

Appliance Dell DL1000

Guía del usuario



Notas, precauciones y avisos

-  **NOTA:** Una NOTA proporciona información importante que le ayuda a utilizar mejor su equipo.
-  **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.

Copyright © 2015 Dell Inc. Todos los derechos reservados. Este producto está protegido por las 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 puede ser marcas comerciales de sus respectivas empresas.

2015 - 12

Rev. A01

Tabla de contenido

| | |
|---|-----------|
| 1 Introducción a Dell DL1000..... | 7 |
| Tecnologías centrales de Dell DL1000..... | 7 |
| Live Recovery..... | 7 |
| Universal Recovery..... | 7 |
| Desduplicación global real | 8 |
| Cifrado..... | 8 |
| Funciones de protección de datos de Dell DL1000..... | 8 |
| Dell DL1000 Core..... | 8 |
| Dell DL1000 Smart Agent..... | 9 |
| Proceso de instantáneas..... | 9 |
| Replicación: sitio de recuperación tras desastres o proveedor de servicio..... | 9 |
| Recuperación..... | 10 |
| Recuperación como servicio (RaaS) | 10 |
| Virtualización y nube..... | 10 |
| Arquitectura de implementación de Dell DL1000..... | 11 |
| Otra información útil..... | 12 |
| 2 Trabajar con DL1000..... | 14 |
| Acceso a la DL1000 Core Console..... | 14 |
| Actualización de los sitios de confianza en Internet Explorer..... | 14 |
| Configuración de exploradores para acceder de manera remota a Core Console..... | 14 |
| Administración de licencias | 15 |
| Cambio de una clave de licencia | 16 |
| Cómo ponerse en contacto con el servidor del portal de licencias | 16 |
| Cambio del idioma de AppAssure manualmente..... | 16 |
| Cambio del idioma del SO durante la instalación..... | 17 |
| Administración de la configuración del Core | 17 |
| Cómo cambiar el nombre de visualización del Core | 18 |
| Cambio de la hora de los trabajos nocturnos | 18 |
| Modificación de la configuración de la cola de transferencias | 18 |
| Ajuste de la configuración del tiempo de espera del cliente | 19 |
| Configuración de los valores de caché de la desduplicación | 19 |
| Modificación de la configuración del motor | 20 |
| Modificación de la configuración de la implementación | 20 |
| Modificación de la configuración de la conexión con la base de datos | 21 |
| Administración de eventos | 21 |
| Configuración de grupos de notificación | 22 |
| Configuración de un servidor de correo electrónico..... | 23 |

| | |
|--|----|
| Configuración de una plantilla de notificaciones de correo electrónico | 24 |
| Configuración de la reducción de repeticiones | 25 |
| Configuración de la retención de eventos | 26 |
| Administración de repositorios | 26 |
| Visualización de los detalles de un repositorio..... | 26 |
| Comprobación de un repositorio | 26 |
| Administración de la seguridad | 27 |
| Cómo agregar una clave de cifrado | 27 |
| Edición de una clave de cifrado | 28 |
| Cómo cambiar la frase de contraseña de la clave de cifrado | 28 |
| Importación de una clave de cifrado | 28 |
| Exportación de una clave de cifrado | 29 |
| Eliminación de una clave de cifrado | 29 |
| Administración de cuentas de servicios en la nube | 29 |
| Cómo agregar una cuenta de servicios en la nube..... | 29 |
| Edición de una cuenta de servicios en la nube..... | 31 |
| Configuración de los valores de la cuenta de servicios en la nube..... | 31 |
| Eliminación de una cuenta en la nube..... | 32 |
| Supervisión de DL1000 | 32 |
| Actualización de DL1000..... | 32 |
| Reparación de DL1000..... | 32 |
| Recuperación automática rápida del appliance (RASR)..... | 33 |

3 Protección de estaciones de trabajo y servidores..... 35

| | |
|---|----|
| Acerca de la protección de estaciones de trabajo y servidores | 35 |
| Implementación de un Agent (Instalación de inserción) | 35 |
| Cómo proteger una máquina | 36 |
| Cómo pausar y reanudar la protección | 38 |
| Implementación del software del Agent al proteger un agente..... | 39 |
| Comprensión de los programas de protección | 40 |
| Creación de programas personalizados..... | 41 |
| Modificación de los programas de protección | 41 |
| Configuración de los valores de la máquina protegida | 43 |
| Visualización y modificación de los valores de configuración | 43 |
| Visualización de la información del sistema de una máquina | 43 |
| Visualización de la información de la licencia | 44 |
| Modificación de la configuración de las transferencias | 44 |
| Archivado de datos..... | 47 |
| Creación de un archivo | 47 |
| Importación de un archivo | 50 |
| Archivado en una nube..... | 51 |
| Visualización de los diagnósticos del sistema | 51 |

| | |
|---|-----------|
| Visualización de los registros de la máquina | 51 |
| Carga de los registros de la máquina..... | 52 |
| Cancelación de operaciones en una máquina | 52 |
| Visualización del estado de la máquina y otros detalles | 52 |
| Administración de varias máquinas | 53 |
| Implementación en varias máquinas | 54 |
| Supervisión de la implementación de varias máquinas | 54 |
| Protección de varias máquinas..... | 54 |
| Supervisión de la protección de varias máquinas | 56 |
| 4 Datos de recuperación..... | 57 |
| Administración de la recuperación | 57 |
| Administración de instantáneas y puntos de recuperación | 57 |
| Visualización de puntos de recuperación | 57 |
| Visualización de un punto de recuperación específico..... | 58 |
| Montaje de un punto de recuperación para una máquina Windows | 59 |
| Desmontaje de puntos de recuperación seleccionados | 60 |
| Desmontaje de todos los puntos de recuperación | 60 |
| Montaje de un punto de recuperación para una máquina Linux | 60 |
| Eliminación de puntos de recuperación | 61 |
| Eliminación de una cadena de puntos de recuperación huérfanos..... | 61 |
| Cómo forzar una instantánea | 62 |
| Restablecimiento de datos | 62 |
| Acerca de la exportación de datos protegidos de máquinas de Windows a máquinas virtuales..... | 63 |
| Administración de exportaciones..... | 64 |
| Exportación de información de copia de seguridad de una máquina Windows a una máquina virtual | 65 |
| Exportación de datos de Windows mediante exportación ESXi | 65 |
| Exportación de datos de Windows mediante una exportación VMware Workstation | 68 |
| Exportación de datos de Windows mediante exportación Hyper-V | 71 |
| Exportación de datos de Windows mediante exportación de VirtualBox de Oracle | 74 |
| Restauración de volúmenes desde un punto de recuperación | 76 |
| Restauración de volúmenes para una máquina Linux mediante la línea de comandos | 80 |
| Cómo iniciar la restauración desde cero para máquinas Windows | 81 |
| Plan para realizar una restauración desde cero para una máquina Windows | 82 |
| Cómo iniciar una restauración desde cero para una máquina Linux | 87 |
| Instalación de la utilidad de pantalla..... | 88 |
| Creación de particiones de inicio en una máquina Linux..... | 89 |
| 5 Replicación de puntos de recuperación..... | 90 |
| Replicación..... | 90 |

| | |
|--|------------|
| Plan para realizar la replicación | 91 |
| Replicación a un Core administrado automáticamente..... | 91 |
| Replicación a un Core administrado por un tercero..... | 95 |
| Replicación de un Agent nuevo | 96 |
| Replicación de los datos de Agent en una máquina | 97 |
| Configuración de la prioridad de replicación para un Agent | 98 |
| Supervisión de la replicación | 98 |
| Administración de configuraciones de replicación | 99 |
| Eliminación de replicación | 100 |
| Extracción de una máquina protegida de la replicación en el Core de origen..... | 100 |
| Extracción de una máquina protegida en el Core de destino..... | 100 |
| Eliminación de un Core de destino de la replicación..... | 101 |
| Eliminación de un Core de origen de la replicación..... | 101 |
| Recuperación de datos replicados | 101 |
| Comprensión de la conmutación por error y la conmutación por recuperación | 102 |
| Cómo realizar una conmutación por error | 102 |
| Cómo realizar una conmutación por recuperación | 103 |
| 6 Emisión de informes..... | 105 |
| Acerca de los informes | 105 |
| Acerca de la barra de herramientas de informes | 105 |
| Acerca de los informes de cumplimiento | 105 |
| Acerca de los informes de errores | 106 |
| Acerca del informe de resumen del Core | 106 |
| Resumen de repositorios | 106 |
| Resumen de Agents | 107 |
| Cómo generar un informe para un Core o Agent | 107 |
| Acerca de los informes de Core de la Central Management Console (Consola de administración central) | 108 |
| Cómo generar un informe desde la Central Management Console (Consola de administración central) | 108 |
| 7 Obtención de ayuda..... | 109 |
| Búsqueda de documentación y actualizaciones de software..... | 109 |
| Documentación..... | 109 |
| Actualizaciones de software..... | 109 |
| Cómo ponerse en contacto con Dell..... | 109 |
| Comentarios sobre la documentación..... | 109 |

Introducción a Dell DL1000

Dell DL1000 combina funciones de copia de seguridad y replicación en un producto unificado de protección de datos. 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 petabytes 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 (DR) y cumplimiento.

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

Tecnologías centrales de Dell DL1000

El servidor combina las siguientes tecnologías:

- [Live Recovery](#)
- [Universal Recovery](#)
- [Desduplicación global real](#)
- [Cifrado](#)

Live Recovery

Live Recovery 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.

Universal Recovery

Universal Recovery 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 Universal Recovery 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 las máquinas 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 instantáneas de volumen de Microsoft (VSS) para detener y desactivar el vaciado de los datos de aplicación en un disco a fin de 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 AppAssure y su transmisión a otro Core de AppAssure 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, Universal Recovery, o Live Recovery.

Recuperación como servicio (RaaS)

Los Managed Service Providers (Proveedores de servicios administrados - MSP) pueden aprovechar todas las ventajas de 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 AppAssure. 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 multi-inquilino. Los proveedores de servicios administrados (MSP) pueden utilizar el DL1000 en múltiples sitios y crear un entorno multi-inquilino en su extremo.

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 Dell 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 (Portal de licencias) de Dell administra los usuarios, grupos y suscripciones de licencia para los Agents y Cores de su entorno. El License Portal (Portal de licencias) permite que los usuarios inicien la sesión, activen las cuentas, descarguen software e implementen Agents y Cores conforme a la licencia para su entorno.

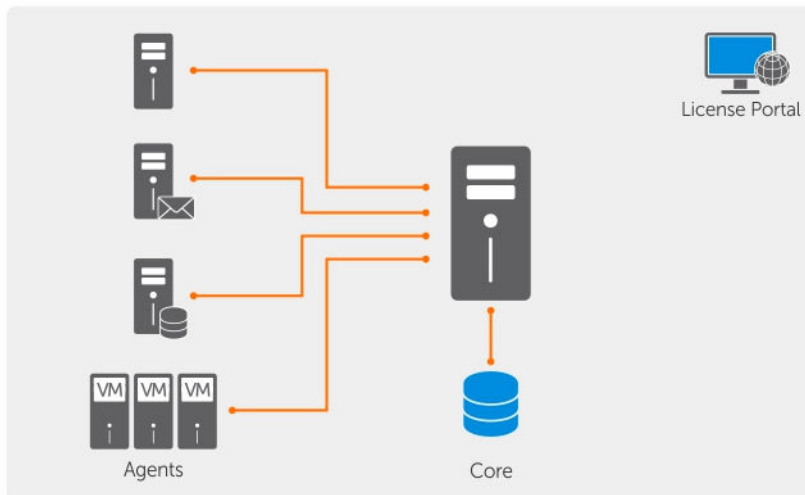


Ilustración 2. Arquitectura de implementación de Dell DL1000

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

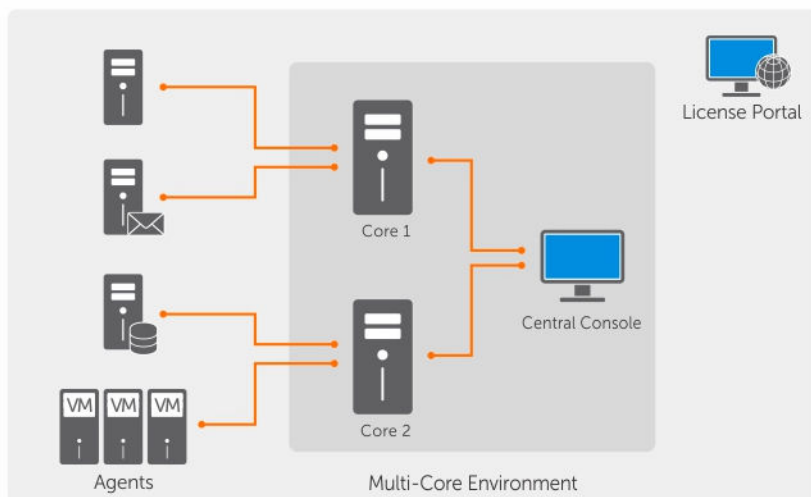


Ilustración 3. Arquitectura de implementación de varios Cores de DL1000

Otra información útil

- ✍ **NOTA:** Para todos los documentos Dell OpenManage, vaya a dell.com/openmanagemanuals.
- ✍ **NOTA:** Compruebe si hay actualizaciones en dell.com/support/home y, si las hay, léalas antes de proceder a la instalación, 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:

| | |
|--|--|
| Getting Started Guide (Guía de introducción) | Proporciona una descripción general de las características del sistema, 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 solución AppAssure. |
| Owner's Manual (Guía del propietario) | Proporciona información sobre las características del sistema y describe cómo solucionar problemas del sistema e instalar o sustituir los componentes del sistema. |
| Deployment Guide (Guía de implementación) | Proporciona información sobre la implementación del hardware y la implementación inicial del appliance AppAssure. |
| User's Guide (Guía del usuario) | Proporciona información sobre la configuración y administración del sistema. |

| | |
|--|--|
| Release Notes (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 DL1000 así como las reglas, recomendaciones y consideraciones de uso. |
| OpenManage Server Administrator User's Guide (Guía del usuario OpenManage Server Administrator) | Proporciona información sobre el uso de Dell OpenManage Server Administrator para administrar su sistema. |
| Soporte de recursos | En el soporte suministrado con el sistema se incluye documentación y herramientas para configurar y administrar el sistema. Esto incluye aquellas relacionadas con el sistema operativo, el software de administración del sistema, las actualizaciones del sistema y los componentes del sistema adquiridos con él. |

Trabajar con DL1000

Acceso a la DL1000 Core Console

Para acceder a DL1000 Core Console:

1. Actualice los sitios de confianza en el explorador.
2. Configure los exploradores para acceder de forma remota a DL1000 Core Console. Consulte [Configuración de exploradores para acceder de manera remota a Core Console](#).
3. Realice una de las siguientes acciones para acceder a DL1000 Core Console:
 - Inicie sesión localmente en el servidor DL1000 Core y, a continuación, haga doble clic en el icono de **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)**.

Configuración de exploradores para acceder de manera remota a Core Console

Para acceder a la Core Console desde una máquina remota, primero debe modificar la configuración del explorador.

 **NOTA:** Para modificar la configuración del explorador, inicie sesión en el sistema como administrador.

 **NOTA:** Google Chrome utiliza la configuración de Microsoft Internet Explorer: deberá utilizar Internet Explorer para cambiar los valores de configuración del explorador Chrome.

