

# ZENworks 2020 Update 2

## Referencia sobre novedades

Agosto 2021

## **Información legal**

Para obtener información acerca de la información legal, las marcas comerciales, las renunciaciones de responsabilidad, las garantías, la exportación y otras restricciones de uso, los derechos del gobierno estadounidense, la directiva de patentes y el cumplimiento de la norma FIPS, consulte el sitio <https://www.novell.com/company/legal/>.

**© Copyright 2008-2021 Micro Focus o uno de sus afiliados.**

La única garantía para los productos y servicios de Micro Focus y sus afiliados y licenciadores ("Micro Focus") está definida de forma expresa en la declaración de garantía que acompaña a estos productos y servicios. Nada en este documento debe interpretarse como constituyente de una garantía adicional. Micro Focus no será responsable de ningún error técnico o de redacción, ni de ninguna omisión incluida en este documento. La información contenida en este documento está sujeta a cambios sin previo aviso.

---

# Tabla de contenido

<b>Acerca de esta guía</b>	<b>5</b>
<b>1 Novedades de ZENworks 2020 Update 2</b>	<b>7</b>
Plataformas compatibles	7
Instalación y actualización	7
Instalación de Docker y Docker Compose	8
Migración de datos del servidor a una nueva vía de archivo	8
Renombrado de los servicios del servidor ZENworks	8
Introducción de una nueva variable de entorno	8
Versión de TLS	8
Sustitución de servidores primarios	9
Traslado de un servidor primario a un dispositivo	9
ZENworks Configuration Management	9
Gestión de dispositivos Windows 10	9
ZENworks Imaging	11
ZENworks Remote Management	11
Gestión móvil	11
Gestión de lotes	12
Miscelánea	12
Mejoras de seguridad en ZENworks	12
Registro de dispositivos	13
Comunicación del dispositivo	13
Exclusiones de la unidad de directiva de cifrado de datos de Microsoft	14
Antimalware	14
Protección contra malware: página de inicio	14
Derecho de actualización de antimalware	14
Directivas de Endpoint Security para Windows	14
Dashlets de seguridad antimalware	15
Página Antimalware del dispositivo	15
Página Detalles de amenazas de malware	16
Tareas rápidas de antimalware	16
Comandos zac de antimalware	16
Páginas de configuración de zona antimalware	16
Página de configuración de contenido a pedido	17
Estado del servicio antimalware	17
Base de datos de antimalware	17



# Acerca de esta guía

Esta *Referencia sobre novedades de ZENworks* describe las nuevas funciones de ZENworks 2020 Update 2. La guía incluye las siguientes secciones:

- ♦ [Capítulo 1, “Novedades de ZENworks 2020 Update 2”, en la página 7](#)

## Usuarios a los que va dirigida

Esta guía está dirigida a administradores de 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 para **comentar este tema** en la parte de abajo de cada página de la documentación en línea.

## Documentación adicional

ZENworks cuenta con documentación adicional (en formatos PDF y HTML) que puede utilizar para conocer e implementar el producto. Si necesita documentación adicional, visite el [sitio Web de documentación de ZENworks](#).



# 1 Novedades de ZENworks 2020 Update 2

Las siguientes secciones describen las nuevas funciones y las mejoras de ZENworks 2020 Update 2:

- ♦ “Plataformas compatibles” en la página 7
- ♦ “Instalación y actualización” en la página 7
- ♦ “Sustitución de servidores primarios” en la página 9
- ♦ “Traslado de un servidor primario a un dispositivo” en la página 9
- ♦ “ZENworks Configuration Management” en la página 9
- ♦ “Mejoras de seguridad en ZENworks” en la página 12
- ♦ “Antimalware” en la página 14

## Plataformas compatibles

En esta versión se admiten las siguientes plataformas nuevas:

- ♦ CentOS como dispositivo gestionado
- ♦ macOS 11 (Big Sur) como dispositivo gestionado
- ♦ Android 11
- ♦ iOS 14
- ♦ SLES 15 SP2
  - ♦ SLES 15 SP2 (servidor primario)
  - ♦ SLES 15 SP2 (dispositivo gestionado, incluido SLES para SAP)
  - ♦ SLED 15 SP2 (dispositivo gestionado)
- ♦ Nuevas plataformas RHEL y Scientific Linux
  - ♦ Scientific Linux 7.7 y 7.8
  - ♦ RHEL 7.8 y 8.2

## Instalación y actualización

Dado que ZENworks pretende adoptar una arquitectura más sólida y flexible y adaptarse a los estándares de Micro Focus, se han introducido algunas mejoras en el proceso de instalación y actualización en la versión ZENworks 2020 Update 2. Los cambios introducidos en esta versión son los siguientes:

## Instalación de Docker y Docker Compose

Antes de actualizar o instalar ZENworks 2020 Update 2 en un servidor primario Linux, debe instalar Docker y Docker Compose en el servidor. Para obtener más información sobre Docker, consulte <https://docs.docker.com/>.

## Migración de datos del servidor a una nueva vía de archivo

Después de actualizar a ZENworks 2020 Update 2 en un servidor primario Windows, Linux o de dispositivo, los datos del servidor ZENworks, como los archivos MSI, los RPM, los registros y los archivos de configuración que se encontraban anteriormente en la vía de Novell, se moverán a la nueva vía de Micro Focus.

Por ejemplo, en un servidor Linux, los archivos de configuración que estaban antes en `/etc/opt/novell/zenworks`, ahora estarán disponibles en `/etc/opt/microfocus/zenworks`. Del mismo modo, en un servidor Windows, los archivos de configuración que se encontraban anteriormente en: `C:\Archivos de programa (x86)\Novell\ZENworks\conf`, ahora estarán disponibles en `C:\Archivos de programa (x86)\Micro Focus\ZENworks\conf`.

Los archivos y datos relacionados con el agente ZENworks se conservarán en la ubicación antigua de Novell.

## Renombrado de los servicios del servidor ZENworks

Después de actualizar a ZENworks 2020 Update 2 en un servidor primario Windows, Linux o de dispositivo, algunos servicios del servidor ZENworks, como el servicio ZENServer, ZENLoader o ZENJoinProxy, pasarán de Novell a Micro Focus. Por ejemplo, en un servidor Linux, `novell-zenserver.service` pasará a llamarse `microfocus-zenserver.service`.

## Introducción de una nueva variable de entorno

Para los servidores Windows, se ha introducido una nueva variable de entorno `%ZENSERVER_HOME%` que señala también a la ubicación de instalación del servidor para la vía que no se usa por defecto (`C:\Archivos de programa (x86)\Micro Focus\ZENworks`).

## Versión de TLS

Si acaba de instalar ZENworks 2020 Update 2, TLS1.2 estará habilitado por defecto en la zona y, cuando intente registrar los dispositivos con una versión de Microsoft .NET anterior a la 4.7, el registro del dispositivo fallará. Sin embargo, el agente se instalará en el dispositivo.

Si va a actualizar una zona existente a ZENworks 2020 Update 2, TLS1.2 no se habilitará por defecto. Si habilita TLS 1.2 en la zona, es posible que algunas de las características no funcionen como se espera. Debe instalar Microsoft .NET 4.7 en todos los dispositivos de la zona.

Si ha habilitado TLS1.2 en la zona, para registrar el dispositivo, este debe estar instalado con Microsoft .NET 4.7.

## Sustitución de servidores primarios

Para obtener más información sobre cómo sustituir el primer servidor primario por el segundo servidor primario, o sobre cómo sustituir un servidor primario existente por uno nuevo, consulte la sección [Replacing Primary Servers](#) (Sustitución de servidores primarios) en la [ZENworks Disaster Recovery Reference](#) (Referencia sobre recuperación tras fallo de ZENworks).

