

Dispositivo Dell DL1000

Guía de implementación

Notas, precauciones y avisos

 **NOTA:** Una NOTA indica información importante que le ayuda a hacer un mejor uso de su producto.

 **PRECAUCIÓN:** Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

 **AVISO:** Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

© 2016 Dell Inc. Todos los derechos reservados. Este producto está protegido por leyes internacionales y de los Estados Unidos sobre los derechos de autor y la protección intelectual. Dell y el logotipo de Dell son marcas comerciales de Dell Inc. en los Estados Unidos y en otras jurisdicciones. El resto de marcas y nombres que se mencionan en este documento pueden ser marcas comerciales de las compañías respectivas.

Tabla de contenido

1 Introducción al DL1000.....	5
Tecnologías centrales de Dell DL1000.....	5
Recuperación en directo.....	5
Recuperación universal.....	5
Desduplicación global real	6
Cifrado.....	6
Funciones de protección de datos de Dell DL1000.....	6
Dell DL1000 Core.....	6
Dell DL1000 Smart Agent.....	7
Proceso de instantáneas.....	7
Replicación: sitio de recuperación tras desastres o proveedor de servicio.....	7
Recuperación.....	8
Recuperación como servicio (RaaS)	8
Virtualización y nube.....	8
Arquitectura de implementación de DL1000.....	8
Otra información útil.....	10
2 Instalación del DL1000.....	11
Introducción.....	11
Configuraciones disponibles.....	11
Información general sobre la instalación.....	11
Requisitos previos de instalación.....	12
Requisitos de red.....	12
Infraestructura de red recomendada.....	12
Configuración del hardware.....	12
Instalación del appliance DL1000 en un bastidor.....	13
Uso del sistema sin un bastidor.....	13
Conexión de cables del appliance.....	13
Conexión del brazo para tendido de cables (opcional).....	14
Cómo encender el dispositivo DL1000.....	14
Configuración del software inicial.....	14
Asistente de configuración del dispositivo de AppAssure.....	15
Asistente de configuración del dispositivo DL.....	17
Recuperación automática rápida del dispositivo (RASR).....	22
Creación de la memoria USB de RASR.....	22
Ejecución de RASR.....	23
Utilidad de recuperación y actualización.....	24
3 Configuración de su DL1000.....	25
Descripción general.....	25
Restablecimiento del sistema operativo a la configuración predeterminada.....	25
Configuración de exploradores para acceder de manera remota a la DL1000Core Console.....	25

Configuración de los valores del explorador en Internet Explorer y en Chrome.....	26
Configuración de los valores del explorador en Firefox.....	26
Acceso a la Core Console DL1000.....	26
Actualización de los sitios de confianza en Internet Explorer.....	27
Cifrado de datos de instantáneas del Agent.....	27
Configuración de un servidor de correo electrónico y de una plantilla de notificaciones de correo electrónico	27
Ajuste del número de secuencias.....	28
4 Preparación para la protección de los servidores.....	30
Descripción general.....	30
Instalación de Agents en clientes.....	30
Implementación del software del Agent al proteger un Agent.....	30
Instalación del software del Agent de Rapid Recovery en máquinas con Windows.....	31
Implementación del software del Agent de Rapid Recovery a una o más máquinas.....	33
Acerca de cómo instalar el software del Agent en máquinas con Linux.....	35
Ubicación de los archivos del Agent de Linux.....	37
Dependencias del Agent.....	38
Instalación del software del Agent de Rapid Recovery en Debian o Ubuntu.....	38
Instalación del software del Agent de Rapid Recovery en SUSE Linux Enterprise Server.....	39
Instalación del Agent en Red Hat Enterprise Linux y CentOS.....	40
Instalación del software del Agent en máquinas con Linux fuera de línea.....	40
Instalación del software del Agent en máquinas con Windows con Server Core.....	41
Configuración del Agent de Rapid Recovery en una máquina con Linux.....	42
Cómo proteger una máquina.....	43
Comprobación de la conectividad de red.....	46
Comprobación de la configuración del firewall.....	46
Comprobación de la resolución de DNS.....	46
Formación de equipos de adaptadores de red.....	47
5 Obtención de ayuda.....	49
Búsqueda de documentación y actualizaciones de software.....	49
Documentación.....	49
Actualizaciones de software.....	49
Cómo ponerse en contacto con Dell.....	49
Comentarios sobre la documentación.....	49

Introducción al DL1000

Dell DL1000 combina funciones de copia de seguridad y replicación en un producto de protección de datos unificado. Proporciona una recuperación fiable de los datos de aplicación a partir de sus copias de seguridad para proteger las máquinas virtuales y las máquinas físicas. Su Appliance es capaz de manejar terabytes de datos con deduplicación global, compresión, cifrado y replicación integrados en la infraestructura de nube privada o pública específica. Los datos y las aplicaciones de servidor se pueden recuperar en minutos con fines de retención de datos y cumplimiento.

DL1000 admite entornos de varios hipervisores en VMware vSphere, Oracle VirtualBox y Microsoft Hyper-V y nubes públicas y privadas.

Temas:

- [Tecnologías centrales de Dell DL1000](#)
- [Funciones de protección de datos de Dell DL1000](#)
- [Arquitectura de implementación de DL1000](#)
- [Otra información útil](#)

Tecnologías centrales de Dell DL1000

El servidor combina las siguientes tecnologías:

- [Recuperación en directo](#)
- [Recuperación universal](#)
- [Deduplicación global real](#)
- [Cifrado](#)

Recuperación en directo

Recuperación en directo es una tecnología de recuperación instantánea para máquinas virtuales (VM) o servidores. Facilita un acceso casi continuo a volúmenes de datos en servidores virtuales o físicos.

La tecnología de copia de seguridad y replicación de DL1000 registra instantáneas simultáneas de varias VM o servidores y proporciona protección del sistema y los datos de manera casi instantánea. Para reanudar el uso del servidor, puede montar el punto de recuperación sin esperar a una restauración completa en el almacenamiento de producción.

Recuperación universal

Recuperación universal ofrece flexibilidad ilimitada para la restauración de máquinas. Puede restaurar sus copias de seguridad desde sistemas físicos a VM, de VM a VM, de VM a sistemas físicos o de sistemas físicos a sistemas físicos y realizar restauraciones desde cero a hardware diferente.

La tecnología Recuperación universal también acelera los movimientos a plataformas diferentes entre máquinas virtuales. Por ejemplo, permite mover de VMware a Hyper-V o de Hyper-V a VMware. Crea recuperación en los niveles de aplicación, de elemento y de objeto (archivos individuales, carpetas, correo electrónico, elementos del calendario, bases de datos y aplicaciones).

Desduplicación global real

La Desduplicación global real elimina los datos redundantes o duplicados mediante la realización de copias de seguridad incrementales del nivel de bloque de las máquinas.

El diseño de disco convencional de un servidor consta de un sistema operativo, de aplicaciones y de datos. En la mayoría de los entornos, los administradores suelen usar una versión habitual de sistema operativo de escritorio y de servidor en varios sistemas para una implementación y una administración efectivas. Cuando la copia de seguridad se realiza a nivel de bloque en varias máquinas, se ofrece una vista más granular de lo que contiene la copia de seguridad y lo que no, con independencia del origen. Entre estos datos se incluyen el sistema operativo, las aplicaciones y los datos de aplicaciones del entorno.



Ilustración 1. Diagrama de una desduplicación global real

Cifrado

DL1000 proporciona cifrado para proteger copias de seguridad y datos almacenados contra el uso y el acceso no autorizados, lo cual garantiza la privacidad de los datos. Se puede acceder a los datos y descifrarlos mediante la clave de cifrado. El cifrado se realiza en línea en los datos de la instantánea, a velocidad de línea sin afectar al rendimiento.

Funciones de protección de datos de Dell DL1000

Dell DL1000 Core

El Core es el componente central de la arquitectura de implementación de DL1000. El Core almacena y administra las copias de seguridad de la máquina y proporciona servicios de copia de seguridad, recuperación, retención, replicación, archivado y administración. El Core es un equipo de red direccionable autocontenido que ejecuta una variante de 64 bits de sistemas operativos Microsoft Windows Server 2012 R2 Foundation y Standard. El appliance realiza una compresión en línea basada en el objetivo, cifrado y desduplicación de los datos recibidos del Agent. A continuación, el Core almacena las copias de seguridad de las instantáneas en el repositorio, que reside en el appliance. Los Cores se emparejan para la replicación.

El repositorio reside en el almacenamiento interno dentro del Core. Para administrar el Core, acceda a la dirección URL siguiente desde un explorador web habilitado para JavaScript: **<https://NOMBRECORE:8006/apprecovery/admin>**.

Dell DL1000 Smart Agent

El Smart Agent está instalado en la máquina protegida por el Core. El Smart Agent rastrea los bloques cambiados en el volumen de disco y, a continuación, toma una imagen de los bloques cambiados a un intervalo de protección predefinido. El enfoque constante e incremental de instantáneas de nivel de bloque evita que se repita la copia de los mismos datos desde la máquina protegida al Core.

Una vez que el Agent está configurado, utiliza tecnología inteligente para hacer un seguimiento de los bloques cambiados en los volúmenes de discos protegidos. Cuando la instantánea está lista, se transfiere rápidamente al Core mediante conexiones de socket inteligentes multiprocesos.

Proceso de instantáneas

El proceso de protección de DL1000 comienza cuando una imagen base se transfiere desde una máquina protegida al Core. En esta fase, se transporta una copia completa de la máquina por la red en condiciones de funcionamiento normales, seguida de instantáneas incrementales que se realizarán de manera permanente. El DL1000 Agent para Windows usa el Servicio de copia de instantáneas de volumen (VSS) de Microsoft para detener y desactivar el vaciado de los datos de aplicación en un disco para capturar una copia de seguridad coherente con el sistema de archivos y con la aplicación. Cuando se crea una instantánea, el escritor de VSS en el servidor de destino evita que se escriba contenido en el disco. Durante el proceso de detención de escritura de contenido en disco, todas las operaciones de E/S del disco se ponen en cola y se reanudan solo después de completarse la instantánea, mientras finalizan todas las operaciones en curso y se cierran los archivos abiertos. El proceso de creación de una copia de instantánea no afecta significativamente al rendimiento del sistema de producción.

DL1000 utiliza Microsoft VSS, ya que tiene soporte incorporado para todas las tecnologías internas de Windows, como NTFS, Registro o Active Directory, para vaciar datos al disco antes de realizar la instantánea. Además, otras aplicaciones empresariales, como Microsoft Exchange y SQL, usan complementos de VSS Writer para que se les notifique cuándo se está preparando una instantánea y cuándo tienen que vaciar las páginas de bases de datos utilizadas al disco para poner la base de datos en un estado de transacción coherente. Los datos capturados se transfieren y almacenan rápidamente en el Core.

Replicación: sitio de recuperación tras desastres o proveedor de servicio

La replicación es el proceso de copia de puntos de recuperación en un Core de Rapid Recovery y su transmisión a otro Core de Rapid Recovery en una ubicación separada para la recuperación tras desastres. El proceso requiere una relación emparejada origen-destino entre dos o más núcleos.

El Core de origen copia los puntos de recuperación de máquinas protegidas seleccionadas y, a continuación, transmite de modo asíncrono y continuo los datos de la instantánea incremental a los Cores de destino en un sitio remoto de recuperación tras desastre. Puede configurar la replicación de salida a un centro de datos propiedad de la empresa o sitio de recuperación tras desastre remoto (es decir, un núcleo de destino administrado automáticamente). O bien, puede configurar la replicación de salida a un tercero proveedor de servicios administrados (MSP) o de servicios en la nube que aloja servicios de recuperación tras desastres y de copia de seguridad fuera del sitio. Al replicar a un Core de destino de terceros, puede utilizar flujos de trabajo integrados que le permiten solicitar conexiones y recibir notificaciones de comentarios automáticas.

La replicación se administra por máquina protegida. Cualquier máquina (o todas las máquinas) protegida o replicada en un Core de origen puede configurarse para replicar a un núcleo de destino.

La replicación se optimiza automáticamente con un algoritmo de lectura-coincidencia-escritura (RMW) que está estrechamente acoplado con la deduplicación. Con la replicación RMW, el servicio de replicación de origen y de destino hace coincidir las claves antes de transferir los datos y, a continuación, replica sólo los datos comprimidos, cifrados y deduplicados de la WAN, haciendo que se reduzcan 10 veces los requisitos de ancho de banda.

La replicación comienza con la inicialización, la transferencia inicial de imágenes base deduplicadas e instantáneas incrementales de los sistemas protegidos, que pueden sumar cientos o miles de gigabytes de datos. La replicación inicial se puede inicializar en el Core de destino mediante soportes externos. Esto resulta normalmente útil para grandes conjuntos de datos o sitios con enlaces lentos. Los datos del archivo de inicialización se comprimen, cifran y deduplican. Si el tamaño total del archivo es mayor que el espacio disponible en el soporte extraíble, el archivo podrá abarcar varios dispositivos, en función del espacio disponible en el soporte. Durante el proceso de inicialización, los puntos de recuperación incrementales se replican en el sitio de destino. Después de que el Core de destino consuma el archivo de inicialización, los puntos de recuperación incrementales recién replicados se sincronizan de forma automática.

Recuperación

La recuperación se puede realizar en el sitio local o en el sitio remoto replicado. Cuando la implementación esté en estado estable con protección local y replicación opcional, DL1000 Core le permitirá realizar la recuperación mediante Verified Recovery, Recuperación universal, o Recuperación en directo.

Recuperación como servicio (RaaS)

Los Managed Service Providers (Proveedores de servicios administrados, MSP) pueden aprovechar todas las ventajas del DL1000 como plataforma para proporcionar recuperación como servicio (RaaS). RaaS facilita la recuperación en la nube completa al replicar los servidores físicos y virtuales de los clientes. La nube del proveedor de servicio se utiliza como máquinas virtuales para permitir realizar operaciones de prueba de recuperación o de recuperación real. Los clientes que deseen realizar recuperación en la nube pueden configurar la replicación en sus máquinas protegidas en los Cores locales de un proveedor de servicio de Rapid Recovery. En caso de desastre, los MSP pueden conseguir que las máquinas virtuales adquieran velocidad nominal de rotación instantáneamente para el cliente.

El DL1000 no es multiinquilino. Los MSP pueden utilizar el DL1000 en varios sitios y crear un entorno multiinquilino por su parte.

Virtualización y nube

DL1000 Core es compatible con la tecnología en la nube, que le permite aprovechar la capacidad informática de la nube para recuperación y archivado.

DL1000 puede exportar cualquier máquina protegida o replicada a versiones con licencias de VMware o Hyper-V. Con las exportaciones continuas, la máquina virtual se actualiza de modo incremental después de cada instantánea. Las actualizaciones incrementales son rápidas y proporcionan clones en espera preparados para activarse con solo presionar un botón. Las exportaciones de máquinas virtuales admitidas son:

- VMware Workstation o Server en una carpeta
- Exportación directa a un host de Vsphere o de VMware ESXi
- Exportar a Oracle VirtualBox
- Microsoft Hyper-V Server en Windows Server 2008 (x64)
- Microsoft Hyper-V Server en Windows Server 2008 R2
- Microsoft Hyper-V Server en Windows Server 2012 R2

Ahora puede archivar los datos del repositorio en la nube mediante plataformas como Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage u otros servicios en la nube basados en OpenStack.

Arquitectura de implementación de DL1000

La arquitectura de implementación de DL1000 consta de componentes locales y remotos. Los componentes remotos pueden ser opcionales para los entornos que no necesiten usar un sitio de recuperación tras desastres o un proveedor de servicio administrado para recuperación externa. Una implementación local básica se compone de un servidor de copia de seguridad denominado Core y una o más máquinas protegidas, conocidas como Agents. El componente externo se habilita mediante la replicación que ofrece capacidades de

recuperación completas en el sitio de recuperación tras desastres. El DL1000 Core utiliza imágenes base e instantáneas incrementales para compilar los puntos de recuperación de los Agents protegidos.

También, DL1000 está habilitado para aplicaciones porque detecta la presencia de Microsoft Exchange y SQL y de sus respectivas bases de datos y archivos de registro. Las copias de seguridad se realizan mediante instantáneas de nivel de bloque que reconocen las aplicaciones. DL1000 realiza el truncamiento de registro del servidor protegido de Microsoft Exchange.

El siguiente diagrama muestra una implementación simple de DL1000. Los Agents de DL1000 se instalan en máquinas, como un servidor de archivos, un servidor de correo electrónico, un servidor de base de datos, o se conectan las máquinas virtuales y se protegen con un único DL1000 Core, que consiste en el repositorio central. El software License Portal de Dell administra los usuarios, grupos y suscripciones de licencia para los Agents y Cores de su entorno. License Portal permite que los usuarios inicien la sesión, activen las cuentas, descarguen software e implementen Agents y Cores conforme a la licencia para su entorno.

