

Referencia sobre la gestión remota

Novell® ZENworks® 10 Configuration Management SP2

10.2

27 de mayo de 2009

www.novell.com



Información legal

Novell, Inc. no otorga ninguna garantía respecto al contenido y el uso de esta documentación y específicamente renuncia a cualquier garantía explícita o implícita de comercialización o adecuación para un fin determinado. Asimismo, Novell, Inc. se reserva el derecho a revisar esta publicación y a realizar cambios en su contenido en cualquier momento, sin obligación de notificar tales cambios a ninguna persona o entidad.

Además, Novell, Inc. no ofrece ninguna garantía con respecto a ningún software y rechaza específicamente cualquier garantía explícita o implícita de comercialización o adecuación para un fin determinado. Por otra parte, Novell, Inc. se reserva el derecho a realizar cambios en cualquiera de las partes o en la totalidad del software de Novell en cualquier momento, sin obligación de notificar tales cambios a ninguna persona ni entidad.

Los productos o la información técnica que se proporcionan bajo este Acuerdo pueden estar sujetos a los controles de exportación de Estados Unidos o a la legislación sobre comercio de otros países. Usted acepta acatar las regulaciones de los controles de exportación y obtener todas las licencias necesarias para exportar, reexportar o importar bienes. También se compromete a no exportar ni reexportar el producto a entidades que figuren en las listas de exclusión de exportación de Estados Unidos, ni a países sometidos a embargo o sospechosos de albergar terroristas, tal y como se especifica en las leyes de exportación de los Estados Unidos. Asimismo, se compromete a no usar el producto para fines prohibidos, como la creación de misiles o armas nucleares, químicas o biológicas. Consulte la [página Web sobre servicios de comercio internacional de Novell \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) para obtener más información sobre la exportación del software de Novell. Novell no se responsabiliza de la posibilidad de que el usuario no pueda obtener los permisos de exportación necesarios.

Copyright © 2007-2009 Novell, Inc. Reservados todos los derechos. Ninguna parte de esta publicación puede ser reproducida, fotocopiada, almacenada en un sistema de recuperación o transmitida sin la expresa autorización por escrito del editor.

Novell, Inc. posee derechos de propiedad intelectual relacionados con la tecnología incorporada en el producto descrito en este documento. En concreto, y sin limitación, estos derechos de propiedad intelectual pueden incluir una o más de las patentes de EE. UU. que aparecen en la [página Web de Novell sobre patentes legales \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/), y una o más patentes adicionales o solicitudes de patentes pendientes en EE. UU. y en otros países.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
EE. UU.
www.novell.com

Documentación en línea: para acceder a la documentación en línea más reciente acerca de este y otros productos de Novell, visite la [página Web de documentación de Novell \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Marcas comerciales de Novell

Para obtener información sobre las marcas comerciales de Novell, consulte [la lista de marcas registradas y marcas de servicio de Novell \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiales de otros fabricantes

Todas las marcas comerciales de otros fabricantes son propiedad de sus propietarios respectivos.

Tabla de contenido

| | |
|--|-----------|
| Acerca de esta guía | 9 |
| 1 Descripción general | 11 |
| 1.1 Terminología de la gestión remota | 11 |
| 1.2 Descripción de las operaciones de gestión remota | 12 |
| 1.2.1 Control remoto | 13 |
| 1.2.2 Vista remota | 13 |
| 1.2.3 Ejecución remota | 13 |
| 1.2.4 Diagnóstico remoto | 13 |
| 1.2.5 Transferencia de archivos | 13 |
| 1.2.6 Activación remota | 14 |
| 1.3 Descripción de las funciones de gestión remota | 14 |
| 1.3.1 Señal visible | 14 |
| 1.3.2 Detección de intrusos | 15 |
| 1.3.3 Cifrado de sesión | 15 |
| 1.3.4 Señal audible | 15 |
| 1.3.5 Bloqueo del teclado y el ratón | 15 |
| 1.3.6 Pantalla en blanco | 15 |
| 1.3.7 Terminación anormal | 15 |
| 1.3.8 Omisión del protector de pantalla | 15 |
| 1.3.9 Interrupción de sesión automática | 15 |
| 1.3.10 Conexión iniciada por el agente | 16 |
| 1.3.11 Sesión de colaboración | 16 |
| 1.3.12 Auditoría de gestión remota | 16 |
| 1.4 Descripción del servidor proxy de gestión remota | 16 |
| 2 Configuración de la gestión remota | 17 |
| 2.1 Configuración de los ajustes de gestión remota | 17 |
| 2.1.1 Configuración de los valores de gestión remota para la zona de gestión | 17 |
| 2.1.2 Configuración de los valores de gestión remota para las carpetas | 20 |
| 2.1.3 Configuración de los valores de gestión remota para los dispositivos | 20 |
| 2.2 Habilitación de la escucha de gestión remota | 21 |
| 2.3 Creación de la directiva de gestión remota | 21 |
| 2.4 Configuración de los derechos del operador remoto | 28 |
| 2.5 Configuración de la contraseña de gestión remota | 29 |
| 2.5.1 Configuración de la contraseña de gestión remota mediante el Centro de control de ZENworks | 29 |
| 2.5.2 Configuración de la contraseña para gestión remota mediante el agente de ZENworks Adaptive | 30 |
| 2.5.3 Eliminación de la contraseña de gestión remota mediante el Centro de control de ZENworks | 31 |
| 2.5.4 Eliminación de la contraseña de gestión remota mediante el agente de ZENworks Adaptive | 31 |
| 2.6 Instalación del visor de gestión remota | 31 |
| 2.7 Actualización del visor de gestión remota | 33 |
| 2.8 Inicio de operaciones de gestión remota | 33 |
| 2.8.1 Inicio de una sesión desde la consola de gestión | 33 |
| 2.8.2 Inicio de una sesión desde el dispositivo gestionado | 45 |
| 2.9 Instalación de un servidor proxy de gestión remota | 46 |

| | | |
|----------|--|-----------|
| 3 | Gestión de sesiones remotas | 47 |
| 3.1 | Gestión de una sesión de Control remoto | 47 |
| 3.1.1 | Uso de las opciones de la barra de herramientas en el visor de gestión remota . . . | 47 |
| 3.1.2 | Sesión de colaboración | 49 |
| 3.2 | Gestión de una sesión de Vista remota | 51 |
| 3.3 | Gestión de una sesión de Ejecución remota | 52 |
| 3.4 | Gestión de una sesión de Diagnóstico remoto | 52 |
| 3.5 | Gestión de una sesión de Transferencia de archivos | 54 |
| 3.6 | Activación de un dispositivo remoto | 57 |
| 3.6.1 | Requisitos previos | 57 |
| 3.6.2 | Reactivación remota de los dispositivos gestionados | 57 |
| 3.7 | Mejora del rendimiento de la gestión remota | 58 |
| 3.7.1 | En la consola de gestión | 58 |
| 3.7.2 | En el dispositivo gestionado | 58 |
| 4 | Seguridad | 59 |
| 4.1 | Autenticación | 59 |
| 4.1.1 | Autenticación de gestión remota basada en derechos | 59 |
| 4.1.2 | Autenticación de gestión remota basada en contraseña | 60 |
| 4.2 | Seguridad de las contraseñas | 61 |
| 4.3 | Puertos | 61 |
| 4.4 | Audit | 61 |
| 4.5 | Solicitud de permiso al usuario del dispositivo gestionado | 62 |
| 4.6 | Terminación anormal | 62 |
| 4.7 | Detección de intrusos | 63 |
| 4.7.1 | Desbloqueo automático del servicio de gestión remota | 63 |
| 4.7.2 | Desbloqueo manual del servicio de gestión remota | 63 |
| 4.8 | Identificación del operador remoto | 63 |
| 4.9 | Configuración del navegador | 64 |
| 4.10 | Seguridad de la sesión | 64 |
| 4.10.1 | Enlace SSL | 64 |
| 4.10.2 | Regeneración de certificados | 65 |
| 5 | Resolución de problemas | 67 |
| A | Información sobre criptografía | 73 |
| A.1 | Información sobre el par de claves del dispositivo gestionado | 73 |
| A.2 | Información sobre el par de claves del operador remoto | 73 |
| A.3 | Información sobre el ticket de gestión remota | 74 |
| A.4 | Información sobre el cifrado de sesiones | 74 |
| B | Prácticas recomendadas | 75 |
| B.1 | Cierre de las escuchas de gestión remota | 75 |
| B.2 | Cierre de aplicaciones lanzadas durante la operación de ejecución remota | 75 |
| B.3 | Identificación del operador remoto en el dispositivo gestionado | 76 |
| B.4 | Realización de una sesión de control remoto en un dispositivo que ya está conectado a través de una conexión de escritorio remoto | 76 |
| B.5 | Determinación del nombre de la consola de gestión | 76 |
| B.6 | Uso del tema Aero en dispositivos con Windows Vista y Windows Server 2008. | 76 |

| | | |
|----------|--|-----------|
| B.7 | Habilitación del botón de secuencia de atención (Ctrl+Alt+Supr) al controlar de forma remota un equipo con Windows Vista o Windows Server 2008 | 77 |
| B.8 | Instalación del servicio de gestión remota en un dispositivo con Windows XP a través de RDP | 77 |
| B.9 | Rendimiento de gestión remota | 77 |
| C | Actualizaciones de la documentación | 79 |
| C.1 | 27 de mayo de 2009: SP2 (10.2) | 79 |
| C.1.1 | Descripción general | 79 |
| C.1.2 | Configuración de la gestión remota | 79 |
| C.1.3 | Seguridad | 80 |

Acerca de esta guía

Esta *Referencia sobre la gestión remota de Novell ZENworks 10 Configuration Management* incluye información sobre la gestión remota. La información incluida en la guía está organizada del modo siguiente:

- ♦ Capítulo 1, “Descripción general”, en la página 11
- ♦ Capítulo 2, “Configuración de la gestión remota”, en la página 17
- ♦ Capítulo 3, “Gestión de sesiones remotas”, en la página 47
- ♦ Capítulo 4, “Seguridad”, en la página 59
- ♦ Capítulo 5, “Resolución de problemas”, en la página 67
- ♦ Apéndice A, “Información sobre criptografía”, en la página 73
- ♦ Apéndice B, “Prácticas recomendadas”, en la página 75
- ♦ Apéndice C, “Actualizaciones de la documentación”, en la página 79

Usuarios a los que va dirigida

Esta guía está dirigida a los administradores de Novell® ZENworks®.

Comentarios

Nos gustaría recibir sus comentarios y sugerencias acerca de este manual y del resto de la documentación incluida con este producto. Utilice la función de comentarios del usuario que se incluye en la parte inferior de cada página de la documentación en línea, o bien acceda al [sitio Web de comentarios sobre la documentación de Novell \(http://www.novell.com/documentation/feedback.html\)](http://www.novell.com/documentation/feedback.html) e introduzca allí sus comentarios.

Documentación adicional

ZENworks Configuration Management cuenta con documentación adicional (en formatos PDF y HTML) que puede utilizar para conocer e implementar el producto. Para obtener información adicional, consulte la [documentación de ZENworks 10 Configuration Management SP2 \(http://www.novell.com/documentation/zcm10/\)](http://www.novell.com/documentation/zcm10/).

Convenciones de la documentación

En la documentación de Novell, los símbolos mayor que (>) se utilizan para separar acciones dentro de un paso y elementos en una ruta de referencia cruzada.

Un símbolo de marca comercial (®, ™, etc.) indica una marca comercial de Novell. Un asterisco (*) sirve para identificar una marca comercial de otro fabricante.

Cuando un nombre de vía de acceso se pueda escribir con una barra invertida para algunas plataformas y una barra normal para otras plataformas, el nombre de la vía de acceso aparecerá con una barra invertida. Los usuarios de plataformas que requieran una barra inclinada, como Linux*, deben usar estas barras, propias de dicho software.

Descripción general

1

Novell® ZENworks® Configuration Management permite gestionar de forma remota dispositivos desde la consola de gestión. La gestión remota permite:

- ♦ Controlar de forma remota el dispositivo gestionado.
- ♦ Ejecutar de forma remota archivos ejecutables en el dispositivo gestionado.
- ♦ Transferir archivos entre la consola de gestión y el dispositivo gestionado.
- ♦ Diagnosticar problemas en el dispositivo gestionado.
- ♦ Activar de forma remota un dispositivo gestionado que esté apagado.

Consulte las siguientes secciones:

- ♦ [Sección 1.1, “Terminología de la gestión remota”, en la página 11](#)
- ♦ [Sección 1.2, “Descripción de las operaciones de gestión remota”, en la página 12](#)
- ♦ [Sección 1.3, “Descripción de las funciones de gestión remota”, en la página 14](#)
- ♦ [Sección 1.4, “Descripción del servidor proxy de gestión remota”, en la página 16](#)

1.1 Terminología de la gestión remota

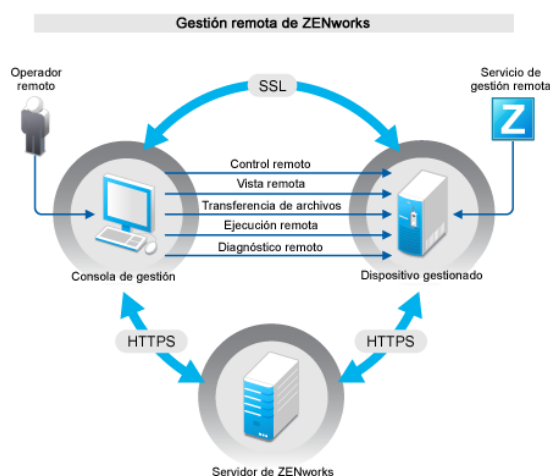
| Términos | Descripción |
|----------------------------|---|
| Dispositivo gestionado | Dispositivo que el usuario desea gestionar de forma remota. Para gestionar un dispositivo de forma remota, asegúrese de que el componente de gestión remota está instalado y el servicio de gestión remota se está ejecutando en el dispositivo. |
| Servidor de gestión | Un dispositivo en el que está instalado el servidor de ZENworks Configuration Management. |
| Consola de gestión | La interfaz para gestionar y administrar los dispositivos. Para realizar las operaciones remotas, debe instalar el visor de gestión remota en la consola. |
| Administrador | Una persona que puede configurar las directivas y los valores de gestión remota y otorgar derechos de gestión remota a los operadores remotos. |
| Servicio de gestión remota | Un componente de dispositivo gestionado que habilita a los operadores remotos para que puedan realizar operaciones remotas en el dispositivo. |
| Visor de gestión remota | Una aplicación de consola de gestión que habilita al operador remoto para que pueda realizar operaciones remotas en el dispositivo gestionado. Permite al operador remoto ver el escritorio del dispositivo gestionado, transferir archivos y ejecutar aplicaciones en el dispositivo gestionado. |

| Términos | Descripción |
|----------------------------------|---|
| Escucha de control remoto | Una aplicación de consola de gestión que habilita a un operador remoto para que pueda aceptar peticiones de asistencia remota de los usuarios del dispositivo gestionado. |
| Servidor proxy de gestión remota | Un servidor proxy que remite las peticiones de operaciones de gestión remota del visor de gestión remota a un dispositivo gestionado. El servidor proxy resulta útil cuando el visor no puede acceder directamente a un dispositivo gestionado que se encuentra en una red privada o al otro lado de un cortafuegos o router que utilice NAT (conversión de la dirección de red). Como requisito previo, el servidor proxy debe estar instalado en un dispositivo gestionado con Windows. |

1.2 Descripción de las operaciones de gestión remota

La gestión remota permite a los administradores controlar un dispositivo sin tener que desplazarse personalmente a la ubicación en la que se encuentre y puede ahorrarle a usted y a su empresa tiempo y dinero. Por ejemplo, usted o el departamento de ayuda técnica de su empresa pueden analizar y solucionar de forma remota los problemas del dispositivo gestionado sin necesidad de acudir personalmente a la estación de trabajo del usuario, reduciendo de esta forma el tiempo de resolución del problema y aumentando la productividad.

Figura 1-1 Operaciones de gestión remota



Las siguientes secciones le ayudarán a entender las distintas operaciones de gestión remota:

- ♦ Sección 1.2.1, “Control remoto”, en la página 13
- ♦ Sección 1.2.2, “Vista remota”, en la página 13
- ♦ Sección 1.2.3, “Ejecución remota”, en la página 13
- ♦ Sección 1.2.4, “Diagnóstico remoto”, en la página 13
- ♦ Sección 1.2.5, “Transferencia de archivos”, en la página 13
- ♦ Sección 1.2.6, “Activación remota”, en la página 14

1.2.1 Control remoto

El control remoto permite controlar de forma remota el dispositivo gestionado desde la consola de gestión, con lo que se puede proporcionar asistencia a los usuarios y ayudarles a resolver problemas del dispositivo.

El control remoto establece una conexión entre la consola de gestión y el dispositivo gestionado. Con las conexiones de control remoto, se pueden llevar a cabo todas las operaciones que el usuario puede realizar en el dispositivo. Para obtener más información, consulte la [Sección 3.1, “Gestión de una sesión de Control remoto”](#), en la página 47.

1.2.2 Vista remota

La vista remota permite conectar de forma remota con un dispositivo gestionado y ver el dispositivo en lugar de controlarlo. Esto le ayudará a solucionar los problemas que tenga el usuario. Por ejemplo, puede observar cómo el usuario de un dispositivo gestionado realiza determinadas tareas para asegurarse que las hace correctamente. Para obtener más información, consulte la [Sección 3.2, “Gestión de una sesión de Vista remota”](#), en la página 51.

1.2.3 Ejecución remota

La ejecución remota permite ejecutar cualquier ejecutable con privilegios de sistema en el dispositivo gestionado desde la consola de gestión. Para ejecutar de forma remota una aplicación, especifique el nombre del ejecutable en la ventana Ejecución remota. Por ejemplo, se puede ejecutar el comando `regedit` para abrir el Editor del registro en el dispositivo gestionado. Para obtener más información, consulte la [Sección 3.3, “Gestión de una sesión de Ejecución remota”](#), en la página 52.

1.2.4 Diagnóstico remoto

El diagnóstico remoto permite realizar diagnósticos de forma remota y analizar problemas del dispositivo gestionado. De esta forma, se aumenta la productividad del usuario, ya que los escritorios se mantienen activos y en funcionamiento. Para obtener más información, consulte la [Sección 3.4, “Gestión de una sesión de Diagnóstico remoto”](#), en la página 52.

Los diagnósticos proporcionan información en tiempo real que se puede utilizar para diagnosticar y solucionar problemas en el dispositivo gestionado. Las aplicaciones de diagnóstico por defecto en el dispositivo gestionado son:

- ♦ Información del sistema
- ♦ Administrador de equipos
- ♦ Servicios
- ♦ Editor del Registro

1.2.5 Transferencia de archivos

La transferencia de archivos permite realizar diversas operaciones de archivo en la consola de gestión y en el dispositivo gestionado, por ejemplo:

- ♦ Copiar archivos entre la consola de gestión y el dispositivo gestionado
- ♦ Cambiar el nombre de archivos o carpetas

- ♦ Suprimir archivos o carpetas
- ♦ Crear carpetas
- ♦ Ver las propiedades de archivos y carpetas
- ♦ Abrir archivos con las aplicaciones asociadas en la consola de gestión

Para obtener más información, consulte la [Sección 3.5, “Gestión de una sesión de Transferencia de archivos”](#), en la [página 54](#).

Importante: el programa de transferencia de archivos permite acceder a las unidades de red de los dispositivos gestionados.

1.2.6 Activación remota

La activación remota permite activar de forma remota un único nodo o un grupo de nodos desactivados de la red, siempre que la tarjeta de red del nodo permita la reactivación en LAN. Para obtener más información, consulte la [Sección 3.6, “Activación de un dispositivo remoto”](#), en la [página 57](#).

1.3 Descripción de las funciones de gestión remota

En las siguientes secciones se describen las distintas funciones de gestión remota:

- ♦ [Sección 1.3.1, “Señal visible”](#), en la [página 14](#)
- ♦ [Sección 1.3.2, “Detección de intrusos”](#), en la [página 15](#)
- ♦ [Sección 1.3.3, “Cifrado de sesión”](#), en la [página 15](#)
- ♦ [Sección 1.3.4, “Señal audible”](#), en la [página 15](#)
- ♦ [Sección 1.3.5, “Bloqueo del teclado y el ratón”](#), en la [página 15](#)
- ♦ [Sección 1.3.6, “Pantalla en blanco”](#), en la [página 15](#)
- ♦ [Sección 1.3.7, “Terminación anormal”](#), en la [página 15](#)
- ♦ [Sección 1.3.8, “Omisión del protector de pantalla”](#), en la [página 15](#)
- ♦ [Sección 1.3.9, “Interrupción de sesión automática”](#), en la [página 15](#)
- ♦ [Sección 1.3.10, “Conexión iniciada por el agente”](#), en la [página 16](#)
- ♦ [Sección 1.3.11, “Sesión de colaboración”](#), en la [página 16](#)
- ♦ [Sección 1.3.12, “Auditoría de gestión remota”](#), en la [página 16](#)

1.3.1 Señal visible

Permite proporcionar una indicación visible en el escritorio del dispositivo gestionado para informar al usuario de que el dispositivo se está gestionando de forma remota. La señal visible muestra la identificación del operador remoto y detalles de la sesión, como el tipo de sesión remota y la hora de inicio de la sesión. El usuario puede interrumpir una sesión remota concreta o cerrar el recuadro de diálogo de señal para interrumpir todas las sesiones remotas.

