Archivo README (LÉAME) de ZENworks 2017 Update 4

Enero de 2019

La información de este archivo README (LÉAME) corresponde a la versión ZENworks 2017 Update 4.

Novedades de ZENworks 2017 Update 4

Para obtener información sobre las nuevas funciones incluidas en esta versión, consulte la Referencia sobre novedades de ZENworks.

Planificación para distribuir ZENworks 2017 Update 4

Use las directrices siguientes para planificar la distribución de ZENworks 2017 Update 4 en la zona de gestión:

- Si utiliza cifrado de disco y desea actualizar al agente de Full Disk Encryption desde una versión anterior a ZENworks 2017 Update 1, DEBE eliminar la directiva de cifrado de discos de los dispositivos gestionados antes de actualizarlos a ZENworks 2017 Update 4.

  Si se dispone a actualizar el agente de Full Disk Encryption desde ZENworks 2017 Update 1 o 2017 Update 2 a la versión ZENworks 2017 Update 4, deje activa la directiva de cifrado de disco: no se requiere ningún cambio antes de la actualización del sistema.

  Para obtener más información sobre cómo actualizar Full Disk Encryption en ZENworks 2017 4 desde una versión anterior a ZENworks 2017 Update 1, consulte la ZENworks 2017 Update 1 - Full Disk Encryption Update Reference (Referencia de actualización de Full Disk Encryption de ZENworks 2017 Update 1).

- Primero debe actualizar los servidores primarios, a continuación los servidores satélite y, por último, los dispositivos gestionados a ZENworks 2017 Update 4. No actualice los dispositivos gestionados ni los servidores satélite (ni añada nuevos agentes de la versión 2017 Update 4 en la zona) hasta que se hayan actualizado todos los servidores primarios de la zona a ZENworks 2017 Update 4.

  Nota: los agentes podrían recibir datos incoherentes de la zona hasta que se hayan actualizado todos los servidores primarios. Por lo tanto, esta parte del proceso debe realizarse en el menor tiempo posible, preferiblemente de inmediato después de que se actualice el primer servidor primario.

- Puede distribuir directamente la versión 2017 Update 4 a los siguientes dispositivos:

Tipo de dispositivo	Sistema operativo	Versión mínima de ZENworks
Servidores primarios	Windows y Linux	ZENworks 2017 y versiones posteriores
Servidores satélites	Windows, Linux y Mac	ZENworks 11.x y versiones posteriores
Dispositivos gestionados	Windows	ZENworks 11.x y versiones posteriores
	Linux	ZENworks 11.x y versiones posteriores
	Mac	ZENworks 11.2 y versiones posteriores

- El sistema se rearranca una vez después de actualizar a ZENworks 2017 Update 4. Sin embargo, será necesario reiniciar dos veces en los siguientes escenarios:
  - Si actualiza desde la versión 11.x a ZENworks 2017 o una versión posterior (2017 Update 1, Update 2, Update 3 o Update 4) con Endpoint Security habilitado, se necesita un segundo rearranque para cargar el controlador ZESNETAccess.
  - Si un dispositivo gestionado utiliza Windows 10 con la autodefensa del cliente habilitada y se dispone a actualizar desde la versión 11.4.x a ZENworks 2017 o una versión posterior (2017 Update 1, Update 2, Update 3 o Update 4), debe inhabilitar la autodefensa del cliente en el Centro de control de ZENworks, rearrancar el dispositivo gestionado y, a continuación, ejecutar la actualización, lo que requiere un segundo rearranque del dispositivo.
  - Si tiene una directiva de cifrado de disco aplicada en un dispositivo gestionado y desea actualizar al agente de Full Disk Encryption a ZENworks 2017 Update 4 desde una versión anterior a ZENwork 2017 Update 1, primero debe eliminar la directiva y descifrar el dispositivo, lo que requiere un rearranque del dispositivo. A continuación, va a actualizar el dispositivo a la versión 2017 Update 4, lo que requiere un segundo rearranque.

