKCS#11 de Oracle Solaris para proteger correctamente las claves de ajuste. El uso del almacén de claves PKCS#11 de Oracle Solaris involucra de inmediato la aceleración criptográfica asistida por hardware de SPARC para todas las operaciones de cifrado. Esto permite a Oracle mejorar ampliamente el rendimiento de las operaciones de cifrado y descifrado asociadas con el cifrado de juegos de datos ZFS, el cifrado de datos transparentes (TDE) de Oracle Database, el cifrado de tablespace, 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). Las máquinas virtuales de base de datos pueden usar un enfoque de cartera compartida mediante el almacén de claves PKCS#11 de Oracle Solaris o para crear un directorio en el almacenamiento

de recursos compartidos ACFS, de manera que la cartera se pueda compartir entre las bases de datos que residen en las máquinas virtuales. El uso de un almacén de claves centralizado y compartido en cada nodo de cálculo permite al sistema realizar mejor las tareas de gestión, mantenimiento y rotación de claves de Oracle TDE en las arquitecturas de base de datos en cluster basadas en la infraestructura de cuadrícula de Oracle, porque las claves se sincronizan entre todos los nodos del cluster. MiniCluster también permite la supresión segura de las máquinas virtuales y de los juegos de datos ZFS asociados, ya que cuenta con la política de cifrado y la gestión de claves en el nivel de juego de datos ZFS (sistema de archivo/ZVOL) para garantizar la supresión por medio de la destrucción de claves.

Auditoría y conformidad

MiniCluster depende del subsistema de auditoría de Oracle Solaris para recopilar, almacenar y procesar la información de eventos de auditoría. Cada máquina virtual (zona no global) genera registros de auditoría que se almacenan localmente en cada uno de los almacenes de auditoría de MiniCluster (zona global). Este enfoque garantiza que las máquinas virtuales individuales no puedan modificar sus políticas de auditoría, sus configuraciones ni sus datos registrados, dado que la responsabilidad es del proveedor de servicios de 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 las máquinas virtuales. Esta utilidad tiene una gran capacidad de configuración y ofrece políticas de auditoría globales, por zona e, incluso, por usuario. Cuando se configuran para usar máquinas virtuales, los registros de auditoría de cada máquina virtual se pueden almacenar en la zona global para protegerlos contra la manipulación. La zona global también aprovecha la utilidad de auditoría nativa de Oracle Solaris para registrar las acciones y los eventos asociados con los eventos de virtualización y administración de MiniCluster.

MiniCluster proporciona herramientas para analizar e informar la conformidad del entorno de tiempo de ejecución de Oracle Solaris en las máquinas virtuales. Las utilidades de conformidad se basan en la implementación del protocolo de automatización de contenido de seguridad (SCAP). MiniCluster admite dos perfiles de referencia de conformidad de seguridad:

- **Perfil de seguridad por defecto**: un perfil equivalente a CIS (basado en la referencia del Centro para la seguridad en Internet [Center for Internet Security]), que está más alineado con los requisitos de conformidad de seguridad establecidos por las normativas, como HIPAA, FISMA, SOX, entre otras.
- **Perfil PCI-DSS**: el estándar de seguridad de datos del sector de tarjetas de pago.
- **Perfil DISA STIG**: el estándar Defense Information System Agency - Security Technical Implementation Guidance. El perfil se basa en el perfil de seguridad por defecto e introduce 75 controles de seguridad adicionales, criptografía FIPS-140-2 y soporte para configurar una contraseña S. *Nota*: Actualmente, este perfil está en etapa de revisión. Solo utilice este perfil para uso experimental en entornos no productivos.

El administrador de MiniCluster puede ejecutar la referencia de conformidad a petición y comprobar la conformidad o la existencia de anomalías en el entorno. Estas herramientas de creación de perfiles asignan controles de seguridad a los requisitos de conformidad establecidos por los estándares del sector. Los informes de conformidad asociados pueden reducir considerablemente los costos y el tiempo de auditoría.

A partir de MiniCluster v.1.1.18, el sistema incluye las siguientes funciones de auditoría:

- **Rol del auditor**: cuando se especifica este rol para un usuario de MCMU, el usuario puede acceder a la página de revisión del auditor en la BUI de MCMU. El usuario no puede ver ni realizar ninguna otra tarea administrativa de MiniCluster.
- **Página de revisión del auditor**: es una página especial de la BUI de MCMU que solo los usuarios con rol de auditor pueden ver. La página proporciona acceso al estado de la agrupación de auditoría y ofrece la capacidad de generar registros de auditoría sobre toda la actividad de los usuarios por zona. Consulte Generación de informes de auditoría [41].

Descripción de la configuración de seguridad

En los siguientes temas, se describen los controles de seguridad de MiniCluster:

Perfiles de seguridad incorporados

La inicialización de MiniCluster se realiza por medio de la BUI o de la CLI de MCMU. Durante la inicialización, MCMU le solicita al instalador que elija uno de los perfiles de seguridad:

- **Perfil de seguridad por defecto**: cumple con requisitos comparables y equivalentes a las referencias establecidas por el Centro para la seguridad informática (CIS, Center for Internet Security) y las evaluaciones de la Guía de implementación técnica de seguridad (STIG, Security Technical Implementation Guide).
- **Perfil PCI-DSS**: cumple con el estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS, Payment Card Industry Data Security Standard) definido por el consejo de estándares de seguridad del sector de tarjetas de pago.
- **Perfil DISA STIG**: el estándar Defense Information System Agency - Security Technical Implementation Guidance. El perfil se basa en el perfil de seguridad por defecto e introduce 75 controles de seguridad adicionales, criptografía FIPS-140-2 y soporte para configurar una contraseña de eeprom. *Nota*: Actualmente, este perfil está en etapa de revisión. Solo utilice este perfil para uso experimental en entornos no productivos.

En función de la política seleccionada, MCMU configura la zona global y las zonas no globales con más de 250 controles de seguridad.

Después de la inicialización, cuando se crean las máquinas virtuales, MCMU le solicita que seleccione uno de los perfiles de seguridad para cada máquina virtual. En función de los requisitos de seguridad, puede tener una combinación de perfiles de seguridad en las máquinas virtuales.

Verificación del perfil de seguridad de máquina virtual (CLI)

Realice el siguiente procedimiento para verificar o identificar el perfil de seguridad configurado para las zonas y las máquinas virtuales.

Nota - Debe acceder al sistema con una cuenta de usuario que tenga el rol `root` para realizar este procedimiento.

Nota - Para identificar el perfil de seguridad asignado a la zona global, en la BUI de MCMU, vaya a Configuración de sistema -> Resumen de entrada de usuario. El perfil de seguridad aparece en la parte inferior de la página.

1. **Inicie sesión en la zona global como `mcinstall`.**

   Para obtener instrucciones sobre cómo acceder al sistema, consulte la *Guía de administración de Oracle MiniCluster S7-2*.

2. **Asuma el rol `root`.**

   Ejemplo:

   ```
   # su root
   ```

3. **Determine el nombre del archivo log de la máquina virtual en cuestión.**

   En este ejemplo, hay un archivo log para cada máquina virtual:

   ```
   # cd /var/opt/oracle.minicluster/mcmubui/MCMU/verification_logs
   # ls
   verify_appvmg1-zone-1-mc4-n1.log  verify_dbvmg1-zone-3-mc4-n1.log
   verify_appvmg1-zone-1-mc4-n2.log  verify_dbvmg1-zone-3-mc4-n2.log
   verify_dbvmg1-zone-1-mc4-n2.log   verify_dbvmg1-zone-4-mc4-n1.log
   verify_dbvmg1-zone-2-mc4-n1.log   verify_dbvmg1-zone-4-mc4-n2.log
   verify_dbvmg1-zone-2-mc4-n2.log
   #
   ```

4. **Visualice los archivos log de verificación.**

   Visualice las últimas líneas del archivo log. Si aparece el comando `(PCI-DSS)`, el perfil de seguridad de la máquina virtual es PCI-DSS. Si no aparece ningún perfil, el perfil de seguridad de la máquina virtual es equivalente a CIS.

