Guía de seguridad de Oracle® Fabric OS 1.0.2

Referencia: E74814-02
Noviembre de 2016

Referencia: E74814-02

Copyright © 2016, Oracle y/o sus filiales. Todos los derechos reservados.

Este software y la documentación relacionada están sujetos a un contrato de licencia que incluye restricciones de uso y revelación, y se encuentran protegidos por la legislación sobre la propiedad intelectual. A menos que figure explícitamente en el contrato de licencia o esté permitido por la ley, no se podrá utilizar, copiar, reproducir, traducir, emitir, modificar, conceder licencias, transmitir, distribuir, exhibir, representar, publicar ni mostrar ninguna parte, de ninguna forma, por ningún medio. Queda prohibida la ingeniería inversa, desensamblaje o descompilación de este software, excepto en la medida en que sean necesarios para conseguir interoperabilidad según lo especificado por la legislación aplicable.

La información contenida en este documento puede someterse a modificaciones sin previo aviso y no se garantiza que se encuentre exenta de errores. Si detecta algún error, le agradeceremos que nos lo comunique por escrito.

Si este software o la documentación relacionada se entrega al Gobierno de EE.UU. o a cualquier entidad que adquiera las licencias en nombre del Gobierno de EE.UU. entonces aplicará la siguiente disposición:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Este software o hardware se ha desarrollado para uso general en diversas aplicaciones de gestión de la información. No se ha diseñado ni está destinado para utilizarse en aplicaciones de riesgo inherente, incluidas las aplicaciones que pueden causar daños personales. Si utiliza este software o hardware en aplicaciones de riesgo, usted será responsable de tomar todas las medidas apropiadas de prevención de fallos, copia de seguridad, redundancia o de cualquier otro tipo para garantizar la seguridad en el uso de este software o hardware. Oracle Corporation y sus subsidiarias declinan toda responsabilidad derivada de los daños causados por el uso de este software o hardware en aplicaciones de riesgo.

Oracle y Java son marcas comerciales registradas de Oracle y/o sus subsidiarias. Todos los demás nombres pueden ser marcas comerciales de sus respectivos propietarios.

Intel e Intel Xeon son marcas comerciales o marcas comerciales registradas de Intel Corporation. Todas las marcas comerciales de SPARC se utilizan con licencia y son marcas comerciales o marcas comerciales registradas de SPARC International, Inc. AMD, Opteron, el logotipo de AMD y el logotipo de AMD Opteron son marcas comerciales o marcas comerciales registradas de Advanced Micro Devices. UNIX es una marca comercial registrada de The Open Group.

Este software o hardware y la documentación pueden proporcionar acceso a, o información sobre contenidos, productos o servicios de terceros. Oracle Corporation o sus filiales no son responsables y por ende desconocen cualquier tipo de garantía sobre el contenido, los productos o los servicios de terceros a menos que se indique otra cosa en un acuerdo en vigor formalizado entre Ud. y Oracle. Oracle Corporation y sus filiales no serán responsables frente a cualesquiera pérdidas, costos o daños en los que se incurra como consecuencia de su acceso o su uso de contenidos, productos o servicios de terceros a menos que se indique otra cosa en un acuerdo en vigor formalizado entre Ud. y Oracle.

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

Seguridad de Oracle Fabric OS 7
Principios de seguridad 7
Mantener el software y las actualizaciones al día 7
Restringir el acceso de red a los servicios críticos 7
Seguir el principio de privilegios mínimos 8
Supervisar la actividad del sistema 8
Mantenerse al día con la información de seguridad más reciente 8
Seguridad del usuario 8
Cuentas de usuario 8
Criterios para contraseñas de cuentas de usuario 9
▼ Definición de una seguridad alta para las contraseñas de usuarios 10
▼ Agregación de un usuario y asignarle el privilegio adecuado 10
Bloqueo del acceso de usuarios no registrados 11
Controles de acceso de la red 11
Configuración de SNMP 11
Supervisión de la actividad del sistema 12

Seguridad de Oracle Fabric OS

En este documento, se proporcionan directrices generales de seguridad para Oracle Fabric OS 1.0.2. Esta información está destinada a administradores de red con experiencia y proporciona directrices generales e instrucciones específicas para mejorar la seguridad.

Consulte estas guías para conocer las directrices de seguridad de otros productos relacionados:

- *Guía de seguridad de Oracle Fabric Manager 5.0.2*
- *Guía de seguridad de hardware de switches Oracle InfiniBand EDR y sistemas de E/S virtualizada*

En estos temas, se explican las directrices de seguridad para Oracle Fabric OS 1.0.2.

