Guía de seguridad de Oracle ILOM

Versiones de firmware 3.0, 3.1 y 3.2

Referencia: E40357-03
Agosto de

Contenido

Uso de esta documentación

- **Descripción general**: la *Guía de seguridad de Oracle ILOM* proporciona información web y de la CLI sobre las directrices de las tareas de seguridad de Oracle ILOM. Utilice esta guía junto con otras guías de la biblioteca de documentación de Oracle ILOM.
- **Destinatarios**: esta guía está destinada a técnicos, administradores de sistema, proveedores de servicios Oracle autorizados y usuarios con experiencia en la gestión de hardware de sistemas.
- **Conocimientos necesarios**: experiencia en la configuración y la gestión de servidores Oracle.

Biblioteca de documentación del producto

Esta guía y otra documentación relacionada están disponibles en las bibliotecas de documentación de Oracle ILOM en http://www.oracle.com/goto/ILOM/docs.

Acceso a My Oracle Support

Los clientes de Oracle disponen de acceso a asistencia técnica electrónica mediante 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 es una persona con discapacidad auditiva.

Accesibilidad a la documentación

Para obtener información sobre el compromiso de Oracle con la accesibilidad, visite el sitio web del Programa de Accesibilidad de Oracle en http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Comentarios

Puede escribir comentarios sobre esta documentación en:

http://www.oracle.com/goto/docfeedback

Funciones de seguridad por versión de firmware de Oracle ILOM

Utilice la siguiente tabla para identificar la versión de firmware en la que comenzó a estar disponible una función de seguridad de Oracle ILOM.

Disponibilidad de versión de firmware	Función de seguridad	Para obtener detalles, consulte:
Todas	Autenticación y autorización	■ "Protección del acceso de usuario de Oracle ILOM" [23]
Todas	Conexión de gestión segura dedicada	■ "Protección de la conexión de gestión física" [13] ■ "Mantenimiento de una conexión de gestión segura" [53]
Todas	Puertos de red preconfigurados y cifrados	■ "Puertos de red y servicios preconfigurados" [18]
Todas	Gestión segura de IPMI 2.0	■ "Configuración del acceso a la gestión de IPMI para máxima seguridad" [49]
Todas	Configuración de cifrado de clave de shell seguro	■ Uso de claves de servidor para cifrar conexiones SSH [44] ■ Cómo agregar claves SSH a cuentas de usuario para la autenticación de CLI automatizada [46]
Todas	Gestión segura de SNMP 3.0	■ "Configuración del acceso a la gestión de SNMP para máxima seguridad" [47]
Todas	Protocolos y certificados SSL	■ Carga de una clave privada y un certificado SSL personalizados en Oracle ILOM [39] ■ Obtención de certificados SSL y claves privadas mediante OpenSSL [37] ■ Activación de propiedades de cifrado SSL y TLS más seguro [40]
Todas	Cifrado de consola remota y protocolos seguros	■ "Uso de KVMS remoto de manera segura" [57]
3.0.4 y versiones posteriores	Configuración de bloqueo de host KVMS	■ Bloqueo del acceso al host al salir de una sesión de KVMS [32]
3.0.4 y versiones posteriores	Configuración de timeout de sesión	■ Establecimiento de un intervalo de timeout para sesiones web inactivas [41] ■ Establecimiento de un intervalo de timeout para sesiones de CLI inactivas [43]

Disponibilidad de versión de firmware	Función de seguridad	Para obtener detalles, consulte:
3.0.12 y versiones posteriores	Sesiones autenticadas de interconexión de host local	■ "Acceso de interconexión a host autenticado y preferible" [54]
3.0.8 y versiones posteriores	Configuración de banner de inicio de sesión	Acceso seguro al sistema con banner de inicio de sesión (3.0.8 y posterior) [34]
3.0.8 a 3.1.2	Acceso seguro de WS-Management	■ "Configuración del acceso a WS-Management para máxima seguridad" [52]
3.1.0 y versiones posteriores	Log de auditoría independiente	■ "Supervisión de eventos de auditoría para encontrar acceso no autorizado" [63]
3.1.0 y versiones posteriores	Comprobación de presencia de seguridad física	■ "Presencia de seguridad física para el restablecimiento de la contraseña predeterminada de la cuenta `root`" [61]
3.2.4 y versiones posteriores	Propiedad configurable de IPMI 1.5	■ "Configuración del acceso a la gestión de IPMI para máxima seguridad" [49]
3.2.4 y versiones posteriores	Versiones 1.1 y 1.2 del protocolo TLS	■ Activación de propiedades de cifrado SSL y TLS más seguro [40]
3.2.4 y versiones posteriores	Recuento de sesiones de KVMS	■ Limitación de sesiones de KVMS visibles para Remote System Console Plus (3.2.4 o posterior) [33]
3.2.4 y versiones posteriores	Compatibilidad de cifrado de cumplimiento con FIPS	■ "Cómo decidir si se debe configurar el modo FIPS en la implementación" [14] ■ "Funciones no admitidas cuando el modo FIPS está activado" [17] ■ "Consideraciones posteriores a la implementación para proteger el acceso de usuario" [60]

Información de seguridad adicional

Para obtener más información sobre cómo proteger Oracle ILOM, consulte las siguientes secciones de esta guía:

- Listas de comprobación de mejores prácticas de seguridad para Oracle ILOM
- Mejores prácticas de seguridad de implementación para Oracle ILOM
- Mejores prácticas de seguridad posteriores a la implementación para Oracle ILOM

Listas de comprobación de mejores prácticas de seguridad para Oracle ILOM

Oracle Integrated Lights Out Manager (ILOM) es un procesador de servicio (SP) preinstalado en todos los servidores Oracle y en la mayoría de los servidores Sun heredados. Los administradores de sistemas usan las interfaces de usuario de Oracle ILOM para realizar tareas de gestión en servidor remoto y operaciones de supervisión de estado del servidor en tiempo real.

Para garantizar que se implementen las mejores prácticas de seguridad para Oracle ILOM en su entorno, los administradores de sistema deberían consultar las tareas de seguridad recomendadas en las siguientes listas de comprobación:

- “Lista de comprobación de seguridad para la implementación del servidor” [9]
- “Lista de comprobación de seguridad posterior a la implementación del servidor” [10]

Información relacionada

- Mejores prácticas de seguridad de implementación para Oracle ILOM .
- Mejores prácticas de seguridad posteriores a la implementación para Oracle ILOM
- Funciones de seguridad por versión de firmware de Oracle ILOM [7]

Lista de comprobación de seguridad para la implementación del servidor

Para determinar qué prácticas de seguridad de Oracle ILOM serían las mejores al planificar la implementación de un nuevo servidor, los administradores de sistema deben consultar la lista de tareas de seguridad recomendadas en la Tabla 1, “Lista de comprobación: cómo configurar la seguridad de Oracle ILOM durante la implementación de un servidor ”, a continuación.

TABLA 1 Lista de comprobación: cómo configurar la seguridad de Oracle ILOM durante la implementación de un servidor

✓	Tarea de seguridad	Versiones de firmware aplicables	Para obtener detalles, consulte:
	Establecer una conexión de gestión dedicada y segura a Oracle ILOM.	Todas las versiones de firmware	■ "Protección de la conexión de gestión física" [13]
	Decidir si el cumplimiento de seguridad de FIPS 140-2 es necesario durante la implementación, o después de ella, o si no es necesario en absoluto.	Versiones de firmware 3.2.4 y posteriores	■ "Cómo decidir si se debe configurar el modo FIPS en la implementación" [14] ■ "Funciones no admitidas cuando el modo FIPS está activado" [17]
	Modificar la contraseña predeterminada proporcionada para la cuenta `root` de administrador preconfigurada.	Todas las versiones de firmware	■ "Cómo evitar la creación de cuentas de usuario compartidas" [24] ■ Modificación de la contraseña predeterminada para la cuenta `root` en el primer inicio de sesión [29]
	Decidir si los servicios preconfigurados de Oracle ILOM y sus puertos de red abiertos se aplican al entorno de destino.	Todas las versiones de firmware	■ "Protección de servicios y puertos de red abiertos" [17]
	Configurar acceso de usuario a Oracle ILOM.	Todas las versiones de firmware	■ "Protección del acceso de usuario de Oracle ILOM" [23] ■ Creación de cuentas de usuario locales con privilegios basados en roles [30]
	Decidir si el acceso al sistema operativo host debe bloquearse al salir de una sesión de KVMS remoto.	Versiones de firmware 3.0.4 y posteriores	■ Bloqueo del acceso al host al salir de una sesión de KVMS [32]
	Decidir si se debe limitar la visualización de sesiones de KVMS remoto iniciadas desde el SP a otros usuarios del SP.	Versiones de firmware 3.2.4 y posteriores	■ Limitación de sesiones de KVMS visibles para Remote System Console Plus (3.2.4 o posterior) [33]
	Decidir si se debe mostrar un mensaje de banner de seguridad durante el inicio de sesión del usuario, o inmediatamente después.	Versiones de firmware 3.0.8 y posteriores	■ Acceso seguro al sistema con banner de inicio de sesión (3.0.8 y posterior) [34]
	Garantizar que se establezcan las propiedades de seguridad máxima para todas las interfaces de usuario de Oracle ILOM.	Todas las versiones de firmware	■ "Configuración de las interfaces de Oracle ILOM para máxima seguridad" [36]

Lista de comprobación de seguridad posterior a la implementación del servidor

Para determinar qué prácticas de seguridad de Oracle ILOM son las mejores para llevar a cabo en los servidores existentes de su entorno, los administradores de sistema deben consultar la lista de tareas de seguridad recomendadas en la Tabla 2, "Lista de comprobación: cómo mantener la seguridad de Oracle ILOM después de implementar un servidor ", a continuación.

TABLA 2 Lista de comprobación: cómo mantener la seguridad de Oracle ILOM después de implementar un servidor

✓	**Tarea de seguridad**	**Versiones de firmware aplicables**	**Para obtener detalles, consulte:**
	Mantener una conexión de gestión segura a Oracle ILOM.	Todas las versiones de firmware	■ "Cómo evitar el acceso no autenticado del dispositivo KCS al host" [54] ■ "Acceso de interconexión a host autenticado y preferible" [54] ■ "Uso de cifrado IPMI 2.0 para proteger el canal" [55]
	Garantizar que las sesiones de KVMS remoto y las sesiones serie basadas en texto se inicien de manera segura desde Oracle ILOM.	Todas las versiones de firmware	■ "Cifrado y comunicación de KVMS remoto" [57] ■ "Protección contra el acceso compartido a KVMS remoto" [58] ■ "Protección contra el acceso compartido a la consola host serie" [59]
	Mantener y realizar un seguimiento del acceso de usuario a Oracle ILOM.	Todas las versiones de firmware	■ "Consideraciones posteriores a la implementación para proteger el acceso de usuario" [60]
	Acciones de seguridad necesarias para restablecer una contraseña perdida para la cuenta `root` de administrador preconfigurada.	Versiones de firmware 3.1 y posteriores	■ "Presencia de seguridad física para el restablecimiento de la contraseña predeterminada de la cuenta `root`" [61]
	Acciones de seguridad necesarias si se debe modificar el modo de cumplimiento con FIPS 140-2 en Oracle ILOM después de implementar el servidor.	Versión de firmware 3.2.4 y posteriores	■ Modificación del modo FIPS posterior a la implementación [64] ■ "Funciones no admitidas cuando el modo FIPS está activado" [17]
	Garantizar que el software y el firmware estén actualizados en el servidor.	Todas las versiones de software	■ "Actualización a las versiones de firmware y software más recientes" [66]

Mejores prácticas de seguridad de implementación para Oracle ILOM

Utilice los siguientes temas para decidir las mejores prácticas de seguridad de Oracle ILOM para utilizar en la implementación del servidor.

Información relacionada

- Listas de comprobación de mejores prácticas de seguridad para Oracle ILOM.
- Mejores prácticas de seguridad posteriores a la implementación para Oracle ILOM
- Funciones de seguridad por versión de firmware de Oracle ILOM [7]

Protección de la conexión de gestión física

Oracle ILOM es una herramienta de gestión fuera de banda (OOB) que utiliza un canal de gestión dedicado para mantener y supervisar los servidores de Oracle. A diferencia de los servidores con herramientas de gestión en banda, los servidores de Oracle incluyen capacidades de gestión remota incorporadas que permiten a los administradores del sistema obtener acceso seguro a Oracle ILOM mediante un conector de red dedicado separado en el procesador de servicio. Aunque la funcionalidad de gestión de Oracle ILOM brinda a los administradores del sistema capacidades específicas para supervisar y gestionar los servidores de Oracle, Oracle ILOM no está diseñado para ser un motor de cálculo de uso general ni se puede acceder a él mediante una conexión de red no segura y no confiable.

Independientemente de que establezca una conexión de gestión física con Oracle ILOM mediante el puerto serie local, el puerto de gestión de red dedicado o el puerto de red de datos estándar, este puerto físico en el servidor o el módulo de supervisión del chasis (CMM) siempre deben estar conectados a una red de confianza interna o a una red privada o de gestión segura

dedicada. Para obtener más directrices para establecer una conexión de gestión física con Oracle ILOM, consulte la siguiente tabla:

Conexión de gestión de puerto física con Oracle ILOM	Hardware de Oracle compatible	Directrices de seguridad de conexión de gestión
Conexión dedicada	■ Servidor (puerto: `NET MGT`) ■ CMM (puerto: `NET MGT`)	Utilice una red interna dedicada para el procesador de servicio (SP) a fin de separarlo del tráfico de la red de datos general. Para obtener más información sobre cómo establecer una conexión de gestión de red dedicada a Oracle ILOM, consulte: ■ Conexión de gestión de red dedicada, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (3.2.x)*
Conexión local	■ Servidor (puerto: `SER MGT`) ■ CMM (puerto: `SER MGT`)	Utilice una conexión de gestión serie local para acceder a Oracle ILOM directamente desde el CMM o el servidor físico. Para obtener más información sobre cómo establecer una conexión de gestión serie local a Oracle ILOM, consulte: ■ Conexión de gestión de red serie local con Oracle ILOM, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (3.2.x)*
Conexión de banda lateral	Servidor (puertos: `NET0`, `NET1`, `NET2` y `NET3`)	Utilice una red de datos Ethernet compartida para acceder al procesador de servicio cada vez que sea necesario para simplificar la organización de cables y la configuración de redes. Para ello, evite tener que utilizar dos conexiones de red separadas. Para obtener más información sobre cómo establecer una conexión de gestión de banda lateral a Oracle ILOM, consulte: ■ Conexión de gestión de banda lateral, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (3.2.x)* **Nota -** La gestión de banda lateral se admite en la mayoría de los servidores de Oracle.

Nota - Para defenderse de los ataques de seguridad, **nunca debe conectar el SP de Oracle ILOM a una red pública**, por ejemplo, Internet. Debe mantener el tráfico de gestión del SP de Oracle ILOM en una red de gestión separada y solamente otorgar acceso a los administradores del sistema.

Cómo decidir si se debe configurar el modo FIPS en la implementación

A partir de la versión 3.2.4 del firmware de Oracle ILOM, la interfaz web y la interfaz de línea de comandos de Oracle ILOM proporcionan un modo configurable para el cumplimiento con los Estándares Federales de Procesamiento de la Información (FIPS, Federal Information

Processing Standards). Cuando este modo está activado, Oracle utiliza algoritmos criptográficos de acuerdo con los estándares de seguridad FIPS 140-2 para proteger los datos valiosos y confidenciales del sistema.

