# Referencia sobre la gestión remota

Novell®
ZENworks® 10 Configuration Management SP3

**10.3**

30 de marzo de 2010

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/) 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.



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).

## 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).

## Materiales de otros fabricantes

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

# Tabla de contenido

# Acerca de esta guía

Esta *Referencia de 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:



### 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) 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 SP3 (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 vía de referencia cruzada.

El 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:



## 1.1 Terminología de la gestión remota

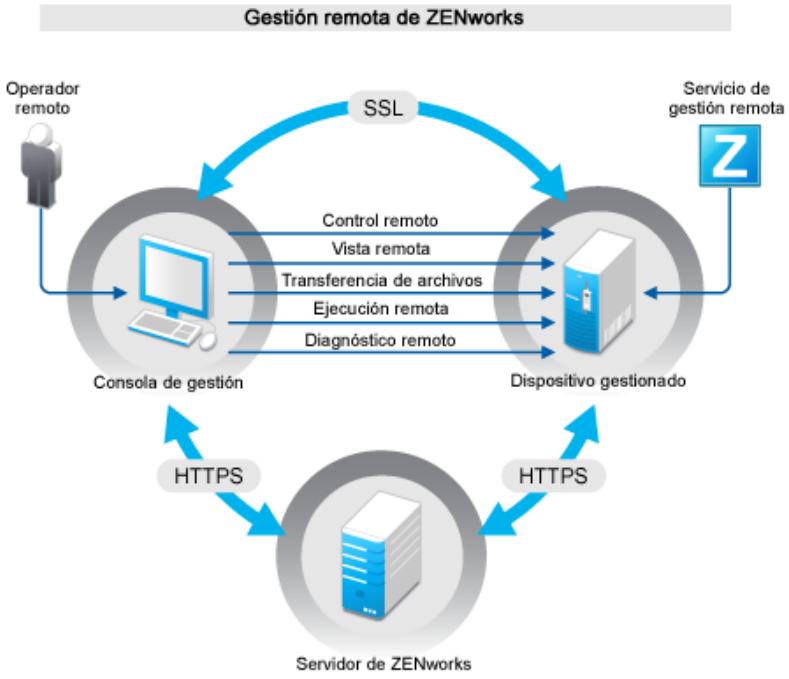
| Términos | Descripción |
|---|---|
| Dispositivo gestionado | Dispositivo que el usuario desea gestionar de forma remota. Para gestionar de forma remota un dispositivo, asegúrese de que el componente de gestión remota está instalado y de que el servicio de gestión remota se está ejecutando en el dispositivo. |
| 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 Windows gestionado o en un dispositivo Linux (servidor primario o dispositivo satélite). |

## 1.2 Descripción de las operaciones de gestión remota

La gestión remota otorga a los administradores el control de un dispositivo sin necesidad de visitas in situ, con lo que puede ahorrarle a usted y a su organización 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 14
- Sección 1.2.3, “Ejecución remota”, en la página 14
- Sección 1.2.4, “Diagnóstico remoto”, en la página 14
- Sección 1.2.5, “Transferencia de archivos”, en la página 14
- Sección 1.2.6, “Activación remota”, en la página 15

## 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 53.

### 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 experimente 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 57.

### 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 58.

### 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 59.

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:

- Transferir archivos entre la consola de gestión y el dispositivo gestionado.
- Renombrar 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 60.

**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 3.7, “Activación de un dispositivo remoto”, en la página 63.

## 1.3 Descripción de las funciones de gestión remota

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



### 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 Detección de intruso reduce de forma significativa el riesgo de que el dispositivo gestionado sea atacado por intrusos. Si el operador remoto no consigue entrar en el dispositivo gestionado en el número permitido de intentos (por defecto son cinco), 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 aseguran mediante el nivel de zócalo con seguridad (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 el control del teclado y del ratón en el dispositivo gestionado durante una sesión remota para impedir que el usuario del dispositivo gestionado pueda interrumpir la sesión.

---

**Nota:** en los dispositivos gestionados con Windows Vista, los bloqueos del ratón y del teclado no funcionan si el tema Aero está habilitado.

---

### 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 del ratón del dispositivo gestionado también se bloquean.

---

**Nota:** cuando se pone en blanco la pantalla de un dispositivo Tablet PC gestionado durante una sesión remota, se reduce el rendimiento de la sesión.

---

### 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 durante la sesión remota.

---

**Nota:** esta función no está disponible en dispositivos gestionados con Windows Vista*, Windows Server 2008 y Windows 7.

---

### 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 44.

---

**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 55.

### 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.

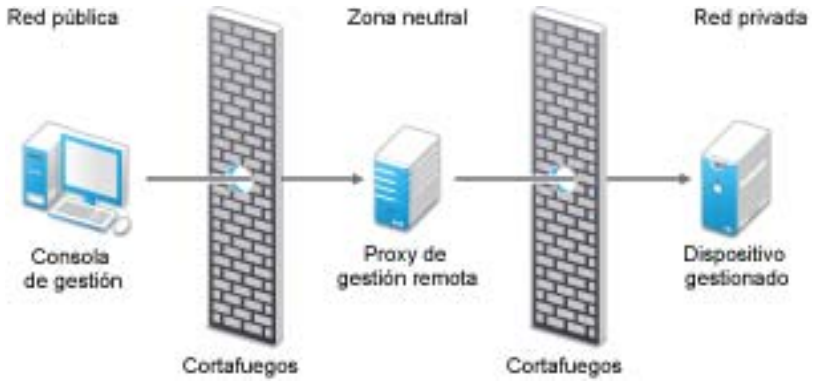
## 1.4 Descripción del servidor proxy de gestión remota

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 se debe dirigir a través de un servidor proxy de gestión remota.

Para obtener más información sobre el encaminamiento de la operación remota a través del servidor proxy a la hora de iniciar una sesión remota desde la consola de gestión, consulte Encaminar a través del servidor proxy en “Inicio de una sesión de gestión remota desde el contexto del dispositivo” en la página 36.

Para obtener más información sobre el encaminamiento de la operación remota a través del servidor proxy a la hora de iniciar una sesión remota desde el contexto del dispositivo, consulte Encaminar a través del servidor proxy en “Inicio de una sesión de gestión remota desde el contexto del usuario” en la página 40.

***Figura 1-2*** *Servidor proxy de gestión remota*




Debe instalar el servidor proxy en un dispositivo que esté situado en una zona desmilitarizada (DMZ). El dispositivo en el que instale el servidor proxy debe ser accesible desde la red pública que tenga la consola de gestión y también deben poder acceder a él los dispositivos que estén en una red privada. Para obtener información acerca de cómo instalar el servidor proxy de gestión remota, consulte la Sección 2.10, “Instalación de un servidor proxy de gestión remota”, en la página 49.

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 Gestión remota 2

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



## 2.1 Configuración de los ajustes de gestión remota

Los valores de gestión remota son un conjunto de reglas que determinan el comportamiento de la ejecución del servicio de gestión remota en el dispositivo gestionado. Los valores incluyen la configuración de los puertos, los valores de sesión y los 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:



### 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 las opciones para los Valores de sesión:

| Campo | Detalles |
|---|---|
| *Buscar nombre DNS del visor en el inicio de la sesión remota* | Habilita el servicio de gestión remota a fin de que pueda buscar el nombre DNS de la consola de gestión al inicio de la sesión remota.<br><br>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.*<br><br>Si en la red no está habilitada la búsqueda DNS inversa, es recomendable desactivar este valor para evitar retrasos importantes en el inicio de la sesión remota. |
| *Permitir sesión remota cuando no haya entrado ningún usuario en el dispositivo gestionado* | Permite a un operador remoto gestionar de forma remota un dispositivo cuando la directiva permite las operaciones remotas, pero ningún usuario ha entrado al dispositivo. Esta opción está seleccionada por defecto. |

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

| Campo | Detalles |
|---|---|
| *Suprimir papel tapiz* | 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. |
| *Habilitar controlador de optimización* | 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, por 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 2.10, “Instalación de un servidor proxy de gestión remota”, en la página 49.

| Tarea | Detalles |
|---|---|
| Adición de un servidor proxy de gestión remota | 1. Haga clic en *Añadir* para acceder al recuadro de diálogo Añadir valores de servidor proxy.<br>2. Cumplimente los siguientes campos:<br>**Servidor proxy:** especifique la dirección IP o el nombre DNS del servidor proxy de gestión remota.<br>**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:<br>◆ 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:<br>123.45.678.12/16: especifica todas las direcciones IP que empiezan por 123.45.<br>123.45.678.12/24: especifica todas las direcciones IP que empiezan por 123.45.678.<br>◆ Escriba el rango de direcciones con el formato **Dirección IP inicial** - **Dirección IP final**. Por ejemplo:<br>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. |
| Supresión de un servidor proxy de gestión remota | 1. Seleccione el servidor proxy que desee suprimir.<br>2. Haga clic en Suprimir y, a continuación, en *Aceptar*. |

**7** (Opcional) Configure una aplicación para que se lance 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

En la tabla siguiente se muestran las tareas que se pueden llevar a cabo para personalizar la lista *Aplicaciones de diagnóstico:*

| Tarea | Detalles |
|---|---|
| Añadir una aplicación | 1. Haga clic en *Añadir.*<br>2. Especifique el nombre y la vía de la aplicación en el dispositivo gestionado.<br>3. Haga clic en *Aceptar.* |
| Suprimir una aplicación | 1. Seleccione la aplicación que desea suprimir.<br>2. Haga clic en Suprimir y, a continuación, en *Aceptar.* |
| Revertir a las aplicaciones por defecto | 1. Haga clic en *Revertir* y, a continuación, en *Aceptar.* |

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, es posible modificarlos para los dispositivos de 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 desee configurar.

3 Haga clic en *Ajustes* y, a continuación, en *Gestión de dispositivos* > *Gestión remota.*

4 Haga clic en *Sobrescribir.*

5 Edite los valores de gestión remota según 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, es posible modificarlos 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 desee configurar.

4 Haga clic en *Ajustes* y, a continuación, en *Gestión de dispositivos* > *Gestión remota.*

5 Haga clic en *Sobrescribir*.

6 Edite los valores de gestión remota según 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 ZENworks Remote Management aparecerá en el área de notificación.

## 2.3 Creación de la directiva de gestión remota

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

Por defecto, se crea una directiva de gestión remota segura en el dispositivo gestionado cuando se distribuye ZENworks Adaptive Agent 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 mostrar 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 busque y seleccione una carpeta. 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 del Centro de control de ZENworks.