1.3.2 Detección de intrusos

La función de detección de intrusos reduce significativamente el riesgo de sufrir ataques por parte de hackers. Si el operador remoto no logra entrar en el dispositivo gestionado con el número de intentos especificado (5 por defecto), el servicio de gestión remota se bloquea y no acepta ninguna petición de sesión remota hasta que se desbloquea.

1.3.3 Cifrado de sesión

Las sesiones remotas se protegen mediante Secure Socket Layer (protocolo TLSv1).

1.3.4 Señal audible

Cuando hay una sesión remota activa en un dispositivo gestionado, puede generar en él un pitido audible a intervalos regulares según la configuración de la directiva de gestión remota.

1.3.5 Bloqueo del teclado y el ratón

Permite bloquear los controles del teclado y el ratón del dispositivo gestionado durante una sesión remota para evitar que el usuario del dispositivo gestionado interrumpa la sesión.

1.3.6 Pantalla en blanco

Permite dejar vacía la pantalla del dispositivo gestionado durante una sesión remota para evitar que el usuario pueda ver las acciones efectuadas por el operador remoto durante la sesión. Los controles del teclado y el ratón del dispositivo gestionado también se bloquean.

1.3.7 Terminación anormal

Permite bloquear el dispositivo gestionado o cerrar la sesión del usuario de este dispositivo si una sesión remota se desconecta de forma repentina.

1.3.8 Omisión del protector de pantalla

Permite anular cualquier protector de pantalla protegido mediante contraseña del dispositivo gestionado durante la sesión remota.

Nota: esta función no está disponible en los dispositivos gestionados con Windows Vista*.

1.3.9 Interrupción de sesión automática

Interrumpe automáticamente una sesión remota si ha estado inactiva durante un periodo de tiempo especificado.

1.3.10 Conexión iniciada por el agente

Permite habilitar al usuario del dispositivo gestionado para que pueda pedir asistencia de un operador remoto. Es posible preconfigurar la lista de operadores remotos que estarán disponibles para el usuario. Para obtener más información, consulte la [Sección 2.8.2, “Inicio de una sesión desde el dispositivo gestionado”, en la página 45.](#)

Nota: esta función sólo se admite en Windows en este momento.

1.3.11 Sesión de colaboración

Permite a un grupo de operadores remotos colaborar para realizar de forma conjunta una sesión remota. El operador remoto maestro puede invitar a otros operadores remotos a la sesión, delegar en ellos derechos de control remoto para resolver un problema, retomar el control e interrumpir una sesión remota. Para obtener más información, consulte la [Sección 3.1.2, “Sesión de colaboración”, en la página 49.](#)

1.3.12 Auditoría de gestión remota

Permite generar registros de auditoría de cada sesión remota que se realice en el dispositivo gestionado. El registro de auditoría se conserva en el dispositivo gestionado y el usuario puede consultarlo.

1.4 Descripción del servidor proxy de gestión remota

No es posible llevar a cabo ninguna operación de gestión remota en dispositivos gestionados que se encuentren en redes privadas o en el otro lado de un cortafuegos o router que utilice NAT (conversión de la dirección de la red). Esto se debe a que el cortafuegos NAT oculta la dirección IP del dispositivo a la red externa y bloquea cualquier petición de conexión realizada al dispositivo.

Para gestionar de forma remota un dispositivo de este tipo, el funcionamiento remoto del dispositivo se debe dirigir a través de un servidor proxy de gestión remota. Debe instalar el servidor proxy en un dispositivo que normalmente estará situado en una zona desmilitarizada (DMZ). Este dispositivo debe ser accesible desde la red pública, debe tener la consola de gestión y debe poder acceder a dispositivos ubicados en una red privada que requieran gestión remota. Para obtener información acerca de cómo instalar el servidor proxy de gestión remota, consulte la [Sección 2.9, “Instalación de un servidor proxy de gestión remota”, en la página 46.](#)

El servidor proxy de gestión remota escucha por defecto en el puerto 5750 en espera de peticiones de gestión remota entrantes del visor de gestión remota y remite la petición al dispositivo.

Configuración de la gestión remota

2

Las siguientes secciones proporcionan información sobre la distribución del componente de gestión remota de Novell® ZENworks® 10 Configuration Management en un entorno de producción:

- ♦ Sección 2.1, “Configuración de los ajustes de gestión remota”, en la página 17
- ♦ Sección 2.2, “Habilitación de la escucha de gestión remota”, en la página 21
- ♦ Sección 2.3, “Creación de la directiva de gestión remota”, en la página 21
- ♦ Sección 2.4, “Configuración de los derechos del operador remoto”, en la página 28
- ♦ Sección 2.5, “Configuración de la contraseña de gestión remota”, en la página 29
- ♦ Sección 2.6, “Instalación del visor de gestión remota”, en la página 31
- ♦ Sección 2.7, “Actualización del visor de gestión remota”, en la página 33
- ♦ Sección 2.8, “Inicio de operaciones de gestión remota”, en la página 33
- ♦ Sección 2.9, “Instalación de un servidor proxy de gestión remota”, en la página 46

2.1 Configuración de los ajustes de gestión remota

Los valores de configuración de gestión remota son reglas que determinan el comportamiento o la ejecución del servicio de gestión remota en el dispositivo gestionado. Los valores incluyen la configuración de los puertos, valores de sesión y valores de rendimiento durante la sesión remota. Estos valores se pueden aplicar en los niveles de zona, carpeta y dispositivo.

Las siguientes secciones proporcionan información acerca de la configuración de los valores de gestión remota en los distintos niveles:

- ♦ Sección 2.1.1, “Configuración de los valores de gestión remota para la zona de gestión”, en la página 17
- ♦ Sección 2.1.2, “Configuración de los valores de gestión remota para las carpetas”, en la página 20
- ♦ Sección 2.1.3, “Configuración de los valores de gestión remota para los dispositivos”, en la página 20

2.1.1 Configuración de los valores de gestión remota para la zona de gestión

Por defecto, los valores de gestión remota que se configuran para la zona de gestión se aplican a todos los dispositivos gestionados.

- 1 En el Centro de control de ZENworks, haga clic en *Configuración*.
- 2 En el panel Valores de zona de gestión, haga clic en *Gestión de dispositivos* y luego en *Gestión remota*.

- 3 Seleccione *Ejecutar servicio de gestión remota en el puerto* y especifique el puerto para habilitar en él la ejecución del servicio de gestión remota.

El servicio de gestión remota escucha por defecto en el puerto 5950.

- 4 Seleccione *Buscar nombre DNS del visor en el inicio de la sesión remota* para habilitar el servicio de gestión remota de forma que se busque el nombre DNS de la consola de gestión al principio de la sesión remota.

El nombre se guarda en los registros de auditoría y se muestra como parte de la información de la sesión durante las sesiones remotas. Si esta opción no está seleccionada, o si el servicio de gestión remota no encuentra el nombre de la consola, se mostrará el nombre *desconocido*.

Si en la red no está habilitada la búsqueda DNS inversa, conviene desactivar este valor para evitar retrasos importantes en el inicio de la sesión remota.

- 5 Seleccione entre las opciones siguientes para mejorar el rendimiento durante la sesión remota:

| Campo | Detalles |
|--|---|
| <i>Suprimir papel tapiz</i> | Suprime el papel tapiz del dispositivo gestionado durante una sesión remota. Así se impide que los datos de mapa de bits del papel tapiz se envíen de forma repetida a la consola de gestión remota, lo que mejora el rendimiento de la sesión. |
| <i>Habilitar controlador de optimización</i> | Habilita el controlador de optimización, que se instala por defecto en todos los dispositivos gestionados. Si se selecciona esta opción, sólo la parte de la pantalla del dispositivo gestionado que cambia se captura y se actualiza en la consola de gestión remota durante la sesión remota, con lo que mejora el rendimiento de la sesión.. |

- 6 (Opcional) Configure un servidor proxy de gestión remota para llevar a cabo operaciones remotas en el dispositivo gestionado.

Si el dispositivo gestionado se encuentra en una red privada o al otro lado de un cortafuegos o router que utilice NAT (conversión de la dirección de red), la operación de gestión remota se puede encaminar a través de un servidor proxy de gestión remota. Deberá instalar el servidor proxy por separado. Para obtener información acerca de cómo instalar el servidor proxy de gestión remota, consulte la [Sección 2.9, “Instalación de un servidor proxy de gestión remota”, en la página 46](#).

| Tarea | Detalles |
|--|---|
| Adición de un servidor proxy de gestión remota | <ol style="list-style-type: none"> Haga clic en <i>Añadir</i> para acceder al recuadro de diálogo Añadir valores de servidor proxy. Cumplimente los siguientes campos: <p>Servidor proxy: especifique la dirección IP o el nombre DNS del servidor proxy de gestión remota.</p> <p>Rango de direcciones IP: especifique las direcciones IP de los dispositivos que desee gestionar de forma remota a través del servidor proxy de gestión remota. Puede especificar el rango de direcciones IP de una de estas formas:</p> <ul style="list-style-type: none"> ♦ Escriba el rango de direcciones IP mediante la notación CIDR (encaminamiento entre dominios sin clase). Con CIDR, la parte de puntos decimales de la dirección IP se interpreta como un número binario de 32 bits que se ha dividido en cuatro bytes de 8 bits. El número que va después de la barra (/n) corresponde a la longitud del prefijo, es decir, el número de bits iniciales compartidos, contados desde el lado izquierdo de la dirección. El número /n puede estar entre 0 y 32, y los números más utilizados son 8, 16, 24 y 32. Ejemplos: <p>123.45.678.12/16: especifica todas las direcciones IP que empiecen por 123.45.</p> <p>123.45.678.12/24: especifica todas las direcciones IP que empiecen por 123.45.678.</p> ♦ Escriba el rango de direcciones con el formato Dirección IP inicial - Dirección IP final. Por ejemplo: <p>123.45.678.12 - 123.45.678.15: especifica todas las direcciones IP incluidas en el rango 123.45.678.12 a 123.45.678.15.</p> |
| Supresión de un servidor proxy de gestión remota | <ol style="list-style-type: none"> Seleccione el servidor proxy que desee suprimir. Haga clic en Suprimir y, a continuación, en <i>Aceptar</i>. |

7 (Opcional) Configure una aplicación para lanzarla en el dispositivo gestionado durante la sesión de diagnóstico remoto añadiéndola a la lista *Aplicaciones de diagnóstico*. La lista incluye por defecto las siguientes aplicaciones:

- ♦ Información del sistema
- ♦ Administrador de equipos
- ♦ Servicios
- ♦ Editor del Registro

La tabla siguiente recoge las tareas que puede realizar para personalizar la lista *Aplicaciones de diagnóstico*:

| Tarea | Detalles |
|---|---|
| Añadir una aplicación | <ol style="list-style-type: none"> 1. Haga clic en <i>Añadir</i>. 2. Especifique el nombre y la vía de la aplicación en el dispositivo gestionado. 3. Haga clic en <i>Aceptar</i>. |
| Suprimir una aplicación | <ol style="list-style-type: none"> 1. Seleccione la aplicación que desea suprimir. 2. Haga clic en Suprimir y, a continuación, en <i>Aceptar</i>. |
| Revertir a las aplicaciones por defecto | <ol style="list-style-type: none"> 1. Haga clic en <i>Revertir</i> y después en <i>Aceptar</i>. |

8 Haga clic en *Aplicar* y después en *Aceptar*.

Los cambios se aplican en el dispositivo cuando se actualiza.

2.1.2 Configuración de los valores de gestión remota para las carpetas

Por defecto, los valores de gestión remota configurados para la zona de gestión se aplican a todos los dispositivos gestionados. Sin embargo, se pueden modificar esos valores para los dispositivos incluidos en una carpeta:

- 1 En el Centro de control de ZENworks, haga clic en *Dispositivos*.
- 2 Haga clic en la carpeta (detalles) cuyos valores de gestión remota desea configurar.
- 3 Haga clic en *Valores* y después en *Gestión de dispositivos > Gestión remota*.
- 4 Haga clic en *Sobrescribir*.
- 5 Edite los valores de gestión remota como sea necesario.
- 6 Para aplicar los cambios, haga clic en *Aplicar*.

O bien

Para volver a los valores de sistema configurados para la zona de gestión, haga clic en *Revertir*.

- 7 Haga clic en *Aceptar*.

Los cambios se aplican en el dispositivo cuando se actualiza.

2.1.3 Configuración de los valores de gestión remota para los dispositivos

Por defecto, los valores de gestión remota configurados para la zona de gestión se aplican a todos los dispositivos gestionados. Sin embargo, puede modificar esos valores para el dispositivo gestionado:

- 1 En el Centro de control de ZENworks, haga clic en *Dispositivos*.
- 2 Haga clic en *Servidores* o en *Estaciones de trabajo* para que aparezca una lista de los dispositivos gestionados.
- 3 Haga clic en el dispositivo cuyos valores de gestión remota desea configurar.
- 4 Haga clic en *Valores* y después en *Gestión de dispositivos > Gestión remota*.

- 5 Haga clic en *Sobrescribir*.
- 6 Edite los valores de gestión remota como sea necesario.
- 7 Para aplicar los cambios, haga clic en *Aplicar*.

O bien

Para volver a los valores de configuración anteriores del dispositivo, haga clic en *Revertir*.

Si los valores de gestión remota del dispositivo se han configurado a nivel de carpeta, los valores vuelven a los configurados a nivel de carpeta; de lo contrario, vuelven a los valores por defecto a nivel de zona.

- 8 Haga clic en *Aceptar*.

Los cambios se aplican en el dispositivo cuando se actualiza.

2.2 Habilitación de la escucha de gestión remota

Para habilitar la escucha de gestión remota con el fin de escuchar conexiones desde un dispositivo gestionado:

- 1 En el Centro de control de ZENworks, haga clic en *Dispositivos*.
- 2 En *Tareas de dispositivo* en el panel izquierdo, haga clic en Escucha de gestión remota.
- 3 En el recuadro de diálogo Escucha de gestión remota, especifique el puerto en el se deben escuchar las conexiones remotas. Por defecto, el número de puerto es 5550.
- 4 Haga clic en *Aceptar*. El icono de la escucha de gestión remota de ZENworks aparecerá en el área de notificación.

2.3 Creación de la directiva de gestión remota

La directiva de gestión remota permite configurar el comportamiento o la ejecución de una sesión de gestión remota en el dispositivo gestionado. La directiva incluye valores para operaciones de gestión remota como control remoto, vista remota, ejecución remota, diagnóstico remoto o transferencia de archivos y permite además controlar los valores de seguridad.

Por defecto, se crea una directiva de gestión remota segura en el dispositivo gestionado cuando se distribuye el agente de ZENworks Adaptive con el componente de gestión remota en el dispositivo. Puede usar la directiva por defecto para gestionar un dispositivo de forma remota. Para sustituir la directiva por defecto, puede crear explícitamente una directiva de gestión remota para el dispositivo.

- 1 En el Centro de control de ZENworks, haga clic en la pestaña *Directivas*.
- 2 En la lista de *Directivas*, haga clic en *Nuevo* y después en *Directiva* para acceder a la página Seleccionar tipo de directiva.
- 3 Seleccione *Directiva para gestión remota*, haga clic en *Siguiente* para acceder a la página Definir detalles y complete los campos:

Nombre de directiva: proporcione un nombre exclusivo para la directiva. El nombre de la directiva no puede coincidir con el nombre de ningún otro elemento (grupo, carpeta, etc.) que se encuentre en la misma carpeta.

Carpeta: escriba el nombre de la carpeta del Centro de control de ZENworks en la que desea que resida la directiva o desplácese hasta ella. La carpeta por defecto es */directivas*, aunque puede crear carpetas adicionales para organizar las directivas.

Descripción: proporcione una breve descripción del contenido de la directiva. Esta descripción se muestra en la página de resumen de la directiva en el Centro de control de ZENworks.

- 4 Haga clic en *Siguiente* para acceder a la página Valores generales de gestión remota. Para aceptar los valores por defecto, continúe con el paso siguiente o utilice la información especificada en la tabla siguiente para cambiar los valores por defecto.

| Campo | Detalles |
|--|---|
| <i>Permitir que el usuario solicite una sesión remota</i> | Permite que el usuario del dispositivo gestionado solicite que un operador lleve a cabo una sesión remota. El operador remoto debe asegurarse de que se está ejecutando la escucha de gestión remota. |
| <i>Terminar la sesión remota cuando se requiera permiso para que un usuario nuevo se registre en el dispositivo gestionado</i> | Termina una sesión remota en curso cuando se requiere permiso de un nuevo usuario que ha entrado en el dispositivo gestionado de forma remota. |
| <i>Mostrar la información de auditoría de la sesión remota al usuario en el dispositivo gestionado</i> | Permite que el usuario del dispositivo gestionado vea la información de auditoría correspondiente a sesiones remotas desde el icono de ZENworks. |
| <i>Mostrar las propiedades de gestión remota en el icono de ZENworks</i> | Permite que el usuario del dispositivo gestionado vea las propiedades asociadas con la directiva de gestión remota en el icono de ZENworks. |
| <i>Editar</i> | Para editar el mensaje que se muestra al usuario del dispositivo gestionado antes de iniciar una sesión remota: <ol style="list-style-type: none"> Haga clic en <i>Editar</i> para acceder al recuadro de diálogo Editar mensaje. Edite el mensaje. Haga clic en <i>Aceptar</i>. |
| <i>Restablecer valor por defecto</i> | Para restablecer el mensaje por defecto: <ol style="list-style-type: none"> Haga clic en <i>Restablecer valor por defecto</i> para recuperar el mensaje por defecto. |
| <i>Añadir una escucha remota</i> | Para añadir una escucha remota: <ol style="list-style-type: none"> Haga clic en <i>Añadir</i>. En el recuadro de diálogo Añadir escucha remota, especifique el nombre DNS o la dirección IP de la consola de gestión y el número de puerto para la escucha de peticiones de sesiones de gestión remota. Haga clic en <i>Aceptar</i>. |
| <i>Suprimir una escucha remota</i> | Para suprimir una escucha remota: <ol style="list-style-type: none"> Seleccione la escucha remota que desee suprimir. Haga clic en <i>Eliminar</i>. |

- 5 Haga clic en *Siguiente* para acceder a la página Valores de control remoto. Para aceptar los valores por defecto, continúe con el paso siguiente o utilice la información especificada en la tabla siguiente para cambiar los valores por defecto.

| Campo | Detalles |
|--|---|
| <i>Permitir que los dispositivos gestionados se puedan controlar de forma remota</i> | Permite las sesiones de control remoto en el dispositivo gestionado. Cuando se selecciona esta opción, se habilitan otras opciones de la página. Cuando se anula la selección de esta opción, se inhabilita la operación de control remoto en el dispositivo. |
| <i>Pedir permiso del usuario en el dispositivo gestionado antes de iniciar el control remoto</i> | Permite pedir permiso al usuario del dispositivo gestionado antes de empezar la sesión de control remoto. |
| <i>Proporcionar una señal visual al usuario del dispositivo gestionado durante el control remoto</i> | Muestra una señal visual en la esquina superior derecha del escritorio del dispositivo gestionado durante la sesión de control remoto. La señal visual permite al usuario del dispositivo gestionado saber que hay una sesión de control remoto en curso. |
| <i>Proporcionar una señal sonora al usuario del dispositivo gestionado cada [] segundos durante el control remoto</i> | Genera una señal sonora en el dispositivo gestionado durante la sesión de control remoto. La señal sonora se produce periódicamente tras el número de segundos especificado. |
| <i>Permitir que la pantalla del dispositivo remoto esté en blanco durante el control remoto</i> | Pone en blanco la pantalla del dispositivo gestionado durante la sesión de control remoto. Cuando se selecciona esta opción, también se bloquean los controles del teclado y del ratón del dispositivo gestionado. |
| <i>Permitir que se bloqueen el ratón y el teclado durante el control remoto</i> | Habilita el bloqueo del teclado y el ratón del dispositivo gestionado durante la sesión de control remoto. |
| <i>Permitir que el protector de pantalla se desbloquee automáticamente durante el control remoto</i> | Permite que se desbloquee un protector de pantalla con contraseña desde el visor de control remoto antes de comenzar la sesión de control remoto en el dispositivo gestionado. |
| <i>Terminar automáticamente la sesión de control remoto tras una inactividad de [] minutos</i> | Termina la sesión de control remoto en el dispositivo gestionado si ha permanecido inactiva durante el intervalo de tiempo especificado. |

- 6** Haga clic en *Siguiente* para acceder a la página Valores de vista remota. Para aceptar los valores por defecto, continúe con el paso siguiente o utilice la información especificada en la tabla siguiente para cambiar los valores por defecto.

