Guía de seguridad del sistema modular Netra

Referencia: E68384-01
Agosto de 2015

Referencia: E68384-01

Copyright © 2015, Oracle y/o sus filiales. Todos los derechos reservados.

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

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

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

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

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

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

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

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

Accesibilidad a la documentación

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

Acceso a Oracle Support

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

Contenido

Visión general de la seguridad 7
Principios básicos de seguridad 7
Consideraciones de seguridad avanzada 8
Funciones de seguridad 9
Aislamiento del tráfico de red 9
Oracle ILOM para gestión segura 9

Planificación de un entorno seguro 11
Red por defecto 11
Cuentas de usuario 12
Configuración de seguridad por defecto 12

Protección del hardware 13
Restricciones de acceso 13
Números de serie 14
Unidades de disco duro 14

Protección del software 15
▼ Prevención del acceso no autorizado (Oracle Linux) 15
▼ Prevención del acceso no autorizado (Oracle ILOM) 15
▼ Prevención del acceso no autorizado (Oracle VM Server con Oracle Linux) 15
Seguridad de Oracle Hardware Management Pack 16

Ubicación de guías de seguridad relacionadas 17
Guías de seguridad 17

Visión general de la seguridad

Sistema modular Netra de Oracle es una plataforma preintegrada y precableada que se puede virtualizar por completo para reducir los costos y el tiempo de despliegue en el centro de datos. El sistema modular incluye el hardware que se especificó y se lo envía después del ensamblaje en la fábrica.

En estos temas, se describen conceptos y características de seguridad para el sistema modular:

- "Principios básicos de seguridad" [7]
- "Consideraciones de seguridad avanzada" [8]
- "Funciones de seguridad" [9]

Principios básicos de seguridad

Siga estos principios de seguridad básicos para todo el software y el hardware del sistema modular.

- Autenticación: la autenticación indica la manera en que se identifica un usuario, generalmente mediante información confidencial, como nombre de usuario y contraseña, o claves compartidas. La autenticación garantiza que los usuarios del hardware o software sean quienes dicen ser. Por defecto, se usan los nombres de usuario y las contraseñas locales para la autenticación. También se puede usar la autenticación basada en claves compartidas.
- Cuentas y auditoría: la función de cuentas y auditoría se usa para mantener un registro de la actividad de un usuario en el sistema. Las funciones de software y de hardware del sistema modular permiten a los administradores supervisar la actividad de conexión y mantener inventarios de hardware.
  - Las conexiones de usuario se supervisan mediante los logs del sistema. Las cuentas de administrador del sistema y de servicio tienen acceso a comandos que, si se usan de manera incorrecta, pueden provocar daños y pérdida de datos.
  - El seguimiento de los activos de hardware se hace mediante números de serie. Los números de referencia de Oracle se registran electrónicamente en tarjetas, los módulos y las placas base, y pueden utilizarse para el inventario.

Consideraciones de seguridad avanzada

Además de los principios de seguridad básicos, el sistema modular ofrece supervivencia y protección profunda. El sistema modular ofrece un conjunto bien integrado de capacidades de seguridad para satisfacer requisitos e inquietudes de seguridad importantes. En las siguientes secciones, se describen estos principios:

- Supervivencia de cargas de trabajo de misión crítica: las organizaciones que seleccionen plataformas de hardware y software para cargas de trabajo de misión crítica pueden tener la tranquilidad de que el sistema modular puede evitar o minimizar el daño ocasionado por acciones accidentales y maliciosas realizadas por usuarios internos o partes externas. Como parte de las mejores prácticas de Oracle Maximum Availability Architecture, las siguientes prácticas aumentan la supervivencia:
  - Se garantiza que los componentes utilizados se crearon, diseñaron y probaron con el fin de que funcionen bien juntos en función de las arquitecturas de despliegue seguras. El sistema modular es compatible con funciones de aislamiento seguro, control de acceso, calidad de servicio y gestión segura.
  - La reducción de la superficie de ataque por defecto de los productos incluidos ayuda a minimizar la exposición total del equipo.
  - Se proporciona protección del equipo, incluidas las interfaces operativa y de gestión, mediante un complemento de protocolos abiertos y verificados, y API que pueden respaldar los objetivos de seguridad tradicionales de autenticación compleja, control de acceso, confidencialidad, integridad y disponibilidad.
  - Se verifica que el software y el hardware incluyan características que mantengan el servicio disponible incluso después de que se produzcan fallos. Estas capacidades son útiles en casos en los que los atacantes intentan desactivar uno o varios componentes individuales del sistema.
- Protección profunda para el entorno operativo: el sistema modular emplea varios controles de seguridad independientes y que se refuerzan entre sí, lo cual ayuda a crear un entorno operativo seguro para cargas de trabajo y datos. El sistema modular aplica el principio de protección profunda de la siguiente manera:
  - Mediante un complemento sólido de funciones para proteger la información en tránsito, en uso e inactiva. Los controles de seguridad están disponibles en las capas de la red y del servidor. Los controles de seguridad únicos de cada capa se pueden integrar con los otros controles para generar arquitecturas de seguridad sólidas y organizadas en capas.
  - Mediante la compatibilidad con el uso de interfaces, protocolos y estándares bien definidos y abiertos. El sistema modular se puede integrar con políticas de seguridad, arquitecturas, prácticas y estándares existentes.

Funciones de seguridad

El hardware y el software del sistema modular están reforzados. Oracle también proporciona configuraciones seguras recomendadas para servicios como NTP y SSH. Asimismo, la arquitectura del sistema modular proporciona capacidades de seguridad para los componentes principales. Estas capacidades de seguridad son aplicadas con mayor frecuencia por organizaciones que despliegan una estrategia de seguridad en capas. Las capacidades se agrupan en las siguientes categorías:

- "Aislamiento del tráfico de red" [9]
- "Oracle ILOM para gestión segura" [9]

Aislamiento del tráfico de red

Si desea consolidar la infraestructura de TI, implementar arquitecturas de servicios compartidos y proporcionar servicios seguros multi-inquilino, considere aislar el tráfico de red. El sistema modular proporciona la flexibilidad para implementar las políticas y las estrategias de aislamiento en función de las necesidades.

En el nivel de la red física, el acceso de los clientes está aislado de la gestión de los dispositivos y de la comunicación entre dispositivos. El tráfico de la red de gestión y de clientes se aísla en redes independientes. El acceso de los clientes se proporciona a través de una red Ethernet de 10 Gbps redundante que garantiza un acceso fiable de alta velocidad a los servicios que se ejecutan en el sistema. El acceso de gestión se proporciona a través de una red Ethernet de 1 Gbps físicamente independiente. Esto proporciona una separación entre las redes operativa y de gestión.

Las organizaciones pueden elegir separar aún más el tráfico de la red Ethernet de acceso de los clientes mediante la configuración de LAN virtuales (VLAN). Las VLAN separan el tráfico de red en función de sus requisitos. Oracle recomienda el uso de protocolos cifrados mediante VLAN para garantizar la confidencialidad y la integridad de las comunicaciones.

Oracle ILOM para gestión segura

Los conjuntos de controles y capacidades de seguridad son necesarios para proteger correctamente las aplicaciones y los servicios individuales. Es igualmente importante tener capacidades de gestión integrales para mantener la seguridad de los servicios y los sistemas desplegados. El sistema modular usa las capacidades de gestión de seguridad de Oracle ILOM.

Oracle ILOM es un SP que está incrustado en los nodos de cálculo del sistema modular. Oracle ILOM se usa para realizar actividades de gestión fuera de banda, como las siguientes:

- Proporcionar acceso seguro para realizar la gestión segura fuera de banda de la base de datos y los servidores de almacenamiento. El acceso incluye acceso basado en web protegido por SSL, acceso de línea de comandos mediante shell seguro, y los protocolos IPMI v2.0 y SNMPv3.
- Separar los requisitos de tareas mediante un modelo de control de acceso basado en roles. Los usuarios individuales se asignan a roles específicos que limitan las funciones que pueden realizar.
- Proporcionar un registro de auditoría de todas las conexiones y los cambios de configuración. Cada entrada del log de auditoría muestra el usuario que realizó la acción y un registro de hora. El registro de auditoría permite a las organizaciones detectar actividades o cambios no autorizados y atribuir esas acciones a usuarios específicos.