4 Haga clic en *Siguiente* para mostrar la página Valores generales de gestión remota. Para aceptar los valores por defecto, diríjase al paso siguiente o utilice la información especificada en la tabla que aparece a continuación para cambiar esos valores.

| Campo | Detalles |
|---|---|
| *Permitir que el usuario solicite una sesión remota* | Permite al usuario del dispositivo gestionado pedir a un operador remoto que efectúe una sesión remota. El operador remoto se debe asegurar de que se estén ejecutando las Escuchas de control remoto. |
| *Terminar la sesión remota cuando se requiera permiso para que un usuario nuevo se registre en el dispositivo gestionado* | Termina una sesión remota en curso cuando se requiera permiso de un nuevo usuario que haya entrado en el dispositivo gestionado de forma remota. |
| *Mostrar la información de auditoría de la sesión remota al usuario en el dispositivo gestionado* | Permite al usuario del dispositivo gestionado ver y auditar la información de sesiones remotas desde el icono de ZENworks. |
| *Mostrar las propiedades de gestión remota en ZENworks Icon* | Permite al usuario del dispositivo gestionado ver las propiedades asociadas con la directiva de gestión remota en el icono de ZENworks. |
| *Editar* | Para editar el mensaje que se muestra al usuario del dispositivo gestionado antes de iniciar una sesión remota:<br>1. Haga clic en *Editar* para ver el recuadro de diálogo Editar mensaje.<br>2. Edite el mensaje.<br>3. Haga clic en *Aceptar.* |
| *Restablecer valor por defecto* | Para restablecer el mensaje por defecto:<br>1. Haga clic en *Restablecer valor por defecto* para recuperar el mensaje por defecto. |
| *Añadir una escucha remota* | Para añadir una escucha remota:<br>1. Haga clic en *Añadir*.<br>2. 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.<br>3. Haga clic en *Aceptar.* |
| *Suprimir una escucha remota* | Para suprimir una escucha remota:<br>1. Seleccione la escucha remota que desee suprimir.<br>2. Haga clic en *Suprimir.* |

5 Haga clic en *Siguiente* para acceder a la página Valores de control remoto. Para aceptar los valores por defecto, diríjase al paso siguiente o utilice la información especificada en la tabla que aparece a continuación para cambiar esos valores.

| Campo | Detalles |
|---|---|
| *Permitir que los dispositivos gestionados se puedan controlar de forma remota* | Permite las sesiones de control remoto en el dispositivo gestionado. Cuando se selecciona esta opción, se habilitan las demás opciones de la página. Cuando se elimina la selección, se inhabilitan las operaciones de control remoto en el dispositivo. |
| *Pedir permiso del usuario en el dispositivo gestionado antes de iniciar el control remoto* | Permite pedir permiso al usuario del dispositivo gestionado antes de empezar la sesión de control remoto. |
| *Proporcionar una señal visual al usuario del dispositivo gestionado durante el control remoto* | 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. |
| *Proporcionar una señal sonora al usuario del dispositivo gestionado cada [ ] segundos durante el control remoto* | Produce 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. |
| *Permitir que la pantalla del dispositivo remoto esté en blanco durante el control remoto* | Permite que la pantalla del dispositivo gestionado esté vacía durante la sesión de control remoto. Cuando se selecciona esta opción, también se bloquean los controles del teclado y del ratón del dispositivo gestionado. |
| *Permitir que se bloqueen el ratón y el teclado durante el control remoto* | Permite bloquear el ratón y el teclado del dispositivo gestionado durante una sesión de control remoto. |
| *Permitir que el protector de pantalla se desbloquee automáticamente durante el control remoto* | 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. |
| *Terminar automáticamente la sesión de control remoto tras una inactividad de [ ] minutos* | Termina una sesión de control remoto en el dispositivo gestionado si permanece inactivo durante el tiempo especificado. |

**6** Haga clic en *Siguiente* para mostrar la página Valores de vista remota. Para aceptar los valores por defecto, diríjase al paso siguiente o utilice la información especificada en la tabla que aparece a continuación para cambiar esos valores.

| Campo | Detalles |
|---|---|
| *Permitir la vista remota del dispositivo gestionado* | Permite las sesiones de vista remota en el dispositivo gestionado. Cuando se selecciona esta opción, se habilitan las demás opciones de la página. Cuando se elimina la selección, se inhabilitan las operaciones de vista remota en el dispositivo. |
| *Pedir permiso del usuario en el dispositivo gestionado antes de iniciar la vista remota* | Permite pedir permiso al usuario del dispositivo gestionado antes de empezar la sesión de vista remota. |

| Campo | Detalles |
|---|---|
| *Proporcionar una señal visual al usuario del dispositivo gestionado durante la vista remota* | 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. |
| *Proporcionar una señal sonora al usuario del dispositivo gestionado cada [ ] segundos durante la vista remota.* | Produce 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 mostrar la página Valores de diagnóstico remoto. Para aceptar los valores por defecto, diríjase al paso siguiente o utilice la información especificada en la tabla que aparece a continuación para cambiar esos valores.

| Campo | Detalles |
|---|---|
| *Permitir el diagnóstico remoto del dispositivo gestionado* | Permite las sesiones de diagnóstico remoto en el dispositivo gestionado. Cuando se selecciona esta opción, se habilitan las demás opciones de la página. Cuando se elimina la selección, se inhabilitan las operaciones de diagnóstico remoto en el dispositivo. |
| *Solicitar permiso al usuario del dispositivo gestionado antes de iniciar el diagnóstico remoto* | Garantiza que el operador de diagnóstico remoto deberá solicitar permiso del usuario del dispositivo gestionado antes de iniciar una sesión de diagnóstico remoto. |
| *Proporcionar una señal visual al usuario del dispositivo gestionado durante el diagnóstico remoto* | 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. |
| *Proporcionar una señal sonora al usuario del dispositivogestionadocada [ ] segundos durante el diagnóstico remoto* | Produce 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. |
| *Permitir que la pantalla del dispositivo remoto esté en blanco durante el diagnóstico remoto* | Permite que la pantalla del dispositivo gestionado esté vacía 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. |
| *Mostrar mensaje de advertencia antes de rearrancar durante [ ] segundos* | Muestra un mensaje de advertencia en el dispositivo gestionado al principio de la sesión de diagnóstico remoto para que el usuario recuerde 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 rearranque el sistema durante la sesión de diagnóstico remoto. |

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

**8** Haga clic en *Siguiente* para acceder a la página Valores de ejecución remota. Para aceptar los valores por defecto, diríjase al paso siguiente o utilice la información especificada en la tabla que aparece a continuación para cambiar esos valores.

| Campo | Detalles |
|---|---|
| *Permitir que se ejecuten programas de forma remota en el dispositivo gestionado* | Permite que se ejecuten programas de forma remota en el dispositivo gestionado. Cuando se selecciona esta opción, se habilitan las demás opciones de la página. Cuando se elimina la selección, se inhabilitan las operaciones de ejecución remota en el dispositivo. |
| *Pedir permiso del usuario en el dispositivo gestionado antes de iniciar la ejecución remota* | Garantiza que el operador remoto deberá solicitar permiso del usuario del dispositivo gestionado antes de iniciar una sesión de ejecución remota. |
| *Presentar señal visual al usuario en el dispositivo gestionado durante la ejecución remota* | 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. |
| *Terminar automáticamente la sesión de diagnóstico remoto tras una inactividad de [ ] minutos* | Termina la sesión de ejecución remota si permanece inactiva durante el 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 |
|---|---|
| *Permitir la transferencia de archivos en el dispositivo gestionado* | Habilita la transferencia de archivos entre la consola de gestión y el dispositivo gestionado. Cuando se selecciona esta opción, se habilitan las demás opciones de la página. Cuando se elimina la selección, se inhabilitan las operaciones de transferencia de archivos en el dispositivo. |
| *Pedir permiso del usuario en el dispositivo gestionado antes de iniciar la transferencia del archivo* | Garantiza que el operador remoto deberá solicitar permiso del usuario del dispositivo gestionado antes de iniciar una sesión de transferencia de archivos. |
| *Presentar señal visual al usuario en el dispositivo gestionado durante la transferencia de archivo* | 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 |
|---|---|
| *Permitir la descarga de archivos desde el dispositivo gestionado* | 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. |
| *Directorio raíz de transferencia de archivo* | 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 |
|---|---|
| *Habilitar autenticación basada en contraseña* | Permite que el usuario remoto utilice una contraseña para autenticarse en el dispositivo gestionado. Seleccione esta opción para configurar los valores del tipo de contraseña. |
| *Longitud mínima de la contraseña* | Permite especificar la longitud mínima de la contraseña. Por defecto, la longitud es de 6 caracteres. |
| *Contraseña de sesión* | 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. |
| *Contraseña permanente* | Seleccione esta opción para definir las contraseñas de ZENworks y de VNC. Se recomienda definir la contraseña de ZENworks, puesto que es más segura que la contraseña 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.<br><br>Para permitir que el usuario defina la contraseña a través del icono de ZENworks, seleccione la opción *Permitir que el usuario sobrescriba las contraseñas por defecto del dispositivo gestionado.* |

| Campo | Detalles |
|---|---|
| *Contraseña de ZENworks* | Para borrar la contraseña de ZENworks:<br>1. Haga clic en *Borrar contraseña.*<br>2. Haga clic en *Aplicar* y después en *Aceptar.*<br>Para definir la contraseña de ZENworks:<br>1. Haga clic en *Definir contraseña.*<br>2. Escriba la contraseña. La longitud máxima de las contraseñas de es de 255 caracteres.<br>3. Haga clic en *Aplicar* y después en *Aceptar.* |
| *Contraseña VNC* | Para borrar la contraseña de VNC:<br>1. Haga clic en *Borrar contraseña.*<br>2. Haga clic en *Aplicar* y después en *Aceptar.*<br>Para definir la contraseña de VNC:<br>1. Haga clic en *Definir contraseña.*<br>2. Escriba la contraseña. La longitud máxima de las contraseñas de es de 8 caracteres.<br>3. Haga clic en *Aplicar* y después en *Aceptar.* |

### *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 las demás opciones de la sección Detección de intruso. |
| *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 de ZENworks Adaptive Agent, haga clic en *Valores de seguridad* y después haga clic en *Habilitar la aceptación de conexiones si hay un bloqueo vigente debido a la detección de intrusos.* Por defecto, el tiempo está definido en 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 las demás opciones de la sección Seguridad de la sesión. |

| Campo | Detalles |
|---|---|
| *Permitir conexión si la consola de gestión remota no tiene un certificado SSL* | 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. |
| *Permitir hasta [ ] niveles de la cadena de certificado del visor* | 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.<br><br>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. |

***Terminación anormal***

| Campo | Detalles |
|---|---|
| *Bloquear dispositivo* | Bloquea el dispositivo gestionado cuando la sesión remota termina de forma anormal. |
| *Salir de sesión del usuario* | 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 inmediatamente, o bien haga clic en *Definir propiedades adicionales* para especificar información adicional, como la asignación, la aplicación o el estado de la directiva o el 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 del dispositivo o derechos específicos del 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 desee asignar derechos de gestión remota.

3 En el panel Derechos asignados, haga clic en *Añadir* y, a continuación, en *Derechos de gestión remota* para mostrar el recuadro de diálogo correspondiente.

4 Seleccione el dispositivo o el usuario al que desee asignar los derechos.

La tabla siguiente contiene información sobre los derechos de gestión remota:

| Derechos de gestión remota | Detalles |
|---|---|
| Control remoto | Asigna al operador remoto los derechos para controlar dispositivos de forma remota. |
| Vista remota | Asigna al operador remoto los derechos para ver dispositivos de forma remota. |
| Diagnóstico remoto | Asigna al operador remoto los derechos para realizar diagnósticos en los dispositivos de forma remota. |
| Ejecución remota | Asigna al operador remoto los 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

En las secciones siguientes se proporciona información sobre la configuración de la contraseña de gestión remota para el servicio de gestión remota del dispositivo gestionado:

- Sección 2.5.1, “Configuración de la contraseña de gestión remota mediante el Centro de control de ZENworks”, en la página 31
- Sección 2.5.2, “Configuración de la contraseña de gestión remota mediante ZENworks Adaptive Agent”, en la página 32
- Sección 2.5.3, “Eliminación de la contraseña de gestión remota mediante el Centro de control de ZENworks”, en la página 33
- Sección 2.5.4, “Eliminación de la contraseña de gestión remota mediante ZENworks Adaptive Agent”, en la página 33

## 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 23”.

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 de gestión remota mediante ZENworks Adaptive Agent

El usuario del dispositivo gestionado puede establecer una contraseña para el servicio de gestión remota si la opción *Permitir que el usuario sobrescriba las contraseñas por defecto del dispositivo gestionado* está activada en la directiva de gestión remota en vigor en el dispositivo gestionado. Esta contraseña tendrá prioridad sobre la establecida en la directiva de gestión remota.