## Traslado de un servidor primario a un dispositivo

Para obtener más información sobre el procedimiento para mover un servidor primario existente (Windows o Linux) a un servidor de dispositivo, consulte [Moving from a Windows or Linux Primary Server to Appliance](#) (Traslado de un servidor primario Windows o Linux a un dispositivo) en la [ZENworks Primary Server and Satellite Reference](#) (Referencia sobre el servidor primario y el servidor satélite de ZENworks).

## ZENworks Configuration Management

- ♦ [“Gestión de dispositivos Windows 10”](#) en la página 9
- ♦ [“ZENworks Imaging”](#) en la página 11
- ♦ [“ZENworks Remote Management”](#) en la página 11
- ♦ [“Gestión móvil”](#) en la página 11
- ♦ [“Gestión de lotes”](#) en la página 12
- ♦ [“Miscelánea”](#) en la página 12

## Gestión de dispositivos Windows 10

En la versión ZENworks 2020 Update 2, se han añadido nuevas funciones que le permitirán gestionar todo el ciclo de vida de los dispositivos con Windows 10 mediante el agente de MDM integrado en estos dispositivos. Para abordar los casos de uso que no cubren las funciones de los dispositivos con Windows 10, también puede distribuir el agente ZENworks en dispositivos que utilicen los agentes de MDM para Windows 10.

Para obtener más información sobre las funciones indicadas en esta sección, consulte la [Windows MDM Reference](#) (Referencia de MDM de Windows).

Las nuevas funciones son las siguientes:

### Funciones de configuración

Ahora puede configurar el Servicio de notificación de Windows (WNS) para enviar notificaciones push a los dispositivos Windows que se gestionan mediante Windows Modern Management.

### Funciones de inscripción

Se han introducido las siguientes funciones de inscripción.

**Métodos de inscripción:** los dispositivos con Windows 10 se pueden inscribir en ZENworks mediante los siguientes métodos.

- ♦ Inscripción del paquete de provisión (PPKG)
- ♦ Unión de Azure Active Directory (Azure AD)
- ♦ Inscripción de AutoPilot

**Distribución del agente ZENworks:** ahora puede distribuir el agente ZENworks en dispositivos con Windows 10 que ya estén inscritos mediante el modo de inscripción de MDM.

**Configuración de las condiciones de uso:** puede asignar la directiva de condiciones de uso a los dispositivos para añadir el contenido de las condiciones de uso que se mostrará en el agente al inscribir dispositivos con Windows 10 mediante la unión de Azure AD o AutoPilot.

## Posibilidades de gestión

Se han introducido las siguientes funciones de gestión:

**Distribución de lotes de MDM de Windows 10:** ahora puede distribuir los siguientes lotes a dispositivos de MDM de Windows 10:

---

**Nota:** la compatibilidad con estos lotes es experimental y debe utilizarse únicamente con fines de evaluación.

---

- ♦ Uso del paquete de instalación de MDM de Windows 10: el lote de instalación de MSI distribuye un paquete de Microsoft Installer (MSI) en dispositivos de MDM de Windows 10.
- ♦ Mediante el lote de CSP de MDM de Windows 10, se distribuyen los proveedores de servicios de configuración (CSP) para distribuir varias configuraciones disponibles a través de los CSP en dispositivos de MDM de Windows 10.

**Inicio de tareas rápidas:** las siguientes tareas rápidas se admiten en dispositivos de MDM de Windows 10:

- ♦ Suprimir dispositivo:
- ♦ Anular registro de dispositivo
- ♦ Retirar dispositivo
- ♦ Anular la retirada del dispositivo
- ♦ Dispositivo perdido
- ♦ Anular inscripción del dispositivo

## Otras funciones

Otras funciones introducidas para las características de MDM de Windows 10 son las siguientes:

- ♦ Los dispositivos con Windows 10 admiten la reconciliación automática.
- ♦ El proceso de reacuñado de CA ahora emite certificados para dispositivos de MDM de Windows 10.
- ♦ El ajuste de API de MS Graph se ha renombrado como Aplicación de MDM de Azure y debe volver a configurarse para aprovechar las nuevas mejoras introducidas en esta versión.