Los administradores del sistema que implementan servidores con el firmware 3.2.4, o una versión posterior, deben decidir si se debe configurar el modo FIPS antes de configurar otras propiedades de Oracle ILOM. De forma predeterminada, el modo de cumplimiento con FIPS en Oracle ILOM está desactivado. Si se cambia el modo de cumplimiento con FIPS, se restablecerán los valores predeterminados de fábrica de todos los datos de configuración.

Para activar el modo de cumplimiento con FIPS en la implementación (antes de configurar las propiedades de Oracle ILOM), consulte Activación del modo FIPS en la implementación [15]. En el caso en que las propiedades de configuración definidas por el usuario ya se hayan establecido en Oracle ILOM y sea necesario modificar la propiedad de FIPS, consulte “Acciones posteriores a la implementación para la modificación del modo FIPS” [64].

▼ Activación del modo FIPS en la implementación

Nota - El modo de cumplimiento con FIPS en Oracle ILOM está representado por las propiedades de condición y estado. La propiedad de condición representa el modo configurado en Oracle ILOM, y la propiedad de estado representa el modo operativo en Oracle ILOM. Cuando la propiedad FIPS State (Condición de FIPS) se modifica, el cambio no afecta al modo operativo (propiedad FIPS Status [Estado de FIPS]) hasta el próximo reinicio de Oracle ILOM.

Antes de empezar

- Las propiedades de condición y estado de FIPS vienen desactivadas de forma predeterminada.
- Cuando FIPS está activado (configurado y operativo) algunas funciones no se admiten en Oracle ILOM. Para obtener una lista de funciones no admitidas cuando FIPS está activado, consulte la Tabla 3, “Funciones no admitidas en Oracle ILOM cuando el modo FIPS está activado”.
- Se necesita el rol Admin (Administrador) (a) para modificar la propiedad FIPS State (Condición de FIPS).
- La propiedad configurable del cumplimiento con FIPS está disponible en Oracle ILOM a partir del firmware 3.2.4 o versiones posteriores. Para las versiones anteriores al firmware 3.2.4, Oracle ILOM no proporciona una propiedad configurable para el cumplimiento con FIPS.
- Cuando se modifican las propiedades de condición y estado del modo FIPS en Oracle ILOM, todos los valores de configuración definidos por el usuario vuelven a los valores de configuración predeterminados de fábrica.

1. **En la interfaz web de Oracle ILOM, haga clic en ILOM Administration (Administración de ILOM) > Management Access (Acceso a gestión) -> FIPS.**

2. **En la página FIPS, realice lo siguiente:**

   a. **Seleccione la casilla de verificación FIPS State (Condición de FIPS) para activar la propiedad de FIPS configurada.**

   b. **Haga clic en Save (Guardar) para aplicar el cambio.**

   Para obtener más información sobre configuración, haga clic en el enlace `More details`.... (Más detalles), en la página web de FIPS.

3. **Para cambiar el estado de modo operativo de FIPS en Oracle ILOM, realice los siguientes pasos para reiniciar Oracle ILOM.**

   a. **En la interfaz web, haga clic en ILOM Administration (Administración de ILOM) -> Maintenance (Mantenimiento) -> SP.**

   b. **En la página de reinicio de SP, haga clic en el botón SP Reset (Reinicio de SP).**

   Una vez que se reinicia Oracle ILOM, sucede lo siguiente:

   - La última condición de FIPS configurada (activado) se aplica en el sistema.
   - Los valores de configuración definidos por el usuario previamente configurados en Oracle ILOM vuelven a los valores predeterminados de fábrica.
   - La propiedad de estado de FIPS se actualiza para reflejar el estado operativo activado actual en Oracle ILOM.

     Para obtener una lista y una descripción completa de los mensajes de estado de FIPS, haga clic en el enlace `More details` (Más detalles) en la página FIPS.
   - Aparece un ícono de escudo de FIPS en el área de la cabecera de la interfaz web.
   - Todas las funciones de FIPS no admitidas se desactivan o eliminan en la interfaz web o la interfaz de línea de comandos.

     Para obtener una lista y una descripción completa de las funciones de FIPS, haga clic en el enlace `More details` (Más detalles) en la página FIPS.

Información relacionada

- “Funciones no admitidas cuando el modo FIPS está activado” [17]
- “Acciones posteriores a la implementación para la modificación del modo FIPS” [64]
- Configuración de propiedades de modo FIPS, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (3.2.x)*

Funciones no admitidas cuando el modo FIPS está activado

Cuando se activa el cumplimiento con FIPS en Oracle ILOM, las siguientes funciones que no cumplen con FIPS 140-2 en Oracle ILOM no se admiten.

TABLA 3 Funciones no admitidas en Oracle ILOM cuando el modo FIPS está activado

Función del modo FIPS no admitida	Descripción
IPMI 1.5	Cuando el modo FIPS está activado y en ejecución en el sistema, la propiedad de configuración de IPMI 1.5 se elimina de la interfaz web y la interfaz de línea de comandos de Oracle ILOM. El servicio de IPMI 2.0 se activa automáticamente en Oracle ILOM. IPMI 2.0 admite tanto el modo que cumple con FIPS como el modo que no cumple con FIPS.
Compatibilidad de firmware para Oracle ILOM System Remote Console	El modo FIPS en Oracle ILOM impide que las versiones anteriores de firmware de Oracle ILOM Remote System Console sean compatibles con las versiones posteriores de firmware de Oracle ILOM Remote System Console. Por ejemplo, la versión de firmware 3.2.4 de cliente Oracle ILOM Remote System Console es compatible con las versiones de firmware 3.2.3 y anteriores de Oracle ILOM Remote System Console. Sin embargo, las versiones de firmware 3.2.2 y anteriores de cliente Oracle ILOM Remote System Console no son compatibles con las versiones de firmware 3.2.4 y posteriores de Oracle ILOM Remote System Console. **Nota -** Esta limitación de compatibilidad de firmware no se aplica a Oracle ILOM Remote System Console Plus. Oracle ILOM Remote System Console Plus se proporciona en los sistemas de procesadores de servicio más nuevos, como los sistemas SPARC T5 y posteriores, o en los sistemas Oracle Server x4-4, x4-8 y posteriores. Oracle ILOM Remote System Console se proporciona en sistemas de procesadores de servicio más antiguos, como SPARC T3 y T4, y en los sistemas Sun Server x4-2/2L/2B y anteriores.
Protocolo ligero de acceso a directorios (LDAP)	Cuando el modo FIPS está activado y en ejecución en el sistema, las propiedades de configuración de LDAP de Oracle ILOM se eliminan automáticamente de la interfaz web y la interfaz de línea de comandos de Oracle ILOM. **Nota -** Los siguientes servicios de autenticación remota se admiten tanto en el modo que cumple con FIPS como en el modo que no cumple con FIPS: Active Directory y LDAP/SSL.
Servicio de autenticación remota telefónica de usuario (RADIUS)	Cuando el modo FIPS está activado y en ejecución en el sistema, las propiedades de configuración de RADIUS de Oracle ILOM se eliminan automáticamente de la interfaz web y la interfaz de línea de comandos de Oracle ILOM. **Nota -** Los siguientes servicios de autenticación remota se admiten tanto en el modo que cumple con FIPS como en el modo que no cumple con FIPS: Active Directory y LDAP/SSL.
DES y MD5 de protocolo simple de administración de redes (SNMP)	Cuando el modo FIPS está activado y en ejecución en el sistema, las propiedades de configuración de SNMP para el protocolo de privacidad DES y el protocolo de autenticación MD5 no se admiten en la interfaz web ni en la interfaz de línea de comandos de Oracle ILOM.

Protección de servicios y puertos de red abiertos

Para garantizar que los servicios y sus respectivos puertos de red estén configurados correctamente en Oracle ILOM, consulte los siguientes temas:

Puertos de red y servicios preconfigurados

Oracle ILOM viene preconfigurado con la mayoría de los servicios activados de forma predeterminada, de modo que su implementación es simple y sencilla. Sin embargo, cada puerto de red de servicio abierto del servidor representa un posible punto de ataque de un usuario malicioso. Por lo tanto, es importante comprender la configuración inicial de Oracle ILOM y su finalidad, y elegir los servicios que son verdaderamente necesarios para un sistema implementado. Para obtener la mayor seguridad, solo active los servicios de Oracle ILOM requeridos.

En la siguiente tabla, se muestran los servicios activados de forma predeterminada en Oracle ILOM.

TABLA 4 Servicios y puertos activados de forma predeterminada

Servicio	Puertos
Redirección de HTTP a HTTPS	80
HTTPS	443
IPMI	623
KVMS remoto para Oracle ILOM Remote Console	5120, 5121, 5122, 5123, 5555, 5556, 7578, 7579
KVMS remoto para Oracle ILOM Remote Console Plus	5120, 5555
Etiqueta de servicio	6481
SNMP	161
Inicio de sesión único	11626
SSH	22

En la siguiente tabla, se muestran los servicios desactivados de forma predeterminada en Oracle ILOM.

TABLA 5 Servicios y puertos desactivados de forma predeterminada

Servicio	Puertos
HTTP	80

Gestión de puertos abiertos y servicios no deseados

Todos los servicios de Oracle ILOM se pueden desactivar, lo que produce el cierre de los respectivos puertos de red abiertos de dichos servicios. Si bien la mayoría de los servicios están activados de forma predeterminada, es posible que desee desactivar algunas funciones o cambiar los valores predeterminados para que el entorno de Oracle ILOM sea más seguro. Se puede desactivar cualquier servicio de Oracle ILOM, pero esto ocasionará la pérdida de funciones. Como regla general, active solo aquellos servicios que sean absolutamente necesarios en el entorno implementado. La pérdida de funciones se debe comparar con el beneficio de seguridad derivado de tener menor cantidad de servicios de red activados.

En la siguiente tabla, se describe el impacto de la activación o la desactivación de cada servicio.

TABLA 6 Servicios desactivados

Servicio	Descripción	Resultado de la activación/desactivación
HTTP	Protocolo no cifrado para acceder a la interfaz web de Oracle ILOM.	La activación de este servicio proporciona un rendimiento más rápido que el HTTP cifrado (HTTPS). Sin embargo, el uso de este protocolo podría derivar en el envío de información confidencial por Internet sin cifrado.
HTTPS	Protocolo cifrado para acceder a la interfaz web de Oracle ILOM.	La activación de este servicio proporciona una comunicación segura entre un explorador web y Oracle ILOM. Sin embargo, debido a que es necesario tener un puerto de red abierto en Oracle ILOM, aumenta la vulnerabilidad a los ataques, como la denegación del servicio.
Servicetag	Protocolo de detección de Oracle utilizado para identificar servidores y facilitar solicitudes de servicio.	La desactivación de este servicio impide que Oracle Enterprise Manager Ops Center detecte a Oracle ILOM, e impide la integración con otras soluciones de servicio automático de Oracle. El estado Servicetag solo se puede configurar desde la interfaz de línea de comandos de Oracle ILOM. Por ejemplo, para modificar la propiedad de estado de servicetag, escriba: `set /SP/services/servicetag state=`*enabled*|*disabled*
IPMI	Protocolo de gestión estándar.	La desactivación de este servicio podría impedir que Oracle Enterprise Manager Ops Center, además de algunos conectores de gestión de Oracle con software de terceros, gestionen el sistema.
SNMP	Protocolo de administración estándar para supervisar el estado de Oracle ILOM y supervisar las notificaciones de capturas recibidas.	La desactivación de este servicio podría impedir que Oracle Enterprise Manager Ops Center, además de algunos conectores de gestión de Oracle con software de terceros, gestionen el sistema.
KVMS	Juego de protocolos para proporcionar almacenamiento, mouse, video y teclado remotos.	La desactivación de este servicio genera la desactivación de la funcionalidad de almacenamiento remoto y consola host, lo que evita el uso de las aplicaciones Oracle ILOM Remote System Console (u Oracle ILOM Remote System Console Plus) y Storage Redirection CLI.
SSH	Protocolo seguro para acceder a un shell remoto.	La desactivación de este servicio impide el acceso a la línea de comandos por medio de la red y podría impedir que Oracle Enterprise Manager Ops Center detecte Oracle ILOM.

Servicio	Descripción	Resultado de la activación/desactivación
SSO	Función de inicio de sesión único que reduce la cantidad de veces que tiene un usuario para introducir un nombre de usuario y una contraseña.	La desactivación de este servicio impide el inicio de KVMS sin tener que volver a introducir una contraseña y permite el desplazamiento desde el módulo de supervisión del chasis (CMM) hasta el SP del blade sin tener que volver a introducir una contraseña.

Para obtener información sobre la activación y desactivación de servicios de red individuales, consulte el siguiente tema “Configuración de servicios y puertos de red” [20].

Configuración de servicios y puertos de red

Para obtener instrucciones sobre cómo configurar los servicios de gestión y sus respectivos puertos de red en Oracle ILOM, consulte los siguientes procedimientos.

- Modificación de puertos y estados de servicios de gestión de protocolo [20]
- Modificación de puertos y estado de servicio de KVMS [22]
- Modificación de puerto y estado de servicio de inicio de sesión único [22]

Para desactivar o activar los servicios y sus respectivos puertos de red, puede utilizar la interfaz de línea de comandos (CLI) la interfaz web de Oracle ILOM. Los procedimientos incluidos en esta sección brindan instrucciones de navegación basada en Web para todas las versiones de firmware de Oracle ILOM. Para obtener instrucciones de la CLI u otros detalles sobre las propiedades de configuración, consulte la documentación correspondiente que se muestra en la sección Información relacionada, que aparece después de cada procedimiento.

▼ Modificación de puertos y estados de servicios de gestión de protocolo

Antes de empezar

Antes de empezar

- Revise las siguientes tablas para determinar qué servicios de protocolo y puertos de red están activados o desactivados de forma predeterminada en Oracle ILOM.
  - Tabla 4, “Servicios y puertos activados de forma predeterminada”
  - Tabla 5, “Servicios y puertos desactivados de forma predeterminada”
- Se necesita el rol Admin (Administrador) (a) en Oracle ILOM para modificar la propiedad de estado de los servicio de protocolo.

Siga estos pasos para modificar la propiedad de estado de un servicio de red.

1. **En la interfaz web de Oracle ILOM, navegue hasta los servicios de acceso a gestión.**

Por ejemplo:

- **En la interfaz web 3.0.x, haga clic en Configuration (Configuración) -> System Management Access (Acceso a gestión del sistema).**
- **En la interfaz web 3.1, y en versiones posteriores, haga clic en ILOM Administration (Administración de ILOM) -> Management Access (Acceso a gestión).**

2. **Haga clic en uno de los separadores de servicio de Management Access -> (Acceso a gestión ->) que se muestran a continuación, según corresponda:**

Management Access ->	Descripción
Web Server	Use la página Web Server (Servidor web) para gestionar el estado de servicio y las asignaciones de puerto para los accesos a la gestión de los protocolos HTTP y HTTPS.
IPMI	Use la página IPMI para gestionar las propiedades de puerto y estado de servicio para el acceso a la gestión del protocolo IPMI.
SNMP	Use la página SNMP para gestionar las propiedades de puerto y estado de servicio para el acceso a la gestión del protocolo SNMP.
SSH	Use la página SSH para gestionar la propiedad de estado de servicio para el acceso a la gestión del shell seguro.