 **NOTA:** Cuando acceda a la consola web de Core, de manera local o remota, asegúrese de que esté activada **Internet Explorer Enhanced Security Configuration (Configuración de seguridad mejorada de Internet Explorer)**. Para activar la **Internet Explorer Enhanced Security Configuration (Configuración de seguridad mejorada de Internet Explorer)**:

1. Abra el **Server Manager (Administrador de servidores)**
2. Seleccione **Local Server IE Enhanced Security Configuration (Configuración de seguridad mejorada de Internet Explorer en servidor local)**, que se muestra a la derecha. Compruebe que está en **On (Activada)**.

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

1. Abra Internet Explorer.
2. En el menú **Tools (Herramientas)**, seleccione las fichas **Internet Options (Opciones de Internet)**, **Security (Seguridad)**.
3. Haga clic en **Trusted Sites (Sitios de confianza)** y, a continuación, haga clic en **Sites (Sitios)**.
4. Deseleccione la opción **Require server verification (https:) for all sites in the zone (Requerir comprobación del servidor (https:) para todos los sitios de esta zona)** y, a continuación, añada `http://<nombre del host o dirección IP del servidor del appliance que aloja AppAssure Core>` a **Trusted Sites (Sitios de confianza)**.
5. Haga clic en **Close (Cerrar)**, seleccione **Trusted Sites (Sitios de confianza)** y, después, haga clic en **Custom Level (Nivel personalizado)**.
6. Desplácese hasta **Miscellaneous (Miscelánea)** → **Display Mixed Content (Mostrar contenido mixto)** y seleccione **Enable (Habilitar)**.
7. 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)**.
8. Haga clic en **OK (Aceptar)** y, después, seleccione la pestaña **Advanced (Opciones avanzadas)**.
9. Vaya hasta **Multimedia** y seleccione **Play animations in webpages (Reproducir animaciones en páginas web)**.
10. Desplácese hasta **Security (Seguridad)**, active la opción **Enable Integrated Windows Authentication (Habilitar autenticación integrada de Windows)** y, a continuación, haga clic en **OK (Aceptar)**.

Para modificar la configuración del explorador Mozilla 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 AppAssure Core; por ejemplo, *dirección IP,nombre del host*.
4. Reinicie Firefox.

Administración de licencias

Puede administrar sus licencias DL1000 directamente desde la Core Console. Desde la consola, puede cambiar la clave de licencia y ponerse en contacto con el servidor de licencias. Desde la página **Licensing**

(Licencias) de la Core Console, también puede acceder a Dell AppAssure License Portal (Portal de licencias).

La página **Licensing (Licencias)** incluye la información siguiente:

- License type (Tipo de licencia)
- License status (Estado de licencia)
- Number of machines protected (Número de máquinas protegidas)
- Status of last response from the licensing server (Estado de la última respuesta desde el servidor de licencias)
- Time of last contact with the licensing server (Hora del último contacto con el servidor de licencias)
- Next scheduled attempt of contact with the licensing server (Siguiendo intento programado para el contacto con el servidor de licencias)
- Restricciones de la licencia

Cambio de una clave de licencia

Para cambiar una clave de licencia:

1. Navegue a la Core Console y seleccione **Configuration (Configuración)** → **Licensing (Licencias)**. Se muestra la página **Licensing (Licencias)**.
2. En la página **License Details (Detalles de la licencia)**, haga clic en **Change (Cambiar)**. Se muestra el cuadro de diálogo **Change License Key (Cambiar clave de licencia)**.
3. En el cuadro de diálogo **Change License Key (Cambiar clave de licencia)**, introduzca la nueva clave de licencia y haga clic en **OK (Aceptar)**.

Cómo ponerse en contacto con el servidor del portal de licencias

La Core Console se pone en contacto con el servidor de portal para actualizar los cambios realizados en el portal de licencias. La comunicación con el servidor del portal tiene lugar de forma automática, en los intervalos establecidos; no obstante puede iniciar la comunicación bajo demanda.

Para establecer contacto con el servidor del portal:

1. Navegue a la Core Console y, a continuación, haga clic en **Configuration (Configuración)** → **Licensing (Licencias)**. Se muestra la página **Licensing (Licencias)**.
2. En la opción **License Server (Servidor de licencias)**, haga clic en **Contact Now (Establecer contacto ahora)**.

Cambio del idioma de AppAssure manualmente

AppAssure le permite cambiar el idioma que ha seleccionado mientras se ejecuta el AppAssure Appliance Configuration Wizard (Asistente de configuración del appliance AppAssure) a uno de los idiomas compatibles.

Para cambiar el idioma de AppAssure al idioma que desee:


1. Inicie el editor del registro mediante el comando `regdit`.
2. Vaya a **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **AppRecovery** → **Core** → **Localization (Localización)**.
3. Abra **Lcid**.
4. Seleccione **decimal**.
5. Introduzca el valor del idioma requerido en la casilla `Datos de valor`, los valores de idioma admitidos son:


- a. Inglés: 1033
 - b. Portugués brasileño: 1046
 - c. Español: 1034
 - d. Francés: 1036
 - e. Alemán: 1031
 - f. Chino simplificado: 2052
 - g. Japonés: 1041
 - h. Coreano: 1042
6. Haga clic con el botón derecho del mouse y reinicie los servicios en el orden indicado:
 - a. Instrumental de administración de Windows
 - b. Servicio web SRM
 - c. AppAssure Core
 7. Borre la caché del explorador.
 8. Cierre el explorador y reinicie la Core Console desde el icono del escritorio.

Cambio del idioma del SO durante la instalación

En una instalación que ejecute Windows, puede usar el panel de control para seleccionar los paquetes de idiomas y configurar valores adicionales internacionales.

Para cambiar el idioma del SO:

 **NOTA:** Se recomienda que el idioma del SO y el idioma de AppAssure sea el mismo idioma. De lo contrario, es posible que aparezcan algunos mensajes sobre idiomas distintos.

 **NOTA:** Se recomienda cambiar el idioma del SO antes de cambiar el idioma de AppAssure.


1. En la página **Start (Inicio)**, escriba el idioma, y asegúrese de que el ámbito de búsqueda se establece en la configuración.
2. En el panel **Results (Resultados)**, seleccione **Language (Idioma)**.
3. En el panel **Change your language preferences (Cambiar sus preferencias de idioma)**, seleccione **Add a language (Agregar un idioma)**.
4. Examine o busque el idioma que desea instalar.
Por ejemplo, seleccione Catalán y, a continuación, seleccione Add (Agregar). Ahora, Catalán se agrega como uno de los idiomas.
5. En el panel Change your language preferences (Cambiar sus preferencias de idioma), seleccione **Options (Opciones)** junto al idioma que ha agregado.
6. Si un paquete de idiomas está disponible para su idioma, seleccione Download and install language pack (Descargar e instalar paquete de idiomas).
7. Cuando el paquete de idiomas está instalado, el idioma se muestra como disponible para su uso para el idioma de visualización de Windows.
8. Para hacer que este idioma sea el idioma de visualización, muévelo hacia la parte superior de su lista de idiomas.
9. Cierre la sesión y vuelva a iniciar sesión en Windows para que el cambio surta efecto.

Administración de la configuración del Core

La configuración del Core se utiliza para definir diversos valores de configuración y rendimiento. La mayoría de los valores se configuran para un uso óptimo, pero puede cambiar los siguientes valores según sea necesario:

- General
- Nightly Jobs (Trabajos nocturnos)
- Transfer Queue (Cola de transferencias)
- Client Timeout Settings (Configuración del tiempo de espera del cliente)
- Deduplication Cache Configuration (Configuración de la caché de deduplicación)
- Database Connection Settings (Configuración de conexión de base de datos)

Cómo cambiar el nombre de visualización del Core

 **NOTA:** Se recomienda seleccionar un nombre de visualización permanente durante la configuración inicial del dispositivo. Si lo cambia posteriormente, deberá realizar algunos pasos manualmente para asegurarse de que el nuevo nombre de host surta efecto y el servidor funcione correctamente.

Para cambiar el nombre de visualización del Core:

1. Navegue a la Core Console y haga clic en **Configuration** → **Settings (Valores de configuración)**.
2. En la sección **General (General)**, haga clic en **Change (Cambiar)**.
Aparecerá el cuadro de diálogo **Display Name (Nombre de visualización)**.
3. En el cuadro de texto **Display Name (Nombre de visualización)**, introduzca el nuevo nombre de visualización para el Core.
4. Haga clic en **OK (Aceptar)**.

Cambio de la hora de los trabajos nocturnos

La opción Nightly Job (Trabajos nocturnos) planifica tareas como resumen, conectividad y truncamiento de los Agents protegidos por el Core.

Para ajustar la hora de los trabajos nocturnos:

1. Navegue a la Core Console y seleccione **Configuration** → **Settings (Valores de configuración)**.
2. En la sección **Nightly Jobs (Trabajos nocturnos)**, haga clic en **Change (Cambiar)**.
Aparecerá el cuadro de diálogo **Nightly Jobs (Trabajos nocturnos)**.
3. En el cuadro de texto **Nightly Jobs Time (Hora de los trabajos nocturnos)**, introduzca la nueva hora de inicio.
4. Haga clic en **OK (Aceptar)**.

Modificación de la configuración de la cola de transferencias

La configuración de la cola de transferencias consiste en valores del nivel de Core que definen el número máximo de transferencias simultáneas y reintentos para los datos que se van a transferir.

Para modificar la configuración de la cola de transferencias:

1. Navegue a la Core Console y haga clic en **Configuration** → **Settings (Valores de configuración)**.
2. En la sección **Transfer Queue (Cola de transferencias)**, haga clic en **Change (Cambiar)**.
Aparecerá el cuadro de diálogo **Transfer Queue (Cola de transferencias)**.
3. En el cuadro de texto **Maximum Concurrent Transfers (Número máximo de transferencias simultáneas)**, introduzca un valor para actualizar el número de transferencias simultáneas.
Escriba un número entre 1 y 60. Cuanto más pequeño sea el número, menor será la carga en la red y en otros recursos del sistema. A medida que aumente la capacidad que se procesa, también aumentará la carga en el sistema.

4. En el cuadro de texto **Maximum Retries (Número máximo de reintentos)**, introduzca un valor para actualizar el número máximo de reintento.
5. Haga clic en **OK (Aceptar)**.

Ajuste de la configuración del tiempo de espera del cliente

La opción Client Timeout Settings (Configuración del tiempo de espera del cliente) especifica el número de segundos o minutos que debe esperar el servidor antes de que se agote el tiempo de espera cuando se conecta a un cliente.

Para ajustar la configuración del tiempo de espera del cliente:

1. Vaya a la Core Console y, a continuación, haga clic en **Configuration → Settings (Valores de configuración)**.
2. En la sección **Client Timeout Settings Configuration (Configuración de los valores del tiempo de espera del cliente)**, haga clic en **Change (Cambiar)**.
Se abrirá el cuadro de diálogo **Client Timeout Settings (Configuración del tiempo de espera del cliente)**.
3. En el cuadro de texto **Connection Timeout (Tiempo de espera de la conexión)**, introduzca el número de minutos y segundos que transcurrirán antes de que se agote el tiempo de espera de la conexión.
4. En el cuadro de texto **Read/Write Timeout (Tiempo de espera de lectura/escritura)**, introduzca el número de minutos y segundos que desea que transcurran antes de que se agote el tiempo de espera durante un evento de lectura/escritura.
5. Haga clic en **OK (Aceptar)**.

Configuración de los valores de caché de la deduplicación

La deduplicación global reduce la cantidad de espacio de almacenamiento en disco necesario para los datos de la copia de seguridad. Deduplication Volume Manager (DVM) combina un conjunto de ubicaciones de almacenamiento en un único repositorio. La caché de deduplicación mantiene las referencias a bloques exclusivos. De manera predeterminada, la caché de la deduplicación es de 1,5 GB. Si la cantidad de información redundante es tan grande que la caché de deduplicación se llena, el repositorio ya no puede aprovechar todas las ventajas de la deduplicación en todo el repositorio para los datos que se agreguen posteriormente. En ese caso, puede aumentar el tamaño de la caché de deduplicación con la modificación de su configuración en la Core Console.

Para configurar los valores de caché de la deduplicación:

1. Navegue a la Core Console y haga clic en **Configuration → Settings (Valores de configuración)**.
2. En la sección **Deduplication Cache Configuration (Configuración de la caché de deduplicación)**, haga clic en **Change (Cambiar)**.
Aparecerá el cuadro de diálogo **Deduplication Cache Configuration (Configuración de la caché de deduplicación)**.
3. En el cuadro de texto **Primary Cache Location (Ubicación de la caché primaria)**, especifique la ubicación actualizada.
4. En el cuadro de texto **Secondary Cache Location (Ubicación de la caché secundaria)**, especifique la ubicación actualizada.
5. En el cuadro de texto **Metadata Cache Location (Ubicación de la caché de metadatos)**, especifique la ubicación de la caché de metadatos actualizada.
6. Haga clic en **OK (Aceptar)**.



NOTA: Debe reiniciar el servicio del Core para que los cambios surjan efecto.

Modificación de la configuración del motor

Para modificar la configuración del motor:

1. Navegue a la Core Console y haga clic en **Configuration** → **Settings (Valores de configuración)**.
2. En la sección **Replay Engine Configuration (Configuración de Replay Engine)**, haga clic en **Change (Cambiar)**.

Aparecerá el cuadro de diálogo **Replay Engine Configuration (Configuración del motor de reproducción)**.

3. En el cuadro de diálogo **Replay Engine Configuration (Configuración de Replay Engine)**, especifique la **dirección IP**. Elija una de las siguientes opciones:
 - Para usar la dirección IP preferente de TCP/IP, haga clic en **Automatically Determined (Determinado automáticamente)**.
 - Para introducir manualmente una dirección IP, haga clic en **Use a specific IP Address (Utilizar una dirección IP específica)**.
4. Introduzca la información de configuración, según se describe a continuación:

| Cuadro de texto | Descripción |
|---------------------------------|---|
| Preferable Port | Introduzca un número de puerto o acepte el valor predeterminado (el puerto predeterminado es 8007). El puerto se utiliza para especificar el canal de comunicación del motor. |
| Admin Group | Introduzca un nombre nuevo para el grupo de administración. El nombre predeterminado es BUILTIN\Administrators . |
| Minimum Async I/O Length | Introduzca un valor o seleccione el valor predeterminado. Describe la longitud de entrada/salida asíncrona mínima. El valor predeterminado es 65536. |
| Receive Buffer Size | Especifique un tamaño de búfer de entrada o acepte el valor predeterminado. El valor predeterminado es 8192. |
| Send Buffer Size | Especifique un tamaño de búfer de salida o acepte el valor predeterminado. El valor predeterminado es 8192. |
| Read Timeout | Introduzca un valor de tiempo de espera de lectura o elija el valor predeterminado. Este es 00:00:30. |
| Write Timeout | Introduzca un valor de tiempo de espera de escritura o elija el valor predeterminado. Este es 00:00:30. |

5. Seleccione **No Delay (Sin retrasos)**.
6. Haga clic en **OK (Aceptar)**.

Modificación de la configuración de la implementación

Para modificar la implementación de las configuraciones:

1. Vaya a la Core Console y haga clic en la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Settings (Valores de configuración)**.
2. En el panel **Deploy Settings (Implementar configuración)**, haga clic en **Change (Cambiar)**. Se abrirá el cuadro de diálogo **Deploy Settings (Implementar configuración)**.