| Campo | Detalles |
|--|---|
| <i>Permitir la vista remota del dispositivo gestionado</i> | Permite las sesiones de vista remota en el dispositivo gestionado. Cuando se selecciona esta opción, se habilitan otras opciones de la página. Cuando se anula la selección de esta opción, se inhabilita la operación de vista remota en el dispositivo. |
| <i>Pedir permiso del usuario en el dispositivo gestionado antes de iniciar la vista remota</i> | Permite pedir permiso al usuario del dispositivo gestionado antes de empezar una sesión de vista remota. |

| Campo | Detalles |
|---|---|
| <i>Proporcionar una señal visual al usuario del dispositivo gestionado durante la vista remota</i> | Presenta una señal visual en la esquina superior derecha del escritorio del dispositivo gestionado durante la sesión de vista remota. La señal visual permite que el usuario del dispositivo gestionado sepa que hay una sesión de vista remota en curso. |
| <i>Proporcionar una señal sonora al usuario del dispositivo gestionado cada [] segundos durante la vista remota.</i> | Emite una señal sonora en el dispositivo gestionado durante la sesión de vista remota. La señal sonora se produce periódicamente tras el número de segundos especificado. |

- 7 Haga clic en *Siguiente* para acceder a la página Valores de diagnóstico remoto. Para aceptar los valores por defecto, continúe con el paso siguiente o utilice la información especificada en la tabla siguiente para cambiar los valores por defecto.

| Campo | Detalles |
|--|---|
| <i>Permitir el diagnóstico remoto del dispositivo gestionado</i> | Permite las sesiones de diagnóstico remoto en el dispositivo gestionado. Cuando se selecciona esta opción, se habilitan otras opciones de la página. Cuando se anula la selección de esta opción, se inhabilita la operación de diagnóstico remoto en el dispositivo. |
| <i>Solicitar permiso al usuario del dispositivo gestionado antes de iniciar el diagnóstico remoto</i> | Garantiza que el operador remoto solicite permiso al usuario del dispositivo gestionado antes de iniciar una sesión de diagnóstico remoto. |
| <i>Proporcionar una señal visual al usuario del dispositivo gestionado durante el diagnóstico remoto</i> | Presenta una señal visual en la esquina superior derecha del escritorio del dispositivo gestionado durante la sesión de diagnóstico remoto. La señal visual permite que el usuario del dispositivo gestionado sepa que hay una sesión de diagnóstico remoto en curso. |
| <i>Proporcionar una señal sonora al usuario del dispositivo gestionado cada [] segundos durante el diagnóstico remoto</i> | Genera una señal sonora en el dispositivo gestionado durante la sesión de diagnóstico remoto. La señal sonora se produce periódicamente tras el número de segundos especificado. |
| <i>Permitir que la pantalla del dispositivo gestionado esté en blanco durante el diagnóstico remoto</i> | Pone en blanco la pantalla del dispositivo gestionado durante la sesión de diagnóstico remoto. El ratón y el teclado del dispositivo gestionado están siempre bloqueados durante las sesiones de diagnóstico remoto. Si se selecciona esta opción, también se desactiva la señal visual del dispositivo gestionado. |
| <i>Mostrar mensaje de advertencia antes de reorganizar durante [] segundos</i> | Muestra un mensaje de advertencia en el dispositivo gestionado al principio de la sesión de diagnóstico remoto, para recordar al usuario que debe guardar los cambios en todas las aplicaciones abiertas. Este mensaje de advertencia se muestra durante el tiempo que se especifique para impedir que el usuario pierda los datos que no haya guardado, en el caso de que el operador reorganice el sistema durante la sesión de diagnóstico remoto. |

| Campo | Detalles |
|---|--|
| <i>Terminar automáticamente la sesión de diagnóstico remoto tras una inactividad de [] minutos</i> | Termina la sesión de diagnóstico remoto si permanece inactiva durante el intervalo de tiempo especificado. |

- 8 Haga clic en *Siguiente* para acceder a la página Valores de ejecución remota. Para aceptar los valores por defecto, continúe con el paso siguiente o utilice la información especificada en la tabla siguiente para cambiar los valores por defecto.

| Campo | Detalles |
|---|--|
| <i>Permitir que se ejecuten programas de forma remota en el dispositivo gestionado</i> | Permite que se ejecuten programas de forma remota en el dispositivo gestionado. Cuando se selecciona esta opción, se habilitan otras opciones de la página. Cuando se anula la selección de esta opción, se inhabilita la operación de ejecución remota en el dispositivo. |
| <i>Pedir permiso del usuario en el dispositivo gestionado antes de iniciar la ejecución remota</i> | Garantiza que el operador remoto solicite permiso al usuario del dispositivo gestionado antes de iniciar una sesión de ejecución remota. |
| <i>Presentar señal visual al usuario en el dispositivo gestionado durante la ejecución remota</i> | Muestra una señal visual en la esquina superior derecha del escritorio del dispositivo gestionado durante la sesión de ejecución remota. La señal visual permite al usuario del dispositivo gestionado saber que hay una sesión de ejecución remota en curso. |
| <i>Terminar automáticamente la sesión de diagnóstico remoto tras una inactividad de [] minutos</i> | Termina la sesión de ejecución remota si permanece inactiva durante el intervalo de tiempo especificado. |

- 9 Haga clic en *Siguiente* para acceder a la página Valores de transferencia de archivo. Para aceptar los valores por defecto, continúe con el paso siguiente o utilice la información especificada en la tabla para cambiar los valores de seguridad por defecto.

| Campo | Detalles |
|---|--|
| <i>Permitir la transferencia de archivos en el dispositivo gestionado</i> | Habilita la transferencia de archivos entre la consola de gestión y el dispositivo gestionado. Cuando se selecciona esta opción, se habilitan otras opciones de la página. Cuando se anula la selección de esta opción, se inhabilita la operación de transferencia de archivos del dispositivo. |
| <i>Pedir permiso del usuario en el dispositivo gestionado antes de iniciar la transferencia del archivo</i> | Garantiza que el operador remoto solicite permiso al usuario del dispositivo gestionado antes de iniciar una sesión de transferencia de archivos. |
| <i>Presentar señal visual al usuario en el dispositivo gestionado durante la transferencia de archivo</i> | Muestra una señal visual en la esquina superior derecha del escritorio del dispositivo gestionado durante la sesión de transferencia de archivos. La señal visual permite al usuario del dispositivo gestionado saber que hay una sesión de transferencia de archivos en curso. |

| Campo | Detalles |
|---|---|
| <i>Permitir la descarga de archivos desde el dispositivo gestionado</i> | Permite a un operador remoto abrir archivos en el dispositivo gestionado y transferirlos a la consola de gestión. Si esta opción no se selecciona, el operador remoto sólo podrá transferir archivos desde la consola de gestión al dispositivo gestionado. |
| <i>Directorio raíz de transferencia de archivo</i> | Especifique el directorio del dispositivo gestionado que el operador remoto deba ver durante una sesión de transferencia de archivos. El operador remoto sólo podrá transferir archivos a ese directorio y sus subdirectorios y desde ellos. El directorio por defecto es Mi PC, lo que significa que el operador remoto podrá ver y transferir archivos de todo el sistema de archivos del dispositivo gestionado. |

- 10** Haga clic en *Siguiente* para acceder a la página Valores de seguridad. Para aceptar los valores por defecto, continúe con el paso siguiente o utilice la información especificada en la tabla para cambiar los valores de seguridad por defecto.

Autenticación con contraseña

| Campo | Detalles |
|---|--|
| <i>Habilitar autenticación basada en contraseña</i> | Permite que el operador remoto utilice una contraseña para autenticarse en el dispositivo gestionado. Seleccione esta opción para configurar los valores del tipo de contraseña. |
| <i>Longitud mínima de la contraseña</i> | Permite especificar la longitud mínima para la contraseña. Por defecto, la longitud mínima es de 6 caracteres. |
| <i>Contraseña de sesión</i> | Seleccione esta opción para solicitar al usuario del dispositivo gestionado que defina una contraseña antes de iniciar una sesión remota nueva. Se recomienda utilizar esta opción porque la contraseña no se almacena en el dispositivo gestionado y es válida sólo para la sesión en curso. |
| <i>Contraseña permanente</i> | <p>Seleccione esta opción para definir las contraseñas de ZENworks y VNC. Se recomienda definir la contraseña de ZENworks, ya que es más segura que la de VNC. Esta contraseña la puede definir el administrador a través de la directiva de gestión remota o el usuario del dispositivo gestionado desde el icono de ZENworks. Si selecciona esta opción se habilitarán las opciones siguientes.</p> <p>Para permitir que el usuario defina la contraseña a través del icono de ZENworks, seleccione la opción <i>Permitir que el usuario sobrescriba las contraseñas por defecto del dispositivo gestionado</i>.</p> |

| Campo | Detalles |
|------------------------|--|
| Contraseña de ZENworks | <p>Para borrar la contraseña de ZENworks:</p> <ol style="list-style-type: none"> 1. Haga clic en <i>Borrar contraseña</i>. 2. Haga clic en <i>Aplicar</i> y después en <i>Aceptar</i>. <p>Para definir la contraseña de ZENworks:</p> <ol style="list-style-type: none"> 1. Haga clic en <i>Definir contraseña</i>. 2. Escriba la contraseña. La longitud máxima de las contraseñas es de 255 caracteres. 3. Haga clic en <i>Aplicar</i> y después en <i>Aceptar</i>. |
| Contraseña de VNC | <p>Para borrar la contraseña de VNC:</p> <ol style="list-style-type: none"> 1. Haga clic en <i>Borrar contraseña</i>. 2. Haga clic en <i>Aplicar</i> y después en <i>Aceptar</i>. <p>Para definir la contraseña de VNC:</p> <ol style="list-style-type: none"> 1. Haga clic en <i>Definir contraseña</i>. 2. Escriba la contraseña. La longitud máxima de las contraseñas es de 8 caracteres. 3. Haga clic en <i>Aplicar</i> y después en <i>Aceptar</i>. |

Detección de intrusos

| Campo | Detalles |
|---|---|
| Habilitar la detección de intrusos | Seleccione esta opción para habilitar la detección de intentos no válidos o no autorizados de lanzar una sesión remota en el dispositivo gestionado. Cuando se selecciona esta opción, se habilitan otras opciones de la sección Detección de intrusos. |
| Suspender la aceptación de conexiones después de [] intentos no válidos consecutivos | Especifique el número máximo de intentos no válidos consecutivos que puede realizar un operador antes de que se bloquee el servicio de gestión remota en el dispositivo gestionado. Por defecto, son cinco intentos. |
| Empezar a aceptar conexiones automáticamente después de [] minutos | Especifique el tiempo en minutos que debe transcurrir antes de que el agente de gestión remota acepte automáticamente conexiones con el dispositivo gestionado. Para desbloquear manualmente el servicio de gestión remota, haga doble clic en el icono del agente de ZENworks Adaptive, haga clic en <i>Valores de seguridad</i> y después haga clic en <i>Habilitar la aceptación de conexiones si hay un bloqueo vigente debido a la detección de intrusos</i> . El valor por defecto es 10 minutos. |

Seguridad de la sesión

| Campo | Detalles |
|-----------------------------|--|
| Habilitar cifrado de sesión | Permite cifrar las sesiones mediante el cifrado SSL (protocolo TLSv1). Cuando se selecciona esta opción, se habilitan otras opciones de la sección Seguridad de la sesión. |

| Campo | Detalles |
|--|--|
| <i>Permitir conexión si la consola de gestión remota no tiene un certificado SSL</i> | Cuando se lanza una sesión remota desde el Centro de control de ZENworks, se genera automáticamente un certificado para un operador remoto. Este certificado se utiliza durante la autenticación. Seleccione esta opción para permitir las conexiones desde una consola de gestión remota que se haya lanzado fuera del Centro de control de ZENworks y que pueda no tener un certificado SSL. |
| <i>Permitir hasta [] niveles de la cadena de certificado del visor</i> | <p>Los esquemas de autenticación basados en contraseña y en derechos de Novell se ejecutan en un canal cifrado SSL. El establecimiento de este canal requiere que el visor presente un certificado. El certificado puede estar firmado por una autoridad intermedia o raíz, con lo que se crea una cadena de certificado.</p> <p>Esta propiedad define el número máximo de niveles que se permiten en la cadena de certificado del visor. Si se utiliza la autoridad certificadora interna de ZENworks (instalada por defecto), se crea automáticamente una cadena de certificado del visor de dos niveles cuando se lanza una sesión remota desde el Centro de control de ZENworks.</p> |

Terminación anormal

| Campo | Detalles |
|------------------------------------|---|
| <i>Bloquear dispositivo</i> | Bloquea el dispositivo gestionado cuando la sesión remota termina de forma anormal. |
| <i>Salir de sesión del usuario</i> | Cierra la sesión del usuario en el dispositivo gestionado cuando la sesión remota termina de forma anormal. |

- 11 Haga clic en *Siguiente* para que aparezca la página de resumen.
- 12 Haga clic en *Finalizar* para crear la directiva en ese momento, o seleccione *Definir propiedades adicionales* para especificar información adicional, como asignación, entrada en vigor y estado de la directiva o grupo al que pertenece.

2.4 Configuración de los derechos del operador remoto

Puede asignar derechos a un operador remoto para que lleve a cabo sesiones remotas en el dispositivo gestionado. El operador remoto puede tener derechos específicos para el dispositivo, así como derechos específicos de usuario.

- 1 En el Centro de control de ZENworks, haga clic en *Configuración*.
- 2 En el panel Administradores, haga clic en el nombre del administrador al que desea asignar los derechos de gestión remota.
- 3 En el panel Derechos asignados, haga clic en *Añadir*, > *Derechos de gestión remota* para acceder al recuadro de diálogo Derechos de gestión remota.
- 4 Seleccione el dispositivo o el usuario al que se deben asignar los derechos.

La tabla siguiente recoge información acerca de los derechos de gestión remota:

| Derechos de gestión remota | Detalles |
|--|---|
| Control remoto | Asigna al operador remoto derechos para controlar dispositivos de forma remota. |
| Vista remota | Asigna al operador remoto derechos para ver dispositivos de forma remota. |
| Diagnóstico remoto | Asigna al operador remoto derechos para diagnosticar dispositivos de forma remota. |
| Ejecución remota | Asigna al operador remoto derechos para ejecutar aplicaciones en los dispositivos de forma remota. |
| Transferir archivos | Asigna al operador remoto derechos para transferir archivos entre dispositivos. |
| Desbloquear servicio de gestión remota | Asigna al operador remoto derechos para desbloquear el servicio de gestión remota si se ha bloqueado debido a la detección de intrusos. |

Nota: los derechos de gestión remota sólo se aplican a la autenticación basada en derechos. Sin embargo, el operador remoto puede llevar a cabo la operación de gestión remota mediante la autenticación basada en contraseña si la directiva de gestión remota lo permite.

5 Haga clic en *Aceptar*.

2.5 Configuración de la contraseña de gestión remota

Las secciones siguientes proporcionan información sobre la configuración de la contraseña para el servicio de gestión remota en el dispositivo gestionado:

- ♦ Sección 2.5.1, “Configuración de la contraseña de gestión remota mediante el Centro de control de ZENworks”, en la página 29
- ♦ Sección 2.5.2, “Configuración de la contraseña para gestión remota mediante el agente de ZENworks Adaptive”, en la página 30
- ♦ Sección 2.5.3, “Eliminación de la contraseña de gestión remota mediante el Centro de control de ZENworks”, en la página 31
- ♦ Sección 2.5.4, “Eliminación de la contraseña de gestión remota mediante el agente de ZENworks Adaptive”, en la página 31

2.5.1 Configuración de la contraseña de gestión remota mediante el Centro de control de ZENworks

El administrador puede definir una contraseña de gestión remota en la página Valores de seguridad durante la creación de una directiva de gestión remota o después de crearla.

Si desea definir la contraseña mientras esté creando la directiva de gestión remota, consulte la “Sección 2.3, “Creación de la directiva de gestión remota”, en la página 21”.

Para editar la contraseña definida en la directiva para gestión remota:

- 1 En el Centro de control de ZENworks, haga clic en *Directivas*.
- 2 Haga clic en la directiva para gestión remota y después en la pestaña *Valores*. >
- 3 En el panel Valores de seguridad, seleccione la contraseña y sustitúyala con la contraseña nueva.
- 4 Haga clic en *Aplicar*.
- 5 Aumente la versión de la directiva en la página de resumen o en las tareas comunes para actualizar el cambio de contraseña en el dispositivo gestionado.

Si desea definir la contraseña después de crear la directiva para gestión remota:

- 1 En el Centro de control de ZENworks, haga clic en *Directivas*.
- 2 Haga clic en la directiva para gestión remota y después en la pestaña *Valores*. >
- 3 En el panel Valores de seguridad, seleccione *Habilitar autenticación basada en contraseña* y elija *Persistente*.
- 4 Haga clic en *Definir contraseña* y especifique la contraseña. Si ya ha definido la contraseña durante la creación de la directiva para gestión remota, puede editarla. Para ello, seleccione la contraseña y sustitúyala con la contraseña nueva.
- 5 Haga clic en *Aplicar*.
- 6 Aumente la versión de la directiva en la página de resumen o en las tareas comunes para actualizar el cambio de contraseña en el dispositivo gestionado.

2.5.2 Configuración de la contraseña para gestión remota mediante el agente de ZENworks Adaptive

El usuario del dispositivo gestionado puede definir una contraseña para el servicio de gestión remota si la opción *Permitir que el usuario sobrescriba las contraseñas por defecto del dispositivo gestionado* está habilitada en la directiva para gestión remota vigente en el dispositivo gestionado. Esta contraseña tiene prioridad sobre la contraseña definida en la directiva para gestión remota.

Para definir una contraseña en el dispositivo gestionado:

- 1 Haga doble clic en el icono del *agente de ZENworks Adaptive* para acceder a la ventana del agente.
- 2 En el panel de la izquierda, acceda a *Gestión remota* y haga clic en *Seguridad*.
- 3 En el panel de la derecha, haga clic en *Definir contraseña* para definir las contraseñas siguientes:
 - ♦ **Contraseña de ZENworks (recomendada):** se utiliza en la autenticación de ZENworks. Puede tener una longitud máxima de 255 caracteres.
 - ♦ **Contraseña de VNC:** se utiliza en la autenticación de VNC para la interoperabilidad con visores VNC de código abierto. Puede tener una longitud máxima de 8 caracteres.
- 4 Haga clic en *Aceptar*.

2.5.3 Eliminación de la contraseña de gestión remota mediante el Centro de control de ZENworks

Para eliminar la contraseña de gestión remota utilizando la directiva:

- 1 En el Centro de control de ZENworks, haga clic en *Directivas*.
- 2 Haga clic en la directiva para gestión remota y después en la pestaña *Valores*. >
- 3 En el panel Valores de seguridad, seleccione *Borrar contraseña* y después haga clic en *Aplicar*.
- 4 Aumente la versión de la directiva en la página de resumen o en las tareas comunes para actualizar los cambios de la directiva en el dispositivo gestionado.

Para eliminar la contraseña de gestión remota definida por el usuario del dispositivo gestionado:

- 1 En el Centro de control de ZENworks, haga clic en *Directivas*.
- 2 Haga clic en la directiva para gestión remota y después en la pestaña *Valores*. >
- 3 En el panel Valores de seguridad, anule la selección de *Permitir que el usuario sobrescriba las contraseñas por defecto del dispositivo gestionado* y haga clic en *Aplicar*.
- 4 Aumente la versión de la directiva en la página de resumen o en las tareas comunes para actualizar los cambios de la directiva en el dispositivo gestionado.

2.5.4 Eliminación de la contraseña de gestión remota mediante el agente de ZENworks Adaptive

El usuario del dispositivo gestionado puede restablecer la contraseña de gestión remota que haya definido con anterioridad.

- 1 Haga doble clic en el icono del *agente de ZENworks Adaptive* para acceder a la ventana del agente.
- 2 En el panel de la izquierda, acceda a *Gestión remota* y haga clic en *Seguridad*.
- 3 En el panel de la derecha, haga clic en *Borrar contraseña* para eliminar las contraseñas.
- 4 Haga clic en *Aceptar*.

La contraseña configurada en la directiva estará vigente, ya que no hay ninguna contraseña definida por el usuario.

2.6 Instalación del visor de gestión remota

El visor de gestión remota es una aplicación de consola de gestión que permite al operador remoto realizar operaciones remotas en el dispositivo gestionado. Permite al operador remoto ver el escritorio del dispositivo gestionado, transferir archivos y ejecutar aplicaciones en el dispositivo gestionado.

Para instalar el visor de gestión remota, haga clic en el enlace *Instalar visor de gestión remota* que se muestra en el Centro de control de ZENworks mientras se realiza una operación de gestión remota en el dispositivo gestionado. Este enlace sólo se muestra si se lleva a cabo la operación de gestión remota en el dispositivo por primera vez y el visor de gestión remota no está ya instalado en el dispositivo gestionado.

Si hay una versión anterior del visor instalada en el dispositivo, se muestra el enlace *Actualizar visor de gestión remota*. Haga clic en ese enlace para actualizar la versión del visor instalada en el dispositivo.