3. **Modifique la propiedad de estado en la página de servicio Management Access -> (Acceso a gestión) y, luego, haga clic en Save (Guardar) para aplicar el cambio.**

Tenga en cuenta que la desactivación de la propiedad de estado de un servicio de protocolo genera el cierre del puerto de red de servicio de protocolo correspondiente e impide el uso del servicio de protocolo con Oracle ILOM.

Información relacionada

- Servicios de gestión y propiedades predeterminadas de red, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Servicios de gestión y propiedades predeterminadas de red, *Guía de configuración y mantenimiento de Oracle ILOM 3.1*
- Configuración de red, *Guía de procedimientos de la CLI para la gestión diaria de Oracle ILOM 3.0*
- Configuración de red, *Guía de procedimientos web para la gestión diaria de Oracle ILOM 3.0*

▼ Modificación de puertos y estado de servicio de KVMS

Antes de empezar

Antes de empezar

- La propiedad de estado de servicio de KVMS está activada de forma predeterminada en Oracle ILOM. Para obtener una lista de los puertos de red abiertos que están asociados con el servicio KVMS, consulte la Tabla 4, “Servicios y puertos activados de forma predeterminada”.
- Se necesita el rol Admin (Administrador) (a) para modificar la propiedad de estado de servicio de KVMS en Oracle ILOM.

1. **Navegue hasta el separador KVMS en la interfaz web de Oracle ILOM.**

   Por ejemplo:

   - **En la interfaz web 3.0.x, haga clic en Remote Control (Control remoto) -> KVMS.**
   - **En la interfaz web 3.1, y en versiones posteriores, haga clic en Remote Console (Consola remota) -> KVMS.**

2. **En el separador KVMS, modifique la propiedad de estado de KVMS y, luego, haga clic en Save (Guardar) para aplicar el cambio.**

   Tenga en cuenta que la desactivación de la propiedad de estado genera el cierre de los puertos de red de servicio de KVMS abiertos, lo que impide el uso de lo siguiente: a) la consola host remota, y b) Oracle ILOM Remote Console y Oracle ILOM Remote Storage CLI, u Oracle ILOM Remote Console Plus.

Información relacionada

- Configuración de valores de KVMS del cliente local, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Configuración de valores de KVMS del cliente local, *Guía de configuración y mantenimiento de Oracle ILOM 3.1*
- Tareas de configuración inicial, *Guía web y de la CLI para consolas de redirección remota de Oracle ILOM 3.0*

▼ Modificación de puerto y estado de servicio de inicio de sesión único

Antes de empezar

Antes de empezar

- La propiedad de estado de servicio de inicio de sesión único (SSO) y el puerto de red correspondiente (1126) están activados de forma predeterminada en Oracle ILOM.

- Se necesita el rol Admin (Administrador) (a) en Oracle ILOM para modificar la propiedad de estado de servicio de SSO.

1. **Navegue hasta el separador User Account (Cuenta de usuario) en la interfaz web de Oracle ILOM.**

   Por ejemplo:

   - **En la interfaz web 3.0.x, haga clic en User Management (Gestión de usuarios) -> User Account (Cuenta de usuario).**
   - **En la interfaz web 3.1, y en versiones posteriores, haga clic en ILOM Administration (Administración de ILOM) -> User Account (Cuenta de usuario).**

2. **En la página User Account (Cuenta de usuario), modifique la propiedad de estado de SSO y, luego, haga clic en Save (Guardar) para aplicar el cambio.**

   Tenga en cuenta que la desactivación de la propiedad de estado de SSO en Oracle ILOM genera: a) que se cierre el puerto de red de SSO abierto; b) que se le solicite a los usuarios que vuelvan a introducir sus contraseñas al iniciar una consola KVMS y c) que se permita a los usuarios de CMM navegar hasta un SP de servidor blade sin tener que volver a introducir la contraseña.

Información relacionada

- Servicio de inicio de sesión único, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Servicio de inicio de sesión único, *Guía de configuración y mantenimiento de Oracle ILOM 3.1*
- Configuración de inicio de sesión único, *Guía de procedimientos de la CLI para la gestión diaria de Oracle ILOM 3.0*
- Configuración de inicio de sesión único, *Guía de procedimientos web para la gestión diaria de Oracle ILOM 3.0*

Protección del acceso de usuario de Oracle ILOM

Para proteger el acceso de usuario en Oracle ILOM, consulte los siguientes temas:

Cómo evitar la creación de cuentas de usuario compartidas

Evite la creación de cuentas compartidas para mantener un entorno seguro. Las cuentas compartidas son cuentas de usuario que comparten una contraseña de cuenta de usuario determinada. En lugar de crear cuentas compartidas, el método ideal para manejar cuentas de usuario consiste en crear una contraseña única para cada usuario que tiene acceso a Oracle ILOM. Asegúrese de que cada combinación de cuenta de usuario y contraseña sea conocida solamente por un usuario.

Nota - Oracle ILOM admite hasta 10 cuentas de usuario locales. Si necesita que más usuarios accedan a Oracle ILOM, puede configurar servicios de directorio, como LDAP o Active Directory, para admitir más cuentas mediante una base de datos centralizada. Para obtener más información, consulte “Perfiles de seguridad y servicios de autenticación remota” [27].

Después de establecer cuentas de usuario individuales con contraseñas únicas, el administrador del sistema debe asegurarse de que se haya asignado una contraseña única a la cuenta `root` de administrador preconfigurada. De lo contrario, si no se proporciona una contraseña única, la cuenta `root` de administrador preconfigurada es considerada una cuenta compartida. Para asegurarse de que los usuarios no autorizados no usen la cuenta `root` de administrador preconfigurada, debe modificar la contraseña o eliminar la cuenta `root` preconfigurada de Oracle ILOM. Para obtener más información sobre la cuenta `root` de administrador preconfigurada, consulte Modificación de la contraseña predeterminada para la cuenta `root` en el primer inicio de sesión [29].

Para obtener más información sobre cómo establecer cuentas seguras con contraseñas únicas, consulte “Directrices de seguridad para la gestión de cuentas de usuario y contraseñas” [25].

Para obtener información sobre la configuración de cuentas de usuario, consulte “Configuración de acceso de usuario para máxima seguridad” [28].

Asignación de privilegios basados en roles

A todas las cuentas de usuario de Oracle ILOM se les asigna un conjunto de privilegios basados en roles. Estos privilegios basados en roles brindan acceso a funciones discretas dentro de Oracle ILOM. Puede configurar una cuenta de usuario para que el usuario pueda supervisar el sistema, pero no pueda realizar cambios de configuración. O bien, puede permitir a un usuario que modifique la mayoría de las opciones de configuración, excepto crear y modificar cuentas de usuario. También es posible restringir las personas que pueden controlar la energía del servidor y las personas que pueden acceder a la consola remota. Es importante comprender los niveles de privilegios y asignarlos correctamente a los usuarios de la organización.

En la siguiente tabla, se define una lista de los privilegios que se pueden asignar a una cuenta de usuario de Oracle ILOM individual.

TABLA 7 Descripciones de privilegios de cuenta de usuario

Rol	Descripción
`Admin` (`a`)	Permite al usuario cambiar todas las opciones de configuración de Oracle ILOM, excepto las opciones de configuración expresamente autorizadas por otros privilegios (como la gestión de usuarios).
`User Management` (`u`)	Permite al usuario agregar y eliminar usuarios, cambiar sus contraseñas y configurar servicios de autenticación. Un usuario con este rol puede crear una segunda cuenta de usuario con todos los privilegios, y, por consiguiente, este rol tiene el nivel más alto de privilegios de todos los roles de usuarios.
`Console` (`c`)	Permite al usuario acceder a la consola host de manera remota. El acceso remoto a la consola puede permitir al usuario acceder al OpenBoot PROM (OBP) o al BIOS, lo que brinda al usuario la posibilidad de cambiar el comportamiento de inicio como una manera de obtener acceso al sistema.
`Reset and Host Control` (`r`)	Permite al usuario controlar la energía del host y restablecer Oracle ILOM.
`Read-only` (`o`)	Permite al usuario tener acceso de solo lectura a las interfaces de usuario de Oracle ILOM. Todos los usuarios tienen este acceso, que les permite leer los registros y la información del entorno, además de ver los valores de configuración.

Para obtener más información sobre la creación de una cuenta de usuario local y la asignación de privilegios basados en roles, consulte Creación de cuentas de usuario locales con privilegios basados en roles [30].

Directrices de seguridad para la gestión de cuentas de usuario y contraseñas

Considere las siguientes directrices de seguridad al gestionar las cuentas de usuario y contraseñas de Oracle ILOM:

- “Directrices para la gestión de cuentas de usuario” [25]
- “Directrices para la gestión de contraseñas” [26]

Directrices para la gestión de cuentas de usuario

Directriz para la gestión de cuenta de usuario	Descripción
No promueva el uso compartido de cuentas de usuario	Siempre se debe crear una cuenta separada para cada usuario de Oracle ILOM. Oracle ILOM admite como máximo 10 cuentas de usuario locales. Si está gestionando un sitio más grande y requiere más de 10 cuentas de usuario, debe considerar utilizar un servicio de autenticación de usuarios de terceros, como LDAP o Active Directory.

Directriz para la gestión de cuenta de usuario	Descripción
	Para obtener más información sobre la implementación de la autenticación de usuarios en Oracle ILOM mediante un servicio de autenticación externo, consulte “Perfiles de seguridad y servicios de autenticación remota” [27].
Seleccione nombres que cumplen con los requisitos para las cuentas de usuario locales	Cuando elija un nombre de usuario para una cuenta de usuario de Oracle ILOM local, el nombre de usuario debe cumplir con lo siguiente: ■ Debe tener entre 4 y 16 caracteres de longitud (el primer carácter debe ser una letra). ■ Debe ser único en la organización. ■ No debe tener espacios, punto (.) ni dos puntos (:).
Seleccione contraseñas que cumplen con los requisitos para las cuentas de usuario locales	Cuando elija una contraseña para la cuenta de usuario de Oracle ILOM local, la contraseña debe cumplir con lo siguiente: ■ Debe ser siempre una contraseña segura que contenga una longitud máxima de dieciséis caracteres. ■ Debe contener una combinación de caracteres en minúscula y mayúscula, además de uno o dos caracteres especiales para crear una contraseña compleja y segura. ■ No debe tener espacios, punto (.) ni dos puntos (:). ■ Debe cumplir con la política de gestión de contraseñas de la empresa. Para obtener más información sobre la gestión de contraseñas en Oracle ILOM, consulte “Directrices de seguridad para la gestión de cuentas de usuario y contraseñas” [25].
Limite los privilegios de cuenta de usuario basados en el rol del puesto (*principios de menor privilegio*)	El principio del menor privilegio indica que, para una buena práctica de seguridad, se le debe dar al usuario la menor cantidad posible de privilegios para hacer su trabajo. El otorgamiento excesivamente ambicioso de responsabilidades, roles, etc. (en especial, al comienzo del ciclo de vida de una organización), puede dejar vulnerable un sistema. Revise los privilegios de usuarios con regularidad para determinar la relevancia con las responsabilidades actuales de los puestos de cada usuario. Oracle ILOM brinda la posibilidad de controlar los privilegios de usuario de cada usuario. Asegúrese de que se asignen los permisos de rol de usuario adecuados a cada cuenta de usuario, según el rol del puesto. Para obtener información sobre cómo crear una cuenta de usuario con privilegios basados en roles, consulte: Creación de cuentas de usuario locales con privilegios basados en roles [30]

Directrices para la gestión de contraseñas

Directriz de gestión de contraseña	Descripción
Cambie la contraseña predeterminada (`changeme`) inmediatamente después del inicio de sesión inicial	Para activar el primer inicio de sesión y acceder a Oracle ILOM, se proporciona una cuenta `root` de administrador local con el sistema. Para crear un entorno seguro, debe cambiar la contraseña de administrador proporcionada (`changeme`) después del inicio de sesión inicial en Oracle ILOM. La obtención de acceso no autorizado a la cuenta de administrador `root` brinda al usuario acceso libre a todas las funciones de Oracle ILOM. Por lo tanto, es importante especificar una contraseña segura.
Cambie todas las contraseñas de la cuenta de Oracle ILOM regularmente	Para evitar la actividad maliciosa y garantizar que las contraseñas se ajusten a las políticas de contraseñas actuales, debe cambiar todas las contraseñas de Oracle ILOM regularmente.

Directriz de gestión de contraseña	Descripción
Aplique prácticas comunes para la creación de contraseñas complejas y seguras	Aplique las siguientes prácticas comunes para la creación de contraseñas complejas y seguras: ■ No cree una contraseña de menos de dieciséis caracteres de longitud. ■ No cree una contraseña que contenga el nombre de usuario, el nombre del empleado o el nombre de un miembro de su familia. ■ No elija contraseñas que se adivinen fácilmente. ■ No cree contraseñas que contengan una cadena consecutiva de números, como 12345. ■ No cree contraseñas que contengan una palabra o cadena que se pueda descubrir fácilmente mediante una simple búsqueda por Internet. ■ No permita que los usuarios vuelvan a utilizar la misma contraseña en varios sistemas. ■ No permita a los usuarios volver a utilizar contraseñas anteriores.
Consulte con el responsable de seguridad de TI para conocer las políticas de gestión de contraseñas	Consulte con el responsable de seguridad de TI para garantizar el cumplimiento de políticas y requisitos de gestión de contraseñas de la empresa.

Perfiles de seguridad y servicios de autenticación remota

Oracle ILOM se puede configurar para utilizar un almacén de usuarios centralizado externo en lugar de tener que configurar usuarios locales en cada instancia de Oracle ILOM. Gracias a esto, también se pueden crear y modificar credenciales de usuarios de manera centralizada y permitir a los usuarios obtener acceso a muchos sistemas diferentes.

Antes de elegir y configurar un servicio de autenticación, debe comprender cómo funcionan estos servicios y cómo se debe configurar cada uno de ellos. Además de la autenticación, cada uno de los servicios admitidos ofrece la posibilidad de configurar reglas de autorización que definen de qué manera se asignan los privilegios de usuario de Oracle ILOM para un usuario remoto determinado. Asegúrese de que se asigne el privilegio o rol de usuario adecuado.

En la siguiente tabla, se describen los servicios de autenticación de usuarios admitidos por Oracle ILOM.

TABLA 8 Perfiles de seguridad y servicios de autenticación remota

Nombre del servicio	Perfil de seguridad	Información
Active Directory	Alto	■ Este servicio es seguro por defecto. ■ El uso del modo de certificación estricta requiere un servidor de certificados, pero agrega una capa adicional de seguridad.
Lightweight Directory Access Protocol/Secure Socket Layer (LDAP/SSL)	Alto	■ Este servicio es seguro por defecto. ■ El uso del modo de certificación estricta requiere un servidor de certificados, pero agrega una capa adicional de seguridad.

Nombre del servicio	Perfil de seguridad	Información
Legacy LDAP	Bajo	■ Utilice este servicio en redes seguras privadas donde no existe sospecha de usuarios maliciosos.
Remote Authentication Dial In User Service (RADIUS)	Bajo	■ Utilice este servicio en redes seguras privadas donde no existe sospecha de usuarios maliciosos.

Los servicios con un perfil de alta seguridad se pueden utilizar en entornos muy seguros, ya que están protegidos por certificados y otras formas de cifrado de alta seguridad para proteger el canal. Los servicios con un perfil de baja seguridad están desactivados de forma predeterminada. Active estos perfiles de baja seguridad solo si comprende y acepta las limitaciones de este nivel bajo de seguridad.