Para obtener más información acerca de la seguridad de Oracle ILOM, consulte la *Guía de seguridad de Oracle ILOM* en `http://www.oracle.com/goto/ILOM/docs`.

Planificación de un entorno seguro

Implemente directrices de seguridad antes de la llegada de Sistema modular Netra. Después de haber instalado el sistema, revise y ajuste periódicamente las directrices de seguridad para permanecer actualizado respecto de los requisitos de seguridad de la organización.

En estos temas, se proporcionan directrices de seguridad para la instalación de Sistema modular Netra:

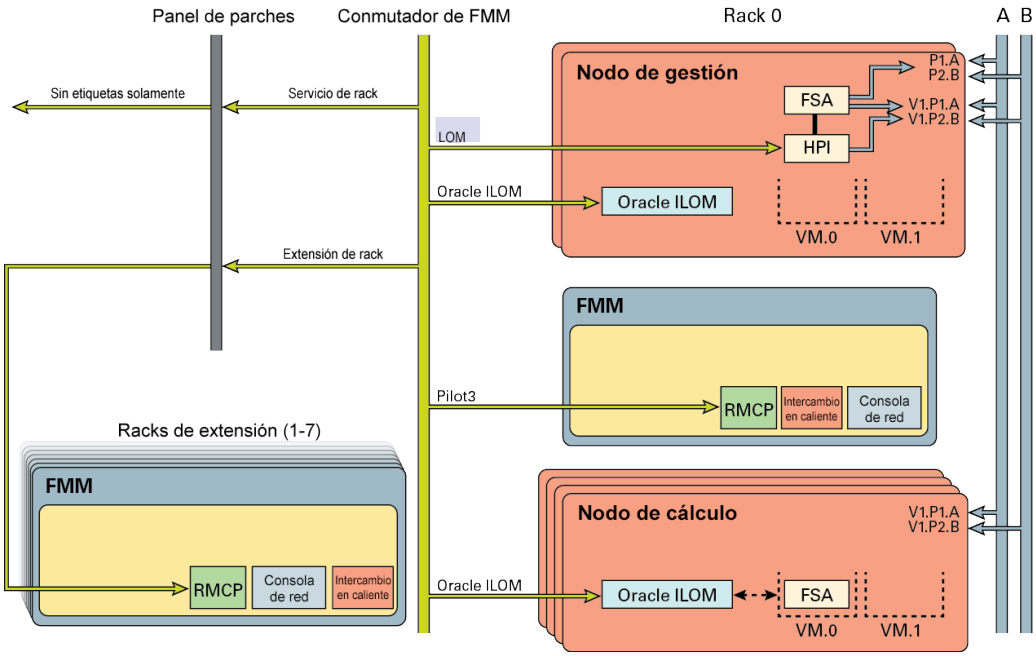
- "Red por defecto" [11]
- "Cuentas de usuario" [12]
- "Configuración de seguridad por defecto" [12]

Póngase en contacto con el responsable de la seguridad de TI para conocer los requisitos de seguridad adicionales relacionados con el sistema y el entorno específico.

Red por defecto

En la figura y las descripciones que aparecen a continuación, se explica la red por defecto de Sistema modular Netra.

- La red de telemetría/sistema (red con luz verde) incluye el puerto de LOM del nodo de gestión en VLAN 4090 por medio del conmutador de FMM.
- La red de ILOM de telemetría en una VLAN 4094 interna con FMM incluye Oracle ILOM de nodos de cálculo y Oracle ILOM de nodos de red por medio del conmutador de FMM.
- El panel de parches extiende la red de telemetría a los racks 1 a 7. Una configuración de varios racks admite las mismas subredes y VLAN con un ID de rack distinto
- La VLAN(1) proporciona otros servicios a la red de telemetría mediante la autenticación adecuada.
- Las redes de datos (A y B) proporcionan acceso en banda al nodo del FSA.
- La aplicación HA puede gestionar los racks mediante las interfaces expuestas del sistema modular (JMX, C- API, etc.).