## Conceptos básicos de Modern Management

La página de inicio de la gestión móvil se ha renovado para incluir la inscripción y la gestión de dispositivos de MDM de Windows 10. Para obtener más información, consulte la [Referencia sobre Modern Management](#).

## ZENworks Imaging

**Restauración de imagen con el nombre del lote en WinPE:** en ZENworks 2020 Update 1 y versiones anteriores, la distribución de WinPE admitía la restauración de la imagen proporcionando el nombre de la imagen con el comando IMG, y el comando no reconocía si el lote se había pasado a través del comando. A partir de ZENworks 2020 Update 2, los comandos de lote IMG se admiten en la distribución de WinPE. Para obtener más información, consulte la guía sobre [servicios de prearranque y generación de imágenes](#).

**Nueva herramienta para leer la información de imagen de ZENworks:** la herramienta zmginfo ayuda a recopilar información sobre una imagen. Es especialmente útil si tiene varias imágenes en el repositorio de contenido o en la vía compartida y necesita recopilar información acerca de cada imagen para ahorrar tiempo. Con la herramienta zmginfo, puede recopilar información básica o completa sobre la imagen. Con zmginfo, el administrador puede crear el xml del lote, que se puede importar como lote y utilizarse para convertir todas las imágenes base de linux en imágenes base de winpe.

Para obtener más información, consulte la guía sobre [servicios de prearranque y generación de imágenes](#).

## ZENworks Remote Management

**Control remoto de un dispositivo que tiene una sesión RDP activa:** ahora podrá lanzar una sesión remota en un dispositivo con una sesión RDP activa, igual que una sesión de gestión remota normal. Para obtener más información, consulte la [Referencia sobre gestión remota](#).

**Grabación de una sesión de gestión remota (asistencia técnica experimental):** permite a los usuarios del dispositivo gestionado registrar la sesión de gestión remota. Para obtener más información, consulte la [Referencia sobre gestión remota](#).

## Gestión móvil

**Habilitación de asignaciones de dispositivos para lotes de Android:** los lotes de Android creados para aplicaciones de Play Store aprobadas que antes estaban restringidas a las asignaciones de usuario, ahora también se pueden asignar a los dispositivos. Para obtener más información, consulte la [Referencia sobre gestión de dispositivos móviles](#).

**Aplicaciones del sistema de provisión:** mediante la función de lotes, puede habilitar o inhabilitar las aplicaciones del sistema en dispositivos Android. Las aplicaciones del sistema son aplicaciones integradas que ya están preinstaladas en el dispositivo. Para obtener más información, consulte la [Referencia sobre gestión de dispositivos móviles](#).

**Conceptos básicos de Modern Management:** la página de inicio de gestión de dispositivos móviles se ha renovado para incluir también la inscripción y la gestión de dispositivos de MDM de Windows 10. Además, en esa página se han incluido algunas funciones adicionales asociadas con la inscripción y la gestión de dispositivos Apple y Android. Para obtener más información, consulte la [Referencia sobre Modern Management](#).

**Modificación de la ubicación del registro del dispositivo Android:** la ubicación de los registros de la aplicación ZENworks en dispositivos Android se ha modificado a `Android/data/com.novell.zapp/files/Documents/zapp.log`. Para compartir estos registros, debe distribuir la aplicación [Archivos](#) en dispositivos Android.

## Gestión de lotes

Se ha introducido una nueva opción **Continuar aunque haya fallo** en el flujo de trabajo Copiar relaciones. Cuando se copian relaciones de un dispositivo a otro conjunto de objetos, si se produce un error, la operación continuará para el resto de objetos. Los detalles de los errores se mostrarán al final de la operación, junto con una opción para exportarlos como referencia para el futuro. Para obtener más información, consulte la [Referencia sobre la distribución de software](#).