- "Principios de seguridad" [7]
- "Seguridad del usuario" [8]
- "Controles de acceso de la red" [11]
- "Supervisión de la actividad del sistema" [12]

Principios de seguridad

En estos temas, se describen los principios fundamentales necesarios para utilizar cualquier aplicación de manera segura.

Mantener el software y las actualizaciones al día

Manténgase al día con la versión de Oracle Fabric OS que ejecute. Puede encontrar versiones actuales del software para descargar en My Oracle Support (`https://support.oracle.com`).

Restringir el acceso de red a los servicios críticos

Mantenga Oracle Fabric OS en dispositivos que se encuentran en una red de gestión segura. Los dispositivos no deben tener acceso a Internet.

Seguir el principio de privilegios mínimos

Otorgue al usuario o administrador el menor privilegio necesario para completar la tarea que se va a realizar. Oracle Fabric OS tiene varios roles que pueden otorgarse a los usuarios. Estos roles otorgan diferentes tipos y cantidades de privilegios.

Supervisar la actividad del sistema

Supervise la actividad del sistema para determinar el funcionamiento de Oracle Fabric OS y para determinar si está registrando una actividad inusual.

Mantenerse al día con la información de seguridad más reciente

Puede acceder a varios orígenes de información de seguridad:

- Para obtener información de seguridad y alertas para una gran variedad de productos de software, consulte `http://www.us-cert.gov`.
- Ejecute la versión más actual del software de Oracle Virtual Networking y consulte su documentación.

Seguridad del usuario

En los siguientes temas, se describen las directrices de seguridad que se deben seguir para Oracle Fabric OS.

Cuentas de usuario

El sistema incluye dos cuentas de gestión por defecto. Aplique contraseñas complejas para esas cuentas mediante políticas.

- `root`: permite obtener acceso administrativo completo al Oracle Fabric OS basado en Linux subyacente. Las credenciales de seguridad son controladas por Oracle Enterprise Linux 6.7 (UEK 4).
- `admin`: permite obtener acceso administrativo a la seguridad y a las herramientas de gestión de Oracle Fabric OS, incluso la capacidad para crear cuentas de usuario. Estos usuarios tienen acceso a la configuración del chasis, pero no pueden volver a definir la configuración

de Linux. Oracle Fabric OS admite el endurecimiento con contraseñas a través del comando `set system password`. Use el procedimiento que se indica a continuación para evitar que los atacantes creen usuarios en el sistema de forma tal que se aprovechen de estas cuentas.

Para evitar el uso compartido de cuentas y contraseñas, proporcione a cada usuario de Oracle Fabric OS un nombre de usuario y una contraseña únicos, y asígneles el rol adecuado según sus tareas.

Los usuarios de Oracle Fabric OS no tienen permitido modificar nada en el nivel de Linux. Se admiten cinco tipos de rol para los usuarios de Oracle Fabric OS:

- Administrador: superusuario. Permite la creación, la edición y la gestión de Oracle Fabric OS.
- Red: permite la creación, la edición y la supresión de perfiles del servidor, vNIC, tarjetas y puertos Ethernet y calidad de servicio de red.
- Operador: permite el acceso de solo lectura, incluso todos los comandos `show`.
- Servidor: permite la creación, la edición y la supresión de perfiles del servidor, además de la capacidad para operar el servidor físico.
- Almacenamiento: permite la creación, edición y supresión de perfiles del servidor para vHBA y puertos y tarjetas de E/S de canal de fibra.

Nota - Siempre asigne a los usuarios el menor privilegio requerido para sus tareas.

Criterios para contraseñas de cuentas de usuario

Se solicita una contraseña a los usuarios para la autenticación. Antes de crear contraseñas de usuario, establezca la seguridad de las contraseñas especificando criterios con el comando `set system password-strength` en Oracle Fabric OS. Utilice los siguientes criterios:

- `min-length`: establece la cantidad mínima de caracteres permitidos para la cadena de contraseña.
- `min-lower-case`: establece la cantidad mínima de letras en minúscula requeridas para las contraseñas.
- `min-number`: establece la cantidad mínima de números requeridos para las contraseñas.
- `min-special`: establece la cantidad mínima de caracteres especiales requeridos para las contraseñas.
- `min-upper-case`: establece la cantidad mínima de letras en mayúscula requeridas para las contraseñas.

Nota - Al instalar el sistema, determine los criterios de seguridad de las contraseñas antes de crear contraseñas de usuarios. Configure la seguridad de contraseñas de usuarios para adherirse a la política de seguridad de la organización.

Definición de una seguridad alta para las contraseñas de usuarios

En este ejemplo, la contraseña para cuentas de usuario locales que no están por defecto deben tener al menos ocho caracteres con un mínimo de tres letras en minúscula, dos números, dos caracteres especiales y una letra en mayúscula.