Para obtener información sobre la configuración del servicio de autenticación remota, consulte la documentación de Oracle ILOM correspondiente indicada a continuación:

- Configuración y mantenimiento de cuentas de usuario, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Configuración y mantenimiento de cuentas de usuario, *Guía configuración y mantenimiento de Oracle ILOM 3.1*
- Gestión de cuentas de usuario, *Guía de procedimientos de la CLI para la gestión diaria de Oracle ILOM 3.0*
- Gestión de cuentas de usuario, *Guía de procedimientos web para la gestión diaria de Oracle ILOM 3.0*

Configuración de acceso de usuario para máxima seguridad

Consulte los siguientes temas para ver cómo configurar el acceso de usuario de Oracle ILOM de la mejor manera para obtener la máxima seguridad.

- Modificación de la contraseña predeterminada para la cuenta `root` en el primer inicio de sesión [29]
- Creación de cuentas de usuario locales con privilegios basados en roles [30]
- Bloqueo del acceso al host al salir de una sesión de KVMS [32]
- Limitación de sesiones de KVMS visibles para Remote System Console Plus (3.2.4 o posterior) [33]
- Acceso seguro al sistema con banner de inicio de sesión (3.0.8 y posterior) [34]

Puede configurar las propiedades de acceso de usuario en Oracle ILOM mediante la interfaz de línea de comandos (CLI) o la interfaz web. Los procedimientos incluidos en esta sección brindan instrucciones de navegación basada en Web para todas las versiones de firmware de Oracle ILOM. Para obtener instrucciones de la CLI u otros detalles sobre las propiedades

de configuración, consulte la documentación correspondiente que se muestra en la sección Información relacionada, que aparece después de cada procedimiento.

▼ Modificación de la contraseña predeterminada para la cuenta root en el primer inicio de sesión

Para activar el primer inicio de sesión y acceder a Oracle ILOM, se proporciona una cuenta root de administrador predeterminada y una contraseña (changme) predeterminada con el sistema. Para impedir el acceso no autorizado a Oracle ILOM, la contraseña predeterminada (changeme) que se envía con la cuenta root preconfigurada se debe cambiar en el primer inicio de sesión. De lo contrario, la cuenta root preconfigurada y la contraseña predeterminada (changeme) funcionarán como una cuenta compartida, lo que permitirá el acceso de administrador a cualquier usuario.

Use las siguientes instrucciones basadas en Web para modificar la contraseña predeterminada (changeme) que se envía con la cuenta root de administrador preconfigurada.

Nota - Si no tiene acceso a la cuenta root preconfigurada y necesita tener acceso a las funciones de administrador de Oracle ILOM, póngase en contacto con el administrador del sistema para obtener una cuenta de usuario con privilegios de administrador.

Antes de empezar

- Consulte “Directrices de seguridad para la gestión de cuentas de usuario y contraseñas” [25].

Nota - La asignación de una contraseña segura a la cuenta root es esencial para impedir el acceso no autorizado a las funciones de Oracle ILOM. Una contraseña segura debe contener una combinación de caracteres en minúscula y mayúscula, y, al menos, un carácter especial, como % o $.

- Se necesita el rol User Management (Gestión de usuarios) (u) para modificar contraseñas de cuentas de usuarios locales en Oracle ILOM.

1. **Navegue hasta la página User Account (Cuenta de usuario) en la interfaz web de Oracle ILOM.**

   Por ejemplo:

   - **En la interfaz web 3.0.x, haga clic en User Management (Gestión de usuarios) -> User Accounts (Cuentas de usuario).**

- **En la interfaz web 3.1, y en versiones posteriores, haga clic en User Management (Gestión de usuarios) -> User Accounts (Cuentas de usuario).**

2. **En la página User Account (Cuenta de usuario), haga clic en Edit (Editar) para la cuenta `root`.**

   Aparece el cuadro de diálogo Edit: User Root (Editar: usuario root).

3. **En el cuadro de diálogo Edit: User Root (Editar: usuario root), realice lo siguiente:**

   - **Introduzca una contraseña única en el cuadro de texto New Password (Nueva contraseña) y, luego, vuelva a introducir la misma contraseña en el cuadro de texto Confirm New Password (Confirmar nueva contraseña).**

   - **Haga clic en Save (Guardar) para aplicar el cambio.**

Información relacionada

- Configuración de una cuenta de usuario local, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Configuración de una cuenta de usuario local, *Guía de configuración y mantenimiento de Oracle ILOM 3.1*
- Modificación de una cuenta de usuario, *Guía de procedimientos de la CLI para la gestión diaria de Oracle ILOM 3.0*
- Modificación de una cuenta de usuario, *Guía de procedimientos web para la gestión diaria de Oracle ILOM 3.0*
- "Presencia de seguridad física para el restablecimiento de la contraseña predeterminada de la cuenta `root`" [61]

▼ Creación de cuentas de usuario locales con privilegios basados en roles

Antes de empezar

Oracle ILOM admite la creación y el almacenamiento de hasta 10 cuentas de usuario locales en un solo SP o módulo de supervisión del chasis (CMM). A los usuarios de Oracle ILOM se les asigna un conjunto de privilegios que les permite usar funciones según los permisos otorgados en su cuenta configurada.

Nota - De manera alternativa, los administradores del sistema pueden configurar Oracle ILOM para que admita cuentas de usuario adicionales por medio de un servicio de autenticación remota. Cuando se cuenta con una configuración de servicio de autenticación remota, los inicios de sesión, las contraseñas y los privilegios se obtienen de un almacén de usuarios externo. Para obtener más información, consulte "Perfiles de seguridad y servicios de autenticación remota" [27].

Para obtener instrucciones basadas en Web para configurar una cuenta de usuario local con privilegios de acceso basados en roles, consulte las siguientes instrucciones.

Antes de empezar

- Consulte "Directrices de seguridad para la gestión de cuentas de usuario y contraseñas" [25].
- Consulte la Tabla 7, "Descripciones de privilegios de cuenta de usuario".
- Se necesita el rol User Management (Gestión de usuarios) (u) de Oracle ILOM para crear una cuenta de usuario local con privilegios.

1. **Navegue hasta la página User Account (Cuenta de usuario) en la interfaz web de Oracle ILOM.**

   Por ejemplo:

   - **En la interfaz web 3.0.x, haga clic en User Management (Gestión de usuarios) -> User Accounts (Cuentas de usuario).**
   - **En la interfaz web 3.1, y en versiones posteriores, haga clic en User Management (Gestión de usuarios) -> User Accounts (Cuentas de usuario).**

2. **En la página User Account (Cuenta de usuario), haga clic en Add (Agregar).**

   Se abre el cuadro de diálogo Add User (Agregar usuario).

3. **En el cuadro de diálogo Add User (Agregar usuario), realice lo siguiente:**

   a. **Especifique el nombre del usuario en el cuadro de texto User Name (Nombre de usuario).**

   b. **En la lista desplegable Roles (Roles), seleccione el perfil de rol de usuario adecuado (Administrator [Administrador], Operator [Operador] o Advanced [Avanzado]).**

c. **Introduzca una contraseña única en el cuadro de texto New Password (Nueva contraseña) y, luego, vuelva a introducir la misma contraseña en el cuadro de texto Confirm New Password (Confirmar nueva contraseña).**

d. **Haga clic en Save (Guardar) para aplicar los cambios.**

Información relacionada

- Creación de cuenta de usuario y asignación de rol de usuario, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Creación de cuenta de usuario y asignación de rol de usuario, *Guía de configuración y mantenimiento de Oracle ILOM 3.1*
- Agregación de cuenta de usuario y asignación de roles, *Guía de procedimientos de la CLI para la gestión diaria de Oracle ILOM 3.0*
- Agregación de cuenta de usuario y asignación de roles, *Guía de procedimientos web para la gestión diaria de Oracle ILOM 3.0*

▼ Bloqueo del acceso al host al salir de una sesión de KVMS

Debido a que la consola host es considerada un recurso de red compartido cuando se usa el KVMS remoto, si un usuario inicia sesión en la consola host y cierra las aplicaciones Oracle ILOM Remote System Console, Remote System Console Plus o Storage Redirection CLI sin cerrar sesión en el sistema operativo host, el segundo usuario que se conecte a la misma consola mediante el KVMS remoto podrá utilizar la sesión del sistema operativo autenticada previamente. Por este motivo, Oracle ILOM ofrece la posibilidad de bloquear automáticamente el sistema operativo host cada vez que se desconecta una sesión de KVMS remoto. Para obtener la máxima seguridad, active o configure esta función en Oracle ILOM.

Para bloquear el escritorio del host remoto después de terminar una sesión de KVMS, consulte las siguientes instrucciones basadas en Web. Para obtener información sobre cómo activar la función de bloqueo de host, consulte la *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*.

Antes de empezar

- Se necesita el rol Console (Consola) (c) para modificar la propiedad del modo de bloqueo de host en Oracle ILOM.
- Para utilizar la función de modo de bloqueo de host en Oracle ILOM, se requiere el firmware 3.0.4 o posterior.
- La función de modo de bloqueo de host está desactivada de forma predeterminada.

1. **Navegue hasta la página KVMS en la interfaz web de Oracle ILOM.**

Por ejemplo:

- **En la interfaz web 3.0.x, haga clic en Remote Console (Consola remota) -> KVMS.**
- **En la interfaz web 3.1, y en versiones posteriores, haga clic en Remote Control (Control remoto) -> KVMS.**

2. **En la sección Host Lock Settings (Configuración de bloqueo de host) de la página KVMS, realice una de las siguientes tareas:**

   - **Especifique un modo de bloqueo (Windows, Custom [Personalizado] o Disabled [Desactivado]).**
   - **Haga clic en Save (Guardar) para aplicar el cambio.**

Información relacionada

- Bloqueo del escritorio del host, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Bloqueo del escritorio del host, *Configuración y mantenimiento de Oracle ILOM 3.1*
- Bloqueo de KVMS, *Guía web y de la CLI para consolas de redirección remota de Oracle ILOM 3.0*

▼ Limitación de sesiones de KVMS visibles para Remote System Console Plus (3.2.4 o posterior)

Antes de empezar

A partir de la versión de firmware 3.2.4, un usuario principal de Remote System Console Plus puede impedir que otros usuarios que hayan iniciado sesión en el SP vean la información confidencial introducida durante una sesión de redirección de video, mediante la limitación del recuento máximo de sesiones de cliente a un (1) visor de sesión. De forma predeterminada, la propiedad de recuento máximo de sesiones de cliente para Oracle ILOM Remote System Console Plus está establecida en cuatro visores de sesión.

Para modificar la propiedad de recuento máximo de sesiones de cliente de Oracle ILOM Remote System Console Plus, consulte las siguientes instrucciones basadas en Web.

Antes de empezar

- La propiedad de recuento máximo de sesiones de cliente de KVMS para Oracle ILOM Remote System Console Plus está disponible a partir de la versión de firmware 3.2.4 o posterior.

Nota - La propiedad de recuento máximo de sesiones de cliente de KVMS no se puede configurar en sistemas que admiten Oracle ILOM Remote Console.

- Oracle ILOM Remote System Console Plus solo está disponible en los sistemas de SP recientemente presentados, a partir de la versión 3.2.1.
- Se necesita el rol Console (Consola) (c) en Oracle ILOM para modificar la propiedad de recuento máximo de sesiones de cliente de KVMS.
- Al restablecer la propiedad de recuento máximo de sesiones de cliente de Oracle ILOM, todas las sesiones de video de Oracle ILOM Remote System Console Plus activas en el SP finalizan.
- De forma predeterminada, se puede iniciar un máximo de cuatro sesiones de redirección de video de Remote System Console Plus, por SP, desde la página de redirección de Oracle ILOM.

1. **Haga clic en Remote Console (Consola remota) -> KVMS, para navegar hasta la página KVMS en la interfaz web de Oracle ILOM.**
2. **En la página KVMS, modifique la propiedad de recuento máximo de sesiones de cliente (valor aceptable:** *4* **(predeterminado)|***1***|***2***|***3***).**
3. **Haga clic en Save (Guardar) para aplicar el cambio.**

Información relacionada

- Propiedades de redirección del dispositivo remoto, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*

▼ Acceso seguro al sistema con banner de inicio de sesión (3.0.8 y posterior)

Antes de empezar

A partir de la versión de firmware 3.0.8, Oracle ILOM permite a los administradores del sistema mostrar un mensaje de banner a todos los usuarios cuando inician sesión en la interfaz web y la CLI de Oracle ILOM. El uso de un banner de inicio de sesión puede ayudar a brindar protección contra el acceso no autorizado al sistema por parte de dispositivos remotos, y a aconsejar a los usuarios legítimos y autorizados sobre sus obligaciones relacionadas con el uso aceptable del sistema.

El mensaje de banner que se implementa se debe redactar teniendo en cuenta la política de seguridad de la información. Para obtener más directrices sobre el mensaje escrito, consulte con el administrador del sitio o el responsable de seguridad.

Para mostrar un mensaje de banner a todos los usuarios en el inicio de sesión, consulte las siguientes instrucciones basadas en Web.

Antes de empezar

- Se necesita el rol Admin (Administrador) (a) para crear un mensaje de banner.
- La configuración del mensaje de banner está disponible a partir de la versión de firmware 3.0.8, o posterior, de Oracle ILOM.
- Los administradores pueden configurar el mensaje de banner para mostrar en la página de inicio de sesión o en un cuadro de diálogo que aparece inmediatamente después de que el usuario inicia sesión en Oracle ILOM.

1. **Navegue hasta la página Banner Message (Mensaje de banner) en la interfaz web de Oracle ILOM.**

   Por ejemplo:

   - **En la interfaz web 3.0.x, haga clic en System Information (Información del sistema) -> Banner Messages (Mensajes de banner).**
   - **En la interfaz web 3.1, y en versiones posteriores, haga clic en ILOM Administration (Administración de ILOM) -> Management Access (Acceso a gestión) -> Banner Messages (Mensajes de banner).**

2. **En la página Banner Message (Mensaje de banner), realice lo siguiente:**

   a. **Si desea que el mensaje aparezca en la página de inicio de sesión, introduzca el mensaje en el cuadro de texto Connect Message (Mensaje de conexión). De lo contrario, introduzca el mensaje en el cuadro de texto Login Message (Mensaje de inicio de sesión) para que el mensaje aparezca en un cuadro de diálogo después de que el usuario inicia sesión.**

   b. **Seleccione la casilla de verificación Login Message Acceptance (Aceptación del mensaje de inicio de sesión) para mostrar el mensaje; de lo contrario, anule la selección de esta casilla de verificación para impedir que aparezca el mensaje.**

   c. **Haga clic en Save (Guardar) para aplicar los cambios.**

Información relacionada

- Propiedades de configuración de mensajes de banner, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Propiedades de configuración de mensajes de banner, *Guía de configuración y mantenimiento de Oracle ILOM 3.1*

- Visualización de mensaje de banner, *Guía de procedimientos de la CLI para la gestión diaria de Oracle ILOM 3.0*
- Visualización de mensaje de banner, *Guía de procedimientos web para la gestión diaria de Oracle ILOM 3.0*

Configuración de las interfaces de Oracle ILOM para máxima seguridad

Para configurar las interfaces de Oracle ILOM para máxima seguridad, consulte los siguientes temas:

- "Configuración de la interfaz web para máxima seguridad" [36]
- "Configuración de la CLI para máxima seguridad" [43]
- "Configuración del acceso a la gestión de SNMP para máxima seguridad" [47]
- "Configuración del acceso a la gestión de IPMI para máxima seguridad" [49]
- "Configuración del acceso a WS-Management para máxima seguridad" [52]

Configuración de la interfaz web para máxima seguridad

Consulte los siguientes temas para ver cómo configurar la interfaz web de Oracle ILOM de la mejor manera para obtener la máxima seguridad.