Para definir una contraseña en el dispositivo gestionado:

1. Haga doble clic en el icono *ZENworks Adaptive Agent* para mostrar la ventana ZENworks Adaptive Agent.
2. En el panel izquierdo, diríjase a *Gestión remota* y haga clic en *Seguridad*.
3. En el panel de la derecha, haga clic en *Definir contraseña* para establecer las contraseñas siguientes:
   - **Contraseña de ZENworks (se recomienda):** se utiliza para la autenticación en ZENworks. Puede tener una longitud máxima de 255 caracteres.
   - **Contraseña de VNC:** se utiliza en la autenticación de VNC para trabajar conjuntamente con los 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 definida mediante 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 esta directiva en la página Resumen o en 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 esta directiva en la página Resumen o en Tareas comunes para actualizar los cambios de la directiva en el dispositivo gestionado.

### 2.5.4 Eliminación de la contraseña de gestión remota mediante ZENworks Adaptive Agent

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

1. Haga doble clic en el icono *ZENworks Adaptive Agent* para mostrar la ventana ZENworks Adaptive Agent.
2. En el panel izquierdo, diríjase 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.

---

**Nota:** la instalación del visor de gestión remota en SUSE® Linux Enterprise Server 11 (SLES 11) o SUSE Linux Enterprise Desktop 11 (SLED 11) requiere el paquete glitz dependiente. Debe instalar el paquete glitz adecuado del sitio Web de openSUSE® (http://software.opensuse.org/112/en).

---

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 Linux de Novell ZENworks 10 Configuration Management SP2 (10.2) a Novell ZENworks 10 Configuration Management SP3 (10.3) o posterior, ejecute el siguiente comando como superusuario o usuario Root:

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

También puede desinstalar la versión anterior, `novell-zenworks-rm-viewer-10.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 33.

# 2.8 Inicio de operaciones de gestión remota

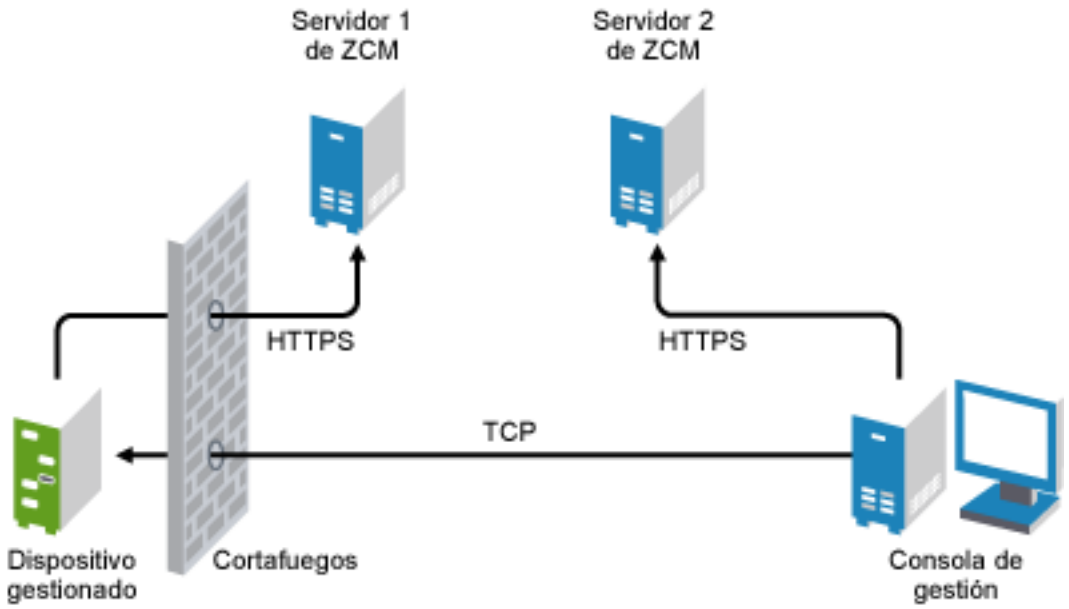
Las operaciones de gestión remota se pueden iniciar de las siguientes formas:

- Sección 2.8.1, “Inicio de una sesión desde la consola de gestión”, en la página 35
- Sección 2.8.2, “Inicio de una sesión desde el dispositivo gestionado”, en la página 44

## 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 la configuración de la zona de gestión de ZENworks abarca dos o más redes privadas habilitadas para NAT que están interconectadas por una red pública, deberá distribuir DNS_ALG en los gateways de esas redes privadas. DNS_ALG se asegura de que las consultas de búsqueda DNS iniciadas por los componentes de ZENworks devuelvan el nombre de host asignado a la dirección privada correcta y habilita la comunicación entre la consola de gestión y los dispositivos gestionados. Para obtener más información acerca de DNS_ALG, consulte DNS ALG RFC - 2694 (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 mediante uno de los siguientes métodos:

- “Inicio de una operación de gestión remota en el Centro de control de ZENworks” en la página 36
- “Inicio de una operación de gestión remota en modo independiente” en la página 43
- “Inicio de una operación de gestión remota mediante las opciones de la línea de comandos” en la página 43

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

Las distintas operaciones de gestión remota se pueden iniciar desde el contexto del dispositivo o desde el contexto del usuario:

- “Inicio de una sesión de gestión remota desde el contexto del dispositivo” en la página 36
- “Inicio de una sesión de gestión remota desde el contexto del usuario” en la página 40

#### 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 desee gestionar de forma remota. Haga clic en *Acción* y seleccione la operación de gestión remota que desee llevar a cabo.

   O bien

   En la opción *Tareas de dispositivo* del panel izquierdo, seleccione la operación de gestión remota que desee llevar a cabo.

   Las operaciones remotas disponibles son:

   - **Control remoto:** muestra el recuadro de diálogo Gestión remota, en el que puede realizar operaciones de control remoto, vista remota o ejecución remota en el dispositivo gestionado.
   - **Diagnóstico remoto:** muestra el recuadro de diálogo Diagnóstico remoto, en el que puede realizar operaciones de diagnóstico remoto en el dispositivo gestionado.

- **Transferir archivos:** muestra el recuadro de diálogo Transferencia de archivos, en el que puede realizar operaciones de transferencia de archivos en el dispositivo gestionado.

**3** Rellene las opciones del recuadro de diálogo que se muestra. La siguiente tabla recoge información acerca de las opciones disponibles:

| Campo | Detalles |
|---|---|
| Dispositivo | Especifique el nombre de host o la dirección IP del dispositivo que desee gestionar de forma remota. |
| Operación | 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 | Seleccione el modo que desee utilizar para autenticarse en el dispositivo gestionado. Los modos de autenticación son:<br>◆ Autenticación basada en derechos<br>◆ Autenticación basada en contraseñas |
| 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 | Seleccione uno de los siguientes modos para la sesión:<br>◆ **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:<br>◆ Invitar a otros operadores a unirse a la sesión remota.<br>◆ Delegar derechos de control remoto a un operador remoto.<br>◆ Recuperar el control del operador remoto.<br>◆ Terminar la sesión remota.<br>Las sesiones que se lancen posteriormente serán sesiones de vista remota.<br>**Nota:** el modo de colaboración no se admite todavía en Linux.<br>◆ **Compartido:** permite que varios usuarios remotos controlen de forma simultánea el dispositivo gestionado.<br>◆ **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.<br>Esta opción sólo está disponible en el recuadro de diálogo Gestión remota. |
| 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. |

| Campo | Detalles |
|---|---|
| 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. |
| Habilitar registro | registra información de la sesión y de depuración en el archivo `novell-zenworks-vncviewer.txt`. 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 de mozilla si se lanza mediante Mozilla* Firefox*. |
| Encaminar a través del servidor proxy | 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.<br><br>Cumplimente los siguientes campos:<br><br>**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.<br><br>**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.<br><br>**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. |
| Utilizar el siguiente par de claves para la identificación | 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:<br><br>**Clave privada:** haga clic en *Examinar* para buscar y seleccionar la clave privada del operador remoto.<br><br>**Certificado:** haga clic en *Examinar* para buscar y seleccionar el certificado correspondiente a la clave privada. Este certificado debe estar encadenado a la autoridad certificadora configurada en la zona.<br><br>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.<br><br>**Habilitar vía de caché:** permite que las vías de la clave primaria y el certificado se almacenen en caché en la consola de gestión.<br><br>Esta opción sólo se admite en Windows en este momento. |

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 ayudar a un usuario realizando una sesión remota en el dispositivo gestionado en el que ese usuario 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 que haya entrado en el dispositivo que se va a gestionar de forma remota.
4. Haga clic en *Acción* y seleccione la operación de gestión remota que desee llevar a cabo.

   Las operaciones disponibles son:

   - **Control remoto:** muestra el recuadro de diálogo Gestión remota, en el que puede realizar operaciones de control remoto, vista remota o ejecución remota en el dispositivo gestionado.
   - **Diagnóstico remoto:** muestra el recuadro de diálogo Diagnóstico remoto, en el que puede realizar operaciones de diagnóstico remoto en el dispositivo gestionado.
   - **Transferir archivos:** muestra el recuadro de diálogo Transferencia de archivos, en el que puede realizar operaciones de transferencia de archivos en el dispositivo gestionado.
5. Rellene las opciones del recuadro de diálogo que se muestra. La siguiente tabla recoge información acerca de las opciones disponibles:

| Campo | Detalles |
|---|---|
| Dispositivo | Especifique el nombre de host o la dirección IP del dispositivo que desee gestionar de forma remota. |
| Operación | 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 | Seleccione el modo que desee utilizar para autenticarse en el dispositivo gestionado. Los modos de autenticación son:<br>◆ Autenticación basada en derechos<br>◆ Autenticación basada en contraseñas |
| 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 | Seleccione uno de los siguientes modos para la sesión:<br>◆ **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:<br>◆ Invitar a otros operadores a unirse a la sesión remota.<br>◆ Delegar derechos de control remoto a un operador remoto.<br>◆ Recuperar el control del operador remoto.<br>◆ Terminar la sesión remota.<br>Las sesiones que se lancen posteriormente serán sesiones de vista remota.<br>**Nota:** el modo de colaboración no se admite todavía en Linux.<br>◆ **Compartido:** permite que varios usuarios remotos controlen de forma simultánea el dispositivo gestionado.<br>◆ **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.<br>Esta opción sólo está disponible en el recuadro de diálogo Gestión remota. |
| 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. |

| Campo | Detalles |
|---|---|
| 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. |
| Habilitar registro | registra información de la sesión y de depuración en el archivo `novell-zenworks-vncviewer.txt`. 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 de mozilla si se lanza mediante Mozilla* Firefox*. |
| Encaminar a través del servidor proxy | 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.<br><br>Cumplimente los siguientes campos:<br><br>**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.<br><br>**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.<br><br>**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. |
| Utilizar el siguiente par de claves para la identificación | 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:<br><br>**Clave privada:** haga clic en *Examinar* para buscar y seleccionar la clave privada del operador remoto.<br><br>**Certificado:** haga clic en *Examinar* para buscar y seleccionar el certificado correspondiente a la clave privada. Este certificado debe estar encadenado a la autoridad certificadora configurada en la zona.<br><br>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.<br><br>**Habilitar vía de caché:** permite que las vías de la clave primaria y el certificado se almacenen en caché en la consola de gestión.<br><br>Esta opción sólo se admite en Windows en este momento. |

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. Para obtener información sobre la instalación del visor, consulte la Sección 2.6, “Instalación del visor de gestión remota”, en la página 33.