  Importante: los dispositivos gestionados donde se ejecutan versiones anteriores a la 11.x deben actualizarse primero a la versión 11.x. El sistema se rearranca después de actualizar a la versión 11.x y, a continuación, se rearranca de nuevo cuando se distribuye la actualización del sistema ZENworks 2017 Update 4.

- Antes de instalar la actualización del sistema, asegúrese de que dispone de espacio libre suficiente en el disco en las ubicaciones siguientes:

Ubicación	Descripción	Espacio de disco
Windows: `%zenworks_home%\install\downloads` **Linux:** `opt/novell/zenworks/install/downloads`	Para mantener los paquetes del agente.	5,7 GB
Windows: `%zenworks_home%\work\content-repo` **Linux:** `/var/opt/novell/zenworks/content-repo`	Para importar el archivo zip en el sistema de contenido.	5,7 GB
Caché del agente	Para descargar el contenido de la actualización del sistema aplicable necesario para actualizar el servidor ZENworks.	1,5 GB
La ubicación donde se copia el archivo de actualización del sistema. Esto solo se aplica al servidor ZENworks que se usa para importar el archivo zip de la actualización del sistema.	Para guardar el archivo zip de actualización del sistema descargado.	5,7 GB

Descarga y distribución de ZENworks 2017 Update 4

Para obtener instrucciones sobre cómo descargar y distribuir ZENworks 4, consulte la *ZENworks 2017 Update System Updates Reference* (Referencia sobre actualizaciones del sistema de ZENworks 2017 Update 1).

Si la zona de gestión está formada por servidores primarios con una versión anterior a ZENworks 2017, puede distribuir ZENworks 2017 Update 4 a esos servidores primarios solo después de que todos ellos se hayan actualizado a ZENworks 2017. Para obtener instrucciones, consulte la *Guía de actualización de ZENworks*.

Para las tareas administrativas, consulte el sitio de documentación de ZENworks 2017 Update 4.

Importante: no actualice el visor de gestión remota hasta que se hayan actualizado todos los servidores satélites proxy de unión de la zona. Para realizar la gestión remota mediante un proxy de unión, debe asegurarse de que se usa la misma versión en el visor y en el proxy de unión.

Asegúrese de leer "Planificación para distribuir ZENworks 2017 Update 4" en la página 1 antes de descargar y distribuir la actualización de ZENworks 2017 Update 4.

Importante: Al distribuir la actualización de ZENworks, en la fase de preparación, el servicio de actualización de ZENworks (ZeUS) de los servidores primarios se sustituirá por el nuevo paquete incluido en la actualización.

No distribuya ZENworks 2017 Update 4 hasta que se hayan actualizado todos los servidores primarios de la zona a ZENworks 2017

Esta actualización requiere realizar cambios de esquema a la base de datos. Durante la instalación inicial del parche, los servicios solo se ejecutarán en el servidor maestro o en el servidor primario dedicado. Esto se hace para garantizar que otros servidores primarios no intenten acceder a las tablas que se van a cambiar en la base de datos.

Después de actualizar el servidor maestro o el servidor primario dedicado, los servicios se reanudan en los servidores restantes y, de forma simultánea, se aplica la actualización.

Nota: no es necesario detener ni iniciar manualmente los servicios en los servidores durante la actualización. Los servicios se detienen y se inician automáticamente.

Al posponer una actualización del sistema y salir del dispositivo gestionado, la actualización del sistema se aplica en el dispositivo.

Para ver la lista de las versiones compatibles de los dispositivos gestionados y los servidores satélite en una zona de gestión con ZENworks 2017 Update 4, consulte Versiones compatibles de los dispositivos gestionados y los servidores satélite.

Problemas resueltos en ZENworks 2017 Update 4

Algunos de los problemas detectados en versiones anteriores se han solucionado en esta. Para obtener una lista de los problemas resueltos, consulte el documento de información técnica TID 7023612 en la base de datos de conocimiento de asistencia.