Nota - Puede configurar las propiedades de interfaz de gestión web en Oracle ILOM mediante la interfaz de línea de comandos (CLI) o la interfaz web. Los procedimientos incluidos en esta sección brindan instrucciones de navegación basada en Web para todas las versiones de firmware de Oracle ILOM. Para obtener instrucciones de la CLI u otros detalles sobre las propiedades de configuración, consulte la documentación correspondiente que se muestra en la sección Información relacionada, que aparece después de cada procedimiento.

- "Mejora de la seguridad mediante el uso de certificados SSL de confianza y claves privadas" [37]
- Activación de propiedades de cifrado SSL y TLS más seguro [40]
- Establecimiento de un intervalo de timeout para sesiones web inactivas [41]

Mejora de la seguridad mediante el uso de certificados SSL de confianza y claves privadas

Los certificados de capa de conexión segura (SSL) se utilizan para cifrar comunicaciones por red y para garantizar la autenticidad de un servidor o un cliente. Oracle ILOM contiene un certificado SSL autofirmado que permite la utilización inmediata del protocolo HTTP sobre SSL sin necesidad de cargar un certificado. Al realizar la conexión a la interfaz web de Oracle ILOM por primera vez, se informa al usuario que se utiliza un certificado autofirmado y se le solicita aceptar su utilización. Mediante el uso del certificado proporcionado, se cifra completamente la comunicación entre el explorador web y Oracle ILOM.

Sin embargo, también es posible crear y cargar un certificado de confianza para tener mayor seguridad. El certificado de confianza significa que el certificado se otorga junto con una autoridad de certificación de confianza. El uso de un certificado de confianza de una autoridad de certificación conocida garantiza la autenticidad del servidor web de Oracle ILOM. Si se usan certificados (autofirmados) que no son de confianza, se corre el riesgo de sufrir ataques de tipo "man in the middle" (MITM).

Para obtener y cargar un certificado firmado por una autoridad de certificación o autofirmado temporal, consulte los siguientes procedimientos:

- Obtención de certificados SSL y claves privadas mediante OpenSSL [37]
- Carga de una clave privada y un certificado SSL personalizados en Oracle ILOM [39]

▼ Obtención de certificados SSL y claves privadas mediante OpenSSL

Este procedimiento es una descripción simplificada de cómo crear un certificado SSL y una clave privada mediante el kit de herramientas OpenSSL.

Nota - Oracle ILOM *no* requiere que se utilice OpenSSL para generar certificados SSL. OpenSSL se usa en este procedimiento solo para fines de demostración. Hay otras herramientas disponibles para generar certificados SSL.

La necesidad de usar un certificado firmado por una autoridad de certificación o autofirmado temporal debe ser determinada por el administrador del sitio o el responsable de seguridad. En caso de que necesite obtener un certificado SSL (ya sea firmado por una autoridad de certificación o autofirmado temporal), puede seguir las instrucciones de línea de comandos de OpenSSL de ejemplo que aparecen a continuación.

Nota - Si se requieren más instrucciones de OpenSSL para generar el certificado SSL, debe consultar la documentación del usuario que se proporciona con el kit de herramientas OpenSSL.

---

1. **Cree un directorio local o un recurso compartido de red para almacenar el certificado y la clave privada.**

2. **Para generar una nueva clave RSA privada con el kit de herramientas OpenSSL, escriba:**

   `openssl genrsa -out <foo>.key 2048`

   Donde <*foo*> equivale al nombre de la clave privada.

   Nota - Esta clave privada es una clave RSA de 2048 bits que se almacena en un formato PEM para que se pueda leer como texto ASCII.

3. **Para generar una solicitud de firma de certificado (CSR) con el kit de herramientas OpenSSL, escriba:**

   `openssl req -new -key <foo>.key -out <foo>.csr`

   Donde <*foo*> equivale al nombre de la solicitud de firma de certificado.

   Nota - Durante la generación de la CSR, se le solicitará información varias veces.

   Debería aparecer un archivo `<foo>.csr` en el directorio en el que se está trabajando actualmente.

4. **Para generar un certificado SSL, realice una de las siguientes tareas:**

   - **Genere un certificado autofirmado temporal (válido por 365 días).**

     El certificado SSL autofirmado se genera a partir de la clave privada `server.key` y los archivos `server.csr`.

     Si usa el kit de herramientas OpenSSL, escriba.

     `openssl x509 -req -days 365 -in <foo>.csr`

     `-signkey <foo>.key -out <foo>.cert`

     Donde <*foo*> equivale al nombre asignado a la clave privada (`.key`) o al certificado (`.cert`).

     Nota - Este certificado temporal generará un error en el explorador cliente, de manera que la autoridad de certificación firmante será desconocida y no será de confianza. Si este error no es aceptable, debe solicitar a la autoridad de certificación que le emita un certificado firmado.

- **Obtenga un certificado firmado oficialmente de un proveedor de autoridad de certificación.**

  Envíe su solicitud de firma de certificado (<*foo*>.csr) a un proveedor de proveedor de autoridad de certificación SSL. La mayoría de los proveedores de autoridad de certificación requieren que se corte y se pegue la salida de la CSR en una pantalla de aplicación web. Es posible que transcurra un máximo de siete días hasta que reciba el certificado firmado.

5. **Cargue la clave privada y el certificado SSL nuevos en Oracle ILOM.**

   Consulte las siguientes instrucciones, Carga de una clave privada y un certificado SSL personalizados en Oracle ILOM [39].

▼ Carga de una clave privada y un certificado SSL personalizados en Oracle ILOM

Antes de empezar

- Se necesita el rol Admin (Administrador) (a) para modificar las propiedades del servidor web en Oracle ILOM.
- Obtenga la clave privada y el certificado HTTPS (autofirmado temporal o firmado por autoridad de certificación) nuevos. Para obtener instrucciones sobre el uso del kit de herramientas OpenSSL, consulte Obtención de certificados SSL y claves privadas mediante OpenSSL [37].
- Asegúrese de poder acceder a la clave privada y el certificado HTTPS nuevos por medio de la red o el sistema de archivos local.

1. **Navegue hasta la página SSL Certificate (Certificado SSL) en la interfaz web de Oracle ILOM.**

   Por ejemplo:

   - **En la interfaz web 3.0.x, haga clic en Configuration (Configuración) -> System Management Access (Acceso a gestión del sistema) -> SSL Certificate (Certificado SSL).**

   - **En la interfaz web 3.1, y en versiones posteriores, haga clic en ILOM Administration (Administración de ILOM) -> Management Access (Acceso a gestión) -> SSL Certificate (Certificado SSL).**

2. **En la página del servidor SSL, realice lo siguiente:**

a. **Haga clic en el botón Load Certificate (Cargar certificado) para cargar el archivo de certificado personalizado designado en las propiedades del método de transferencia de archivos.**

b. **Haga clic en el botón Load Custom Private Key (Cargar clave privada personalizada) para cargar el archivo de clave privada personalizada designado en las propiedades del método de transferencia de archivos.**

c. **Haga clic en Save (Guardar) para aplicar los cambios.**

Información relacionada

- Propiedades de configuración de clave privada y certificado SSL, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Propiedades de configuración de clave privada y certificado SSL, *Guía de configuración y mantenimiento de Oracle ILOM 3.1*
- Carga del certificado SSL, *Guía de procedimientos de la CLI para la gestión diaria de Oracle ILOM 3.0*
- Carga del certificado SSL, *Guía de procedimientos web para la gestión diaria de Oracle ILOM 3.0*

▼ Activación de propiedades de cifrado SSL y TLS más seguro

De forma predeterminada, Oracle ILOM le permite utilizar solo los protocolos de cifrado de capa de conexión segura (SSLv3 y TLS v1.0, v1.1, y v1.2) más seguros con los cifrados más potentes. Sin embargo, en algunos casos, puede ser necesario activar SSLv2 o cifrados débiles para admitir el uso de exploradores web más antiguos.

Nota - La compatibilidad con SSL y TLSv1.0 está disponible a partir de la versión de firmware 3.1.0. La compatibilidad con TLS v1.1 y v1.2 está disponible en Oracle ILOM a partir de la versión de firmware 3.2.4.

De ser posible, configure la interfaz web con los valores de seguridad de servidor web predeterminados que se suministran con el sistema. Para ver o modificar las propiedades de seguridad del servidor web en Oracle ILOM, consulte las siguientes instrucciones basadas en Web.

Antes de empezar

- Se necesita el rol Admin (Administrador) (a) para modificar las propiedades del servidor web en Oracle ILOM.

- SSLv3 y TLS v1.0 son admitidos y están activados de forma predeterminada en los SP de los servidores que ejecutan las versiones de firmware 3.1.x, 3.2.1, 3.2.2 y 3.2.3.
- SSLv3 y TLS v1.0, v1.1 y v1.2 son admitidos y están activados de forma predeterminada en los SP de los servidores que ejecutan la versión de firmware 3.2.4, y versiones posteriores.
- Las propiedades de SSLv2 y de los cifrados débiles están desactivadas de forma predeterminada.

1. **En la interfaz web de Oracle ILOM, haga clic en ILOM Administration (Administración de ILOM) > Management Access (Acceso a gestión) -> Web Server (Servidor web).**
2. **En la página Web Server (Servidor web), visualice o modifique las propiedades de seguridad web para SSL, TLS o cifrados débiles.**
3. **Haga clic en Save (Guardar) para aplicar los cambios.**

Información relacionada

- Propiedades de configuración de servidor web, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Propiedades de configuración de servidor web, *Guía de configuración y mantenimiento de Oracle ILOM 3.1*

▼ Establecimiento de un intervalo de timeout para sesiones web inactivas

Los intervalos de timeout de sesión web de Oracle ILOM proporcionan seguridad para los usuarios con acceso web que se olvidan de cerrar sesión. Los intervalos de timeout de sesión web permiten determinar la cantidad de minutos que pasarán hasta que la sesión web HTTP o HTTPS inactiva se cierre automáticamente. Esta función reduce el riesgo de que un usuario no autorizado encuentre un equipo sin supervisión con una sesión web autenticada establecida en Oracle ILOM.

Para ver o modificar los intervalos de timeout de sesión web establecidos para sesiones HTTP y HTTPS, consulte las siguientes instrucciones basadas en Web.

Antes de empezar

- El intervalo de timeout de sesión web predeterminado establecido para conexiones HTTP y HTTPS es de 15 minutos.

Nota - Si se reduce el timeout de sesión, el usuario podría tener que volver a introducir su nombre de usuario y contraseña con mayor frecuencia cuando las sesiones caduquen. Sin embargo, si se reduce el timeout de sesión, se reduce también la cantidad de tiempo que las sesiones web autenticadas sin supervisión permanecen activas.

- Se necesita el rol Admin (Administrador) (a) para modificar las propiedades del servidor web.
- Las propiedades de intervalo de timeout de sesión HTTP y HTTPS solo se pueden configurar en Oracle ILOM para los SP de servidores que ejecutan la versión de firmware 3.0.4, o versiones posteriores.

1. **Navegue hasta la página Web Server (Servidor web).**

   Por ejemplo:

   - **En la interfaz web 3.0.x, haga clic en Configuration (Configuración) -> System Management Access (Acceso a gestión del sistema) -> Web Server (Servidor web).**
   - **En la interfaz web 3.1, y en versiones posteriores, haga clic en ILOM Administration (Administración de ILOM) -> Management Access (Acceso a gestión) -> Web Server (Servidor web).**

2. **En la página Web Server (Servidor web), realice lo siguiente:**

   a. **Navegue hasta la propiedad HTTP or HTTP Session Timeout (Timeout de sesión HTTP o HTTP).**

   b. **Introduzca un número entre 1 y 720 para especificar la cantidad de minutos que pasarán hasta que la sesión web inactiva se cierre automáticamente.**

   c. **Haga clic en Save (Guardar) para aplicar los cambios.**

Información relacionada

- Propiedades de configuración de servidor web, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Propiedades de configuración de servidor web, *Guía de configuración y mantenimiento de Oracle ILOM 3.1*
- Establecimiento de timeout de sesión, *Guía de procedimientos web para la gestión diaria de Oracle ILOM 3.0*

Configuración de la CLI para máxima seguridad

Consulte los siguientes temas para ver cómo configurar de una mejor manera la interfaz de línea de comandos (CLI) de Oracle ILOM para obtener la máxima seguridad.

Puede configurar las propiedades de gestión de la CLI en Oracle ILOM mediante la interfaz de línea de comandos (CLI) o la interfaz web. Los procedimientos incluidos en esta sección brindan instrucciones de navegación basada en Web para todas las versiones de firmware de Oracle ILOM. Para obtener instrucciones de la CLI u otros detalles sobre las propiedades de configuración, consulte la documentación correspondiente que se muestra en la sección Información relacionada, que aparece después de cada procedimiento.

▼ Establecimiento de un intervalo de timeout para sesiones de CLI inactivas

La CLI de Oracle ILOM, a la cual se accede conectándose a Oracle ILOM mediante el protocolo de shell seguro (SSH) o mediante una conexión serie, admite la configuración de un intervalo de timeout de sesión para el cierre de sesiones de CLI inactivas. Cuando se configura, esta función reduce el riesgo de que un usuario no autorizado encuentre un equipo sin supervisión con una sesión de CLI autenticada en Oracle ILOM.

Para obtener la máxima seguridad, configure el intervalo de timeout de sesión de CLI en cualquier entorno donde la CLI de Oracle ILOM se utilice en una consola compartida. Idealmente, debería establecer el intervalo de timeout de sesión de CLI en 15 minutos o menos.

Para ver o modificar la propiedad de intervalo de timeout establecido para las sesiones de CLI de Oracle ILOM inactivas, consulte las siguientes instrucciones basadas en Web.

Antes de empezar

Antes de empezar

- Se necesita el rol Admin (Administrador) (a) para modificar las propiedades de CLI.
- El valor de intervalo de timeout de sesión de CLI predeterminado para conexiones SSH está desactivado y establecido en 0 (cero) minutos.

Nota - Cuando el intervalo de timeout de CLI está establecido en 0 (cero), Oracle ILOM no cierra las sesiones de CLI inactivas, independientemente del tiempo que una sesión permanezca inactiva.

- La propiedad de intervalo de timeout de sesión de CLI solo se puede configurar en Oracle ILOM para los SP de servidores que ejecutan la versión de firmware 3.0.4, o versiones posteriores.

