Guía de usuario de HP Integrated Lights-Out 2
para las versiones 1.75 y 1.77 del firmware

Referencia 394326-079

Abril de 2009 (Novena edición)

Público al que va dirigido

Esta guía está dirigida a la persona encargada de la instalación, administración y solución de problemas de los servidores y sistemas de almacenamiento. HP le considera una persona cualificada para la reparación de los equipos informáticos y preparada para reconocer las dificultades de los productos con niveles de energía peligrosos.

Tabla de contenido

1 Introducción al funcionamiento

En esta sección:

Introducción a la guía

HP iLO 2 proporciona varios modos de configurar, actualizar y utilizar servidores de forma remota. En la *Guía de usuario de HP Integrated Lights-Out 2* se describen estas funciones y el uso que reciben con la utilidad de configuración basada en ROM (RBSU, ROM-Based Setup Utility) y la interfaz basada en explorador. Algunas de estas funciones disponen de licencias y únicamente es posible acceder a ellas tras adquirir una licencia opcional. Si desea obtener más información, consulte "Concesión de licencias (Concesión de licencias en la página 21)".

En la *Guía de recursos de líneas y secuencias de comandos del procesador de gestión HP Integrated Lights-Out* se describen la sintaxis y las herramientas disponibles para utilizar iLO 2 a través de una línea de comandos o una interfaz de secuencias de comandos.

En esta documentación se describe HP Integrated Lights-Out para servidores ProLiant ML/DL, así como los blades de servidor BladeSystem de ProLiant. Si desea obtener información acerca de iLO para servidores y blades de servidor Integrity, consulte la página Web de HP (http://www.hp.com/go/integrityiLO.)

En esta guía se incluye información acerca de las versiones 1.11, 1.2x, 1.3x, 1.70, 1.75 y 1.77 del firmware de iLO 2.

Novedades de esta versión de iLO 2

La versión 1.77 de iLO 2 permite optimizar el aprovechamiento de la energía mediante la utilización de un modo de alimentación HEM (High Efficiency Mode, Modo de alta eficacia.) Si desea obtener más información, consulte "Eficacia de la alimentación (Eficacia de la alimentación en la página 134)".

La versión 1.75 de iLO 2 añade compatibilidad para:

- Compatibilidad con el modelo con licencia: iLO 2 ofrece las licencias de iLO Advanced e iLO Advanced para BladeSystem en forma de actualizaciones que se pueden comprar de las funciones de gestión remota estándar que se encuentran disponibles en HP ProLiant y BladeSystem. Para obtener más información, consulte la página Web de HP (http://www.hp.com/go/ilo.)
- Compatibilidad mejorada con cuentas de directorio para hasta 15 contextos de búsqueda.
- Compatibilidad de los servicios de directorio con Windows 2008 Active Directory.

- Generación de informes de estado de la temperatura de las unidades, cuando es compatible con la plataforma.
- Servidores adicionales:
  - ProLiant BL260c G6
  - ProLiant BL460c G6
  - ProLiant BL490c G6
  - ProLiant DL320 G6
  - ProLiant DL360 G6
  - ProLiant DL380 G6
  - ProLiant ML310 G5p
  - ProLiant ML330 G6
  - ProLiant ML350 G6
  - ProLiant ML370 G6

Perspectiva general de iLO 2

iLO 2 puede realizar de forma remota muchas funciones que normalmente requieren la visita a los servidores del centro de datos, la sala de ordenadores o la ubicación remota. A continuación, se presentan algunos ejemplos sobre el uso de las funciones de iLO 2.

- La consola remota de iLO 2 y la alimentación virtual permiten visualizar un servidor remoto bloqueado en situaciones de pantalla azul y reiniciar el servidor sin asistencia in situ.
- La consola remota de iLO 2 permite cambiar la configuración del BIOS, si fuera necesario.
- La tecnología Virtual KVM de iLO 2 ofrece una consola remota de alto rendimiento que permite la administración remota de sistemas operativos y aplicaciones en situaciones habituales.
- El CD/DVD-ROM o disquete virtuales de iLO 2 permiten la instalación de un sistema operativo o firmware del sistema de memoria flash a través de la red desde las imágenes de estaciones de trabajo o de servidores Web centralizados.
- La carpeta virtual de iLO 2 permite actualizar los controladores del sistema operativo o copiar los archivos del sistema sin soporte físico o sin crear una imagen de disco.
- Las secuencias de comandos de iLO 2 permiten utilizar alimentación y soportes virtuales en otras herramientas de secuencias de comandos para automatizar las tareas de implementación y aprovisionamiento.
- iLO 2 participa activamente en la supervisión y el mantenimiento del estado del servidor, denominado como estado integrado. iLO 2 controla las temperaturas del servidor y envía señales de corrección a los ventiladores para mantener una refrigeración adecuada de este. Además de la supervisión de la temperatura, iLO 2 dispone de supervisión del estado del ventilador, del estado de los suministros de alimentación, de los reguladores de tensión y de las unidades de disco duro internas.

Estos son sólo algunos ejemplos de los modos en que puede utilizar iLO 2 para gestionar servidores HP ProLiant desde la oficina, hogar o lugar de viaje. Cuando comience a utilizar iLO 2 y a definir sus propios requisitos de infraestructura, consulte esta guía para conocer otros modos de simplificar las necesidades de gestión de servidores remotos.

Para obtener información acerca de las funciones disponibles en cada una de las versiones de iLO 2, consulte "Concesión de licencias (Concesión de licencias en la página 21)".

Diferencias entre iLO 2 e iLO

iLO 2 está basado en iLO y comparte muchas funciones comunes. Sin embargo, para utilizar iLO 2 con el fin de acceder a una consola remota basada en texto anterior al sistema operativo, deberá utilizar la consola remota de serie. Si desea obtener más información, consulte "Descripción general de la consola remota basada en texto (Descripción general de la consola remota basada en texto en la página 107)".

A continuación se indican las diferencias existentes entre iLO 2 e iLO:

Característica	iLO 2	iLO
Funciones estándar		
Consola de texto	Previo a OS	Previo a OS y OS
Consola remota de serie (puerto serie virtual)	Previo a OS y OS	Previo a OS y OS
Supervisión y mantenimiento del estado del servidor	Sí	No
Funciones avanzadas		
Consola de texto	Previo a OS y OS	Previo a OS y OS
Consola remota	Sí (Virtual KVM)	Sí
Integrated Remote Console (Consola remota integrada)	Sí	No
Compatibilidad con Microsoft® JVM	Sí	No
Botón Acquire (Adquirir) de la consola remota	Sí	Sí
Integración de servicios de Terminal Server	Sí	Sí
integración de directorios de esquema HP	Sí	Sí
Integración de directorios sin esquema	Sí	Sí
Autenticación basada en dos factores	Sí	Sí
Generación de informes del regulador de alimentación	Sí	Sí
Disquete y CD/DVD-ROM virtuales	Sí	Sí
Soporte virtual con llave USB	Sí	Sí
Carpeta virtual	Sí	No

Integración de Insight Essentials Rapid Deployment Pack de HP

El paquete Insight Essentials Rapid Deployment Pack se integra en iLO 2 para permitir la gestión de los servidores remotos y el rendimiento de las operaciones de la consola remota, independientemente del estado del sistema operativo o del hardware.

El servidor de implementación permite utilizar las funciones de gestión de alimentación de iLO 2 para encender, apagar o apagar y encender consecutivamente el servidor de destino. Cada vez que un servidor se conecta al servidor de implementación, éste sondea el servidor de destino para comprobar si está instalado el dispositivo de gestión LOM. Si está instalado, el servidor recopila información, como el nombre DNS, la dirección IP y el nombre del usuario. La seguridad se garantiza al requerir la especificación por parte del usuario de la contraseña correcta correspondiente a dicho nombre de usuario.

Para obtener mayor información acerca del paquete Insight Essentials Rapid Development Pack, consulte la documentación que viene en el CD del paquete Insight Essentials Rapid Development Pack o en la página Web de HP (http://www.hp.com/servers/rdp.)

Gestión del servidor por medio de aplicaciones que cumplen con los requisitos de IPMI versión 2.0

La gestión de servidor a través del IPMI es un método estandarizado para controlar y supervisar el servidor. iLO 2 permite la gestión del servidor basado en la especificación de IPMI versión 2.0.

La especificación IPMI define una interfaz estandarizada para la gestión de la plataforma. La especificación IPMI define los siguientes tipos de gestión de la plataforma:

- Supervisión de la información del sistema, como ventiladores, temperatura y fuentes de alimentación
- Capacidad de recuperación, así como las operaciones de reiniciar y encender/apagar el sistema
- Capacidad de registrar eventos anormales tales como lecturas de sobrecalentamiento o fallos de ventiladores
- Capacidad de inventario, como por ejemplo identificar componentes de hardware que han fallado

Las comunicaciones IPMI son dependientes en el BMC y el SMS. El BMC gestiona la interfaz entre el SMS y el hardware de gestión de la plataforma. iLO 2 emula la funcionalidad del BMC y la funcionalidad del SMS se puede obtener por medio de varias herramientas estándares industriales. Para obtener información adicional, consulte las especificaciones del IPMI en la página Web de Intel® (http://www.intel.com/design/servers/ipmi/tools.htm.)

iLO 2 proporciona la interfaz KCS, o interfaz abierta, para las comunicaciones SMS. La interfaz KCS ofrece una serie de registros de comunicaciones asignados para Entrada/Salida. La dirección base del sistema por defecto para la interfaz SMS asignada de Entrada/Salida es 0xCA2 y está alineada por bytes en esta dirección del sistema.

La interfaz KCS es accesible al software SMS que se ejecuta en el sistema local. Los siguientes son algunos ejemplos de aplicaciones de software compatibles:

- IPMI versión 2.0 Command Test Tool es una herramienta de línea de comandos de bajo nivel de MS-DOS que activa comandos IPMI con formato hexadecimal para enviarse a un IPMI BMC que implementa la interfaz KCS. Puede encontrar esta herramienta en la página Web de Intel® (http://www.intel.com/design/servers/ipmi/tools.htm.)
- IPMItool es una utilidad para la gestión y configuración de dispositivos que admiten las especificaciones de la versión 1.5 y versión 2.0 del IPMI y que pueden usarse en un ambiente Linux. Puede encontrar esta herramienta en la página Web de IMPItool (http://ipmitool.sourceforge.net/index.html.)

Funcionalidad del IPMI proporcionada por iLO 2

Cuando se emula un BMC para la interfaz IPMI, iLO 2 admite todos los comandos obligatorios enumerados en las especificaciones de la versión 2.0 del IPMI. Vea la especificación de la versión 2.0 del IPMI para obtener una lista de estos comandos. Además, el SMS debería usar los métodos descritos

en la especificación para determinar qué funciones del IPMI están activadas o desactivadas en el BMC (por ejemplo, mediante el uso del comando Get Device ID.)

Si el sistema operativo del servidor está funcionando y el controlador de salud está activo, cualquier trafico IPMI que pase a través de la interfaz KCS podrá afectar el rendimiento del controlador de salud y el rendimiento total de salud del sistema. No emita ningún comando IPMI a través de la interfaz KCS que podría tener un efecto dañino sobre la supervisión realizada por el controlador de salud. Entre estos comandos se incluyen todos los comandos que establecen o cambian los parámetros IPMI, por ejemplo `Set Watchdog Timer` y `Set BMC Global Enabled`. Cualquier comando IPMI que sólo devuelva datos es de uso seguro, tal como `Get Device ID` y `Get Sensor Reading`.

Descripción general de compatibilidad de WS-Management

La implementación del firmware de iLO 2 de WS-Management sigue la especificación *Web Services for Management* (Servicios Web para Gestión) 1.0.0a de DTMF.

Autenticación

- iLO 2 utiliza una autenticación básica sobre SSL compatible con el perfil: `wsman:secprofile/https/basic`
- Los usuarios autentificados disponen de autorización para ejecutar los comandos de WS-Management según los privilegios designados en su cuenta local o de directorio.
- Para activar la autenticación básica en Microsoft® Windows Vista™, escriba `gpedit.msc` en la línea de comandos para ejecutar Editor de objetos de directiva de grupo. Seleccione **Configuración del equipo> Plantillas administrativas> Componentes de Windows> Administración remota de Windows (WinRM)> Cliente WinRM**. Establezca la opción Permitir autenticación básica en **Habilitada**.

Compatibilidad

- WS-Management en iLO 2 es compatible con la utilidad WinRM de Windows Vista™, Microsoft® Operations Manager 3 y el Management Pack suministrado por HP.
- El conjunto completo de comandos de WS-Management está disponible en los servidores de iLO 2 compatibles con el estado del sistema integrado. Un subconjunto muy reducido de estos comandos se encuentra disponible en los servidores no compatibles con el estado de sistemas integrados.

Se encuentran disponibles comandos para la invocación remota de los siguientes dispositivos:

- Alimentación del servidor
- UID

Estado

WS-Management en iLO 2 devuelve información sobre el estado de los ventiladores, la temperatura, las fuentes de alimentación y VRM.

Perspectiva general de la interfaz del explorador de iLO 2

La interfaz del explorador de iLO 2 agrupa tareas similares para una navegación y flujo de trabajo simples. Estas tareas se organizan en fichas de nivel superior por la parte superior de la interfaz de iLO 2. Estas fichas, entre las que se encuentran System Status (Estado del sistema), Remote Console (Consola remota), Virtual Media (Soportes virtuales), Power Management (Gestión de alimentación) y Administration (Administración), se encuentran visibles en todo momento.

Cada una de las fichas de nivel superior de iLO 2 cuenta con un menú en el lado izquierdo de la interfaz que dispone de distintas opciones. Este menú varía cada vez que se selecciona una ficha de nivel superior y muestra las opciones disponibles en la ficha. Cada opción de menú muestra un título de página que describe la información o configuración disponible en la página. Es posible que el título de la página no refleje el nombre mostrado en la opción de menú.

En la ayuda de iLO 2 se presenta ayuda sobre todas las páginas de iLO 2. Todas las páginas de iLO 2 cuentan con enlaces que proporcionan información resumida acerca de las funciones de iLO 2 e información útil para optimizar su funcionamiento. Para acceder a la ayuda específica de la página, haga clic en el **signo de interrogación (?)** situado en la parte derecha de la ventana del explorador.

Las tareas de usuario habituales se encuentran en las fichas System Status (Estado del sistema), Remote Console (Consola remota), Virtual Media (Soportes virtuales) y Power Management (Gestión de alimentación) de la interfaz de iLO 2. En la sección "Utilización de iLO 2 (Utilización de iLO 2 en la página 81)" se encuentra una descripción de estas tareas.

Normalmente, los usuarios avanzados o administradores que gestionan usuarios utilizan la ficha Administration (Administración) para establecer la configuración global y de red, y para configurar o activar las funciones más avanzadas de iLO 2. En las secciones "Instalación de iLO 2 (Instalación de iLO 2 en la página 9)" y "Configuración de iLO 2 (Configuración de iLO 2 en la página 18)" se tratan estas tareas.

Las áreas específicas de la funcionalidad e integración de iLO 2 se encuentran detalladas en:

- Servicios de directorio (Servicios de directorio en la página 150)
- Gestión remota habilitada por directorio (Gestión remota habilitada por directorio en la página 185)
- Utilidad de migración de directorios HPQLOMIG (Utilidad de migración de directorios HPQLOMIG en la página 193)
- Integración de HP Systems Insight Manager (Integración de HP Systems Insight Manager en la página 204)
- Solución de problemas con la placa iLO 2 (Solución de problemas con la placa iLO 2 en la página 210)
- Esquema de los servicios de directorio (Esquema de los servicios de directorio en la página 238)

Sistemas operativos cliente y exploradores compatibles

- Microsoft® Internet Explorer 7
  - Este explorador es compatible con los productos de Microsoft® Windows®.
  - HP admite Microsoft® JVM y SUN Java™ 1.4.2_13. Para descargar la versión de JVM recomendada para la configuración de su sistema, consulte la página Web de HP (http://www.hp.com/servers/manage/jvm.)
- Microsoft® Internet Explorer 6 con Service Pack 1 o posterior
  - Este explorador es compatible con los productos de Microsoft® Windows®.
  - HP admite Microsoft® JVM y SUN Java™ 1.4.2_13. Para descargar la versión de JVM recomendada para la configuración de su sistema, consulte la página Web de HP (http://www.hp.com/servers/manage/jvm.)
- Firefox 2.0
  - Este explorador es compatible con Red Hat Enterprise Linux Desktop 4 y Novell Linux Desktop 9.
  - HP admite Microsoft® JVM y SUN Java™ 1.4.2_13. Para descargar la versión de JVM recomendada para la configuración de su sistema, consulte la página Web de HP (http://www.hp.com/servers/manage/jvm.)

Puede que algunas combinaciones de explorador y de sistema operativo no funcionen correctamente, según la implementación de las tecnologías de exploración necesarias.

Software de sistemas operativos de servidores compatibles

iLO 2 es un microprocesador independiente que se ejecuta en un sistema operativo integrado. La arquitectura garantiza la disponibilidad de la mayoría de las funciones de iLO 2, con independencia del sistema operativo del servidor host.

Para cerrar el sistema operativo host correctamente, la integración de HP SIM precisa disponer de controladores de estado y agentes de gestión o acceso a la consola remota.

iLO 2 proporciona dos controladores de interfaz:

- Controlador de controladores de gestión avanzada de servidores de iLO 2 (controlador de estado): proporciona compatibilidad con la gestión del sistema, incluida la supervisión de los componentes del servidor, el registro de sucesos y la compatibilidad con los agentes de gestión.
- iLO 2 Management Interface Driver: permite al software de sistema y a los agentes Insight SNMP comunicarse con iLO 2.

Estos controladores y agentes están disponibles para los siguientes sistemas operativos de red:

- Microsoft®
  - Servidor Windows® 2008 Server
  - Windows® 2008 Advanced Server
  - Windows Server® 2003
  - Windows Server® 2003, Web Edition

- Windows® Small Business Server 2003 (serie ML300)
- Windows Vista®

- Red Hat
  - RedHat Enterprise Linux 3 (x86)
  - RedHat Enterprise Linux 3 (AMD64/EM64T)
  - RedHat Enterprise Linux 4 (x86)
  - RedHat Enterprise Linux 4 (AMD64/EM64T)
  - RedHat Enterprise Linux 5 (x86)
  - RedHat Enterprise Linux 5 (AMD64/EM64T)
- SUSE
  - SUSE LINUX Enterprise Server 9 (x86)
  - SUSE LINUX Enterprise Server (AMD64/EM64T)
  - SUSE LINUX Enterprise Server 10

2 Instalación de iLO 2

En esta sección:

Instalación rápida

Para instalar rápidamente iLO 2 con la configuración predeterminada para las funciones de iLO 2 Standard e iLO Advanced, siga los pasos que se detallan a continuación:

1. Prepare la configuración: decida cómo desea gestionar la red y la seguridad (Preparación para la configuración de iLO 2 en la página 10.)
2. Conecte iLO 2 a la red (Conexión a la red en la página 12.)
3. Si no está utilizando una dirección IP dinámica, use la utilidad RBSU de iLO 2 para configurar una dirección IP estática (Configuración de la dirección IP en la página 12.)
4. Inicie sesión en iLO 2 desde un explorador compatible o una línea de comandos que emplee el nombre de usuario, la contraseña y el nombre de DNS predeterminados suministrados en la ficha iLO 2 Network Settings (Configuración de red de iLO 2) que contiene el servidor (Primer inicio de sesión en iLO 2 en la página 13.)
5. Cambie el nombre de usuario y la contraseña predeterminados de la cuenta del administrador por unos que usted prefiera.
6. Si está utilizando la función de cuentas locales, configure las cuentas de usuario (Configuración de cuentas de usuario en la página 13.)
7. Active las funciones avanzadas de iLO 2 (Activación de las funciones con licencia de iLO 2 mediante un explorador en la página 14.)
8. Instale los controladores del dispositivo iLO 2 (Instalación de los controladores del dispositivo iLO 2 en la página 15.)

Preparación para la configuración de iLO 2

Antes de instalar los procesadores de administración de iLO 2, debe decidir cómo gestionar la red y la seguridad. Las preguntas que se presentan a continuación le ayudarán a configurar iLO 2 para adaptarlo a sus necesidades:

1. ¿Cómo se debe conectar iLO 2 a la red? Si desea obtener una representación gráfica y una explicación de las conexiones disponibles, consulte la sección "Conexión a la red (Conexión a la red en la página 12)".

   Normalmente, iLO 2 se conecta a la red mediante:

   - Una red corporativa en la que tanto la tarjeta de interfaz de red (NIC, Network Interface Card) como el puerto iLO 2 están conectados a la red corporativa. Esta conexión permite acceder a iLO 2 desde cualquier lugar de la red y reduce la cantidad de hardware de red e infraestructura necesarios para la compatibilidad con iLO 2. No obstante, en una red corporativa, el tráfico de red puede dificultar el rendimiento de iLO 2.
   - Una red de gestión dedicada con el puerto iLO 2 en una red independiente. Una red independiente mejora el rendimiento y la seguridad, ya que le permite controlar físicamente las estaciones de trabajo que están conectadas a la red. Una red independiente también proporciona acceso redundante al servidor cuando se produce un fallo de hardware en la red corporativa. Con esta configuración, no se puede acceder a iLO 2 directamente desde la red corporativa.

2. ¿Cómo consigue iLO 2 una dirección IP?

   Para acceder a iLO 2 tras conectarlo a la red, el procesador de gestión debe adquirir una dirección IP y una máscara de subred utilizando un proceso estático o dinámico:

   - De manera predeterminada está configurada la dirección IP dinámica. iLO 2 obtiene la dirección IP y la máscara de subred a partir de los servidores DNS/DHCP. Este método es el más sencillo.
   - La dirección IP estática se utiliza para configurar una dirección IP estática si los servidores DNS/DHCP no están disponibles en la red. Es posible configurar una dirección IP estática en iLO 2 a través de la utilidad RBSU.

     Si utiliza una IP estática, debe tener una dirección IP antes de iniciar la instalación de iLO 2.

3. ¿Qué seguridad de acceso es necesaria? ¿Qué cuentas y privilegios de usuario se necesitan?

   iLO 2 ofrece diversas opciones para controlar el acceso de los usuarios. Para impedir el acceso no autorizado a los activos de TI corporativos, debe seleccionar uno de los siguientes métodos:

   - En iLO 2 se pueden guardar cuentas locales con hasta 12 nombres de usuario y contraseñas. Esto es perfecto para entornos pequeños como laboratorios y pequeñas y medianas empresas.
   - Los servicios de directorio utilizan el directorio corporativo (Microsoft® Active Directory o Novell eDirectory) para gestionar el acceso de los usuarios de iLO 2. Esta opción es perfecta para entornos con un gran número de usuarios en constante cambio. Si desea utilizar los servicios de directorio, deje al menos una cuenta local habilitada para un acceso alternativo.

     Para obtener más información acerca de la seguridad de acceso a iLO 2, consulte la sección "Seguridad (Seguridad en la página 40)".

4. ¿Cómo desea configurar iLO 2?

iLO 2 admite distintas interfaces para su configuración y funcionamiento. En esta guía se describen las siguientes interfaces:

- La utilidad RBSU de iLO 2 (Configuración de iLO 2 a través de la utilidad RBSU de iLO 2 en la página 14) puede utilizarse cuando el entorno del sistema no utiliza DHCP, DNS ni WINS.
- La configuración basada en explorador (Configuración de iLO 2 a través de la opción basada en explorador en la página 14) puede utilizarse cuando es posible conectarse a iLO 2 en la red mediante un explorador. Este método también puede volver a configurar un dispositivo iLO 2 ya configurado.
- SMASH CLP puede utilizarse cuando puede accederse a una línea de comandos a través de Telnet, SSH o un puerto serie físico. Consulte la *Guía de recursos de líneas y secuencias de comandos del procesador de gestión HP Integrated Lights-Out*.

Los valores predeterminados de iLO 2 permiten utilizar la mayoría de las características sin necesidad de realizar una configuración adicional. Sin embargo, la amplia flexibilidad de configuración de iLO 2 permite la personalización para múltiples entornos de empresa. Consulte la sección "Configuración de iLO 2 (Configuración de iLO 2 en la página 18)" para obtener información acerca de todas las opciones que se encuentran disponibles.

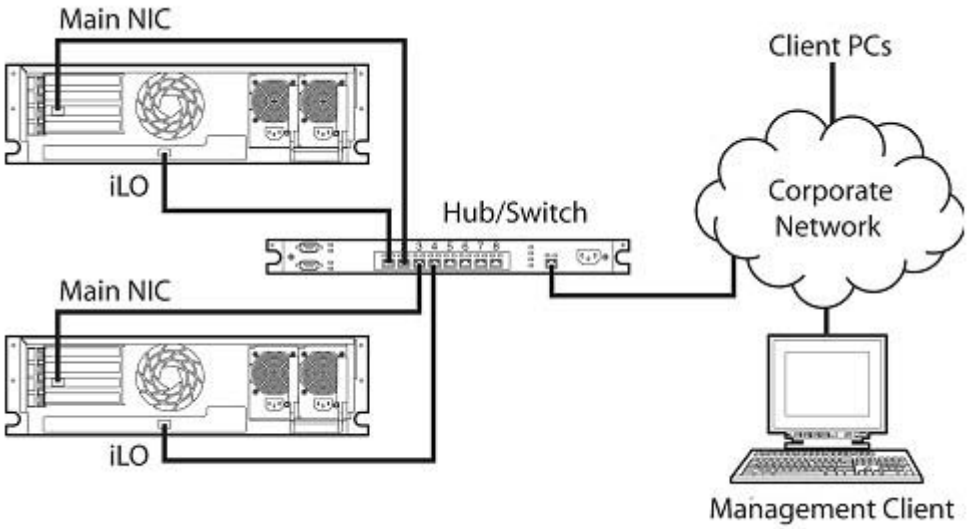
Para una instalación avanzada de varios procesadores de gestión de iLO 2 mediante comandos de secuencias de comandos, están disponibles los siguientes métodos. Las secuencias de comandos son archivos de texto escritos en un lenguaje de secuencias de comandos basados en XML denominado RIBCL. Puede utilizar las secuencias de comandos RIBCL para configurar iLO 2 en la red durante la implementación inicial o desde un host ya implementado. Cada método aparece descrito en la *Guía de recursos de líneas y secuencias de comandos del procesador de gestión HP Integrated Lights-Out*.

- CPQLOCFG es una utilidad de Microsoft® Windows® que envía secuencias de comandos RIBCL a iLO 2 a través de la red.
- HPONCFG es una utilidad de instalación cifrada local en línea que se ejecuta en el host y pasa líneas de comandos RIBCL al sistema iLO 2 local. Hay versiones para Windows® y Linux de esta utilidad, por lo que es necesario disponer de iLO 2 Management Interface Driver de HP.
- Perl es un lenguaje de secuencias de comandos que se puede utilizar desde clientes de Linux para enviar secuencias de comandos RIBCL a iLO 2 a través de la red.

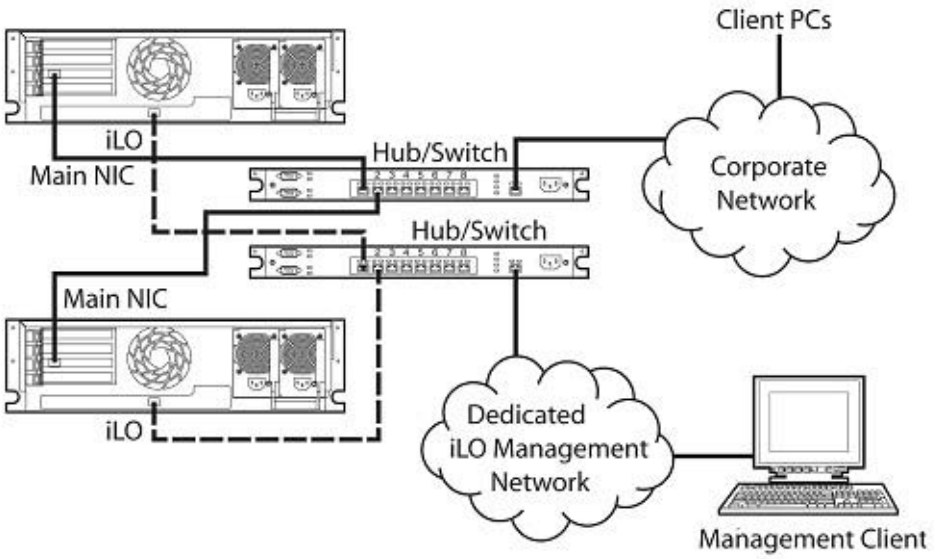
Conexión a la red

Normalmente iLO 2 está conectado a la red de uno de estos dos modos. iLO 2 puede conectarse a través de una:

- **Red corporativa** en la que se conectan ambos puertos a la red corporativa. En esta configuración, el servidor dispone de dos puertos de red (una NIC de servidor y otro de iLO 2) que se pueden conectar a una red corporativa.



- Red de **gestión dedicada** con el puerto de iLO 2 en una red independiente.



Configuración de la dirección IP

Este paso sólo es necesario si utiliza una dirección IP estática. Al utilizar una dirección IP dinámica, su servidor DHCP asignará automáticamente una dirección IP para iLO 2. HP recomienda utilizar DNS o DHCP con iLO 2 para simplificar la instalación.

Para configurar una dirección IP estática, utilice la RBSU de iLO 2 con el siguiente procedimiento para deshabilitar DNS y DHCP y configurar la dirección IP y la máscara de subred:

1. Reinicie o encienda el servidor.
2. Pulse la tecla **F8** cuando así se lo indiquen durante la Autocomprobación al arrancar (POST). Se ejecuta RBSU de iLO 2.
3. Seleccione **Network (Red)**>**DNS/DHCP**, pulse la tecla **Intro** y, a continuación, seleccione **DHCP Enable (Activar DHCP)**. Pulse la barra espaciadora para desactivar DHCP. Asegúrese de que DHCP Enable [Activar DHCP] se encuentra definido como Off [Desactivado] y guarde los cambios.
4. Seleccione **Network (Red)**>**NIC>TCP/IP**, pulse la tecla **Intro** y, a continuación, introduzca la información correspondiente en los campos IP Address (Dirección IP), Subnet Mask (Máscara de subred) y Gateway IP Address (Dirección IP de la puerta de enlace.)
5. Guarde los cambios.
6. Abandone la utilidad RBSU de iLO 2. Los cambios se harán efectivos cuando salga de la utilidad RBSU de iLO 2.

Primer inicio de sesión en iLO 2

iLO 2 está configurado con un nombre de usuario, una contraseña y un nombre DNS predeterminados. La información de usuario predeterminada se encuentra en la ficha iLO 2 Network Settings (Configuración de red de iLO 2) del servidor que contiene el procesador de gestión de iLO 2. Utilice estos valores para acceder de manera remota a la placa iLO 2 desde un equipo cliente de red mediante un explorador Web estándar.

Por motivos de seguridad, HP recomienda cambiar la configuración predeterminada después de iniciar sesión por primera vez en iLO 2.

Los valores predeterminados son:

- Nombre de usuario: Administrador
- Contraseña: cadena alfanumérica de ocho caracteres aleatorios
- Nombre DNS:*ILOXXXXXXXXXXXX*, donde las *X* representan el número de serie del servidor

NOTA: En el nombre de usuario y en la contraseña se distingue entre mayúsculas y minúsculas.

Si escribe un nombre de usuario y una contraseña incorrectos o falla un intento de inicio de sesión, iLO 2 impone un retraso de seguridad. Para obtener más información acerca de la seguridad del inicio de sesión, consulte "Seguridad de inicio de sesión (Seguridad de inicio de sesión en la página 43)".

Configuración de cuentas de usuario

iLO 2 viene preconfigurado con valores predeterminados de fábrica, entre los que se incluye una cuenta y una contraseña de usuario predeterminadas. Por motivos de seguridad, HP recomienda cambiar la configuración predeterminada después de iniciar sesión por primera vez en iLO 2. Estos cambios pueden realizarse con cualquier interfaz de usuario de iLO 2. En esta guía de usuario se explican los procedimientos de RBSU y explorador. Otras opciones, entre las que se incluye SMASH CLP y los métodos de secuencia de comandos, aparecen descritas en *"Guía de recursos de líneas y secuencias de comandos del procesador de gestión HP Integrated Lights-Out"*.

Si iLO 2 se conecta a una red que ejecuta DNS o DHCP, puede utilizarse inmediatamente sin necesidad de cambiar ningún valor.

Configuración de iLO 2 a través de la utilidad RBSU de iLO 2

RBSU de iLO 2 es el método que recomienda HP para configurar inicialmente iLO 2, y para establecer los parámetros de red de iLO 2 para entornos que no utilizan DHCP, DNS ni WINS. RBSU proporciona las herramientas básicas para la configuración de red de iLO 2 y las cuentas de usuario para utilizar iLO 2 en la red.

Puede utilizar RBSU para configurar parámetros de red, configuración de directorio, configuración global y cuentas de usuario. La utilidad RBSU de iLO 2 no es adecuada para una administración continua. La utilidad RBSU está disponible cada vez que el servidor se inicia y puede ejecutarse de manera remota desde la consola remota de iLO 2.

La utilidad RBSU de iLO 2 puede desactivarse en las preferencias de Global Settings (Configuración global.) Si desactiva RBSU de iLO 2 impedirá la reconfiguración desde el host a menos que esté definido el conmutador de anulación de seguridad de iLO 2.

Para ejecutar RBSU de iLO 2 para configurar cuentas locales:

1. Reinicie o encienda el servidor.
2. Pulse la tecla **F8** cuando así se lo indiquen durante la Autocomprobación al arrancar (POST.) Se ejecuta RBSU de iLO 2.
3. Si el sistema lo requiere, escriba un Id. de usuario y una contraseña válidos con los privilegios de iLO 2 adecuados (**Administer User Accounts>Configure iLO 2 Settings** (Administración de cuentas de usuario) > Configurar valores de iLO 2.) La información de cuenta predeterminada se encuentra en la ficha iLO 2 Network Settings (Configuración de red de iLO 2) del servidor que contiene el procesador de gestión de iLO 2. Si iLO 2 no se ha configurado para ser la respuesta de inicio de sesión para RBSU, no aparecerá ninguna línea de comandos.
4. Realice y guarde los cambios necesarios en la configuración de iLO 2.
5. Abandone la utilidad RBSU de iLO 2.

Configuración de iLO 2 a través de la opción basada en explorador

Utilice el método de configuración basado en el explorador si puede conectarse a iLO 2 en la red mediante un explorador. Asimismo, puede utilizar este método para volver a configurar un dispositivo iLO 2 ya configurado.

Con un explorador compatible, acceda a iLO 2 desde un cliente de red remoto, especificando el nombre DNS, el nombre de usuario y la contraseña predeterminados. El nombre de DNS y la información de cuenta predeterminada se encuentran en la ficha iLO 2 Network Settings (Configuración de red de iLO 2) del servidor que contiene el procesador de gestión de iLO 2.

Cuando haya iniciado la sesión correctamente en iLO 2, podrá cambiar los valores predeterminados de las cuentas de usuario locales. Para ello, deberá seleccionar la ficha iLO 2 Administration (Administración de iLO 2.)

Activación de las funciones con licencia de iLO 2 mediante un explorador

La página Licensing (Concesión de licencias) permite ver el estado actual de la licencia e introducir una clave para activar las funciones con licencia de iLO 2. La información de la licencia actual y de la versión iLO 2 aparecen en esta sección. Si se instala una licencia (incluso una licencia de evaluación), se

mostrará el número de licencia. Consulte "Concesión de licencias (Concesión de licencias en la página 21)" para obtener más información acerca de las opciones de licencia de iLO 2.

1. Inicie sesión en iLO 2 a través de un explorador compatible.
2. Haga clic en **Administration (Administración)>Licensing (Concesión de licencias)** para abrir la pantalla de activación de licencias de iLO 2.

3. Introduzca la clave de licencia. Pulse el **tabulador** o haga clic en un campo para pasar de un campo a otro. El campo Activation Key (Tecla de activación) avanza automáticamente según va introduciendo los datos. Haga clic en **Licensing (Concesión de licencias)** si desea borrar los campos y volver a cargar la página.
4. Haga clic en **Install (Instalar)**. Se muestra la confirmación de EULA. Los detalles del CLUF están disponibles en la página Web de HP (http://www.hp.com/servers/lights-out) y en el paquete de licencia.
5. Haga clic en **Aceptar**.

Las funciones avanzadas de iLO 2 ya están activadas.

Instalación de los controladores del dispositivo iLO 2

iLO 2 Management Interface Driver activa el software de sistema como SNMP Insight Agents y el servicio de transferencia de los servicios de Terminal Server para establecer la comunicación con iLO 2.

Los controladores de dispositivos que se necesitan para permitir iLO 2 forman parte de la PSP que se encuentra en el CD de SmartStart, el CD de gestión o en la página Web de HP (http://www.hp.com/servers/lights-out.)

Todos los controladores compatibles con su servidor e iLO 2 pueden descargarse desde la página Web de HP (http://www.hp.com/servers/lights-out.)

Para descargar los controladores:

1. Haga clic en el gráfico iLO 2.
2. Seleccione **Software and Drivers (Software y controladores)**.

Compatibilidad de controladores de dispositivos de Microsoft

Los controladores de dispositivos compatibles con iLO 2 forman parte de PSP, que se encuentra en la página Web de HP (http://www.hp.com/support) o en el CD de SmartStart. Antes de proceder a la instalación de los controladores de Windows®, consiga la documentación de Windows® y las últimas versiones del Service Pack de Windows®.

iLO 2 necesita los siguientes archivos previos:

- CPQCIDRV.SYS proporciona compatibilidad con iLO 2 Management Interface Driver.
- CPQASM2.SYS, SYSMGMT.SYS eSYSDOWN.SYS proporciona compatibilidad con el controlador de controladores de gestión avanzada del servidor iLO 2.

El software PSP para los productos de Microsoft® Windows® incluye un instalador que analiza los requisitos del sistema e instala todos los controladores. El software PSP está disponible en la página Web de HP (http://www.hp.com/support) o en el CD de SmartStart.

Para instalar los controladores en el software PSP:

1. Descargue el software PSP de la página Web de HP (http://www.hp.com/support.)
2. Ejecute el archivo SETUP.EXE incluido en la descarga y siga las instrucciones de instalación.

Para obtener información adicional acerca de la instalación de PSP, lea el archivo de texto incluido en la descarga de PSP.

Compatibilidad de controladores de dispositivos de Linux

Puede descargar los archivos LSP que contienen el controlador de iLO 2, los agentes base y los agentes de estado desde la página Web de HP (http://www.hp.com/support.) Las instrucciones acerca de cómo instalar o actualizar el controlador de iLO 2 están disponibles en dicha página Web. Los agentes de gestión de HP para Linux son:

- Paquete ASM (agentes hp-snmp) que combina el controlador de estado, el visor IML, los agentes base, el agente de estado y el agente de equipo estándar en un solo paquete.
- Paquete RSM (hp-iLO) que combina el controlador RIB, el programa daemon de bastidor, el agente RIB y el agente de bastidor en un solo paquete.

Para cargar los paquetes de controladores de estado y de iLO 2, use los siguientes comandos:

```
rpm –ivh hp-snmp-agents-d.vv.v-pp.Linux_version.i386.rpm
```

```
rpm –ivh hp-iLO-d.vv.v-pp.Linux_version.i386.rpm
```

donde *d* es la letra de distribución y versión de Linux, y

vv.v-pp corresponden a los números de versión.

Para obtener información adicional, consulte la página Web de software y controladores (http://www.hp.com/support.)

Para quitar los paquetes de controladores de estado y de iLO 2, use los siguientes comandos:

```
rpm –e hp-snmp-agents
```

```
rpm –e hp-iLO
```

Para obtener información adicional, consulte la página Web de software y controladores (http://www.hp.com/support.)

Compatibilidad de controladores de dispositivos de Novell NetWare

Los controladores de dispositivos necesarios para la compatibilidad con iLO 2 se encuentran en el CD de SmartStart y en la página Web de HP (http://www.hp.com/support.) El software PSP para Novell NetWare incluye un instalador que analiza los requisitos del sistema e instala todos los controladores.

iLO 2 requiere los siguientes archivos:

- El archivo CPQHLTH.NLM proporciona el Controlador de estado para Novell NetWare.
- El archivo CPQCI.NLM proporciona compatibilidad con iLO 2 Management Interface Driver.

Al actualizar los controladores iLO 2, asegúrese de que iLO 2 ejecuta la versión más reciente del firmware de iLO 2. Puede obtener la versión más reciente como Smart Component en la página Web de HP (http://www.hp.com/servers/lights-out.)

Para instalar los controladores, descargue el software PSP de la página Web de HP (http://www.hp.com/support) en un servidor NetWare. Cuando haya descargado el software PSP, siga las instrucciones de instalación del componente Novell NetWare para completar la instalación. Para obtener información adicional acerca de la instalación de PSP, lea el archivo de texto incluido en la descarga de PSP.

Cuando utilice Novell NetWare 6.X, use el controlador de vídeo ATI ES1000 proporcionado por el sistema operativo para obtener mejores resultados.

3 Configuración de iLO 2

En esta sección:

Perspectiva de la configuración de iLO 2

Normalmente, los usuarios avanzados o administradores cuya función es gestionar usuarios y establecer la configuración global y de red, también configuran iLO 2. Es posible configurar iLO 2 a través de la GUI basada en explorador de iLO 2 y de las herramientas de secuencias de comandos, por ejemplo CPQLOCFG y HPONCFG (descritas en la *Guía de recursos de líneas y secuencias de comandos del procesador de gestión HP Integrated Lights-Out*.)

La ficha Administration (Administración) de iLO 2 permite configurar y gestionar la configuración de usuario, las alertas SNMP (a través de la integración con HP SIM), la configuración de seguridad, la concesión de licencias, la administración de certificados, la configuración de directorios y la configuración del entorno de red. Esta ficha incluye las siguientes opciones de menú:

- Firmware de iLO 2 (Actualización del firmware de iLO 2 en la página 18)
- Concesión de licencias (Concesión de licencias en la página 21)
- Administración de usuarios (Administración de usuarios en la página 23)
- Valores de configuración
  - Acceso (Configuración del acceso a iLO 2 en la página 29)
  - Seguridad (Seguridad en la página 40)
  - Red (Red en la página 63)
  - Gestión (Valores de configuración de SNMP/Insight Manager en la página 70)

Actualización del firmware de iLO 2

Las actualizaciones de firmware mejoran la funcionalidad de iLO 2. En la página Web de HP (http://www.hp.com/servers/lights-out) encontrará la versión más reciente del firmware. Seleccione el producto de iLO 2 que desee y, a continuación, seleccione **Software & Drivers (Software y**

controladores). Cuando aparezcan el software y los controladores, seleccione el producto de iLO 2 y el sistema operativo que desee y haga clic en **Locate Software (Buscar software)**. También puede localizar el software de iLO 2 mediante las opciones **Operating System (Sistema operativo) y Category (Categoría)**.

Es necesario disponer del privilegio Configure iLO 2 (Configurar iLO 2) (Configurar los ajustes de los dispositivos locales) para actualizar el firmware salvo que ajuste a continuación el conmutador de anulación de seguridad (Administración del conmutador de anulación de la seguridad de la placa iLO 2 en la página 41.) Si el conmutador de anulación de seguridad está configurado, cualquier usuario de iLO 2 puede actualizar el firmware. Las actualizaciones de firmware deben ejecutarse desde un contexto raíz o administrador del sistema operativo del host.

Para actualizar iLO 2 elija uno de los siguientes métodos:

- Actualización en línea del firmware: descargue el componente del sistema operativo apropiado y ejecútelo desde el contexto raíz o administrador del sistema operativo. Este software de actualización en línea del firmware se ejecuta en el sistema operativo del host y actualiza el firmware de iLO 2 sin necesidad de iniciar una sesión en iLO 2.
- Actualización de firmware sin conexión para mantenimiento de SmartStart: descargue el archivo de imagen del firmware de iLO 2 que desee instalar y consulte la sección "Actualización de iLO 2 mediante un explorador (Actualización de iLO 2 mediante un explorador en la página 19)".
- CD-ROM de mantenimiento de firmware: descargue el componente para crear un CD ejecutable que contenga muchas actualizaciones de firmware para servidores y opciones de ProLiant.
- Secuencias de comandos con CPQLOCFG: descargue el componente CPQLOCFG para obtener la utilidad de secuencia de comandos basada en red, CPQLOCFG. CPQLOCFG permite utilizar secuencias de comandos RIBCL que realizan de forma segura en la red actualizaciones de firmware, configuración de iLO 2 y operaciones de iLO 2 en masa. Los usuarios de Linux deben revisar las muestras de secuencias de comandos PERL y XML de HP Lights-Out para Linux.
- Secuencias de comandos con HPONCFG: descargue el componente HPONCFG para obtener la utilidad de secuencias de comandos basada en host, HPONCFG. Esta utilidad permite utilizar secuencias de comandos RIBCL que realizan actualizaciones de firmware, configuración del procesador de Lights-Out y operaciones en masa, desde un Administrador o acceso a una cuenta raíz en los sistemas operativos del host admitidos.
- Compatibilidad de directorios HP para procesadores de gestión: descargue el archivo ejecutable de compatibilidad de directorios HP para procesadores de gestión para obtener los componentes de compatibilidad de directorios. Uno de los componentes, HPLOMIG, puede utilizarse para detectar los procesadores iLO, iLO 2, RILOE y RILOE II y actualizar el firmware. No tiene que utilizar la integración de directorios para aprovechar esta funcionalidad.

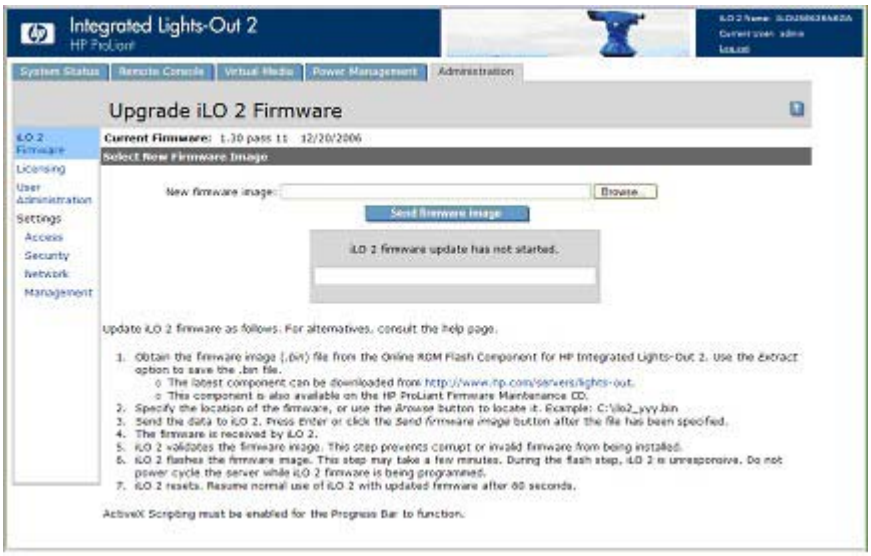
Actualización de iLO 2 mediante un explorador

Es posible finalizar la actualización de firmware de cualquier cliente de red a través de un explorador compatible. Para actualizar el firmware de iLO 2, debe disponer del privilegio de firmware de iLO 2. El firmware más reciente para iLO 2 está disponible en la página Web de HP (http://www.hp.com/servers/lights-out.)

Para actualizar el firmware de iLO 2 mediante un explorador compatible:

1. Inicie una sesión en iLO 2 con una cuenta con el privilegio Configure iLO 2 Settings (Configurar valores de iLO 2.)

2. Haga clic en **Administration (Administración)>Upgrade iLO 2 Firmware (Actualizar firmware de iLO2)**. Se mostrará la página Upgrade iLO 2 Firmware (Actualizar firmware de iLO 2.)



3. Escriba el nombre del archivo en el campo New firmware image (Nueva imagen de firmware) o busque el archivo.
4. Haga clic en **Send firmware image (Enviar imagen de firmware)**. La actualización del firmware tarda unos minutos. Una barra de progreso mostrará el progreso de la actualización del firmware.

No interrumpa una sesión de actualización de firmware de iLO 2. El sistema de iLO 2 se reinicia automáticamente una vez se haya llevado a cabo correctamente la actualización del firmware. El reinicio del sistema de iLO 2 no afecta al servidor ni al sistema operativo host.

Si la actualización del firmware se interrumpe o falla, vuelva a intentar realizarla inmediatamente. No reinicie el sistema iLO 2 antes de volver a intentar una actualización del firmware.

Actualización del firmware mediante el CD de mantenimiento

Para utilizar HP Smart Update Manager que se encuentra en el CD de mantenimiento del firmware:

1. Coloque el CD de mantenimiento del firmware en una llave USB mediante la utilidad USB Key Creator Utility.
2. Copie CP009768.exe en el directorio /compaq/swpackages de la llave USB.
3. Siga los pasos indicados en HP Smart Update Manager para completar la actualización del firmware.

Recuperación tras fallo al actualizar el firmware de iLO 2

Para recuperarse tras un fallo al actualizar el firmware utilizando HP Drive Key Boot Utility:

1. Copie el componente flash sin conexión iLO 2 en la clave de unidad USB.
2. Asegúrese de que el conmutador de anulación de seguridad de iLO 2 está deshabilitado.
3. Inicie la llave del controlador USB que contiene el componente flash de iLO 2.

   Para descargar HP Drive Key Boot Utility y para obtener información acerca de cómo crear una llave USB de arranque, consulte la página Web de HP (http://www.hp.com/go/support.)

4. Después de que aparezca la primera pantalla, pulse las teclas **Ctrl+Alt+F1** para cambiar a la consola de texto.
5. Cambie al directorio en el que está guardado el componente flash. Para ello escriba `cd /mnt/usb/components/` en la línea de comandos #.
6. Introduzca los siguientes comandos para eliminar el controlador de HP Lights-Out cargado:

   ```
   /etc/init.d/hp-snmp-agents stop
   ```

   ```
   /etc/init.d/hp-ilo stop
   ```

   o

   ```
   /etc/init.d/hpasm stop
   ```

7. Ejecute el componente mediante la opción --direct. Por ejemplo:

   ```
   ./CP00xxxx.scexe --direct
   ```

8. Escriba **y** en la línea de comandos Continue (y/N)?.
9. Cuando la programación se haya completado correctamente, active el conmutador de anulación de seguridad y reinicie el servidor.

Ir a una versión anterior de firmware de iLO 2

Para utilizar una versión anterior de firmware de iLO 2, debe eliminar el subprograma 1.3.0.19 de ActiveX de Remote Console 1.30 de iLO 2 de su explorador cliente Internet Explorer. Para eliminar el subprograma:

1. Abra Internet Explorer.
2. Seleccione **Herramientas>Opciones de Internet>Configuración>Ver objetos**.
3. Para eliminar 1.30.19, haga clic con el botón derecho en la **consola remota 1.3.0.18 de iLO2**.

Concesión de licencias

iLO Advanced Pack de HP e iLO Advanced Pack de HP para licencias de BladeSystem permiten activar las funciones opcionales de iLO 2 que no se suministran con un sistema sin licencia. Para obtener información adicional, consulte la página Web de HP.

Si adquiere iLO Advanced Pack o iLO Advanced Pack para BladeSystem con cualquier paquete de productos de software de Insight Control o iLO Power Management Pack, HP le proporcionará asistencia técnica y servicios de actualización. Si desea obtener más información, consulte "Información sobre compatibilidad (Información sobre compatibilidad en la página 245)".

Si adquiere iLO Advanced Pack o iLO Advanced Pack para BladeSystem como activación única de las funciones con licencia, las actualizaciones funcionales futuras se deberán adquirir. Si desea obtener más información, consulte "Información sobre compatibilidad (Información sobre compatibilidad en la página 245)".

Es necesario disponer de una licencia de iLO Advanced o iLO Advanced Pack para BladeSystem para cada uno de los servidores en los que se instale y utilice el producto. Las licencias no son transferibles. No es posible disponer de licencia para un servidor ML/DL ProLiant de HP con iLO Advanced para BladeSystem. Para obtener información adicional, consulte el CLUF (contrato de licencia de usuario final.)

HP continuará proporcionando versiones de mantenimiento con parches y mejoras de las características de iLO Standard e iLO Standard Blade Edition sin cargo adicional.

Existe una clave de licencia de evaluación de 60 días disponible para descargarse en la página Web de HP. La licencia de evaluación activa las funciones de iLO 2 Advanced y permite acceder a ellas. Sólo es posible instalar una licencia de evaluación por cada iLO 2. Una vez finalizado el periodo de evaluación, las funciones de iLO 2 se desactivan.

Se encuentran disponibles las siguientes versiones de iLO 2:

NOTA: Las funciones marcadas con asterisco (*) no son compatibles en todos los sistemas.

Característica	iLO 2 Advanced	iLO 2 Advanced para BladeSystem	iLO 2 Standard	iLO 2 Standard Blade Edition
Control de reinicio y alimentación virtual	√	√	√	√
Acceso a la consola de servidor mediante POST	√	√	√	√
Consola de texto después de POST	√	√	—	—
Registros de eventos	√	√	√	√
Estado del sistema* y configuración	√	√	√	√
UID	√	√	√	√
DMTF SMASH standard CLP	√	√	√	√
Creación de secuencias de comandos RIBCL/XML	√	√	√	√
Secuencias de comandos de WS Management	√	√	√	√
Acceso al explorador	√	√	√	√
Acceso de SSH	√	√	√	√
Shared Network Port (Puerto de red compartido)	√	—	√	—
Acceso en serie	√	√	√	√
Consola remota de serie	√	√	√	√
Consola remota integrada	√	√	—	√
Consola remota	√	√	—	√
Subprograma de soportes virtuales	√	√	—	√
Compatibilidad con tarjeta digital segura*	√	√	—	√
Transferencia de los servicios de Terminal Server	√	√	—	√

Característica	iLO 2 Advanced	iLO 2 Advanced para BladeSystem	iLO 2 Standard	iLO 2 Standard Blade Edition
Secuencias de comandos de soportes virtuales	√	√	—	—
Integración de directorios	√	√	—	—
Generación de errores relacionados con la alimentación*	√	√	—	—
Límites de la alimentación dinámica	√	√	—	—
Límites de la alimentación de grupo	√	√	—	—
Autenticación de tarjeta inteligente basada en dos factores	√	√	—	—
Inicio de sesión único de HP SIM	√	√	—	—
Depurador Kernel para Windows	√	√	—	—
Reproducción de la consola	√	√	—	—
Consola remota compartida	√	√	—	—
Boot/fault console capture (Captura de consola de inicio/fallo)	√	√	—	—
Reproductor de vídeo de iLO (es necesario disponer de licencia para efectuar la captura)	√	√	√	√

Además de las licencias del servidor único estándar iLO Advanced, hay otras dos opciones de licencia:

- El Flexible Quantity License Kit (Kit de licencias de cantidad flexible) permite adquirir un solo paquete de software, una copia de la documentación y una sola clave de licencia para activar el número exacto de licencias solicitadas.
- El Activation Key Agreement (Acuerdo de clave de activación) permite la adquisición por volumen del software ProLiant Essentials e Insight Control a lo largo del tiempo, normalmente junto con los nuevos servidores ProLiant de adquisición periódica.

Administración de usuarios

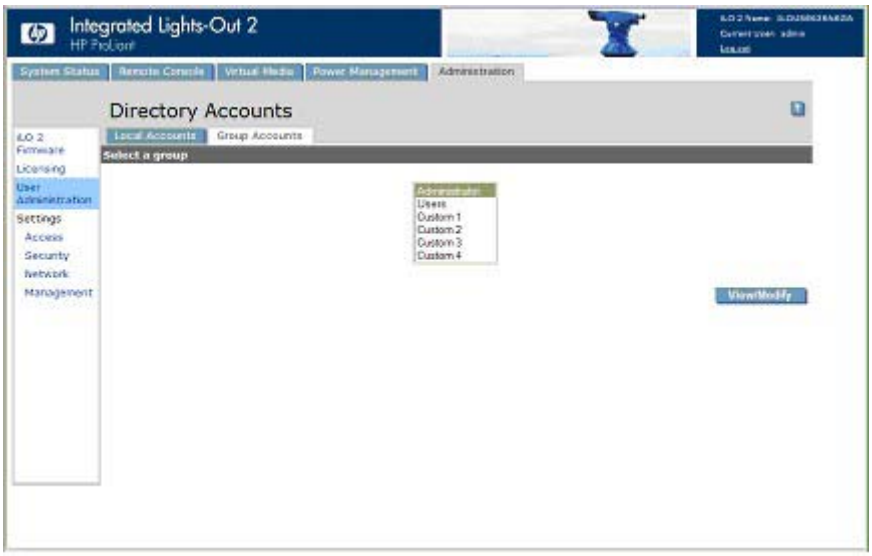
iLO 2 permite gestionar las cuentas de usuario almacenadas de forma local en la memoria segura de iLO 2 y en las cuentas de grupo del directorio. Utilice MMC o ConsoleOne para gestionar las cuentas de usuario del directorio.

iLO 2 admite hasta 12 usuarios con nombres de inicio de sesión, codificación avanzada de contraseñas y derechos de acceso personalizables. Los privilegios controlan la configuración de usuario individual. Los usuarios pueden tener privilegios personalizados según sus requisitos individuales de acceso. Para poder admitir más de 12 usuarios, es necesario disponer del Advanced Pack, que permite la integración con un número ilimitado de cuentas de usuario basadas en directorio.

Es necesario disponer del privilegio Administer User Accounts (Administración de cuentas de usuario) para ver a los usuarios iLO 2, añadir nuevos usuarios y modificar o eliminar los usuarios existentes. Si no cuenta con este privilegio, sólo podrá ver y modificar su cuenta.

Para acceder a las cuentas locales, haga clic en **Administration (Administración)>User Administration (Administración de usuarios)>Local Accounts (Cuentas locales)**.

La opción Directory Accounts (Cuentas de directorio) de iLO 2 permite ver los grupos de iLO 2 y modificar su configuración. Es necesario tener el privilegio Administer Directory Groups (Administrar grupos de directorio.) Para acceder a Directory Accounts (Cuentas de directorio), haga clic en **Administration (Administración)>User Administration (Administración de usuarios)>Group Accounts (Cuentas de grupo)**.



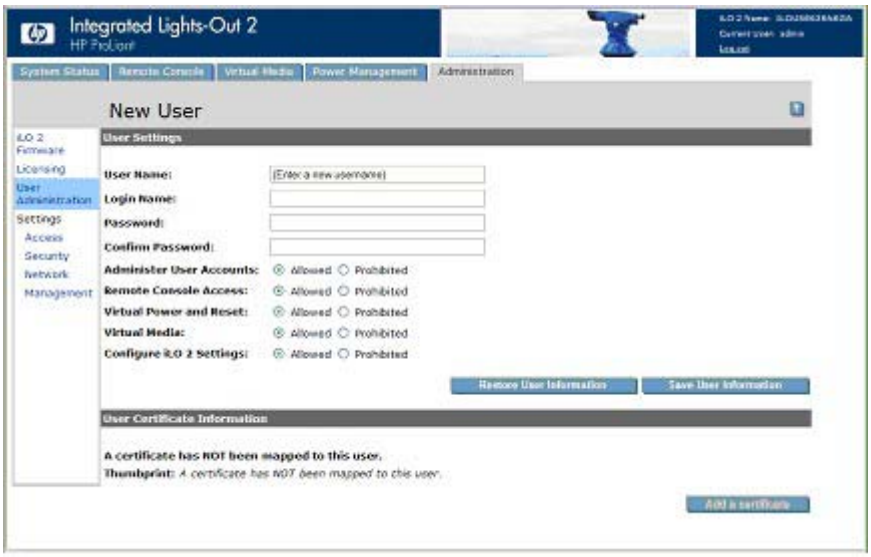
Adición de un nuevo usuario

NOTA: Sólo los usuarios que disponen del privilegio Administer User Accounts (Administración de cuentas de usuario) pueden gestionar otros usuarios en iLO 2.

Puede asignar un privilegio de acceso diferente a cada usuario. Cada usuario puede disponer de un conjunto exclusivo de privilegios, diseñado para las tareas que el usuario debe realizar. Puede permitir o denegar el acceso a las funciones críticas, por ejemplo, el acceso remoto, la administración de usuario, la alimentación virtual y otras funciones.

Para añadir un nuevo usuario a iLO 2:

1. Inicie sesión en iLO 2 con una cuenta que tenga el privilegio Administer User Accounts (Administración de cuentas de usuario.)
2. Haga clic en **Administration (Administration)**.
3. Seleccione **User Administration (Administración)>Local Accounts (Cuentas locales)**.
4. Haga clic en **New (Nuevo)**.



5. Complete los campos. Las siguientes opciones están disponibles:
   - User Name (Nombre de usuario) se muestra en la lista de usuarios y en la página principal. No es obligatorio que coincida con el nombre de inicio de sesión. La longitud máxima del nombre de usuario es de 39 caracteres. Los caracteres del nombre de usuario deben ser imprimibles.
   - Login Name (Nombre de inicio de sesión) es el nombre que debe utilizar al iniciar sesión en iLO 2. La longitud máxima del nombre de inicio de sesión es de 39 caracteres. Sólo se deben utilizar caracteres imprimibles para el nombre de inicio de sesión.
   - Los campos Password (Contraseña) y Confirm Password (Confirmar contraseña) permiten establecer y confirmar la contraseña que se utilizará cuando inicie sesión en iLO 2. La longitud mínima de la contraseña se establece en la página Access Options (Opciones de acceso.) La longitud máxima de la contraseña es de 39 caracteres. Para confirmar la contraseña, escríbala dos veces.
   - Administer User Accounts (Administración de cuentas de usuario) es un privilegio de usuario que permite añadir, modificar y eliminar cuentas de usuario iLO 2 locales. Asimismo, permite cambiar los privilegios de todos los usuarios, incluida su propia concesión de todos los

permisos. Sin este privilegio, sólo podrá ver su propia configuración y cambiar su propia contraseña.

- Remote Console Access (Acceso a consola remota) es un privilegio de usuario que permite acceder de forma remota a Remote Console (Consola remota) y Remote Serial Console (Consola remota de serie) del sistema host, incluido el control de vídeo, del teclado y del ratón. Para utilizar esta función, es necesario tener acceso al sistema remoto.
- Virtual Power and Reset (Alimentación virtual y reinicio) es un privilegio de usuario que permite encender y apagar o reiniciar la plataforma host. Cualquiera de estas actividades interrumpirá la disponibilidad del sistema. Asimismo, es posible diagnosticar el sistema mediante el botón NMI virtual.
- Virtual Media (Soportes virtuales) es un privilegio de usuario que permite utilizar los soportes virtuales en la plataforma host.
- Configure iLO 2 Settings (Configurar valores de iLO 2) es un privilegio que permite configurar la mayoría de ajustes de iLO 2, incluida la configuración de seguridad. Permite actualizar de forma remota el firmware de iLO 2. No se incluye la administración de cuentas de usuario. Esta configuración cambia raras veces.

  Una vez que haya configurado iLO 2 correctamente, cancele este privilegio para todos los usuarios de manera que no puedan cambiar la configuración. Un usuario con el privilegio Administer User Accounts (Administración de cuentas de usuario) puede activar y desactivar este privilegio. Si la utilidad RBSU de iLO 2 está activada, es posible volver a configurar iLO 2.
- User Certificate Information (Información acerca del certificado de usuario) asigna un certificado al usuario. Los certificados de usuario son necesarios únicamente para la autenticación basada en dos factores. Si no se ha asignado ningún certificado a la cuenta de usuario, aparecerá el mensaje `A certificate has NOT been mapped to this user` junto al botón Add a Certificate (Añadir un certificado.) Haga clic en este botón para asignar un certificado al usuario. Una vez asignado el certificado a la cuenta de usuario, aparecerá una huella digital del certificado de 40 dígitos junto al botón Remove this Certificate (Eliminar este certificado) que permite eliminar el certificado. Si se desactiva la opción Two-Factor Authentication (Autenticación basada en dos factores), se asignará un certificado diferente a cada usuario. Un usuario que presenta un certificado cuando se conecta a iLO 2 se autentica como el usuario al que se ha asignado el certificado. La opción Two-Factor Authentication (Autenticación basada en dos factores) debe estar activada para realizar la autenticación a través de un certificado.

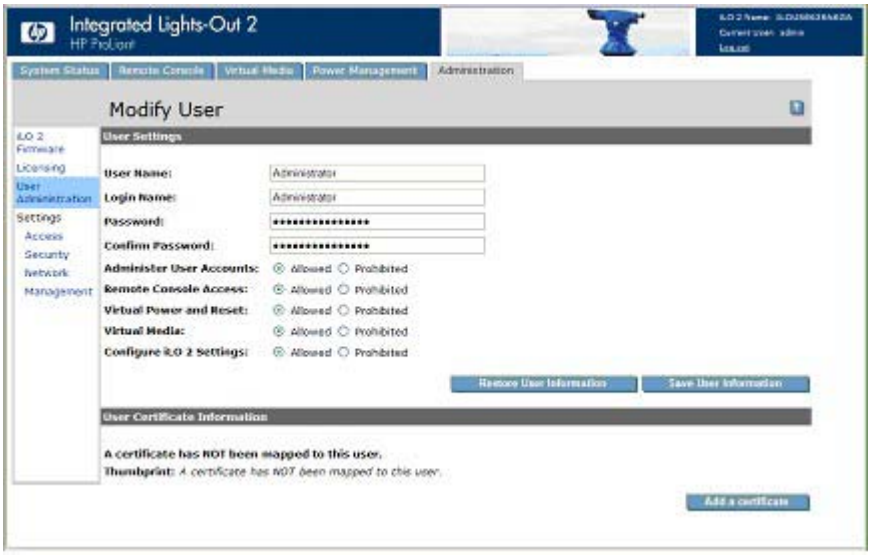
6. Cuando esté completo el perfil del usuario, haga clic en **Save User Information (Guardar información de usuario)** para volver a la pantalla User Administration (Administración de usuarios.) Para limpiar el perfil de usuario mientras se introduce un usuario nuevo, haga clic en **Restore User Information (Restaurar información de usuario)**.

Visualización o modificación de la configuración de un usuario existente

1. Inicie sesión en iLO 2 con una cuenta que tenga el privilegio Administer User Accounts (Administración de cuentas de usuario.)

   Debe tener el privilegio Administer User Accounts (Administración de cuentas de usuario) para gestionar a otros usuarios en iLO 2. Todos los usuarios pueden cambiar sus respectivas contraseñas mediante la función View/Modify User (Ver/Modificar usuario.)
2. Haga clic en **Administration (Administración)>User Administration (Administración de usuarios)**, y seleccione el nombre del usuario cuya información desee modificar.

3. Haga clic en **View/Modify (Ver/Modificar)**.



4. Cambie la información de usuario según sea necesario.
5. Cuando haya cambiado los campos, haga clic en **Save User Information (Guardar información de usuario)** para volver a la pantalla User Administration (Administración de usuarios.) Para recuperar la información original del usuario, haga clic en **Restore User Information (Restaurar información de usuario)**. Se descartarán todos los cambios realizados en el perfil.

Eliminación de un usuario

NOTA: Sólo los usuarios que disponen del privilegio Administer User Accounts (Administración de cuentas de usuario) pueden gestionar otros usuarios en iLO 2.

Para eliminar la información de un usuario existente:

1. Inicie sesión en iLO 2 con una cuenta con el privilegio Administer User Accounts (Administración de cuentas de usuario.) Haga clic en **Administration (Administration)**.
2. Haga clic en **User Administration (Administración de usuarios)** y seleccione en la lista el nombre del usuario cuya información desea modificar.
3. Haga clic en **Delete User (Eliminar usuario)**. Aparecerá una ventana con la pregunta `Are you sure you want to delete the selected user? (¿Está seguro de que desea eliminar el usuario seleccionado?)`. Haga clic en **Aceptar**.

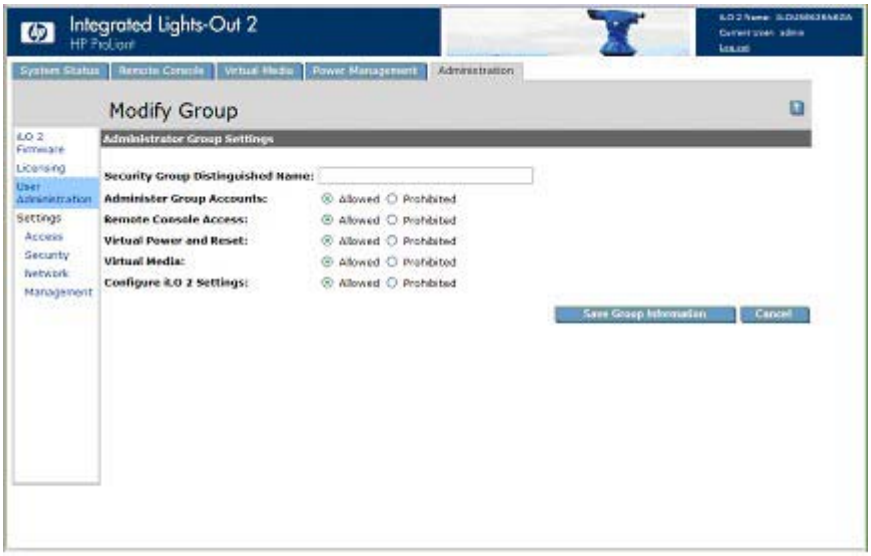
Administración de grupos

iLO 2 permite ver los grupos de iLO 2 y modificar su configuración. Es necesario tener el privilegio Administer Directory Groups (Administrar grupos de directorio.) Para ver o modificar un grupo:

1. Haga clic en **Administration (Administración)>User Administration (Administración de usuarios)>Group Accounts (Cuentas de grupo)**.

2. Seleccione el grupo y haga clic en **View/Modify Group (Ver/modificar grupo)**. Aparecerá la página Modify Group (Modificar grupo.)

   Haga clic en **Cancel (Cancelar)** para volver a la página Group Administration (Administración de grupos.)



Los siguientes valores de configuración están disponibles:

- Security Group Distinguished Name (Nombre completo del grupo de seguridad) es el nombre completo de un grupo del directorio. Se conceden a todos los miembros del grupo los privilegios establecidos para el grupo. El grupo especificado en Security Group Distinguished Name (Nombre completo del grupo de seguridad) debe existir en el directorio y los usuarios que necesitan acceso a iLO 2 deben ser miembros de este grupo. Complete este campo con un nombre completo del directorio (por ejemplo, CN=Group1 (Grupo 1),OU=Managed Groups (Grupos gestionados), DC=dominio, DC=extensión.)
- Administer Group Accounts (Administración de cuentas de grupo) permite a los usuarios que pertenecen a este grupo modificar los privilegios de cualquier grupo.
- Remote Console Access (Acceso a consola remota) permite acceder de forma remota a la consola remota del sistema host, incluido Remote Serial Console (Consola remota de serie.) Para poder utilizar esta función, es necesario tener acceso al sistema remoto.
- Virtual Power and Reset (Alimentación virtual y reinicio) permite apagar y encender o reiniciar la plataforma host. Estas actividades interrumpen la disponibilidad del sistema. Si selecciona esta opción, también podrá diagnosticar el sistema a través del botón NMI virtual.
- Virtual Media (Soportes virtuales) permite utilizar los soportes virtuales en la plataforma host.
- Configure iLO 2 Settings (Configurar valores de iLO 2) permite configurar la mayoría de los ajustes de iLO 2, incluidos los ajustes de seguridad. Si se selecciona, es posible actualizar el firmware de iLO 2 de forma remota. Esta configuración no incluye la administración de cuentas de grupos. Esta configuración cambia raras veces.

  Una vez que haya configurado iLO 2 correctamente, cancele este privilegio para todos los grupos de manera que no puedan cambiar la configuración. Los usuarios con el privilegio Administer Group Accounts (Administración de cuentas de grupo) pueden activar o desactivar este privilegio. iLO 2 también se puede volver a configurar si la utilidad RBSU de iLO 2 está activada.

Haga clic en **Save Group Information (Guardar información de grupo)** para guardar la información actualizada o en **Cancel (Cancelar)** para descartar los cambios y volver a la página Group Administration (Administración de grupos.)

Configuración del acceso a iLO 2

iLO 2 permite configurar los servicios que desea que se activen en iLO 2 y el acceso de los usuarios a iLO 2. Para configurar opciones de servicios de iLO 2(Opciones de servicios en la página 29), haga clic en **Administration (Administración)>Access (Acceso)**. Aparecerá la página (ficha) Services (Servicios.) Para configurar opciones de acceso a iLO 2 (Opciones de acceso en la página 36), haga clic en **Administration (Administración)>Access (Acceso)>Options (Opciones)** (ficha.) Debe tener el privilegio Configure iLO 2 Settings (Configurar valores de iLO 2) para modificar los servicios de iLO 2 y acceder a las opciones.

Opciones de servicios

La ficha Services (Servicios) permite seleccionar qué servicios desea activar en iLO 2, incluidos SSH, SSL, la consola remota, telnet y los servicios de Terminal Server. La ficha Services (Servicios) también permite establecer los puertos de cada opción seleccionada. La configuración de la página Services (Servicios) se aplica a todos los usuarios de iLO 2. Es necesario disponer del privilegio Configure iLO 2 Settings (Configurar valores de iLO 2) para modificar la configuración en esta página.

Para acceder a Services (Servicios), haga clic en **Administration (Administración)>Access (Acceso) >Services (Servicios)**. Haga clic en **Apply (Aplicar)** para guardar la información actualizada. Es necesario reiniciar iLO 2 para que se apliquen los cambios. Si se han realizado cambios para activar o desactivar la funcionalidad de Lights-Out, al hacer clic en **Apply (Aplicar)** finalizará la conexión con el explorador y se reiniciará iLO 2. Antes de intentar restablecer la conexión, debe esperar como mínimo 30 segundos.

En la ficha Services (Servicios) se incluyen los siguientes ajustes:

Parámetro	Valor predeterminado	Descripción
Secure Shell(SSH) Access (Acceso de Shell de seguridad)	Enabled (Activado)	Este parámetro permite especificar si la función SSH en iLO 2 debe estar activada o desactivada.
Secure Shell (SSH) Port (Puerto de Shell de seguridad)	22	Este parámetro permite configurar el puerto de SSH de iLO 2 para que se utilice en comunicaciones SSH.
Telnet Access (Acceso Telnet)	Disabled (Desactivado)	Este valor le permite conectar un cliente Telnet a la consola remota/puerto Telnet, proporcionando acceso a CLP de iLO 2. Son válidas las siguientes opciones de configuración: • Enabled (Activado): iLO 2 permitirá a los clientes Telnet conectarse a una consola remota/puerto Telnet. Los analizadores de puertos de red pueden detectar que iLO 2 está conectado a este puerto. Se permite la comunicación no codificada entre CLP de iLO 2 y clientes Telnet. • Disabled (Desactivado): iLO 2 no permitirá a los clientes Telnet conectarse a una consola remota/puerto Telnet. Los analizadores de los puertos de red normalmente no detectarán si este puerto está abierto en iLO 2. iLO 2 se conectará a este puerto durante unos segundos cuando se abra la consola remota, pero no se aceptarán las conexiones Telnet. La comunicación entre iLO 2 y la consola remota siempre está codificada.
Remote Console/Telnet Port (Consola remota/Puerto Telnet)	23	Este valor permite especificar el puerto que utiliza la consola remota de iLO 2 para las comunicaciones de la consola remota.
Web Server Non-SSL Port (Puerto no SSL del servidor Web)	80	Este parámetro permite especificar el puerto que utiliza el servidor Web integrado en iLO 2 para las comunicaciones no codificadas.
Web Server SSL Port (Puerto SSL del servidor Web)	443	Este parámetro permite especificar el puerto que utiliza el servidor Web integrado en iLO 2 para las comunicaciones codificadas.
Terminal Services Passthrough (Transferencia de los servicios de Terminal Server)	Disabled (Desactivado)	Este valor permite controlar la capacidad de admitir una conexión mediante iLO 2 entre un cliente de servicios de Microsoft® Terminal Server y un servidor de servicios de Terminal Server que esté

Parámetro	Valor predeterminado	Descripción
		en ejecución en el host. Son válidas las siguientes opciones de configuración: • Automatic (Automático): cuando se inicia la consola remota, también se inicia el cliente de los servicios de Terminal Server. • Enabled (Activado): la función de transferencia está habilitada y puede conectar el cliente de los servicios de Terminal Server directamente a iLO 2 sin iniciar sesión en iLO 2. • Disabled (Desactivado): la función de transferencia está deshabilitada.
Terminal Services Port (Puerto de los servicios de Terminal Server)	3389	Este valor permite especificar el puerto de los servicios de Terminal Server que utiliza iLO 2 para las comunicaciones codificadas con el software de transferencia de los servicios de Terminal Server del servidor. Si el puerto de los servicios de Terminal Server se encuentra configurado en un ajuste distinto del predeterminado, deberá cambiar el número de puerto manualmente.
Virtual Media Port (Puerto de soportes virtuales)	17988	Este parámetro permite especificar el puerto para la compatibilidad de soportes virtuales en comunicaciones iLO 2.
Shared Remote Console Port (Puerto de consola remota compartida)	9300	Este valor permite especificar el puerto de la consola remota compartida. El puerto de consola remota compartida se abre en el cliente para permitir que los usuarios adicionales se conecten con la consola remota de igual manera. Este puerto sólo se abre cuando la consola remota compartida se encuentra en uso.
Console Replay Port (Puerto de reproducción de la consola)	17990	Este valor permite especificar el puerto de reproducción de la consola. El puerto de reproducción de la consola se abre en el cliente para activar la transferencia de búferes de captura interna del cliente para su reproducción. Este puerto sólo se abre cuando se transfiere un búfer de captura al cliente.
Raw Serial Data Port (Puerto de datos de serie no procesado)	3002	Este ajuste permite especificar la dirección del puerto de datos de serie no procesado. El puerto de datos de serie no procesado sólo está abierto mientras se usa la utilidad WiLODbg.exe para depurar el servidor host de manera remota.

Opción Terminal Services Passthrough

Los sistemas operativos Microsoft® Windows® proporcionan los servicios de Terminal Server. La opción de transferencia de los servicios de Terminal Server de iLO 2 sirve de conexión entre el servidor de los servicios de Terminal Server en el sistema host y el cliente de los servicios de Terminal Server en el sistema cliente. Cuando se activa la opción de transferencia de los servicios de Terminal Server, el firmware de iLO 2 activa un socket, conectándose de forma predeterminada al puerto 3389. Todos los datos recibidos de los servicios de Terminal Server en este puerto se reenvían al servidor y todos los datos que los servicios de Terminal Server reciben del servidor pasan al socket. El firmware de iLO 2 lee todos los elementos recibidos en este puerto como un paquete RDP. Los paquetes RDP se intercambian entre el firmware de iLO 2 y el servidor (RDP) de los servicios de Terminal Server a través de la dirección de host local en el servidor. El servicio proporcionado facilita la comunicación entre el firmware de iLO 2 y el servidor RDP. El servidor RDP interpreta el servicio como una conexión RDP externa establecida. Para obtener más información acerca del servicio RDP (Remote Desktop Protocol, Protocolo de escritorio remoto), consulte la sección "Servicio de transferencia RDP de Windows® (Servicio de transferencia RDP de Windows en la página 33)".

Una sesión de Terminal Sevices proporciona una vista de mejora del rendimiento de la consola del sistema host. Cuando el sistema operativo no está disponible (o bien el servidor o cliente de los servicios de Terminal Server no está disponible), es la consola remota tradicional de iLO 2 la que proporciona la vista de la consola del sistema host. Para obtener más información acerca de la consola remota y los servicios de Terminal Server, consulte la sección “Consola remota y clientes de los servicios de Terminal Server (Consola remota y clientes de los servicios de Terminal Server en la página 34)”.

Para configurar la opción de transferencia de servicios de Terminal Server, consulte las secciones "Requisitos del cliente de los servicios de Terminal Server (Requisitos del cliente de los servicios de Terminal Server en la página 32)" e "Instalación de transferencia de los servicios de Terminal Server (Instalación de la transferencia de los servicios de Terminal Server en la página 33)".

Requisitos del cliente de los servicios de Terminal Server

El cliente de los servicios Terminal Server está disponible en equipos cliente Microsoft® Windows® que funcionen con:

- Windows Server® 2003

  En los servidores Windows Server® 2003, se integra el cliente de servicios de Terminal Server y la conexión RDP. El cliente es una parte del sistema operativo y se activa mediante el uso compartido de escritorio remoto. Para activar el uso compartido del escritorio, seleccione **Mi PC>Propiedades>Remoto>Escritorio remoto**. El cliente de los servicios de Terminal Server en Windows Server® 2003 permite opciones de la línea de comandos y se inicia perfectamente desde el subprograma de la consola remota.

- Windows Server® 2008

  En los servidores Windows Server® 2008, se integra el cliente de servicios de Terminal Server y la conexión RDP. El cliente es una parte del sistema operativo y se activa mediante el uso compartido de escritorio remoto. Para activar el uso compartido del escritorio, seleccione **Mi PC>Propiedades>Remoto>Escritorio remoto**. El cliente de los servicios de Terminal Server en Windows Server® 2008 permite opciones de la línea de comandos y se inicia perfectamente desde el subprograma de la consola remota.

- Windows® XP

  En los servidores Windows® XP, el cliente de servicios de Terminal Server y la conexión RDP están integrados. El cliente es una parte del sistema operativo y se activa mediante el uso compartido de escritorio remoto. Para activar el uso compartido del escritorio, seleccione **Inicio>Programas>Accesorios>Comunicaciones>Escritorio remoto**. El cliente de los

servicios de Terminal Server en Windows® XP proporciona opciones de la línea de comandos y se inicia desde el subprograma de la consola remota.