## Miscelánea

**Se permite a los clientes utilizar la versión más reciente del paquete puppet-agent:**

Anteriormente, ZENworks proporcionaba el paquete puppet-agent como parte de la compilación, lo que permitía a los usuarios utilizar la directiva Puppet. Sin embargo, con las continuas actualizaciones de puppet-agent tras el lanzamiento de ZENworks, los usuarios no podían utilizar la versión más reciente del paquete puppet-agent. A partir de esta versión, para que la directiva de Puppet entre en vigor en dispositivos gestionados Linux con ZENworks 2020 Update 2 y versiones posteriores, debe asegurarse de que el paquete puppet-agent esté instalado en los dispositivos. Para obtener más información, consulte la [Referencia sobre directivas de configuración](#).

## Mejoras de seguridad en ZENworks

Las mejoras de seguridad introducidas en esta versión le permiten registrarse y comunicarse de forma segura con los dispositivos incluso en un entorno DMZ.

- ♦ Si acaba de instalar ZENworks 2020 Update 2, la configuración de seguridad estará habilitada por defecto en todos los servidores primarios.
- ♦ Si está actualizando los servidores primarios, los ajustes de seguridad estarán inhabilitados por defecto.
- ♦ Si ha añadido un nuevo servidor primario a la zona, después de actualizar a ZENworks 2020 Update 2, los ajustes de seguridad estarán habilitados por defecto.

Debe ejecutar el siguiente comando zman para habilitar los ajustes:

- ♦ `zman ssassc` (Security-Set-Agent-Server-Secure-Communication) se ha introducido para habilitar o inhabilitar la autenticación para la comunicación entre el agente ZENworks y los servidores ZENworks.

Para obtener más información sobre las mejoras de seguridad introducidas en esta versión, consulte la [Referencia sobre dispositivos de seguridad de ZENworks](#).

## **Registro de dispositivos**

### **Aprobación previa del registro de dispositivos**

Los dispositivos preaprobados son aquellos que ha aprobado el administrador para que formen parte de la zona. Esto es especialmente útil cuando tiene que aprobar previamente dispositivos al inscribir en masa un conjunto conocido de dispositivos. También se puede utilizar para permitir la reconciliación de dispositivos conocidos, si es necesario.

### **Uso de la clave de autorización**

El agente ZENworks puede utilizar una clave de autorización para autorizarse a sí mismo a registrarse en la zona y para cualquier comunicación con el servidor durante la instalación.

### **Protección del dispositivo gestionado y del registro de dispositivos iOA**

Para registrar agentes iOA más recientes o dispositivos gestionados en la zona, debe especificar una clave de autorización durante el registro del dispositivo o asegurarse de que el dispositivo forma parte de la lista de dispositivos preaprobados.

## **Comunicación del dispositivo**

### **Uso de OSP para la comunicación de dispositivos, incluida la entrada al ZCC**

Para la mayoría de las funciones, ZENworks ha cambiado al protocolo O-Auth para establecer la identidad del usuario. Por lo tanto, se ha introducido un nuevo servicio denominado OSP que se utiliza para entrar en el Centro de control de ZENworks, para la comunicación entre servicios y para la comunicación entre dispositivos y servidores.

### **Protección del contenido y la recopilación entre dispositivos, servidores primarios y servidores satélite**

Con la introducción de esta nueva función de seguridad, la recopilación de extremo a extremo y la transferencia de contenido entre los dispositivos gestionados, los servidores primarios y los servidores satélite se realizan a través de SSL. Esto se puede lograr configurando el ajuste dentro del Centro de control de ZENworks o utilizando los comandos zman recién introducidos.

## Protección de la comunicación del servicio Web entre el dispositivo y el servidor primario o satélite

Para asegurar aún más la comunicación del servicio Web entre el agente ZENworks y los servidores primario y satélite de ZENworks, en esta versión se han introducido mejoras de seguridad en las llamadas al servicio Web.

## Exclusiones de la unidad de directiva de cifrado de datos de Microsoft

Las unidades de datos extraíbles ahora se pueden excluir del cifrado por tipo de unidad en la directiva de cifrado de datos de Microsoft cuando la directiva se aplica en los dispositivos gestionados.