   - Ejemplo de las últimas 22 líneas de una máquina virtual con perfil PCI-DSS:

     ```
     # tail -22 verify_dbvmg1-zone-1-mc4-n2.log

     (PCI-DSS) Checking /etc/cron.d/at.allow:
     Passed/Configured
     ```

```
(PCI-DSS) Checking audit configuration (user audit flags):
Passed/Configured

(PCI-DSS) Checking audit configuration (non-attributable audit flags):
Passed/Configured

(PCI-DSS) Checking audit configuration (audit_binfile plugin):
Passed/Configured

(PCI-DSS) Checking audit flags on root and tadmin roles:
Passed/Configured

Check if tenant-key exists in keystore:
Passed/Configured

Check if immutability is enabled:
Failed/Not Configured
```

- Ejemplo de las últimas 22 líneas de una máquina virtual con perfil equivalente a CIS:

```
# tail -22 verify_dbvmg1-zone-1-mc4-n2.log
Checking if NDP routing daemon is disabled:
Passed/Configured

Checking if r-protocol services are disabled:
Passed/Configured

Checking if rpc/bind is enabled and configured correctly:
Passed/Configured

Checking if NFS v2/v3 is disabled:
Passed/Configured

Checking if GDM is enabled:
Failed/Not Configured

Check if tenant-key exists in keystore:
Passed/Configured

Check if immutability is enabled:
Failed/Not Configured
```

Protección de datos

En los siguientes temas, se describen las tecnologías de protección de datos de MiniCluster:

Protección de datos con cifrado de juegos de datos ZFS

En MiniCluster, la protección de datos inactivos se configura automáticamente por medio del cifrado de juegos de datos ZFS. El cifrado está configurado de la siguiente manera:

- Todos los juegos de datos ZFS están cifrados en las máquinas virtuales, incluidos los sistemas de archivos root y de intercambio.
- Todos los juegos de datos ZFS se cifran en la zona global, con excepción de los sistemas de archivos raíz y de intercambio.

Puede verificar la configuración del cifrado visualizando las claves de cifrado. Consulte Visualización de claves de cifrado de juegos de datos ZFS (BUI) [21].

▼ Visualización de claves de cifrado de juegos de datos ZFS (BUI)

Realice el siguiente procedimiento para ver los detalles de las claves de cifrado.

1. **Acceda a la BUI de MCMU.**

Para obtener información detallada sobre cómo acceder a la BUI de MCMU, consulte la *Guía de administración de Oracle MiniCluster S7-2*.

2. **En el panel de navegación, seleccione Configuración de sistema -> Seguridad.**

   Haga clic en un nodo para ver los detalles.

Servicio de shell seguro

MiniCluster requiere el uso del protocolo de red SSH para que iniciar sesión de manera segura en los nodos de cálculo (zonas globales) y en las instancias de máquina virtual (zonas no globales) de MiniCluster.

Cuando un usuario inicia sesión por primera vez usando SSH, el sistema genera automáticamente un nuevo par de claves SSH para el usuario.

▼ Cambio de claves SSH (BUI)

Realice el siguiente procedimiento para cambiar las claves SSH para una zona o una máquina virtual con una de las siguientes configuraciones:

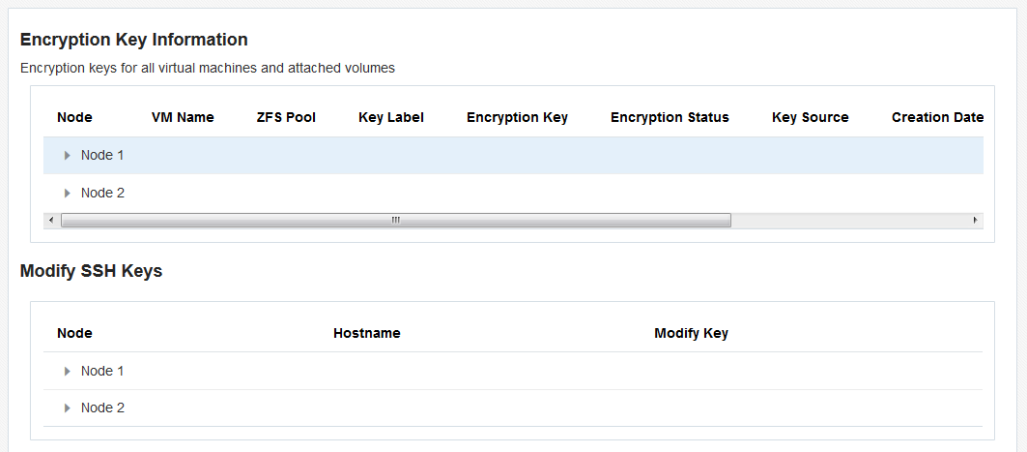
- Insertar nueva clave para autorizar uso de SSH sin contraseña: requiere la introducción de un nombre de usuario de máquina virtual, un nombre de máquina virtual y una clave pública RSA.
- Generar automáticamente nuevas claves para las máquinas virtuales.

Nota - Para realizar este procedimiento usando la CLI de MCMU, consulte la *Guía de administración Oracle MiniCluster S7-2*.

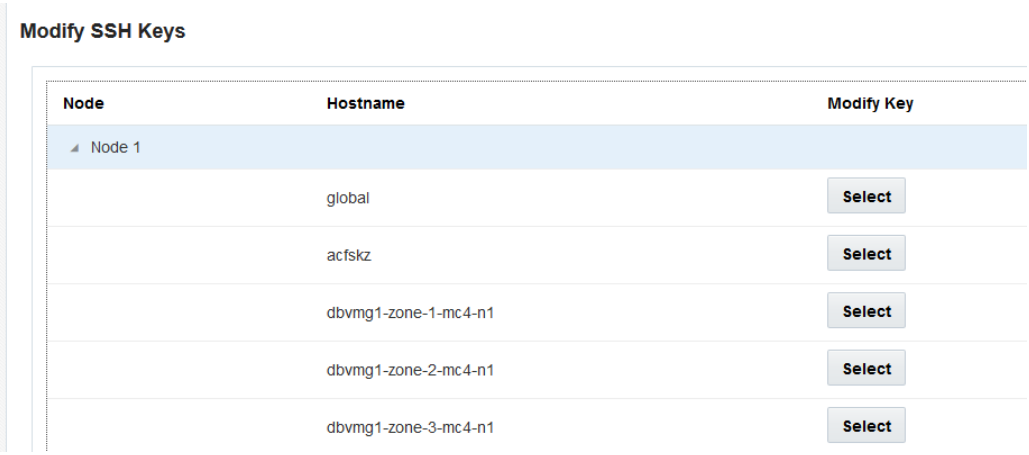
---

1. **Acceda a la BUI de MCMU.**

2. **En el panel de navegación, seleccione Configuración de sistema -> Seguridad.**



3. **En el panel Modificar claves SSH, haga clic en un nodo para ampliar la vista.**



4. **En la máquina virtual que desee cambiar, haga clic en Seleccionar.**

5. **Seleccione una opción en el menú desplegable y haga clic en Siguiente.**

   Las opciones son las siguientes:

   - Insertar nueva clave para autorizar uso de SSH sin contraseña
   - Generar automáticamente nuevas claves para máquinas

6. **Haga clic en Siguiente.**

7. **Si autorizó el uso de SSH sin contraseña, introduzca la siguiente información y luego haga clic en Siguiente:**

   - Nombre de usuario de la máquina
   - Nombre de host de la máquina
   - Clave pública RSA de la máquina

8. **Haga clic en Configurar SSH.**

   Se aplica el cambio.

Comunicación segura con IPsec

Se recomienda el uso de IPsec (seguridad IP) y de IKE (intercambio de claves de Internet) para proteger la confidencialidad y la integridad de las comunicaciones basadas en IP entre zonas y el tráfico NFS que fluye en las redes. Se recomienda el uso de IPsec porque admite la autenticación de pares en el nivel de red, la autenticación de origen de datos, la confidencialidad de datos, la integridad de datos y la protección de la reproducción. Cuando se usan en la plataforma Oracle MiniCluster, IPsec e IKE pueden aprovechar automáticamente la aceleración criptográfica asistida por hardware y, de esta manera, minimizar el impacto en el rendimiento que tiene el uso de la criptografía para proteger la información confidencial que fluye en este canal de red.

▼ Configuración de IPsec e IKE

Antes de poder configurar IPsec, se deben definir los nombres de host específicos o las direcciones IP que se usan entre los pares que se comunican.

En el ejemplo de este procedimiento, se usan las direcciones IP 10.1.1.1 y 10.1.1.2 para designar dos zonas no globales de Solaris que son controladas por un inquilino único. La comunicación entre estas dos direcciones se protegerá con IPsec. El ejemplo se presenta desde la perspectiva de la zona no global asociada con la dirección IP 10.1.1.1.