También puede instalar el visor en el dispositivo manualmente:

En Windows:

- 1 En el Centro de control de ZENworks, haga clic en *Configuración*.
- 2 En el panel de navegación izquierdo, haga clic en *Descargar herramientas de ZENworks*.
- 3 En el panel de navegación izquierdo de la página de descargas de ZENworks, haga clic en *Herramientas administrativas*.
- 4 Haga clic en `novell-zenworks-rm-viewer-<versión>.msi`.
- 5 (Condicional) Si ha lanzado el Centro de control de ZENworks desde Internet Explorer, lleve a cabo una de las siguientes acciones:
 - ♦ Haga clic en *Ejecutar* para instalar el visor.
 - ♦ Haga clic en *Guardar* para almacenar el archivo en una ubicación temporal. Haga doble clic en el archivo para instalar el visor.
- 6 (Condicional) Si ha lanzado el Centro de control de ZENworks desde Firefox, haga clic en *Guardar archivo* para guardar el archivo en una ubicación temporal y haga doble clic en el archivo para instalar el visor.

En Linux:

- 1 En el Centro de control de ZENworks, haga clic en *Configuración*.
- 2 En el panel de navegación izquierdo, haga clic en *Descargar herramientas de ZENworks*.
- 3 En el panel de navegación izquierdo de la página de descargas de ZENworks, haga clic en *Herramientas administrativas*.
- 4 Haga clic en `novell-zenworks-rm-viewer-<versión>.noarch.rpm`.
- 5 Decida entre instalar el visor inmediatamente o guardar el archivo RPM para instalarlo después.
 - ♦ Para llevar a cabo la instalación inmediatamente, haga clic en *Abrir con* para abrir el visor de gestión remota con zen-installer, especifique la contraseña del usuario Root y haga clic en *Aceptar*.
 - ♦ Para guardar el archivo RPM del visor en el directorio de descarga por defecto para instalarlo posteriormente, haga clic en *Guardar en disco*. Para instalar el archivo RPM, realice una de las siguientes acciones:
 - ♦ Haga clic en el archivo RPM del visor, especifique la contraseña del usuario Root y haga clic en *Aceptar*.
 - ♦ Ejecute el siguiente comando como superusuario o como usuario Root:

```
rpm -ivh novell-zenworks-rm-viewer-<versión>.noarch.rpm
```


2.7 Actualización del visor de gestión remota

Si lleva a cabo una operación de gestión remota en un dispositivo gestionado con Windows en el que ya hay instalada una versión anterior del visor de gestión remota, el enlace *Actualizar visor de gestión remota* se mostrará en el Centro de control de ZENworks. Haga clic en ese enlace para actualizar la versión del visor instalada en el dispositivo.

Para actualizar el visor de gestión remota en un dispositivo con Linux desde Novell ZENworks 10 Configuration Management con SP1 (10.1) a Novell ZENworks 10 Configuration Management SP2 (10.2), ejecute el siguiente comando como superusuario o usuario Root:

```
rpm -Uvh --no-postun novell-zenworks-rm-viewer-version>.noarch.rpm
```

También puede desinstalar la versión anterior, `novell-zenworks-rm-viewer-10.1.x.x.rpm`, e instalar la nueva versión. Para obtener más información acerca de la instalación del visor, consulte la [Sección 2.6, “Instalación del visor de gestión remota”, en la página 31](#).

2.8 Inicio de operaciones de gestión remota

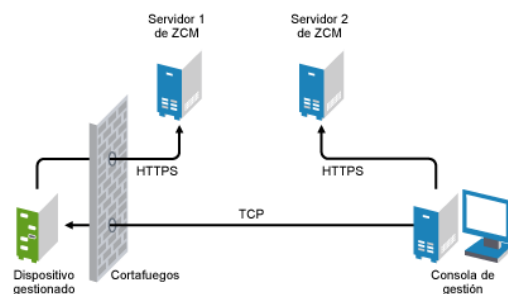
Las operaciones de gestión remota se pueden iniciar de las siguientes formas:

- [Sección 2.8.1, “Inicio de una sesión desde la consola de gestión”, en la página 33](#)
- [Sección 2.8.2, “Inicio de una sesión desde el dispositivo gestionado”, en la página 45](#)

2.8.1 Inicio de una sesión desde la consola de gestión

En esta situación, la sesión remota la inicia el administrador desde la consola de gestión. La consola de gestión se encuentra normalmente en una red corporativa y el dispositivo gestionado puede estar dentro o fuera de esa red. La siguiente ilustración representa una sesión remota iniciada en el dispositivo gestionado desde la consola de gestión.

Figura 2-1 Sesión iniciada desde la consola



El agente de gestión remota se inicia automáticamente cuando arranca el dispositivo gestionado. Cuando realiza la distribución del dispositivo gestionado, se crea una directiva para gestión remota por defecto en él. Se puede gestionar el dispositivo de forma remota con esta directiva por defecto en el modo de autenticación basada en derechos únicamente. Si crea una directiva para gestión remota nueva, sustituye a la directiva por defecto.

Si desea permitir que se establezcan conexiones desde una red pública en una red privada, distribuya el gateway de nivel de aplicación DNS (DNS_ALG). Para obtener más información sobre DNS_ALG, consulte [RFC 2694 \(http://www.ietf.org/rfc/rfc2694\)](http://www.ietf.org/rfc/rfc2694).

Si desea gestionar un dispositivo de forma remota utilizando su nombre DNS, asegúrese de que el servicio DNS dinámico esté disponible en la red.

El operador remoto puede iniciar una sesión de cualquiera de las siguientes formas:

- ♦ “Inicio de una operación de gestión remota en el Centro de control de ZENworks” en la página 34
- ♦ “Inicio de una operación de gestión remota en modo independiente” en la página 39
- ♦ “Inicio de una operación de gestión remota mediante las opciones de la línea de comandos” en la página 40

Inicio de una operación de gestión remota en el Centro de control de ZENworks

Puede iniciar las distintas operaciones de gestión remota desde el contexto del dispositivo o del usuario:

- ♦ “Inicio de una sesión de gestión remota desde el contexto del dispositivo” en la página 34
- ♦ “Inicio de una sesión de gestión remota desde el contexto del usuario” en la página 36

Inicio de una sesión de gestión remota desde el contexto del dispositivo

Para iniciar una sesión de gestión remota en un dispositivo:

- 1 En el Centro de control de ZENworks, haga clic en la pestaña *Dispositivos*.
- 2 Haga clic en *Servidores* o en *Estaciones de trabajo* y seleccione el dispositivo que desea gestionar de forma remota. Haga clic en *Acción* y seleccione la operación de gestión remota que desea realizar.

O bien

En *Tareas de dispositivo* del panel izquierdo, seleccione la operación de gestión remota que desea realizar.

Las operaciones remotas disponibles son:

- ♦ **Control remoto:** muestra el recuadro de diálogo Gestión remota que permite realizar una operación de control remoto, vista remota o ejecución remota en el dispositivo gestionado.
 - ♦ **Diagnóstico remoto:** muestra el recuadro de diálogo Diagnóstico remoto que permite realizar una operación de diagnóstico remoto en el dispositivo gestionado.
 - ♦ **Transferir archivos:** muestra el recuadro de diálogo Transferencia de archivos que permite realizar una operación de transferencia de archivos en el dispositivo gestionado.
- 3 Complete las opciones del recuadro de diálogo que aparecerá. La tabla siguiente contiene información sobre las distintas opciones disponibles:

| Campo | Detalles |
|---|---|
| Dispositivo | Especifique el nombre de host o la dirección IP del dispositivo que desea gestionar de forma remota. |
| Funcionamiento | Seleccione el tipo de operación remota que desee realizar en el dispositivo gestionado. Esta opción sólo está disponible en el recuadro de diálogo Gestión remota. |
| Aplicación | Seleccione la aplicación que desee lanzar en el dispositivo que desee diagnosticar de forma remota. Esta opción sólo está disponible en el recuadro de diálogo Diagnóstico remoto. |
| Autenticación | <p>Seleccione el modo que desee utilizar para autenticarse en el dispositivo gestionado. Los modos de autenticación son:</p> <ul style="list-style-type: none"> ♦ Autenticación basada en derechos ♦ Autenticación basada en contraseña |
| Puerto | Especifique el número de puerto en el que escucha el servicio de gestión remota. Por defecto, el número de puerto es 5950. |
| Modo de sesión | <p>Seleccione uno de los siguientes modos para la sesión:</p> <ul style="list-style-type: none"> ♦ Colaborar: permite lanzar una sesión de control remoto y de vista remota en el modo de colaboración. Este modo se selecciona por defecto para la operación de control remoto. Si se lanza la sesión de control remoto en el dispositivo gestionado primero, se obtienen los privilegios de un operador remoto maestro, que incluyen: <ul style="list-style-type: none"> ♦ Invitar a otros operadores a unirse a la sesión remota. ♦ Delegar derechos de control remoto a un operador remoto. ♦ Recuperar el control del operador remoto. ♦ Terminar la sesión remota. <p>Las sesiones siguientes que se lancen son sesiones de vista remota.</p> ♦ Compartido: permite que varios usuarios remotos controlen de forma simultánea el dispositivo gestionado. ♦ Exclusivo: permite mantener una sesión remota exclusiva en el dispositivo gestionado. No se puede iniciar ninguna otra sesión remota en el dispositivo gestionado una vez que se lanza una sesión en modo exclusivo. Este modo se selecciona por defecto para la operación de vista remota. <p>Esta opción sólo está disponible en el recuadro de diálogo Gestión remota.</p> |
| Cifrado de sesión | Garantiza que la sesión remota está protegida con el cifrado SSL (protocolo TLSv1). |
| Habilitar almacenamiento en el caché | Habilita el almacenamiento en caché de los datos de una sesión de gestión remota para mejorar el rendimiento. Esta opción está disponible para las operaciones de control remoto, visualización remota y diagnóstico remoto. Esta opción sólo se admite en Windows en este momento. |
| Habilitar la optimización del ancho de banda dinámico | Permite detectar el ancho de banda de red disponible y ajustar en función de ello los valores de la sesión a fin de mejorar el rendimiento. Esta opción está disponible para las operaciones de control remoto, visualización remota y diagnóstico remoto. |

| Campo | Detalles |
|---------------------------------------|---|
| Habilitar registro | Registra información de la sesión y de depuración en el archivo <code>novell-zenworks-vncviewer.txt</code> . El archivo se guarda por defecto en el escritorio si se lanza el Centro de control de ZENworks desde Internet Explorer, o en el directorio de instalación del programa si se lanza a través de Mozilla* FireFox *. |
| Encaminar a través del servidor proxy | <p>Permite encaminar la operación de gestión remota del dispositivo gestionado a través de un servidor proxy de gestión remota. Si el dispositivo gestionado se encuentra en una red privada o al otro lado de un cortafuegos o router que utilice NAT (conversión de la dirección de red), la operación de gestión remota se puede encaminar a través de un servidor proxy de gestión remota. Esta opción sólo se admite en Windows en este momento.</p> <p>Cumplimente los siguientes campos:</p> <p>Servidor proxy: especifique el nombre DNS o la dirección IP del servidor proxy de gestión remota. Por defecto, el servidor proxy configurado en el panel Valores de servidor proxy para realizar la operación remota en el dispositivo aparece en este campo. Puede especificar un servidor proxy distinto.</p> <p>Puerto del servidor proxy: especifique el número de puerto en el que escucha el servidor proxy de gestión remota. Por defecto, el puerto es el 5750.</p> <hr/> <p>Nota: la auditoría de gestión remota muestra la dirección IP del dispositivo que ejecuta el servidor proxy de gestión remota, no la dirección IP de la consola de gestión.</p> <hr/> <p>Utilizar el siguiente par de claves para la identificación</p> <p>Si se utiliza una autoridad certificadora (CA) interna, no se muestran las opciones siguientes. Si se utiliza una autoridad certificadora (CA) externa, rellene los campos siguientes:</p> <p>Clave privada: haga clic en <i>Examinar</i> para buscar y seleccionar la clave privada del operador remoto.</p> <p>Certificado: haga clic en <i>Examinar</i> para buscar y seleccionar el certificado correspondiente a la clave privada. Este certificado debe estar encadenado a la autoridad certificadora configurada en la zona.</p> <p>Los formatos que se admiten para la clave y el certificado son: DER, PEM y PFX. Si se utiliza el formato PFX, tanto la clave como el certificado deben estar disponibles en el mismo archivo. Deberá proporcionar el archivo como entrada para la clave y el certificado.</p> <p>Habilitar vía de caché: permite que las vías de la clave primaria y el certificado se almacenen en caché en la consola de gestión.</p> <p>Esta opción sólo se admite en Windows en este momento.</p> |

4 Haga clic en *Aceptar* para lanzar la operación remota seleccionada.

Inicio de una sesión de gestión remota desde el contexto del usuario

Si desea prestar asistencia a un usuario realizando una sesión remota en el dispositivo gestionado en el que haya entrado:

- 1 En el Centro de control de ZENworks, haga clic en la pestaña *Usuarios*.
- 2 Haga clic en el origen de usuarios.

- 3 Seleccione el usuario para gestionar de forma remota el dispositivo al que haya entrado.
- 4 Haga clic en *Acción* y seleccione la operación de gestión remota que desea realizar.

Las operaciones disponibles son:

- ♦ **Control remoto:** muestra el recuadro de diálogo Gestión remota que permite realizar una operación de control remoto, vista remota o ejecución remota en el dispositivo gestionado.
 - ♦ **Diagnóstico remoto:** muestra el recuadro de diálogo Diagnóstico remoto que permite realizar una operación de diagnóstico remoto en el dispositivo gestionado.
 - ♦ **Transferir archivos:** muestra el recuadro de diálogo Transferencia de archivos que permite realizar una operación de transferencia de archivos en el dispositivo gestionado.
- 5 Complete las opciones del recuadro de diálogo que aparecerá. La tabla siguiente contiene información sobre las distintas opciones disponibles:

| Campo | Detalles |
|---|---|
| Dispositivo | Especifique el nombre de host o la dirección IP del dispositivo que desea gestionar de forma remota. |
| Funcionamiento | Seleccione el tipo de operación remota que desee realizar en el dispositivo gestionado. Esta opción sólo está disponible en el recuadro de diálogo Gestión remota. |
| Aplicación | Seleccione la aplicación que desee lanzar en el dispositivo que desee diagnosticar de forma remota. Esta opción sólo está disponible en el recuadro de diálogo Diagnóstico remoto. |
| Autenticación | <p>Seleccione el modo que desee utilizar para autenticarse en el dispositivo gestionado. Los modos de autenticación son:</p> <ul style="list-style-type: none"> ♦ Autenticación basada en derechos ♦ Autenticación basada en contraseña |
| Puerto | Especifique el número de puerto en el que escucha el servicio de gestión remota. Por defecto, el número de puerto es 5950. |
| Modo de sesión | <p>Seleccione uno de los siguientes modos para la sesión:</p> <ul style="list-style-type: none"> ♦ Colaborar: permite lanzar una sesión de control remoto y de vista remota en el modo de colaboración. Este modo se selecciona por defecto para la operación de control remoto. Si se lanza la sesión de control remoto en el dispositivo gestionado primero, se obtienen los privilegios de un operador remoto maestro, que incluyen: <ul style="list-style-type: none"> ♦ Invitar a otros operadores a unirse a la sesión remota. ♦ Delegar derechos de control remoto a un operador remoto. ♦ Recuperar el control del operador remoto. ♦ Terminar la sesión remota. <p>Las sesiones siguientes que se lancen son sesiones de vista remota.</p> ♦ Compartido: permite que varios usuarios remotos controlen de forma simultánea el dispositivo gestionado. ♦ Exclusivo: permite mantener una sesión remota exclusiva en el dispositivo gestionado. No se puede iniciar ninguna otra sesión remota en el dispositivo gestionado una vez que se lanza una sesión en modo exclusivo. Este modo se selecciona por defecto para la operación de vista remota. <p>Esta opción sólo está disponible en el recuadro de diálogo Gestión remota.</p> |
| Cifrado de sesión | Garantiza que la sesión remota está protegida con el cifrado SSL (protocolo TLSv1). |
| Habilitar almacenamiento en el caché | Habilita el almacenamiento en caché de los datos de una sesión de gestión remota para mejorar el rendimiento. Esta opción está disponible para las operaciones de control remoto, visualización remota y diagnóstico remoto. Esta opción sólo se admite en Windows en este momento. |
| Habilitar la optimización del ancho de banda dinámico | Permite detectar el ancho de banda de red disponible y ajustar en función de ello los valores de la sesión a fin de mejorar el rendimiento. Esta opción está disponible para las operaciones de control remoto, visualización remota y diagnóstico remoto. |

| Campo | Detalles |
|---------------------------------------|---|
| Habilitar registro | Registra información de la sesión y de depuración en el archivo <code>novell-zenworks-vncviewer.txt</code> . El archivo se guarda por defecto en el escritorio si se lanza el Centro de control de ZENworks desde Internet Explorer, o en el directorio de instalación del programa si se lanza a través de Mozilla* FireFox *. |
| Encaminar a través del servidor proxy | <p>Permite encaminar la operación de gestión remota del dispositivo gestionado a través de un servidor proxy de gestión remota. Si el dispositivo gestionado se encuentra en una red privada o al otro lado de un cortafuegos o router que utilice NAT (conversión de la dirección de red), la operación de gestión remota se puede encaminar a través de un servidor proxy de gestión remota. Esta opción sólo se admite en Windows en este momento.</p> <p>Cumplimente los siguientes campos:</p> <p>Servidor proxy: especifique el nombre DNS o la dirección IP del servidor proxy de gestión remota. Por defecto, el servidor proxy configurado en el panel Valores de servidor proxy para realizar la operación remota en el dispositivo aparece en este campo. Puede especificar un servidor proxy distinto.</p> <p>Puerto del servidor proxy: especifique el número de puerto en el que escucha el servidor proxy de gestión remota. Por defecto, el puerto es el 5750.</p> <hr/> <p>Nota: la auditoría de gestión remota muestra la dirección IP del dispositivo que ejecuta el servidor proxy de gestión remota, no la dirección IP de la consola de gestión.</p> <hr/> <p>Utilizar el siguiente par de claves para la identificación</p> <p>Si se utiliza una autoridad certificadora (CA) interna, no se muestran las opciones siguientes. Si se utiliza una autoridad certificadora (CA) externa, rellene los campos siguientes:</p> <p>Clave privada: haga clic en <i>Examinar</i> para buscar y seleccionar la clave privada del operador remoto.</p> <p>Certificado: haga clic en <i>Examinar</i> para buscar y seleccionar el certificado correspondiente a la clave privada. Este certificado debe estar encadenado a la autoridad certificadora configurada en la zona.</p> <p>Los formatos que se admiten para la clave y el certificado son: DER, PEM y PFX. Si se utiliza el formato PFX, tanto la clave como el certificado deben estar disponibles en el mismo archivo. Deberá proporcionar el archivo como entrada para la clave y el certificado.</p> <p>Habilitar vía de caché: permite que las vías de la clave primaria y el certificado se almacenen en caché en la consola de gestión.</p> <p>Esta opción sólo se admite en Windows en este momento.</p> |

6 Haga clic en *Aceptar* para lanzar la operación remota seleccionada.

Inicio de una operación de gestión remota en modo independiente

Antes de iniciar la operación de gestión remota en el modo independiente, instale el visor de gestión remota:

Lleve a cabo los pasos siguientes para instalar el visor:

1 En el Centro de control de ZENworks, haga clic en *Configuración*

- 2 En el panel de navegación izquierdo, haga clic en *Descargar herramientas de ZENworks*.
- 3 En el panel de navegación izquierdo de la página de descargas de ZENworks, haga clic en *Herramientas administrativas*.
- 4 Haga clic en `novell-zenworks-rm-viewer-versión.msi` y guarde el archivo en una ubicación temporal.
- 5 Haga doble clic en el archivo `.msi` para instalar la última versión del visor de gestión remota de ZENworks.

El archivo se instala automáticamente en el directorio `C:\Document and Settings\usuario\ApplicationData\Novell\ZENworks\Remote Management\bin`.

Para iniciar la operación de gestión remota en modo independiente:

- 1 Haga doble clic en el archivo `nzrViewer.exe` para lanzar el cliente de gestión remota de ZENworks.
- 2 En la ventana de conexión de gestión remota de ZENworks que aparecerá, especifique el nombre DNS o la dirección IP del dispositivo gestionado y el número de puerto con el formato *Dirección IP~Puerto*. Por ejemplo, `10.0.0.0~1000`.
- 3 Indique el nombre DNS o la dirección IP del servidor proxy de gestión remota y el número de puerto en uno de los siguientes formatos:
 - ♦ *Dirección IP~Puerto*. Por ejemplo: `10.0.0.0~5750`.
 - ♦ *Dirección IP~Puerto*. Por ejemplo: `10.0.0.0~50`.
- 4 Haga clic en *Conectar*.

Si la autenticación es correcta, se inicia la sesión remota. Por defecto, se lanza una sesión de control remoto.

Inicio de una operación de gestión remota mediante las opciones de la línea de comandos

Antes de lanzar una operación de gestión remota desde la línea de comandos, compruebe que la opción *Permitir conexión si la consola de gestión remota no tiene un certificado SSL* de los valores de seguridad de la directiva de gestión remota está habilitada.