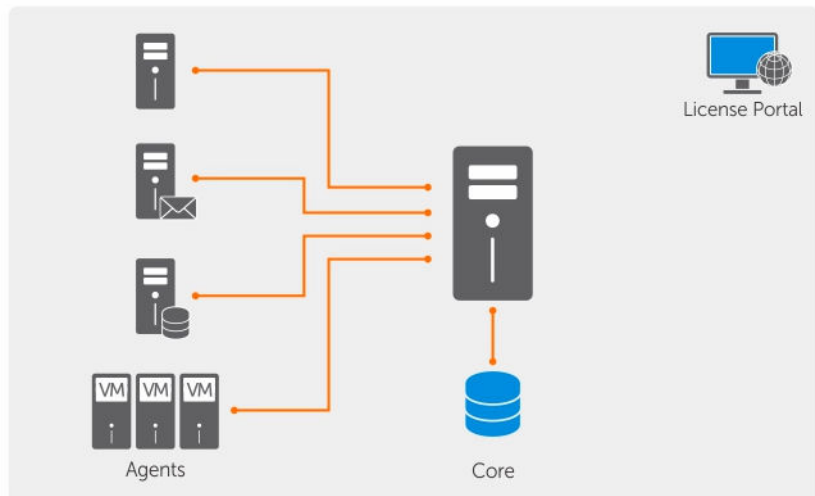


Ilustración 2. Arquitectura de implementación de Dell DL1000

También puede implementar varios Cores de DL1000, como se muestra en el siguiente diagrama. Una consola central administra varios Cores.

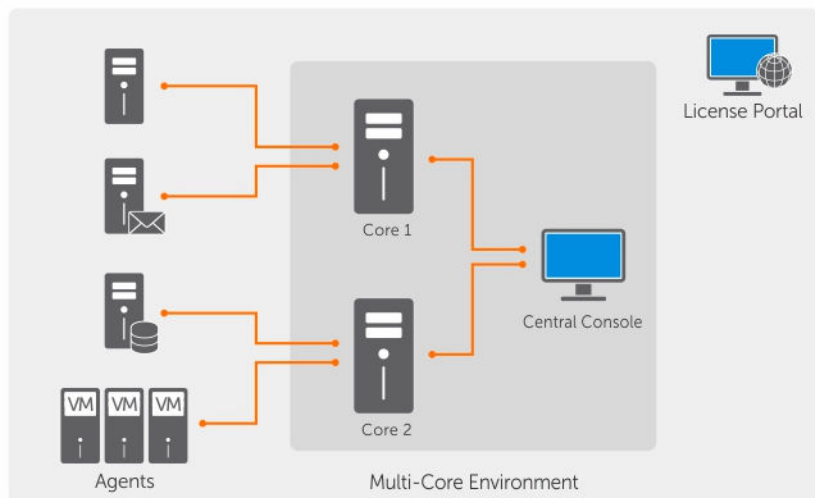


Ilustración 3. Arquitectura de implementación de varios Cores de DL1000

Otra información útil

- NOTA:** Para todos los documentos Dell OpenManage, vaya a Dell.com/openmanagemanuals.
- NOTA:** Compruebe siempre si hay actualizaciones en Dell.com/support/home y, si las hay, léalas primero ya que a menudo sustituyen a la información contenida en otros documentos.
- NOTA:** Para cualquier documento relacionado con Dell OpenManage Server Administrator, consulte Dell.com/openmanage/manuals.

La documentación de su producto incluye:

Guía de introducción	Proporciona una descripción general de la configuración de su sistema y las especificaciones técnicas. Este documento también se envía con su sistema.
System Placemat (Hoja de instrucciones del sistema)	Proporciona información sobre cómo configurar el hardware e instalar el software en su appliance.
Owner's Manual (Guía de introducción)	Proporciona información sobre las características del sistema y describe cómo solucionar problemas del sistema e instalar o sustituir los componentes del sistema.
Guía de implementación	Proporciona información sobre la implementación del hardware y la implementación inicial del appliance AppAssure.
Guía del usuario	Proporciona información sobre la configuración y administración del sistema.
Notas de publicación	Proporciona información sobre el producto e información adicional sobre el Dell DL1000 Appliance.
Interoperability Guide (Guía de interoperabilidad)	Proporciona información sobre el software y el hardware compatibles con el appliance, así como las reglas, recomendaciones y consideraciones de uso.
OpenManageServer Administrator User's Guide (Guía del usuario OpenManage Server Administrator)	Proporciona información sobre el uso de Dell OpenManage Server Administrator para administrar su sistema.

Instalación del DL1000

Introducción

El DL Backup to Disk Appliance permite:

- Copias de seguridad más rápidas, así como situaciones de recuperación más rápidas que con las metodologías de copia de seguridad y los dispositivos de cinta convencionales.
- Capacidad de deduplicación opcional
- Protección de datos continua para el centro de datos y los servidores de oficina remotos
- Implementación rápida y fácil que reduce el tiempo necesario para iniciar la protección de datos críticos

Configuraciones disponibles

El appliance DL viene con las siguientes configuraciones:

Tabla 1. Configuraciones disponibles

Capacidad	Configuración de hardware
1 TB sin VM	Unidad de 2 TB con una partición de sistema operativo/software de 200 GB y espacio de repositorio utilizable de 1 TB
2 TB sin VM	Unidad de 3 TB con una partición de sistema operativo/software de 200 GB y espacio de repositorio utilizable de 2 TB
3 TB sin VM	Unidad de 4 TB con una partición de sistema operativo/software de 200 GB y espacio de repositorio utilizable de 3 TB
3 TB con 2 VM	Unidad de 4 TB con una partición de sistema operativo/software de 200 GB, una partición de 300 GB para almacenamiento en VM y espacio de repositorio utilizable de 3 TB

Cada configuración incluye también el siguiente hardware y software:

- Sistema Dell DL1000
- Controladoras RAID Dell PowerEdge (PERC)
- Software Dell AppAssure

Información general sobre la instalación

La instalación de DL1000 requiere la instalación de los Servicios del Core de Rapid Recovery y del Agent de Rapid Recovery en los sistemas que tienen que estar protegidos. Si se configuran más núcleos, debe instalar los Servicios de la consola de administración central de Rapid Recovery.

Para instalar el DL1000 siga estos pasos:

- 1 Obtenga la clave de licencia permanente. En la Core Console, puede administrar sus licencias de DL1000 directamente, cambie la clave de licencia y póngase en contacto con el servidor de licencias. También puede acceder al Portal de licencias de Rapid Recovery desde la página Licensing (Licencias) en la Core Console.

① **NOTA: El appliance se configura y se envía con una licencia de software temporal de 30 días.**

- 2 Revise los requisitos previos de instalación.
- 3 Configuración del hardware.
- 4 Configuración del software inicial (Asistente de configuración del dispositivo DL)
- 5 Instalación de la Core Management Console.

Requisitos previos de instalación

Requisitos de red

Su appliance requiere el siguiente entorno de red:

- Red activa con cables y conexiones Ethernet disponibles.
- Una dirección IP estática y una dirección IP de servidor DNS, si no las proporciona el Protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol, o DHCP por sus siglas en inglés)
- Nombre de usuario y contraseña con privilegios de administración.

Infraestructura de red recomendada

Hace diez años, la infraestructura de red troncal contaba con todas las características estándar velocidades de 100 megabits por segundo. Las exigencias para el tráfico de red y la entrada y salida ha aumentado constantemente y sustancialmente. Como resultado, las normas de redes troncales han aumentado por encima para satisfacer la demanda. Red moderna vecinos admiten velocidades (como Gigabit Ethernet (GbE), el cual transfiere en tramas Ethernet 1 gigabit por segundo, o 10 GbE, lo que representa una velocidad diez veces más rápido.

Para ejecutar Rapid Recovery, Dell requiere una infraestructura de red de un mínimo de 1 GbE para un rendimiento eficiente. Dell recomienda redes 10 GbE para entornos robustos. También se recomiendan las redes de 10 GbE al proteger los servidores que incorporan grandes volúmenes (5 TB o más).

Si hay varias tarjetas de interfaz de red (NIC) disponibles en la máquina del Core que son compatibles con la agrupación de NIC (NIC físicas agrupar varios en una única NIC lógica), y si los conmutadores en la red que permiten y, a continuación, mediante la agrupación de NIC en el Core puede proporcionar mayor rendimiento. En tales casos, la agrupación de repuesto que admiten tarjetas de red formación de equipos NIC en cualquier base de datos protegida máquinas, cuando sea posible, también puede aumentar el rendimiento general.

Si el core utiliza iSCSI o Network Attached Storage (NAS), Dell recomienda utilizar tarjetas NIC independiente para su almacenamiento y el tráfico de la red, respectivamente.

Utilice cables de red con los correspondientes para obtener la clasificación esperado ancho de banda. Dell recomienda que se prueben el rendimiento de la red regularmente y ajuste el hardware según corresponda.

Estas sugerencias se basan en necesidades de red típica de una infraestructura de red para admitir todas las operaciones comerciales, además de las capacidades de copia de seguridad, replicación y recuperación que Rapid Recovery proporciona.

Configuración del hardware

El appliance se envía con un solo sistema DL1000. Antes de configurar el hardware del appliance, consulte la *Getting Started Guide (Guía de instrucción)* para el sistema enviado con el appliance. Desempaquete y configure el hardware del appliance DL1000.

① **NOTA: El software está preinstalado en el dispositivo. Los soportes físicos incluidos con el sistema deben utilizarse solo si es necesario recuperar el sistema.**

Para configurar el hardware de DL1000:

- 1 Monte el sistema DL1000 en bastidor y conéctelo.
- 2 Encienda el sistema DL1000.

Instalación del appliance DL1000 en un bastidor

Si su sistema incluye un kit de rieles, busque las *Rack Installation Instructions* (Instrucciones de instalación en bastidor) proporcionadas con el kit del bastidor. Siga las instrucciones para instalar los rieles y el DL1000 en el bastidor.

Uso del sistema sin un bastidor

Puede utilizar el sistema sin el bastidor del servidor. Cuando se utiliza el sistema sin un bastidor asegúrese de seguir las pautas siguientes:

- El sistema debe colocarse en una superficie estable y sólida que admite el sistema completo.

NOTA: El sistema no debe colocarse en posición vertical.

- No coloque el sistema sobre el suelo.
- No coloque nada encima del sistema. El panel superior puede desviarse por el peso y provocar daños en el sistema.
- Asegúrese de que haya suficiente espacio alrededor del sistema para una ventilación adecuada.
- Asegúrese de que el sistema se haya instalado según las condiciones de temperatura recomendadas en la sección Especificación técnica: medioambiental de la *Dell DL1000 Appliance Owner's Manual* (Manual del propietario del Dell DL1300 Appliance) en [Dell.com/support/home](https://www.dell.com/support/home).

PRECAUCIÓN: Si no sigue estas pautas, pueden producirse daños en el sistema o lesiones físicas.

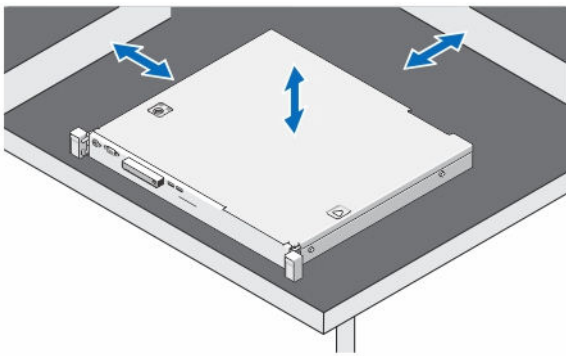


Ilustración 4. Uso del sistema sin un bastidor

Conexión de cables del appliance

Busque la *Dell DL1000 Appliance Getting Started Guide* (Guía de introducción del Dell DL1300 Appliance) enviada con el appliance y siga las instrucciones para conectar el teclado, el mouse, el monitor, la alimentación y los cables de red al sistema DL1000.

Conexión del brazo para tendido de cables (opcional)

Si el appliance incluye un brazo para tendido de cables (CMA), busque la documentación *CMA Installation Instructions* (Instrucciones de instalación del CMA) enviada con el kit del CMA y sígalas para instalarlo.

Cómo encender el dispositivo DL1000

Después del cableado del appliance, encienda el sistema.

NOTA: Se recomienda conectar el dispositivo a un Sistema de alimentación ininterrumpida (SAI) para obtener una fiabilidad y una disponibilidad óptimas. Para obtener más información, consulte la *Guía de introducción a Dell DL1000* en Dell.com/support/manuals.

Configuración del software inicial

Al activar el dispositivo por primera vez y cambiar la contraseña de la máquina, el **AppAssure Appliance Configuration Wizard (Asistente de configuración del dispositivo de AppAssure)** se inicia automáticamente.

- 1 Después de activar el sistema, seleccione el idioma del sistema operativo desde las opciones de idioma de Windows.
El Contrato de licencia de usuario final (CLUF) se muestra en la página **Settings (Configuración)**.
- 2 Para aceptar el CLUF, haga clic en el botón **I accept (Acepto)**.
Se muestra una página para cambiar la contraseña de administrador.
- 3 Haga clic en **OK (Aceptar)** en el mensaje que le solicita cambiar la contraseña.
- 4 Introduzca y confirme la nueva contraseña.
Un mensaje le solicita que confirme que la contraseña se ha cambiado.
- 5 Haga clic en **Aceptar**.
Después de introducir la contraseña se muestra la pantalla **Press Ctrl+Alt+Delete to Sign in (Presione Ctrl+Alt+Supr para iniciar sesión)**.
- 6 Inicie sesión mediante la contraseña de administrador cambiada.
Aparece la pantalla **Select the language for AppAssure Appliance (Seleccione el idioma para el dispositivo de AppAssure)**.
- 7 Seleccione el idioma para el appliance de la lista de idiomas admitidos.
Aparece la pantalla **EULA (CLUF)**.
- 8 Para aceptar el CLUF, haga clic en el botón **Accept EULA (Aceptar CLUF)**.

NOTA: Puede continuar ejecutando el AppAssure Appliance Configuration Wizard (Asistente de configuración del dispositivo DL de AppAssure) solo si acepta el CLUF. De lo contrario, el dispositivo cerrará sesión de inmediato.

Aparece la pantalla de bienvenida del **AppAssure Appliance Configuration wizard (Asistente de configuración del dispositivo DL de AppAssure)**.

NOTA: El asistente de AppAssure Appliance Configuration wizard (Asistente de configuración del appliance AppAssure) puede tardar hasta 30 segundos en aparecer en la consola del sistema.

Asistente de configuración del dispositivo de AppAssure

⚠ PRECAUCIÓN: Asegúrese de completar todos los pasos de AppAssure Appliance Configuration Wizard (Asistente de configuración del appliance AppAssure) antes de realizar cualquier otra tarea o cambiar su configuración en el appliance. No haga ningún cambio a través del Panel de control, utilice la Microsoft Windows Update (Actualización de Microsoft Windows), actualice el software AppAssure o instale las licencias, hasta que finalice el asistente. El servicio de actualización de Windows se deshabilita temporalmente durante el proceso de configuración. Salir del AppAssure Appliance Configuration Wizard (Asistente de configuración del appliance AppAssure) antes de que finalice puede provocar errores en el funcionamiento del sistema.

El **AppAssure Appliance Configuration wizard (Asistente de configuración del dispositivo de AppAssure)** lo guía a través de los siguientes pasos para configurar el software en el dispositivo:

- Configuración de la interfaz de red
- Configuración de los valores de dominio y nombre de host
- Configuración de los valores SNMP
- Aprovisionamiento de almacenamiento

Una vez finalizada la instalación mediante el asistente, la Core Console se inicia automáticamente.

Configuración de la interfaz de red

Para configurar las interfaces de red disponibles:

- 1 En la pantalla **AppAssure Appliance Configuration Wizard Welcome (Bienvenido al Asistente de configuración del appliance AppAssure)**, haga clic en **Next (Siguiente)**.

La página **Network interfaces (Interfaces de red)** muestra las interfaces de red conectadas disponibles.

- 2 Seleccione las interfaces de red que desea configurar.

ⓘ NOTA: El AppAssure Appliance Configuration wizard (Asistente de configuración del AppAssure appliance) configura interfaces de red como puertos individuales (no en equipo). Para mejorar el rendimiento de ingesta, puede crear un canal de ingesta más grande por medio de la formación de equipos NIC. Sin embargo, esto debe hacerse después de la configuración inicial del appliance.

- 3 Si se necesita, conecte interfaces de red adicionales y haga clic en **Refresh (Actualizar)**.

Se muestran las interfaces de red conectadas adicionales.

- 4 Haga clic en **Next (Siguiente)**.

Se muestra la página **Configure selected network interface (Configurar interfaz de red seleccionada)**.

- 5 Seleccione el protocolo de Internet adecuado para la interfaz seleccionada.

Puede elegir **IPv4** o **IPv6**.

Se muestran los detalles de red dependiendo del protocolo de Internet que ha seleccionado.