1. **Inicie sesión en Oracle Fabric OS.**

   Consulte "Inicio de sesión en Oracle Fabric OS (SSH)" de *Guía de administración de Oracle Fabric OS 1.0.2*..

2. **Configure la seguridad de las contraseñas.**

   ```
   [OFOS] set system password-strength -min-length=8 -min-lower-case=3 -min-number=2 -min-special=2 -
   min-upper-case=1
   ```

   Para obtener más información sobre el uso de Oracle Fabric OS para establecer una contraseña segura, consulte "Configuración de seguridad de las contraseñas del sistema" de *Guía de administración de Oracle Fabric OS 1.0.2* o "set system" de *Referencia de comandos de Oracle Fabric OS 1.0.2*.

Agregación de un usuario y asignarle el privilegio adecuado

Debe tener privilegios de administrador para agregar a usuarios y asignarles roles.

Para obtener más información sobre la agregación de usuarios, consulte "Privilegios de visualización de un usuario" de *Guía de administración de Oracle Fabric OS 1.0.2* o "user" de *Referencia de comandos de Oracle Fabric OS 1.0.2*.

1. **Inicie sesión en la GUI de Oracle Fabric Manager.**

   Consulte "Inicio de sesión en Oracle Fabric Manager (GUI)" de *Guía de administración de Oracle Fabric OS 1.0.2*.

2. **En la GUI, agregue a un usuario y asígnele un rol.**

   Consulte "Asignación de un rol a un usuario" de *Guía de administración de Oracle Fabric Manager 5.0.2*. Para obtener una lista de roles, consulte "Usuarios y roles" de *Guía de administración de Oracle Fabric OS 1.0.2*.

3. **En la GUI de Oracle Fabric Manager o en Oracle Fabric OS, verifique que el usuario se haya configurado correctamente.**

   ```
   [OFOS] show user frank
   ```

```
name        role             descr
---------------------------------
frank       administrators
1 record displayed
```

4. **En Oracle Fabric OS, pruebe la nueva cuenta de usuario.**

```
[OFOS] quit
Connection to 192.168.8.133 closed.
$ ssh frank@192.168.8.133
Password:
[OFOS] pwd
/home/frank
```

Bloqueo del acceso de usuarios no registrados

Por defecto, los usuarios no registrados no pueden acceder a Oracle Fabric OS. Un usuario registrado tiene un rol de usuario definido en Oracle Fabric OS, además de la cuenta de usuario subyacente. Si se cambia alguna opción de configuración para permitir usuarios no registrados, un usuario con una cuenta que se puede autenticar en el host podrá iniciar sesión en Oracle Fabric OS y recibir el rol de operador (acceso de solo lectura). Cuando se bloquean usuarios no registrados, es posible que ocurra la autenticación de host de un usuario no registrado, pero Oracle Fabric OS denegará el acceso de ese usuario y, como resultado, indicará que la autenticación falló.

Para verificar este nivel de seguridad, asegúrese de que el acceso de usuarios no registrados esté desactivado.

Controles de acceso de la red

El tejido anuncia los siguientes puertos:

- **Puerto 22 ssh**: gestión de la CLI.
- **Puerto 8080 http**: acceso de cliente de Oracle Fabric Manager sin cifrar.
- **Puerto 7443 https**: acceso de cliente de Oracle Fabric Manager cifrado.
- **Puerto 161 SNMP**: supervisión de SNMP.
- **Puerto 6522**: permite que Oracle Fabric Manager detecte dispositivos Fabric Interconnect.

Configuración de SNMP

Oracle Fabric OS admite SNMPv3. Siempre use SNMPv3 y el protocolo de autenticación correcto.

Supervisión de la actividad del sistema

Los archivos log se almacenan en el directorio `/log`. Los diversos subsistemas tienen entradas de archivos log separadas, incluso `dmesg`.

Los mensajes estándar `syslog` van al archivo `user.log`, donde ocurren la rotación de logs y el archivo automático para hasta 10 archivos gzip:

Nota - Supervise archivos log con regularidad y archívelos para facilitar las revisiones de seguridad en caso de una infracción de seguridad.

---

1. **Consulte la actividad de inicio de sesión de la CLI.**

   ```
   [OFOS] more /log/cli.log
   ```

2. **Consulte los mensajes de inicio diariamente.**

   ```
   [OFOS] more /log/dmesg
   ```

Para obtener información detallada sobre los archivos log, consulte “Resolución de problemas de archivos log del sistema” de *Guía de administración de Oracle Fabric OS 1.0.2*.