Para instalar el visor de gestión remota:

- 1 En el Centro de control de ZENworks, haga clic en *Configuración*
- 2 En el panel de navegación izquierdo, haga clic en *Descargar herramientas de ZENworks*.
- 3 En el panel de navegación izquierdo de la página de descargas de ZENworks, haga clic en *Herramientas administrativas*.
- 4 Haga clic en `novell-zenworks-rm-viewer-versión.msi` y guarde el archivo en una ubicación temporal.
- 5 Haga doble clic en el archivo `.msi` para instalar la última versión del visor de gestión remota de ZENworks.

El archivo se instala automáticamente en el directorio `C:\Document and Settings\usuario\ApplicationData\Novell\ZENworks\Remote Management\bin`.

Para iniciar la operación de gestión remota utilizando las opciones de la línea de comandos:

1 En el indicador de la línea de comandos, cambie al directorio donde esté instalado el archivo `novell-zenworks-rm-viewer-versión.msi`.

2 Ejecute el comando siguiente:

```
nzrViewer [/opciones<parámetros si los hay>][Dirección IP del dispositivo gestionado] [~~puerto] [/proxy servidor_proxy] [~~puerto]
```

El puerto por defecto del dispositivo gestionado es el 5950 y el del servidor proxy es el 5750.

Para obtener información sobre las opciones de la línea de comandos disponibles, consulte la [Tabla 2-1](#).

3 Haga clic en *Conectar*.

Si la autenticación es correcta, se inicia la sesión remota. Si no ha especificado el tipo de operación remota en la línea de comandos, se lanza una sesión de control remoto por defecto.

Sin embargo, las siguientes limitaciones se aplican al inicio de una operación de gestión remota desde las opciones de la línea de comandos:

- ♦ Si se utiliza una autoridad certificadora (CA) externa, se deben especificar las opciones de línea de comandos `key`, `cert` y `CACert` en el comando `nzrViewer` para la autenticación SSL. Si no desea especificar las opciones, asegúrese de que esté habilitada la opción *Permitir conexión si la consola de gestión remota no tiene un certificado SSL* en los valores de configuración de seguridad de la directiva de gestión remota. No se recomienda optar por esta posibilidad porque reduce la seguridad del dispositivo.
- ♦ Si el dispositivo gestionado forma parte de la zona de gestión, asegúrese de que el certificado que presenta el visor es válido, está firmado y está encadenado con la autoridad certificadora. Si no es así, fallará la autenticación SSL.

Nota: cuando se lanza una sesión remota desde el Centro de control de ZENworks, el certificado se genera automáticamente desde el Centro de control y se transfiere al visor para lanzar la sesión. El certificado sólo es válido durante cuatro días.

- ♦ El dispositivo gestionado emplea el certificado proporcionado por el visor para identificar al operador remoto. Si el visor no proporciona ningún certificado, el usuario no se identifica y aparece como *desconocido* en los registros de mensajes de permiso, señal sonora y auditoría.

Tabla 2-1 Opciones de la línea de comandos para lanzar una operación remota

| Opción de la línea de comandos | Parámetro | Descripción |
|--------------------------------|---------------|--|
| listen | <i>puerto</i> | Habilita la escucha para las peticiones de sesión remota en el puerto especificado. Por defecto, el puerto es el 5550. |
| restricted | | Oculto la barra de herramientas y el menú del sistema. |
| viewonly | | Lanza una operación de vista remota en el dispositivo gestionado. |
| remotecontrol | | Lanza una operación de control remoto en el dispositivo gestionado. |
| ftponly | | Lanza una operación de transferencia de archivos en el dispositivo gestionado. |

| Opción de la línea de comandos | Parámetro | Descripción |
|--------------------------------|--------------------------|--|
| remoteexecute | | Lanza una operación de ejecución remota en el dispositivo gestionado. |
| diagnostics | <i>nombre_aplicación</i> | Lanza una operación de diagnóstico remoto en el dispositivo gestionado. Si se especifica el parámetro de nombre de aplicación, se lanza esa aplicación en el dispositivo gestionado. |
| filecompressionlevel | <i>nivel</i> | <p>Proporciona los medios para optimizar el proceso de compresión de archivos para obtener más velocidad o mayor compresión durante una operación de transferencia de archivos. El nivel de compresión puede variar entre 0 y 9:</p> <ul style="list-style-type: none"> ♦ 0 indica que no se aplica compresión alguna ♦ 1 proporciona la velocidad mayor ♦ 9 proporciona el mayor nivel de compresión <p>Si no se especifica el nivel de compresión, se utiliza el nivel de compresión por defecto, 6, que está optimizado en términos de velocidad y compresión.</p> |
| noencrypt | | Lanza la sesión remota en modo no cifrado. |
| fullscreen | | Lanza una operación remota en modo de pantalla completa en el dispositivo gestionado. |
| notoolbar | | Oculto la barra de herramientas en la ventana de visualización. |
| exclusive | | Lanza la sesión remota en modo exclusivo. |
| 8bit | | Especifica la profundidad de color que se debe utilizar para representar los datos de la sesión. |
| compartido | | Habilita una conexión compartida, lo que permite compartir el escritorio con otros clientes que ya lo están usando. Esta opción tiene el valor True (verdadero) por defecto. |
| collaborate | | Lanza la sesión remota en modo de colaboración. |
| noshared | | Habilita una conexión sin compartir, con lo que se desconectan los demás clientes conectados o se rechaza la nueva conexión, en función de la configuración del servidor. |
| swapmouse | | Cambia los botones del ratón. |
| nocursor | | Muestra sólo el puntero del ratón del dispositivo gestionado. El puntero del ratón local no se muestra. |
| dotcursor | | Muestra el puntero del ratón local como un punto. Esta opción tiene el valor True (verdadero) por defecto. |
| smalldotcursor | | Muestra el puntero del ratón local como un punto pequeño. |
| normalcursor | | Muestra el puntero del ratón local con la forma por defecto. |
| belldeiconify | | Permite la transmisión de un carácter de timbre que provoca que se emita un sonido en el visor. Esta opción hace también que se maximice un visor VNC minimizado cuando se recibe el carácter de timbre. |

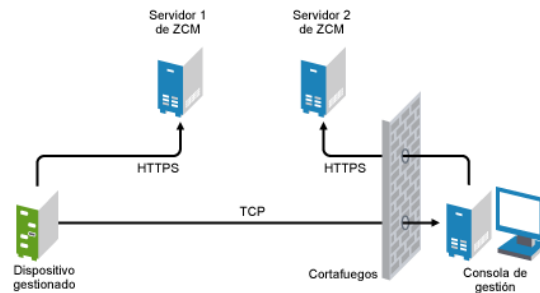
| Opción de la línea de comandos | Parámetro | Descripción |
|--|-----------------------|--|
| emulate3 | | Los usuarios que dispongan de un ratón con dos botones pueden simular un botón central presionando los dos botones a la vez. Esta opción tiene el valor True (verdadero) por defecto. |
| noemulate3 | | No se emula un ratón de tres botones. |
| nojpeg | | Inhabilita la compresión con pérdida JPEG. No se recomienda su uso porque se puede reducir la eficacia del codificador. Puede que le interese utilizar esta opción si es absolutamente necesario para obtener una calidad de imagen perfecta. |
| nocursorshape | | Inhabilita las actualizaciones de la forma del cursor para gestionar los movimientos del cursor remoto. El uso de las actualizaciones de la forma del cursor disminuye el retraso en relación con los movimientos del cursor remoto y puede mejorar el uso del ancho de banda drásticamente. |
| noremotecursor | | No muestra el cursor remoto. |
| fitwindow | | Oculto la barra de desplazamiento en la ventana de visualización. |
| scale | <i>percentage</i> | Amplía la ventana de visualización con el porcentaje de escala especificado. |
| emulate3timeout | <i>ms</i> | Especifica el tiempo límite para la simulación del ratón de tres botones. |
| disableclipboard | | Inhabilita la copia de datos en el portapapeles. |
| delay | | Reproduce un área de visualización y espera el intervalo de tiempo especificado antes de recuperar la siguiente actualización. |
| loglevel | <i>n</i> | Especifica los niveles de registro de información. |
| console | | Registra información en una ventana de consola. |
| logfile | <i>nombre_archivo</i> | Nombre del archivo de registro donde se debe registrar la información. |
| config | <i>nombre_archivo</i> | Nombre del archivo de configuración que se debe utilizar para cargar los valores de configuración predefinidos. |
| key | <i>nombre_archivo</i> | Nombre del archivo donde se almacena la clave privada. Esta clave se utiliza en las operaciones de enlace SSL con el dispositivo gestionado. |
| Importante: las opciones key y cert se deben utilizar juntas. Si se utilizan estas opciones con el comando <code>nzrViewer</code> , debe inhabilitar por motivos de seguridad la opción <i>Permitir conexión si la consola de gestión remota no tiene un certificado SSL</i> en los valores de seguridad de la directiva para gestión remota. | | |

| Opción de la línea de comandos | Parámetro | Descripción |
|--------------------------------|-----------------------|---|
| cert | <i>nombre_archivo</i> | Nombre del archivo donde se almacena el certificado correspondiente a la clave privada. Importante: las opciones key y cert se deben utilizar juntas. Si se utilizan estas opciones con el comando <code>nzrViewer</code> , debe inhabilitar por motivos de seguridad la opción <i>Permitir conexión si la consola de gestión remota no tiene un certificado SSL</i> en los valores de seguridad de la directiva para gestión remota. |
| CAcert | <i>nombre_archivo</i> | Nombre del archivo donde se almacena el certificado raíz. Este certificado se utiliza para comprobar el certificado del dispositivo gestionado durante operaciones de enlace SSL. |
| encoding | <i>encname</i> | Especifica el cifrado que se debe utilizar en la sesión. Los distintos tipos de cifrado son: Raw, CopyRect, RRE, CoRRE, Hextile, Zlib y Tight. |
| compresslevel | <i>n</i> | Especifica el nivel de compresión necesario para comprimir los datos de la sesión remota con valores entre 0 y 9. En el nivel 1 se emplea un mínimo de tiempo de la CPU y se consigue un grado de compresión débil, mientras que el nivel 9 ofrece mayor compresión pero es peor en lo que se refiere al consumo de tiempo de la CPU del servidor. Los niveles más altos se deben utilizar con conexiones de red muy lentas y los más bajos cuando se trabaje en redes LAN de alta velocidad. Se recomienda no utilizar el nivel de compresión 0. |
| quality | <i>n</i> | Especifica el nivel de calidad de JPEG, comprendido entre 0 y 9. El nivel de calidad 0 ofrece imágenes de muy poca calidad pero un impresionante grado de compresión, mientras que el nivel 9 ofrece imágenes de muy alta calidad con un grado de compresión inferior. |
| zenrights | | Especifica que se debe utilizar el esquema de autenticación basada en derechos de ZENworks. |
| zenpasswd | | Especifica que se debe utilizar el esquema de autenticación basada en contraseña de ZENworks. |
| locale | | Especifica la configuración regional en la que se deben mostrar los recursos. Por defecto, se utiliza el inglés. Los valores posibles para esta opción son: Inglés, Francés, Alemán, Español, Portugués, Japonés, Italiano, Chino(taiwanés) y Chino (tradicional). |
| proxy | <i>servidor_proxy</i> | Especifica el nombre DNS o la dirección IP del servidor proxy de gestión remota y el número de puerto en uno de los siguientes formatos: <ul style="list-style-type: none"> ◆ <i>Dirección IP~Puerto</i>. Por ejemplo: 10.0.0.0~5750. ◆ <i>Dirección IP~Puerto</i>. Por ejemplo: 10.0.0.0~50. |

2.8.2 Inicio de una sesión desde el dispositivo gestionado

En esta situación, la sesión remota la inicia el usuario del dispositivo gestionado. Resulta útil en los casos en que no se puede conectar con el dispositivo gestionado desde la consola de gestión. La siguiente ilustración representa una sesión remota iniciada por el usuario del dispositivo gestionado.

Figura 2-2 Sesión iniciada por el agente



El usuario del dispositivo gestionado puede solicitar que un operador remoto lleve a cabo una sesión remota en el dispositivo si:

- ♦ El operador remoto ha lanzado la escucha de gestión remota para escuchar la peticiones de sesión remota del usuario.
- ♦ La opción *Permitir que el usuario solicite una sesión remota* está habilitada en la directiva para gestión remota.
- ♦ El puerto en el que la escucha de gestión remota atiende las conexiones remotas debe estar abierto en el cortafuegos de la consola de gestión. El puerto por defecto es 5550.

Para pedir una sesión:

- 1 Haga doble clic en el icono de ZENworks del área de notificación.
- 2 En el panel izquierdo, diríjase a *Gestión remota* y haga clic en *General*.
- 3 Haga clic en *Pedir sesión remota* para acceder al recuadro de diálogo Pedir sesión.

El administrador determinará si es posible pedir una sesión de control remoto, lo que significa que esta opción puede estar inhabilitada, sobre todo si la empresa o el departamento no cuenta con personal de servicio de asistencia técnica para atender como operadores remotos. Si la opción *Pedir sesión remota* no aparece como un texto enlazado, la opción no está disponible.

- 4 En la lista *Operadores remotos a la escucha*, seleccione el operador remoto con el que desee abrir una sesión remota.

O bien

Si el operador remoto no está incluido en la lista, proporcione la información de conexión correspondiente en los campos *Pedir conexión*.

- 5 En el campo *Operación*, seleccione el tipo de operación que desea abrir (Control remoto, Vista remota, Diagnóstico remoto, Transferencia de archivos o Ejecución remota).

Para obtener información sobre las distintas operaciones, consulte la [Sección 1.2, “Descripción de las operaciones de gestión remota”](#), en la [página 12](#).

- 6 Haga clic en *Pedir* para lanzar la sesión.

Si desea permitir que se establezcan conexiones desde una red pública en una red privada, distribuya el gateway de nivel de aplicación DNS (DNS_ALG). Para obtener más información sobre DNS_ALG, consulte [RFC 2694 \(http://www.ietf.org/rfc/rfc2694\)](http://www.ietf.org/rfc/rfc2694).

2.9 Instalación de un servidor proxy de gestión remota

Si un dispositivo gestionado se encuentra en una red privada o al otro lado de un cortafuegos o router que utilice NAT (conversión de la dirección de red), la operación de gestión remota se puede encaminar a través de un servidor proxy de gestión remota. El servidor proxy sólo se puede instalar en un dispositivo gestionado Windows.

Para instalar el servidor proxy, lleve a cabo los pasos siguientes:

- 1 En el dispositivo, abra un navegador Web y acceda a la página de descargas de ZENworks:
`https://servidor/zenworks-setup`
donde *servidor* es el nombre DNS o la dirección IP de un servidor de ZENworks.
- 2 En el panel de navegación izquierdo, haga clic en *Herramientas administrativas*.
- 3 Haga clic en `novell-zenworks-rm-repeater-versión_producto.msi` y guarde el archivo en una ubicación temporal.

versión_producto corresponde a la versión del producto ZENworks.

- 4 Instale la aplicación del proxy ejecutando el siguiente comando:

```
msiexec /i novell-zenworks-rm-repeater-<versión>.msi  
TARGETDIR="Directorio_instalación_ZENworks"
```

Gestión de sesiones remotas

3

En las secciones siguientes se proporciona información que le ayudará a gestionar con eficacia las sesiones remotas de Novell® ZENworks® 10 Configuration Management:

- ♦ Sección 3.1, “Gestión de una sesión de Control remoto”, en la página 47
- ♦ Sección 3.2, “Gestión de una sesión de Vista remota”, en la página 51
- ♦ Sección 3.3, “Gestión de una sesión de Ejecución remota”, en la página 52
- ♦ Sección 3.4, “Gestión de una sesión de Diagnóstico remoto”, en la página 52
- ♦ Sección 3.5, “Gestión de una sesión de Transferencia de archivos”, en la página 54
- ♦ Sección 3.6, “Activación de un dispositivo remoto”, en la página 57
- ♦ Sección 3.7, “Mejora del rendimiento de la gestión remota”, en la página 58




3.1 Gestión de una sesión de Control remoto








La gestión remota permite controlar de forma remota los dispositivos gestionados. Con las conexiones de control remoto, el operador remoto puede no sólo ver el dispositivo gestionado, sino también asumir el control del dispositivo, lo que permite proporcionar asistencia al usuario y resolver los problemas que puedan darse en él. Para obtener información sobre el lanzamiento de una sesión de control remoto, consulte la [Sección 2.8, “Inicio de operaciones de gestión remota”, en la página 33](#).





3.1.1 Uso de las opciones de la barra de herramientas en el visor de gestión remota

La siguiente tabla describe las distintas opciones que están disponibles en la barra de herramientas del visor de gestión remota durante las sesiones de control remoto. Además incluye las teclas de acceso directo si están disponibles.

Tabla 3-1 Opciones de la barra de herramientas del visor de gestión remota

| Opción | Tecla de acceso directo | Función |
|---|-------------------------|--|
| <i>Opciones de conexión</i>  | Ctrl+Alt+Mayús+P | Permite configurar distintos parámetros de sesión, como el formato y el cifrado para mejorar el rendimiento, el registro o la gestión del cursor local y remoto. |
| <i>Información de conexión</i>  | Ctrl+Alt+Mayús+I | Proporciona el nombre de host, el puerto, la resolución de pantalla y la versión del protocolo del dispositivo gestionado. |
| <i>Pantalla completa</i>  | Ctrl+Alt+Mayús+F | Permite alternar entre los modos de pantalla completa y normal. |

| Opción | Tecla de acceso directo | Función |
|--|-------------------------|---|
| <i>Pedir actualización de pantalla</i>  | Ctrl+Alt+Mayús+H | Renueva la ventana de visualización. |
| <i>Enviar Ctrl+Alt+Supr</i>  | | Transfiere la pulsación de las teclas Ctrl+Alt+Supr al dispositivo gestionado. |
| <i>Enviar Ctrl+Esc</i>  | | Activa el menú Inicio en el dispositivo gestionado. |
| <i>Enviar presión/ liberación de tecla Alt</i>  | | Al hacer clic en esta opción y pulsar la tecla ALT en el teclado, se envía la pulsación de la tecla Alt al dispositivo gestionado. |
| <i>Borrar o mostrar pantalla</i>  | Ctrl+Alt+Mayús+B | <p>Borra el contenido de la pantalla del dispositivo gestionado o lo muestra. Cuando esto ocurre, el usuario del dispositivo no puede ver las operaciones que realiza en él el operador remoto. Además, se bloquean los controles del teclado y el ratón del dispositivo gestionado.</p> <p>Esta opción sólo se habilita si la opción <i>Permitir que la pantalla del dispositivo remoto esté en blanco</i> está activada en la directiva para gestión remota vigente en el dispositivo gestionado.</p> |
| <i>Bloquear o desbloquear teclado y ratón</i>  | Ctrl+Alt+Mayús+L | <p>Bloquea o desbloquea el teclado y el ratón del dispositivo gestionado. Cuando se bloquean los controles del teclado y el ratón, el usuario del dispositivo gestionado no los puede utilizar.</p> <p>Esta opción sólo se habilita si la opción <i>Permitir que se bloqueen el ratón y el teclado del dispositivo gestionado</i> está activada en la directiva para gestión remota vigente en el dispositivo gestionado.</p> |
| <i>Transferir archivos</i>  | Ctrl+Alt+Mayús+T | <p>Lanza una sesión de transferencia de archivos desde el dispositivo gestionado y hacia él.</p> <p>Esta opción sólo se habilita si la opción <i>Permitir la transferencia de archivos en el dispositivo gestionado</i> está activada en la directiva para gestión remota vigente en el dispositivo gestionado. Para obtener más información sobre la transferencia de archivos, consulte la Sección 3.5, “Gestión de una sesión de Transferencia de archivos”, en la página 54.</p> |

| Opción | Tecla de acceso directo | Función |
|--|-------------------------|---|
| Colaboración  | | <p>Lanza una sesión de colaboración de gestión remota de ZENworks en el dispositivo gestionado, lo que permite invitar a varios operadores remotos a unirse a la sesión de gestión remota. También se pueden delegar los derechos de control remoto a otro operador para que ayude a resolver un problema. Esta opción sólo se admite en Windows en este momento.</p> <p>Para obtener más información sobre la función de colaboración, consulte la Sección 3.1.2, “Sesión de colaboración”, en la página 49.</p> |
| Ejecución remota  | Ctrl+Alt+Mayús+U | <p>Lanza una sesión de ejecución remota en el dispositivo gestionado que permite lanzar de forma remota cualquier ejecutable en el dispositivo gestionado.</p> <p>Esta opción sólo se habilita si la opción <i>Permitir que se ejecuten programas de forma remota en el dispositivo gestionado</i> está activada en la directiva para gestión remota vigente en el dispositivo gestionado.</p> |
| Anular protector de pantalla  | Ctrl+Alt+Mayús+O | <p>Anula el protector de pantalla protegido mediante contraseña del dispositivo durante la sesión remota.</p> <p>Esta opción se habilita sólo si la opción <i>Permitir que el protector de pantalla se desbloquee automáticamente durante el control remoto</i> está activada en la directiva para gestión remota vigente en el dispositivo gestionado.</p> |
| Desconectar  | Alt+F4 | <p>Cierra la sesión remota.</p> |

3.1.2 Sesión de colaboración

La función de sesión de colaboración permite invitar a varios operadores remotos a que se unan a la sesión de gestión remota si han lanzado la escucha de gestión remota para atender las peticiones de sesión remota. También se pueden delegar los derechos de control remoto a un operador remoto para que ayude a resolver un problema y, posteriormente, recuperar el control. Esta opción sólo se admite en Windows en este momento.