- 6 Para asignar los detalles del protocolo de Internet, realice una de las siguientes acciones:

- Para asignar los detalles del protocolo de Internet seleccionado automáticamente, seleccione **Obtain an IPV4 address automatically (Obtener una dirección IPV4 automáticamente)**.
- Para asignar la conexión de red manualmente, seleccione **Use the following IPV4 address (Utilizar la siguiente dirección IPV4)** e introduzca los siguientes detalles:
 - **IPv4 Address (Dirección IPV4)** o **IPv6 Address (Dirección IPv6)**
 - **Subnet mask (Máscaras de subred)** para IPv4 y **Subnet prefix length (Longitud del prefijo de subred)** para IPv6
 - **Puerta de enlace predeterminada**

- 7 Para asignar los detalles del servidor DNS, realice una de las siguientes acciones:

- Para asignar la dirección del servidor DNS automáticamente, seleccione **Obtain DNS server address automatically (Obtener una dirección del servidor DNS automáticamente)**.

- Para asignar el servidor DNS manualmente, seleccione **Use the following DNS server address (Utilizar la siguiente dirección del servidor DNS)** e introduzca los siguientes detalles:
 - **Servidor DNS preferido**
 - **Servidor DNS alternativo**
- 8 Haga clic en **Next (Siguiente)**.
Se muestra la página **Configure hostname and domain setting (Configurar los valores de dominio y nombre de host)**.

Para obtener más información sobre la formación de equipos de NIC, consulte [Formación de equipos de adaptadores de red](#).

Configuración de los valores de dominio y nombre de host

Debe asignar un nombre de host para el appliance. Se recomienda que cambie el nombre de host antes de empezar con las copias de seguridad. De manera predeterminada, el nombre de host es el nombre del sistema asignado por el sistema operativo.

NOTA: Si desea cambiar el nombre de host, se recomienda que lo cambie en este momento. Cambiar el nombre de host después de completar el AppAssure Appliance Configuration Wizard (Asistente de configuración del appliance AppAssure) requiere llevar a cabo varios pasos.

Para configurar los valores de dominio y nombre de host:

- 1 En la página **Configure host name and domain setting (Configurar el nombre de host y los valores del dominio)**, en el cuadro de texto **New host name (Nuevo nombre de host)** introduzca un nombre de host adecuado.
- 2 Si no desea conectar el appliance se una al dominio, seleccione **No** en **Do you want this appliance to join a domain? (¿Desea unir este appliance a un dominio?)**

NOTA: Si su DL1000 se ha instalado con Microsoft Windows Server 2012 Foundation Edition, la opción para unirse a un dominio estará deshabilitada.

De manera predeterminada, se selecciona **Yes (Sí)**.

- 3 Si desea conectar el appliance a un dominio, introduzca los siguientes detalles:

- **Nombre de dominio**
- **Nombre de usuario del dominio**

NOTA: El usuario del dominio debe tener derechos administrativos locales.

- **Contraseña de usuario del dominio**

- 4 Haga clic en **Next (Siguiente)**.

NOTA: Se necesita reiniciar la máquina al cambiar el nombre de host o el dominio. Después de reiniciar, el AppAssure Appliance Configuration Wizard (Asistente de configuración del appliance AppAssure) se iniciará automáticamente. Si el appliance está unido a un dominio, después del reinicio, deberá iniciar sesión como usuario del dominio con privilegios administrativos en el appliance.

Se muestra la página **Configure SNMP Settings (Configurar valores SNMP)**.

Configuración de los valores SNMP

El Simple Network Management Protocol (Protocolo simple de administración de redes - SNMP) es un protocolo de administración de redes utilizado frecuentemente que permite las funciones de administración compatibles con SNMP tales como la búsqueda de dispositivos, supervisión y generación de eventos. SNMP proporciona la administración de red del protocolo TCP/IP.

Para configurar alertas SNMP para el servidor:

- 1 En la página **Configure SNMP Settings (Configurar valores de SNMP)**, seleccione **Configure SNMP on this appliance (Configurar SNMP en este appliance)**.

NOTA: Anule la selección de **Configure SNMP on this appliance (Configurar SNMP en este servidor)** si no desea configurar las alertas y los detalles SNMP en el servidor y salte al paso 6.

- En **Communities (Comunidades)**, introduzca uno o más nombres de comunidades SNMP.
Utilice comas para separar varios nombres de comunidades.
- En **Accept SNMP packets from these hosts (Aceptar paquetes SNMP de estos hosts)**, introduzca los nombres de hosts con los que el servidor puede comunicarse.
Separe los nombres de host con comas o déjelo en blanco para permitir la comunicación con todos los hosts.
- Para configurar las alertas SNMP, introduzca el **Community Name (Nombre de comunidad)** y los **Trap destinations (Destinos de capturas)** para las alertas SNMP y haga clic en **Add (Agregar)**.
Repita este paso para agregar más direcciones SNMP.
- Para quitar una dirección SNMP configurada, en **Configured SNMP addresses (Direcciones SNMP configuradas)**, seleccione la dirección SNMP adecuada y haga clic en **Remove (Quitar)**.
- Haga clic en **Next (Siguiente)**.
Se muestra la página **Thank You (Gracias)**.
- Para completar la configuración, haga clic en **Next (Siguiente)**.
- Haga clic en **Exit (Salir)** en la página **Configuration Complete (Configuración finalizada)**.
Se abre la Core console en el explorador web predeterminado.

Aprovisionamiento de almacenamiento

Para completar el aprovisionamiento de discos para todo el almacenamiento disponible para crear un nuevo repositorio de AppAssure:

- En la página **Provisioning (Aprovisionamiento)**, haga clic en **Next (Siguiente)**.
Aparecerá la página **Provisioning (Aprovisionamiento)** para la capacidad de almacenamiento disponible para aprovisionamiento. Esta capacidad se utiliza para crear un Repositorio AppAssure nuevo.

NOTA: Para el sistema de configuración DL1000 3 TB (2 MV), puede asignar espacio de disco a las VM en espera

El aprovisionamiento de discos para el sistema se completa y se crea un nuevo repositorio.

- Haga clic en **Next (Siguiente)**.
Aparecerá la página **Configuration Complete (Configuración finalizada)**, haga clic en **Exit (Salir)**.

Asistente de configuración del dispositivo DL

NOTA: Se abrirá el Asistente de configuración del dispositivo DL solo cuando se actualice el dispositivo utilizando la utilidad RUU más reciente.

PRECAUCIÓN: Asegúrese de completar todos los pasos del Asistente de configuración del dispositivo DL antes de realizar cualquier otra tarea o cambiar su configuración en el dispositivo. No haga ningún cambio a través del Panel de control, utilice la Actualización de Microsoft Windows, actualice el software Rapid Recovery o instale las licencias, hasta que finalice el asistente. El servicio de actualización de Windows se deshabilita temporalmente durante el proceso de configuración. Si sale del Asistente de configuración del dispositivo DL antes de que finalice, puede provocar errores en el funcionamiento en el sistema.

El Asistente de configuración del dispositivo DL lo guía a través de los siguientes pasos para configurar el software en el dispositivo:

- Configuración de la interfaz de red
- Registro y configuración de host
- Alertas y supervisión
- Acceso y administración
- Configuración de Copia de seguridad de Windows
- Aprovisionamiento de almacenamiento

- [Configuración de la Política de retención y opciones de actualización](#)

NOTA: Una vez que haya completado la configuración del dispositivo, puede omitir el asistente o continuar realizando la **Machine protection (Protección de máquina)**, **Replication (Replicación)**, **Virtual Machine Exports/Standby (Exportaciones de máquinas virtuales/en espera)**. Si elige omitir el asistente, la **Core Console** se inicia automáticamente y puede llevar a cabo protección de máquinas, replicación y exportaciones de máquinas virtuales en etapas posteriores.

Para obtener más información sobre cómo llevar a cabo estas tareas, consulte la *Guía de usuario de Rapid Recovery en dispositivos DL* en www.dell.com/support/home.

Configuración de la interfaz de red

Para configurar las interfaces de red disponibles:

- 1 En la pantalla **DL Appliance Configuration Wizard Welcome (Bienvenida al Asistente de configuración del dispositivo DL)**, haga clic en **Next (Siguiente)**.
Se abre la página **License Agreement (Acuerdo de licencia)**.
- 2 Para aceptar el acuerdo, haga clic en **I accept license agreement (Acepto el acuerdo de licencia)** y, a continuación, haga clic en **Next (Siguiente)**.
La página **Network interfaces (Interfaces de red)** muestra las interfaces de red conectadas disponibles.
- 3 Si es necesario, conecte interfaces de red adicionales y haga clic en **Refresh (Actualizar)**.
Se muestran las interfaces de red conectadas adicionales.
- 4 Seleccione la interfaces de red que correspondan a su entorno.
Tiene las siguientes opciones: IPV4 y IPV6.

Se muestran los detalles de red dependiendo del protocolo de Internet que ha seleccionado.

- 5 Para activar IPV4, seleccione **Enable an IPv4 interface (Habilitar una interfaz IPV4)**.
 - a Para asignar los detalles del protocolo de Internet para la interfaz IPV4, realice una de las siguientes acciones:
 - Para asignar los detalles del protocolo de Internet seleccionado automáticamente, seleccione **Obtain an IPv4 address automatically (Obtener una dirección IPV4 automáticamente)**.
 - Para asignar la conexión de red manualmente, seleccione **Set manually IPv4 address (Establecer manualmente la dirección IPV4)** e introduzca los siguientes detalles:
 - **Dirección IPV4**
 - **Máscara de subred**
 - **Default Gateway**
- 6 Para activar IPV6, seleccione **Enable an IPv6 interface (Habilitar una interfaz IPV6)**.
 - a Para asignar los detalles del protocolo de Internet para la interfaz IPV6, realice una de las siguientes acciones:
 - Para asignar los detalles del protocolo de Internet seleccionados automáticamente, seleccione **Obtain an IPv6 address automatically (Obtener una dirección IPV6 automáticamente)**.
 - Para asignar la conexión de red manualmente, seleccione **Set manually IPv6 address (Establecer manualmente la dirección IPV6)** e introduzca los siguientes detalles:
 - **Dirección IPV6**
 - **Longitud del prefijo de la subred**
 - **Default Gateway**
- 7 Para activar el la formación de equipos de NIC, seleccione **Enable NIC teaming (Activar la formación de equipos de NIC)**.
Para obtener más información sobre la formación de equipos de NIC, consulte [Formación de equipos de adaptadores de red](#).
- 8 Haga clic en **Siguiente**.
Aparece la página **Registro**.

Registro y configuración de host

Registre su dispositivo con la clave de licencia que corresponda para disponer de las funciones acordadas. Se recomienda que cambie el nombre de host antes de empezar con las copias de seguridad. De manera predeterminada, el nombre de host es el nombre del sistema asignado por el sistema operativo.

NOTA: Si desea cambiar el nombre de host, se recomienda que lo cambie en este momento. Al cambiar el nombre de host después de finalizar el DL Appliance Configuration Wizard (Asistente de configuración del dispositivo DL), tendrá que seguir varios pasos.

- 1 En la página **Registration (Registro)**, seleccione una de las siguientes opciones:
 - **Register Now (Registrar ahora):** para registrar el dispositivo con la licencia adquirida. Introduzca la siguiente información: número de licencia en el campo `License number` (número de licencia) y la dirección de correo electrónico válida en el campo `Email address` (dirección de correo electrónico).
 - **Use trial license (Utilizar licencia de prueba):** para registrar el dispositivo con la licencia de prueba. La licencia de prueba caduca después de 30 días. Para seguir utilizando el producto sin interrupción, registre el dispositivo durante ese periodo.
- 2 Haga clic en **Siguiente**.
Se mostrará la página **Host Settings (Configuración de host)**.
- 3 De manera predeterminada, el nombre de host del dispositivo se muestra en el campo `Host Name` (Nombre de host). Para cambiar el nombre de host del dispositivo, introduzca nombre adecuado en el campo **Host Name (Nombre de host)**.
- 4 Si desea unir el dispositivo al dominio, seleccione la casilla de verificación **Join this system to a domain (Unir este sistema a un dominio)** y especifique la siguiente información:
En caso contrario, vaya al paso 5.

NOTA: No se puede unir a un dominio en Windows Server 2012 R2 Foundation Edition. En este caso, no se puede seleccionar la casilla de verificación **Join this system to a domain (Unir este sistema a un dominio)**.

Cuadro de texto	Descripción
Dirección de dominio	Dirección del dominio al que desea agregar el sistema
Administrador de dominio	Administrador de dominio
Contraseña	Contraseña

- 5 Haga clic en **Siguiente**.
Aparece la página **Alerts and Monitoring (Alertas y supervisión)**.

Alertas y supervisión

Para activar alertas de cambios en el hardware y software, tiene dos opciones: SNMP y SMTP. El Simple Network Management Protocol (Protocolo simple de administración de redes, SNMP) es un protocolo de administración de redes utilizado frecuentemente que habilita funciones de administración compatibles con SNMP como búsqueda de dispositivos, supervisión y generación de eventos. SNMP proporciona la administración de red del protocolo TCP/IP. Puede utilizar el Simple Network Management Protocol (Protocolo simple de administración de red, SNMP) o el Simple Mail Transfer Protocol (Protocolo simple de transferencia de correo, SMTP) para establecer alertas y la supervisión del dispositivo.

Para recibir notificaciones, configure las opciones aquí:

NOTA: Se recomienda que configure alertas. También tiene la opción de omitir la configuración de alertas. Para hacerlo, vaya al paso 3.


- 1 Dispone de las siguientes opciones para activar alertas:
 - Para activar el sistema alertas de SNMP, seleccione **Enable system SNMP alerts (Activar el sistema de alertas de SNMP)**.
 - 1 En `SNMP Community` (Comunidad SNMP), introduzca uno o más nombres de comunidades SNMP. Utilice comas para separar los nombres de las comunidades.

- 2 En `SNMP Trap destinations` (Destinos de captura de SNMP), introduzca los destinos de captura y, a continuación, haga clic en **Add (Agregar)**.
- Para activar el software de alertas de SNMP, seleccione la opción **Enable software SNMP alerts (Activar alertas de SNMP)**.
 - 1 En `SNMP Community` (Comunidad SNMP), introduzca uno o más nombres de comunidades SNMP. Utilice comas para separar los nombres de las comunidades.
 - 2 En `SNMP Trap destinations` (Destinos de captura de SNMP), introduzca los destinos de captura y, a continuación, haga clic en **Add (Agregar)**.
- 2 Para establecer alertas de software a través de correo electrónico, seleccione la opción **Notify via email (Notificar por correo electrónico)** e introduzca la dirección de correo electrónico válida.
- 3 Haga clic en **Siguiente**.

Aparece la página `Access and Management` (Acceso y administración).

Acceso y administración


Para acceder y administrar el aparato, configure las opciones de Acceso y administración. Siga los siguientes pasos para configurar las opciones de Acceso y administración del aparato:

- 1 En la página **Acceso y administración**, seleccione o deseleccione las siguientes opciones para acceder y administrar el aparato mediante lo siguiente:
 - Activar Escritorio remoto
 - Activar el Firewall de Windows
 - Activar seguridad mejorada de IE
 - Activar las actualizaciones de Windows
 - Usar servidor proxy
- 2 Si selecciona **Usar servidor proxy**, introduzca la dirección del proxy en el cuadro de texto `Dirección del proxy` y el número del puerto en el cuadro de texto `Puerto`.
- 3  **NOTA: Si desea seleccionar las opciones de configuración predeterminadas de Acceso y administración, haga clic en el botón Restablecer valores predeterminados.**

Haga clic en **Siguiente**.

Se muestra la página **Opciones de copia de seguridad de configuración del dispositivo**.

Configuración de Copia de seguridad de Windows

 **NOTA: Todas las versiones DL, excepto DL 1000, admiten la función de copia de seguridad de Windows.**

Las **Opciones de configuración de la copia de seguridad del dispositivo** le permiten establecer la frecuencia con la que se creará una copia de seguridad de la configuración de su dispositivo. Los datos de Copia de seguridad de Windows ayudan a recuperar los valores de configuración de cualquier estado antes de que se produjeran los errores.

- 1 En la **Opciones de configuración de la copia de seguridad del dispositivo**, seleccione **Realizar copia de seguridad de la configuración del dispositivo**.

Dispone de las siguientes opciones: diario, semanal y mensual.

- 2 Para establecer la frecuencia de la Copia de seguridad de Windows, seleccione una de las opciones siguientes:

Opción	Descripción
Diario	Realiza una copia de los valores de configuración cada día a las 12:01 a. m.
Semanal	Realiza una copia de los valores de configuración cada semana el domingo a las 12:01 a. m.
Mensual	Realiza una copia de los valores de configuración el primer domingo de cada mes a las 12:01 a. m.

- 3 Haga clic en **Siguiente**.

Aparecerá la página **Aprovisionamiento de almacenamiento**.

Aprovisionamiento de almacenamiento

El dispositivo le permite aprovisionar su almacenamiento interno para crear discos virtuales (VD) para alojar los repositorios y reposo virtual, archivos u otros propósitos.

- 1 En la **página Aprovisionamiento de almacenamiento**, seleccione las siguientes opciones de configuración para su almacenamiento. El Nombre del repositorio se muestra como **Repositorio 1** de manera predeterminada.