Realice los siguientes pasos para configurar el uso de IPsec e IKE entre un par de zonas no globales designadas (máquinas virtuales):

1. **Defina la política de seguridad para IPsec.**

   Defina la política de seguridad que se aplicará entre las dos zonas que se comunican.

   En este ejemplo, se cifrarán todas las comunicaciones de red entre 10.1.1.1 y 10.1.1.2:

```
{laddr 10.1.1.1 raddr 10.1.1.2}
ipsec{encr_algs aes encr_auth_algs sha256 sa shared}
```

2. **Almacene la política en el archivo `/etc/inet/ipsecinit.conf`.**

3. **Verifique que la política de IPsec sea correcta desde el punto de vista sintáctico.**

   Ejemplo:

   ```
   # ipsecconf –c –f ipsecinit.conf
   ```

4. **Configure el servicio de intercambio de claves de internet (IKE).**

   Configure el servicio según la configuración de host y de algoritmo que aparece en el archivo `/etc/inet/ike/config`.

   ```
   { label "ipsec"

   local_id_type ip

   remote_addr 10.1.1.2

   p1_xform { auth_method preshared oakley_group 5

   auth_alg sha256 encr_alg aes } }
   ```

5. **Configure la clave compartida previamente.**

   Antes de que se pueda activar IPsec, se debe compartir el material de claves con ambos nodos, de manera que puedan autenticarse entre sí.

   La implementación de IKE de Oracle Solaris admite una variedad de tipos de clave, incluidos los certificados y las claves compartidas previamente. Para que resulte más sencillo, en este ejemplo, se usan claves compartidas previamente que se almacenan en el archivo `/etc/inet/secret/ike.preshared`. Sin embargo, si lo desean, las organizaciones pueden usar métodos de autenticación más seguros.

   Edite el archivo /etc/inet/secret/ike.preshared e introduzca la información de claves compartidas previamente. Por ejemplo:

   ```
   {
   localidtype IP
   localid 10.1.1.1
   remoteid type IP
   key "This is an ASCII phrAz, use strOng p@sswords"
   }
   ```

6. **Active los servicios IKE e IPsec en ambo pares.**

   Los servicios se deben activar en los dos pares que se comunican para que la comunicación cifrada sea posible.

   Ejemplo:

   ```
   # svcadm enable svc:/network/ipsec/policy:default
   # svcadm enable svc:/network/ipsec/ike:default
   ```

Control de acceso

En estos temas, se describen las funciones de control de acceso disponibles en MiniCluster:

▼ Cambio de las contraseñas de usuario `root` por defecto de Oracle ILOM

El sistema se envía con contraseñas por defecto asignadas a las cuentas de usuario root de Oracle ILOM en ambos nodos. Esto permite que el proceso de instalación se realice con una cuenta de acceso inicial predecible. Inmediatamente después de la instalación, cambie las contraseñas por defecto para garantizar una seguridad óptima.

1. **Inicie sesión en Oracle ILOM en el nodo 1 como `root`.**

   Use el comando `ssh` para conectarse a Oracle ILOM.

   Para obtener los nombres de host de Oracle ILOM, en la utilidad BUI, seleccione Configuración de sistema -> Información de sistema. Los nombres de host aparecen en la columna ILOM.

   Sintaxis:

   ```
   % ssh root@node1_ILOM_hostname_or_IPaddress
   ```

   Escriba la contraseña de usuario root por defecto de Oracle ILOM: welcome1

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

```
-> set /SP/users/root password
Enter new password: *********
Enter new password again: **********
```

3. **Repita los pasos para cambiar la contraseña de usuario `root` de Oracle ILOM en el nodo 2.**

4. **Actualice Oracle Engineered Systems Hardware Manager con las contraseñas nuevas.**

   Consulte "Actualización de contraseñas de componentes" de *Guía de administración de Oracle MiniCluster S7-2*.

Configuración de contraseñas de EEPROM

Cada nodo de MiniCluster tiene una EEPROM, a veces denominada OpenBoot PROM, que es firmware de bajo nivel que contiene algunos parámetros de configuración y controladores que facilitan el inicio del sistema. Por defecto, la función de contraseña de EEPROM está desactivada.

En entornos seguros, use este procedimiento para activar la función de contraseña y establecer una. La contraseña se activa y se aplica a ambos nodos automáticamente.

Este procedimiento sustituye los métodos más antiguos en los que la contraseña se establece en el símbolo del sistema `ok` de OpenBoot o en Oracle Solaris con el comando `eeprom`.

Atención - Es importante recordar la contraseña. Si olvida la contraseña, debe llamar a los servicios de soporte para que su sistema se pueda iniciar nuevamente.

Nota - En este procedimiento, se describe cómo configurar las contraseñas mediante la BUI de MCMU. También puede usar el comando `mcmu security -e`.

1. **Inicie sesión en MCMU como administrador principal, por ejemplo, `mcinstall`.**

2. **En el panel de navegación, seleccione Configuración de sistema -> Seguridad.**

3. **Realice una de estas acciones:**

   - Para activar y establecer la contraseña, haga clic en Activar, introduzca la contraseña dos veces y haga clic en Establecer contraseña.
   - Para desactivar la característica, haga clic en Desactivar y, luego, en Confirmar.
   - Para cambiar la contraseña existente, haga clic en Cambiar contraseña, introduzca la nueva contraseña dos veces y haga clic en Actualizar.

Aprovisionamiento de usuarios

Durante la instalación de MiniCluster, el proceso de instalación requiere que usted cree y registre el primer usuario de MCMU, llamado `mcinstall`. Se recopila la información demográfica del usuario, que incluye la dirección de correo electrónico y el número de teléfono. El usuario `mcinstall` es la primera cuenta de administrador principal. Cuando `mcinstall` inicia sesión por primera vez, la utilidad solicita que `mcinstall` cree una contraseña nueva de acuerdo con las políticas de contraseñas de Oracle Solaris que están asociadas con el perfil de seguridad.

Durante el registro del usuario `mcinstall`, se le solicita que especifique una persona que actúe como supervisor de MCMU. Es supervisor solamente se identifica mediante un nombre y una dirección de correo electrónico. El supervisor no es un usuario de MCMU y no tiene credenciales de inicio de sesión.

Tanto el supervisor como los usuarios mcinstall están asociados con nombres de personas reales y direcciones de correo electrónico válidas.

Cuando se aprovisionan nuevos usuarios de MCMU, a cada cuenta de usuario se le asigna un rol de administrador principal o de administrador secundario (consulte “Control de acceso basado en roles ” [30]). Antes de que se active la cuenta nueva, el usuario `mcinstall` y el supervisor deben aprobar la nueva cuenta de usuario por medio de una URL que reciben por correo electrónico (consulte “Proceso de aprobación de usuarios de MCMU” [29]). En el primer inicio de sesión, se obliga al usuario a definir una contraseña que cumpla con las políticas de contraseñas de MCMU. Consulte “Políticas de autenticación de usuarios y de contraseñas” [33].

Proceso de aprobación de usuarios de MCMU

Todas las cuentas de usuario de MCMU requieren la aprobación de dos personas: el supervisor y el administrador principal de MCMU. El proceso es el siguiente:

1. El posible usuario (o un administrador de MCMU que realice la tarea en su nombre) accede a la página de registro de MCMU y proporciona los siguientes detalles obligatorios:

- Nombre de usuario de MCMU
- Dirección de correo electrónico
- Nombre completo
- Número de teléfono
- Rol de MCMU

2. MCMU envía al supervisor y al administrador principal de MCMU un correo electrónico para que aprueben o denieguen la solicitud. El correo electrónico incluye la URL de la función de aprobación/denegación de MCMU e incluye un identificador de clave única.
3. Cuando el supervisor y el administrador principal aprueban la cuenta, la cuenta de usuario se activa y MCMU envía al usuario nuevo un correo electrónico en el que se confirma la activación de la cuenta. El usuario recibe una cuenta de MCMU a la que puede acceder mediante la BUI o la CLI de MCMU. El usuario también recibe una cuenta de usuario de Oracle Solaris. Si el usuario existe en un LDAP corporativo y MiniCluster está configurado con un cliente LDAP, el usuario solo puede usar LDAP para la cuenta de Oracle Solaris.

Todos los usuarios registrados se almacenan en el repositorio de MCMU. Un administrador de MCMU puede verificar los usuarios, incluidos sus roles y el supervisor, en MCMU, yendo a Configuración de sistema -> Cuentas de usuario. Ejemplo:

En los temas que aparecen a continuación en esta sección, se describe cómo realizar estas tareas.