1. **Navegue hasta la página CLI en la interfaz web de Oracle ILOM.**

   Por ejemplo:

   - **En la interfaz web 3.0.x, haga clic en Configuration (Configuración) -> System Management Access (Acceso a gestión del sistema) -> CLI.**
   - **En la interfaz web 3.1, y en versiones posteriores, haga clic en ILOM Administration (Administración de ILOM) -> Management Access (Acceso a gestión) -> CLI.**

2. **En la página CLI, establezca un intervalo de timeout de sesión de CLI mediante los pasos que se indican a continuación.**

   a. **Seleccione la casilla de verificación Enable (Activar).**

   b. **Introduzca un número entre 1 y 1440 para especificar la cantidad de minutos que pasarán hasta que la sesión de línea de comandos inactiva se cierre automáticamente.**

   c. **Haga clic en Save (Guardar) para aplicar los cambios.**

Información relacionada

- Propiedades de configuración de timeout de sesión de CLI, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Propiedades de configuración de timeout de sesión de CLI, *Guía de configuración y mantenimiento de Oracle ILOM 3.1*
- Establecimiento de timeout de sesión de CLI, *Guía de procedimientos de la CLI para la gestión diaria de Oracle ILOM 3.0*

▼ Uso de claves de servidor para cifrar conexiones SSH

Oracle ILOM proporciona la función del servidor de shell seguro (SSH), que permite a los clientes remotos conectarse a Oracle ILOM y gestionar esta aplicación de manera segura mediante una interfaz de línea de comandos. El protocolo SSH utiliza las claves del servidor para cifrar el canal de gestión y proteger todas las comunicaciones. Los clientes SSH también utilizan estas claves para verificar la autenticidad del servidor SSH.

Oracle ILOM genera un conjunto de claves SSH únicas en el primer inicio de un sistema predeterminado de fábrica. En el caso de que se necesiten nuevas claves de servidor, Oracle ILOM admite la capacidad de generar manualmente claves de servidor SSH adicionales.

Para ver o generar manualmente claves de cifrado de servidor SSH, consulte las siguientes instrucciones basadas en Web.

Antes de empezar

- Se necesita el rol Admin (Administrador) (a) para modificar las propiedades del servidor SSH.

1. **Navegue hasta la página SSH Server (Servidor SSH) en la interfaz web de Oracle ILOM.**

   Por ejemplo:

   - **En la interfaz web 3.0.x, haga clic en System Management (Gestión del sistema) -> SSH Server (Servidor SSH).**
   - **En la interfaz web 3.1, y en versiones posteriores, haga clic en ILOM Administration (Administración de ILOM) -> Management Access (Acceso a gestión) -> SSH Server (Servidor SSH).**

2. **En la página SSH Server (Servidor SSH), revise la información de clave RSA y DSA generada, o realice lo siguiente:**

   a. **Haga clic en Generate RSA Key (Generar clave RSA) para generar una clave nueva.**

   b. **Haga clic en Generate DSA Key (Generar clave DSA) para generar una clave nueva.**

Información relacionada

- Propiedades de configuración de servidor SSH, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Propiedades de configuración de servidor SSH, *Guía de configuración y mantenimiento de Oracle ILOM 3.1*
- Generación de una clave SSH nueva, *Guía de procedimientos web para la gestión diaria de Oracle ILOM 3.0*
- Generación de una clave SSH nueva, *Guía de procedimientos de la CLI para la gestión diaria de Oracle ILOM 3.0*

▼ Cómo agregar claves SSH a cuentas de usuario para la autenticación de CLI automatizada

Los pares de claves SSH generadas de manera personalizada (DSA o RSA) se pueden usar par cuentas de usuario individuales, con la clave pública cargada en Oracle ILOM. Esto resulta útil cuando se usan secuencias de comandos que se ejecutan sin intervención manual y no incluyen contraseñas en texto no cifrado incrustadas. Los usuarios pueden escribir secuencia de comandos que ejecutan comandos de procesador de servicio de manera automática o regular por medio de una conexión SSH basada en red desde un sistema remoto.

Para cargar y agregar una cuenta de Oracle ILOM con una clave SSH pública generada, consulte las siguientes instrucciones basadas en Web.

Antes de empezar

- Genere las claves SSH privada y pública mediante una herramienta de conectividad SSH, como ssh-keygen, y, luego, almacene los archivos de claves SSH generadas en un sistema SSH remoto.
- Se necesita el rol User Management (Gestión de usuarios) (u) para agregar claves públicas SSH a otras cuentas de usuario.
- Se necesita el rol Read Only (Solo lectura) (o) para agregar una clave pública SSH a la cuenta de usuario propia.

1. **Navegue hasta la página User Account (Cuenta de usuario) en la interfaz web de Oracle ILOM.**

   Por ejemplo:

   - **En la interfaz web 3.0.x, haga clic en User Management (Gestión de usuarios) -> User Accounts (Cuentas de usuario).**
   - **En la interfaz web 3.1, y en versiones posteriores, haga clic en ILOM Administration (Administración de ILOM) -> User Management (Gestión de usuarios) -> User Accounts (Cuentas de usuario).**

2. **En la página User Account (Cuenta de usuario), realice lo siguiente:**

   a. **Desplácese hasta la sección SSH Keys (Claves SSH) y haga clic en Add (Agregar).**

   b. **Seleccione una cuenta de usuario de la lista User (Usuario).**

   c. **Seleccione un método de transferencia de la lista y, luego, especifique las propiedades del método de transferencia requeridas para cargar la clave SSH pública.**

3. **Haga clic en Load (Cargar) para cargar la clave SSH pública y agregarla a la cuenta de usuario seleccionada.**

Información relacionada

- Autenticación de CLI con clave SSH local, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Autenticación de CLI con clave SSH local, *Guía de configuración y mantenimiento de Oracle ILOM 3.1*
- Gestión de cuentas de usuario, *Guía de procedimientos web para la gestión diaria de Oracle ILOM 3.0*
- Gestión de cuentas de usuario, *Guía de procedimientos de la CLI para la gestión diaria de Oracle ILOM 3.0*

Configuración del acceso a la gestión de SNMP para máxima seguridad

SNMP es un protocolo estándar utilizado para supervisar o gestionar un sistema. Oracle ILOM proporciona una solución SNMP para supervisión y gestión, pero se debe configurar antes de utilizar. Es importante comprender las implicancias de seguridad de las diversas opciones de SNMP que puede configurar el usuario antes de configurar este servicio. Para obtener información detallada, consulte lo siguiente:

- Uso de la autenticación de usuario y el cifrado de SNMPv3 [47]
- “MIB de SNMP de Sun que admiten objetos configurables” [49]

▼ Uso de la autenticación de usuario y el cifrado de SNMPv3

SNMPv1 y SNMPv2c no proporcionan cifrado y utilizan cadenas comunitarias como forma de autenticación. Las cadenas comunitarias se envían en texto no cifrado por la red y, generalmente, se comparten entre un grupo de personas, en lugar de pertenecer exclusivamente a un usuario. En cambio, SNMPv3 utiliza el cifrado para proporcionar un canal seguro, además de contraseñas y nombres de usuario individuales. Las contraseñas de usuarios de SNMPv3 están localizadas, por lo que se pueden almacenar de manera segura en estaciones de gestión.

SNMPv1, SNMPv2c y SNMPv3 son compatibles con Oracle ILOM y se pueden activar o desactivar por separado. Además, se puede activar o desactivar “sets” para proporcionar una capa adicional de seguridad. Esta opción configurable permite determinar si el servicio SNMP permitirá la configuración de las propiedades de MIB de SNMP configurables. La desactivación de "sets" efectivamente hace que el servicio SNMP solo se pueda utilizar para fines de supervisión.

De forma predeterminada, SNMPv1 y SNMPv2c están desactivados. SNMPv3 está activado de forma predeterminada, pero requiere la creación de uno o varios usuarios de SNMP antes de su uso. No hay usuarios de SNMPv3 preconfigurados.

Para configurar la gestión de SNMP en Oracle ILOM, consulte las siguientes instrucciones basadas en Web.

Antes de empezar

- Para obtener la máxima seguridad de SNMP, utilice SNMPv1 y SNMPv2c solo para fines de supervisión y no active "sets" cuando estos protocolos menos seguros estén activados.
- La propiedad "sets" de SNMP solo se debe activar para la gestión de SNMPv3. La propiedad "sets" de SNMP está desactivada de forma predeterminada.
- La propiedad "sets" de SNMPv3 requiere la configuración de cuentas de usuario de SNMPv3. No se ofrecen cuentas de usuario de SNMPv3 preconfiguradas.
- La propiedad de estado del servicio SNMP está activada de forma predeterminada.
- Se necesitan los privilegios del rol Admin (Administrador) (a) para modificar las propiedades de SNMP.
- Se necesitan los privilegios del rol User management (Gestión de usuarios) (u) para agregar o modificar las cuentas de usuario de SNMPv3.

1. **Navegue hasta la página SNMP en la interfaz web de Oracle ILOM.**

   Por ejemplo:

   - **En la interfaz web 3.0.x, haga clic en System Management Access (Acceso a gestión del sistema) -> SNMP.**
   - **En la interfaz web 3.1, y en versiones posteriores, haga clic en ILOM Administration (Administración de ILOM) -> Management Access (Acceso a gestión) -> SNMP.**

2. **En la página SNMP, vea o modifique las propiedades de SNMP y, luego, haga clic en Save (Guardar) para aplicar los cambios.**

   Para obtener más instrucciones, consulte la documentación mencionada en la sección Información relacionada de este procedimiento. Para los usuarios que ejecutan la versión de firmware 3.2, o una versión posterior, haga clic en el enlace `More details` (Más información) de la página SNMP para obtener más información.

Información relacionada

- Configuración de SNMP, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*

- Configuración de SNMP, *Referencia de gestión de protocolos SNMP e IPMI de Oracle ILOM (firmware 3.2.x)*
- Configuración de SNMP, *Referencia de gestión de protocolos SNMP, IPMI, CIM y WS-MAN de Oracle ILOM 3.1*
- Configuración de SNMP, *Referencia de gestión de protocolos SNMP, IPMI, CIM y WS-MAN de Oracle ILOM 3.0*

MIB de SNMP de Sun que admiten objetos configurables

Las MIB de Sun de Oracle que admiten objetos configurables y para las cuales se aplica “sets” son las siguientes:

- `SUN-HW-CTRL-MIB`: esta MIB se utiliza para configurar políticas de hardware, como políticas de gestión de energía.
- `SUN-ILOM-CONTROL-MIB`: esta MIB se utiliza para configurar funciones de Oracle ILOM, como crear usuarios y configurar servicios.

Nota - Puede establecer un objeto MIB cuando: 1) el objeto MIB admite modificación, 2) el elemento `MAX-ACCESS` para el objeto MIB se establece en `read-write` y 3) el usuario que intenta realizar este establecimiento tiene autorización para hacerlo.

Configuración del acceso a la gestión de IPMI para máxima seguridad

Consulte los siguientes temas para ver cómo configurar el acceso a la gestión de IPMI de Oracle ILOM de la mejor manera para obtener la máxima seguridad.

▼ Uso de IPMI v2.0 para autenticación mejorada y cifrado de paquetes

Aunque Oracle ILOM admite IPMI v1.5 y v2.0 para la gestión remota, los administradores del sistema siempre deben utilizar la interfaz -I lanplus de IPMI v2.0 para gestionar los servidores de Oracle de manera segura. La interfaz -I lanplus brinda autenticación mejorada y controles de integración de datos a partir de la versión 2.0 de IPMI.

A partir de la versión de firmware 3.2.4, Oracle ILOM proporciona una propiedad configurable para activar o desactivar sesiones de IPMI v1.5. Para mayor seguridad, la propiedad de IPMI v1.5 está desactivada de forma predeterminada. Cuando la propiedad de IPMI v1.5 está desactivada, todas las conexiones de sesiones de IPMI v1.5 a Oracle ILOM se impiden (se bloquean).

Consulte el siguiente procedimiento para ver o modificar la propiedad de estado de servicio de IPMI, o la propiedad configurable de IPMI v1.5, que está disponible a partir de la versión de firmware 3.2.4.

Antes de empezar

- Se necesita el rol Admin (Administrador) (a) para modificar las propiedades de IPMI en Oracle ILOM.
- La propiedad de estado del servicio IPMI está activada de forma predeterminada. Antes del primer uso, se deben configurar las cuentas de usuario en Oracle ILOM con los privilegios basados en roles adecuados (Administrator [Administrador], Operator [Operador]) para realizar la funciones de gestión de IPMI.
- Para los SP que ejecutan el firmware 3.2.4 de Oracle ILOM, o una versión posterior, se admiten sesiones de gestión de IPMI v2.0 y, de forma predeterminada, no se admiten sesiones de gestión de IPMI v1.5. Se puede configurar la propiedad de IPMI v1.5 en Oracle ILOM.

Nota - Cuando las sesiones de IPMI v1.5 están desactivadas en Oracle ILOM, los usuarios de IPMItool deben usar la opción -I lanplus de IPMI 2.0.

- Para los SP que ejecutan el firmware 3.2.3 de Oracle ILOM, o versiones anteriores, Oracle ILOM admite sesiones de gestión de IPMI v2.0 y v1.5 No se puede configurar la propiedad de IPMI v1.5 en Oracle ILOM.

Nota - Las sesiones de IPMI v1.5 no admiten autenticación mejorada ni cifrado de paquetes. Para tener acceso a la autenticación mejorada y el cifrado de paquetes de IPMI, debe usar IPMI v2.0.

---

1. **Navegue hasta la página IPMI en la interfaz web de Oracle ILOM.**

   Por ejemplo:

   - **En la interfaz web 3.0, haga clic en Configuration (Configuración) -> System Management Access (Acceso a gestión del sistema) -> IPMI.**

- **En la interfaz web 3.1, y en versiones posteriores, haga clic en ILOM Administration (Administración de ILOM) -> Management Access (Acceso a gestión) -> IPMI.**

2. **En la página IPMI, vea o configure las propiedades de IPMI adecuadas y, luego, haga clic en Save (Guardar) para aplicar los cambios.**

   Para obtener más instrucciones de configuración de IPMI, consulte la documentación adecuada que se muestra a continuación en la sección Información relacionada.

Información relacionada

- Gestión del servidor mediante IPMI, *Referencia de gestión de protocolos SNMP e IPMI de Oracle ILOM (firmware 3.2.x)*
- Gestión del servidor mediante IPMI, *Referencia de gestión de protocolos SNMP, IPMI, CIM y WS-MAN de Oracle ILOM 3.1*
- Gestión del servidor mediante IPMI, *Referencia de gestión de protocolos SNMP, IPMI, CIM y WS-MAN de Oracle ILOM 3.0*
- “Mejores prácticas y directrices de seguridad de IPMI” [51]
- “Compatibilidad con el conjunto de cifrado de autenticación de IPMI 2.0” [52]

Mejores prácticas y directrices de seguridad de IPMI

Para garantizar que las sesiones de gestión del sistema IPMI establecidas sean seguras y no sean vulnerables a los ciberataques, los administradores del sistema:

- Nunca deben establecer sesiones de gestión remota de IPMI con la versión 1.5 de IPMI (interfaz de IPMItool `-I lan`). Deben utilizar explícitamente la versión 2.0 de IPMI cuando usen utilidades de la línea de comandos, como IPMItool (interfaz de IPMItool `-I lanplus`).
- Deben cambiar la contraseña de IPMI de forma regular. Deben asegurarse de que el ciclo de vida de las cuentas de usuario de Oracle ILOM se gestione correctamente.

  Para obtener más información, consulte “Protección del acceso de usuario de Oracle ILOM” [23].
- Deben restringir el acceso a la red desde el exterior. Deben usar el canal de gestión Ethernet dedicado para comunicarse con Oracle ILOM.

  Para obtener más información, consulte “Protección de la conexión de gestión física” [13].
- Deben trabajar con el responsable de seguridad de TI para desarrollar un conjunto de mejores prácticas y políticas de la gestión de servidores y seguridad de IPMI.