NOTA: El tamaño del repositorio depende de las licencias que se aplican durante el registro del dispositivo.

- Si ha aplicado la licencia de prueba durante el registro del dispositivo, no habrá restricciones de tamaño del repositorio.
- Si ha aplicado una licencia adquirida al registrar el dispositivo, el tamaño del repositorio corresponde al modelo. Por ejemplo: en el dispositivo DL 1000 1 TB se crea un repositorio de 1 TB.

- 2 Seleccione **Allocate a portion of your storage for Virtual Standby, archives, or other purposes (Asignar una parte de su almacenamiento para reposo virtual, archivos, u otros propósitos)**.
- 3 Asignar el porcentaje de espacio de almacenamiento que disponible después de crear el repositorio mediante el control deslizante. También puede utilizar el campo **Tamaño** para especificar el tamaño exacto.

Un disco virtual de capacidad especificada para alojar las máquinas virtuales (VM) en reposo virtual, los archivos, se crea otro propósito.

- 4 Haga clic en **Siguiente**.

El repositorio inicial se crea y se crean los VDs iniciales para alojar las máquinas virtuales u otros propósitos.

Aparecerá la página **Política de retención**.

Configuración de la Política de retención y opciones de actualización

Las políticas de retención imponen los periodos durante los cuales las copias de seguridad se almacenan en medios a corto plazo (rápidos y costosos). A veces, ciertos requisitos empresariales y técnicos exigen ampliar la retención de estas copias de seguridad, pero el uso del almacenamiento rápido resulta inasequible. En el dispositivo, las políticas de retención se pueden personalizar para especificar la duración del periodo en que se mantiene un punto de recuperación de la copia de seguridad. Cuando la antigüedad de los puntos de recuperación se acerca al final de su periodo de retención, estos se vuelven obsoletos y quedan eliminados de la agrupación de retención.

NOTA: Si la restricción de licencia de la política de retención es predeterminada, la política de retención no se puede configurar para establecer un periodo de retención superior a tres meses. Si intenta hacerlo, verá un mensaje de error.

- 1 Las siguientes opciones le permiten definir la duración con la que se almacenan las instantáneas de copia de seguridad de las máquinas protegidas y modificar el proceso de consolidación de la fusión y la eliminación de las copias de seguridad antiguas. La página **Política de retención** muestra las siguientes opciones:

Tabla 2. Opciones de programación de la política de retención predeterminada

Cuadro de texto	Descripción
Conserve todos los puntos de recuperación durante n [duración de retención].	Especifica el período de retención de los puntos de recuperación. Introduzca el número que represente el periodo de retención y seleccione la duración. El valor predeterminado es 3. Puede elegir días, semanas, meses o años.
Y luego puede conservar un punto de recuperación por hora durante n [duración de retención].	Proporciona un nivel de retención más granular. Se utiliza como bloque de construcción con la configuración primaria para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente el periodo de retención y seleccione la duración. El valor predeterminado es 2.

Cuadro de texto	Descripción
	Puede elegir días, semanas, meses o años.
Y luego puede conservar un punto de recuperación por día durante n [duración de retención].	Proporciona un nivel de retención más granular. Se utiliza como bloque de construcción para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente el periodo de retención y seleccione la duración. El valor predeterminado es 4 días. Puede elegir días, semanas, meses o años.
Y luego puede conservar un punto de recuperación por semana durante n [duración de retención].	Proporciona un nivel de retención más granular. Se utiliza como bloque de construcción para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente el periodo de retención y seleccione la duración. El valor predeterminado es 3 semanas. Puede elegir semanas, meses o años.
Y luego puede conservar un punto de recuperación por mes durante n [duración de retención].	Proporciona un nivel de retención más granular. Se utiliza como bloque de construcción para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente el periodo de retención y seleccione la duración. El valor predeterminado es 2 meses. Puede elegir meses o años.
Y luego puede conservar un punto de recuperación por año durante n [duración de retención].	Introduzca el número que represente el período de retención y seleccione el período de tiempo. Puede elegir años.

- 2 Haga clic en **Siguiente**.
Se muestra la página **Opciones de actualización**.
- 3 Para buscar actualizaciones de software del dispositivo, seleccione la opción **Buscar actualizaciones de software del dispositivo**.
Si hay alguna actualización, se descargará e instalará tras finalizar con el asistente.
- 4 Para activar las actualizaciones del Core de Rapid Recovery, seleccione **Activar actualizaciones del Core de Rapid Recovery** y, a continuación, seleccione una de las siguientes opciones:
 - Notificar actualizaciones, pero no instalarlas automáticamente
 - Instalar automáticamente las actualizaciones
- 5 Haga clic en **Finalizar**.
Se aplica la configuración del dispositivo.

Recuperación automática rápida del dispositivo (RASR)

Rapid Appliance Self Recovery (Recuperación automática rápida del dispositivo, RASR) es un proceso de restauración desde cero en el que las unidades del sistema operativo se restituyen a la imagen predeterminada de fábrica.

Creación de la memoria USB de RASR

Para crear una memoria USB de RASR:

- 1 Vaya a la pestaña **Appliance (Dispositivo)**.
- 2 Seleccione **Appliance (Dispositivo) > Backup (Copia de seguridad)** en el panel de navegación de la izquierda.

Se muestra la ventana **Create RASR USB Drive (Crear unidad USB de RASR)**.

① **NOTA:** Inserte una memoria USB de 16 GB o mayor antes de intentar crear la clave RASR.

- Después de insertar una memoria USB de 16 GB o más, haga clic en **Create RASR USB Drive now (Crear unidad USB de RASR ahora)**.

Se muestra el mensaje **Prerequisite Check (Verificación de requisitos previos)**.

Después de que se hayan comprobado los requisitos previos, se abrirá la ventana **Create the RASR USB Drive (Crear la unidad USB de RASR)**, que muestra el tamaño mínimo requerido para crear la unidad USB y una **List of Possible target paths (Lista de posibles rutas de destino)**.

- Seleccione el destino y haga clic en **Create (Crear)**.

Aparece un cuadro de diálogo de advertencia.

- Haga clic en **Sí**.

Se ha creado la memoria de la unidad USB de RASR.

- ① **NOTA:** Asegúrese de utilizar la función **Extracción de la unidad de Windows** para preparar la memoria USB para su extracción. De lo contrario, el contenido de la memoria USB puede dañarse y la memoria USB no funcionará como se espera.

Extraiga la memoria USB de RASR que se ha creado para cada dispositivo DL, etiquétela y guárdela para su uso en el futuro.

Ejecución de RASR

① **NOTA:** Dell recomienda crear una clave USB RASR después de haber configurado el dispositivo. Para crear una clave USB RASR, consulte el apartado [Creación de la clave USB RASR](#).

① **NOTA:** Asegúrese de contar con los más recientes RUU a los que pueda acceder el dispositivo.

① **NOTA:** Para realizar la recuperación del sistema mediante RASR, consulte el documento *Recuperación de un dispositivo de recuperación y copia de seguridad™ DL mediante un dispositivo de Copia de seguridad y recuperación mediante Recuperación automática rápida del dispositivo (RASR)* en Dell.com/support/home.

Para restablecer la configuración predeterminada de fábrica:

- Introduzca la llave USB RASR creada.
- Reinicie el dispositivo y seleccione **Boot Manager (F11) (Administrador de arranque [F11])**.
- En el **Boot Manager Main Menu (Menú principal del administrador de arranque)**, seleccione **One-shot BIOS Boot Menu (Menú de inicio de BIOS único)**.
- En el **Boot Manager Boot Menu (Menú del administrador de arranque)**, seleccione la unidad USB conectada.
- Seleccione el diseño del teclado.
- Haga clic en **Troubleshoot (Solución de problemas) > Rapid Appliance Self Recovery (Recuperación automática rápida del dispositivo)**.
- Seleccione el sistema operativo de destino (SO).
RASR se inicia y aparece la pantalla de **bienvenida**.
- Haga clic en **Siguiente**.
Se muestra la pantalla de verificación **Prerequisites (Prerrequisitos)**.


① **NOTA:** Antes de ejecutar la RASR, asegúrese de que se verifican todos los prerrequisitos de hardware y otros.

- Haga clic en **Siguiente**.

Se muestra la pantalla **Recovery Mode Selection (Selección de modo de recuperación)** con tres opciones:

- System Recovery (Recuperación del sistema)**
- Windows Recovery Wizard (Asistente de recuperación de Windows)**

• **Factory Reset (Restablecer valores de fábrica)**

- 10 Seleccione la opción **Factory Reset (Restablecer valores de fábrica)**.
Esta opción recuperará el disco del sistema operativo desde la imagen de fábrica.
- 11 Haga clic en **Siguiente**.
Aparece el siguiente mensaje de aviso en un cuadro de diálogo: `This operation will recover the operating system. All OS disk data will be overwritten .`
- 12 Haga clic en **Sí**.
El disco del sistema operativo inicia la restauración de las configuraciones de fábrica.
- 13 La página **RASR completada** aparece una vez finalizado el proceso de recuperación. Haga clic en **Finalizar**.
- 14 Iniciar el sistema después restaurar.
- 15  **NOTA: Continúe configurando solo si aparece el Asistente de configuración del dispositivo AppAssure. Si no, vaya al paso 17.**


Espere a que cargue el Asistente de configuración del dispositivo AppAssure. Cierre el asistente utilizando el Administrador de tareas de Windows.
- 16 Ejecute el archivo **launchRUU.exe** del paquete RUU. Siga las instrucciones y seleccione la opción para continuar con la instalación de RUU y finalice la instalación de RUU.
- 17 Se inicia el **Asistente de configuración del dispositivo DL** y le guiará a través del resto del proceso de restauración.

El dispositivo funciona correctamente ahora.

Utilidad de recuperación y actualización

La utilidad Recovery and Update Utility (Utilidad de actualización y recuperación, RUU) es un instalador todo en uno para recuperar y actualizar el software de dispositivos DL (DL1000, DL1300, DL4000 y DL4300). Incluye el software Rapid Recovery y componentes específicos del dispositivo.

La utilidad RUU se compone de versiones actualizadas de funciones y características de Windows Server, .Net 4.5.2, LSI Provider, DL Applications, OpenManage Server Administrator y el software Rapid Recovery Core. Además, la utilidad Recovery and Update Utility (Utilidad de recuperación y actualización, RUU) también actualiza el contenido de Rapid Appliance Self Recovery (Recuperación automática rápida del dispositivo, RASR).

 **NOTA: Si actualmente utiliza cualquiera de las versiones del Core de AppAssure, la versión de Rapid Recovery 6.0.2.144 o anterior, la utilidad RUU actualiza a la versión más reciente disponible en la carga útil. No es posible omitir la actualización y esta actualización no es reversible. Si no desea actualizar el software del Core, no ejecute la utilidad RUU.**

Para instalar la versión más reciente de la utilidad RUU:

- 1 Vaya al Portal de licencias en la sección Descargas o vaya a support.dell.com y descargue el instalador de la utilidad RUU.
- 2 Para iniciar el proceso de RUU, ejecute el archivo **launchRUU.exe** del paquete de RUU.

 **NOTA: Es posible que el sistema se reinicie durante el proceso de actualización de la utilidad RUU.**

Configuración de su DL1000

Descripción general

Después de completar el Asistente de configuración del dispositivo DL, lleve a cabo los siguientes procedimientos para garantizar que el dispositivo de copia de seguridad y los servidores, cuya copia de seguridad está realizando el dispositivo, estén correctamente configurados.

La configuración incluye tareas como la configuración de exploradores para acceder de forma remota a la Core Console DL1000, la administración de licencias y la configuración de alertas y notificaciones. Después de completar la configuración del Core, puede proteger los Agents y realizar la recuperación.

- ① **NOTA:** El dispositivo está configurado con una licencia de software temporal de 30 días. Para obtener una clave de licencia permanente, inicie sesión en el protección de datos de Dell | Recuperación rápida de licencias en www.dell.com/DLActivation. Para obtener más detalles sobre cómo cambiar una clave de licencia, consulte el tema "Actualizar o cambiar una licencia" en la *Guía de usuario de Rapid Recovery 6.0 en dispositivos DL* en dell.com/support/home.
- ① **NOTA:** Mientras se utiliza el dispositivo de copia de seguridad en disco DL1000, se recomienda que utilice la pestaña Dispositivo para configurar el Core.

Restablecimiento del sistema operativo a la configuración predeterminada

Para restablecer el sistema operativo a la configuración predeterminada, realice lo siguiente:

- 1 Inicie sesión como administrador y abra el símbolo del sistema.
- 2 Vaya a `c:\windows\system32\sysprep` y ejecute el comando `sysprep.exe/generalize/oobe/reboot`.
- 3 Seleccione:
 - **English (Inglés)** como idioma
 - **United States (Estados Unidos)** como país/región
 - **US** como diseño del teclado

Configuración de exploradores para acceder de manera remota a la DL1000Core Console

Para poder acceder correctamente a la Core Console desde una máquina remota, primero debe modificar la configuración del explorador. En el siguiente procedimiento se detalla cómo modificar la configuración de los exploradores Internet Explorer, Google Chrome y Mozilla Firefox.

- ① **NOTA:** Para modificar la configuración del explorador, debe iniciar sesión en la máquina con privilegios de administrador.
- ① **NOTA:** Como Chrome utiliza la configuración de Internet Explorer, deberá usar Internet Explorer para realizar cambios en Chrome.
- ① **NOTA:** Asegúrese de que la configuración de seguridad mejorada de Internet Explorer está encendida cuando acceda a la Core Web Console, ya sea de manera local o remota. Para activar la configuración de seguridad mejorada de Internet Explorer, abra **Administrador de servidores > Servidor local > Configuración de seguridad mejorada de IE** se muestra la opción, asegúrese de que está Encendida.

Configuración de los valores del explorador en Internet Explorer y en Chrome

Para modificar la configuración del explorador en Internet Explorer y en Chrome:

- 1 En la pantalla **Internet Options (Opciones de Internet)**, seleccione la pestaña **Security (Seguridad)**.
- 2 Haga clic en **Trusted Sites (Sitios de confianza)** y, a continuación, haga clic en **Sites (Sitios)**.
- 3 Anule la selección de la opción **Require server verification (https:) for all sites in the zone (Requerir comprobación del servidor [https:] para todos los sitios de la zona)** y, a continuación, agregue `http://<nombre del host o dirección IP del servidor del dispositivo que aloja el Core de Rapid Recovery>` a **Trusted Sites (Sitios de confianza)**.
- 4 Haga clic en **Close (Cerrar)**, seleccione **Trusted Sites (Sitios de confianza)** y, después, haga clic en **Custom Level (Nivel personalizado)**.
- 5 Desplácese hasta **Miscellaneous (Miscelánea)** → **Display Mixed Content (Mostrar contenido mixto)** y seleccione **Enable (Habilitar)**.
- 6 Desplácese a la parte inferior de la pantalla hasta **User Authentication (Autenticación del usuario)** → **Logon (Inicio de sesión)** y, a continuación, seleccione **Automatic logon with current user name and password (Inicio de sesión automático con el nombre de usuario y contraseña actuales)**.
- 7 Haga clic en **OK (Aceptar)** y, después, seleccione la pestaña **Advanced (Opciones avanzadas)**.
- 8 Vaya hasta **Multimedia** y seleccione **Play animations in webpages (Reproducir animaciones en páginas web)**.
- 9 Desplácese hasta **Security (Seguridad)**, active la opción **Enable Integrated Windows Authentication (Habilitar autenticación integrada de Windows)** y, a continuación, haga clic en **OK (Aceptar)**.

Configuración de los valores del explorador en Firefox

Para modificar la configuración del explorador en Firefox:

- 1 En la barra de direcciones de Firefox, escriba **about:config** y, a continuación, haga clic en **I'll be careful, I promise (¡Tendré cuidado, lo prometo!)** si aparece el cuadro de diálogo.
- 2 Busque el término **ntlm**.
La búsqueda debería devolver al menos tres resultados.
- 3 Haga doble clic en **network.automatic-ntlm-auth.trusted-uris** y escriba la siguiente configuración según convenga para su máquina:
 - En las máquinas locales, introduzca el nombre de host.
 - En las máquinas remotas, escriba el nombre del host o la dirección IP, separados por comas, del servidor que aloja el Core; por ejemplo, *dirección IP,nombre del host*.
- 4 Reinicie Firefox.