Control de acceso basado en roles

No hay ningún usuario `root` en MiniCluster. Por el contrario, root es un rol que se asigna a los usuarios de MCMU que están registrados como administradores principales.

Cuando se crea un usuario de MCMU, se le asigna uno de los siguientes roles:

- **Administrador principal (**rol `root`**)**: el rol `root` define los derechos y los privilegios de los administradores principales del sistema MiniCluster, incluidos todos los nodos de cálculo, las redes, la base de datos y el almacenamiento. Los usuarios que tiene el rol `root` pueden realizar todas las operaciones de instalación y todas las operaciones administrativas críticas

sin restricciones. Como administradores principales, pueden delegar operaciones y aprobar la agregación o la supresión de usuarios, incluidos los nuevos administradores principales y secundarios. El usuario debe iniciar sesión con sus propias credenciales. Todas las acciones y operaciones que se realizan se registran y se auditan en función del identificador de usuario, no del identificador de rol.

- **Administrador secundario (**rol `mcadmin`**)**: este rol define los derechos y los privilegios de los administradores secundarios de las zonas no globales y los dominios de MiniCluster. Por defecto, este rol solo permite un acceso de solo lectura a MCMU. Todas las acciones y operaciones que se realizan se registran y se auditan en función del identificador de usuario, no del identificador de rol.
- **Administrador inquilino (**rol `tadmin`**)**: este rol define los derechos y los privilegios del administrador de una máquina virtual de MiniCluster. El rol define los derechos y los privilegios de un administrador de máquina virtual que realiza las operaciones administrativas cotidianas relacionadas con la instalación y el despliegue de aplicaciones. Todas las acciones se auditan en función del identificador de usuario, no del identificador de rol.
- **Auditor (rol** `auditor`**)**: los usuarios con este rol solo tienen acceso a la página de revisión de auditoría de la BUI de MCMU donde pueden ver el estado de la agrupación de auditoría y generar informes sobre la actividad de usuario. Solo los usuarios con este rol pueden acceder a la página de revisión de auditoría. Los auditores no pueden acceder a MCMU (a excepción de la página de auditoría) ni pueden iniciar sesión en las zonas de núcleo o las máquinas virtuales.

Cuentas de usuario

MiniCluster incluye las cuentas de usuario que aparecen en la siguiente tabla.

Usuario	Contraseña	Rol	Descripción
`mcinstall`	La contraseña se configura durante la instalación. Se puede restablecer y cambiar mediante MCMU.	`root`	El proceso de instalación requiere la creación de `mcinstall` como administrador principal de MCMU y la creación de una contraseña. Esta cuenta está destinada al administrador principal de MCMU. Esta cuenta de usuario se usa para las siguientes actividades: ■ Permite realizar la inicialización del sistema en el momento de la instalación ejecutando `installmc`. ■ Administración del sistema, incluidas las máquinas virtuales, mediante la BUI de MCMU o la CLI `mcmu`. ■ Permite asumir el rol `root` (`su` para root) en las máquinas virtuales de aplicación, en la zona global y en las zonas de núcleo para obtener los privilegios de superusuario.
Supervisor de MCMU: el nombre de	N/D	N/D	En el software de MiniCluster, el usuario supervisor solo tiene un nombre de usuario y una dirección de correo electrónico. No tiene credenciales de inicio de

Usuario	Contraseña	Rol	Descripción
la cuenta se determina en el momento de la instalación			sesión. Puede usar esta cuenta para proporcionar un segundo nivel en el proceso de aprobación de usuarios de MCMU. Este usuario recibe un correo electrónico cada vez que se crea un nuevo usuario de MCMU. El administrador principal y el supervisor deben aprobar el nuevo usuario para que se active la cuenta de usuario. Puede usar esta cuenta para proporcionar una segunda capa en el proceso de aprobación de usuarios de MCMU asignando otra persona que no sea el administrador principal como supervisor.
(Opcional) *Administrador de inquilino*: el nombre de la cuenta se determina en el momento del registro del usuario	Se determina cuando se inicia sesión por primera vez.	`tadmin`	Este usuario puede realizar todas las actividades posteriores a la instalación solo en las máquinas virtuales. Este usuario no puede acceder a las zonas globales ni de núcleo y no puede ejecutar la CLI o la BUI de MCMU.
(Opcional) *Administrador secundario*: el nombre de la cuenta se determina en el momento del registro del usuario	Se determina cuando se inicia sesión por primera vez.	`mcadmin`	Cuando se crea un usuario de MCMU y se lo asigna como administrador secundario, tiene acceso de solo lectura a las zonas no globales.
`oracle`	La contraseña es igual a la contraseña de `mcinstall`.	`root`	Esta cuenta de usuario se usa para las siguientes actividades: ■ Se usa como cuenta de inicio de sesión por primera vez en las máquinas virtuales de base de datos, desde la que puede configurar las máquinas virtuales de base de datos con una base de datos, datos y otras cuentas, según sea necesario. ■ Permite asumir el rol root (`su` para root) en las máquinas virtuales de base de datos para obtener los privilegios de superusuario.

La contraseña de MCMU por defecto que se usa en el primer inicio de sesión es `welcome1`. Una vez que se introduce la contraseña `welcome1`, la utilidad obliga al usuario a crear una contraseña nueva que cumpla con las políticas de contraseñas. Consulte "Políticas de autenticación de usuarios y de contraseñas" [33].

Todas las acciones que realizan todos los usuarios de MCMU se registran según el identificador del usuario. Para obtener información sobre los informes de auditoría, consulte Creación de informes de auditoría y de conformidad [39].

Nota - Las cuentas de usuario de MCMU no se usan para el uso cotidiano del sistema, como el uso de aplicaciones y bases de datos. Esas cuentas de usuario se gestionan mediante Oracle Solaris, la aplicación, la base de datos de las máquinas virtuales y los servicios de nombre del sitio.

Políticas de autenticación de usuarios y de contraseñas

A todos los usuarios aprovisionados en MiniCluster se les asigna un rol con políticas de contraseñas estrictas y cifrado de contraseñas que se aplican según el perfil de seguridad.

La política de seguridad por defecto establece los siguientes requisitos de contraseñas de MCMU:

- Debe tener un mínimo de 14 caracteres.
- Debe tener un carácter numérico como mínimo.
- Debe tener un carácter alfabético en mayúscula como mínimo.
- Debe ser distinta de la contraseña anterior en al menos tres caracteres.
- No puede ser igual a las últimas diez contraseñas.

Todos los usuarios inician sesión en sus cuentas de Oracle Solaris por medio de su propia contraseña de usuario únicamente.

▼ Verificación de los roles de usuario de Oracle Solaris

1. **Inicie sesión en la zona global de MiniCluster y asuma el rol root.**
   Para obtener más detalles, consulte la *Guía de administración de Oracle MiniCluster S7-2*.

2. **Verifique la lista de roles disponibles.**

```
# logins -r
```

3. **Verifique el rol de usuario y la contraseña necesarios para la autenticación:**

```
# grep root /etc/user_attr
root::::audit_flags=lo\:no;type=role;roleauth=user
mcinstall::::auths=solaris.system.maintenance;roles=root
```

Supresión segura de máquinas virtuales

Solo el administrador principal de MCMU puede suprimir máquinas virtuales o grupos de máquinas virtuales. Cuando se suprime un componente de máquina virtual, las claves correspondientes se suprimen automáticamente y se envía un correo electrónico al administrador principal.

Para verificar esta función, antes de suprimir un componente de máquina virtual, inicie sesión en la BUI de MCMU como administrador principal y consulte las claves de cifrado (Configuración de sistema -> Seguridad). Suprima el componente de máquina virtual y, luego,

vuelva a consultar las claves. La máquina virtual y la etiqueta de clave asociada del componente suprimido ya no aparecerán.

▼ Verificación de reglas de firewall basado en host

Todos los entornos de cálculo, incluidas las zonas globales, las zonas de núcleo y las zonas no globales, se configuran automáticamente con firewalls IPFilter. No se requiere ninguna acción manual.

Para verificar los firewalls IPFilter que están en uso, realice los siguientes pasos.