Para iniciar la operación de gestión remota en modo independiente:

1. Haga doble clic en el archivo `nzrViewer.exe` para lanzar el cliente de ZENworks Remote Management.
2. En la ventana de conexión de ZENworks Remote Management 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, instale el visor de gestión remota. Para obtener información sobre la instalación del visor, consulte la Sección 2.6, “Instalación del visor de gestión remota”, en la página 33.

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 está instalado el visor. El visor se instala por defecto en el directorio `<Carpeta_de_datos_de_aplicación_del_usuario>\Novell\ZENworks\Remote Management\bin`.
2. Ejecute el comando siguiente:

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

   El puerto por defecto para el dispositivo gestionado es el 5950.

   Para obtener información sobre las opciones de la línea de comandos disponibles, consulte la Sección 2.9.1, “Opciones de la línea de comandos para lanzar una operación remota”, en la página 46.
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 no quiere especificar las opciones de línea de comandos `key`, `cert` y `CAcert` en el comando `nzrViewer` para la autenticación SSL, asegúrese de que la opción *Permitir conexión si la consola de gestión remota no tiene un certificado SSL* de la configuración de seguridad de la directiva de gestión remota está habilitada. 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.

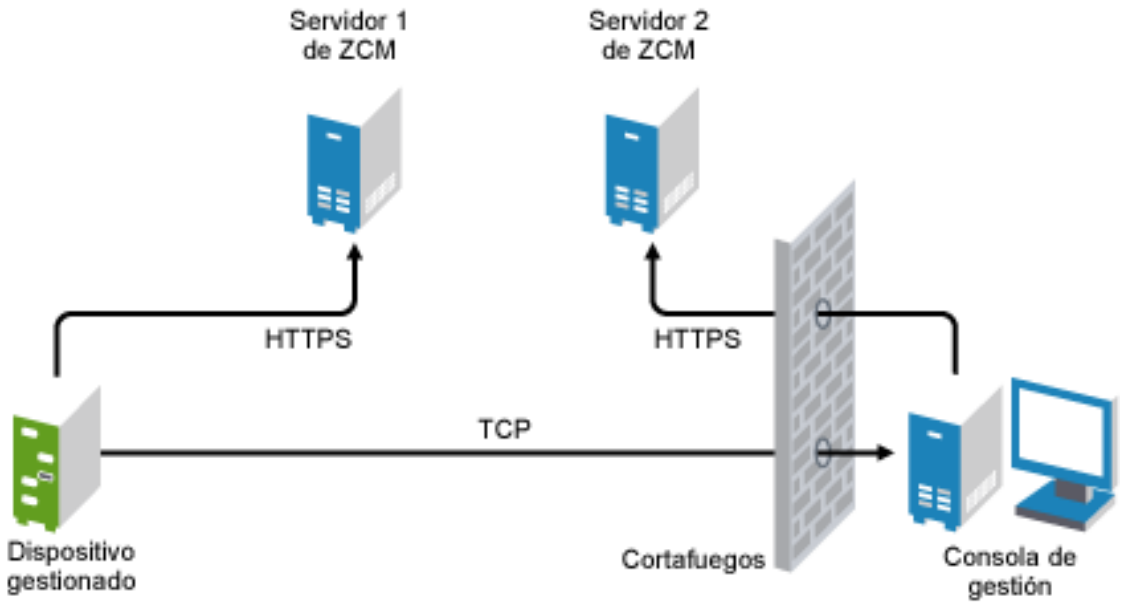
---

- 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.

## 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 gestión remota, 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 aparece en la lista, proporcione la información de conexión del operador en los campos *Pedir conexión.*
5. En el campo *Operación,* seleccione el tipo de operación que desee 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 las conexiones establecidas desde una red pública a una red privada, distribuya el gateway a nivel de aplicación DNS (DNS_ALG). Para obtener más información sobre DNS_ALG, consulte RFC 2694 (http://www.ietf.org/rfc/rfc2694).

# 2.9 Opciones para lanzar una operación de gestión remota

Si lanza una operación de gestión remota desde la línea de comandos, puede especificar opciones para controlar el comportamiento de la sesión remota. Por ejemplo, si especifica la opción `remotecontrol`, se lanza una operación de control remoto en el dispositivo; mientras que si se especifica la opción `notoolbar`, se oculta la barra de herramientas de la ventana de visualización.

La gestión remota usa varias opciones de forma interna a la hora de lanzar una operación de gestión remota en un dispositivo. Por ejemplo, la opción `zenrights` especifica que el esquema de autenticación es la autenticación de derechos de ZENworks. No debe especificar estas opciones internas si usa la línea de comandos para lanzar una operación de sesión remota en un dispositivo. Para obtener más información sobre las opciones que se usan de forma interna, consulte la Sección 2.9.2, “Opciones internas para lanzar una operación remota”, en la página 49.

Revise las secciones siguientes para obtener más información sobre las opciones de gestión remota:

- Sección 2.9.1, “Opciones de la línea de comandos para lanzar una operación remota”, en la página 46
- Sección 2.9.2, “Opciones internas para lanzar una operación remota”, en la página 49

## 2.9.1 Opciones de la línea de comandos para lanzar una operación remota

Utilice las siguientes opciones de la línea de comandos para controlar una operación remota:

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

| Opción de la línea de comandos | Parámetro | Descripción |
|---|---|---|
| listen | *puerto* | Habilita la escucha para las peticiones de sesión remota en el puerto especificado. Por defecto, el puerto es el 5550. |
| restricted | | Oculta 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. |
| remoteexecute | | Lanza una operación de ejecución remota en el dispositivo gestionado. |
| diagnostics | *nombre_aplicación* | 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 | *nivel* | 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:<br>◆ 0 indica que no se aplica compresión alguna<br>◆ 1 proporciona la velocidad mayor<br>◆ 9 proporciona el mayor nivel de compresión<br>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. |
| noencrypt | | Lanza la sesión remota en modo no cifrado. |
| fullscreen | | Lanza una operación remota en modo de pantalla completa en el dispositivo gestionado. |
| notoolbar | | Oculta 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. |
| shared | | 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. |

| Opción de la línea de comandos | Parámetro | Descripción |
|---|---|---|
| collaborate | | Lanza la sesión remota en modo de colaboración. Esta opción no se puede usar todavía en Linux. |
| 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. |
| 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 | | Oculta la barra de desplazamiento en la ventana de visualización. |
| scale | *porcentaje* | Amplía la ventana de visualización con el porcentaje de escala especificado. |
| emulate3timeout | *ms* | 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 | *n* | Especifica los niveles de registro de información. |

| Opción de la línea de comandos | Parámetro | Descripción |
|---|---|---|
| console | | Registra información en una ventana de consola. |
| logfile | *nombre_archivo* | Nombre del archivo de registro donde se debe registrar la información. |
| config | *nombre_archivo* | Nombre del archivo de configuración que se debe utilizar para cargar los valores de configuración predefinidos. |
| key | *nombre_archivo* | Nombre del archivo donde se almacena la clave privada. Esta clave se utiliza en las operaciones de enlace SSL con el dispositivo gestionado.<br><br>**Importante:** las opciones key y cert se deben utilizar juntas. Si se utilizan estas opciones con el comando `nzrViewer`, debe inhabilitar por motivos de seguridad la opción *Permitir conexión si la consola de gestión remota no tiene un certificado SSL* en los valores de seguridad de la directiva para gestión remota. |
| cert | *nombre_archivo* | Nombre del archivo donde se almacena el certificado correspondiente a la clave privada.<br><br>**Importante:** las opciones key y cert se deben utilizar juntas. Si se utilizan estas opciones con el comando `nzrViewer`, debe inhabilitar por motivos de seguridad la opción *Permitir conexión si la consola de gestión remota no tiene un certificado SSL* en los valores de seguridad de la directiva para gestión remota. |
| CAcert | *nombre_archivo* | 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 | *nombrecodificación* | 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 | *n* | 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 | *n* | 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. |
| zenpasswd | | Especifica que se debe utilizar el esquema de autenticación basada en contraseña de ZENworks. |

| Opción de la línea de comandos | Parámetro | Descripción |
|---|---|---|
| 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 | servidor_proxy | 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:<br>◆ *Dirección IP~~Puerto*. Por ejemplo: 10.0.0.0~~5750.<br>◆ *Dirección IP~Puerto*. Por ejemplo: 10.0.0.0~50.<br>El puerto por defecto para el servidor proxy es 5750. |

## 2.9.2 Opciones internas para lanzar una operación remota

La tabla siguiente muestra las opciones que se usan de forma interna en la gestión remota. Estas opciones no se deben usar para lanzar una operación de gestión remota desde la línea de comandos.

***Tabla 2-2*** *Opciones internas para lanzar una operación remota*

| Opción | Descripción |
|---|---|
| zenrights | Especifica la autenticación de derechos de ZENworks como esquema de autenticación. |
| pipe | Especifica la información de autenticación. |

# 2.10 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 se puede instalar en un dispositivo gestionado Windows o un dispositivo Linux (servidor primario o satélite). El servidor proxy de gestión remota escucha por defecto en el puerto 5750.

Para obtener más información sobre el servidor proxy de gestión remota, consulte la Sección 1.4, “Descripción del servidor proxy de gestión remota”, en la página 17.

Para obtener información sobre los requisitos del sistema que deben cumplir los dispositivos gestionados Windows o los dispositivos Linux para habilitar la instalación del servidor proxy en el dispositivo, consulte “Requisitos del sistema” en la *Guía de instalación de ZENworks 10 Configuration Management*.

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

En Windows:

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>.msi` y guarde el archivo en una ubicación temporal.

   *versión* es la versión del producto de ZENworks.
4. Instale la aplicación del proxy ejecutando el siguiente comando:

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

En Linux:

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>.noarch.rpm`.
4. Elija entre instalar el servidor proxy inmediatamente o guardar el archivo RPM para instalarlo después.
   - Para instalar inmediatamente el servidor proxy, haga clic en *Abrir con* para abrir el servidor proxy de gestión remota con zen-installer, especifique la contraseña raíz y haga clic en *Aceptar*.
   - Para guardar el archivo RPM del servidor proxy 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 servidor proxy, especifique la contraseña raíz y haga clic en *Aceptar*.
     - Ejecute el siguiente comando como superusuario o como usuario Root:

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

El servidor proxy de gestión remota está diseñado para ejecutarse automáticamente tras la instalación. Es posible personalizar su comportamiento modificando la configuración por defecto del dispositivo. Para obtener más información sobre la configuración del servidor proxy de gestión remota, consulte la Sección 2.11, “Configuración de un servidor proxy de gestión remota”, en la página 50.