Servicio de transferencia RDP de Windows

Para utilizar la función Terminal Services Passthrough (Transferencia de servicios de Terminal Server) de iLO 2, es necesario instalar un servicio de transferencia en el sistema host. Este servicio muestra el nombre del proxy de iLO 2 en la lista de host de servicios disponibles. El servicio utiliza la seguridad y fiabilidad de Microsoft® .NET framework. Una vez iniciado el servicio, éste sondea iLO 2 para detectar si se ha establecido una conexión RDP con el cliente. Si se ha establecido una conexión RDP con el cliente, el servicio establece una conexión TCP con el host local y comienza el intercambio de paquetes. El puerto utilizado para establecer la comunicación con el host local se lee en el Registro de Windows® en la ubicación siguiente:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\Wds
\rdpwd\Tds\tcp\PortNumber
```

Normalmente, se trata del puerto 3389.

Instalación de la transferencia de los servicios de Terminal Server

En la siguiente sección se describe cómo instalar la transferencia de servicios de Terminal Server en Windows Server® 2008, Windows Server® 2003 y Microsoft® Windows® XP.

- Windows Server® 2003 y Windows Server® 2008

  Los servidores Windows® requieren Microsoft® .NET Framework para admitir el uso de servicios de Terminal Server de iLO 2. Es necesario que el servidor en el que se encuentra iLO 2 tenga instalado el servicio de transferencia de servicios de Terminal Server e iLO 2 Management Interface driver para Windows Server ® 2008 y Windows Server® 2003.

  a. Instale iLO 2 Management Interface driver.

  b. Instale el servicio de transferencia. Para instalar el servicio, inicie el instalador de componentes y siga las directrices del asistente para la instalación.

  Si el servicio ya está instalado, debe reiniciar o reiniciar manualmente el servidor una vez instalado el controlador.

  c. Active el cliente de los servicios de terminal Server.

  En Windows Server® 2003 y Windows Server® 2008, active el uso compartido del escritorio remoto haciendo clic en la ficha **Remoto**, bajo Mi PC y Propiedades.

  Si la instalación de iLO 2 ha finalizado y la opción Terminal Services Passthrough (Transferencia de los servicios de Terminal Server) está configurada en automática, los servicios de Terminal Server se iniciarán una vez finalizada la instalación.

- Microsoft® Windows® XP

  En Windows® XP, la opción de conexión a escritorio remoto está integrada y no tiene otros requisitos de instalación.

Los errores que se producen durante la instalación y ejecución del servicio de transferencia se registran en el Registro de sucesos de la aplicación del servidor. Es posible eliminar el servicio de transferencia mediante la opción Agregar o quitar programas del Panel de Control.

Activación de la opción Terminal Services

De manera predeterminada, la función de transferencia de de servicios de Terminal Server se encuentra deshabilitada y puede habilitarse en la página Administration (Administración)>Access (Acceso)

>Services (Servicios.) El botón Terminal Services (Servicios de Terminal Server) de la consola remota permanece desactivado hasta que se activa esta función.

Para utilizar la función, instale el controlador de interfaz de gestión de Lights-Out más reciente y, a continuación, instale el servicio Terminal Services Passthrough (Transferencia de los servicios de Terminal Server) para Microsoft® Windows® en el servidor.

Cuando la opción Terminal Services Passthrough (Transferencia de los servicios de Terminal Server) está ajustada a Enabled (Activado) o Automatic (Automático) en la página Administration (Administración)>Access (Acceso)>Services (Servicios) y el cliente de los servicios de Terminal Server está instalado en el cliente de Windows® (se instala por defecto en Windows® XP), el botón Terminal Services (Servicios de Terminal Server) se activa. Al hacer clic en el botón Terminal Services (Servicios de Terminal Server), el subprograma intenta iniciar los servicios de Terminal Server, aunque el servidor no se esté ejecutando en un sistema operativo Windows®.

Es necesario cumplir con los requisitos de licencia de Microsoft®, que son los mismos que se necesitan para realizar una conexión por medio de la NIC del servidor. Por ejemplo, cuando están configurados para el acceso administrativo, los servicios de Terminal Server no permiten más de dos conexiones, independientemente de si éstas se establecen a través de la NIC del servidor, de iLO 2 o de ambos.

Mensaje de advertencia de los servicios de Terminal Server

Los usuarios de los servicios de Terminal Server que trabajan con Windows® 2003 Server pueden notar lo siguiente al utilizar la función de transferencia de servicios de Terminal Server de iLO 2. Si se establece una sesión de los servicios de Terminal Server a través de iLO 2 y se establece una segunda sesión de los servicios de Terminal Server mediante un administrador de Windows® (modo Consola), se desconectará la primera sesión de los servicios de Terminal Server. Sin embargo, la primera sesión no recibirá el mensaje de advertencia que indique esta desconexión hasta transcurrido aproximadamente un minuto. Durante este minuto, la primera sesión de los servicios de Terminal Server estará disponible o activa. Este comportamiento es normal, pero es diferente del observado cuando los administradores de Windows® establecen dos sesiones de los servicios de Terminal Server. En este caso, la primera sesión de los servicios de Terminal Server recibirá el mensaje de advertencia de forma inmediata.

Pantalla de la opción Terminal Services Passthrough

Es posible que el firmware de iLO 2 no muestre de forma precisa la opción Terminal Services Passthrough (Transferencia de los servicios de Terminal Server.) La opción Terminal Services Passthrough (Transferencia de los servicios de Terminal Server) puede mostrarse activa aunque el sistema operativo no tenga activados los servicios de Terminal Server (por ejemplo, si el sistema operativo del host es Linux, que no es compatible con el funcionamiento de los servicios de Terminal Server.)

Consola remota y clientes de los servicios de Terminal Server

Mediante la conexión de la red de gestión a iLO 2, se puede usar una sesión de la consola remota de iLO 2 para mostrar al host una sesión de los servicios de Terminal Server. Cuando se ejecute el subprograma de la consola remota de iLO 2, se iniciará el cliente de los servicios de Terminal Server según las preferencias del usuario. Es preciso instalar Sun JVM para que esta función funcione correctamente. Si no está instalado Sun JVM, la consola remota no podrá iniciar automáticamente el cliente de los servicios de Terminal Server.

Si está activada la transferencia de los servicios de Terminal Server y está disponible el servidor de los servicios de Terminal Server, el cambio entre la consola remota de iLO 2 y el cliente de los servicios de Terminal Server se produce sin problemas, ya que el servidor pasa de un entorno previo al sistema operativo al entorno de ejecución del sistema operativo y a un entorno en el que éste no está disponible. Dicho funcionamiento está disponible mientras no se inicie el cliente de los servicios de Terminal Server

antes de que esté disponible la consola remota. Si están disponibles la consola remota y el cliente de los servicios de Terminal Server, la consola remota iniciará el cliente de los servicios de Terminal Server cuando sea apropiado.

Al utilizar la opción de transferencia de los servicios de Terminal Server con Windows Server® 2003 y Windows Server® 2008, se produce un retraso de aproximadamente 30 segundos después de mostrarse el cuadro de diálogo CTRL-ALT-DEL antes de que se inicie el cliente de los servicios de Terminal Server. Este retraso de 30 segundos representa el tiempo que tarda el servicio en conectarse al cliente RDP que se ejecuta en el servidor. Si se reinicia el servidor desde el cliente de los servicios de Terminal Server, la pantalla de la consola remota se volverá gris o negra durante un minuto como máximo mientras iLO 2 determina que ya no está disponible el servidor de los servicios de Terminal Server.

Si el modo de los servicios de Terminal Server está establecido en Enabled (Activado) pero desea usar la consola remota, inicie el cliente de los servicios de Terminal Server directamente desde el menú del cliente de los servicios de Terminal Server. Al iniciarse directamente desde el menú del cliente se permite la utilización simultánea del cliente de los servicios de Terminal Server y de la consola remota.

Los servicios de Terminal Server se pueden activar y desactivar en cualquier momento. Al cambiar la configuración de los servicios de Terminal Server, se reiniciará el firmware de iLO 2. Al volver a configurar el firmware de iLO 2 se interrumpe cualquier conexión abierta a iLO 2.

Cuando la consola remota inicia el cliente de los servicios de Terminal Server, ésta entra en modo de inactividad para evitar que se consuma ancho de banda de la CPU. La consola remota sigue conectada al puerto predeterminado 23 para comprobar si hay comandos de iLO 2.

iLO 2 trasfiere sólo una conexión de los servicios de Terminal Server de una vez. Los servicios de Terminal Server tienen un límite de dos sesiones concurrentes.

La consola remota se activará y estará disponible si está en modo de inactividad y el cliente de los servicios de Terminal Server se ve interrumpido por cualquiera de los sucesos siguientes:

- El usuario cierra el cliente de los servicios de Terminal Server.
- Se cierra el sistema operativo Windows®.
- Se bloquea el sistema operativo Windows®.

Solución de problemas de servicios de Terminal Server

Para solucionar problemas con la Transferencia de los servicios de Terminal Server de iLO 2:

1. Compruebe que los servicios de Terminal Server se encuentran activados en el host mediante la selección de **Mi PC>Propiedades>Remoto>Escritorio remoto**.
2. Asegúrese de que la configuración de la transferencia de iLO 2 está activa o en modo automático en la configuración global de iLO 2.
3. Asegúrese de disponer de la licencia correspondiente para iLO Advanced Pack.
4. Asegúrese de que iLO 2 Management Interface Driver está instalado en el host. Para comprobar el controlador, seleccione **Mi PC>Propiedades>Hardware>Administrador de dispositivos>Multifunction Adapters**.
5. Asegúrese de que el servicio de transferencia de los servicios de Terminal Server y el proxy de iLO 2 están instalados y se están ejecutando en el host. Para comprobar estos servicios, seleccione **Panel de control>Herramientas administrativas>Servicios** e intente reiniciar el servicio.
6. Asegúrese de que el Registro de sucesos de la aplicación no está completo.

Se pueden producir problemas de inicio en el servicio de transferencia de los servicios de Terminal Server si el Registro de sucesos de la aplicación del sistema operativo está completo. Para visualizar el registro de eventos, seleccione **Administración de equipos>Herramientas del sistema>Visor de eventos>Aplicación**.

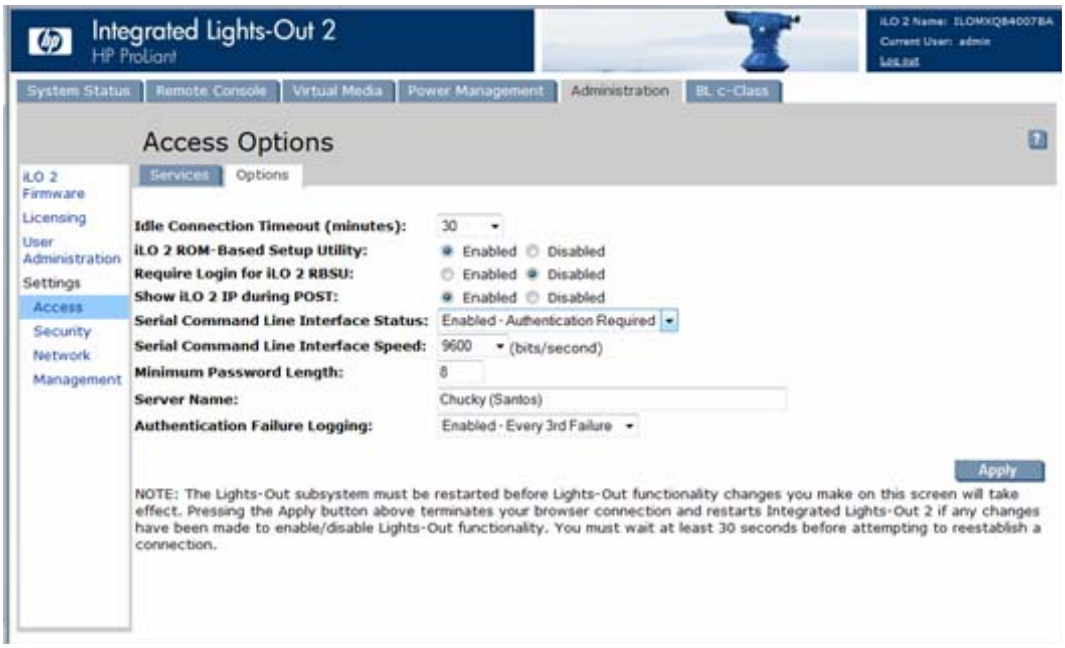
7. Asegúrese de que la asignación de puerto de los servicios de Terminal Server es correcta.
8. Asegúrese de que el cliente de los servicios de Terminal Server, `mstsc.exe` se encuentre en `\WINDOWS\SYSTEM32`.

   En caso de que no sea así, establezca la configuración de la transferencia en **Enabled (Activado)** y active manualmente el cliente de los servicios de Terminal Server.

Opciones de acceso

iLO 2 permite modificar el acceso a iLO 2, incluido el tiempo de inactividad de la conexión, la funcionalidad iLO 2, la utilidad RBSU de iLO 2, los requisitos de inicio de sesión, los parámetros CLI, la longitud mínima de la contraseña y el nombre del servidor. La configuración de la página Access Options (Opciones de acceso) se aplica a todos los usuarios de iLO 2. Es necesario disponer del privilegio Configure iLO 2 Settings (Configurar valores de iLO 2) para modificar la configuración en esta página.

Para visualizar o modificar el acceso a iLO 2, haga clic en **Administration (Administración)>Access (Acceso)>Options (Opciones)** y haga clic en **Apply (Aplicar)** para guardar la información actualizada. Es necesario reiniciar iLO 2 para que se apliquen las actualizaciones. Si se han realizado cambios para activar o desactivar la funcionalidad de Lights-Out, haga clic en **Apply (Aplicar)** para finalizar la conexión con el explorador y reiniciar iLO 2. Antes de intentar restablecer la conexión, debe esperar como mínimo 30 segundos.



En la ficha Options (Opciones) se incluyen los siguientes ajustes:

Parámetro	Valor predeterminado	Descripciones
Idle Connection Timeout (minutes) [Tiempo de Espera de inactividad de la conexión (minutos)]	30 minutos	Este valor determina el intervalo de tiempo de inactividad del usuario, en minutos, antes de que el servidor Web y

Parámetro	Valor predeterminado	Descripciones
		la sesión de la consola remota terminen automáticamente. Son válidas las siguientes opciones de configuración: 15, 30, 60, 120 minutos o 0 (infinito.) El valor de tiempo de espera infinito no cierra la sesión de los usuarios inactivos.
Lights-Out Functionality (Funcionalidad de Lights-Out)	Enabled (Activado)	Este valor permite establecer la conexión a iLO 2. Si está deshabilitado, no se podrá establecer ninguna conexión a iLO 2. La red y las comunicaciones 10/100 de iLO 2 con controladores del sistema operativo se desactivan si la funcionalidad de Lights-Out está desactivada. El puerto de diagnóstico de iLO 2 de un servidor HP ProLiant BL p Class también está deshabilitado. Si la funcionalidad de iLO 2 está desactivada (incluido el puerto de diagnóstico de iLO 2), es necesario utilizar el conmutador de anulación de la seguridad del servidor para activar iLO 2. Para localizar el conmutador de anulación de la seguridad y configurarlo para la anulación, consulte la documentación de su servidor. Encienda el servidor y utilice la utilidad RBSU de iLO 2 para establecer Lights-Out Functionality (Funcionalidad de Lights-Out) en Enabled (Activado.)
ROM-Based Setup Utility de iLO2	Enabled (Activado)	Este ajuste permite activar o desactivar la ROM-Based Setup Utility de iLO 2. Normalmente, la ROM de las opciones de iLO2 le solicita que pulse **F8** para acceder a la RBSU, pero si iLO 2 o RBSU de iLO 2 se encuentran desactivados, la solicitud de RBSU es omitida.
Require Login for iLO 2 RBSU (Requerir inicio de sesión para RBSU de iLO 2)	Disabled (Desactivado)	Este valor permite acceder a la utilidad RBSU con o sin desafío en las credenciales de usuario. Si el valor se ha configurado en Enabled (Activado) y pulsa la tecla **F8** durante el proceso POST para entrar en la utilidad RBSU de iLO 2, aparece un cuadro de diálogo de inicio de sesión.
Show iLO 2 during POST (Mostrar iLO 2 durante POST)	Disabled (Desactivado)	Esta configuración permite la visualización de la dirección IP de red de iLO 2 durante el proceso de POST del servidor host.
Serial Command Line Interface Status (Estado de interfaz de línea de comando de serie)	Enabled (Activado)-Authentication Required (Autenticación necesaria)	Este parámetro permite cambiar el modelo de inicio de sesión de la función CLI a través del puerto serie. Son válidas

Parámetro	Valor predeterminado	Descripciones
		las siguientes opciones de configuración: • Enabled (Activado)-Authentication Required (Autenticación necesaria) • Enabled (Activado)-No Authentication (Sin autenticación) • Disabled (Desactivado)
Serial Command Line Interface Speed (Velocidad de interfaz de línea de comando de serie)	9600	Este parámetro permite utilizar el puerto serie para cambiar la velocidad del puerto serie para la función CLI. Las siguiente velocidades (en bits/s) son válidas: 9.600, 19.200, 38.400, 57.600 y 115.200. Para un funcionamiento óptimo, la configuración del puerto serie debe establecerse en No parity (Sin paridad), 8 bits de datos y 1 bit de parada (N/8/1.) La velocidad del puerto serie definida por este parámetro debe coincidir con la velocidad del puerto serie definida en la configuración de RBSU de la memoria ROM del sistema.
Minimum Password Length (Longitud mínima de la contraseña)	8	Este valor especifica el número mínimo de caracteres permitidos cuando se establece o se cambia una contraseña de usuario. La longitud de caracteres puede establecerse en un valor comprendido entre 0 y 39.
Server Name (Nombre del servidor)	—	Esta configuración le permite especificar el nombre del servidor host. Este valor se asigna cuando se utilizan los agentes de gestión de HP ProLiant. Si no utiliza estos agentes y aparece el mensaje del host sin nombre, puede cambiarlo desde aquí. Si se están ejecutando los agentes, se podrá sobrescribir el valor que asigne. Para obligar al explorador a actualizarse, guarde la configuración y pulse **F5**.
Authentication Failure Logging (Fallo de autenticación en inicio de sesión)	Enabled-Every 3rd Failure (Activado: cada 3 fallos)	Este ajuste permite configurar los criterios de inicio de sesión para las autenticaciones que presentan fallos. Se admiten todos los tipos de inicio de sesión y cada uno de ellos funciona de manera independiente. Son válidas las siguientes opciones de configuración: • Enabled-Every Failure (Activado: cada fallo): se graba una entrada de registro de inicio de sesión después de cada fallo al intentar iniciar sesión. • Enabled-Every 2nd Failure (Activado: cada dos fallos): se graba una entrada de registro de inicio de sesión cada dos fallos al intentar iniciar sesión.

Parámetro	Valor predeterminado	Descripciones
		• Enabled-Every 3rd Failure (Activado: cada 3 fallos): se graba una entrada de registro de inicio de sesión cada tres fallos al intentar iniciar sesión. • Enabled-Every 5th Failure (Activado: cada 5 fallos): se graba una entrada de registro de inicio de sesión cada 5 fallos al intentar iniciar sesión. • Disabled (Desactivada): no se graba ninguna entrada de registro de inicio de sesión que presente fallos.

Cuando se inicia sesión en iLO 2 con clientes SSH o Telnet, las líneas de comandos con el número del nombre de inicio de sesión y la contraseña que ofrece iLO 2 coinciden con el valor del parámetro Authentication Failure Logging (Fallo de autenticación en inicio de sesión) (o 3 cuando está desactivada.) Sin embargo, el número de líneas de comandos puede verse afectado por las configuraciones de su cliente SSH o Telnet. Los inicios de sesión en SSH y Telnet también suponen retrasos tras un fallo en el inicio de sesión. Durante el retraso, el inicio de sesión se desactiva y, por lo tanto, no se produce ningún fallo de inicio de sesión. Por ejemplo, para generar un registro de fallo de autenticación SSH con el valor predeterminado (por ejemplo, Enabled-Every 3rd Failure [Activado: cada 3 fallos]), se producen 3 fallos consecutivos de inicio de sesión (suponiendo que el cliente SSH esté configurado con un número de línea de comandos de la contraseña >= 3):

1. Ejecute el cliente SSH e inicie sesión con un nombre de inicio de sesión y contraseña incorrectos. Recibirá tres líneas de comandos de la contraseña. Tras la tercera contraseña incorrecta, la conexión finaliza y se graba el primer fallo de inicio de sesión. El contador de fallos de inicio de sesión SSH se establece en 1.
2. Ejecute el cliente SSH hasta que reciba la línea de comandos de inicio de sesión. Inicie sesión con un nombre de inicio de sesión y contraseña incorrectos. Recibirá tres líneas de comandos de la contraseña. Tras la tercera contraseña incorrecta, la conexión finaliza y se graba el segundo fallo de inicio de sesión. El contador de fallos de inicio de sesión SSH se establece en 2.
3. Ejecute el cliente SSH hasta que reciba la línea de comandos de inicio de sesión. Inicie sesión con un nombre de inicio de sesión y contraseña incorrectos. Recibirá tres líneas de comandos de la contraseña. Tras la tercera contraseña incorrecta, la conexión finaliza y se graba el tercer fallo de inicio de sesión. El contador de fallos de inicio de sesión SSH se establece en 3.

En este momento, el firmware de iLO 2 graba una entrada de registro de fallo de inicio de sesión SSH y establece el contador de fallos de inicio de sesión SSH en 0.

Acceso a la consola remota y a la consola remota de serie de iLO 2

Para obtener información acerca de la configuración de cliente recomendada para la consola remota de iLO 2, la configuración del servidor, la optimización de la compatibilidad del ratón y la configuración de la consola remota de serie, consulte la sección "iLO 2 Remote Console" (iLO 2 Remote Console en la página 89.)

Seguridad

iLO 2 permite personalizar la configuración de seguridad. Para acceder a la configuración de la seguridad de iLO 2, seleccione **Administration (Administración)>Security (Seguridad)**. Entre las opciones de seguridad de iLO 2 se incluyen:

- Administración de la clave SSH (Administración de la clave SSH en la página 44)
- Administración del certificado SSL (Administración del certificado SSL en la página 44)
- Autenticación basada en dos factores (Autenticación basada en dos factores en la página 45)
- Configuración de directorio (Configuración de directorio en la página 52)
- Cifrado de iLO 2
- Inicio de sesión único de HP SIM (Inicio de sesión único de HP SIM (SSO) en la página 57)
- Bloqueo de equipo de consola remota (Bloqueo de equipo de consola remota en la página 61)

Las opciones de seguridad de iLO 2 permiten a iLO 2 ofrecer las siguientes funciones de seguridad:

- Puertos TCP/IP definidos por el usuario
- Acciones de usuario registradas en el registro de sucesos de iLO 2.
- Retrasos progresivos para los intentos de inicios de sesión con fallo
- Compatibilidad con certificados firmados X.509 CA
- Compatibilidad con la seguridad en RBSU
- Comunicación cifrada a través de:
  - Administración de la clave SSH
  - Administración del certificado SSL
- Compatibilidad con servicios de directorio basados en LDAP opcionales

Algunas de estas opciones son funciones con licencia. Para comprobar las opciones disponibles, consulte la sección "Concesión de licencias" (Concesión de licencias en la página 21.)

Directrices generales de seguridad

A continuación se muestran las directrices generales relativas a la seguridad para iLO 2:

- Para obtener la seguridad máxima, iLO 2 debe configurarse en una red de gestión independiente.
- iLO 2 no debe conectarse directamente a Internet.
- Debe utilizarse un explorador con el sistema de codificación de 128 bits.

Directrices para las contraseñas

A continuación, se muestra una lista de las directrices recomendadas para establecer contraseñas. Las contraseñas:

- Nunca deben escribirse ni grabarse.
- Nunca deben compartirse con otras personas.

- No deben contener palabras que se encuentren en un diccionario o que sean fáciles de adivinar, como el nombre de la compañía, los nombres de producto o el nombre o el ID del usuario.
- Deben presentar, al menos, tres de las cuatro funciones siguientes:
  - Al menos un carácter numérico
  - Al menos un carácter especial
  - Al menos un carácter en minúsculas
  - Al menos un carácter en mayúsculas;

Las contraseñas establecidas para un ID de usuario temporal, para volver a establecer una contraseña o un ID de usuario bloqueado también deben ajustarse a estos estándares. Las contraseñas carecen de longitud mínima, pero su longitud máxima es de 39 caracteres. La longitud mínima predeterminada está establecida en ocho caracteres. No se recomienda establecer una longitud mínima de contraseña inferior a ocho caracteres, a menos que disponga de una red de administración segura físicamente que no se extienda más allá del centro de datos seguro.

Seguridad en RBSU

La utilidad RBSU de iLO 2 permite ver y modificar la configuración de iLO 2. Es posible configurar los ajustes de acceso de RBSU a través de la utilidad RBSU, un explorador Web (Opciones de acceso (Opciones de acceso en la página 36)), las secuencias de comandos RIBCL o el conmutador de anulación de la seguridad de iLO 2. La utilidad RBSU dispone de tres niveles de seguridad:

- Inicio de sesión de la utilidad RBSU no necesario (predeterminado)

  Cualquiera que tenga acceso al host durante el proceso de POST puede acceder a la utilidad RBSU de iLO 2 para visualizar y modificar los ajustes de la configuración. Esta configuración es aceptable si está controlado el acceso al host.
- Inicio de sesión de la utilidad RBSU necesario (más seguro)

  Si es necesario iniciar una sesión en la utilidad RBSU, los menús de configuración activos se controlarán por medio de los derechos de acceso del usuario autenticado.
- Utilidad RBSU desactivada (más seguro)

  Si la utilidad RBSU de iLO 2 está desactivada, no se permite el acceso del usuario. Esto evita la modificación por medio de la interfaz de la utilidad RBSU.

Administración del conmutador de anulación de la seguridad de la placa iLO 2

El conmutador de anulación de la seguridad de iLO 2 concede al administrador acceso total al procesador iLO 2. Este acceso puede ser necesario para alguna de las siguientes condiciones:

- iLO 2 debe reactivarse después de su desactivación.
- Se bloquearon todas las cuentas de usuario con el privilegio Administer User Accounts (Administración de cuentas de usuario.)
- Una configuración incorrecta impide que iLO 2 aparezca en la red y la RBSU se ha desactivado.
- Es necesario guardar el bloque de inicio en la memoria flash.

Las ramificaciones de la configuración del conmutador de anulación de la seguridad incluyen:

- Todas las comprobaciones de autorización de la seguridad están desactivadas mientras el conmutador esté configurado.
- La utilidad RBSU de iLO 2 se ejecuta si se reinicia el servidor host.

- iLO 2 no está desactivado y puede mostrarse en la red tal como se ha configurado.
- Si se desactiva iLO 2 mientras el conmutador de anulación de la seguridad está activado, no se cerrará la sesión del usuario y se completará el proceso de desactivación hasta que el servidor se apague y se vuelva a encender.
- El bloque de inicio se expone para ser programado.

En las páginas del explorador de iLO 2 aparece un mensaje de advertencia que indica que el conmutador de anulación de la seguridad de iLO 2 se encuentra en uso. Mediante una entrada en el registro de iLO 2 se indica el uso del Conmutador de anulación de la seguridad. También puede enviarse un aviso SNMP cuando se configura o se elimina el Conmutador de anulación de la seguridad.

Al establecer el conmutador de anulación de la seguridad puede guardarse en la memoria flash el bloque de inicio de iLO 2. HP no considera la actualización del bloque de inicio de iLO 2 por parte de los clientes. En caso de necesitar actualizar un bloque de inicio de iLO 2, se necesitará la presencia física en el servidor para volver a programar el bloque de inicio y reiniciar iLO 2. El bloque de inicio quedará expuesto hasta que se reinicie iLO 2. Para obtener la máxima seguridad, HP recomienda desconectar iLO 2 de la red hasta que finalice el reinicio. El conmutador de anulación de la seguridad de iLO 2 se encuentra dentro del servidor y su acceso se realiza abriendo el receptáculo del servidor.

Para configurar el Conmutador de anulación de la seguridad de iLO 2:

1. Apague el servidor.
2. Configure el conmutador.
3. Encienda el servidor.

Invierta el procedimiento para eliminar el conmutador de anulación de la seguridad de iLO 2.

En función del servidor, el Conmutador de anulación de la seguridad de iLO 2 puede ser un simple puente o una posición específica del conmutador en un panel de interruptor DIP. Para acceder y localizar el Conmutador de anulación de la seguridad de iLO 2, consulte la documentación del servidor. El Conmutador de anulación de la seguridad de iLO 2 también se puede encontrar mediante los diagramas del panel de acceso del servidor.

Compatibilidad del módulo de plataforma segura

TPM es una función de seguridad del sistema basada en hardware. Se trata de un chip de ordenador que almacena de manera segura elementos utilizados para autenticar la plataforma. Entre estos elementos pueden incluirse contraseñas, certificados o claves de cifrado. También es posible utilizar un TPM para almacenar mediciones de plataforma para ayudar a garantizar que la plataforma es de confianza. iLO 2 ofrece compatibilidad para el módulo mezzanine TPM en servidores de la serie ProLiant 100 y ProLiant 300/500.

En un sistema compatible, iLO 2 decodifica el registro de TPM y cambia el estado de la configuración a iLO 2, CLP y a la interfaz XML. En la página System Status (Estado del sistema) se muestra el estado de la configuración de TPM. Si el sistema host o la ROM del sistema no admite TPM, el estado de TPM

no se visualizará en la página Status Summary (Resumen de estado.) En la página Status Summary (Resumen de estado) se muestra la siguiente información de estado de TPM:

- Not Present (No presente): no se encuentra instalado ningún módulo TPM.
- Present (Presente): aparece en las siguientes situaciones:
  - Cuando se encuentra instalado un módulo TPM pero se encuentra desactivado.
  - Cuando se encuentra instalado y activado un módulo TPM.
  - Cuando se encuentra instalado y activado un módulo TPM y la medición de la ROM de expansión se encuentra activada. Si la medición de la ROM de expansión se encuentra activada, la página Update iLO 2 Firmware (Actualizar el firmware de iLO 2) mostrará un mensaje de advertencia legal cuando haga clic en **Send firmware image (Enviar imagen de firmware)**.

Acceso y cuentas de usuario

iLO 2 admite la configuración de hasta 12 cuentas de usuario local. Cada una de estas cuentas puede administrarse mediante las siguientes funciones:

- Privilegios (Privilegios en la página 43)
- Seguridad de inicio de sesión (Seguridad de inicio de sesión en la página 43)

iLO 2 puede configurarse para utilizar un directorio que autentique y autorice a sus usuarios. Esta configuración permite un número prácticamente ilimitado de usuarios y aumenta el número de dispositivos de Lights-Out de una empresa. Además, el directorio proporciona un punto central de gestión de usuarios y dispositivos Lights-Out, e impone una directiva de seguridad más estricta. iLO 2 permite utilizar usuarios locales, usuarios de directorios o ambos.

Existen dos opciones de configuración disponibles: mediante un directorio que se ha extendido con el esquema de HP (Configuración de la integración de directorios con esquema de HP en la página 158) o mediante el esquema de directorio predeterminado (esquema libre (Configuración de la integración del directorio de esquema libre en la página 154)).

Privilegios

iLO 2 permite al administrador controlar el acceso de cuenta de usuario a las funciones de iLO 2 mediante privilegios. Cuando un usuario intenta utilizar una función, el sistema iLO 2 comprueba si el usuario dispone del privilegio antes de concederle permiso para realizar la función.

Cada característica disponible mediante iLO 2 se puede controlar con privilegios, incluidos Administer User Accounts (Administración de cuentas de usuario), Remote Console Access (Acceso a la consola remota), Virtual Power and Reset (Alimentación y Reinicio virtuales), Virtual Media (Soportes virtuales) y Configure iLO 2 Settings (Configurar valores de iLO 2.) Los privilegios de cada usuario pueden configurarse en la página User Administration (Administración de usuarios) de la ficha Administration (Administración.)

Seguridad de inicio de sesión

iLO 2 proporciona varias funciones de seguridad de inicio de sesión. Tras un primer intento fallido de inicio de sesión, iLO 2 impone un retraso de cinco segundos. Tras un segundo intento fallido de inicio de sesión, iLO 2 impone un retraso de 10 segundos. Tras el tercer intento fallido, iLO 2 impone un retraso de 60 segundos. A todos los siguientes intentos fallidos se aplican estos valores. Durante cada retraso aparecerá una página de información. Esta situación continuará hasta que se produzca un inicio de sesión válido. Esta función contribuye a la defensa de posibles ataques contra el puerto de inicio de sesión del explorador.

iLO 2 guarda una entrada de registro detallado de los intentos de inicio de sesión fallidos, lo que impone un retraso de 60 segundos.

Administración de la clave SSH

iLO 2 permite autorizar hasta cuatro claves SSH a la vez desde la ficha SSH Key (Clave SSH.) La ficha SSH Key (Clave SSH) también muestra el propietario de cada calve SSH autorizada (si se ha autorizado alguna clave.) Un usuario puede tener varias claves.

Para añadir una clave autorizada a iLO 2, debe enviarse a iLO 2 la ruta de la clave pública. El archivo de claves debe contener el nombre de usuario detrás de la clave, ya que iLO 2 asocia cada una de las claves con la cuenta de usuario local. Si la cuenta local no existe o se elimina, la clave no es válida (la clave no se muestra si la cuenta local no existe.)

Como alternativa, puede autorizar claves SSH para un servidor HP SIM ejecutando la herramienta mxagentconfig desde el servidor HP SIM. Deberá especificar la dirección y las credenciales de usuario de iLO 2. Consulte la documentación de HP SIM para obtener más información.

Para autorizar una clave nueva:

1. En la interfaz de iLO 2, haga clic en **Administration (Administración)>Security (Seguridad) >SSH Key (Clave SSH)**.
2. Haga clic en **Browse (Examinar)**, y busque el archivo de claves.
3. Haga clic en **Authorize Key (Autorizar clave)**.

Puede ver o eliminar cualquier clave previamente autorizada seleccionando la clave y haciendo clic en **View Selected Key (Ver clave seleccionada)** o en **Delete Selected Key (Eliminar clave seleccionada)**. Los botones View Selected Key (Ver clave seleccionada) y Delete Selected Key (Eliminar clave seleccionada) sólo aparecen si hay claves SSH instaladas.

Administración del certificado SSL

iLO 2 permite crear solicitudes de certificado, importar certificados y ver la información de administración asociada a un certificado almacenado. La CA (certificate authority, entidad emisora de certificados) codifica la información acerca del certificado en el certificado e iLO 2 la extrae.

De manera predeterminada, iLO 2 crea un certificado con firma automática para las conexiones SSL. Este certificado activa iLO 2 sin necesidad de realizar ningún paso de configuración adicional. Las funciones de seguridad de iLO 2 se pueden mejorar mediante la importación de un certificado de confianza. Para obtener más información acerca de los certificados y de los servicios de Certificate Server, consulte las secciones “Introducción a los servicios de Certificate Server" (Introducción a los servicios de Certificate Server en la página 154) e “Instalación de los servicios de Certificate Server" (Instalación de los servicios de Certificate Server en la página 155.)

Para acceder a la información del certificado, haga clic en **Administration (Administración)>Security (Seguridad)>SSL Certificate (Certificado SSL)**. La ficha SSL Certificate (Certificado SSL) muestra la siguiente información:

- El campo Issued To (Emitido a) muestra la entidad a la que se emitió el certificado.
- El campo Issued By (Emitido por) muestra la CA que emitió el certificado.
- En el campo Valid From (Válido desde) se muestra la primera fecha en que el certificado es válido.
- En el campo Valid Until (Válido hasta) se muestra la fecha en la que caducará el certificado.
- El campo Serial Number (Número de serie) muestra el número de serie asignado al certificado por la CA.

Las siguientes opciones están disponibles en la ficha SSL Certificate (Certificado SSL):

- Create Certificate Request (Crear solicitud de certificado): utilice este botón para crear una solicitud de certificado. Al hacer clic en este botón, se crea una solicitud de certificado (en PKCS formato #10) que se puede enviar a una CA. Esta solicitud de certificado está codificada en Base64. Una CA procesa esta solicitud y devuelve una respuesta (certificado X.509) que se puede importar a iLO 2.

  La CR (Certificate Request, Solicitud de certificado) contienen un par de claves pública/privada que valida la comunicación entre el explorador cliente e iLO 2. La CR generada se conserva en la memoria hasta que se genera una CR nueva, iLO 2 se reinicia o se importa un certificado a través del proceso de generación. Es posible generar la solicitud de certificado y copiarla en el portapapeles del cliente, salir de la página Web de iLO 2 para recuperar el certificado y, a continuación, volver para importar el certificado.

  Cuando envíe la solicitud a la CA, asegúrese de realizar las siguientes tareas:

  a. Utiliza el nombre de iLO 2 tal como aparece en la pantalla System Status (Estado del sistema) como dirección URL del servidor.

  b. Solicitar la generación del certificado en formato RAW.

  c. Incluir las líneas de certificado `Begin` y `End`.

  Cada vez que se hace clic en **Create Certificate Request (Crear solicitud de certificado)**, se genera una nueva solicitud de certificado, aunque el nombre de iLO 2 sea el mismo.

- Import Certificate (Importar certificado): utilice este botón cuando regrese a la página Certificate Administration (Administración del certificado) con un certificado que desee importar. Haga clic en **Import Certificate (Importar certificado)** para ir directamente a la pantalla Certificate Import (Importación del certificado) sin generar una solicitud de certificado nueva. Un certificado sólo funciona con las claves generadas para la solicitud de certificado original desde la que fue generado. Si se ha reiniciado iLO 2 o se ha generado otra solicitud de certificado desde que se envió la solicitud original a la CA, debe generarse una solicitud de certificado nueva y enviarse a la CA.

Puede crear una solicitud de certificado o importar un certificado existente utilizando los comandos XML de RIBCL. Estos comandos permiten crear secuencias de comandos y automatizar la distribución de certificados a servidores iLO 2 en lugar de distribuirlos manualmente a través de la interfaz del explorador. Para obtener más información, consulte la *Guía de recursos de líneas y secuencias de comandos del procesador de gestión HP Integrated Lights-Out*.

Autenticación basada en dos factores

El acceso a iLO 2 requiere la autenticación del usuario. Esta versión del firmware proporciona un esquema de autenticación mejorado para iLO 2 mediante dos factores de autenticación: una contraseña o un PIN, y una clave privada de un certificado digital. Para utilizar la autenticación basada en dos factores el usuario debe confirmar su identidad proporcionando los dos factores. Los certificados digitales y las claves privadas se pueden almacenar en el lugar deseado, por ejemplo, en una tarjeta inteligente, identificador USB o unidad de disco duro.

La ficha Two-Factor Authentication (Autenticación basada en dos factores) permite configurar los valores de seguridad y revisar, importar o eliminar un certificado CA de confianza. El valor Two-Factor Authentication Enforcement (Aplicación de la autenticación basada en dos factores) controla si el usuario utiliza la autenticación basada en dos factores al iniciar la sesión. Para exigir la autenticación basada en dos factores, haga clic en **Enabled (Activado)**. Para desactivar el requisito de la autenticación basada en dos factores y permitir iniciar sesión con sólo el nombre de usuario y la contraseña, haga clic en **Disabled (Desactivado)**. No es posible cambiar el valor a Enabled (Activado)

si no se configura un certificado CA de confianza. Para proporcionar la seguridad necesaria, se realizan los siguientes cambios de configuración cuando se activa la autenticación basada en dos factores:

- Telnet Access (Acceso Telnet): Disabled (Desactivado)
- Secure Shell (SSH) Access (Acceso de Shell de seguridad): Disabled (Desactivado)
- Serial Command Line Interface Status (Estado de interfaz de línea de comando de serie): Disabled (Desactivado)

Si se requiere acceso telnet, SSH o CLI de serie, vuelva a activar estas configuraciones una vez la autenticación basada en dos factores esté activada. De todas formas, para acceder a iLO 2 con telnet, SSH o CLI de serie, sólo se requiere un único factor, puesto que estos métodos de acceso no proporcionan un medio de autenticación de dos factores.

Cuando se activa la autenticación basada en dos factores, se desactiva el acceso con la utilidad CPQLOCFG, ya que CPQLOCFG no cumple con todos los requisitos de autenticación. Sin embargo, la utilidad HPONCFG funciona porque se necesitan privilegios de administrador en el sistema host para ejecutar la utilidad.

Se necesita un certificado CA de confianza para que la autenticación basada en dos factores funcione. No es posible cambiar el valor Two-Factor Authentication Enforcement (Aplicación de la autenticación basada en dos factores) a Enabled (Activado) si no se ha configurado un certificado CA de confianza. Asimismo, es necesario asignar un certificado de cliente a una cuenta de usuario local si se utilizan este tipo de cuentas. En el caso de que iLO 2 utilice una autenticación de directorio, entonces es opcional asignar un certificado de cliente a las cuentas de usuario locales.

Para cambiar la configuración de seguridad de autenticación basada en dos factores en iLO2:

1. Inicie una sesión en iLO 2 con una cuenta con el privilegio Configure iLO 2 Settings (Configurar valores de iLO 2.)
2. Haga clic en **Administration (Administración)>Security (Seguridad)>Two-Factor Authentication (Autenticación basada en dos factores)**.
3. Cambie la configuración introduciendo los valores que seleccione en estos campos.
4. Haga clic en **Apply (Aplicar)** para guardar los cambios.

La configuración de Certificate Revocation Checking (Comprobación de la revocación del certificado) controla si iLO 2 utiliza los puntos de distribución de la CRL de certificado para descargar las CRL más recientes y verificar la revocación del certificado de cliente. Si el certificado del cliente se encuentra en la CRL o si no es posible descargar la CRL, el acceso se denegará. El punto de distribución de la CRL debe estar disponible y ser accesible para iLO 2 cuando el valor de Certificate Revocation Checking (Comprobación de la revocación del certificado) es **Yes (Sí)**.

La configuración de Certificate Owner Field (Campo de propietario de certificado) especifica qué atributo del certificado de cliente se debe usar para autenticar el directorio. Utilice únicamente el valor Certificate Owner Field (Campo de propietario de certificado) si la autenticación del directorio está activada. La configuración de Certificate Owner Field (Campo de propietario de certificado) depende de la versión compatible de directorio que se utilice, de la configuración del directorio y de la política de emisión de certificados de la organización. Si se ha especificado SAN, iLO 2 extrae el User Principle Name (Nombre de principio del usuario) del atributo Subject Alternative Name (Nombre alternativo de asunto) y lo utiliza al autenticarse con el directorio (por ejemplo, nombreusuario@dominio.extensión.) Por ejemplo, si el nombre de asunto es `/DC=com/DC=domain/OU=organization/CN=user`, iLO 2 obtendrá `CN=user,OU=organization,DC=domain,DC=com`.

Configuración de la autenticación basada en dos factores por primera vez

Cuando configure la autenticación basada en dos factores por primera vez, podrá utilizar cuentas de usuario locales o de directorio. Si desea obtener más información acerca de la configuración de autenticación basada en dos factores, consulte la sección "Autenticación basada en dos factores" (Autenticación basada en dos factores en la página 45.)

Configuración de cuentas de usuario locales

1. Obtenga el certificado público de la CA que emite certificados de usuario o tarjetas inteligentes en su organización.
2. Exporte el certificado en formato codificado en Base64 a un archivo del escritorio (por ejemplo, CAcert.txt.)
3. Obtenga el certificado público del usuario que necesita acceso a iLO 2.
4. Exporte el certificado en formato codificado en Base64 a un archivo del escritorio (por ejemplo, Usercert.txt.)
5. Abra el archivo CAcert.txt en el bloc de notas, seleccione todo el texto y pulse las teclas **Ctrl+C** para copiarlo.
6. Inicie sesión en iLO 2 y desplácese a la página Two-Factor Authentication Settings (Configuración de la autenticación basada en dos factores.)
7. Haga clic en **Import Trusted CA Certificate (Importar el certificado CA de confianza)**. Aparece la página Import Root CA Certificate (Importar certificado raíz de CA.)
8. Haga clic en la zona de texto en blanco para que el cursor se sitúe en ella y, a continuación, pulse las teclas **Ctrl+V** para pegar el contenido del portapapeles.
9. Haga clic en **Import Root CA Certificate (Importar certificado raíz de CA)**. Volverá a aparecer la página de los valores de configuración de la autenticación basada en dos factores con información incluida en Trusted CA Certificate Information (información acerca del certificado CA aprobado).
10. Abra el archivo del certificado de usuario del escritorio con el bloc de notas, seleccione todo el texto y pulse las teclas **Ctrl+C** para copiarlo en el portapapeles.
11. Vaya a la página User Administration (Administración de usuarios) en iLO 2 y seleccione el usuario para el que ha obtenido un certificado público, o cree un nuevo usuario.
12. Haga clic en **View/Modify (Ver/Modificar)**.
13. Haga clic en **Add a certificate (Añadir un certificado)**.
14. Haga clic en la zona de texto en blanco para que el cursor se sitúe en ella y, a continuación, pulse las teclas **CTRL+V** para pegar el contenido del portapapeles.
15. Haga clic en **Add user Certificate (Añadir certificado de usuario)**. Volverá a aparecer la página Modify User (Modificar usuario) con un número de 40 dígitos en el campo Thumbprint (Huella digital.) Podrá comparar el número de la huella digital que aparece para el certificado con Microsoft® Certificate Viewer.
16. Desplácese a la página Two-Factor Authentication Settings (Configuración de la autenticación basada en dos factores.)
17. Seleccione **Enabled (Activado)** en la opción Two-Factor Authentication (Autenticación basada en dos factores.)
18. Seleccione **Disabled (Desactivado)** en la opción Certificate Revocation Checking (Comprobación de la revocación del certificado.) Este es el valor predeterminado.

19. Haga clic en **Apply (Aplicar)**. iLO 2 se reinicia. Cuando iLO 2 trate de ir de nuevo a la página de inicio, el explorador abrirá la página Client Authentication (Autenticación de cliente) con una lista de certificados disponibles para el sistema.

    En el caso de que el certificado de usuario no esté registrado en el equipo cliente, no lo verá en la lista. El certificado de usuario se debe registrar en el equipo de cliente antes de usarlo. Si no hay certificados de cliente en el sistema cliente, es posible que no aparezca la página Client Authentication (autenticación de cliente) y, en su lugar, se muestre la página con el error “Page cannot be displayed” (No se puede mostrar la página.) Para solucionarlo, el certificado de cliente debe estar registrado en el equipo cliente. Para obtener más información acerca de la exportación y el registro de certificados de cliente, consulte la documentación de su tarjeta inteligente o póngase en contacto con la entidad emisora de certificados.

20. Seleccione el certificado que se añadió al usuario en iLO 2. Haga clic en **OK (Aceptar)**.

21. Si el sistema se lo pide, inserte la tarjeta inteligente o introduzca su PIN o contraseña.

Cuando haya concluido el proceso de autenticación, tendrá acceso a iLO 2.

Configuración de cuentas de usuario de directorio

1. Obtenga el certificado público de la CA que emite certificados de usuario o tarjetas inteligentes en su organización.

2. Exporte el certificado en formato codificado en Base64 a un archivo del escritorio (por ejemplo, CAcert.txt.)

3. Abra el archivo en el Bloc de notas, seleccione todo el texto y pulse las teclas **Ctrl+C** para copiar el contenido en el portapapeles.

4. Inicie sesión en iLO 2 y desplácese a la página **Two-Factor Authentication Settings (Configuración de la autenticación basada en dos factores)**.

5. Haga clic en **Import Trusted CA Certificate (Importar el certificado CA de confianza)**. Aparecerá otra página.

6. Haga clic en la zona de texto en blanco para que el cursor se sitúe en ella y, a continuación, pulse las teclas **Ctrl+V** para pegar el contenido del portapapeles.

7. Haga clic en **Import Root CA Certificate (Importar certificado raíz de CA)**. Volverá a aparecer la página de los valores de configuración de la autenticación basada en dos factores con información incluida en Trusted CA Certificate Information (información acerca del certificado CA aprobado.)

8. Cambie Enforce Two-Factor Authentication (Exigir la autenticación basada en dos factores) a **Yes (Sí)**.

9. Cambie la opción Certificate Revocation Checking (Comprobación de la revocación del certificado) a **No (opción predeterminada)**.

10. Cambie el valor de Certificate Owner Field (Campo de propietario de certificado) a **SAN**. Si desea obtener más información, consulte la sección "Autenticación basada en dos factores" (Autenticación basada en dos factores en la página 45.)

11. Haga clic en **Apply (Aplicar)**. iLO 2 se reinicia. Cuando iLO 2 trate de ir de nuevo a la página de inicio, el explorador abrirá la página Client Authentication (Autenticación de cliente) con una lista de certificados disponibles para el sistema.

12. Seleccione el certificado que se añadió al usuario en iLO 2. Haga clic en **OK (Aceptar)**.

13. Si el sistema se lo pide, inserte la tarjeta inteligente o introduzca su PIN o contraseña. La página de inicio se debería mostrar con la dirección de correo electrónico del usuario en el campo Directory User (Usuario de directorio.) No es posible cambiar el campo Directory User (usuario de directorio.)
14. Introduzca la contraseña para el usuario de directorio. Haga clic en **Login (Iniciar sesión)**.

Cuando haya concluido el proceso de autenticación, tendrá acceso a iLO 2. Consulte la sección “Directory settings (Configuración de directorio) (Configuración de directorio en la página 52)” para obtener más información acerca de la configuración de usuarios de directorio y privilegios.

Configuración de un usuario para la autenticación basada en dos factores

Para autenticar un usuario con una cuenta de iLO 2 local, un certificado debe estar asociado al nombre de usuario local del usuario. En la página de Administration (administración)>Modify User (modificar usuario), si se ha asignado un certificado al usuario, aparecerá una huella digital (un algoritmo hash SHA1 del certificado) con un botón que permite eliminar dicho certificado. En caso de que no se haya asignado un certificado al usuario, se mostrará `Thumbprint: A certificate has NOT been mapped to this user (Huella digital: no se ha asignado un certificado a este usuario)` con un botón que inicia el proceso de importación del certificado.

Para configurar un usuario para la autenticación basada en dos factores y añadir un certificado de usuario:

1. Inicie una sesión en iLO 2 con una cuenta con el privilegio Configure iLO 2 Settings (Configurar valores de iLO 2.)
2. Haga clic en **Administration (Administración)>User Administration (Administración de usuarios)**. Seleccione un usuario.
3. Haga clic en **View/Modify (Ver/Modificar)**.
4. En la sección User Certificate Information (Información acerca del certificado de usuario), haga clic en **Add a certificate (Añadir un certificado)**.
5. En la página Map User Certificate (Asignar un certificado de usuario), pegue el certificado de usuario en el cuadro de texto y haga clic en **Import Certificate (Importar certificado)**. Para obtener más información acerca de la creación, copia o pegado de la información sobre certificados, consulte la sección "Configuración de la autenticación basada en dos factores por primera vez" (Configuración de la autenticación basada en dos factores por primera vez en la página 47.)

Inicio de sesión con la autenticación basada en dos factores

Cuando se establece la conexión con la placa iLO 2 y se solicita la autenticación basada en dos factores, en la página Client Authentication (Autenticación de cliente) se le pedirá que seleccione el certificado que desea utilizar. La página Client Authentication (autenticación de cliente) muestra todos los certificados disponibles para autenticar a un cliente. Seleccione el certificado. El certificado puede ser un certificado asignado a un usuario local de iLO 2 o un certificado de usuario específico emitido para la autenticación en el dominio.

Tras la selección, si el certificado está protegido con una contraseña o está almacenado en una tarjeta inteligente, aparecerá otra página en la que se le solicitará que introduzca el PIN o la contraseña asociada con el certificado seleccionado.

El certificado es examinado por iLO 2 para garantizar que fue emitido por una CA de confianza comprobando la firma con el certificado de CA configurado en iLO 2. iLO 2 verifica si el certificado ha sido revocado y si dirige a un usuario de la base de datos de usuarios locales de iLO 2. Si todas estas pruebas son satisfactorias, entonces aparecerá la interfaz de usuario normal de iLO 2.

Si la autenticación de las credenciales no se realiza correctamente, aparecerá la página de Login Failed (error en el inicio de sesión.) Si el inicio de sesión no se realiza correctamente, se le proporcionarán instrucciones para cerrar el explorador, abrir una página nueva del explorador y volver a intentar la conexión. En el caso de que se active la autenticación de directorio y falle la autenticación de usuario local, iLO 2 mostrará una página de inicio de sesión con el campo de nombre de usuario de directorio con el User Principal Name (Nombre de principio del usuario) del certificado o el Distinguished Name (Nombre distinguido) (derivado del asunto del certificado.) ILO 2 solicita la contraseña para la cuenta. Se autenticará después de proporcionar dicha contraseña.

Uso de la autenticación basada en dos factores junto con la autenticación de directorio

En algunos casos, la configuración de la autenticación basada en dos factores junto con la autenticación de directorio es complicada. iLO 2 puede utilizar el esquema extendido de HP o el esquema del directorio predeterminado para integrar los servicios de directorio. Para garantizar la seguridad, cuando se exige la autenticación basada en dos factores, iLO 2 utiliza un atributo del certificado de cliente como nombre de inicio de sesión del usuario de directorio. El atributo de certificado de cliente que utiliza iLO 2 viene determinado por la configuración de los valores de Certificate Owner Field (Campo de propietario del certificado) en la página Two-Factor Authentication Settings (Configuración de la

autenticación basada dos factores.) Si el valor de Certificate Owner Field (Campo de propietario del certificado) es SAN, iLO 2 obtiene el nombre de inicio de sesión del usuario de directorio a partir del atributo UPN del SAN. Si el valor es Subject (Asunto), iLO 2 obtiene el nombre completo de usuario de directorio a partir del asunto del certificado.

La elección del valor de Certificate Owner Field (Campo de propietario del certificado) depende del método de integración de directorios que se utilice, de la arquitectura de directorios y de la información que se incluya en los certificados de usuario emitidos. Los siguientes ejemplos suponen que se dispone de los permisos necesarios.

Autenticación mediante Default Directory Schema (Esquema de directorio predeterminado), parte 1: El nombre completo de un usuario en un directorio es CN=John Doe,OU=IT,DC=MyCompany,DC=com, y los atributos del certificado de John Doe son los siguientes:

- Asunto: DC=com/DC=MyCompany/OU=IT/CN=John Doe
- SAN/UPN: john.doe@MyCompany.com

La autenticación en iLO 2 con el nombre de usuario: john.doe@MyCompany.com y la contraseña funcionará si **no** se exige la autenticación basada en dos factores. Tras activar la autenticación basada en dos factores, si se ha seleccionado SAN en la página Two-Factor Authentication Settings (Configuración de la autenticación basada en dos factores), la página de inicio de sesión rellenará automáticamente el campo Directory User (Usuario de directorio) con john.doe@MyCompany.com. Se puede introducir la contraseña, pero el usuario **no** será autenticado. El usuario no es autenticado porque john.doe@MyCompany.com, que se obtuvo del certificado, no es el nombre completo del usuario en el directorio. En este caso, deberá seleccionar **Subject (Asunto)** en la página Two-Factor Authentication Settings (Configuración de la autenticación basada en dos factores.) Seguidamente, el campo Directory User (Usuario de directorio) en la página de inicio de sesión se llenará con CN=John Doe,OU=IT,DC=MyCompany,DC=com, que es el nombre completo real del usuario. Si se introduce la contraseña correcta, el usuario se autenticará.

Autenticación mediante Default Directory Schema (Esquema de directorio predeterminado), parte 2: El nombre completo de un usuario en un directorio es CN=john.doe@MyCompany.com,OU=IT,DC=MyCompany,DC=com, y los atributos del certificado de John Doe son los siguientes:

- Asunto: DC=com/DC=MyCompany/OU=Employees/CN=John Doe/ E=john.doe@MyCompany.com
- SAN/UPN: john.doe@MyCompany.com
- La búsqueda de contexto en la página de Directory Settings (Valores de configuración de directorio) está ajustada a: OU=IT,DC=MyCompany,DC=com

En este ejemplo, si se ha seleccionado SAN en la página Two-Factor Authentication Settings (Configuración de la autenticación basada en dos factores), el campo Directory User (Usuario de directorio) de la página de inicio de sesión se llenará con john.doe@MyCompany.com. Una vez que se haya introducido la contraseña correcta, el usuario se autenticará. El usuario será autenticado incluso en el caso de que john.doe@MyCompany.com no sea el nombre completo de usuario. El usuario será autenticado porque iLO 2 trata de autenticar mediante los campos de búsqueda de contexto (CN=john.doe@MyCompany.com, OU=IT, DC=MyCompany, DC=com) configurados en la página Directory Settings (Valores de directorio.) Puesto que se trata del nombre completo correcto del usuario, iLO 2 consigue encontrar el usuario en el directorio.

NOTA: Al seleccionar Subject (Asunto) en la página Two-Factor Authentication Settings (Configuración de la autenticación basada en dos factores) la autenticación es fallida, puesto que el asunto del certificado no es el nombre completo del usuario en el directorio.

Si se autentica utilizando el método del esquema extendido de HP, HP recomienda seleccionar la opción SAN en la página Two-Factor Authentication Settings (Configuración de la autenticación basada en dos factores.)

Configuración de directorio

iLO 2 se conecta a Microsoft® Active Directory, Novell e-Directory y otros servicios de directorio compatibles con LDAP 3.0 para la autorización y autenticación de usuarios. Es posible configurar iLO 2 para autenticar y autorizar a los usuarios a través de la integración de directorios de esquema HP o a través de la integración de directorios sin esquema. iLO 2 únicamente establece la conexión a los servicios de directorio mediante conexiones protegidas por SSL con el puerto LDAP del servidor de directorios. El puerto LDAP seguro predeterminado es el puerto 636. La compatibilidad de los servicios de directorio es una función con licencia que se encuentra disponible mediante la adquisición de licencias opcionales. Si desea obtener más información, consulte "Concesión de licencias (Concesión de licencias en la página 21)". Si desea obtener información adicional acerca de los directorios, consulte "Servicios de directorio (Servicios de directorio en la página 150)".

Las cuentas de usuario almacenadas localmente, que se encuentran en la página Administration (Administración), pueden permanecer activas siempre y cuando la compatibilidad del directorio de iLO 2 esté activada. Esta compatibilidad permite tanto los accesos de usuario basado en directorio como de usuario basado en directorio y local. Por lo general, los administradores pueden eliminar las cuentas de usuario local (excepto si se trata de una cuenta de acceso de emergencia) tras la correcta configuración de iLO 2 para acceder al servicio de directorio. Asimismo, puede desactivar el acceso a estas cuentas si la compatibilidad de directorios está activada.

Configuración de los valores de directorio

iLO 2 permite a los administradores centralizar la administración de cuentas de usuario a través de los servicios de directorio. Debe tener el privilegio Configure iLO 2 Settings (Configurar los ajustes de iLO 2) para configurar y probar los servicios de directorio de iLO 2. Para acceder a Directory Settings (Valores de directorio), haga clic en **Administration (Administración)>Security (Seguridad)>Directory (Directorio)**.

La configuración del directorio de iLO 2 permite controlar el comportamiento relacionado con el directorio del directorio de iLO 2 en el que ha iniciado sesión. Esta configuración incluye:

- Disable Directory Authentication (Desactivar autenticación de directorio): permite activar o desactivar la compatibilidad de directorios en este directorio de iLO 2.
  - Si la autenticación de directorios está activada y correctamente configurada, los usuarios pueden iniciar sesión a través de las credenciales de directorio.
  - Si la autenticación de directorios está desactivada, las credenciales de usuario no se validan a través del directorio.
- Use HP Extended Schema (Utilizar esquema extendido de HP): permite seleccionar la autorización y autenticación de directorios a través de los objetos de directorio creados con el esquema de HP. Seleccione esta opción si el directorio se ha extendido con el esquema de HP y desea utilizarlo.
- Use Directory Default Schema (Utilizar el esquema de directorio predeterminado): permite seleccionar la autorización y la autenticación de directorios a través de las cuentas de usuario del directorio. Seleccione esta opción si el directorio no se ha extendido con el esquema de HP. Las cuentas de usuario y los miembros del grupo se utilizan para autenticar y autorizar usuarios. Tras introducir la información de red del directorio, haga clic en **Administer Groups (Administrar grupos)** y escriba uno o más privilegios y nombres completos de directorios válidos para conceder a los usuarios el acceso a iLO 2.
- Enable Local User Accounts (Activar cuentas de usuario local): permite limitar el acceso a los usuarios locales.
  - Si se activa la opción Local User Accounts (Cuentas de usuario local), un usuario podrá iniciar sesión a través de las credenciales de usuario almacenadas de forma local.
  - Si se desactiva la opción Local User Accounts (Cuentas de usuario local) , el acceso del usuario está restringido sólo a las credenciales de directorio válidas.

    Es posible acceder a través de Local User Accounts (Cuentas de usuario local) si la opción Directory Support (Soporte de directorios) está desactivada y/o se revoca la licencia de iLO 2 Select o iLO 2 Advanced. No es posible desactivar el acceso de los usuarios locales si se ha iniciado sesión a través de la cuenta de usuario local.

La configuración del servidor de directorio de iLO 2 permite identificar el puerto y la dirección del servidor de directorios. Esta configuración incluye:

- Directory Server Address (Dirección del servidor de directorios): permite especificar la dirección IP y el nombre DNS de red del servidor de directorios. Es posible especificar varios servidores si se separan por una coma (,) o por un espacio ( ). Si selecciona la opción Use Directory Default Schema (Utilizar el esquema de directorio predeterminado), escriba un nombre DNS en el campo Directory Server Address (Dirección del servidor de directorios) para permitir la autenticación con un Id. de usuario. Por ejemplo:

  ```
  directory.hp.com
  192.168.1.250, 192.168.1.251
  ```

- Directory Server LDAP Port (Puerto LDAP del servidor de directorios): permite especificar el número de puerto del servicio LDAP seguro en el servidor. El valor predeterminado de este puerto es 636. No obstante, es posible especificar un valor diferente si el servicio del directorio está configurado para utilizar un puerto diferente.
- iLO 2 Directory Properties (Propiedades del directorio de iLO 2): permite identificar el objeto LOM en el árbol de directorios. Esta información se utiliza para determinar los derechos de acceso del usuario. En este momento, es posible configurar iLO 2 con la contraseña en el objeto LOM; sin

embargo, esta información no se utilizará hasta que se proporcione la compatibilidad de configuración del directorio.

- LOM Object Distinguished Name (Nombre completo de objetos LOM): permite especificar dónde se enumera esta instancia LOM en el árbol de directorios. Por ejemplo: cn=iLO 2 Mail Server,ou=Management Devices,o=hp

  Los contextos de búsqueda del usuario no se aplican al LOM Object Distinguished Name (Nombre completo de objetos LOM cuando se accede al servidor del directorio.

- LOM Object Password (Contraseña del objeto LOM): permite especificar la contraseña del objeto iLO 2 que iLO 2 utiliza para comprobar las actualizaciones del directorio (LOM Object Distinguished Name, Nombre completo de objetos LOM.)

- Confirm Password (Confirmar contraseña): permite verificar la contraseña del objeto LOM. Si modifica la contraseña del objeto LOM, introduzca la nueva contraseña en este campo.

- User Login Search Contexts (Contextos de búsqueda de inicio de sesión de usuario) permite especificar los subcontextos del directorio común; de este modo, los usuarios no deben introducir el nombre completo al iniciar sesión.

  Es posible identificar todos los objetos enumerados en un directorio a través de sus nombres únicos completos. Sin embargo, es posible que los usuarios no conozcan sus nombres completos, ya que estos pueden ser largos, o es posible que tengan cuentas en distintos contextos de directorio. iLO 2 intenta ponerse en contacto con el servicio del directorio a través del nombre completo y, a continuación, aplica los contextos de búsqueda de forma ordenada hasta que encuentra la coincidencia.

  Directory User Contexts (Contextos de usuario del directorio) especifican los contextos del nombre de usuario que se aplican al nombre de inicio de sesión.

  Ejemplo 1:

  En vez de iniciar sesión como cn=user,ou=engineering,o=hp, un contexto de búsqueda de `ou=engineering,o=hp` permite el inicio de sesión como `user`

  Ejemplo 2:

  Si un sistema está gestionado por la gestión de información, servicios y formación, los contextos como:

  ```
  Directory User Context 1:ou=IM,o=hp
  Directory User Context 2:ou=Services,o=hp
  Directory User Context 3:ou=Training,o=hp
  ```

  Permita a los usuarios de cualquiera de estas organizaciones que inicien sesión simplemente utilizando sus nombres comunes. Si existe un usuario tanto en la unidad organizativa IM y la unidad organizativa de formación, el inicio de sesión se intenta en primer lugar como cn=usuario,ou=IM,o=hp.

  Ejemplo 3 (sólo Active Directory):

  Microsoft Active Directory permite un formato de credencial de usuario alternativo. Los contextos de búsqueda en este formato no pueden probarse excepto mediante un intento de inicio de sesión satisfactorio. Un usuario puede iniciar sesión como:

  ```
  user@domain.hp.com
  in which case a search context of
  @domain.hp.com
  ```

```
allows the user to login as
user
```

Para probar la comunicación entre el servidor de directorio e iLO 2, haga clic en **Test Settings (Probar configuración)**. Si desea obtener más información, consulte la sección "Pruebas de directorio (Pruebas de directorio en la página 55)".

Pruebas de directorio

Para validar los actuales valores de configuración de directorio para iLO 2, haga clic en **Test Settings (Probar configuración)** de la página Directory Settings (Configuración de directorio.) Aparece la página Directory Tests (Pruebas de directorio.)

La página de pruebas muestra los resultados de una serie de pruebas simples diseñadas para validar los valores de configuración de directorio actuales. Asimismo, incluye un registro de pruebas que muestra los resultados de las pruebas así como cualquier problema que se haya detectado. Una vez configurados correctamente los valores del directorio, no necesitará volver a ejecutar estas comprobaciones. La pantalla Directory Tests (Pruebas de directorio) no requiere que haya iniciado una sesión como usuario de directorio.

Para comprobar la configuración de directorio:

1. Escriba el nombre completo y la contraseña de un administrador de directorios. Una buena elección serían las mismas credenciales utilizadas al crear los objetos iLO 2 en el directorio. iLO 2 no almacena estas credenciales; se utilizan para comprobar los contextos de búsqueda de usuarios y objetos de iLO 2.
2. Escriba un nombre de usuario y una contraseña de prueba. Normalmente, esta cuenta se utiliza para acceder a la placa iLO 2 que se está probando. Puede ser la misma cuenta que la del administrador del directorio. No obstante, las pruebas no pueden verificar la autenticación del usuario con una cuenta de superusuario. iLO 2 no almacena estas credenciales.
3. Haga clic en **Start Test (Iniciar prueba)**. Varias pruebas comienzan a realizarse en segundo plano, empezando con un ping de red del usuario de directorio mediante el establecimiento de una conexión SSL al servidor y evaluando los privilegios tal como se evaluarían durante un inicio de sesión normal.

Mientras se actualizan las pruebas, la página se actualiza periódicamente. En cualquier momento durante la ejecución de las pruebas, puede detenerlas o actualizar manualmente la página. Consulte el enlace de ayuda de la página para obtener información de las pruebas y de las acciones si se producen problemas.

Cifrado

iLO 2 proporciona seguridad mejorada para la gestión remota en entornos de TI distribuidos. Los datos de explorador Web están protegidos por el cifrado SSL. El cifrado SSL de los datos HTTP garantiza la seguridad de los datos mientras se transmiten a través de la red. iLO 2 proporciona soporte a dos de las intensidades de cifrado más fuertes disponibles: Estándar de cifrado avanzado (AES, Advanced Encryption Standard) y Estándar de cifrado triple de datos (3DES, Triple Data Encryption Standard.) iLO 2 es compatible con los siguientes sistemas de cifrado:

- AES de 256 bits con RSA, DHE y un SHA1 MAC
- AES de 256 bits con RSA y un SHA1 MAC
- AES de 128 bits con RSA, DHE y un SHA1 MAC
- AES de 128 bits con RSA y un SHA1 MAC

- 168-bit Triple DES with RSA and a SHA1 MAC
- Triple DES de 168 bits con RSA, DHE y un SHA1 MAC

iLO 2 también proporciona un cifrado mejorado a través del puerto SSH para las transacciones CLP seguras. iLO 2 es compatible con las intensidades de cifrado AES128-CBC y 3DES-CBC a través del puerto SSH.

Si se activa, iLO 2 impone el uso de estos sistemas de cifrado mejorados (tanto AES como 3DES) a través de canales seguros, incluidas las transmisiones HTTP seguras a través del explorador, el puerto SSH y el puerto XML. Cuando se activa el cifrado de AES/3DES, es necesario utilizar una intensidad de cifrado igual o superior a AES/3DES para conectarse a iLO 2 a través de los canales seguros. Las comunicaciones y conexiones a través de canales menos seguros (por ejemplo, el puerto telnet) no se ven afectadas por la configuración de la aplicación de cifrado de AES/3DES.

De manera predeterminada, los datos de la consola remota utilizan un cifrado bidireccional RC4 de 128 bits. La utilidad CPQLOCFG utiliza un cifrado Triple DES de 168 bits con RSA y un SHA1 MAC para enviar de manera segura las secuencias de comandos RIBCL a iLO 2 a través de la red.

Configuración de cifrado

A través de la interfaz de iLO 2, CLP o RIBCL, puede ver y modificar la configuración de cifrado actual.

Para ver y modificar la configuración de cifrado actual a través de la interfaz de iLO 2:

1. Haga clic en **Administration (Administración)>Security (Seguridad)>Encryption (Cifrado)**.

   Aparecerá la página Encryption (Cifrado), donde se muestra la configuración de cifrado actual para iLO 2. Tanto el sistema de cifrado negociado actualmente como la configuración de la aplicación de cifrado se muestran en esta página.

   - Current Negotiated Cipher (Cifrado negociado actual) muestra el cifrado que se encuentra en uso en la sesión actual del explorador. Una vez que haya iniciado sesión en iLO 2 a través del explorador, éste e iLO 2 negocian la configuración del cifrado que se utilizará durante la sesión. La sección Current Negotiated Cipher (Cifrado negociado actual) de la página Encryption (Cifrado) muestra el cifrado negociado.

     Encryption Enforcement Settings (Configuración de la aplicación de cifrado) muestra los valores de configuración de cifrado actuales para iLO 2. Si la opción Enforce AES/3DES Encryption (Aplicar cifrado AES/3DES) está activada, iLO 2 puede aceptar conexiones únicamente a través del explorador y de la interfaz SSH que cumplen con la intensidad de cifrado mínima. Si se activa esta opción de configuración, se deberá utilizar una intensidad de cifrado de al menos AES o 3DES para establecer la conexión con iLO 2. La opción Enforce AES/3DES Encryption (Aplicar cifrado AES/3DES) se puede activar o desactivar.

2. Para guardar los cambios, haga clic en **Apply (Aplicar)**.

   Cuando cambie el ajuste de aplicación a Enable (Activar) y haga clic en Apply **(Aplicar)** y cierre todos los exploradores abiertos. Todos los exploradores que permanezcan abiertos continuarán utilizando un cifrado distinto a AES/3DES.

Para ver o modificar los ajustes de cifrado actuales a través de CLP o RIBCL, consulte la *Guía de recursos de líneas y secuencias de comandos del procesador de gestión HP Integrated Lights-Out*.

Conexión a iLO 2 a través del cifrado AES/3DES

Tras activar la configuración Enforce AES/3DES Encryption (Aplicar cifrado AES/3DES), iLO 2 solicita la conexión a través de canales seguros (explorador Web, SSH o puerto XML) usando una intensidad de cifrado de al menos AES o 3DES.

Para conectarse a iLO 2 a través de un explorador, este último debe estar configurado con una intensidad de cifrado de al menos AES o 3DES. Si el explorador web no utiliza el cifrado AES o 3DES, iLO 2 mostrará un mensaje de error en el que se solicita que cierre la conexión actual y seleccione el cifrado correcto.

Consulte la documentación del explorador para seleccionar una intensidad de cifrado de al menos AES o 3DES. Los distintos exploradores utilizan diferentes métodos de selección de cifrado negociado. Antes de cambiar la intensidad de cifrado del explorador, es necesario cerrar la sesión de iLO 2 mediante el explorador actual. Los cambios realizados en la configuración de cifrado del explorador mientras está conectado a iLO 2 pueden hacer que el explorador siga utilizando el cifrado AES/3DES.

Todos los exploradores y sistemas operativos cliente compatibles con iLO 2 admiten la función AES/3DES Encryption (Cifrado AES/3DES) de iLO 2, excepto si se utiliza Windows 2000 Professional con Internet Explorer. De manera predeterminada, Windows 2000 Professional no admite los cifrados AES o 3DES. Si un cliente utiliza Windows® 2000 Professional, es necesario utilizar otro explorador o actualizar el sistema operativo.

Internet Explorer no dispone de una configuración de intensidad de cifrado que pueda seleccionar el usuario. Debe editar el registro para permitir que Internet Explorer establezca la conexión con iLO 2 cuando la configuración Enforce AES/3DES Encryption (Aplicar cifrado AES/3DES) está activada. Para activar el cifrado AES/3DES en Internet Explorer, abra el Registro y establezca `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy` en 1.

NOTA: La modificación incorrecta del Registro puede provocar daños graves en el sistema. HP recomienda crear una copia de seguridad de los datos valiosos del ordenador antes de efectuar cambios en el Registro. Si desea obtener información acerca de cómo restablecer su registro, consulte el artículo de la base de datos Knowledge Base de Microsoft (http://support.microsoft.com/kb/307545.)

Para establecer la conexión a iLO 2 a través de una conexión SSH, consulte la documentación de la utilidad SSH y establezca la intensidad de cifrado.

Cuando se establece la conexión a través del canal XML, la utilidad CPQLOCFG utiliza un cifrado 3DES de manera predeterminada. CPQLOCFG 2.26 o versiones posteriores muestra la siguiente intensidad de conexión actual en la salida XML. Por ejemplo:

```
Connecting to Server..
Negotiated cipher: 168-bit Triple DES with RSA and a SHA1 MAC
```

El cifrado AES no es compatible con Internet Explorer en un cliente Windows® 2000 Professional. Para utilizar el cifrado AES con este sistema operativo, utilice otro explorador (por ejemplo, Mozilla.)

Inicio de sesión único de HP SIM (SSO)

HP SIM SSO le permite navegar directamente desde HP SIM a su procesador LOM, omitiendo un paso de inicio de sesión intermedio. Para utilizar SSO, se requiere una versión actual de HP SIM y el procesador LOM se debe configurar para que admita los enlaces desde HP SIM. HP SIM requiere las actualizaciones y los parches más recientes para funcionar correctamente. Para obtener más información acerca de HP Systems Insight Manager y las actualizaciones disponibles, consulte la página Web de HP (http://www.hp.com/go/hpsim.)

HP SIM SSO es una función con licencia que se encuentra disponible mediante la adquisición de licencias opcionales. Si desea obtener más información, consulte "Concesión de licencias (Concesión de licencias en la página 21)".

La página HP SIM SSO permite visualizar y configurar los valores de SSO a través de la interfaz de iLO 2. Para obtener más información, consulte la sección "Configuración de HP SIM SSO" (Configuración de HP SIM SSO en la página 60.)

Asimismo, es posible acceder a los valores de configuración de HP SIM SSO mediante secuencias de comandos y archivos de texto, así como a través de una línea de comandos que utiliza clientes basados en texto, como, por ejemplo, SSH sobre la red, o desde el sistema operativo en el equipo host. La secuencia de comandos de SSO permite utilizar la misma configuración de SSO en todos sus procesadores LOM. Para obtener más información, ejemplos de secuencias de comandos y extensiones CLP que permiten leer, modificar y escribir los valores de configuración de HP SIM SSO, consulte la *Guía de recursos de líneas y secuencias de comandos del procesador de gestión HP Integrated Lights-Out*.

Configuración de iLO 2 para HP SIM SSO

Antes de iniciar la configuración de SSO, debe disponer de la dirección de red de HP SIM y asegurarse de que se ha instalado una clave de licencia. Para configurar SSO:

1. Active Single Sign-On Trust Mode (Modo fiable de inicio de sesión único) seleccionando **Trust by Certificate (Confiar según certificado)** (recomendado), **Trust by Name (Confiar según nombre)** o **Trust All (Confiar en todo)**.
2. Añada el certificado HP SIM del servidor a iLO 2.
   a. Haga clic en **Add an HP SIM Server (Añadir un servidor HP SIM)**.
   b. Introduzca la dirección de red del servidor HP SIM.
   c. Haga clic en **Import Certificate (Importar certificado)**.

      El tamaño del repositorio de certificados permite cinco certificados típicos de iLO 2. No obstante, los tamaños de los certificados pueden variar si no se emite alguno de los certificados típicos. Hay 6 KB de almacenamiento combinado destinados para los certificados y nombres de servidor de iLO 2. Cuando se utiliza el almacenamiento destinado, no se admiten más importaciones.

Tras configurar SSO en iLO 2, inicie sesión en HP SIM, busque el procesador LOM y seleccione **Tools (Herramientas)>System Information (Información del sistema)>iLO as... (iLO como...)** HP SIM inicia un nuevo explorador que con una sesión iniciada en el procesador de gestión LOM.

Adición de servidores de confianza HP SIM

Es posible instalar certificados del servidor HP SIM mediante secuencias de comandos adecuadas para la implementación masiva. Para obtener más información, consulte la *Guía de recursos de líneas y*

secuencias de comandos del procesador de gestión HP Integrated Lights-Out. Para agregar los registros del servidor HP SIM mediante un explorador:

1. Haga clic en **Administration (Administración)>Security (Seguridad)>HP SIM SSO**.
2. Haga clic en **Add an HP SIM Server (Añadir un servidor HP SIM)**.
3. Para autenticar el servidor, seleccione una de las siguientes opciones:

   - Para añadir un servidor HP SIM a través de la autenticación Trust by Name (Confiar según nombre), introduzca el nombre de red completo del servidor HP SIM en la sección Add a Trusted HP SIM Server Name (Añadir un nombre de servidor HP SIM de confianza.) Haga clic en **Add Server Name (Añadir nombre de servidor)**.

     La autenticación Trust by Name (Confiar según nombre) utiliza nombres de dominio completamente calificados; por ejemplo, sim-host.hp.com en lugar de sim-host. Si no está seguro del nombre del dominio completamente calificado, utilice el comando `nslookup host`.

   - Para recuperar e importar un certificado desde un servidor HP SIM de confianza, introduzca el nombre de red completo de un servidor HP SIM en la sección Retrieve and import a certificate from a trusted HP SIM Server (Recuperar e importar un certificado desde un servidor HP SIM fiable.) Haga clic en **Import Certificate (Importar certificado)** para solicitar el certificado al servidor HP SIM e importarlo automáticamente. Este registro es compatible con las opciones SSO Trust by Name (Confiar según nombre de SSO) y SSO Trust by Certificate (Confiar según certificado de SSO.)

     Para impedir la manipulación inadecuada del certificado, importe directamente un certificado de servidor HP SIM. Para importar directamente un certificado de servidor HP SIM, recupere la fecha del certificado HP SIM mediante una de las siguientes opciones:

     - En una ventana de explorador independiente, diríjase al servidor HP SIM con la URL:

       `http://<sim network address>:280/GetCertificate`

       Corte y pegue los datos del certificado de HP SIM en iLO 2.

     - Exporte el certificado de servidor HP SIM de la interfaz de usuario de HP SIM mediante la selección de **Options (Opciones)>Security (Seguridad)>Certificates (Certificados)>Server Certificate (Certificado de servidor)**. Con el editor de texto, abra un archivo y copie y pegue todos los datos no procesados del certificado en iLO 2.

     - Mediante las herramientas de la línea de comandos del servidor HP SIM, es posible extraer el certificado de HP SIM utilizando un alias tomcat codificado para el certificado de HP SIM. Por ejemplo:

       `mxcert -l tomcat`

       Aparecen los datos del certificado:

       ```
       -----BEGIN CERTIFICATE-----
       several lines of encoded data
       -----END CERTIFICATE-----
       ```

     Una vez pegados los datos del certificado x.509 cifrado según base-64 del servidor HP SIM en la sección Directly import a HP SIM Server Certificate (Importar directamente un certificado de servidor HP SIM), haga clic en **Import Certificate (Importar certificado)** para grabar los datos. Este tipo de registro es compatible con las opciones SSO Trust by Name (Confiar según nombre de SSO) y SSO Trust by Certificate (Confiar según certificado de SSO.)

Existen otros modos de recuperar los datos del certificado de servidor HP SIM. Para obtener más información, consulte la documentación de HP SIM.

Configuración de HP SIM SSO

La página HP SIM SSO permite visualizar y configurar los valores de inicio de sesión único de iLO 2. Es necesario disponer del privilegio Configure iLO 2 (Configurar iLO 2) para cambiar esta configuración. Para acceder a la configuración de iLO 2 SSO, haga clic en **Administration (Administración) >Security (Seguridad)>HP SIM SSO**.

La página HP Systems Insight Manager Single Sign-On Settings (Configuración de inicio de sesión único de HP Systems Insight Manager) incluye los siguientes campos y opciones:

- Single Sign-On Trust Mode (Modo fiable de inicio de sesión único): permite controlar el modo en que se aceptan las conexiones iniciadas en SSO:
  - Trust None (Confiar en ninguna) (predeterminada): rechaza todas las solicitudes de conexión de SSO.
  - Trust by Certificate (Confiar según certificado) (la más segura): permite únicamente las conexiones de SSO desde un servidor HP SIM que coincida con un certificado anteriormente importado en iLO 2.
  - Trust by Name (Confiar según nombre): permite las conexiones de SSO desde un servidor HP SIM que coincida con un nombre DNS o certificado anteriormente importado en iLO 2.
  - Trust All (Confiar en todo) (la menos segura): acepta cualquier conexión SSO iniciada desde cualquier servidor HP SIM.

    Los usuarios que inician sesión en HP SIM se autorizan según la asignación de función del servidor HP SIM. La asignación de función se transmite al procesador LOM cuando se intenta un inicio de sesión único. En la sección Single Sign-On Settings (Configuración de inicio de sesión único), puede configurar los privilegios de iLO 2 para cada una de las funciones Para obtener más información acerca de cada privilegio, consulte la sección "Administración de usuarios (Administración de usuarios en la página 23)".

    Mediante el uso de cuentas de usuario basadas en directorio, SSO intenta recuperar los privilegios asignados en esta sección. La configuración de directorio de Lights-Out no se aplica. Las asignaciones de privilegios predeterminadas son:
  - Usuario: únicamente inicio de sesión

- Operador: inicio de sesión, consola remota, alimentación y reinicio y soporte virtual
- Administrator (Administrador): Login (Iniciar sesión), Remote Console (Consola remota), Power and Reset (Alimentación y reinicio), Virtual Media (Soportes virtuales), Configure iLO 2 (Configurar iLO 2) y Administer Users (Administrar usuarios)

- HP SIM Trusted Servers (Servidores HP SIM de confianza): permite visualizar el estado de los servidores HP SIM de confianza configurados para utilizar SSO con el procesador LOM actual. Para añadir un nombre de servidor, importar un certificado de servidor o instalar directamente un certificado de servidor, haga clic en **Add a SIM Server (Añadir un servidor SIM)**. Para obtener más información, consulte la sección "Adición de servidores de confianza HP SIM (Adición de servidores de confianza HP SIM en la página 58)".

  En la tabla de servidores se muestra una lista de los servidores HP SIM registrados y se incluye el estado de cada uno de ellos. El número real de sistemas permitidos depende del tamaño de los datos certificados almacenados.

  Aunque es posible que un sistema esté registrado, SSO puede verse rechazado debido al nivel de confianza actual o al estado del certificado. Por ejemplo, si se registra un nombre de servidor HP SIM y el nivel de confianza se establece en Trust by Certificate (Confiar según certificado), SSO no estará permitido para ese servidor. Asimismo, si se importa un certificado de servidor HP SIM caducado, este servidor no permitirá el SSO. Además, los registros no se utilizan cuando SSO está desactivado. iLO 2 no obliga la revocación del certificado de servidor de SSO.

  - Status (Estado): indica el estado del registro (si tiene alguno instalado.)
  - Description (Descripción): permite visualizar en nombre del servidor (o el asunto del certificado.) Una imagen en miniatura del certificado indica que el registro contiene un certificado almacenado.
  - Actions (Acciones): muestra las acciones que se pueden realizar en un registro seleccionado. Las acciones mostradas dependen del tipo y número de registros instalados:
    - — Remove Name (Eliminar nombre): permite eliminar el registro del nombre del servidor.
    - — Remove Certificate (Eliminar certificado): permite eliminar el registro del certificado.

Bloqueo de equipo de consola remota

La función Remote Console Computer Lock (Bloqueo de equipo de consola remota) mejora la seguridad de un servidor gestionado de iLO 2 mediante el bloqueo automático de un sistema operativo o mediante el cierre de la sesión de un usuario cuando finaliza la sesión de la consola remota o se pierde el enlace de red con iLO 2. A diferencia de Remote Console (Consola remota) e Integrated Remote Console (Consola remota integrada), esta función es estándar y no requiere una licencia adicional. Por lo tanto, si abre una ventana Remote Console Session (Sesión de consola remota) o Integrated Remote Console (Consola remota integrada) y esta función está configurada, cuando se cierre la ventana, el sistema operativo se bloqueará, incluso si las licencias de funciones adicionales no están instaladas.

Puede visualizar y configurar los ajustes de Remote Console Computer Lock (Bloqueo de equipo de consola remota) a través de las fichas Administration (Administración) o Remote Console (Consola remota) en la interfaz de iLO 2. De manera predeterminada, la función Remote Console Computer Lock (Bloqueo de equipo de consola remota) está desactivada.

Para cambiar los valores de Remote Console Computer Lock (Bloqueo de equipo de consola remota):

1. Inicie una sesión en iLO 2 con una cuenta con el privilegio Configure iLO 2 Settings (Configurar valores de iLO 2.)

2. Haga clic en **Administration (Administración)>Security (Seguridad)>Remote Console (Consola remota)**. Aparecerá la página Computer Lock Settings (Valores de bloqueo de equipo.)

3. Modifique los valores según sus necesidades.

   - Windows: utilice esta opción para establecer que iLO 2 bloquee un servidor gestionado que ejecute un sistema operativo Windows®. Cuando finaliza la sesión de consola remota o se pierde el enlace de red con iLO 2, el servidor muestra automáticamente el cuadro de diálogo Computer Locked (Equipo bloqueado.)
   - Custom (Personalizar): utilice esta opción para configurar iLO 2 y utilizar una secuencia de teclas personalizada con el fin de bloquear un servidor gestionado o cerrar la sesión de un usuario en dicho servidor. Es posible seleccionar hasta cinco teclas de la lista. La secuencia de teclas seleccionada se envía automáticamente al sistema operativo del servidor cuando finaliza la sesión de consola remota o se pierde el enlace de red con iLO 2.
   - Disabled (Desactivado): utilice esta opción para desactivar la función Remote Console Computer Lock (Bloqueo de equipo de consola remota.) Aunque se finalice la sesión de consola remota o se pierda el enlace de red con iLO 2, el servidor gestionado no se bloqueará.

     Es posible crear una secuencia de teclas para Remote Console Computer Lock (Bloqueo de equipo de consola remota) mediante las teclas que se muestran en la siguiente tabla.

ESC	F4	1	e
L_ALT	F5	2	f
R_ALT	F6	3	g
L_MAYÚS	F7	4	h
R_MAYÚS	F8	5	i
L-CTRL	F9	6	j
R_CTRL	F10	7	k
L_GUI	F11	8	l
R_GUI	F12	9	m
INSERT	" " (Espacio)	:	n
SUPR	!	;	o
INICIO	"	<	p
FIN	#	=	q
RE_PÁG	$	>	r
AV_PÁG	%	?	s
INTRO	&	@	t
TAB	'	[	u
ENTRAR	(	\	v

RETROCESO	)	]	w
+ de teclado numérico	*	^	x
- de teclado numérico	+	_	s
BLOQ DESPL	,	'	z
PET SIS	-	a	{
F1	.	b	}
F2	/	c	|
F3	0	d	~

4. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Asimismo, es posible configurar esta función a través de líneas o secuencias de comandos. Para obtener más información, consulte la *Guía de recursos de líneas y secuencias de comandos del procesador de gestión HP Integrated Lights-Out*.

Red

Las fichas Network Settings (Configuración de red) y DCHP/DNS de la sección Network (Red) permiten ver y modificar la configuración de red en iLO 2.

Sólo los usuarios que tengan el privilegio Configure iLO 2 (Configurar iLO 2) pueden cambiar esta configuración. Los usuarios que no tengan el privilegio Configure iLO 2 Settings (Configurar valores de iLO 2) podrán ver los valores de configuración asignados.

Para cambiar la configuración de red de iLO 2:

1. Inicie una sesión en iLO 2 con una cuenta con el privilegio Configure iLO 2 Settings (Configurar valores de iLO 2.) Haga clic en **Administration (Administration)>Network (Red)**.
2. Seleccione **Network Settings (Configuración de red)** o **DHCP/DNS**.
3. Cambie la configuración según sus necesidades.
4. Tras realizar cualquier cambio en los parámetros, haga clic en **Apply (Aplicar)** para completar los cambios.

iLO 2 se reinicia y finaliza la conexión del explorador en iLO 2. Para volver a establecer una conexión, espere 60 segundos antes de iniciar otra sesión con el explorador.

Configuración de red

La página Network Settings (Configuración de red) muestra la dirección IP de la NIC, la máscara de subred y otra información relacionada con TCP/IP y su configuración. Desde la pantalla Network Settings (Configuración de red) puede activar o desactivar DHCP y, en los servidores que no usan DHCP, puede configurar una dirección IP estática. Todos los usuarios pueden ver la configuración de red, pero sólo los que tengan el privilegio Configure iLO 2 (Configurar iLO 2) pueden cambiar esta configuración. Para acceder a la página Network Settings (Configuración de red), haga clic en

Administration (Administración)>Network (Red)>Network (Red). En la página Network Settings (Configuración de red) se incluye la siguiente información y ajustes:

- NIC permite configurar la NIC de iLO 2 en Enabled (Activada), Disabled (Desactivada) o Shared Network Port (Puerto de red compartido.)
  - Enabled (Activada): permite activar la interfaz de red de iLO 2 principal.
  - Desactivada: permite desactivar la interfaz de red de iLO 2. Es necesario utilizar la utilidad RBSU de iLO 2 u otra utilidad de secuencias de comandos basada en host para volver a activar la interfaz de red.
  - Shared Network Port (Puerto de red compartido): permite activar la red a través del puerto Ethernet del host designado. El puerto se muestra como dos direcciones independientes Ethernet MAC e IP en la red. Para obtener más información, consulte la sección "Puerto de red compartido de iLO 2" (Puerto de red compartido de iLO 2 en la página 65.)
- DHCP permite seleccionar la dirección IP estática (desactivada) o activar el uso de un servidor DHCP para obtener una dirección IP del subsistema Integrated Lights-Out 2.

  No puede establecer la dirección IP de iLO 2 ni la máscara de subred si DHCP está activado. La desactivación de DHCP permite configurar la dirección IP. Para ofrecer mayor comodidad, el campo IP Address (Dirección IP) también se muestra en la página DHCP/DNS Settings (Configuración de DHCP/DNS.) Si se cambia el valor de cualquiera de las páginas, se cambiará la configuración de DHCP.
- IP Address (Dirección IP) es la dirección IP de iLO 2. Si se utiliza DHCP, la dirección IP de iLO 2 se proporciona automáticamente. Si no es el caso, escriba una dirección IP estática. Para ofrecer mayor comodidad, el campo IP Address (Dirección IP) se muestra en la página DHCP/DNS. Si se introducen valores en este campo en cualquiera de las páginas, la dirección IP de iLO 2 cambia.
- Subnet Mask (Máscara de subred) es la máscara de subred de la red IP de iLO 2. Si se utiliza DHCP, se proporcionará automáticamente la máscara de subred. Si no es el caso, escriba la máscara de subred de la red.
- Gateway IP Address (Dirección IP de la puerta de enlace) muestra la dirección IP de la puerta de enlace de red. Si DHCP se encuentra en uso, la dirección IP de la puerta de enlace se proporciona automáticamente. Si no es el caso, escriba la dirección de la puerta de enlace de red.
- iLO 2 Subsystem Name (Nombre de subsistema de iLO 2) es el nombre utilizado por el subsistema de iLO 2. Si DHCP y DNS están correctamente configurados, es posible utilizar este nombre en lugar de la dirección IP para establecer la conexión con el subsistema de iLO 2. Para obtener más información, consulte la sección "Limitaciones de nombre de subsistema de iLO 2" (Limitaciones de nombre de subsistema de iLO 2 en la página 65.)
- Link (Enlace) controla la velocidad y dúplex del transceptor de red de iLO 2. Es posible resaltar la velocidad actual de enlace de la NIC dedicada primaria de iLO 2. En la configuración de del enlace se incluyen los siguientes elementos:
  - Automatic (Automático) (predeterminado): permite a iLO 2 negociar la mayor velocidad de enlace y dúplex admitidos cuando se conecta a la red.
  - 100 Mb/FD: provoca una conexión de 100 Mb a través del dúplex integral.
  - 100 Mb/HD: provoca una conexión de 100 Mb a través del semidúplex.
  - 10 Mb/FD: provoca una conexión de 10 Mb a través del dúplex completo.
  - 10 Mb/HD: provoca una conexión de 10 Mb a través del semidúplex.

Si la opción de detección automática se encuentra desactivada, el conmutador de red deberá disponer de los mismos ajustes que iLO 2 para evitar que se produzcan problemas con el acceso a iLO 2.

Limitaciones de nombre de subsistema de iLO 2

El nombre de subsistema de iLO 2 representa el nombre DNS del subsistema de iLO 2. Por ejemplo, `ilo` en lugar de `ilo.hp.com`. Este nombre sólo puede usarse si DHCP y DNS están configurados correctamente para conectarse al nombre de subsistema de iLO 2 en vez de a la dirección IP.

- Limitaciones de servicio de nombres: el nombre de subsistema se utiliza como parte del nombre DNS y el nombre WINS. Sin embargo, las limitaciones de DNS y WINS difieren:
  - DNS permite caracteres alfanuméricos y guiones. WINS permite caracteres alfanuméricos, guiones y caracteres de subrayado.
  - Los nombres de subsistema de WINS se truncan a los 15 caracteres; los DNS, no.

    Si necesita utilizar caracteres de subrayado, pueden escribirse en RBSU o mediante la utilidad de secuencias de comandos de iLO 2.

    NOTA: Las limitaciones del servicio de nombres también se aplican al nombre de dominio.

    Para evitar problemas de espacio de nombres:
  - No utilice el carácter de subrayado.
  - Limite los nombres de subsistema a 15 caracteres.
  - Compruebe que puede hacer ping a iLO mediante la dirección IP y el nombre DNS/WINS.
  - Compruebe que NSLOOKUP resuelve correctamente la dirección de red de iLO y que no hay conflictos de espacio de nombres.
  - Compruebe que DNS y WINS resuelven correctamente el nombre (si utiliza ambos.)
  - Vacíe el nombre DNS si hace algún cambio de espacio de nombres.

Puerto de red compartido de iLO 2

La opción Shared Network Port (Puerto de red compartido) de iLO 2 permite seleccionar entre la NIC del sistema o la NIC de gestión dedicada de iLO 2 para la gestión del servidor. Cuando se activa la opción Shared Network Port (Puerto de red compartido) de iLO 2, tanto el tráfico de red compartido como el tráfico de red de iLO 2 se transfieren a la NIC del sistema.

iLO 2 proporciona soporte a los servidores que no disponen de una NIC de gestión dedicada de iLO 2. En los servidores que utilizan la NIC de gestión dedicada de iLO 2, la configuración estándar del hardware proporciona la conectividad de la red de iLO 2 únicamente a través de la conexión del puerto de red compartido de iLO 2. iLO 2 detecta la ausencia de una NIC de gestión dedicada de iLO 2 y se establece automáticamente en el puerto de red compartido. Es posible que en algunos de estos servidores, una NIC de gestión dedicada se encuentre disponible como opción de hardware. Si una NIC de gestión dedicada de iLO 2 se encuentra disponible como opción de hardware, iLO 2 se establece de manera predeterminada en la NIC de gestión dedicada de iLO 2. En los servidores que utilizan la NIC de gestión dedicada de iLO 2, es posible activar el funcionamiento del puerto de red compartido a través de la interfaz de iLO 2.

El puerto de red compartido de iLO 2 utiliza el puerto de red etiquetado como NIC 1 situado en el panel posterior del servidor. Es posible que la numeración de la NIC del sistema operativo no coincida con la numeración del sistema. El puerto de red compartido iLO 2 no afecta al rendimiento de iLO 2. El tráfico pico de iLO 2 es inferior a 2 Mb (en una NIC con capacidad de 1000 Mb) y el tráfico medio de iLO 2 es poco frecuente y bajo.

El puerto de red compartido no está disponible en HP ProLiant ML310 G3, ML310 G4, BL20p G4 ni en ninguno de los servidores blade c-Class.

Restricciones y funciones del puerto de gestión compartido de iLO 2

El puerto de red compartido de iLO 2 y el puerto de la NIC de gestión dedicada de iLO 2 se utilizan para la gestión del servidor de iLO 2. El puerto de red compartido de iLO 2 y el puerto de la NIC de gestión dedicada de iLO 2 sólo se pueden utilizar para la gestión del servidor de iLO 2. El puerto de red compartido de iLO 2 y el puerto de la NIC de gestión dedicado de iLO 2 no pueden funcionar simultáneamente. Si se activa la NIC de iLO 2 dedicada, se desactivará el puerto de red compartido de iLO 2. Si se activa el puerto de red compartido de iLO 2, se desactivará la NIC de gestión dedicada de iLO 2.

No obstante, la desactivación del puerto de red dedicado no supone la desactivación completa del sistema NIC. Todavía se producirá tráfico de red regular en el sistema NIC. Cuando se desactiva el tráfico de red del puerto de red compartido, el tráfico que provenga o se dirija a iLO 2 no se pasa a iLO 2 por medio de puerto de red compartido, ya que no comparten el puerto de red compartido.

El puerto de red compartido no debe considerarse una función de disponibilidad, sino que se utiliza para permitir la consolidación del puerto de red gestionado. El uso de esta función puede crear un punto de fallo único; es decir, si el puerto falla o se desconecta, tanto el host como iLO 2 dejan de estar disponibles en la red.

Activación de la función del puerto de red compartido de iLO 2

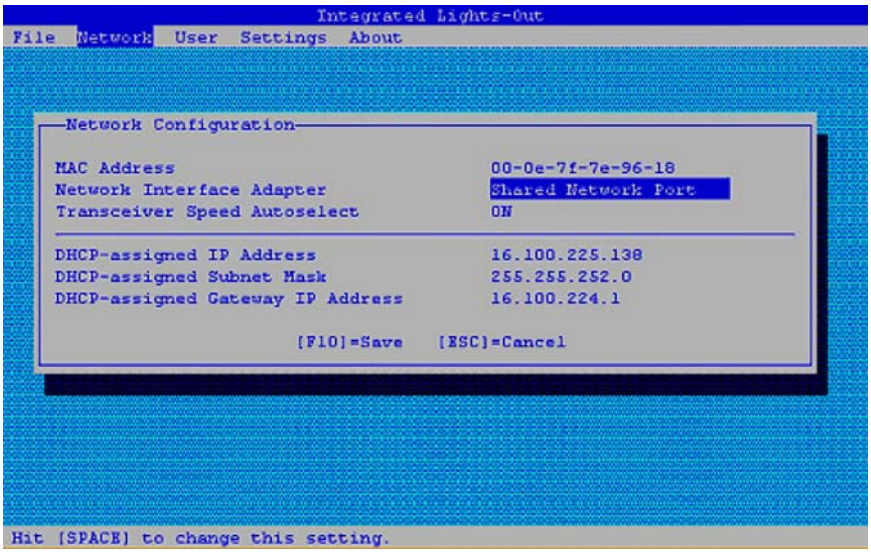
De forma predeterminada, la función del puerto de red compartido de iLO 2 estará desactivada. Esta función se puede activar por medio de:

- iLO 2 RBSU (RBSU de iLO 2)
- La interfaz Web de iLO 2
- XML scripting (Secuencias de comandos XML)

Activación de la función del puerto de red compartido de iLO 2 por medio de RBSU de iLO 2

1. Conecte el puerto 1 de la NIC del servidor a la LAN.
2. Durante la ejecución del proceso POST, pulse **F8** cuando se le solicite para entrar en la RBSU de iLO 2.
3. Seleccione **Network (Red)>NIC>TCP/IP**, y pulse la tecla **Enter (Intro)**.

4. En el menú Network Configuration (Configuración de red), configure el campo Network Interface Adapter (Adaptador de interfaz de red) como Shared Network Port (Puerto de red compartido) pulsando la barra espaciadora. La opción Shared Network Port (Puerto de red compartido) sólo está disponible en los servidores compatibles.



5. Pulse la tecla **F10** para guardar la configuración.
6. Seleccione **File (Archivo)>Exit (Salir)**, y pulse la tecla **Intro**.

Después del reinicio de iLO 2, se activa la función del puerto de red compartido. Todo el tráfico de red que vaya a iLO 2 u originado en iLO 2 se dirige por medio del puerto 1 de la NIC del sistema.

Activación de la función del puerto de red compartido de iLO 2 por medio de la interfaz Web

1. Conecte el puerto 1 de la NIC de iLO 2 a una LAN.
2. Abra un explorador y desplácese hasta el nombre de DNS o la dirección IP de iLO 2.
3. Seleccione **Administration (Administration)>Network Settings (Configuración de red)**.
4. En la página Network Settings (Configuración de red), seleccione **Shared Network Port (Puerto de red compartido)**. La función Shared Network Port (Puerto de red compartido) sólo está disponible en los servidores compatibles.
5. Haga clic en **Apply (Aplicar)** en la parte inferior de la página.
6. Haga clic en **Yes (Sí)** en el cuadro de diálogo de advertencia y, a continuación, haga clic en **OK (Aceptar)**.

Después del reinicio de iLO 2, se activa la función del puerto de red compartido. Todo el tráfico de red que vaya a iLO 2 u originado en iLO 2 se dirige por medio del puerto 1 de la NIC del sistema.

Sólo el puerto de red compartido o la NIC de gestión dedicada de iLO 2 están activos para la gestión de servidores. No es posible que estén activos al mismo tiempo.

Reactivación del puerto de gestión de iLO 2 dedicado

Las secuencias de comandos de la interfaz Web de iLO 2, RBSU o XML (descritas en la guía de referencia de líneas y secuencias de comandos) deben utilizarse para reactivar la NIC de gestión dedicada de iLO 2. La reactivación de iLO 2 por medio de RBSU requiere el reinicio del sistema.

Para reactivar la NIC de gestión dedicada de iLO 2 utilizando RBSU:

1. Conecte el puerto de NIC de gestión dedicado de iLO 2 a una LAN desde la que se administre el servidor.
2. Reinicie el servidor.
3. Durante la ejecución del proceso POST, pulse **F8** cuando se le solicite para entrar en la RBSU de iLO 2.
4. Seleccione **Network (Red)>NIC>TCP/IP**, y pulse la tecla **Enter (Intro)**.
5. En el menú Network Configuration (Configuración de red), pulse la barra espaciadora para ajustar el campo Network Interface Adapter (Adaptador de interfaz de red) en ON (Activado.)
6. Pulse la tecla **F10** para guardar la configuración.
7. Seleccione **File (Archivo)>Exit (Salir)**, y pulse la tecla **Intro**.

Después del reinicio de iLO 2, se activa el puerto de gestión dedicado de iLO 2.

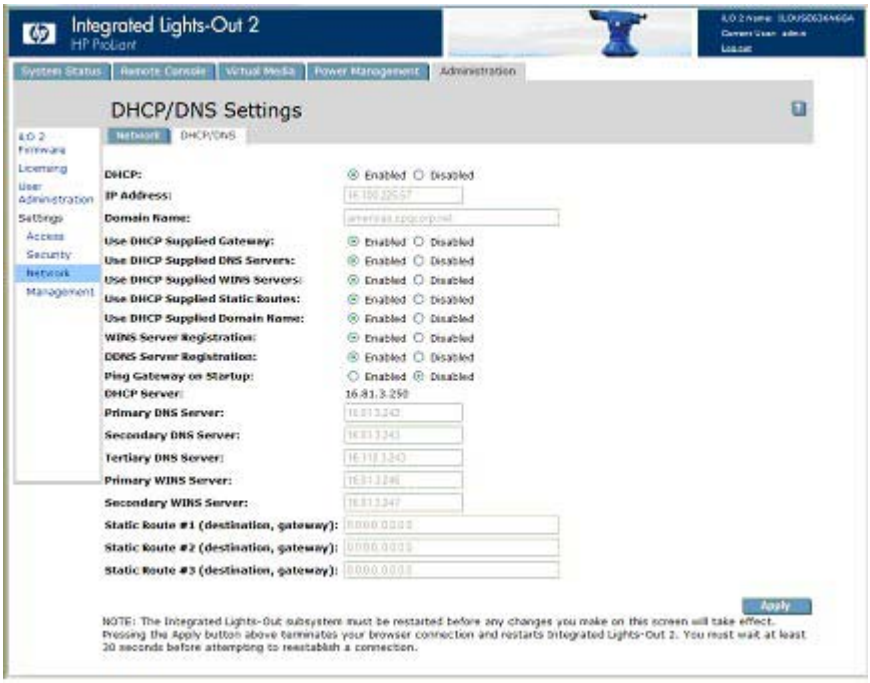
Para reactivar la NIC de gestión dedicada de iLO 2 utilizando la interfaz de iLO 2:

1. Abra un explorador y desplácese hasta el nombre de DNS o la dirección IP de iLO 2.
2. En la página Network Settings (Configuración de red), seleccione **Enabled (Activado)** en la NIC de iLO 2.
3. Haga clic en **Apply (Aplicar)**. Aparece un cuadro de diálogo de advertencia.
4. Haga clic en **Yes (Sí)** y, a continuación, en **OK (Aceptar)**.

Después del reinicio de iLO 2, se activa la NIC de gestión dedicada de iLO 2. Cuando utilice IRC mediante un puerto de NIC de gestión dedicado de iLO 2 y en función del tráfico de red, es posible que no tenga el tiempo suficiente para pulsar las teclas RBSU durante el proceso de POST.

Configuración de DHCP/DNS

La página iLO 2 DHCP/DNS Settings (Configuración de DNCP/DNS) de iLO 2 muestra la información de configuración de DHCP/DNS para iLO 2. Todos los usuarios pueden visualizar la configuración de DHCP/DNS, pero es necesario disponer del privilegio Configure iLO 2 Settings (Configurar los ajustes de iLO 2) para poder cambiarlos. Asimismo, es posible cambiar estos ajustes desde la utilidad RBSU de iLO 2 (F8 durante POST.) Para acceder a la configuración de DHCP/DNS, haga clic en **Administration (Administración)>Network (Red)>DHCP/DNS**. Aparecerá la página DHCP/DNS Settings (Configuración de DHCP/DNS.)



Las siguientes opciones están disponibles:

- DHCP permite seleccionar la dirección IP estática (desactivada) o activar el uso de un servidor DHCP para obtener una dirección IP para el subsistema de iLO 2.

  No es posible establecer la dirección IP de iLO 2 si DHCP está activado. La desactivación de DHCP permite configurar la dirección IP. Para ofrecer mayor comodidad, el campo IP Address (Dirección IP) también se muestra en la página Network Settings (Configuración de red.) Si se cambia el valor de cualquiera de las páginas, se cambiará la configuración de DHCP.

- IP Address (Dirección IP) es la dirección IP de iLO 2. Si se utiliza DHCP, la dirección IP de iLO 2 se proporciona automáticamente. Si no es el caso, escriba una dirección IP estática. Para ofrecer mayor comodidad, el campo IP Address (Dirección IP) se muestra en la página Network Settings (Configuración de red.) Si se cambia el valor de cualquiera de las páginas, se cambiará la dirección IP de iLO 2.

- Domain Name (Nombre de dominio) es el nombre del dominio en el que reside el subsistema de iLO 2. Si DHCP está activado, le asignará el nombre. La activación de DHCP permite configurar las siguientes opciones de DHCP:

  - Use DHCP Supplied Gateway (Utilizar puerta de enlace suministrada por DHCP): cambia si iLO 2 utiliza la puerta de enlace suministrada por el servidor DHCP. Si no es el caso, escriba una dirección de puerta de enlace en la casilla Gateway IP Address (Dirección IP de puerta de enlace.)

  - Use DHCP Supplied DNS Servers (Utilizar servidores DNS suministrados por DHCP): cambia si iLO 2 utiliza la lista de servidores DNS suministrada por el servidor DHCP. Si no es el caso, escriba la dirección del servidor DNS en los campos Primary (Primario), Secondary (Secundario) y Tertiary (Terciario) del servidor DNS.

  - Use DHCP Supplied WINS Servers (Utilizar servidores WINS suministrados por DHCP): cambia si iLO 2 utiliza la lista de servidores WINS suministrada por el servidor DHCP. Si no es el caso, escriba la dirección del servidor WINS en los campos Primary (Primario) y Secondary (Secundario) del servidor WINS.

- Use DHCP Supplied Static Routes (Utilizar rutas estáticas suministradas por DHCP): cambia si iLO 2 utiliza la ruta estática suministrada por el servidor DHCP. Si no es el caso, escriba la dirección de la ruta estática en los campos Static Route #1 (Primera ruta estática), Static Route #2 (Segunda ruta estática) o Static Route #3 (Tercera ruta estática.)
- Use DHCP Supplied Domain Name (Utilizar nombre de dominio suministrado por DHCP): cambia si iLO 2 utiliza el nombre de dominio suministrado por el servidor DHCP. Si no es el caso, escriba un nombre de dominio en el cuadro Domain Name (Nombre de dominio.)

- WINS Server Registration (Registro de servidor WINS) cambia si iLO 2 registra su nombre con un servidor WINS.
- DDNS Server Registration (Registro de servidor DNS) cambia si iLO 2 registra su nombre con un servidor DDNS.
- La opción Ping Gateway on Startup (Solicitar puerta de enlace al inicio) hace que iLO 2 envíe cuatro paquetes de solicitud ICMP echo a la puerta de enlace cuando se inicia iLO 2. Esta opción asegura que la entrada de memoria caché de ARP para iLO 2 está actualizada en el enrutador responsable del transporte de paquetes desde y hacia iLO 2.
- DCHP Server (Servidor DHCP) es la dirección IP del servidor DHCP. No es posible asignar este campo. Si DHCP está activado, los datos se reciben desde DHCP y se representa la última dirección del servidor DHCP válida conocida.
- El servidor DNS primario, secundario y terciario son las direcciones IP de los servidores DNS. Si el servidor DHCP proporciona los valores, estos campos se completan automáticamente. Si no es el caso, introduzca las direcciones IP de forma manual.
- El servidor WINS primario y secundario son las direcciones IP de los servidores WINS. Si el servidor DHCP proporciona los valores, estos campos se completan automáticamente. Si no es el caso, introduzca las direcciones IP de forma manual.
- El campo Static Route #1, Static Route #2, and Static Route #3 (destination, gateway) (Ruta estática 1, Ruta estática 2 y Ruta estática 3. Vía de acceso, destino) sirve para las direcciones de la puerta de enlace de destino de la red. Introduzca hasta tres pares de rutas de puerta de enlace/destino de red.

Valores de configuración de SNMP/Insight Manager

La opción Management (Gestión) de la sección Administration (Administración) muestra la página SNMP/Insight Manager Settings (Valores de configuración de SNMP/Insight Manager.) La página SNMP/Insight Manager Settings (Valores de configuración de SNMP/Insight Manager) le permite configurar los avisos SNMP, generar un aviso de prueba y configurar la integración con HP SIM.

Activación de los avisos SNMP

iLO 2 admite hasta tres direcciones IP para recibir avisos SNMP. Normalmente, las direcciones utilizadas son las mismas que la dirección IP de la consola de servidor HP SIM.

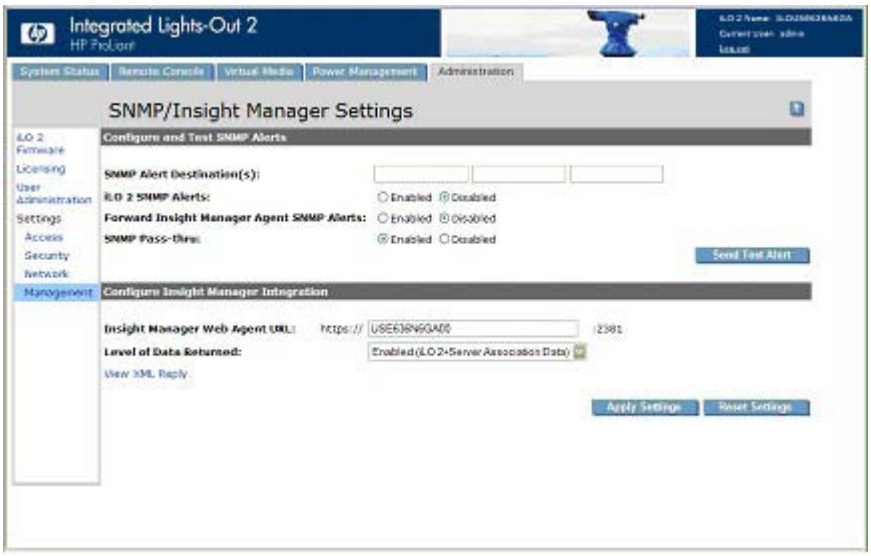
sólo los usuarios que tengan el privilegio Configure iLO 2 (Configurar iLO 2) pueden cambiar esta configuración. Los usuarios que no tengan el privilegio Configure iLO 2 Settings (Configurar valores de iLO 2) sólo podrán ver los valores de configuración asignados.

En la pantalla SNMP/Insight Manager Settings (Valores de configuración de SNMP/Insight Manager) están disponibles los siguientes avisos:

- SNMP Alert Destination(s) (Destinos de aviso SNMP)
- iLO 2 SNMP Alerts (Avisos SNMP de iLO 2)

- Forward Insight Manager Agent SNMP Alerts (Reenviar avisos SNMP del Agente Insight Manager)
- SNMP Pass-thru (Transferencia de SNMP)
- p-Class Alert Forwarding (Reenvío de avisos p-Class) (sólo aparece en servidores p-Class)

Para obtener más información, consulte la *Guía de recursos de líneas y secuencias de comandos del procesador de gestión HP Integrated Lights-Out*.



Para configurar los avisos:

1. Inicie una sesión en iLO 2 con una cuenta con el privilegio Configure iLO 2 Settings (Configurar valores de iLO 2.)
2. Seleccione **Management (Gestión)** en la ficha Administration (Administración.) Aparece la pantalla SNMP/Insight Manager Settings (Valores de configuración de SNMP/Insight Manager.)
3. En los campos SNMP Alert Destination(s) (Destinos de aviso SNMP), escriba hasta tres direcciones IP para recibir los avisos SNMP y seleccione las opciones de aviso que desee que admita iLO 2.
4. Haga clic en **Apply Settings (Aplicar configuración)**.

Los avisos de prueba incluyen una captura SNMP de Insight Manager y sirven para verificar la conectividad de la red de iLO 2 en HP SIM. Sólo los usuarios que tengan el privilegio Configure iLO 2 Settings (Configurar valores de iLO) podrán enviar avisos de prueba.

Compruebe que ha guardado los cambios de los campos SNMP Alert Destination(s) (Destinos de aviso SNMP) antes de enviar un aviso de prueba.

Para enviar un aviso de prueba:

1. Seleccione **Management (Gestión)** en la ficha Administration (Administración.) Aparece la pantalla SNMP/Insight Manager Settings (Valores de configuración de SNMP/Insight Manager.)
2. Haga clic en **Send Test Alert (Enviar aviso de prueba)** en la sección Configure and Test SNMP Alerts (Configurar y probar avisos SNMP) para generar un aviso de prueba y enviarlo a las direcciones TCP/IP almacenadas en los campos SNMP Alert Destinations (Destinos de aviso SNMP.)

3. Después de generar el aviso, aparece una pantalla de confirmación.
4. Consulte la consola HP SIM para ver si se ha recibido la captura.

Definiciones de capturas SNMP generadas

Es posible generar las siguientes capturas SNMP en los servidores BL c-Class e iLO 2:

- ALERT_TEST se utiliza para verificar que la configuración de SNMP, la consola SNMP del cliente y la red funcionan correctamente. Mediante la interfaz de iLO 2 es posible generar este aviso y comprobar que éste se ha recibido en la consola SNMP. Asimismo, es posible su generación a través de la ROM de opciones de iLO 2 y comprobar los valores de configuración de SNMP.
- ALERT_SERVER_POWER se produce cuando el procesador de gestión de iLO 2 detecta una transición inesperada de la alimentación del sistema host, ya se de ON a OFF o de OFF a ON. Las transiciones de la alimentación del sistema host se consideran inesperadas cuando el cambio se produce debido a sucesos que el procesador de gestión desconoce. Este aviso no se genera cuando el sistema se enciende o apaga mediante la interfaz de iLO 2, CLI, RIBCL u otra función de gestión. Si el servidor se apaga debido al sistema operativo, porque se pulsa el botón de alimentación físico u otro método, se generará y enviará el aviso.
- ALERT_SERVER_RESET tiene lugar cuando el procesador de gestión de iLO 2 se utiliza para llevar a cabo un inicio en frío o en caliente del sistema host. Este aviso también se envía cuando el procesador de gestión de iLO 2 detecta que el sistema host se está restableciendo por causas que desconoce. Algunos comportamientos o acciones del sistema operativo pueden provocar la detección de este tipo de sucesos y la transmisión del aviso.
- ALERT_ILLEGAL_LOGIN es un aviso SNMP que se transmite cuando se intenta establecer una conexión mediante un nombre de usuario o contraseña no válidos. Este aviso se transmite independientemente del tipo de conexión: interfaz Web, puerto serie, telnet, SSH o RIBCL.
- ALERT_LOGS_FULL es un aviso SNMP que se transmite cuando el registro de sucesos de iLO 2 está lleno y se intenta registrar un suceso nuevo.
- ALERT_SELFTEST_FAILURE es un aviso SNMP que se transmite cuando iLO 2 detecta un error en cualquiera de los componentes internos supervisados. Si se detecta un error, se transmite un aviso SNMP.
- El aviso ALERT_SECURITY_ENABLED se transmite cuando el procesador de gestión de iLO 2 detecta un cambio a activado en el conmutador de anulación de seguridad.
- El aviso ALERT_SECURITY_DISABLED se transmite cuando el procesador de gestión de iLO 2 detecta un cambio a desactivado en el conmutador de anulación de seguridad.
- El aviso ALERT_HOST_GENERATED se genera cuando se ha solicitado al procesador de gestión de iLO 2 la transmisión de un aviso de host (transferencia de SNMP) y el procesador de gestión no ha podido transmitir el aviso SNMP original. iLO 2 intenta transmitir esta alerta genérica con el fin de informar a la consola de gestión SNMP de que no se ha podido transmitir una alerta desde el sistema host.

Configuración de la integración de Insight Manager

La URL Insight Manager Web Agent (Agente Web de Insight Manager) (nombre DNS o dirección IP) establece el destino del explorador del enlace Insight Agent en páginas de iLO 2. Normalmente, este enlace es la dirección IP o el nombre DNS del agente de gestión que se ejecuta en el sistema operativo del servidor host.

Escriba la dirección IP del servidor host. El protocolo (https://) y el número de puerto (:2381) se añaden automáticamente a la dirección IP o al nombre DNS para permitir el acceso a los agentes Web de Insight Management desde iLO 2.

Si la URL Insight Manager Web Agent (Agente Web de Insight Manager) se configura mediante otro método (por ejemplo, CPQLOCFG), haga clic en el botón Actualizar del explorador para mostrar la URL actualizada.

El valor Level of Data Returned (Nivel de datos devueltos) controla el contenido de un mensaje de detección anónimo recibido por iLO 2. La información devuelta se utiliza para las solicitudes de identificación HTTP de Insight Manager. Las siguientes opciones están disponibles:

- Enabled (Activado) (predeterminado) permite a Insight Manager asociar el procesador de gestión con el servidor host y proporciona los datos suficientes para permitir la integración con HP SIM.
- Disabled (Desactivado) impide que iLO 2 responda las solicitudes HP SIM.
- View XML Reply (Ver respuesta XML) le permite examinar los datos devueltos en las configuraciones.

  Visualice la respuesta que se devolverá a Insight Manager cuando solicite identificación del procesador de gestión utilizando este enlace.

Para ver los resultados de los cambios realizados, haga clic en **Apply Settings (Aplicar configuración)** para guardar los cambios. Haga clic en **Reset Settings (Reiniciar configuración)** para borrar los campos y devolver la página a su estado anterior. Este botón no guarda los cambios.

Para obtener más información acerca de Insight Agents, haga clic en **System Status (Estado del sistema)>Insight Agent**.

ProLiant BL p-Class, configuración

Existe la posibilidad de acceder a los servidores ProLiant BL p-Class y configurarlos de los siguientes modos:

- Mediante el puerto de diagnóstico de la placa iLO 2 de la parte delantera del servidor
- “Configuración basada en explorador” (Configuración de iLO 2 a través de la opción basada en explorador en la página 14), que permite configurar inicialmente el sistema a través del puerto de diagnóstico de iLO 2
- Asistente de instalación paso a paso HP BladeSystem Setup

Al seleccionar las ranuras p-Class en receptáculos con planos traseros de gestión actualizados que son compatibles con ranuras de alta densidad, el iLO 2 puede utilizarse para la configuración inicial de receptáculos con IP estática. La configuración inicial de la ranura en el compartimento 1 permite a todos los iLO 2 siguientes del receptáculo recibir asignaciones de IP estática predeterminadas. Esta función es compatible con dispositivos iLO 1.55 y posteriores.

ProLiant BL p-Class, requisitos de usuario

- Los usuarios deben tener el privilegio de Configure iLO 2 Settings (Configurar valores de iLO 2.)
- Una conexión de red con iLO 2 debe estar disponible y funcionar correctamente.

Configuración del compartimento con IP estática

La configuración del compartimento con IP estática se implementa a través de la opción Static IP Bay Settings (Configuración del compartimento de IP estática) de la ficha BL p-Class. Esta opción facilita la implementación inicial de un receptáculo completo o la implementación subsiguiente de los blades

del receptáculo existente. A pesar de que el método preferido para asignar direcciones IP a iLO 2 en cada servidor blade es mediante DHCP y DNS, estos protocolos no siempre están disponibles en redes que no sean de producción.

Por ejemplo, después de configurar los valores del compartimento de IP estática para la ranura en el compartimento 1, las siguientes adiciones de ranuras al receptáculo suponen las siguientes direcciones sin DHCP. Las direcciones de red se asignan por posición de ranura en compartimento 1: 192.168.1.1, en compartimento 2: 192.168.1.2, y así sucesivamente. La distribución de las siguientes ranuras no exige una configuración adicional y la dirección de red corresponde al número de compartimento.

La configuración del compartimento con IP estática automatiza el primer paso de la implementación del blade BL p-Class, al activar el procesador de gestión iLO 2 en cada ranura para obtener una dirección IP predefinida, sin depender de DHCP. Se podrá acceder inmediatamente a iLO 2 para la implementación del servidor mediante Virtual Media y otras funciones de administración remota.

La configuración del compartimento de IP estática utiliza el método de direccionamiento de configuración del compartimento de IP estática, que permite asignar direcciones IP a cada iLO 2 basándose en la ubicación de la ranura en el receptáculo del servidor respectivo. Al proporcionar un conjunto de direcciones IP al receptáculo, se obtiene la ventaja de una configuración del compartimento con IP estática sin que sea necesario configurar localmente cada iLO 2 individual.

Al utilizar la configuración iLO 2 del compartimento con IP estática:

- Se evitan costes de infraestructura DHCP para mantener el entorno del blade
- Se facilita la configuración con una generación automática de direcciones iLO 2 para todos los compartimentos o sólo para los seleccionados.

La configuración de compartimento con IP estática no es compatible con los receptáculos de ranura de la serie G1 BL. Para visualizar la generación de receptáculos, haga clic en **BL p-Class>Rack View (Vista de bastidor)>Details (Detalles)** para un receptáculo específico. La configuración del compartimento de IP estática no es compatible con el receptáculo cuando la opción Enclosure Type details (Detalles del tipo de receptáculo) muestra el mensaje `BL Enclosure G1`.

Cuando se vuelve a implementar una ranura, es posible que la configuración de compartimento de IP estática no se realice como se esperaba. Para solucionarlo, compruebe que la ranura esté utilizando el firmware iLO 2 actual y, a continuación, reinicie la configuración de iLO 2 a los valores predeterminados de fábrica utilizando la RBSU de iLO 2.

Configuración de receptáculo de ranura ProLiant BL p-Class

Para configurar un receptáculo de ranura BL p-Class utilizando un direccionamiento de compartimento con IP estática:

1. Instale un blade de servidor en el compartimento 1 del receptáculo BL p-Class. El blade de servidor no necesita configurarse o tener un sistema operativo instalado. El blade de servidor debe configurarse antes de instalar ranuras adicionales en el receptáculo.
2. Conecte un dispositivo cliente al puerto de la ranura del panel frontal iLO 2 con el cable de E/S local. El cable E/S local conecta con el puerto E/S en la parte frontal del blade de servidor. Esta conexión activa la IP estática 192.168.1.1 para la interfaz de Web iLO 2.
3. Configure el valor del receptáculo. Utilizando la interfaz de Web iLO 2, seleccione la ficha BL p-Class para acceder a Enclosure Static IP Settings (Valores de IP estática de receptáculo.) La ficha BL p-Class proporciona una interfaz de usuario para configurar el nivel del receptáculo de direcciones IP estáticas.

4. Seleccione una dirección IP inicial razonable con los últimos dígitos de la dirección correspondiente al número de compartimento de cada ranura, por ejemplo de 192.168.100.1 a 192.168.100.16, para crear un sistema numérico de fácil memorización.

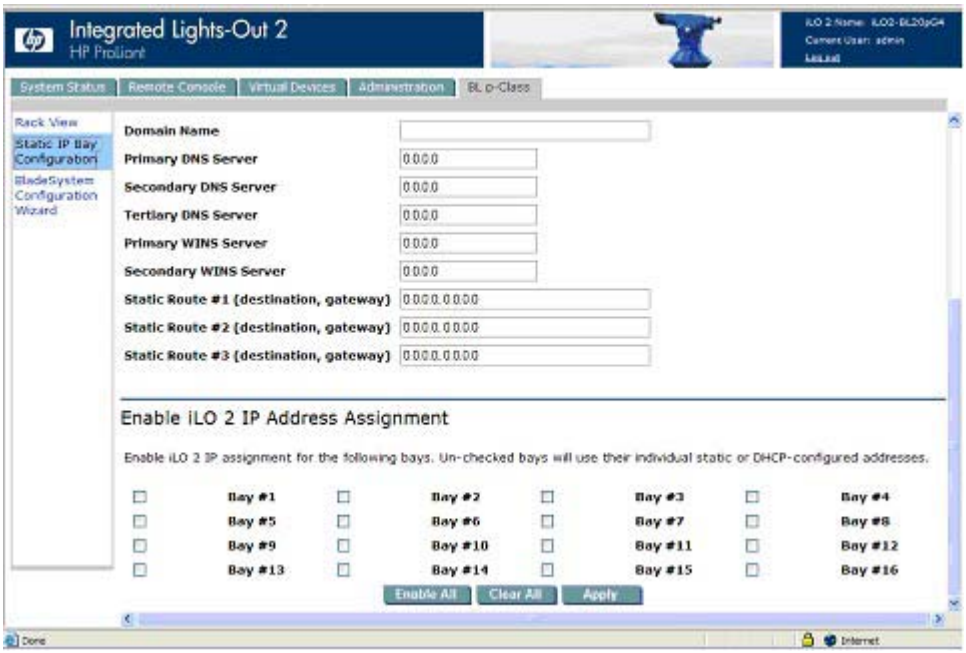
5. Reinicie el compartimento 1 si es necesario. La ranura del compartimento 1 sólo debe reiniciarse si desea que utilice una dirección de configuración de ranura con IP estática al marcar la activación de la máscara de función para el compartimento 1. Antes de reiniciar la ranura, vaya a la página del explorador Network Settings (Configuración de red), seleccione **Enable Static IP Settings (Activar valores de IP estática)** y haga clic en **Apply (Aplicar)** para obligar a la ranura a reiniciar y utilizar la nueva IP estática de receptáculo asignada.

Si múltiples receptáculos se implementan al mismo tiempo, se pude repetir fácilmente el proceso moviendo una única ranura al compartimento 1 de cada receptáculo para llevar a cabo la configuración.

Configuración de los valores del compartimento de IP estática

Los valores del compartimento de IP estática están disponibles en la ficha BL p-Class y le permiten configurar y distribuir el servidor con ranura. Al configurar estos valores, debe utilizar la ranura en el compartimento 1.

La casilla de verificación Enable Static IP Bay Configuration Settings (Activar los valores de configuración de la ranura con IP estática) disponible en la ficha Network Settings (Configuración de red), no mostrada, le permite activar o desactivar la configuración de la ranura de IP estática. La nueva opción Enable Static IP Bay Configuration Settings (Activar los valores de configuración de la ranura con IP estática) sólo está disponible en servidores blade. Al activar Static IP Bay Configuration (Configuración de ranura con IP estática), se desactivan todos los campos excepto iLO 2 Subsystem Name (Nombre de subsistema de iLO 2.) Sólo pueden activarse en una vez Static IP Bay Configuration o DHCP. Desactive las señales Static IP Bay Configuration (Configuración del compartimento con IP estática) y DHCP de iLO 2 para utilizar una dirección IP definida por el usuario. La opción Enable Static IP Bay Configuration Settings (Activar los valores de configuración de la ranura con IP estática) permanece desactivada si la infraestructura no admite Static IP Bay Configuration (Configuración de ranura con IP estática.)



Parámetros estándar de configuración de ProLiant BL p-Class

Beginning IP Address (Bay 1) (Dirección IP de inicio (Compartimento 1): asigna la dirección IP de inicio. Todas las direcciones IP deben ser direcciones válidas.

Ending IP Address (Bay 16) (Dirección IP de finalización (Compartimento 16)): asigna la dirección IP de finalización. Todas las direcciones IP deben ser direcciones válidas.

Subnet Mask (Máscara de subred): permite asignar la máscara de subred para la puerta de enlace predeterminada. Este campo debe completarse si Static IP Bay Configuration (Configuración de ranura con IP estática) o DHCP están configuradas. Todo el rango de la dirección IP debe ajustarse a la máscara de subred.

Gateway IP Address (Dirección IP de la puerta de enlace): permite asignar la dirección IP del router de red encargado de conectar la subred de Remote Insight con la subred en la que se encuentra el PC de gestión. Este campo debe completarse si Static IP Bay Configuration (Configuración de ranura con IP estática) o DHCP están configuradas.

Parámetros avanzados de configuración de ProLiant BL p-Class

Domain Name (Nombre de dominio): permite asignar el nombre de dominio en el que participará iLO 2.

Primary DNS Server (Servidor DNS primario): asigna una única dirección IP de servidor DNS en la red.

Secondary DNS Server (Servidor DNS secundario): asigna una única dirección IP de servidor DNS en la red.

Tertiary DNS Server (Servidor DNS terciario): asigna una única dirección IP de servidor DNS en la red.

Primary WINS Server (Servidor WINS primario): asigna una única dirección IP de servidor WINS en la red.

Secondary WINS Server (Servidor WINS secundario): asigna una única dirección IP de servidor WINS en la red.

Static Route #1, #2, and #3 (destination gateway) (Ruta estática 1, 2 y 3. Vía de acceso destino): asigna la ruta estática adecuada de la dirección IP de destino y vía de acceso en la red (los valores IP predeterminados son 0.0.0.0 y 0.0.0.0, donde la primera dirección IP corresponde a la IP destino y la segunda a la IP de la puerta de enlace.)

Activación de la asignación de direcciones IP de iLO 2

Las casillas de verificación de la ranura 1 a la 16 le permiten seleccionar qué servidores blade BL p-Class se configurarán. Puede habilitar todo, borrar todo o aplicar la selección.

HP BladeSystem Setup

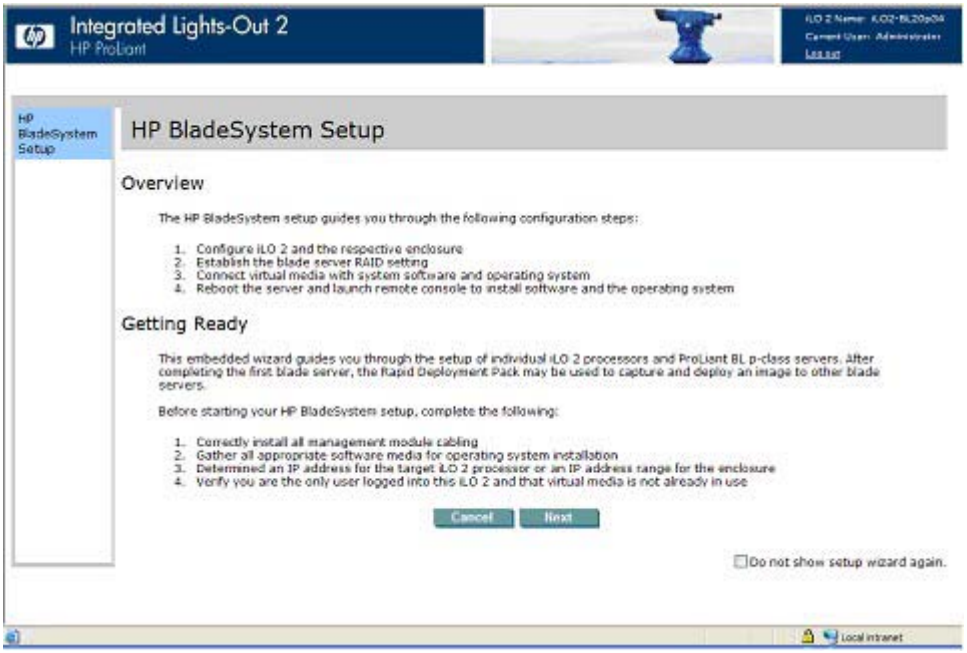
El asistente HP BladeSystem Setup proporciona instrucciones paso a paso para simplificar la configuración de una ranura individual sin necesidad de DHCP ni PXE. La página HP BladeSystem Setup se inicia cuando se haya autenticado con iLO 2 desde el puerto frontal.

El blade de servidor debe tener instalados los cables correctamente para la conectividad con iLO 2. Conéctese al blade de servidor a través del puerto E/S con la ranura en el bastidor. Este método requiere una conexión del cable E/S local al puerto E/S y a un equipo cliente. Utilizando la dirección IP estática que aparece en la etiqueta del cable de E/S y la información de acceso inicial en la parte frontal del blade de servidor, puede acceder al blade de servidor a través de su interfaz estándar para explorador Web.

Aunque se puede utilizar cualquier ranura para acceder, si se utiliza la configuración de dirección IP estática para configurar las opciones de red de la placa iLO 2, debe utilizarse la primera ranura del receptáculo para acceder.

La primera página del asistente se inicia de forma automática si:

- Se trata de una nueva ranura directamente de fábrica y ha iniciado una sesión en la placa iLO 2 desde el puerto frontal.
- No ha completado totalmente el asistente haciendo clic en **Finish (Finalizar)** en la última página, ni ha seleccionado **Do not show setup wizard again (No volver a mostrar el asistente de configuración)** ni ha hecho clic en **Cancel (Cancelar)** en la primera página.
- Ha configurado iLO 2 con los valores predeterminados de fábrica.



Haga clic en **Cancel (Cancelar)** para cerrar el asistente de configuración automatizado. Haga clic en **Next (Siguiente)** para configurar el servidor blade. El asistente de instalación le guiará a través de los siguientes procesos:

1. Configuración de iLO 2
2. Verificación de servidor RAID
3. Conexión de soportes virtuales
4. Instalación de software

Pantalla iLO 2 configuration (Configuración de iLO 2)

Esta pantalla permite cambiar los siguientes valores:

- Contraseña de administrador. HP recomienda cambiar la contraseña predeterminada.
- Valores de configuración de red Los siguientes valores son los predeterminados:
  - Enable DHCP (Activar DHCP): Yes (Sí)
  - Enable Static IP Bay Configuration (Activar la configuración de la ranura IP estática): No
- Si está conectada a la ranura 1 del receptáculo, puede habilitar la configuración de compartimento con IP estática a fin de preconfigurar la dirección estática de los demás procesadores iLO 2 del receptáculo.

En la configuración predeterminada, el iLO 2 actualizado obtiene su dirección IP mediante DHCP. Los demás procesadores iLO 2 del receptáculo deben configurarse de manera independiente. Si no se modifican estos valores, al hacer clic en **Next (Siguiente)**, aparece la siguiente página del asistente de configuración. Si se modifica alguno de estos valores, iLO 2 se reinicia para cargar los valores actualizados.

Las siguientes combinaciones de configuración también están disponibles (la configuración predeterminada está entre paréntesis):

- Enable DHCP (Yes) (Activar DHCP (Sí)) y Enable Static IP Bay Configuration (Yes) (Activar la configuración de la ranura IP estática (Sí))

  Esta configuración hace que iLO 2 se configure de modo que obtenga su dirección IP mediante DHCP. Al hacer clic en **Next (Siguiente)**, aparece la página Static IP Bay Configuration (Configuración de compartimento con IP estática), lo que le permitirá especificar las direcciones IP de los demás iLO 2 del receptáculo. Después de hacer clic en **Next (Siguiente)**, se le solicitará que confirme que desea utilizar DHCP para la dirección IP de iLO 2.

- Enable DHCP (No) (Activar DHCP (No)) y Enable Static IP Bay Configuration (Yes) (Activar la configuración de la ranura IP estática (Sí))

  Esta combinación hace que iLO 2 se configure para que su dirección IP se establezca según los valores especificados mediante la configuración de compartimento con IP estática. Al hacer clic en **Next (Siguiente)**, aparece la página Static IP Bay Configuration (Configuración de compartimento con IP estática.)

- Enable DHCP (No) (Activar DHCP (No)) y Enable Static IP Bay Configuration (No) (Activar la configuración de la ranura IP estática (No))

  Esta combinación hace que iLO 2 se configure para que su dirección IP se establezca según los valores especificados mediante la página Network Settings (Configuración de red.) Al hacer clic en **Next (Siguiente)** aparece la página Network Settings (Configuración de red.)

Para guardar cambios en la red deberá tener el privilegio Configure iLO 2 (Configurar iLO 2.)

Haga clic en **Next (Siguiente)** para guardar los cambios y continuar.

Pantalla Verify Server RAID Configuration (Verificar configuración de servidor RAID)

Este paso del asistente de instalación le permitirá verificar y aceptar los valores de configuración RAID del servidor. Verifique el nivel de RAID detectado en los discos duros del servidor blade mostrado en la página Web y realice los pasos siguientes:

- Haga clic en **Next (Siguiente)** para mantener los valores de RAID actuales.
- Haga clic en **Default Setting (Configuración predeterminada)** para configurar automáticamente el nivel RAID basándose en el número de unidades instaladas. Se le solicitará que confirme si desea restablecer el nivel RAID, dado que esta acción podría provocar una pérdida de datos. Restablecer el nivel RAID exige reiniciar o encender el servidor. iLO 2 muestra una página que indica que se está produciendo esta acción. La página se actualizará automáticamente cada 10 segundos. Tras el reinicio del servidor, se mostrará de nuevo la siguiente página del asistente de instalación. Si se produce un error durante el proceso de restablecimiento de RAID, la página de configuración de RAID se volverá a mostrar con datos del error. Es más probable que se produzca un error, si el servidor está en POST. Si es el caso, salga de cualquier programa de RBSU en ejecución, permita que se complete la POST e intente la operación de nuevo.

Puede cambiar el nivel RAID manualmente mediante RBSU. Si el sistema operativo ya está instalado, modificar el nivel RAID provoca una pérdida de datos.

Pantalla Connect Virtual Media (Conectar soporte virtual)

Este paso del asistente de instalación le permitirá verificar y aceptar la unidad que desee utilizar durante la instalación del sistema operativo. En Settings (Configuración), seleccione la unidad local y el tipo de soporte que desee utilizar durante la instalación del sistema operativo. Haga clic en **Launch Virtual Media (Iniciar soporte virtual)** para iniciar el subprograma Virtual Media (Soporte virtual.)

- Compruebe que el soporte del sistema operativo esté conectado. En el subprograma Virtual Media (Soporte virtual), aparece un icono verde junto al soporte seleccionado en ese momento.
- Compruebe que el soporte del sistema operativo se encuentre en la unidad local pertinente.
- Acepte los certificados de seguridad a medida que aparezcan.

Cuando haya terminado de configurar las opciones, haga clic en **Next (Siguiente)** para guardar los valores y continuar. Aparece el subprograma Virtual Media (Soporte virtual.) Una vez disponible el subprograma, puede cambiar la unidad seleccionada o elegir otras opciones no disponibles en la página del asistente de instalación.

Pantalla Install Software (Instalar software)

Este paso del asistente de instalación permite iniciar la consola remota e instalar el sistema operativo. Para iniciar el proceso de instalación del sistema operativo:

- Haga clic en **Launch Software Installation (Iniciar instalación de software)** para iniciar la consola remota. iLO 2 iniciará automáticamente un encendido o reinicio del servidor para iniciar la instalación del sistema operativo mediante el soporte virtual seleccionado anteriormente.
- Acepte los certificados de seguridad a medida que aparezcan.

Haga clic en **Finish (Finalizar)** para completar el proceso de configuración.

Parámetros de configuración del puerto de diagnóstico de iLO 2

El puerto de diagnóstico de iLO 2, situado delante de los servidores ProLiant BL p-Class le permite acceder y solucionar problemas del servidor mediante un cable de diagnóstico. El puerto de diagnóstico de iLO 2 utiliza una dirección IP estática. No utilizará DHCP para obtener una dirección IP, registrarse con WINS o DNS dinámico ni utilizar una vía de acceso. El cable del puerto de diagnóstico no se debe

dejar conectado sin una conexión de red activa, ya que puede deteriorar el rendimiento de red en el puerto de red de iLO 2 estándar.

En Network Settings (Configuración de red) puede configurar información de puerto de diagnóstico específica. Para obtener más información acerca de cómo utilizar el puerto y el cable de diagnóstico, consulte la Guía de instalación y Configuración del servidor blade.

A continuación se muestran los campos que pueden configurarse para el puerto de diagnóstico:

- Enable NIC (Activar la NIC)

  Si el valor de Enable NIC es Yes (Sí), el puerto de diagnóstico está activado.

- Transceiver Speed Autoselect (Selección automática de la velocidad del transceptor)
- Velocidad
- Duplex (dúplex)
- IP Address (Dirección IP)

  Utilice este parámetro para asignar una dirección IP estática a iLO 2 en la red. De manera predeterminada, DHCP se encarga de asignar la dirección IP. De manera predeterminada, la dirección IP es 192.168.1.1, para todos los puertos de diagnóstico de la placa iLO 2.

- Subnet Mask (máscara de subred)
  - Use el parámetro de máscara de subred para asignar la máscara de subred al puerto de diagnóstico de iLO 2. De manera predeterminada, la máscara de subred es 255.255.255.0 para todos los puertos de diagnóstico de la placa iLO 2.
  - El uso del puerto de diagnóstico se detecta automáticamente cuando se conecta un cable de una red activa. Al cambiar entre los puertos de diagnóstico y los de la parte posterior, tiene que dejar 90 segundos para que se complete el cambio de red antes de intentar la conexión a través del explorador Web.

    NOTA: El puerto de diagnóstico no cambiará si hay una sesión de consola remota activa o una actualización de firmware en curso.

4 Utilización de iLO 2

En esta sección:

Información sobre el estado del sistema y el resumen de estado

Al acceder a iLO 2 por primera vez, la interfaz abre la página Status Summary (Resumen de estado) que contiene información sobre el estado del sistema y el resumen de estado y permite acceder a la información de estado, a los registros del sistema y a la información sobre Insight Agent. Las opciones disponibles en la sección System Status (Estado del sistema) son: Summary (Resumen), System Information (Información del sistema), iLO 2 Log (Registro iLO 2), IML (IML), Diagnostics (Diagnóstico), iLO 2 User Tips (Consejos de usuario de iLO 2) e Insight Agents (Agentes Insight.)

En la página Status Summary (Resumen de estado) aparecen detalles de nivel superior sobre el sistema y el subsistema iLO 2, así como enlaces a las funciones utilizadas de forma más habitual. Para acceder a la página Status Summary (Resumen de estado) desde otras áreas de la interfaz iLO 2, haga clic en **System Status (Estado del sistema)>Summary (Resumen)**.

La información de estado incluye:

- Server Name (Nombre del servidor): permite visualizar el nombre del servidor y constituye un enlace con Administration (Administración)>Options (Opciones)>Access (Acceso.)
- UUID: permite visualizar el ID del servidor.
- Server Serial Number/Product ID (Número de serie/ID de producto del servidor): indica el número de serie que el servidor tiene asignado de fábrica. Puede cambiar este valor de configuración mediante la RBSU del sistema durante POST. El ID del producto distingue entre diferentes sistemas con números de serie similares. Aunque la identificación de producto se asigna en el momento de la fabricación del sistema, este valor se puede cambiar mediante la RBSU del sistema durante POST.
- System ROM (ROM del sistema): muestra la familia y la versión del sistema ROM activo. Si el sistema admite una memoria ROM del sistema de copia de seguridad, también aparece la fecha de la copia de seguridad.
- System Health (Estado del sistema): resume el estado de los subsistemas supervisados, incluido el estado total y la redundancia (capacidad de controlar un fallo) y constituye un enlace con System (Sistema)>Status (Estado)>System Information Summary (Resumen de información del sistema.)
- Internal Health LED (LED de estado interno): representa el indicador del estado interno del servidor (si se admite.) Resume los problemas con ventiladores, sensores de temperatura, VRM y otros subsistemas supervisados del servidor. Si desea obtener más información, consulte "Resumen de información del sistema (Resumen de información del sistema en la página 83)".
- TPM Status (Estado de TPM): permite visualizar la configuración del estado de TPM. Si el sistema host o la ROM del sistema no admite TPM, el estado de TPM no se visualizará en la página Status Summary (Resumen de estado.) Si desea obtener más información, consulte "Compatibilidad del módulo de plataforma segura".
- Server Power (Alimentación de servidor): permite visualizar el estado de alimentación actual del servidor (ON/STANDBY) cuando se ha cargado la página y constituye un enlace con Server (Servidor)>Power Management (Gestión de alimentación.) Los usuarios con el privilegio Virtual Power and Reset (Alimentación y reinicio virtuales) también pueden utilizar el botón Momentary Press (Pulsar momentáneamente.)
- UID Light (Luz de UID): permite visualizar el estado de la luz de UID cuando se ha cargado la página. Puede controlar el estado de UID utilizando el botón Turn UID On (Encender UID) además de los botones UID físicos del chasis del servidor.

  El UID le ayuda a identificar y ubicar un sistema, especialmente en entornos de bastidores de alta densidad. Además, el UID indica que hay una operación crítica en proceso en el host, como el acceso de la consola remota o una actualización de firmware.

  △ **PRECAUCIÓN:** No elimine la alimentación de un servidor mientras su UID parpadea.

  El estado actual del UID (encendido o apagado) es el último estado seleccionado mediante uno de estos métodos. Si se selecciona un estado nuevo mientras el UID está parpadeando, este estado nuevo se convierte en el estado actual y da resultado cuando el UID deja de parpadear. Mientras el UID está parpadeando, su estado actual se muestra junto con el parpadeo de la ficha. Cuando el UID deja de parpadear, la ficha se elimina.

  El UID no se admite en HP ProLiant ML310 G3.
- Last Used Remote Console (Última consola remota usada): muestra la consola remota iniciada anteriormente y su disponibilidad, lo que le permite al usuario iniciar rápidamente su consola remota preferida. Puede utilizar la consola remota si está disponible y si dispone del privilegio de

usuario adecuado. Puede seleccionar otra consola siguiendo el enlace Last Used Remote Console (Última consola remota usada.)

- Latest IML Entry (Última entrada IML): permite visualizar la entrada más reciente efectuada en el IML.
- iLO 2 Name (Nombre de iLO 2): permite visualizar el nombre que se encuentra asignado al subsistema iLO 2. De manera predeterminada, es la palabra iLO añadida al número de serie del sistema. Este valor se utiliza para el nombre de red y debe ser único.
- License Type (Tipo de licencia): permite visualizar si desea que el sistema disponga de una licencia de funciones instalada y que constituya un enlace a Administration (Administración)>Licensing (Concesión de licencias.) No se puede acceder a algunas funciones de iLO 2 a menos que tengan una licencia.
- iLO 2 Firmware Version (Versión del firmware de iLO 2): muestra información sobre la versión del firmware de iLO 2 instalado en este momento y constituye un enlace a la página iLO 2 Release Notes (Notas de versión de iLO 2) que destaca las nuevas capacidades de la versión actual del firmware y en las versiones anteriores seleccionadas
- IP Address (Dirección IP): permite visualizar la dirección IP de red del subsistema iLO 2 y constituye un enlace con Administration (Administración)>Network Settings (Configuración de red.)
- Active Sessions (Sesiones activas): permite visualizar todos los usuarios que se encuentran conectados actualmente a iLO 2.
- Latest iLO 2 Event Log Entry (Última entrada en el registro de sucesos de iLO 2): muestra la entrada más reciente en el registro de sucesos de iLO 2.
- iLO 2 Date (Fecha de iLO 2): muestra la fecha (MM/DD/AAAA) que se indica en el calendario interno del subsistema de iLO 2. El calendario interno de iLO 2 se sincroniza con el sistema host en POST y en el momento en que se ejecutan Insight Agents.
- iLO 2Date/Time (Fecha/hora de iLO 2): permite visualizar el reloj interno del subsistema iLO 2. El reloj interno de iLO 2 se sincroniza con el sistema host en POST y en el momento en que se ejecutan Insight Agents.

Resumen de información del sistema

System Information (información del sistema) muestra el estado del sistema bajo seguimiento. Muchas de las funciones necesarias para operar y gestionar los componentes del servidor HP Proliant se han pasado del controlador de estado al microprocesador de iLO 2. Estas funciones están disponibles sin necesidad de instalar y cargar el controlador de estado del sistema operativo instalado. El microprocesador de iLO 2 controla estos dispositivos cuando el servidor se enciende durante el reinicio del servidor, la inicialización del sistema operativo y el funcionamiento. El control se prolonga durante un fallo inesperado en el sistema operativo. Para acceder a System Information (Información del sistema), haga clic en **System Status (Estado del sistema)>System Information (Información del sistema)**. Aparecerá la ficha System Health Summary (Resumen de estado del sistema.) En System Information (Información del sistema) también aparecen las siguientes fichas de estado integradas: Fans (Ventiladores) (Ventiladores en la página 84), Temperatures (Temperaturas) (Temperaturas en la página 85), Power (Alimentación) (Power en la página 85), Processors (Procesadores) (Procesadores en la página 86), Memory (Memoria) (Memoria en la página 86) y NIC (NIC en la página 86.)

La ficha Summary (Resumen) muestra el estado de los subsistemas de la plataforma host supervisados de un vistazo, resumiendo la condición de los subsistemas supervisados, incluido el estado general y

la redundancia (capacidad de controlar un fallo.) Los subsistemas pueden incluir ventiladores, sensores de temperatura, fuentes de alimentación y módulos reguladores de tensión.

- Fans (Ventiladores): muestra el estado de los ventiladores reemplazables dentro del chasis del servidor. Estos datos incluyen el área que enfría cada ventilador y las velocidades actuales de estos.
- Temperatures (Temperaturas): muestra las condiciones de temperatura que se controla a través de sensores situados en distintos puntos dentro del chasis del servidor, así como la temperatura del procesador. La temperatura está supervisada para mantener la temperatura de la ubicación bajo el umbral de precaución. Si la temperatura supera el umbral de precaución, la velocidad del ventilador se aumenta al máximo.
- VRMs (VRM): permite visualizar el estado de los VRM. Se necesita un VRM por cada procesador que tenga el sistema. El VRM ajusta la alimentación necesaria para satisfacer los requisitos de alimentación del procesador respaldado. Un VRM fallido impide que el procesador sea respaldado y, por tanto, debería sustituirse.
- Power Supplies (Fuentes de alimentación): permite visualizar la presencia y estado de las fuentes de alimentación instaladas.
  - OK (Adecuado): indica que la fuente de alimentación está instalada y operativa.
  - Unpowered (Sin alimentación): indica que la fuente de alimentación está instalada pero no operativa. Compruebe que el cable de alimentación está enchufado.
  - Not present (No presente): indica que el suministro de alimentación no se encuentra instalado. En esta condición, la alimentación no es redundante.
  - Failed (Fallo): indica que se debería reemplazar la fuente de alimentación.

Para acceder a la ficha Summary (Resumen) desde otras áreas de la interfaz iLO 2, haga clic en **System Status (Estado del sistema)>System Information (Información del sistema)>Summary (Resumen)**.

Ventiladores

iLO 2, junto con el hardware adicional, controla el funcionamiento y velocidad de los ventiladores. Los ventiladores proporcionan el enfriamiento esencial de los componentes para asegurar la fiabilidad y un correcto funcionamiento. La ubicación, colocación, diseño y control de velocidad de los ventiladores tienen en cuenta diversas temperaturas controladas en todo el sistema para ofrecer un enfriamiento adecuado con niveles mínimos de ruido.

Las directrices de funcionamiento difieren de un servidor a otro dependiendo de la configuración de los ventiladores y los requisitos de ventilación. El control de los ventiladores tiene en cuenta la temperatura interna del sistema, aumentando la velocidad de los ventiladores para proporcionar más enfriamiento y reduciendo dicha velocidad si el enfriamiento es suficiente. En el improbable caso de que un ventilador fallase, algunas directrices de funcionamiento de ventiladores podrían aumentar la velocidad de los otros ventiladores, registrar el evento en el IML y encender los indicadores LED.

La supervisión del subsistema de ventiladores incluye configuraciones de suficiencia, redundancia y no redundancia de los ventiladores. El fallo de un ventilador es un suceso aislado, pero para garantizar la fiabilidad y el tiempo de funcionamiento, los servidores ProLiant disponen de configuraciones redundantes de ventiladores. En los servidores ProLiant que admiten configuraciones de redundancia, uno o varios ventiladores podrían fallar y ofrecer, aún así, un enfriamiento suficiente para poder continuar con el funcionamiento. iLO 2 aumenta el control de los ventiladores para mantener un funcionamiento seguro del servidor en caso del fallo de un ventilador, operaciones de mantenimiento o cualquier otro evento que altere el enfriamiento del servidor.

En las configuraciones no redundantes o en las configuraciones redundantes donde tiene lugar el fallo de varios ventiladores, el sistema podría ser incapaz de ofrecer el enfriamiento necesario para proteger el sistema del daño y asegurar la integridad de los datos. Bajo esta condición, además de las directrices de enfriamiento, el sistema podría comenzar un apagado adecuado del sistema operativo y del servidor.

La ficha Fan (Ventilador) muestra el estado de los ventiladores reemplazables dentro del chasis del servidor. Estos datos incluyen el área que enfría cada ventilador y la velocidad actual del ventilador.

Temperaturas

La ficha Temperaturas (Temperaturas) muestra el valor de umbral, ubicación, estado y temperatura de los sensores de temperatura del chasis del servidor. La temperatura está supervisada para mantener la temperatura de la ubicación bajo el umbral de precaución. Si uno o varios sensores exceden este umbral, iLO 2 implementa la directriz de recuperación para impedir el daño de los componentes del servidor.

- Si la temperatura supera el umbral de precaución, la velocidad del ventilador se aumenta al máximo.
- Si la temperatura supera la temperatura crítica, se lleva a cabo un apagado adecuado del servidor.
- Si la temperatura supera el umbral de gravedad, el servidor se apaga inmediatamente para impedir daños permanentes.

Las directrices de supervisión difieren dependiendo de los requisitos del servidor. Las directrices incluyen, por lo general, el aumento de la velocidad de los ventiladores para un enfriamiento máximo, el registro del evento de temperatura en el registro IML, la indicación visual del evento mediante los indicadores LED y el comienzo de un apagado adecuado del sistema operativo para evitar daños en los datos.

Tras corregir las condiciones de exceso de temperatura, se implementan directrices adicionales entre las que se incluyen el devolver la velocidad normal del ventilador" registro del evento en el IML, apagado de los indicadores LED y, si es apropiado, cancelar los apagados que hayan en progreso.

Power

La ficha VRMs/Power Supplies (Fuentes de alimentación) muestra el estado de todos los VRM o fuentes de alimentación. Se necesita un VRM por cada procesador que tenga el sistema. Los VRM ajustan la alimentación necesaria para satisfacer los requisitos de alimentación del procesador respaldado. Un VRM se puede sustituir si falla. Un VRM que falla impide que el procesador sea respaldado.

iLO 2 también supervisa las fuentes de alimentación del sistema para garantizar un tiempo de funcionamiento máximo del servidor y del sistema operativo. Las fuentes de alimentación pueden verse afectadas por las bajadas de tensión u otras condiciones eléctricas, o porque se desenchufe un cable de CA de manera accidental. Estas condiciones resultan en una pérdida de redundancia si se configuran fuentes de alimentación redundantes o resultan en una pérdida de funcionamiento si no están en uso las fuentes de alimentación redundantes. De manera adicional, en caso de que se detectase un fallo en la fuente de alimentación (fallo de hardware) o que se desenchufe un cable de alimentación de CA, se registran los eventos pertinentes en el IML y se utilizan los indicadores LED.

iLO 2 supervisa las fuentes de alimentación para asegurar que estén instaladas correctamente. Esta información se muestra en la página System Information (información del sistema.) Revisar la página System Information (información del sistema) y el IML le ayudarán a decidir cuándo reparar o sustituir una fuente de alimentación, impidiendo una interrupción en el servicio.

Procesadores

La ficha Processors (Procesadores) muestra las ranuras disponibles para procesadores, el tipo de procesador instalado en la ranura y un breve resumen de estado del subsistema de procesadores Si están disponibles, se mostrarán la velocidad del procesador instalado en MHz y la capacidad de caché.

Memoria

La ficha Memory (Memoria) muestra las ranuras de memoria disponibles y el tipo de memoria instalada en la ranura, en su caso.

NIC

La ficha NIC muestra las direcciones MAC de las NIC integradas. Esta página no muestra adaptadores de red adicionales.

Registro de iLO 2

La página iLO 2 Log (Registro de iLO 2) muestra el registro de sucesos de iLO 2, un registro de los sucesos importantes detectados por iLO 2. Los sucesos registrados incluyen sucesos de servidor importantes, tales como un corte en el suministro de alimentación del servidor o un reinicio del servidor y sucesos de iLO 2 tales como intentos de inicio de sesión no autorizados. Entre los otros sucesos registrados se incluyen los inicios de sesión correctos o incorrectos en el explorador y en la consola remota, alimentación virtual y sucesos de apagado y encendido, acciones de vaciar registro de sucesos y algunos cambios de configuración, tales como crear o eliminar un usuario.

iLO 2 proporciona una codificación segura por contraseña, realizando un seguimiento de todos los inicios de sesión y manteniendo un registro de todos los errores que se produzcan durante el mismo. Authentication Failure Logging (Registro con fallo de autenticación) permite configurar los criterios de registro de las autenticaciones erróneas. Es posible configurar el seguimiento de los intentos fallidos de autenticación para cada intento o para cada dos, tres o cinco intentos, y capturar el nombre del cliente de cada entrada registrada con el fin de mejorar las capacidades de asistencia en entornos DHCP, así como el registro del nombre de cuenta, el nombre del ordenador y la dirección IP. Si los intentos de inicio de sesión fallan, iLO 2 también genera avisos y los envía a una consola de gestión remota.

Es posible que las versiones del firmware anteriores no admitan los sucesos registrados por versiones posteriores del firmware de iLO 2. Si un firmware incompatible registra un suceso, éste se muestra como `UNKNOWN EVENT TYPE (Tipo de suceso desconocido)`. Puede borrar el registro de sucesos para eliminar esas entradas o para actualizar el firmware a la última versión admitida.

Para acceder al registro de iLO 2 Log, haga clic en **System Status (Estado del sistema)>iLO 2 Log (Registro de iLO 2)**.

Para vaciar el registro de sucesos:

1. Haga clic en **Clear Event Log (Vaciar registro de sucesos)** para eliminar toda la información almacenada en el registro de sucesos.
2. Haga clic en **OK (Aceptar)** para confirmar que desea vaciar el registro de sucesos. Se registrará una línea indicando que el registro se vació.

RGL

La página IML muestra el Integrated Management Log (Registro de gestión integrada), un registro de sucesos históricos que han sucedido en el servidor registrados por varios componentes de software. Los sucesos son generados por el ROM del sistema y por servicios como el controlador de gestión de sistemas (de estado.) El IML le permite ver los sucesos registrados del servidor remoto. En los sucesos

registrados se incluyen todos los sucesos específicos del servidor registrados por el controlador de estado del sistema, incluida la información del sistema operativo y los códigos POST basados en la ROM. Para obtener más información, consulte la guía del servidor.

Las entradas de IML pueden ayudar en el diagnóstico de problemas o facilitar la identificación de posibles problemas antes de que se produzcan. Para evitar una posible interrupción del servicio, se recomienda realizar una acción preventiva. iLO 2 gestiona el IML, al que puede accederse mediante un explorador admitido, incluso cuando el servidor está apagado. El hecho de poder ver el registro de eventos incluso cuando el servidor está apagado puede ser útil para solucionar problemas del servidor host remoto.

Puede ordenar el registro haciendo clic en el encabezado de cualquier columna de datos. Una vez ordenado, haciendo clic otra vez en el mismo encabezado de columna se invierte el orden del registro. Los registros muy grandes tardan varios minutos en ordenarse y mostrarse. Puede borrar los eventos de este registro en la página principal del servidor Insight Manager Web Agents (Agentes Web de Insight Manager.)

El procesador iLO 2 registra la siguiente información en el IML basándose en los acontecimientos del sistema.

- Ventilador insertado
- Ventilador extraído
- Fallo del ventilador
- Ventilador degradado
- Ventilador reparado
- Pérdida de redundancia del ventilador
- Ventiladores redundantes
- Fuente de alimentación introducida
- Fuente de alimentación extraída
- Error de alimentación
- Pérdida de redundancia de las fuentes de alimentación
- Fuentes de alimentación redundantes
- Temperatura superior al umbral
- Temperatura normal
- Cierre automático iniciado
- Cierre automático cancelado

Diagnóstico

La opción Diagnostics (Diagnósticos) de la ficha System Status (Estado del sistema) muestra la pantalla Server and iLO 2 Diagnostics (Diagnóstico de iLO 2 y servidor.) En la pantalla Server and iLO 2 Diagnostic (Diagnóstico de iLO 2 y servidor) se muestran los resultados de la autocomprobación de iLO 2 y se ofrecen opciones para generar un NMI en el sistema y para reiniciar iLO 2.

NOTA: Cuando está conectado a través del puerto de diagnóstico, el servidor del directorio no está disponible. Sólo puede iniciar la sesión utilizando una cuenta local.

En la página Diagnostics (Diagnósticos) se incluyen las secciones siguientes:

- Botón Non-Maskable Interrupt (NMI) (Interrupción no enmascarable)

  La sección del botón Non-Maskable Interrupt (NMI) (Interrupción no enmascarable) contiene el botón Generate NMI to System (Generar NMI en el sistema) que permite detener la depuración del sistema operativo. Esta es una función avanzada y sólo debe utilizarse para la depuración de nivel de kernel. Los posibles usos de la función Generate NMI to System (Generar NMI en el sistema) incluyen lo siguiente:

  - Utilice la función Demonstrate ASR (Demostrar ASR) sólo si el controlador de gestión de sistemas (de estado) está cargado y ASR está desactivado. El host se reinicia automáticamente después de que se produzca un NMI.
  - Utilice la función Debug (Depurar) si una aplicación de software suspende el sistema. El botón Generate NMI to System (Generar NMI en el sistema) puede utilizarse para llamar al depurador del sistema operativo.
  - Inicie el volcado de un host que no responda si desea capturar el contexto del servidor.

    Se requiere el privilegio Virtual Power and Reset (Alimentación y reinicio virtuales) para generar un NMI. Un NMI inesperado normalmente señala un estado grave en la plataforma host. Cuando se recibe un NMI inesperado por el sistema operativo de host, aparece una terminación anormal, un error crítico, una pantalla azul u otras excepciones graves, incluso si el sistema operativo no responde o está bloqueado. La generación de un NMI inesperado puede utilizarse para diagnosticar un sistema operativo bloqueado. La generación de un NMI bloquea el sistema operativo, provocando pérdida de datos y del servicio.

    La generación de un NMI sólo debería utilizarse en casos de diagnósticos extremos en los que el sistema operativo no funcionara correctamente y un equipo de asistencia con experiencia ha recomendado proceder con un NMI. La generación de un NMI como herramienta de diagnóstico y depuración se utiliza principalmente cuando el sistema operativo ya no está disponible. La generación de un NMI no debe usarse durante el funcionamiento normal del servidor. El botón Generate NMI to System (Generar NMI en el sistema) no permite cerrar ordenadamente el sistema operativo.

- Resultados de la autocomprobación de iLO 2

  En la sección iLO 2 Self-Test Results (Resultados de la autocomprobación de iLO 2) se muestran los resultados de los diagnósticos internos de iLO 2. iLO 2 lleva a cabo una serie de procedimientos de inicialización y diagnóstico en los subsistemas del sistema iLO 2. Los resultados se muestran en la pantalla Server and iLO 2 Diagnostics (Diagnóstico de iLO 2 y servidor.) Todos los subsistemas comprobados deben mostrar Passed (Correcto) en circunstancias normales. Para cada prueba se muestra uno de los tres resultados siguientes: Passed (Correcto), Fault (Incorrecto), o N/A (No disponible.)

  El estado de estas autocomprobaciones es indicado por los resultados de la prueba e intenta identificar las áreas con problemas. Si el resultado de la prueba es Fault (Incorrecto), siga cualquier información que aparezca en la pantalla. Las pruebas específicas que se ejecutan dependen del sistema. No todas las pruebas se ejecutan en todos los sistemas. Consulte la página iLO 2 Diagnostics (Diagnóstico de iLO 2) para comprobar las pruebas que se han realizado automáticamente en el sistema.

- Reset Integrated Lights-Out 2 (Reiniciar Integrated lights-Out 2)

  La sección Reset Integrated Lights-Out 2 (Reiniciar Integrated Lights-Out 2) contiene el botón Reset (Reiniciar) que permite volver a iniciar el procesador de iLO 2. El uso de Reset (Reiniciar) no implica ningún cambio en la configuración. Al reiniciar, se desconecta cualquier conexión activa en iLO 2 y se finalizan todas las actualizaciones que se estén llevando a cabo en el firmware. Debe

tener el privilegio Configure iLO 2 (Configurar los ajustes de los dispositivos locales) para reiniciar iLO 2 utilizando esta opción.

Insight Agents

Los agentes de HP Insight Manager admiten una interfaz de explorador para el acceso a los datos de gestión en tiempo de ejecución a través de HP System Management Homepage. HP System Management Homepage es una interfaz segura basada en Web que consolida y simplifica la gestión de servidores y sistemas operativos individuales. Al agregar datos de agentes de HP Insight Manager y otras herramientas de gestión, System Management Homepage proporciona una interfaz intuitiva para revisar en profundidad la configuración del hardware y los datos de estado, las medidas de rendimiento, los umbrales del sistema y la información de control de la versión de software.

Los agentes pueden proporcionar automáticamente el enlace a iLO 2 o puede entrar manualmente en el enlace mediante Administration (Administración)/Management (Gestión.)

Para obtener más información, consulte "HP Systems Insight Manager integration" (Integración de HP Systems Insight Manager) y la página Web de HP (http://www.hp.com/servers/manage.)

iLO 2 Remote Console

iLO 2 Remote Console redirige la consola del servidor host al explorador del cliente de red y proporciona acceso de texto completo (estándar), vídeo de modo gráfico, teclado y ratón al servidor de host remoto (si dispone de licencia.) iLO 2 utiliza una tecnología de teclado, vídeo y ratón (KVM, keyboard, video, mouse) virtual para mejorar el rendimiento de la consola remota comparado con otras soluciones de KVM.

Con el acceso a la consola remota podrá ver los mensajes de arranque de POST al mismo tiempo que se reinicia el servidor host remoto y podrá dar comienzo a rutinas de configuración basadas en ROM para configurar el hardware del servidor host remoto. Cuando instale de forma remota sistemas operativos, las consolas remotas gráficas (si dispone de licencia) le permitirán ver y controlar las pantallas del servidor host sin interrupciones durante todo el proceso de instalación.

El acceso a la consola remota le proporciona un control absoluto sobre el servidor host remoto como si estuviera delante del sistema, incluido el acceso al sistema de archivos y a las unidades de red remotos. La consola remota permite cambiar los valores de configuración del hardware y software del servidor host remoto, instalar aplicaciones y controladores, cambiar la resolución de pantalla del servidor remoto y cerrar sin problemas el sistema remoto.

En iLO 2 se pueden registrar simultáneamente hasta 10 usuarios. Sin embargo, sólo cuatro usuarios pueden acceder a una consola remota integrada compartida. Si trata de abrir la consola remota cuando está en uso, aparecerá un mensaje de advertencia indicando que la está utilizando otro usuario. Para ver la sesión de la consola remota en curso, consulte la sección "Consola remota compartida" (Consola remota compartida en la página 100) para obtener más información. Para controlar la sesión, utilice la función Remote Console Acquire (Adquisición de consola remota.) Para obtener más información, consulte la sección "Adquisición de la consola remota (Adquisición de la consola remota en la página 104)".

Desde la página Remote Console Information (Información sobre la consola remota) se puede acceder a enlaces a distintas opciones de acceso a la consola remota. Una vez decidida la opción de consola

que desea utilizar, haga clic en el enlace pertinente. iLO 2 proporciona las opciones siguientes de acceso a la consola remota:

- Integrated Remote Console (Consola remota integrada) (Opción de Consola remota integrada en la página 96): permite acceder al KVM del sistema y controlar Virtual Power (Alimentación virtual) y Virtual Media (Soporte virtual) desde una misma consola con el uso de Microsoft® Internet Explorer.
- Integrated Remote Console Fullscreen (Pantalla completa de la consola remota integrada) (Pantalla completa de IRC en la página 95): permite cambiar el tamaño de la consola remota integrada a la misma resolución de visualización que la del host remoto.

  Las opciones Integrated Remote Console (Consola remota integrada) e Integrated Remote Console Fullscreen (Pantalla completa de la consola remota integrada) utilizan ActiveX y requieren Microsoft® Internet Explorer™.
- Remote Console (Consola remota) (Consola remota en la página 105): permite acceder al KVM del sistema a través de una consola basada en el subprograma Java. La consola remota es el soporte de consola remota familiar desarrollado a partir del producto iLO original. La compatibilidad de Remote Console (Consola remota) requiere que Java™ esté instalado en el sistema cliente. La opción Remote Console (Consola remota) funciona con todos los sistemas operativos y exploradores compatibles con iLO 2.
- Remote Serial Console (Consola remota de serie) (Consola remota de serie en la página 113): permite acceder a una consola de serie VT320 desde una consola basada en un subprograma de Java conectada al puerto serie virtual de iLO 2. La consola remota de serie está disponible sin una licencia adicional y es adecuada para sistemas operativos host que no requieren acceso a la consola gráfica.

iLO 2 Standard proporciona acceso de consola de servidor desde el encendido del servidor hasta POST. Las opciones Integrated Remote Console (Consola remota integrada), Integrated Remote Console Fullscreen (Pantalla completa de la consola remota integrada) y Remote Console (Consola remota) son consolas remotas gráficas que convierten un explorador compatible en un escritorio virtual y le permiten controlar totalmente la pantalla, el teclado y el ratón del servidor host. La consola independiente del sistema operativo admite los modos gráficos que muestran actividades del servidor host remoto, como las operaciones de inicio y cierre (si dispone de licencia.)

El acceso de la consola remota al servidor host después del proceso POST del servidor es una función con licencia disponible con la adquisición de licencias opcionales. Si desea obtener más información, consulte "Concesión de licencias (Concesión de licencias en la página 21)". Para acceder a iLO 2 Remote Console, haga clic en **Remote Console (Consola remota)**. Aparecerá la página Remote Console Information (Información sobre la consola remota.)

Descripción general de la consola remota y opciones de licencia

Las conexiones de la consola remota y de la consola remota integrada son gráficas y deben procesarse mediante un programa cliente que pueda procesar comandos gráficos de iLO 2. Se proporcionan dos clientes para procesar los gráficos de iLO 2:

- Consola remota basada en Java™
- Consola remota integrada basada en Windows® Active X

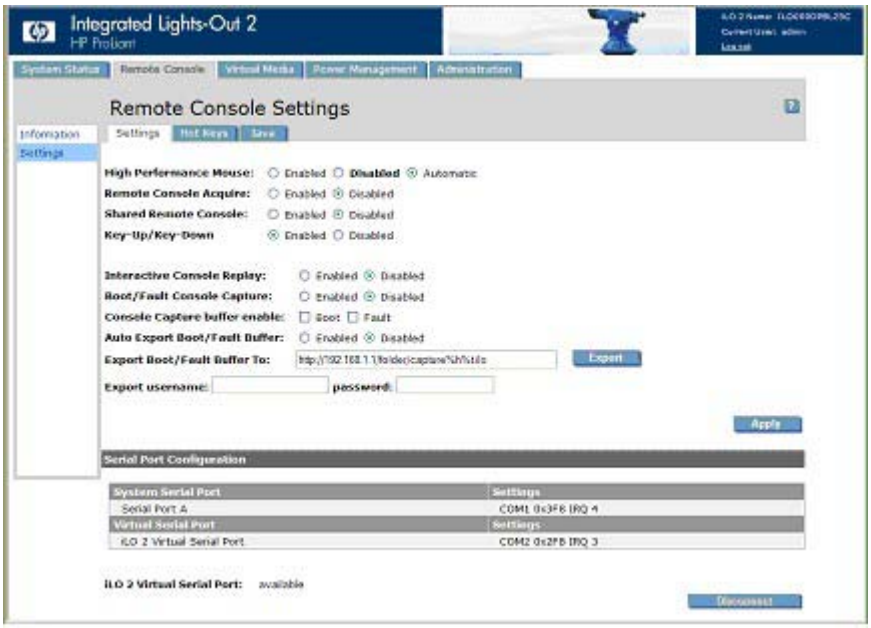
Para los clientes que no comprenden los gráficos de iLO 2, SSH y telnet, es necesario utilizar la consola remota de serie iLO 2 o adquirir una licencia avanzada de iLO para utilizar la consola basada en texto después del proceso POST.

Las consolas ESX, en particular la consola ESX 1, no son completamente compatibles con la consola remota iLO 2 y la consola remota integrada. ESX no es compatible con la consola remota de serie.

Las ranuras de iLO 2 incluyen iLO 2 Standard Blade Edition, que, a su vez, incluye la consola remota. Sin embargo, los modelos HP Proliant ML y HP Proliant DL incluyen una licencia iLO Standard, que no incluye la consola remota ni la consola remota integrada. Según se enciende el servidor para iniciar un sistema operativo, la iLO 2 Standard de los modelos HP ProLiant ML and ProLiant DL muestra un mensaje que indica la necesidad de adquirir una licencia iLO 2 Advanced. Si desea obtener más información, consulte "Concesión de licencias (Concesión de licencias en la página 21)".

Configuración de la consola remota

La configuración y las opciones de iLO 2 Remote Console se establecen en la página Remote Console Settings (Configuración de la consola remota.) Para acceder a la página Remote Console Settings (Configuración de la consola remota), haga clic en **Remote Console (Consola remota)>Settings (Configuración)**.



En la página Remote Console Settings (Configuración de la consola remota) se incluyen tres fichas:

Valores de configuración

- La configuración High Performance Mouse (Ratón de alto rendimiento) puede ayudar a suavizar los problemas de sincronización del ratón de la consola remota, pero esta función no se admite en todos los sistemas operativos. El cambio de configuración tiene sus efectos cuando se inicia o reinicia la consola remota. Las siguientes opciones están disponibles:
  - Disabled (Desactivado): permite que el ratón utilice el modo de coordinadas relativas que es compatible con la mayoría de sistemas operativos.
  - Enabled (Activado): permite que el ratón utilice el modo de coordinadas absolutas y acabe así con los problemas de sincronización en los sistemas operativos que lo admitan.
  - Automatic (Automático): permite que iLO 2 seleccione el modo de ratón más adecuado cuando se carga el controlador de iLO 2 en el sistema operativo host. El modo seleccionado tiene continuidad a menos que se indique otro modo al cargar el controlador del sistema operativo o si elige otra configuración.
- Remote Console Acquire (Adquisición de consola remota): permite que un usuario tome la sesión de otro usuario en la consola remota. Este valor de configuración activa o desactiva la función de adquisición.

- Shared Remote Console (Consola remota compartida): permite que varios usuarios visualicen y controlen la consola de servidor simultáneamente. Este valor de configuración activa o desactiva la función de uso compartido.
- Interactive Console Replay (Reproducción de la consola interactiva): permite volver a reproducir el vídeo de consola capturado de secuencias de inicio y fallo junto con capturas de consola manuales iniciadas por el usuario.
- Key-Up/Key-Down (Tecla arriba/Tecla abajo): permite alternar entre el uso del modelo de teclado de informe del dispositivo de interfaz humana (HID human interface device) y el modelo de teclado de códigos ASCII y ESC en la consola remota integrada (IRC, Integrated Remote Console.) De manera predeterminada, el modelo de teclado de informe HID se encuentra activado pero puede provocar la repetición de caracteres en redes de alta latencia. Si se produce repetición de caracteres al utilizar la IRC, ajuste Key-Up/Key-Down (Tecla arriba/Tecla abajo) en **Disabled (Desactivado)**.
- Boot/Fault Console Capture (Captura de consola de inicio/fallo): permite capturar vídeo de la consola en búferes internos de cualquier secuencia de inicio y fallo. El espacio del búfer interno está limitado a la captura de la secuencia de inicio o fallo más reciente. El espacio del búfer es limitado. Cuanto más dinámica y más alta sea la resolución gráfica de la consola de servidor, menos cantidad de datos se podrá almacenar en el búfer. Seleccione el tipo de vídeo que desea capturar mediante las opciones siguientes:
  - Console Capture Buffer (Búfer de captura de la consola): permite seleccionar el tipo de secuencia de la consola que desea capturar. Se puede activar un búfer cualquiera o ambos al mismo tiempo. Los búferes comparten la misma área de datos internos, de modo que la activación de ambos búferes reduce la cantidad de vídeo de consola que se puede capturar. Se pueden cambiar los búferes activados en cualquier momento para maximizar su uso. Cuando se cambia la configuración del búfer, ambos búferes se reinician y se pierde la información que pudieran contener.
  - Auto Export/Fault Buffer (Búfer de exportación/fallo automático): permite activar o desactivar la exportación automática de los datos de la consola capturados.
- Export Boot/Fault Buffer (Exportar búfer de inicio/fallo): permite especificar la dirección URL de un servidor Web que acepta una transferencia de datos de método PUT o POST. Por ejemplo: `http://192.168.1.1/images/capture%h%t.ilo` transfiere los búferes de captura interna a un servidor web en la dirección IP 192.168.1.1 y guarda los datos en la carpeta `images` con el nombre de archivo `captureServerNameDateTime-Boot(o Fault.)ilo`, donde:
  - %h especifica la adición del nombre de servidor al nombre de archivo
  - %t especifica que se incluirá un sello de fecha en el nombre del archivo
  - Se añade Boot (Inicio)o Fault (Fallo) para distinguir el tipo de búfer entre un suceso de secuencia de arranque o de secuencia de fallo

    Para obtener más información sobre la configuración del servidor Web y sobre cómo configurar un servidor Web Apache para aceptar búferes de captura exportados, consulte la sección "Configuración de Apache para aceptar búferes de captura exportados" (Configuración de Apache para aceptar búfer de captura exportados en la página 226.)
  - Export (Exportar): permite desencadenar una exportación manual.
  - Export username (Nombre de usuario de exportación): el nombre de usuario para el servidor Web que se especifica en la URL.
  - Password (Contraseña): la contraseña del servidor Web que se especifica en la URL.

Una vez realizados los cambios, haga clic en **Apply (Aplicar)**.

- Serial Port Configuration (Configuración de puerto serie): muestra la configuración actual de los puertos serie del sistema y el puerto serie virtual. También se muestra la configuración para los puertos serie de sistema y virtuales, los puertos COM en uso y los números IRQ.
- iLO 2 Virtual Serial Port (Puerto serie virtual de iLO 2): muestra el estado actual de la conexión del puerto serie virtual. Los posibles modos disponibles son: modo in use raw (en uso no procesado) o modo in use normal (en uso normal.) Si la conexión está en uso, el botón Disconnect (Desconectar) está disponible y se puede utilizar para desconectar una conexión de un puerto serie virtual. El modo Raw (sin procesar) indica que un cliente está conectado mediante la utilidad WiLODbg.exe que se utiliza para la depuración de kernel Windows® remota.

Hot Keys (Teclas de acceso directo): permite definir secuencias de pulsación de teclas que se transmitirán al servidor host remoto al pulsar una tecla de acceso directo. Las teclas de acceso directo de la consola remota permiten transmitir secuencias de clave específicas, como Alt+Tab y Alt+PetSys al servidor desde la sesión de Java™ de la consola remota. Para obtener información, consulte la sección "Teclas de acceso directo de la consola remota (Teclas de acceso directo de la consola remota en la página 93)".

Java: muestra los requisitos de Java™ para cada sistema operativo compatible y un enlace para descargar Java™. Para obtener más información, consulte la sección "Sistemas operativos cliente y exploradores compatibles" (Sistemas operativos cliente y exploradores compatibles en la página 7.)

Teclas de acceso directo de la consola remota

La página Program Remote Console Hot Keys (Programar teclas de acceso directo de la consola remota) permite definir hasta seis combinaciones de varias teclas asignadas a cada tecla de acceso directo. Cuando se pulsa una tecla de acceso directo en la consola remota en sistemas cliente, la combinación de teclas especificada (pulsando todas al mismo tiempo) se transmite al servidor host remoto en lugar de la tecla de acceso directo. Para acceder a los símbolos Alt Gr en teclados internacionales, utilice teclas de acceso directo para definirlos. Para obtener una lista de las teclas de acceso directo, consulte la sección "Teclas de acceso directo compatibles" (Teclas de acceso directo compatibles en la página 94.)

Las teclas de acceso directo de la consola remota están activas durante la sesión de la consola remota a través de IRC, subprograma de consola remota y durante una sesión de texto de la consola remota a través de un cliente telnet. Al utilizar IRC, el estado del LED del teclado para Bloq Num, Bloq Mayús y Bloq Despl del teclado del cliente no necesariamente reflejan el estado del teclado del servidor. Sin embargo, al pulsar cualquiera de las teclas de bloqueo se cambiará el estado de bloqueo del servidor.

Para definir una tecla de acceso directo de la consola remota:

1. Haga clic en **Remote Console (Consola remota)>Hot Keys (Teclas de acceso directo)**.
2. Seleccione la tecla de acceso directo que desea definir y utilice los cuadros desplegables para seleccionar la secuencia de teclas que desea transmitir al servidor host al pulsar la tecla de acceso directo.
3. Haga clic en **Save Hot Keys (Guardar las teclas de acceso directo)** cuando termine de establecer las secuencias de teclas.

La página Remote Console Hot Keys (Teclas de acceso directo del programa de la consola remota) también contiene la opción Reset Hot Keys (Reiniciar teclas de acceso directo.) Esta opción borra todas las entradas de los campos de teclas de acceso directo. Haga clic en **Save Hot Keys (Guardar teclas de acceso directo)** para guardar los campos borrados.

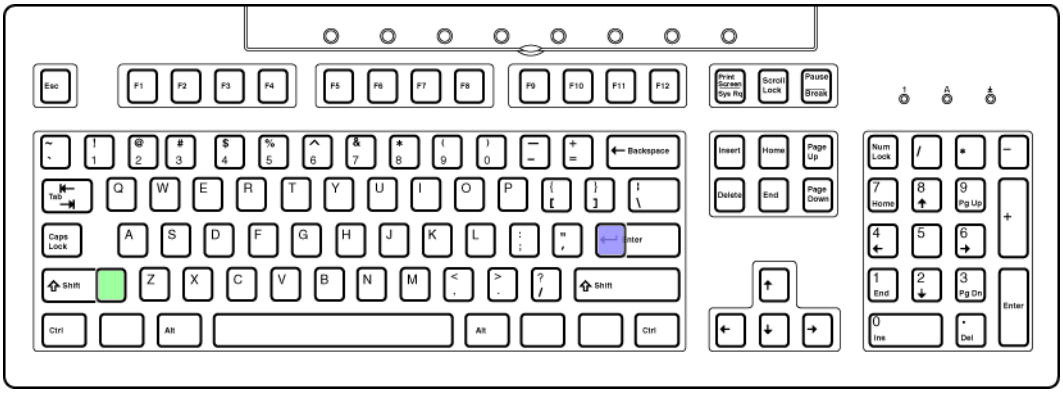
Teclas de acceso directo compatibles

En la página Program Remote Console Hot Keys (Programar teclas de acceso directo de la consola remota), se pueden definir hasta 6 grupos distintos de teclas de acceso directo para su uso en una sesión de la consola remota. Cada tecla de acceso directo representa una combinación de hasta 5 teclas diferentes que se envía al equipo host cada vez que se pulse la tecla de acceso directo durante una sesión de la consola remota. Se transmite la combinación de teclas seleccionada (todas las teclas pulsadas a la vez.) Para obtener más información, consulte la sección "Teclas de acceso directo de la consola remota (Teclas de acceso directo de la consola remota en la página 93)". La siguiente tabla recoge las teclas que están disponibles para combinarlas en una secuencia de teclas de acceso directo de la consola remota.

ESC	F12	:	o
L_ALT	" " (Espacio)	<	p
R_ALT	!	>	q
L_MAYÚS	#	=	r
R_MAYÚS	$	?	s
INSERT	%	@	t
SUPR	&	[	u
INICIO	~	]	v
FIN	(	\	w
RE PÁG	)	^	x
AV PÁG	*	_	s
INTRO	+	a	z
TAB	-	b	{
ENTRAR	.	c	}
F1	/	d	|
F2	0	e	;
F3	1	f	'
F4	2	g	L_CTRL
F5	3	h	R_CTRL
F6	4	i	+ de teclado numérico
F7	5	j	- de teclado numérico
F8	6	k	BLOQ DESPL
F9	7	l	RETROCESO
F10	8	m	PET SIS
F11	9	n	

Teclas de acceso directo y teclados internacionales

Para configurar las teclas de acceso directo en un teclado internacional, seleccione las teclas en su teclado en la misma posición que en un teclado de EE. UU. Para crear una tecla de acceso directo utilizando la tecla Alt Gr internacional, utilice R_ALT en la lista de teclas. Utilice el diseño del teclado de EE. UU. mostrado para seleccionar las teclas.



Las teclas sombreadas no existen en los teclados de EE. UU.

- La tecla sombreada verde se conoce como las teclas \ y | que no pertenecen a EE. UU en un teclado internacional.
- La tecla sombreada violeta se conoce como la tecla # y ~ que no pertenece a EE. UU. en un teclado internacional.

Teclas de acceso directo y puerto serie virtual

Estando conectado a la función de puerto serie virtual de iLO 2 mediante telnet, la secuencia de teclas CTRL+P+! (tecla CTRL, tecla P, tecla Mayús y tecla 1 pulsadas simultáneamente) normalmente provoca el reinicio del servidor remoto.

Utilice la secuencia de teclas CTRL+P 6 para apagar el servidor remoto y la secuencia de teclas CTRL+P 1 para encenderlo.

Si iLO 2 deja de responder, cierre la sesión del puerto serie virtual. iLO 2 se reiniciará de forma automática al cabo de unos tres minutos y volverá a su funcionamiento normal.

Pantalla completa de IRC

La opción Integrated Remote Console Fullscreen (Pantalla completa de la consola remota integrada) le permite redimensionar el IRC a la misma resolución de pantalla que el host remoto. Para volver al escritorio cliente, salga de la consola.

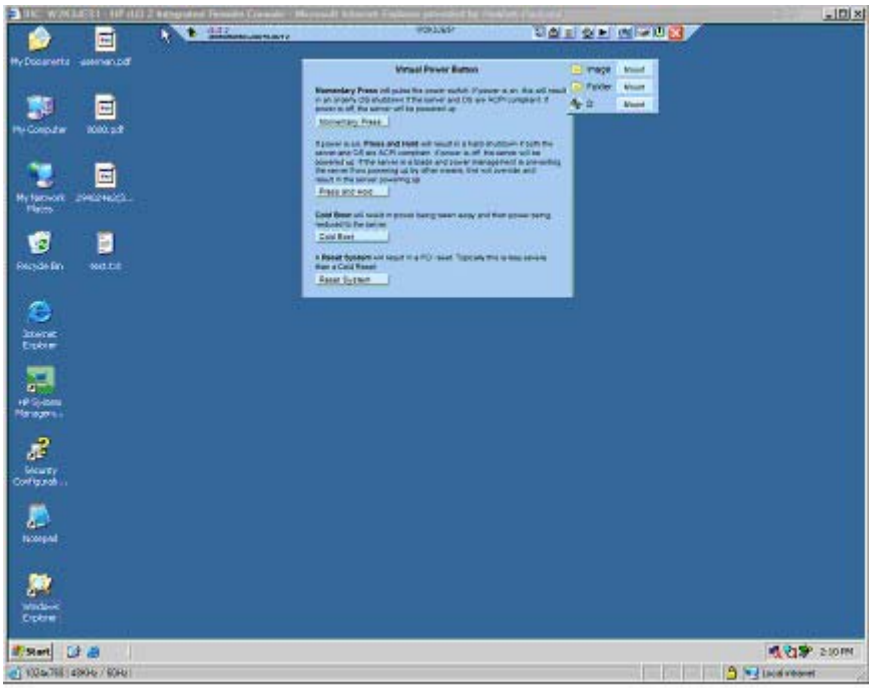
La pantalla completa de la consola remota hace que el cliente redimensione a la misma resolución que el servidor remoto. La pantalla completa de la consola remota integrada intenta tomar la mejor configuración de pantalla del cliente para dicha resolución; sin embargo, algunos monitores pueden encontrar problemas con las frecuencias de actualización de la pantalla más altas que admite el adaptador de vídeo. Si esto sucede, haga clic con el botón derecho del ratón para comprobar las propiedades del escritorio en **Escritorio** y seleccione **Propiedades>Configuración>Avanzado>Monitor** y seleccione una frecuencia de actualización de la pantalla inferior.

Si desea obtener más información acerca de la visualización de la pantalla completa de la consola remota integrada, consulte la sección "Consola remota integrada (Opción de Consola remota integrada en la página 96)".

Opción de Consola remota integrada

La consola remota integrada ofrece una interfaz de consola remota de alto rendimiento para los clientes de Windows®, combinando KVM, Virtual Power (Alimentación virtual) y la funcionalidad Virtual Media (Soportes virtuales.) La opción Integrated Remote Console (Consola remota integrada) es un control de ActiveX que se ejecuta desde Microsoft® Internet Explorer. La opción Integrated Remote Console es una función con licencia disponible con la adquisición de licencias opcionales. Si desea obtener más información, consulte "Concesión de licencias (Concesión de licencias en la página 21)".

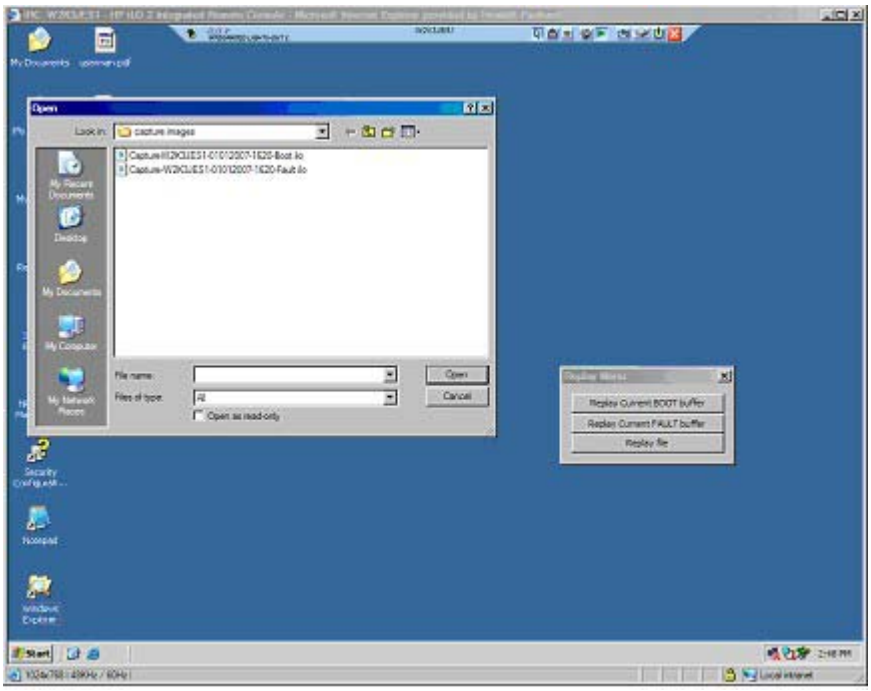
Integrated Remote Console admite simultáneamente cuatro sesiones de consola remota con el mismo servidor si se activa a través de la pantalla Remote Console Settings (Configuración de la consola remota), SMACH CLI (OEM) o RIBCL. Para obtener más información sobre el uso de varias sesiones de consola remota, consulte la sección "Consola remota compartida" (Consola remota compartida en la página 100.)



Las opciones Integrated Remote Console (Consola remota integrada) e Integrated Remote Console Fullscreen (Pantalla completa de la consola remota integrada) muestran una barra de menús y botones que se representan en la pantalla. La barra de menú tiene las siguientes opciones:

- Remote Console Replay (Reproducción de la consola remota) (icono de reproducción): muestra el cuadro de diálogo Replay Menu (Menú de reproducción) (si se activa Boot/Fault Console Capture [Captura de consola de inicio/fallo]) o inicia el cuadro de diálogo Open File (Abrir archivo) si no se activa Boot/Fault Console Capture (Captura de la consola de inicio/fallo.)
    - Replay Current BOOT buffer (Reproducir búfer de inicio actual) y Replay Current FAULT buffer (Reproducir búfer de fallo actual): permite transferir los búferes capturados internamente al cliente mediante el uso del puerto de reproducción de consola especificado en la ficha Administration (Administración)>Access (Acceso.) Haga clic en **Replay Current BOOT buffer (Reproducir búfer de inicio actual)** o **Replay Current FAULT buffer (Reproducir búfer de fallo actual)** para cambiar el menú Remote Console (Consola remota) por el menú Replay Console (Consola de reproducción.)

- Replay file (Reproducir archivo): muestra un cuadro de diálogo Open (Abrir) que permite ver un archivo guardado previamente. Después de seleccionar un archivo y hacer clic en **Open (Abrir)**, el menú Remote Console (Consola remota) cambia al menú Replay Console (Consola de reproducción.)



- Replay (Reproducir) (icono de reproducción en el menú principal): muestra la consola de reproducción. La consola de reproducción proporciona el control de reproducción del búfer de datos seleccionado y muestra el tiempo transcurrido de reproducción.

La consola de reproducción presenta las siguientes opciones:

- Haga clic en **Play (Reproducir)** para iniciar la reproducción. Después de hacer clic en Play (Reproducir) se puede realizar lo siguiente:

  — Hacer clic en **Pause (Pausa)** para detener la reproducción y mantener la posición actual. Para reanudar la reproducción, haga clic en **Play (Reproducir)** desde el estado pausado y la reproducción se reanudará desde su posición actual.

  —Hacer clic en **Stop (Detener)** para detener la reproducción y volver a colocar la reproducción al principio del búfer de datos.

  — Hacer clic en **Fast-forward (Avance rápido)** para aumentar la velocidad de reproducción en 2x, 4x o 8x la velocidad normal.

- La opción Close (Cerrar) aparece al finalizar la reproducción. Haga clic en **Close (Cerrar)** para salir de la consola de reproducción y para que aparezca la barra de menús de la consola remota.

- Record (Grabar) (icono de una cámara): permite grabar de forma manual el vídeo de la consola de servidor actual. Pulse **Record (Grabar)** para que aparezca un cuadro de diálogo Save (Guardar) que permite especificar el nombre del archivo y la ubicación en la que se debe guardar la sesión de grabación actual. Durante una sesión de grabación, la opción Record (Grabar)

aparecerá pulsada y su color cambiará a verde. Mientras está activada, cualquier actividad de la consola de servidor que aparezca en la consola remota integrada se guardará en el archivo especificado. Si hace clic en **Record (Grabar)** durante una sesión de grabación, la grabación se detiene y el botón Record (Grabar) deja de aparecer pulsado y recupera su estado normal. Para reproducir la grabación, haga clic en **Replay (Reproducir)**.

- Control (Controlar): permite al líder de la sesión hacerse con el control absoluto si se ha otorgado control para un cliente satélite.
- Lock (Bloquear): permite impedir cualquier aparición de solicitudes de cliente satélite adicional en la consola del líder de la sesión.
- Client List (Lista de clientes): muestra el nombre de usuario y el nombre de DNS (si está disponible) o la dirección IP de los clientes de satélite actuales.
- Drive (Unidad): permite visualizar todos los soportes disponibles.
- Power (Alimentación) (icono de alimentación en verde): muestra el estado de alimentación y permite acceder a las opciones de alimentación. El botón de alimentación se pone de color verde al encenderse el servidor. Cuando pulsa el botón **Power (Alimentación)**, en la pantalla Virtual Power Button (Botón de alimentación virtual) aparecen cuatro opciones: Momentary Press (Pulsar momentáneamente), Press and Hold (Mantener pulsado), Cold Boot (Inicio en frío) y Reset System (Reiniciar sistema.)

  Cuando se pulsan los botones Drives (Unidades) o Power (Alimentación), el menú que aparece permanece abierto aunque se aleje el ratón de la barra de menú.
- CAD: permite iniciar el cuadro diálogo para enviar las teclas Ctrl-Alt-Supr (o cualquiera de las seis teclas de acceso directo) al servidor.
- Thumb tack (Tachuela): permite mantener abierto el menú principal de la consola remota o cerrarlo cuando se aleja el ratón.
- Exit (Salir) (icono X en rojo): permite cerrar y salir de la consola remota.

Las mejoras en seguridad de Internet Explorer 7 muestran la barra de direcciones en todas las ventanas abiertas recientemente. Si desea eliminar la barra de direcciones de la IRC, deberá cambiar la configuración de seguridad por un nivel distinto al predeterminado. Para eliminar la barra de direcciones, establezca la opción "Permitir que los sitios web abran ventanas sin barras de dirección o de estado" en **Enable (Activar)**.

Optimización del rendimiento del ratón para la consola remota o la consola remota integrada

En algunas configuraciones de Microsoft® Windows® es necesario ajustar correctamente la velocidad del ratón para que el ratón de la consola remota funcione correctamente.

SLES 9

Determine qué dispositivo de ratón es el ratón de la consola remota. Para ello utilice el comando `xsetpointer -l` para que enumere todos los ratones.

1. Determine el ratón que desea modificar. Para ello, establezca una referencia cruzada entre el resultado de xsetpointer y la configuración X (o bien /etc/X11/XF86Config o bien /etc/X11/xorg.conf)
2. Seleccione el ratón de la consola remota como el ratón que desea modificar. Por ejemplo:

   ```
   xsetpointer Mouse[2]
   ```
3. Establezca los parámetros de velocidad. Por ejemplo:

```
xset m 1/1 1.
```

Red Hat Enterprise Linux

Establezca los parámetros de velocidad mediante:

```
xset m 1/1 1
```

Sincronización del ratón en Windows®

La configuración predeterminada del ratón de alto rendimiento de la página Global Setting (Configuración global) está diseñada para utilizar los valores más adecuados según el sistema operativo del servidor. Para que funcione correctamente es necesario cargar el controlador HP ProLiant Lights-Out Management Interface y reiniciar el servidor tras la instalación del controlador. Si detecta algún problema al sincronizar el ratón en Windows, cambie la configuración de ratón de alto rendimiento a **Yes (Sí)**.

Configuración de la opción High Performance Mouse

Cuando utilice la consola remota, puede desactivar la función High Performance Mouse (Ratón de alto rendimiento.) Esta función mejora notablemente el funcionamiento y la precisión del puntero en los sistemas operativos que lo admiten. El ratón de alto rendimiento de iLO 2 es un puntero que proporciona unas coordenadas de posición absolutas para describir su ubicación similar a los ratones USB para equipos portátiles. Un ratón convencional envía información de posición relativa (como por ejemplo, el ratón se ha desplazado 12 píxeles hacia la derecha.) El ordenador host puede modificar la información de posición relativa para permitir funciones tal como la aceleración del ratón. Al utilizar la consola remota, el cliente no es consciente de estas modificaciones. Por consiguiente, falla la sincronización entre los cursores del ratón del cliente y del host.

Tanto el subprograma Integrated Remote Console (Consola remota integrada) y Remote Console (Consola remota) envían coordinadas de cursor absolutas y relativas a iLO 2. Cuando iLO 2 está en modo High Performance Mouse (Ratón de alto rendimiento), desecha las coordinadas relativas y envía las coordinadas absolutas en el emulador de ratón USB para equipos portátiles. El resultado es que el servidor "ve" los movimientos del ratón como si la información de las coordenadas se hubiera originado en un ratón USB local de un equipo portátil. Cuando iLO 2 no está en modo High Performance Mouse (Ratón de alto rendimiento), se desechan las coordenadas absolutas y se envían las coordenadas relativas al emulador de ratón USB relativo.

Esta función sólo es compatible con sistemas operativos que permitan utilizar ratones USB para equipos portátiles. Los usuarios de Windows® deben activar la opción High Performance Mouse (Ratón de alto rendimiento) en la pantalla Remote Console Settings (Configuración de la consola remota.) Los usuarios de Linux deberían activar la opción High Performance Mouse (Ratón de alto rendimiento) una vez instalado el controlador iLO 2 High Performance Mouse para Linux . Los servidores con otros sistemas operativos que tengan problemas con el ratón de la consola remota deben desactivar la opción High Performance Mouse (Ratón de alto rendimiento.)

Al utilizar la consola remota integrada desde iLO 2 y SmartStart, el ratón remoto y el local no se alinean. Los valores de configuración High Performance Mouse (Ratón de alto rendimiento) deben estar desactivados mientras se encuentre en SmartStart. Si el ratón local y el remoto pierden su alineación mientras está utilizando la función High Performance Mouse (Ratón de alto rendimiento), puede utilizar la tecla Ctrl para volverlos a alinear. También puede utilizar la consola remota de Java™ en lugar de la consola remota integrada.

La opción High Performance Mouse (Ratón de alto rendimiento) reduce los problemas de sincronización del ratón en sistemas operativos de host compatibles. Puede seleccionar este modo en la página Remote Console Settings (Configuración de la consola remota) antes de iniciar la consola remota. Sin

embargo, es posible que no sea compatible con todos los sistemas operativos, particularmente durante la instalación. Para obtener un mejor rendimiento:

- Seleccione una resolución de pantalla del servidor remoto inferior para mejorar el rendimiento de la consola remota. La resolución máxima admitida es de 1280 x 1024 píxeles.
- Establezca la resolución de pantalla del cliente más elevada que la del servidor remoto para maximizar la visibilidad de la consola remota.
- La calidad del color del servidor remoto no afecta al rendimiento de la consola remota. La consola remota se procesa en 4096 colores (12 bits.)
- Utilice un puntero del ratón no animado en el sistema remoto.
- Desactive el rastro del ratón en el sistema remoto.

Para configurar el servidor host, ajuste los siguientes valores de configuración en el Panel de control:

1. Seleccione **Ratón>Punteros>Combinación>Combinación predeterminada de Windows**. Haga clic en **Aceptar**.
2. En la página Ratón>Punteros, seleccione **Habilitar sombra del puntero**. Haga clic en **Aceptar**.
3. Seleccione **Pantalla>Configuración>Avanzado>Solucionar problemas>Aceleración de hardware>Completa**. Haga clic en **Aceptar**.
4. Seleccione **Sistema>Avanzado>Configuración de rendimiento>Efectos visuales>Ajustar para obtener el mejor rendimiento**. Haga clic en **Aceptar**.

O bien, la utilidad de configuración en línea de HP (HPONCFG) puede ajustar estos valores. También puede editar valores de High Performance Mouse utilizando el comando XML `MOD_GLOBAL_SETTINGS`. Para obtener más información sobre el uso del comando RIBCL `MOD_GLOBAL_SETTINGS`, consulte la *Guía de recursos de líneas y secuencias de comandos del procesador de gestión HP Integrated Lights-Out*.

Consola remota compartida

Shared Remote Console (Consola remota compartida) es una función de iLO 2 que permite la conexión de hasta cuatro sesiones en el mismo servidor. Esta función no sustituye la función Acquire (Adquisición) descrita en "Adquisición de la consola remota" (Adquisición de la consola remota en la página 104) ni da control sobre la alimentación a los clientes con acceso total (lectura/escritura.) Shared Remote Console (Consola remota compartida) no admite el traspase de la designación de host de servidor a otro usuario ni que una conexión fallida de usuario se vuelva a conectar después de fallar. Para permitir el acceso de usuario después de un fallo es necesario reiniciar la sesión en la consola remota.

Shared Remote Console (Consola remota compartida) es una función con licencia disponible con la adquisición de licencias opcionales. Si desea obtener más información, consulte "Concesión de licencias (Concesión de licencias en la página 21)".

Shared Remote Console (Consola remota compartida) y el modo Forced Switch (Cambio forzado) están desactivados de manera predeterminada. Debe activar y configurar estas funciones a través del explorador, SMASH CLI (OEM) o RIBCL. Todas las sesiones de consola se cifran primero con una autenticación del cliente y, después, el líder de la sesión decide si se permitirá la nueva conexión.

El primer usuario a iniciar la sesión de consola remota se conecta normalmente al servidor y se designa líder de la sesión (host de sesión.) Cualquier usuario posterior que solicite acceso a la consola remota inicia una solicitud de acceso, una conexión a cliente satélite dirigida al líder de la sesión. En el escritorio del líder de sesión aparece una ventana por cada solicitud de cliente satélite en la que se indica el nombre de usuario y el nombre de DNS (si está disponible) del solicitante or su dirección IP.

Los hosts de sesión tienen la opción de otorgar o denegar el acceso. Dentro del marco del explorador de la consola remota aparece una lista de los nombres de usuario y los nombres de host de sesión. Las sesiones de cliente satélite finalizan cuando finaliza el host de sesión.

Las sesiones compartidas no funcionan bien con las funciones Console Capture (Captura de consola) y de reproducción de iLO 2. Si una sesión de satélite ve una sesión capturada, durante el tiempo de reproducción la sesión de satélite no recibirá los mensajes de control del líder de la sesión. Si el host de sesión empieza a ver los datos de vídeo capturados durante una sesión compartida, el vídeo se muestra en todas las sesiones de consola remota de satélite.

Uso de Console Capture

La opción Console Capture (Captura de consola) es una función de la consola remota que permite grabar y reproducir un flujo de vídeo de sucesos como, por ejemplo, el inicio, los sucesos ASR y los fallos detectados del sistema operativo. También puede iniciar y detener manualmente la grabación del vídeo de consola. La opción Console Capture (Captura de consola) sólo está disponible a través de la interfaz de usuario de iLO 2 y no se puede acceder a ella mediante secuencias de comandos XML ni CLP. La opción Console Capture (Captura de consola) es una función con licencia disponible con la adquisición de licencias opcionales. Si desea obtener más información, consulte "Concesión de licencias (Concesión de licencias en la página 21)".

En el procesador de gestión se reserva un área de búfer para almacenar los datos de vídeo capturados. Este área de búfer se comparte con el búfer de actualización del firmware, de modo que cualquier información capturada se pierde al iniciar el proceso de actualización del firmware. No es posible capturar datos de vídeo durante el proceso de actualización del firmware.

El espacio del búfer es limitado. En el área de búfer sólo se guarda un suceso de cada tipo a la vez. Se pueden transferir búferes de datos capturados a un cliente que ejecute la IRC para su reproducción. También se puede configurar iLO 2 para que envíe automáticamente los datos de vídeo capturados a un servidor Web de la misma red que la de iLO 2 cuando se produce un suceso. El servidor Web debe aceptar transferencias de datos del método POST. Puede seleccionar Boot buffer only (Sólo búfer de inicio), Fault buffer (Búfer de fallo) o combinar las dos opciones como un gran búfer para disponer de más espacio con el fin de capturar las secuencias de inicio de Linux.

Se asigna un nombre exclusivo a los datos del búfer exportados para facilitar su identificación para la reproducción. Para la reproducción se requiere un iLO 2 con licencia en la red. Algunos sistemas operativos (por ejemplo, Linux) pueden llenar rápidamente el búfer. Si deja la consola del sistema en modo de texto, ayudará a maximizar la cantidad de información capturada. Asimismo, si se limita o reduce el número de elementos de consola gráfica activos se ayudará a optimizar el espacio del búfer interno.

Se puede capturar vídeo de la consola de servidor de forma manual mediante la función IRC Record (Grabación IRC.) Todos los datos capturados de forma manual se guardan en un archivo local en el cliente para una posterior reproducción.

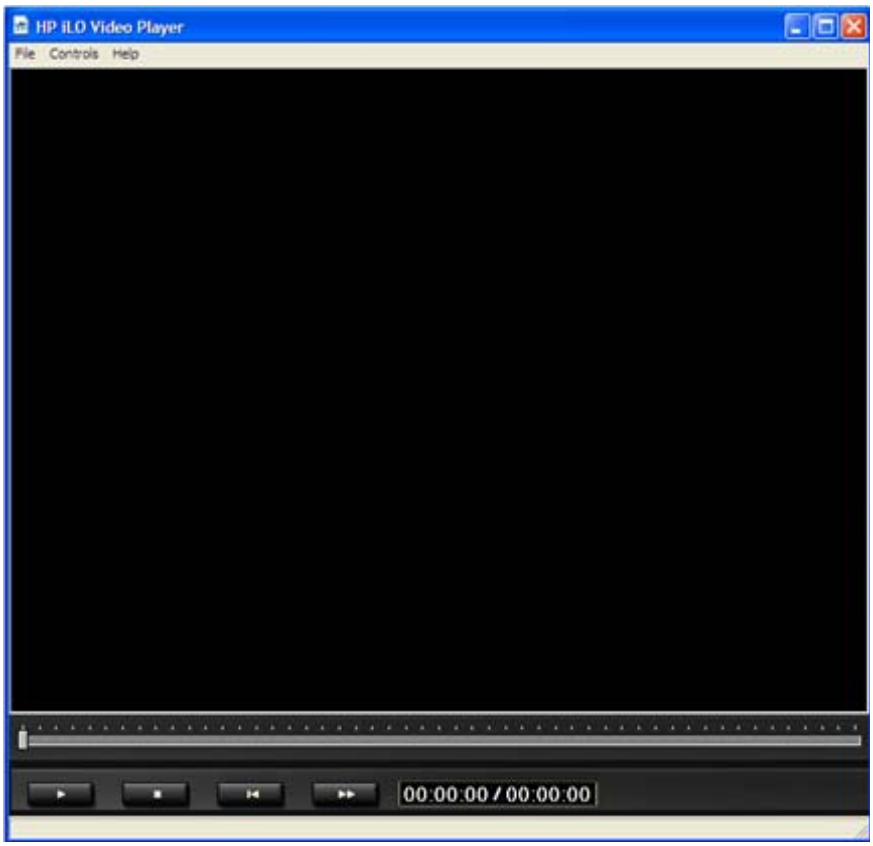
Utilización del reproductor de vídeo de iLO de HP

El reproductor de vídeo de iLO de HP permite reproducir archivos de la Console Capture (Captura de consola) iLO 2 sin necesidad de instalar iLO 2 en su sistema local. El reproductor de vídeo iLO está diseñado como un reproductor multimedia normal con controles similares. Es posible ejecutar el reproductor de vídeo de iLO como una aplicación independiente en un servidor o en un cliente. Normalmente, la aplicación se encuentra localizada en el cliente. Los archivos de captura de iLO 2 se crean mediante la función Console Capture (Captura de consola) de iLO 2; consulte la sección "Uso de Console Capture (Uso de Console Capture en la página 101)".

Para utilizar el reproductor de vídeo de iLO, es necesario disponer de los sistemas operativos Microsoft Windows® 2000, Windows® XP o Windows Vista® e Internet Explorer (versión 6 o posterior) instalados en el sistema.

Interfaz de usuario del reproductor de vídeo de iLO

Al iniciar el reproductor de vídeo de iLO de HP, la interfaz de usuario aparece y sirve como punto de control para todas las funciones de reproducción.



Opciones del menú del reproductor de vídeo de iLO:

- File (Archivo)
  - Open (Abrir): permite abrir archivos de captura de vídeo.
  - Exit (Salir): permite cerrar el reproductor de vídeo de iLO.
- Controles
  - Play (Reproducir): permite reproducir o reiniciar el archivo de captura de vídeo actual.
  - Stop (Detener): permite detener la reproducción del archivo de captura de vídeo actual.

- Skip to Start (Omitir hasta el principio): permite reiniciar la reproducción del archivo de captura de vídeo actual.
- Change Speed (Cambiar velocidad): permite cambiar la velocidad de reproducción del archivo de captura de vídeo de iLO actual.

- Ayuda
  - Help Topics (Temas de ayuda): permite abrir el archivo de ayuda del reproductor de vídeo de iLO.
  - About (Acerca de): permite abrir la página iLO Video Player About (Acerca del reproductor de vídeo de iLO.)

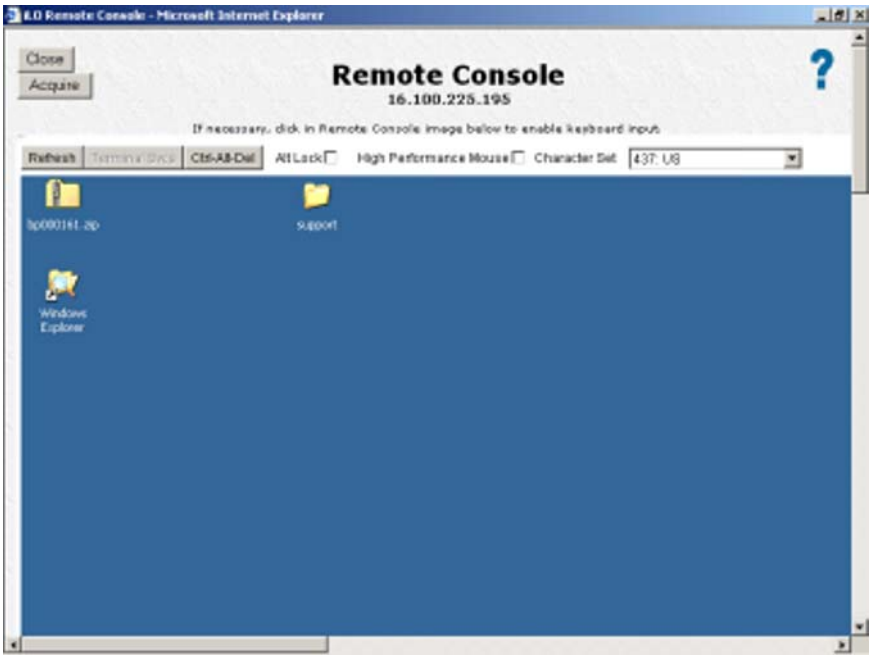
Controles del reproductor de vídeo de iLO

Control	Nombre	Función
 	Play/Pause (Reproducir/Pausa)	Permite iniciar la reproducción si el archivo seleccionado actualmente no se está reproduciendo o se encuentra en pausa. Si la reproducción se encuentra en curso, permite introducir una pausa en el archivo. Si no se encuentra seleccionado ningún archivo, el botón aparecerá deshabilitado.
	Stop (Detener)	Permite detener la reproducción. Si no se encuentra seleccionado ningún archivo, el botón aparecerá deshabilitado.
	Skip to Start (Omitir hasta el principio)	Permite reiniciar la reproducción desde el principio del archivo. Si no se encuentra seleccionado ningún archivo, el botón aparecerá deshabilitado.
	Seek (Buscar)	Permite desplazar la reproducción del vídeo hacia delante o hacia atrás. Si no se encuentra seleccionado ningún archivo, el botón aparecerá deshabilitado.
	Change Speed (Cambiar velocidad)	Permite cambiar la velocidad de la reproducción del archivo seleccionado en estos momentos. Las velocidades de reproducción disponibles son 1x, 2x, 4x, 8x y 16x. Las velocidades van alternando si se pulsa el botón sucesivamente en el siguiente orden: 2x, 4x, 8x, 16x y 1x. Si no se encuentra seleccionado ningún archivo, el botón aparecerá deshabilitado.
	File Position (Posición del archivo)	Permite visualizar los parámetros de tiempo del archivo seleccionado en

Control	Nombre	Función
		estos momentos y aparece en formato HH:MM:SS. • El tiempo restante que figura a la izquierda indica la posición de reproducción actual del archivo. • El tiempo situado a la derecha indica el tiempo de reproducción total del archivo.

Adquisición de la consola remota

Cuando se ha activado el valor Remote Console Acquire (Adquisición de consola remota) en la pantalla Remote Console Settings (Valores de configuración de la consola remota), la página Remote Console (Consola remota) muestra el botón Acquire (Adquirir.) Si al abrir la página de la consola remota se informa de que otro usuario está utilizando la consola remota, haga clic en el botón Acquire para finalizar la sesión del otro usuario e iniciar una en la ventana actual.



Al hacer clic en Acquire, le solicitan que verifique la interrupción de la sesión del otro usuario. Tras perder la conexión, el otro usuario recibe una notificación de que otro usuario ha adquirido la sesión de la consola remota. No se ofrece ningún aviso con anterioridad. Tras confirmar que desea continuar con la operación de adquisición, una ventana de alerta le notificará que la operación podría tardar 30 segundos o más en completarse. Al pulsar el botón Acquire (Adquirir), éste se desactiva y se inicia la operación de adquisición. En los exploradores que lo admiten, el botón adoptará un color gris claro para indicar que está desactivado. En otros exploradores, es posible que no se produzca ninguna indicación visible de que el botón está desactivado.

Los usuarios sólo disponen de un comando de adquisición cada cinco minutos. Si otro usuario ha adquirido recientemente la consola remota, al hacer clic en el botón Acquire podrá aparecerle una página en la que se le informe de que está vigente el período de cinco minutos de desactivación de adquisición. Cierre la ventana y vuelva a iniciar la consola remota. En la página nueva, el botón Acquire

está desactivado hasta que transcurra el período de desactivación de la adquisición. Al activar el botón Acquire (esta operación sucede automáticamente y no tiene que actualizar la página), puede intentar volver a adquirir la sesión de la consola remota. En los exploradores que lo admiten, el botón aparece de color gris claro para indicar que está desactivado durante este periodo de cinco minutos. En otros exploradores, puede que no se produzca ninguna indicación visible de que el botón está desactivado, por lo que tampoco habrá ninguna indicación visual cuando se termine en periodo de desactivación.

Sólo puede llevarse a cabo un intento de adquisición por cada ventana de sesión de la consola remota. Si logra adquirir la consola remota y, al mismo tiempo, un tercero la adquiere a partir de usted, debe abrir una nueva ventana de consola remota para intentar a adquirir la sesión de nuevo.

Consola remota

Remote Console (Consola remota) es un subprograma de Java™ que procesa la consola remota con una amplia compatibilidad de exploradores, incluidos los exploradores de Windows® y Linux. Los exploradores compatibles aparecen en una lista en la sección "Sistemas operativos cliente y exploradores compatibles" (Sistemas operativos cliente y exploradores compatibles en la página 7.) Remote Console (Consola remota) es una función con licencia disponible con la adquisición de licencias opcionales. Si desea obtener más información, consulte "Concesión de licencias (Concesión de licencias en la página 21)".

Remote Console (Consola remota) utiliza cursores duales que ayudan a distinguir entre los punteros de ratón local y remoto. El cursor del ratón del equipo cliente aparece en la consola remota en forma de cruz. Para un mejor funcionamiento, no olvide configurar la pantalla del sistema operativo host tal como se describe en las secciones "Valores de configuración recomendados para el cliente" (Valores de configuración recomendados para el cliente en la página 106) y "Valores de configuración recomendados para el servidor" (Valores de configuración recomendados para el servidor en la página 107.)

Para sincronizar los cursores remoto y local si se descompensan, haga lo siguiente:

- Haga clic con el botón secundario del ratón, arrastre y mueva el cursor local en forma de cruz hasta alinearlo con el del servidor remoto.
- Mantenga pulsada la tecla **Crtl** derecha y mueva el cursor local en forma de cruz hasta alinearlo con el cursor del ratón del servidor remoto.

El cursor local toma la forma del cursor remoto. El cursor se muestra como único si el cursor local y remoto están alineados perfectamente y la aceleración del hardware está ajustada en Full (Completa) en el servidor gestionado.

Funciones y controles de la consola remota

El subprograma de la consola remota contiene botones que proporcionan funciones y control mejorados a iLO 2. Las opciones son:

- Refresh (Actualizar): permite actualizar la pantalla de iLO 2.
- Terminal Svcs (Servicios de Terminal Server): permite iniciar el cliente de Microsoft® Terminal Services instalado en el sistema. Este botón aparece desactivado si los servicios de Terminal Server no están activados o no están instalados en el servidor.
- (Ctrl-Alt-Supr): permite introducir la secuencia de teclas Ctrl+Alt+Supr en la consola remota.
- Alt Lock (Bloq Alt): cuando se selecciona, permite enviar cualquier tecla pulsada al servidor como si hubiera pulsado la tecla Alt y otra tecla simultáneamente.
- Character Set (Conjunto de caracteres): permite cambiar el conjunto de caracteres que la consola remota utiliza por defecto. Si modifica el conjunto de caracteres de la consola remota, se asegurará de que los caracteres se muestren correctamente.
- Close (Cerrar): permite cerrar la sesión de la consola remota y cierra la ventana Remote Console (Consola remota.)

Valores de configuración recomendados para el cliente

Lo ideal es que la resolución de imagen del sistema operativo del servidor remoto sea igual o inferior a la del ordenador con función de explorador. Las resoluciones de servidor mayores transmiten más información, ralentizando el rendimiento global.

Utilice los siguientes valores de configuración del cliente y del explorador para optimizar el rendimiento:

- **Propiedades de pantalla**
  - Seleccione una opción superior a 256 colores.
  - Seleccione una resolución de pantalla mayor que la del servidor remoto.
  - Propiedades de pantalla X de Linux: en la pantalla X Preferences (Preferencias de X), establezca el tamaño de la fuente en **12**.
- **Consola remota**
  - Para la velocidad de la consola remota, HP recomienda utilizar un equipo cliente a 700 MHz o más rápido con 128 MB o más de memoria.
  - Para ejecutar el subprograma Java™ de la consola remota, HP recomienda utilizar un cliente con procesador único.
- **Propiedades del ratón**
  - Elija un valor intermedio para la velocidad del puntero del ratón.
  - Aplique un valor bajo a la aceleración del puntero del ratón o desactívela.

Valores de configuración recomendados para el servidor

En la siguiente lista encontrará los valores de configuración recomendados para el servidor en función del sistema operativo utilizado.

NOTA: Para mostrar la pantalla del servidor host en el subprograma Consola remota del cliente, establezca la resolución de pantalla del servidor a un valor menor o igual que el del cliente.

Valores de Microsoft® Windows® Server 2003

Para optimizar el rendimiento, ajuste las **Propiedades de pantalla** del servidor a un fondo liso (sin dibujos) y establezca las **Propiedades del ratón** del servidor en **Deshabilitar rastro del puntero**.

Valores de servidores Red Hat y SuSE de Linux

Para optimizar el rendimiento, establezca Propiedades del ratón>Velocidad del puntero en **1x**. Para KDE, acceda al **Control Center (Centro de control)**, elija **Peripherals/Mouse (Periféricos/ratón)** y seleccione la ficha **Advanced (Opciones avanzadas)**.

Descripción general de la consola remota basada en texto

iLO y sus antecesores son compatibles con la consola real basada en texto verdadero. La información de vídeo se obtiene a partir del servidor y los contenidos de la memoria de vídeo se envían al procesador de gestión, comprimido, codificado y reenviado a la aplicación cliente de gestión. iLO utiliza un búfer de marco de pantalla, que detecta cambios en la información del texto, codifica los cambios y envía los caracteres (incluida la información de posición de la pantalla) a las aplicaciones cliente basadas en texto. Este método proporciona compatibilidad con los clientes estándar basados en texto, buen rendimiento y simplicidad. No obstante, no es posible mostrar información gráfica o distinta de ASCII y la información de la posición de la pantalla (caracteres mostrados) puede enviarse fuera del orden.

La consola remota utiliza tecnología de teclado, vídeo y ratón virtual (KVM) y no dispone de una verdadera consola basada en texto. iLO 2 utiliza el puerto DVO de adaptador de vídeo para acceder a la memoria de vídeo directamente. Este método aumenta significativamente el rendimiento de iLO 2. Sin embargo, la secuencia de vídeo digital no contiene datos de texto útiles. Los datos que se obtienen a partir del puerto DVO representan los datos gráficos (no basados en caracteres) y no se trata de datos

de texto o ASCII. Una aplicación de cliente basada en texto, por ejemplo, telnet o SSH, no puede procesar los datos de vídeo.

Consola basada en texto durante POST

La consola remota basada en texto de iLO 2 estándar sigue disponible en iLO 2 hasta que la Autocomprobación al arrancar (POST, Power-On Self-Test) del sistema operativo se haya completado. El firmware de iLO 2 estándar sigue utilizando la funcionalidad del puerto serie virtualizado del procesador de gestión. En el firmware iLO 2, el puerto serie virtual ha sido renombrado como consola remota de serie. iLO 2 utiliza la consola de serie remota para acceder a una consola remota basada en texto anterior al sistema operativo. El subprograma de la consola remota de serie de iLO 2 aparece como una consola basada en texto, pero la información se procesa mediante datos de vídeo gráficos. iLO 2 muestra esta información a través del subprograma de la consola remota mientras se encuentra en estado de servidor previo al sistema operativo, lo cual permite a un iLO 2 sin licencia observar e interactuar con el servidor durante actividades de POST.

Para una ranura iLO 2 (y una ranura iLO bajo Linux en formato gráfico), introduzca `getty()` en el puerto serie del servidor y, a continuación, utilice iLO 2 Remote Serial Console o iLO Virtual Serial Port (comando CPL `start /system1/oemhp_vsp1`) para ver una sesión de inicio en el sistema operativo Linux a través del puerto serie.

Una sesión de iLO 2 sin licencia no puede utilizar el acceso a la consola remota después de que el servidor complete la POST y comience a cargar el sistema operativo. Para utilizar la consola remota y la consola de texto de iLO después de POST, es necesario disponer de iLO 2 Advanced o iLO 2 Advanced para BladeSystem.

Consola basada en texto después de POST

La función iLO 2 Text Console after POST (Consola de texto de iLO 2 después de POST) es una consola basada en texto a la que se puede acceder desde telnet o SSH después de POST. Cuando se utiliza SSH, el flujo de datos, incluidas las credenciales de autenticación, es protegido mediante el método de cifrado admitido por el cliente SSH e iLO 2. HP recomienda utilizar SSH para conectarse a la consola de texto de iLO 2.

iLO 2 también admite la utilización de telnet para conectarse a la consola de texto de iLO 2. No obstante, el flujo de datos no se cifra cuando se utiliza una conexión telnet normal. Como parte de la política de seguridad predeterminada, la utilización de telnet está deshabilitada. Es necesario habilitar telnet para permitir el acceso a la CLI y a la consola de texto de iLO 2.

Para obtener más información acerca de la seguridad de los métodos de comunicación utilizados por iLO 2, consulte la sección *Integrated Lights-Out security technology brief (Resumen de la tecnología de seguridad de Integrated Lights-Out)* en la página Web de HP (http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00212796/c00212796.pdf.)

La presentación de los colores, los caracteres y del control de pantalla depende del cliente que está utilizando, y puede ser cualquier telnet estándar (si está habilitado) o cliente SSH compatible con iLO 2. La consola de texto de iLO 2 está habilitada de manera predeterminada en la versión 1.50 y posteriores del firmware de iLO 2. Entre las funciones y la compatibilidad se incluye lo siguiente:

- Visualización de pantallas de modo de texto de 80 x 25 (configuraciones de color estándar) cuando el sistema se encuentra activado, incluyendo:
  - Proceso de arranque del sistema (POST)
  - ROMS de opción estándar
  - Cargadores de arranque de texto (LILO o GRUB)
  - Sistema operativo Linux en modo VGA 80x25

- DOS
- Otros sistemas operativos basados en texto

  La compatibilidad de la pantalla del modo de texto no incluye gráficos, otras resoluciones de texto VGA (132x48, 80x48) ni otras resoluciones de texto implementadas a través de un controlador (implementadas gráficamente.)

- Teclas de acceso directo de la consola remota
- Teclados de idioma internacional (si el sistema del servidor y del cliente se configuran de manera similar)
- Caracteres de dibujo de líneas cuando se seleccionan la fuente y la página de códigos correctas en la aplicación cliente

Para utilizar la función iLO 2 Text Console (Consola de texto de iLO 2) correctamente, es necesario actualizar la memoria ROM del HOST. iLO 2 admite iLO 2 Text Console (Consola de texto iLO 2) en los servidores ProLiant BL460c G1, BL480c G1, ML350 G5, DL360 G5, ML370 G5, DL380 G5, BL680 G5 y DL580 G5 de HP.

Utilización de la consola de texto de iLO

Para iniciar una sesión de la consola de texto de iLO 2:

1. Inicie una sesión de SSH o telnet.

   Asegúrese de ajustar la codificación de caracteres de la aplicación del terminal en Western (ISO-8859-1.)

2. Inicie sesión en iLO 2.
3. Cuando se le solicite, introduzca `textcons`.

   Se visualizará un mensaje en el que se le indicará que el software de la consola de texto de iLO 2 se está iniciando.

Para salir de una consola de texto de iLO 2 y regresar a la sesión de la CLI, pulse las teclas **ESC (** simultáneamente.

Personalización de la consola de texto de iLO 2

Cuando inicie la consola de texto de iLO 2, utilice las opciones y argumentos de comando `textcons` para personalizar el funcionamiento de la pantalla. En general, no es necesario modificar estas opciones.

- Control del índice de muestreo

  Es posible utilizar la opción `textcons speed` para indicar en milisegundos la duración de los períodos comprendidos entre los muestreos. Un período de muestreo es el período de tiempo en el que el firmware de iLO 2 examina los cambios de la pantalla y actualiza la consola de texto de iLO 2. El ajuste de la velocidad puede suavizar el tráfico innecesario en enlaces de red largos o lentos, reducir el ancho de banda utilizado y el tiempo consumido por la CPU de iLO 2. Los valores razonables correspondientes están comprendidos entre 1 y 5000 (entre 1 ms y 5 segundos.) Por ejemplo:

  ```
  textcons speed 500
  ```

- Control del suavizado

  iLO 2 intenta transmitir datos únicamente cuando cambian y se estabilizan en la pantalla. Si una línea de la pantalla de texto está cambiando constantemente de un modo más rápido al que puede mostrar iLO 2, la línea no se transmitirá hasta que se estabilice. Por ejemplo, durante un `ls -R` de un sistema de archivos grande, el monitor físico muestra texto de un modo más rápido del que se puede interpretar. Sucede lo mismo en una sesión de la consola de texto de iLO 2. En este caso, los datos se visualizan rápidamente y son esencialmente indescifrables. Sin embargo, en este caso, los datos se transmiten mediante iLO 2 a través de la red y consumen ancho de banda. El comportamiento predeterminado es el suavizado (retraso 0), mediante el que únicamente se transmiten datos cuando los cambios se estabilizan en la pantalla. Es posible controlar o desactivar la función de suavizado mediante la opción de retraso. Por ejemplo:

  ```
  textcons speed 500 delay 10
  ```

- Control de la compatibilidad de los teclados internacionales

  Durante la utilización de la consola de texto de iLO 2, iLO 2 puede emular la asignación de caracteres entre el cliente, telnet y el servidor. La asignación predeterminada es la correspondiente a la traducción del teclado USB 101 (o la no traducción.)

  Para controlar la traducción, utilice la opción `xlt` con el número de referencia adecuado. Por ejemplo, para ajustar la consola de texto de iLO 2 en un índice de muestreo de 50 ms mediante la traducción de un teclado británico, introduzca:

  ```
  textcons speed 50 xlt 41
  ```

  Para traducir a otro idioma, utilice una de las siguientes opciones:

Teclado	Número de referencia
Estados Unidos	0
Británico	1
Belga	2
Danés	3
Finés	4
Francés	5
Francés (Canadá)	6

Teclado	Número de referencia
Alemán	7
Italiano	8
Español (América Latina)	9
Noruego	10
Portugués	11
Español	12
Sueco	13
Francés (Suiza)	14
Alemán (Suiza)	16

- Configuración de las teclas de acceso directo de la consola remota

  Para utilizar las secuencias de teclas especiales que no se pueden copiar en el cliente de la consola remota, las teclas de acceso directo de la consola remota configuradas para la consola remota funcionan en la consola de texto de iLO 2. Para obtener más información, consulte la sección "Teclas de acceso directo de la consola remota (Teclas de acceso directo de la consola remota en la página 93)".

- Configuración de la asignación de caracteres

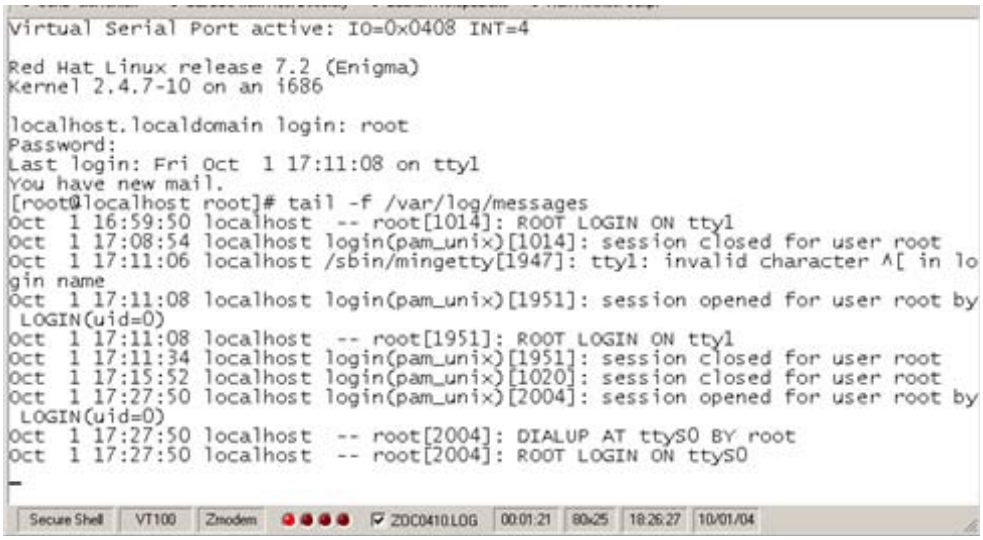
  En general, en el conjunto de caracteres ASCII, CONTROL (caracteres ASCII superiores a 32) no se puede imprimir ni visualizar. Estos caracteres pueden utilizarse para representar elementos como flechas, estrellas o círculos. Algunos de estos caracteres se asignan a representaciones de código ASCII equivalentes. A continuación se enumeran los equivalentes admitidos:

Valor del carácter	Descripción	Equivalente asignado
0x07	Asterisco pequeño	*
0x0F	Asterisco	*
0x10	Puntero hacia la derecha	>
0x11	Puntero hacia la izquierda	<
0x18	Flecha arriba	^
0x19	Flecha abajo	v
0x1A	Flecha izquierda	>
0x1B	Flecha derecha	>
0x1E	Puntero hacia arriba	^
0x1F	Puntero hacia abajo	v
0xFF	Bloque sombreado	espacio en blanco

Utilización de una sesión de Linux

Es posible ejecutar un puerto serie virtual de iLO 2 en un sistema Linux si el sistema está configurado para presentar una sesión de terminal en el puerto serie. Esta función permite utilizar un servicio de registro remoto. Es posible iniciar sesión de manera remota en el puerto serie y redireccionar el

resultado a un archivo de registro. Los mensajes del sistema dirigidos al puerto serie se registrarán de manera remota.



Algunos modos de texto de Linux son en realidad modos gráficos y no pueden visualizarse mediante la consola de texto de iLO 2. Por ejemplo, los terminales de SLES son texto en modo de gráficos, y aunque parece que están basados en texto, no se visualizan correctamente en la consola de texto de iLO 2. Si intenta utilizar un modo no compatible, la consola de texto de iLO 2 muestra un mensaje en el que se indica que el servidor está utilizando un modo gráfico.

Es posible que algunas secuencias de caracteres del teclado requeridas por Linux en el modo de texto no puedan pasarse a la consola de texto de iLO 2. Por ejemplo, la combinación de teclas alt + tabulador puede ser interceptada por el cliente. Para solucionar estos problemas, configure una tecla de acceso directo para la combinación de teclas. Para obtener más información, consulte la sección "Teclas de acceso directo de la consola remota (Teclas de acceso directo de la consola remota en la página 93)".

Puerto serie virtual y consola remota de serie

El procesador de gestión contiene el hardware de puerto serie que puede sustituir al puerto serie físico en la placa principal del servidor. Mediante un conmutador electrónico, el firmware de iLO 2 desconecta el puerto serie físico del servidor y ordena a su propio hardware de puerto serie que se conecte. El hardware de puerto serie iLO 2 establece una conexión entre el servidor y la red del procesador de gestión. El firmware encapsula los caracteres que envía el servidor al puerto serie en los paquetes de red y envía estos paquetes al subprograma o aplicación de la consola remota de serie (la aplicación puede ser un cliente SSH o telnet.) Los caracteres que envía la aplicación o subprograma remoto se recopilan en los paquetes de red y se envían al firmware de iLO 2 que, a continuación, extrae los caracteres y los incluye en el servidor. La consola remota de serie de iLO 2 proporciona una ruta bidireccional de comunicación serie entre el usuario remoto y el servidor.

Mediante la consola remota de serie de iLO, el usuario remoto puede llevar a cabo operaciones como, por ejemplo, la interacción con la secuencia POST del servidor y la secuencia de arranque del sistema operativo; el establecimiento de una sesión de inicio con el sistema operativo, la interacción con el sistema operativo y la ejecución e interacción con aplicaciones en el sistema operativo del servidor. Los usuarios del sistema operativo Microsoft® Windows Server™ 2003 pueden ejecutar el subsistema del EMS a través de la consola remota de serie. EMS resulta de utilidad para la depuración de los problemas y arranque del sistema operativo en el nivel kernel del sistema operativo.

Consola remota de serie

La consola remota de serie permite acceder a una consola de serie VT320 desde una consola basada en un subprograma de Java™ conectada al puerto serie virtual de iLO 2. Iniciar la consola remota de serie permite intercambiar datos de texto con el host. La opción Remote Serial Console (Consola remota de serie) es compatible con los sistemas operativos host Windows® y Linux y requiere JVM.

El flujo de datos es una corriente bidireccional que se envía al puerto serie del servidor. En un puerto serie de servidor HP ProLiant pueden aparecer tres tipos de datos:

- Consola EMS de Windows®
- Sesión de usuario Linux mediante la serie tty (ttyS0)
- Diálogo System POST (si está activada el redireccionamiento de la consola de serie BIOS)

La configuración actual se muestra en la página de información de la consola remota cuando hace clic en la ficha Remote Console (Consola remota.) Puede modificar la configuración actual mediante el uso de la utilidad RBSU del sistema host, a la que se accede durante el reinicio del servidor.

Configuración de la consola remota de serie

Para un buen uso de la consola remota de serie, el software y el firmware del servidor deben estar configurados correctamente. Para configurar el firmware POST del servidor, se deberá invocar la utilidad RBSU del sistema del servidor para establecer los parámetros del puerto serie. Debe configurar la RBSU para activar el modo BIOS Serial Console Redirection (Redireccionamiento de la consola de serie BIOS.) Este modo da instrucciones a la memoria ROM del sistema del servidor para enviar datos al puerto serie del servidor y recibir datos de él. Cuando el firmware de iLO 2 entra en modo Remote Serial Console (Consola remota de serie), iLO 2 activa un puerto serie en lugar de un puerto serie de servidor, intercepta y retransmite los datos salientes al cliente de consola remota de serie, recibe datos entrantes(del cliente de consola remota de serie) y los retransmite a la memoria ROM del sistema.

Una vez que el servidor haya finalizado el proceso POST, la memoria ROM del sistema de servidor transfiere el control al cargador de inicio del sistema operativo. Si utiliza Linux, puede configurar el cargador de inicio del sistema operativo para que interactúe con el puerto serie del servidor en lugar de hacerlo con el teclado, el ratón y la consola VGA. Este valor de configuración permite ver e interactuar

con la secuencia de inicio del sistema operativo a través de la consola remota de serie. Consulte la sección "Ejemplo de configuración con Linux" (Ejemplo de configuración con Linux en la página 114) para ver un ejemplo de un cargador de inicio del sistema operativo Linux.

Una vez finalizado el cargador de inicio del sistema operativo, el sistema operativo prosigue con la carga. Si utiliza el sistema operativo Linux, puede configurarlo para que proporcione una sesión de registro al sistema a través del puerto serie, lo que permite que la consola remota de serie le solicite el ID de registro y la contraseña como usuario del sistema. Este valor de configuración permite interactuar con el sistema operativo como usuario o como administrador del sistema.

Aunque para utilizar la consola remota de serie se requieren más pasos de configuración que para utilizar la consola remota o IRC, la consola remota de serie permite a los usuarios telnet o SSH interactuar con el servidor de forma remota y sin necesidad de disponer de una licencia avanzada iLO 2 y es la única forma en que iLO 2 presenta una consola remota basada en texto real.

Ejemplo de configuración con Linux

El cargador de inicio es la aplicación que se carga desde el dispositivo ejecutable cuando el ROM del sistema de servidor finaliza POST. Para los sistemas operativos Linux, el cargador de inicio que se utiliza generalmente es GRUB. Para configurar GRUB para que utilice la consola remota de serie, modifique el archivo de configuración de GRUB tenga un aspecto parecido al siguiente (muestra de Red Hat Linux 7.2):

```
serial -unit=0 -speed=115200
terminal -timeout=10 serial console
default=0
timeout=10
#splashimage=(hd0,2) /grub/splash.zpm.gz
title Red Hat Linux (2.4.18-4smp)

root (hd0,2)
kernel /vmlinuz-2.4.18-4smp ro root=/dev/sda9 console=tty0
console=ttyS0,115200
initrd /initrd-2.4.18-rsmp.img
```

Una vez que Linux se haya iniciado completamente, se puede redirigir una consola de registro a un puerto serie. Los dispositivos /dev/ttyS0 y /dev/ttyS1, si están configurados, permiten obtener sesiones tty de serie a través de la consola remota de serie. Para iniciar una sesión shell en un puerto de serie configurado, añada la línea siguiente al archivo /etc/inittab para empezar el proceso de registro automáticamente durante el inicio del sistema (este ejemplo invoca la consola de registro en /dev/ttyS0):

```
Sx:2345:respawn:/sbin/agetty 115200 ttyS0 vt100
```

Para obtener más información acerca de la configuración de Linux para utilizarlo con la consola remota de serie, consulte la publicación técnica *Integrated Lights-Out Virtual Serial Port configuration and operation HOWTO (Configuración y funcionamiento del puerto serie virtual de Integrated Lights-Out)* en la página Web de HP (http://www.hp.com/servers/lights-out.)

Mejoras del puerto serie virtual

El firmware de iLO 2 1.35 implementa un indicador dinámico que informa inmediatamente a la memoria ROM del sistema de servidor de una conexión iLO 2 Remote Serial Console. Una vez que el código POST de la memoria ROM del sistema reconoce la conexión de la consola remota de serie, el sistema empieza a redirigir los datos de entrada y salida al puerto serie del servidor y a la consola remota de serie. Es posible establecer una sesión de consola remota de serie en cualquier momento antes o durante la secuencia POST del sistema, y también ver y modificar el proceso POST. Una vez desconectada la sesión de la consola remota de serie, el firmware de iLO 2 reinicia el indicador dinámico para informar a la memoria ROM del sistema de servidor de que la sesión ha dejado de estar activa. A

continuación, la memoria ROM del sistema de servidor cancela la redirección al puerto serie del servidor.

La instalación de la utilidad RBSU de la memoria ROM del sistema se debe configurar para utilizar el puerto serie virtual iLO 2 para que esta mejora sea operativa. Si desea obtener más información, consulte la sección "Configuración de la consola remota de serie (Configuración de la consola remota de serie en la página 113)".

Consola EMS de Windows®

La consola Windows® EMS, si está activada, proporciona la capacidad de realizar EMS en los casos donde se ha impedido el funcionamiento normal del vídeo, los controladores de dispositivos u otras funciones del sistema operativo así como la realización de acciones correctivas normales.

No obstante, iLO 2 permite utilizar EMS en la red con un explorador Web. Microsoft® EMS le permite mostrar procesos que se están ejecutando, cambiar la prioridad de los mismos y detenerlos. La consola EMS y la consola remota de iLO 2 pueden utilizarse al mismo tiempo.

El puerto serie de Windows® RMS se debe activar mediante la utilidad RBSU del sistema host. La configuración permite la activación o desactivación del puerto EMS así como la selección del puerto COM. El sistema iLO 2 detecta automáticamente si el puerto EMS está activado o desactivado y la selección del puerto COM.

Para obtener la línea de comandos `SAC>`, es posible que haya que escribir `Enter` después de conectar a través de la consola de puerto serie virtual.

Para obtener más información acerca de las funciones EMS, consulte la documentación de Windows® Server 2003.

Modo no procesado de puerto serie virtual

Es posible utilizar la función de puerto serie virtual de iLO 2 para conectar el Windows® Kernel Debugger® de un cliente remoto a través de WiLODbg.exe. WiLODbg.exe omite la descodificación de bytes del firmware de iLO 2. Tras omitir la descodificación de bytes, el puerto serie virtual se encuentra en modo RAW (no procesado) y se envía directamente al puerto serie.

La utilidad WiLODbg.exe se ejecuta en un sistema cliente con la aplicación WinDBG.exe o KD.exe de Microsoft® instaladas. Cuando se ejecuta WiLODbg.exe, se establece una conexión de puerto serie virtual con iLO 2 y se activa el modo RAW. Además, WiLODbg.exe inicia WinDBG.exe automáticamente con los conmutadores adecuados necesarios para que WinDBG.exe establezca la conexión con el dispositivo iLO 2 remoto.

Para configurar el servidor, debe configurar la utilidad RBSU del sistema:

1. Para activar un puerto serie virtual, asigne el puerto serie virtual un puerto COM desde el menú System Options (Opciones del sistema.)
2. Establezca la opción BIOS Serial Console Port (Puerto de consola de serie BIOS) y EMS Console (Consola EMS) en **Disable (Desactivar)** o ajústela en el mismo puerto que un puerto serie integrado.
3. Establezca el puerto de depuración de Microsoft® Windows® en el mismo puerto que el puerto serie virtual. Puede utilizar el comando `bootcfg` o modificar el archivo boot.ini.

   Ejemplo si se utiliza el comando `bootcfg`:

   En la línea de comandos de un servidor Windows®, introduzca el siguiente comando:

   ```
   Bootcfg /debug on /port com2 /baud 115200 /id 1
   ```

   Ejemplo de un archivo boot.ini modificado:

```
[boot loader]
timeout=5
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Debug (com2)" /
fastdetect /debug /debugport=com2 /baudrate=115200
```

Si el servidor se ha configurado para arrancar en modo de depuración y se ha establecido una conexión con el puerto serie virtual normal durante el arranque del servidor, se enviará una serie de bytes de datos de depuración al cliente del puerto serie virtual. Para evitar que esto se produzca, no arranque el servidor en modo de depuración cuando se encuentre en uso una conexión de puerto serie virtual normal.

En Serial Port Configuration (Configuración de puerto serie) se muestra información acerca de la configuración del servidor, los puertos serie disponible y el estado del puerto serie virtual. Los estados que se muestran son:

- Available (Disponible): el puerto serie virtual no se está utilizando
- In use (Utilizado): el modo normal se encuentra ajustado cuando el puerto serie virtual se encuentra conectado normalmente
- In use (En uso): modo no procesado cuando se utiliza la utilidad WiLODbg.exe para la conexión

Cuando el puerto serie virtual está en uso, el botón Disconnect (Desconectar) está activado y puede utilizarse para finalizar cualquier tipo de conexión de puerto serie virtual. Si se hace uso de las funciones Disconnect (Desconectar) para finalizar una conexión establecida a través de SSH con un puerto serie virtual, la conexión con SSH se cancela por completo y no se vuelve a la línea de comandos `<hpiLO->`. Se producirá una desconexión similar si la conexión del puerto serie virtual se establece a través de telnet. Si se utiliza un subprograma de conexión serie remota para establecer la conexión desde un explorador, el subprograma se desconectará. Para restablecer la conexión serie remota, es necesario cerrar y volver a abrir la ventana del subprograma.

Uso de un Windows Kernel Debugger remoto

Para iniciar un Windows® Kernel Debugger, debe ejecutar la utilidad WiLODbg.exe en un sistema cliente que tenga instalado WinDBG.exe o KD.exe de Microsoft® y, a continuación, reiniciar el servidor remoto en modo de depuración para conectar el depurador. WiLODbg ejecuta automáticamente WinDBG.exe o KD.exe. Por ejemplo:

```
WiLODbg <IP Address>[ -c CommandLine][ -e][ -k][ -p Password][ -s
SocketNumber][
-t][ -u Username]
If a parameter has whitespace in it, enclose it in quotes.
```

Parámetros necesarios:

`IP Address = <String>`: dirección IP en formato por puntos o nombre UNC completo. <String> es una serie de caracteres. Los parámetros necesarios deben indicarse en el orden que se muestra en el ejemplo.

Parámetros opcionales:

- `-c CommandLine = <String>`: proporciona parámetros adicionales de la línea de comandos al depurador seleccionado. Si existen espacios integrados o guiones (-) deben incluirse entre comillas. <String> es una serie de caracteres.
- `-e = <Boolean>`: permite activar el cifrado del enlace de las comunicaciones. En esta versión, el cifrado únicamente funciona con la opción de telnet. Esta opción está desactivada de forma predeterminada.

- `-k = <Boolean>`: utilice KD en lugar de WinDbg. De forma predeterminada, se utiliza WinDbg.
- `-p Password = <String>`: permite ajustar la contraseña para utilizarla para el inicio de sesión en iLO 2. Si no se suministra una contraseña, se solicitará una. `<String>` es una serie de caracteres.
- `-s SocketNumber = <Integer>`: establece el número de socket para la conexión con iLO 2. SocketNumber (Número de socket) debe coincidir con los parámetros de Raw Serial Data Port (Puerto de datos de serie no procesado) del iLO 2 al que se conecta. El socket predeterminado es 3002. `<Integer> = [sign]digits.`
- `-t = <Boolean>`: esta utilidad del depurador permite utilizar de forma indirecta una conexión telnet. La configuración predeterminada es la conexión del socket con el socket 3002.
- `-u Username = <String>`: permite ajustar el nombre de usuario para el inicio de sesión en iLO 2. Si no se suministra un nombre de usuario, se solicitará uno. <String> es una serie de caracteres. Las opciones no siguen un orden determinado.

Ejemplo de líneas de comandos:

- Para establecer la conexión con iLO 2 en 16.100.226.57, valide el usuario con el nombre de usuario `admin` y la contraseña `mypass` e inicie WinDBG.exe con la línea de comandos adicional:

  ```
  wilodbg 16.100.226.57 -c "-b" -u admin -p mypass
  ```

  En este ejemplo se inicia WinDBG.exe con una línea de comandos adicional de `-b` y se utiliza una conexión de socket directa de WinDBG.exe a iLO 2 a través del puerto 3002.

- Para establecer la conexión con iLO 2 en 16.100.226.57, valide el usuario de iLO 2 con el nombre de usuario `admin` y la contraseña `mypass` e inicie `kd` con una línea de comandos adicional para `kd` de `-b`:

  ```
  wilodbg 16.100.226.57 -k -c "-b" -u admin -p mypass -s 7734
  ```

  En este ejemplo se inicia `kd` con una línea de comandos adicional para `kd` de `-b` y se utiliza una conexión de socket directa de `kd` a iLO 2 a través del puerto 7734. Para hacer uso de este ejemplo, es necesario configurar iLO 2 para que utilice el puerto 7734.

- Para establecer la conexión con iLO 2 en 16.100.226.57 y solicitar un nombre de usuario y contraseña:

  ```
  wilodbg 16.100.226.57 -c "-b" -t -e
  ```

  En este ejemplo se inicia WinDBG.exe con una línea de comandos adicional de `-b`, se hace uso de una conexión de telnet cifrada de WiLODbg a iLO 2 y los datos de WinDBG.exe se transmiten a la conexión cifrada de telnet a través de la utilidad.

Soportes virtuales

Virtual Media es una función con licencia. Si no dispone de licencia aparece el mensaje `iLO 2 feature not licensed (La función iLO 2 no dispone de licencia).` Si desea obtener más información, consulte "Concesión de licencias (Concesión de licencias en la página 21)". La capacidad de utilizar Virtual Media de iLO 2 se otorga o restringe con los privilegios de usuario de iLO 2. Debe disponer de privilegios de soportes virtuales para seleccionar un dispositivo de soporte virtual y conectarlo al servidor host.

La opción Virtual Media (Soportes virtuales) de iLO 2 proporciona una unidad de CD/DVD-ROM y una unidad de disquete virtual, que pueden indicar a un servidor host remoto que reinicie y utilice soportes estándar desde cualquier punto de la red. Los dispositivos de soportes virtuales se encuentran

disponibles cuando el sistema host se está reiniciando. Los dispositivos de soportes virtuales de iLO 2 se conectan al servidor host mediante tecnología USB. USB también proporciona nuevas funciones a los dispositivos de soportes virtuales de iLO 2 cuando se conectan a sistemas operativos compatibles con USB. Los diferentes sistemas operativos proporcionan distintos niveles de compatibilidad con USB.

- Si está activada la función de disquete virtual, a la unidad de disquete no puede accederse desde el sistema operativo del cliente.
- Si está activada la función de CD/DVD-ROM virtual, no es posible acceder a la unidad de CD/DVD-ROM desde el sistema operativo cliente.

△ **PRECAUCIÓN:** Para evitar que se produzcan daños en los archivos y en los datos, no acceda al soporte local cuando utilice un soporte local como soporte virtual.

Puede acceder a los soportes virtuales de un servidor host de un cliente mediante una interfaz gráfica que emplee un subprograma Java™ y mediante una interfaz de secuencia de comandos que emplee un motor XML. El subprograma de Virtual Media no dispone de un tiempo de espera cuando Virtual Media está conectado al servidor host. El subprograma Virtual Media se cierra si el usuario cierra sesión.

Para acceder a dispositivos Virtual Media de iLO 2 mediante la interfaz basada en el explorador, haga clic en **Virtual Media (Soporte virtual)>Virtual Media Applet (Subprograma de soporte virtual)**. Un subprograma carga la compatibilidad con el dispositivo de disquete o CD/DVD-ROM virtual.

También puede acceder a los soportes virtuales a través de la consola remota integrada. La consola remota integrada permite acceder a KVM y controlar Virtual Power (Alimentación virtual) y Virtual Media (Soporte virtual) desde una misma consola en Microsoft® Internet Explorer. Para obtener más información acerca del acceso a Virtual Power (Alimentación virtual) y Virtual Media (Soporte virtual) mediante la consola remota integrada, consulte la sección "Opción de Consola remota integrada" (Opción de Consola remota integrada en la página 96.)

Uso de los dispositivos de soportes virtuales de iLO 2

Puede acceder a los soportes virtuales de un servidor host de un cliente mediante una interfaz gráfica que emplee un subprograma Java™ y mediante una interfaz de secuencia de comandos que emplee un motor XML.

Para acceder a los dispositivos de soportes virtuales de iLO 2 mediante una interfaz gráfica, seleccione **Virtual Media (Soportes virtuales)** en la ficha Virtual Devices (Dispositivos virtuales.) Un subprograma carga la compatibilidad con el dispositivo de disquete o CD/DVD-ROM virtual.

Virtual Media y Windows 7

De manera predeterminada, Windows 7 desactiva la alimentación del concentrador virtual de ILO si no hay ningún dispositivo de soporte virtual activado o conectado durante el arranque. Para evitar este problema, anule manualmente la función de gestión de la alimentación en Windows 7 a través del Panel de control para que el concentrador virtual no se apague.

1. Abra **Administrador de dispositivos**.
2. Haga clic en **Ver**.
3. Seleccione **Dispositivos por conexión** en el menú.
4. Seleccione y amplíe **Controladora de host PCI a USB estándar universal** para visualizar los dispositivos USB, incluido el concentrador USB genérico. La opción Concentrador USB genérico corresponde al controlador de concentrador USB virtual de iLO 2.
5. Haga clic con el botón derecho del ratón en **Concentrador USB genérico** y seleccione **Propiedades**.

6. Seleccione la ficha **Administración de energía**.
7. Desmarque la casilla de verificación **Permitir que el equipo apague este dispositivo para ahorrar energía**.

Disquete/llave USB virtual de iLO 2

La unidad de disquete virtual de iLO 2 está disponible durante el reinicio del servidor para todos los sistemas operativos. Si inicia el sistema desde el disquete virtual de iLO 2, podrá actualizar la ROM del sistema host, distribuir un sistema operativo desde unidades de red y realizar la recuperación tras fallos en los sistemas operativos, etc.

Si el sistema operativo del servidor host admite dispositivos de almacenamiento masivo con conexión USB o dispositivos digitales seguros, la unidad de disquete/llave USB virtual de iLO 2 también estará disponible una vez cargado el sistema operativo del servidor host. Puede utilizar la unidad de disquete/llave USB virtual de iLO 2 cuando el sistema operativo del servidor se ejecuta para actualizar controladores de dispositivos, crear un disquete de reparación de emergencia y realizar otras tareas. Puede resultar especialmente útil disponer del disquete virtual cuando el servidor está ejecutándose si usted tiene que diagnosticar y reparar un problema con el controlador NIC.

La opción Virtual Floppy/USBKey (Disquete/llave USB virtual) puede ser la unidad física de disquete, de llave USB o la unidad digital segura en la que se ejecuta el explorador web o un archivo de imagen almacenado en la unidad de disco duro local o en la unidad de red. Para obtener un rendimiento máximo, HP recomienda utilizar ficheros de imágenes locales almacenados en la unidad de disco duro del PC cliente o en una unidad de red accesible mediante un enlace de red de alta velocidad.

Para utilizar una unidad de disquete o de llave USB física en el PC cliente.

1. Seleccione **Local Media Drive (Unidad de soporte local)** en la sección Virtual Floppy/USBKey (Unidad USB/disquete virtual.)
2. Seleccione la letra de la unidad local deseada de disquete o de llave USB en el PC cliente en el menú desplegable. Para garantizar que el disquete origen o el archivo de imagen no se modifica durante el empleo, seleccione la opción **Force read-only access (Acceso obligado de sólo lectura)**.
3. Haga clic en **Connect (Conectar)**.

El icono de la unidad conectada y el LED cambiarán de estado para reflejar el estado actual de la unidad de disquete virtual.

Para utilizar un archivo de imagen:

1. Seleccione **Local Image File (Archivo de imágenes local)** dentro de la sección Virtual Floppy/USBKey (Disquete/llave USB virtual) del subprograma Virtual Media.
2. Introduzca la ruta o el nombre de archivo de la imagen en el cuadro de texto o haga clic en **Browse (examinar)** para localizar el archivo de imagen mediante el diálogo **Choose Disk Image File (Seleccionar archivo de imágenes de disco)**. Para garantizar que el disquete origen o el archivo de imagen no se modifica durante el empleo, seleccione la opción **Force read-only access (Acceso obligado de sólo lectura)**.
3. Haga clic en **Connect (Conectar)**.

El icono de la unidad conectada y el LED cambiarán de estado para reflejar el estado actual de la unidad de disquete o llave USB virtuales o el dispositivo digital seguro. Una vez establecida la conexión, el servidor host podrá disponer de los dispositivos hasta que se cierre del subprograma Virtual Media. Cuando haya finalizado, puede desconectar el dispositivo del servidor host o cerrar el subprograma.

NOTA: El subprograma Virtual Media debe permanecer abierto en el explorador mientras se utilice un dispositivo de Virtual Media.

El servidor host podrá disponer del disquete/llave USB virtual de iLO 2 durante la ejecución si el sistema operativo del servidor host admite unidades de disquete o de llave USB. Consulte “Compatibilidad con USB del sistema operativo” (Compatibilidad con USB del sistema operativo en la página 121) para obtener información sobre los sistemas operativos que son compatibles con el almacenamiento masivo USB en el momento de la publicación del presente manual.

El disquete/llave USB virtual de iLO 2 aparece ante el sistema operativo igual que cualquier otra unidad. Al utilizar iLO 2 por primera vez, el sistema operativo del host le sugerirá instalar un asistente de nuevo hardware encontrado.

Al acabar de utilizar los soportes virtuales de iLO 2 y desconectarlos, recibirá un mensaje de advertencia del sistema operativo del host respecto a la eliminación poco segura de un dispositivo. Esta advertencia puede evitarse si utiliza la característica proporcionada por el sistema operativo para detener el dispositivo antes de desconectarlo de los Soportes virtuales.

Notas acerca de los sistemas operativos del disquete/llave USB virtual

- MS-DOS

  Durante el inicio del sistema y sesiones de MS-DOS, el dispositivo de disquete virtual aparece como unidad de disquete estándar del BIOS. Este dispositivo aparece como unidad A. Si existe una unidad de disquete físicamente conectada, permanecerá oculta y no disponible durante este período de tiempo. La unidad de disquete local física y el disquete virtual no se pueden usar simultáneamente.

- Windows Server® 2008 o posterior y Windows Server® 2003

  Las unidades de disquete y de llave USB virtuales aparecen automáticamente después de que Microsoft® Windows® detecte la instalación del dispositivo USB. Úselas como si se tratase de un dispositivo localmente asociado.

  Para utilizar el disquete virtual durante la instalación de Windows® como disquete de controladores, desactive la unidad integrada en la RBSU del host, la cual fuerza al disquete virtual a aparecer como unidad A.

  Para utilizar la llave USB virtual durante una instalación de Windows® como un disquete de controladores, cambie el orden de arranque de la unidad de llave USB en la RBSU del sistema. En el orden de arranque, HP recomienda colocar la unidad de llave USB en primer lugar.

- Windows Vista®

  Los soportes virtuales no funcionan correctamente con un sistema operativo Windows Vista® que utilice Internet Explorer 7 con la opción Modo protegido activada. Si intenta utilizar los soportes virtuales con la opción de modo protegido activada, se mostrarán varios mensajes de error, entre ellos, `could not open cdrom (the parameter is incorrect (No se ha podido abrir el cdrom [el parámetro no es correcto])`. Para utilizar los soportes virtuales, haga clic en **Herramientas/Opciones de Internet/Seguridad**, elimine **Habilitar Modo protegido** y, a continuación, haga clic en **Aplicar**. Tras desactivar el modo protegido, debe cerrar todas las instancias de explorador abiertas y reiniciar el explorador.

- NetWare 6.5

  NetWare 6.5 es compatible con disquetes y unidades de llave USB. Consulte "Montaje de un disquete/llave USB virtual en NetWare 6.5" (Montaje de un disquete/llave USB virtual en NetWare 6.5 en la página 122) para obtener instrucciones detalladas al respecto.

- Red Hat y SUSE Linux

  Linux es compatible con disquetes y llaves USB. Consulte "Montaje de soportes/llaves USB virtuales en Linux" (Montaje de soportes/llaves USB virtuales en Linux en la página 122) para obtener instrucciones detalladas al respecto.

Compatibilidad con USB del sistema operativo

Para utilizar dispositivos de soportes virtuales su sistema operativo debe permitir la utilización de dispositivos USB. Su sistema operativo debe permitir además dispositivos de almacenamiento masivo USB. En la actualidad, Windows Server® 2008, Windows® 2003, Red Hat Enterprise Linux 3, Red Hat Enterprise Linux 4, Red Hat Enterprise Linux 5, SUSE SLES 9 y SUSE SLES 10 admiten dispositivos USB. Es posible que haya otros sistemas operativos que también sean compatibles con los dispositivos de almacenamiento masivo USB.

Durante el inicio del sistema, el BIOS del ROM proporcionará compatibilidad con USB hasta que el sistema operativo se cargue. Como MS-DOS utiliza el BIOS para comunicarse con los dispositivos de almacenamiento, los disquetes de la utilidad que inician DOS también funcionarán con un soporte virtual.

NOTA: Red Hat Enterprise Linux 3 no permitirá proporcionar un disquete de controlador mediante un soporte virtual.

Montaje de un disquete/llave USB virtual en NetWare 6.5

1. Acceda a iLO 2 mediante un explorador.
2. Seleccione **Virtual Media (Soportes virtuales)** en la ficha Virtual Devices (Dispositivos virtuales.)
3. Inserte el soporte en la unidad de disquete local, seleccione una unidad de disquete y haga clic en **Connect (Conectar)**. O bien, seleccione la imagen de disquete que desee utilizar y haga clic en **Connect (Conectar)**.

En NetWare 6.5, use el comando `lfvmount` en la consola del servidor para asignar una letra de unidad al dispositivo.

El sistema operativo NetWare 6.5 asignará la primera letra de unidad disponible a la unidad de disquete virtual. Ahora se puede usar el comando `volumes` en la consola del servidor para mostrar el estado de montaje de esta nueva unidad.

Cuando se muestre la letra de unidad, se podrá acceder a la unidad a través de la GUI del servidor, así como la consola del sistema.

Una vez montada la unidad de disquete virtual, si se cambia el soporte en la unidad de disquete local, se deberá usar de nuevo el comando `lfvmount` en la consola del servidor para ver los nuevos soportes en el sistema operativo NetWare 6.5.

Montaje de soportes/llaves USB virtuales en Linux

1. Acceda a iLO 2 mediante un explorador.
2. Seleccione **Virtual Media (Soportes virtuales)** en la ficha Virtual Devices (Dispositivos virtuales.)
3. Seleccione una unidad o una imagen de disquete.
   a. Para una unidad de disquete o de imagen, seleccione Local Media Drive (Unidad de soporte local) o Local Image File (Archivo de imagen local) y haga clic en **Connect (conectar)**.
   b. Para una imagen o unidad de llave USB, seleccione Local Image File (Archivo de imagen local) y haga clic en **Connect (conectar)**.

      Para unidades físicas de llave USB, escriba `/dev/sda` en el cuadro de texto Local Image File (archivo de imagen local.)
4. Cargue los controladores USB usando los comandos siguientes:

```
modprobe usbcore
modprobe usb-storage
modprobe usb-ohci
```

5. Cargue el controlador de disco SCSI usando los comandos siguientes:

```
modprobe sd_mod
```

6. Monte la unidad.
   - Para montar la unidad de disquete, utilice el comando siguiente:

     ```
     mount /dev/sda /mnt/floppy –t vfat
     ```
   - Para montar la unidad de llave USB, utilice el comando siguiente:

     ```
     mount /dev/sda1 /mnt/keydrive
     ```

NOTA: Use el comando `man mount` para tipos de sistemas de archivos adicionales.

La unidad de disquete y de llave pueden usarse en un sistema de archivos Linux si está configurado como tal mediante el comando `mount`. No obstante, a los disquetes de 1,44 Mb se suele acceder mediante las utilidades mtools distribuidas con Red Hat y SLES. La configuración predeterminada de mtools no reconoce un disquete conectado a USB. Para activar los diversos comandos m con el fin de acceder al dispositivo de disquete virtual, modifique el archivo /etc/mtools.conf existente y añada la siguiente línea:

```
drive v: file="/dev/sda" exclusive
```

Para activar los diversos comandos mtools con el fin de acceder al dispositivo de llave USB virtual, modifique el archivo /etc/mtools.conf existente y añada la siguiente línea:

```
drive v: file="/dev/sda1" exclusive
```

Para realizar una lista de la tabla de partición del dispositivo de llave USB virtual para hallar la partición deseada, utilice el comando siguiente:

```
fdisk -l /dev/sda
```

Mediante esta modificación, el conjunto de mtools puede acceder al disquete virtual como v. Por ejemplo:

```
mcopy /tmp/XXX.dat v:
mdir v:
mcopy v:foo.dat /tmp/XXX
```

Cambio de disquetes

Al utilizar la unidad de disquete o de llave USB virtual iLO 2, si la unidad de disquete físico en el equipo cliente es una unidad de disquete USB, no se reconocerán las operaciones de cambio de disco. Por ejemplo, en esta configuración, si se obtiene una lista de directorio de un disquete y se cambia el disquete, la consiguiente lista de directorio mostrará la lista para el primer disquete. Si al utilizar el disquete /llave USB virtual de iLO 2 son necesarios cambios de disco, asegúrese de que el equipo cliente contiene una unidad de disquete que no sea USB.

CD/DVD-ROM virtual de iLO 2

El CD/DVD-ROM virtual de iLO 2 está disponible durante el reinicio del servidor para todos los sistemas operativos especificados en la sección “Compatibilidad con USB del sistema operativo” (Compatibilidad con USB del sistema operativo en la página 121.) Si reinicia el sistema desde el CD/DVD-ROM virtual de iLO 2, podrá distribuir un sistema operativo desde unidades de red, realizar la recuperación tras fallo en los sistemas operativos, etc.

Si el sistema operativo del servidor host admite dispositivos de almacenamiento masivo con conexión USB, la unidad de CD/DVD-ROM virtual de iLO 2 también estará disponible una vez cargado el sistema operativo del servidor host. Puede utilizar la unidad de CD/DVD-ROM virtual de iLO 2 cuando el sistema operativo del servidor host se ejecuta para actualizar controladores de dispositivos, instalar software y realizar otras tareas. Puede resultar especialmente útil disponer del CD/DVD-ROM virtual cuando el servidor está ejecutándose si tiene que diagnosticar y reparar un problema con el controlador de NIC

El CD/DVD-ROM virtual puede ser la unidad de CD/DVD-ROM física en la que se ejecuta el explorador Web o un archivo de imagen almacenado en la unidad de disco duro local o en una unidad de red.

NOTA: Para obtener un rendimiento óptimo, utilice archivos de imágenes. HP recomienda utilizar archivos de imágenes locales almacenados en la unidad de disco duro del PC cliente o en una unidad de red accesible mediante un enlace de red de alta velocidad.

Para utilizar una unidad de CD/DVD-ROM física en el PC cliente.

1. Seleccione **Local Media Drive (Unidad de soporte local)** en la sección Virtual CD/DVD-ROM (CD/DVD-ROM virtual.)
2. En el menú desplegable, seleccione la letra de la unidad de CD/DVD-ROM física deseada en el PC cliente.
3. Haga clic en **Connect (Conectar)**.

Para utilizar un archivo de imagen:

1. Seleccione **Local Image File (Archivo de imágenes local)** dentro de la sección Virtual CD/DVD-ROM (CD/DVD-ROM virtual) del subprograma Virtual Media (Soportes virtuales.)
2. Introduzca la ruta o el nombre de archivo de la imagen en el cuadro de texto o haga clic en **Browse (Examinar)** para localizar el archivo de imagen mediante el diálogo Choose Disk Image File (Seleccionar archivo de imágenes de disco.)
3. Haga clic en **Connect (Conectar)**.

El icono de la unidad conectada y el indicador LED cambiarán de estado para reflejar el estado actual de la unidad de CD/DVD-ROM virtual. Una vez establecida la conexión, el servidor host podrá disponer de los dispositivos virtuales hasta que se cierre del subprograma Virtual Media (Soportes virtuales.) Cuando termine de utilizar la unidad de CD/DVD-ROM virtual, puede desconectar el dispositivo del servidor host o cerrar el subprograma. El subprograma Virtual Media (Soportes virtuales) debe permanecer abierto al utilizar un dispositivo de soporte virtual.

El servidor host podrá disponer del CD/DVD-ROM de Virtual Media (Soportes virtuales) de iLO 2 durante la ejecución si el sistema operativo del servidor host admite unidades de disquete USB. Consulte “Compatibilidad con USB del sistema operativo” (Compatibilidad con USB del sistema operativo en la página 121) para obtener información sobre los sistemas operativos que son compatibles con el almacenamiento masivo USB en el momento de la publicación del presente manual.

El CD/DVD-ROM de Virtual Media (Soportes virtuales) de iLO 2 aparece ante el sistema operativo igual que cualquier otro CD/DVD-ROM. Al utilizar iLO 2 por primera vez, el sistema operativo del host le sugerirá instalar un asistente de nuevo hardware encontrado.

Al acabar de utilizar los soportes virtuales de iLO 2 y desconectarlos, recibirá un mensaje de advertencia del sistema operativo del host respecto a una eliminación poco segura de un dispositivo. Esta

advertencia puede evitarse si utiliza la característica proporcionada por el sistema operativo para detener el dispositivo antes de desconectarlo de los Soportes virtuales.

Notas acerca de los sistemas operativos del CD/DVD-ROM de Virtual Media

- MS-DOS

  El CD/DVD-ROM virtual no es compatible con MS-DOS.

- Windows Server® 2008 y Windows Server® 2003

  El CD/DVD-ROM virtual aparece automáticamente después de que Windows® reconozca el montaje del dispositivo USB. Utilícelo como utilizaría un dispositivo CD/DVD-ROM conectado de forma local.

- Linux

  - Red Hat Linux

    En los servidores con un CD/DVD-ROM IDE conectado de manera local, el dispositivo de CD/DVD-ROM virtual está disponible en /dev/cdrom1. Sin embargo, en los servidores con un CD/DVD-ROM conectado de manera local, como los sistemas de ranuras BL-class, el CD/DVD-ROM virtual es el primer CD/DVD-ROM accesible desde /dev/cdrom.

    El CD/DVD-ROM virtual se puede montar como un dispositivo de CD/DVD-ROM normal mediante:

    mount /mnt/cdrom1

  - SLES 9

    El sistema operativo SLES 9 coloca los CD/DVD-ROM conectados a USB en otra ubicación, por lo que el CD/DVD-ROM virtual se encuentra en /dev/scd0, a menos que haya ya un CD/DVD-ROM local conectado a UBS, en cuyo caso se encontrará en /dev/scd1.

    El CD/DVD-ROM virtual se puede montar como un dispositivo de CD/DVD-ROM normal mediante:

    mount /dev/scd0 /media/cdrom11

    Consulte la sección "Montaje de un CD/DVD-ROM de soporte virtual USB en Linux" (Montaje de un CD/DVD-ROM de soporte virtual USB en Linux en la página 125) para obtener instrucciones detalladas.

Montaje de un CD/DVD-ROM de soporte virtual USB en Linux

1. Acceda a iLO 2 mediante un explorador.
2. Seleccione **Virtual Media (Soportes virtuales)** en la ficha Virtual Devices (Dispositivos virtuales.)
3. Seleccione el CD/DVD-ROM que desee utilizar y haga clic en **Connect (Conectar)**.
4. Monte la unidad mediante el siguiente comando:

   ```
   mount /dev/cdrom1 /mnt/cdrom1
   ```

   Para SLES 9:

   ```
   mount /dev/scd0 /media/cdrom1
   ```

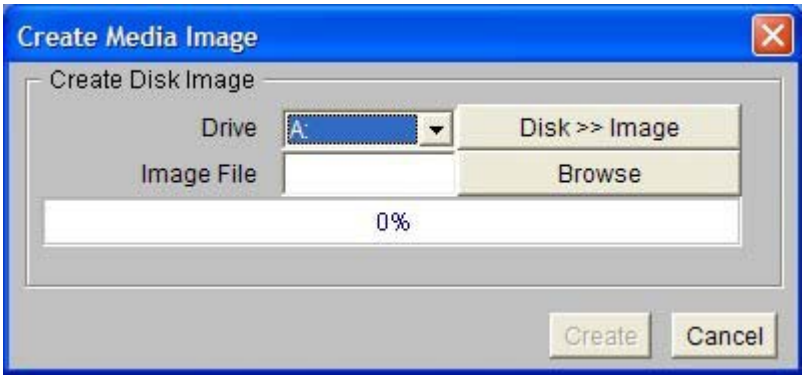
Creación de archivos de imágenes de disco iLO 2

La función de soportes virtuales de iLO 2 permite crear archivos de imágenes de disquetes y CD-ROM dentro del mismo subprograma. No puede crear archivos de imágenes de DVD si utiliza el subprograma

Virtual Media (Soportes virtuales.) Los archivos de imagen creados con el subprograma son imágenes de sistema de archivo ISO-9660. El rendimiento del soporte virtual de iLO 2 es más rápido cuando se utilizan archivos de imagen. La utilidad de creación de archivos de imágenes de disco de CD-ROM y de disquetes virtuales de iLO 2 está integrada en el subprograma Virtual Media (Soportes virtuales), sin embargo, también pueden crearse imágenes mediante herramientas estándar del sector, como DD.

Para crear un archivo de imagen:

1. Click Haga clic en **Create Disk Image (Crear imagen de disco)**.
2. Seleccione la unidad de soporte local del menú desplegable.
3. Escriba la ruta o el nombre de archivo en el cuadro de texto o haga clic en **Browse (examinar)** para seleccionar un archivo de imagen existente o para cambiar el directorio en el que se creará el archivo de imagen.
4. Haga clic en **Create (Crear)**. El subprograma de Soportes virtuales comienza el proceso de creación del archivo de imágenes. El proceso estará completo cuando la barra de progreso alcance el 100%. Para cancelar la creación de un archivo de imagen, haga clic en **Cancel (Cancelar)**.



La opción Disk (Disco)>>Image (Imagen) sirve para crear archivos de imágenes de disquetes o CD-ROM físicos. Esta opción no es válida para una imagen de CD-ROM Virtual. El botón Disk (Disco) >>Image (Imagen) cambia a Image (Imagen)>>Disk (Disco) cuando se hace clic en él. Haga clic en este botón para cambiar de la creación de archivos de imagen a partir de disquetes físicos a la creación de disquetes físicos a partir de archivos de imagen.

Carpeta virtual

La carpeta virtual de iLO 2 emula un dispositivo USB y crea dinámicamente una imagen de soporte de una carpeta o directorio seleccionada. Una vez creada la imagen virtual de una carpeta o directorio, el servidor se conecta a la imagen creada como dispositivo de almacenamiento USB y permite navegar hasta el servidor y transferir los archivos de la imagen generada por iLO 2 a cualquier ubicación del servidor.

La función de carpeta virtual sólo está disponible dentro de IRC. La carpeta virtual no es iniciable, es de sólo lectura y la carpeta montada es estática. Los cambios realizados en el archivo cliente no se replican en la carpeta montada.

Virtual Folder (Carpeta virtual) es una función con licencia disponible con la adquisición de iLO 2 Advanced o de iLO 2 Select. La función de carpeta virtual permite acceder, explorar y transferir archivos de un cliente a un servidor gestionado. La función de carpeta virtual admite la capacidad de montaje y desmontaje de un directorio en un directorio local o de red al que no se puede acceder a través del cliente y que se monta o desmonta como dispositivo Virtual Media.

Notas del sistema operativo de la carpeta virtual

- MS-DOS

  Durante el inicio del sistema y sesiones de MS-DOS, el dispositivo Virtual Folder (Carpeta virtual) aparece como unidad de disquete estándar del BIOS. Este dispositivo aparece como unidad A. Si existe una unidad de disquete físicamente conectada, permanecerá oculta y no disponible durante este período de tiempo. La unidad de disquete local física y Virtual Folder no se pueden usar simultáneamente.

- Windows®

  Virtual Folder (Carpeta virtual) aparece de forma automática después de que Microsoft® Windows® haya reconocido el montaje del dispositivo USB virtual. Puede utilizar la carpeta del modo que utilizaría un dispositivo localmente asociado. Virtual Folder (Carpeta virtual) no es iniciable. Intentar iniciarla desde la carpeta puede impedir el inicio del servidor.

- NetWare 6.5

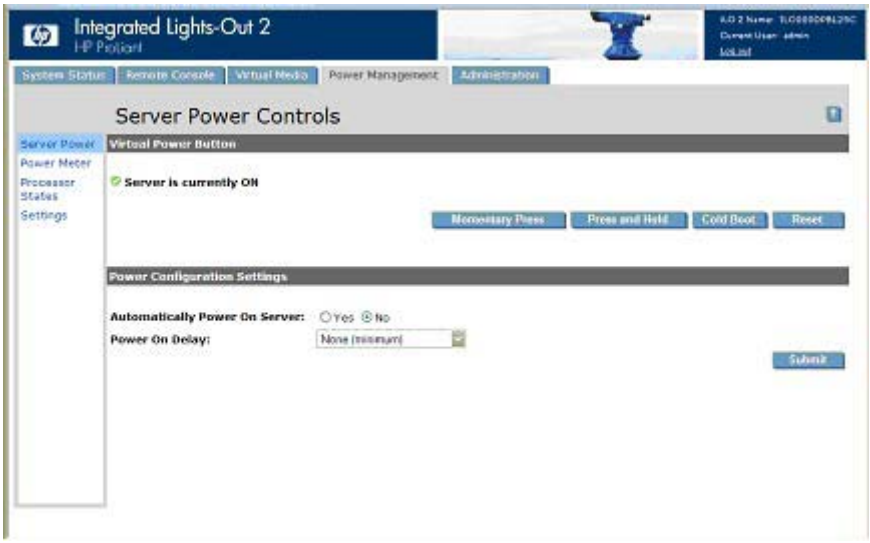
  NetWare 6.5 es compatible con el uso de Virtual Folder (Carpeta virtual) como unidad de llave o disquete USB. Consulte la sección "Montaje de un disquete/llave USB virtual en NetWare 6.5 (Montaje de un disquete/llave USB virtual en NetWare 6.5 en la página 122)" para obtener instrucciones detalladas al respecto.

- Red Hat y SLES Linux

  Linux admite el uso de Virtual Folder (Carpeta virtual.) Virtual Folder (Carpeta virtual) utiliza un formato de sistema de archivos FAT 16. Para obtener más información, consulte la sección "Montaje de soportes/llaves USB virtuales en Linux (Montaje de soportes/llaves USB virtuales en Linux en la página 122)".

Gestión de la alimentación

iLO 2 Power Management (Gestión de alimentación) permite ver y supervisar el estado y el uso de la alimentación del servidor, supervisar el procesador y modificar la configuración de la alimentación. La página Power Management (Gestión de alimentación) presenta cuatro opciones de menú: Server Power (Alimentación de servidor), Power Meter (Medidor de alimentación), Processor States (Estados de procesador) y Settings (Configuración.) Al seleccionar **Power Management (Gestión de alimentación)**, aparece la página Server Power Controls (Controles de alimentación de servidor.) La página Server Power Controls (Controles de alimentación de servidor) consta de dos secciones: Virtual Power Button (Botón de alimentación virtual) y Power Configuration Settings (Valores de configuración de alimentación.)



En la sección Virtual Power Button (Botón de alimentación virtual) se muestra el estado actual de alimentación del servidor así como las opciones de control de alimentación del servidor remoto. El estado de alimentación que aparece es el estado de alimentación del servidor en el momento de abrir la página. El servidor puede estar en On (Encendido), Off (Apagado) o Reset (Reinicio.) Utilice la función de actualización del explorador para mantener actualizado el estado del indicador de alimentación.

Para cambiar el estado actual de alimentación del servidor con las opciones de Virtual Power Button (Botón de alimentación virtual), debe disponer de privilegios de Virtual Power and Reset (Reinicio y alimentación virtual.) Algunas de las opciones de control de alimentación causan problemas al cerrar el sistema operativo. Se debe iniciar un cierre del sistema operativo mediante la consola remota antes de utilizar las opciones de Virtual Power Button (Botón de alimentación virtual.) Las siguientes opciones están disponibles:

- Pulsando el botón Momentary Press (Pulsar momentáneamente) se consigue un comportamiento idéntico a pulsar el botón físico de alimentación.
- Press and Hold (Mantener pulsado) es idéntico que pulsar el botón físico de alimentación durante cinco segundos y soltarlo. Esta opción ofrece una funcionalidad compatible con la interfaz avanzada de alimentación y configuración (ACPI, Advanced Configuration and Power Interface) que implementan algunos sistemas operativos. El comportamiento de estos sistemas operativos varía en función de si se pulsan un instante o de forma prolongada. El comportamiento de esta opción puede burlar las funciones de cierre correcto del sistema operativo.
- Cold Boot (Inicio en frío) del sistema elimina inmediatamente la alimentación del sistema. El sistema se reiniciará después de seis segundos aproximadamente. Esta opción no está disponible cuando se apaga el servidor. Esta opción burla las funciones de cierre correcto del sistema operativo.
- La opción Reset System (Reiniciar sistema) permite reiniciar el sistema. Esta opción no está disponible cuando se apaga el servidor. El comportamiento de esta opción puede burlar las funciones de cierre correcto del sistema operativo.

La sección Power Configuration Settings (Valores de configuración de alimentación) permite controlar la forma en que se enciende del servidor remoto cuando se le aplica alimentación. Las siguientes opciones están disponibles:

- Automatically Power On Server (Encender el servidor automáticamente) permite que iLO 2 encienda un servidor cuando se le aplica alimentación, como por ejemplo, cuando se enchufa o cuando se activa la unidad de alimentación ininterrumpida (UPS, Unlimited Power Supply) después de un corte en el suministro de alimentación. Debe tener el privilegio Virtual Power and Reset (Alimentación virtual y reinicio) para modificar este valor de configuración.

  Si se pierde la alimentación de forma inesperada mientras el servidor se está encendiendo, el servidor siempre se vuelve a encender, aunque la opción Automatically Power On Server (Encender el servidor automáticamente) esté establecida en No.

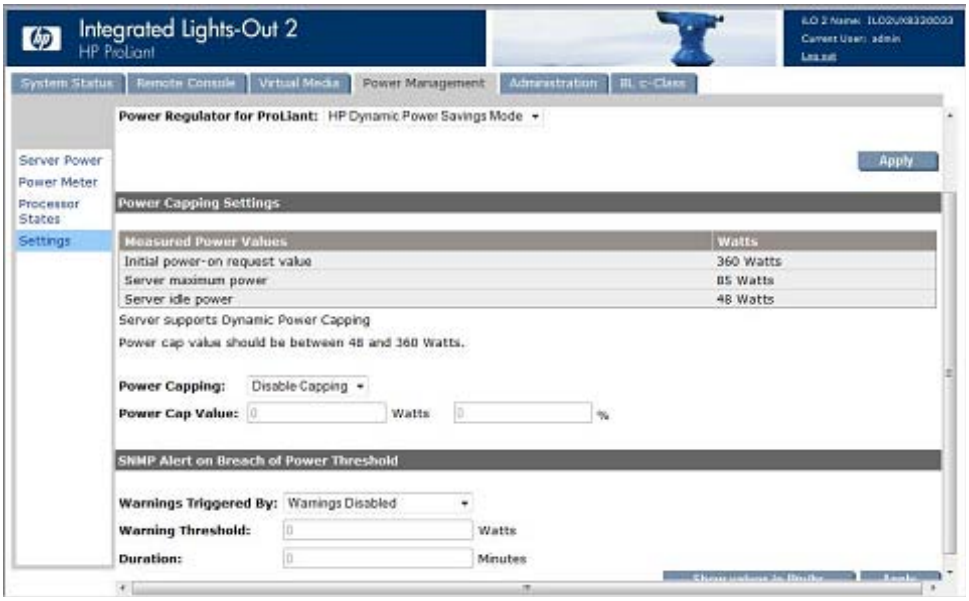
- Power On Delay (Retraso en alimentación) se utiliza para alternar la alimentación del servidor en un centro de datos. Los servidores blade los controla la infraestructura del bastidor y no admiten el retraso de alimentación. La opción Power On Delay (Retraso de alimentación) no interfiere con el botón de alimentación.

  El retraso se produce antes de que iLO 2 encienda el servidor, incluido el encendido automático y la recuperación de alimentación. Algunos servidores no pueden forzar la demora en el caso de restauración de la alimentación. El firmware iLO 2 requiere apenas 10 segundos para que el encendido del servidor surta efecto. Debe tener el privilegio Virtual Power and Reset (Alimentación virtual y reinicio) para modificar este valor de configuración.

Configuración de la alimentación del servidor

La función Power Regulator for ProLiant (Regulador de alimentación para ProLiant) permite a iLO 2 modificar de forma dinámica los niveles de voltaje y frecuencia del procesador en función de las condiciones de funcionamiento para proporcionar ahorro de energía con un efecto mínimo sobre el rendimiento. Los procesadores que admiten esta función presentan estados de frecuencia y voltaje predefinidos conocidos como *p-states*. El software puede pasar el procesador de un estado predefinido a otro de forma dinámica. P-0 es la combinación de frecuencia y voltaje más elevada que puede admitir el procesador. La modificación del estado predefinido del procesador en función del uso de la CPU permite un ahorro significativo de energía con la mínima degradación en el rendimiento al reducir la frecuencia y voltaje del procesador cuando el sistema se encuentra inactivo y aumentando el voltaje y frecuencia del procesador cuando es necesario.

La página Power Management Settings (Configuración de la gestión de alimentación) permite ver y controlar el modo del regulador de alimentación del servidor. Es necesario disponer del privilegio Configure iLO 2 Settings (Configurar valores de iLO 2) para cambiar este valor de configuración.



- La sección Power Regulator for ProLiant (Regulador de alimentación para ProLiant) presenta las opciones siguientes:
  - Enable HP Dynamic Power Savings Mode (Activar modo de ahorro de energía dinámico de HP) establece el nivel de alimentación según el uso.
  - Enable HP Static Low Power Mode (Activar modo estático de baja potencia de HP) establece el nivel de alimentación del procesador al mínimo.
  - HP Static High Performance Mode (Modo de alto rendimiento de HP Static) ajusta el procesador al estado más alto de procesador respaldado y lo fuerza a permanecer en ese estado.
  - Enable OS Control Mode (Activar modo de control del SO) define el procesador a su máxima alimentación.

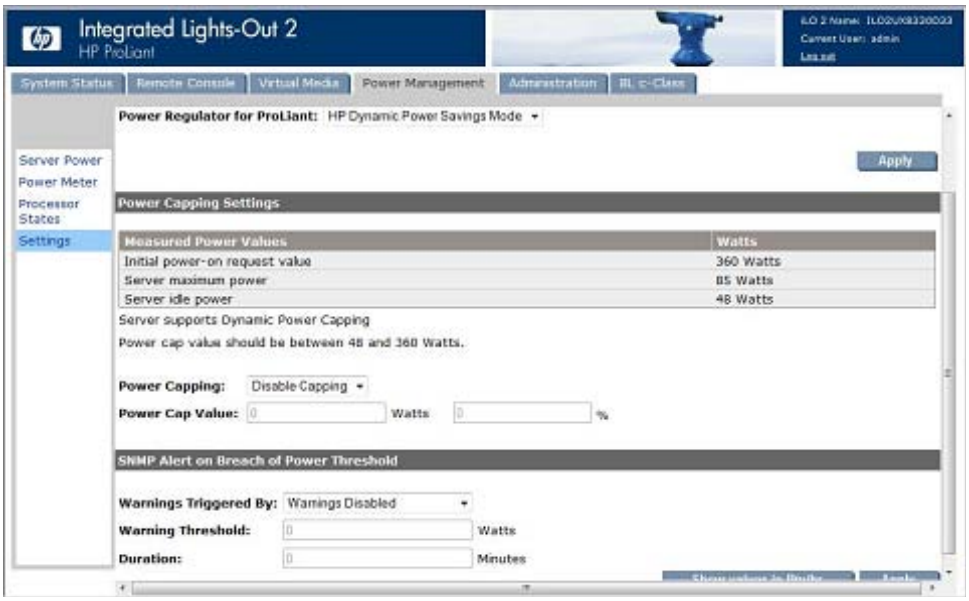
    Después de seleccionar una de las opciones de Power Regulator for ProLiant (Regulador de alimentación para ProLiant), haga clic en **Apply (Aplicar)** para guardar la configuración. El servidor requiere un reinicio para que los cambios surtan efecto. Esta configuración no puede cambiarse mientras el servidor esté en POST. Si la configuración no cambia después de hacer clic en **Apply (Aplicar)**, es posible que el servidor se esté reiniciando o requiera un reinicio. Salga de cualquier programa de RBSU en ejecución y, a continuación, permita que se complete el proceso POST e intente la operación de nuevo.
- La sección Power Capping Settings (Configuración de límites de alimentación) permite ver los valores de alimentación medidos, establecer un límite de alimentación y desactivar los límites de alimentación.

  Los valores de alimentación medidos incluyen el valor máximo de suministro de alimentación del servidor, la alimentación máxima del servidor y la alimentación de inactividad del servidor. El valor máximo de suministro de alimentación hace referencia a la cantidad máxima de alimentación que puede suministrar la fuente de alimentación del servidor. Los valores de alimentación máxima y alimentación de inactividad del servidor vienen determinados por dos pruebas de alimentación que realiza la memoria ROM durante el proceso POST.

  La opción Power Cap Setting (Configuración de límites de alimentación) permite establecer un límite de alimentación en el servidor. Una vez establecido el límite de alimentación, la lectura de alimentación media del servidor debería ser igual o inferior al valor del límite. Puede establecer el

límite de alimentación especificando un valor en vatios o en Btu/h (haga clic en **Show values in Btu/hr (Mostrar valores en Btu/h)**) o bien un porcentaje. El porcentaje hace referencia a la diferencia entre los valores de alimentación máxima y de alimentación de inactividad. El valor límite no puede ser inferior que la alimentación de inactividad del servidor.

Power Capping Settings (Configuración de límites de alimentación) se desactiva cuando el servidor forma parte de una limitación de alimentación dinámica del receptáculo. Estos valores se ajustan y modifican mediante Onboard Administrator (Administrador a bordo) o Insight Power Manager (Administrador de alimentación Insight.)



- Si el servidor dispone de hardware y software compatible con los límites de la alimentación dinámica, se mostrará el mensaje `System supports Dynamic Power Capping (El sistema admite la limitación de la alimentación dinámica)`. Los límites de la alimentación dinámica proporcionan protección a los interruptores eléctricos.
- Si no se muestra el mensaje `System supports Dynamic Power Capping (El sistema admite los límites de la alimentación dinámica)`, el servidor admitirá los límites de alimentación normales. Los límites de alimentación normales no reaccionan con la suficiente rapidez como para suministrar protección a los interruptores eléctricos.

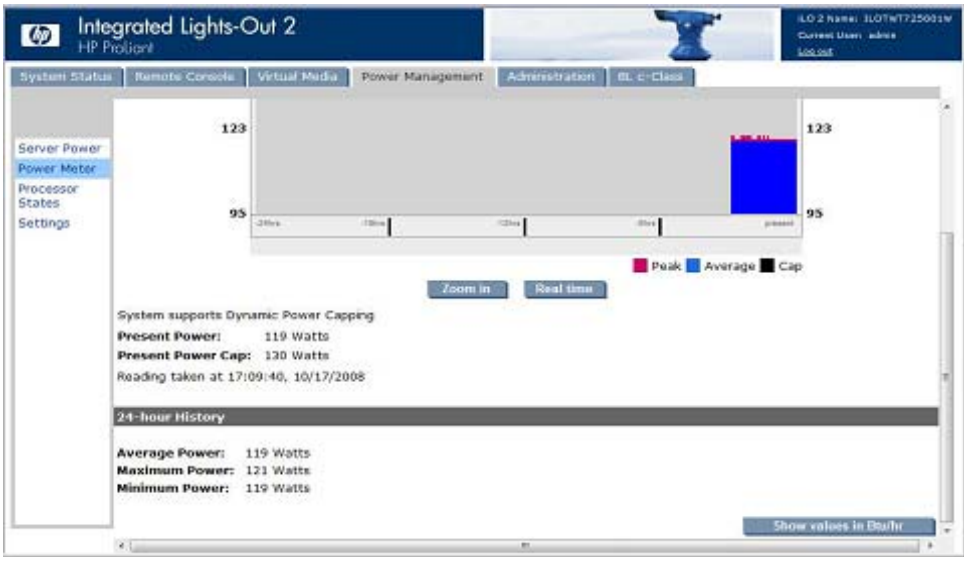
  Si desea obtener más información acerca de los límites de la alimentación dinámica, consulte "Límites de alimentación dinámica para blades de servidor".

- La sección SNMP Alert on breach of power threshold (Alerta SNMP cuando se sobrepasa el límite de alimentación) permite el envío de advertencias de SNMP cuando el consumo de energía sobrepasa un límite definido. Es posible ajustar lo siguiente:
  - Warnings Triggered By (Advertencias provocadas por): permite determinar si desea que las advertencias estén basadas en el consumo de energía máximo, en el consumo de energía medio o desactivadas.
  - Warning Threshold (Límite de advertencia): permite ajustar el límite mínimo que el consumo de energía no debe rebasar para provocar una alerta SNMP.
  - Duration (Duración): permite ajustar la duración de tiempo en minutos durante la que el consumo de energía debe ser superior al límite de advertencia antes de que se active una alerta SNMP. La duración máxima permitida es de 240 minutos y debe ser múltiplo de 5.

Para utilizar la configuración seleccionada, haga clic en **Apply (Aplicar)**. Algunos servidores permiten una modificación del nivel de alimentación del procesador a través de la utilidad RBSU del sistema. Consulte la guía de usuario del sistema para obtener más información.

Datos de alimentación del servidor

iLO 2 permite ver de forma gráfica el uso de alimentación del servidor. En la página Power Meter Readings (Lecturas del medidor de alimentación) se muestra la utilización de la alimentación del servidor en un gráfico. Para acceder a Power Meter Readings (Lecturas del medidor de alimentación), seleccione **Power Management (Gestión de alimentación)** y haga clic en **Power Meter (Medidor de alimentación)**. La página Power Meter Readings (Lecturas del medidor de alimentación) consta de dos secciones: Power Meter Readings (Lecturas del medidor de alimentación) y 24-Hour History (Historial de 24 horas.)



En la sección Power Meter Readings (Lecturas del medidor de alimentación) aparece lo siguiente:

- El gráfico de datos muestra el uso de alimentación del servidor a lo largo de las 24 horas previas. iLO 2 reúne cada cinco minutos la información de uso de alimentación del servidor. Para cada intervalo de 5 minutos se almacenan el pico y el promedio de uso de alimentación en un búfer circular. Estos dos valores se muestran en forma de un gráfico de barras, con los valores medios en azul y los valores de pico en rojo. Estos datos se reinician siempre que el servidor o el iLO 2 se reinician.
  - Para aumentar la visibilidad, haga clic en **Zoom in (Aumentar)**, que sirve para aumentar la anchura horizontal de las barras de datos en el gráfico de datos de alimentación. En este modo aparece un deslizador para permitir inspeccionar los datos dentro de una ventana del mismo tamaño.
  - Para visualizar la utilización de la alimentación actual, haga clic en **Real Time (Tiempo real)**. La gráfica de datos Real Time (Tiempo real) muestra información sobre el consumo de alimentación en los 20 minutos anteriores, incluyendo los consumos de energía máximo y medio y la limitación de la alimentación.
- Compatibilidad actual con Dynamic Power Capping (Limitación de alimentación dinámica).

- El valor Present Power (Alimentación presente) muestra la lectura de alimentación actual del servidor.
- Present Power Cap (Límite de alimentación presente) muestra la configuración actual de límite de alimentación.

En la sección 24-Hour History (Historial de 24 horas) se muestra lo siguiente:

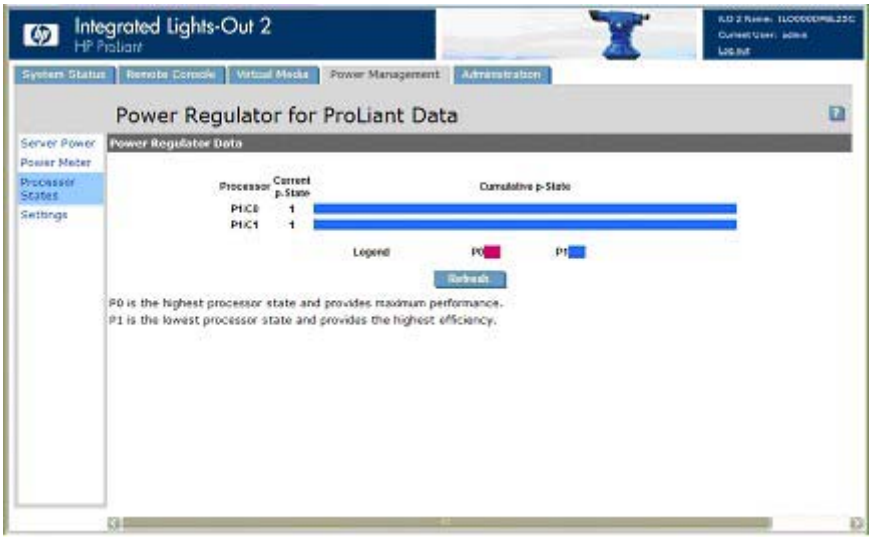
- Average Power Reading (Lectura de alimentación media) muestra la media de las lecturas de alimentación tomadas del servidor a lo largo de las últimas 24 horas. Si el servidor no ha estado en funcionamiento durante 24 horas, el valor es el de la media de todas las lecturas tomadas desde que se inició el servidor.
- Maximum Power (Alimentación máxima) muestra la lectura máxima de las lecturas de alimentación tomadas del servidor a lo largo de las últimas 24 horas. Si el servidor no ha estado en funcionamiento durante 24 horas, el valor es el de la lectura máxima de todas las lecturas tomadas desde que se inició el servidor.
- Minimum Power (Alimentación mínima) muestra la lectura mínima de las lecturas de alimentación tomadas del servidor a lo largo de las últimas 24 horas. Si el servidor no ha estado en funcionamiento durante 24 horas, el valor es el de la lectura mínima de todas las lecturas tomadas desde que se inició el servidor.
- La opción Show value in BTUs (Mostrar los valores en BTU) cambia los datos visualizados de vatios a BTU.

Estados del procesador

La página Power Regulator for ProLiant Data (Regulador de alimentación para datos ProLiant) permite ver los estados del procesador (p-state) y una media variable del porcentaje de tiempo que cada procesador lógico ha dedicado en cada estado p-state en las últimas 24 horas. Haga clic en **Refresh (Actualizar)** para actualizar el gráfico de datos p-state.

Debe disponer del privilegio de Configure iLO 2 Settings (Configurar valores de iLO 2) para ver la página Power Regulator for ProLiant Data (Regulador de alimentación para datos ProLiant.) Power Regulator for ProLiant Data (Regulador de alimentación para datos ProLiant) es una función con licencia disponible con la adquisición de licencias opcionales. Si desea obtener más información, consulte "Concesión de licencias (Concesión de licencias en la página 21)".

Para acceder a la página Power Regulator for ProLiant Data (Regulador de alimentación para datos ProLiant), haga clic en **Power Management (Gestión de alimentación)>Processor States (Estados del procesador)**.



En la página Power Regulator Data (Datos del regulador de alimentación) se muestran los datos recopilados de p-state, desde el encendido del servidor y después los actualiza cada 5 minutos. La memoria ROM lee el estado actual de cada procesador lógico. El registro de estado de las plataformas basadas en Intel® refleja la frecuencia y el voltaje de funcionamiento actuales. Debido a las distintas dependencias del procesador, el estado puede o no reflejar un estado predefinido absoluto. La frecuencia puede estar en un estado predefinido y el voltaje en un estado predefinido superior. La memoria ROM del sistema actualiza el número de estados predefinidos del estado predefinido para la frecuencia actual y no para el voltaje actual.

Los datos se muestran a través del gráfico de barras, donde el total de la barra representa el 100% del tiempo que cubren los datos. Se muestra un gráfico de datos por cada procesador o núcleo. No se muestran los gráficos de datos para varios subprocesos en un procesador o núcleo que admita Hyper-Threading. Cada parte de la barra está marcada con colores diferentes según el estado predefinido en que se encontraba el procesador y cada parte coloreada representa en escala el porcentaje de tiempo total que el utilizó procesador en ese estado predefinido. Al detener el ratón sobre el gráfico de barras se muestra un mensaje que indica lo que representa el porcentaje numérico de esa parte de la barra.

Eficacia de la alimentación

iLO 2 permite implementar un uso de la alimentación mejorado mediante el High Efficiency Mode (Modo de alta eficacia) (HEM.) El modo HEM permite mejorar la eficacia de la alimentación del sistema mediante la colocación de los suministros de alimentación secundarios en modo de reducción. Cuando los suministros de alimentación secundarios se encuentran en modo de reducción, los suministros principales proporcionan toda la alimentación de cc al sistema. Los suministros de alimentación resultan más eficientes (más vatios de salida de cc por cada vatio de entrada de ca) a niveles de salida de alimentación de mayor potencia, y la eficacia de la alimentación general mejora.

Cuando el sistema comienza a utilizar más del 70% de la capacidad de la salida de alimentación máxima de los suministros de alimentación principales, los suministros secundarios vuelven a presentar un funcionamiento normal (fuera del modo reducido.) Cuando el uso de la alimentación cae por debajo del 60% de la capacidad de los suministros principales, los suministros secundarios regresan al modo reducido. El modo HEM permite obtener un consumo de energía igual al de la salida de alimentación máxima de los suministros principal y secundario, mientras se mantiene una eficacia mejorada con niveles de uso de alimentación inferiores.

El modo HEM no afecta a la redundancia de la alimentación. Si se produce un fallo en los suministros principales, los suministros secundarios comenzarán inmediatamente a suministrar alimentación de cc al sistema, evitando que no se pueda utilizar la unidad.

Únicamente es posible configurar el modo HEM a través de la utilidad RBSU. No es posible modificar estos ajustes a través de iLO. Los ajustes del modo HEM son Enabled (Activado) o Disabled (Desactivado) (también denominado Balanced Mode (Modo equilibrado)), y los ajustes para el suministro principal, Odd (Impar) o Even (Par.) Estos ajustes pueden visualizarse en la sección High Efficiency Mode (Modo de alta eficacia) & Standby Power Save Mode (Modo de ahorro de energía en modo de espera) de la ficha System Information (Información del sistema)>Power (Alimentación.) En esta sección se visualiza la siguiente información:

- Si el modo HEM se encuentra activado o desactivado
- Qué suministros de alimentación son principales (si el modo HEM se encuentra activado)
- Qué suministros de alimentación no son compatibles con el modo HEM

Cierre correcto

La capacidad que posee el microprocesador iLO 2 para llevar a cabo un cierre correcto requiere la cooperación del sistema operativo. Para llevar a cabo un cierre correcto, el controlador de estado debe estar cargado. iLO 2 se comunica con éste y con el método del sistema operativo correspondiente para cerrar el sistema con seguridad con el fin de asegurar la integridad de los datos.

En caso de que el controlador de estado no está cargado, el procesador iLO 2 intentará que el sistema operativo se cierre correctamente a través del botón de alimentación. iLO 2 emula la pulsación de un botón de alimentación físico con el fin de sugerir al sistema operativo que se cierre correctamente. El comportamiento del sistema operativo depende de su configuración y de la configuración para la pulsación de un botón de alimentación.

La configuración de EAAS de RBSU de la memoria ROM del HOST permite la desactivación de la función de cerrado automática. Esta configuración permite la desactivación del cierre automático excepto en las condiciones más extremas en que podrían producirse daños físicos.

Si se inicia con Windows Server® 2003, la directiva de grupo del ordenador deshabilita el cierre correcto del sistema mediante una pulsación momentánea salvo que exista un administrador que haya iniciado

sesión en el sistema operativo. Para cambiar este ajuste y permitir un cierre correcto, lleve a cabo lo siguiente:

1. Desde una línea de comandos, ejecute el comando `gpedit.misc`.
2. Ajuste Configuración del equipo>Configuración de Windows>Configuración de seguridad>Directivas locales>Opciones de seguridad>Apagar: permita que se cierre el sistema sin necesidad de iniciar sesión en **Enabled (Habilitado)**.

Gestión avanzada de ProLiant BL p-Class

iLO 2 Advanced es un componente estándar de las ranuras del servidor ProLiant BL p-Class que proporciona el estado del servidor y capacidad de gestión de las ranuras del servidor remoto. Se accede a sus funciones desde un dispositivo cliente de red con un explorador Web compatible. Además de otras funciones, iLO 2 Advanced proporciona capacidad de teclado, ratón y vídeo (texto y gráficos) para el blade de servidor, independientemente del estado del sistema operativo del host o del blade de servidor host.

iLO 2 incluye un microprocesador inteligente, memoria segura y una interfaz de red dedicada. Este diseño hace a iLO 2 independiente del blade de servidor host y de su sistema operativo. iLO 2 proporciona acceso remoto a cualquier cliente de red autorizado, envía alertas y ofrece otras funciones de gestión del blade de servidor.

Con un explorador Web compatible, puede realizar las operaciones siguientes:

- Acceder de forma remota a la consola del blade de servidor host, lo que incluye todos los modos de texto y pantallas de modo de gráficos con control total del teclado y el ratón.
- Encender, apagar y reiniciar el blade de servidor host de manera remota.
- Iniciar de forma remota un blade de servidor host de una imagen de disquete virtual para actualizar el ROM o instalar un sistema operativo.
- Enviar mensajes de aviso desde iLO 2 Advanced, independientemente del estado del blade de servidor host.
- Acceder a las funciones avanzadas de solución de problemas que ofrece iLO 2 Advanced.
- Ejecute un explorador Web, utilice un sistema de alerta SNMP y diagnostique el blade de servidor con HP Systems Insight Manager.
- Configure los valores del compartimento con IP estática para las NIC de gestión iLO 2 dedicados en cada blade de servidor en un receptáculo para aumentar la velocidad de implantación.

El blade de servidor debe tener instalados los cables correctamente para la conectividad con iLO 2. Conecte el blade de servidor mediante uno de los siguientes métodos:

- Mediante una red ya existente (en el bastidor.) Este método precisa la instalación del blade de servidor en su receptáculo y asignarle una dirección IP manualmente o con DHCP.
- Mediante el puerto E/S del blade de servidor.
  - En el bastidor: este método requiere una conexión del cable I/O local al puerto I/O y a un cliente PC. Utilizando la dirección IP estática que aparece en la etiqueta del cable de E/S y la información de acceso inicial situada en la parte frontal del blade de servidor, puede acceder al blade de servidor con la consola remota de iLO 2 Advanced.
  - Fuera del bastidor, con la estación de diagnóstico: este método requiere alimentar la ranura del servidor con la estación de diagnóstico opcional y conectarla a un equipo externo con la dirección IP estática y el cable E/S local. Consulte la documentación adjunta de la estación de diagnóstico o al CD de Documentación para obtener instrucciones sobre el cableado.
  - Mediante los conectores del panel trasero del blade de servidor (fuera del bastidor, con la estación de diagnóstico): este método permite configurar un blade de servidor fuera del bastidor alimentando la ranura con la estación de diagnóstico y conectando con una red existente mediante un conmutador. Un servidor DHCP en la red asigna la dirección IP.

La ficha BL p-Class permite controlar valores de configuración específicos del bastidor de servidores blade ProLiant BL p-Class. iLO 2 también proporciona el estado basado en Web del bastidor de servidores ProLiant BL p-Class.

Rack View

La página Rack View (Vista de bastidor) presenta una vista general de todos los receptáculos y sus servidores blade, componentes de red y fuentes de alimentación. Cuando un componente está presente en el bastidor, se muestra y se puede seleccionar en la página Rack View (Vista de bastidor) Los compartimentos en blanco o vacíos no se pueden seleccionar. La información específica acerca de cada componente, como el nombre de la ranura, la dirección IP y el tipo de producto, aparece a medida que desplaza el cursor del ratón sobre cada componente. Al hacer clic en un componente aparecerán opciones de configuración e información adicional en la pantalla adyacente.

La pantalla Rack View (Vista de bastidor) presenta los siguientes campos:

- Nombre de bastidor
- Logged-in iLO Location (Ubicación de inicio de sesión de iLO)

  Esta sección muestra la ranura en la que ha iniciado sesión Sólo puede configurar los parámetros de esta ranura.
- Selected Bay Location (Ubicación de compartimento seleccionado)

  Esta sección indica el compartimento seleccionado actualmente. Podrá ver información sobre muchos tipos diferentes de componentes, lo que incluye ranuras, fuentes de alimentación, componentes de red y receptáculos.
- Enclosure Details (Detalles del receptáculo)

  Se puede acceder a información acerca de un receptáculo concreto seleccionando **Details (Detalles)** en los encabezados de receptáculo enumerados.

Existe un botón Refresh (Actualizar) para obtener información actualizada en Rack View (Vista de bastidor.) Haga clic en **Refresh (Actualizar)** para forzar que vuelva a dibujarse toda la representación gráfica del bastidor. Esta operación tardará unos momentos.

Si la información de la vista de bastidor no puede obtenerse correctamente, aparecerá un mensaje de error en lugar de los componentes procesados. El botón Refresh (Actualizar) puede utilizarse para realizar otro intento de obtener los datos correctos para la vista de bastidor. La función Rack View (Vista de bastidor) requiere la versión 2.10 o posterior del firmware del blade de servidor y del módulo de gestión de la alimentación para mostrarse correctamente.

Información y configuración de ranuras

La opción de configuración de ranuras proporciona información acerca de la identidad, ubicación y dirección de red de la ranura seleccionada en la página Rack View (Vista de bastidor.) Para ver estas opciones, seleccione un componente de ranura y seleccione **Configure (Configurar)** en la página Rack View (Vista de bastidor) (Rack View en la página 137.) Puede modificar algunas de las opciones de la ranura en la que haya iniciado sesión actualmente. Para guardar los cambios, haga clic en **Apply (Aplicar)**.

Los siguientes campos están disponibles:

- Identification Information (Información de identificación)
  - Bay Name (Nombre de compartimento)
  - Bay Number (Número de compartimento)
- Power On Control (Control de encendido)
  - Power Source (Fuente de alimentación)
  - Enable Automatic Power On (Activar encendido automático)
  - Enable Rack Alert Logging (IML) [Activar registro de avisos de bastidor (IML)]

Información del receptáculo

La información de receptáculo es específica del receptáculo seleccionado. Se puede acceder a información acerca de un receptáculo concreto seleccionando **Details (Detalles)** en los encabezados de receptáculo enumerados. Se encuentra disponible una determinada cantidad de información sobre bastidor, incluidos el nombre y número de serie

Para los receptáculos que no contienen la ranura en la que ha iniciado sesión se encuentra disponible un conjunto básico de información que incluye el nombre, el número de serie y el tipo de receptáculo.

Para el receptáculo que contiene el compartimento en el que ha iniciado sesión se encuentra disponible un conjunto avanzado de información que incluye:

- Nombre
- Serial Number (Número de serie)
- Enclosure Type (Tipo de receptáculo)
- Firmware Revision (Revisión del firmware)
- Hardware Revision (Revisión del hardware)
- Enclosure temperature (Temperatura del receptáculo)
- Management Module UID (UID del módulo de gestión)

Algunos campos pueden modificarse y actualizarse haciendo clic en el botón **Apply (Aplicar)**.

Información sobre alimentación del receptáculo

La página Power Enclosure Information (Información sobre alimentación del receptáculo) proporciona información de diagnóstico acerca del módulo de gestión de la alimentación y los componentes que contiene el receptáculo de alimentación. Esta información proporciona una vista general acerca del buen estado y la situación del receptáculo y los componentes.

Los siguientes campos están disponibles:

- Nombre de bastidor
- Rack Serial Number (Número de serie del bastidor)
- Nombre de chasis
- Enclosure Serial Number (Número de serie del receptáculo)
- Enclosure Type (Tipo de receptáculo)
- Firmware Revision (Revisión del firmware)
- Hardware Revision (Revisión del hardware)
- Load Balance wire (Cable de equilibrio de carga)
- Enclosure temperature (Temperatura del receptáculo)
- Enclosure temperature side A and B (Temperatura del receptáculo lados A y B)
- Management Module UID (UID del módulo de gestión)

Algunos campos pueden modificarse y actualizarse haciendo clic en el botón **Apply (Aplicar)**.

Información sobre componentes de red

La pantalla de información sobre componentes de red muestra el estado del panel de parches o el conmutador de interconexión que haya seleccionado. La información mostrada incluye Fuse A (Fusible A), Fuse B (Fusible B) y Network Component Type (Tipo de componente de red.)

Control de la placa iLO 2 sobre los indicadores LED del servidor ProLiant BL p-Class

iLO 2 puede supervisar los servidores BL p-Class mediante el seguimiento de POST y el LED de estado del servidor.

Seguimiento de la POST del servidor

Hay información limitada mientras el servidor está arrancando debido a la naturaleza no jerárquica de los servidores ProLiant BL p-Class. iLO 2 proporciona información de arranque haciendo parpadear en color verde el LED de estado del servidor durante la POST del servidor. El LED se quedará en ámbar permanentemente si el inicio no se realiza correctamente. El LED permanecerá en verde permanentemente al final de un inicio correcto.

Tras un inicio correcto, se devuelve al servidor el control del LED de estado del servidor, que puede apagar el LED o bien configurarlo en otro color que represente el estado del hardware del servidor.

Notificación de alimentación insuficiente

iLO 2 enciende el LED de estado del servidor en rojo permanente si iLO 2 no puede encender el servidor porque no hay alimentación suficiente en la infraestructura del bastidor.

Reenvío de avisos de ProLiant BL p-Class

iLO 2 admite capturas SNMP de infraestructura de ranuras en función de la transferencia. El informe del estado de la infraestructura de ranuras por parte de iLO 2 no necesita la compatibilidad del sistema operativo. Los avisos (capturas) se originan en el Enclosure Manager (Gestor del receptáculo) y en el Power Supply Manager (Gestor del suministro de alimentación) y se transmiten a iLO 2. El firmware p-Class de iLO 2 reenvía los avisos de infraestructura como capturas SNMP a una consola de gestión correctamente configurada. Estos avisos permiten supervisar que los avisos de p-Class se produzcan en una consola de gestión de SNMP.

El reenvío de avisos de p-Class viene desactivado de forma predeterminada y se puede activar desde la página Web de SNMP/Insight Manage Settings.

iLO 2 identifica y reenvía los siguientes avisos:

ID de aviso	Descripción
22005	Fallo en la temperatura del receptáculo
22006	Degradación de la temperatura del receptáculo
22007	Temperatura del receptáculo adecuada
22008	Fallo en el ventilador del receptáculo
22009	Ventilador del receptáculo degradado
22010	Funcionamiento adecuado del ventilador del receptáculo
22013	Fallo en la alimentación del bastidor
22014	Alimentación del bastidor degradada
22015	Suministro de alimentación del bastidor adecuado
22023	Fallo en el servidor del bastidor por alimentación insuficiente

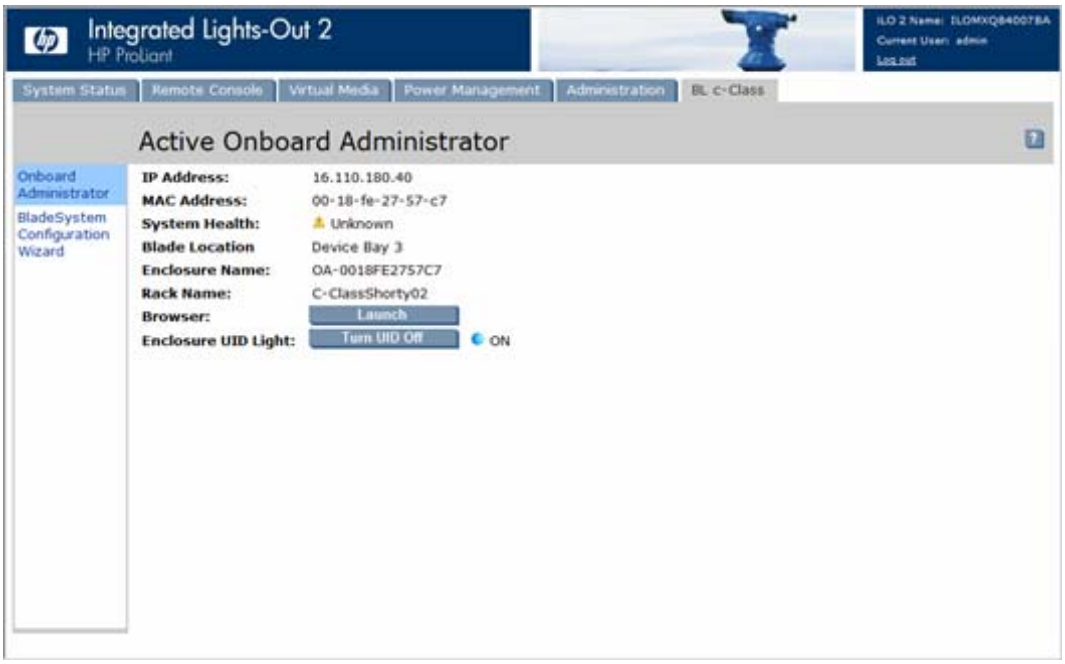
Onboard Administrator de HP BladeSystem de ProLiant

OnBoard Administrator (Administrador a bordo) de HP BladeSystem es el procesador de gestión de receptáculo, subsistema y base de firmware que se emplea para permitir el uso de HP BladeSystem y todos los dispositivos gestionados dentro del receptáculo.

Puede acceder a iLO 2 a través de la opción HP Onboard Administrator iLO (Opción iLO en la página 147) sea mediante el enlace de Web Administration (Administración Web) (Administración Web en la página 148) o directamente. Para iniciar sesión directamente en iLO 2, consulte la sección “Primer inicio de sesión en iLO 2” (Primer inicio de sesión en iLO 2 en la página 13)" para obtener información adicional.

Ficha BL c-Class de iLO 2

La ficha BL c-Class de la interfaz Web de iLO 2 le permite acceder al Onboard Administrador y a BladeSystem Configuration Wizard (asistente de configuración de BladeSystem.) Si desea obtener más información acerca de BladeSystem Configuration Wizard (Asistente de configuración de BladeSystem), consulte el documento *HP BladeSystem Onboard Administrator User Guide (Guía de usuario de HP BladeSystem Onboard Administrator)*.



La opción Onboard Administrador le permite ver una breve perspectiva general del estado del sistema del servidor así como ejecutar un explorador (que inicia la pantalla HP Onboard Administrator Rack View) o encender y apagar la luz de UID.

Direccionado IP de compartimento del receptáculo

Durante la finalización del asistente para primera instalación se le pedirá que configure su direccionado IP de compartimento de receptáculo. Si desea obtener más información acerca de todo el proceso de instalación mediante el asistente, consulte el documento *Guía de usuario de HP BladeSystem Onboard Administrator*.

Los puertos iLO 2 con blades de servidor y los puertos de gestión del módulo de interconexión pueden obtener direcciones IP en la red de gestión de 3 modos diferentes: Dirección DHCP, dirección IP estática o EBIPA. Si su red dispone de un servicio DHCP externo o si desea asignar manualmente direcciones

IP estáticas una a una a los blades de servidor y módulos de interconexión, haga clic en **Skip (Omitir)** para omitir este paso.

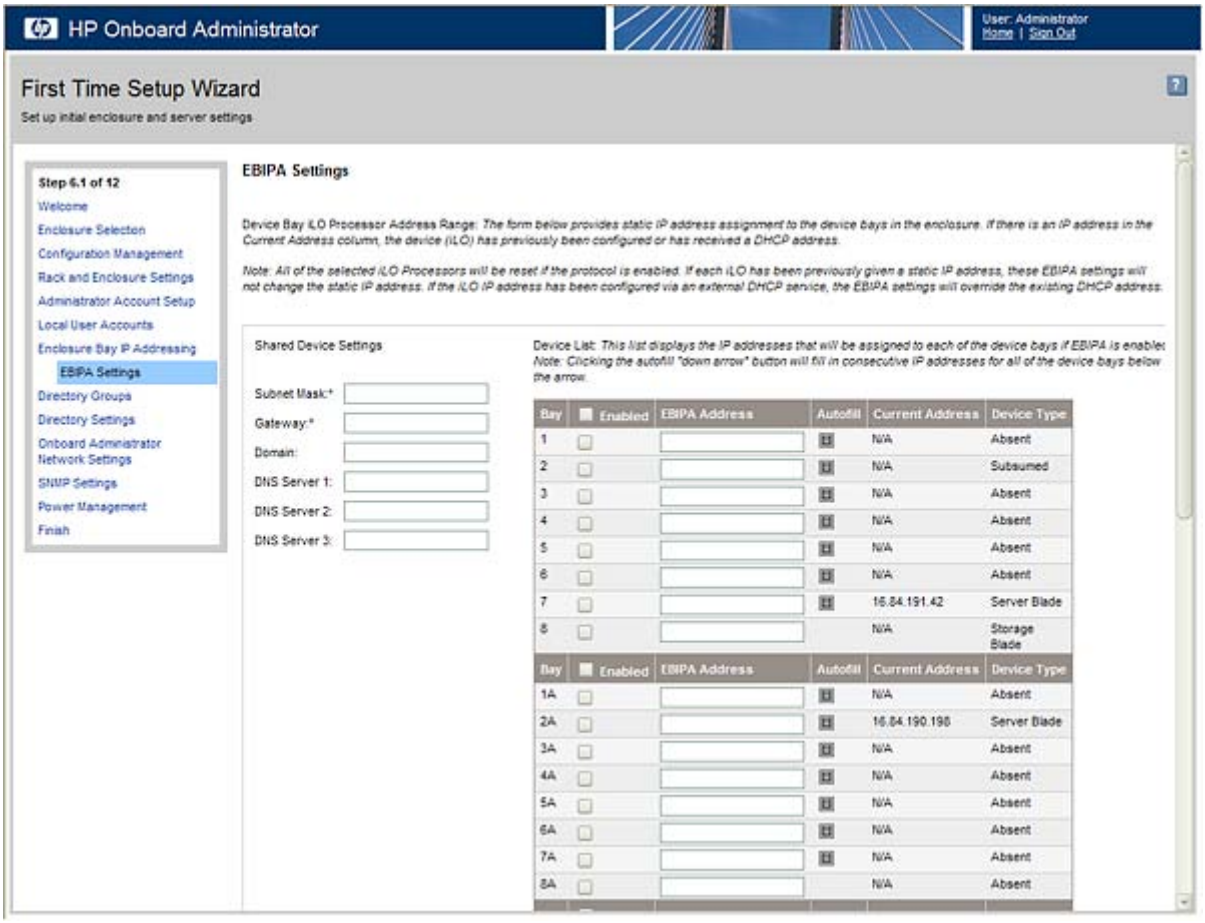
- Direcciones DHCP: el blade de servidor iLO 2 dispone de una función de asignación de DHCP predeterminada, obtenida a través del conector de red del Onboard Administrator activo. Los módulos de interconexión que tienen una conexión de red de gestión interna al Onboard Administrator puede que también tengan, por defecto, direccionamiento DHCP.

  El Onboard Administrator GUI enumera la dirección IP del puerto del blade de servidor iLO 2 y el puerto de gestión del módulo de interconexión.

- IP estática
  - Manual: si en la instalación se requiere una asignación de dirección IP estática, puede modificar individualmente cada uno de los puertos iLO 2 del blade de servidor y los puertos de administración de módulos de interconexión a direcciones estáticas exclusivas o utilizar EBIPA para volver a asignar un rango de direcciones IP estáticas al blade de servidor individual y a los compartimentos de los módulos de interconexión.
  - EBIPA: cuando se inserta un blade de servidor o módulo de interconexión en un compartimento que tiene EBIPA activada, el puerto de administración obtendrá la dirección IP estática específica por parte del administrador integrado si dicho dispositivo está configurado para DHCP.

El administrador establece un rango independiente para los compartimentos del blade de servidor y las de los módulos de interconexión utilizando el asistente de configuración EBIPA del Onboard Administrator. La primera dirección de un rango se asigna al primer compartimento y, luego, a compartimentos consecutivos a lo largo del rango.

Por ejemplo, si establece el intervalo EBIPA del compartimento del servidor entre 16.100.226.21 y 16.100.226.36, al puerto iLO 2 del compartimento del dispositivo n.º 1 se asignará 16.100.226.21, mientras que al puerto iLO 2 del compartimento del dispositivo n.º 12 se asignará 16.100.226.32. Si establece el intervalo EBIPA del compartimento de interconexión entre 16.200.139.51 y 16.209.139.58, al puerto de administración del módulo de interconexión del compartimento de interconexión n.º 1 se asignará 16.200.139.51, mientras que al puerto de administración del módulo de interconexión del compartimento de interconexión n.º 7 se asignará 16.200.139.57.



Para activar la configuración EBIPA para los compartimentos de servidor en este receptáculo, seleccione **Enable Enclosure Bay IP Addressing for Server Bay iLO 2 Processors (Activar el direccionado IP de compartimento del receptáculo para los procesadores iLO 2 de compartimento del servidor)** y, a continuación, introduzca la información siguiente.

Campo	Valor posible	Descripción
Dirección inicial	###.###.###.### donde ### varía de 0 a 255	Dirección IP inicial para los compartimentos del dispositivo o de interconexión. Haga clic en la flecha junto al campo Beginning Address (Dirección inicial), y haga clic en **Update List (Actualizar lista)** para actualizar la lista de interconexión o del dispositivo.
Subnet Mask (máscara de subred)	###.###.###.### donde ### varía de 0 a 255	Máscara de subred de los compartimentos del dispositivo o de interconexión
Gateway (Vía de Acceso)	###.###.###.### donde ### varía de 0 a 255	Dirección IP de la puerta de enlace para los compartimentos de dispositivo o de interconexión
Dominio	Una cadena de caracteres, incluyendo todos los caracteres alfanuméricos y el guión (-)	El nombre del dominio de los compartimentos de dispositivo o interconexión
Servidor DNS 1	###.###.###.### donde ### varía de 0 a 255	La dirección IP del servidor de DNS primario

Campo	Valor posible	Descripción
Servidor DNS 2	###.###.###.### donde ### varía de 0 a 255	La dirección IP del servidor de DNS secundario
Servidor DNS 3	###.###.###.### donde ### varía de 0 a 255	La dirección IP del servidor de DNS terciario
Servidor NTP 1	###.###.###.### donde ### varía de 0 a 255	La dirección IP del servidor primario utilizado para sincronizar la hora y la fecha mediante el protocolo NTP
Servidor NTP 2	###.###.###.### donde ### varía de 0 a 255	La dirección IP del servidor secundario utilizado para sincronizar la hora y la fecha mediante el protocolo NTP

Límites de alimentación dinámica para blades de servidor

El límite de alimentación dinámica es una función de iLO 2 disponible para los blades de servidor c-Class a la que se puede acceder a través de HP Onboard Administrator. Si desea obtener más información acerca de todas las opciones de configuración de alimentación de los blades de servidor c-Class, consulte la *HP BladeSystem Onboard Administrator User Guide (Guía de usuario de HP BladeSystem Onboard Administrator)*.

La función de límite de alimentación dinámica únicamente se encuentra disponible si la plataforma de hardware del sistema, el BIOS (ROM) y la versión del firmware del microcontrolador de alimentación admite esta función. Si el sistema es capaz de ejecutar la función de límite de alimentación dinámica, iLO 2 funcionará automáticamente en modo de límite de alimentación dinámica.

En Onboard Administrator (Administrador a bordo), existen dos opciones de límite de alimentación dinámica:

- Dynamic Power (Alimentación dinámica)

  Si está activada, la alimentación dinámica coloca las fuentes de alimentación sin utilizar en modo de espera para aumentar la eficiencia de la fuente de alimentación del receptáculo, de modo que se reduce al mínimo el consumo de energía del receptáculo durante una menor demanda de energía. Una mayor demanda de energía regresará automáticamente las fuentes de alimentación en espera a su rendimiento completo. Si Dynamic Power (Alimentación dinámica) está:

  - Enabled (Activada) (ajuste predeterminado): algunas de las fuentes de alimentación pueden colocarse automáticamente en espera para aumentar la eficiencia general del subsistema de alimentación del receptáculo.
  - Disabled (Desactivada): todos los suministros de alimentación comparten la carga. La eficiencia del subsistema de alimentación varía según la carga.

- Enclosure Dynamic Power Cap (Límite de la alimentación dinámica del receptáculo)

  Ajuste opcional que permite ajustar un límite en un grupo de servidores de un receptáculo. Ajuste el límite entre los valores mostrados encima del campo Enclosure Dynamic Power Cap (Límite de la alimentación dinámica del receptáculo.) Estos valores están basados en la configuración actual del receptáculo.

  A medida que se ejecutan los servidores, la demanda de energía varía para cada servidor. Se establece un límite de alimentación para cada servidor para suministrar a este alimentación suficiente para satisfacer sus necesidades de carga de trabajo y seguir cumpliendo con el límite de alimentación dinámica del receptáculo.

Es posible utilizar el Static Power Limit (Límite de alimentación estática) o el Enclosure Dynamic Power Cap (Límite de la alimentación dinámica del receptáculo) en las siguientes situaciones:

- Si la alimentación de la instalación se limita al receptáculo, puede introducir un límite fijo en cada receptáculo. Por ejemplo, si la ubicación alojada limita el receptáculo a 5.000 vatios. Escriba 5.000 en el campo Limit Enclosure Input Watts (Límite de vatios de entrada del receptáculo.) El administrador integrado limitará la asignación total de energía a 5.000 vatios, lo cual puede hacer que no se suministre energía a algunos de los blades de servidor.
- Si las instalaciones limitan la capacidad de ventilación del receptáculo, divida el límite de Btu/hr disponible en el receptáculo por 3,41 para determinar el límite de vatios para dicho receptáculo. Introduzca dicho límite de vatios para restringir la carga térmica de los receptáculos. Por ejemplo: Si la instalación limita el receptáculo individual a 27.280 Btu/hr y, a continuación, 27.280 dividido por 3,41 da como resultado 8.000 vatios. Introduzca este límite de vatios para restringir dicho receptáculo a 27.280 Btu/hr. Este límite puede hacer que no se suministre energía a algunos de los blades de servidor.
- Si necesita restringir la carga eléctrica de un receptáculo o la salida térmica, es mejor utilizar un Enclosure Dynamic Power Cap (Límite de la alimentación dinámica del receptáculo.) Permite encender más ranuras que con un Static Power Limit (Límite de alimentación estática.) Un Static Power Limit (Límite de alimentación estática) es mejor en los siguientes casos:

  — Si no desea que existan límites ajustados dinámicamente en los blades de servidor.

  — Si prefiere que no se encienda un blade de servidor si no se le puede asignar alimentación completa (aunque normalmente consuma menos.)

  — Si más de 1/4 de las ranuras del receptáculo no cumplen los requisitos de firmware o hardware de Enclosure Dynamic Power Cap (Límite de la alimentación dinámica del receptáculo.)

  — Si no dispone de suministros de alimentación de ca redundantes.

  — Si no ajusta un límite en un receptáculo vacío. De este modo se desactiva el Static Power Limit (Límite de alimentación estática) y el Enclosure Dynamic Power Cap (Límite de la alimentación dinámica del receptáculo.)

Si desea obtener más información acerca del Static Power Limit (Límite de alimentación estática), consulte la *HP BladeSystem Onboard Administrator User Guide (Guía de usuario de HP BladeSystem Onboard Administrator)*.

Ventilador virtual de iLO 2

En los servidores blade c-Class, HP Onboard Administrator controla los ventiladores del receptáculo. El firmware iLO 2 no puede detectar estos ventiladores de receptáculo. En lugar de ello, el firmware iLO 2 controla un sensor de la temperatura ambiente que se encuentra en el servidor blade. Esta información aparece en la interfaz de iLO 2 y Onboard Administrator la recupera de forma periódica. Onboard Administrator utiliza la información recopilada sobre el sensor de todos los procesadores de gestión iLO 2 del receptáculo para determinar la velocidad de los ventiladores del receptáculo.

Opción iLO

La opción iLO de HP Onboard Administrator permite acceder a iLO 2 Web Administration (Administración web de iLO 2) (Administración Web en la página 148), a Integrated Remote Console Fullscreen (Pantalla completa de la consola remota integrada) (Pantalla completa de IRC en la página 95), Integrated Remote Console (Consola remota integrada) (Opción de Consola remota integrada en la página 96), Remote Console (Consola remota) y a la Remote Serial Console (Consola

remota de serie) (Consola remota de serie en la página 113.) Haciendo clic en los enlaces de esta sección hará que se abran las sesiones de iLO 2 requeridas en ventanas nuevas, mediante el uso de SSO, que no requiere que se introduzca nombre de usuario ni contraseña de iLO 2.

Si la configuración de su explorador no permite que se abran nuevas ventanas, los enlaces no funcionarán correctamente. Si desea obtener ayuda para apagar los programas de bloque de ventanas pop-up, consulte la ayuda en línea.

Administración Web

El enlace Web Administration (Administración Web) que se encuentra en la interfaz de HP Onboard Administrator, permite acceder a la interfaz gráfica de iLO 2. La página System Status (estado del sistema) se muestra, dando una perspectiva general del estado del servidor.

Características de BL p-Class y BL c-Class

Los servidores HP ProLiant BL p-Class y ProLiant c-Class comparten características comunes. En la siguiente tabla se recogen las diferencias que existen entre ellos:

Característica	BL c-Class	BL p-Class
Comunicaciones del receptáculo	Ethernet	i2c
Direccionamiento IP basado en el receptáculo	DHCP	SBIPC
Autenticación de receptáculo a iLO 2	Mutuo	No admitido
Ventilador del servidor	Virtual	Física
Configuración e información del servidor blade	Sin restricciones	Restringido
Alimentación en caso de anulación	No admitido	Admitido
Dongle delantero	SUV (no iLO 2)	SUVi
Gestión de bastidor	Soporte completo mediante HP Onboard Administrator	Soporte limitado mediante iLO 2

5 Servicios de directorio

En esta sección:

Introducción de la integración de directorios

iLO 2 puede configurarse para utilizar un directorio que autentique y autorice a sus usuarios. Antes de configurar iLO 2 para directorios debe decidir si desea utilizar la opción de esquema extendido de HP.

Las ventajas de utilizar la opción del esquema extendido de HP son:

- Existe más flexibilidad para controlar el acceso. Por ejemplo, el acceso se puede limitar a una hora del día o para un determinado rango de direcciones IP.
- Los grupos se mantienen en el directorio, no en cada iLO 2.
- RILOE y RILOE II únicamente funcionan con el esquema extendido de HP. (El esquema libre se añadirá a RILOE II más adelante.)

iLO 2, RILOE y RILOE II únicamente funcionarán con eDirectory con el esquema extendido de HP.

Consulte la lista completa de ventajas en la sección "Ventajas de la integración de directorios" (Ventajas de la integración de directorios en la página 150.) La sección "Gestión remota habilitada por directorio" (Gestión remota habilitada por directorio en la página 185) detalla el modo de habilitar funciones, grupos y seguridad y obligarlos a utilizar directorios. Para obtener más información, en la página Web de HP (http://www.hp.com/servers/lights-out) hay disponibles notas técnicas acerca de la integración de directorios.

Ventajas de la integración de directorios

- Escalabilidad: permite ampliar el directorio para hacerlo compatible con miles de usuarios en miles de dispositivos iLO 2.
- Security (Seguridad): se heredan sólidas directivas de contraseñas de usuario del directorio. Algunos ejemplos de estas directivas son la complejidad de las contraseñas de usuario, la frecuencia de rotación o la caducidad.
- Anonimato (ausencia de): en algunos entornos, los usuarios comparten cuentas de Lights-Out, lo que produce que en ciertos casos no se conozca quién realiza una operación determinada ni qué cuenta (o función) se emplea.
- Administración basada en funciones: es posible crear funciones (por ejemplo, administrativa, de control remoto del host o de control total) y asociar los usuarios o los grupos de usuarios a dichas

funciones. Un cambio en una única función se aplica a todos los usuarios de los dispositivos Lights-Out asociados con dichas funciones.

- Punto único de administración: es posible utilizar herramientas administrativas nativas, como MMC o ConsoleOne, para administrar los usuarios de Lights-Out.
- Inmediatez: cualquier cambio en el directorio afecta de forma automática a todos los procesadores de Lights-Out asociados. De esta forma, se elimina la necesidad crear secuencias de comandos para la realización de este proceso.
- Eliminación de otro nombre de usuario y contraseña: puede utilizar contraseñas y cuentas de usuario existentes en el directorio sin necesidad de registrar ni recordar un nuevo conjunto de credenciales de Lights-Out.
- Flexibilidad: puede crear una única función para un único usuario en un único dispositivo iLO 2 o puede crear una única función para varios usuarios en varios dispositivos iLO 2. También es posible utilizar diferentes combinaciones de funciones según las necesidades de su empresa.
- Compatibilidad: la integración del directorio de Lights-Out se aplica a los productos iLO 2, RILOE y RILOE II. La integración es compatible con Active Directory y con eDirectory.
- Estándares: el directorio de Lights-Out es compatible con las versiones de compilación posteriores al estándar LDAP 2.0 para el acceso seguro al directorio.

Ventajas y desventajas de los directorios sin esquema y del directorio de esquema HP

Los directorios mejoran la seguridad y permiten gestionar el acceso y los derechos desde una ubicación centralizada. Asimismo, permiten una configuración flexible. Algunas prácticas de configuración de directorios funcionan con iLO 2 mejor que otras. Antes de configurar iLO 2 para directorios, debe decidir si desea utilizar el directorio sin esquema o los métodos de integración de directorios de esquema de HP. Responda a las siguientes preguntas. Éstas le ayudarán a evaluar los requisitos de integración de los directorios:

1. ¿Puede aplicar extensiones de esquema a su directorio?
   - No. ¿Utiliza Microsoft Active Directory?
   - No. Es posible que la integración de directorios no sea adecuada para su entorno. Contemple la posibilidad de implementar un servidor de directorios para evaluar las ventajas de la integración de directorios.

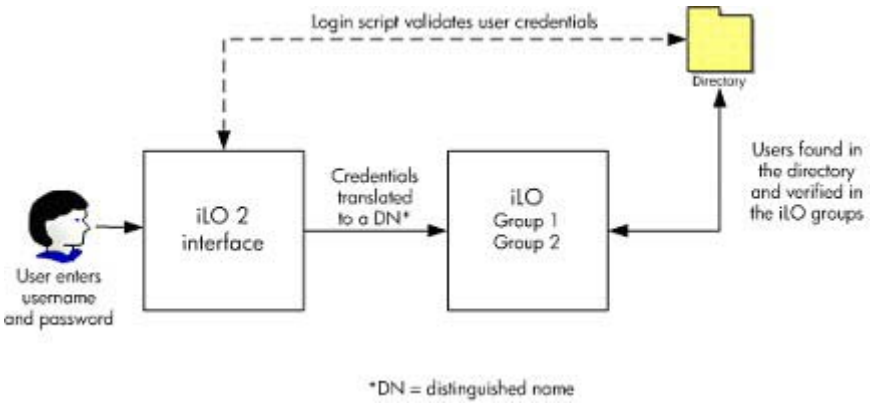
     — Sí. Utilice la integración de directorios sin esquema basada en grupo.
   - Sí. Diríjase a la pregunta 2.
2. ¿Es su configuración ampliable?
   - No. Implemente una instancia de la integración de directorios sin esquema para evaluar si este método de integración de directorios cumple o no con su política y requisitos de procedimientos. Si es necesario, podrá implementar la integración de directorios de esquema de HP más adelante.
   - Sí. Utilice la integración de directorios de esquema de HP.

     Las preguntas siguientes le pueden ayudar a determinar si la configuración es escalable:
   - ¿Tiene la posibilidad de realizar cambios en los derechos o privilegios de un grupo de usuarios de directorio?

- ¿Creará con regularidad secuencias de comandos de los cambios de iLO 2?
- ¿Utiliza más de cinco grupos para controlar los privilegios de iLO 2?

Integración de directorios sin esquema

Mediante el método de integración de directorios libre de esquemas, los usuarios y miembros de un grupo residen en el directorio pero los privilegios de grupo residen en el iLO 2 individual. iLO 2 utiliza credenciales de inicio de sesión para leer el objeto de usuario en el directorio y recuperar los miembros de grupos de usuario, que se comparan con los guardados en iLO 2. Si se produce alguna coincidencia, se otorga autorización. Por ejemplo:



Ventajas de utilizar la integración de directorios sin esquema:

- No hay necesidad de ampliar el esquema de directorio.
- Cuando los controles ActiveX están activados en el explorador e inicio de sesión, los formatos NetBIOS y de correo electrónico son compatibles.
- Los usuarios del directorio no requieren configuración o la configuración necesaria es mínima. Si no hay ninguna configuración, el directorio utiliza los usuarios y miembros de grupos existentes para acceder a iLO 2. Por ejemplo, si cuenta con un administrador de dominio denominado Usuario 1, puede copiar el nombre distinguido del grupo de seguridad del administrador de dominio a iLO 2 y darle todos los privilegios. Usuario1 ya podrá acceder a iLO 2.

Desventajas de utilizar la integración de directorios sin esquema

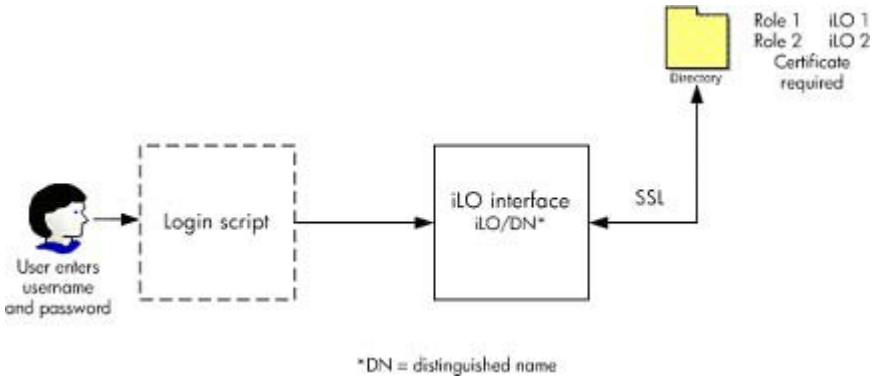
- Únicamente es compatible con Microsoft® Active Directory
- Los privilegios de grupo se administran en cada iLO 2. Sin embargo, este inconveniente queda minimizado por el hecho que los privilegios de grupo apenas cambian, y la tarea de cambiar los miembros de grupos se administra en el directorio y no en cada iLO 2 independiente. HP ofrece herramientas que permiten realizar cambios simultáneamente a un gran número de iLO 2.

integración de directorios de esquema HP

La integración de directorios de esquema de HP consta de una clase denominada hpqRole, que es una integración de directorios de esquema de HP de subclase y consta de una clase denominada hpqRole (una subclase de Grupo), una denominada hpqTarget (una subclase de Usuario), junto con otras clases de ayuda. Una instancia de una hpqRole es simplemente una función. Una instancia de una hpqTarget equivale a un dispositivo iLO 2.

Una función está formada por uno o varios dispositivos iLO 2 y uno o varios usuarios. La función cuenta con una lista de privilegios de los que disfrutan los usuarios con iLO 2 en la función. Todos los accesos

a iLO 2 se gestionan agregando y eliminando de la función usuarios y dispositivos iLO 2, así como gestionando los privilegios de la función. Por ejemplo:



Ventajas de utilizar la integración de directorios de esquema de HP:

- Mayor flexibilidad en el control de acceso. Por ejemplo, el acceso se puede limitar a una hora del día o para un determinado rango de direcciones IP.
- Los grupos y permisos se mantienen en el directorio, no en cada dispositivo iLO 2, y HP proporciona los complementos necesarios para gestionar grupos y los destinos de HP para usuarios y equipos de Active Directory y eDirectory ConsoleOne.
- Integración con eDirectory

Desventajas de la integración de directorios de esquema de HP:

- El esquema del directorio debe extenderse. Sin embargo, esta tarea se ha minimizado, ya que HP proporciona el archivo .ldf y un asistente para extender el esquema y, además, las últimas versiones de Active Directory permiten deshacer los cambios realizados en los esquemas.

  Si desea obtener información acerca de cómo ampliar el esquema y la configuración de la información de ajustes de directorios, consulte *Integrating HP ProLiant Lights-Out processors with Microsoft® Active Directory (Integración de los procesadores HP ProLiant Lights-Out con Microsoft® Active Directory* (http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00190541/c00190541.pdf.)

- Requisitos de certificados

  iLO 2 debe establecer la comunicación con el directorio mediante LDAP a través de SSL. Para la comunicación es necesario que el servidor de directorios disponga de un certificado. La instalación del certificado para el dominio lo replica a través de los controladores de dominio en dicho dominio. Para obtener información acerca de la instalación del certificado, consulte la sección Customer Advisory (Asesoramiento al cliente) de la página Web de HP (http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp.)

- Opciones de recuperación de errores

  Para activar la recuperación de errores (redundancia), utilice el nombre de dominio como nombre del servidor de directorios al configurar iLO 2. La mayoría de los servidores DNS resuelven un nombre de dominio a un servidor de directorios en funcionamiento (controlador de dominio.)

- Formato de inicio de sesión

  Es posible utilizar los formatos de nombre completo, NetBIOS y UPN como nombres de inicio de sesión. La secuencia de comandos de inicio de sesión para iLO 2 comunica con el sistema operativo cliente e intenta traducir el nombre de inicio de sesión a un nombre distinguido de directorio. Para que la secuencia de comandos de inicio de sesión pueda llevar a cabo esta acción,

el nombre del directorio debe ser un nombre DNS, no una dirección IP. Además, tanto el cliente como iLO 2 deben tener acceso al servidor de directorios utilizando el mismo nombre. Tanto el cliente como iLO 2 deben encontrarse en el mismo dominio DNS.

- Destinos múltiples

  No es necesario utilizar varios destinos en el directorio. La integración de directorios de esquema de HP únicamente requiere un objeto hpqTarget, que puede representar un gran número de dispositivos LOM.

Configuración de la integración del directorio de esquema libre

Antes de configurar la opción de esquema libre, el sistema debe cumplir todos los requisitos previos listados en la sección "Preparación de Active Directory" (Preparación de Active Directory en la página 154.)

Es posible configurar iLO 2 en directorios de tres formas:

- Utilizando manualmente un explorador (Configuración basada en explorador del esquema libre en la página 156.)
- Utilizando una secuencia de comandos (Configuración de secuencias de comandos sin esquemas en la página 156.)
- Utilizando HPLOMIG (Configuración basada en HPLOMIG del esquema libre en la página 156.)

Preparación de Active Directory

La opción de esquema libre es compatible con los siguientes sistemas operativos:

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory

Se debe activar SSL en el directorio. Para activar SSL, instale un certificado para el dominio en Active Directory. iLO 2 únicamente se comunica con el directorio a través de una conexión SSL segura. Para más información, consulte el artículo número 247078 de la Microsoft® Knowledge Base: *Enabling SSL Communication over LDAP for Windows® 2000 Domain Controllers (Activación de la comunicación SSL a través de LDAP para los controladores de dominio de Windows® 2000* en la página Web de Microsoft® (http://support.microsoft.com/.)

Para validar la configuración, debería disponer del nombre completo de directorio para al menos un usuario, y el nombre completo de un grupo de seguridad del que el usuario sea miembro.

Introducción a los servicios de Certificate Server

Los Servicios de Certificate Server se utilizan para emitir certificados firmados digitalmente a los hosts de la red. Los certificados se utilizan para establecer conexiones SSL con el host y verificar la autenticidad del host.

La instalación de los Servicios de Certificate Server permite a Active Directory la recepción de un certificado que permite a los procesadores de Lights-Out conectarse al servicio de directorio. Sin un certificado, iLO 2 no puede conectarse al servidor del directorio.

Todos los servidores de directorios con los que desee conectar iLO 2 deberán emitir un certificado. Si instala un servicio de certificados empresariales, Active Directory puede, automáticamente, solicitar e instalar certificados para todos los controladores de Active Directory de la red.

Instalación de los servicios de Certificate Server

1. Seleccione **Inicio>Configuración>Panel de control**.
2. Haga doble clic en **Agregar o quitar programas**.
3. Haga clic en **Agregar o quitar componentes de Windows** para iniciar el Asistente para componentes de Windows.
4. Seleccione la casilla de verificación **Servicios de Certificate Server**. Haga clic en **Siguiente**.
5. Haga clic en **Aceptar** cuando se muestre la advertencia que indica que no se ha podido cambiar el nombre del servidor. Se selecciona la opción de CA raíz empresarial porque no hay ninguna CA registrada en el directorio activo.
6. Introduzca la información correspondiente a su sitio y su organización. Acepte el periodo de tiempo predeterminado de dos años en el campo `Valid for (Válido durante)`. Haga clic en **Siguiente**.
7. Acepte la ubicación predeterminada de la base de datos de certificados y del registro de la base de datos. Haga clic en **Siguiente**.
8. Desplácese hasta la carpeta c:\I386 cuando se le pida el CD de Windows® 2000 Advanced Server.
9. Haga clic en **Finish (Finalizar)** para cerrar el Asistente.

Comprobación de servicios Certificate Server

Puesto que los procesadores de gestión se comunican con Active Directory mediante SSL, debe crear un certificado o instalar los Servicios de Certificate Server. Es necesario instalar una CA empresarial, ya que emitirá certificados a objetos de su dominio de organización.

Para verificar que los servicios de Certificate Server se encuentran instalados, seleccione **Inicio>Programas>Herramientas administrativas>Entidad de certificación**. Si no están instalados los servicios de Certificate Server, se mostrará el siguiente mensaje de error.

Configuración de la solicitud de certificado automática

Para especificar la emisión de un certificado al servidor:

1. Seleccione **Start (Inicio)>Run (Ejecutar)**, e introduzca `mmc`.
2. Haga clic en **Add (Agregar)**.
3. Seleccione **Group Policy (Directiva de grupo)**, y haga clic en **Add (Añadir)** para agregar el complemento a MMC.
4. Haga clic en **Browse (Explorar)** y seleccione el objeto de directiva de dominio predeterminado. Haga clic en **OK (Aceptar)**.
5. Seleccione **Finish (Finalizar)>Close (Cerrar)>OK (Aceptar)**.
6. Amplíe **Configuración del equipo>Configuración de Windows>Configuración de seguridad>Directivas de claves públicas**.
7. Haga clic con el botón secundario del ratón en **Automatic Certificate Requests Settings (Configuración de solicitudes de certificado automáticas)** y seleccione **New (Nuevo) >Automatic Certificate Request (Solicitud de certificado automática)**.
8. Haga clic en **Next (Siguiente)** cuando se inicie el asistente para la configuración de solicitudes automáticas.

9. Seleccione la plantilla **Domain Controller (Controlador de dominio)** y haga clic en **Next (Siguiente)**.
10. Seleccione la autorización de certificado de la lista. (Es el mismo CA que se define durante la instalación de los servicios de Certificate Server.) Haga clic en **Siguiente**.
11. Haga clic en **Finish (Finalizar)** para cerrar el Asistente.

Configuración basada en explorador del esquema libre

El esquema libre se puede configurar mediante la interfaz basada en explorador de iLO 2.

1. Inicie una sesión en iLO 2 con una cuenta con el privilegio Configure iLO 2 Settings (Configurar valores de iLO 2.) Haga clic en **Administration (Administration)**.

NOTA: Sólo los usuarios que tengan el privilegio Configure iLO 2 (Configurar iLO 2) pueden cambiar esta configuración. Los usuarios que no tengan el privilegio Configure iLO 2 Settings (Configurar valores de iLO 2) sólo podrán ver los valores de configuración asignados.

2. Haga clic en **Directory Settings (Configuración de directorio)**.
3. Seleccione **Use Directory Default Schema (Utilizar el esquema de directorio predeterminado)** en la sección de Authentication Settings (Valores de autenticación.) Para obtener más información, consulte la sección "Opciones de configuración del esquema libre" (Opciones de configuración del esquema libre en la página 157.)
4. Haga clic en **Apply Settings (Aplicar configuración)**.
5. Haga clic en **Test Settings (Probar valores de configuración)**.

Configuración de secuencias de comandos sin esquemas

Para configurar la opción de directorios sin esquemas con las secuencias de comandos XML de RIBCL, realice lo siguiente:

1. Descargue y revise la guía de recursos de las secuencias y líneas de comandos.
2. Escriba una secuencia de comandos que configure iLO 2 para que sea compatible con directorios sin esquemas y, a continuación, ejecútela. La siguiente secuencia de comandos se puede utilizar como plantilla.

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="admin" PASSWORD="password">
<DIR_INFO MODE = "write">
<MOD_DIR_CONFIG>
<DIR_ENABLE_GRP_ACCT value = "yes"/>
<DIR_GRPACCT1_NAME value ="CN=Administrators,
CN=Builtin,DC=HP,DC=com "/>
<DIR_GRPACCT1_PRIV value = "1"/>
</MOD_DIR_CONFIG>
</DIR_INFO>
</LOGIN>
</RIBCL>
```

Configuración basada en HPLOMIG del esquema libre

HPLOMIG es la manera más sencilla para configurar una gran cantidad de procesadores LOM para directorios. Para utilizar HPLOMIG, descargue la utilidad HPQLOMIG y documentación adicional de la página Web de HP (http://www.hp.com/servers/lights-out.) HP recomienda utilizar HPLOMIG cuando

se configuran varios procesadores LOM para directorios. Si desea obtener más información acerca de la utilización de HPLOMIG, consulte "Utilidad de migración de directorios HPQLOMIG (Utilidad de migración de directorios HPQLOMIG en la página 193)".