1. **Inicie sesión en la zona global del nodo 1 como `mcinstall` y asuma el rol `root`.**

   Para obtener instrucciones sobre el inicio de sesión en Oracle ILOM, consulte la *Guía de administración de Oracle MiniCluster S7-2*.

```
% ssh mcinstall@mc4-n1
Password: ***************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: ***************
#
```

2. **Compruebe la configuración de IPFilter.**

   Asegúrese de que las reglas del archivo `/etc/ipf/ipf.conf` coincidan con la siguiente salida de la pantalla.

```
# cat /etc/ipf/ipf.conf
block in log on all
block out log on ipmppub0 all
pass in quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 443 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1159 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1158 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port 5499 >< 5550 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1522 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1523 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp/udp from any to any port = domain keep state
pass in quick on ipmppub0 proto icmp icmp-type echo keep state
pass out quick on ipmppub0 proto icmp icmp-type echo keep state
pass in quick on ipmppub0 proto udp from any to any port = 123 keep state
pass out quick on ipmppub0 proto udp from any to any port = 123 keep state
block return-icmp in proto udp all
```

3. **Verifique que todos servicios IPF estén en línea.**

```
# svcs | grep svc:/network/ipfilter:default
online         22:13:55 svc:/network/ipfilter:default
# ipfstat -v
bad packets:            in 0    out 0
 IPv6 packets:          in 0 out 0
 input packets:         blocked 2767 passed 884831 nomatch 884798 counted 0 short 0
output packets:         blocked 0 passed 596143 nomatch 595516 counted 0 short 0
 input packets logged:  blocked 0 passed 0
output packets logged:  blocked 0 passed 0
 packets logged:        input 0 output 0
 log failures:          input 0 output 0
fragment state(in):     kept 0  lost 0  not fragmented 0
fragment reassembly(in):        bad v6 hdr 0     bad v6 ehdr 0  failed reassembly 0
fragment state(out):    kept 0  lost 0  not fragmented 0
packet state(in):       kept 0  lost 0
packet state(out):      kept 0  lost 0
ICMP replies:   0       TCP RSTs sent:  0
Invalid source(in):     0
Result cache hits(in):  0       (out):  0
IN Pullups succeeded:   0       failed: 3462
OUT Pullups succeeded:  0       failed: 0
Fastroute successes:    0       failures:       0
TCP cksum fails(in):    0       (out):  0
IPF Ticks:      92894
Packet log flags set: (0)
        none
```

4. **Asegúrese de que se pueda acceder a las bases de datos y a las aplicaciones sin cambiar las reglas de firewall.**

▼ Verificación del entorno de inicio verificado

El inicio verificado de Oracle Solaris es una función de integridad y antimalware que reduce el riesgo de introducir componentes críticos de núcleo e inicio modificados accidentalmente o maliciosos. Esta función comprueba las firmas criptográficas de fábrica del firmware, del sistema de inicio y del núcleo.

Por defecto, las zonas globales de MiniCluster están configuradas con el inicio verificado de Oracle Solaris. En caso de que desee verificar si el sistema está configurado con el inicio verificado, realice los siguientes pasos.

1. **Inicie sesión en Oracle ILOM en uno de los nodos.**

   Para obtener instrucciones sobre el inicio de sesión en Oracle ILOM, consulte la *Guía de administración de Oracle MiniCluster S7-2*.

2. **Compruebe la configuración del inicio verificado en Oracle ILOM.**

   Asegúrese de que `boot_policy` esté configurado en `warning`.

```
-> show /HOST/verified_boot

 /HOST/verified_boot
    Targets:
        system_certs
        user_certs
```

```
    Properties:
        boot_policy = warning

    Commands:
        cd
        show
```

3. **Compruebe la configuración de la política de inicio verificado.**

   Asegúrese de que `module_policy` esté configurado en `enforce`.

```
-> show /HOST/verified_boot module_policy

  /HOST/verified_boot
    Properties:
        module_policy = enforce
```

4. **Inicie la consola host para acceder a la zona global.**

   Inicie sesión como `mcinstall`.

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

Serial console started.  To stop, type #.

Minicluster Setup successfully configured
mc4-n1 console login: mcinstall
Password: **************
Last login: Tue Jun 28 10:17:38 2016 on rad/47
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall %
```

5. **En la zona global, intente comprobar si el sistema se inició con una configuración de inicio verificado.**

   Busque la cadena `NOTICE: Verified boot enabled; policy=warning` en el archivo `messages`.

```
mcinstall % cat /var/adm/messages | grep Verified
Jun 29 11:39:15 mc4-n1 unix: [ID 402689 kern.info] NOTICE: Verified boot enabled;
 policy=warning
```

▼ Restricción del acceso al almacenamiento compartido

MiniCluster incluye una matriz de almacenamiento con una combinación de unidades SSD y HDD. Las unidades HDD se pueden configurar para proporcionar almacenamiento compartido a las máquinas virtuales.

MiniCluster incluye una función de aislamiento de almacenamiento compartido: un conmutador que facilita el aislamiento del almacenamiento compartido aplicado solo a las zonas globales y de núcleo. Esto ayuda a aislar el entorno de grupo de máquinas virtuales activado para seguridad y conformidad con el fin de impedir el uso compartido de archivos con las zonas globales y de núcleo. De esta manera, se garantiza que los grupos de máquinas virtuales ya no estén conectados a los montajes NFS y que los servicios NFS estén desactivados.

En los entornos altamente seguros, no active el almacenamiento compartido para las máquinas virtuales de base de datos ni para las máquinas virtuales de aplicación. Si se activa el almacenamiento compartido, las máquinas virtuales deben poder acceder al sistema de archivos en modo de solo lectura. Para obtener instrucciones sobre cómo activar o desactivar el almacenamiento compartido, consulte la *Guía de administración de Oracle MiniCluster S7-2* disponible en: `http://docs.oracle.com/cd/E69469_01`.

El directorio `/sharedstore` es el punto de montaje del almacenamiento compartido:

- **Configure el almacenamiento compartido teniendo en cuenta las siguientes recomendaciones en función de las necesidades de seguridad:**
  - Asegúrese de que el almacenamiento compartido no esté disponible para las máquinas virtuales de base de datos ni para las máquinas virtuales de aplicación o de que esté disponible en modo de solo lectura.
  - En despliegues de producción, asegúrese de que las zonas de núcleo no sean accesibles mediante redes públicas ni de manera directa para los clientes. Se deben finalizar todos los accesos directos y usos de servicios almacenamiento compartido desde redes públicas o accesos de cliente. Si hay máquinas virtuales que requieren acceso al sistema de archivos `/sharedstore` mediante NFS, asegúrese de que se proporcione mediante los canales IPSEc/IKE.

Creación de informes de auditoría y de conformidad

En estos temas, se describen las capacidades de creación de informes de auditoría y de conformidad disponibles en MiniCluster:

▼ Verificación de políticas de auditoría

La política de auditoría se configura durante la instalación de las zonas globales y de las zonas no globales en el momento de selección del perfil de conformidad (equivalente a CIS por defecto o PCI-DSS).

Para verificar si las políticas de auditoría están activadas, realice los siguientes pasos.

1. **Inicie sesión en la zona global como `mcinstall` y asuma el rol `root`.**

   Para obtener instrucciones sobre el inicio de sesión en Oracle ILOM, consulte la *Guía de administración de Oracle MiniCluster S7-2*.

```
% ssh mcinstall@mc4-n1
Password: **************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: **************
#
```

2. **Verifique que el servicio de auditoría esté en línea.**

```
# svcs | grep svc:/system/auditd
online         22:14:37 svc:/system/auditd:default
```

3. **Verifique que el plugin de auditoría esté activo.**

```
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile (active)
        Attributes: p_age=0h;p_dir=/var/audit;p_fsize=0;p_minfree=1
```

4. **Verifique las políticas de auditoría activas.**

```
# auditconfig -getpolicy
configured audit policies = argv,cnt,perzone,zonename
active audit policies = argv,cnt,perzone,zonename
```

5. **Verifique que todos los roles se capturen para la política de auditoría `cusa`.**

```
# userattr audit_flags root
cusa:no
# userattr audit_flags mcadmin
fw,fc,fd,ps,lo,ex,ua,as,cusa:no
```

▼ Revisión de logs de auditoría

1. **Inicie sesión en la zona global como `mcinstall` y asuma el rol `root`.**

   Para obtener instrucciones sobre el inicio de sesión en Oracle ILOM, consulte la *Guía de administración de Oracle MiniCluster S7-2*.