# 2.11 Configuración de un servidor proxy de gestión remota

Cuando se instala un servidor proxy de gestión remota en un dispositivo, en este dispositivo se configuran por defecto algunos ajustes que es posible editar.


- Sección 2.11.1, “Ajustes del servidor proxy de gestión remota en dispositivos Windows”, en la página 51
- Sección 2.11.2, “Ajustes del servidor proxy de gestión remota en servidores primarios Linux o en servidores satélite”, en la página 51


## 2.11.1 Ajustes del servidor proxy de gestión remota en dispositivos Windows

En los dispositivos Windows, los ajustes del registro para el servidor proxy de gestión remota están disponibles en `HKLM\SOFTWARE\Novell\ZCM\Remote Management\Proxy`.

**ClientPort:** permite especificar el número de puerto que usa el servidor proxy para escuchar las peticiones de sesión remota del visor de gestión remota. El valor por defecto es 5750.

**SessionEncryption:** permite especificar si el flujo de datos inicial entre el servidor proxy y el visor de gestión remota está cifrado. El valor por defecto es Verdadero. Este ajuste no es aplicable después de que el servidor proxy establezca conexión con el dispositivo gestionado. El cifrado de la sesión se controla a partir de entonces mediante la directiva de gestión remota y las preferencias del operador remoto. Debe dejar el valor de este ajuste en Verdadero, ya que si lo cambia a Falso, otros procesos externos sin autenticar distintos al del visor de gestión remota podrían establecer conexiones con los dispositivos situados en la red privada.

**SSLClientAuthentication:** permite especificar si el servidor proxy puede aceptar peticiones de conexión de visores que no cuenten con un certificado válido. Los valores posibles son Verdadero y Falso. El valor por defecto es Verdadero.

## 2.11.2 Ajustes del servidor proxy de gestión remota en servidores primarios Linux o en servidores satélite

En un servidor primario Linux o en un servidor satélite, los ajustes del servidor proxy de gestión remota se encuentran en el archivo `/etc/opt/novell/zenworks/repeater/nzrepeater.ini`. Algunos de los ajustes son:

**viewerport:** permite especificar el número de puerto que usa el servidor proxy de gestión remota para escuchar las peticiones de sesión remota del visor de gestión remota. El valor por defecto es 5750.

**runasuser:** permite especificar el usuario cuyo papel debe adoptar el servidor proxy. El servidor proxy de gestión remota sólo requiere privilegios de usuario para realizar operaciones remotas. El valor por defecto es zenworks. Sin embargo, es posible especificar un usuario distinto.

**strictimpersonation:** especifica si la sesión remota debe continuar como usuario `Root` si el usuario indicado en runasuser no existe. Los valores posibles son Verdadero y Falso. el valor por defecto es Falso, que indica que la sesión remota continúa como usuario `Root` si el usuario especificado en la opción runasuser no existe.

**sslauth:** especifica si la autenticación SSL está habilitada o no. Los valores posibles son 0 y 1. El valor por defecto es 1, que indica que está habilitada.

---

**Advertencia:** no se recomienda inhabilitar la autenticación SSL, ya que se permitiría que los procesos externos pudieran acceder a los dispositivos de la red sin autenticación alguna.

---

**verifyViewerCert:** especifica si hay que verificar los certificados del visor de gestión remota. Este ajuste sólo es aplicable si la autenticación SSL está habilitada. Los valores posibles son 0 y 1. El valor por defecto es 1, que indica que los certificados del visor de gestión remota se deben verificar. Cuando se inicia una sesión desde un visor independiente, puede que el operador remoto no cuente con los certificados requeridos, que están encadenados a la autoridad certificadora raíz. En tal caso, el servidor proxy no consigue conectar con el servidor.

**loggingenabled:** especifica si los mensajes se deben registrar en el dispositivos. Los valores posibles son Verdadero y Falso. El valor por defecto es Verdadero.

Para obtener información sobre los ajustes del registro, consulte el archivo `/etc/opt/novell/zenworks/repeater/nzrepeater.ini`.

# 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:



## 3.1 Gestión de una sesión de control remoto

La gestión remota permite controlar de forma remota un dispositivo gestionado. Con las conexiones de control remoto, el operador remoto puede pasar de ver el dispositivo gestionado a tomar el control de este dispositivo, con lo que podrá asistir al usuario y resolver problemas en el dispositivo gestionado. 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 35.

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

En la tabla siguiente se describen las distintas opciones de la barra de herramientas disponibles en el visor de gestión remota durante una sesión de control remoto. Además incluye las teclas de acceso directo si están disponibles.

***Tabla 3-1*** *Opciones de la barra de herramientas en el 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 y 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. |

| Opción | Tecla de acceso directo | Función |
|---|---|---|
| *Pantalla completa*<br>  | Ctrl+Alt+Mayús+F | Permite cambiar entre la pantalla completa y el modo normal. |
| *Pedir actualización de pantalla*<br>  | Ctrl+Alt+Mayús+H | Renueva la ventana de visualización. |
| *Enviar Ctrl+Alt+Supr*<br>  | | Transfiere la pulsación de las teclas Ctrl+Alt+Supr al dispositivo gestionado.<br>La capacidad para simular las funciones de Ctrl+Alt+Supr en dispositivos con Windows 7 está inhabilitada actualmente. |
| *Enviar Ctrl+Esc*<br>  | | Activa el menú Inicio en el dispositivo gestionado. |
| *Enviar presión/ liberación de tecla Alt*<br>  | | Si se hace clic en esta opción y se pulsa la tecla Alt del teclado, se envía la pulsación de la tecla Alt al dispositivo gestionado. |
| *Borrar o mostrar pantalla*<br>  | Ctrl+Alt+Mayús+B | Borra el contenido de la pantalla del dispositivo gestionado o lo muestra. Si la pantalla del dispositivo está en blanco, las operaciones realizadas por el operador remoto en el dispositivo no serán visibles para el usuario del dispositivo. Además, se bloquean los controles del teclado y el ratón del dispositivo gestionado.<br>Esta opción sólo se habilita si la opción *Permitir que la pantalla del dispositivo remoto esté en blanco* está activada en la directiva de gestión remota vigente en el dispositivo gestionado. |
| *Bloquear o desbloquear teclado y ratón*<br>  | Ctrl+Alt+Mayús+L | Bloquea o desbloquea el teclado y el ratón del dispositivo gestionado. Si el control del ratón y el teclado del dispositivo está bloqueado, el usuario del dispositivo gestionado no podrá usar estos elementos.<br>Esta opción sólo se habilita si la opción *Permitir que se bloqueen el ratón y el teclado del dispositivo gestionado durante el control remoto* está activada en la directiva de gestión remota vigente en el dispositivo gestionado. |

| Opción | Tecla de acceso directo | Función |
|---|---|---|
| *Transferir archivos*  | Ctrl+Alt+Mayús+T | Lanza una sesión de transferencia de archivos desde el dispositivo gestionado y hacia él.<br><br>Esta opción sólo se habilita si la opción *Permitir la transferencia de archivos en el dispositivo gestionado* está activada en la directiva de gestión remota vigente en el dispositivo gestionado. Si desea obtener más información sobre la transferencia de archivos, consulte la Sección 3.5, “Gestión de una sesión de transferencia de archivos”, en la página 60. |
| *Colaboración*  | | Lanza una sesión de colaboración de ZENworks Remote Management 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.<br><br>Para obtener más información sobre las sesiones de colaboración, consulte la Sección 3.1.2, “Sesión de colaboración”, en la página 55. |
| *Ejecución remota*  | Ctrl+Alt+Mayús+U | Lanza una sesión de ejecución remota en el dispositivo gestionado que permite lanzar de forma remota cualquier ejecutable en el dispositivo gestionado.<br><br>Esta opción sólo se habilita si la opción *Permitir que se ejecuten programas de forma remota en el dispositivo gestionado* está activada en la directiva de gestión remota vigente en el dispositivo gestionado. |
| *Anular protector de pantalla*  | Ctrl+Alt+Mayús+O | Anula el protector de pantalla protegido mediante contraseña del dispositivo durante la sesión remota.<br><br>Esta opción sólo se habilita si la opción *Permitir que el protector de pantalla se desbloquee automáticamente durante el control remoto* está activada en la directiva de gestión remota vigente en el dispositivo gestionado. |
| *Desconectar*  | Alt+F4 | Cierra la sesión remota. |

## 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 primero en el dispositivo gestionado, se obtienen los privilegios de un operador remoto maestro. Las sesiones de colaboración se pueden utilizar para:

- Invitar a varios operadores remotos a unirse a la sesión de control remoto.

- Delegar los derechos de control remoto a otro operador para que ayude a resolver un problema y recuperar el control posteriormente.
- Terminar una sesión remota.

Para lanzar la 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 35.
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. Los operadores remotos se muestran con entradas independientes precedidas 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 la sesión y se encuentra en modo de vista remota.
- Un círculo gris 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 23”.

En la tabla siguiente se muestran las acciones que se pueden realizar como operador remoto maestro durante la 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 | 1. Seleccione un operador remoto presente en la ventana de sesión de colaboración.<br>2. Haga clic en *Invitar.* | Si el operador remoto acepta la petición y se une a la sesión, el círculo gris correspondiente cambia a rojo.<br>Por defecto, la nueva sesión se inicia en el modo de vista remota. |
| Delegar los derechos de control remoto al operador remoto | 1. Seleccione el operador remoto en el que desee delegar los derechos de control remoto.<br>2. Haga clic en *Delegar.* | El operador remoto seleccionado pasará al modo de control remoto y el círculo rojo correspondiente cambiará a verde.<br>El operador remoto maestro puede cambiar automáticamente al modo de vista remota. |

| Tarea | Pasos | Información adicional |
|---|---|---|
| Recuperar los derechos de control remoto del operador remoto | 1. Haga clic en *Recuperar control.* | El operador remoto cambia al modo de vista remota y el círculo verde correspondiente cambia a rojo.<br><br>El operador remoto maestro puede cambiar automáticamente al modo de control remoto. |
| Terminar la sesión remota | 1. Seleccione el operador remoto cuya sesión remota desee terminar.<br>2. Haga clic en *Terminar.* | Si el operador remoto seleccionado estaba en modo de control remoto, se recuperan los derechos de control remoto.<br><br>La sesión del operador remoto termina y el color del círculo correspondiente cambia a gris. |
| Invitar a un operador remoto externo | 1. Haga clic en *Invitar externo* para invitar a operadores remotos que no aparezcan en la ventana de la sesión de colaboración a unirse a la sesión remota.<br>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.<br>3. Haga clic en *Invitar.* | |

Si el operador remoto maestro desconecta la sesión remota, todos los operadores remotos se desconectarán de la sesión.

# 3.2 Gestión de una sesión de vista remota

La vista remota permite conectar de forma remota con un dispositivo gestionado y ver el escritorio del dispositivo. 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 35.

En la tabla siguiente se describen las distintas opciones de la barra de herramientas disponibles en el visor de gestión remota durante una sesión de vista remota.