3. En el cuadro de texto **Agent Installer Name (Nombre de Agent Installer)**, escriba el nombre del archivo ejecutable del agente. El predeterminado es **Agentweb.exe**.
4. En el cuadro de texto **Core Address (Dirección de Core)**, escriba la dirección del Core.
5. En el cuadro de texto **Failed Receive Timeout (Tiempo de espera de error de recepción)**, especifique el número de minutos que se debe esperar sin actividad para agotar el tiempo de espera.
6. En el cuadro de texto **Max Parallel Installs (Máx. instalaciones en paralelo)**, especifique un número para el máximo de instalaciones en paralelo que pueden realizarse.
7. Seleccione uno o ambos de los valores de configuración opcionales siguientes.
 - Automatic reboot after install (Reinicio automático después de la instalación)
 - Protect After Deploy (Proteger tras implementar)
8. Haga clic en **OK (Aceptar)**.

Modificación de la configuración de la conexión con la base de datos

Para modificar la configuración de la conexión con la base de datos:

1. Navegue a la Core Console y haga clic en **Configuration → Settings (Valores de configuración)**.
2. En la sección **Database Connection Settings (Configuración de la conexión de la base de datos)**, realice una de las acciones siguientes:
 - Para restaurar la configuración predeterminada, haga clic en **Restore Default (Restaurar valores predeterminados)**.
 - Para modificar la configuración de conexión de la base de datos, haga clic en **Change (Cambiar)**.

Al hacer clic en esa opción, se abrirá el cuadro de diálogo **Database Connection Settings (Configuración de la conexión de la base de datos)**.

3. Introduzca la configuración para modificar la conexión con la base de datos como se describe a continuación:

| Cuadro de texto | Descripción |
|---|--|
| Host Name | Introduzca un nombre de host para la conexión de la base de datos. |
| Port | Especifique un número de puerto para la conexión de la base de datos. |
| User Name (optional) | Introduzca un nombre de usuario para acceder y administrar la configuración de conexión de la base de datos. Se utiliza para especificar las credenciales de inicio de sesión para acceder a la conexión con la base de datos. |
| Password (optional) | Introduzca una contraseña para acceder y administrar la configuración de conexión de la base de datos. |
| Retain event and job history for, days | Introduzca el número de días que se conservará el historial de eventos y trabajos de la conexión de la base de datos. |

4. Haga clic en **Test Connection (Probar conexión)** para verificar la configuración.
5. Haga clic en **Save (Guardar)**.

Administración de eventos

El Core incluye conjuntos de eventos predefinidos que pueden utilizarse para notificar a los administradores problemas graves del Core o de los trabajos de copia de seguridad.

En la ficha **Events (Eventos)**, puede administrar grupos de notificación, la configuración SMTP del correo electrónico, la configuración del servidor, los registros de rastreo habilitados, la configuración de servicios en la nube, la reducción de la repetición y la retención de eventos.

La opción Notification Groups (Grupos de notificación) le permite administrar los grupos de notificación, desde los que podrá:

- Especificar un evento para el cual desee generar una alerta en los casos siguientes:
 - Clusters
 - Attachability
 - Trabajos
 - Licencias
 - Log Truncation (Truncamiento de registro)
 - Archive
 - Core Service (Servicio de Core)
 - Exportar
 - Protection
 - Replicación
 - Rollback
- Especificar el tipo de alerta (error, aviso o informativa).
- Especificar a quién y dónde se envían las alertas. Las opciones incluyen:
 - Dirección de correo electrónico
 - Registros de eventos de Windows
 - Servidor Syslog
- Especificar un umbral de tiempo para la repetición.
- Especificar el período de retención de todos los eventos.

Configuración de grupos de notificación

Para configurar grupos de notificación:

1. En la Core Console, seleccione **Configuration** → **Events (Configuración > Eventos)**.
2. Haga clic en **Add Group (Agregar grupo)**.
Aparece el cuadro de diálogo **Add Notification Group (Agregar grupo de notificación)**, que muestra dos paneles:
 - **Enable Alerts (Activar las alertas)**
 - **Notification Options (Opciones de notificación)**

Activación de alertas

La activación de alertas permite definir un conjunto de eventos del sistema para el registro, la creación de informes y la configuración de alertas.

 **NOTA:** Para crear alertas de todos los eventos, seleccione **All Alerts (Todas las alertas)**.

- Para crear alertas específicas de errores, advertencias y mensajes de información, o una combinación de todos ellos, seleccione una de las opciones siguientes:
 - icono en forma de triángulo rojo (Error)

- icono de triángulo amarillo (Advertencia)
- círculo azul (Información)
- flecha curva (Restaura predeterminados)
- Para crear alertas de eventos específicos, haga clic en el símbolo > junto al grupo correspondiente y marque la casilla de verificación para activar la alerta.

Configuración de Opciones de notificación

1. En el panel **Notification Options (Opciones de notificación)**, especifique cómo se tramitará el proceso de notificación.

Las opciones de notificación son:


| Cuadro de texto | Descripción |
|------------------------------------|---|
| Notify by e-mail | <p>Designa los destinatarios de la notificación por correo electrónico. Puede introducir varias direcciones de correo electrónico separadas, así como copias y copias ocultas, tal como se muestra a continuación:</p> <ul style="list-style-type: none"> • A: • CC: • CCO: |
| Notify by Windows Event Log | <p>Seleccione esta opción si desea que la notificación de las alertas se entregue mediante el registro de eventos de Windows.</p> |
| Notify by sys logd | <p>Seleccione esta opción si desea informar de las alertas a través de sys logd. Introduzca los detalles para el sys logd en los siguientes cuadros de texto:</p> <ul style="list-style-type: none"> • Nombre del host: • Puerto: 1 |
| Notify by Toast alerts | <p>Seleccione esta opción si desea que la alerta aparezca como un mensaje emergente en la esquina inferior derecha de la pantalla.</p> |

2. Haga clic en **OK (Aceptar)**.

Se muestra el mensaje siguiente: **The Group name cannot be changed after the creation of the Notification Group. Are you sure you want to use this name? (El nombre de grupo no se puede cambiar después de la creación del grupo de notificación. ¿Está seguro de que desea utilizar este nombre?)**.

- Para guardar el nombre de grupo, haga clic en **Yes (Sí)**.
- Para cambiar el nombre de grupo, haga clic en **No**. Vuelva a la ventana **Notification Options (Opciones de notificación)**, actualice el nombre de grupo y otros valores del grupo de notificación y guarde su trabajo.

Configuración de un servidor de correo electrónico

 **NOTA:** Debe configurar los valores de grupo de notificación, incluyendo la habilitación de la opción **Notify by email (Notificar por correo electrónico)**, antes de enviar mensajes de alerta por correo electrónico.

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

1. En la Core Console, haga clic en **Configuration** → **Events (Configuración > Eventos)**.
2. En el panel **Email Settings (Configuración de correo)**, haga clic en **SMTP server (Servidor SMTP)**. Aparecerá el cuadro de diálogo **SMTP Server Settings (Configuración del servidor SMTP)**.
3. Especifique los detalles del servidor de correo electrónico de la siguiente manera:

| Cuadro de texto | Descripción |
|--------------------------|--|
| SMTP Server | 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 . |
| 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 . |
| Username | Introduzca un nombre de usuario para el servidor de correo electrónico. |
| Password | Introduzca una contraseña para acceder al servidor de correo electrónico. |
| Port | 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). |

4. Haga clic en **Send Test Email (Enviar correo electrónico de prueba)** y proceda del modo siguiente:
 - a. En el cuadro de diálogo Send Test Email (Enviar correo electrónico de prueba), escriba una dirección de correo electrónico de destino para el mensaje de prueba y, a continuación, haga clic en **Send (Enviar)**.
 - b. Si el mensaje de prueba falla, salga del cuadro de diálogo de error y del cuadro de diálogo **Send Test Email (Enviar correo electrónico de prueba)** y revise los valores de configuración del servidor de correo electrónico. Repita el paso 4.
 - c. Haga clic en **OK (Aceptar)** para confirmar.
 - d. Compruebe que se ha enviado el mensaje de correo electrónico de prueba.
 - e. Vuelva al cuadro de diálogo SMTP Server Settings (Configuración del servidor SMTP) y haga clic en **Save (Guardar)** para cerrar el cuadro de diálogo y guardar la configuración.

Configuración de una plantilla de notificaciones de correo electrónico

Para que se reciban notificaciones de correo electrónico acerca de eventos, debe configurar un servidor de correo electrónico y una plantilla de notificaciones de correo electrónico.



NOTA: Para que se reciban mensajes de alerta por correo electrónico, configure los valores del grupo de notificación y active la opción **Notify by email (Notificar por correo electrónico)**.

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

1. En la Core Console, haga clic en **Configuration (Configuración) → Events (Eventos)**.
2. En el panel **Email Settings (Configuración del correo electrónico)**, haga clic en **Change (Cambiar)**. Aparecerá el cuadro de diálogo **Edit Email Notification Configuration (Editar configuración de notificación por correo electrónico)**.
3. 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 |
|----------------------|--|
| 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, <hostname> - <level> <name>. |
| Email | Introduzca la información para el texto de la plantilla que describe el evento, cuándo se ha producido y la gravedad. |

4. Haga clic en **Send Test Email (Enviar correo electrónico)** y proceda del modo siguiente:
 - a. En el cuadro de diálogo Send Test Email (Enviar correo electrónico de prueba), escriba una dirección de correo electrónico de destino para el mensaje de prueba y, a continuación, haga clic en **Send (Enviar)**.
 - b. Si el mensaje de prueba falla, salga del cuadro de diálogo de error y el cuadro de diálogo Send Test Email (Enviar correo electrónico de prueba), haga clic en **OK (Aceptar)** para guardar la configuración de la plantilla de correo electrónico actual y modificar la configuración del servidor de correo electrónico, consulte [Configuring An Email Server And Email Notification Template \(Configuración de un servidor de correo electrónico y de una plantilla de notificaciones de correo electrónico\)](#). Asegúrese de que ha vuelto a introducir la contraseña de esa cuenta de correo electrónico. Guarde la configuración y, a continuación, vuelva al paso 4.
 - c. Haga clic en **OK (Aceptar)** para confirmar.
 - d. Compruebe que se ha enviado el mensaje de correo electrónico de prueba.
 - e. Vuelva al cuadro de diálogo **Edit Email Notification Configuration (Editar configuración de notificación por correo electrónico)**, haga clic en **OK (Aceptar)** para cerrarlo y guardar su configuración.

Configuración de la reducción de repeticiones

Para configurar la reducción de repeticiones:

1. En la Core Console, haga clic en **Configuration → Events (Configuración > Eventos)**.
2. En la sección **Repetition Reduction (Reducción de repeticiones)**, haga clic en **Change (Cambiar)**. Aparecerá el cuadro de diálogo **Enable Repetition Reduction (Habilitar reducción de repeticiones)**.
3. Seleccione **Enable Repetition Reduction (Habilitar reducción de repeticiones)**.
4. En el cuadro de texto **Store events for (Almacenar eventos durante)**, introduzca el número de minutos durante los que se almacenarán los eventos para la reducción de repeticiones.
5. Haga clic en **OK (Aceptar)**.

Configuración de la retención de eventos

Para configurar la retención de eventos:

1. En la Core Console, haga clic en **Configuration** → **Settings (Valores de configuración)**.
2. En **Database Connection Settings (Configuración de conexión de base de datos)**, haga clic en **change (cambiar)**.
Aparecerá el cuadro de diálogo **Database Connection Settings (Configuración de conexión de base de datos)**.
3. En el cuadro de texto **Retain event and job history for (Conservar historial de sucesos y trabajos durante)**, introduzca el número de días que desea conservar la información sobre los eventos.
Por ejemplo, puede seleccionar 30 days (default) (30 días [predeterminado]).
4. Haga clic en **Save (Guardar)**.

Administración de repositorios

Un repositorio sirve para almacenar las instantáneas que se capturan desde las estaciones de trabajo y los servidores protegidos. El repositorio de DL1000 está preconfigurado y reside en el almacenamiento interno del sistema.

Los conceptos y consideraciones clave del repositorio incluyen:

- El repositorio se basa en el AppAssure Scalable Object File System (Sistema de archivos de objeto ampliable de AppAssure).
- Todos los datos almacenados en un repositorio se deduplican globalmente.
- El Scalable Object File System (Sistema de archivos de objeto ampliable) puede ofrecer rendimiento ampliable de E/S junto con deduplicación global de datos, Core y administración de retención.


Visualización de los detalles de un repositorio

Para ver los datos de un repositorio:

1. En la Core Console, haga clic en **Configuration (Configuración)** → **Repositories (Repositorios)**.
2. Haga clic en el símbolo > situado junto a la columna **Status (Estado)** del repositorio para el que desea ver los detalles.
3. Los datos del repositorio incluyen la ubicación de almacenamiento y las estadísticas. Entre los datos de la ubicación de almacenamiento se incluye la ruta de acceso a metadatos, la ruta de acceso a datos y el tamaño. Entre la información estadística se incluye:
 - **Deduplication (Desduplicación)**: número de aciertos de deduplicación de bloques y de desaciertos de deduplicación de bloques y la velocidad de compresión de bloques.
 - **Record I/O (E/S de registro)**: que incluye la velocidad (MB/s), la velocidad de lectura (MB/s) y la velocidad de escritura (MB/s).
 - **Storage Engine (Motor de almacenamiento)**: que notifica la velocidad (MB/s), la velocidad de lectura (MB/s) y la velocidad de escritura (MB/s).


Comprobación de un repositorio

La Core Console puede realizar la comprobación de diagnóstico de un volumen de repositorio cuando se producen errores. Los errores del Core pueden ser el resultado de un apagado incorrecto o un error de hardware.

 **NOTA:** Este procedimiento se debe realizar únicamente con fines de diagnóstico.

Para comprobar un repositorio:

1. Haga clic en **Configuration (Configuración)** → **Repositories (Repositorios)**.
2. Haga clic en el icono Settings (Configuración) junto a la columna Compression Ratio (Relación de compresión) debajo del botón **Actions (Acciones)**.
3. Haga clic en **Check (Comprobar)**.
Aparecerá el cuadro de diálogo **Check Repository (Comprobar repositorio)**.
4. En el cuadro de diálogo **Check Repository (Comprobar repositorio)**, haga clic en **Check (Comprobar)**.

 **NOTA:** Cuando se realiza una comprobación, se cancelan todas las tareas activas asociadas con este repositorio. Antes de que comience la comprobación, aparecerá un mensaje que le pedirá que confirme continuar. Se recomienda recrear la memoria caché de los puntos de recuperación. Si la comprobación falla, tendrá que restaurar el repositorio desde un archivo.

Administración de la seguridad

DL1000 proporciona un cifrado muy fuerte. Por ello, las copias de seguridad de máquinas protegidas son inaccesibles. Solo el usuario con la clave de cifrado puede acceder y descifrar los datos. El cifrado no afecta al rendimiento. Los conceptos y las consideraciones clave de seguridad incluyen:

- El cifrado se realiza mediante AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) que cumple SHA-3.
- La deduplicación funciona en el dominio de Core para garantizar la privacidad.
- El cifrado se realiza sin afectar al rendimiento.
- Puede agregar, quitar, importar, exportar, modificar y eliminar una clave de cifrado configurada en el Core.