Si se lanza la sesión de control remoto en el dispositivo gestionado primero, se obtienen los privilegios del operador remoto maestro. Puede usar la sesión de colaboración para lo siguiente:

- ♦ Invitar a varios operadores a que se unan a la sesión de control remoto.
- ♦ Delegar los derechos de control remoto a un operador remoto para que ayude a resolver un problema y, posteriormente, recuperar el control.
- ♦ Terminar una sesión remota.

Para lanzar una sesión de colaboración:

- 1 Lance la sesión de control remoto en el dispositivo gestionado en el modo de colaboración.

Para obtener información sobre el lanzamiento de una sesión de control remoto, consulte la [Sección 2.8, “Inicio de operaciones de gestión remota”, en la página 33](#).

- 2 En la barra de herramientas del visor de gestión remota, haga clic en  para acceder a la ventana de sesión de colaboración.

La ventana de sesión de colaboración muestra los operadores remotos que se han añadido en la directiva de gestión remota vigente en el dispositivo. Cada operador remoto constituye una entrada independiente precedida por un círculo de color:

- ♦ Un círculo gris indica que el operador remoto no se ha unido a la sesión.
- ♦ Un círculo rojo indica que el operador remoto se ha unido a la sesión y se encuentra en modo de vista remota..
- ♦ Un círculo verde indica que el operador remoto se ha unido a la sesión y se le han delegado los derechos de control remoto de la sesión.

Para obtener más información sobre la adición de operadores remotos, consulte la [“Sección 2.3, “Creación de la directiva de gestión remota”, en la página 21”](#).

La tabla siguiente recoge las acciones que puede realizar como operador remoto maestro durante una sesión de colaboración:

Tabla 3-2 Opciones de la ventana de sesión de colaboración

| Tarea | Pasos | Información adicional |
|--|--|---|
| Invitar a un operador remoto a que se una a la sesión remota | <ol style="list-style-type: none">1. Seleccione un operador remoto que aparezca en la ventana de sesión de colaboración.2. Haga clic en <i>Invitar</i>. | <p>Si el operador remoto acepta la petición y se une a la sesión, el círculo gris correspondiente cambia a rojo.</p> <p>Por defecto, la nueva sesión se inicia en el modo de vista remota.</p> |
| Delegar los derechos de control remoto al operador remoto | <ol style="list-style-type: none">1. Seleccione el operador remoto en el que desee delegar los derechos de control remoto.2. Haga clic en <i>Delegar</i>. | <p>El operador remoto seleccionado pasará al modo de control remoto y el círculo rojo correspondiente cambiará a verde.</p> <p>El operador remoto maestro pasará automáticamente al modo de vista remota.</p> |
| Recuperar los derechos de control remoto del operador remoto | <ol style="list-style-type: none">1. Haga clic en <i>Recuperar control</i>. | <p>El operador remoto cambia al modo de vista remota y el círculo verde correspondiente cambia a rojo.</p> <p>El operador remoto maestro cambia automáticamente al modo de control remoto.</p> |

| Tarea | Pasos | Información adicional |
|--------------------------------------|---|---|
| Terminar la sesión remota | <ol style="list-style-type: none"> 1. Seleccione el operador remoto cuya sesión remota desee terminar. 2. Haga clic en <i>Terminar</i>. | <p>Si el operador remoto seleccionado estaba en modo de control remoto, se recuperan los derechos de control remoto.</p> <p>La sesión del operador remoto termina y el color del círculo correspondiente cambia a gris.</p> |
| Invitar a un operador remoto externo | <ol style="list-style-type: none"> 1. Haga clic en <i>Invitar externo</i> para invitar a operadores remotos que no aparezcan en la ventana de sesión de colaboración a unirse a la sesión remota. 2. Especifique el nombre DNS o la dirección IP del dispositivo del operador remoto y el número de puerto. Por ejemplo, 10.0.0.0 ~1000. 3. Haga clic en <i>Invitar</i>. | |




El operador remoto maestro desconecta la sesión remota y a continuación termina la sesión para todos los operadores remotos.




3.2 Gestión de una sesión de Vista remota

La vista remota permite conectar de forma remota con un dispositivo gestionado para ver el escritorio. Para obtener información sobre el lanzamiento de una sesión de vista remota, consulte la [Sección 2.8, “Inicio de operaciones de gestión remota”, en la página 33](#).

La tabla siguiente describe las distintas opciones disponibles en la barra de herramientas del visor de gestión durante una sesión de vista remota.

Tabla 3-3 Opciones de la barra de herramientas del visor de gestión remota

| Opción | Tecla de acceso directo | Función |
|--|-------------------------|--|
|  Opciones de conexión | Ctrl+Alt+Mayús+P | Permite configurar distintos parámetros de sesión, como el formato y el cifrado para mejorar el rendimiento, el registro o la gestión del cursor local y remoto. |
|  Información de conexión | Ctrl+Alt+Mayús+I | Proporciona el nombre de host, el puerto, la resolución de pantalla y la versión del protocolo del dispositivo gestionado. |
|  Pantalla completa | Ctrl+Alt+Mayús+F | Permite alternar entre los modos de pantalla completa y normal. |

| Opción | Tecla de acceso directo | Función |
|---|-------------------------|--------------------------------------|
|  Pedir actualización de pantalla | Ctrl+Alt+Mayús+H | Renueva la ventana de visualización. |
|  Desconectar | Alt+F4 | Cierra la sesión remota. |
|  | | |

3.3 Gestión de una sesión de Ejecución remota

La ejecución remota permite iniciar ejecutables de forma remota con privilegios de sistema en el dispositivo gestionado. Para ejecutar una aplicación en el dispositivo gestionado, se debe iniciar la sesión de ejecución remota.

- 1 Lance la sesión de ejecución remota.

Para obtener información sobre el lanzamiento de una sesión de ejecución remota, consulte la [Sección 2.8, “Inicio de operaciones de gestión remota”, en la página 33.](#)

- 2 Especifique el nombre del ejecutable.

Si la aplicación no se encuentra en la vía del sistema del dispositivo gestionado, deberá proporcionar la vía completa de la aplicación. Si no especifica la extensión del archivo que desea ejecutar en el dispositivo gestionado, la ejecución remota le asignará la extensión `.exe`.

- 3 Haga clic en *Ejecutar*.

La ejecución remota de la aplicación especificada puede fallar si la aplicación no está disponible en la vía definida del dispositivo gestionado.

Advertencia: por defecto, el módulo de gestión remota se ejecuta como servicio con privilegios de sistema en el dispositivo gestionado. Por tanto, todas las aplicaciones que se lanzan durante la sesión de ejecución remota se ejecutan también con privilegios de sistema. Por motivos de seguridad, es muy recomendable cerrar la aplicación tras usarla.

3.4 Gestión de una sesión de Diagnóstico remoto

La gestión remota permite realizar diagnósticos remotos y analizar problemas en el dispositivo gestionado. Esta función ayuda a reducir el tiempo dedicado a la resolución de problemas y permite asistir a los usuarios sin necesidad de que un técnico se desplace para revisar el dispositivo que falla in situ. De esta forma, se aumenta la productividad del usuario, ya que los escritorios se mantienen activos y en funcionamiento.

Cuando se lanza una sesión de diagnóstico remoto en el dispositivo gestionado, se puede acceder únicamente a las aplicaciones de diagnóstico configuradas para el dispositivo en los valores de gestión remota para diagnosticar y resolver problemas en el dispositivo. Durante la sesión, las aplicaciones de diagnóstico se muestran como iconos de una barra de herramientas. Por defecto, se configuran las siguientes aplicaciones de diagnóstico en los valores de gestión remota:

Tabla 3-4 Opciones de la barra de herramientas del visor de gestión remota











| Opción | Tecla de acceso directo | Función |
|--|-------------------------|--|
|  Opciones de conexión | Ctrl+Alt+Mayús+P | Permite configurar distintos parámetros de sesión, como el formato y el cifrado para mejorar el rendimiento, el registro o la gestión del cursor local y remoto. |
|  Información de conexión | Ctrl+Alt+Mayús+I | Proporciona el nombre de host, el puerto, la resolución de pantalla y la versión del protocolo del dispositivo gestionado. |
|  Pantalla completa | Ctrl+Alt+Mayús+F | Permite alternar entre los modos de pantalla completa y normal. |
|  Pedir actualización de pantalla | Ctrl+Alt+Mayús+H | Renueva la ventana de visualización. |
|  Transferir archivos | Ctrl+Alt+Mayús+T | <p>Lanza una sesión de transferencia de archivos desde el dispositivo gestionado y hacia él.</p> <p>Esta opción sólo se habilita si la opción <i>Permitir la transferencia de archivos en el dispositivo gestionado</i> está activada en la directiva para gestión remota vigente en el dispositivo gestionado. Para obtener más información sobre la transferencia de archivos, consulte la Sección 3.5, “Gestión de una sesión de Transferencia de archivos”, en la página 54.</p> |
|  Desconectar | Alt+F4 | Cierra la sesión remota. |

Tabla 3-5 Aplicaciones de diagnóstico remoto

| Icono | Aplicación |
|---|--------------------------|
|  | Información de sistema |
|  | Administrador de equipos |
|  | Servicios |
|  | Editor del Registro |

Puede configurar las aplicaciones que se deben ejecutar en el dispositivo gestionado durante la sesión de diagnóstico remoto. Para obtener más información sobre la configuración de las aplicaciones de diagnóstico, consulte la [Sección 2.1, “Configuración de los ajustes de gestión remota”](#), en la página 17.



3.5 Gestión de una sesión de Transferencia de archivos





La gestión remota permite transferir archivos entre la consola de gestión y el dispositivo gestionado. Para obtener más información sobre el lanzamiento de una sesión de transferencia de archivos, consulte la [Sección 2.8, “Inicio de operaciones de gestión remota”](#), en la [página 33](#).



En la ventana Transferencia de archivos, el panel del equipo local muestra todos los archivos y carpetas en la consola de gestión, y el panel del equipo remoto muestra todos los archivos y carpetas en el directorio especificado en la opción *Directorio raíz de transferencia de archivo* en la directiva para gestión remota. Si no se ha especificado *Directorio raíz de transferencia de archivo* en la directiva, o si el dispositivo gestionado no tiene ninguna directiva asociada, podrá realizar operaciones de transferencia de archivos en todo el sistema de archivos del dispositivo remoto.

La tabla siguiente describe los controles y las opciones que están disponibles cuando se trabaja con archivos desde la ventana de transferencia de archivos. El menú *Acciones* no se puede usar todavía en Linux. Sin embargo, puede realizar la operación haciendo clic en el icono correspondiente de la barra de herramientas.

Tabla 3-6 Opciones de la ventana de transferencia de archivos

| Tareas | Teclas aceleradoras | Pasos | Información adicional |
|----------------------------|---------------------|--|-----------------------|
| Crear nueva carpeta local | Alt+L | <ol style="list-style-type: none">Haga clic en <i>Acciones</i> > <i>Nueva carpeta local</i>. O bien Haga clic en  en el panel del equipo local.Siga las indicaciones que aparecen en la pantalla. | |
| Crear nueva carpeta remota | Alt+V | <ol style="list-style-type: none">Haga clic en <i>Acciones</i> > <i>Nueva carpeta remota</i>. O bien Haga clic en  en el panel del equipo remoto.Siga las indicaciones que aparecen en la pantalla. | |
| Abrir un archivo | | <ol style="list-style-type: none">Haga doble clic en el archivo para abrirlo en su aplicación asociada. | |

| Tareas | Teclas aceleradoras | Pasos | Información adicional |
|--|---------------------|--|--|
| Cambiar el nombre de archivos o carpetas | Alt+N | <ol style="list-style-type: none"> 1. Seleccione el archivo o la carpeta cuyo nombre desee cambiar. 2. Haga clic en <i>Acciones</i> > <i>Renombrar</i>. O bien Haga clic en . 3. Siga las indicaciones que aparecen en la pantalla. | |
| Suprimir archivos o carpetas | Alt+D | <ol style="list-style-type: none"> 1. Seleccione los archivos o las carpetas que desee suprimir. 2. Haga clic en <i>Acciones</i> > <i>Suprimir</i>. O bien Haga clic en . 3. Siga las indicaciones que aparecen en la pantalla. | Puede utilizar las teclas Mayús y Ctrl para seleccionar varios archivos a la vez. |
| Actualizar carpeta local | Alt+E | <ol style="list-style-type: none"> 1. Haga clic en <i>Acciones</i> > <i>Actualizar carpeta local</i>. O bien Haga clic en  en el panel del equipo local. | |
| Actualizar carpeta remota | Alt+M | <ol style="list-style-type: none"> 1. Haga clic en <i>Acciones</i> > <i>Actualizar carpeta remota</i>. O bien Haga clic en  en el panel del equipo remoto. | |
| Ordenar archivos locales | | <ol style="list-style-type: none"> 1. Haga clic en <i>Acciones</i> > <i>Ordenar local</i>. 2. Seleccione el tipo de orden. Es posible ordenar los archivos por nombre, tamaño o fecha. | También se pueden ordenar haciendo clic en los encabezados de columna respectivos. |

| Tareas | Teclas aceleradoras | Pasos | Información adicional |
|------------------------------------|---------------------|--|--|
| Ordenar archivos remotos | | <ol style="list-style-type: none"> 1. Haga clic en <i>Acciones</i> > <i>Ordenar remoto</i> 2. Seleccione el tipo de orden. Es posible ordenar los archivos por nombre, tamaño o fecha. | También se pueden ordenar haciendo clic en los encabezados de columna respectivos. |
| Cargar archivos o carpetas | | <ol style="list-style-type: none"> 1. Seleccione los archivos que desee cargar en el equipo remoto. 2. Seleccione la carpeta de destino en el panel del equipo remoto. 3. Haga clic en <i>Acciones</i> > <i>Cargar</i>. <p>O bien Haga clic en ➡.</p> | <p>La opción <i>Acción</i> > <i>Cargar</i> sólo está disponible si el equipo activado es el local.</p> <p>Puede utilizar las teclas Mayús y Ctrl para seleccionar varios archivos a la vez.</p> |
| Descargar archivos o carpetas | Alt+O | <ol style="list-style-type: none"> 1. Seleccione los archivos que desee descargar al equipo local. 2. Seleccione la carpeta de destino en el panel del equipo local. 3. Haga clic en <i>Acciones</i> > <i>Descargar</i>. <p>O bien Haga clic en ⬅.</p> | <p>La opción <i>Acción</i> > <i>Descargar</i> sólo está disponible si el equipo activado es el remoto.</p> <p>Puede utilizar las teclas Mayús y Ctrl para seleccionar varios archivos a la vez.</p> |
| Cancelar transferencia de archivos | Alt+C | <ol style="list-style-type: none"> 1. Haga clic en <i>Acciones</i> > <i>Cancelar transferencia de archivos</i>. | También puede cancelar la operación de transferencia de archivos haciendo clic en el botón de cancelación. |
| Mostrar propiedades del archivo | Alt+P | <ol style="list-style-type: none"> 1. Seleccione los archivos. 2. Haga clic en <i>Acciones</i> > <i>Propiedades</i>. <p>O bien Haga clic en .</p> | <p>Puede utilizar las teclas Mayús y Ctrl para seleccionar varios archivos a la vez.</p> <p>Muestra el tamaño acumulado de los archivos y las carpetas seleccionados.</p> |
| Mover a la carpeta padre | | <ol style="list-style-type: none"> 1. Haga clic en  para desplazarse a la carpeta padre. | |

3.6 Activación de un dispositivo remoto

La activación remota permite activar de forma remota un único nodo o un grupo de nodos desactivados de la red, siempre que la tarjeta de red del nodo esté habilitada para la reactivación en LAN.

- ♦ Sección 3.6.1, “Requisitos previos”, en la página 57
- ♦ Sección 3.6.2, “Reactivación remota de los dispositivos gestionados”, en la página 57

3.6.1 Requisitos previos

Antes de reactivar los dispositivos gestionados, se deben cumplir los requisitos siguientes:

- ♦ Asegúrese de que la tarjeta de red del dispositivo gestionado admita la función de reactivación en LAN. Además, asegúrese de que ha habilitado la opción de reactivación en LAN en la configuración de BIOS del dispositivo gestionado.
- ♦ Asegúrese de que el dispositivo gestionado esté registrado en la zona de gestión de ZENworks.
- ♦ Asegúrese de que el nodo remoto esté en el estado de apagado por software. En este estado, la CPU está desconectada y la tarjeta de interfaz de red utiliza una cantidad mínima de alimentación eléctrica. A diferencia del estado hard-off, el estado soft-off permite que el equipo conserve la alimentación aunque esté apagado.

3.6.2 Reactivación remota de los dispositivos gestionados

Para realizar una reactivación remota:

- 1 En el Centro de control de ZENworks, haga clic en *Dispositivos*.
- 2 Haga clic en *Servidores* o en *Estaciones de trabajo* para que aparezca una lista de los dispositivos gestionados.
- 3 Seleccione el dispositivo que desea reactivar.
- 4 Haga clic en *Tareas rápidas* > *Activar* para acceder al recuadro de diálogo Activar.
- 5 Seleccione una de las opciones siguientes para especificar los servidores que deben enviar peticiones de activación a los dispositivos gestionados:
 - ♦ **Detectar el servidor automáticamente:** ZENworks detecta automáticamente el servidor primario más cercano al dispositivo gestionado. Si el servidor y el dispositivo remoto se encuentran en subredes distintas, asegúrese de que el router que los conecta esté configurado para remitir las difusiones orientadas a subredes a través del puerto UDP 1761.
 - ♦ **Utilice los siguientes dispositivos:** haga clic en *Añadir* para seleccionar un dispositivo servidor proxy que exista en la misma subred que el dispositivo que se debe activar.
Si el router está configurado para remitir las difusiones orientadas a subredes a través del puerto UDP 1761, no es necesario emplear un servidor proxy.
- 6 (Opcional) Seleccione una de las siguientes opciones para especificar la dirección IP que se debe utilizar para enviar la difusión de activación:
 - ♦ **Detectar la dirección IP automáticamente:** ZENworks detecta automáticamente la dirección de difusión de la subred para enviar la difusión de activación al dispositivo gestionado.

- ♦ **Use la siguiente dirección IP:** especifique la dirección IP para enviar la difusión de activación al dispositivo gestionado y haga clic en *Añadir*.
- 7** En la opción *Número de reintentos*, especifique el número de intentos permitidos para activar el dispositivo. El valor por defecto es 1.
- 8** En la opción *Intervalo de tiempo entre reintentos*, especifique el periodo de tiempo que debe transcurrir entre dos intentos. El valor por defecto es 2 minutos.
- 9** Haga clic en *Aceptar*.

Los valores por defecto para las opciones *Número de reintentos* e *Intervalo de tiempo entre reintentos* se configuran para la zona de gestión. Se pueden sustituir esos valores con otros que se configuren en el dispositivo.

3.7 Mejora del rendimiento de la gestión remota

El rendimiento de la gestión remota durante una sesión remota a través de un enlace de red lento o rápido cambia en función del tráfico de la red. Para obtener un tiempo de respuesta mejor, pruebe con una o varias de las posibilidades siguientes:

- ♦ **Sección 3.7.1, “En la consola de gestión”, en la página 58**
- ♦ **Sección 3.7.2, “En el dispositivo gestionado”, en la página 58**

3.7.1 En la consola de gestión

En la ventana Conexión de gestión remota de ZENworks de la consola, haga clic en *Opciones* y defina los valores siguientes:

- ♦ Para obtener el máximo rendimiento de la gestión remota a través de un enlace lento:
 - ♦ Seleccione la opción *Usar color de 8 bits*.
 - ♦ Defina el valor 6 en *Nivel de compresión personalizado*.
- ♦ Seleccione la opción *Bloquear eventos de movimiento del ratón*.
- ♦ Habilite la opción *Suprimir papel tapiz* en los valores de gestión remota.

3.7.2 En el dispositivo gestionado

- ♦ La velocidad de la sesión de gestión remota depende de la capacidad de procesamiento del dispositivo gestionado. Se recomienda emplear un equipo Pentium* III a 700 MHz (o superior) con 256 MB de RAM o más.
- ♦ No establezca un papel tapiz.

Las secciones siguientes proporcionan información relativa a la seguridad que debe conocer para utilizar el componente de gestión remota de Novell® ZENworks® 10 Configuration Management.