Opciones de configuración del esquema libre

Las opciones de configuración son las mismas independientemente del método (explorador, HPQLOMIG o secuencia de comandos) que se utilice para configurar el directorio.

Tras activar los directorios y seleccionar la opción esquema libre, tiene las siguientes opciones.

Minimum Login Flexibility (Flexibilidad mínima de inicio de sesión)

- Introduzca el nombre DNS del servidor de directorio o la dirección IP y el puerto LDAP. Normalmente, el puerto LDAP para una conexión SSL es 636.
- Introduzca el nombre completo para al menos un grupo. Este grupo puede ser un grupo de seguridad (por ejemplo: "CN=Administrators,CN=Builtin,DC=HP,DC=com") o cualquier otro grupo, mientras los usuarios que pretendan acceder a iLO 2 sean miembros del grupo.

  Con una configuración mínima, podrá iniciar sesión en iLO 2 mediante el nombre completo y la contraseña. Deberá ser miembro de un grupo que iLO 2 reconozca.

Better Login Flexibility (Mejor flexibilidad de inicio de sesión)

- Además de los valores de configuración mínimos, introduzca al menos un contexto de usuario de directorio.

  En el momento de iniciar sesión, se combinan el nombre de inicio de sesión y el contexto de usuario para formar el nombre completo de usuario. Por ejemplo, si el usuario inicia sesión como "JOHN.SMITH" y se configura un contexto de usuario como "CN=USERS,DC=HP,DC=COM", el nombre completo que iLO 2 probará será "CN=JOHN.SMITH,CN=USERS,DC=HP,DC=COM".

Maximum Login Flexibility (Flexibilidad máxima de inicio de sesión)

- Configure iLO 2 de la manera que se describe.
- Configure iLO 2 con un nombre DNS, pero no con una dirección IP para la dirección de red del servidor de directorio. El nombre DNS se puede resolver en una dirección IP de iLO 2 y del sistema cliente.
- Active los controles ActiveX en el explorador. La secuencia de comandos de inicio de sesión en iLO 2 tratará de ejecutar un control de Windows® para convertir el nombre de inicio de sesión en un nombre completo.

  La configuración de iLO 2 con una flexibilidad máxima de inicio de sesión permitirá iniciar sesión mediante un nombre completo y una contraseña, su nombre tal y como aparece en el directorio, en formato NetBIOS (domain/login_name) o en formato de correo electrónico (login_name@domain.)

NOTA: La configuración de seguridad del sistema o el software instalado puede evitar que la secuencia de comandos de inicio de sesión ejecute el control de Windows® ActiveX. En el caso de que esto suceda, el explorador mostrará un mensaje de aviso en la barra de estado, una ventana de mensaje o quizás no responda. Para facilitar la identificación del software o la configuración que causa el problema, cree otro perfil e inicie la sesión en el sistema.

En algunos casos, puede que no sea posible que funcione la opción de flexibilidad máxima de inicio de sesión. Por ejemplo, si el cliente e iLO 2 se encuentran en dominios DNS distintos, es posible que uno de los dos no consiga resolver el nombre de servidor de directorio en una dirección IP.

Grupos anidados sin esquema

Numerosas organizaciones tienen a sus usuarios y administradores organizados en grupos. Se recomienda este tipo de organización en grupos existentes, ya que es posible asociarlos con uno o más objetos de función de Integrated Lights-Out Management (Gestión de Integrated Lights-Out.) Cuando los dispositivos están asociados a los objetos de función, es posible utilizar los controles del administrador para acceder a los dispositivos de Lights-Out asociados a la función, añadiendo o eliminando miembros de los grupos.

Si se utiliza Microsoft® Active Directory, es posible colocar un grupo dentro de otro grupo, creando de este modo un grupo anidado. Los objetos de función se consideran grupos y pueden incluir directamente otros grupos. Es posible añadir el grupo anidado existente directamente a la función y asignar los derechos y restricciones apropiados. Se pueden añadir nuevos usuarios al grupo existente o a la función.

En implementaciones anteriores, sólo un usuario sin esquema que fuera miembro directo del grupo primario tenía permiso para iniciar sesión en iLO 2. Con el uso de la integración sin esquema, los usuarios que son miembros indirectos (miembros de un grupo anidado de un grupo principal) pueden iniciar sesión en iLO 2.

Novell eDirectory no permite grupos anidados. En eDirectory, cualquier usuario que pueda leer una función se considera miembro de dicha función. Al añadir un grupo, una unidad organizativa u organización existente a una función, añada el objeto como un elemento de confianza de la función. Todos los miembros del objeto se consideran miembros de la función. Se pueden añadir nuevos usuarios al objeto existente o a la función.

Cuando se usan asignaciones de derechos de administración o de directorio para ampliar los miembros de la función, los usuarios deberán poder leer el objeto LOM que representa al dispositivo LOM. Algunos entornos requieren que los elementos de confianza de una función sean también los elementos de confianza del objeto LOM para poder autenticar correctamente a los usuarios.

Configuración de la integración de directorios con esquema de HP

Cuando se utiliza la integración de directorios de esquema HP, iLO 2 es compatible tanto con Active Directory como con eDirectory. Sin embargo, los servicios de estos directorios requieren que se amplíe el esquema.

Funciones compatibles con la integración de directorios de esquema HP

Las funciones de los servicios de directorio de iLO 2 permiten:

- Autentificar usuarios de una base de datos compartida, consolidada y ampliable.
- Controlar privilegios de usuario (autorización) mediante el servicio de directorio.
- Utilizar funciones del servicio de directorio para la administración de niveles de grupos de los procesadores de gestión y usuarios de iLO 2.

La extensión del esquema debe realizarla un Administrador de esquemas. La base de datos de usuarios locales se conserva. Tiene la opción de no utilizar directorios, utilizar una combinación de directorios y cuentas locales o utilizar directorios exclusivamente para la autenticación.

NOTA: Cuando está conectado a través del puerto de diagnóstico, el servidor del directorio no está disponible. Sólo puede iniciar la sesión utilizando una cuenta local.

Configuración de los servicios de directorio

Para activar correctamente la gestión habilitada por el directorio en cualquier procesador de gestión de Lights-Out:

1. Planificación

   Consulte las secciones siguientes:

   - "Servicios de directorio (Servicios de directorio en la página 150)"
   - "Esquema de los servicios de directorio (Esquema de los servicios de directorio en la página 238)"
   - "Gestión remota habilitada por directorio (Gestión remota habilitada por directorio en la página 185)"

2. Instalación

   a. Descargue el paquete HP Lights-Out Directory Package que contiene el instalador de esquema, el instalador de complementos de gestión, así como las utilidades de migración de la página Web de HP (http://www.hp.com/servers/lights-out.)

   b. Ejecute una vez el instalador de esquema (Instalador de esquema en la página 161) para extender el esquema.

   c. Ejecute el instalador de complementos de gestión (Instalador de complementos de gestión en la página 163) e instale el complemento apropiado para el servicio de directorio en cuestión en una o varias estaciones de trabajo de gestión.

3. Actualización

   a. Actualice el ROM del procesador de gestión de Lights-Out con el firmware preparado para directorio.

   b. Configure el servidor de directorios así como el nombre completo de los objetos del procesador de gestión en la página Directory Settings (Configuración de directorio) (Configuración de directorio en la página 52) en la GUI de iLO 2.

4. Gestión

   a. Cree un objeto de dispositivo de gestión y un objeto de función (Objetos de servicios de directorio en la página 170) mediante el complemento.

   b. Asigne derechos al objeto de función según sea necesario y asocie la función al objeto de dispositivo de gestión.

   c. Añada usuarios al objeto de función.

   Para obtener información adicional acerca de la administración de los servicios de directorios, consulte “Gestión remota habilitada por directorio” (Gestión remota habilitada por directorio en la página 185.) En las secciones "Servicios de directorio para Active Directory" (Servicios de directorio para Active Directory en la página 163) y "Servicios de directorio para eDirectory" (Servicios de directorio para eDirectory en la página 175) se incluyen ejemplos.

5. Manejo de excepciones

   - El uso de las utilidades de migración de Lights-Out es más sencillo con una única función de Lights-Out. Si tiene planeado crear varias funciones en el directorio, es posible que necesite utilizar utilidades de edición de líneas de comandos del directorio, como líneas de comandos VB o LDIFDE, para crear asociaciones de funciones complejas. Consulte “Uso de herramientas de importación masiva” (Uso de herramientas de importación masiva en la página 191) para obtener más información.

- Si dispone de procesadores iLO 2 o RILOE con firmware antiguo, es posible que necesite actualizarlo manualmente por medio de un explorador. Los requisitos mínimos de firmware para la actualización del firmware remoto por medio de RIBCL y la utilidad de migración de directorios son:

Producto LOM	Firmware mínimo permitido
RILOE	2.41
RILOE II	Todas las versiones
iLO	1.4x
iLO 2	1.1x

Tras extender el esquema, puede finalizar la configuración de los servicios de directorio mediante las utilidades de migración de directorios Lights-Out de HP (Utilidad de migración de directorios HPQLOMIG en la página 193.) El paquete Lights-Out Directory Package de HP incluye las utilidades de migración. La versión 1.13 de la utilidad de migración de directorios permite a Lights-Out importar y exportar, y es compatible con distintas credenciales de usuario para todos los procesadores de Lights-Out.

Documentación de esquema

Como ayuda para el proceso de planificación y aprobación, HP proporciona documentación relativa a los cambios efectuados en el esquema durante el proceso de configuración de éste. Para comprobar los cambios realizados en el esquema existente, consulte “Esquema de los servicios de directorio” (Esquema de los servicios de directorio en la página 238.)

Compatibilidad de los servicios de directorio

Mediante la integración del directorio de esquema HP, iLO 2 es compatible con los servicios de directorio siguientes:

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory
- Microsoft® Windows® Server 2008 Active Directory
- Novell eDirectory 8.7.3
- Novell eDirectory 8.7.1

El software de iLO 2 está diseñado para ejecutarse en las herramientas de gestión Usuarios y equipos de Microsoft® Active Directory y Novell ConsoleOne, lo que permite gestionar cuentas de usuario en Microsoft® Active Directory o Novell eDirectory. Esta solución no establece diferencias entre el funcionamiento de eDirectory con NetWare, Linux o Windows®. Para generar una ampliación de esquema de eDirectory se requiere Java™ 1.4.0 o posterior para la autenticación SSL.

iLO 2 admite la ejecución de Microsoft® Active Directory en cualquiera de los sistemas operativos siguientes:

- Windows Server® 2008
- Windows Server® 2003

iLO 2 admite eDirectory si se ejecuta con Novell.

Software necesario para el esquema

iLO 2 precisa software específico, que ampliará el esquema y proporcionará complementos para gestionar la red de iLO 2. Se puede descargar un Smart Component de HP que contiene el instalador del esquema y el instalador de complementos de gestión. Smart Component de HP se puede descargar de la página Web de HP (http://www.hp.com/servers/lights-out.)

No se puede ejecutar el instalador del esquema en un controlador de dominio que dispone de Windows Server® 2008 Core. Windows Server® 2008 Core no utiliza una interfaz gráfica de usuario (por razones de seguridad y de rendimiento.) Para utilizar el instalador del esquema, es necesario instalar una interfaz gráfica de usuario en el controlador de dominio o utilizar un controlador de dominio que disponga de una versión anterior de Windows®.

Instalador de esquema

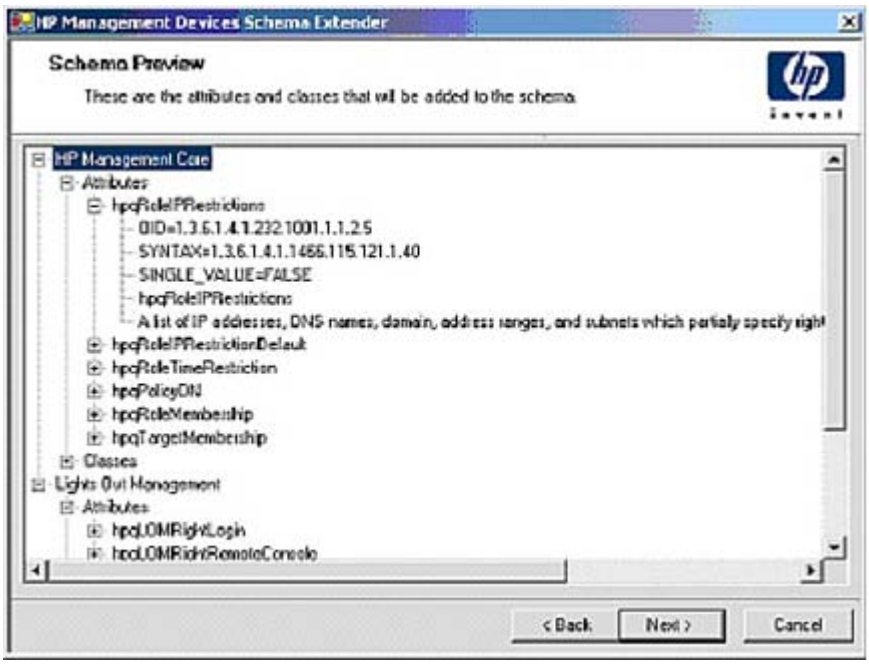
Con el instalador de esquema se incluyen uno o varios archivos .xml. Estos archivos contienen el esquema que se añadirá al directorio. Normalmente, uno de estos archivos contendrá el esquema básico común a todos los servicios de directorio admitidos. Los archivos adicionales sólo contienen esquemas específicos de producto. Para utilizar el instalador es necesario el programa .NET framework.

El instalador muestra tres pantallas importantes:

- Vista previa del esquema
- Configuración
- Results

Vista previa del esquema

La pantalla Schema Preview (Vista previa del esquema) permite al usuario ver las ampliaciones propuestas del esquema. Esta pantalla lee los archivos de esquema seleccionados, analiza los XML y los muestra de forma arborescente. Elabora una lista de todos los detalles de sus atributos y los clasifica por el orden en que se van a instalar.



Configuración

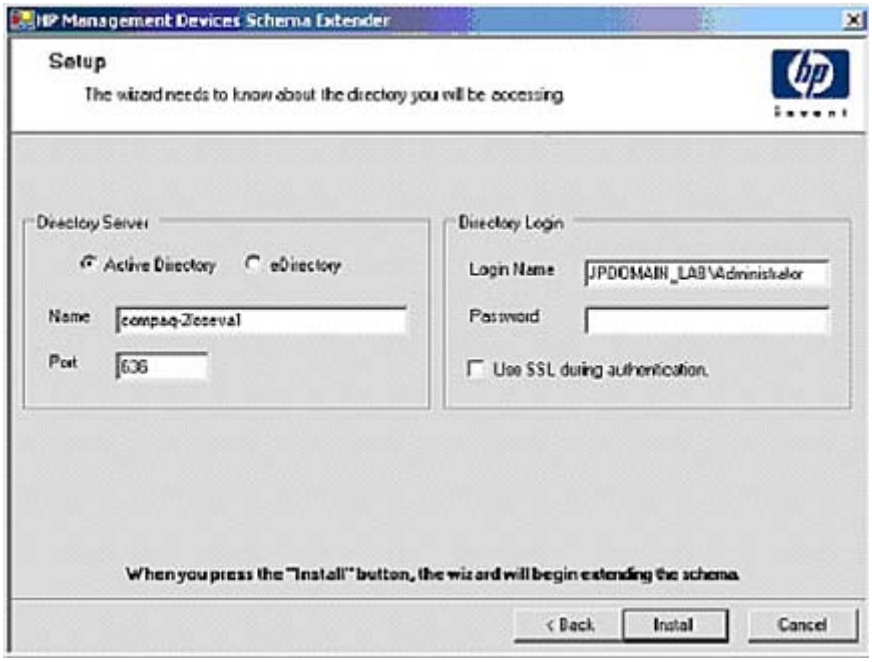
La pantalla Setup (Configuración) se utiliza para especificar la información correspondiente antes de ampliar el esquema.

La sección Directory Server (Servidor de directorios) de la pantalla Setup (Configuración) permite seleccionar si se utilizará Active Directory o eDirectory, así como establecer el nombre del equipo y el puerto que se va a usar para las comunicaciones LDAP.

NOTA: La ampliación del esquema en Active Directory requiere que el usuario sea un administrador de esquemas autenticado, que el esquema no esté protegido contra escritura y que el directorio sea el propietario de la función FSMO en el árbol. El instalador intentará convertir el servidor de directorios de destino en el maestro de esquema FSMO del bosque.

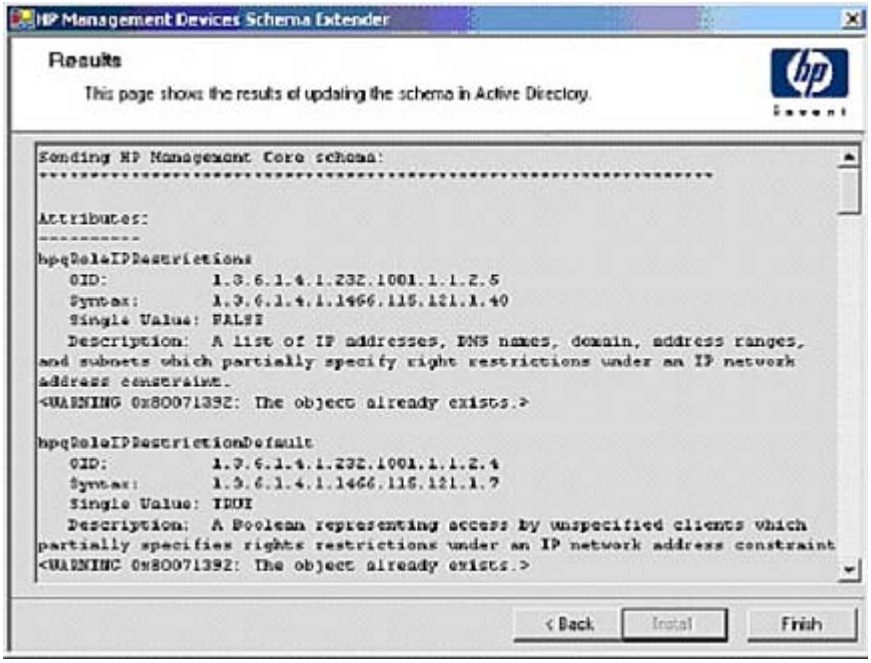
Para tener acceso de escritura al esquema con Windows® 2000 es necesario cambiar el bloqueo interno del registro de seguridad. Si elige la opción **Active Directory**, el soporte de ampliación del sistema intentará cambiar el registro. Esto sólo funcionará si el usuario cuenta con los permisos necesarios. En Windows® Server 2003 se activa automáticamente el acceso de escritura al esquema.

La sección Directory Login (Inicio de sesión en el directorio) de la pantalla Setup (Configuración) permite escribir el nombre de inicio de sesión y la contraseña, que pueden ser necesarios para finalizar la ampliación del esquema. La opción Use SSL during authentication (Usar SSL durante la autenticación) establece la forma de autenticación segura que se va a utilizar. Si está seleccionada esta opción, se usa la autenticación de directorio mediante SSL. Si no está seleccionada y se selecciona Active Directory, se usará la autenticación de Windows NT®. Si no está seleccionada y se selecciona eDirectory, la autenticación del administrador y la extensión del esquema se realizarán mediante una conexión no cifrada (texto sin cifrar.)



Results

La pantalla Results (Resultados) muestra los resultados de la instalación, incluido si el esquema se ha podido ampliar y los atributos que se han cambiado.



Instalador de complementos de gestión

El instalador de complementos de gestión instala los complementos necesarios para gestionar los objetos de iLO 2 en un directorio de Usuarios y equipos de Active Directory de Microsoft® o en un directorio de Novell ConsoleOne.

Los complementos de iLO 2 se utilizan para realizar las siguientes tareas al crear un directorio de iLO 2:

- Crear y gestionar los objetos de iLO 2 y de función (los objetos de directiva se admitirán más adelante)
- Realizar las asociaciones entre los objetos de iLO 2 y los objetos de función (o directiva)

Servicios de directorio para Active Directory

En las secciones siguientes se recogen los requisitos previos de instalación, la preparación y un ejemplo funcional de los servicios de directorio para Active Directory. HP ofrece una utilidad que automatiza gran parte del proceso de configuración de directorios. Puede descargar la compatibilidad de directorios de HP para los procesadores de gestión en la página Web de HP (http://h18004.www1.hp.com/support/files/lights-out/us/index.html.)

Requisitos previos para instalar Active Directory

- Para permitir la conexión segura de iLO 2 en la red, Active Directory debe disponer de un certificado digital instalado.
- Active Directory debe disponer de un esquema extendido para describir las propiedades y clases de objeto Lights-Out.
- La versión de firmware debe ser iLO v1.40 o posterior, o iLO v1.00 o posterior.
- Debe disponer de la licencia necesaria para las funciones avanzadas de iLO 2.

  Puede evaluar las funciones avanzadas de iLO por medio de una licencia de evaluación gratuita que puede descargar de la página Web de HP (http://h10018.www1.hp.com/wwsolutions/ilo/iloeval.html.)

Los servicios de directorio para iLO 2 utilizan LDAP sobre SSL para comunicarse con los servidores de directorio. Antes de instalar los complementos y el esquema para Active Directory, consulte y tenga a mano la siguiente documentación:

NOTA: La instalación de los servicios de directorio para iLO 2 requiere ampliar el esquema de Active Directory. Este esquema se puede completar con un Active Directory Schema Administrator (administrador de esquema de Active Directory.)

- *Extending the Schema (Extensión del esquema)* incluido en el Microsoft® Windows® 2000 Server Resource Kit, disponible en la página Web de Microsoft® (http://msdn.microsoft.com.)
- *Installing Active Directory (Instalación de Active Directory)* incluido en el Microsoft® Windows® 2000 Server Resource Kit
- Artículos de Microsoft® Knowledge Base

  Puede acceder a estos artículos por medio de la opción de búsqueda del número de ID del artículo en la base de datos Knowledge Base de la página Web de Microsoft® (http://support.microsoft.com/.)

  - 216999 *Installing the Remote Server Administration Tools in Windows® 2000 (Instalar las herramientas de administración del servidor remoto en Windows® 2000)*
  - 314978 *Using the Adminpak.msi to Install a Server Administration Tool in Windows® 2000 (Utilizar Adminpak.msi para instalar una herramienta de administración del servidor en Windows® 2000)*
  - 247078 *Enabling SSL Communication over LDAP for Windows® 2000 Domain Controllers (Activación de la comunicación SSL con LDAP para controladores de dominio de Windows® 2000)*
  - 321051 *Enabling LDAP over SSL with a Third-Party Certificate Authority (Activación de LDAP con SSL con una autorización certificada de otro fabricante)*
  - 299687 *MS01-036: Function Exposed By Using LDAP over SSL Could Enable Passwords to Be Changed (La función expuesta mediante el uso de LDAP sobre SSL permite cambiar las contraseñas)*

iLO 2 requiere una conexión segura para comunicar con el servicio de directorio. Para ello, se requiere la instalación de la CA de Microsoft®. Consulte el artículo 321051 de la referencia técnica de la base de datos Knowledge Base de Microsoft®: *How to Enable LDAP over SSL with a Third-Party Certification Authority (Cómo habilitar LDAP a través de SSL con una entidad emisora de certificados externa)*.

Instalación de Active Directory en Windows Server 2008

En el esquema predeterminado:

1. Desactive IPV6 e instale Active Directory, DNS y un certificado raíz de CA en Windows Server® 2008.
2. Inicie sesión en iLO y acceda a la página Directory Settings (Valores de configuración de directorio.) Haga clic en **Administration (Administración)>Security (Seguridad)>Directory (Directorio)**.
3. En Directory Settings (Valores de configuración de directorio), introduzca los ajustes correspondientes a su directorio.
4. En Directory User Context (Contexto de usuario del directorio), introduzca los ajustes correspondientes a su directorio.

5. Cree los grupos de administrador para los usuarios de iLO.
6. Haga clic en **Administration (Administración)>Network (Red)>DHCP/DNS** y en Domain Name (Nombre de dominio) y Primary DNS server (Servidor DNS principal), modifique los ajustes correspondientes a su entorno.

En el esquema extendido:

1. Desactive IPV6 e instale Active Directory, DNS y un certificado raíz de CA en Windows Server® 2008.
2. El componente LDAP de iLO requiere .Net Framework 1.1_4322. Instale .Net Framework.
3. Instale el componente LDAP de iLO más reciente (versión sp31581 o posterior.)
4. Amplíe el esquema mediante HP Management Devices Schema Extender.
5. Instale el complemento para componentes LDAP de HP.
6. Cree el dispositivo de HP y la función de HP.
7. Inicie sesión en iLO y acceda a la página Directory Settings (Valores de configuración de directorio.) Haga clic en **Administration (Administración)>Security (Seguridad)>Directory (Directorio)**.
8. Introduzca los valores de configuración del directorio correspondientes a su directorio.
9. Acceda a Directory User Context (Contexto de usuario del directorio.)
10. Haga clic en **Administration (Administración)>Network (Red)>DHCP/DNS** y en Domain Name (Nombre de dominio) y Primary DNS server (Servidor DNS principal), modifique los ajustes correspondientes a su entorno.

El componente LDAP no funciona con una instalación de Windows Server® 2008 core.

Preparación de los servicios de directorio para Active Directory

Para configurar los servicios de directorio con el fin de utilizarlos con los procesadores de gestión de iLO 2:

1. Instalar Active Directory Para obtener más información, consulte el documento *Installing Active Directory (Instalación de Active Directory)*, incluido en el Microsoft® Windows® 2000 Server Resource Kit.
2. Instale Microsoft® Admin Pack (el archivo ADMINPAK.MSI, que se encuentra en el subdirectorio i386 del CD Windows® 2000 Server o Advance Server.) Para ampliar información, consulte el artículo 216999 de la Microsoft® Knowledge Base.
3. En Windows® 2000, el interbloqueo de seguridad que impide que se escriba accidentalmente en el esquema debe desactivarse temporalmente. La utilidad del extensor de esquema puede hacerlo si se está ejecutando el servicio de registro remoto y el usuario dispone de derechos suficientes. También se puede realizar estableciendo `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\ServicesParameters\Schema Update Allowed` del registro en un valor distinto de cero (consulte la sección "Order of Processing When Extending the Schema" (Orden de procesamiento al ampliar el esquema) de *Installation of Schema Extensions (Instalación de ampliaciones de esquema)* del kit de recursos de Windows® 2000 Server) o mediante los pasos siguientes. Este paso no es necesario si utiliza Windows® Server 2003.

NOTA: La modificación incorrecta del Registro puede provocar daños graves en el sistema. HP recomienda crear una copia de seguridad de los datos valiosos del ordenador antes de efectuar cambios en el Registro.

a. Inicie MMC.

b. Instale el completo Active Directory Schema en MMC.

c. Con el botón secundario del ratón, haga clic en **Active Directory Schema (Esquema de Active Directory)** y seleccione **Operations Master (Maestro de operaciones)**.

d. Seleccione **The Schema may be modified on this Domain Controller (El esquema debe modificarse en este controlador de dominio)**.

e. Haga clic en **OK (Aceptar)**.

Es posible que la carpeta Active Directory Schema (Esquema de Active Directory) tenga que ampliarse para que esté disponible la casilla de verificación.

4. Crear un certificado o instalar los servicios de certificado. Este paso es necesario para crear un certificado o instalar los Servicios de Certificate Server, ya que iLO 2 se comunica con Active Directory mediante SSL. Se puede instalar Active Directory antes de los servicios de certificado.

5. Para especificar la emisión de un certificado al servidor que ejecuta Active Directory:

a. Ejecute Microsoft® Management Console en el servidor y añada el complemento de directiva de dominio predeterminado (Directiva de grupo y, a continuación, vaya al objeto de directiva de dominio predeterminado.)

b. Haga clic en **Configuración del equipo>Configuración de Windows>Configuración de seguridad>Directivas de claves públicas**.

c. Haga clic con el botón secundario del ratón en **Automatic Certificate Requests Settings (Configuración de solicitudes de certificado automáticas)** y seleccione **New (Nuevo) >Automatic Certificate Request (Solicitud de certificado automática)**.

d. Utilice el asistente para seleccionar la plantilla de controlador de domino y la autorización de certificado que desee.

6. Descargue el Smart Component, que contiene los instaladores para la ampliación del esquema y los complementos. Smart Component se puede descargar de la página Web de HP (http://www.hp.com/servers/lights-out.)

7. Arranque la aplicación de instalación para la ampliación del esquema, que amplia el esquema de directorio con los objetos HP adecuados.

El instalador del esquema vincula los complementos de Active Directory snap-ins al nuevo esquema. La utilidad de configuración de la instalación de complementos es una secuencia de comandos de instalación MSI de Windows® y se ejecuta donde se admita MSI (Windows® XP, Windows® 2000, Windows® 98.) Sin embargo, algunas partes de la aplicación de ampliación del esquema requieren .NET Framework, que se puede descargar de la página Web de Microsoft® (http://www.microsoft.com.)

Instalación e inicialización de complementos para Active Directory

1. Arranque la aplicación para instalar los complementos e instálelos.
2. Configure el servicio de directorio para que tenga los objetos y relaciones adecuados para la gestión de iLO 2.
   a. Utilice los complementos de gestión de HP para crear los objetos de función iLO 2, Policy, Admin y User.
   b. Utilice los complementos de gestión de HP para generar las asociaciones entre el objeto de iLO 2, el objeto de directiva y el objeto de función.
   c. Dirija el objeto de iLO 2 a los objetos de función Admin y User (las funciones Admin y User señalarán automáticamente al objeto de iLO 2.)

      Si desea obtener más información acerca de objetos de iLO 2, consulte "Objetos de servicios de directorio (Objetos de servicios de directorio en la página 170)".

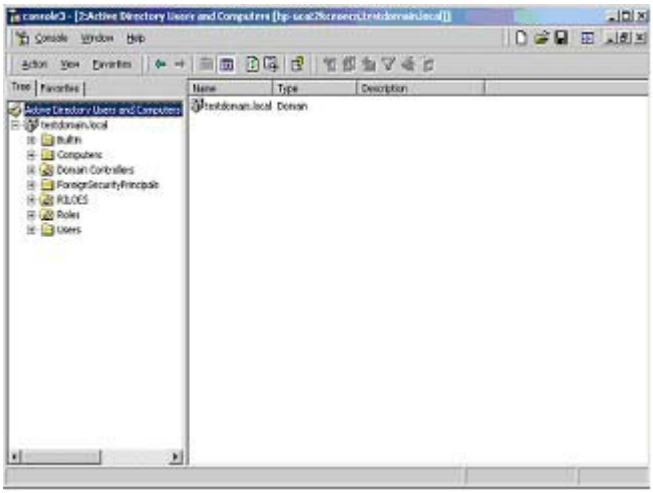
Como mínimo, debe crear:

- Un objeto de función que contendrá uno o varios usuarios y objetos iLO 2.
- Un objeto de iLO 2 correspondiente a cada procesador de gestión de iLO 2 que utilizará el directorio.

Ejemplo: Creación y configuración de objetos de directorio para utilizarlos con iLO 2 en Active Directory

El siguiente ejemplo muestra cómo configurar funciones y dispositivos de HP en el directorio de una empresa con el domino *testdomain.local*, que consiste en dos unidades organizativas, *Roles (Funciones)* y *RILOES*.

Supongamos que una compañía tiene un directorio empresarial que incluye el dominio *testdomain.local*, organizado como se muestra en la siguiente pantalla.



Cree una unidad organizativa, que contendrá los dispositivos Lights-Out gestionados en el dominio. En el presente ejemplo se han creado dos unidades organizativas, llamadas *Roles (Funciones)* y *RILOES*.

1. Utilice los complementos de Usuarios y equipo de Active Directory proporcionados por HP para crear objetos de gestión de Lights-Out en la unidad organizativa *RILOES* para varios dispositivos iLO 2.

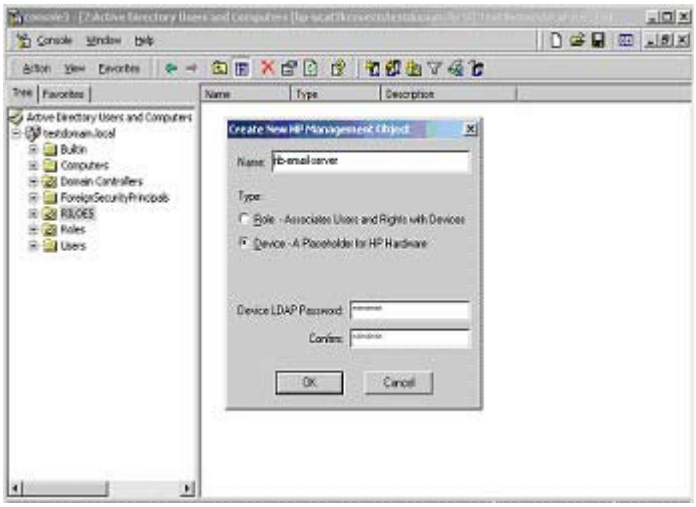
   a. Haga clic con el botón secundario del ratón en la unidad organizativa RILOES que se encuentra en el dominio *testdomain.local* y seleccione **NewHPObject**.

   b. Seleccione **Device (Dispositivo)** en el cuadro de diálogo Create New HP Management Object (Crear nuevo objeto de gestión de HP.)

   c. Escriba un nombre adecuado en el campo Name (Nombre) del cuadro de diálogo. En este ejemplo, se utilizará el nombre DNS de host del dispositivo iLO 2, *rib-email-server*, como el nombre del objeto de gestión de Lights-Out, y el apellido será *RILOEII*.

   Escriba y confirme una contraseña en los campos Device LDAP Password (Contraseña LDAP de dispositivo) y Confirm (Confirmar.) El dispositivo utilizará esta contraseña para autenticarse en el directorio y debe ser única para el dispositivo. Esta contraseña es la que se utilizará en la pantalla Directory Settings (Configuración de directorio) de iLO 2.

   d. Haga clic en **OK (Aceptar)**.



2. Utilice los complementos suministrados por HP, Active Directory Users (Usuarios de Active Directory) y Computers (Ordenadores) para crear objetos de función en la unidad organizativa *Roles (Funciones)* para los distintos dispositivos.

   a. Con el botón secundario del ratón, haga clic en la unidad organizativa Roles (Funciones) y seleccione sucesivamente **New (Nuevo)** y **Object (Objeto)**.

   b. Seleccione **Role (Función)** para el tipo de campo en el cuadro de diálogo Create New HP Management Object (Crear nuevo objeto de gestión de HP.)

   c. Escriba un nombre adecuado en el campo Name (Nombre) del cuadro de diálogo New HP Management Object (Nuevo objeto de gestión de HP.) En el presente ejemplo, la función incluirá a usuarios de confianza para la gestión del servidor remoto y llevará el nombre de *remoteAdmins*. Haga clic en **OK (Aceptar)**.

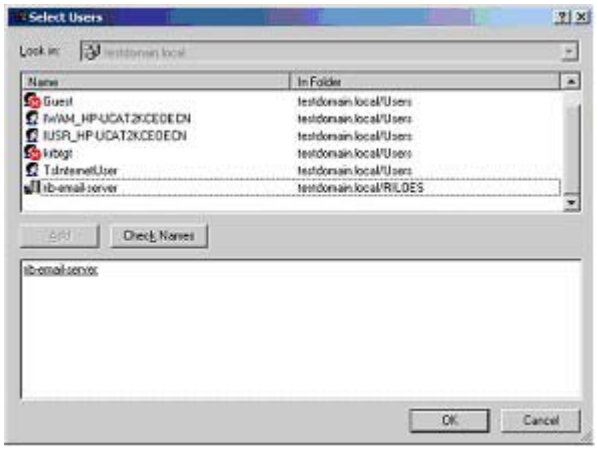
   d. Repita el proceso para crear una función para los monitores de servidor remotos, llamada *remoteMonitors*.

3. Utilice los complementos suministrados por HP, Active Directory Users (Usuarios de Active Directory) y Computers (Ordenadores) para asignar permisos de función y asociar las funciones a distintos usuarios y dispositivos.

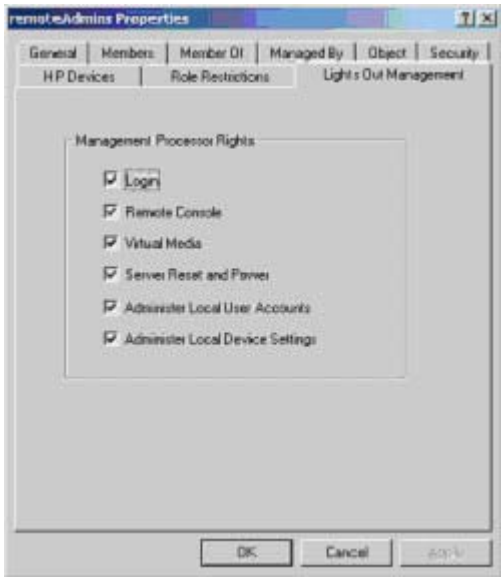
   a. Con el botón secundario del ratón, haga clic en la función **remoteAdmins**, que se encuentra en la unidad organizativa Roles (Funciones) del dominio *testdomain.local*, y selecciones **Properties (Propiedades)**.

   b. Seleccione la ficha **HP Devices (Dispositivos HP)** y, a continuación, **Add (Añadir)**.

   c. En el cuadro de diálogo Select Users (Elegir usuarios), seleccione el objeto de gestión Lights-Out creado en el paso 2, *rib-email-server*, en la carpeta testdomain.local/RILOES. Cierre el cuadro de diálogo haciendo clic en **OK (Aceptar)**, y a continuación haga clic en **Apply (Aplicar)** para guardar la lista.



   d. Incluya usuarios en la función. Haga clic en la ficha **Members (Miembros)** y añada usuarios mediante el botón Add (Añadir) y el cuadro de diálogo Select Users (Seleccionar usuarios.) Los dispositivos y usuarios ya están asociados a la función.



4. Utilice la ficha Lights Out Management (Gestión de Lights Out) para establecer los derechos de la función. Todos los usuarios y grupos de una función tendrán los derechos asignados a la misma en todos los dispositivos iLO 2 gestionados por dicha función. En este ejemplo, a los usuarios de la función *remoteAdmins* se les concederá acceso completo a las funciones de iLO 2. Seleccione

los cuadros de la derecha, y a continuación haga clic en **Apply (Aplicar)**. Haga clic en **OK (Aceptar)** para cerrar la hoja de propiedades.

5. Siguiendo el mismo procedimiento del paso 4, modifique las propiedades de la función *remoteMonitors*, añada el dispositivo *rib-email-server* a la lista Managed Devices (Dispositivos gestionados) en la ficha HP Devices (Dispositivos HP) y añada usuarios a la función *remoteMonitors* mediante la ficha Members (Miembros.) A continuación, en la ficha Lights Out Management (Gestión de Lights Out), seleccione la casilla situada junto a Login (Inicio de sesión.) Haga clic en **Apply (Aplicar)** y **OK (Aceptar)**. Los miembros de la función *remoteMonitors* podrán autenticarse y ver el estado del servidor.

Los derechos de usuario para cualquier iLO 2 se calculan como la suma de todos los derechos asignados por todas las funciones de las que el usuario es miembro y en las que iLO 2 es un dispositivo gestionado. Como muestran los anteriores ejemplos, los usuarios que pertenezcan tanto a la función *remoteAdmins* como a *remoteMonitors*, tendrán todos los permisos, puesto que la función *remoteAdmins* los tiene asignados todos.

Para configurar iLO 2 y asociarla a un objeto de gestión de Lights-Out utilizado en este ejemplo, utilice valores de configuración similares a los siguientes en la pantalla Directory Settings (Configuración de directorio.)

```
RIB Object DN = cn=rib-email-server,ou=RILOES,dc=testdomain,dc=local
Directory User Context 1 = cn=Users,dc=testdomain,dc=local
```

Por ejemplo, para acceder, el usuario *Mel Moore*, con ID único *MooreM*, que se encuentra situado en la unidad organizativa de usuarios del dominio *testdomain.local*, que es también miembro de una de las funciones *remoteAdmins* o *remoteMonitors*, estará autorizado a iniciar sesión en iLO 2. Mel deberá introducir `testdomain\moorem,`, `moorem@testdomain.local,` o `Mel Moore,` en el campo Login Name (Nombre de inicio de sesión) de la pantalla de inicio de sesión de iLO 2, y utilizará la contraseña de Active Directory en el campo Password (Contraseña) de la pantalla.

Objetos de servicios de directorio

Una de las claves de la gestión basada en directorios es precisamente la presencia virtual de los dispositivos gestionados en el servicio de directorio. Esta presencia virtual permite al administrador establecer relaciones entre el dispositivo gestionado y los usuarios o grupos de usuarios ya incluidos en el servicio de directorio. La gestión de usuario de iLO 2 requiere tres objetos básicos en el servicio de directorio:

- Objeto de gestión Lights-Out
- Objeto de función
- Objetos de usuario

Cada objeto representa un dispositivo, un usuario o una relación que se necesita para la gestión basada en directorios.

NOTA: Después de instalar los complementos, es necesario reiniciar ConsoleOne y MMC para poder ver los nuevos elementos.

Tras instalar el complemento, se pueden crear los objetos y funciones de iLO 2 en el directorio. Utilizando la herramienta Users and Computers (Usuarios y ordenadores), proceda como se describe a continuación:

- Crear los objetos de iLO 2 y de función.
- Incluir usuarios en la función.
- Establecer los permisos y restricciones de los objetos de función.

Complementos de Active Directory

En las secciones siguientes se describen las opciones de gestión adicionales que están disponibles en Usuarios y equipos de Active Directory después de haber instalado los complementos de HP.

HP Devices

La ficha HP Devices (Dispositivos HP) se utiliza para añadir los dispositivos HP que se van a gestionar en una función. Al hacer clic en **Add (Añadir)** se puede buscar un dispositivo HP específico y añadirlo a la lista de dispositivos miembros. Al hacer clic en **Remove (Quitar)** se puede buscar un dispositivo HP específico y quitarlo de la lista de dispositivos miembros.

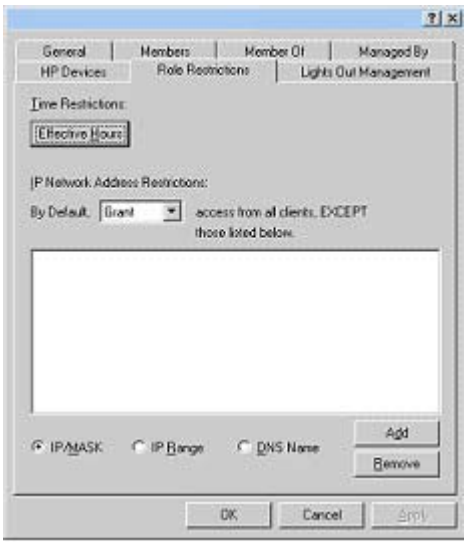
Members

Después de crear los objetos de usuario, la ficha Members (Miembros) permite gestionar los usuarios de la función. Al hacer clic en **Add (Añadir)** se puede buscar el usuario específico que se desea añadir. Al resaltar un usuario existente y hacer clic en **Remove (Quitar)** se quita el usuario de la lista de miembros válidos.

Restricciones de función de Active Directory

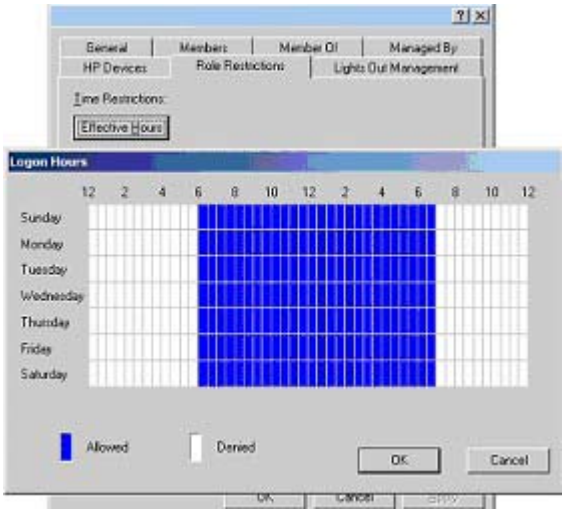
La ficha Role Restrictions (Restricciones de función) permite establecer restricciones de inicio de sesión para la función. Estas restricciones incluyen:

- Restricciones de tiempo
- Restricciones de dirección de red IP
  - Máscara IP
  - Rango IP
  - Nombre DNS



Restricciones de tiempo

Para gestionar las horas disponibles en las que los miembros de la función pueden iniciar sesión, haga clic en **Effective Hours (Horas efectivas)** de la ficha Role Restrictions (Restricciones de función.) En la ventana emergente Logon Hours (Horas de inicio de sesión), puede seleccionar las horas disponibles para iniciar sesión por cada día de la semana en incrementos de media hora. Puede cambiar un solo cuadro haciendo clic en él, o puede cambiar una sección de cuadros haciendo clic, manteniendo pulsado el botón del ratón, arrastrando el cursor por los cuadros que desea cambiar y soltando el botón del ratón. La configuración predeterminada permite el acceso a cualquier hora.



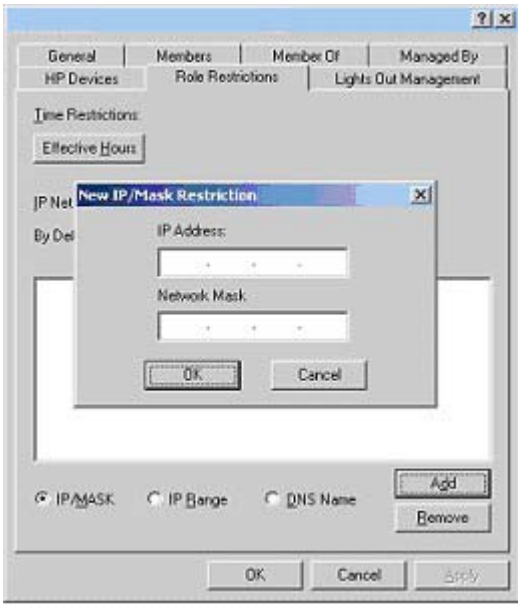
Dirección IP de cliente obligatoria o acceso al nombre DNS

Se pueden autorizar o denegar accesos a través de una dirección IP, un rango de direcciones IP o un nombre DNS.

1. En el menú desplegable By Default (Predeterminado), seleccione **Grant (Conceder)** o **Deny (Denegar)** para conceder o denegar el acceso desde todas las direcciones excepto las direcciones IP, los rangos de direcciones IP y los nombres DNS especificados.
2. Seleccione las direcciones que desea añadir, seleccione el tipo de restricción y haga clic en **Add (Añadir)**.
3. En la ventana emergente de nueva restricción, escriba la información y haga clic en **OK (Aceptar)**. Se muestra la ventana emergente de nueva restricción.

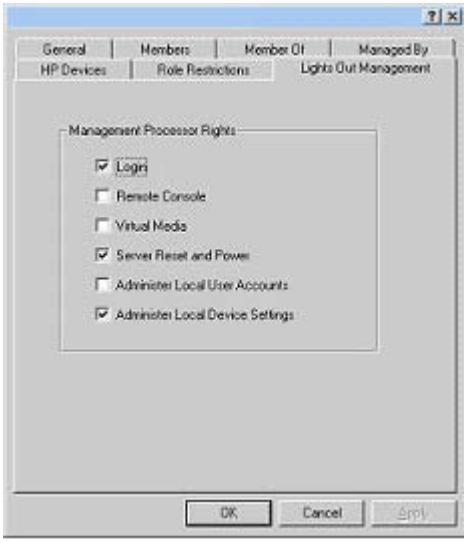
   La opción DNS Name (Nombre DNS) permite restringir el acceso en función de un único nombre DNS o un subdominio, escrito con el formato host.compañía.com o *.dominio.compañía.com.
4. Haga clic en **OK (Aceptar)** para guardar los cambios.

Para eliminar cualquiera de las entradas de la lista, resáltela colocando el cursor encima y haga clic en **Remove (Quitar)**.



Gestión de Lights-Out de Active Directory

Después de crear una función, hay que establecer los permisos correspondientes. Los objetos de usuario y de grupos de usuarios ya pueden ser miembros de la función, otorgando a los usuarios los mismos derechos establecidos para la función. Los derechos se gestionan en la ficha Lights Out Management (Gestión de Lights Out.)



Los derechos disponibles son:

- **Login (Inicio de sesión)**: esta opción permite controlar si desea que los usuarios pueden iniciar sesión en los dispositivos asociados.
- **Remote Console (Consola remota)**: esta opción permite al usuario acceder a la consola remota.
- **Virtual Media (Soportes virtuales)**: esta opción permite el acceso de usuario a los soportes virtuales de iLO 2.

- **Server Reset and Power (Reinicio y alimentación de servidor)**: esta opción permite el acceso del usuario al botón Virtual Power (Alimentación virtual) de iLO 2 para reiniciar el servidor o apagarlo de forma remota.
- **Administer Local User Accounts (Administrar cuentas de usuario local)**: esta opción permite al usuario administrar cuentas. El usuario puede modificar la configuración de su propia cuenta y la de otros usuarios, y añadir y borrar usuarios.
- **Administer Local Device Settings (Administrar valores de configuración de dispositivos locales)**: esta opción permite al usuario configurar los valores de los procesadores de gestión de iLO 2. Estos valores de configuración incluyen las opciones disponibles en las pantallas Global Settings (Configuración global), Network Settings (Configuración de red), SNMP Settings (Configuración de SNMP) y Directory Settings (Configuración de directorio) del explorador Web de iLO 2.

Servicios de directorio para eDirectory

En las secciones siguientes se recogen los requisitos previos de instalación, la preparación y un ejemplo funcional de los servicios de directorio para eDirectory.

Requisitos previos para instalar eDirectory

Los servicios de directorio para iLO 2 utilizan LDAP a través de SSL para comunicarse con los servidores de directorio. El software de iLO 2 está diseñado para instalarse en un árbol de eDirectory versión 8.6.1 (y posteriores.) HP no recomienda instalar este producto si se dispone de servidores eDirectory con una versión anterior a eDirectory 8.6.1. Antes de instalar los complementos y las ampliaciones del esquema de eDirectory, consulte y tenga a su disposición los siguientes documentos de información técnica, que se pueden obtener del servicio de asistencia de Novell (http://support.novell.com.)

La instalación de los servicios de directorio para iLO 2 requiere la ampliación del esquema de eDirectory. La extensión del esquema debe realizarla un administrador.

- TID10066591 *Novell eDirectory 8.6 NDS compatibility (Compatibilidad de Novell eDirectory 8.6 NDS)*
- TID10057565 *Unknown objects in a mixed environment (Objetos desconocidos en un entorno mixto)*
- TID10059954 *How to test whether LDAP is working correctly (Cómo comprobar que LDAP está funcionando correctamente)*
- TID10023209 *How to configure LDAP for SSL (secure) connections (Cómo configurar LDAP para conexiones SSL seguras)*
- TID10075010 *How to test LDAP authentication (Cómo probar la autenticación LDAP)*

Instalación e inicialización de complementos para eDirectory

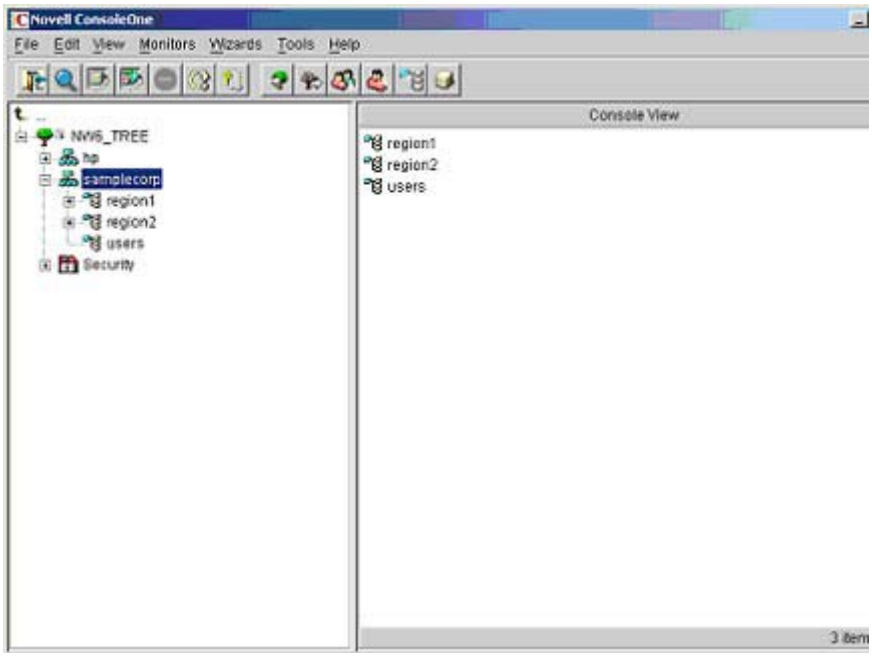
Consulte "Instalación e inicialización de complementos (Instalación e inicialización de complementos para Active Directory en la página 167)" para obtener instrucciones detalladas acerca del uso de la aplicación de instalación de complementos.

NOTA: Después de instalar los complementos, es necesario reiniciar ConsoleOne y MMC para poder ver los nuevos elementos.

Ejemplo: Creación y configuración de objetos de directorio para utilizarlos con dispositivos LOM en eDirectory

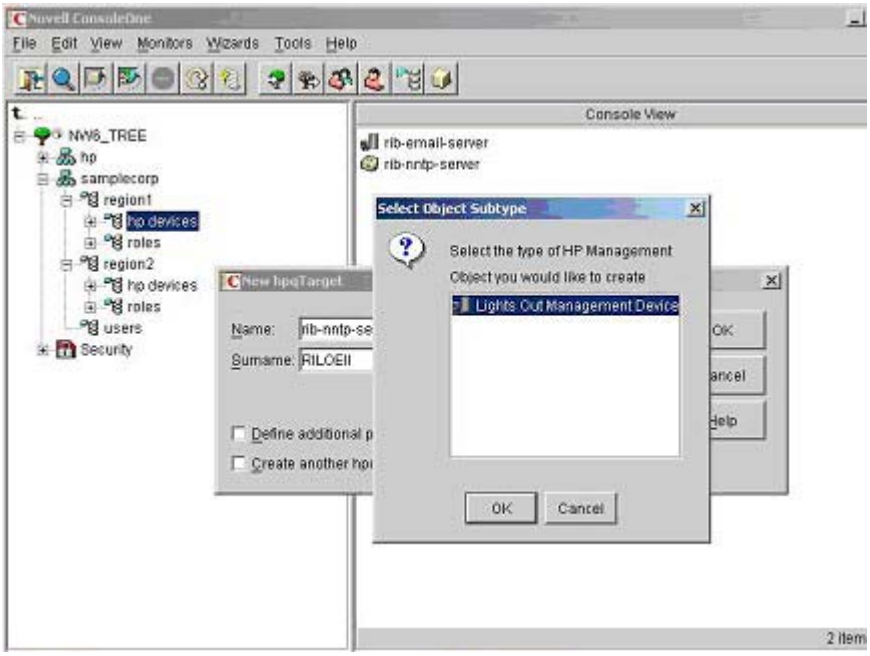
El siguiente ejemplo muestra cómo configurar funciones y dispositivos de HP en el directorio de una empresa llamada *samplecorp*, con dos ámbitos llamados *region1* y *region2*.

Supongamos que *samplecorp* tiene un directorio de empresa organizado como muestra la siguiente pantalla.



1. Cree unidades organizativas en cada región. Cada unidad organizativa debe contener los dispositivos y funciones LOM específicos para tal región. En el presente ejemplo, en cada ámbito ("*region1*" y "*region2*") se han creado dos unidades organizativas, llamadas "*roles*" (funciones) y "*hp devices*" (dispositivos HP.)
2. Cree objetos LOM en las unidades organizativas de *hp devices (dispositivos HP)* para distintos dispositivos iLO 2 mediante la herramienta de complementos ConsoleOne que proporciona HP.
   a. Con el botón secundario del ratón, haga clic en la unidad organizativa **hp devices** que se encuentra en el dominio *region1*, y seleccione sucesivamente **New (Nuevo)**>**Object (Objeto)**.
   b. Seleccione **hpq Target** en la lista de clases y haga clic en **OK (Aceptar)**.
   c. Introduzca el nombre y apellido adecuados en la página **New hpqTarget**. En este ejemplo, se utilizará el nombre DNS de host del dispositivo iLO 2, *rib-email-server*, como el nombre del objeto LOM, y el apellido será *RILOEII*. Haga clic en **OK (Aceptar)**. Aparecerá la página Select Object Subtype (Seleccionar subtipo de objeto.)
   d. Seleccione **Lights Out Management Device (Dispositivo de gestión de Lights Out)** y haga clic en **OK (Aceptar)**.

e. Repita el proceso para varios dispositivos iLO 2 más que dispongan de los nombres DNS "*rib-nntp-server"* y "*rib-file-server-users1"* en *hp devices (Dispositivos HP)* debajo de *region1* y "*rib-file-server-users2"* y "*rib-app-server"* en *hp devices (Dispositivos HP)* debajo de *region2*.



3. Cree objetos Role (Función) de HP en la unidad organizativa *roles* mediante la herramienta de complementos ConsoleOne que proporciona HP.

   a. Con el botón secundario del ratón, haga clic en la unidad organizativa *roles* que se encuentra en el dominio *region2* y seleccione **New (Nuevo)**>**Object (Objeto)**.

   b. Seleccione **hpqRole** en la lista de clases y haga clic en **OK (Aceptar)**.

   c. Introduzca un nombre adecuado en la página **New hpqRole**. En el presente ejemplo, la función incluirá a usuarios de confianza para la gestión del servidor remoto y llevará el nombre de "*remoteAdmins"*. Haga clic en **OK (Aceptar)**. Aparecerá la página Select Object Subtype (Seleccionar subtipo de objeto.)

   d. Como esta función puede gestionar los permisos para los dispositivos de Lights-Out Management, seleccione en la lista **Lights Out Management Devices (Dispositivos de gestión de Lights Out)** y, a continuación, haga clic en **OK (Aceptar)**.

   e. Repita el proceso para crear una función para los monitores de servidor remotos, llamada "*remoteMonitors*", en *roles* en el dominio *region1*, "*remoteAdmins*" y una función "*remoteMonitors*" en *roles* en la unidad organizativa *region2*.

4. Asigne los derechos a la función y asocie las funciones a distintos usuarios y dispositivos mediante la herramienta de complementos ConsoleOne que proporciona HP.

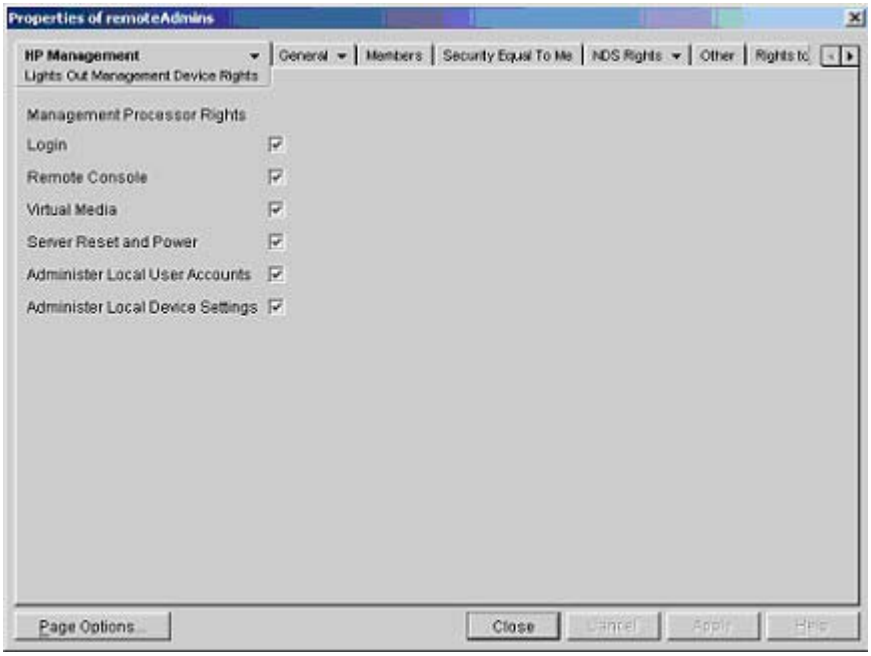
   a. Con el botón secundario del ratón, haga clic en la función **remoteAdmins** que se encuentra en la unidad organizativa *roles* de la unidad organizativa *region1*, y seleccione **Properties (Propiedades)**.

   b. Seleccione la ficha **Role Managed Devices (Dispositivos gestionados por función)** de la opción HP Management (Gestión HP) y haga clic en **Add (Añadir)**.

c. Desde la página Select Objects (Seleccionar objetos), busque la unidad organizativa *hp devices* dentro de la unidad organizativa *region1*. Seleccione los tres objetos LOM creados en el paso 2. Haga clic en **OK**>**Apply (Aceptar>Aplicar)**.

d. Haga clic en la ficha **Members (Miembros)** y añada usuarios a la función haciendo clic en el botón **Add (Añadir)** en la página Select Object (Seleccionar objeto.) Los dispositivos y usuarios ya están asociados a la función.

e. Establezca los derechos de la función mediante la opción Lights Out Management Device Rights (Derechos de dispositivos de gestión de Lights Out) en la ficha HP Management (Gestión de HP.) Todos los usuarios de una función tienen los derechos asignados a la misma en todos los dispositivos iLO 2 gestionados por dicha función. En este ejemplo, a los usuarios de la función *remoteAdmins* se les concederá acceso completo a las funciones de iLO 2. Seleccione los cuadros de diálogo de la derecha, y a continuación haga clic en **Apply (Aplicar)**. Para cerrar la hoja de propiedades, haga clic en **Close (Cerrar)**.



5. Aplicando el proceso explicado en el paso 4, cambie las propiedades de la función *remoteMonitors*:

a. Añada los tres dispositivos iLO 2 de *hp devices* situados en la unidad organizativa *region1* a la lista **Managed Devices (Dispositivos gestionados)** de la opción Role Managed Devices (Dispositivos gestionados por función) de la ficha HP Management (Gestión de HP.)

b. Añada usuarios a la función *remoteMonitors* utilizando la ficha Members (Miembros.)

c. Seleccione la casilla de verificación Login (Inicio de sesión) y haga clic en **Apply (Aplicar) >Close (Cerrar)**. Mediante la opción Lights Out Management Device Rights (Derechos de dispositivos de gestión de Lights Out) de la ficha HP Management (Gestión de HP), los miembros de la función *remoteMonitors* podrán autenticarse y ver el estado del servidor.

Los derechos de usuario para cualquier dispositivo LOM se calcula como la suma de todos los derechos asignados por todas las funciones del usuario y en las que LOM es un dispositivo gestionado. Como muestran los anteriores ejemplos, los usuarios que pertenezcan tanto a la función *remoteAdmins* como a *remoteMonitors*, tendrán todos los permisos, puesto que la función *remoteAdmins* los tiene asignados todos.

Para configurar un dispositivo LOM y asociarlo con un objeto LOM utilizado en este ejemplo, utilice valores de configuración similares a los que se muestran a continuación en la página Directory Settings (Configuración de directorio.)

NOTA: Para separar cada componente de los nombres LDAP se utilizan comas, y no puntos.

```
RIB Object DN = cn=rib-email-server,ou=hp devices,ou=region1,o=samplecorp
Directory User Context 1 = ou=users,o=samplecorp
```

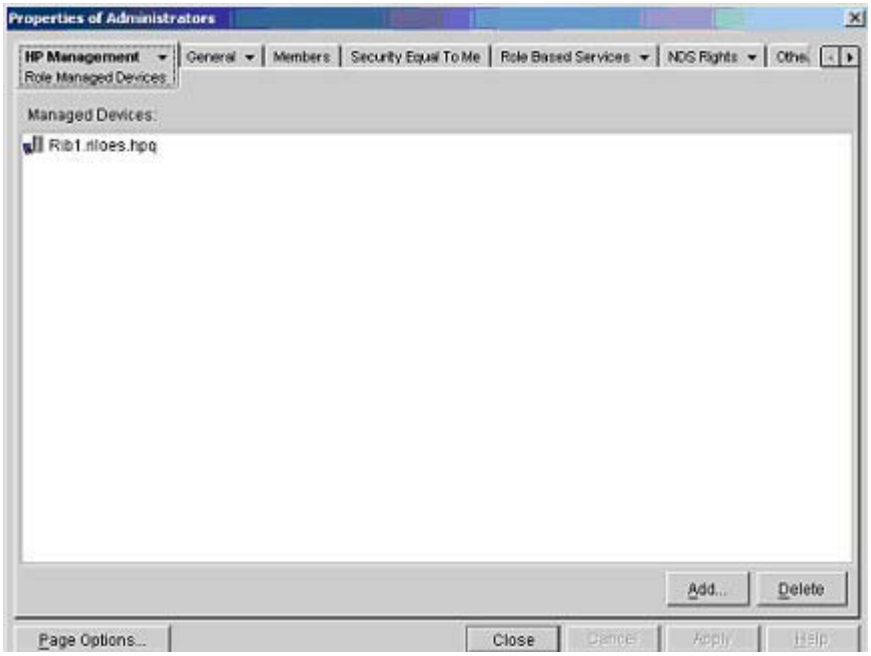
Por ejemplo, el usuario *CSmith*, situado en la unidad organizativa *users* de la organización *samplecorp*, que también es miembro de una de las funciones *remoteAdmins* o *remoteMonitors* podrá iniciar sesión en iLO 2. El usuario introduce `csmith` (no distingue entre mayúsculas y minúsculas) en el campo Login Name (Nombre de inicio de sesión) de la pantalla de inicio de sesión de iLO 2 y utiliza la contraseña de eDirectory en el campo Password (Contraseña) de dicha pantalla para acceder.

Objetos de los servicios de directorio para eDirectory

Los objetos de servicios de directorio permiten virtualizar los dispositivos gestionados así como las relaciones entre el dispositivo gestionado y el usuario o los grupos que ya contiene el servicio de directorio.

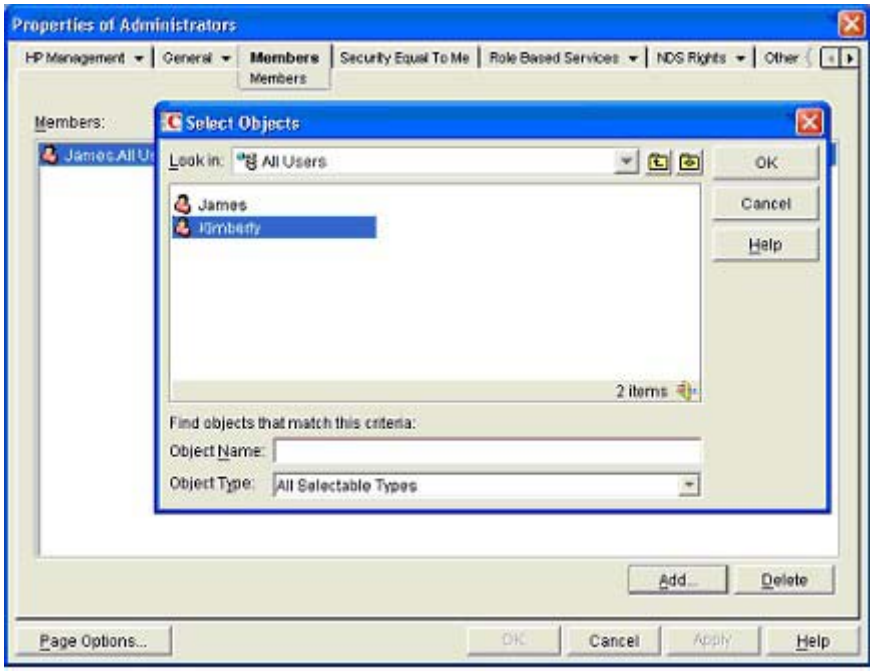
Dispositivos gestionados por función

La subficha Role Managed Devices (Dispositivos gestionados por función) en la ficha HP Management (Gestión de HP) se utiliza para añadir los dispositivos HP que se gestionarán en una función. Si hace clic en **Add (Añadir)** podrá buscar el dispositivo de HP que le interese y sumarlo a los demás dispositivos gestionados.



Members

Después de crear los objetos de usuario, la ficha Members (Miembros) permite gestionar los usuarios de la función. Al hacer clic en **Add (Añadir)** se puede buscar el usuario específico que se desea añadir. Al resaltar un usuario existente y hacer clic en **Delete (Borrar)** se quita el usuario de la lista de miembros válidos.

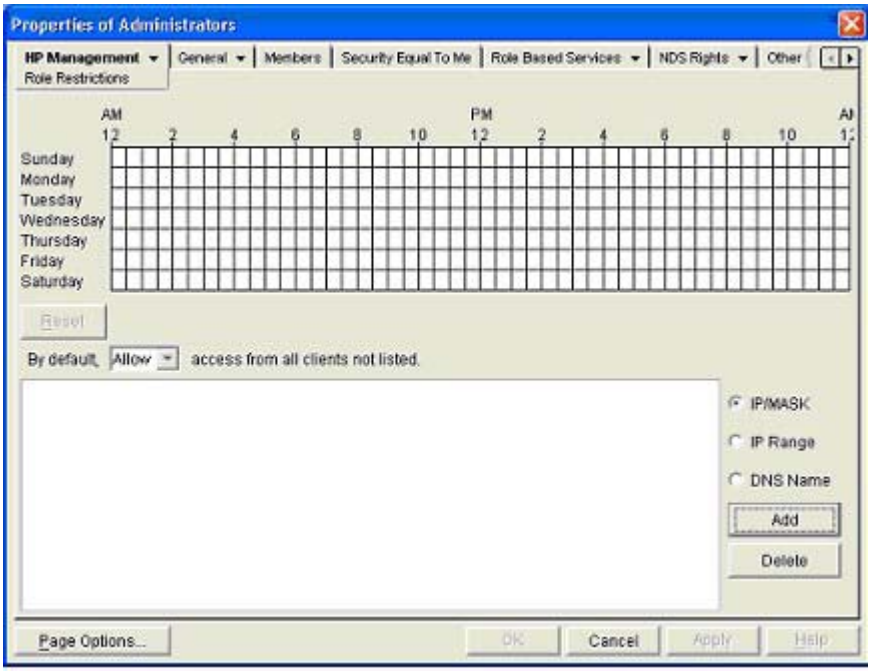


Restricciones de función de eDirectory

La ficha Role Restrictions (Restricciones de función) permite establecer restricciones de inicio de sesión para la función. Estas restricciones incluyen:

- Restricciones de tiempo
- Restricciones de dirección de red IP
  - Máscara IP
  - Rango IP

- Nombre DNS



Restricciones de tiempo

Puede gestionar las horas disponibles en las que los miembros de la función pueden iniciar sesión utilizando la cuadrícula de horas mostrada en la subficha Role Restrictions (Restricciones de función.) De este modo podrá seleccionar el horario de disponibilidad para cada día de la semana, en bloques de media hora. Puede cambiar un único módulo horario haciendo clic encima de él, o varios módulos consecutivos haciendo clic y, sin soltar el botón, arrastrando el ratón por todos los módulos que desea cambiar; cuando los haya seleccionado todos, deje de presionar el botón. La configuración predeterminada permite el acceso a cualquier hora.

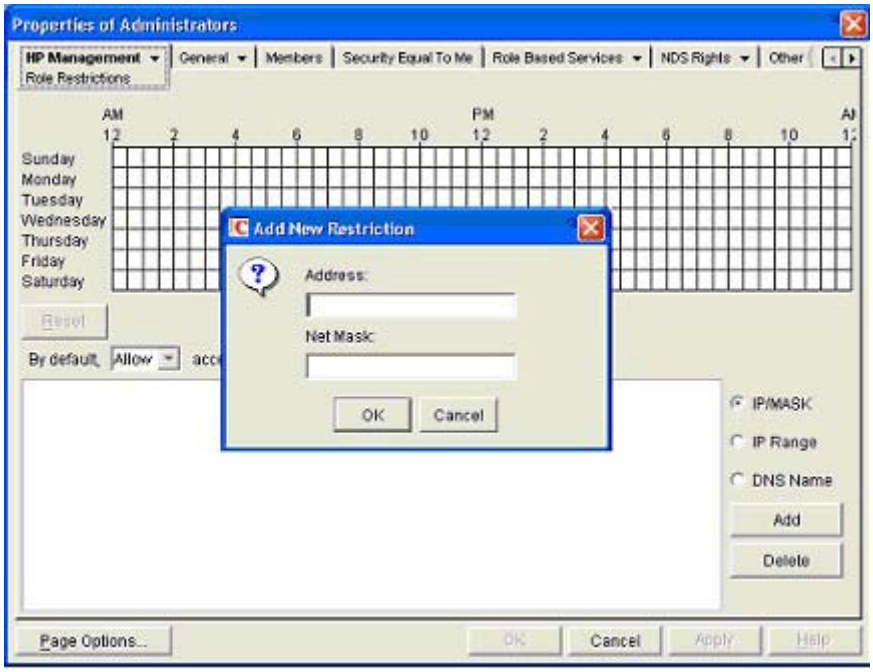
Dirección IP de cliente obligatoria o acceso al nombre DNS

Se pueden autorizar o denegar accesos a través de una dirección IP, un rango de direcciones IP o un nombre DNS.

1. En el menú desplegable By Default (Predeterminado), seleccione **Allow (Permitir)** o **Deny (Denegar)** para permitir o denegar el acceso desde todas las direcciones excepto las direcciones IP, los rangos de direcciones IP y los nombres DNS especificados.
2. Seleccione las direcciones que desea añadir, seleccione el tipo de restricción y haga clic en **Add (Añadir)**.
3. En la ventana emergente Add New Restriction (Añadir nueva restricción), escriba la información y haga clic en **OK (Aceptar)**. Se muestra la ventana emergente Add New Restriction (Añadir nueva restricción) para la opción IP/Mask (IP/Máscara.)

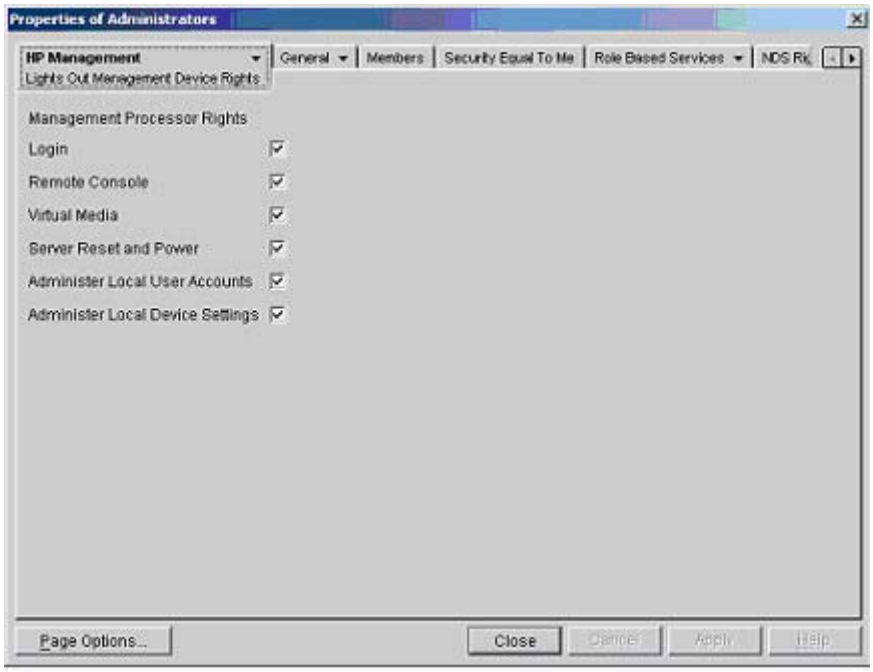
   La opción DNS Name (Nombre DNS) permite restringir el acceso en función de un único nombre DNS o un subdominio, escrito con el formato host.compañía.com o *.dominio.compañía.com.
4. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Para eliminar cualquiera de las entradas, resáltela colocando el cursor en el campo y haga clic en **Delete (Borrar)**.



Gestión de eDirectory Lights-Out

Después de crear una función, hay que establecer los permisos correspondientes. Los objetos de usuario y de grupos de usuarios ya pueden ser miembros de la función, otorgando a los usuarios los mismos derechos establecidos para la función. Los derechos se gestionan en la subficha Lights Out Management Device Rights (Derechos de dispositivos de gestión de Lights Out) de la ficha HP Management (Gestión de HP.)



Los derechos disponibles son:

- Login (Inicio de sesión): esta opción controla si los usuarios pueden iniciar sesión en los dispositivos asociados.

  El acceso de inicio de sesión puede utilizarse a fin de crear un usuario que sea miembro del servicio técnico y reciba avisos de iLO 2, pero que no tenga acceso de inicio de sesión a iLO 2.

- Remote Console (Consola remota): esta opción permite al usuario acceder a la consola remota.
- Virtual Media (Medios virtuales): esta opción permite al usuario acceder al disquete virtual de iLO 2 y a las funciones de medios virtuales.
- Server Reset and Power (Reinicio y apagado del servidor): esta opción permite al usuario reiniciar o apagar el servidor de forma remota.
- Administer Local User Accounts (Administrar cuentas de usuario locales): esta opción permite al usuario administrar cuentas. El usuario puede modificar la configuración de su propia cuenta y la de otros usuarios, y añadir y borrar usuarios.
- Administer Local Device Settings (Administrar configuración de dispositivos locales): esta opción permite al usuario configurar los parámetros de iLO 2. Estos valores de configuración incluyen las opciones disponibles en las pantallas Global Settings (Configuración global), Network Settings (Configuración de red), SNMP Settings (Configuración de SNMP) y Directory Settings (Configuración de directorio) del explorador de iLO 2.

Inicio de sesión del usuario mediante servicios de directorio

El campo Login Name (Nombre de inicio de sesión) en la página de inicio de iLO 2 acepta todo lo que se indica a continuación:

- usuarios de directorio
- nombres LDAP completos

  Ejemplo: CN=John Smith,CN=Users,DC=HP,DC=COM, o @HP.com

NOTA: La forma abreviada del nombre de inicio no indica al directorio a qué dominio se desea acceder. Es necesario indicar el nombre del dominio o utilizar el nombre LDAP de la cuenta completo.

- DOMINIO\nombre de usuario (sólo Active Directory)

  Ejemplo: HP\jsmith

- nombreusuario@dominio (sólo Active Directory)

  Ejemplo: jsmith@hp.com

NOTA: Los usuarios de directorio especificados mediante el formato que se puede buscar @ se pueden encontrar en uno de los tres contextos que se pueden buscar, configurados en Directory Settings (Configuración de directorio.)

- Forma del nombre de usuario:

  Ejemplo: John Smith

NOTA: Los usuarios de directorio especificados mediante el formato de nombre de usuario se pueden encontrar en uno de los tres contextos que se pueden buscar, configurados en Directory Settings (Configuración de directorio.)

- Usuarios locales: ID de inicio de sesión

NOTA: En la página de inicio de iLO 2, la longitud máxima del nombre de inicio de sesión es de 39 caracteres para los usuarios locales. Para los usuarios de los servicios de directorio, la longitud máxima del nombre de inicio de sesión es de 256 caracteres.

6 Gestión remota habilitada por directorio

En esta sección:

Introducción a la gestión remota habilitada por directorio

Esta sección está dedicada a los administradores que conocen los servicios de directorio y el producto iLO 2 y que desean utilizar la opción de integración de directorios con esquema de HP para iLO 2. Debe estar familiarizado con la sección “Servicios de directorio" (Servicios de directorio en la página 150), además de saber crear y comprender los ejemplos.

La gestión remota habilitada por directorio permite:

- Crear objetos de gestión de Lights-Out

  Debe crear un objeto de dispositivo LOM para representar cada dispositivo que el servicio de directorio va a usar para autenticar y autorizar a los usuarios. Consulte la sección "Servicios de directorio (Servicios de directorio en la página 150)" para obtener información adicional acerca de la creación de objetos de dispositivo LOM para Active Directory (Servicios de directorio para Active Directory en la página 163) y eDirectory (Servicios de directorio para eDirectory en la página 175.) En general, podrá usar los complementos de HP proporcionados para crear objetos. Se recomienda asignar nombres significativos a los objetos de dispositivo LOM, como la dirección de red del dispositivo, el nombre DNS, el nombre del servidor host o el número de serie.