Cómo agregar una clave de cifrado

Para agregar una clave de cifrado:

1. En la Core Console, haga clic en **Configuration** → **Security (Configuración > Seguridad)**.
2. En el menú desplegable **Actions (Acciones)**, haga clic en **Add Encryption Key (Agregar clave de cifrado)**.
Se abrirá el cuadro de diálogo **Create Edit Encryption Key (Crear clave de cifrado)**.
3. En el cuadro de diálogo **Create Encryption Key (Crear clave de cifrado)**, introduzca los detalles para la clave según se describe a continuación:

| Cuadro de texto | Descripción |
|--------------------|--|
| Name | Introduzca un nombre para la clave de cifrado. |
| Descripción | Introduzca una descripción para la clave de cifrado. Se utiliza para proporcionar más detalles para la clave de cifrado. |
| Passphrase | Introduzca una frase de contraseña. Se utiliza para controlar el acceso. |

| Cuadro de texto | Descripción |
|---------------------------|---|
| Confirm Passphrase | Vuelva a introducir la frase de contraseña. Se utiliza para confirmar la entrada de la frase de contraseña. |

- Haga clic en **OK (Aceptar)**.



PRECAUCIÓN: Se recomienda que proteja la frase de contraseña. Si pierde la frase de contraseña, no podrá recuperar los datos.

Edición de una clave de cifrado

Para editar una clave de cifrado:

- En la Core Console, haga clic en **Configuration** → **Security (Configuración > Seguridad)**. Se muestra la pantalla **Encryption Keys (Claves de cifrado)**.
- Haga clic en > junto al nombre de la clave de cifrado que desea editar y, a continuación, haga clic en **Edit (Editar)**. Aparecerá el cuadro de diálogo **Edit Encryption Key (Editar clave de cifrado)**.
- En el cuadro de diálogo **Edit Encryption Key (Editar clave de cifrado)**, edite el nombre o modifique la descripción de la clave de cifrado.
- Haga clic en **OK (Aceptar)**.

Cómo cambiar la frase de contraseña de la clave de cifrado

Para cambiar la frase de contraseña de la clave de cifrado:

- En la Core Console, haga clic en la **Configuration** → **Security (Configuración > Seguridad)**.
- Haga clic en > junto al nombre de la clave de cifrado que desea editar y, a continuación, haga clic en **Change Passphrase (Cambiar frase de contraseña)**. Aparecerá el cuadro de diálogo **Change Passphrase (Cambiar frase de contraseña)**.
- En el cuadro de diálogo **Change Passphrase (Cambiar frase de contraseña)**, escriba la nueva frase de contraseña de la Core y vuelva a escribirla para confirmarla.
- Haga clic en **OK (Aceptar)**.



PRECAUCIÓN: Se recomienda proteger la contraseña. Si la pierde, no podrá acceder a los datos del sistema.

Importación de una clave de cifrado

Para importar una clave de cifrado:

- En la Core Console, haga clic en **Configuration** → **Security (Configuración > Seguridad)**.
- Haga clic en el menú desplegable **Actions (Acciones)** y, a continuación, haga clic en **Import (Importar)**. Aparecerá el cuadro de diálogo **Import Key (Importar clave)**.
- En el cuadro de diálogo **Import Key (Importar clave)**, haga clic en **Browse (Examinar)** para buscar la clave de cifrado que desea importar y, después, haga clic en **Open (Abrir)**.
- Haga clic en **OK (Aceptar)**.

Exportación de una clave de cifrado

Para exportar una clave de cifrado:

1. En la Core Console, haga clic en **Configuration** → **Security (Configuración > Seguridad)**.
2. En el menú desplegable Configuration (Configuración) de la clave de cifrado que desea exportar, seleccione **Export (Exportar)**.
Aparecerá el cuadro de diálogo **Export Key (Exportar clave)**.
3. En el cuadro de diálogo **Export Key (Exportar clave)**, haga clic en **Save File (Guardar archivo)** para guardar y almacenar las claves de cifrado en una ubicación segura.
4. Haga clic en **OK (Aceptar)**.

Eliminación de una clave de cifrado

Para eliminar una clave de cifrado:

1. En la Core Console, haga clic en **Configuration** → **Security (Configuración > Seguridad)**.
2. En el menú desplegable Configuration (Configuración) para la clave de cifrado que desea eliminar, seleccione **Remove (Quitar)**.
Se abrirá el cuadro de diálogo **Remove Key (Quitar clave)**.
3. En el cuadro de diálogo **Remove Key (Quitar clave)**, haga clic en **OK (Aceptar)** para eliminar la clave de cifrado.



NOTA: Los datos no se descifran al eliminar una clave de cifrado.

Administración de cuentas de servicios en la nube

Su appliance DL le permite hacer una copia de seguridad de los datos mediante la creación de un archivo de copia de seguridad de los puntos de recuperación de una nube. Con su appliance DL, puede crear, editar y administrar su cuenta en la nube a través de un proveedor de almacenamiento en la nube. Puede archivar sus datos en la nube mediante servicios como Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage u otros servicios en la nube basados en OpenStack. Consulte los temas siguientes para administrar sus cuentas de servicios en la nube:

- [Cómo agregar una cuenta de servicios en la nube](#)
- [Edición de una cuenta de servicios en la nube](#)
- [Configuración de los valores de la cuenta de servicios en la nube](#)
- [Eliminación de una cuenta de servicios en la nube](#)

Cómo agregar una cuenta de servicios en la nube

Antes de poder exportar los datos archivados a una nube, debe agregar la cuenta de su proveedor de servicios en la nube en la Core Console.

Para agregar una cuenta de servicios en la nube.

1. En la Core Console, haga clic en la pestaña **Tools (Herramientas)**.
2. En el menú de la izquierda, haga clic en **Clouds (Nubes)**.
3. En la página **Clouds (Nubes)**, haga clic en **Add New Account (Agregar cuenta nueva)**.
Se abrirá el cuadro de diálogo **Add New Account (Agregar cuenta nueva)**.
4. En la lista desplegable **Cloud Type (Tipo de nube)**, seleccione un proveedor compatible de servicios en la nube.

5. Basándose en el tipo de nube que haya seleccionado en el paso 4, introduzca los detalles que se describen en la tabla siguiente.

Tabla 1. Cómo agregar una cuenta de servicios en la nube

| Tipo de nube | Cuadro de texto | Descripción |
|-------------------------------|----------------------|--|
| Microsoft Azure | Storage Account Name | Escriba el nombre de la cuenta de almacenamiento de Windows Azure. |
| | Access Key | Introduzca la clave de acceso de su cuenta. |
| | Display Name | Cree el nombre para mostrar de esta cuenta en AppAssure; por ejemplo, Windows Azure 1. |
| Amazon S3 | Access Key | Introduzca la clave de acceso de su cuenta de servicios en la nube de Amazon. |
| | Secret Key | Escriba la clave secreta de esta cuenta. |
| | Display Name | Cree el nombre para mostrar de esta cuenta en AppAssure; por ejemplo, Amazon 1. |
| Powered by OpenStack | User Name | Escriba el nombre de usuario de su cuenta de servicios en la nube en OpenStack. |
| | API Key | Escriba la clave API de su cuenta. |
| | Display Name | Cree el nombre para mostrar de esta cuenta en AppAssure; por ejemplo, OpenStack 1. |
| | Tenant ID | Escriba su Id. de inquilino para esta cuenta. |
| | Authentication URL | Especifique la URL de autenticación para esta cuenta. |
| Rackspace Cloud Block Storage | User Name | Escriba el nombre de usuario para la cuenta de servicios en la nube de Rackspace. |
| | API Key | Escriba la clave API de esta cuenta. |
| | Display Name | Cree el nombre para mostrar de esta cuenta en AppAssure; por ejemplo, Rackspace 1. |


6. Haga clic en **Add (Agregar)**.

El cuadro de diálogo se cierra y la cuenta se muestra en la página **Clouds (Nubes)** de la Core Console.

Edición de una cuenta de servicios en la nube

Realice los pasos siguientes para editar una cuenta de servicios en la nube:

1. En la Core Console, haga clic en la pestaña **Tools (Herramientas)**.
2. En el menú de la izquierda, haga clic en **Clouds (Nubes)**.
3. Junto a la cuenta de servicios en la nube que desea modificar, haga clic en el menú desplegable y, a continuación, haga clic en **Edit (Editar)**.
Se abre la ventana **Edit Account (Editar cuenta)**.
4. Edite los detalles según sea necesario y, a continuación, haga clic en **Save (Guardar)**.

 **NOTA:** El tipo de nube no se puede editar.

Configuración de los valores de la cuenta de servicios en la nube

Los valores de configuración de la nube le permiten determinar la cantidad de veces que AppAssure debería intentar conectarse a su cuenta de servicios en la nube, y la cantidad de tiempo empleado en un intento antes de que se agote el tiempo de espera.

Para configurar los valores de la conexión de la cuenta de servicios en la nube:


1. En la Core Console, haga clic en la pestaña **Configuration (Configuración)**.
2. En el menú de la izquierda, haga clic en **Settings (Configuración)**.
3. En la página **Settings (Configuración)**, desplácese hacia abajo hasta la opción **Cloud Configuration (Configuración de la nube)**.
4. Haga clic en el menú desplegable junto a la cuenta de servicios en la nube que desee configurar y, a continuación, realice una de las acciones siguientes:
 - Haga clic en **Edit (Editar)**.
Aparece el cuadro de diálogo **Cloud Configuration (Configuración de la nube)**.
 1. Utilice las teclas de flecha hacia arriba y hacia abajo para editar las opciones siguientes:
 - **Request Timeout (Tiempo de espera de solicitud):** Se muestra en minutos y segundos, determina la cantidad de tiempo que AppAssure debe invertir en cada intento para conectarse a la cuenta de servicios en la nube cuando hay un retraso. Los intentos de conexión cesarán después del lapso de tiempo especificado.
 - **Retry Count (Número de reintentos):** Determina el número de intentos que AppAssure debe llevar a cabo antes de determinar que no se puede conectar con la cuenta de servicios en la nube.
 - **Write Buffer Size (Tamaño del búfer de escritura):** Determina el tamaño del búfer que se reserva para escribir los datos archivados en la nube.
 - **Read Buffer Size (Tamaño del búfer de lectura):** Determina el tamaño de bloque reservado para leer los datos archivados desde la nube.
 2. Haga clic en **Next (Siguiendo)**.
 - Hacer clic en **Reset (Restablecer)** devuelve la configuración a los valores predeterminados siguientes:
 - **Request Timeout (Tiempo de espera de solicitud):** 01:30 (minutos y segundos)
 - **Retry Count (Número de reintentos):** 3 (intentos)

Eliminación de una cuenta en la nube

Puede eliminar una cuenta de servicios en la nube, interrumpir el servicio en la nube o dejar de usarla para un Core determinado.

Para eliminar una cuenta de servicios en la nube:

1. En la Core Console, haga clic en la ficha **Tools (Herramientas)**.
2. En el menú de la izquierda, haga clic en **Clouds (Nubes)**.
3. Junto a la cuenta de servicios en la nube que desea editar, haga clic en el menú desplegable y, a continuación, haga clic en **Remove (Quitar)**.
4. En la ventana **Delete Account (Eliminar cuenta)**, haga clic en **Yes (Sí)** para confirmar que desea eliminar la cuenta.
5. Si la cuenta de servicios en la nube está actualmente en uso, en una segunda ventana se le preguntará si desea eliminarla. Haga clic en **Yes (Sí)** para confirmar.


 **NOTA:** La eliminación de una cuenta que está actualmente en uso hace que fallen todos los trabajos de archivo programados para esa cuenta.


Supervisión de DL1000

Puede supervisar el estado de los subsistemas de DL1000 Appliance mediante la pestaña **Appliance** de la página **Overall Status (Estado general)**. En la página **Overall Status (Estado general)** se muestra un indicador de estado al lado de cada subsistema, junto con una descripción que indica el estado de condición del subsistema.


La página Overall Status (Estado general) también proporciona enlaces a herramientas que permiten profundizar en los detalles de cada subsistema, lo que puede ser útil para la solución de problemas de advertencias o errores. El enlace **System Administrator (Administrador del sistema)**, que está disponibles para los subsistemas de hardware de almacenamiento y hardware del dispositivo, le solicitará que inicie una sesión en la aplicación System Administrator (Administrador de sistemas) que se utiliza para la administración del hardware. Para obtener más información sobre la aplicación System Administrator (Administrador de sistemas), consulte la *OpenManage Server Administrator User's Guide (Guía del usuario del Administrador de sistemas de OpenManage)* en dell.com/support/manuals.

Actualización de DL1000

 **NOTA:** Dell recomienda descargar la última versión disponible de AppAssure desde Dell License Activation Portal (Portal de activación de licencias de Dell) mediante el programa de instalación.

 **NOTA:** Para otras actualizaciones de software, recibirá una notificación para actualizar a la versión más reciente.


Reparación de DL1000

 **NOTA:** Antes de comenzar el proceso de reparación, asegúrese de detener los servicios del Core.

Recuperación automática rápida del appliance (RASR)

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


Para llevar a cabo la RASR:

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

1. Introduzca la llave USB RASR creada.
2. Reinicie el appliance mediante la memoria USB de RASR.
3. Haga clic en **Rapid Appliance Self Recovery (Recuperación automática rápida del appliance)**. Aparecerá una pantalla de bienvenida.

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

Se muestra la pantalla de verificación **Prerequisites (Prerrequisitos)**.

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

5. Haga clic en **Next (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)**

6. Seleccione la opción **Factory Reset (Restablecer valores de fábrica)**.

Esta opción recuperará el disco del sistema operativo desde la imagen de fábrica.

7. Haga clic en **Next (Siguiente)**.

Aparece la pantalla **Storage Configuration (Configuración de almacenamiento)**.


8. En la pantalla **OS Recovery (Recuperación del sistema operativo)**, se muestra el mensaje de advertencia siguiente en un cuadro de diálogo: `This operation will recover the operating system. All OS disk data will be overwritten.`

9. Haga clic en **Yes (Sí)**.

El disco del sistema operativo inicia la restauración de las configuraciones de fábrica.

10. Haga clic en **Finish (Finalizar)**.

Creación de la memoria USB de RASR

 **NOTA:** Después de la configuración inicial del software, el asistente **AppAssure Appliance Configuration Wizard (Asistente de configuración del Appliance AppAssure)** se inicia automáticamente. El icono de estado de la pestaña **Appliance** es de color amarillo.

Para crear una memoria USB de RASR:

1. Vaya a la pestaña **Appliance**.
2. Uso del panel de navegación de la izquierda, seleccione **Appliance** → **Backup (Copia de seguridad)**. Se muestra la ventana **Create RASR USB Drive (Crear unidad USB de RASR)**.

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

3. 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)**.

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

Aparece un cuadro de diálogo de advertencia.

5. Haga clic en **Yes (Sí)**.

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


6.  **NOTA:** Asegúrese de utilizar la Extracción segura de la unidad USB o la función de 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, etiquétela y guárdela para su uso en el futuro.