- ♦ Sección 4.1, “Autenticación”, en la página 59
- ♦ Sección 4.2, “Seguridad de las contraseñas”, en la página 61
- ♦ Sección 4.3, “Puertos”, en la página 61
- ♦ Sección 4.4, “Audit”, en la página 61
- ♦ Sección 4.5, “Solicitud de permiso al usuario del dispositivo gestionado”, en la página 62
- ♦ Sección 4.6, “Terminación anormal”, en la página 62
- ♦ Sección 4.7, “Detección de intrusos”, en la página 63
- ♦ Sección 4.8, “Identificación del operador remoto”, en la página 63
- ♦ Sección 4.9, “Configuración del navegador”, en la página 64
- ♦ Sección 4.10, “Seguridad de la sesión”, en la página 64

4.1 Autenticación

El servicio de gestión remota debe estar instalado en el dispositivo para que el operador remoto pueda gestionarlo de forma remota. El servicio se inicia automáticamente cuando arranca el dispositivo gestionado. Cuando un operador remoto inicia una sesión remota en el dispositivo gestionado, la sesión se inicia en el dispositivo sólo si el operador remoto está autorizado a realizar las operaciones remotas en el dispositivo gestionado.

Para evitar el acceso no autorizado al dispositivo gestionado, en el servicio de gestión remota del dispositivo gestionado se utilizan los siguientes modos de autenticación:

- ♦ Sección 4.1.1, “Autenticación de gestión remota basada en derechos”, en la página 59
- ♦ Sección 4.1.2, “Autenticación de gestión remota basada en contraseña”, en la página 60

4.1.1 Autenticación de gestión remota basada en derechos

En la autenticación basada en derechos, se asignan derechos al operador remoto para lanzar una sesión remota en el dispositivo gestionado. Por defecto, el administrador y el superadministrador de ZENworks tienen derechos para realizar operaciones remotas en todos los dispositivos gestionados, con independencia de si el usuario local o el usuario de ZENworks han entrado en el dispositivo.

El operador remoto no necesita ningún derecho exclusivo para llevar a cabo una sesión remota en el dispositivo si no hay ningún usuario que haya entrado en el dispositivo gestionado o si un usuario ha entrado en él, pero no en ZENworks. Sin embargo, el operador remoto necesita derechos de gestión remota exclusivos para realizar una operación remota en el dispositivo gestionado cuando un usuario de ZENworks ha entrado en el dispositivo. Se recomienda encarecidamente utilizar la autenticación basada en derechos porque es segura y ofrece un alto nivel de protección.

El uso de la autenticación basada en derechos requiere que el agente de ZENworks esté instalado en el dispositivo. No basta con instalar únicamente el servicio de gestión remota en el dispositivo.

4.1.2 Autenticación de gestión remota basada en contraseña

En la autenticación basada en contraseña, el operador remoto debe introducir una contraseña para lanzar la sesión remota en el dispositivo gestionado.

Los dos tipos de esquemas de autenticación basada en contraseña que se utilizan son:

- ♦ **Contraseña de ZENworks:** este esquema se basa en el protocolo de contraseña remota segura (SRP), versión 6a. La longitud máxima de las contraseñas de ZENworks es de 255 caracteres.
- ♦ **Contraseña de VNC:** se trata del esquema de autenticación basada en contraseña VNC tradicional. La longitud máxima de las contraseñas de VNC es de 8 caracteres. Este esquema de contraseña es inherentemente débil y se proporciona únicamente para asegurar la interoperabilidad con los componentes de código abierto.

Si se utiliza la autenticación basada en contraseña, se recomienda encarecidamente utilizar el esquema de contraseña de ZENworks, ya que es más seguro y ofrece más protección que el esquema de contraseña de VNC.

Los esquemas de contraseña funcionan en los modos siguientes:

- ♦ **Modo de sesión:** la contraseña que se define en este modo sólo es válida para la sesión en curso. El usuario del dispositivo gestionado debe definir una contraseña al iniciar la sesión remota y comunicarla al operador remoto por un medio independiente, como el teléfono. Al iniciar la sesión remota en el dispositivo gestionado, el operador remoto debe introducir la contraseña correcta en el recuadro de diálogo de contraseña de sesión que se muestra. Si el operador remoto no escribe la contraseña correcta en los dos minutos siguientes a la aparición del recuadro de diálogo, la sesión se cierra por razones de seguridad. Si se utiliza la autenticación basada en contraseña, se recomienda encarecidamente utilizar este modo de autenticación porque la contraseña sólo es válida para la sesión en curso y no se guarda en el dispositivo gestionado.
- ♦ **Modo persistente:** en este modo, la contraseña la puede definir el administrador a través de la directiva para gestión remota o el usuario del dispositivo gestionado a través del icono de ZENworks si la opción *Permitir que el usuario sobrescriba las contraseñas por defecto del dispositivo gestionado* está seleccionada en los valores de seguridad de la directiva para gestión remota.

Si hay una contraseña definida por el usuario del dispositivo gestionado y otra en la directiva, la contraseña definida por el usuario tiene prioridad sobre la contraseña configurada en la directiva.

El administrador puede impedir que el usuario del dispositivo gestionado defina la contraseña e incluso restablecer la contraseña definida por el usuario para asegurarse de que la contraseña configurada en la directiva se aplique siempre durante la autenticación. Para obtener más información sobre la contraseña definida por el usuario del dispositivo gestionado, consulte la [Sección 2.5.3, “Eliminación de la contraseña de gestión remota mediante el Centro de control de ZENworks”](#), en la página 31.

4.2 Seguridad de las contraseñas

Utilice contraseñas seguras. Tenga en mente las siguientes recomendaciones:

- ♦ **Longitud:** la longitud mínima recomendada es de 6 caracteres. Para que una contraseña sea segura, debe tener al menos 8 caracteres, aunque las contraseñas más largas son mejores. La longitud máxima es de 255 caracteres para las contraseñas de ZENworks y de 8 caracteres para las contraseñas de VNC.
- ♦ **Complejidad:** para que una contraseña sea segura, debe incluir una combinación de letras y números. Debe además incluir letras en mayúscula y en minúscula y al menos un carácter numérico. Se puede aumentar el nivel de seguridad de las contraseñas añadiendo números, especialmente en el centro y no al principio o al final únicamente. Los caracteres especiales, como &, *, \$ y > aumentan significativamente la seguridad de la contraseña. No se deben emplear palabras reconocibles, como nombres propios o palabras del diccionario, ni información personal como números de teléfono, fechas de nacimiento o aniversario o códigos postales.

4.3 Puertos

Por defecto, el servicio de gestión remota se ejecuta en el puerto 5950 y la escucha de gestión remota en el puerto 5550. El cortafuegos está configurado para permitir que se utilice cualquier puerto en el servicio de gestión remota, pero se debe configurar para que permita el uso del puerto para la escucha de gestión remota.

4.4 Audit

ZENworks Configuration Management mantiene un registro de todas las sesiones remotas que se llevan a cabo en el dispositivo gestionado. Este registro se mantiene en el dispositivo gestionado y lo pueden ver el usuario y el administrador. El administrador puede ver los registros de todas las sesiones remotas llevadas a cabo en el dispositivo. El usuario puede ver los registros de todas las sesiones remotas que se han llevado a cabo en el dispositivo mientras estaba dentro del sistema.

Para ver el registro de auditoría:

- 1 Haga doble clic en el icono de ZENworks del área de notificación del dispositivo gestionado.
- 2 En el panel de la izquierda, acceda a *Gestión remota* y haga clic en *Seguridad*.
- 3 Haga clic en *Mostrar información de auditoría* para ver la información de auditoría de las operaciones remotas realizadas en el dispositivo.

| Campo | Descripción |
|-----------------------------|---|
| <i>Usuario de ZENworks</i> | Nombre del usuario de ZENworks que ha entrado en el dispositivo gestionado al iniciar la sesión remota. |
| <i>Operador remoto</i> | Nombre del operador remoto que ha efectuado la operación. |
| <i>Equipo de la consola</i> | Nombre de host del dispositivo desde el que se ha realizado la operación remota. |

| Campo | Descripción |
|-----------------------------|---|
| <i>IP de la consola</i> | Dirección IP del dispositivo para el que se ha efectuado la operación. Nota: si la operación de gestión remota del dispositivo se encamina a través de un servidor proxy de gestión remota, se muestra la dirección IP del dispositivo que ejecuta el servidor proxy. |
| <i>Funcionamiento</i> | Tipo de operación realizada: control remoto, ejecución remota, vista remota, diagnóstico remoto o transferencia de archivos. |
| <i>Inicio</i> | Hora a la que empezó la operación remota. |
| <i>Hora de finalización</i> | Hora a la que finalizó la operación remota. |
| <i>Estado</i> | El estado de la operación remota: Correcto, En ejecución o Fallo. Se muestra también la causa del fallo. |

4.5 Solicitud de permiso al usuario del dispositivo gestionado

El administrador puede configurar la directiva de gestión remota para que los operadores remotos soliciten permiso al usuario del dispositivo gestionado antes de iniciar una operación remota en él.

Cuando el operador remoto inicia una sesión remota en el dispositivo gestionado, el servicio de gestión remota comprueba si la opción de solicitud de permiso al usuario del dispositivo gestionado para esa operación remota está habilitada en la directiva vigente en el dispositivo. Si la opción está habilitada y no hay ningún usuario que haya entrado en el dispositivo, se procede con la sesión remota. Sin embargo, si la opción está habilitada y hay un usuario que ha entrado en el dispositivo gestionado, se muestra al usuario un mensaje configurado en la directiva para gestión remota solicitando su permiso para lanzar una sesión remota en el dispositivo. La sesión sólo se inicia si el usuario concede el permiso.

4.6 Terminación anormal

Cuando se desconecta de forma inesperada una sesión remota, la función de terminación anormal permite bloquear el dispositivo gestionado o cerrar la sesión del usuario en el dispositivo gestionado, según la configuración de los valores de seguridad de la directiva para gestión remota. La sesión remota termina anormalmente en las siguientes circunstancias:

- ♦ La red falla y el visor de gestión remota y el servicio de gestión remota no se pueden comunicar.
- ♦ El visor de gestión remota se cierra anormalmente desde el administrador de tareas.
- ♦ Se inhabilita la red en el dispositivo gestionado o en la consola de gestión.

En algunas circunstancias, el servicio de gestión remota puede tardar hasta un minuto en determinar la terminación anormal de la sesión.

4.7 Detección de intrusos

La función de detección de intrusos reduce significativamente el riesgo de sufrir ataques por parte de hackers. Si el operador remoto no logra entrar en el dispositivo gestionado con el número de intentos especificado (5 por defecto), el servicio de gestión remota se bloquea y no acepta ninguna petición de sesión remota hasta que se desbloquea. El administrador puede desbloquear el servicio de gestión remota manual o automáticamente.

4.7.1 Desbloqueo automático del servicio de gestión remota

El servicio de gestión remota se desbloquea automáticamente cuando transcurre el tiempo especificado en la opción *Comenzar a aceptar conexiones automáticamente transcurridos [] minutos* > de la directiva para gestión remota. El periodo de tiempo por defecto es 10 minutos. Puede cambiar el tiempo por defecto en los valores de seguridad de la directiva para gestión remota.

4.7.2 Desbloqueo manual del servicio de gestión remota

Puede desbloquear manualmente el servicio de gestión remota desde el dispositivo gestionado o desde el Centro de control de ZENworks.

Para desbloquear el servicio de gestión remota desde el Centro de control de ZENworks, el operador remoto debe tener derechos para desbloquear el servicio en el dispositivo gestionado.

- 1 En el Centro de control de ZENworks, haga clic en *Dispositivos*.
- 2 Haga clic en *Servidores* o en *Estaciones de trabajo* para que aparezca una lista de los dispositivos gestionados.
- 3 Seleccione el dispositivo que se debe desbloquear.
- 4 Haga clic en *Acción* y después en *Desbloquear gestión remota*.
- 5 Haga clic en *Aceptar*.

Para desbloquear el servicio de gestión remota desde el dispositivo gestionado:

- 1 Haga doble clic en el icono de ZENworks del área de notificación del dispositivo gestionado.
- 2 En el panel izquierdo, acceda a *Gestión remota* y haga clic en *Seguridad*.
- 3 Haga clic en *Habilitar la aceptación de conexiones si hay un bloqueo vigente debido a la detección de intrusos*.

4.8 Identificación del operador remoto

Cuando un operador remoto lanza una sesión remota desde el Centro de control de ZENworks, se genera automáticamente un certificado que permite que el dispositivo gestionado identifique al operador remoto. Sin embargo, si el operador remoto lanza la sesión en modo independiente, el certificado no se genera y el operador se registra como usuario desconocido en los registros de auditoría y en los recuadros de diálogo de señal visible y de solicitud de permiso del usuario. El servicio de gestión remota recupera la identidad del operador remoto utilizando el certificado proporcionado por la consola de gestión durante la operación de enlace SSL. La operación de enlace SSL se produce con todos los tipos de autenticación, excepto con la autenticación basada en contraseña de VNC.

El servicio de gestión remota del dispositivo muestra los detalles del operador remoto en el recuadro de diálogo de señal visible si la opción *Proporcionar una señal visual al usuario del dispositivo gestionado* está habilitada en la directiva vigente en el dispositivo. También incluye la información sobre el operador remoto en los registros de auditoría de gestión remota.

4.9 Configuración del navegador

Si utiliza Internet Explorer para lanzar el Centro de control de ZENworks en dispositivos con Windows Vista, desactive el modo protegido en los valores de seguridad del navegador (*Herramientas > Opciones de Internet > Seguridad*).

4.10 Seguridad de la sesión

ZENworks Configuration Management emplea Secure Socket Layer (SSL) para proteger las sesiones remotas. Sin embargo, las sesiones remotas que se ejecutan con la autenticación basada en contraseña de VNC no se protegen. El proceso de autenticación se produce a través de un canal seguro cuando tiene lugar la operación de enlace SSL, con independencia de si el cifrado de la sesión está configurado en la directiva para gestión remota o no.

Cuando se completa la autenticación, la sesión remota pasa al modo no protegido si la opción *Habilitar el cifrado de sesión* está inhabilitada en la directiva para gestión remota y si el operador remoto inhabilita la opción *Cifrado de sesión* al iniciar una sesión remota en el dispositivo gestionado. Se recomienda sin embargo continuar la sesión en un modo protegido porque no influye de forma significativa en el rendimiento.

4.10.1 Enlace SSL

Cuando se instala el agente de ZENworks Adaptive en un dispositivo gestionado, el servicio de gestión remota genera un certificado autofirmado con una validez de 10 años.

Cuando un operador remoto inicia una sesión remota en el dispositivo gestionado, el visor de gestión remota solicita que el operador remoto verifique el certificado del dispositivo gestionado. El certificado muestra distintos datos, como el nombre del dispositivo gestionado, la autoridad emisora del certificado, la validez del certificado y la huella. Por razones de seguridad, el operador remoto debe verificar las credenciales del dispositivo gestionado comparando la huella del certificado con la huella comunicada por el usuario del dispositivo gestionado a través de un medio independiente. En ese momento, el operador remoto dispone de las opciones siguientes:

- ♦ **Aceptar el certificado de forma permanente:** si el usuario que ha entrado en la consola de gestión acepta el certificado de forma permanente, el certificado no se muestra en las siguientes sesiones remotas que inicien los usuarios que entren en esa consola.
- ♦ **Aceptar el certificado de forma temporal:** si el usuario que ha entrado en la consola de gestión acepta el certificado de forma temporal, el certificado se acepta únicamente para la sesión en curso. Se le solicita al usuario que verifique el certificado cuando se inicie una nueva conexión con el dispositivo gestionado.
- ♦ **Rechazar el certificado:** si el usuario que ha entrado en la consola de gestión rechaza el certificado, termina la sesión remota.

4.10.2 Regeneración de certificados

El dispositivo gestionado vuelve a generar un certificado autofirmado nuevo si:

- ♦ El nombre del dispositivo gestionado ha cambiado
- ♦ El certificado tiene una fecha posterior y no es válido en ese momento
- ♦ El certificado ha caducado
- ♦ El certificado está a punto de caducar
- ♦ Falta el certificado

Por defecto, el certificado se vuelve a generar una vez cada 10 años.

Resolución de problemas

5

Las siguientes secciones describen las situaciones que se pueden presentar mientras se utiliza el componente de gestión remota de Novell® ZENworks® 10 Configuration Management.

- ♦ “No es posible anular el protector de pantalla del dispositivo gestionado.” en la página 67
- ♦ “Durante una sesión de gestión remota, si sale y vuelve a entrar en un equipo con Windows 2000* Professional, puede que no se restaure el fondo de pantalla definido en él.” en la página 68
- ♦ “No es posible lanzar una sesión remota en el dispositivo gestionado, que tiene activado un nivel de calidad del color muy bajo.” en la página 68
- ♦ “No es posible lanzar el visor de gestión remota.” en la página 69
- ♦ “La terminación anormal de la sesión puede fallar en los dispositivos gestionados con Windows Vista.” en la página 69
- ♦ “La escucha de gestión remota no puede aceptar peticiones de sesión remota desde el dispositivo gestionado si el puerto al que está asociada no está abierto en el cortafuegos de la consola de gestión.” en la página 69
- ♦ “Solución de mensajes de error que aparecen mientras se utiliza el componente de gestión remota.” en la página 69
- ♦ “¿Cómo puedo habilitar el registro de depuración de gestión remota en el dispositivo en el que se lanza el Centro de control de ZENworks?” en la página 70
- ♦ “Instalación de una nueva versión del controlador de duplicación.” en la página 70
- ♦ “El dispositivo gestionado no ha podido iniciar el esquema de cifrado de Novell para la sesión. Asegúrese de que el dispositivo está sincronizado con la hora UTC con este sistema. Si el problema persiste, póngase en contacto con el servicio de asistencia técnica de Novell.” en la página 70
- ♦ “Las aplicaciones como Regedit, si se lanzan en un dispositivo gestionado de 64 bits a través de la ejecución remota, no pueden acceder a determinadas claves del registro.” en la página 71
- ♦ “La opción para borrar la pantalla puede fallar cuando se controla de forma remota un dispositivo con Windows.” en la página 71
- ♦ “Cuando se lanza una sesión de gestión remota en un dispositivo gestionado con Windows 2000 Professional, el dispositivo rearranca.” en la página 71
- ♦ “Se inician varias instancias del visor de gestión remota en el dispositivo con el navegador Internet Explorer 7.” en la página 71
- ♦ “No es posible utilizar el icono Ctrl-Alt-Supr mientras se controla de forma remota un dispositivo con Windows Vista o Windows Server 2008*.” en la página 72
- ♦ “El modo de sesión por defecto no se selecciona en el módulo integrable de gestión remota.” en la página 72
- ♦ “El enlace Instalar visor de gestión remota permanece activo en un dispositivo de Windows Vista con el navegador Internet Explorer 7.” en la página 72

No es posible anular el protector de pantalla del dispositivo gestionado.

Origen: ZENworks 10 Configuration Management; gestión remota.

- Explicación: Cuando se activa un protector de pantalla protegido mediante contraseña en el dispositivo gestionado antes de que se inicie una sesión de control remoto, el servicio de gestión remota intenta anular el protector de pantalla para que el operador remoto pueda ver el escritorio del usuario. El operador remoto puede también anular el protector de pantalla durante la sesión remota haciendo clic en el icono *Omitir protector de pantalla* de la barra de herramientas del visor de gestión remota.
- Causa posible: Si el protector de pantalla se activa debido a la inactividad de la sesión remota.
- Acción: Haga clic en el icono *Omitir protector de pantalla* de la barra de herramientas del visor de gestión remota. Puede que tenga que hacer clic en el icono varias veces para que surta efecto.
- Causa posible: La función de anulación del protector de pantalla no se admite en la plataforma Windows Vista.
- Acción: Ninguna.
- Causa posible: El protector de pantalla se puede interrumpir si se envían movimientos del ratón al dispositivo gestionado.
- Acción: Seleccione la opción *Bloquear eventos de movimiento del ratón* en la ventana de opciones del visor de gestión remota de ZENworks para impedir que se envíen movimientos del ratón al dispositivo gestionado.
- Causa posible: La identificación y autenticación gráfica (GINA) del dispositivo gestionado se activa debido a la interrupción del protector de pantalla en él.
- Acción: Vuelva a entrar en el dispositivo gestionado.

Durante una sesión de gestión remota, si sale y vuelve a entrar en un equipo con Windows 2000* Professional, puede que no se restaure el fondo de pantalla definido en él.

- Origen: ZENworks 10 Configuration Management; gestión remota.
- Acción: Ninguna.

No es posible lanzar una sesión remota en el dispositivo gestionado, que tiene activado un nivel de calidad del color muy bajo.

- Origen: ZENworks 10 Configuration Management; gestión remota.
- Explicación: Puede que no sea posible lanzar una sesión de control remoto, vista remota o diagnóstico remoto en un dispositivo gestionado que utilice un nivel de calidad del color muy bajo (inferior a 8 bits por píxel, bpp).
- Acción: Aumente la calidad del color del dispositivo a 16 bpp o más mediante el procedimiento siguiente:
1. Haga clic con el botón derecho en el escritorio.
 2. Haga clic en *Propiedades*.
 3. En la ventana Propiedades de Pantalla, haga clic en *Configuración*.
 4. Seleccione la calidad del color adecuada y haga clic en *Aceptar*.

No es posible lanzar el visor de gestión remota.

Origen: ZENworks 10 Configuration Management; gestión remota.

Causa posible: Puede que no sea posible lanzar el visor de gestión remota si se suprime o renombra el archivo ejecutable correspondiente.