## Antimalware

ZENworks Antimalware es un nuevo componente de ZENworks Endpoint Security Management situado en el grupo de seguridad del Centro de control de ZENworks. Antimalware es una completa solución que protege los dispositivos gestionados contra las amenazas de malware más recientes. Cuando se distribuye a los dispositivos de la zona, el agente antimalware recibe continuamente actualizaciones de los archivos de firmas de malware del Servicio en la nube de antimalware para detectar infecciones de malware mediante exploraciones al acceder y a petición. Los archivos infectados se ponen en cuarentena hasta que se desinfectan.

Para obtener más información sobre los temas de esta sección, consulte lo siguiente:

- ♦ [Referencia sobre antimalware de ZENworks Endpoint Security](#)

## Protección contra malware: página de inicio

La página de inicio de la seguridad incluye una página adicional con pestañas titulada “Protección contra malware”. Puede utilizar esta página como punto de acceso único para configurar, distribuir y personalizar todas las funciones que ofrece ZENworks Antimalware.

## Derecho de actualización de antimalware

El derecho de actualización de antimalware es necesario para distribuir directivas de antimalware a los dispositivos. El derecho se habilita automáticamente para el período de evaluación al activar Endpoint Security Management en el modo de evaluación.

## Directivas de Endpoint Security para Windows

Se utilizan cuatro directivas nuevas para gestionar la distribución, la personalización y la continuidad del sistema antimalware:

**Directiva de aplicación antimalware:** esta es la directiva básica que instala el agente antimalware en los dispositivos gestionados. Debe distribuirse para utilizar cualquiera de las demás directivas de antimalware. Incluye configuraciones para todo tipo de exploraciones de malware, incluidas

exploraciones al acceder, completas, rápidas, de dispositivos externos y contextuales a petición. También hay ajustes para el comportamiento de la cuarentena y la definición del contenido que se debe excluir de las exploraciones.

Si se conservan los ajustes por defecto de los derechos de usuario final y las notificaciones cuando se distribuye la directiva, los usuarios finales tendrán acceso a la consola de estado del agente en sus puestos finales, lo que les permitirá iniciar sus propias exploraciones, ver el estado de exploración y actualización del agente, y recibir notificaciones sobre la actividad del agente controlada por la directiva.

**Directiva de exclusiones de exploración antimalware:** el sistema antimalware tiene exclusiones de exploración integradas y personalizadas que puede añadir a cualquiera de las directivas de antimalware. La directiva de exclusiones de exploración se emplea en la asignación de dispositivos cuando se asignan también otras directivas de antimalware a los mismos dispositivos, lo que simplifica la propagación de las exclusiones de exploración por la zona. Las exclusiones se pueden habilitar o inhabilitar para tipos de exploración específicos

**Directiva de exploración antimalware personalizada:** se utiliza para un enfoque más específico. Permite explorar las unidades locales en los dispositivos gestionados cuando se sospecha de una amenaza específica o para orientar las exploraciones a ubicaciones específicas en esos dispositivos. Incluye su propia programación, en lugar de utilizar la programación de la zona configurada para la directiva de aplicación de antimalware

**Directiva de exploración antimalware de red:** esta directiva también se utiliza para un enfoque más específico, en concreto, para explorar carpetas y archivos en unidades de red. También tiene su propia programación e incluye un ajuste adicional para la autenticación en ubicaciones de red.

## Dashlets de seguridad antimalware

Se proporcionan cuatro dashlets nuevos que se utilizan por defecto en la consola de seguridad para supervisar las amenazas de malware, las exploraciones en busca de malware y las actualizaciones de firmas de malware.

**Estado de malware del dispositivo:** este dashlet muestra el estado de malware de cada dispositivo de la zona durante un período de detección seleccionado.

**Última exploración de parches del dispositivo:** este dashlet muestra el estado de los dispositivos de la zona frente a las amenazas de malware. Por defecto, muestra información sobre cualquier tipo de exploración que se haya realizado en los dispositivos durante un período de tiempo especificado.

**Principales amenazas de malware:** este dashlet muestra la lista de las principales amenazas de malware de la zona. Por defecto, se muestran según el número de dispositivos infectados.