Compatibilidad con el conjunto de cifrado de autenticación de IPMI 2.0

Los controles de autenticación, confidencialidad e integridad en la versión 2.0 de IPMI se admiten mediante conjuntos de cifrado. Estos conjuntos de cifrado utilizan el protocolo de intercambio de claves autenticado RMCP+ según se describe en la especificación de IPMI 2.0.

Oracle ILOM admite los siguientes algoritmos de claves de conjuntos de cifrado para establecer sesiones de IPMI 2.0 seguras entre el cliente y el servidor.

- **Conjunto de cifrado 2**: el conjunto de cifrado 2 utiliza los algoritmos de autenticación e integridad.
- **Conjunto de cifrado 3**: el conjunto de cifrado 3 utiliza los 3 algoritmos para autenticación, confidencialidad e integridad.

Nota - Para garantizar que todo el tráfico de IPMI 2.0 esté cifrado, Oracle ILOM no implementa ninguna compatibilidad con el modo de funcionamiento con tipo de cifrado 0 (no cifrado) de IPMI 2.0.

Configuración del acceso a WS-Management para máxima seguridad

A partir de la versión de firmware 3.0.8 y hasta la versión de firmware 3.1.2, Oracle ILOM proporciona una interfaz estándar de servicios web para supervisar el estado del servidor y proporcionar información de inventario mediante un protocolo denominado Ws-Management (Ws-Man).

La interfaz de Ws-Man de Oracle ILOM también permite el control de pares del host y el restablecimiento del SP de Oracle ILOM. Ws-Man es un protocolo basado en el protocolo simple de acceso a objetos (SOAP) que aprovecha los protocolos HTTP(S). La interfaz de Ws-Man de Oracle ILOM se puede utilizar con HTTP o HTTPS como transporte. Si se utiliza HTTPS, el canal se cifra mediante un certificado SSL. Para obtener información sobre los beneficios de seguridad derivados del uso de certificados SSL, además de la diferencia entre certificados autofirmados y certificados de confianza, consulte “Mejora de la seguridad mediante el uso de certificados SSL de confianza y claves privadas” [37].

Utilice esta interfaz de servicios web solo si se utilizan certificados SSL. Para obtener la máxima seguridad, utilice HTTPS como mecanismo de transporte. Para obtener más información sobre la configuración de las propiedades del servidor web, consulte “Configuración de la interfaz web para máxima seguridad” [36].

Mejores prácticas de seguridad posteriores a la implementación para Oracle ILOM

Utilice los siguientes temas para decidir cuáles son las mejores prácticas de seguridad de Oracle para llevar a cabo después de implementar el servidor.

Información relacionada

- Mejores prácticas de seguridad de implementación para Oracle ILOM
- Listas de comprobación de mejores prácticas de seguridad para Oracle ILOM

Mantenimiento de una conexión de gestión segura

Tenga en cuenta la siguiente información para mantener una conexión de gestión segura a Oracle ILOM.

Cómo evitar el acceso no autenticado del dispositivo KCS al host

Los servidores Oracle admiten una conexión estándar de baja velocidad entre el host y Oracle ILOM denominada interfaz KCS (Keyboard Controller Style). Esta interfaz KCS admitida cumple plenamente con la especificación IPMI (Intelligent Platform Management Interface), versión 2.0 y, asimismo, no se puede desactivar.

Si bien el acceso a dispositivo KCS puede ser una manera práctica para configurar Oracle ILOM desde el host, este tipo de acceso también puede presentar riesgos de seguridad, ya que cualquier usuario del sistema operativo que tiene acceso al núcleo o a los controladores del dispositivo físico KCS puede modificar los valores de configuración de Oracle ILOM sin autenticación. Normalmente, solo los usuarios administrador o `root` pueden acceder al dispositivo KCS. Sin embargo, es posible configurar la mayoría de los sistemas operativos para proporcionar mayor acceso al dispositivo KCS.

Por ejemplo, un usuario del sistema operativo con acceso a KCS puede hacer lo siguiente:

- Agregar o crear usuarios de Oracle ILOM.
- Cambiar contraseñas de usuario.
- Acceder a la CLI de Oracle ILOM como administrador de ILOM.
- Acceder a los logs y la información del hardware.

Por lo general, el dispositivo se denomina `/dev/kcs0` o `/dev/bmc` en Linux u Oracle Solaris, y `ipmidrv.sys` o `imbdrv.sys` en Microsoft Windows. El acceso a este dispositivo, al que también se denomina controlador de gestión de placa base (BMC, Baseboard Management Controller) o controlador IPMI, debe ser controlado cuidadosamente mediante el uso de mecanismos de control de acceso adecuados que son parte del sistema operativo host.

Como alternativa al uso del dispositivo KCS de IPMI del host para establecer los valores de configuración de Oracle ILOM, tenga en cuenta el uso de la interfaz de interconexión de Oracle ILOM. Para obtener más detalles, consulte “Acceso de interconexión a host autenticado y preferible” [54].

Para obtener más información sobre cómo controlar o proteger el acceso a dispositivos de hardware, como el dispositivo KCS, consulte la documentación proporcionada con el sistema operativo host.

Acceso de interconexión a host autenticado y preferible

Como una alternativa más rápida a la interfaz KCS, los clientes del sistema operativo host se pueden comunicar con Oracle ILOM mediante una interconexión interna de alta velocidad. La

interconexión es implementada por una conexión interna de Ethernet por USB ejecutando una pila de IP. Se le otorga a Oracle ILOM una dirección IP interna y no enrutable, que un cliente del host puede usar para establecer conexión.

A diferencia de la interfaz KCS, que depende del acceso protegido a un dispositivo de hardware, la interconexión LAN está disponible para todos los usuarios del sistema operativo de forma predeterminada. Por lo tanto, la conexión a Oracle ILOM mediante la interconexión LAN requiere autenticación, tal como si la conexión fuese por la red hacia el puerto de gestión de Oracle ILOM.

Además, todos los servicios o protocolos expuestos en la red de gestión están disponibles para el host mediante la interconexión LAN. Es posible utilizar un explorador web en el host para acceder a la interfaz web de Oracle ILOM o utilizar un cliente de shell seguro para conectarse a la interfaz de línea de comandos de Oracle ILOM. En todos los casos, se deben proporcionar una contraseña y un nombre de usuario válidos para utilizar la interconexión LAN.

La interconexión LAN está desactivada de forma predeterminada. Cuando está desactivada, no hay un dispositivo Ethernet visible para el sistema operativo host, y el canal no existe. Oracle Hardware Management Pack ayuda a aprovisionar y configurar la interconexión LAN.

Para obtener información sobre cómo gestionar Oracle ILOM mediante una interconexión de host dedicada y segura, consulte una de las siguientes fuentes:

- Para las versiones de firmware 3.2 o posteriores, consulte "Conexión de gestión de SP de interconexión dedicada" en la *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2x)*
- Para las versiones de firmware 3.1.x, consulte “Conexión de gestión de SP de interconexión dedicada” en la *Guía de configuración y mantenimiento de Oracle ILOM 3.1*
- Para la versión de firmware 3.0.12 a 3.0.16, consulte "Configuración de interconexión de host local" en la *Guía de procedimientos web de Oracle ILOM 3.0.*

Uso de cifrado IPMI 2.0 para proteger el canal

Intelligent Platform Management Interface (IPMI) versión 2.0 admite un protocolo de red cifrado denominado Remote Management and Control Protocol+ (RMCP+). Este protocolo utiliza un mecanismo de desafío/respuesta basado en claves simétrico para cifrar el canal. Este mecanismo garantiza que no se envíen datos confidenciales no cifrados por la red y que se requiera una contraseña de usuario para cifrar y descifrar el tráfico. Para garantizar que todo el tráfico de IPMI 2.0 esté cifrado, Oracle ILOM no implementa ninguna compatibilidad con el modo de funcionamiento con tipo de cifrado 0 (no cifrado) de IPMI 2.0.

En el caso de IPMItool, utilice el indicador `-I lanplus` para señalar que se debe establecer una sesión RMCP+ cifrada.

Para obtener más información, consulte la documentación de `ipmitool`.

Nota - A partir de la versión de firmware 3.2.4, Oracle ILOM proporciona una propiedad configurable para IPMI 1.5. De forma predeterminada, la propiedad IPMI 1.5 está desactivada. Para obtener más detalles, consulte Uso de IPMI v2.0 para autenticación mejorada y cifrado de paquetes [49].

Uso de protocolos seguros para gestión remota

Oracle ILOM admite diversos protocolos de gestión remota. En algunos casos, se admiten las versiones cifradas y no cifradas del mismo protocolo. Por razones de seguridad, de ser posible, siempre se debe utilizar el protocolo más seguro disponible. Para obtener una lista de protocolos cifrados y no cifrados admitidos, consulte la siguiente tabla.

TABLA 9 Protocolos seguros admitidos

Categoría	Seguro/cifrado	No cifrado
Acceso al explorador web	HTTPS	HTTP
Acceso a la línea de comandos	SSH	Ninguno admitido
Acceso a IPMI	IPMI v2.0	IPMI v1.5
Acceso al protocolo	SNMPv3	SNMPv1/v2c

Establecimiento de una conexión de gestión de red confiable y segura

Todos los servidores de Oracle con Oracle ILOM tienen un puerto de gestión dedicado que se utiliza para conectarse a Oracle ILOM por una red. El uso de un puerto de gestión dedicado proporciona una red privada y segura para la gestión. Algunos sistemas también admiten la gestión de banda lateral que permite que se pueda acceder al host y a Oracle ILOM en los puertos de datos de servidores estándar. El uso de la gestión de banda lateral simplifica la gestión de cables y la configuración de redes, ya que evita la necesidad de llevar a cabo dos conexiones de red separadas. Sin embargo, también significa que el tráfico de Oracle ILOM potencialmente podría ser enviado por una red no confiable si el puerto de gestión de banda lateral o dedicado no estuviera conectado a una red de confianza.

Para mantener el entorno más confiable y seguro para Oracle ILOM, el puerto de gestión de red dedicado o el puerto de gestión de banda lateral del servidor debe estar siempre conectado a una red interna de confianza o a una red privada o de gestión segura dedicada.

Establecimiento de una conexión de gestión serie local segura

Puede conectar localmente un servidor de terminales o una terminal de volcado a Oracle ILOM mediante el puerto de gestión serie físico ubicado en el servidor. Para mantener una conexión de gestión local segura a Oracle ILOM, evite conectar un dispositivo de terminal al puerto de gestión serie local, si el dispositivo también está conectado a una red privada o interna.

Uso de KVMS remoto de manera segura

Oracle ILOM ofrece la posibilidad de redirigir de manera remota el teclado, el video y el mouse del servidor host a un cliente remoto, además de montar el almacenamiento remoto. Estas funciones se denominan, en conjunto, KVMS remoto. El KVMS remoto le permite ver la consola gráfica del sistema operativo host en el servidor mediante la ejecución de aplicaciones Java denominadas Oracle ILOM Remote Console, Remote Console Plus y Storage Redirection CLI en un equipo cliente.

Para garantizar que las sesiones de KVMS remoto y las sesiones serie basadas en texto se inicien de manera segura desde Oracle ILOM, tenga en cuenta lo siguiente:

- “Cifrado y comunicación de KVMS remoto” [57]
- “Protección contra el acceso compartido a KVMS remoto” [58]
- “Protección contra el acceso compartido a la consola host serie” [59]

Cifrado y comunicación de KVMS remoto

Las aplicaciones Oracle ILOM Remote System Console, Remote System Console Plus y Storage Redirection CLI utilizan diversos protocolos de red para comunicarse de forma remota con Oracle ILOM. Mediante estas aplicaciones Java, puede controlar el mouse y el teclado del host y montar un dispositivo de almacenamiento local (como una unidad de CD o DVD) en el servidor remoto.

En la siguiente tabla, se describe en forma más detallada la manera en que se trasmite la información de KVMS remoto por la red.

TABLA 10 Cifrado y funciones de KVMS

Función de KVMS	Cifrada o no cifrada	Descripción
Redirección de mouse	Cifrada	Las coordenadas del mouse se envían de manera segura por la red a Oracle ILOM.

Función de KVMS	Cifrada o no cifrada	Descripción
Redirección de teclado	Cifrada	Cualquier carácter que ingrese en el equipo cliente se transmite hacia Oracle ILOM mediante un protocolo cifrado.
Redirección de video	Cifrada	Los datos de video se transmiten mediante el uso de un protocolo cifrado entre el cliente Java y Oracle ILOM.
Redirección de almacenamiento	No cifrada	Los datos que se leen y se escriben en un dispositivo de almacenamiento se transmiten por la red a Oracle ILOM sin cifrado.

Para obtener una lista de los puertos de red activados mediante KVMS remoto, consulte la Tabla 4, “Servicios y puertos activados de forma predeterminada”.

Protección contra el acceso compartido a KVMS remoto

Una consola de video de KVMS remoto redirige lo que vería si observara un monitor físico conectado a ese servidor. Si bien es posible tener múltiples clientes remotos con sesiones de KVMS en Oracle ILOM, cada sesión mostrará exactamente el mismo video, ya que, por lo general, hay una única salida de video para cada servidor.

Asimismo, cualquier cosa que introduzca en la pantalla desde una sesión de KVMS remoto podrá ser vista por otros usuarios de KVMS conectados al mismo equipo. Lo más importante, si un usuario inicia sesión como usuario con privilegios en el sistema operativo host en las aplicaciones Oracle ILOM Remote Console, Remote Console Plus o Storage Redirection CLI, los demás usuarios de KVMS podrán compartir esa sesión autenticada. Por lo tanto, es importante comprender que la función de KVMS remoto permite conexiones compartidas.

Para evitar que queden sesiones del sistema operativo autenticadas inactivas al finalizar una sesión de redirección de KVMS remoto, debe:

- Configurar Oracle ILOM para bloquear el sistema operativo host de manera automática al finalizar una sesión de redirección de KVMS remoto.

  Para obtener instrucciones, consulte Bloqueo del acceso al host al salir de una sesión de KVMS [32].
- Establecer un intervalo de timeout en el sistema operativo host para cerrar sesiones de usuario autenticadas y desatendidas de manera automática.

  Para obtener instrucciones, consulte la documentación del usuario para el sistema operativo host.

Si es un usuario de Oracle ILOM Remote System Console Plus y necesita limitar el número de sesiones de KVMS iniciadas desde Oracle ILOM que se pueden ver, consulte Limitación de sesiones de KVMS visibles para Remote System Console Plus (3.2.4 o posterior) [33].

Protección contra el acceso compartido a la consola host serie

La consola host de la mayoría de los sistemas operativos también está disponible mediante una consola serie basada en texto. Esta consola se activa ejecutando el comando `start /HOST/console` en la línea de comandos de la CLI de Oracle ILOM. Al igual que la consola gráfica, solo existe una consola serie disponible para todos los usuarios de Oracle ILOM. Por lo tanto, se considera un recurso compartido. Si un usuario inicia sesión en el sistema operativo host desde la consola serie y, a continuación, finaliza la redirección de la consola sin cerrar sesión, el segundo usuario de la consola serie podría acceder a la sesión del sistema operativo autenticada previamente.