Acceso a la Core Console DL1000

Asegúrese de actualizar los sitios de confianza como se indica en el tema [Updating Trusted Sites In Internet Explorer](#) (Actualización de los sitios de confianza en Internet Explorer), y configure los exploradores como se indica en el tema [Configuración de exploradores para acceder de manera remota a la DL1000Core Console](#). Después de haber actualizado los sitios de confianza en Internet Explorer y haber configurado los exploradores, realice una de las siguientes acciones para acceder a la Core Console:

- Inicie sesión localmente en el servidor Core y, a continuación, haga doble clic en el icono **Core Console**
- Escriba una de las URL siguientes en el explorador de web:
 - **https://<NombreDesuServidorCore>:8006/apprecovery/admin/core**
 - **https://<DirecciónIPdesuServidorCore>:8006/apprecovery/admin/core**

Actualización de los sitios de confianza en Internet Explorer

Para actualizar los sitios de confianza en Internet Explorer:

- 1 Abra Internet Explorer.
- 2 Si **File (Archivo)**, **Edit View (Editar vista)** y demás menús no aparecen, presione <F10>.
- 3 Haga clic en el menú **Tools (Herramientas)** y seleccione **Internet Options (Opciones de Internet)**.
- 4 En la ventana **Internet Options (Opciones de Internet)**, haga clic en la pestaña **Security (Seguridad)**.
- 5 Haga clic en **Trusted Sites (Sitios de confianza)** y, a continuación, haga clic en **Sites (Sitios)**.
- 6 En **Add this website to the zone (Agregar este sitio web a la zona)**, introduzca **https://[Display Name]**, usando el nuevo nombre que haya proporcionado para el nombre de visualización.
- 7 Haga clic en **Add (Agregar)**.
- 8 En **Add this website to the zone (Agregar este sitio web a la zona)**, escriba **about:blank**.
- 9 Haga clic en **Add (Agregar)**.
- 10 Haga clic en **Close (Cerrar)** y, a continuación, en **OK (Aceptar)**.

Cifrado de datos de instantáneas del Agent

El Core puede cifrar datos de instantáneas del Agent en el repositorio. En vez de cifrar todo el repositorio, DL1000 le permite especificar una clave de cifrado durante la protección de un Agent en un repositorio que permite volver a utilizar las claves para diferentes Agents.

Para cifrar los datos de instantáneas del Agent:

- 1 Desde el Core, haga clic en **Configuration (Configuración)** → **Manage (Administrar)** → **Security (Seguridad)**.
- 2 Haga clic en **Actions (Acciones)** y, a continuación, haga clic en **Add Encryption Key (Agregar clave de cifrado)**. Se muestra la página **Create Encryption Key (Crear clave de cifrado)**.
- 3 Complete la siguiente información:

Campo	Descripción
Nombre	Introduzca un nombre para la clave de cifrado.
Comentario	Introduzca un comentario para la clave de cifrado. Se utiliza para proporcionar detalles adicionales sobre la clave de cifrado.
Passphrase	Introduzca una frase de contraseña. Se utiliza para controlar el acceso.
Confirmar contraseña	Vuelva a introducir la frase de contraseña. Se utiliza para confirmar la entrada de la frase de contraseña.

NOTA: Se recomienda anotar la frase de contraseña del cifrado, ya que si esta se pierde los datos serán inaccesibles. Para obtener más información, consulte el capítulo **Managing Security (Administración de seguridad)** en la *Dell DL1000 Appliance User's Guide (Guía del usuario del Dell DL1300 Appliance)*.

Configuración de un servidor de correo electrónico y de una plantilla de notificaciones de correo electrónico

Si desea recibir notificaciones de correo electrónico acerca de eventos, configure un servidor de correo electrónico y una plantilla de notificaciones de correo electrónico.

NOTA: También debe configurar los valores del grupo de notificación, incluida la habilitación de la opción **Notify by email** (Notificar por correo electrónico), antes de que se envíen los mensajes de alerta de correo electrónico. Para obtener más información sobre la especificación de eventos para recibir alertas de correo electrónico, consulte **Configuring Notification Groups For System Events** (Configuración de grupos de notificación para eventos del sistema) en la *Dell DL1000 Appliance User's Guide* (Guía del usuario Dell DL1300 Appliance) en Dell.com/support/home.

Para configurar un servidor de correo electrónico y una plantilla de notificaciones de correo electrónico:

- 1 En **Core**, seleccione la pestaña **Configuration (Configuración)**.
- 2 En la opción **Manage (Administrar)**, haga clic en **Events (Eventos)**.
- 3 En el panel **Email SMTP Settings (Configuración SMTP de correo electrónico)**, haga clic en **Change (Cambiar)**.
Se muestra el cuadro de diálogo **Edit Email Notification Configuration (Editar configuración de notificación por correo electrónico)**.
- 4 Seleccione **Enable Email Notifications (Habilitar notificaciones de correo electrónico)** y, a continuación, introduzca los detalles para el servidor de correo electrónico de la siguiente manera:

Cuadro de texto	Descripción
Servidor SMTP	Introduzca el nombre del servidor de correo electrónico que utilizará la plantilla de notificaciones de correo electrónico. La convención de nombres incluye el nombre de host, el dominio y el sufijo; por ejemplo, smtp.gmail.com .
Puerto	Introduzca un número de puerto. Se utiliza para identificar el puerto para el servidor de correo electrónico. Por ejemplo, el puerto 587 para Gmail. El valor predeterminado es 25.
Timeout (seconds)	Introduzca un valor entero para especificar cuánto tiempo debe intentar una conexión antes de que se agote el tiempo de espera. Se utiliza para establecer el tiempo, en segundos, durante el que se intenta la conexión al servidor de correo electrónico antes de que se agote el tiempo de espera. El valor predeterminado es 30 segundos.
TLS	Seleccione esta opción si el servidor de correo electrónico utiliza una conexión segura como, por ejemplo, Seguridad de la capa de transporte (TLS) o Capa de sockets seguros (SSL).
Nombre de usuario	Introduzca un nombre de usuario para el servidor de correo electrónico.
Contraseña	Introduzca una contraseña para acceder al servidor de correo electrónico.
From	Introduzca una dirección de correo electrónico del remitente. Se utiliza para especificar la dirección de correo electrónico del remitente para la plantilla de notificaciones de correo electrónico; por ejemplo, noreply@localhost.com .
Email Subject	Introduzca un asunto para la plantilla de correo electrónico. Se utiliza para definir el asunto de la plantilla de notificaciones de correo electrónico; por ejemplo, <code><hostname> - <level> <name></code> .
Correo electrónico	Introduzca la información para el texto de la plantilla que describe el evento, cuándo se ha producido y la gravedad.

- 5 Haga clic en **Send Test Email (Enviar correo electrónico de prueba)** y revise los resultados.
- 6 Cuando los resultados de la prueba sean satisfactorios, haga clic en **OK (Aceptar)**.

Ajuste del número de secuencias

De manera predeterminada, Rapid Recovery se configura para permitir tres secuencias simultáneas en el dispositivo. Se recomienda que el número de secuencias se establezca entre 10 y 15 para obtener un rendimiento óptimo.

Para cambiar el número de secuencias simultáneas:

- 1 Seleccione la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Settings (Configuración)**.
- 2 Seleccione cambiar en **Transfer Queue (Cola de transferencias)**.
- 3 Cambie el **Número máximo de transferencias** a un número entre 10 y 15 para obtener un rendimiento óptimo, pero si el rendimiento parece insatisfactoria, intente ajustar manualmente.

Preparación para la protección de los servidores

Descripción general

Para proteger sus datos mediante DL 1000, agregue las estaciones de trabajo y los servidores de protección en la Core Console. Por ejemplo, el servidor de Exchange, SQL Server, Linux, etc.

En la Core Console, puede identificar la máquina en la que haya un Agent instalado y especificar qué volúmenes proteger, por ejemplo, un espacio de almacenamiento de Microsoft Windows. Puede definir programaciones de protección, agregar medidas de seguridad adicionales, como cifrado y mucho más. Para obtener más información sobre cómo acceder a la Core Console para proteger estaciones de trabajo y servidores, consulte [Cómo proteger una máquina](#).

Temas:

- [Instalación de Agents en clientes](#)
- [Acerca de cómo instalar el software del Agent en máquinas con Linux](#)
- [Instalación del software del Agent en máquinas con Linux fuera de línea](#)
- [Cómo proteger una máquina](#)

Instalación de Agents en clientes

Los clientes que cuenten con el respaldo del dispositivo DL 1000 deben tener instalado el Agent de Rapid Recovery. La Core Console de Rapid Recovery le permite implementar Agents en las máquinas. La implementación de Agents en máquinas requiere una configuración previa de los valores para seleccionar un solo tipo de agent para enviar a los clientes. Este método funciona bien si todos los clientes están ejecutando el mismo sistema operativo. Sin embargo, si hay versiones diferentes de sistemas operativos, es más fácil instalar los Agents en los máquinas.

También puede implementar el software del Agent en la máquina del Agent durante el proceso de protección de una máquina. Esta opción está disponible para máquinas que no tengan ya el software del Agent instalado. Para obtener más información sobre la implementación del software del Agent al proteger una máquina, consulte la *Guía de usuario de Rapid Recovery en dispositivos DL* en Dell.com/support/home.

Implementación del software del Agent al proteger un Agent

Puede descargar e implementar Agents cuando está agregando un Agent para protegerlo.

NOTA: Este procedimiento no es necesario si ya tiene instalado el software del Agent en un sistema que desea proteger. Si no instala el software del Agent antes de proteger una máquina, no podrá seleccionar volúmenes específicos para la protección en este asistente. En este caso, de manera predeterminada, todos los volúmenes de la máquina del Agent se incluirán para la protección. Rapid Recovery admite la protección y recuperación de máquinas configuradas con las particiones EISA. También se admiten máquinas con Windows 8, Windows 8.1, Windows 2012 y Windows 2012 R2 que usan el Entorno de recuperación de Windows (Windows RE).

1 Realice uno de los siguientes pasos:

- Si inicia desde el Asistente de protección de la máquina, continúe con el paso 2 . . .
- Si inicia desde la Core Console de Rapid Recovery, haga clic en **Protect (Proteger)** en la barra de botones.

- Se abrirá el **Protect Machine Wizard (Asistente de protección de la máquina)**.
- En la página **Welcome (Bienvenida)**, seleccione las opciones de instalación adecuadas:
 - Si no necesita definir un repositorio o establecer el cifrado, seleccione **Typical (Típica)**.
 - Si necesita crear un repositorio o definir un repositorio diferente para las copias de seguridad de la máquina seleccionada, o si desea establecer el cifrado con el asistente, seleccione **Advanced (show optional steps) (Avanzado [mostrar pasos opcionales])**.
 - Si no desea ver la página **Welcome (Bienvenida)** del Asistente de protección de la máquina en el futuro, seleccione la opción **Omitir esta página de bienvenida la próxima vez que el asistente se abra**.
 - Cuando esté satisfecho con las opciones en la página de bienvenida, haga clic en **Siguiente**. Aparecerá la página **Connection (Conexión)**.
 - En la página **Connection (Conexión)**, introduzca la información sobre la máquina a la que desea conectarse tal como se describe en la tabla y, a continuación, haga clic en **Nextiguente**.

Tabla 3. Configuración de la conexión de la máquina

Cuadro de texto	Descripción
Host	El nombre de host o la dirección IP de la máquina que desea proteger.
Puerto	El número de puerto con el que se comunica el Core de Rapid Recovery con el Agent de la máquina. El número de puerto predeterminado es 8006.
Nombre de usuario	El nombre de usuario que utiliza para conectarse a esta máquina; por ejemplo, Administrador (o, si la máquina está en un dominio, [nombre del dominio] \Administrador).
Contraseña	La contraseña que se utiliza para conectar a esa máquina.

Si la página **Install Agent (Instalar Agent)** se abre a continuación en el Asistente de protección de la máquina, indica que Rapid Recovery no detecta el Agent de Rapid Recovery en la máquina e instalará la versión actual del software.

- NOTA:** El software del Agent debe estar instalado en la máquina que desea proteger. Asimismo, la máquina se debe reiniciar para poder crear copias de seguridad en el Core. Para que el instalador reinicie la máquina protegida, seleccione la opción **After installation, restart the machine automatically (recommended) (Reiniciar la máquina automáticamente tras la instalación [recomendado])** antes de hacer clic en **Next (Siguiente)**.

Haga clic en **Siguiente**.

Instalación del software del Agent de Rapid Recovery en máquinas con Windows

Implemente el archivo de instalación del Agent de Rapid Recovery en la máquina que desea proteger utilizando uno de los métodos descritos en el tema "Instalación del software del Agent de Rapid Recovery" en la *Protección de datos de Dell | Guía de instalación y mejora de Rapid Recovery 6.0*. A continuación, inicie el programa de instalación como se describe a continuación para instalar o actualizar el software en cada máquina con Windows que desea proteger en el Core de Rapid Recovery.

NOTA: Ejecute el instalador con privilegios de administrador local.

- En la máquina que desea proteger, haga doble clic en el archivo de instalación ejecutable del Agent de Rapid Recovery para iniciar el instalador.
En función de la configuración de la máquina, se muestra la ventana Control de cuentas de usuario o Abrir archivo: advertencia de seguridad.
- Si se le solicita permiso, confirme que desea ejecutar el instalador y realizar cambios en el sistema.
- Si faltan componentes .NET o si necesitan ser actualizados, acepte las indicaciones para descargar e instalar el marco.
- En el campo idioma, seleccione la opción que corresponda para el idioma y, a continuación, haga clic en **Aceptar**.

- 5 Elija una de las siguientes opciones:
 - Si es la primera vez que se instala el software del Agent de Rapid Recovery en esta máquina, el instalador se prepara la instalación, y, a continuación, aparecerá el Asistente de instalación del Agent de Rapid Recovery. Continúe con el paso 6.
 - Si esta máquina tiene una versión anterior del Agent de AppAssure o si tiene instalado el software del Agent de Rapid Recovery, verá un mensaje en que se le pregunta si desea o no actualizar a la versión actual.
 - 1 Haga clic en **Sí**.

Aparece el Asistente de instalación de Rapid Recovery, que muestra la página **Progreso** del asistente. La aplicación se descarga en la carpeta de destino, y muestra el progreso en la barra de progreso. Cuando haya terminado, el asistente se dirigirá automáticamente a la página **Completado**.
 - 2 Vaya al paso 12.
- 6 En el Asistente de instalación de Rapid Recovery, en la página **Bienvenida**, haga clic en **Siguiente** para continuar con la instalación. Aparece la página **Licence Agreement (Acuerdo de licencia)**.
- 7 En la pantalla **Acuerdo de licencia**, seleccione **I accept the terms in the license agreement (Acepto los términos del Acuerdo de licencia)** y, a continuación, haga clic en **Next (Siguiente)**. Aparecerá la página **Prerequisites (Requisitos previos)**.
- 8 El instalador del Agent de Rapid Recovery verifica que existan los archivos de los prerequisites.
 - Si existen dichos archivos, aparecerá un mensaje indicándole que todos los prerequisites están instalados en la máquina.
 - Si no existen dichos archivos, el instalador del Agent de Rapid Recovery identifica los archivos necesarios y muestra los resultados correspondientes; por ejemplo, CRT 2013 (x64) ENU (código distribuible para Microsoft Visual Studio®), o Microsoft System CLR Types para SQL Server 2008 R2 (x64). Haga clic en **Install Prerequisites (Instalar prerequisites)**.
- 9 Cuando finalice la instalación de los archivos de los prerequisites, haga clic en **Next (Siguiente)**. Aparecerá la página **Installation Options (Opciones de instalación)**.
- 10 En la página **Opciones de instalación**, revise las opciones de instalación. Si es necesario, modifíquelas como se describe a continuación.
 - En el campo de texto **Destination Folder (Carpeta de destino)**, revise la carpeta de destino para la instalación. Si desea cambiar la ubicación, haga lo siguiente:
 - Haga clic en el ícono de la carpeta.
 - En el cuadro de diálogo **Explorar en destino**, seleccione una nueva ubicación.
 - Haga clic en **Aceptar**.
 - En el campo de texto de **Número de puerto**, introduzca un número de puerto que se debe usar para la comunicación entre el software del Agent de la máquina protegida y el Core de Rapid Recovery.

NOTA: El valor predeterminado es 8006. Si cambia el número de puerto, anótelos en caso de que tenga que ajustar las opciones de configuración en otro momento.
 - Seleccione **Allow Agent to automatically send diagnostic and usage information to Dell Inc. (Permitir al Agent enviar un diagnóstico e información de uso automáticamente a Dell Inc.)** para enviar información de uso y diagnóstico a Dell. Si no desea enviar esta información, anule la selección de esta opción.
- 11 Una vez esté satisfecho con las opciones de instalación, haga clic en **Instalar**. Aparecerá la página **Progress (Progreso)** que incluye una barra de estado que le permite supervisar el progreso de la instalación.

Cuando la instalación se haya completado, aparecerá la página **Completado**. Vaya al paso 12.
- 12 En la página **Completado**, si aparece un mensaje que indica que se debe reiniciar el sistema para poder aplicar la instalación, realice uno de los siguientes pasos:
 - Para reiniciar ahora, seleccione **Yes, I want to restart my computer now (Sí, deseo reiniciar mi equipo ahora)**.
 - Para reiniciar más tarde, deje en blanco la opción **Yes, I want to restart my computer now (Sí, quiero reiniciar mi equipo ahora)** opción.
- 13 En la página **Completado**, haga clic en **Finalizar**. El asistente de instalación se cierra y ha terminado la instalación del Agent.