```
% ssh mcinstall@mc4-n1
Password: ***************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: ***************
#
```

2. **Use el comando `audit` como se muestra a continuación.**

   Esta es la sintaxis para ver los logs de auditoría:

   `auditreduce -z` *vm_name audit_file_name* `| praudit -s`

```
# cd /var/share/audit
#
# ls
20160628051437.not_terminated.mc4-n1
#
# auditreduce  -z dbvmg1-zone-1-mc4-n1 20160628051437.not_terminated.mc4-n1 | praudit -s
file,2016-06-27 22:58:53.000 -07:00,
header,127,2,AUE_zone_state,,mc4-n1.us.oracle.com,2016-06-27 22:58:53.354 -07:00
subject,mcinstall,root,root,root,root,26272,415120213,9462 65558 mc4-n1.us.oracle.com
text,boot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
header,88,2,AUE_zone_state,na,mc4-n1.us.oracle.com,2016-06-27 23:02:30.767 -07:00
text,reboot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
file,2016-06-27 23:02:30.000 -07:00,
```

Generación de informes de auditoría

Use este procedimiento para generar informes de auditoría para un nodo, o para zonas globales o máquinas virtuales individuales.

1. **Inicie sesión en MCMU como usuario que tiene asignado el rol de auditor.**

   Para obtener información sobre los usuarios y los roles de MCMU, consulte la *Guía de administración de Oracle MiniCluster S7-2*, disponible en: http://docs.oracle.com/cd/E69469_01.

2. **En el panel de navegación, seleccione Configuración de sistema -> Seguridad.**

   Aparecerá la página de revisión de auditoría.

   Nota - Solo los usuarios de MCMU que tienen asignado el rol de auditor pueden acceder a esta página.

3. **Compruebe la sección Estado de agrupación de auditoría.**

   En esta sección, se muestra la cantidad de espacio que se usa y que está disponible para las agrupaciones de auditoría en cada nodo.

4. **Para generar un informe de todo el nodo, haga clic en el botón Generar para uno de los nodos y vaya al Paso 6.**

   También puede generar un informe para una máquina virtual o zona específica. Consulte el Paso 5.

5. **Para generar un informe para una máquina virtual o zona global específica, realice los siguientes pasos.**

a. **Haga clic en el triángulo que aparece junto a un nodo para ampliar la vista.**

b. **Para la máquina virtual o la zona global, haga clic en Generar informe para todos los usuarios.**

6. **En el cuadro de diálogo Registro de auditoría, configure los parámetros del registro de auditoría.**

Estas son las opciones:

- **Completo**: seleccione esta opción si desea un informe que incluya todos los registros de auditoría.
- **Para un período en particular**: seleccione esta opción si desea especificar un período determinado y, a continuación, introduzca las fechas de inicio y de finalización.

7. **Haga clic en uno de los botones de recuperación.**

Estas son las opciones:

- **Recuperar registro de auditoría**: genera un registro de auditoría completo.
- **Recuperar registro de inicio de sesión**: genera actividades de usuario, como inicios de sesión, cierres de sesión y acciones de usuario.

8. **Haga clic en el botón Haga clic aquí y seleccione descargar el archivo XML.**

El archivo XML se puede importar en las aplicaciones de análisis de auditoría, como Oracle Audit Vault.

9. **Haga clic en Cerrar.**

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, el uso de esta se puede activar si es necesario.

Algunas funciones y capacidades de Oracle ILOM no están disponibles cuando se configuran para la operación que cumple con FIPS 140. Se proporciona una lista de esas funciones en la *Guía de seguridad de Oracle ILOM*, en la sección "Funciones no admitidas cuando el modo FIPS está activado".

Consulte también “Conformidad con FIPS-140-2 nivel 1” [44].

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 sitio 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 manera 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.**

2. **Determine si Oracle ILOM está configurado para la 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 se representa mediante 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 procesador de servicio de Oracle ILOM para que se aplique el cambio.