Problemas que siguen existiendo en ZENworks 2017 Update 4

Algunos de los problemas descubiertos en versiones anteriores a ZENworks 2017 Update 4 aún no se han resuelto. Consulte los documentos Readme (Léame) siguientes para obtener más información:

- Archivo Readme (Léame) de ZENworks 2017
- Archivo README (LÉAME) de ZENworks 2017 Update 1
- Archivo README (LÉAME) de ZENworks 2017 Update 2
- Archivo README (LÉAME) de ZENworks 2017 Update 3

Problemas conocidos

Esta sección contiene información acerca de los problemas que se pueden producir al trabajar con ZENworks 2017 Update 4:

El porcentaje de brillo establecido como parte de la directiva de control de dispositivos móviles no se puede aplicar en dispositivos Android

A un dispositivo gestionado de trabajo Android se le asigna una directiva de control de dispositivos móviles con un valor específico de porcentaje de brillo, definido en el campo **Definir porcentaje de brillo,** pero el valor de brillo no se aplica en el dispositivo y aparece un mensaje de error que indica que la aplicación no es compatible en los mensajes de estado de la directiva.

Solución: ninguna.

El arranque directo es incompatible con los dispositivos Android P (9.0)

Tal como ha confirmado Google, la función de arranque directo no funciona en los dispositivos con Android P.

Solución: ninguna.

La configuración de protección del dispositivo no funciona en los dispositivos en los que la aplicación del agente de ZENworks se ha actualizado desde una versión anterior a la 17.4.0

Cuando la aplicación del agente ZENworks de un dispositivo se actualiza a la versión 17.4.0, la configuración de protección del dispositivo habilitada como parte de la directiva de control de dispositivos móviles asignada no funciona en el dispositivo.

Solución: anule la inscripción del dispositivo mediante la tarea rápida **Anular inscripción** en ZCC y vuelva a inscribirlo. Vuelva a asignar la misma directiva de control de dispositivos móviles. La configuración de protección del dispositivo se habilitará correctamente en el dispositivo.

La configuración de protección del dispositivo no se puede aplicar en los dispositivos con Android Lollipop y Marshmallow inscritos en el modo de perfil de trabajo

Cuando se habilita la configuración de protección del dispositivo como parte de la directiva de control de dispositivos móviles, la directiva no se puede aplicar en los dispositivos con Android Lollipop y Marshmallow inscritos en el modo de perfil de trabajo. El estado de la directiva se muestra como erróneo en ZCC y en los registros del dispositivo aparece el mensaje de error “You can not set trust agent configuration for a managed profile” (No puede establecer la configuración de agente de confianza para un perfil gestionado).

Solución: ninguna.

La tarea rápida Desbloquear dispositivo no se puede aplicar en los dispositivos con Android Lollipop y Marshmallow inscritos en el modo de perfil de trabajo

La tarea rápida Desbloquear dispositivo no se puede aplicar en los dispositivos con Android Lollipop y Marshmallow inscritos en el modo de perfil de trabajo El estado de la tarea rápida se muestra como erróneo en ZCC y en los registros del dispositivo aparece el mensaje de error “You cannot reset password for managed profile” (No puede restablecer la contraseña para un perfil gestionado).

Solución: ninguna.

Después de actualizar ZENworks, el RPM novell-zenworks-xplat-uninstall muestra una versión incorrecta en ZDC

Después de actualizar la zona de gestión de ZENworks, el RPM novell-zenworks-xplat-uninstall muestra una versión incorrecta de ZDC.

Solución: ninguna.

Espere a que se lleve a cabo la acción de actualización en el servidor primario.

Caracteres no deseados en el nombre de carpeta de dispositivos Intel AMT

En la pestaña **ZCC** > **Dispositivos** > **Descubiertos** aparecen caracteres no deseados en el nombre de carpeta **Dispositivos Intel AMT**.

Solución: ninguna.