- Configurar los dispositivos de gestión de Lights-Out

  Cada dispositivo LOM que usa el servicio de directorio para autenticar y autorizar a los usuarios debe configurarse con los valores de configuración de directorio apropiados. Consulte la sección "Configuración de los valores de directorio (Configuración de los valores de directorio en la página 52)" para obtener más información acerca de los valores específicos del directorio. En general, podrá configurar cada dispositivo con los valores apropiados para la dirección del servidor de directorios, el nombre completo de objetos LOM y contextos de usuarios. La dirección de servidor es la dirección IP o el nombre DNS de un servidor de directorios local o, para mayor redundancia, un nombre DNS de host múltiple.

Creación de funciones para seguir la estructura organizativa

A menudo, los administradores dentro de una organización forman parte de una jerarquía en la que los administradores subordinados deben asignar derechos independientemente de los administradores de mayor rango. En este caso, resulta útil tener una función que representa los derechos asignados por los administradores de nivel superior y permitir que los administradores subordinados creen y gestionen sus propias funciones.

Uso de grupos existentes

Numerosas organizaciones tienen a sus usuarios y administradores organizados en grupos. En muchos casos, se recomienda usar los grupos existentes y asociarlos a uno o varios objetos de función de gestión de Lights-Out. Cuando los dispositivos están asociados a los objetos de función, el administrador controla el acceso a los dispositivos de Lights-Out asociados a la función añadiendo o eliminando miembros de los grupos.

Cuando se usa Microsoft® Active Directory, es posible ubicar un grupo con otro o grupos anidados. Los objetos de función se consideran grupos y pueden incluir directamente otros grupos. Añada el grupo anidado existente directamente a la función y asigne los derechos y restricciones apropiados. Se pueden añadir nuevos usuarios al grupo existente o a la función.

Novell eDirectory no permite grupos anidados. En eDirectory, cualquier usuario que pueda leer una función se considera miembro de dicha función. Al añadir un grupo, una unidad organizativa u organización existente a una función, añada el objeto como un elemento de confianza de la función. Todos los miembros del objeto se consideran miembros de la función. Se pueden añadir nuevos usuarios al objeto existente o a la función.

Cuando se usan asignaciones de derechos de administración o de directorio para ampliar los miembros de la función, los usuarios deberán poder leer el objeto LOM que representa al dispositivo LOM. Algunos entornos requieren que los elementos de confianza de una función sean también los elementos de confianza del objeto LOM para poder autenticar correctamente a los usuarios.

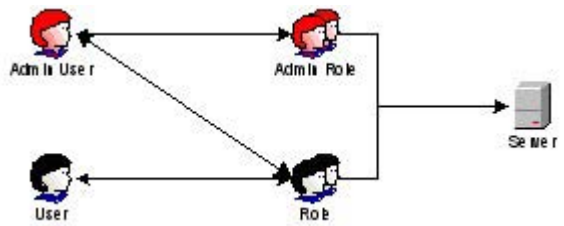
Uso de varias funciones

La mayoría de las implementaciones no requieren que el mismo usuario esté presente en las múltiples funciones que gestionan el mismo dispositivo. No obstante, estas configuraciones pueden resultar útiles a la hora de crear complejas relaciones de derechos. Al crear relaciones de varias funciones, los usuarios reciben todos los derechos asignados por cada función aplicable. Las funciones sólo pueden conceder derechos; nunca pueden revocarlos. Si una función concede un derecho a un usuario, éste tiene el derecho, incluso si el usuario está en otra función que no conceda dicho derecho.

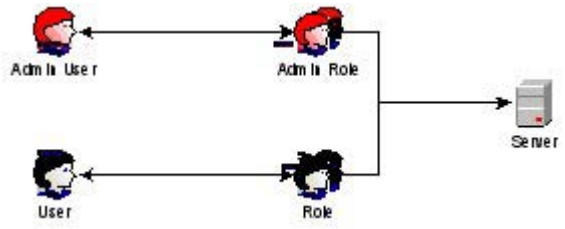
Normalmente, un administrador de directorios crea una función básica con el número mínimo de derechos asignados y, a continuación, crea funciones adicionales para añadir más derechos. Estos derechos adicionales se añaden en casos específicos o a un conjunto específico de usuarios de la función básica.

Por ejemplo, una organización puede tener dos tipos de usuarios, administradores del dispositivo LOM o servidor host y usuarios del dispositivo LOM. En esta situación, tiene sentido crear dos funciones, una para los administradores y otra para los usuarios. Algunos de los dispositivos que incluyen ambas funciones son idénticos pero los derechos que conceden son distintos. A veces resulta útil conceder derechos genéricos a la menor función e incluir a los administradores LOM en dicha función, así como la función administrativa.

Un usuario admin obtiene el derecho de inicio de sesión del grupo de usuarios normales. Los derechos más avanzados se asignan a través de la función Admin, que asigna derechos adicionales: reinicio del servidor y consola remota.

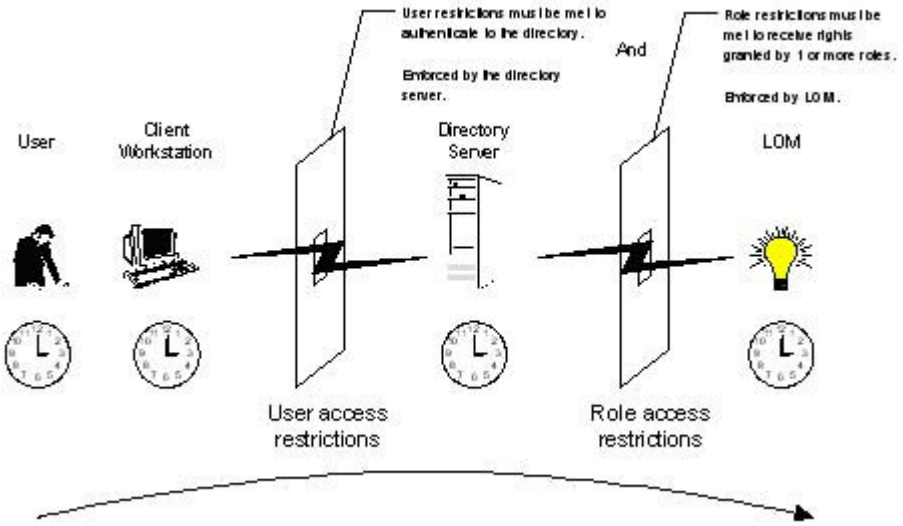


La función Admin asigna todos los derechos administrativos: reinicio del servidor, consola remota e inicio de sesión.



Cómo se imponen las restricciones de inicio de sesión en el directorio

Hay dos grupos de restricciones que limitan potencialmente el acceso de un usuario de directorio a los dispositivos LOM. Las restricciones de acceso del usuario limitan el acceso de un usuario para autenticar el directorio. Las restricciones de acceso a las funciones limitan la capacidad de un usuario autenticado para recibir privilegios LOM basados en los derechos especificados en una o varias funciones.



Funciones restrictivas

Las restricciones permiten a los administradores limitar el ámbito de una función. Una función sólo concede derechos a los usuarios que cumplen con las restricciones de la función. Al usar funciones restringidas, los usuarios dispondrán de unos derechos dinámicos que podrán cambiar según la hora del día o la dirección de red del cliente.

NOTA: Si los directorios están activados, el acceso a un iLO 2 específico depende de si el usuario tiene acceso de lectura a un objeto de función que contiene el objeto iLO 2 correspondiente. Esto incluye, sin limitación, a los miembros que aparecen en el objeto de función. Si la función está configurada para admitir permisos heredables con el fin de propagarse desde un elemento principal, los miembros del elemento principal con privilegios de acceso de lectura también tendrán acceso a iLO 2. Para ver la lista de control de acceso, desplácese hasta Users and Computers (Usuarios y equipos), abra la pantalla de propiedades del objeto de función y seleccione la ficha **Security (Seguridad)**.

Para obtener instrucciones detalladas sobre cómo crear restricciones de red y de tiempo para una función, consulte las secciones "Restricciones de función de Active Directory" (Restricciones de función de Active Directory en la página 172), "Restricciones de función de eDirectory" (Restricciones de función de eDirectory en la página 180.)

Restricciones de tiempo de las funciones

Los administradores pueden asignar restricciones de tiempo a las funciones LOM. Los derechos especificados para los dispositivos LOM de una función se conceden únicamente a los usuarios si son miembros de la función y cumplen con las restricciones de tiempo de dicha función.

Los dispositivos LOM usan la hora de host local para imponer las restricciones de tiempo. Si no esta configurado el reloj del dispositivo LOM, no se aplicará la restricción de tiempo de la función a menos que no se hayan especificado restricciones de tiempo en dicha función.

Las restricciones de tiempo basadas en la función pueden cumplirse únicamente si se ha configurado la hora en el dispositivo LOM. La hora suele configurarse al iniciarse el host y se mantiene ejecutando los agentes en el sistema operativo del host, lo que permite al dispositivo LOM compensar los años bisiestos y las variaciones de hora con respecto al host. Sucesos, como un corte de alimentación imprevisto o una actualización del firmware de LOM, pueden ser los responsables de que no se configure el reloj del dispositivo LOM. Asimismo, la hora del host debe ser correcta para que el dispositivo LOM conserve la hora tras las actualizaciones del firmware.

Restricciones de dirección de las funciones

Las restricciones de dirección de las funciones las impone el firmware LOM, basándose en la dirección de red IP del cliente. Cuando se cumplen las restricciones para una función, se aplican los derechos concedidos por la función.

Las restricciones de dirección pueden resultar difíciles de gestionar si se intenta obtener acceso a través de servidores de seguridad o servidores proxy de red. Cualquiera de estos mecanismos puede cambiar la dirección de red aparente del cliente y, de este modo, ser el responsable de que las restricciones de dirección se impongan de una manera inesperada.

Restricciones de usuario

Puede limitar el acceso mediante restricciones de tiempo o dirección.

Restricciones de dirección de usuario

Los administradores pueden asignar restricciones de dirección de red a una cuenta de usuario de directorio; dichas restricciones las impone el servidor de directorios. Consulte la documentación del servicio de directorio para obtener información detallada sobre cómo se imponen las restricciones de dirección en los clientes LDAP, como un usuario que inicia sesión en un dispositivo LOM.

Es posible que las restricciones de dirección de red asignadas al usuario en el directorio no se impongan de la manera esperada si el usuario de directorio inicia sesión a través de un servidor proxy. Cuando un usuario inicia sesión en un dispositivo LOM como usuario de directorio, el dispositivo LOM intenta realizar la autenticación en el directorio como dicho usuario, lo que significa que las restricciones de dirección asignadas a la cuenta de usuario se aplican cuando se accede al dispositivo LOM. No obstante, dado que el usuario inicia sesión en el dispositivo LOM a través de un servidor proxy, la dirección de red del intento de autenticación es la del dispositivo LOM y no la de la estación de trabajo del cliente.

Restricciones de los intervalos de direcciones IP

Las restricciones de los intervalos de direcciones IP permiten al administrador especificar las direcciones de red cuyo acceso se concede o se deniega mediante la restricción. El intervalo de direcciones suele especificarse con un formato de intervalo de menor a mayor. Un intervalo de direcciones puede especificarse para conceder o denegar el acceso a una sola dirección. Las direcciones comprendidas en el intervalo de direcciones IP de menor a mayor cumplen con la restricción de dirección IP.

Restricciones de dirección IP y máscara de subred

Las restricciones de dirección IP y máscara de subred permiten al administrador especificar un intervalo de direcciones cuyo acceso se concede o se deniega mediante la restricción. Este formato tiene las mismas funciones que una dirección IP pero puede resultarle más nativo al entorno de red. Un intervalo de direcciones IP y máscaras de subred suele especificarse mediante una dirección de subred y una máscara de bits de dirección que identifica las direcciones que están en la misma red lógica.

En términos binarios, si los bits de una dirección de equipo cliente sumados a los bits de la máscara de subred coinciden con la dirección de subred de la restricción, el equipo cliente cumple con la restricción.

Restricciones basadas en DNS

Las restricciones basadas en DNS usan el servicio de nomenclatura de red para examinar el nombre lógico del equipo cliente buscando los nombres de equipo asignados a las direcciones IP del cliente. Las restricciones DNS requieren un servidor de nombres funcionales. Si el servicio de nombres deja de funcionar o no se puede acceder al mismo, no se pueden aplicar las restricciones DNS y se generará un error.

Las restricciones basadas en DNS pueden limitar el acceso a un solo nombre de equipo específico o a equipos que comparten un sufijo de dominio común. Por ejemplo, la restricción DNS www.hp.com se aplica a los equipos host que tienen asignado el nombre de dominio www.hp.com. Sin embargo, la restricción DNS *.hp.com se aplica a todos los equipos cuyo origen es HP.

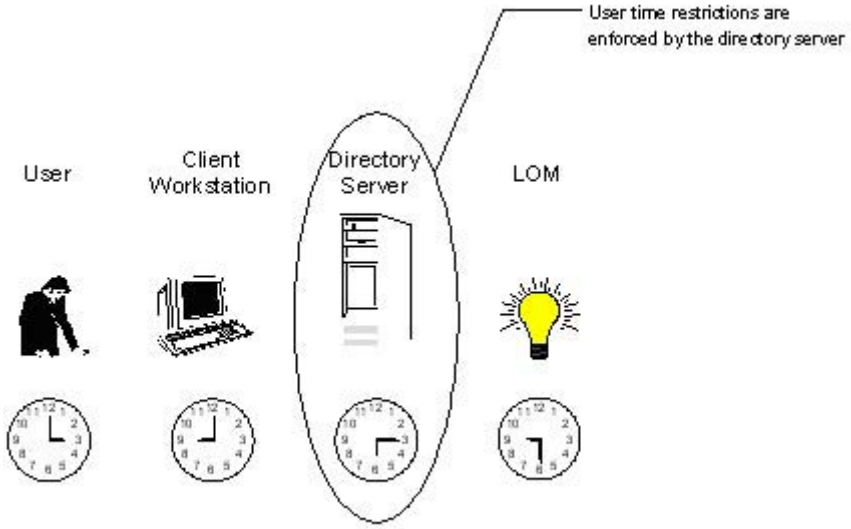
Las restricciones DNS pueden causar cierta ambigüedad debido a que un host puede tener varias conexiones de red. Las restricciones DNS no coinciden necesariamente una por una con un solo sistema.

El uso de las restricciones basadas en DNS puede originar algunas complicaciones en materia de seguridad. Los protocolos de los servicios de nombres son inseguros. Cualquier persona con intenciones maliciosas y con acceso a la red puede ubicar un servicio DNS en la red creando criterios de restricción de direcciones falsos. Se han de tener en cuenta las directivas de seguridad de la organización al implementar las restricciones de dirección basadas en DNS.

Cómo se imponen las restricciones de tiempo del usuario

Los administradores pueden asignar restricciones de tiempo a las cuentas de usuario de directorio. Las restricciones de tiempo limitan la capacidad del usuario para iniciar sesión (autenticar) en el directorio. Normalmente, las restricciones de tiempo se imponen utilizando la hora del servidor de directorios. Sin embargo, si el servidor de directorios está ubicado en otra zona horaria o se accede a una réplica en otra zona horaria, se podrá usar la información de zona horaria del objeto gestionado para ajustar el tiempo relativo.

El servidor de directorios evalúa las restricciones de tiempo, pero la determinación puede verse complicada por cambios de zona horaria o mecanismos de autenticación.



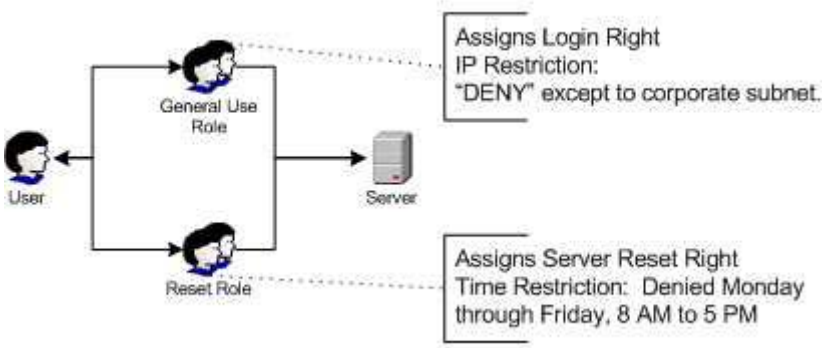
Creación de varias restricciones y funciones

La aplicación más útil de las múltiples funciones incluye la restricción de una o varias funciones de modo que los derechos no se aplican en todas las situaciones. Otras funciones conceden otros derechos en otras condiciones. El uso de múltiples restricciones y funciones permite al administrador crear relaciones de derechos complejas y arbitrarias con un número mínimo de funciones.

Por ejemplo, una organización puede disponer de una directiva de seguridad que permite a los administradores LOM usar el dispositivo LOM desde la red corporativa. Sin embargo, sólo pueden restablecer el servidor fuera de las horas de trabajo.

Los administradores de directorios pueden verse tentados de crear dos funciones para hacer frente a esta situación. Sin embargo, es preciso actuar con gran cautela. Crear una función que conceda los derechos de inicio de servidor necesarios y restringir su uso a un horario fuera de las horas de oficina puede permitir a administradores que no pertenezcan a la red corporativa reiniciar el servidor, lo que es contrario a la mayoría de las directivas de seguridad.

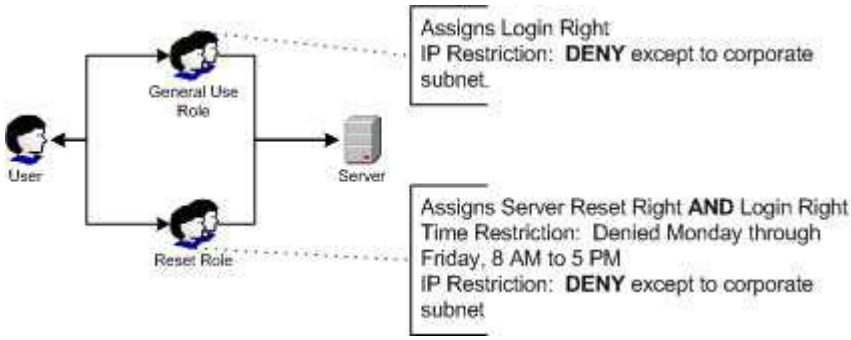
En el ejemplo, la directiva de seguridad establece que el uso general se limita a los clientes que forman parte de la subred corporativa y que la capacidad de reiniciar el servidor se limita además a las horas fuera del horario de trabajo.



Como alternativa, el administrador de directorios puede crear una función que conceda el derecho de inicio de sesión y lo limite a la red corporativa. A continuación, puede crear otra función que conceda sólo el derecho de reinicio del servidor y limite su uso a las horas fuera del horario de trabajo. Esta

configuración es más fácil de gestionar pero resulta más peligrosa ya que la administración en curso puede crear otra función que conceda a los usuarios de direcciones que no pertenecen a la red corporativa el derecho de inicio de sesión, lo que podría conceder de manera no intencionada a los administradores LOM en la función de reinicio del servidor la capacidad de reiniciar el servidor desde cualquier ubicación, siempre que cumplan las restricciones de tiempo de dicha función.

La anterior configuración cumple con la directiva de seguridad corporativa. Sin embargo, al añadir otra función que concede el derecho de inicio de sesión se pueden conceder de manera inadvertida privilegios de reinicio de servidor desde fuera de la subred corporativa y fuera de las horas de trabajo. Una solución más gestionable consistiría en restringir la función de reinicio así como la función de uso general.



Uso de herramientas de importación masiva

Añadir y configurar numerosos objetos LOM requiere mucho tiempo. HP proporciona varias utilidades para ayudar a realizar estas tareas.

- Utilidad de migración de Lights-Out de HP

  La utilidad de migración de Lights-Out de HP, HPQLOMIG.EXE, importa y configura varios dispositivos LOM. HPQLOMIG.EXE incluye una interfaz GUI que proporciona un enfoque paso a paso respecto a la implementación o actualización de grandes cantidades de procesadores de gestión. HP recomienda usar este método de GUI al actualizar numerosos procesadores de gestión. Para obtener más información, consulte la sección "Utilidad de migración de directorios HPQLOMIG" (Utilidad de migración de directorios HPQLOMIG en la página 193.)

- Utilidad de comandos de migración de Lights-Out de HP

  La utilidad de migración de comandos de migración de Lights-Out de HP, HPQLOMGC.EXE, ofrece un enfoque basado en la línea de comandos respecto a la migración, en lugar de un enfoque basado en la interfaz GUI. Esta utilidad funciona conjuntamente con las funciones de ejecución de aplicaciones y consultas de HP SIM para configurar muchos dispositivos a la vez. Quizás los clientes que deben configurar sólo algunos dispositivos LOM para usar los servicios de directorio prefieran el enfoque basado en la línea de comandos. Para obtener más información, consulte la sección "Utilidad de migración de directorios HPQLOMIG" (Utilidad de migración de directorios HPQLOMIG en la página 193.)

- Utilidades de HP SIM:

  - Gestionar varios dispositivos LOM.
  - Detectar los dispositivos LOM como procesadores de gestión mediante CPQLOCFG para enviar un archivo de secuencias de comandos XML de RIBCL a un grupo de dispositivos LOM para gestionar dichos dispositivos LOM. Los dispositivos LOM llevan a cabo las acciones designadas por el archivo RIBCL y envían una respuesta al archivo de registro

CPQLOCFG. Para obtener más información, consulte la *Guía de recursos de líneas y secuencias de comandos del procesador de gestión HP Integrated Lights-Out*.

- Utilidades de importación tradicionales

  Los administradores familiarizados con herramientas como LDIFDE o el Asistente para la importación y exportación de NDS, pueden usar estas utilidades para importar o crear numerosos objetos de dispositivo LOM en el directorio. No obstante, los administradores deben configurar los dispositivos manualmente, tal y como se ha descrito previamente, aunque pueden hacerlo en cualquier momento. Las interfaces de programación y de secuencias de comandos también pueden usarse para crear los objetos de dispositivos LOM de la misma manera que usuarios u otros objetos. La sección "Esquema de los servicios de directorio (Esquema de los servicios de directorio en la página 238)" recoge información más detallada sobre los atributos y los formatos de datos de atributos al crear objetos LOM.

7 Utilidad de migración de directorios HPQLOMIG

En esta sección:

Introducción a la utilidad HPQLOMIG

La utilidad HPQLOMIG es para clientes que tengan instalados previamente procesadores de gestión y deseen simplificar la migración de estos procesadores hacia una gestión por directorios. HPQLOMIG automatiza algunos de los pasos de la migración necesarios para que los procesadores de gestión admitan servicios de directorio. HPQLOMIG puede realizar lo siguiente:

- Detectar procesadores de gestión en la red.
- Actualizar el firmware de procesador de gestión a la versión que admita servicios de directorio o directorios sin esquema.
- Asignan un nombre a los procesadores de gestión para identificarlos en el directorio.
- Crean objetos en el directorio correspondiente a cada procesador de gestión y los asocian a una función.
- Configuran los procesadores de gestión para que puedan comunicar con el directorio.

Compatibilidad

La utilidad HPQLOMIG funciona con Microsoft® Windows® y requiere Microsoft® .NET Framework. Para obtener información adicional y descargar .NET Framework, consulte la página Web de Microsoft® (http://www.microsoft.com/net.) La utilidad HPQLOMIG admite los sistemas operativos siguientes:

- Active Directory
  - Windows® 2000
  - Windows® Server 2003
- Novell eDirectory 8.6.2
  - Windows® 2000
  - Windows® Server™ 2003

Lights-Out Directory Package de HP

Todo el software de migración así como el extensor de esquema y los complementos de gestión se incluyen en el paquete de Smart Component de HP. Para completar la migración de los procesadores de gestión, es necesario ampliar el esquema e instalar complementos de gestión antes de ejecutar la herramienta de migración. Smart Component se encuentra en la página Web de gestión de Lights-Out de HP (http://www.hp.com/servers/lights-out.)

Para instalar las utilidades de migración, haga clic en **LDAP Migration Utility (Utilidad de migración LDAP)** en el Smart Component. Se ejecutará el programa de instalación de Microsoft® MSI, que instalará HPQLOMIG, las DLL necesarias, el contrato de licencia y otros archivos en el directorio C:\Archivos de programa\Hewlett-Packard\HP Lights-Out Migration Tool. Puede seleccionar otro directorio. El instalador creará un acceso directo a HPQLOMIG en el menú Inicio e instalará un archivo XML de muestra.

NOTA: La utilidad de instalación mostrará un mensaje de error y se cerrará si detecta que .NET Framework no está instalado.

Uso de HPQLOMIG

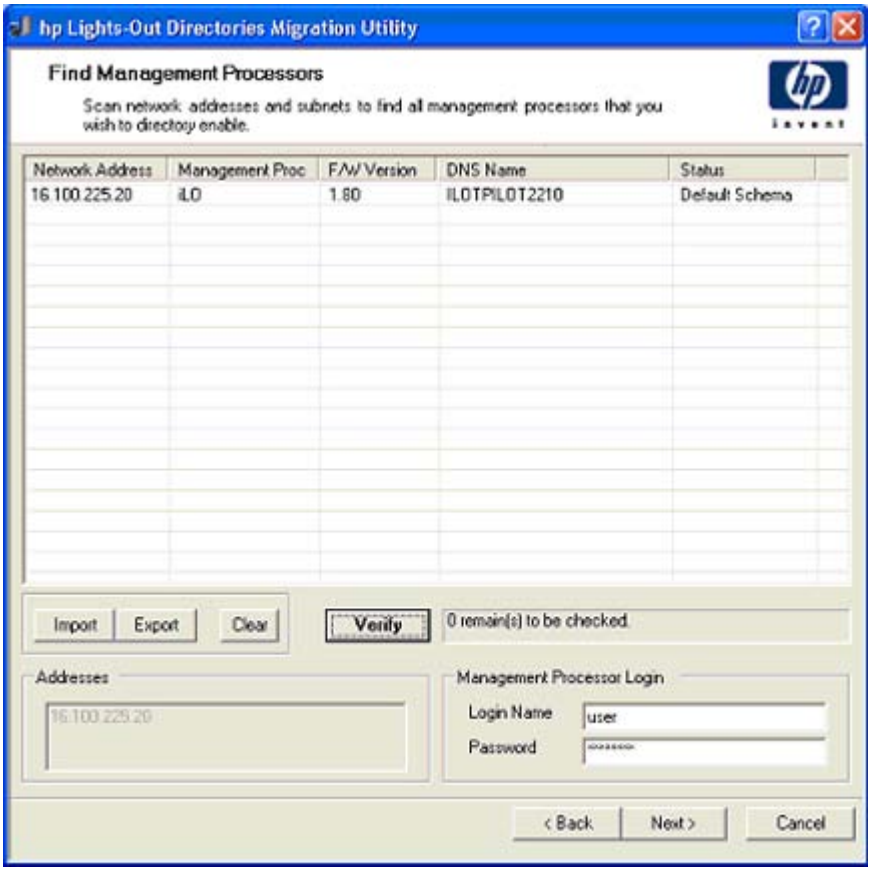
La utilidad HPQLOMIG automatiza el proceso de migración de procesadores de gestión al crear objetos en el directorio que correspondan a cada uno de los procesadores de gestión y asignarles a una función. HPQLOMIG cuenta con una GUI y proporciona al usuario un enfoque de asistente respecto a la implementación o actualización de grandes cantidades de procesadores de gestión.

Búsqueda de procesadores de gestión

El primer paso de la migración consiste en detectar todos los procesadores de gestión que desea activar para los servicios de directorio. Puede buscar procesadores de gestión con nombres DNS, direcciones IP o comodines de direcciones IP. Las siguientes reglas se aplican a las variables que se especifican en el campo Addresses (Direcciones):

- Los nombres DNS, las direcciones IP y los comodines de direcciones IP deben delimitarse con punto y coma.
- El comodín de direcciones IP utiliza el carácter “*” en los campos de octetos tercero y cuarto. Por ejemplo, la dirección IP 16.100.*.* es válida, mientras que la dirección IP 16.*.*.* no lo es.
- Los intervalos también pueden especificarse con un guión. Por ejemplo, 192.168.0.2-10 es un intervalo válido. El guión sólo puede utilizarse en el octeto situado en el extremo derecho.
- Una vez que se hace clic en **Find (Buscar)**, HPQLOMIG comienza a sondear con ping y a conectarse al puerto 443 (el puerto SSL predeterminado.) La finalidad de estas acciones es determinar rápidamente si la dirección de red objetivo es un procesador de gestión. Si el dispositivo no responde al comando ping o no se conecta adecuadamente al puerto 443, no se trata de un procesador de gestión.

Si hace clic en **Next (Siguiente)**, **Back (Atrás)** o sale de la aplicación durante la detección, las operaciones que se realicen en la dirección de red actual se completarán, pero aquellas que se realicen en direcciones de red subsiguientes quedarán canceladas.



Para iniciar el proceso de detección de procesadores de gestión:

1. Haga clic en **Inicio** y seleccione **Programas>Hewlett-Packard, Lights-Out Migration Utility** para iniciar el proceso de migración.
2. Haga clic en **Next (Siguiente)** para omitir la pantalla de bienvenida.
3. Especifique las variables en el campo Addresses (Direcciones) para buscar los procesadores de gestión.
4. Escriba su nombre de inicio de sesión, su contraseña y haga clic en **Find (Buscar)**. El botón Find (Buscar) cambia a Verify (Verificar) cuando se completa la búsqueda.

   También puede introducirse una lista de procesadores de gestión haciendo clic en **Import (Importar)**. El archivo es un archivo de texto simple con un procesador de gestión por línea. Los campos están delimitados por puntos y comas. Los campos son los siguientes:

   - Dirección de red
   - Tipo de procesador de gestión
   - Firmware Version (Versión del firmware)
   - Nombre DNS
   - Nombre de usuario
   - Contraseña
   - Configuración del directorio

     Por ejemplo, una línea podría contener:

```
16.100.225.20;iLO;1.80;ILOTPILOT2210;usuario;contraseña;Esquema
predeterminado
```

Si, por razones de seguridad, no pueden encontrarse en el archivo el nombre y la contraseña, deje estos campos en blanco pero conserve los puntos y comas.

Actualización del firmware en los procesadores de gestión

La pantalla de Actualización del firmware le permite actualizar los procesadores de gestión a la versión de firmware que admite directorios. Esta pantalla también permite designar la ubicación de la imagen de firmware para cada procesador de gestión introduciendo la ruta o haciendo clic en **Browse (Examinar)**.

NOTA: Es necesario que pueda accederse a las imágenes binarias del firmware para los procesadores de gestión desde el sistema que ejecuta la utilidad de migración. Se pueden descargar estas imágenes binarias de la página Web de HP (http://www.hp.com/servers/lights-out.)

Procesador de gestión	Versión de firmware mínima
RILOE	2.50
RILOE II	1.10
iLO	1.40
iLO 2	1.00

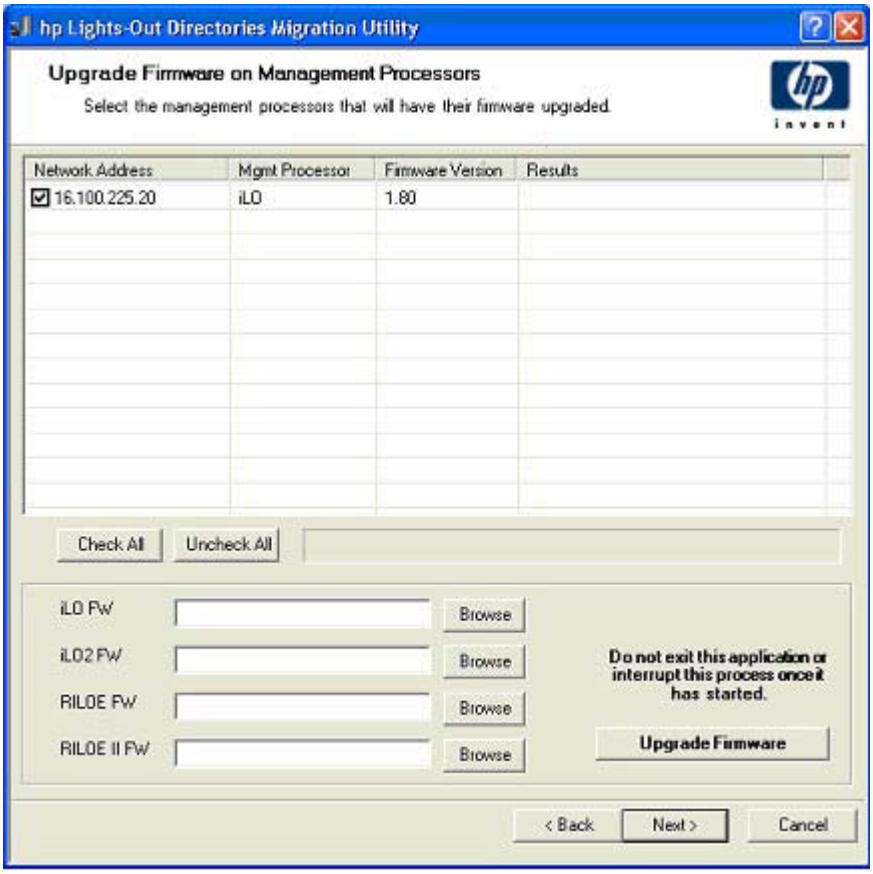
El proceso de actualización puede tardar bastante tiempo dependiendo del número de procesadores de gestión seleccionados. La actualización del firmware de un único procesador de gestión puede tardar un máximo de cinco minutos en completarse. Si una actualización no se realiza correctamente, aparece un mensaje en la columna Results (Resultados) y HPQLOMIG continúa actualizando el resto de los procesadores de gestión detectados.

NOTA: HP recomienda comprobar el proceso de actualización y comprobar los resultados en un entorno de prueba antes de ejecutar la utilidad en una red de producción. Si se realiza una transferencia incompleta de la imagen del firmware a un procesador de gestión, es posible que tenga que volver a programar de nuevo el procesador de gestión con un disquete.

Para actualizar el firmware en los procesadores de gestión:

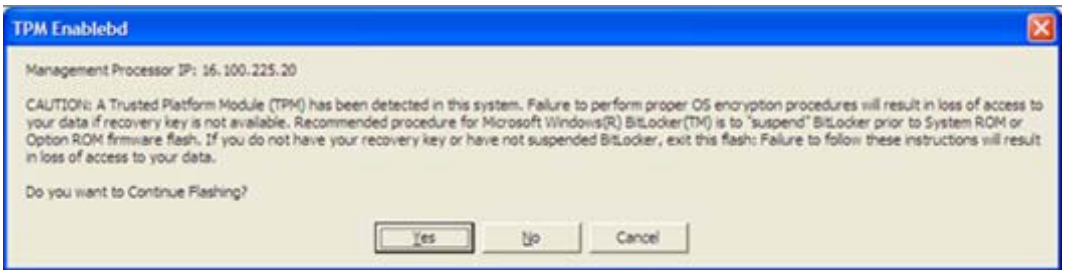
1. Seleccione los procesadores de gestión que van a actualizarse.
2. Para cada uno de los tipos de procesadores de gestión detectados, escriba el nombre correcto de la ruta de la imagen de firmware o explore la imagen.
3. Haga clic en **Upgrade Firmware (Actualizar firmware)**. Se actualizan los procesadores de gestión seleccionados. Aunque esta utilidad le permite actualizar cientos de procesadores de gestión, sólo pueden actualizarse 25 al mismo tiempo. Durante este proceso, la actividad de red es considerable.

4. Una vez realizada la actualización, haga clic en **Next (Siguiente)**.



Durante el proceso de actualización del firmware, se desactivan todos los botones para impedir la exploración. Aún así, todavía puede cerrar la aplicación con la “X” situada en la parte superior derecha de la pantalla. Si la GUI se cierra mientras se programa el firmware, la aplicación continúa ejecutándose en segundo plano y se completa la actualización del firmware en todos los dispositivos seleccionados.

HPLOMIG admite actualizaciones de firmware en servidores que disponen de un chip TPM. Si se encuentra presente y activado en el servidor un módulo TPM y la medición de ROM opcional se encuentra activada, HPLOMIG mostrará un mensaje de advertencia (mostrado a continuación.) Si selecciona Yes (Sí), HPLOMIG continuará con el proceso de actualización. De lo contrario, la actualización del firmware del servidor seleccionado se omitirá. Este mensaje se muestra cada vez que se detecta un servidor con un módulo TPM durante la actualización del firmware.

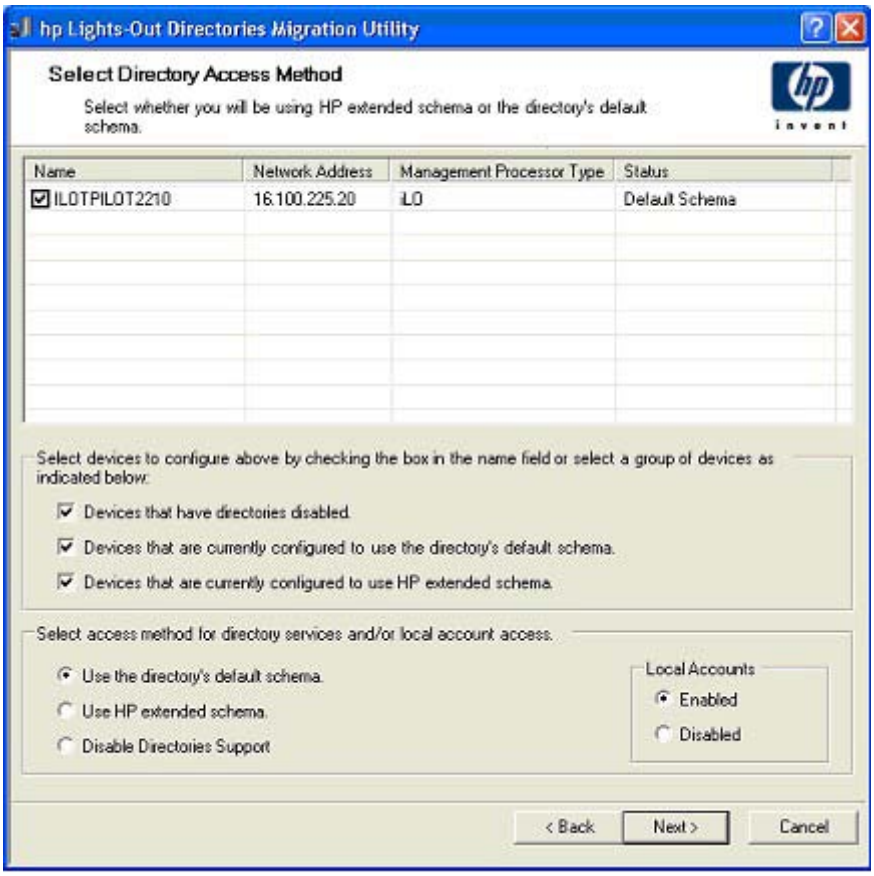


Selección de un método de acceso al directorio

Tras la página Firmware Upgrade (Actualización de firmware), se muestra la página Select Directory Access Method (Seleccionar método de acceso al directorio.) Puede seleccionarse qué procesadores

de gestión se desean configurar (con respecto al uso del esquema) y cómo se realizará la configuración. La página Select Directory Access Method (Seleccionar método de acceso al directorio) ayuda a evitar una sobrescritura accidental de los iLO 2 ya configurados para el esquema HP o de aquellos que tienen directorios desactivados.

Esta página determina si el esquema HP Extended, sin esquema (esquema predeterminado) o sin directorios admiten el seguimiento de páginas de configuración.



Para configurar el procesador de gestión para:

- Servicios de directorio, consulte la sección "Configuración de directorios cuando se selecciona HP Extended schema (Esquema extendido HP)" (Configuración de directorios cuando se selecciona HP Extended schema en la página 199.)
- Compatibilidad con los directorios sin esquema (esquema predeterminado), consulte la sección "Configuración para la integración de un directorio sin esquema".

Asignación de un nombre a los procesadores de gestión

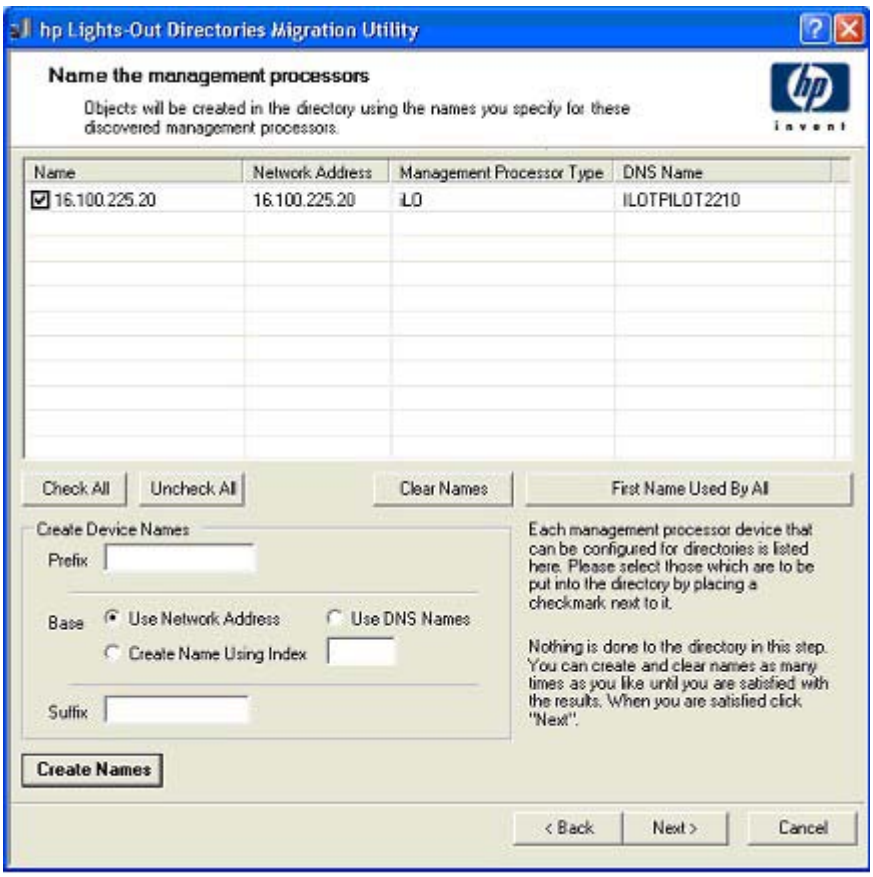
En esta pantalla puede asignar un nombre a los objetos de dispositivo de gestión de Lights-Out del directorio y crear objetos de dispositivo correspondientes para todos los procesadores que se van a gestionar. Puede crear nombres con uno o más de los siguientes elementos:

- La dirección de red
- El nombre DNS
- Un índice
- Creación manual de un nombre

- Adición de un prefijo a todos
- Adición de un sufijo a todos

Para asignar un nombre a los procesadores de gestión, haga clic en el campo **Name (Nombre)** y escriba el nombre, o bien:

1. Seleccione **Use Network Address (Utilizar dirección de red)**, **Use DNS Names (Utilizar nombres DNS)** o **Create Name Using Index (Crear un nombre con el índice)**. También puede dar nombre a cada uno de los objetos de directorio del procesador de gestión haciendo clic dos veces en el campo de nombre con un retraso entre clics.
2. Introduzca el texto o añada (sufijo o prefijo) a todos los nombres (opcional.)
3. Haga clic en **Generate Names (Generar nombres)**. Los nombres aparecen en la columna Name (Nombre) a medida que se generan. En este punto, no se escriben nombres en el directorio ni en los procesadores de gestión. Los nombres se almacenan hasta la página siguiente.
4. Para cambiar los nombres (opcional), haga clic en **Clear All Names (Borrar todos los nombres)** y modifíquelos en los procesadores de gestión.
5. Una vez modificados los nombres, haga clic en **Next (Siguiente)**.



Configuración de directorios cuando se selecciona HP Extended schema

La pantalla Configure Directory (Configurar directorios) permite crear un objeto de dispositivo para cada uno de los procesadores de gestión detectados y asociar el nuevo objeto a una función anteriormente definida. Por ejemplo, el directorio define a un usuario como miembro de una función (como la de administrador) que tiene una serie de privilegios sobre un objeto de dispositivo específico (como una tarjeta RILOE II.)

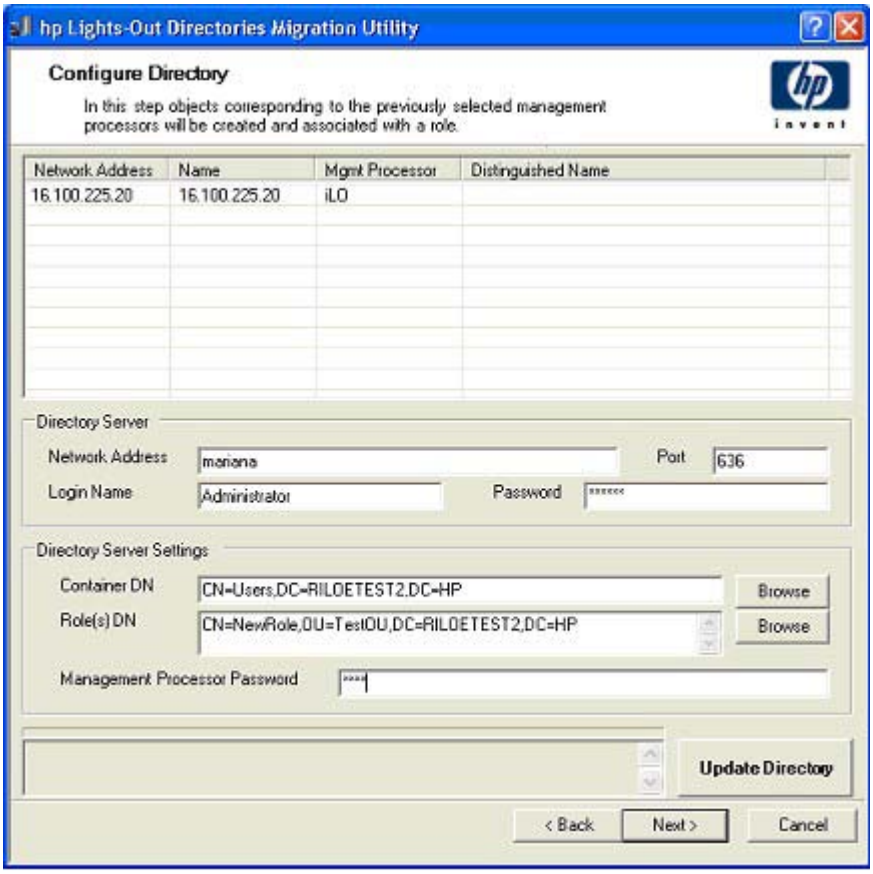
Los campos que aparecen en la pantalla Configure Directory (Configurar directorio) son:

- **Network Address (dirección de red)**: dirección de red del servidor del directorio, que puede ser una dirección IP o un nombre DNS válido.
- **Port (Puerto)**: el puerto SSL al directorio. La entrada predeterminada es 636. Los procesadores de gestión sólo pueden comunicarse con el directorio a través del SSL.
- **Login Name (Nombre de inicio de sesión)** y **Password (Contraseña)**: estos campos se utilizan para iniciar sesión con una cuenta con acceso de administrador de dominios al directorio.
- **Container DN (Nombre completo de contenedor)**: una vez que tenga la información relativa a la dirección de red, el puerto y el inicio de sesión, puede hacer clic en **Browse (Examinar)** para buscar los nombres completos de contenedor y función. El Nombre completo de contenedor es donde la utilidad de migración creará todos los objetos de procesador de gestión en el directorio.
- **Role DN (Nombre completo de función)**: aquí es donde reside la función que se va a asociar a los objetos de dispositivo y donde debe crearse antes de ejecutar esta utilidad.

Para configurar los objetos de dispositivo que se asociarán a una función:

1. Especifique la dirección de red, el nombre de inicio de sesión y la contraseña del servidor de directorios designado.
2. Escriba el nombre completo de contenedor en el campo Container DN (Nombre completo de contenedor) o haga clic en **Browse (Examinar)**.
3. Asocie los objetos de dispositivo con un miembro de una función. Para ello, especifique el nombre completo de la función en el campo Role DN o haga clic en **Browse (Examinar)**.
4. Haga clic en **Update Directory (Actualizar directorio)**. La herramienta conectará con el directorio, crea los objetos del procesador de gestión y los agrega a las funciones seleccionadas.

5. Una vez asociados los objetos de dispositivo a una función, haga clic en **Next (Siguiente)**.

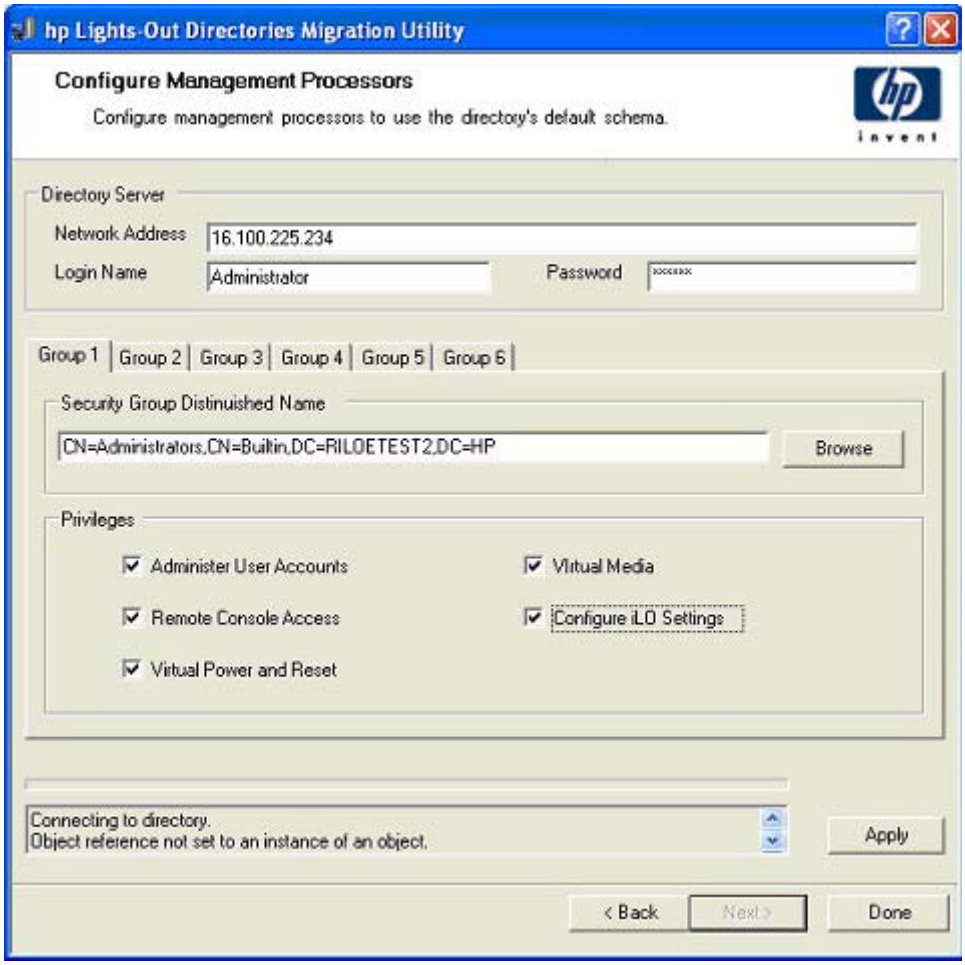


Configuración de directorios cuando se selecciona la integración sin esquema

Los campos que aparecen en la pantalla Configure Management Processors (Configurar procesadores de gestión) son:

- **Network Address (Dirección de red)**: dirección de red del servidor del directorio, que puede ser una dirección IP o un nombre DNS válidos.
- **Login Name (Nombre de inicio de sesión)** y **Password (Contraseña)**: estos campos se utilizan para iniciar sesión con una cuenta con acceso de administrador de dominios al directorio.
- **Security Group Distinguished Name (Nombre completo del grupo de seguridad)**: el nombre completo del grupo del directorio que contiene un conjunto de usuarios iLO 2 con un conjunto de privilegios común. Si el nombre de directorio, nombre de inicio y la contraseña son correctos, puede hacer clic en el botón **Browse (Examinar)** para acceder al grupo y seleccionarlo.
- **Privileges (Privilegios)**: los privilegios iLO 2 asociados con el grupo seleccionado. El privilegio de inicio queda implícito si el usuario es un miembro del grupo.

Los valores de la configuración de los procesadores de gestión se almacenan hasta la página siguiente del asistente.



Configuración de los procesadores de gestión para los directorios

El último paso en el proceso de migración consiste en configurar los procesadores de gestión para que se comuniquen con el directorio. Esta pantalla le permite crear contextos de usuario.

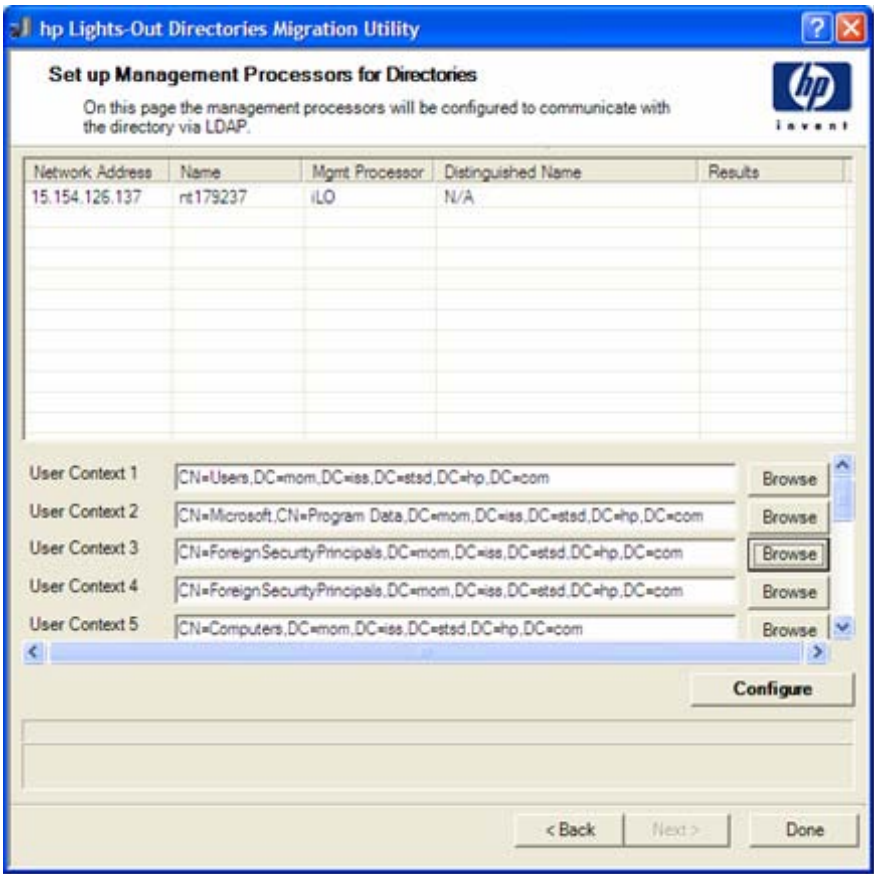
Los contextos de usuario permiten a éste utilizar nombres de objeto cortos o de usuario para iniciar sesión en lugar del nombre completo. Por ejemplo, en un contexto de usuario como éste: CN=Users,DC=RILOETEST2,DC=HP, “John Smith” puede iniciar sesión con John Smith en lugar de CN=John Smith,CN=Users, DC=RILOETEST2,DC=HP. También se admite el formato @. Por ejemplo, @RILOETEST2.HP en un campo de contexto permite al usuario iniciar sesión con jsmith (suponiendo que jsmith es el nombre corto del usuario.)

Para configurar los procesadores de gestión para que se comuniquen con el directorio:

1. Especifique los contextos de usuario o haga clic en **Browse (Examinar)**.
2. Para la opción Directories Support (Compatibilidad de directorios) y Local Accounts (Cuentas locales), seleccione **Enabled (Activada)** o **Disabled (Desactivada)**.

   El acceso remoto se desactiva si se desactivan la compatibilidad de directorios y las cuentas locales. Para volver a establecer el acceso, reinicie el servidor y utilice RBSU F8 para restaurar el acceso.

3. Haga clic en **Configure (Configurar)**. La utilidad de migración se conecta a todos los procesadores de gestión seleccionados y actualiza su configuración tal y como ha especificado. HPLOMIG admite la configuración de 15 contextos de usuario. Para acceder a los campos de contexto de usuario, utilice la barra de desplazamiento.



Cuando haga clic en Configure (Configurar), HPLOMIG mostrará el siguiente mensaje:

El mensaje indica que los 15 contextos de usuario son aplicables únicamente a equipos iLO 2 con versiones de firmware compatibles (1.75 o posterior.) Para el resto de procesadores de gestión, únicamente son aplicables los primeros tres campos User Context (Contexto de usuario.)

4. Cuando se complete el proceso, haga clic en **Done (Hecho)**.

8 Integración de HP Systems Insight Manager

En esta sección:

Integración de iLO 2 con HP SIM

iLO 2 se integra completamente con HP SIM en entornos operativos clave. La integración plena con Systems Insight Manager proporciona también una sola consola de gestión para ejecutar un explorador Web estándar. Mientras el sistema operativo está ejecutándose, puede establecer una conexión con iLO 2 utilizando HP SIM.

La integración con HP SIM ofrece:

- Compatibilidad con la entrega de capturas SNMP a una consola HP SIM

  La entrega a una consola HP SIM se puede configurar para enviar capturas SNMP a un buscapersonas o un correo electrónico.

- Compatibilidad con la gestión de SNMP

  HP SIM puede acceder a la información de los agentes de Insight Manager a través de iLO 2.

- Compatibilidad con un procesador de gestión

  HP SIM añade compatibilidad con un tipo de dispositivo nuevo, el procesador de gestión. Todos los dispositivos iLO 2 de los servidores en una red se descubren en HP SIM como procesadores de gestión. Los procesadores de gestión están asociados con los servidores en los que están instalados.

- Agrupamiento de los procesadores de gestión de iLO 2.

  Todos los dispositivos iLO 2 pueden agruparse de manera lógica y mostrarse en una página. Esta función ofrece acceso a iLO 2 desde un punto de HP SIM.

- Hipervínculos de iLO 2

  HP SIM ofrece un hipervínculo en la página del dispositivo del servidor para iniciarla y conectarla con iLO 2.

- Agentes de gestión de HP

iLO 2, combinado con los Agentes de gestión de HP, proporciona acceso remoto a la información de gestión del sistema mediante la interfaz basada en explorador de iLO 2.

Descripción general del funcionamiento de HP SIM

HP SIM le permite:

- Identificar los procesadores de iLO 2.
- Crear una asociación entre iLO 2 y su servidor.
- Crear enlaces entre iLO 2 y su servidor.
- Ver la información y el estado correspondientes a iLO 2 y al servidor.
- Controlar la cantidad de información detallada mostrada para iLO 2.
- Crear una imagen de la infraestructura de bastidor del ProLiant BL p-Class.

En las siguientes secciones se proporciona un resumen de cada una de las funciones. Para obtener información detallada sobre estas ventajas y sobre cómo utilizar HP SIM, consulte la *HP Systems Insight Manager Technical Reference Guide (Guía de referencia técnica de HP Systems Insight Manager)*, suministrada con HP SIM y disponible en la página Web de HP (http://www.hp.com/go/hpsim.)

Establecimiento de SSO mediante HP SIM

1. Navegue hasta un equipo iLO 2 e inicie sesión con credenciales de administrador.
2. Seleccione la ficha **Administration (Administración)**.
3. En el menú, seleccione **Security (Seguridad)**.
4. Seleccione la ficha **HP SIM SSO**.
5. Ajuste Single Sign-On Trust Mode (Modo fiable de inicio de sesión único) **Trust by Certificate (Confiar según certificado)**, y haga clic en **Apply (Aplicar)**.
6. Haga clic en **Add HP SIM Server (Añadir un servidor HP SIM)**. Se mostrará la página HP Systems Insight Manager Single Sign-On Settings (Configuración de inicio de sesión único de HP Systems Insight Manager.)
7. En Retrieve and import a certificate from a trusted HP SIM Server (Recuperar e importar un certificado desde un servidor HP SIM fiable), introduzca el nombre de host o la dirección IP del servidor HP SIM y haga clic en **Import Certificate (Importar certificado)**. El servidor se agregará a la lista HP SIM Trusted Servers (Servidores HP SIM de confianza) de la ficha HP SIM SSO.
8. Inicie sesión en el servidor HP SIM al que accedió en el paso 7 y descubra este <LOM_server_name>. Una vez completado el proceso de descubrimiento, SSO se habilitará para este equipo iLO 2.

   Si desea obtener más información acerca de las tareas de descubrimiento, consulte la *HP Systems Insight Manager Technical Reference Guide (Guía de referencia técnica de HP Systems Insight Manager)*. Si desea obtener más información acerca de las opciones de SSO de iLO 2, consulte "Inicio de sesión único de HP SIM (SSO) (Inicio de sesión único de HP SIM (SSO) en la página 57)".

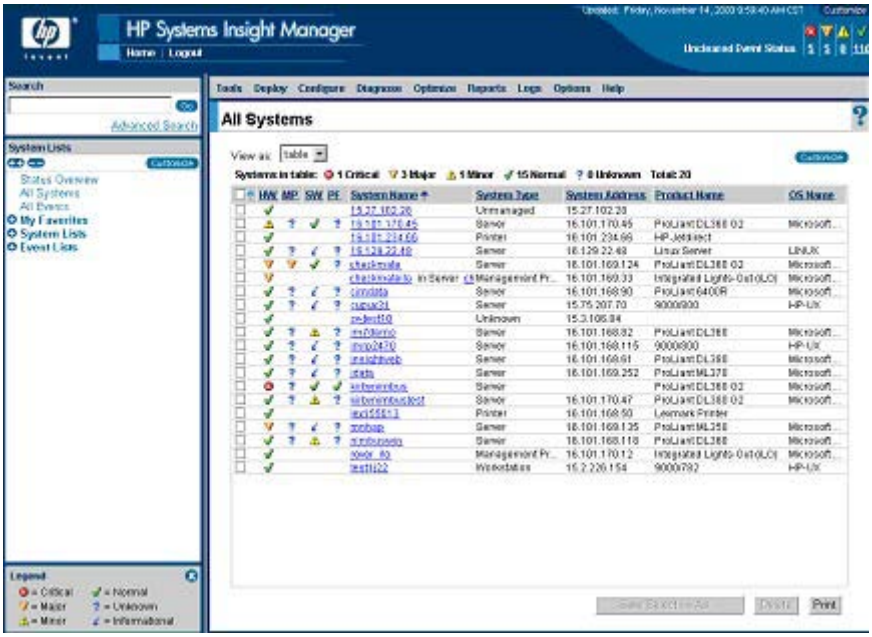
Identificación y asociación de HP SIM

HP SIM puede identificar un procesador iLO 2 y crear una asociación entre iLO 2 y el servidor. El administrador del dispositivo LOM puede configurar iLO 2 para que responda a las solicitudes de identificación de HP SIM.

Estado de HP SIM

En HP SIM, iLO 2 se identifica como procesador de gestión. HP SIM muestra el estado del procesador de gestión dentro de la System List (Lista de sistemas.)

El procesador de gestión iLO 2 aparece como un icono en la lista de dispositivos en la misma fila que su servidor host. El color del icono representa el estado del procesador de gestión.



Para visualizar una lista completa con los estados de los dispositivos, consulte la *HP Systems Insight Manager Technical Reference Guide (Guía de referencia técnica de HP Systems Insight Manager)* que se encuentra en la página Web de HP (http://www.hp.com/go/hpsim.)

Enlaces de HP SIM

Para que la gestión resulte más sencilla, HP SIM crea enlaces a las siguientes ubicaciones:

- iLO 2 y el servidor host desde cualquier lista de sistemas
- El servidor desde la página de sistemas de iLO 2
- iLO 2 desde la página de sistemas del servidor

Las páginas Systems List (Lista de sistemas) muestran iLO 2, el servidor y la relación entre iLO 2 y el servidor. Por ejemplo, la página puede mostrar el servidor, el nombre de iLO 2 junto al servidor y el *nombre de iLO 2***EN***el servidor* en el campo System Name (Nombre del sistema) para iLO 2.

Al hacer clic en un icono de estado de iLO 2, se abrirá la interfaz Web de iLO 2. Al hacer clic en el icono de estado del hardware, se accederá a los agentes de Insight Manager del dispositivo. Si hace clic en iLO 2 o el nombre del servidor, se abrirá la página de sistemas del dispositivo. La página de sistemas incluye las fichas Identity (Identidad), Tools & Links (Herramientas y Enlaces) y Event (Suceso.) Estas

fichas facilitan información sobre la identidad, el estado, los eventos y los enlaces del dispositivo asociado.

Listas de sistemas de HP SIM

Los procesadores de gestión de iLO 2 pueden visualizarse en HP SIM. Un usuario con derechos de configuración puede crear y utilizar conjuntos de sistemas personalizados en los procesadores de gestión del grupo. Para obtener más información, consulte la *HP Systems Insight Manager Technical Reference Guide (Guía de referencia técnica de HP Systems Insight Manager)*, suministrada con HP SIM y disponible en la página Web de HP (http://www.hp.com/go/hpsim.)

Recepción de avisos SNMP en HP SIM

Es posible configurar iLO 2 para que reenvíe avisos desde los agentes de gestión del sistema operativo host y enviar los avisos generados por iLO 2 a HP SIM.

HP SIM proporciona compatibilidad con una gestión total de SNMP e iLO 2 admite la entrega de capturas SNMP a HP SIM. Puede consultar el registro de sucesos, seleccionar el suceso y ver la información acerca del aviso.

La configuración de la recepción de avisos SNMP en HP SIM es un proceso que consta de dos pasos. El proceso requiere que HP SIM detecte iLO 2 y lo configure para permitir los avisos de SNMP.

1. Para permitir que iLO 2 envíe capturas SNMP, haga clic en **SNMP/Insight Manager Settings (Configuración de SNMP/Insight Manager)** de la ficha Administration (Administración) del marco de navegación de iLO 2 para activar los avisos SNMP y proporcionar una dirección IP de captura SNMP para iLO 2. Esta dirección IP debe ser la dirección del equipo que ejecuta HP SIM. Consulte la sección "Activación de los avisos SNMP (Activación de los avisos SNMP en la página 70)".
2. Para que iLO 2 se detecte en HP SIM, configure iLO 2 como un dispositivo administrado para HP SIM. Al añadir iLO 2 a HP SIM, la interfaz NIC en iLO 2 funciona como un puerto de gestión dedicado y aísla el tráfico de gestión de la interfaz NIC del servidor host remoto.
   - Inicie HP SIM.
   - Seleccione **Options (Opciones)>Discovery (Descubrimiento)>Automatic Discovery (Descubrimiento automático)**.
   - Seleccione la tarea de detección que se debe ejecutar y haga clic en Edit (Editar.)
   - Seleccione **IP range pinging (Sondeo de intervalo de IP)**. Si la dirección IP no se encuentra en los intervalos de inclusión del sondeo, plantillas o sección de archivos de hosts, introduzca la dirección IP.

- Haga clic en **OK (Aceptar)**.
- Para añadir iLO 2 a HP SIM, siga uno de los procedimientos siguientes:
  - Haga clic en **Save and Run (Guardar y ejecutar)**. Una vez finalizado el proceso de detección, las consultas adicionales muestran el dispositivo como un procesador de gestión.

    Quizás tenga que modificar la cadena de comunidad de lectura de SNMP (por ejemplo, cambiándola a “public”) para que iLO 2 aparezca en la lista de sistemas supervisados. Es posible cambiar la cadena de comunidad de SNMP. Para ello, acceda a la página Systems Protocol Settings (Configuración de protocolo de sistemas.) Para acceder a estos ajustes, seleccione **Options (Opciones)>Protocol Settings (Configuración de protocolo)>System Protocol Settings (Configuración de protocolo de sistemas)**.
  - Haga clic en **Options (Opciones)>Protocol Settings (Configuración de protocolo) >Global Protocol Settings (Configuración de protocolo global)**, y ajuste las cadenas de comunidad para utilizarlas durante el descubrimiento en Default SNMP Settings (Configuración SNMP predeterminada.) Una vez establecidas, puede utilizar los pasos de A a E para ejecutar el proceso de detección.

    Para los sucesos importantes y no vaciados, en All Events (Todos los sucesos) se mostrarán las capturas iLO 2. Haga clic en **Event Type (Tipo de suceso)** para obtener más información sobre el suceso.

  NOTA: Es preciso instalar HP Insight Agents para iLO 2 en el servidor host remoto para permitir la gestión de iLO 2. Consulte la sección "Instalación de los controladores del dispositivo iLO 2" para obtener más información sobre la instalación y configuración de agentes.

coincidencia de puertos de HP SIM

HP SIM está configurado para que inicie una sesión HTTP y busque a iLO 2 en el puerto 80. El puerto puede cambiarse. Si desea cambiar el número de puerto, también debe cambiarlo en Network Settings (Configuración de red) y en HP SIM.

Para cambiar el número de puerto en HP SIM, añada el puerto al archivo config\identification \additionalWsDisc.props en el directorio en el que está instalado HP SIM. La entrada debe empezar por el puerto HTTP para iLO 2. No es necesario que haya ninguna entrada en este archivo para iLO 2 si permanece en el puerto 80 estándar. Es muy importante que la entrada esté en una sola línea, que el número de puerto esté al principio y que los demás elementos sigan al pie de la letra el ejemplo siguiente (incluido el uso de mayúsculas y minúsculas.)

En el siguiente ejemplo se muestra cuál es la entrada si iLO 2 debe detectarse en el puerto 55000 (todo esto debe estar en una sola línea en el archivo):

```
55000=iLO
2, ,true,false,com.hp.mx.core.tools.identification.mgmtproc.MgmtProcessorPa
rser
```

Revisión de Advanced Pack Licence en HP SIM

HP SIM muestra el estado de licencia de los procesadores de gestión de iLO 2. Puede utilizar esta información para determinar cuántos y qué tipos de dispositivos iLO 2 tienen licencia para el paquete avanzado de iLO.

Para ver información sobre la licencia, haga clic en **Deploy (Implementar)>License Manager (Administrador de licencias)>Manage Keys (Gestionar claves)**. Para asegurar que los datos son

recientes, ejecute la tarea de identificación de los sistemas para los procesadores de gestión. Consulte la documentación de HP SIM para obtener más información sobre las tareas de inicio.

9 Solución de problemas con la placa iLO 2

En esta sección:

Indicadores LED de POST de iLO 2

Durante el arranque inicial de la placa iLO 2, los indicadores LED de POST parpadean para mostrar el progreso de dicho proceso. Una vez finalizado el proceso de arranque, el LED de HB parpadea cada segundo. El LED 7 también parpadea de forma intermitente durante el funcionamiento normal.

Los otros indicadores LED (del 1 al 6) se encenderán tras el arranque del sistema para indicar que se ha producido un error de hardware. Si se detecta un fallo en el hardware, reinicie iLO 2. Para conocer la ubicación de los indicadores LED, consulte la documentación del servidor.

Un fallo de tiempo de ejecución de la placa iLO 2 se indica mediante el LED 7 y el de HB, que permanecen en estado Encendido o Apagado constantemente. Un error en tiempo de ejecución de la placa iLO 2 también se puede indicar mediante un patrón de parpadeo repetido en los ocho LED. Si se produce un error en tiempo de ejecución, reinicie la placa iLO 2.

Si observa un patrón de parpadeo secuencial en los ocho LED que se repite indefinidamente, esto indica que se ha producido un fallo en la memoria flash (actualización del firmware) y que se encuentra en modo de recuperación de la memoria flash. Para obtener más información, consulte la sección “Recuperación de memoria flash de iLO”.

A continuación se muestra la asignación de los indicadores LED:

HB	7	6	5	4	3	2	1

Indicador LED	Código de POST (actividad completada)	Descripción	Fallo indicado
Ninguno	00	Configurar selecciones de chip.	
1 ó 2	02—Funcionamiento normal	Determinar la plataforma.	
2 y 1	03	Establecer bit RUNMAP	
3	04	Inicializar el Controlador SDRAM.	
3 y 2	06	Activar la caché I.	
3, 2 y 1	07	Inicializar (sólo) la caché D	
4	08	Copiar el cargador secundario en la RAM.	No se pudo copiar el cargador secundario.
4 y 1	09	Comprobar el cargador secundario	No se ejecutó el cargador secundario.
4 y 2	0a	Iniciar el cargador secundario	Fallo en la prueba de la memoria SDRAM.
4, 2 y 1	0b	Copiar la ROM en la RAM	No se pudo copiar el bloque de arranque.
4 y 3	0c	Comprobar la imagen de la ROM en la RAM.	Falló la ejecución del bloque de arranque.
4, 3 y 1	0d	Se inició el Bloque de arranque principal	El bloque de arranque no pudo encontrar una imagen válida.
Ninguno		Iniciar la inicialización del Tiempo de ejecución C	
4, 3 y 2	0e	() principal ha tomado el control.	Fallo en la autocomprobación principal.
Varía	Varía	Cada subsistema puede realizar una autocomprobación	
4, 3, 2 y 1	0f	Iniciar ThreadX	Fallo en el inicio de RTOS.
Ninguno	00	Inicialización principal de () completa.	Fallo en el inicio del subsistema.
HB y 7		Parpadea mientras el procesador de iLO 2 ejecuta código de firmware. No cambia el valor de los seis indicadores LED inferiores	

El firmware de microprocesador de la placa iLO 2 incluye un código que comprueba la consistencia. Si alguna de dichas comprobaciones falla, el microprocesador ejecuta FEH. El FEH muestra información

mediante los indicadores LED de POST de la placa iLO 2. Los códigos de FEH se distinguen mediante un patrón con parpadeo alterno del número 99 más el resto del código de error.

Código FEH	Comprobación de consistencia	Explicación
9902	TXAPICHK	Se llamó a una función de RTOS de forma inadecuada o con un valor incorrecto.
9903	TXCONTEXT	El contexto guardado de uno o más subprocesos está dañado.
9905	TRAP	Falló una sonda de pila, la dirección de retorno no es válida o se detectó una instrucción de captura incorrecta.
9966	NMIWR	Se escribió de forma inesperada con memoria insuficiente.
99C1	CHKNULL	Se modificó el vector de reinicio.

Entradas del registro de sucesos

Pantalla del registro de sucesos	Explicación del registro de sucesos
Server power failed (Fallo en la alimentación del servidor)	Aparece cuando falla la alimentación del servidor.
Browser login (Inicio de sesión en el explorador): *Dirección IP*	Muestra la dirección IP del explorador que inició la sesión.
Server power restored (Alimentación del servidor restablecida)	Aparece al restablecerse la alimentación del servidor.
Browser logout (Fin de sesión en el explorador): *Dirección IP*	Muestra la dirección IP del explorador que cerró la sesión.
Server reset (Servidor reiniciado)	Aparece al reiniciarse el servidor.
Failed Browser login – IP Address (Falló el inicio de sesión en el explorador – Dirección IP): *Dirección IP*	Aparece cuando falla el inicio de sesión del explorador.
iLO 2 Self Test Error (Error de la autocomprobación de iLO 2): #	Aparece cuando iLO 2 ha realizado una prueba interna con errores. La causa probable es el fallo de un componente crítico. Se recomienda que no se siga utilizando la placa iLO 2 en este servidor.
iLO 2 reset (Reinicio de iLO 2)	Aparece cuando iLO 2 se reinicia.
On-board clock set; was #:#:#:#:#:# *(Reloj integrado establecido como #:#:#:#:#:#)*	Aparece al establecerse el reloj integrado.
Server logged critical error(s) (El servidor registró errores críticos)	Aparece cuando el servidor registra errores críticos.
Event log cleared by: (Registro de sucesos vaciado por: *User (Usuario)*	Aparece cuando un usuario elimina el registro de sucesos.
iLO reset to factory defaults (iLO 2 reiniciado a valores predeterminados de fábrica)	Aparece al restablecerse los valores predeterminados de iLO 2.
iLO 2 ROM upgrade to (Actualización de ROM de iLO 2 a) #	Aparece al actualizar la ROM.
iLO 2 reset for ROM upgrade (iLO 2 reiniciado para actualización de ROM)	Aparece al reiniciar iLO 2 para la actualización de la ROM.
iLO 2 reset by user diagnostics (iLO 2 reiniciado por diagnóstico de usuario)	Aparece cuando un diagnóstico de usuario reinicia iLO 2.

Pantalla del registro de sucesos	Explicación del registro de sucesos
Power restored to iLO 2 (Alimentación restablecida para iLO 2)	Aparece al restablecerse la alimentación de iLO 2.
iLO 2 reset by watchdog (Reinicio de iLO 2 mediante protección)	Aparece cuando se produce un error en iLO 2 y se reinicia automáticamente. Si persiste el problema, llame al servicio al cliente.
iLO 2 reset by host (Reinicio de iLO 2 mediante host)	Aparece cuando el servidor reinicia iLO 2.
Recoverable iLO 2 error, code (Error de iLO 2 recuperable, código) #	Aparece cuando se produce un error poco importante en iLO 2 y el procesador se reinicia automáticamente. Si persiste el problema, llame al servicio al cliente.
SNMP trap delivery failure: IP address (Fallo en la entrega de avisos SNMP): *Dirección IP*	Aparece cuando la captura SNMP no conecta con la dirección IP indicada.
Test SNMP trap alert failed for (Falló el aviso de capturas SNMP de comprobación para): *Dirección IP*	Aparece cuando la captura SNMP no conecta con la dirección IP indicada.
Power outage SNMP trap alert failed for (Corte en el suministro de alimentación, falló el aviso de capturas SNMP para): *Dirección IP*	Aparece cuando la captura SNMP no conecta con la dirección IP indicada.
Server reset SNMP trap alert failed for (Reinicio del servidor, falló el aviso de capturas SNMP para): *Dirección IP*	Aparece cuando la captura SNMP no conecta con la dirección IP indicada.
Illegal login SNMP trap alert failed for (Inicio de sesión ilegal, falló el aviso de capturas SNMP para): *Dirección IP*	Aparece cuando la captura SNMP no conecta con la dirección IP indicada.
Diagnostic error SNMP trap alert failed for (Error de diagnóstico, falló el aviso de capturas SNMP para): *Dirección IP*	Aparece cuando la captura SNMP no conecta con la dirección IP indicada.
Host generated SNMP trap alert failed for (Falló el aviso de capturas SNMP generadas por el host para): *Dirección IP*	Aparece cuando la captura SNMP no conecta con la dirección IP indicada.
Network resource shortage SNMP trap alert failed for (Escasez de recursos de red, falló el aviso de capturas SNMP para): *Dirección IP*	Aparece cuando la captura SNMP no conecta con la dirección IP indicada.
iLO 2 network link up (Conexión a la red de iLO 2)	Aparece cuando la red está conectada a iLO 2.
iLO 2 network link down (Desconexión de la red a iLO 2)	Aparece cuando la red no está conectada a iLO 2.
iLO 2 Firmware upgrade started by (Actualización de firmware de iLO 2 iniciada por): *User (Usuario)*	Aparece cuando un usuario inicia una actualización del firmware.
Host server reset by (Servidor host reiniciado por): *User (Usuario)*	Aparece cuando un usuario reinicia el servidor host.
Host server powered OFF by (Servidor host apagado por): *User (Usuario)*	Aparece cuando un usuario apaga el servidor host.
Host server powered ON by (Servidor host encendido por): *User (Usuario)*	Aparece cuando un usuario enciende el servidor host.
Virtual Floppy in use by: (Disquete virtual utilizado por) *User (Usuario)*	Aparece cuando un usuario utiliza un disquete virtual.
Remote Console login (Inicio de sesión en la consola remota): *User (Usuario)*	Aparece cuando un usuario inicia una sesión en la consola remota.
Remote Console Closed (Consola remota cerrada)	Aparece al cerrarse una sesión de la consola remota.
Failed Console login – IP Address (Falló el inicio de sesión – Dirección IP): *Dirección IP*	Muestra un inicio de sesión fallido de la consola y la dirección IP.

Pantalla del registro de sucesos	Explicación del registro de sucesos
Added User (Usuario añadido): *User (Usuario)*	Aparece cuando se añade un usuario local.
User Deleted by (Usuario eliminado por): *User (Usuario)*	Aparece cuando se elimina un usuario local.
Modified User (Usuario modificado): *User (Usuario)*	Aparece cuando se modifica un usuario local.
Browser login (Inicio de sesión en el explorador): *User (Usuario)*	Aparece cuando un usuario autorizado inicia sesión en iLO 2 con un explorador de Internet.
Browser logout (Fin de sesión en el explorador): User (Usuario)	Aparece cuando un usuario autorizado cierra sesión en iLO 2 con un explorador de Internet.
Failed Browser login – IP Address (Falló el inicio de sesión en el explorador – Dirección IP): *Dirección IP*	Aparece cuando falla un intento de inicio de sesión del explorador.
Remote Console login (Inicio de sesión en la consola remota): *User (Usuario)*	Aparece cuando un usuario autorizado se conecta mediante el puerto de la consola remota.
Remote Console Closed (Consola remota cerrada)	Aparece cuando se desconecta un usuario autorizado de la consola remota o cuando el puerto de ésta se cierra tras un intento fallido de inicio de sesión.
Failed Console login – IP Address (Falló el inicio de sesión en la consola – Dirección IP): *Dirección IP*	Aparece al fallar tres intentos de inicio de sesión de un usuario registrado mediante el puerto de la consola remota.
Added User (Usuario añadido): *User (Usuario)*	Aparece cuando se efectúa una nueva entrada en la lista de usuarios autorizados.
User Deleted by (Usuario eliminado por): *User (Usuario)*	Aparece cuando se elimina una entrada de la lista de usuarios autorizados. La sección User (Usuario) muestra el usuario que solicitó la eliminación.
Event Log Cleared (Borrado el registro de sucesos): *User (Usuario)*	Aparece cuando el usuario elimina el registro de sucesos.
Power Cycle (Reset) [Apagado y encendido (reinicio)]: *User (Usuario)*	Aparece al restablecerse el suministro de la alimentación.
Virtual Power Event (Suceso del Botón de alimentación virtual: *User (Usuario)*	Aparece cuando se utiliza el botón de alimentación virtual.
Security Override Switch Setting is On (El valor del conmutador de anulación de la seguridad está activado)	Aparece cuando el sistema se inicia con el conmutador de anulación de la seguridad activado.
Security Override Switch Changed to Off (El conmutador de anulación de la seguridad ha cambiado a apagado)	Aparece cuando el sistema se inicia con el conmutador de anulación de la seguridad desactivado.
On-board clock set; was previously "[NOT SET]" (Reloj integrado establecido como [NOT SET])	Aparece al establecerse el reloj integrado. Mostrará la hora anterior o el valor “NOT SET” (No establecido) si no se había establecido ninguna hora anteriormente.
Logs full SNMP trap alert failed for (Registros llenos, falló el aviso de capturas SNMP): *Dirección IP*	Aparece cuando los registros están llenos y el aviso de capturas SNMP falló para una dirección IP específica.
Security disabled SNMP trap alert failed for (Seguridad deshabilitada; fallo en el aviso de capturas SNMP de comprobación para): *Dirección IP*	Aparece cuando la seguridad se ha deshabilitado y el aviso de capturas SNMP falló para una dirección IP específica.
Security enabled SNMP trap alert failed for (Seguridad habilitada; fallo en el aviso de capturas SNMP de comprobación para): *Dirección IP*	Aparece cuando la seguridad se ha habilitado y el aviso de capturas SNMP falló para una dirección IP específica.
Virtual Floppy connected by User (Disquete virtual conectado por Usuario)	Aparece cuando un usuario autorizado conecta el disquete virtual.

Pantalla del registro de sucesos	Explicación del registro de sucesos
Virtual Floppy disconnected by *User* (Disquete virtual desconectado por Usuario.)	Aparece cuando un usuario autorizado desconecta el disquete virtual.
License added by (Licencia añadida por): *User (Usuario)*	Aparece cuando un usuario autorizado añade una licencia.
License removed by (Licencia eliminada por): *User (Usuario)*	Aparece cuando un usuario autorizado elimina una licencia.
License activation error by (Error de activación de licencia por): *User (Usuario)*	Aparece cuando se produce un error al activar la licencia.
iLO 2 RBSU user login (Inicio de sesión de usuario en la utilidad RBSU del sistema iLO 2): *User (Usuario)*	Aparece cuando un usuario autorizado inicia sesión en la utilidad RBSU de iLO 2.
Power on request received by (Solicitud de encendido recibida por): *Tipo*	Se recibió una solicitud de encendido como uno de los tipos siguientes: Power Button (botón de encendidoBotón de encendido) Activación por LAN Encendido automático
Virtual NMI selected by (NMI Virtual seleccionado por): *User (Usuario)*	Aparece cuando un usuario no autorizado selecciona el botón de NMI Virtual.
Virtual Serial Port session started by (Sesión de puerto serie virtual iniciada por): *User (Usuario)*	Aparece cuando se inicia una sesión de puerto serie virtual.
Virtual Serial Port session stopped by (Sesión de puerto serie virtual detenida por): *User (Usuario)*	Aparece cuando finaliza una sesión de puerto serie virtual.
Virtual Serial Port session login failure from (Fallo de inicio de sesión de puerto serie virtual de): *User (Usuario)*	Aparece cuando hay un fallo de inicio de sesión de puerto serie virtual.

Problemas relacionados con el hardware y el software

iLO 2 utiliza el cableado Ethernet estándar, es decir, CAT5 UTP con conectores RJ-45. El cableado directo es necesario para el enlace del hardware a un hub Ethernet estándar. Utilice un cable de cruce para una conexión de PC directa.

El puerto de gestión de iLO 2 debe estar conectado a una red conectada a un servidor DHCP e iLO 2 debe aparecer en la red antes de aplicar el suministro de alimentación. DHCP envía una petición inmediatamente después de aplicar el suministro de alimentación. Si la petición de DHCP no obtiene respuesta durante el primer inicio de iLO 2, volverá a enviar la petición en intervalos de 90 segundos.

El servidor DHCP se debe configurar para proporcionar la resolución de nombres DNS y WINS. iLO 2 se puede configurar para funcionar con una dirección IP estática tanto en la configuración de ROM de la opción F8 o en la página Web Network Settings (Configuración de red.)

El nombre DNS predeterminado aparece en la etiqueta de configuración de red y puede utilizarse para ubicar iLO 2 sin necesidad de conocer la dirección IP asignada.

Si se utiliza una conexión directa con el PC, debe utilizarse una dirección IP estática puesto que no hay ningún servidor DHCO en el enlace.

Desde la utilidad RBSU de iLO 2, pulse la tecla **F1** en la página DNS/DHCP para acceder a las opciones avanzadas y ver el estado de las solicitudes DHCP de iLO 2.

Compatibilidad con JVM

Para garantizar que los subprogramas iLO 2 Remote Console y Virtual Media funcionan según lo esperado, instale Java Runtime Environment, Standard Edition 1.4.2_13. Para encontrar un enlace a la última versión admitida de JRE, desde la interfaz del explorador de iLO 2, seleccione **Remote Console (Consola remota)>Settings (Configuración)>Java**.