Implementación del software del Agent de Rapid Recovery a una o más máquinas

Puede simplificar la tarea de implementación del software del Agent de Rapid Recovery a una o más máquinas con Windows mediante el Asistente de implementación del software del Agent.

NOTA: Antes, esta función se denominaba "implementación masiva."

Al utilizar el Asistente de implementación del software del Agent, Rapid Recovery puede detectar automáticamente máquinas en un host y le permite seleccionar las máquinas en las que desea realizar la implementación. Para las máquinas en dominios o hosts distintos a los de Active Directory o vCenter o ESX(i), puede conectarse manualmente en máquinas individuales mediante sus direcciones IP y las credenciales correspondientes. También puede actualizar el software en máquinas que ya cuentan con la protección de Rapid Recovery.

Desde dentro de la Core Console, puede ejecutar cualquiera de las siguientes tareas:

- Implementación en máquinas en un dominio de Active Directory
- Implementación en máquinas en host virtual VMware vCenter/ESX(i)

NOTA: Dell recomienda limitar el número de máquinas en realiza la implementación de forma simultánea a 50 o menos a fin de evitar limitaciones de recursos que pueden provocar que falle la operación de implementación.

Instalación de Agents de Microsoft Windows en el cliente

Para instalar los Agents:

- 1 Asegúrese de que el cliente tenga instalado el marco Microsoft .NET4:
 - a En el cliente, inicie el **Administrador del servidor Windows**.
 - b Haga clic en **Configuración > Servicios**.
 - c Asegúrese de que Microsoft .NET Framework se muestra en la lista de servicios.
Si no está instalado, puede obtener una copia en **microsoft.com**.
- 2 Instale el Agent:
 - a En el dispositivo, comparta el directorio **C:\Program Files\AppRecovery** con el/los cliente/s de los que desea crear una copia de seguridad.
 - b En el sistema del cliente, asigne una unidad en **C:\Program Files\AppRecovery** en el dispositivo DL.
 - c En el sistema del cliente, abra el directorio **C:\Program Files\AppRecovery** y haga doble clic en el Agent que corresponda al sistema del cliente para iniciar la instalación.

Implementación en máquinas en un dominio de Active Directory

Utilice este procedimiento para implementar simultáneamente el software del Agent de Rapid Recovery en una o más máquinas en un dominio de Active Directory.

Antes de iniciar este procedimiento, tenga a la mano la información del dominio y las credenciales de inicio de sesión para el servidor de Active Directory.

- 1 En la Core Console de Rapid Recovery, haga clic en el menú desplegable **Protect (Proteger)** After installation, restart the machine automatically (recommended) y, haga clic en **Deploy Agent Software (Implementar el software del Agent)**.
Se abre el Deploy Agent Software Wizard (Asistente de implementación del software del Agent).
- 2 En la página **Connection (Conexión)** del asistente, seleccione **Active Directory** de la lista desplegable **Source (Origen)**.
- 3 Introduzca la información del dominio y las credenciales de inicio de sesión como se describe en la tabla siguiente.

Tabla 4. Información sobre el dominio y las credenciales

Cuadro de texto	Descripción
Host	El nombre de host o la dirección IP del dominio de Active Directory.
Nombre de usuario	El nombre de usuario que utiliza para conectarse al dominio; por ejemplo, Administrador o, si la máquina está en un dominio, [nombre de dominio]\Administrator).
Contraseña	La contraseña segura que se utiliza para conectarse al dominio.

- Haga clic en **Siguiente**.
- En la página **Machines (Máquinas)**, seleccione las máquinas en las que desea implementar el software del Agent de Rapid Recovery.
- De manera opcional, para reiniciar automáticamente las máquinas protegidas una vez que el Agent está instalado, seleccione **After Agent installation, restart the machines automatically (Recommended) (Reiniciar la máquina automáticamente tras la instalación del Agent [recomendado])**.
- Haga clic en **Finalizar**.
El sistema comprueba de forma automática cada una de las máquinas que haya seleccionado.
Si Rapid Recovery detecta cualquier problema durante la verificación automática, el asistente procede a una página de Advertencias, donde podrá borrar las máquinas que seleccione y comprobar manualmente las máquinas seleccionadas. Si las máquinas que ha agregado pasan la comprobación automática, aparecerán en el panel Implementar Agent en máquinas.
- Si se muestra la página Warning (Advertencia), pero aún está satisfecho con sus elecciones, haga clic en **Finish (Finalizar)** nuevamente.

El software del Agent de Rapid Recovery se implemente en las máquinas especificadas. Las máquinas todavía no estén protegidas. Para proteger las máquinas, consulte el tema "Protección de varias máquinas en el dominio de Active Directory" en la *Guía de usuario de Rapid Recovery 6.0 en dispositivos DL*.

Implementación en máquinas en host virtual VMware vCenter/ESX(i)

Utilice este procedimiento para implementar simultáneamente el software del Agent de Rapid Recovery en una o más máquinas en host virtual VMware vCenter/ESX(i).

Antes de iniciar este procedimiento, debe tener la siguiente información:

- Las credenciales de inicio de sesión del host virtual VMware vCenter/ESX(i).
- Ubicación del host.
- Las credenciales de inicio de sesión para cada uno de las máquinas que desee proteger.

NOTA: Todas las máquinas virtuales deben tener VMware Tools (Herramientas de VM) instaladas; de lo contrario, Rapid Recovery no podrá detectar el nombre del host de la máquina virtual en la que realizará la implementación. En lugar del nombre del host, Rapid Recovery usa el nombre de la máquina virtual, lo que puede provocar problemas si el nombre del host no coincide con el nombre de la máquina virtual.

- En la Core Console de Rapid Recovery, haga clic en el menú desplegable **Protect (Proteger)** After installation, restart the machine automatically (recommended) y, haga clic en **Deploy Agent Software (Implementar el software del Agent)**.
Se abre el **Deploy Agent Software Wizard (Asistente de implementación del software del Agent)**.
- En la página **Conexión** del asistente, seleccione **vCenter / ESX(i)** de la lista desplegable **Origen**.
- Introduzca la información del host y las credenciales de inicio de sesión como se describe en la tabla siguiente.

Tabla 5. VCenter/ESX(i) configuración de conexión

Cuadro de texto	Descripción
Host	Escriba el nombre o la dirección IP del host virtual de VMware vCenter Server/ESX(i).
Puerto	El puerto utilizado para conectarse al host virtual.

Cuadro de texto	Descripción
	El valor predeterminado es 443.
Nombre de usuario	El nombre de usuario utilizado para conectarse a la máquina virtual; por ejemplo, Administrador o, si la máquina está en un dominio, [nombre de dominio]\Administrador.
Contraseña	Introduzca la contraseña segura que utiliza para conectarse al host virtual.

- 4 Haga clic en **Siguiente**.
 - 5 En la página **Máquinas** del asistente, Seleccione una de las siguientes opciones en el menú desplegable:
 - Hosts y clústeres
 - Máquinas virtuales y plantillas
 - 6 Expanda la lista de máquinas y, a continuación, seleccione las máquinas virtuales en las que desea implementar el software. Aparece una notificación si Rapid Recovery detecta que una máquina está fuera de línea o que las herramientas de VMware no están instaladas.
 - 7 Si desea reiniciar las máquinas automáticamente después de la implementación, seleccione **After Agent installation, restart the machines automatically (Recommended) (Reiniciar la máquina automáticamente tras la instalación [recomendado])**.
 - 8 Haga clic en **Siguiente**.
Rapid Recovery comprueba de forma automática cada una de las máquinas que haya seleccionado.
 - 9 En la página **Ajustes** del asistente, escriba las credenciales de cada máquina en el siguiente formato:
hostname: :username: :password.
- NOTA:** Introduzca una máquina en cada línea.
- 10 Haga clic en **Finalizar**.
El sistema comprueba de forma automática cada una de las máquinas que haya seleccionado.
Si Rapid Recovery detecta cualquier problema durante la verificación automática, el asistente procede a una página de Advertencias, donde podrá borrar las máquinas que seleccione y comprobar manualmente las máquinas seleccionadas. Si las máquinas que ha agregado pasan la comprobación automática, aparecerán en el panel Implementar Agent en máquinas.
 - 11 Si se muestra la página Warning (Advertencia), pero aún está satisfecho con sus elecciones, haga clic en **Finish (Finalizar)** nuevamente.

El software del Agent de Rapid Recovery implementa se implementa en las máquinas especificadas.

Acerca de cómo instalar el software del Agent en máquinas con Linux

Al instalar el software del Agent en máquinas con Linux que desea proteger, siga las siguientes instrucciones. Una vez completada la instalación, configure el Agent como se describe en el tema "Configuración del Agent de Rapid Recovery en una máquina con Linux" en *Protección de datos de Dell | Guía de instalación y mejora de Rapid Recovery 6.0*.

PRECAUCIÓN: Después de configurar el software del Agent en la máquina con Linux, reinicie la máquina. Al reiniciar se garantiza que se utiliza la versión adecuada del controlador de núcleo para proteger la máquina.

El método para la instalación y extracción el software del Agent en máquinas con Linux ha cambiado. A partir de la versión 6.0.1, se aplican los siguientes factores:

- Un conjunto de instrucciones se aplica a las instalaciones del Agent en máquinas con Linux con acceso a Internet en el momento. Esto se conoce como instalación en línea. En lugar de utilizar secuencias de comandos de shell, se utilizan administradores para instalar o quitar el software Rapid Recovery desde un repositorio local al que se hace referencia en la máquina con Linux.

NOTA: El repositorio se utiliza para organizar por etapas los archivos para los administradores de paquetes relevantes. Este repositorio no está relacionado con el repositorio de Rapid Recovery.

- Si va a instalar un Agent en una máquina con Linux sin acceso a Internet (como, por ejemplo, una máquina de aire con una separación segura o máquina independiente), esto se conoce como instalación fuera de línea. Para este proceso, primero debe descargar un paquete de instalación desde una máquina con Linux con acceso a Internet y, a continuación, traslade los archivos de instalación al equipo protegido para realizar la instalación.

Debido a que las distintas distribuciones de Linux compatibles utilizan otros administradores de paquetes para la instalación en línea, el procedimiento para instalar, actualizar o eliminar el Agent en cualquier sistema operativo Linux admitido depende del administrador de paquetes que utiliza. Los administradores de paquetes y las distribuciones de Linux que admiten se describen en la siguiente tabla.

Tabla 6. Administradores de paquetes y distribuciones de Linux admitidos

Administrador de paquetes	Distribución de Linux
YUM	Distribuciones de Linux basadas en Red Hat Enterprise Linux (RHEL), incluyendo RHEL, CentOS y Oracle Linux.
zypper	SUSE Linux Enterprise Server (SLES) versiones 11, 12
apt	Distribuciones de Linux basada en Debian, incluyendo Debian 7 u 8 y Ubuntu 12.04 y posteriores

Al ser una configuración de un solo paso para cada máquina con Linux, debe configurar su almacén local de software para indicar la ubicación donde el administrador de paquetes obtendrá los archivos de instalación de Dell Rapid Recovery.

NOTA: Este proceso se representa mediante los pasos del 1 al 4 en cada uno de los procedimientos de instalación. Al actualizar las ediciones futuras del Agent de Rapid Recovery en una máquina con Linux con el repositorio configurado, no necesitará realizar estos pasos.

Después de configurar un repositorio de software en la máquina con Linux, el administrador de paquetes podrá descargar e instalar los paquetes necesarios para la instalación o extracción del software del Agent de Rapid Recovery y los componentes relacionados, como por ejemplo, aamount (ahora denominada local mount), aavdisk (ahora denominado rapidrecovery-vdisk), y Mono (un conjunto de herramientas de fuente abierta, que cumple con el estándar Ecma, compatible con .NET Framework que se utiliza para portar el software del Agent en las plataformas Linux).

Para cada administrador de paquetes, puede ejecutar el comando adecuado en la línea de comandos para determinar si está configurado para descargar los paquetes de Rapid Recovery. Estos comandos se enumeran en la tabla siguiente.

Tabla 7. Comando para mostrar la configuración del repositorio del administrador de paquetes

Administrador de paquetes	Comando para generar una lista de repositorios configurados
YUM	Lista de repositorios YUM
zypper	Lista de repositorios zypper
apt	Lista de repositorios apt

Las versiones anteriores del software del Agent de AppAssure se deben eliminar completamente de las máquinas con Linux antes de instalar la versión del Agent de Rapid Recovery y proteger la máquina con Linux mediante el Core de Rapid Recovery. Esto se aplica a las instalaciones en línea o fuera de línea. Para eliminar el Agent de AppAssure se emplean secuencias de comandos de shell. Las instrucciones de desinstalación varían según la distribución de Linux que esté utilizando. Para obtener más información acerca de la desinstalación del Agent de AppAssure desde una máquina con Linux, consulte el tema "Desinstalación del software del Agent de AppAssure desde una máquina con Linux" en la *Protección de datos de Dell | Guía de instalación y mejora de Rapid Recovery 6.0*.

NOTA: Para extraer el nuevo software del agent de Rapid Recovery se emplea el administrador de paquetes para cada distribución. Por lo tanto, si desinstala una versión del Agent de Rapid Recovery, consulte el procedimiento correspondiente en el tema "Desinstalación del software del Agent de AppAssure desde una máquina con Linux" en la *Protección de datos de Dell | Guía de instalación y mejora de Rapid Recovery 6.0*.

Si instala el Agent de Rapid Recovery en una máquina con Linux en que nunca se ha instalado un Agent de AppAssure, determine el paquete adecuado manager desde la tabla anterior. A continuación, siga el procedimiento de instalación que corresponde.

Después de configurar el software del Agent en la máquina con Linux, reinicie la máquina. Al reiniciar se garantiza que se utiliza la versión adecuada del controlador de núcleo para proteger la máquina.

Por lo tanto, el proceso de instalación al actualizar de AppAssure a Rapid Recovery implica:

- Extracción del software del Agent de AppAssure (no es necesario para las primeras instalaciones)
- Determinar el administrador de paquetes relevante para su distribución de Linux
- Seguir el procedimiento de instalación del Agent de Rapid Recovery en la máquina con Linux, incluyendo el repositorio del software (pasos 1 al 4 del procedimiento de instalación)
- Ejecute la utilidad de configuración para configurar el puerto, configurar usuarios, agregar exclusiones del servidor de seguridad, instalar el módulo de kernel e iniciar el servicio del Agent.
- Reinicie la máquina con Linux

Las instrucciones para instalar el software del Agent en una máquina con Linux varían ligeramente según de la distribución de Linux que esté utilizando. Para obtener más información sobre la preparación para instalar el software del Agent y para una máquina con Linux conectada a Internet, consulte el tema correspondiente. Puede elegir entre las siguientes secciones:

- [Instalación del software del Agent de Rapid Recovery en Debian o Ubuntu](#)
- [Instalación del software del Agent de Rapid Recovery en SUSE Linux Enterprise Server](#)

Para obtener más información sobre la preparación para instalar el software del Agent en una máquina con Linux que no está conectada a Internet, consulte el tema:

- [Instalación del software del Agent en máquinas con Linux fuera de línea](#)

Antes de comenzar la instalación del software del Agent, consulte los temas: Descargar la distribución de Linux, Acerca de la seguridad, Ubicación de los archivos del Agent de Linux, Dependencias del Agent, Información de las secuencias de comandos de Linux en *Protección de datos de Dell | Guía de instalación y mejora de Rapid Recovery 6.0*.

Ubicación de los archivos del Agent de Linux

Se necesitan varios archivos para que un equipo con Linux admita el software Rapid Recovery Agent. En todas las distribuciones de Linux compatibles, estos archivos se encuentran en los directorios siguientes:

- mono:
`/opt/apprecovery/mono`
- agent:
`/opt/apprecovery/agent`
- montaje local:
`/opt/apprecovery/local_mount`
- rapidrecovery-vdisk y aavdctl:
`/usr/bin/aavdisk`
- archivos de configuración para rapidrecovery-vdisk:
`/etc/apprecovery/aavdisk.conf`
- contenedor adicional para agent y local_mount
`/usr/bin/agent`
`/usr/bin/local_mount`
- secuencias de comandos de ejecución automática para agent y rapidrecovery-vdisk:
`/etc/init.d/rapidrecovery-agent`
`/etc/init.d/rapidrecovery-vdisk`

Dependencias del Agent

Las siguientes dependencias son necesarias y se instalan como parte del paquete del instalador del Agent:

- Para Debian y Ubuntu:
 - El Agent de Rapid Recovery requiere:
`dkms, gcc, make, linux-headers-`uname-r`
libc6 (>=2.7-18), libblkid1, libpam0g, libpcre3`
 - El mono de Rapid Recovery requiere:
`libc6 (>=2.7-18)`
- Para Red Hat Enterprise Linux, CentOS y Oracle Linux:
 - El nbd-dkms requiere
`dkms, gcc, make, kernel-headers-`uname-r` kernel-devel-`uname-r``
 - El Agent de Rapid Recovery requiere:
`dkms, gcc, make, kernel-headers-`uname-r` kernel-devel-`uname-r`,
nbd-dkms, libblkid, pam, pcre`
 - El mono de Rapid Recovery requiere:
`glibc >=2.11`
- Para SUSE Linux Enterprise Server:
 - El nbd-dkms requiere:
`dkms, gcc, make, kernel-syms`
 - El Agent de Rapid Recovery requiere:
`dkms, kernel-syms, gcc, make, libblkid1, pam, pcre`
 - El mono de Rapid Recovery requiere:
`glibc >= 2.11`

Instalación del software del Agent de Rapid Recovery en Debian o Ubuntu

El archivo .deb del Agent de Rapid Recovery es un archivo que contiene información específica para el administrador del paquete apt. Realice los siguientes pasos para instalar el Agent de Rapid Recovery en máquinas con Debian o Ubuntu en línea.