Protección de estaciones de trabajo y servidores

Acerca de la protección de estaciones de trabajo y servidores


Para proteger sus datos con DL1000, añada las estaciones de trabajo y los servidores que desea proteger en la Core Console; por ejemplo, el servidor de Exchange, SQL Server o el servidor de Linux.

 **NOTA:** En este capítulo, el término *máquina* también se refiere al software del Agent de AppAssure instalado en esa máquina.

En la Core Console, puede identificar la máquina en la que está instalado el software de un Agent de AppAssure y especificar qué volúmenes proteger, definir programas para la protección, agregar medidas de seguridad adicionales como el cifrado, etc. Para obtener más información sobre cómo acceder a la Core Console para proteger estaciones de trabajo y servidores, consulte [Cómo proteger una máquina](#).

Implementación de un Agent (Instalación de inserción)

DL1000 le permite implementar el instalador AppAssure Agent Installer en máquinas Windows individuales para ofrecer protección. Realice los pasos siguientes para enviar el instalador a un Agent. Para implementar Agents en varias máquinas simultáneamente, consulte [Implementación en varias máquinas](#).

 **NOTA:** Los Agents deben estar configurados con una política de seguridad que permita la instalación remota.

Para implementar un Agent:


1. En el área de navegación izquierda de la Core Console, haga clic en **Protected Machines (Máquinas protegidas)**.
2. Haga clic en **Actions** → **Deploy Agent (Acciones > Implementar Agent)**. Aparecerá el cuadro de diálogo **Deploy Agent (Implementar Agent)**.
3. En el cuadro **Deploy Agent (Implementar Agent)**, introduzca la configuración de inicio de sesión según se indica en la tabla siguiente.

| Cuadro de texto | Descripción |
|-----------------|--|
| Machine | Introduzca el nombre de host o dirección IP de la máquina que quiere implementar. |
| Username | Introduzca el nombre de usuario con el que conectar a esta máquina (por ejemplo, administrador). |
| Password | Introduzca la contraseña para conectar a esta máquina. |

| Cuadro de texto | Descripción |
|---------------------------------------|---|
| Automatic reboot after install | Seleccione para especificar si el Core debe iniciarse después de finalizar la implementación e instalación de AppAssure Agent Installer. |
| 4. | Haga clic en Verify (Comprobar) para validar las credenciales que ha introducido. El cuadro Deploy Agent (Implementar Agent) muestra un mensaje para indicar que la validación se ha realizado. |
| 5. | Haga clic en Abort (Abortar) si desea cancelar el proceso de verificación. Una vez completado el proceso de verificación, aparece un mensaje que indica que la verificación ha terminado. |
| 6. | Haga clic en Deploy (Implementar) . Se muestra un mensaje que indica que se ha iniciado la implementación. Puede ver el progreso en la pestaña Events (Eventos) . |
| 7. | Haga clic en Show details (Mostrar detalles) para ver más información sobre el estado de la implementación del Agent. |
| 8. | Haga clic en OK (Aceptar) . |

Cómo proteger una máquina

En este tema se describe cómo proteger los datos de una máquina determinada.

 **NOTA:** La máquina debe tener el software AppAssure Agent instalado para poder protegerse. Puede instalar el software de AppAssure Agent antes de realizar este procedimiento, o bien implementarlo en el agente a medida que configura la protección en el cuadro de diálogo **Connection (Conexión)**. Para instalar el software de AppAssure Agent durante el proceso de protección de una máquina, consulte [Deploying The Agent Software When Protecting An Agent \(Implantación del software del Agent al proteger un agente\)](#).

Cuando agregue protección, debe especificar el nombre o la dirección IP de la máquina a proteger y los volúmenes en esa máquina a proteger, así como definir el programa de protección para cada volumen.

Para proteger varias máquinas a la vez, consulte [Protección de varias máquinas](#).

Para proteger una máquina:

1. Si aún no lo ha hecho, reinicie la máquina en la que esté instalado el software AppAssure Agent.
2. En la Core Console de la máquina del Core, haga clic en **Protect (Proteger)** → **Protect Machine (Proteger máquina)** en la barra de botones. Se abrirá el asistente **Protect Machine Wizard (Asistente de proteger máquina)**.
3. En la página **Welcome (Bienvenidos)**, seleccione las opciones de instalación adecuadas:
 - Si no necesita definir un repositorio o establecer el cifrado, seleccione **Typical (Típica)**.
 - Si no desea ver la página **Welcome (Bienvenidos)** del asistente **Protect Machine Wizard (Asistente de proteger máquina)** en el futuro, seleccione la opción **Skip this Welcome page the next time the wizard opens (Omitir esta página de bienvenida la próxima vez que se abra el asistente)**.
4. Haga clic en **Next (Siguiente)**.
5. En el cuadro de diálogo **Connection (Conexión)**, introduzca la información sobre la máquina a la que desea conectarse, tal como se describe en la tabla siguiente.

| Cuadro de texto | Descripción |
|-----------------|--|
| Host | El nombre de host o la dirección IP de la máquina que desea proteger. |
| Port | El número de puerto con el que el AppAssure Core se comunica con el Agent en la máquina. El número de puerto predeterminado es 8006. |
| Username | El nombre de usuario que se utiliza para conectarse a ese sistema; por ejemplo, administrador. |
| Password | La contraseña que se utiliza para conectar a esa máquina. |

6. Haga clic en **Next (Siguiente)**. Si la página **Protection (Protección)** se abre a continuación en el asistente **Protect Machine Wizard (Asistente de proteger máquina)**, vaya al paso 7.




NOTA: Si la página **Install Agent (Instalar agente)** se abre a continuación en el asistente **Protect Machine Wizard (Asistente de proteger máquina)**, significa que el software de Agent no está instalado aún en la máquina designada. Haga clic en **Next (Siguiente)** para instalar el software de Agent. El software de Agent debe estar instalado en la máquina que desea proteger, y que deberá reiniciarse primero para que pueda hacer la copia de seguridad en el Core. Para que el instalador reinicie la máquina Agent, seleccione la opción **After installation, restart the machine automatically (recommended) (Después de la instalación, reiniciar la máquina automáticamente [recomendado])** antes de hacer clic en **Next (Siguiente)**.

7. Este campo muestra el nombre de host o la dirección IP especificada en el cuadro de diálogo **Connect (Conectar)**. De manera opcional, escriba un nombre nuevo para la máquina que se mostrará en la Core Console.
8. Seleccione el programa de protección adecuado:
- Para usar el programa de protección predeterminado, en la opción **Schedule Settings (Configuración de programación)**, seleccione **Default protection (3 hour snapshots of all volumes) (Protección predeterminada (instantáneas cada tres hora de todos los volúmenes))**. Con un programa de protección predeterminado, el Core realizará instantáneas de la máquina del agente una vez cada 3 horas. Las instantáneas de la máquina del agente pueden tomarse una vez cada hora (mínimo). 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 pestaña Summary (Resumen) de la máquina agente específica.
 - Para definir un programa de protección diferente, en la opción **Schedule Settings (Configuración de programación)**, seleccione **Custom protection (Protección personalizada)**.
9. Seleccione una de las siguientes opciones:
- Si en el asistente **Protect Machine Wizard (Asistente de proteger máquina)** ha seleccionado una configuración típica y ha especificado la protección predeterminada, haga clic en **Finish (Finalizar)** para confirmar la selección, cerrar el asistente y proteger la máquina especificada.
 - La primera vez que se agrega protección para una máquina, se transferirá una imagen base (es decir, una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el AppAssure Core conforme a lo programado, salvo que haya especificado pausar la protección inicialmente.
 - Si ha seleccionado una configuración típica para el asistente **Protect Machine Wizard (Asistente de proteger máquina)** y ha especificado una protección personalizada, haga clic en **Next (Siguiente)** para configurar un programa de protección personalizado. Para obtener más información sobre cómo definir un programa de protección, consulte Creación de programas de protección personalizados.
 - Si ha seleccionado Advanced configuration (Configuración avanzada) para el asistente **Protect Machine Wizard (Asistente de proteger máquina)**, haga clic en **Next (Siguiente)** y continúe en el paso 12 para ver las opciones de repositorio y cifrado.
 - Si ha seleccionado Advanced configuration (Configuración avanzada) para el asistente **Protect Machine Wizard (Asistente de proteger máquina)** y ha especificado una protección

personalizada, haga clic en **Next (Siguiente)** y continúe en el paso 10 para seleccionar qué volúmenes se van a proteger.

10. En la página **Protection Volumes (Volúmenes con protección)**, seleccione los volúmenes en la máquina Agent que desea proteger. Si en la lista se incluye algún volumen que no desea incluir en la protección, haga clic en la columna seleccionada para deseleccionarla. A continuación, haga clic en **Next (Siguiente)**.


 **NOTA:** Se recomienda proteger 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 **Protection Schedule (Programa de protección)**, defina un programa personalizado.
12. En la página **Repository (Repositorio)**, seleccione **Use an existing repository (Usar un repositorio existente)**.

13. Haga clic en **Next (Siguiente)**.
Se abrirá la página **Encryption (Cifrado)**.

14. Opcionalmente, en la página **Encryption (Cifrado)**, seleccione **Enable Encryption (Habilitar el cifrado)** para activarlo.

Aparecerán los campos de **Encryption key (Clave de cifrado)** en la página **Encryption (Cifrado)**.

 **NOTA:** Si activa el cifrado, se aplicará a los datos de todos los volúmenes protegidos para esta máquina Agent. Puede cambiar la configuración posteriormente en la pestaña **Configuration (Configuración)** de la Core Console.

 **PRECAUCIÓN:** AppAssure utiliza cifrado AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) con claves de 256 bits. Usar el cifrado es opcional, pero Dell recomienda encarecidamente que se 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 los datos. Sin la frase de contraseña, es imposible recuperar los datos.

15. Para agregar una clave de cifrado para el Core, introduzca la información tal como se describe en la tabla siguiente.

| Cuadro de texto | Descripción |
|---------------------------|---|
| Name | Introduzca un nombre para la clave de cifrado. |
| Descripción | Introduzca una descripción para proporcionar detalles adicionales para la clave de cifrado. |
| Passphrase | Introduzca la frase de contraseña usada para controlar el acceso. |
| Confirm Passphrase | Vuelva a introducir la frase de contraseña que acaba de introducir. |

16. Haga clic en **Finish (Finalizar)** para guardar y aplicar la configuración.


La primera vez que se agrega protección para una máquina, se transferirá una imagen base (es decir, una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Core conforme a lo programado, salvo que haya especificado pausar la protección inicialmente.

Cómo pausar y reanudar la protección

Cuando se hace una pausa en la protección, se detienen temporalmente todas las transferencias de datos desde la máquina actual.


Para pausar la protección:

1. En la Core Console, haga clic en el menú desplegable **Protected Machines (Máquinas protegidas)** en el área de navegación de la izquierda.
2. Seleccione **Pause Protection (Pausar protección)** para la máquina en la que desea pausar la protección.
Aparecerá el cuadro de diálogo **Pause Protection (Pausar protección)**.
3. Seleccione una de las opciones siguientes y haga clic en **OK (Aceptar)**.
 - Si desea pausar la protección hasta que la reanude explícitamente, seleccione **Pause until resumed (Pausar hasta reanudar)**.
 - Si desea pausar la protección durante un período especificado, seleccione **Pause for (Pausar durante)** y, a continuación, en los controles de Days (Días), Hours (Horas) y Minutes (Minutos), escriba o seleccione el período de pausa adecuado según corresponda.


 **NOTA:** Para reanudar la protección, seleccione **Resume Protection (Reanudar protección)** en el menú desplegable **Protected Machines (Máquinas protegidas)**.


Implementación del software del Agent al proteger un agente

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

 **NOTA:** Este proceso no es necesario si ya tiene instalado el software del Agent en un sistema que desee proteger.

Para implementar Agents cuando está agregando un Agent para protección:

1. Haga clic en **Protected Machines (Máquinas protegidas)** en el panel de navegación de la izquierda.
2. Haga clic en **Actions (Acciones) → Deploy Agent (Implementar Agent)**.
Aparecerá el cuadro de diálogo **Deploy Agent (Implementar Agent)**.
3. Introduzca la configuración de protección e inicio de sesión de la siguiente manera:
 - **Host name (Nombre de host):** especifica el nombre de host o dirección IP del sistema que desee proteger.
 - **User name (Nombre de usuario):** especifica el nombre de usuario utilizado para conectarse a este sistema; por ejemplo, administrador.
 - **Password (Contraseña):** especifica la contraseña utilizada para conectarse a este sistema.
 - **Protect machine after install (Proteger máquina después de la instalación):** al seleccionar esta opción, AppAssure toma una instantánea base de los datos después de agregar la máquina que se va a proteger. Esta opción está seleccionada de manera predeterminada. Si anula la selección de esta opción, deberá forzar una instantánea manual cuando esté listo para iniciar la protección de los datos.
 - **Display name (Nombre para mostrar):** especifica un nombre para el sistema que se muestra en la Core Console. El nombre para mostrar puede ser el mismo valor que el nombre de host.
 - **Port (Puerto):** especifica el número de puerto con el que el Core se comunica con el Agent del sistema. El valor predeterminado es 8006.
 - **Repository (Repositorio):** seleccione el repositorio en el que almacenar los datos de este Agent.
 **NOTA:** Puede almacenar datos de varios Agents en un solo repositorio.
 - **Encryption Key (Clave de cifrado):** especifica si el cifrado debería aplicarse a los datos para cada volumen de este sistema para almacenarlos en el repositorio.

 **NOTA:** La configuración del cifrado de un repositorio se define en la pestaña **Configuration (Configuración)** de la Core Console.

4. Haga clic en **Deploy (Implementar)**.

Se cierra el cuadro de diálogo **Deploy Agent (Implementar Agent)**. Puede que haya un retraso antes de que aparezca el Agent seleccionado en la lista de sistemas protegidos.

Comprensión de los programas de protección

El programa de protección define cuándo se transfieren las copias de seguridad desde las máquinas Agent protegidas al AppAssure Core.

Los programas de protección se definen inicialmente mediante el asistente **Protect Machine Wizard (Asistente de proteger máquina)** o el asistente **Protect Multiple Machines Wizard (Asistente para proteger varias máquinas)**. A continuación, puede modificar el programa existente en cualquier momento desde la pestaña Summary (Resumen) de una máquina Agent específica.

AppAssure proporciona un programa de protección predeterminado, con dos períodos de protección definidos. El primer período es de días laborables (de lunes a viernes), con un único período de tiempo definido (desde las 12:00 AM a las 11:59 PM). El intervalo predeterminado (el período de tiempo entre instantáneas) es de 3 horas. El segundo período es el de los fines de semana (sábados y domingos). El intervalo predeterminado para el segundo período es de 3 horas.

Cuando la protección se habilita por primera vez, el programa se activa. Por lo tanto, con la configuración predeterminada, independientemente de la hora del día, la primera copia de seguridad se realiza cada 3 horas.

La primera transferencia de copia de seguridad guardada en el Core se denomina instantánea de la imagen base. Todos los datos en todos los volúmenes especificados (incluido el sistema operativo, las aplicaciones y las configuraciones), se guardan en el Core. A partir de ese momento, las instantáneas incrementales (copias de seguridad más pequeñas que solo incluyen los datos modificados en el Agent desde la última copia de seguridad) se guardan en el Core periódicamente, según el intervalo definido.