***Tabla 3-3*** *Opciones de la barra de herramientas en el visor de gestión remota*

| Opción | Tecla de acceso directo | Función |
|---|---|---|
| *Opciones de conexión*<br>  | Ctrl+Alt+Mayús+P | Permite configurar distintos parámetros de sesión, como el formato y el cifrado, para mejorar el rendimiento, el registro y la gestión del cursor local y remoto. |

| Opción | Tecla de acceso directo | Función |
|---|---|---|
| *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 cambiar entre la pantalla completa y el modo normal. |
| *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 de forma remota archivos ejecutables con privilegios de sistema en el dispositivo gestionado. Para ejecutar una aplicación en un dispositivo gestionado, lance 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 35.
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 esta aplicación no está disponible en la vía indicada del dispositivo gestionado.

**Advertencia:** por defecto, el módulo de gestión remota se ejecuta como un servicio con privilegios de sistema en el dispositivo gestionado. Por lo tanto, todas las aplicaciones que se lancen durante la sesión de ejecución remota también se ejecutarán con estos privilegios. 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, sólo es posible acceder a las aplicaciones de diagnóstico configuradas para el dispositivo en los valores de gestión remota para realizar labores de diagnóstico y solucionar problemas del dispositivo. Durante la sesión, las aplicaciones de diagnóstico se muestran como iconos en una barra de herramientas. Las siguientes aplicaciones de diagnóstico están configuradas por defecto en los valores de gestión remota:

***Tabla 3-4*** *Opciones de la barra de herramientas en el 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 y 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 cambiar entre la pantalla completa y el modo normal. |
| *Pedir actualización de pantalla*  | Ctrl+Alt+Mayús+H | Renueva la ventana de visualización. |
| *Transferir archivos*  | Ctrl+Alt+Mayús+T | Lanza una sesión de transferencia de archivos desde el dispositivo gestionado y hacia él.<br><br>Esta opción sólo se habilita si la opción *Permitir la transferencia de archivos en el dispositivo gestionado* está activada en la directiva de gestión remota vigente en el dispositivo gestionado. Si desea obtener más información sobre la transferencia de archivos, consulte la Sección 3.5, “Gestión de una sesión de transferencia de archivos”, en la página 60. |
| *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 lanzar 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 19.

## 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 35.

En la ventana Transferencia de archivos, el panel del equipo local muestra todos los archivos y las carpetas de la consola de gestión, mientras que el panel del equipo remoto muestra todos los archivos y carpetas del directorio especificado en la opción *Directorio raíz de transferencia de archivo* de la directiva de gestión remota. Si el *Directorio raíz de transferencia de archivo* no se ha especificado 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 Transferencia de archivos*

| Tareas | Teclas aceleradoras | Pasos | Información adicional |
|---|---|---|---|
| Crear nueva carpeta local | Alt+L | 1. Haga clic en *Acciones > Nueva carpeta local*.<br>O bien<br>Haga clic en en el panel del equipo local.<br>2. Siga las indicaciones que aparecen en la pantalla. | |
| Crear nueva carpeta remota | Alt+V | 1. Haga clic en *Acciones > Nueva carpeta remota.*<br>O bien<br>Haga clic en en el panel del equipo remoto.<br>2. Siga las indicaciones que aparecen en la pantalla. | |
| Abrir un archivo | | 1. Haga doble clic en el archivo para abrirlo en su aplicación asociada. | |
| Cambiar el nombre de archivos o carpetas | Alt+N | 1. Seleccione el archivo o la carpeta cuyo nombre desee cambiar.<br>2. Haga clic en *Acciones > Renombrar.*<br>O bien<br>Haga clic en .<br>3. Siga las indicaciones que aparecen en la pantalla. | |
| Suprimir archivos o carpetas | Alt+D | 1. Seleccione los archivos o las carpetas que desee suprimir.<br>2. Haga clic en *Acciones > Suprimir.*<br>O bien<br>Haga clic en .<br>3. Siga las indicaciones que aparecen en la pantalla. | Puede utilizar las teclas Mayús y Ctrl para seleccionar varios archivos a la vez. |

| Tareas | Teclas aceleradoras | Pasos | Información adicional |
|---|---|---|---|
| Actualizar carpeta local | Alt+E | 1. Haga clic en *Acciones > Actualizar carpeta local.*<br>O bien<br>Haga clic en en el panel del equipo local. | |
| Actualizar carpeta remota | Alt+M | 1. Haga clic en *Acciones > Actualizar carpeta remota.*<br>O bien<br>Haga clic en en el panel del equipo remoto. | |
| Ordenar archivos locales | | 1. Haga clic en *Acciones > Ordenar local.*<br>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. |
| Ordenar archivos remotos | | 1. Haga clic en *Acciones > Ordenar remoto*<br>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 | | 1. Seleccione los archivos que desea cargar en el equipo remoto.<br>2. Seleccione la carpeta de destino en el panel del equipo remoto.<br>3. Haga clic en *Acciones > Cargar.*<br>O bien<br>Haga clic en . | La opción *Acción > Cargar* sólo está disponible si el equipo activado es el local.<br>Puede utilizar las teclas Mayús y Ctrl para seleccionar varios archivos a la vez. |

| Tareas | Teclas aceleradoras | Pasos | Información adicional |
|---|---|---|---|
| Descargar archivos o carpetas | Alt+O | 1. Seleccione los archivos que desee descargar al equipo local.<br>2. Seleccione la carpeta de destino en el panel del equipo local.<br>3. Haga clic en *Acciones > Descargar.*<br>O bien<br>Haga clic en ⬅. | La opción *Acción > Descargar* sólo está disponible si el equipo activado es el remoto.<br>Puede utilizar las teclas Mayús y Ctrl para seleccionar varios archivos a la vez.<br>. |
| Cancelar transferencia de archivos | Alt+C | 1. Haga clic en *Acciones > Cancelar transferencia de archivos.* | También puede cancelar la operación de transferencia de archivos haciendo clic en el botón de cancelación. |
| Mostrar propiedades del archivo | Alt+P | 1. Seleccione los archivos.<br>2. Haga clic en *Acciones > Propiedades.*<br>O bien<br>Haga clic en . | Puede utilizar las teclas Mayús y Ctrl para seleccionar varios archivos a la vez.<br>Muestra el tamaño acumulado de los archivos y las carpetas seleccionados. |
| Mover a la carpeta padre | | 1. Haga clic en .. para desplazarse a la carpeta padre. | |

# 3.6 Gestión de una sesión de servidor proxy de gestión remota

Los servidores proxy de gestión remota permiten realizar una 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).

Para obtener más información sobre el servidor proxy de gestión remota, consulte la Sección 1.4, “Descripción del servidor proxy de gestión remota”, en la página 17.

Para obtener más información sobre la instalación de un servidor proxy de gestión remota, consulte la Sección 2.10, “Instalación de un servidor proxy de gestión remota”, en la página 49.

Para obtener más información sobre la configuración de un servidor proxy de gestión remota, consulte la Sección 2.11, “Configuración de un servidor proxy de gestión remota”, en la página 51.

# 3.7 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 permita la reactivación en LAN.

Activar un dispositivo que tenga varias NIC (tarjetas de interfaz de red) se realiza correctamente sólo si una o varias de las NIC están configuradas para una subred que contenga el dispositivo que está difundiendo el paquete Wake-on-LAN.



## 3.7.1 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.

## 3.7.2 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 desee activar.
4. Haga clic en *Tareas rápidas* > *Activar* para mostrar el 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.

# 3.8 Mejora del rendimiento de la gestión remota

El rendimiento durante una sesión de gestión remota a través de un enlace lento o un enlace rápido varía en función del tráfico de la red. Para mejorar el tiempo de respuesta, intente alguna de estas estrategias:


- Sección 3.8.1, “En la consola de gestión”, en la página 65
- Sección 3.8.2, “En el dispositivo gestionado”, en la página 65


## 3.8.1 En la consola de gestión

En la ventana Conexión de ZENworks Remote Management de la consola, haga clic en *Opciones* y establezca los siguientes valores:

- Para maximizar el rendimiento de la gestión remota cuando se usan conexiones lentas:
  - Seleccione la opción *Usar color de 8 bits.*
  - Establezca el *Nivel de compresión personalizado* en el nivel 6.
- Seleccione la opción *Bloquear eventos de movimiento de ratón.*
- Habilite la opción *Suprimir papel tapiz* en los valores de gestión remota.

## 3.8.2 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.

# Seguridad

# 4

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:



## 4.1 Autenticación

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

Para evitar el acceso sin autorización al dispositivo gestionado, el servicio de gestión remota del dispositivo gestionado utiliza los siguientes métodos de autenticación:



### 4.1.1 Autenticación de gestión remota basada en derechos

En la autenticación basada en derechos, los derechos se asignan al operador remoto para que lance una sesión remota en el dispositivo gestionado. Por defecto, el administrador de ZENworks y el superadministrador tienen derechos para realizar operaciones remotas en todos los dispositivos gestionados, independientemente de si el usuario local o el usuario de ZENworks han entrado o no al dispositivo.

El operador remoto no necesitará ningún derecho exclusivo para realizar una sesión remota en el dispositivo gestionado si ningún usuario ha entrado en el dispositivo gestionado o si alguno ha entrado en el dispositivo gestionado pero no en ZENworks. Sin embargo, el operador remoto necesitará derechos de gestión remota exclusivos para realizar la operación remota en el dispositivo gestionado si algún usuario de ZENworks ha entrado en el dispositivo. Se recomienda encarecidamente utilizar la autenticación basada en derechos, ya que es segura.

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.

Este modo de autenticación no se admite si se lanza la operación de gestión remota en el modo independiente o desde la línea de comandos.

### 4.1.2 Autenticación de gestión remota basada en contraseñas

En la autenticación basada en contraseñas, se pide al operador remoto que introduzca una contraseña para lanzar la sesión remota en el dispositivo gestionado.

Los dos tipos de esquemas de autenticación mediante contraseñas que se usan son:

- **Contraseña de ZENworks:** este esquema está basado 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 de contraseña de VNC tradicional. La longitud máxima de las contraseñas de VNC es de 8 caracteres. El esquema de contraseña es intrínsecamente débil y sólo se proporciona para que funcione 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 contraseñas funcionan en los modos siguientes:

- **Modo de sesión:** las contraseñas definidas en este modo sólo son válidas 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. Cuando se inicia una sesión remota con el dispositivo gestionado, el operador remoto debe introducir la contraseña correcta en el recuadro de diálogo de la contraseña de la sesión que se muestra. Si no lo hace en los dos minutos posteriores a que se muestre el recuadro de diálogo, la sesión se cerrará por motivos de seguridad. Si se utiliza la autenticación basada en contraseñas, se recomienda encarecidamente que se utilice este modo de autenticación, ya que la contraseña sólo es válida durante la sesión en curso y no se guarda en el dispositivo gestionado.
- **Modo persistente:** en este modo, la contraseña la puede definir el administrador mediante la directiva de gestión remota o el usuario del dispositivo gestionado mediante el 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 de gestión remota.

  Si la contraseña se define tanto por el usuario del dispositivo gestionado como en la directiva, la definida por el usuario tendrá prioridad.

  El administrador puede impedir que el usuario del dispositivo gestionado pueda definir la contraseña, o incluso restablecer la contraseña definida por el usuario para garantizar que la contraseña configurada en la directiva se aplique siempre durante la autenticación. Para obtener más información sobre el restablecimiento de la contraseña por parte del 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 33.