```
-> reset /SP
```

Conformidad con FIPS-140-2 nivel 1

Las aplicaciones criptográficas alojadas en MiniCluster dependen de la función de estructura criptográfica de Oracle Solaris, que está validada para la 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 nivel de núcleo y espacio de usuario. Estos módulos de biblioteca proporcionan funciones de cifrado, descifrado, hash, 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 objetos OpenSSL incluido en Oracle Solaris está validado para la 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, que son proveedores de FIPS 140-2, se ejecutan en modos que cumplen con FIPS 140, 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) [43].

En esta tabla, se muestran los algoritmos aprobados por FIPS que admite Oracle Solaris en MiniCluster.

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 claves 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 PKCS #1.5 de RSA: 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

Clave o CSP	Número de certificado	
Estándar de hash seguro (SHS)		
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	#1425	#1596
Autenticación de mensajes basada en hash (con claves)		
HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	#1425	#1596
Generadores de números aleatorios		
Generador de números aleatorios FIPS 186-2 swrand	#1154	#1222
Generador de números aleatorios FIPS 186-2 n2rng	#1152	#1226

Oracle Solaris ofrece dos proveedores de algoritmos criptográficos validados para FIPS 140-2 nivel 1.

- 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, hash, 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 de objetos 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 de 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 SSH de Solaris. Debido a que los módulos del proveedor FIPS 140-2 hacen un uso intensivo de la CPU, no están activados por defecto. Como administrador, usted 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 llamado *Using a FIPS 140 Enabled System in Oracle Solaris 11.2* (Uso de un sistema activado para FIPS 140 en Oracle Solaris 11.2), disponible en la sección Protección del sistema operativo Oracle Solaris 11 en: `http://docs.oracle.com/cd/E36784_01`.

Evaluación de la conformidad de seguridad

En los siguientes temas, se describen la función de referencias de seguridad de MiniCluster:

Referencias de conformidad de seguridad

Cuando se instala el sistema, se selecciona un perfil de seguridad (equivalente a CIS, PCI-DSS o DISA-STiG) y el sistema se configura automáticamente para cumplir con ese perfil de seguridad. Para garantizar que el sistema continúe funcionando de acuerdo con los perfiles de seguridad, MCMU proporciona los medios para ejecutar las referencias de seguridad y para acceder a los informes de referencia. Puede administrar las referencias por medio de la BUI y la CLI de MCMU.

La ejecución de referencias de seguridad ofrece los siguientes beneficios:

- Le permite evaluar el estado de seguridad actual de las máquinas virtuales de aplicación y de base de datos.
- Las pruebas de conformidad de seguridad admiten los estándares equivalentes a CIS (por defecto), PCI-DSS y DISA-STiG en función del nivel de seguridad que se configuró durante la instalación.
- Las pruebas de conformidad de seguridad se ejecutan automáticamente cuando el sistema se inicia y se pueden ejecutar a petición o en intervalos programados.
- Solo los administradores principales de MCMU tienen acceso a las puntuaciones y los informes de conformidad, a los cuales pueden acceder fácilmente desde la BUI de MCMU.
- Los informes de conformidad proporcionan recomendaciones para la corrección de errores.

Nota - Actualmente, el perfil DISA-STIG está en etapa de revisión. Solo utilice este perfil para uso experimental en entornos no productivos.

Programación de una referencia de conformidad de seguridad (BUI)

Realice el siguiente procedimiento para programar una referencia de seguridad por medio de la BUI de MCMU. Si desea usar la CLI de MCMU en su lugar, consulte la *Guía de administración de Oracle MiniCluster S7-2*.

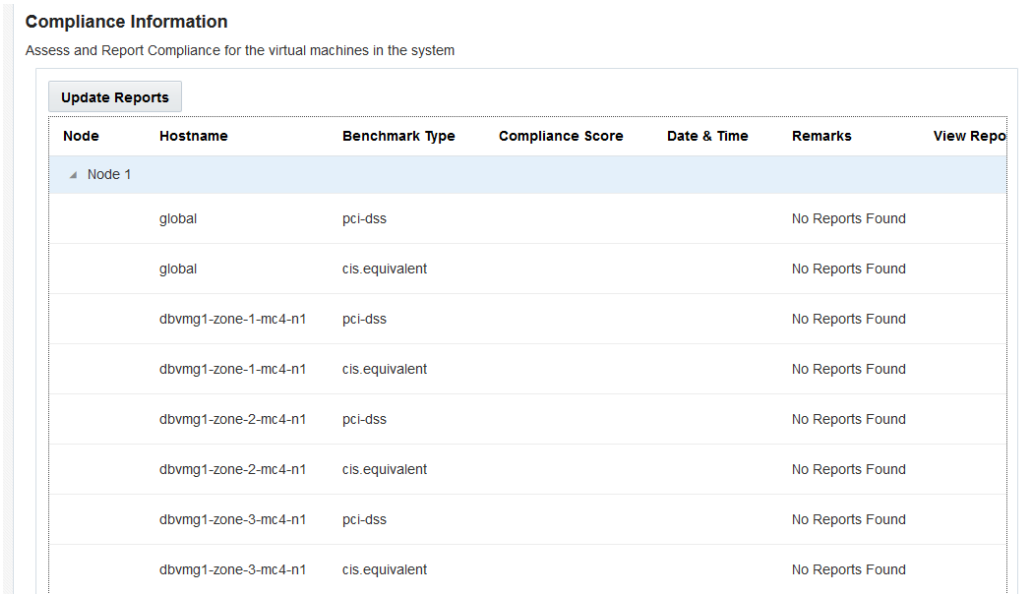
1. **Inicie sesión en la BUI de MCMU como administrador principal.**

   Para obtener instrucciones, consulte la *Guía de administración de Oracle MiniCluster S7-2*.

2. **En la página Inicio, desplácese hacia abajo hasta el panel Información de conformidad.**

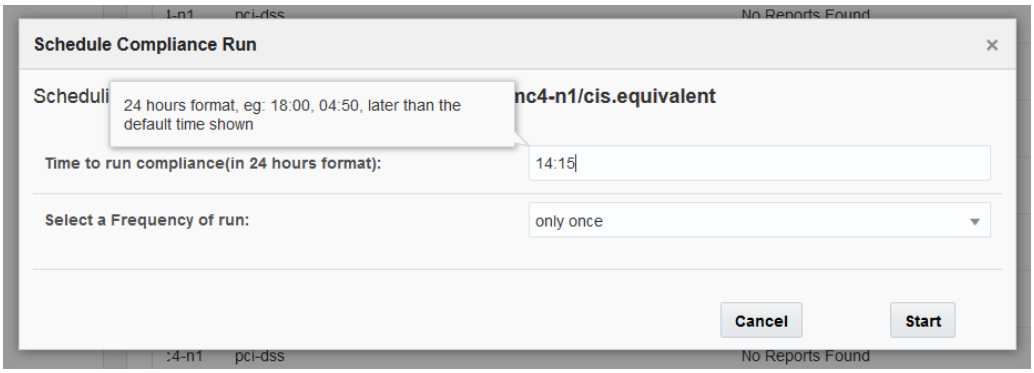
3. **Haga clic en un nodo para ver los detalles.**

   Cada zona y cada máquina virtual se configuran con un perfil de seguridad (ya sea PCI-DSS o equivalente a CIS). Cuando programe una referencia, seleccione una referencia que corresponda al perfil de seguridad del componente.



4. **Desplácese hacia la derecha y haga clic en el botón Programar para una de las máquinas virtuales.**

Aparecerá la página de ejecución de programa de evaluación de conformidad.



5. **Especifique la hora y la frecuencia y, luego, haga clic en Iniciar.**

   Después de que se ejecute la prueba de conformidad de seguridad a la hora programada, abra el informe. Consulte Visualización de informes de referencias (BUI) [49].

▼ Visualización de informes de referencias (BUI)

Estos son los resultados de conformidad aceptables:

	Equivalente a CIS	PCI-DSS
Zonas globales	El 88 % aproximadamente	El 88 % aproximadamente
Máquinas virtuales	El 90 % aproximadamente	El 93 % aproximadamente

Estos son los resultados conocidos de pruebas de conformidad con fallos debido a problemas de Oracle Solaris:

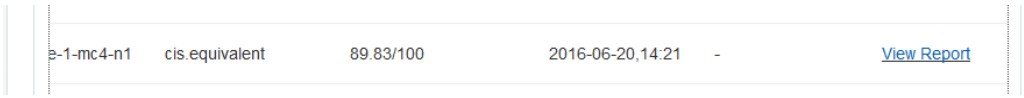
- Integridad de paquetes (core os, rad-python)
- GDM
- Daemon de enrutamiento
- Direcciones de bucle de retorno SSH: la mitigación no soluciona el problema
- Servicios de nombres que no reconocen DNS
- Cliente LDAP

Estos son los resultados conocidos de pruebas de conformidad con fallos debido a problemas con la configuración requerida por el cliente de MiniCluster:

- Servicios de cliente NFS: lo servicios seleccionados deben estar disponibles
- Configuración de contraseña de eeprom: configuración opcional

1. **Inicie sesión en la BUI de MCMU.**
2. **En la página Inicio, desplácese hacia abajo hasta el panel Información de conformidad.**
3. **Haga clic en Actualizar informes.**

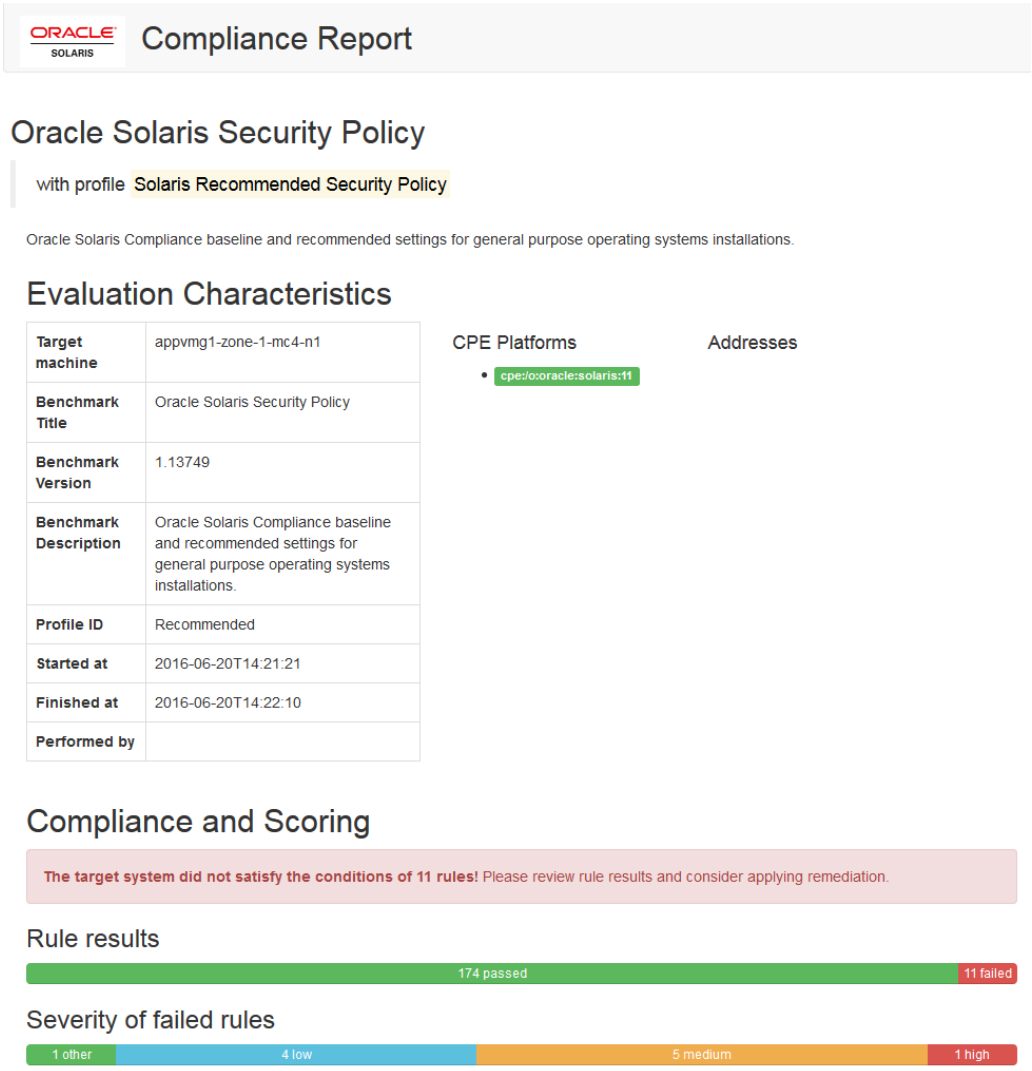
   El proceso de actualización tardará un minuto aproximadamente en completarse.
4. **Expanda la información del nodo e identifique el informe de conformidad.**



5. **Desplácese hacia la derecha y haga clic en Ver informe.**

   Aparecerá el informe de referencia.

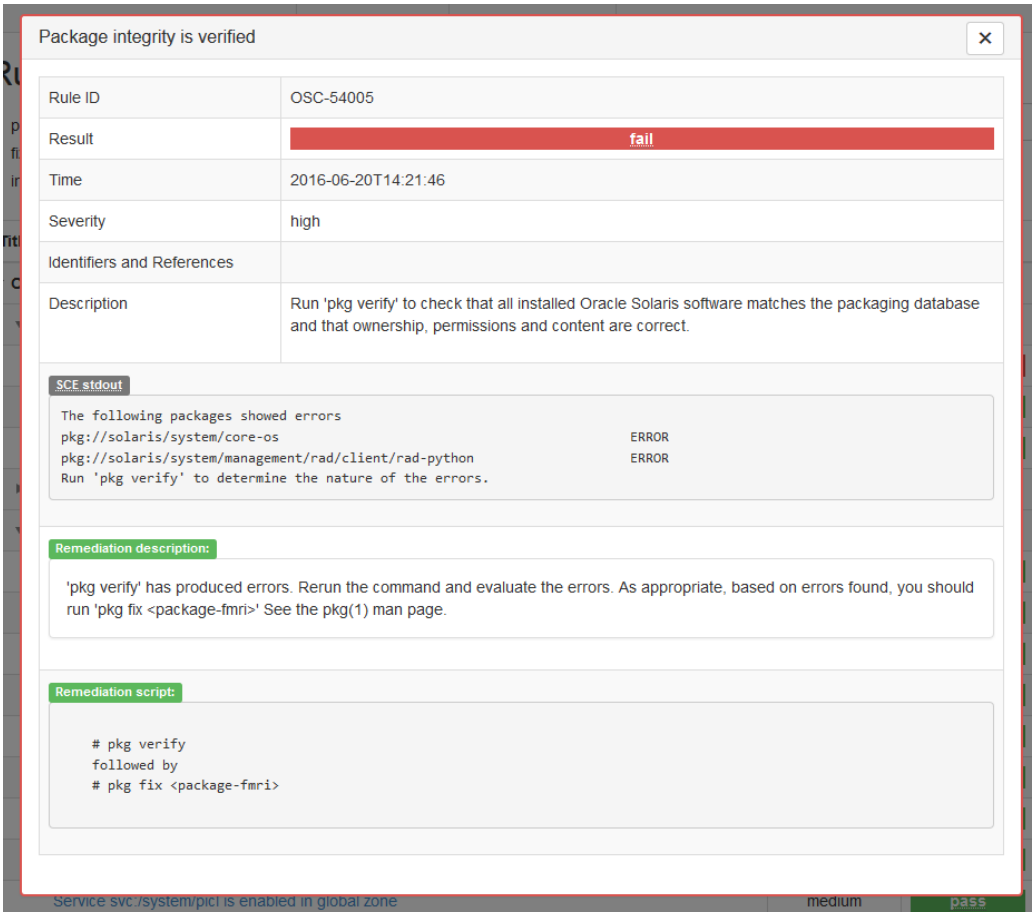
En la visión general de regla, puede seleccionar los tipos de prueba que desea mostrar en función de los resultados. También puede especificar una cadena de búsqueda en el campo de búsqueda.



6. **En función del informe, puede verificar los controles de seguridad, las puntuaciones de conformidad, las anomalías y los procesos de corrección de errores.**

7. **Haga clic en el nombre de una prueba para obtener detalles y la información de corrección de errores recomendada.**

Nota - Puede mostrar todos los detalles de todas las pruebas haciendo clic en Mostrar todos los detalles de resultado en la parte inferior del informe.



Descripción de los controles de seguridad del servidor SPARC S7-2

En estos temas, se describen los controles de seguridad para el hardware y el entorno de OpenBoot.

Descripción de la seguridad del hardware

El aislamiento físico y el control de acceso son la base para crear la arquitectura de seguridad. Asegurarse de que el servidor físico esté instalado en un entorno seguro permite protegerlo contra el acceso no autorizado. Asimismo, el registro de todos los números de serie ayuda a prevenir el riesgo de robo, reventa o cadena de suministro (es decir, la inserción de componentes falsificados o peligrosos en la cadena de suministro de la organización).

En estas secciones, se proporcionan directrices generales de seguridad de hardware para MiniCluster.

Restricciones de acceso

- Instale servidores y equipos similares en una habitación cerrada con llave y de acceso restringido.
- Si el equipo se instala en un rack que tiene una puerta con llave, cierre siempre la puerta hasta que se tenga que reparar algún componente dentro del rack. Cerrar las puertas también restringe el acceso a dispositivos de conexión en caliente o de intercambio en caliente.
- 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 al 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 switches de red pueden tener conexiones USB. El acceso físico es un método más seguro para acceder a un componente, ya que elimina la posibilidad de ataques basados en red.
- Conecte la consola a un KVM externo para hacer posible el acceso remoto a la consola. Generalmente, los dispositivos KVM son compatibles con la autenticación de doble factor, el control de acceso centralizado y la auditoría. Para obtener más información sobre las directrices de seguridad y las mejores prácticas para KVM, consulte la documentación incluida con el dispositivo KVM.

Números de serie

- Mantenga un registro de los números de serie de todo el hardware.
- 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 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 una emergencia del sistema. Los documentos impresos podrían ser su única prueba para demostrar la propiedad.

Los lectores inalámbricos de identificación por radiofrecuencia (RFID) pueden simplificar aún más el seguimiento de activos. Las notas del producto de Oracle *Cómo realizar un seguimiento de los activos del sistema Oracle Sun mediante RFID* están disponibles en:

`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf`

Unidades de disco duro

Por lo general, las unidades de disco duro se usan para almacenar información confidencial. Para proteger esta información contra la divulgación no autorizada, sanee los discos duros antes de reutilizarlos, retirarlos o desecharlos.

- Use herramientas de borrado de disco, como el comando `format` (1M) de Oracle Solaris, para borrar por completo todos los datos del disco duro.
- Se recomienda a las organizaciones que consulten 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

  http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf

Restricción del acceso a OpenBoot

En estos temas, se describe cómo restringir el acceso desde el símbolo del sistema de OpenBoot.

Para obtener instrucciones sobre cómo configurar una contraseña para OpenBoot, consulte Configuración de contraseñas de EEPROM [28].

- Acceso al símbolo del sistema de OpenBoot [55]
- Comprobación de inicios de sesión con error [56]
- Suministro de un banner de encendido [56]

Para obtener información sobre la configuración de las variables de seguridad de OpenBoot, consulte la documentación de OpenBoot en:

http://www.oracle.com/goto/openboot/docs

▼ Acceso al símbolo del sistema de OpenBoot

En este procedimiento, se describe cómo acceder al símbolo del sistema de OpenBoot en los nodos de cálculo de MiniCluster para configurar los controles de seguridad.

Debe apagar el sistema para acceder al símbolo del sistema de OpenBoot. Realice los procedimientos adecuados para apagar las máquinas virtuales correctamente, como se describe en la *Guía de administración de Oracle MiniCluster S7-2*.

1. **Inicie sesión en Oracle ILOM en un nodo y ejecute el siguiente comando.**