NOTA: Este procedimiento aplica a máquinas con Linux conectadas a Internet. Si desea llevar a cabo una instalación del Agent de Rapid Recovery fuera de línea en cualquier máquina con Linux, consulte [Instalación del software del Agent en máquinas con Linux fuera de línea](#).

- 1 Abra una sesión de terminal con acceso a la raíz.
- 2 Para determinar el directorio de trabajo actual, escriba `PWD` y presione la tecla **Intro**. Por ejemplo, supongamos que su directorio es `/home/rapidrecovery/`.
- 3 Descargue el archivo de instalación .deb del Agent de Rapid Recovery que corresponda en el Portal de licencias en <https://licenseportal.com> en su directorio de trabajo actual.
Para obtener más información acerca del Portal de licencias, consulte *Dell Data Protection | Portal de licencias de Rapid Recovery Guía de usuario*.
- 4 Para establecer una conexión duradera entre la máquina con Linux y el repositorio Dell remoto en el que se almacenan componentes y el software de Rapid Recovery, escriba el siguiente comando:

```
dpkg -i <.deb installation file you downloaded>
```

Por ejemplo, si el archivo del instalador se llama `rapidrecovery-repo 6.0.2.999.deb` en el directorio `/home/rapidrecovery/`, escriba el comando siguiente y, a continuación, presione **Intro**:

```
dpkg -i rapidrecovery-repo-6.0.2.999.deb
```

Los paquetes y archivos que faltan o que el Agent requiera se pueden descargar en el repositorio remoto y se pueden instalar automáticamente como parte de la secuencia de comandos.

NOTA: Para obtener más información sobre los requisitos de la instalación en máquinas con Linux, consulte [Dependencias del Agent](#).

- 5 Instale el Agent de Rapid Recovery invocando el administrador de paquetes `apt`, actualizando el administrador de repositorios. Escriba el siguiente comando y, a continuación, presione **Intro**:

```
apt-get update
```

- 6 Indíquelo al administrador de paquetes que instale software del Agent de Rapid Recovery . Escriba el siguiente comando y, a continuación, presione **Intro**:

```
apt-get install rapidrecovery-agent
```

- 7 El administrador de paquetes se prepara para instalar todos los archivos dependientes. Si se le solicita que confirme la instalación de archivos sin firmar, introduzca **y**, a continuación, pulse **Intro**.

Se instalan los archivos del Agent de Rapid Recovery.

Instalación del software del Agent de Rapid Recovery en SUSE Linux Enterprise Server

El archivo `.rpm` del Agent de Rapid Recovery contiene información del repositorio para SUSE Linux Enterprise Server (SLES). Esta distribución utiliza el administrador de paquetes `zypper`. Siga los siguientes pasos para instalar el Agent de Rapid Recovery en SLES.

NOTA: Este procedimiento aplica a máquinas con Linux conectadas a Internet. Si desea llevar a cabo una instalación del Agent de Rapid Recovery fuera de línea en cualquier máquina con Linux, consulte [Instalación del software del Agent en máquinas con Linux fuera de línea](#).

- 1 Abra una sesión de terminal con acceso a la raíz.
- 2 Para determinar el directorio de trabajo actual, escriba `PWD` y presione la tecla **Intro**. Por ejemplo, supongamos que su directorio es `/home/rapidrecovery/`.
- 3 Descargue el archivo de instalación `.rpm` del Agent de Rapid Recovery que corresponda en el Portal de licencias en <https://licenseportal.com> en su directorio de trabajo actual.
Para obtener más información acerca del Portal de licencias, consulte *Dell Data Protection | Portal de licencias de Rapid Recovery Guía de usuario*.
- 4 Para establecer una conexión duradera entre la máquina con Linux y el repositorio Dell remoto en el que se almacenan componentes y el software de Rapid Recovery, escriba el siguiente comando:

```
rpm -ivh <.rpm installation file you downloaded>
```

Por ejemplo, si el archivo del instalador se llama `rapidrecovery-repo 6.0.2.999.rpm` en el directorio `/home/rapidrecovery/`, escriba el comando siguiente y, a continuación, presione **Intro**:

```
rpm -ivh rapidrecovery-repo-6.0.2.999.rpm
```

Los paquetes y archivos que faltan o que el Agent requiera se pueden descargar en el repositorio remoto y se pueden instalar automáticamente como parte de la secuencia de comandos.

NOTA: Para obtener más información sobre los requisitos de la instalación en máquinas con Linux, consulte [Dependencias del Agent](#).

- 5 Instale el Agent de Rapid Recovery invocando el administrador de paquetes zypper, actualizando el administrador de repositorios. Escriba el siguiente comando y, a continuación, presione **Intro**:


```
apt-get update
```
- 6 Indíquelo al administrador de paquetes que instale software del Agent de Rapid Recovery . Escriba el siguiente comando y, a continuación, presione **Intro**:


```
apt-get install rapidrecovery-agent
```
- 7 El administrador de paquetes se prepara para instalar todos los archivos dependientes. Si se le solicita que confirme la instalación de archivos sin firmar, introduzca **y**, a continuación, pulse **Intro**.
Se instalan los archivos del Agent de Rapid Recovery.

Instalación del Agent en Red Hat Enterprise Linux y CentOS

① NOTA: Antes de realizar estos pasos, asegúrese de haber descargado el paquete del instalador Red Hat or CentOS en el /home/system directory. Los pasos siguientes son los mismos para los entornos de 32 bits y 64 bits.

Para instalar un Agent en Red Hat Enterprise Linux y CentOS:

- 1 Abra una sesión de terminal con acceso a la raíz.
- 2 Para hacer ejecutable el instalador del Agent, escriba el siguiente comando:
`chmod +x appassure-installer__rhel_amd64_5.x.x.xxxxx.sh` y, a continuación, presione <Intro>.

① NOTA: Para entornos de 32 bits, el instalador se llama `appassureinstaller__rhel_i386_5.x.x.xxxxx.sh`

El archivo se hace ejecutable.

- 3 Para extraer e instalar el Agent, escriba el siguiente comando:
`/appassure-installer__rhel_amd64_5.x.x.xxxxx.sh` y, a continuación, presione <Intro>.

El Agent de Linux inicia el proceso de extracción e instalación. Los paquetes y archivos que faltan solicitados por el Agent se descargan e instalan automáticamente como parte de la secuencia de comandos.

Para obtener información sobre los archivos que el Agent necesita, consulte [Dependencias del Agent](#).

Después de que termine el instalador, el agent se ejecutará en la máquina. Para obtener más información sobre cómo proteger esta máquina con el Core, consulte la sección "Cómo proteger estaciones de trabajo y servidores" en la *Guía de usuario de Rapid Recovery 6.0 en dispositivos DLen* Dell.com/support/home.

Instalación del software del Agent en máquinas con Linux fuera de línea

Para realizar esta tarea, se requiere acceso a una máquina con Linux en línea, a medios de almacenamiento extraíbles, y acceso a la máquina con Linux final. Si el Agent de AppAssure está instalado en la máquina con Linux fuera de línea, primero desinstálelo antes de instalar el Agent de Rapid Recovery. Para obtener más información, consulte la sección "Desinstalación del software del Agent de AppAssure Agent en máquinas con Linux" en *Protección de datos de Dell | Guía de instalación y mejora de Rapid Recovery*.

Al instalar el software del Agent en máquinas con Linux que no tienen acceso a Internet, siga este procedimiento. Una vez completada la instalación, configure el Agent como se describe en el tema [Configuración del Agent de Rapid Recovery en una máquina con Linux](#).

① NOTA: Si se realiza la instalación en varias distribuciones de Linux, siga este procedimiento una vez para cada distribución.

- 1 En una máquina con Linux con acceso a Internet, abra una ventana de terminal y escriba el siguiente comando:
`wget http://s3.amazonaws.com/repolinux/6.0.2/packages-downloader.sh`

La secuencia de comandos de shell descarga en el directorio actual.

- 2 Ejecute la secuencia de comandos de shell. Para ello, ejecute el siguiente comando:

```
bash packages-downloader.sh
```

La secuencia de comandos se ejecuta y le solicita que seleccione una distribución de Linux específica y la arquitectura.

- 3 Escriba el índice del paquete de instalación que desea ver y presione **Intro**.

Por ejemplo, para obtener un paquete de instalación para Red Hat Enterprise Linux 7, escriba 3 y presione **Intro**.

El instalador que corresponde se extrae en el directorio `~/rapidrecovery.packages/`.

NOTA: Los caracteres de tilde `~/` representan el directorio de inicio.

- 4 Copie los paquetes del Agent de Rapid Recovery de medios extraíbles. La ubicación específica de los medios extraíbles pueden variar según la distribución de Linux. Escriba el siguiente comando y, a continuación, pulse **Intro**:

```
cp -R ~/rapidrecovery.packages/ <your_removable_media>
```

Por ejemplo, si utiliza una unidad USB extraíble que está montada en ubicación `/medio/unidad USB-1`, escriba el siguiente comando y, a continuación, presione **Intro**:

```
cp -R ~/rapidrecovery.packages /media/USB-drive-1
```

Todos los archivos necesarios se copian en el medio extraíble.

- 5 Retire el soporte extraíble, introdúzcalo en la máquina con Linux fuera de línea y monte la unidad.

- 6 Copie los datos del dispositivo montado en el directorio de inicio o en otra ubicación que desee. Por ejemplo, escriba el siguiente comando y, a continuación, presione **Intro**:

```
cp -R /media/USB-drive-1 ~/rapidrecovery.packages
```

- 7 Cambie al directorio de Rapid Recovery. Por ejemplo, escriba el siguiente comando y, a continuación, presione **Intro**:

```
cd ~/rapidrecovery.packages
```

- 8 Ejecute la instalación del Agent con privilegios de raíz. Este comando varía en función de la distribución de Linux.

- Para Red Hat, SLES, Oracle, y CentOS, escriba el siguiente comando y, a continuación, presione **Intro**:

```
sudo rpm -i *.rpm
```

- Para Debian y Ubuntu, escriba el siguiente comando y, a continuación, pulse **Intro**:

```
sudo dpkg -i *.deb
```

El administrador de paquetes local ejecuta la instalación del Agent de Rapid Recovery.

Una vez completada la instalación, configure el Agent como se describe en el tema [Configuración del Agent de Rapid Recovery en una máquina con Linux](#).

PRECAUCIÓN: Después de configurar el software del Agent en la máquina con Linux, reinicie la máquina. Al reiniciar se garantiza que se utiliza la versión adecuada del controlador de núcleo para proteger la máquina.

Instalación del software del Agent en máquinas con Windows con Server Core

Siga los pasos del siguiente procedimiento para instalar el software del Agent en una máquina con Windows con Server Core.

NOTA: El siguiente procedimiento es para instalar el software del Agent en modo de consola. Si desea instalarlo en modo silencioso, añada `/silent` al nombre del archivo de instalación en la línea de comandos. Por ejemplo, `Agent-X64-6.X.X.xxxxx.exe /silent`.

- 1 Descargue el archivo de instalación del Agent de Rapid Recovery en Dell Data Protection | Portal de licencias de Rapid Recovery o desde el Core de Rapid Recovery.
- 2 Desde el símbolo del sistema, vaya al directorio que contiene el archivo de instalación del Agent de Rapid Recovery e introduzca el nombre del archivo de instalación para comenzar la instalación:

```
Agent-X64-6.x.x.xxxxx.exe
```

El programa de instalación instala el software del Agent y muestra el progreso en la consola. Tras finalizar, las nuevas instalaciones reinician automáticamente la máquina. Es posible que las mejoras del Agent no requieran reiniciar la máquina.

Configuración del Agent de Rapid Recovery en una máquina con Linux

Ejecute la utilidad de configuración de Rapid Recovery después de instalar el software del Agent en una máquina con Linux. Este compila e instala el módulo de kernel en la máquina con Linux que desea proteger en su Core.

La utilidad de configuración ofrece varias opciones de configuración, y proporciona los pasos numerados en las sugerencias de las instrucciones cuando detecta la información de configuración específica.

Complete los pasos a continuación para configurar el software del Agent de Rapid Recovery en cualquier máquina con Linux. Algunas opciones de configuración varían en función de la distribución de Linux que está instalando.

- 1 Abra una sesión de terminal con acceso a la raíz.
- 2 Inicie la utilidad de configuración; para ello, escriba el comando siguiente y, a continuación, presione Intro:

```
sudo /usr/bin/rapidrecovery-config
```

La utilidad de configuración se inicia. Este comando enumera varias opciones de configuración, cada uno con un número de índice que introducir para el paso de configuración que corresponda.

- 3 Configure el puerto de esta máquina protegida; para ello, escriba el comando siguiente y, a continuación, presione Intro. El puerto predeterminado es 8006.

```
1 <agent_port>
```

Por ejemplo, si utiliza el puerto predeterminado, escriba el comando:

```
1 8006
```

- 4 Configure usuarios disponibles para protección, escribiendo el siguiente comando y, a continuación, presione Intro:

```
1 <user_names_separated_by_comma>
```

Por ejemplo, si el nombre de usuario es michael, administrador y test_user1, escriba el comando:

```
2 michael,administrator,test_user1
```

- 5 Configure reglas de servidor de seguridad para seleccionar un administrador de configuración de servidor de seguridad. Esta acción establece las excepciones del servidor de seguridad para el puerto indicadas en el paso 1.

Si la utilidad detecta uno o más administradores de configuración del servidor de seguridad (como lokkit o firewalld), aparecerán en la utilidad en la línea 3. Seleccione el administrador de configuración que corresponda y entre en él, empezando por el número de comando (3), y, a continuación, presione Intro:

```
3 <firewall_configuration>
```

Por ejemplo, si usa firewalld, escriba el comando:

```
3 firewalld
```

- 6 Consulte la lista de módulos de núcleo compatible con la utilidad; para ello, escriba el número de comando y, a continuación, presione Intro:

4

Un subshell hace que todos los módulos de núcleo sean compatibles para la instalación. Por ejemplo, el siguiente se podría devolver:

```
Searching for all available for installation kernels.
This might take a while, depending on the Internet connection speed.
Kernels compatible for module installation:
 0 - linux-image-3.16.0.23-generic
 1 - linux-image-3.16.0.31-generic
 2 - linux-image-3.16.0.33-generic
 3 - linux-image-3.16.0.34-generic
Input indices of the kernel modules you wish to install, delimited by space; use 'all' to
install into all supported kernels, or 'q' to quit.
```

- 7 Configure el módulo de kernel de Rapid Recovery que corresponda.

Por ejemplo, para introducir módulos de núcleo para 3.16.0-23 y 3.16.0-34, introduzca 1 4 y presione Intro.

Para introducir todos los módulos de kernel, introdúzcalos a11 y presione Intro.

- 8 Después de configurar el software del Agent, reinicie la máquina. Al reiniciar se garantiza que se utiliza la versión adecuada del controlador de núcleo para proteger la máquina.

Después de completar este proceso, el repositorio local se ha configurado en esta máquina con Linux. El software del Agent esdtá instalado y el módulo de kernel está cargado.

El siguiente paso es para proteger la máquina en el Core de Rapid Recovery.

Cómo proteger una máquina

Si ya tiene instalado el software del Agent de Rapid Recovery en la máquina que desea proteger, pero no lo ha reiniciado aún, primero reinicie la máquina.

En este tema se describe cómo iniciar la protección de los datos en una sola máquina que especifique mediante el Asistente de protección de la máquina.

Cuando agrega protección, tiene que definir la información de conexión, como la dirección IP y el puerto, y proporcionar las credenciales de la máquina que desea proteger. De manera opcional, puede proporcionar un nombre de visualización para que aparezca en la Core Console en lugar de la dirección IP. Si lo cambia, no se mostrará la dirección IP de la máquina protegida cuando vea los detalles en la Core Console. También puede definir la programación de la protección de la máquina.

El flujo de trabajo del asistente de protección puede variar ligeramente en función de su entorno. Por ejemplo, si el software del Agent de Rapid Recovery está instalado en la máquina que desea proteger, no se le solicitará que lo instale desde el asistente. Asimismo, si ya existe un repositorio en el Core, no se le solicitará que cree uno nuevo.

- 1 Realice uno de los siguientes pasos:

- Si inicia en el Asistente de protección de la máquina, continúe con el paso 2.
- Si inicia desde la Core Console de Rapid Recovery, haga clic en **Protect (Proteger)** en la barra de botones.