## 4.2 Seguridad de la contraseña

Utilice contraseñas seguras. Recuerde estas directrices:

- **Longitud:** la longitud mínima recomendada es de 6 caracteres. Las contraseñas seguras tienen como mínimo 8 caracteres; pero cuanto más largas, mejor. La longitud máxima de las contraseñas de ZENworks es de 255 caracteres, y de 8 caracteres en el caso de las contraseñas de VNC.
- **Complejidad:** las contraseñas seguras contienen una mezcla de letras y números. Deben contener tanto mayúsculas como minúsculas y al menos un carácter numérico. Si se añaden números a las contraseñas, sobre todo en la mitad y no sólo al principio o al final, se aumenta la seguridad de la contraseña. El uso de caracteres especiales como &, *, $ y > aumentan en gran medida la seguridad de la contraseña. No utilice palabras reconocibles, como nombres propios o palabras que aparezcan en el diccionario, ni información personal como números de teléfonos, fechas de nacimiento, aniversarios, direcciones ni códigos postales.

## 4.3 Puertos

Por defecto, el servicio de gestión remota se ejecuta en el puerto 5950 y las escuchas 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.

El servidor proxy de gestión remota escucha por defecto en el puerto 5750.

## 4.4 Audit

ZENworks Configuration Management conserva un registro de todas las sesiones remotas realizadas en el dispositivo gestionado. Este registro se conserva en el dispositivo gestionado y puede consultarlo tanto el usuario como el administrador. El administrador puede ver los registros de todas las sesiones remotas realizadas 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 en el área de notificación del dispositivo gestionado.
2. En el panel izquierdo, diríjase a *Gestión remota* y haga clic en *Seguridad.*
3. Haga clic en *Mostrar información de auditoría* para mostrar la información de auditoría de las operaciones remotas realizadas en el dispositivo.

| Campo | Descripción |
|---|---|
| *Usuario de ZENworks* | El nombre del usuario de ZENworks que ha entrado al dispositivo gestionado al inicio de la sesión remota. |
| *Operador remoto* | Nombre del operador remoto que ha efectuado la operación. |
| *Equipo de la consola* | El nombre de host del dispositivo para el que se ha efectuado la operación. |

| Campo | Descripción |
|---|---|
| *IP de la consola* | Dirección IP del dispositivo para el que se ha efectuado la operación.<br><br>**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. |
| *Funcionamiento* | El tipo de operación efectuada: Control remoto, Ejecución remota, Vista remota, Diagnóstico remoto o Transferencia de archivos. |
| *Inicio* | La hora a la que se inició la operación remota. |
| *Hora de finalización* | La hora a la que se completó la operación remota. |
| *Estado* | El estado de la operación remota: Correcto, En ejecución o Fallo. También se muestra el motivo del fallo. |

## 4.5 Solicitar permiso al usuario del dispositivo gestionado

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

Cuando el operador remoto inicia una sesión remota en el dispositivo gestionado, el servicio de gestión remota comprueba si la opción *Pedir permiso del usuario en el dispositivo gestionado* para esa operación remota está habilitada en la directiva en vigor en el dispositivo. Si la opción está habilitada y no hay ningún usuario en el dispositivo, la sesión remota continúa. Pero, si la opción está habilitada y hay un usuario en el dispositivo gestionado, se muestra un mensaje configurado en la directiva de gestión remota al usuario pidiéndole permiso para lanzar una sesión remota en el dispositivo. La sesión sólo se inicia si el usuario otorga el permiso.

## 4.6 Terminación anormal

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

- La red falla y el visor de gestión remota y el servicio de gestión remota no son capaces de comunicarse.
- El visor de gestión remota se cierra de forma brusca desde el administrador de tareas.
- La red se desactiva 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 que se ha producido una terminación anormal de la sesión.

# 4.7 Detección de intrusos

La función Detección de intruso reduce de forma significativa el riesgo de que el dispositivo gestionado sea atacado por intrusos. Si el operador remoto no consigue entrar en el dispositivo gestionado en el número permitido de intentos (por defecto son cinco), 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. pero se puede cambiar en los valores de seguridad de la directiva de 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 desee desbloquear.
4. Haga clic en *Acción* y, a continuación, 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 en el área de notificación del dispositivo gestionado.
2. En el panel izquierdo, diríjase 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 ayuda al dispositivo gestionado a identificar al operador remoto. Sin embargo, si el operador remoto lanza la sesión en modo independiente, el certificado no se genera y el operador remoto se registra como *Un usuario desconocido* en los registros de auditoría, en la señal visible y en el recuadro de diálogo para pedir permiso al usuario. El servicio de gestión remota recupera la identidad del operador remoto mediante el certificado proporcionado por la consola de gestión durante la fase de acuerdo de nivel de zócalo con seguridad (SSL). El acuerdo SSL se produce en todos los tipos de autenticación, excepto en la autenticación mediante contraseña de VNC.

El servicio de gestión remota del dispositivo muestra los detalles del operador remoto en el recuadro de diálogo de la señal visible si la opción *Proporcionar una señal visual al usuario del dispositivo gestionado* está habilitada en la directiva en vigor 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 utiliza el nivel de zócalo con seguridad (SSL) para proteger las sesiones remotas. Sin embargo, las sesiones remotas lanzadas mediante 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 Acuerdo SSL

Cuando se instala ZENworks Adaptive Agent 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 pide al operador remoto que verifique el certificado del dispositivo remoto. El certificado muestra detalles como el nombre del dispositivo gestionado, la autoridad que lo ha emitido, su validez y la huella digital. Por motivos de seguridad, el operador remoto debe verificar las credenciales del dispositivo gestionado comparando la huella digital del certificado con la que ha comunicado el usuario del dispositivo gestionado mediante algún sistema ajeno al equipo informático. A continuación, el operador remoto puede llevar a cabo una de estas acciones:

- **Aceptar el certificado de forma permanente:** si un usuario que haya entrado a la consola de gestión acepta el certificado de forma permanente, este certificado no se mostrará en la sesiones remotas siguientes que inicie ese usuario en esa consola.
- **Aceptar el certificado de forma temporal:** si un usuario que haya entrado a la consola de gestión acepta el certificado de forma temporal, ese certificado sólo se aceptará para la sesión en curso. La siguiente vez que inicie una conexión con el dispositivo gestionado, se le volverá a pedir al usuario que verifique el certificado.
- **Rechazar el certificado:** si un usuario que haya entrado a la consola de gestión rechaza el certificado, la sesión remota terminará.

## 4.10.2 Regeneración del certificado

El dispositivo gestionado vuelve a generar un certificado autofirmado en las siguientes circunstancias:

- El nombre del dispositivo gestionado cambia.
- 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.

El certificado se vuelve a generar por defecto 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.

- "El visor de gestión remota no se lanza en dispositivos con Windows Vista, Windows 7, Windows Server 2008 o Windows Server 2008 R2" en la página 81
- "Durante una sesión de control remoto, al hacer clic en el icono Ctrl+Alt+Supr del visor de gestión remota, se puede mostrar la ventana de secuencia de atención segura sin incluir ninguno de los controles" en la página 81
- "Puede que no esté visible el escritorio de un dispositivo cuando se controla o se ve de forma remota" en la página 82
- "No es posible transferir de forma remota archivos a carpetas restringidas en un dispositivo con Windows Vista, Windows 7, Windows Server 2008 o Windows Server 2008 R2" en la página 82
- "No es posible lanzar una sesión remota en un dispositivo con SUSE Linux Enterprise Server 11 mediante Mozilla Firefox" en la página 82
- "En enlace Actualizar visor de gestión remota no se muestra si se lanza el Centro de control de ZENworks mediante Internet Explorer 8" en la página 83

### 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 por contraseña en el dispositivo gestionado antes de que se inicie la sesión de control remoto, el servicio de gestión remota intenta anularlo para que el operador remoto pueda ver el escritorio del usuario. El operador remoto también puede anular el protector de pantalla durante la sesión remota haciendo clic en el icono *Anular protector de pantalla* de la barra de herramientas del visor de gestión remota.

Causa posible: El protector de pantalla se activa debido a la inactividad de la sesión remota.

Acción: Haga clic en el icono *Anular protector de pantalla* de la barra de herramientas del visor de gestión remota. Puede que tenga que hacer clic en el icono varias veces hasta que surta efecto.

Causa posible: En dispositivos con Windows Vista, Windows 7, Windows Server 2008 o Windows Server 2008 R2 no es posible anular la función de protector de pantalla.

Acción: Ninguna.

Causa posible: El protector de pantalla puede haberse interrumpido si se han enviado movimientos del ratón al dispositivo gestionado.

Acción: Seleccione la opción *Bloquear eventos de movimiento de ratón* en la ventana de opciones del visor de ZENworks Remote Management para evitar que los movimientos del ratón se envíen al dispositivo gestionado.

Causa posible: La autenticación e identificación gráfica (GINA) del dispositivo gestionado se activa debido a la interrupción del protector de pantalla.

Acción: Vuelva a entrar al 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, de vista remota o de diagnóstico remoto en un dispositivo gestionado que se ejecute con una resolución de color muy baja (con menos de 8 bits por píxel).

Acción: Aumente la resolución de color del dispositivo a 16 bits por píxel o una superior siguiendo este procedimiento:

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 resolución de 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 el visor de gestión remota no se lance si su archivo ejecutable se ha suprimido o se ha renombrado.

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`.

### En dispositivos gestionados con Windows Vista, Windows 7, Windows Server 2008 o Windows Server 2008 R2, la terminación anormal de la sesión puede fallar

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, Windows 7, Windows Server 2008 o Windows Server 2008 R2 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.

### Las escuchas de gestión remota no aceptan las peticiones de sesión remota del dispositivo gestionado si el puerto en el que escuchan no está abierto en el cortafuegos de la consola de gestión

Origen: ZENworks 10 Configuration Management; Gestión remota.

Acción: Abra el puerto de escucha en el cortafuegos de la consola de gestión.

### Solución de problemas relacionados con los mensajes de error que se producen al utilizar el componente de gestión remota

Origen: ZENworks 10 Configuration Management; Gestión remota.

Acción: Para solucionar los problemas relacionados con los mensajes de error que aparecen mientras se usa el componente de gestión remota, envíe los archivos de registro siguientes al servicio de asistencia técnica de Novell (http://support.novell.com):

- `WinVNCApp.log` y `WinVNC.log` para Windows Vista, Windows 7, Windows Server 2008 o Windows Server 2008 R2
- `WinVNC.log` para todos los demás dispositivos gestionados

Para acceder al archivo de registro:

1. Abra el Editor del Registro.
2. Acceda a `HKLM\Software\Novell\ZCM\Remote Management\Agent`.
3. Cree una entrada DWORD denominada DebugMode y establezca el valor 2.
4. Cree una entrada DWORD denominada DebugLevel y establezca el valor hexadecimal `a` (equivalente al valor decimal 10).
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`
- `WinVNCApp.log`

### 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).

### Instalación de una nueva versión del controlador de duplicación

Origen: ZENworks 10 Configuration Management; Gestión remota.

Causa posible: Cuando se instala ZENworks Adaptive Agent 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.

Podrá realizar sesiones de control remoto en el dispositivo, pero el rendimiento se ralentizará.

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 gestionado está sincronizado con la hora UTC con este sistema. Si el problema persiste, póngase en contacto con el servicio técnico de Novell.

Origen: ZENworks 10 Configuration Management; Gestión remota.