Puede crear un programa personalizado para cambiar la frecuencia de las copias de seguridad. Por ejemplo, puede cambiar el intervalo para el período del día laborable a 60 minutos, lo que da como resultado que se tomen instantáneas cada hora. O bien, puede aumentar el intervalo de los fines de semana, de 60 minutos a 180 minutos, lo que da como resultado que se tomen las instantáneas cada tres horas cuando el tráfico es bajo.

Otras opciones de la página del asistente **Protection Schedule Wizard (Asistente del programa de protección)** incluyen la definición de la hora para una protección diaria. Este valor produce una única copia de seguridad diariamente en el período definido (el valor predeterminado es 12:00 PM).

La opción para pausar la protección inicialmente impide que se tome una imagen base (y, de hecho, impide todas las copias de seguridad) hasta que se reanude la protección explícitamente. Cuando esté listo para iniciar la protección de las máquinas conforme a la programación de la protección, deberá reanudar explícitamente la protección.

Creación de programas personalizados

1. En la página **Protection Schedule (Programa de protección)** de **Protect Machine (Proteger máquina)** o **Protect Multiple Machines Wizard (Asistente para proteger varias máquinas)**, haga lo siguiente para cambiar la programación del intervalo de cualquier período:
 - a. Seleccione **Periods (Períodos)**.

Se muestran los períodos existentes y se pueden modificar. Los campos editables incluyen la hora de inicio, la hora de finalización y un intervalo (en minutos) para cada período.
 - b. Haga clic en el campo del intervalo y escriba un intervalo adecuado en minutos.

Por ejemplo, resalte el intervalo existente y reemplácelo por el valor de **60** para hacer instantáneas cada 60 minutos en este período.
2. Para crear períodos pico y no pico para los días laborables, cambie el rango de tiempo del período de los días de la semana, de modo que no incluyan un período de 24 horas, establezca un intervalo óptimo para el pico, seleccione **Take snapshots for the remaining time (Tomar instantáneas el resto del tiempo)** y establezca un intervalo fuera de las horas pico como sigue:
 - a. Seleccione **Periods (Períodos)**.

Se muestran los períodos existentes y se pueden modificar.
 - b. Haga clic en la casilla **From (De)** para cambiar la hora de inicio de este período.

Aparecerá el cuadro de diálogo **Choose Time (Elegir hora)**.
 - c. Arrastre los controles deslizantes Hours and Minutes (Horas y minutos) de manera adecuada para la hora de inicio deseada y, a continuación, haga clic en **Done (Terminado)**. Para especificar la hora actual, haga clic en **Now (Ahora)**.
 - d. Haga clic en la casilla **To (A)** para cambiar la hora de finalización de este período.

Aparecerá el cuadro de diálogo **Choose Time (Elegir hora)**.
 - e. Arrastre los controles deslizantes Hours and Minutes (Horas y minutos) de manera adecuada para la hora de inicio deseada y, a continuación, haga clic en **Done (Terminado)**. Para especificar la hora actual, haga clic en **Now (Ahora)**.
3. Para establecer una sola hora del día para una única copia de seguridad que se lleve a cabo cada día, seleccione **Daily protection time (Tiempo de protección diario)** y, a continuación, especifique una hora con el formato HH: MM AM.
4. Para definir el programa sin iniciar copias de seguridad, seleccione **Initially pause protection (Pausar protección inicialmente)**.

Una vez que se hace una pausa en la protección desde el asistente, permanecerá en pausa hasta que se reanude explícitamente. Una vez que reanude la protección, las copias de seguridad se realizarán según la programación establecida.
5. Haga clic en **Finish (Finalizar)** o en **Next (Siguiente)**.

Modificación de los programas de protección

Puede modificar los programas de protección de volúmenes específicos de una máquina.

Para modificar los programas de protección:

1. En la Core Console, seleccione la máquina con un programa de protección definido que desea cambiar.


Se mostrará la pestaña Summary (Resumen) de la máquina.
2. Seleccione los volúmenes para la máquina protegida que desea cambiar y, a continuación, haga clic en **Set a schedule (Configurar un programa)**. Para seleccionar todos los volúmenes al mismo tiempo, haga clic en la casilla de verificación en la fila del encabezado.

Inicialmente, todos los volúmenes comparten el mismo programa de protección. Normalmente, es una buena práctica para proteger, como mínimo, el volumen System Reserved (Reservado para el sistema) y el volumen con el sistema operativo (por lo general, la unidad C).

Aparecerá el cuadro de diálogo **Protection Schedule (Programa de protección)**.

3. En el cuadro de diálogo **Protection Schedule (Programa de protección)**, si ha creado previamente una plantilla de programa de protección y desea aplicarla a este Agent, seleccione la plantilla en la lista desplegable y, a continuación, vaya al paso 9.
4. Si desea guardar este nuevo programa de protección como plantilla, especifique un nombre para la plantilla en el cuadro de texto.
5. Si desea eliminar un período de tiempo existente desde el programa, deselectione las casillas de verificación al lado de cada opción de período de tiempo. Las opciones incluyen lo siguiente:
 - **Mon - Fri (De lunes a viernes)**. Este intervalo de tiempo se refiere a una semana laboral típica de cinco días.
 - **Sat - Sun (Sábado y domingo)**. Este rango de tiempo indica un fin de semana típico.
6. Si las horas de inicio y de finalización del día de la semana van de las 12:00 AM a las 11:59 PM, entonces existe un único período. Para cambiar las horas de inicio y final de un período de tiempo definido, haga lo siguiente:
 - a. Seleccione el período de tiempo adecuado.
 - b. Haga clic en la casilla **Start Time (Hora de inicio)** para cambiar la hora de inicio de este período.
 - c. Arrastre los controles deslizantes Hours and Minutes (Horas y minutos) de manera adecuada para la hora de inicio deseada y, a continuación, haga clic en **Done (Terminado)**. Para especificar la hora actual, haga clic en **Now (Ahora)**.
 - d. Haga clic en la casilla **End Time (Hora de finalización)** para cambiar la hora final de este período. Aparecerá el cuadro de diálogo **Choose Time (Elegir hora)**.
 - e. Arrastre los controles deslizantes Hours and Minutes (Horas y minutos) de manera adecuada para la hora de inicio deseada y, a continuación, haga clic en **Done (Terminado)**. Para especificar la hora actual, haga clic en **Now (Ahora)**.
 - f. Cambie el intervalo de acuerdo a sus requisitos. Por ejemplo, si define un período pico, cambie el intervalo de 60 minutos a 20 minutos para tomar instantáneas tres veces cada hora.
7. Si se ha definido un periodo distinto al de 12:00 AM a 11:59 PM en el paso 6, si desea que las copias de seguridad se lleven a cabo en el resto de intervalos de tiempo, deberá agregar periodos adicionales para definir la protección mediante los pasos siguientes:
 - a. Haga clic en **+ Add period (+ Agregar período)**.

En la categoría adecuada (días de la semana o fines de semana), aparecerá un nuevo período de tiempo. Si el primer período se ha iniciado pasadas las 12:00 AM, AppAssure inicia automáticamente este periodo a las 12:00. Siguiendo el ejemplo anterior, este segundo período comienza a las 12:00 AM. Es posible que deba ajustar horas o minutos para las horas de inicio y finalización.
 - b. Arrastre el control deslizante Hours and Minutes (Horas y minutos) de manera adecuada para obtener la hora de inicio y la hora de finalización deseadas, según corresponda.
 - c. Cambie el intervalo de acuerdo a sus requisitos. Por ejemplo, si define un período no pico, cambie el intervalo de 60 minutos a 120 minutos para tomar instantáneas cada dos horas.
8. Si fuera necesario, continúe para crear períodos adicionales y configure las horas de inicio y finalización y los intervalos según corresponda.

 **NOTA:** Si desea eliminar un periodo que ha agregado, haga clic en la **X** situada en el extremo derecho de ese período. Si elimina un periodo por error, puede hacer clic en **Cancel (Cancelar)**.
9. Cuando el programa de protección cumpla sus requisitos, haga clic en **Apply (Aplicar)**. El cuadro de diálogo **Protection Schedule (Programa de protección)** se cerrará.


Configuración de los valores de la máquina protegida

Una vez agregada la protección para las máquinas en AppAssure, puede modificar los valores básicos de configuración de la máquina (como el nombre y el nombre de host), la configuración de protección (cambiar la programación de protección para los volúmenes en la máquina, agregando o quitando volúmenes, o pausando la protección), etc.

Visualización y modificación de los valores de configuración

Para ver y modificar valores de configuración:

1. En la Core Console, navegue a la máquina que desea modificar.
2. Haga clic en **Configuration** → **Settings (Valores de configuración)**.
3. Haga clic en **Change (Cambiar)** para modificar la configuración de la máquina, según se muestra en la tabla siguiente.

| Cuadro de texto | Descripción |
|-----------------------|--|
| Display Name | Introduzca el nombre de visualización de la máquina. Un nombre para esta máquina que se mostrará en la Core Console. De forma predeterminada, es el nombre del host de la máquina. Puede cambiarlo por un nombre más fácil de identificar si lo desea. |
| Host Name | Introduzca el nombre del host de la máquina. |
| Port | Introduzca un número de puerto para la máquina. El Core usa el puerto predeterminado 8006 para comunicarse con esta máquina. |
| Encryption Key | Edite la clave de cifrado si es necesario. Especifique si el cifrado se aplica a los datos de cada volumen de esta máquina que se almacenarán en el repositorio. |
| Repository | Seleccione un repositorio para los puntos de recuperación. Muestra el repositorio en el Core donde se almacenarán los datos de esta máquina.  NOTA: Este valor solo se puede cambiar si no hay puntos de recuperación o si falta el repositorio anterior. |

Visualización de la información del sistema de una máquina

La Core Console muestra todas las máquinas que se protegen.

Para ver la información del sistema de una máquina:

1. En el área de navegación izquierda de la Core Console, bajo **Protected Machines (Máquinas protegidas)**, seleccione la máquina para ver información detallada del sistema.
2. Haga clic en la pestaña **Tools (Herramientas)**.

La pestaña System Information (Información del sistema) incluye lo siguiente:

- Host Name

- Versión del SO
- Arquitectura del SO
- Memoria (física)
- Nombre de visualización
- Nombre de dominio completo
- Tipo de máquina virtual (si procede)

La información detallada sobre los volúmenes contenidos en esta máquina incluye:

- Name
- Id. de dispositivo
- Sistema de archivos
- Capacidad (incluida nativa, formateada y usada)

Otra información de la máquina que se muestra incluye:

- Procesadores
- Adaptadores de red
- Direcciones IP asociadas con esta máquina

Visualización de la información de la licencia

Puede ver la información sobre el estado actual de la licencia del software de Agent de AppAssure instalado en una máquina.

Para ver la información de la licencia:

1. En el panel de navegación, seleccione la máquina que desea ver.
2. Haga clic en **Configuration** → **Licensing (Configuración > Licencias)**.

La pantalla **Status (Estado)** muestra los detalles sobre la licencia del producto.

Modificación de la configuración de las transferencias

Puede modificar la configuración para administrar procesos de transferencia de datos en una máquina protegida. La configuración de transferencia que se describe en esta sección es a nivel de Agent. Para ver cómo transferir datos en el Core, consulte [Modificación de la configuración de la cola de transferencias](#).



PRECAUCIÓN: La modificación de la configuración de transferencia puede tener graves consecuencias en su entorno de AppAssure. Antes de cambiar los valores de esta configuración, consulte la **Transfer Performance Tuning Guide (Guía de configuración para la ejecución de transferencias)** en la base de conocimiento de Dell AppAssure.

Hay tres tipos de transferencias en DL1000:

| | |
|-----------------------------|--|
| Instantáneas | La transferencia que realiza la copia de seguridad de los datos de la máquina protegida. |
| Exportación de la VM | Tipo de transferencia que crea una máquina virtual con toda la información y los parámetros de la copia de seguridad según se hayan especificado en el programa definido para proteger la máquina. |
| Restaurar | Un proceso que restaura información de copia de seguridad en una máquina protegida. |

La transferencia de datos en DL1000 conlleva la transmisión de un volumen de datos a través de una red desde las máquinas de AppAssure Agent hasta el Core. En caso de replicación, la transferencia también se puede efectuar desde el Core de origen hasta el de destino.



Además, la transferencia de datos se puede optimizar para un sistema mediante una configuración opcional de rendimiento. Esta configuración controla el uso del ancho de banda de los datos durante los procesos de copia de seguridad de máquinas de Agent, y permite realizar exportaciones de MV o reversiones. Estos son algunos de los factores que influyen en el rendimiento de la transferencia de datos:




- Número de transferencias de datos de Agent simultáneas
- Número de flujos de datos simultáneos
- Número de cambios de datos en el disco
- Ancho de banda de red disponible
- Rendimiento del subsistema del disco del repositorio
- Cantidad de memoria disponible para el almacenamiento en búfer de los datos

Puede ajustar las opciones de rendimiento para que mejor se adapten a sus necesidades empresariales y adaptarlas a su entorno.

Para modificar la configuración de las transferencias:

1. En la Core Console, navegue a la máquina que desea modificar.
2. Haga clic en la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Transfer Settings (Configuración de transferencia)**.
Aparecerá la página actual de **Transfer Settings (Configuración de transferencia)**.
3. En la página **Transfer Settings (Configuración de transferencia)**, haga clic en **Change (Cambiar)**.
Aparecerá el cuadro de diálogo **Transfer Settings (Configuración de transferencia)**.
4. Introduzca las opciones de **Transfer Settings (Configuración de transferencia)** para la máquina como se describe en la tabla siguiente.

| Cuadro de texto | Descripción |
|-----------------------------------|---|
| Priority | Establece la prioridad de transferencia entre las máquinas protegidas. Permite asignar la prioridad mediante la comparación con otras máquinas protegidas. Seleccione un número del 1 al 10, siendo el 1 la máxima prioridad. La configuración predeterminada establece una prioridad de 5.  NOTA: La prioridad se aplica a las transferencias que hay en la cola. |
| Maximum Concurrent Streams | Establece el número máximo de enlaces TCP que se envían al Core para el procesamiento paralelo por Agent.  NOTA: Dell recomienda establecer este valor en 8. Si experimenta la pérdida de paquetes, pruebe a aumentar el valor. |
| Maximum Concurrent Writes | Establece el número máximo de acciones de escritura en disco simultáneas por conexión de Agent. |

| Cuadro de texto | Descripción |
|-------------------------------------|--|
| | <p> NOTA: Dell recomienda establecer este valor en el mismo valor seleccionado para Maximum Concurrent Streams (Número máximo de transmisiones simultáneas). Si experimenta la pérdida de paquetes, elija un valor algo inferior. Por ejemplo, si el número máximo de transmisiones simultáneas está establecido en 8, configure esta opción en 7.</p> |
| Maximum Retries | Establece el número máximo de reintentos para cada máquina protegida, si algunas de las operaciones no se pueden completar. |
| Maximum Segment Size | <p>Especifica la cantidad máxima de datos, en bytes, que un equipo puede recibir en un único segmento TCP. La configuración predeterminada es 4194304.</p> <p> PRECAUCIÓN: No cambie la configuración predeterminada de esta opción.</p> |
| Maximum Transfer Queue Depth | Especifica el número de comandos que se pueden establecer de manera simultánea. Puede ajustar esta opción en un número más alto si en su sistema se realiza un número elevado de operaciones de entrada/salida simultáneas. |
| Outstanding Reads per Stream | <p>Especifica el número de operaciones de lectura en cola que se almacenará en el back-end. Esta configuración permite controlar la puesta en cola de los Agents.</p> <p> NOTA: Dell recomienda establecer este valor en 24.</p> |
| Excluded Writers | <p>Seleccione un escritor si desea excluirlo. Debido a que los escritores que aparecen en la lista son específicos de la máquina que se está configurando, puede que no aparezcan todos los escritores en la lista. Estos son algunos de los que aparecerán:</p> <ul style="list-style-type: none"> • ASR Writer (Escritor ASR) • BITS Writer (Escritor BITS) • COM+ REGDB Writer (Escritor COM+ REGDB) • Performance Counters Writer (Escritor de contadores de rendimiento) • Registry Writer (Escritor de registro) • Shadow Copy Optimization Writer (Escritor de optimización de instantáneas) • SQLServerWriter (Escritor SQLServer) • System Writer (Escritor del sistema) • Task Scheduler Writer (Escritor del programador de tareas) • VSS Metadata Store Writer (Escritor del almacén de metadatos de VSS) • WMI Writer (Escritor WMI) |
| Transfer Data Server Port | Configura el puerto para las transferencias. La configuración predeterminada es 8009. |
| Transfer Timeout | Especifica los minutos y segundos que un paquete puede permanecer como estático sin transferirse. |

| Cuadro de texto | Descripción |
|------------------------------|--|
| Snapshot Timeout | Especifica el tiempo máximo de espera, en minutos y segundos, para tomar una instantánea. |
| Network Read Timeout | Especifica los minutos y segundos del tiempo máximo de espera para una conexión de lectura. Si la lectura de red no se realiza en este tiempo, la operación se repite. |
| Network Write Timeout | Especifica el tiempo máximo de espera, en segundos, para una conexión de escritura. Si la escritura de red no se realiza en este tiempo, la operación se repite. |

- Haga clic en **OK (Aceptar)**.