Acción: Vuelva a instalar el visor de gestión remota descargando la última versión de `novell-zenworks-rm-viewer.msi` desde `https://dirección_IP_del_servidor_de_ZENworks/zenworks-remote-management`.

La terminación anormal de la sesión puede fallar en los dispositivos gestionados con Windows Vista.

Origen: ZENworks 10 Configuration Management; gestión remota.

Explicación: Durante una sesión remota, si el usuario inhabilita la conexión de red en un dispositivo gestionado con Windows Vista, puede que ZENworks no lo identifique como terminación anormal y no bloquee el dispositivo ni termine la sesión del usuario en el dispositivo gestionado.

Acción: Ninguna.

La escucha de gestión remota no puede aceptar peticiones de sesión remota desde el dispositivo gestionado si el puerto al que está asociada no está abierto en el cortafuegos de la consola de gestión.

Origen: ZENworks 10 Configuration Management; gestión remota.

Acción: En el cortafuegos de la consola de gestión, abra el puerto de escucha.

Solución de mensajes de error que aparecen mientras se utiliza el componente de gestión remota.

Origen: ZENworks 10 Configuration Management; gestión remota.

Acción: Para solucionar los mensajes de error que se pueden presentar mientras se utiliza el componente de gestión remota, envíe los archivos `WinVNCAApp.log` y `WinVNC.log` en el caso de dispositivos con Windows Vista, o el archivo `WinVNC.log` en otros dispositivos gestionados al servicio de [asistencia de Novell \(http://support.novell.com\)](http://support.novell.com).

Para acceder a los archivos de registro:

1. Abra el Editor del Registro.
2. Diríjase a `HKLM\Software\Novell\ZENworks\Remote Management\Agent`.
3. Cree una entrada DWORD llamada `DebugMode` y asígnele el valor 2.
4. Cree una entrada DWORD llamada `DebugLevel` y asígnele el valor hexadecimal a (igual a 10 en valor decimal).
5. Reinicie el servicio de gestión remota.

Se crearán los siguientes archivos de registro de gestión remota en `directorio_de_instalación_de_ZENworks\logs`:

- ♦ WinVNC.log
- ♦ WinVNCAApp.log (sólo con Windows Vista)

¿Cómo puedo habilitar el registro de depuración de gestión remota en el dispositivo en el que se lanza el Centro de control de ZENworks?

Origen: ZENworks 10 Configuration Management; gestión remota.

Acción: Para habilitar los registros, consulte el documento de información técnica TID 3418069 en la [base de conocimiento del servicio de asistencia de Novell \(http://support.novell.com/search/kb_index.jsp\)](http://support.novell.com/search/kb_index.jsp).

Instalación de una nueva versión del controlador de duplicación.

Origen: ZENworks 10 Configuration Management; gestión remota.

Causa posible: Cuando se instala el agente de ZENworks Adaptive en un dispositivo gestionado con Windows 2003 de 64 bits, no se instala el controlador de duplicación en el dispositivo. El mensaje *Instale una versión más reciente del controlador Mirage* se registra en el Centro de control de ZENworks.

Puede llevar a cabo sesiones remotas en el dispositivo, pero el rendimiento se verá ralentizado.

Acción: No tenga en cuenta este mensaje.

Causa posible: Si controla de forma remota un dispositivo que ya está conectado mediante una conexión de escritorio remoto (RDP), el mensaje *Instale una versión más reciente del controlador Mirage* se registra en el Centro de control de ZENworks.

Puede llevar a cabo sesiones remotas en el dispositivo, pero el rendimiento se verá ralentizado.

Acción: No tenga en cuenta este mensaje.

El dispositivo gestionado no ha podido iniciar el esquema de cifrado de Novell para la sesión. Asegúrese de que el dispositivo está sincronizado con la hora UTC con este sistema. Si el problema persiste, póngase en contacto con el servicio de asistencia técnica de Novell.

Origen: ZENworks 10 Configuration Management; gestión remota

Acción: Cuando actualice o registre el dispositivo gestionado, haga lo siguiente:

1. Actualice el nombre del dominio del nuevo certificado de CA en el registro con la nueva información:

Clave: HKLM\Software\Novell\ZENworks

Valor: CASubject

2. Importe el certificado de CA de la nueva zona al almacén de certificados raíz de confianza.
3. Importe el certificado de CA de la zona anterior del almacén de certificados raíz de confianza.

Las aplicaciones como Regedit, si se lanzan en un dispositivo gestionado de 64 bits a través de la ejecución remota, no pueden acceder a determinadas claves del registro.

Origen: ZENworks 10 Configuration Management; gestión remota.

Causa posible: Las aplicaciones que se lanzan en un dispositivo gestionado de 64 bits mediante la ejecución remota se ejecutan en un entorno WOW (Windows On Windows).

Acción: Lance las aplicaciones mediante la operación de diagnóstico remoto.

La opción para borrar la pantalla puede fallar cuando se controla de forma remota un dispositivo con Windows.

Origen: ZENworks 10 Configuration Management; gestión remota.

Causa posible: Los controladores de versiones anteriores de Windows no permiten la opción de energía de borrado de la pantalla.

Acción: Debe instalar el controlador gráfico específico del sistema.

Cuando se lanza una sesión de gestión remota en un dispositivo gestionado con Windows 2000 Professional, el dispositivo rearranca.

Origen: ZENworks 10 Configuration Management; gestión remota.

Causa posible: El controlador de vídeo no está instalado en el dispositivo.

Acción: Debe instalar el controlador de vídeo específico del sistema.

Se inician varias instancias del visor de gestión remota en el dispositivo con el navegador Internet Explorer 7.

Origen: ZENworks 10 Configuration Management; gestión remota.

Causa posible: Si lanza una operación de gestión remota en un dispositivo que cuenta con el navegador Internet Explorer 7, se lanzan varias instancias del visor de gestión remota en el dispositivo si la consola de gestión tiene instalado software para acelerar las descargas, como FlashGet.

Acción: Inhabilite temporalmente los complementos de los aceleradores de descargas:

1. Lance Internet Explorer 7.
2. Haga clic en *Herramientas > Administrar complementos*.
3. Haga clic en *Habilitar o deshabilitar complementos* e inhabilite el complemento del acelerador de descargas.
4. Lance la operación de gestión remota.

Acción: Pruebe a utilizar el navegador Firefox para realizar la operación.

No es posible utilizar el icono Ctrl-Alt-Supr mientras se controla de forma remota un dispositivo con Windows Vista o Windows Server 2008*.

Origen: ZENworks 10 Configuration Management; gestión remota.

Explicación: Si se lanza una operación de control remoto en un dispositivo con Windows Vista o Windows Server 2008 con el control de cuentas de usuario (UAC) inhabilitado, el icono *Ctrl-Alt-Del* aparece sombreado.

Acción: Habilite el control de cuentas de usuario.

El modo de sesión por defecto no se selecciona en el módulo integrable de gestión remota.

Origen: ZENworks 10 Configuration Management; gestión remota.

Explicación: Si utiliza Internet Explorer para abrir el Centro de control de ZENworks y realizar una operación de gestión remota en un dispositivo, no se selecciona el modo de sesión por defecto en el módulo integrable de gestión remota. Sin embargo, si no selecciona ningún modo de sesión, se lanza la operación de control remoto en el modo de colaboración por defecto y la operación de vista remota en el modo exclusivo por defecto.

Acción: Seleccione el modo de sesión para realizar la operación remota.

El enlace Instalar visor de gestión remota permanece activo en un dispositivo de Windows Vista con el navegador Internet Explorer 7.

Origen: ZENworks 10 Configuration Management; gestión remota.

Explicación: En un dispositivo de Windows Vista que cuente con el navegador Internet Explorer 7, puede fallar la instalación del *visor de gestión remota* si el control ActiveX* no está activado.

Acción: Haga lo siguiente para activar el control de cuentas de usuario en el dispositivo con Windows Vista:

1. Haga clic en *Inicio > Configuración > Panel de control > Cuentas de usuario > Cuentas de usuario > Activar o desactivar el Control de cuentas de usuario*.
2. Seleccione *Usar el Control de cuentas de usuario (UAC) para ayudar a proteger el equipo*.
3. Haga clic en *Aceptar*.

Acción: Si no desea activar el control de cuentas de usuario, debe actualizar a Windows Vista SP1.

Información sobre criptografía

A

Las siguientes secciones contienen información acerca de los distintos certificados que se generan mientras se utiliza el componente de gestión remota de Novell® ZENworks® 10 Configuration Management.

- ♦ Sección A.1, “Información sobre el par de claves del dispositivo gestionado”, en la página 73
- ♦ Sección A.2, “Información sobre el par de claves del operador remoto”, en la página 73
- ♦ Sección A.3, “Información sobre el ticket de gestión remota”, en la página 74
- ♦ Sección A.4, “Información sobre el cifrado de sesiones”, en la página 74

A.1 Información sobre el par de claves del dispositivo gestionado

Certificado generado por: servicio de gestión remota
Certificado generado mediante: OpenSSL v0.9.8e (versión de Novell)
Certificado firmado por: autofirmado
Certificado firmado mediante: OpenSSL v0.9.8e (versión de Novell)
Certificado verificado por: visor de gestión remota
Certificado verificado mediante: OpenSSL v0.9.8e (versión de Novell)
Utilizado por: servicio de gestión remota
Utilizado para: establecer una sesión segura con el visor de gestión remota
Tipo de clave privada: RSA
Nivel de la clave: 1024 bits
Algoritmo de la firma: RSA-SHA256
Validez: 10 años

A.2 Información sobre el par de claves del operador remoto

Este certificado sólo es válido cuando se distribuye la CA interna.

Certificado generado por: el servidor de ZENworks que alberga el Centro de control de ZENworks
Certificado generado mediante: biblioteca Bouncy Castle (bcprov-jdk15-134.jar)
Certificado firmado por: el servidor de ZENworks que alberga el Centro de control de ZENworks
Certificado firmado mediante: biblioteca Bouncy Castle (bcprov-jdk15-134.jar)
Certificado verificado por: servicio de gestión remota
Certificado verificado mediante: OpenSSL v0.9.8e (versión de Novell)
Utilizado por: el visor de gestión remota y el servicio de gestión remota
Utilizado para: establecer una sesión segura e identificar al operador remoto
Tipo de clave privada: RSA
Nivel de la clave: 1024 bits
Algoritmo de la firma: RSA-SHA1

Validez: 4 días

A.3 Información sobre el ticket de gestión remota

Este certificado sólo es válido para la autenticación basada en derechos.

Ticket generado por: el servidor de ZENworks que alberga el Centro de control de ZENworks

Ticket generado mediante: biblioteca Bouncy Castle (bcprov-jdk15-134.jar)

Certificado firmado por: el servidor de ZENworks que alberga el Centro de control de ZENworks

Ticket firmado mediante: biblioteca Bouncy Castle (bcprov-jdk15-134.jar)

Certificado verificado por: servicio Web de gestión remota (en el servidor de ZENworks)

Certificado verificado mediante: biblioteca Bouncy Castle (bcprov-jdk15-134.jar)

Utilizado por: el visor de gestión remota y el servicio Web de gestión remota

Utilizado para: autenticar al operador remoto y verificar los derechos para realizar una operación

Algoritmo de la firma: RSA-SHA1

Validez: 2 minutos

A.4 Información sobre el cifrado de sesiones

Sesión establecida entre: el servicio de gestión remota y el visor de gestión remota

Protocolo de cifrado: SSL (TLSv1)

Cifrado de sesión: AES256-SHA

Modo de autenticación SSL: Mutuo/Servidor

Prácticas recomendadas

B

Las siguientes secciones describen las prácticas que conviene observar al utilizar el componente de gestión remota de Novell® ZENworks® 10 Configuration Management.

- ♦ Sección B.1, “Cierre de las escuchas de gestión remota”, en la página 75
- ♦ Sección B.2, “Cierre de aplicaciones lanzadas durante la operación de ejecución remota”, en la página 75
- ♦ Sección B.3, “Identificación del operador remoto en el dispositivo gestionado”, en la página 76
- ♦ Sección B.4, “Realización de una sesión de control remoto en un dispositivo que ya está conectado a través de una conexión de escritorio remoto”, en la página 76
- ♦ Sección B.5, “Determinación del nombre de la consola de gestión”, en la página 76
- ♦ Sección B.6, “Uso del tema Aero en dispositivos con Windows Vista y Windows Server 2008”, en la página 76
- ♦ Sección B.7, “Habilitación del botón de secuencia de atención (Ctrl+Alt+Supr) al controlar de forma remota un equipo con Windows Vista o Windows Server 2008”, en la página 77
- ♦ Sección B.8, “Instalación del servicio de gestión remota en un dispositivo con Windows XP a través de RDP”, en la página 77
- ♦ Sección B.9, “Rendimiento de gestión remota”, en la página 77

B.1 Cierre de las escuchas de gestión remota

Cuando un operador remoto lanza la escucha de gestión remota para atender las peticiones de sesión remota del usuario del dispositivo gestionado, ZENworks emite un ticket para habilitar la autenticación del operador remoto en el dispositivo gestionado. La duración de este ticket es de dos días.

La escucha de gestión remota se sigue ejecutando aunque el operador remoto salga del sistema o cierre el Centro de control de ZENworks. Si el ticket sigue siendo válido, cualquier otro operador remoto puede usar la escucha para atender las peticiones de sesión remota de los usuarios del dispositivo gestionado. Por razones de seguridad, debe cerrar la escucha de gestión remota antes de salir del navegador o cerrarlo.

Para cerrar las escuchas de gestión remota, haga clic con el botón derecho en el icono *Escucha de gestión remota* de ZENworks del área de notificación y después haga clic en *Cerrar daemon de escucha*.

B.2 Cierre de aplicaciones lanzadas durante la operación de ejecución remota

por defecto, el módulo de gestión remota se ejecuta como servicio con privilegios de sistema en el dispositivo gestionado. Por tanto, todas las aplicaciones que se lanzan durante la sesión de ejecución remota se ejecutan también con privilegios de sistema. Por motivos de seguridad, se recomienda encarecidamente cerrar las aplicaciones después de usarlas.

B.3 Identificación del operador remoto en el dispositivo gestionado

Cuando un operador remoto lanza una sesión remota en un dispositivo gestionado a través del Centro de control de ZENworks, ZENworks emite automáticamente un certificado que ayuda al dispositivo gestionado a identificar el operador remoto si se usa una autoridad certificadora interna. No obstante, si se utiliza una autoridad certificadora externa, el operador remoto deberá proporcionar manualmente el certificado que está encadenado a la autoridad certificadora distribuida y que se ha verificado para la autenticación de clientes SSL. Para obtener más información acerca de cómo utilizar la autoridad certificadora externa, consulte *Utilizar el siguiente par de claves para la identificación* en la **Sección 2.8, “Inicio de operaciones de gestión remota”**, en la **página 33**.

Si el operador remoto lanza una operación remota en un dispositivo gestionado sin proporcionar un certificado, su nombre se registrará como *Un usuario desconocido* en los registros de auditoría, la señal visible y el recuadro de diálogo de petición de permiso al usuario. Para asegurarse de que el operador remoto proporcione el certificado, anule la selección de *Permitir conexión si la consola de gestión remota no tiene un certificado SSL* en la directiva de gestión remota.

B.4 Realización de una sesión de control remoto en un dispositivo que ya está conectado a través de una conexión de escritorio remoto

Para controlar de forma remota un dispositivo que ya está conectado a través de una conexión de escritorio remoto (RDP), asegúrese de que se cumple una de las siguientes condiciones:

- ♦ La sesión RDP está en curso en el dispositivo gestionado.
- ♦ El dispositivo gestionado se ha desbloqueado manualmente una vez finalizada la sesión RDP en el dispositivo.


B.5 Determinación del nombre de la consola de gestión

Si la opción *Buscar nombre DNS del visor en el inicio de la sesión remota* está habilitada en la directiva de gestión remota, el dispositivo gestionado intenta determinar el nombre de la consola de gestión remota al principio de la sesión. Esto puede provocar un retraso significativo en el inicio de la sesión remota si la red no tiene habilitadas las búsquedas DNS inversas. Para evitar el retraso, inhabilite la opción *Buscar nombre DNS del visor en el inicio de la sesión remota* en la directiva.

B.6 Uso del tema Aero en dispositivos con Windows Vista y Windows Server 2008

Para mejorar el rendimiento de las sesiones remotas, la gestión remota emplea un controlador de duplicación que detecta los cambios en la pantalla. Si el controlador de duplicación no es compatible con el tema de escritorio Aero, cualquier intento de cargarlo en un dispositivo con el tema Aero habilitado cambiará el dispositivo al tema de escritorio por defecto. Esto puede afectar a la experiencia de los usuarios, de modo que no es recomendable utilizar el tema Aero en un dispositivo que desee gestionar de forma remota.

B.7 Habilitación del botón de secuencia de atención (Ctrl+Alt+Supr) al controlar de forma remota un equipo con Windows Vista o Windows Server 2008

Para habilitar el icono  (Ctrl+Alt+Supr) en la barra de herramientas del visor de gestión remota al controlar de forma remota un dispositivo con Windows Vista o Windows Server 2008, asegúrese de que el control de cuentas de usuario (UAC) esté habilitado en el dispositivo gestionado.

B.8 Instalación del servicio de gestión remota en un dispositivo con Windows XP a través de RDP

Durante la instalación del servicio de gestión remota en un dispositivo gestionado, ZENworks instala automáticamente un controlador de duplicación denominado DFMirage en el dispositivo. Si desea instalar el servicio de gestión remota en un dispositivo con Windows XP a través de una sesión de conexión de escritorio remoto (RDP), asegúrese de que los parches proporcionados en el [sitio Web de soporte de Microsoft \(http://support.microsoft.com/kb/952132\)](http://support.microsoft.com/kb/952132) están instalados en el dispositivo.

B.9 Rendimiento de gestión remota

El rendimiento de la gestión remota durante una sesión remota a través de un enlace de red lento o rápido cambia en función del tráfico de la red. Para mejorar el tiempo de respuesta, consulte la [Sección 3.7, “Mejora del rendimiento de la gestión remota”, en la página 58.](#)

Actualizaciones de la documentación

C

Esta sección contiene información sobre las modificaciones en el contenido de la documentación que se han realizado en esta *Referencia sobre la gestión remota de ZENworks* tras la publicación inicial de Novell® ZENworks® 10 Configuration Management SP2. Los cambios se muestran según la fecha de publicación.

La documentación de este producto está disponible en Web en dos formatos: HTML y PDF. La documentación HTML y PDF está actualizada con los cambios que aparecen en esta sección.

Si necesita saber si la copia de la documentación en PDF que está usando es la más reciente, consulte la fecha de publicación que aparece en la página del título.

La documentación se ha actualizado en las siguientes fechas:

- ♦ Sección C.1, “27 de mayo de 2009: SP2 (10.2)”, en la página 79

C.1 27 de mayo de 2009: SP2 (10.2)

Se han realizado actualizaciones en las siguientes secciones:

- ♦ Sección C.1.1, “Descripción general”, en la página 79
- ♦ Sección C.1.2, “Configuración de la gestión remota”, en la página 79
- ♦ Sección C.1.3, “Seguridad”, en la página 80

C.1.1 Descripción general

Se han realizado los siguientes cambios:

| Ubicación | Cambio |
|--|---------------------------------|
| Sección 1.1, “Terminología de la gestión remota”, en la página 11 | Se ha actualizado esta sección. |
| Sección 1.4, “Descripción del servidor proxy de gestión remota”, en la página 16 | Se ha añadido esta sección. |

C.1.2 Configuración de la gestión remota

Se han realizado los siguientes cambios:

| Ubicación | Cambio |
|------------------------|--|
| Paso 6 en la página 18 | Añadida información acerca de la configuración del servidor proxy de gestión remota para realizar operaciones remotas en dispositivos NAT. |

| Ubicación | Cambio |
|---|--|
| "Inicio de una operación de gestión remota en el Centro de control de ZENworks" en la página 34 | Añadida información acerca de cómo especificar un servidor proxy para llevar a cabo operaciones remotas en un dispositivo NAT. |
| "Inicio de una operación de gestión remota en el Centro de control de ZENworks" en la página 34 | Añadida información acerca de cómo proporcionar la información de pares de claves para gestionar de forma remota un dispositivo cuando hay una autoridad certificadora externa distribuida en la zona. |
| Sección 2.9, "Instalación de un servidor proxy de gestión remota", en la página 46 | Añadida información acerca de cómo instalar el servidor proxy de gestión remota. |
| "Inicio de una operación de gestión remota en modo independiente" en la página 39 | Sección actualizada. |
| "Inicio de una operación de gestión remota mediante las opciones de la línea de comandos" en la página 40 | Sección actualizada. |
| Sección 2.6, "Instalación del visor de gestión remota", en la página 31 | Sección añadida. |
| Sección 2.7, "Actualización del visor de gestión remota", en la página 33 | Sección añadida. |

C.1.3 Seguridad

Se han realizado los siguientes cambios:

| Ubicación | Cambio |
|--|---------------------------------|
| Sección 4.1.1, "Autenticación de gestión remota basada en derechos", en la página 59 | Se ha actualizado esta sección. |