Oracle ILOM envía una señal de solicitud de transferencia de datos (DTR) al sistema operativo host cuando finaliza la sesión de redirección de la consola. Muchos sistemas operativos cierran la sesión de un usuario automáticamente cuando se recibe esta señal. Sin embargo, no todos los sistemas operativos admiten esta función:

- Oracle Linux 5 admite la señal DTR que funciona de forma predeterminada.
- Oracle Linux 6 admite DTR, pero se debe activar manualmente.
- Oracle Solaris no admite la señal DTR. Para reducir el riesgo de seguridad, los usuarios pueden configurar el timeout de la sesión en el sistema operativo host.

Para obtener directrices para evitar que queden sesiones del sistema operativo autenticadas inactivas al finalizar una sesión de redirección serie de host, tenga en cuenta lo siguiente:

- Determine si se admite la función de señal DTR en el sistema operativo host y, de ser así, asegúrese de que esta función esté activada de forma predeterminada.

  Para obtener información sobre la señal DTR, consulte la documentación del usuario para el sistema operativo host.
- Configure un intervalo de timeout de sesión en el sistema operativo host.

  Para obtener información sobre cómo establecer un intervalo de timeout de sesión en el sistema operativo host, consulte la documentación del usuario para el sistema operativo host.

Consideraciones posteriores a la implementación para proteger el acceso de usuario

Para garantizar el mantenimiento de un acceso de usuario seguro, tenga en cuenta lo siguiente:

Aplicación de la gestión de contraseñas

Cambie todas las contraseñas de Oracle ILOM regularmente. Esto previene la actividad maliciosa y garantiza que las contraseñas se ajusten a las políticas de contraseñas actuales.

Por lo general, los usuarios cambian sus propias contraseñas; sin embargo, los administradores del sistema con privilegios de gestión de usuarios pueden modificar contraseñas asociadas con otras cuentas de usuario.

Para cambiar la contraseña asociada con una cuenta de usuario de Oracle ILOM, consulte las siguientes instrucciones basadas en Web.

Nota - Para obtener instrucciones de la CLI u otros detalles sobre las propiedades de configuración de gestión de usuarios, consulte la documentación que se muestra en la sección Información relacionada, que aparece en el siguiente procedimiento.

▼ Modificación de contraseña de cuenta de usuario local

Antes de empezar

- Consulte "Directrices de seguridad para la gestión de cuentas de usuario y contraseñas" [25].
- Se necesita el rol User Management (Gestión de usuarios) (u) para modificar contraseñas o privilegios que están asociados a otras cuentas de usuario.
- El rol Operator (Operador) (o) permite a los usuarios modificar la contraseña de sus cuentas.

1. **Navegue hasta la página User Account (Cuenta de usuario) en la interfaz web de Oracle ILOM.**

Por ejemplo:

- **En la interfaz web 3.0.x, haga clic en User Management (Gestión de usuarios) -> User Accounts (Cuentas de usuario).**
- **En la interfaz web 3.1, y en versiones posteriores, haga clic en User Management (Gestión de usuarios) -> User Accounts (Cuentas de usuario).**

2. **En la página User Account (Cuenta de usuario), haga clic en Edit (Editar) para la cuenta que desea modificar.**

   Aparece el cuadro de diálogo Edit: User Name (Editar: nombre de usuario).

3. **En el cuadro de diálogo Edit: User Name (Editar: nombre de usuario), realice lo siguiente:**

   - **Introduzca una contraseña única en el cuadro de texto New Password (Nueva contraseña) y, luego, vuelva a introducir la misma contraseña en el cuadro de texto Confirm New Password (Confirmar nueva contraseña).**
   - **Haga clic en Save (Guardar) para aplicar el cambio.**

Información relacionada

- Configuración de una cuenta de usuario local, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Configuración de una cuenta de usuario local, *Guía de configuración y mantenimiento* de Oracle ILOM 3.1
- Modificación de una cuenta de usuario, *Guía de procedimientos de la CLI para la gestión diaria de Oracle ILOM 3.0*
- Modificación de una cuenta de usuario, *Guía de procedimientos web para la gestión diaria de Oracle ILOM 3.0*

Presencia de seguridad física para el restablecimiento de la contraseña predeterminada de la cuenta `root`

Si se pierde la contraseña de usuario `root` de Oracle ILOM, esta se puede restablecer. Para restablecer la contraseña `root`, conéctese a Oracle ILOM mediante el puerto serie. Si bien, en la mayoría de los casos, la conexión al puerto serie de Oracle ILOM requiere el acceso físico al sistema, la consola serie se puede conectar a un servidor de terminales. El servidor de terminales proporciona eficazmente acceso de red al puerto serie físico.

Para evitar la posibilidad de restablecer la contraseña `root` por la red cuando se utiliza un servidor de terminales, existe la función de comprobación de presencia física para la mayoría de los servidores. Esto requiere pulsar un botón en el servidor para probar el acceso físico al servidor. Para obtener la máxima seguridad, asegúrese de que la función de comprobación de presencia esté activada cada vez que el puerto serie de Oracle ILOM esté conectado al servidor de terminales.

Para ver o modificar la función de comprobación de presencia física, consulte las siguientes instrucciones basadas en Web.

Nota - Para obtener instrucciones de la CLI u otros detalles sobre las propiedades de la cuenta `root`, consulte la documentación que se muestra en la sección Información relacionada, que aparece en el siguiente procedimiento.

▼ Establecimiento de la comprobación de presencia física

Antes de empezar

- El modo de comprobación de presencia física de Oracle ILOM está activado de forma predeterminada.
- Las versiones de firmware 3.1 o posteriores son necesarias para utilizar el modo de comprobación de presencia física en Oracle ILOM.

1. **En la interfaz web de Oracle ILOM, haga clic en ILOM Administration (Administración de ILOM) -> Identification (Identificación).**

2. **En la página Identification (Identificación), vaya hasta la propiedad de comprobación de presencia física y, luego, lleve a cabo una de las siguientes acciones:**

   - **Seleccione la casilla de verificación Physical Presence (Presencia física) para activar la propiedad. Si la propiedad está activada, se debe pulsar el botón Locator (Localizador) del sistema físico para poder recuperar la contraseña predeterminada de Oracle ILOM.**

     O bien:

   - **Desmarque la casilla de verificación Physical Presence (Presencia física) para desactivar la propiedad. Si la propiedad está desactivada, se puede restablecer la contraseña de usuario root de administrador predeterminada de Oracle ILOM sin pulsar el botón Locator (Localizador) del sistema físico.**

3. **Haga clic en Save (Guardar) para aplicar el cambio.**

Información relacionada

- Propiedades de configuración de identificación de dispositivo, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Propiedades de configuración de identificación de dispositivo, *Guía de configuración y mantenimiento de Oracle ILOM 3.1*
- Recuperación de contraseña de cuenta `root` , *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*
- Recuperación de contraseña de cuenta `root`, *Guía de configuración y mantenimiento de Oracle ILOM 3.1*

Supervisión de eventos de auditoría para encontrar acceso no autorizado

El log de auditoría de Oracle ILOM registra todos los cambios de configuración e inicios de sesión. Cada entrada del log de auditoría registra el usuario y el registro de hora asociado con el evento. Los eventos de auditoría pueden ser una herramienta útil para rastrear cambios y, además, para determinar si se han producido cambios o accesos no autorizados en Oracle ILOM.

Para visualizar eventos en el log de auditoría de Oracle ILOM, consulte las siguientes instrucciones basadas en Web.

Nota - Para obtener instrucciones de la CLI u otros detalles sobre el log de auditoría, consulte la documentación que se muestra en la sección Información relacionada del siguiente procedimiento.

▼ Visualización de log de auditoría

Antes de empezar

- El log de auditoría está disponible en Oracle ILOM a partir de la versión de firmware 3.1. En las versiones anteriores al firmware 3.1, los eventos de auditoría se capturaban en el log de eventos de Oracle ILOM.
- Se necesitan los privilegios del rol Admin (Administrador) (a) en Oracle ILOM para borrar entradas del log de auditoría.

1. **En la interfaz web, haga clic en ILOM Administration (Administración de ILOM) -> Logs -> Audit (Auditoría).**

2. **En la página Audit log (Log de auditoría), utilice los controles para filtrar las entradas del log o para borrar eventos del log.**

   Los usuarios que ejecutan versiones de firmware 3.2 o posteriores, deben hacer clic en el enlace `More details` (Más detalles) en la página Audit (Auditoría) para obtener más información.

Información relacionada

- Gestión de entradas de log de Oracle ILOM, *Guía del usuario para supervisión y diagnóstico del sistema de Oracle ILOM (firmware 3.2.x)*
- Gestión de entradas de log de Oracle ILOM, *Guía del usuario de Oracle ILOM 3.1*

Acciones posteriores a la implementación para la modificación del modo FIPS

A partir de la versión de firmware 3.2.4, Oracle ILOM proporciona una propiedad configurable para el cumplimiento con FIPS. De forma predeterminada, esta propiedad está desactivada. Una vez que se modifica el estado operativo del cumplimiento con FIPS en Oracle ILOM, se restablecen los valores de configuración predeterminados de fábrica de todas las propiedades de configuración definidas por el usuario. Para evitar la pérdida de valores de configuración definidos por el usuario en Oracle ILOM, el cumplimiento con FIPS debe ser modificado antes de configurar cualquier otro valor de configuración de Oracle ILOM. Si el cumplimiento con FIPS debe modificarse después de la implementación de la configuración de Oracle ILOM, consulte las siguientes instrucciones para evitar la pérdida de valores de configuración definidos por el usuario.

▼ Modificación del modo FIPS posterior a la implementación

Utilice este procedimiento si necesita modificar el estado operativo del modo FIPS después de realizar una actualización de firmware o de especificar propiedades de configuración definidas por el usuario en Oracle ILOM.

Nota - El modo de cumplimiento con FIPS en Oracle ILOM está representado por propiedades de condición y estado. La propiedad de condición representa el modo configurado en Oracle ILOM, y la propiedad de estado representa el modo operativo en Oracle ILOM. Cuando la propiedad FIPS State (Condición de FIPS) se modifica, el cambio no afecta al modo operativo (propiedad FIPS Status [Estado de FIPS]) hasta el próximo reinicio de Oracle ILOM.

Antes de empezar

- La propiedad configurable del cumplimiento con FIPS está disponible en Oracle ILOM a partir del firmware 3.2.4 o versiones posteriores. Para las versiones anteriores al firmware 3.2.4, Oracle ILOM no proporciona una propiedad configurable para el cumplimiento con FIPS.
- Cuando FIPS está activado (configurado y operativo) algunas funciones no se admiten en Oracle ILOM. Para obtener una lista de funciones no admitidas cuando FIPS está activado, consulte "Funciones no admitidas cuando el modo FIPS está activado" [17].
- Se necesita el rol de Admin (Administrador) (a) para realizar este procedimiento.

1. **En la interfaz web de Oracle ILOM, haga una copia de seguridad de la configuración de Oracle ILOM.**

   Por ejemplo:

   a. **Haga clic en ILOM Administration (Administración de ILOM) -> Configuration Management (Gestión de configuración) -> Backup/Restore (Copia de seguridad/Restauración).**

   b. **En la página Backup/Restore (Copia de seguridad/Restauración), haga clic en el enlace More details... (Más detalles) para obtener más instrucciones.**

Nota - Para simplificar la reconexión a Oracle ILOM después de actualizar el firmware, debe activar las opciones de actualización de firmware para conservar la configuración.

Nota - Si realiza el paso 2 antes del paso 1, deberá editar el archivo de configuración XML con copia de seguridad y eliminar la configuración de FIPS. De lo contrario, tendrá una configuración incoherente entre el archivo XML de Oracle ILOM con copia de seguridad y el estado de modo FIPS operativo que se ejecuta en el servidor, lo cual no está permitido.

---

2. **Si es necesaria una actualización de firmware, siga los siguientes pasos:**

   a. **Haga clic en ILOM Administration (Administración de ILOM) -> Maintenance (Mantenimiento) -> Firmware Update (Actualización de firmware).**

   b. **En la página Firmware Update (Actualización de firmware), haga clic en el enlace More details... (Más detalles) para obtener más instrucciones.**

3. **Modifique el modo de cumplimiento con FIPS en Oracle ILOM de la siguiente manera:**

a. **Haga clic en ILOM Administration (Administración de ILOM) -> Management Access (Acceso a gestión) -> FIPS.**

b. **En la página FIPS, haga clic en el enlace `More details` (Más detalles) para obtener instrucciones sobre cómo hacer lo siguiente:**

   - **Modificar la configuración de FIPS State (Condición de FIPS).**
   - **Actualizar el estado operativo de FIPS en el sistema mediante el restablecimiento del SP.**

4. **Restaurar la configuración de Oracle ILOM con copia de seguridad de la siguiente manera:**

   a. **Haga clic en ILOM Administration (Administración de ILOM) -> Configuration Management (Gestión de configuración) -> Backup/Restore (Copia de seguridad/Restauración).**

   b. **En la página Backup/Restore (Copia de seguridad/Restauración), haga clic en el enlace `More details` (Más detalles) para obtener más instrucciones.**

Información relacionada

- “Cómo decidir si se debe configurar el modo FIPS en la implementación” [14]
- “Funciones no admitidas cuando el modo FIPS está activado” [17]
- Configuración de propiedades de modo FIPS, *Guía del administrador para configuración y mantenimiento de Oracle ILOM (firmware 3.2.x)*

Actualización a las versiones de firmware y software más recientes

Mantenga actualizadas las versiones de software y firmware del servidor.

- Consulte regularmente si se publicaron actualizaciones en My Oracle Support.
- Instale siempre las versiones de firmware y software más recientes disponibles para el servidor le permitirá aprovechar las correcciones de errores y las mejoras.
- Instale los parches de seguridad necesarios para el software instalado.

Para actualizar el firmware de Oracle ILOM en el servidor, consulte las siguientes instrucciones.

▼ Actualización del firmware de Oracle ILOM

Antes de empezar

- Se necesita el rol Admin (Administrador) (a) en Oracle ILOM para actualizar el firmware de Oracle ILOM.
- Notifique a todos los usuarios de Oracle ILOM de la actualización programada de firmware y pídales que cierren todas las sesiones de cliente hasta que finalice la actualización de firmware.
- El proceso de actualización de firmware requiere varios minutos para finalizar y, durante este tiempo, no se deben realizar otras tareas de Oracle ILOM.

1. **Descargue la actualización de software más reciente disponible para el servidor desde el sitio web My Oracle Support (MOS).**

   De ser necesario, consulte la documentación que se proporciona con el servidor para obtener instrucciones sobre cómo obtener actualizaciones de software de MOS.

   Nota - La versión de firmware de Oracle ILOM más reciente disponible para el servidor se incluye en el parche de software más reciente publicado en MOS para el servidor.

   ---

2. **Coloque la imagen de firmware en una unidad local o de red compartida.**

3. **Vaya hasta la página Firmware Update (Actualización de firmware) en la interfaz web.**

   Por ejemplo:

   - **En la interfaz web 3.0.x, haga clic en Maintenance (Mantenimiento) -> Firmware.**
   - **En la interfaz web 3.1, o en versiones posteriores, haga clic en ILOM Administration (Administración de ILOM) -> Maintenance (Mantenimiento) -> Firmware Upgrade (Actualización de firmware).**

4. **En la página Firmware Upgrade (Actualización de firmware), haga clic en el modo Enter Firmware Upgrade (Introducir actualización de firmware) y, luego, siga las indicaciones.**

   Para usuarios con firmware de Oracle ILOM 3.2 o posterior, haga clic en el enlace `More details` (Más detalles) de la página Firmware Upgrade (Actualización de firmware).