```
-> set /HOST/bootmode script="setenv auto-boot? false
-> start /HOST/console
```

Inicie sesión en la consola host con el usuario `mcinstall` y ejecute `su` para `root`.

2. **Una vez que se hayan apagado todas las máquinas virtuales, con el rol root, detenga la zona global.**

```
# init 0
.
.
.
```

```
{0} ok
```

Comprobación de inicios de sesión con error

1. **Determine si alguien intentó acceder al entorno de OpenBoot y no pudo, mediante el parámetro `security-#badlogins`, como en el siguiente ejemplo.**

   ```
   {0} ok printenv security-#badlogins
   ```

   Si este comando devuelve un valor mayor que Ø, se registró un intento de acceso fallido al entorno de OpenBoot.

2. **Restablezca el parámetro escribiendo el siguiente comando.**

   ```
   {0} ok setenv security-#badlogins 0
   ```

Suministro de un banner de encendido

Si bien no se trata de un control exploratorio ni preventivo directo, un banner se puede usar por los siguientes motivos:

- Transmitir propiedad.
- Advertir a los usuarios sobre el uso aceptable del servidor.
- Indicar que el acceso o las modificaciones a los parámetros de OpenBoot están restringidos a personal autorizado.

- **Use los siguientes comandos para activar un mensaje de advertencia personalizado.**

  ```
  {0} ok setenv oem-banner banner-message
  {0} ok setenv oem-banner? true
  ```

  El mensaje del banner puede tener hasta 68 caracteres. Se aceptan todos los caracteres imprimibles.

Índice

V