La regla de control de acceso no fiable no bloquea el tráfico de red en los dispositivos con la directiva de cortafuegos de Endpoint Security aplicada

Cuando una lista de control de acceso (ACL) se configura con una o más reglas de control de acceso no fiable en la directiva de cortafuegos, el acceso de red basado en los parámetros de la regla no se bloquea.

Solución: utilice la configuración de puertos nativa para bloquear el acceso de red.

La entrada a la sesión en modo pasivo de ZENworks no funciona después de actualizar a Windows v1709, v1803 o v1809

Después de actualizar el dispositivo a Windows 10 v1709 (Fall Creators Update), v1803 o Windows 10 v1809 (actualización de abril de 2018), el modo pasivo de entrada a ZENworks deja de funcionar.

Solución: consulte el TID 7022478 en la base de datos de conocimientos de Micro Focus.

Las tareas rápidas y las actualizaciones del sistema no se ejecutan en los agentes de ZENworks

Al asignar una tarea rápida o una actualización del sistema a un agente de ZENworks, la tarea asignada o la actualización no se ejecutan en el agente y se registra el error **TaskNotifier, "Got 503 from Server** (Mensaje 503 recibido del servidor) en el registro de ZeUS.

Para confirmar el error “TaskNotifier, "Got 503 from Server”, lleve a cabo el siguiente procedimiento:

1. En el agente, en Technician Application (haga clic con el botón derecho en el **icono de ZENworks** y seleccione **Technician Application**), el valor Registro debe configurarse para incluir **errores, advertencias, información y depuración**.
2. Después de cambiar el nivel del registro en el agente, asigne las tareas rápidas o actualizaciones del sistema.
3. En el archivo `zeus-messages.log` se registra el mensaje de error **TaskNotifier, "Got 503 from Server** (Mensaje 503 recibido del servidor) (ubicación: `%ZENWORKS_HOME%\ZeUS\logs\`).

El error **TaskNotifier, "Got 503 from Server** indica que el servidor ha rechazado la conexión porque la capacidad por defecto (10000) está casi agotada.

Este error se produce cuando el número de agentes conectados a un servidor es superior al valor de *maxConnections* en el archivo `server.xml`. El valor por defecto de *maxConnections* es de 10000.

Solución:

Añada el número del parámetro *maxConnections* al archivo `server.xml`.

Para añadir el número del parámetro maxConnections al archivo server.xml:

1. En la siguiente línea del archivo server.xml, añada el parámetro maxConnections = "20000", tal como se indica a continuación:

   <!-- Define a non-SSL HTTP/1.1 Connector on port 80 --> <Connector acceptCount="1000" connectionTimeout="60000" maxConnections="20000" disableUploadTimeout="true" enableLookups="false" maxHttpHeaderSize="8192" maxSpareThreads="75" maxThreads="600" minSpareThreads="25" port="80" protocol="org.apache.coyote.http11.Http11NioProtocol" redirectPort="443" />

   Nota: Por defecto, el valor del parámetro maxConnections es 10000 y no aparece en el archivo server.xml. Si el número 10000 es insuficiente, añada el parámetro y aumente el valor en función del número de agentes de la zona. En este ejemplo, el valor de maxConnections es de 20000.

   ---

2. Reinicie los servicios de ZENworks.

El servicio novell-proxydhcp podría no funcionar en los servidores satélites de generación de imágenes RHEL 7.5 y 7.6

El servicio *novell-proxydhcp* podría no funcionar en RHEL 7.5 y 7.6, ya que el puerto 67 que necesita *este* servicio lo utiliza el servicio *dnsmasq*.

Solución: ejecute el comando `systemctl disable libvirtd.service` y reinicie el dispositivo:

Documentación adicional

Este documento incluye información específica de la versión ZENworks 2017 Update 4. Para toda la documentación restante de ZENworks 2017, consulte el *sitio Web de documentación de ZENworks 2017*.

Información legal

Para obtener información acerca de la información legal, las marcas comerciales, las renuncias 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 2008-2019 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.