Archivado de datos

Las políticas de retención establecen los períodos durante los cuales las copias de seguridad se almacenan en soportes a corto plazo (rápidos y caros). A veces, determinados requisitos empresariales y técnicos exigen ampliar la retención de estas copias de seguridad, pero el uso de almacenamiento rápido resulta inasequible. Por tanto, este requisito crea una necesidad de almacenamiento a largo plazo (lento y barato). Las empresas a menudo utilizan el almacenamiento a largo plazo para archivar datos de cumplimiento y de no cumplimiento. La función de archivo en AppAssure se utiliza para admitir la retención ampliada de datos de cumplimiento y de no cumplimiento. También se utiliza para inicializar los datos de replicación en un Core de réplica remoto.


Creación de un archivo

Para crear un archivo:

- En la Core Console, haga clic en **Tools (Herramientas)** → **Archive (Archivo)** → **Create (Crear)**. Aparecerá el cuadro de diálogo del asistente **Add Archive Wizard (Asistente para agregar archivo)**.
- En la página **Create (Crear)** del asistente **Add Archive Wizard (Asistente para agregar archivo)**, seleccione una de las opciones siguientes en la lista desplegable **Location Type (Tipo de ubicación)**:
 - Local
 - Network (Red)
 - Cloud (Nube)
- En función del tipo de ubicación que haya seleccionado en el paso 3, introduzca los detalles para el archivo según se describen en la tabla siguiente.

Tabla 2. Creación de un archivo

| Opción | Cuadro de texto | Descripción |
|--------|-----------------|--|
| Local | Output location | Especifique la ubicación de salida, que se utiliza para definir la ruta de acceso a la ubicación en la que desea que resida el |

| Opción | Cuadro de texto | Descripción |
|---------|-----------------|--|
| Network | Output location | archivo; por ejemplo, d:\work\archive. Especifique la ubicación de salida, que se utiliza para definir la ruta de acceso a la ubicación en la que desea que resida el archivo; por ejemplo, \servername\sharename. |
| | User Name | Introduzca un nombre de usuario. Se utiliza para establecer las credenciales de inicio de sesión para el recurso compartido de red. |
| | Password | Introduzca una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de sesión para el recurso compartido de red. |
| Cloud | Account | Seleccione una cuenta en la lista desplegable.  NOTA: Para seleccionar una cuenta de servicios en la nube, primero debe añadirla a la Core Console. Consulte Cómo agregar una cuenta de servicios en la nube . |
| | Container | En el menú desplegable, seleccione un contenedor asociado con la cuenta. |
| | Folder Name | Escriba un nombre para la carpeta en la que se van a guardar los datos archivados. El nombre predeterminado es AppAssure-5-Archive-[FECHA DE CREACIÓN]-[HORA DE CREACIÓN] |

4. Haga clic en **Next (Siguiete)**.
5. En la página **Machines (Máquinas)** del asistente, seleccione las máquinas protegidas que contienen los puntos de recuperación que desea archivar.
6. Haga clic en **Next (Siguiete)**.
7. En la página **Options (Opciones)**, introduzca la información que se describe en la tabla siguiente.

Cuadro de texto

Descripción

Maximum Size

Los grandes archivos de datos pueden dividirse en múltiples segmentos. Para seleccionar la cantidad máxima de espacio que desea reservar para crear el archivo, lleve a cabo una de las acciones siguientes:

- Seleccione Entire Target (Todo el destino) para reservar todo el espacio disponible en la ruta de acceso en el destino proporcionado en el paso 4 (por ejemplo, si la ubicación es D:\work\archive, se reservará todo el espacio disponible en la unidad D:).
- Seleccione el cuadro de texto en blanco, utilice las teclas de flecha hacia arriba y hacia abajo para introducir una cantidad y, a continuación, seleccione una unidad de medida en la lista desplegable para personalizar el espacio máximo que desea reservar.



NOTA: Los archivos en la nube de Amazon se dividen en segmentos de 50 GB. Los archivos en la nube de Windows Azure se dividen automáticamente en segmentos de 200 GB.

Recycle action

Seleccione una de las siguientes opciones de acción de reciclaje:

- **Do not reuse (No reutilizar):** no sobrescribe ni borra los datos archivados existentes de la ubicación. Si la ubicación no está vacía, fallará la escritura del archivo.
- **Replace this Core (Reemplazar este Core):** sobrescribe los datos archivados que ya existen y que pertenecen a este Core, pero deja intactos los datos de los otros Cores.
- **Erase completely (Borrar completamente):** borra todos los datos archivados del directorio antes de escribir el archivo nuevo.
- **Incremental (Incremental):** permite agregar puntos de recuperación a un archivo existente. Compara los puntos de recuperación para evitar duplicar datos que ya existen en el archivo.

Comment

Introduzca la información adicional que sea necesario capturar para el archivo. El comentario se mostrará si usted importa el archivo más tarde.

Use compatible format

Seleccione esta opción para archivar los datos en un formato que sea compatible con las versiones anteriores de Cores.



NOTA: El nuevo formato ofrece mejor rendimiento; sin embargo, no es compatible con versiones anteriores de Cores.

8. Haga clic en **Next (Siguiete)**.

9. En la página Date Range (Intervalo de fechas), especifique Start Date (Fecha de inicio) y Expiration Date (Fecha de caducidad) de los puntos de recuperación que se van a archivar.

- Para especificar una hora, haga clic en la hora que se indica (la predeterminada es 8:00 AM) para que se muestren las barras deslizantes y seleccionar horas y minutos.
- Para especificar una fecha, haga clic en el cuadro de texto para ver el calendario y, a continuación, haga clic en el día que prefiera.

10. Haga clic en **Finish (Finalizar)**.


Importación de un archivo

Para importar un archivo:

1. En la Core Console, haga clic en **Tools (Herramientas)** → **Archive (Archivo)** → **Import (Importar)**.
2. Para **Location Type (Tipo de ubicación)**, seleccione una de las opciones siguientes en la lista desplegable:
 - Local
 - Network (Red)
 - Cloud (Nube)
3. En función del tipo de ubicación que haya seleccionado en el paso 3, introduzca los detalles para el archivo según se describen en la tabla siguiente.

Tabla 3. Importación de un archivo

| Opción | Cuadro de texto | Descripción |
|---------|-----------------|---|
| Local | Output location | Especifique la ubicación de salida, que se utiliza para definir la ruta de acceso a la ubicación en la que desea que resida el archivo; por ejemplo, d:\work\archive. |
| | Network | Especifique la ubicación de salida, que se utiliza para definir la ruta de acceso a la ubicación en la que desea que resida el archivo; por ejemplo, \servername\sharename. |
| | User Name | Introduzca un nombre de usuario. Se utiliza para establecer las credenciales de inicio de sesión para el recurso compartido de red. |
| Network | Password | Introduzca una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de sesión para el recurso compartido de red. |
| | Cloud | Seleccione una cuenta en la lista desplegable. |

| Opción | Cuadro de texto | Descripción |
|--------|-----------------|---|
| | |  NOTA: Para seleccionar una cuenta de servicios en la nube, primero debe añadirla a la Core Console. Consulte Cómo agregar una cuenta de servicios en la nube . |
| | Container | En el menú desplegable, seleccione un contenedor asociado con la cuenta. |
| | Folder Name | Escriba un nombre para la carpeta en la que se van a guardar los datos archivados. El nombre predeterminado es AppAssure-5-Archive-[FECHA DE CREACIÓN]-[HORA DE CREACIÓN] |

4. Haga clic en **Check File (Comprobar archivo)** para validar la existencia del archivo que se va a importar.
Aprecerá el cuadro de diálogo **Restore (Restaurar)**.
5. En el cuadro de diálogo **Restore (Restaurar)**, verifique el nombre del Core de origen.
6. Seleccione los Agents que se van a importar desde el archivo.
7. Seleccione el repositorio.
8. Haga clic en **Restore (Restaurar)** para importar el archivo.

Archivado en una nube

Para archivar los datos en una nube puede transferirlos a una variedad de proveedores de servicios en la nube directamente desde la Core Console. Las nubes compatibles incluyen Windows Azure, Amazon, Rackspace y cualquier proveedor basado en el estándar OpenStack.

Para exportar un archivo a una nube:

- Agregue su cuenta de servicios en la nube a la Core Console. Para obtener más información, consulte [Cómo agregar una cuenta de servicios en la nube](#).
- Archive los datos y exportélos a su cuenta de nube.
- Recupere los datos archivados importando desde la ubicación en la nube.

Visualización de los diagnósticos del sistema

En AppAssure, la información de diagnóstico está disponible para que pueda ver los datos del registro de cualquier máquina protegida. Además, puede ver y cargar información de diagnóstico para el Core.

Visualización de los registros de la máquina

Si se producen errores o problemas con la máquina, puede ser útil consultar los registros para solucionarlos.

Para ver los registros de la máquina:

1. En la Core Console, haga clic en **Tools** → **Diagnostics** → **View Log (Herramientas > Diagnósticos > Ver registro)** .
Aparece la página **Download Core Log (Descargar el registro del Core)**.
2. Seleccione **Click here to begin the download (Haga clic aquí para iniciar la descarga)**
Aparecerá un mensaje que le indica que abra o guarde el archivo.
3. Elija el método que prefiera para manejar el archivo de registro.

Carga de los registros de la máquina

1. Navegue a la Core Console y haga clic en **Tools** → **Diagnostics** → **Upload Log (Herramientas > Diagnósticos > Cargar registros)**.
Aparecerá la página **Upload Log (Cargar registros)**.
2. Seleccione **Click here to begin the upload (Haga clic aquí para iniciar la carga)**.
La pestaña Events (Eventos) muestra el progreso de la carga de la información del registro del Core y todas las máquinas protegidas.

Cancelación de operaciones en una máquina

Puede cancelar las operaciones que se ejecutan actualmente en una máquina. Puede cancelar una instantánea actual o cancelar todas las operaciones actuales, que incluyen exportaciones y replicaciones. Para cancelar las operaciones de una máquina:

1. En la Core Console, seleccione la máquina en la que desea cancelar las operaciones.
2. En **Events (Eventos)**, expanda los detalles del evento o la operación que desea cancelar.
3. Haga clic en **Cancel (Cancelar)**.

Visualización del estado de la máquina y otros detalles

Para ver el estado y otros detalles de la máquina:

1. En la Core Console, navegue a la máquina protegida que desea ver.

La información sobre la máquina se muestra en la página **Summary (Resumen)**. A continuación, se describen los detalles que se incluyen:

- Host name
- Last Snapshot (Última instantánea tomada)
- Next Snapshot (Siguiendo instantánea programada)
- Encryption (Estado de cifrado)
- Version number (Número de versión)
- Mountability Check (Estado de comprobación de capacidad de montaje)
- Checksum Check (Estado de comprobación de suma de comprobación)
- Last Log Truncation (Último truncamiento del registro realizado)

También se muestra información sobre los volúmenes contenidos en esta máquina, que incluye:

- Name

- File System Type (Tipo de sistema de archivos)
- Space Usage (Uso del espacio)
- Current Schedule (Programa actual)
- Next Snapshot (Próxima instantánea)
- Total size (Tamaño total)
- Used Space (Espacio utilizado)
- Free Space (Espacio libre)

Si SQL Server está instalado en la máquina, también se muestra información detallada sobre el servidor, como por ejemplo:

- Estado en línea
- Name
- Install Path (Ruta de instalación)
- Version

Si Exchange Server está instalado en la máquina, también se muestra información detallada sobre el servidor y los almacenes de correo, como por ejemplo:

- Version
- Install Path (Ruta de instalación)
- Data Path (Ruta de acceso datos)
- Name Exchange Databases Path (Poner nombre a ruta de acceso a bases de datos de Exchange)
- Log File Path (Ruta de acceso al archivo de registro)
- Log Prefix (Prefijo de registro)
- System Path (Ruta de acceso al sistema)
- MailStore Type (Tipo de almacén de correo)

Administración de varias máquinas

En este tema se describen las tareas que los administradores deben realizar para implementar el software de AppAssure Agent de forma simultánea en varias máquinas Windows.

Para implementar y proteger varios Agents, debe realizar las tareas siguientes:

1. Implementar AppAssure en varias máquinas.
Consulte [Implementación en varias máquinas.](#)
2. Supervisar la actividad de la implementación por lotes.
Consulte [Supervisión de la implementación de varias máquinas.](#)
3. Proteger varias máquinas.
Consulte [Protección de varias máquinas.](#)



NOTA: Este paso puede omitirse si seleccionó la opción Protect machine after install (Proteger la máquina después de la instalación) durante la implementación.


4. Supervisar la actividad de la protección por lotes.
Consulte [Supervisión de la protección de varias máquinas.](#)

Implementación en varias máquinas

Puede simplificar la tarea de implementación del software AppAssure Agent en varias máquinas Windows mediante la función Bulk Deploy (Implementación masiva) de AppAssure. Puede realizar la Implementación masiva en:

- Máquinas en un host virtual VMware vCenter/ESXi
- Máquinas en un dominio de Active Directory
- Máquinas en cualquier otro host

La función Bulk Deploy (Implementación masiva) detecta automáticamente máquinas en un host y le permite seleccionar aquellas en las que desee realizar la implementación. De manera alternativa, puede introducir manualmente información del host y la máquina.