**Versión de firmas de malware del dispositivo:** este dashlet muestra la lista de versiones de firmas de malware y las versiones del agente antimalware instaladas en los dispositivos de la zona.

## Página Antimalware del dispositivo

Esta página es una pestaña nueva a la que se accede cuando se selecciona un dispositivo. Proporciona una instantánea del estado de las amenazas de malware, la programación de exploración y la información de los archivos en cuarentena del dispositivo seleccionado. También puede realizar acciones específicas en los archivos, realizar exploraciones iniciales y actualizar las versiones del agente antimalware y de las firmas de malware en el dispositivo.

## Página Detalles de amenazas de malware

Para acceder a esta página, haga clic en el enlace de una amenaza de malware en la sección Amenazas de malware de la página Antimalware de un dispositivo. Proporciona información detallada sobre la amenaza seleccionada, así como detalles de los dispositivos que se han infectado.

## Tareas rápidas de antimalware

Cuando se seleccionan uno o varios dispositivos que tienen el agente antimalware instalado en el grupo Dispositivos del Centro de control de ZENworks, hay cinco tareas rápidas nuevas disponibles para ejecutar en los dispositivos seleccionados. Son estas:

- ♦ Iniciar una exploración de malware
- ♦ Actualizar firmas de malware
- ♦ Actualizar agente antimalware
- ♦ Restaurar archivo de la cuarentena de malware
- ♦ Suprimir archivo de la cuarentena de malware

## Comandos zac de antimalware

El sistema antimalware incluye varios comandos zac nuevos específicos para este componente. Sirven para iniciar exploraciones de malware en los dispositivos; comprobar el estado de malware del agente antimalware; instalar, actualizar o eliminar el agente y suprimir archivos de la cuarentena, entre otras acciones.

## Páginas de configuración de zona antimalware

Ahora se incluyen tres páginas nuevas de configuración de zonas en el grupo Seguridad de la página principal de configuración de ZENworks. Cada una de estas páginas incluye ajustes por defecto que puede personalizar. Son estas:

**Programaciones del agente antimalware:** permite configurar las programaciones de exploraciones de malware y las actualizaciones de firmas de malware. Esta programación se puede anular en cada carpeta de dispositivos y en el nivel de los dispositivos.

**Notificaciones del agente antimalware:** permite configurar las alertas y notificaciones que muestra el agente antimalware en los dispositivos gestionados. Puede anular estos ajustes en la carpeta de dispositivos y en el nivel de los dispositivos.

**Configuración antimalware:** define el servidor primario de ZENworks que se debe utilizar como servidor antimalware, que debe configurarse manualmente para distribuir el componente de antimalware. También configura la programación de mantenimiento del agente antimalware.

## **Página de configuración de contenido a pedido**

Esta nueva página de configuración de la zona se incluye ahora en los grupos Lote, Directiva y Contenido de la página principal de configuración de ZENworks. Gestiona la velocidad de descarga de contenido y el tamaño de caché de contenido para la distribución de contenido en la zona, que actualmente incluye los archivos de firma de antimalware y las actualizaciones del agente antimalware.

## **Estado del servicio antimalware**

Ahora se puede acceder al estado del servicio antimalware en la página Diagnóstico del Centro de control de ZENworks.

## **Base de datos de antimalware**

La base de datos de antimalware es nueva en ZENworks 2020 Update 2. Su propósito es proporcionar datos para las funciones de supervisión de antimalware mediante la página Antimalware y los dashlets de seguridad de antimalware. Cuando se configura, esta base de datos se sincroniza con la base de datos de ZENworks y, por lo tanto, debe ser del mismo tipo. Por ejemplo: PostgreSQL, Microsoft SQL Server u Oracle.

La base de datos de antimalware se configura en la página de inicio de Protección contra malware en la sección Seguridad del Centro de control de ZENworks. Si la base de datos de antimalware se configura con una base de datos externa que aún no existe, se puede crear una desde un comando de la interfaz de línea de comandos mediante el archivo `setup.exe`.