Los subprogramas iLO 2 Remote Console, Remote Serial Console y Virtual Media requieren que JVM esté instalado en el servidor cliente. Si se accede a los subprogramas Remote Console y Virtual Media con una versión de Java™ Runtime Environment Standard Edition posterior a 1.4.2_13, es posible que no funcionen correctamente. Si utiliza otra versión de JVM, es posible que se produzcan las siguientes situaciones:

- Si se abre el subprograma Remote Console con Java™ Runtime Environment versión 1.5.x o 1.6.x, es posible que se produzca lo siguiente:
  - Aparece el mensaje Automation server cannot create object (El servidor de automatización no puede crear objetos.) Si hace clic en **OK (Aceptar)**, desaparece el mensaje y el subprograma funciona normalmente.
  - La tecla TAB no funciona correctamente. La tecla TAB se desplaza por las distintas partes de la ventana del subprograma Remote Console, en lugar de desplazarse por dentro del subprograma en sí.
- Si se abre el subprograma Virtual Media con Java™ Runtime Environment versión 1.5.x o 1.6.x, es posible que se produzca lo siguiente:
  - Al hacer clic en el botón **Create Disk Image (Crear imagen de disco)**, aparece otra ventana. La ventana puede aparecer sin los botones Create (Crear) y Cancel (Cancelar) o sólo con texto. Si se cierra la ventana y se abre de nuevo, los botones aparecerán correctamente.
  - Al seleccionar un archivo de imagen en el subprograma, aparece una ventana para la selección de archivos. Una vez seleccionado el archivo, la ventana se cierra y se vuelve a la ventana normal del subprograma. Sin embargo, el área del archivo de imagen no se actualiza y el subprograma no responde. Para actualizar la ventana original del subprograma Virtual Media y activarla para que se mantenga centrada en el sistema, haga clic en otra ventana. El subprograma no responde hasta que se cierra la ventana del subprograma Virtual Media y se abre de nuevo.

Problemas en el inicio de sesión

Utilice la siguiente información para resolver problemas en el inicio de sesión:

- Inténtelo con el inicio de sesión predeterminado, que se encuentra en la etiqueta de configuración de red.
- Si olvida su contraseña, un administrador con el privilegio Administer User Accounts (Administración de cuentas de usuario) puede reiniciar la sesión.
- Si el administrador también olvida su contraseña, éste deberá utilizar el Conmutador de anulación de la seguridad o definir una cuenta de administrador y una contraseña mediante HPONCFG.
- Compruebe si existen problemas habituales, como:
  - La contraseña, ¿cumple las restricciones establecidas para contraseñas? Por ejemplo, ¿contiene la contraseña caracteres en mayúsculas y minúsculas?
  - ¿Está utilizando un explorador incompatible?

No se acepta el nombre de inicio de sesión ni la contraseña

Si se ha conectado a iLO 2, pero ésta no acepta su nombre de inicio de sesión ni su contraseña, debe verificar que la información de inicio de sesión está configurada correctamente. Consiga que un usuario con el privilegio Administer User Accounts inicie sesión y cambie su contraseña. Si, aún así, no puede conectarse, pida al usuario que vuelva a iniciar sesión, elimine su cuenta de usuario y vuelva a establecerla.

NOTA: La utilidad RBSU también se puede usar para corregir problemas de inicio de sesión.

Cierre de sesión prematuro del usuario de directorio

Errores en la red pueden ser los responsables de que iLO 2 concluya que una conexión de directorio ya no es válida. Si iLO 2 no puede detectar el directorio, iLO 2 finaliza la conexión al directorio. Cuando se intenta seguir usando la conexión finalizada, el explorador abre la página de inicio de sesión.

Al abrirse la página de inicio de sesión, puede parecer que se trata de un cierre de sesión prematuro. Un cierre de sesión prematuro puede producirse durante una sesión activa si:

- Se interrumpe la conexión de red.
- Se cierra el servidor de directorios.

Para recuperarse de un cierre de sesión prematuro, vuelva a iniciar la sesión y siga utilizando iLO 2. Si el servidor del directorio no está disponible, deberá utilizar una cuenta local.

El puerto de gestión de iLO 2 no es accesible por nombre

El puerto de gestión de iLO 2 se puede registrar con un servidor WINS o un servidor DDNS para proporcionar la resolución de nombre a dirección IP necesaria para acceder al puerto de gestión de iLO 2 por nombre. El servidor WINS o el servidor DDNS debe estar conectado y en funcionamiento antes de conectar el puerto de gestión de iLO 2 y éste debe tener una ruta válida al servidor WINS o al servidor DDNS.

Además, el puerto de gestión de iLO 2 debe estar configurado con la dirección IP del servidor WINS o del servidor DDNS. Puede utilizar DHCP para configurar el servidor DHCP con las direcciones IP necesarias. También puede escribir las direcciones IP mediante la utilidad RBSU o seleccionando la opción **Network Settings (Configuración de red)** de la ficha Administration (Administración.) El puerto de gestión de iLO 2 debe estar configurado para el registro con un servidor WINS o DDNS. Estas opciones están activadas de manera predeterminada y pueden cambiarse usando RBSU o seleccionando la opción **Network Settings (Configuración de red)** en la ficha Administration (Administración.)

Los clientes que accedan al puerto de gestión iLO 2 deben estar configurados para utilizar el mismo servidor DDNS en el que la dirección IP del puerto de gestión iLO 2 se haya registrado.

Si está utilizando un servidor WINS y un servidor DNS no dinámico, el acceso al puerto de gestión de iLO 2 puede ser mucho más rápido si configura el servidor DNS de manera que utilice el servidor WINS para la resolución de nombres. Consulte la documentación apropiada de Microsoft® para obtener más información.

La utilidad RBSU de iLO 2 no está disponible tras reiniciar iLO 2 y el servidor

Si se reinicia el procesador de iLO 2 y lo hace también el servidor inmediatamente, existe una ligera posibilidad de que el firmware de iLO 2 no se inicialice por completo cuando el servidor realice su inicialización e intente invocar la utilidad RBSU de iLO 2. En este caso, la utilidad RBSU de iLO 2 no estará disponible o el código de la ROM de opciones de iLO 2 se omitirá totalmente. Si esto ocurre,

reinicie el servidor por segunda vez. Para evitar este problema, espere unos segundos antes de reiniciar el servidor después de reiniciar el procesador de iLO 2.

Imposibilidad de acceder a la página de inicio de sesión

Si no puede acceder a la página de inicio de sesión, debe comprobar que el nivel de codificación SSL del explorador está definido en 128 bits. El nivel de codificación SSL de iLO 2 está definido en 128 bits y no puede modificarse. Los niveles de codificación del explorador y de la placa iLO 2 deben ser idénticos.

Imposibilidad de acceder a iLO 2 mediante Telnet

Si no puede acceder a iLO 2 mediante Telnet, debe comprobar Remote Console Port Configuration (Configuración del puerto de consola remota) y Remote Console Data Encryption (Cifrado de datos de la consola remota) en la pantalla Global Settings (Configuración global.) Si Remote Console Port Configuration (Configuración del puerto de consola remota) está establecido en Automatic (Automático), el subprograma Consola remota activa el puerto 23, inicia una sesión y, a continuación, cierra el puerto 23 cuando la sesión ha finalizado. Telnet no puede activar automáticamente el puerto 23, por lo que falla.

Imposibilidad de acceder a los soportes virtuales o a la consola remota gráfica

Los soportes virtuales y la consola remota gráfica sólo están activos si se posee la licencia del Pack avanzado opcional de la tarjeta iLO. Aparecerá un mensaje donde se informa al usuario que las funciones no estarán disponibles si no se posee una licencia. Aunque es posible que hasta un máximo de 10 usuarios inicien sesión en el sistema iLO 2, sólo un usuario puede acceder a la consola remota. Aparecerá un mensaje de advertencia para informar de que la Consola remota ya está en uso.

Imposibilidad de conectarse a iLO 2 después de cambiar la configuración de red

Compruebe que los dos dispositivos conectados, la tarjeta NIC y el conmutador, tienen los mismos valores de configuración para las opciones transceiver speed autoselect (selección automática de la velocidad del transceptor), speed (velocidad) y duplex (dúplex.) Por ejemplo, si un dispositivo selecciona automáticamente la conexión, el otro dispositivo debe hacerlo así también. Puede acceder a la configuración de la NIC del sistema iLO 2 desde la pantalla Network Settings (Configuración de red.)

Imposibilidad de conectarse al puerto de diagnóstico de iLO 2

Si no puede conectarse al puerto de diagnóstico de iLO 2 a través de la NIC, tenga en cuenta lo siguiente:

- El uso del puerto de diagnóstico se detecta automáticamente cuando se conecta un cable de una red activa. Al cambiar entre los puertos de diagnóstico y los de la parte posterior, tiene que dejar un minuto para que se complete el cambio de red antes de intentar la conexión a través del explorador Web.
- Si hay en progreso una actividad crítica, el puerto de diagnóstico no se puede usar hasta que ésta se haya completado. Las actividades críticas son las siguientes:
  - Actualización del firmware
  - Una sesión de la consola remota
  - Inicialización de SSL
- Si utiliza una estación de trabajo cliente que contiene más de una NIC activada, por ejemplo una tarjeta inalámbrica y una tarjeta de red, un problema de ruta puede impedir el acceso al puerto de diagnóstico. Para resolver este problema:

1. Tenga sólo una NIC activa en la estación de trabajo cliente. Por ejemplo, desactive la tarjeta de red inalámbrica.
2. Configure la dirección IP de la red de estación de trabajo cliente para que coincida con la red del puerto de diagnóstico de iLO 2 con el fin de que se cumplan las siguientes condiciones:
   - La configuración de la dirección IP es 192.168.1. *X*, donde *X* es cualquier número diferente de 1, debido a que la dirección IP del puerto de diagnóstico está establecida en 192.168.1.1.
   - La configuración de la máscara de subred es 255.255.255.0.

Imposibilidad de conectarse al procesador de la placa iLO 2 mediante la NIC

Si no puede conectarse a iLO 2 a través de la NIC, intente alguno o todos los métodos de solución de problemas siguientes:

- Confirme que está encendido el indicador LED verde (estado del enlace) del conector RJ-45 de iLO 2. Esta condición indica que la conexión es correcta entre la NIC de PCI y el conmutador de red.
- Compruebe si parpadea el indicador LED verde, ya que éste indica que existe un tráfico normal de red.
- Ejecute la utilidad RBSU de iLO 2 para confirmar que la NIC está activada y verificar la máscara de subred y la dirección IP asignadas.
- Ejecute la utilidad RBSU de iLO 2 y use la ficha F1 – Advanced (Opciones avanzadas) de la página DNS/DHCP para ver el estado de las solicitudes DHCP.
- Solicite eco para la dirección IP de la NIC desde una estación de trabajo en red independiente.
- Intente conectarse con el software del explorador introduciendo la dirección IP de la NIC como URL. Puede ver la página principal de iLO 2 desde esta dirección.
- Reinicie iLO 2.

NOTA: Si se establece una conexión de red, es posible que tenga que esperar un máximo de 90 segundos a que aparezca la petición del servidor DHCP.

Los servidores ProLiant BL p-Class tienen disponible un puerto de diagnóstico. Si conecta un cable de una red activa al puerto de diagnóstico, la placa iLO 2 cambiará automáticamente del puerto iLO 2 al puerto de diagnóstico. Al cambiar entre los puertos de diagnóstico y los de la parte posterior, tiene que dejar un minuto para que se complete el cambio de red antes de intentar la conexión a través del explorador.

Imposibilidad de iniciar una sesión en iLO 2 tras instalar el certificado iLO 2

Si el certificado iLO 2 con firma automática se encuentra instalado de forma permanente en varios exploradores y la placa iLO 2 se restablece, puede que no sea posible volver a iniciar una sesión iLO 2, ya que iLO 2 genera un nuevo certificado con firma automática cada vez que se restablece. Cuando se instala un certificado en el explorador, éste se indexa según el nombre contenido en el certificado. Este nombre es único para cada iLO 2. Cada vez que se restablece iLO 2, genera un nuevo certificado con el mismo nombre.

Para evitar este problema, no instale el certificado iLO 2 con firma automática en el almacén de certificados del explorador. Si desea instalar el certificado iLO 2, debe solicitar un certificado permanente a una CA e importarlo a iLO 2. Este certificado permanente puede instalarse en el almacén de certificados del explorador.

Problemas relacionados con el servidor de seguridad

iLO 2 se comunica a través de diferentes puertos TCP/IP configurables. Si estos puertos están bloqueados, el administrador debe configurar el servidor de seguridad para permitir las comunicaciones en estos puertos. Consulte la sección Administration (Administrador) de la interfaz de usuario iLO 2 para visualizar o cambiar las configuraciones del puerto.

Problemas relacionados con el servidor proxy

Si el software del explorador Web está configurado para utilizar un servidor proxy, no se conectará a la dirección IP de iLO 2. Para resolver este problema, configure el explorador de tal modo que no utilice el servidor proxy para la dirección IP de iLO 2. Por ejemplo, en Internet Explorer, seleccione **Herramientas>Opciones de Internet>Conexiones>Configuración de LAN>Opciones avanzadas**, a continuación, escriba la dirección IP de iLO 2 o el nombre DNS en el campo Excepciones.

Error de autenticación basada en dos factores

Cuando intente autenticar iLO 2 mediante la autenticación basada en dos factores, es posible que reciba el mensaje `The page cannot be displayed (No se puede mostrar la página).` Este mensaje puede aparecer por los siguientes motivos:

- No se han registrado certificados de usuario en el sistema cliente. Para corregir este error, registre el certificado de usuario necesario en el sistema cliente, para lo que quizás necesite el software proporcionado por el proveedor de la tarjeta inteligente.
- El certificado de usuario se almacena en una tarjeta inteligente o identificador USB que no se encuentra conectado al sistema cliente. Para corregir este error, conecte la tarjeta inteligente o el identificador USB correspondiente al sistema cliente.
- El certificado de usuario no ha sido emitido por la CA de confianza. El certificado de la CA de confianza está configurado en iLO 2 en la página Two-Factor Authentication Settings (Configuración de la autenticación basada en dos factores.) El certificado configurado como CA de confianza debe ser un certificado público de la CA que emite certificados en su organización. Para corregir este problema, configure el certificado correspondiente como la CA de confianza en la página de configuración Two-Factor Authentication (Autenticación basada en dos factores) o utilice un certificado de usuario emitido por la CA de confianza que ya está configurada.

- El certificado de usuario ha caducado o aún no es válido. Independientemente de si el certificado caducado se asigna a un usuario local o corresponde a una cuenta de usuario del directorio, iLO 2 no permitirá la autenticación con un certificado que haya caducado o que aún no sea válido. Compruebe las fechas de validez del certificado para comprobar que este es el motivo del mensaje `Page cannot be displayed (No se puede mostrar la página)`. Para corregir este problema, emita un certificado válido al usuario. Asigne el certificado a la cuenta de usuario iLO 2 local si está autenticando los usuarios de iLO 2 locales y compruebe que la hora del reloj de iLO 2 está correctamente configurada.
- El certificado de usuario no se firmó digitalmente con el mismo certificado que se especifica como CA de confianza. Aunque el nombre del certificado de CA de confianza pueda coincidir con el emisor del certificado de usuario, es posible que este certificado se haya firmado digitalmente por un certificado diferente. Consulte la ruta de certificación del certificado de usuario y asegúrese de las claves públicas de la emisión del certificado es la misma que la clave pública del certificado CA de confianza. Para corregir este problema, configure el certificado correspondiente como la CA de confianza en la página de configuración Two-Factor Authentication (Autenticación basada en dos factores) o utilice un certificado de usuario emitido por la CA de confianza.

Solución de problemas de aviso y captura

Aviso	Explicación
Test Trap (Captura de prueba)	Esta captura la genera un usuario a través de la página Web de configuración.
Server Power Outage (Corte en el suministro de alimentación del servidor)	El servidor ha perdido el suministro de alimentación.
Server Reset (Servidor reiniciado)	El servidor se ha reiniciado.
Failed Login Attempt (Intento fallido de inicio de sesión)	Ha habido un fallo en el intento de inicio de sesión del usuario remoto.
General Error (Error general)	Esta es una condición de error que no está predefinida por la MIB no modificable.
Logs (Registros)	El registro circular se ha desbordado.
Security Override Switch Changed (Cambio del conmutador de anulación de la seguridad): On/Off (Activado/Desactivado)	El estado del conmutador de anulación de la seguridad ha cambiado (se ha activado o desactivado.)
Rack Server Power On Failed (Fallo de encendido del servidor montado en bastidor)	No se pudo encender el servidor porque el bastidor BL p-Class indica que no hay suficiente alimentación.
Rack Server Power On Manual Override (Anulación manual de encendido del servidor montado en bastidor)	El cliente forzó manualmente el servidor para que se encendiera a pesar de que el informe de BL p-Class indicara que no hay suficiente alimentación.
Rack Name Changed (Cambio de nombre del bastidor)	Se cambió el nombre del bastidor ProLiant BL p-Class.

Imposibilidad de recibir alarmas HP SIM (capturas SNMP) desde iLO 2

Un usuario que dispone del privilegio Configure iLO 2 Settings (Configurar los valores de iLO 2) debe conectarse a iLO 2 para configurar los parámetros de las capturas SNMP. Cuando se conecte a iLO 2, asegúrese de que los tipos de avisos y los destinos de capturas correctos están activados en la pantalla SNMP/Insight Manager Settings (Configuración de SNMP/Insight Manager) de la aplicación de la consola iLO 2.

Conmutador de anulación de la seguridad de la placa iLO 2

El conmutador de anulación de la seguridad de la placa iLO 2 permite el acceso de emergencia al administrador con control físico de la placa de sistema del servidor. Al establecer el conmutador de anulación de la seguridad de iLO 2, se permite el acceso al inicio de sesión con todos los privilegios, sin necesidad de un ID de usuario ni de una contraseña.

El conmutador de anulación de la seguridad de iLO 2 se encuentra dentro del servidor y su acceso se realiza abriendo el receptáculo del servidor. Para establecer el conmutador de anulación de la seguridad de la placa iLO 2, el servidor debe estar apagado y desconectado de la fuente de alimentación. Establezca el conmutador y después encienda el servidor. Invierta el procedimiento para eliminar el conmutador de anulación de la seguridad de iLO 2.

En las páginas Web de iLO 2 aparecerá un mensaje de advertencia indicando que el conmutador de anulación de la seguridad de iLO 2 se encuentra en uso. Se añadirá una entrada al registro de la placa iLO 2 en la que se indica el uso del conmutador de anulación de la seguridad de iLO 2. Asimismo, también puede enviarse un aviso SNMP en el que se indique el establecimiento o la eliminación del conmutador de anulación de la seguridad.

En el caso poco probable de que sea necesario, establezca el conmutador de anulación de la seguridad para que el bloque de inicio de la placa iLO 2 pueda guardarse en memoria flash. El bloque de inicio se mostrará hasta que se reinicie el sistema iLO 2. HP recomienda desconectar la placa iLO 2 de la red hasta que se complete el reinicio.

En función del servidor, el conmutador de anulación de la seguridad de la placa iLO 2 puede ser un simple puente o una posición específica del conmutador en un panel de interruptor DIP. Para acceder al conmutador de anulación de la seguridad de la placa iLO 2, consulte la documentación del servidor.

Mensaje de error del código de autenticación

En un explorador Mozilla, es posible que reciba un mensaje de error de código de autenticación incorrecto, que indica que el certificado y el par de claves públicas o privadas para iniciar una sesión SSL en el explorador han cambiado. Este mensaje de error puede producirse cuando no se usa un certificado proporcionado por el cliente, ya que iLO 2 genera su propio certificado con firma automática cada vez que se reinicia.

Para resolver este problema, cierre y reinicie el explorador Web, o instale sus propios certificados en iLO 2.

Solución de problemas de directorio

Las siguientes secciones ilustran procedimientos de solución de problemas de directorio.

Problemas de inicio de sesión con formato dominio/nombre

Para iniciar sesión utilizando el formato dominio/nombre, deben estar activados los controles ActiveX. Para verificar que su explorador está permitiendo al archivo de comandos de inicio de sesión llamar a los controles ActiveX, abra Internet Explorer y ajuste los controles ActiveX en **Preguntar**. Debería aparecer una ilustración similar a la siguiente.

Los controles de ActiveX está activados y veo una solicitud, pero el formato de inicio de sesión dominio/nombre no funciona

1. Inicie sesión con una cuenta local y determine el nombre del servidor de directorio.
2. Verifique que el nombre del servidor de directorio es un nombre y no una dirección IP.
3. Verifique que puede hacer ping en el nombre del servidor de directorio desde su cliente.
4. Ejecute las pruebas de configuración del directorio. Verifique que el ping se recibió correctamente. Para obtener información adicional acerca de cómo probar la configuración del directorio, consulte la sección "Pruebas de directorio" (Pruebas de directorio en la página 55.)

Parece que no funcionan los contextos de usuario

Consulte al administrador de la red. El nombre completo de su objeto de usuario debe encontrarse en el directorio. Su nombre de inicio es lo que aparece después del primer CN=. El recordatorio del nombre completo debería aparecer en uno de los campos de contexto de usuario. Los contextos de usuario no distinguen entre mayúsculas y minúsculas. Sin embargo, todo lo demás, incluyendo los espacios, forma parte del contexto de usuario.

El usuario del directorio no cierra sesión una vez transcurrido el tiempo de espera del directorio

Si ajusta el tiempo de espera de iLO 2 en Infinite timeout (Tiempo de espera infinito), la consola remota sondea periódicamente el firmware para verificar que existe la conexión. Cuando se produce este sondeo, el firmware de iLO 2 solicita al directorio permisos de usuario. Esta consulta periódica mantiene la conexión de directorio activa, impidiendo que se produzca un tiempo de espera y el inicio de sesión del usuario.

Solución de problemas de la consola remota

Las siguientes secciones ilustran procedimientos de solución de problemas con la consola remota. En general:

- Los programas de bloqueo de ventanas emergentes impiden iniciar Remote Console (Consola remota) y Virtual Serial Port (Puerto de serie virtual.)
- Las aplicaciones de bloqueo de ventanas emergentes definidas para evitar la apertura automática de nuevas ventanas impiden la ejecución de Remote Console (Consola remota) y Virtual Serial Port (Puerto de serie virtual.) Desactive los programas de bloqueo de ventanas emergentes antes de iniciar Remote Console (Consola remota) o Virtual Serial Port (Puerto de serie virtual.)

El subprograma de la consola remota muestra una X roja cuando se ejecuta en un explorador cliente Linux

Los exploradores Mozilla se deben configurar para que acepten cookies.

1. Abra el menú Preferences (Preferencias) y seleccione **Privacy (Privacidad)& Security (Seguridad)>Cookies**.
2. En la pantalla de nivel de privacidad, seleccione **Allow cookies based on privacy settings (Permitir cookies basándose en niveles de privacidad)** y haga clic en **View (Ver)**.
3. En la pantalla Cookies, seleccione **Allow cookies based on privacy settings (Permitir cookies basándose en niveles de privacidad)**.

El nivel de privacidad se debe establecer como Medio o Bajo.

Imposibilidad de desplazar el cursor único de la consola remota hasta las esquinas de la ventana de la consola remota

En algunos casos, quizá no pueda desplazar el cursor del ratón hasta las esquinas de la ventana de la consola remota. Si es así, haga clic con el botón secundario del ratón, arrastre el cursor fuera de la ventana de la consola remota y, a continuación, vuelva a arrastrarlo dentro.

Si el ratón sigue sin funcionar correctamente o si esta situación se produce con frecuencia, compruebe que los valores de configuración del ratón coinciden con los recomendados en la sección "Optimización del rendimiento del ratón para la consola remota o la consola remota integrada" (Optimización del rendimiento del ratón para la consola remota o la consola remota integrada en la página 98.)

La consola remota ya no se abre en la sesión de explorador existente

Con la función de transferencia de los servicios de Terminal Server, el subprograma Consola remota presenta un comportamiento ligeramente diferente al de versiones anteriores del firmware de iLO 2. Si ya se ha abierto una sesión de la consola remota y se vuelve a hacer clic en el enlace Remote Console (Consola remota), no se reiniciará la sesión de la consola remota. Al usuario puede parecerle que se ha quedado congelada la sesión de la consola remota.

Por ejemplo, si se llevan a cabo los siguientes pasos:

1. En Cliente-1, inicie sesión en iLO 2 y abra una sesión de la consola remota.
2. En Cliente-2, inicie sesión en iLO 2 e intente abrir una sesión de la consola remota. Aparecerá el mensaje `Remote console is already opened by another session (Ya hay otra sesión abierta en la consola remota)`. Se trata de una respuesta esperada ya que la consola remota admite una sola sesión a la vez.
3. Vuelva a Cliente-1 y cierre la sesión de la consola remota.
4. En Cliente-2, haga clic en el enlace Remote Console (Consola remota) mientras que el antiguo subprograma Consola remota sigue abierto. No se actualizará la sesión de la consola remota y seguirá mostrándose el mensaje mencionado en el paso 2.

Si bien este comportamiento es distinto al de versiones anteriores del firmware de iLO, se trata de un comportamiento esperado en esta versión del firmware. Para evitar problemas de esta índole, cierre siempre una sesión abierta de la consola remota antes de intentar reabrirla.

La ventana de texto de la consola remota no se actualiza correctamente

Cuando se utiliza la consola remota para mostrar ventanas de texto que se desplazan a gran velocidad, dichas ventanas puede que no se actualicen correctamente. Este error se produce cuando las

actualizaciones del vídeo suceden más rápido de lo que el firmware de iLO 2 es capaz de detectar y mostrar. Normalmente, sólo se actualiza la esquina superior izquierda de la ventana de texto, mientras que el resto permanece estático. Después que termine el desplazamiento, haga clic en **Refresh (Actualizar)** para regenerar adecuadamente la ventana de texto.

Un ejemplo de este problema ocurre durante el proceso de arranque y autocomprobación de Linux, en el que se pueden perder algunos mensajes de la POST. Uno de las posibles problemas es que el proceso de arranque solicite la respuesta del teclado y se pierda. Para evitarlo, se debe ralentizar el proceso de inicio y autocomprobación, editando la secuencia de comandos de inicio de Linux para facilitar más tiempo a la respuesta del teclado.

La consola remota se vuelve gris o negra

La pantalla de la consola remota se volverá gris o negra cuando se reinicie el servidor desde el cliente de los servicios de Terminal Server. La pantalla permanecerá gris o negra durante un período de tiempo de 30 segundos a 1 minuto. El cliente se cerrará porque no está disponible el servidor de los servicios de Terminal Server. La consola remota de iLO 2 debería hacerse cargo, pero la pantalla de la consola remota se volverá gris o negra. Cuando se restablezca la pantalla, la consola remota funcionará normalmente.

Solución de problemas de la consola remota de serie

La opción Remote Serial Console (Consola remota de serie) depende del puerto serie virtual. Éste debe estar correctamente activado y configurado en la utilidad RBSU del host. Puede acceder al puerto serie virtual mediante SSH o Telnet (si está activado.) Si UART y el puerto serie virtual comparten la misma configuración, podrá acceder a CLP desde una sesión de serie del host. Para acceder a CLP desde una sesión de serie del host escriba **Esc(** (escapar seguido de paréntesis de apertura) para pasar al intérprete de líneas de comandos.

Las aplicaciones de bloqueo de ventanas emergentes impedirán que se ejecute la opción de consola remota de serie. Desactive los programas de bloqueo de ventanas emergentes antes de iniciar Remote serial Console (Consola remota de serie.)

Solución de problemas de la consola remota integrada

Los problemas que se presentan con la consola remota integrada son:

- Problemas con Internet Explorer 7
- Configuración del servidor Web Apache para la exportación
- No se produce reproducción de consola mientras el servidor está apagado
- Se omite información durante la reproducción del búfer de inicio y fallo

Internet Explorer 7 y una pantalla de consola remota que parpadea

Al utilizar Internet Explorer 7 con la pantalla remota puede que la pantalla de la consola remota parpadee y sea difícil de leer. Si establece la aceleración del hardware del sistema en un nivel inferior ayudará paliar el parpadeo. Para cambiar el nivel de aceleración del hardware, seleccione **Panel de control>Pantalla** y, a continuación, seleccione la ficha **Configuración** tab. En la sección Configuración, haga clic en **Opciones avanzadas**. Cuando aparece la página Opciones avanzadas, seleccione la ficha **Solucionador de problemas**. Baje la **aceleración del hardware** hasta que el parpadeo desaparezca.

Configuración de Apache para aceptar búfer de captura exportados

Para activar la función Console Replay Export (Exportar reproducción de consola) para que funcione correctamente, debe configurar el servidor Web para que acepte los datos del búfer. A continuación se incluye un ejemplo de cambios de configuración realizados en Apache versión 2.0.59(Win32) en un servidor que ejecuta Microsoft Windows Server™ 2003.

Debe seleccionar una ubicación en la que guardar los datos exportados, establecer los permisos de Apache para escribir en esta ubicación y configurar la autenticación. Para configurar la autenticación, debe ejecutar `htpasswd.exe` y crear los nombres de usuario y contraseñas para que Apache pueda realizar la autenticación cuando reciba una solicitud de acceso a la ubicación de exportación. Para obtener más información sobre cómo configurar usuarios, consulte la base de software Apache (http://httpd.apache.org/docs/2.0/howto/auth.html.)

WebDAV proporciona un entorno de colaboración para que edite y gestione archivos en servidores Web. Técnicamente, DAV es una extensión al protocolo http. Puede realizar cambios en el archivo de configuración para activar WebDAV cargando sus módulos de soporte del objeto compartido dinámico. Se deben añadir las dos líneas siguientes a la lista de módulos del archivo `http.conf`: `LoadModule dav_module modules/mod_dav.so` y `LoadModule dav_fs_module modules/mod_dav_fs.so`.

También debe activar la autenticación cargando los módulos `LoadModule auth_module modules/mod_auth.so, LoadModule auth_digest_module modules/mod_auth_digest.so`.

Si no existe ningún directorio para la base de datos DavLock, deberá crear uno. Todo lo que se necesita es un directorio DAV dentro de Apache2. Se hace referencia al directorio en el archivo de configuración. A continuación se muestra un ejemplo de los cambios en `http.conf` para añadir esta compatibilidad:

```
# Davlock database location
DavLockDb "C:/apache/Apache2/Apache2/dav/davlock"
# location of data being exported
Alias /images/ "C:/images/"
# Configuration of the directory to support PUT Method with authentication
<Directory "C:/images">
AllowOverride FileInfo AuthConfig Limit
AuthType Digest
# if digest is not supported by your configuration use the following
# AuthType Basic
# location of the usernames and passwords used for authentication
AuthUserFile "C:/Program Files/apache group/Apache2/passwd/passwords"
# specifies the user that is required for authentication, can be a group
# For group change to the following after creating the appropriate group
# Require group GroupName
Require user Administrator
Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
Dav On
<Limit GET PUT OPTIONS PROPFIND>
Order allow,deny
Allow from all
</Limit>
</Directory>
```

No se produce reproducción de consola mientras el servidor está apagado

La reproducción de búfer de captura y sesiones de consola grabadas no está disponible cuando el servidor está apagado. Para reproducir los búfer capturados, se pueden exportar los búfer a un servidor

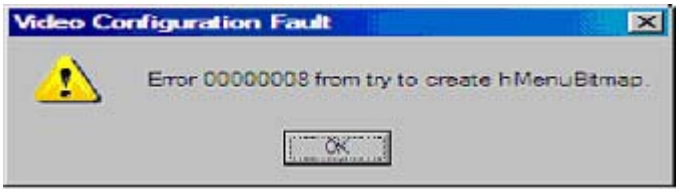
Web y reproducir los archivos en otra consola IRC de servidor. Exporte manualmente el búfer con el botón de exportación situado en la página Remote Console (Consola remota)>Settings (Configuración) después de configurar el servidor Web y la ubicación de exportación.

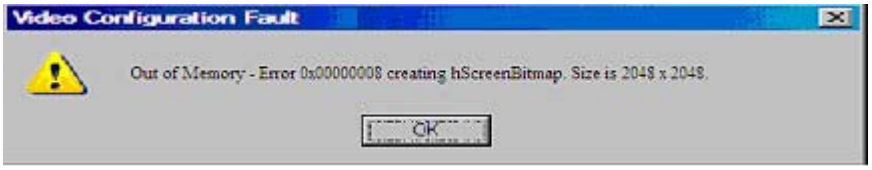
Se omite información durante la reproducción del búfer de inicio y fallo

Una cierta cantidad de pérdida de información de pantalla es normal y se puede producir durante la reproducción de búfer de inicio y fallo. Para ayudar a paliar el problema, asegúrese de que la IRC está activa durante el inicio y fallo. Si se siguen produciendo pérdidas de información, intente realizar una captura manual de estas secuencias. Para capturar una secuencia de servidor de forma manual, inicie la IRC y haga clic en el botón de grabación.

Error de memoria llena al iniciar la consola remota integrada

El sistema cliente puede quedarse sin memoria si se abren demasiadas sesiones de IRC a la vez. Cada sesión de IRC requiere un mínimo de 16 MB de memoria para el espacio de búfer de pantalla y Virtual Folder (Carpeta Virtual) puede utilizar unas 100 MB. Si aparece un cuadro de mensaje al iniciar IRC, significa que el cliente no dispone de la memoria suficiente para los datos de pantalla. Por ejemplo:





Para corregir estos tipos de errores, cierre algunas sesiones de IRC o añada memoria al equipo cliente para permitir la apertura simultánea de más sesiones.

El líder de sesión no recibe solicitudes de conexión cuando la IRC está en modo de reproducción

Como líder de una sesión, al reproducir datos de vídeo de captura, la IRC no muestra el mensaje de advertencia `Deny or Accept (Denegar o aceptar)` cuando otro usuario intenta acceder a la IRC o compartirla. En lugar de ello, la nueva sesión de IRC esperará y al final cerrará la sesión. Si necesita acceder a la IRC, intente acceder a IRC y tiempo de espera, utilice la función Acquire (Adquirir) para hacerse con el control de la IRC.

El LED del teclado no actúa correctamente

El LED del teclado cliente no refleja el estado real de las distintas teclas de bloqueo del teclado. Sin embargo, las teclas Bloq Mayús, Bloq Num y Bloq Despl son completamente funcionales cuando se utiliza la opción de teclado Key Up/Down (Tecla arriba/abajo) en la IRC.

IRC inactiva

La iLO 2 IRC puede volverse inactiva o desconectarse durante periodos de mucha actividad. Una IRC inactiva indica el problema. La actividad de IRC se ralentiza antes de quedar inactiva. Entre los síntomas de una IRC afectada se incluyen:

- La pantalla de IRC no se actualiza.
- No se registra la actividad del teclado y el ratón.
- No se registran las solicitudes de la consola remota compartida.
- La conexión de Virtual Media muestra un dispositivo de soporte virtual vacío (en blanco.)

Aunque puede reproducir un archivo capturado en una IRC inactiva, no se puede recuperar el estado activo de la IRC.

Este problema se puede presentar cuando hay varios usuarios registrados en iLO 2, hay una sesión de Virtual Media conectada y se está realizando una operación de copia continua, o hay una sesión de IRC abierta. La operación de copia continua de Virtual Media toma prioridad y, por consiguiente, la IRC pierde sincronización. Al final, la conexión de Virtual Media se reinicia varias veces y hace que la unidad de soporte USB del sistema operativo pierda sincronización con el cliente Virtual Media.

Para solucionar este problema, vuélvase a conectar a IRC y a Virtual Media. Si es posible, reduzca el número de sesiones de usuario simultáneas en iLO 2. Si fuera necesario, reinicie iLO 2 (el servidor no necesita reiniciarse.)

IRC Failed to connect to server error message

Es posible que iLO 2 emita el mensaje `Failed to connect to server (No se ha podido conectar al servidor)` al intentar establecer una sesión de IRC. Verifique una conexión telnet disponible.

El cliente iLO 2 IRC espera un tiempo específico a que se establezca la conexión de IRC con iLO 2. Si el servidor cliente no recibe ninguna respuesta en ese tiempo, emite un mensaje de error.

Algunas posibles causas para la aparición de este mensaje son:

- La respuesta de red está retrasada.
- Se solicita una sesión de consola remota compartida, pero el líder de la sesión de la consola remota retrasa el envío de un mensaje de aceptación o denegación.

Para solucionar este problema, vuelva a intentar establecer la conexión IRC. Si es posible, corrija el retraso de la red y vuelva a intentar establecer conexión con IRC. Si la solicitud era para una sesión de consola remota compartida, intente ponerse en contacto con el líder de sesión y volver a intentar presentar la solicitud. Si la función Acquire (Adquirir) de la consola remota está activada, utilice el botón Acquire (Adquirir) en lugar de solicitar una sesión de consola remota compartida.

Los iconos de la barra de herramientas de IRC no se actualizan

Al conectar con IRC en iLO 2 versión 1.30, se instala un objeto IRC (subprograma iLO 2 Remote Console) en el explorador. El objeto incluye iconos de la barra de herramientas para nuevas funciones incluidas en iLO 2 versión 1.30. Al explorar a iLO 2 versión 1.29 o anterior, el objeto IRC no se sustituye por la versión incluida en el firmware anterior. Como resultado, los iconos de la barra de herramientas aparecen para funciones incluidas en iLO 2 versión 1.30 que no están disponibles en versiones anteriores. Si hace clic en un icono, es posible que aparezca un mensaje de error.

Para eliminar el objeto IRC de forma manual:

1. Desde un explorador Microsoft® Internet Explorer 6 browser, haga clic en **Herramientas>Opciones de Internet**.
2. Seleccione **Archivos temporales de Internet>Configuración**.
3. Haga clic en **Ver objetos**.
4. Haga clic con el botón secundario del ratón en **iLO 2 Remote Console Applet** y haga clic en **Quitar**.
5. Haga clic en **Aceptar** para quitar el objeto y, a continuación, en **Aceptar** para cerrar.

La interfaz GNOME no se bloquea

Al finalizar iLO 2 Remote Console o perder la conectividad de red de iLO 2 no se bloquea la interfaz GNOME cuando iLO 2 y la interfaz GNOME están configurados para la función Remote Console Lock (Bloqueo de la consola remota.)

El controlador de teclado de GNOME requiere un tiempo para procesar las secuencias de tecla que contienen pulsaciones de teclas de modificador. Este problema no se produce cuando las secuencias de teclas se introducen de forma manual a través de IRC, pero sí cuando iLO 2 envía la secuencia de teclas. ILO 2 envía la secuencia de teclas con modificador de pulsación de teclas más rápido de lo que el controlador de teclado GNOME es capaz de procesar.

Una solución para este problema consiste en utilizar la GUI de Linux KDE en lugar de GNOME. El controlador de pulsación de teclas KDE no necesita mucho tiempo para procesar las secuencias de teclas que contienen teclas de modificador. Las dos interfaces, KDE y GNOME, se suministran con todas las distribuciones de Linux.

Repetición de teclas en la consola remota

Al utilizar la consola remota bajo ciertas condiciones de latencia de red, puede registrar varias pulsaciones de tecla para una sola pulsación de tecla. Para obtener más información, consulte la sección "Configuración de la consola remota (Configuración de la consola remota en la página 91)".

La reproducción de la consola remota no funciona cuando el servidor host está apagado

Cuando está conectada a un servidor host apagado, la reproducción de la consola remota no funciona. Para acceder a los archivos de la consola remota grabados, encienda el servidor o conéctese a un iLO 2 en un servidor que esté encendido.

Solución de problemas de SSH y Telnet

Las siguientes secciones ilustran procedimientos de solución de problemas con SSH y telnet.

Entrada de PuTTY inicial lenta

Durante la conexión inicial con un sistema cliente PuTTY, se acepta una entrada lenta durante aproximadamente 5 segundos. Este problema puede solucionarse con la modificación de las opciones de configuración en el sistema cliente en las opciones de conexión TCP de bajo nivel. Debe desactivar la opción **Disable Nagle's algorithm (Desactivar algoritmo de Nagle)**. En las opciones de telnet, defina el modo de negociación de telnet como **Passive (Pasivo)**.

El sistema cliente PuTTY no responde con un puerto de red compartido

Cuando utilice un sistema cliente PuTTY con un puerto de red compartido, es posible que la sesión PuTTY no responda cuando se transfiera una gran cantidad de datos o cuando se utilice un puerto de serie virtual o una consola remota. Para solucionar este problema, cierre el sistema cliente PuTTY y vuelva a iniciar la sesión.

Soporte de texto SSH desde una sesión de consola remota

El acceso SSH y telnet desde la consola remota de texto admite la configuración estándar de 80 x 25 de pantalla de texto. Este modo es compatible con la consola remota de texto con la mayoría de interfaces de modo de texto disponibles en los sistemas operativos actuales. Si se utiliza telnet o SSH con una configuración de texto superior a 80 x 25, puede que no visualice el texto de forma correcta. HP recomienda configurar la aplicación de texto en modo 80 x 25 o utilizar el subprograma iLO 2 Remote Console suministrado con la interfaz Web.

Solución de problemas de servicios de Terminal Server

Las siguientes secciones ilustran procedimientos de solución de problemas con los servicios de Terminal Server.

El botón Terminal Services no funciona

La opción Terminal Services (Servicios de Terminal Server) no funcionará si está seleccionada la opción Deny (Denegar) en la advertencia de seguridad Java emergente. Al seleccionar la opción Deny, se indica al explorador que el subprograma Consola remota no es de confianza. La consola remota no podrá ejecutar ningún código que requiera un mayor nivel de confianza. Si está seleccionada la opción Deny, la consola remota no podrá ejecutar el código necesario para activar el botón Terminal Services (Servicios de Terminal Server.) En la consola Java aparecerá el mensaje `"Security Exception - Access denied" (Excepción de seguridad - Acceso denegado).`

El servidor Proxy de Terminal Services no responde

Siempre que se restablece iLO 2 (como, por ejemplo, cuando se cambia la configuración de la red o la configuración global), la función de transferencia de los servicios de Terminal Server deja de estar disponible durante dos minutos a partir del inicio del restablecimiento. iLO 2 requiere unos 60 segundos para completar el restablecimiento y POST, además de un tiempo de liberación de búfer de 60 segundos, antes de continuar. Transcurridos los dos minutos, el estado cambia a Available (Disponible) y la función de transferencia de los servicios de Terminal Server vuelve a estar disponible para su uso.

Solución de problemas de vídeo y monitor

En las secciones siguientes se abordan los elementos que deben tenerse en cuenta a la hora de resolver problemas de vídeo y monitor.

Directrices generales

- La resolución de la pantalla del cliente debe ser superior a la resolución de la pantalla del servidor remoto.
- La consola remota de iLO 2 sólo admite el chip de vídeo ATI Rage XL, integrado en el sistema. La consola remota de iLO 2 no funciona si se instala un complemento de tarjeta de vídeo. Todas las demás funciones de iLO 2 están disponibles si decide utilizar un complemento de tarjeta de vídeo.
- Sólo está permitido que acceda un usuario cada vez a la consola remota. Compruebe si algún otro usuario inició sesión en el sistema iLO 2.

Telnet se muestra incorrectamente en DOS®

Cuando se utiliza la sesión telnet de iLO 2 para mostrar pantallas de texto que implican una ventana de DOS® maximizada, la sesión Telnet no puede representar nada salvo la parte superior de la pantalla si la pantalla del servidor es mayor que 80x25.

Para corregirlo, ajuste las propiedades de las ventanas de DOS® para limitar su tamaño a 80x25 antes de maximizar la ventana de DOS.

- En la barra de título de la ventana de DOS®, haga clic con el botón secundario del ratón y seleccione **Properties (Propiedades)** y **Layout (Diseño)**.
- En la ficha Diseño, cambie el alto de Tamaño del búfer de pantalla a 25.

Las aplicaciones de vídeo no aparecen en la consola remota

Algunas aplicaciones de vídeo, como Microsoft® Media Player, no se muestran en la consola remota, o lo hacen incorrectamente. Este problema ocurre a menudo con aplicaciones que usan registros de superposiciones de vídeo. Normalmente, las aplicaciones que reproducen flujo de vídeo usan registros de superposiciones de vídeo. iLO 2 no se ha diseñado para utilizarla con este tipo de aplicaciones.

La interfaz de usuario no se visualiza correctamente

En los servidores ProLiant que utilizan Red Hat EL 4.0 y otros sistemas de Linux e iLO 2, el texto de los botones de la interfaz de usuario puede aparecer cortado por la parte inferior del botón. Este error se produce porque Mozilla Firefox no muestra el tamaño de texto que específica iLO 2 en los botones. Para visualizar el texto correctamente, seleccione **View (Ver)>Text Size (Tamaño de texto)>Decrease (Disminuir)** hasta que el texto aparezca correctamente.

Solución de problemas de Virtual Media

Las siguientes secciones ilustran procedimientos de solución de problemas con Virtual Media (Soportes virtuales.)

El subprograma Virtual Media tiene una X roja y no se visualiza

Puede que el subprograma Virtual Media produzca una X roja si se utiliza un explorador o JVM no compatibles o si la opción Habilitar todos las cookies no está activada. Para corregir este problema, asegúrese de que se usa un explorador y una versión de JVM compatibles en el sistema cliente. Para ello, revise la matriz de soporte de la sección "Sistemas operativos cliente y exploradores compatibles" (Sistemas operativos cliente y exploradores compatibles en la página 7.) Asegúrese, además, que la opción Enable All Cookies (Habilitar todos las cookies) está seleccionada en el menú de opciones o de preferencias del explorador. Algunos exploradores no tienen activadas las cookies de forma predeterminada.

El subprograma Virtual Floppy Media no responde

El subprograma de soportes iLO 2 Virtual Floppy (Disquete virtual) puede no responder cuando la unidad de disquete contenga errores de soporte.

Para evitar que el subprograma de soporte de disquete virtual no responda, ejecute el archivo CHKDSK.EXE (o alguna otra función similar) para comprobar si el soporte de disquete presenta errores. En caso de que el soporte físico contenga errores, vuelva a cargar la imagen del disquete en un disquete nuevo.

Solución de problemas del reproductor de vídeo iLO

Las siguientes secciones ilustran procedimientos de solución de problemas con el reproductor de vídeo iLO.

El archivo de captura de vídeo no se reproduce

Compruebe que el archivo sea una captura de iLO 2 de HP válida y que no se encuentre dañado.

El archivo de captura de vídeo no se reproduce de manera correcta

Los archivos de captura de iLO 2 son grabaciones de la actividad de la pantalla. Durante períodos prolongados de actividad de la pantalla, la inactividad grabada se trunca para reducir el tamaño del archivo y mejorar el rendimiento de la reproducción. Esto puede provocar que la reproducción parezca que se inicia y se detiene o que se reproduzca de manera incorrecta.

Solución de problemas de la consola de texto remota

En las secciones siguientes se abordan los elementos que deben tenerse en cuenta a la hora de resolver problemas de la consola de texto remota.

Visualización del instalador de Linux en la consola de texto

Cuando se instala Linux mediante la consola de texto, es posible que la pantalla de instalación inicial no se visualice debido a que la pantalla se encuentra en modo de gráficos. Para corregir esto y continuar con la instalación, lleve a cabo una de las siguientes acciones:

- En la mayoría de versiones de Linux, introduzca `linux text nofb`. Los caracteres que introduzca no se visualizarán. Si se introduce el comando correctamente, la pantalla cambiará del modo de gráficos al modo de texto mientras se visualiza la pantalla.
- En SLES 9 y SLES 10, pulse ciegamente **F2** y ↓ (flecha hacia abajo) desde la consola de texto. Si se lleva a cabo esta acción correctamente, se seleccionará el modo de texto y aparecerá la pantalla.

Traspaso de datos a través de un terminal SSH

Si utiliza un terminal SSH para acceder a la consola de texto, es posible que SSH intercepte los datos de pulsación de teclas y no pase la acción a la consola de texto. Cuando se produce esto, parece como si la pulsación de teclas no llevase a cabo su función. Para corregir este problema, desactive los accesos directos del terminal SSH.

Solución de problemas diversos

En las secciones siguientes se describen diversos problemas de hardware o software.

Uso compartido de cookies entre instancias del explorador e iLO 2

iLO 2 utiliza cookies de sesión de explorador en parte para distinguir inicios de sesión independientes (cada ventana del explorador muestra un inicio de sesión de usuario independiente) al tiempo que comparte la misma sesión activa con iLO 2. Estos inicios de sesión múltiples pueden confundir al explorador. Esta confusión puede aparecer como un problema de iLO 2; sin embargo, se trata de una manifestación del comportamiento típico del explorador.

Un explorador puede abrir ventanas adicionales debido a varios procesos. Las ventanas de explorador abiertas desde un explorador abierto representan distintos aspectos del mismo programa en la memoria. En consecuencia, cada ventana de explorador comparte propiedades con la ventana principal, incluidas las cookies.

Instancias compartidas

Cuando iLO 2 abre otra ventana de explorador (por ejemplo, la ventana de consola remota, de soportes virtuales o de ayuda), esta ventana comparte la misma conexión a iLO 2 y la cookie de sesión.

El servidor Web de iLO 2 toma decisiones en materia de direcciones URL basándose en cada solicitud que recibe. Por ejemplo, si una solicitud no tiene derechos de acceso, se abre la página de inicio de sesión, independientemente de la solicitud original. El redireccionamiento basado en servidor web, que se obtiene mediante la selección de **File (Archivo)>New (Nuevo)>Window (Ventana)** o pulsando las teclas **Ctrl+N**, permite abrir una instancia duplicada del explorador original.

Comportamiento del orden de cookies

Durante el inicio de sesión, la página de inicio de sesión genera una cookie de sesión de explorador que enlaza la ventana a la sesión apropiada en el firmware. El firmware realiza un seguimiento de los inicios de sesión del explorador como sesiones individuales que aparecen en la sección Active Sessions (Sesiones activas) de la página de estado de iLO 2.

Por ejemplo, cuando el Usuario1 inicia sesión, el servidor Web genera la vista de marcos inicial, con el usuario actual Usuario1 en el panel superior, los elementos de menú en el panel izquierdo y los datos de la página en el panel inferior derecho. Cuando el usuario Usuario1 hace clic en los distintos enlaces, sólo se actualizan los elementos de menú y los datos de la página.

Si mientras está conectado el Usuario1 otro usuario, Usuario2, abre otra ventana de explorador en el mismo cliente e inicia sesión, el segundo inicio de sesión sobrescribe la cookie generada en la sesión original de Usuario1. Suponiendo que el Usuario2 es otra cuenta de usuario, se genera otro marco y se abre una nueva sesión. La segunda sesión se muestra en la sección Active Sessions (Sesiones activas) de la página de estado de iLO 2 como current user: User2 (usuario actual: Usuario2.)

El segundo inicio de sesión sustituye efectivamente la primera sesión (Usuario1) borrando la cookie generada durante el inicio de sesión de Usuario1. Este comportamiento equivale a cerrar el explorador de Usuario1 sin hacer clic en el enlace Cerrar sesión. La sesión huérfana de Usuario1 se reclama cuando transcurre el tiempo de espera de la sesión.

Dado que el marco de usuario actual no se actualiza a menos que el explorador se vea forzado a actualizar toda la página, Usuario1 puede seguir navegando mediante su ventana de explorador. Sin embargo, el explorador funciona ahora usando la configuración de cookies de la sesión de Usuario2, incluso si no resulta aparente.

Si Usuario1 continúa navegando en este modo (Usuario1 y Usuario2 comparten el mismo proceso porque Usuario2 inició sesión y reinició la cookie de sesión), pueden darse las siguientes situaciones:

- La sesión de Usuario1 se comporta de manera coherente con los privilegios asignados a Usuario2.
- La actividad de Usuario1 mantiene activa la sesión de Usuario2, pero ésta puede interrumpirse de manera inesperada.

- Si se termina la sesión en cualquiera de las dos ventanas, ambas sesiones finalizarán. La siguiente actividad en la otra ventana puede redirigir al usuario a la página de inicio de sesión si se supera el tiempo de espera de la sesión o se supera el tiempo de espera de manera prematura.
- Al hacer clic en Log Out (Finalizar sesión) en la segunda sesión (User2), se muestra el mensaje `Logging out: unknown page to display before redirecting the user to the login page (Finalizando sesión: se visualizará una página desconocida antes de redireccionar al usuario a la página de inicio de sesión).`
- Si Usuario2 cierra sesión y, a continuación, inicia de nuevo sesión como Usuario3, Usuario1 asume la sesión de Usuario3.
- Si Usuario1 está a punto de iniciar sesión y Usuario2 ya ha iniciado sesión, Usario1 puede cambiar la dirección URL para redirigir a la página de índice. Parece que Usuario1 ha accedido a iLO 2 sin iniciar sesión.

Estos comportamientos se mantienen mientras estén abiertas las ventanas duplicadas. Todas las actividades se atribuyen al mismo usuario, mediante el conjunto de cookies de la última sesión.

Visualización de la cookie de sesión actual

Tras iniciar sesión, se puede obligar al explorador a mostrar la cookie de sesión actual escribiendo `javascript:alert(document.cookie)` en la barra de direcciones URL. El primer campo visible es el ID de la sesión. Si este ID es el mismo en las diferentes ventanas de explorador, esas ventanas están compartiendo la misma sesión de iLO 2.

Puede obligar al explorador a actualizar y revelar su verdadera identidad pulsando la tecla **F5**, seleccionando **Ver**>**Actualizar** o mediante el botón Actualizar.

Prevención de problemas relacionados con las cookies

Para evitar los problemas de comportamiento relacionados con las cookies:

- Inicie un nuevo explorador por cada inicio de sesión haciendo doble clic en el icono o acceso directo del explorador.
- Haga clic en el enlace **Log Out (Cerrar sesión)** para cerrar la sesión de iLO 2 antes de cerrar la ventana del explorador.

Imposibilidad de acceder a las descargas de ActiveX

Si su red no permite controles de ActiveX, puede capturar DVC.DLL desde un sistema único y distribuir después el archivo a los equipos cliente de la red.

1. Inicie una sesión en iLO 2.
2. Escriba **https://ilo_name/dvc.cab** en la barra de dirección del explorador.
3. Aparecerá el cuadro de diálogo de descarga de archivos. Haga clic en **Abrir** y guarde el archivo DVC.DLL en su unidad local.
4. Copie el archivo DVC.DLL en el sistema cliente que no permite las descargas de ActiveX.
5. Desde este sistema cliente, abra una ventana de línea de comandos. Acceda al directorio que contiene el archivo DVC.DLL y escriba `regsvr32 dvc.dll`.

Imposibilidad de recibir información SNMP desde HP SIM

Los agentes que se ejecutan en el servidor administrado suministran información SNMP a HP SIM. Para que los agentes puedan pasar información a través de iLO 2, es preciso que estén instalados los

controladores de dispositivos iLO 2. Consulte la sección “Instalación de los controladores del dispositivo iLO 2” para obtener instrucciones de instalación.

Si instaló los controladores y los agentes para iLO 2, compruebe que iLO 2 y el equipo de gestión se encuentran en la misma subred. Puede comprobarlo rápidamente si solicita eco para iLO 2 desde el equipo de gestión. Consulte al administrador de red para conocer las rutas correctas de acceso a la interfaz de red de iLO 2.

La fecha o la hora de las entradas del registro de sucesos es incorrecta

Puede actualizar la hora y la fecha en iLO 2 si ejecuta la utilidad RBSU. Esta utilidad establece automáticamente la hora y la fecha del procesador según las del servidor. Los agentes de Insight Management también pueden actualizar estos datos en los sistemas operativos de red admitidos.

Imposibilidad de actualizar el firmware de la placa iLO 2

Si desea actualizar el firmware de la placa iLO 2 y éste no responde, no acepta la actualización de firmware o finaliza antes de que le lleve a cabo con éxito la actualización, utilice una de las siguientes opciones para restaurar el firmware de la placa iLO 2. Consulte la guía de recursos de líneas y secuencias de comandos de iLO 2 para obtener información sobre el uso de las funciones de las secuencias de comandos de iLO 2.

- **Actualización en línea del firmware**: descargue este componente y ejecútelo desde el contexto raíz o Administrador de un sistema operativo compatible. Este software se ejecuta en el sistema operativo del host y actualiza el firmware de iLO 2 sin necesidad de iniciar una sesión en iLO 2.
- **Actualización de firmware sin conexión para mantener SmartStart**: descargue el componente que desee utilizar con el CD de mantenimiento de firmware de SmartStart en la utilidad de actualización de ROM de la ficha Maintenance (Mantenimiento.) Estos componentes también pueden utilizarse con HP Drive K Boot Utility.
- **CD-ROM de mantenimiento de firmware**: descargue el componente para crear un CD-ROM ejecutable que contenga muchas actualizaciones de firmware para servidores y opciones de ProLiant.
- **Secuencias de comandos con CPQLOCFG**: descargue el componente CPQLOCFG para obtener la utilidad de secuencia de comandos basada en red, CPQLOCFG. CPQLOCFG permite utilizar secuencias de comandos RIBCL que realizan de forma segura en la red actualizaciones de firmware, configuración de iLO 2 y operaciones de iLO 2 en masa. Los usuarios de Linux deben revisar las muestras de secuencias de comandos PERL y XML de HP Lights-Out para Linux.
- **Secuencias de comandos con HPONCFG**: descargue el componente HPONCFG para obtener la utilidad de secuencias de comandos basada en host, HPONCFG. Esta utilidad permite utilizar secuencias de comandos RIBCL que realizan actualizaciones de firmware, configuración del procesador de LOM y operaciones en masa, desde un Administrador o acceso a una cuenta raíz en los sistemas operativos del host admitidos.
- **Compatibilidades de directorios HP para procesadores de gestión**: descargue el componente para obtener los componentes de compatibilidad de directorios. Uno de los componentes, HPLOMIG, puede utilizarse para descubrir los procesadores iLO, iLO 2, RILOE y RILOE II y actualizar el firmware. No tiene que utilizar la integración de directorios para aprovechar esta funcionalidad.

Pasos de diagnóstico

Antes de intentar una recuperación de memoria flash del firmware, use los pasos de diagnóstico siguientes para comprobar si es necesario realizarla:

1. Intente conectase a la placa iLO 2 mediante el explorador Web. Si no puede conectar, existe un problema de comunicación.
2. Intente sondear el ping de iLO 2. Si tiene éxito, la red funcionará.

iLO 2 no responde a las solicitudes SSL

iLO 2 no responde a las solicitudes SSL cuando aparece una advertencia de Java™. Si un usuario inicia la sesión en una conexión de explorador iLO 2 y no completa el proceso respondiendo a la advertencia de certificación Java, el explorador iLO 2 no responderá a futuras solicitudes del explorador. El usuario deberá continuar el proceso de inicio de sesión para liberar el servidor Web iLO 2.

Comprobación de SSL

La siguiente comprobación verifica si aparece el cuadro de diálogo de seguridad correcto. Los servidores que no funcionen correctamente mostrarán el mensaje `No se puede mostrar la página`. Si esta prueba falla, querrá decir que el controlador de dominio no acepta las conexiones SSL y que probablemente no disponga de ninguna certificación.

1. Abra un explorador y vaya a la página <https://<*controlador de dominio*>:636.

   Puede utilizar el <*dominio*> en lugar del <*controlador de dominio*> que se envía al DNS y comprueba qué controlador de dominio gestiona las solicitudes del dominio. Compruebe varios controladores de dominio para verificar que todos dispongan de certificación.

2. Si SSL funciona correctamente en el controlador de dominio (dispone de certificación), aparecerá un mensaje de seguridad preguntando si desea continuar accediendo al sitio o si desea visualizar el certificado del servidor. Si hace clic en **Sí** no aparecerá ninguna página Web. Se trata de una situación normal. Este proceso es automático; sin embargo, requiere reiniciar el sistema. Para evitar reiniciar el sistema:

   a. Abra MMC y añada el complemento de certificado. Cuando se le solicite, seleccione **Computer Account (Cuenta de sistema)** para el tipo de certificado que desee ver. Haga clic en **OK (Aceptar)** para volver al complemento de certificados.

   b. Seleccione la carpeta **Personal>Certificates**. Haga clic con el botón derecho del ratón sobre la carpeta y seleccione **Request New Certificate (Solicitar nuevo certificado)**.

   c. Asegúrese de que el tipo es el controlador de dominio y haga clic en **Next (Siguiente)** hasta que se use un certificado.

También puede utilizar la herramienta Microsoft® LDP para comprobar las conexiones SSL. Para obtener más información sobre la herramienta LDP, vaya al sitio web de Microsoft® (http://www.microsoft.com/support.)

Un certificado antiguo puede causar problemas con SSL en el direccionamiento del controlador de dominio si apunta a un CA aprobado anteriormente con el mismo nombre. Esta situación es muy poco común, aunque se podría producir si se añadiera un servicio de certificación y se eliminara, a continuación, para luego volver a añadirlo en el controlador de dominio. Para eliminar los certificados anteriores y emitir uno nuevo, siga las instrucciones descritas en el paso 2.

Reinicio de iLO 2

En raras ocasiones, quizás sea necesario reiniciar iLO 2. Por ejemplo, si iLO 2 no responde al explorador. Para reiniciar iLO 2, desconecte completamente el servidor y el suministro de alimentación.

iLO 2 puede reiniciarse automáticamente en determinadas ocasiones. Por ejemplo, un temporizador de protección interno de iLO 2 se reiniciará si el firmware detecta un problema en iLO 2. Si se completa una actualización de firmware o se cambia un valor de red, el sistema iLO 2 también se reiniciará.

Los agentes de HP Insight Manager 5.40 de HP y posteriores pueden reiniciar iLO 2. Para reiniciar iLO 2, seleccione una de estas acciones:

- En la sección iLO 2 de la página Web de los agentes de gestión de HP, seleccione la opción **Reset** iLO 2 (Reiniciar iLO 2.)
- Haga clic en **Apply (Aplicar)** de la página Network Settings (Configuración de red) para obligar al procesador de gestión de iLO 2 a reiniciarse. No es necesario que cambie ningún parámetro antes de hacer clic en Apply.
- Haga clic en **Reset (Reiniciar)** de la página Diagnostic (Diagnóstico) de la interfaz del explorador de iLO 2.

El nombre del servidor se conserva tras ejecutar la utilidad ERASE

El campo Server Name (Nombre de servidor) se comunica a iLO 2 a través de los agentes de Insight Manager.

Para borrar el campo Server Name (Nombre de servidor) tras una redistribución de un servidor, realice una de las siguientes opciones:

- Cargue los agentes de Insight Manager para actualizar el campo Server Name (Nombre de servidor) con un nombre de servidor nuevo.
- Utilice la función Reset to Factory Defaults (Reiniciar a valores predeterminados) de la utilidad RBSU de iLO 2 para borrar el campo Server Name (Nombre de servidor.)

  Mediante este procedimiento se quita toda la información de configuración de iLO 2 y no sólo la información del campo Server Name.
- Cambie el nombre del servidor en la página Administration (Administration)>Access (Acceso) >Options (Opciones) en la interfaz del explorador de iLO 2.

Solución de problemas de un host remoto

La solución de problemas de un host remoto puede requerir el reinicio del sistema remoto. Puede reiniciar fácilmente el servidor host remoto con las opciones que figuran en la ficha Virtual Devices (Soportes virtuales.)

10 Esquema de los servicios de directorio

En esta sección:

Principales clases y atributos OID del protocolo LDAP de gestión de HP

Algunos de los cambios realizados durante el proceso de configuración de esquema se realizan en:

- Principales clases (Principales clases en la página 238)
- Principales atributos (Principales atributos en la página 238)

Principales clases

Nombre de clase	OID asignado
hpqTarget	1.3.6.1.4.1.232.1001.1.1.1.1
hpqRole	1.3.6.1.4.1.232.1001.1.1.1.2
hpqPolicy	1.3.6.1.4.1.232.1001.1.1.1.3

Principales atributos

Nombre de atributo	OID asignado
hpqPolicyDN	1.3.6.1.4.1.232.1001.1.1.2.1
hpqRoleMembership	1.3.6.1.4.1.232.1001.1.1.2.2
hpqTargetMembership	1.3.6.1.4.1.232.1001.1.1.2.3
hpqRoleIPRestrictionDefault	1.3.6.1.4.1.232.1001.1.1.2.4
hpqRoleIPRestrictions	1.3.6.1.4.1.232.1001.1.1.2.5
hpqRoleTimeRestriction	1.3.6.1.4.1.232.1001.1.1.2.6

Definición de las principales clases

A continuación figura la definición de las principales clases de gestión de HP.

hpqTarget

OID	1.3.6.1.4.1.232.1001.1.1.1.1
Descripción	Esta clase define los objetos Target, estableciendo la base para que los productos HP puedan usar la gestión habilitada por directorio.
Tipo de clase	Estructural
Superclases	usuario
Atributos	hpqPolicyDN—1.3.6.1.4.1.232.1001.1.1.2.1 hpqRoleMembership—1.3.6.1.4.1.232.1001.1.1.2.2
Comentarios	Ninguno

hpqRole

OID	1.3.6.1.4.1.232.1001.1.1.1.2
Descripción	Esta clase define los objetos Role, estableciendo la base para que los productos HP puedan usar la gestión habilitada por directorio.
Tipo de clase	Estructural
Superclases	group
Atributos	hpqRoleIPRestrictions—1.3.6.1.4.1.232.1001.1.1.2.5 hpqRoleIPRestrictionDefault—1.3.6.1.4.1.232.1001.1.1.2.4 hpqRoleTimeRestriction—1.3.6.1.4.1.232.1001.1.1.2.6 hpqTargetMembership—1.3.6.1.4.1.232.1001.1.1.2.3
Comentarios	Ninguno

hpqPolicy

OID	1.3.6.1.4.1.232.1001.1.1.1.3
Descripción	Esta clase define los objetos Policy, estableciendo la base para que los productos HP puedan usar la gestión habilitada por directorio.
Tipo de clase	Estructural
Superclases	top
Atributos	hpqPolicyDN—1.3.6.1.4.1.232.1001.1.1.2.1
Comentarios	Ninguno

Definición de los principales atributos

A continuación figura la definición de los principales atributos de clases de gestión de HP.

hpqPolicyDN

OID	1.3.6.1.4.1.232.1001.1.1.2.1
Descripción	Nombre completo de la directiva que controla la configuración general de este destino.
Sintaxis	Nombre completo—1.3.6.1.4.1.1466.115.121.1.12
Opciones	De un solo valor.
Comentarios	Ninguno

hpqRoleMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.2
Descripción	Proporciona una lista de objetos hpqTarget a los que pertenece este objeto.
Sintaxis	Nombre completo—1.3.6.1.4.1.1466.115.121.1.12
Opciones	De varios valores.
Comentarios	Ninguno

hpqTargetMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.3
Descripción	Proporciona una lista de objetos hpqTarget que pertenecen a este objeto.
Sintaxis	Nombre completo—1.3.6.1.4.1.1466.115.121.1.12
Opciones	De varios valores.
Comentarios	Ninguno

hpqRoleIPRestrictionDefault

OID	1.3.6.1.4.1.232.1001.1.1.2.4
Descripción	Cadena booleana que representa el acceso por clientes no especificados y que especifica parcialmente restricciones de los derechos en una restricción de dirección de red IP
Sintaxis	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Opciones	De un solo valor.
Comentarios	Si el valor de este atributo es TRUE, las restricciones IP se cumplirán para los clientes de red ordinarios. Si el valor de este atributo es FALSE, las restricciones IP no se cumplirán para los clientes de red ordinarios.

hpqRoleIPRestrictions

OID	1.3.6.1.4.1.232.1001.1.1.2.5
Descripción	Proporciona una lista de direcciones IP, nombres DNS, intervalos de direcciones de dominio y subredes que especifican parcialmente restricciones de los derechos en una restricción de dirección de red IP.
Sintaxis	Cadena de octeto—1.3.6.1.4.1.1466.115.121.1.40
Opciones	De varios valores.
Comentarios	Este atributo se usa únicamente en los objetos de función. Las restricciones IP se cumplen cuando la dirección coincide y se deniega el acceso general; no se cumplen cuando la dirección coincide y se permite el acceso general. Los valores son un byte identificador seguido de un número de bytes específico del tipo que indica una dirección de red. • Para las subredes IP, el identificador es <0x01>, seguido de la dirección de red IP en el orden de red, seguida de la máscara de subred IP en el orden de red. Por ejemplo, la subred IP 127.0.0.1/255.0.0.0 se representaría como <0x01 0x7F 0x00 0x00 0x01 0xFF 0x00 0x00 0x00>. Para los intervalos IP, el identificador es <0x02>, seguido de la dirección IP de límite mínimo, seguida de la dirección IP de límite máximo. Ambas son inclusivas y están en el orden de red; por ejemplo, el intervalo IP 10.0.0.1 a 10.0.10.255 se representaría como <0x02 0x0A 0x00 0x00 0x01 0x0A 0x00 0x0A 0xFF> • Para los nombres DNS o dominios, el identificador es <0x03>, seguido del nombre DNS codificado en ASCII. Los nombres DNS pueden llevar el prefijo * (ASCII 0x2A) para indicar que deben corresponder a todos los nombres que terminan con la cadena especificada: por ejemplo, el dominio DNS *.acme.com se representa como <0x03 0x2A 0x2E 0x61 0x63 0x6D 0x65 0x2E 0x63 0x6F 0x6D>. Se permite el acceso general.

hpqRoleTimeRestriction

OID	1.3.6.1.4.1.232.1001.1.1.2.6
Descripción	Una cuadrícula horaria de siete días, con una resolución de 30 minutos, que especifica las restricciones de los derechos en una restricción de tiempo.
Sintaxis	Cadena de octeto {42}—1.3.6.1.4.1.1466.115.121.1.40
Opciones	De un solo valor.
Comentarios	Este atributo se usa únicamente en los objetos ROLE.

Las restricciones de tiempo se cumplen cuando el bit correspondiente a la actual hora real local del dispositivo es 1 y no se cumple cuando el bit es 0.

- El bit menos significativo del primer byte corresponde al período de tiempo comprendido entre la medianoche del domingo y las 12:30 a.m.
- Cada bit más significativo y cada byte secuencial se corresponden al siguiente bloque de media hora de la semana.
- El bit más significativo (octavo) del byte 42 corresponde al período de tiempo comprendido entre las 11:30 p.m. del sábado hasta la medianoche del domingo.

Clases y atributos OID del protocolo LDAP específicos de la gestión de Lights-Out

Los siguientes atributos y clases de esquema pueden depender de los atributos o clases definidos en la sección Principales clases y atributos de gestión de HP.

Clases de gestión de Lights-Out

Nombre de clase	OID asignado
hpqLOMv100	1.3.6.1.4.1.232.1001.1.8.1.1

Atributos de gestión de Lights-Out

Nombre de clase	OID asignado
hpqLOMRightLogin	1.3.6.1.4.1.232.1001.1.8.2.1
hpqLOMRightRemoteConsole	1.3.6.1.4.1.232.1001.1.8.2.2
hpqLOMRightVirtualMedia	1.3.6.1.4.1.232.1001.1.8.2.3
hpqLOMRightServerReset	1.3.6.1.4.1.232.1001.1.8.2.4
hpqLOMRightLocalUserAdmin	1.3.6.1.4.1.232.1001.1.8.2.5
hpqLOMRightConfigureSettings	1.3.6.1.4.1.232.1001.1.8.2.6

Definición de las clases de gestión de Lights-Out

A continuación figura la definición de la principal clase de gestión de Lights-Out.

hpqLOMv100

OID	1.3.6.1.4.1.232.1001.1.8.1.1
Descripción	Esta clase define los derechos y valores de configuración que se usan con los productos de gestión de Lights-Out de HP.
Tipo de clase	Auxiliar

Superclases	Ninguno
Atributos	hpqLOMRightConfigureSettings—1.3.6.1.4.1.232.1001.1.8.2.1 hpqLOMRightLocalUserAdmin—1.3.6.1.4.1.232.1001.1.8.2.2 hpqLOMRightLogin—1.3.6.1.4.1.232.1001.1.8.2.3 hpqLOMRightRemoteConsole—1.3.6.1.4.1.232.1001.1.8.2.4 hpqLOMRightServerReset—1.3.6.1.4.1.232.1001.1.8.2.5 hpqLOMRightVirtualMedia—1.3.6.1.4.1.232.1001.1.8.2.6
Comentarios	Ninguno

Definición de los atributos de gestión de Lights-Out

A continuación figura la definición de los principales atributos de clases de gestión de Lights-Out.

hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.1
Descripción	Derecho de inicio de sesión para los productos de gestión de Lights-Out de HP
Sintaxis	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Opciones	De un solo valor.
Comentarios	Tiene sentido únicamente en los objetos ROLE. Si su valor es TRUE, se concede el derecho a los miembros de la función.

hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.2
Descripción	Derecho de consola remota para los productos de gestión de Lights-Out. Tiene sentido únicamente en los objetos ROLE.
Sintaxis	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Opciones	De un solo valor.
Comentarios	Este atributo se usa únicamente en los objetos ROLE. Si el valor de este atributo es TRUE, se concede el derecho a los miembros de la función.

hpqLOMRightVirtualMedia

OID	1.3.6.1.4.1.232.1001.1.8.2.3
Descripción	Derecho de soportes virtuales para los productos de gestión de Lights-Out de HP
Sintaxis	Boolean—1.3.6.1.4.1.1466.115.121.1.7

Opciones	De un solo valor.
Comentarios	Este atributo se usa únicamente en los objetos ROLE. Si el valor de este atributo es TRUE, se concede el derecho a los miembros de la función.

hpqLOMRightServerReset

OID	1.3.6.1.4.1.232.1001.1.8.2.4
Descripción	Derecho de reinicio del servidor remoto y derecho del botón de alimentación para los productos de gestión de Lights-Out de HP
Sintaxis	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Opciones	De un solo valor.
Comentarios	Este atributo se usa únicamente en los objetos ROLE. Si el valor de este atributo es TRUE, se concede el derecho a los miembros de la función.

hpqLOMRightLocalUserAdmin

OID	1.3.6.1.4.1.232.1001.1.8.2.5
Descripción	Derecho de administración de la base de datos de usuarios locales para los productos de gestión de Lights-Out de HP
Sintaxis	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Opciones	De un solo valor.
Comentarios	Este atributo se usa únicamente en los objetos ROLE. Si el valor de este atributo es TRUE, se concede el derecho a los miembros de la función.

hpqLOMRightConfigureSettings

OID	1.3.6.1.4.1.232.1001.1.8.2.6
Descripción	Derecho de configuración de los dispositivos para los productos de gestión de Lights-Out de HP
Sintaxis	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Opciones	De un solo valor.
Comentarios	Este atributo se usa únicamente en los objetos ROLE. Si el valor de este atributo es TRUE, se concede el derecho a los miembros de la función.

11 Asistencia técnica

En esta sección:

Información sobre compatibilidad

iLO Advanced Pack de HP e iLO Advanced Pack de HP para BladeSystem incluido con conjuntos Insight Control e iLO Power Management Pack incluyen un servicio de actualización y soporte técnico las 24 horas del día los 7 días de la semana de software HP. Este servicio permite acceder a los recursos técnicos de HP que ofrecen ayuda para resolver problemas de funcionamiento o implementación de software. Además, este servicio permite acceder a actualizaciones de software y manuales de referencia en formato electrónico o de soporte físico que HP pone a su disposición.

HP ofrece asistencia técnica para productos y actualizaciones de productos para iLO Advanced de HP e iLO Advanced Pack de HP para clientes de BladeSystem de dos maneras:

- Al adquirir licencias individuales, recibirá soporte que cubre el inicio del software técnico sin ningún cargo adicional llamando al servicio técnico de HP hasta 90 días a partir de la fecha de compra. Se ofrece asistencia telefónica en la que se ayuda a los clientes en la instalación y configuración, así como en las preguntas referentes a las secuencias fijas y a sus respectivos usos. En la página Web de HP (http://www.hp.com/country/us/en/support.html) se incluyen los números de teléfono del servicio técnico en todo el mundo. Es posible comprar actualizaciones por separado según su criterio.
- Cuando se obtienen iLO Advanced Pack de e iLO Advanced Pack de HP para BladeSystem con la compra de un conjunto Insight Control e iLO Power Management Pack, las licencias incluyen un año de servicio de actualización y soporte técnico las 24 horas del día los 7 días de la semana de software HP.

  Con la asistencia técnica y el servicio de actualización incluidos,iLO Advanced Pack de HP e iLO Advanced Pack de HP para los clientes de BladeSystem se aprovechan de la rápida resolución de problemas y la notificación y entrega proactiva de las actualizaciones de software de iLO Advanced e iLO Select. Para obtener más información, consulte la página Web de HP (http://www.hp.com/go/ilo), seleccione el producto deseado y consulte las especificaciones rápidas.

  Para activar el servicio de actualización y soporte técnico de software HP para iLO Advanced e iLO Select, debe registrar la compra del software en la página Web de HP (http://www.hp.com/go/ilo.) **Si no se consigue registrar el servicio se pone en peligro el cumplimiento del servicio**.

  Después del registro se le entrega el identificador de acuerdo de servicio (SAID, Service Agreement Identifier.) Después de haber recibido el SAID, puede ir a la página Web del gestor de actualizaciones de software (SUM) para ver el contrato y elegir la entrega electrónica (además de las actualizaciones estándar basadas en soporte.) Para obtener más información sobre este servicio, consulte la página Web de HP (http://www.hp.com/services/insight.)

HP también ofrece un gran número de servicios de asistencia técnica de software adicionales. Muchos de ellos se suministran sin cargo adicional.

- Soporte que cubre el inicio del software técnico: se ofrece asistencia telefónica para ayudarle a efectuar la instalación básica, la configuración y las preguntas acerca de la utilización. Este soporte es ofrecido por el experto equipo de especialistas de Insight Control Management de HP y Systems Insight Manager y se encuentra disponible sin cargo adicional hasta 90 días a partir de la fecha de compra del servidor. Para obtener asistencia técnica en EE. UU., llame al teléfono
- 1-800-HP-INVENT (1-800-474-6836.) (Cuando se le indique, diga "Insight Manager, P2P o SMP".) En la página Web de HP (http://www.hp.com/country/us/en/wwcontact.html) se encuentran disponibles los números de teléfono del servicio técnico en todo el mundo de HP.
- Únase al debate (http://forums.itrc.hp.com): el foro de asistencia técnica de HP es una herramienta basada en la comunidad y protagonizada por los usuarios que está diseñada para que los clientes de HP puedan debatir acerca de los productos de HP. Para debatir acerca del software Insight Control e Insight Essentials, haga clic en **Management Software and System Tools (Software de gestión y herramientas del sistema)**.
- Páginas de descarga de software y controladores (http://www.hp.com/support): en estas páginas se ofrece el software y los controladores más recientes para los productos ProLiant.
- Seguridad de la gestión (http://www.hp.com/servers/manage/security): HP se muestra proactivo en su enfoque de la calidad y seguridad de todos sus software de gestión. Asegúrese de visitar este sitio web a menudo para obtener las actualizaciones de seguridad que se pueden descargar más recientes.
- Obtenga la versión más reciente de SmartStart (http://www.hp.com/servers/smartstart): es posible descargar los CD de SmartStart, Management y Firmware siguiendo un proceso de registro simple desde la página Web de SmartStart. Para recibir kits físicos con cada versión, es posible solicitar kits de versión individuales desde la página Web de SmartStart. Para recibir notificaciones proactivas cuando se encuentren disponibles las versiones de SmartStart, suscríbase a Subscriber's Choice (Elección del suscriptor) (http://www.hp.com/go/subscriberschoice.)

Información de contacto de HP

Para conocer el nombre del distribuidor autorizado de HP más cercano:

- Consulte la página Web de contacto de HP (en inglés) (http://welcome.hp.com/country/us/en/wwcontact.html.)

Para dirigirse al servicio técnico de HP:

- En los Estados Unidos, consulte las opciones de contacto en la página Web de contacto de HP de los Estados Unidos (http://welcome.hp.com/country/us/en/contact_us.html.) Para ponerse en contacto con HP vía telefónica:
  - Llame al 1-800-HP-INVENT (1-800-474-6836.) Este servicio está disponible 24 horas al día, 7 días a la semana. Para una mejora continua de la calidad, las llamadas pueden ser grabadas o supervisadas.
  - Si ha adquirido un Care Pack (actualización de servicios), llame al 1-800-633-3600. Para obtener más información acerca de los Care Pack, consulte la página Web de HP (http://www.hp.com/hps.)
- En los demás países/regiones, consulte la página Web de contacto de HP (en inglés) (http://welcome.hp.com/country/us/en/wwcontact.html.)

Antes de ponerse en contacto con HP

Antes de llamar a HP, compruebe que dispone de la información siguiente:

- Número de registro de asistencia técnica (si corresponde)
- Número de serie del producto
- Modelo y número del producto
- Número de referencia del producto
- Mensajes de error correspondientes
- Tarjetas o hardware adicionales
- Hardware o software de otros fabricantes
- Tipo y revisión del sistema operativo

Siglas y abreviaturas

ACPI Advanced Configuration and Power Interface (Interfaz avanzada de alimentación y configuración)

ARP Address Resolution Protocol (Protocolo de resolución de direcciones)

ASCII American Standard Code for Information Interchange (Código americano convencional para intercambio de información)

ASM Advanced Server Management (Gestión avanzada de servidores)

ASR Automatic Server Recovery (Recuperación automática del servidor)

BMC baseboard management controller (controlador de administración de placa base)

CA Certificate Authority (Entidad emisora de certificados)

CLI Command Line Interface (Interfaz de línea de comando)

CLP command line protocol (protocolo de líneas de comandos)

CLUF End user license agreement (contrato de licencia del usuario final)

CR Certificate Request (Solicitud de certificado)

CRL certificate revocation list (lista de revocaciones de certificados)

DAV Distributed Authoring and Versioning (Versiones y autores distribuidos)

DDNS Dynamic Domain Name System (Sistema de nombres de dominio dinámico)

DHCP Dynamic Host Configuration Protocol (protocolo de configuración dinámica de host)

DLL Dynamic link library (Biblioteca de enlaces dinámicos)

DMTF Distributed Management Task Force (Fuerza de tareas de gestión distribuidas)

DNS Domain Name System (Sistema de nombres de dominio)

DVO Digital Video Out (Salida de vídeo digital)

EAAS Environment Abnormality Auto-Shutdown (Cierre automático de anormalidades en el entorno)

EBIPA Enclosure Bay IP Addressing (Dirección IP de bahía del receptáculo)

EMS Emergency Management Services (Servicios de gestión de emergencias)

FEH fatal exception handler (controlador de excepciones graves)

GNOME GNU Network Object Model Environment (Entorno modelo de objeto de red GNU)

GUI Graphical User Interface (Interfaz gráfica de usuario)

HB heartbeat (latencia)

HEM High Efficiency Mode (Modo de alta eficacia)

HID human interface device (dispositivo de interfaz humana)

HPONCFG HP Lights-Out Online Configuration utility (Función de configuración en línea de Lights-Out de HP)

HPQLOMGC HP Lights-Out Migration Command Line (Línea de comandos de migración de Lights-Out de HP)

HPQLOMIG HP Lights-Out Migration (Migración de Lights-Out de HP)

HP SIM HP Systems Insight Manager

ICMP Internet Control Message Protocol (Protocolo de mensajes de control de Internet)

iLO Integrated Lights-Out (dispositivo Lights-out integrado)

iLO 2 Integrated Lights-Out 2

IP Internet Protocol (Protocolo Internet)

IPMI Intelligent Platform Management Interface (Interfaz de gestión de plataforma inteligente)

IRC Integrated Remote Console (Consola remota integrada)

IRQ interrupt request (petición de interrupción)

JVM Java Virtual Machine (Sistema virtual Java)

KCS Keyboard Controller Style (Estilo de controlador de teclado)

KDE K Desktop Environment (Entorno de escritorio K) (para Linux)

KVM keyboard, video, and mouse (teclado, vídeo y ratón)

LAN local area network (red de área local)

LDAP Lightweight Directory Access Protocol (Protocolo ligero de acceso a directorios)

LED light-emitting diode (diodo emisor de luz)

LOM Lights-Out Management (Gestión de Lights-Out)

LSB least significant bit (bit menos significativo)

MAC Media Access Control (Control de acceso a medios)

MLA Master License Agreement (Acuerdo de licencia principal)

MMC Microsoft® Management Console

MP Protocolo Multilink Point-to-Point

MTU maximum transmission unit (unidad de transmisión máxima)

NIC Network Interface Controller (controlador de interfaz de red)

NMI Non-Maskable Interrupt (interrupción no enmascarable)

NVRAM non-volatile memory (memoria no volátil)

PERL Practical Extraction and Report Language (Lenguaje de extracción práctica y creación de informes)

PKCS Public-Key Cryptography Standards (Normas de cifrado de clave pública)

POST Power-On Self-Test (autocomprobación al arrancar)

PSP ProLiant Support Pack

RAS Remote access service (servicio de acceso remoto)

RBSU ROM-Based Setup Utility

RDP Remote Desktop Protocol (Protocolo de escritorio remoto)

RGL Registro de gestión integrado

RIB Remote Insight Board (Placa de Remote Insight)

RIBCL Remote Insight Board Command Language (Lenguaje de comandos de la placa Remote Insight)

RILOE Remote Insight Lights-Out Edition

RILOE II Remote Insight Lights-Out Edition II

ROM read-only memory (memoria de sólo lectura)

RSA Rivest, Shamir, and Adelman public encryption key (clave de cifrado pública Rivest, Shamir y Adelman)

RSM Remote Server Management (Gestión de servidores remotos)

SAID Service Agreement Identifier (Identificador de acuerdo de servicio)

SBIPC Static Bay IP Configuration (Configuración del compartimento con IP estática)

SLES SUSE Linux Enterprise Server

SMASH System Management Architecture for Server Hardware (Arquitectura de gestión de sistemas para hardware de servidor)

SNMP Simple Network Management Protocol (Protocolo de gestión de red simple)

SSH Shell de seguridad

SSL Secure Sockets Layer (Nivel de sockets seguro)

SSO Single Sign-On (Inicio de sesión único)

SUM software update manager (gestor de actualización de software)

SUV serie, USB y vídeo

TCP Transmission Control Protocol (Protocolo de control de transmisión)

TPM Trusted platform module (módulo de plataforma segura)

UART universal asynchronous receiver-transmitter (transmisor-receptor asincrónico universal)

UID Unit Identification (identificación de unidades)

USB universal serial bus (bus serie universal)

VM Virtual Machine (máquina virtual)

VPN Virtual Private Networking (Redes privadas virtuales)

VRM voltage regulator module (módulo regulador de tensión)

WINS Windows® Internet Naming Service (Servicio de denominación Internet de Windows®)

WS web services (servicios Web)

XML Extensible Markup Language (Lenguaje de formato extensible)

Índice

B

C

D

I

J

K

R

T

U

V

W

X