Causa posible: El dispositivo gestionado se ha actualizado o se ha registrado y esta información no se ha actualizado en el registro del dispositivo gestionado.

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

1. Actualice el nombre de dominio del nuevo certificado de la CA en el registro con los nuevos detalles:

   **Clave:** HKLM\Software\Novell\ZCM

   **Valor:** CASubject
2. Importe el certificado de CA de la nueva zona al almacén raíz de certificados de confianza.
3. Elimine el certificado de CA de la zona antigua del almacén raíz de certificados de confianza.

Causa posible: El dispositivo gestionado se ha movido a una zona de gestión distinta.

Acción: Gestione el dispositivo desde la nueva zona de gestión.

### 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 lanzadas en dispositivos gestionados de 64 bits mediante la ejecución remota se ejecutan en el entorno WOW (Windows On Windows).

Acción: Lance las aplicaciones mediante el 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, Windows Server 2008 o Windows Server 2008 R2

Origen: ZENworks 10 Configuration Management; Gestión remota.

Explicación: Si se lanza una operación de control remoto en un dispositivo con Windows Vista, Windows Server 2008 o Windows Server 2008 R2 con el control de cuentas de usuario (UAC) inhabilitado, el icono *Ctrl+Alt+Supr* aparece atenuado.

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 sigue activo en dispositivos con Windows Vista, Windows 7, Windows Server 2008 o Windows Server 2008 R2 que tengan el navegador Internet Explorer 7

Origen: ZENworks 10 Configuration Management; Gestión remota.

Explicación: En un dispositivo con Windows Vista, Windows 7, Windows Server 2008 o Windows Server 2008 R2 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 UAC en el dispositivo con Windows Vista, debe actualizar a Windows Vista SP1.

### Es posible que falle la instalación del visor de gestión remota

Origen: ZENworks 10 Configuration Management; Gestión remota.

Explicación: La instalación del visor de gestión remota puede fallar. Este error es inherente a la estructura MSI.

Acción: Realice uno de los siguientes pasos:

- Desinstale el visor de gestión remota mediante Agregar o quitar programas y vuelva a instalarlo
- Use Microsoft Windows Installer Cleanup Utility para eliminar la aplicación y, a continuación, vuelva a instalarla. Esta utilidad se puede descargar del sitio de asistencia técnica de Microsoft (http://support.microsoft.com/kb/290301)

### El visor de gestión remota no se lanza en dispositivos con Windows Vista, Windows 7, Windows Server 2008 o Windows Server 2008 R2

Origen: ZENworks 10 Configuration Management; Gestión remota.

Explicación: En dispositivos con Windows Vista, Windows 7, Windows Server 2008 o Windows Server 2008 R2, el visor de gestión remota falla aunque el guión de seguridad se complete correctamente.

Acción: Añada el servidor que está ejecutando el Centro de control de ZENworks a la lista de sitios de confianza y vuelva a intentarlo.

### Durante una sesión de control remoto, al hacer clic en el icono Ctrl+Alt+Supr del visor de gestión remota, se puede mostrar la ventana de secuencia de atención segura sin incluir ninguno de los controles

Origen: ZENworks 10 Configuration Management; Gestión remota.

Acción: Haga clic en el icono *Ctrl+Alt+Supr* del visor de gestión remota y pulse la tecla Esc para salir de la ventana de secuencia de atención segura (SAS). A continuación, haga clic de nuevo en el icono *Ctrl+Alt+Supr* del visor de gestión remota.

### Puede que no esté visible el escritorio de un dispositivo cuando se controla o se ve de forma remota

Origen: ZENworks 10 Configuration Management; Gestión remota.

Explicación: Si se controla o se ve de forma remota un dispositivo en el que se haya realizado una sesión RDP, puede que se muestre una pantalla en negro en lugar del escritorio del dispositivo.

Acción: Para ver el escritorio del dispositivo:

1. Desbloquee el escritorio manualmente.
2. Vuelva a iniciar una sesión RDP en la sesión de la consola del dispositivo ejecutando el siguiente comando:

   ```
   mstsc /console
   ```

### No es posible transferir de forma remota archivos a carpetas restringidas en un dispositivo con Windows Vista, Windows 7, Windows Server 2008 o Windows Server 2008 R2

Origen: ZENworks 10 Configuration Management; Gestión remota.

Explicación: Si ejecuta una operación de transferencia de archivos para transferirlos remotamente hasta carpetas restringidas de un dispositivo con Windows Vista, Windows 7, Windows Server 2008 o Windows Server 2008 R2 que tenga habilitado el control de cuentas de usuario (UAC), la operación falla.

Acción: Realice las siguientes acciones para desactivar el control de cuentas de usuario (UAC) 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. Deseleccione *Usar el Control de cuentas de usuario (UAC) para ayudar a proteger el equipo.*
3. Haga clic en *Aceptar.*

Acción: Realice las siguientes acciones para desactivar el control de cuentas de usuario (UAC) en el dispositivo con Windows 7:

1. Haga clic en *Inicio* > *Panel de control* > *Cuentas de usuario* > *Cambiar configuración del control de cuentas de usuario*.
2. Desplace la barra del control deslizante hasta el valor más bajo (hacia *No notificar nunca*) con la indicación de que no se realice ninguna notificación.
3. Haga clic en *Aceptar*.
4. Reinicie el dispositivo.

### No es posible lanzar una sesión remota en un dispositivo con SUSE Linux Enterprise Server 11 mediante Mozilla Firefox

Origen: ZENworks 10 Configuration Management; Gestión remota.

Explicación: El módulo auxiliar (plug-in) de gestión remota para Firefox está instalado en el directorio `/usr/lib/firefox`, que es también el directorio de instalación por defecto de Firefox. Si ha instalado Firefox en un directorio distinto en el dispositivo SLES 11, no es posible lanzar una sesión remota mediante Firefox en el dispositivo.

Acción: Copie el archivo `nsZenworksPluginSample.so` del directorio `/usr/lib/firefox/plugins` al directorio de los módulos auxiliares de Firefox.

### En enlace Actualizar visor de gestión remota no se muestra si se lanza el Centro de control de ZENworks mediante Internet Explorer 8

Origen: ZENworks 10 Configuration Management; Gestión remota.

Explicación: Si actualiza a ZENworks Configuration Management SP3 desde ZENworks Configuration Management SP2 y lanza el Centro de control de ZENworks mediante Internet Explorer 8, el enlace *Actualizar visor de gestión remota* no se muestra en el Centro de control de ZENworks.

Acción: Para ver el enlace *Actualizar visor de gestión remota*, lleve a cabo estos pasos:

1. Lance Internet Explorer 8.
2. Haga clic en *Herramientas* > *Opciones de Internet* para mostrar el recuadro de diálogo Opciones de Internet.
3. Haga clic en la pestaña *Seguridad.*
4. Haga clic en la opción *Nivel personalizado.*
5. Asegúrese de que los siguientes ajustes están habilitados:
   - *Ejecutar controles y complementos de ActiveX*
   - *Inicializar y generar scripts de los controles ActiveX no marcados como seguros para scripts*
6. Reinicie el navegador.

# Detalles criptográficos

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.



## A.1 Detalles del 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 Detalles del 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

# Mejores prácticas

B

En las secciones siguientes se explican prácticas recomendables a la hora de usar el componente de gestión remota de Novell® ZENworks® 10 Configuration Management.



## B.1 Cierre de las escuchas de gestión remota

Cuando un operador remoto lanza las escuchas de gestión remota para escuchar las peticiones de sesión remota del usuario del dispositivo gestionado, ZENworks emite un ticket para habilitar al operador remoto para que pueda autenticarse en el dispositivo gestionado. Este ticket caduca a los dos días.

Las escuchas de gestión remota siguen ejecutándose incluso después de que el operador remoto salga del Centro de control de ZENworks o lo cierre. Si el ticket es aún válido, cualquier otro operador remoto podrá utilizar las escuchas para escuchar las peticiones de sesión remota de los usuarios del dispositivo gestionado. Por motivos de seguridad, se deben cerrar las escuchas de gestión remota antes de salir del navegador o de cerrarlo.

Para cerrar las escuchas de gestión remota, haga clic con el botón derecho en el icono *Escucha de ZENworks Remote Management* 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 35.

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, Windows 7, Windows Server 2008 y Windows Server 2008 R2

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.

Si desea conservar el tema Aero durante la sesión remota del dispositivo gestionado, debe inhabilitar el controlador de duplicación en el dispositivo. Para inhabilitar el controlador de duplicación, deseleccione el ajuste *Habilitar controlador de optimización* en el dispositivo. Para obtener más información sobre este ajuste, consulte Configuración de los valores de gestión remota para la zona de gestión.

Sin embargo, si se habilita el tema Aero en el dispositivo gestionado, el rendimiento de la sesión remota en el dispositivo se podría ver afectada.

## 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) 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 3.8, “Mejora del rendimiento de la gestión remota”, en la página 65.

# Actualizaciones de la documentación

C

Esta sección incluye información acerca de los cambios del contenido de la documentación que se han realizado en esta *Referencia de la gestión remota* de Novell® ZENworks® 10 Configuration Management SP3. La información puede ayudarle a estar al día de las actualizaciones de la documentación.

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.

Se han efectuado las siguientes actualizaciones en el documento:

- Sección C.1, “30 de marzo de 2010: SP3 (10.3)”, en la página 91

## C.1 30 de marzo de 2010: SP3 (10.3)

Se han realizado actualizaciones en las siguientes secciones:

| Ubicación | Cambio |
|---|---|
| “Servidor proxy de gestión remota” en la página 12 | Sección actualizada. |
| Sección 1.3, “Descripción de las funciones de gestión remota”, en la página 15 | Sección actualizada. |
| Sección 2.5, “Configuración de la contraseña de gestión remota”, en la página 31 | Sección actualizada. |
| Sección 2.9, “Opciones para lanzar una operación de gestión remota”, en la página 45 | Sección añadida. |
| Sección 2.10, “Instalación de un servidor proxy de gestión remota”, en la página 49 | Se ha actualizado la sección para añadir la asistencia para instalar el servidor proxy de gestión remota en Linux. |
| Sección 2.11, “Configuración de un servidor proxy de gestión remota”, en la página 50 | Sección añadida. |
| Sección 3.7, “Activación de un dispositivo remoto”, en la página 63 | Se ha actualizado la sección para añadir información sobre la activación de un dispositivo con varias tarjetas de interfaz de red. |

| Ubicación | Cambio |
| --- | --- |
| Sección 3.6, “Gestión de una sesión de servidor proxy de gestión remota”, en la página 63 | Sección añadida. |
| Capítulo 5, “Resolución de problemas”, en la página 75 | Se han añadido los siguientes casos:<br>◆ “No es posible lanzar una sesión remota en un dispositivo con SUSE Linux Enterprise Server 11 mediante Mozilla Firefox” en la página 82<br>◆ “En enlace Actualizar visor de gestión remota no se muestra si se lanza el Centro de control de ZENworks mediante Internet Explorer 8” en la página 83 |
| Capítulo 5, “Resolución de problemas”, en la página 75 | Se ha añadido el caso siguiente:<br>No es posible transferir de forma remota archivos a carpetas restringidas en un dispositivo con Windows Vista o Windows 7 |
| Sección B.6, “Uso del tema Aero en dispositivos con Windows Vista, Windows 7, Windows Server 2008 y Windows Server 2008 R2”, en la página 88 | Sección actualizada. |