Se abrirá el **Protect Machine Wizard (Asistente de protección de la máquina)**.

- 2 En la página **Welcome (Bienvenida)**, seleccione las opciones de instalación adecuadas:

- Si no necesita definir un repositorio o establecer el cifrado, seleccione **Typical (Típica)**.
- Si necesita crear un repositorio o definir un repositorio diferente para las copias de seguridad de la máquina seleccionada, o si desea establecer el cifrado con el asistente, seleccione **Advanced (show optional steps) (Avanzado [mostrar pasos opcionales])**.
- Si no desea ver la página **Welcome (Bienvenida)** del Asistente de protección de la máquina en el futuro, seleccione la opción **Omitir esta página de bienvenida la próxima vez que el asistente se abra**.

- 3 Cuando esté satisfecho con las opciones en la página de bienvenida, haga clic en **Siguiente**.

Aparecerá la página **Connection (Conexión)**.

- 4 En la página **Connection (Conexión)**, introduzca la información sobre la máquina a la que desea conectarse tal como se describe en la tabla y, a continuación, haga clic en **Nextiguiente**.

Tabla 8. Configuración de la conexión de la máquina

Cuadro de texto	Descripción
Host	El nombre de host o la dirección IP de la máquina que desea proteger.
Puerto	El número de puerto con el que se comunica el Core de Rapid Recovery con el Agent de la máquina. El número de puerto predeterminado es 8006.
Nombre de usuario	El nombre de usuario que utiliza para conectarse a esta máquina; por ejemplo, Administrador (o, si la máquina está en un dominio, [nombre del dominio] \Administrador).
Contraseña	La contraseña que se utiliza para conectar a esa máquina.

Si la página **Install Agent (Instalar Agent)** se abre a continuación en el Asistente de protección de la máquina, indica que Rapid Recovery no detecta el Agent de Rapid Recovery en la máquina e instalará la versión actual del software. Vaya al paso 7.

Si la página **Upgrade Agent (Actualizar Agent)** se abre a continuación en el asistente, indica que existe una versión antigua del software del Agent en la máquina que desea proteger.

NOTA: El software del Agent debe estar instalado en la máquina que desea proteger. Asimismo, la máquina se debe reiniciar para poder crear copias de seguridad en el Core. Para que el instalador reinicie la máquina protegida, seleccione la opción **After installation, restart the machine automatically (recommended)** (Reiniciar la máquina automáticamente tras la instalación [recomendado]) antes de hacer clic en **Next (Siguiente)**.

- 5 En la página **Upgrade Agent (Actualizar Agent)**, realice una de las acciones siguientes:
 - Para implementar la nueva versión del software del Agent (coincidente con la versión del Core de Rapid Recovery), seleccione **Upgrade the Agent to the latest version of the software (Actualizar el Agent para descargar la última versión del software)**.
 - Para continuar protegiendo la máquina sin que se actualice la versión del software del Agent, desactive la opción **Actualizar el Agent a la versión más reciente del software**.
- 6 Haga clic en **Siguiente**.
- 7 De manera opcional, en la página **Protection (Protección)**, si desea que la dirección IP se muestre con un nombre distinto en la Core Console de Rapid Recovery en esta máquina protegida, escriba un nombre en el cuadro de diálogo del campo **Display Name (Nombre)**.
Puede introducir hasta 64 caracteres. No utilice caracteres especiales mencionados en el tema "Caracteres no permitidos" en la *Guía de usuario de Rapid Recovery en dispositivos DL*. Asimismo, asegúrese de que el nombre no comience con ninguna de las combinaciones de caracteres mencionadas en el tema de frases prohibidas en la *Guía de usuario de Rapid Recovery en dispositivos DL*.
- 8 Seleccione la programación de protección que corresponda como se describe a continuación:
 - Para usar la programación de protección predeterminada, en la opción Configuración de programación, seleccione **Protección predeterminada**.

Con una programación de protección predeterminada, el Core capturará instantáneas de todos los volúmenes en la máquina protegida una vez por hora. Para cambiar la configuración de la protección en cualquier momento después de cerrar el asistente, incluida la elección de los volúmenes que se van a proteger, vaya a la página Resumen de la máquina protegida específica.

- Para definir otra programación de protección, en la opción Configuración de programación, seleccione **Custom protection (Protección personalizada)**.
- 9 Continúe con la configuración de la manera siguiente:
 - Si seleccionó una configuración típica del Asistente de protección de la máquina y ha especificado la protección predeterminada, haga clic en **Finish (Finalizar)** para confirmar la selección, cierra el asistente y proteger la máquina especificado.
La primera vez que se agrega protección a un equipo, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio Core de Rapid Recovery de acuerdo con la programación definida, salvo que haya especificado pausar la protección inicialmente.

- Si seleccionó una configuración típica para el Asistente de protección de la máquina y especificó una protección personalizada, haga clic en **Next (Siguiente)** para configurar una programación de protección personalizada. Para obtener más información sobre cómo definir una programación de protección personalizada, consulte "Creación de programas de protección personalizadas" en la *Guía de usuario de Rapid Recovery 6.0 en dispositivos DL*.
 - Si seleccionó la Configuración avanzada para el Asistente de protección de la máquina, haga clic en **Siguiente** y proceda al paso 14 para ver las opciones de repositorio y cifrado.
 - Si seleccionó la Configuración avanzada para el Asistente de protección de la máquina, haga clic en **Siguiente** y proceda al paso 11 para elegir los volúmenes que desea proteger.
- 10 En la página **Protection Volumes (Protección de volúmenes)**, seleccione los volúmenes que desea proteger. Si en la lista se incluye algún volumen que no desea proteger, haga clic en la columna de verificación para deseccionarla. A continuación, haga clic en **Siguiente**.

NOTA: Típicamente, se recomienda proteger, al menos, el volumen **System Reserved (Reservado para el sistema)** y el **volumen con el sistema operativo (por lo general, la unidad C)**.

- 11 En la página **Programación de protección**, defina una programación personalizada y, a continuación, haga clic en **Siguiente**. Para obtener más información sobre cómo definir una programación de protección personalizada, consulte "Creación de programaciones de protección personalizadas" en la *Guía de usuario de Rapid Recovery 6.0 en dispositivos DL*.
- Si ya ha configurado la información del repositorio y seleccionó la Opción avanzada en el paso 1, aparecerá la página Cifrado. Proceda al paso 13.
- 12 De manera opcional, en la página **Cifrado**, seleccione **Activar el cifrado** para activar el cifrado. Aparecerán los campos de clave de cifrado en la página **Encryption (Cifrado)**.

NOTA: Si activa el cifrado, se aplicará a los datos de todos los volúmenes protegidos de esta máquina. Puede cambiar la configuración del cifrado posteriormente en la Core Console de Rapid Recovery. Para obtener más información sobre el cifrado, consulte el tema "Descripción las claves de cifrado" en la *Guía de usuario de Rapid Recovery 6.0 en dispositivos DL* en www.dell.com/support/home.

PRECAUCIÓN: Rapid Recovery utiliza cifrado AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) con claves de 256 bits. Aunque el uso de cifrado es opcional, Dell recomienda encarecidamente que establezca una clave de cifrado y que proteja la frase de contraseña que defina. Guarde la frase de contraseña en un lugar seguro, ya que es fundamental para la recuperación de datos. Sin una frase de contraseña, la recuperación de datos no es posible.

- 13 En la página **Cifrado**, seleccione una de las siguientes opciones:
- Si desea cifrar esta máquina protegida y mediante una clave de cifrado que ya está definido en este Core de Rapid Recovery, seleccione **Cifrar los datos mediante una clave de cifrado existente** y, a continuación, seleccione la clave apropiada en el menú desplegable. Continúe con el paso siguiente.
 - Si desea agregar una nueva clave de cifrado para el Core y aplicar dicha clave de esta máquina protegida, introduzca la información según se describe en la tabla siguiente.

Tabla 9. Configuración de la clave de cifrado

Cuadro de texto	Descripción
Nombre	Introduzca un nombre para la clave de cifrado. Los nombres clave de cifrado debe contener entre 1 y 130 caracteres alfanuméricos. No se podrá incluir caracteres especiales como barra diagonal inversa, barra diagonal, canalización, dos puntos, asterisco, comilla, signo de interrogación, paréntesis y corchetes abiertos o cerrados, & gato. Esta información se muestra en el campo Descripción al ver las claves de cifrado desde la Core Console.
Descripción	Escriba un comentario para la clave de cifrado. Esta información se muestra en el campo Descripción al ver las claves de cifrado desde la Core Console.
Passphrase	Introduzca la frase de contraseña usada para controlar el acceso. Se recomienda evitar el uso de caracteres especiales mencionados anteriormente.

Cuadro de texto	Descripción
	Guarde la frase de contraseña en un lugar seguro. La Asistencia de Dell no puede recuperar una frase de contraseña. Una vez que haya creado una clave de cifrado y la haya aplicado a una o más máquinas protegidas, no podrá recuperar los datos si pierde la frase de contraseña.
Confirm Passphrase	Vuelva a introducir la frase de contraseña que acaba de introducir.

- 14 Haga clic en **Finish (Finalizar)** para guardar y aplicar la configuración.
- La primera vez que se agrega protección a un equipo, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio Core de Rapid Recovery de acuerdo con la programación definida, salvo que haya especificado pausar la protección inicialmente.
- 15 Si recibe un mensaje de error, el appliance no podrá conectarse al sistema para hacer una copia de seguridad. Para resolver el problema haga lo siguiente:
- Compruebe la conectividad de red.
 - Compruebe la configuración del servidor de seguridad.
 - Compruebe que los Servicios de Rapid Recovery y RPC se están ejecutando.
 - Compruebe las búsquedas de servicios de nombres de dominio (si aplica).

Comprobación de la conectividad de red

Para comprobar la conectividad de red:

- En el sistema del cliente al que está intentando conectarse, abra una interfaz de línea de comandos.
- Ejecute el comando **ipconfig** y anote la dirección IP del cliente.
- Abra una interfaz de línea de comandos en el appliance.
- Ejecute el comando **ping <IP address of client>**.
- Según el resultado, realice una de las siguientes opciones:
 - Si el cliente no responde al ping, compruebe la conectividad del servidor y la configuración de red.
 - Si el cliente responde, compruebe que la configuración del servidor de seguridad permita que se ejecuten los componentes de DL1000.

Comprobación de la configuración del firewall

Si el cliente está conectado correctamente a la red, pero la consola Core no lo puede ver, compruebe el servidor de seguridad para garantizar que están permitidas las comunicaciones entrantes y salientes necesarias.

Para comprobar la configuración del servidor de seguridad en Core y cualquier cliente del que hace una copia de seguridad:

- En el appliance DL1000, haga clic en **Inicio > Panel de control**.
- En el **Panel de control**, haga clic en **Sistema y seguridad** y bajo **Firewall de Windows** haga clic en **Comprobar estado del firewall**.
- Haga clic en **Configuración avanzada**.
- En la pantalla **Firewall de Windows con seguridad avanzada**, haga clic en **Reglas de entrada**.
- Asegúrese de que el Core y los puertos muestran **Yes (Sí)** en la columna **Enabled (Habilitado)**.
- Si la regla no está habilitada, haga doble clic en Core y seleccione **Enable Rule (Habilitar regla)**.
- Haga clic en **Outbound Rules (Reglas de salida)** y compruebe lo mismo para Core.

Comprobación de la resolución de DNS

Si la máquina de la que está intentando hacer una copia de seguridad utiliza DNS, compruebe que las búsquedas hacia adelante e inversas de DNS son correctas.

Para asegurarse de que las búsquedas inversas son correctas:

- 1 En el appliance, vaya a los hosts en `C:\Windows\system32\drivers\etc`.
- 2 Introduzca la dirección IP de cada cliente que hace una copia de seguridad para DL1000.

Formación de equipos de adaptadores de red

De manera predeterminada, los adaptadores de red (NIC) en el appliance DL1000 no están conectados, lo que afecta al rendimiento del sistema. Se recomienda que agrupe las NIC a una sola interfaz. La formación de equipos NIC necesita la:

- Reinstalación de Broadcom Advanced Control Suite
- Creación del equipo NIC

Reinstalación de Broadcom Advanced Configuration Suite

Para reinstalar Broadcom Advanced Configuration Suite:

- 1 Vaya a `C:\Install\BroadcomAdvanced` y haga doble clic en **setup**. Aparecerá el **InstallShield Wizard (Asistente de InstallShield)**.
- 2 Haga clic en **Next (Siguiente)**.
- 3 Haga clic en **Modify, Add, or Remove (Modificar, agregar o quitar)**. Se muestra la pantalla **Custom Setup (Instalación personalizada)**.
- 4 Haga clic en **CIM Provider (Proveedor de CIM)** y, a continuación, seleccione **This feature will be installed on local hard drive (Esta función se instalará en una unidad de disco duro local)**.
- 5 Haga clic en **BASP** y, a continuación, seleccione **This feature will be installed on local hard drive (Esta función se instalará en una unidad de disco duro local)**.
- 6 Haga clic en **Next (Siguiente)**.
- 7 Haga clic en **Install (Instalar)**.
- 8 Haga clic en **Finish (Finalizar)**.

Creación del equipo NIC

NOTA: Nota: se recomienda no utilizar la interfaz de formación de equipos nativa en Windows 2012 Server. El algoritmo de formación de equipos está optimizado para tráfico de salida y no de entrada. Ofrece un rendimiento malo con una carga de trabajo de copia de seguridad, incluso con más puertos de red en el equipo.

Para crear un equipo NIC:

- 1 Vaya a **Start (Inicio) > Search (Búsqueda) > Broadcom Advanced Control Suite**.
NOTA: Al utilizar **Broadcom Advanced Control Suite**, solo seleccione las tarjetas de red **Broadcom**.
- 2 En el **Broadcom Advanced Control Suite**, seleccione **Teams (Equipos) > Go to Team View (Ir a vista de equipo)**.
- 3 En la **Hosts list (Lista de hosts)** en el lado izquierdo, haga clic con el botón derecho del mouse en el nombre de host del appliance DL1000 y seleccione **Create Team (Crear equipo)**. Se muestra la ventana **Broadcom Teaming Wizard (Asistente para la formación de grupos de Broadcom)**.
- 4 Haga clic en **Next (Siguiente)**.
- 5 Introduzca un nombre para el equipo y haga clic en **Next (Siguiente)**.
- 6 Seleccione el **Team Type (Tipo de equipo)** y haga clic en **Next (Siguiente)**.
- 7 Seleccione el adaptador que desea que sea parte del equipo y haga clic en **Add (Agregar)**.
- 8 Repita estos pasos para los otros adaptadores que son parte del equipo.
- 9 Cuando todos los adaptadores están seleccionados en el equipo, haga clic en **Next (Siguiente)**.

- 10 Seleccione una NIC en espera si desea que una NIC se utilice de manera predeterminada en caso de que el equipo falle.
- 11 Seleccione si desea configurar **LiveLink** y, a continuación, haga clic en **Next (Siguiendo)**.
- 12 Seleccione **Skip Manage VLAN (Omitir Administrar VLAN)** y haga clic en **Next (Siguiendo)**.
- 13 Seleccione **Commit changes to system (Confirmar cambios en el sistema)** y haga clic en **Finish (Finalizar)**.
- 14 Haga clic en **Yes (Sí)** cuando se le avise de que la conexión de red se ha interrumpido.

 **NOTA:** La creación del equipo NIC puede tardar aproximadamente cinco minutos.

Obtención de ayuda

Búsqueda de documentación y actualizaciones de software

Hay enlaces directos a Rapid Recovery la documentación y a las actualizaciones de software del dispositivo DL1000 desde la Core Console.

Documentación

Para acceder al enlace de la documentación:

- 1 En la Core Console, haga clic en la pestaña **Appliance**.
- 2 En el panel de la izquierda, navegue al enlace **Appliance > Documentation**(Appliance> Documentación) .

Actualizaciones de software

Para acceder al enlace de las actualizaciones de software:

- 1 En la Core Console, haga clic en la pestaña **Appliance**.
- 2 En el panel de la izquierda, navegue al enlace **Appliance > Software Updates**(Appliance > Actualizaciones de software).

Cómo ponerse en contacto con Dell

① **NOTA: Si no dispone de una conexión a Internet activa, puede encontrar información de contacto en la factura de compra, en el albarán o en el catálogo de productos de Dell.**

Dell proporciona varias opciones de servicio y asistencia en línea y por teléfono. Si no tiene una conexión a Internet activa, puede encontrar información de contacto en su factura de compra, en su albarán de entrega, en su recibo o en el catálogo de productos Dell. La disponibilidad varía según el país y el producto y es posible que algunos de los servicios no estén disponibles en su área. Para ponerse en contacto con Dell por cuestiones relacionadas con ventas, asistencia técnica o atención al cliente, vaya a **software.dell.com/support**.

Comentarios sobre la documentación

Haga clic en el enlace **Feedback (Comentarios)** en cualquiera de las páginas de documentación de Dell, rellene el formulario y haga clic en **Submit (Enviar)** para enviar sus comentarios.