Cuentas de usuario

En esta tabla, se enumeran los usuarios y las contraseñas por defecto para los componentes del sistema modular. Cambie todas las contraseñas por defecto después de instalar Sistema modular Netra.

Componente	Nombre de usuario y contraseña
Conmutadores Ethernet	`root/changeme` **Nota -** Proteja los valores `enable mode password` y `secret` para el usuario `admin`.
Nodos de gestión y de cálculo	`root/changeme`

Configuración de seguridad por defecto

El sistema modular se instala con muchos parámetros de seguridad configurados por defecto. Cuando sea posible y resulte práctico, configure los parámetros de seguridad por defecto. Consulte los parámetros de seguridad por defecto en su versión de Oracle ILOM, en `http://www.oracle.com/goto/ILOM/docs`.

Protección del hardware

El aislamiento físico y el control de acceso son la base para crear la arquitectura de seguridad. Garantizar que el sistema físico esté instalado en un entorno seguro permite proteger el sistema contra el acceso no autorizado. De manera similar, el registro de todos los números de serie ayuda a evitar el uso no autorizado de los componentes de hardware.

En estas secciones, se proporcionan directrices generales de seguridad de hardware para el sistema modular.

- "Restricciones de acceso" [13]
- "Números de serie" [14]
- "Unidades de disco duro" [14]

Restricciones de acceso

- Instale sistemas y equipos relacionados en una habitación cerrada con llave y de acceso restringido.
- Si el equipo se instala en un rack con una puerta con llave, cierre siempre la puerta hasta que se tenga que reparar algún componente dentro del rack. Cerrar las puertas también restringe el acceso a dispositivos de conexión o intercambio en caliente.
- Almacene las piezas de repuesto en un armario cerrado. Restrinja el acceso al armario cerrado a personal autorizado.
- Verifique periódicamente el estado y la integridad de las cerraduras del rack y el armario de repuestos para brindar protección contra la manipulación de cerraduras o puertas abiertas accidentalmente, o para detectar si esto ha sucedido.
- Almacene las llaves del armario en una ubicación segura con acceso limitado.
- Restrinja el acceso a consolas USB. Los dispositivos como los controladores del sistema, las PDU y los conmutadores de red pueden tener conexiones USB. El acceso físico es un método más seguro para acceder a un componente, ya que elimina la posibilidad de ataques basados en red.
- Conecte la consola a un KVM externo para hacer posible el acceso remoto a la consola. Generalmente, los dispositivos KVM son compatibles con la autenticación de doble factor, el control de acceso centralizado y la auditoría. Para obtener más información sobre las directrices de seguridad y las mejores prácticas para los KVM, consulte la documentación incluida con el dispositivo KVM.

Números de serie

Evite el uso no autorizado de los componentes de hardware; para ello, registre cuidadosamente todos los números de serie que se reciben y se colocan en el inventario. Antes de instalar o usar un componente, confirme su autenticidad mediante la comparación del número de serie con el número que se registró cuando se recibió el componente. Siga estas prácticas para proteger el hardware:

- Mantenga un registro de los números de serie de todo el hardware.
- Realice una marca de seguridad en todos los elementos importantes del hardware de la computadora, como las piezas de repuesto. Utilice plumas ultravioleta o etiquetas en relieve especiales.
- Mantenga las licencias y las claves de activación de hardware en una ubicación segura y de fácil acceso para el administrador del sistema en caso de una emergencia del sistema. Los documentos impresos podrían ser su única prueba para demostrar la propiedad.

Los lectores inalámbricos de identificación por radiofrecuencia (RFID) pueden simplificar aún más el seguimiento de activos. Consulte las notas del producto de Oracle, *Cómo realizar un seguimiento de sus activos del sistema Oracle Sun mediante RFID*, en `http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf`.

Unidades de disco duro

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

- Consulte sus políticas de protección de datos para determinar el método más apropiado para sanear los discos duros.
- Si es necesario, aproveche el servicio de retención de dispositivos y datos de clientes de Oracle.

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

Protección del software

La mayoría de las medidas de seguridad del hardware se implementan por medio de medidas de software. En estas secciones, se proporcionan directrices generales de seguridad de software para Sistema modular Netra.

- Prevención del acceso no autorizado (Oracle Linux) [15]
- Prevención del acceso no autorizado (Oracle ILOM) [15]
- Prevención del acceso no autorizado (Oracle VM Server con Oracle Linux) [15]
- "Seguridad de Oracle Hardware Management Pack" [16]

Prevención del acceso no autorizado (Oracle Linux)

- **Use los comandos del sistema operativo Oracle Linux para restringir el acceso al software, reforzar el sistema operativo, usar las funciones de seguridad y proteger las aplicaciones.**

  Consulte *Oracle Linux: Guía de seguridad para la versión 6* en `http://docs.oracle.com/cd/E37670_01/E36387/html/index.html`.

Prevención del acceso no autorizado (Oracle ILOM)

- **Use los comandos de Oracle ILOM para restringir el acceso al firmware de Oracle ILOM, cambiar la contraseña predeterminada de fábrica, limitar el uso de la cuenta de superusuario root y proteger la red privada del SP.**

  Consulte su versión de la *Guía de seguridad de Oracle ILOM* en `http://www.oracle.com/goto/ILOM/docs`.

Prevención del acceso no autorizado (Oracle VM Server con Oracle Linux)

- **Use los comandos de Oracle Linux para restringir el acceso al software Oracle VM Server, usar funciones de seguridad y proteger las aplicaciones.**

Consulte la *Guía de seguridad de Oracle VM para la versión 3.3* en http://docs.oracle.com/cd/E50245_01/E50254/html/index.html.

Seguridad de Oracle Hardware Management Pack

Oracle Hardware Management Pack cuenta con dos componentes: un agente de supervisión SNMP y una familia de herramientas de interfaz de línea de comandos (herramientas CLI) compatibles con distintos sistemas operativos para gestionar el servidor.

- Plugins de SNMP de Hardware Management Agent: SNMP es un protocolo estándar que supervisa o gestiona un sistema. Con los plugins de SNMP de Hardware Management Agent, puede usar SNMP para supervisar los sistemas Oracle en el centro de datos, sin necesidad de conectarse a dos puntos de gestión (el host y Oracle ILOM). Esta funcionalidad le permite usar una dirección IP única (la dirección IP del host) para supervisar varios sistemas.

  Los plugins de SNMP se ejecutan en el sistema operativo host de los sistemas de Oracle. El plugin de SNMP extiende el agente SNMP nativo en el sistema operativo host a fin de proporcionar capacidades adicionales de MIB de Oracle. Oracle Hardware Management Pack no incluye un agente SNMP. Para Oracle Linux, se agrega un módulo al agente `net-snmp`. Para Microsoft Windows, el plugin extiende el servicio SNMP nativo. La configuración de seguridad relacionada con SNMP para Oracle Hardware Management Pack es determinada por la configuración de un servicio o agente SNMP nativo, no por el plugin.

  Tenga en cuenta que SNMPv1 y SNMPv2c no proporcionan cifrado y utilizan cadenas comunitarias como forma de autenticación. SNMPv3 es más seguro y es la versión recomendada, ya que utiliza el cifrado para proporcionar un canal seguro, además de nombres de usuario y contraseñas individuales.
- Documentación de Oracle Hardware Management Pack: para obtener directrices de seguridad específicas de Oracle Hardware Management Pack, consulte la *Guía de seguridad de Oracle Hardware Management Pack (HMP)* en http://www.oracle.com/goto/OHMP/docs.

Ubicación de guías de seguridad relacionadas

Guías de seguridad

En estas guías, se describen políticas y procedimientos para proteger productos relacionados:

- *Oracle Server X5-2 Security Guide*
- *Oracle Switch ES2-72 and Oracle Switch ES2-64 Security Guide*
- *Oracle Linux: Guía de seguridad para la versión 6* en `http://docs.oracle.com/cd/E37670_01/E36387/html/index.html`
- *Guía de seguridad de Oracle ILOM* en `http://www.oracle.com/goto/ILOM/docs`
- *Guía de seguridad de Oracle VM para la versión 3.3* en `http://docs.oracle.com/cd/E50245_01/E50254/html/index.html`
- *Guía de seguridad de Oracle Hardware Management Pack (HMP)* en `http://www.oracle.com/goto/OHMP/docs`