 **NOTA:** Las máquinas que implemente deben tener acceso a Internet para descargar e instalar BITS, porque AppAssure usa la versión web del AppAssure Agent Installer para implementar los componentes de la instalación. Si el acceso a Internet no está disponible, puede insertar el programa de instalación de AppAssure Agent desde la máquina del Core. Puede descargar actualizaciones del Core y del Agent desde el License Portal (Portal de licencias).

Supervisión de la implementación de varias máquinas

Puede ver el progreso de la implementación del software AppAssure Agent en las máquinas.

Para supervisar la implementación en varias máquinas:


1. En la Core Console, haga clic en **Events (Eventos)** → **Alerts (Alertas)**.
2. Navegue a la pestaña Home (Inicio) del AppAssure Core y, a continuación, haga clic en la pestaña **Events (Eventos)**.

En la lista se muestran los eventos de alerta y se indica la hora en que se inició el evento y un mensaje. Para cada implementación correcta del software de Agent, verá una alerta que indica que se ha agregado la máquina protegida.

3. Opcionalmente, haga clic en cualquier enlace de una máquina protegida. Se muestra la pestaña Summary (Resumen) de la máquina seleccionada, que muestra la información pertinente, que incluye:
 - El nombre de host de la máquina protegida
 - La última instantánea, si procede
 - La hora de la siguiente instantánea programada, basada en el programa de protección que haya seleccionado
 - Tiempo restante
 - La clave de cifrado, si la hay, que se utiliza para este Agent protegido
 - La versión del software Agent

Protección de varias máquinas

Tras la implementación masiva del software AppAssure Agent en las máquinas de Windows, debemos protegerlas para proteger los datos. Si selecciona **Protect Machine After Install (Proteger máquina tras la instalación)** al implementar el Agent, podrá saltarse este procedimiento.

 **NOTA:** Las máquinas de Agent se deben configurar con una política de seguridad que permita que la instalación remota sea posible.

Para proteger varias máquinas:

1. En la Core Console, haga clic en **Protect (Proteger)** → **Bulk Protect (Protección masiva)**. Se abrirá el asistente **Protect Multiple Machines Wizard (Asistente para proteger varias máquinas)**.
2. Seleccione la opción de instalación adecuada:
 - Si no necesita definir un repositorio o establecer el cifrado, seleccione **Typical (Típica)**.
 - Si no desea volver a ver la página Welcome (Bienvenidos) del asistente Protect Multiple Machines Wizard (Asistente para proteger varias máquinas), seleccione **Skip this Welcome page the next time the wizard opens (Omitir esta página de bienvenida la próxima vez que se abra el asistente)**.
3. Haga clic en **Next (Siguiente)**. Aparecerá la página **Connection (Conexión)**.
4. Agregue las máquinas que desea proteger haciendo clic en una de las siguientes opciones.
 - Haga clic en **Active Directory** para especificar máquinas en un dominio de Active Directory. Introduzca los credenciales como se describe en la tabla a continuación y haga clic en **Next (Siguiente)**.
 - Haga clic en **vCenter/ESXi** para especificar máquinas virtuales en un host virtual vCenter/ESXi. Introduzca los credenciales como se describe en la tabla a continuación y haga clic en **Next (Siguiente)**.

| Cuadro de texto | Descripción |
|-----------------|--|
| Host | El nombre de host o la dirección IP del dominio de Active Directory o el host virtual del VMware vCenter Server/ESXi(i). |
| Username | Introduzca el nombre de usuario que se utiliza para conectar a esa máquina; por ejemplo, Administrador. |
| Password | Introduzca la contraseña segura que se utiliza para conectarse a esta máquina. |

- Para agregar las máquinas manualmente, seleccione **Add the machines manually (Agregar las máquinas manualmente)**. Haga clic en **Next (Siguiente)**.
5. En la página **Machines (Máquinas)**, para especificar las máquinas de forma manual, escriba los detalles siguientes de la conexión para cada una de las máquinas en una línea separada y, a continuación, haga clic en **Next (Siguiente)**. `hostname::username::password::port`
 6. En la página **Machines (Máquinas)**, para especificar las máquinas identificadas en un dominio de Active Directory o desde un host virtual VMware vCenter/ESXi(i), seleccione en la lista cada una de las máquinas que desea proteger y, a continuación, haga clic en **Next (Siguiente)**. El sistema verifica cada máquina que agrega automáticamente y aparecerá en la página **Protection (Protección)**.
 7. En la página **Protection (Protección)**, seleccione el programa de protección adecuado:
 - A continuación, para usar el programa de protección predeterminado, en la opción **Schedule Settings (Configuración de programación)**, seleccione **Default protection (hourly snapshots of all volumes) (Protección predeterminada (instantáneas cada hora de todos los volúmenes))**.
 - Si desea definir un programa de protección diferente, en la opción Schedule Settings (Configuración de programación), seleccione **Custom protection (Protección personalizada)** y, a continuación, haga clic en **Next (Siguiente)**.
 8. Continúe con la configuración de la manera siguiente:
 - Si ha seleccionado una configuración típica para el asistente **Protect Multiple Machines Wizard (Asistente para proteger varias máquinas)** y la protección predeterminada, haga clic en **Finish (Finalizar)** para confirmar la selección, cerrar el asistente y proteger las máquinas que ha especificado.

- Si ha seleccionado una configuración típica para el asistente **Protect Multiple Machines Wizard (Asistente para proteger varias máquinas)** y ha especificado la protección personalizada, haga clic en **Next (Siguiente)** y configure un programa personalizado.
 - Si ha seleccionado Advanced configuration (Configuración avanzada) para el asistente Protect Machine Wizard (Asistente para proteger máquina), haga clic en **Next (Siguiente)** y continúe en el paso 9 para ver las opciones de repositorio y cifrado.
9. En la página **Repository (Repositorio)**, seleccione **Use an existing repository (Usar un repositorio existente)**.
 10. Haga clic en **Next (Siguiente)**.
Se abrirá la página de **Encryption (Cifrado)**.
 11. En la página **Encryption (Cifrado)**, seleccione **Enable Encryption (Habilitar el cifrado)** para activarlo. Aparecerán los campos de Encryption key (Clave de cifrado) en la página **Encryption (Cifrado)**.

 **NOTA:** Si activa el cifrado, se aplicará a los datos de todos los volúmenes protegidos para las máquinas que haya especificado que se protejan. Puede cambiar la configuración posteriormente en la pestaña **Configuration (Configuración)** de la Core Console. Para obtener más información sobre el cifrado, consulte [Administración de la seguridad](#).
 12. Para agregar una clave de cifrado para el Core, introduzca la información tal como se describe en la tabla siguiente.

| Cuadro de texto | Descripción |
|---------------------------|---|
| Name | Introduzca un nombre para la clave de cifrado. |
| Description | Introduzca una descripción para proporcionar detalles adicionales para la clave de cifrado. |
| Passphrase | Introduzca la frase de contraseña usada para controlar el acceso. |
| Confirm Passphrase | Vuelva a introducir la frase de contraseña que acaba de introducir. |

13. Haga clic en **Finish (Finalizar)** para guardar y aplicar la configuración.

Supervisión de la protección de varias máquinas

Puede supervisar el progreso a medida que AppAssure aplica las políticas y programas de protección a las máquinas.

Para supervisar la protección de varias máquinas, navegue a la pestaña Home (Inicio) de la Core Console y haga clic en **Events (Eventos)**.

La pestaña Events (Eventos) muestra Tasks (Tareas), Alerts (Alertas) y Events (Eventos). Cuando se transfieren los volúmenes, el estado y las horas de inicio y de finalización se indican en el panel Tasks (Tareas). También puede filtrar las tareas por estado (active (activo), waiting (en espera) completed (completado) y failed (error)).

A medida que se añade cada máquina protegida, se registra una alerta que indica si la operación ha sido correcta o si se han registrado errores.

Datos de recuperación

Administración de la recuperación

AppAssure Core puede restaurar datos o recuperar máquinas en máquinas físicas o virtuales instantáneamente desde puntos de recuperación. Los puntos de recuperación contienen instantáneas de volúmenes de Agents capturadas a nivel de bloque. Estas instantáneas son sensibles a las aplicaciones, lo que implica que se completen todas las transacciones abiertas y registros de transacciones en movimiento y que las cachés se despejen a disco antes de crear la instantánea. El uso de instantáneas sensibles a las aplicaciones junto con Verified Recovery permite al Core realizar varios tipos de recuperaciones, que incluyen:

- Recuperación de archivos y carpetas
- Recuperación de volúmenes de datos, mediante Live Recovery
- Recuperación de volúmenes de datos para Microsoft Exchange Server y Microsoft SQL Server, mediante Live Recovery
- Restauración desde cero, mediante Universal Recovery
- Recuperación desde cero de hardware diferente, mediante Universal Recovery
- Exportación ad-hoc y continua a máquinas virtuales

Administración de instantáneas y puntos de recuperación

Un punto de recuperación es una colección de instantáneas tomadas de volúmenes de disco independientes que se almacenan en el repositorio. Las instantáneas capturan y almacenan el estado de un volumen de disco en un punto específico en el tiempo mientras las aplicaciones que generan los datos aún están en uso. En AppAssure, puede forzar instantáneas, pausar instantáneas de manera temporal o ver listas de los puntos de recuperación actuales en el repositorio, así como eliminarlos si es necesario. Los puntos de recuperación se usan para restaurar las máquinas protegidas o montar máquinas en un sistema de archivos local.

Las instantáneas que AppAssure captura se capturan a nivel de bloque y son sensibles a las aplicaciones. Esto implica que se completen todas las transacciones abiertas y registros de transacciones en movimiento y que las cachés se despejen a disco antes de crear la instantánea.

AppAssure utiliza un controlador de filtro de volumen de bajo nivel que se conecta a los volúmenes montados y, a continuación, realiza el seguimiento de todos los cambios a nivel de bloque para la siguiente instantánea inminente. Se utiliza Microsoft Volume Shadow Services (VSS) para facilitar instantáneas consistentes de bloqueo de aplicación.

Visualización de puntos de recuperación

Para ver los puntos de recuperación:

1. En el área de navegación izquierda de la Core Console, seleccione la máquina para la que desea ver los puntos de recuperación y, a continuación, haga clic en la pestaña **Recovery Points (Puntos de recuperación)**.

Puede ver la información sobre los puntos de recuperación de la máquina según se describe en la tabla siguiente:

| Información | Descripción |
|----------------------|--|
| Status | Indica el estado actual del punto de recuperación. |
| Encrypted | Indica si el punto de recuperación está cifrado. |
| Contents | Muestra los volúmenes incluidos en el punto de recuperación. |
| Type | Define un tipo de punto de recuperación, básico o diferencial. |
| Creation Date | Muestra la fecha de creación del punto de recuperación. |
| Size | Muestra la cantidad de espacio que el punto de recuperación consume en el repositorio. |

Visualización de un punto de recuperación específico

Para ver un punto de recuperación específico:

1. En el área de navegación izquierda de la Core Console, seleccione la máquina para la que desea ver los puntos de recuperación y seleccione **Recovery Points (Puntos de recuperación)**.
2. Haga clic en el símbolo > junto a un punto de recuperación de la lista para expandir la vista. Podrá ver información más detallada acerca del contenido del punto de recuperación para la máquina seleccionada, además de acceder a diversas operaciones que se pueden ejecutar en el punto de recuperación, y que se enumeran en la siguiente tabla:

| Información | Descripción |
|---------------------------|--|
| Actions (Acciones) | <p>En el menú Actions (Acciones) se incluyen las siguientes operaciones que se pueden ejecutar en el punto de recuperación seleccionado:</p> <p>Mount (Montar): seleccione esta opción para montar el punto de recuperación seleccionado. Para obtener más información acerca de cómo montar un punto de recuperación seleccionado, consulte Montaje de un punto de recuperación para una máquina Windows.</p> <p>Export (Exportar): la opción Export (Exportar) permite exportar el punto de recuperación seleccionado a ESXi, a una estación de trabajo VMware o a HyperV.</p> <p>Restore (Restaurar): seleccione esta opción para restaurar desde el punto de recuperación seleccionado al volumen que especifique.</p> |
| Contents | <p>El área Contents (Contenido) incluye una fila para cada volumen en el punto de recuperación expandido, que mostrará la información siguiente para cada volumen:</p> <p>Status (Estado): indica el estado actual del punto de recuperación.</p> <p>Title (Título): muestra el volumen específico del punto de recuperación.</p> |

Size (Tamaño): muestra la cantidad de espacio que el punto de recuperación consume en el repositorio.

3. Haga clic en el símbolo > junto a un volumen en el punto de recuperación seleccionado para expandir la vista.

Puede ver la información sobre el volumen seleccionado en el punto de recuperación expandido según se describe en la tabla siguiente:

| Cuadro de texto | Descripción |
|---------------------------|--|
| Title | Indica el volumen específico del punto de recuperación. |
| Raw Capacity | Indica la cantidad de espacio de almacenamiento libre en el volumen. |
| Formatted Capacity | Indica la cantidad de espacio de almacenamiento disponible para los datos una vez que el volumen se ha formateado. |
| Used Capacity | Indica la cantidad de espacio de almacenamiento utilizada actualmente en el volumen. |

Montaje de un punto de recuperación para una máquina Windows

En AppAssure puede montar un punto de recuperación para una máquina Windows para acceder a los datos almacenados a través de un sistema de archivos local.

Para montar un punto de recuperación para una máquina Windows:

1. En la Core Console, elija la máquina que desea montar en un sistema de archivos local. Aparece la pestaña **Summary (Resumen)** para la máquina seleccionada.
2. Seleccione la pestaña **Recovery Points (Puntos de recuperación)**.
3. En la lista de puntos de recuperación, haga clic en > para expandir el punto de recuperación que desea montar.
4. En los detalles expandidos de ese punto de recuperación, haga clic en **Mount (Montar)**. Aparecerá el cuadro de diálogo **Mount Recovery Point (Montar punto de recuperación)**.
5. En el cuadro de diálogo **Mount (Montar)**, edite los cuadros de texto para montar un punto de recuperación como se describe en la tabla siguiente:

| Cuadro de texto | Descripción |
|-------------------------------------|--|
| Mount Location: Local Folder | Especifica la ruta de acceso que se utiliza para acceder al punto de recuperación montado. |
| Volume Images | Especifica las imágenes de volumen que desea montar. |
| Mount Type | Especifica la forma para acceder a los datos para el punto de recuperación montado. <ul style="list-style-type: none">• Mount Read-only (Montaje de solo lectura).• Mount Read-only with previous writes (Montaje de solo lectura con escrituras previas).• Mount Writable (Montaje con capacidad de escritura). |

| Cuadro de texto | Descripción |
|--|--|
| Create a Windows share for this Mount | Opcionalmente, seleccione la casilla de verificación para especificar si el punto de recuperación montado se puede compartir y, en ese caso, configurar los derechos de acceso, incluidos el nombre del recurso compartido y los grupos de acceso. |

- Haga clic en **Mount (Montar)** para montar el punto de recuperación.

Desmontaje de puntos de recuperación seleccionados

Para desmontar puntos de recuperación seleccionados:

- Navigue a la Core Console y haga clic en **Tools** → **Mounts (Herramientas > Montajes)**.
- En la página **Local Mounts (Montajes locales)**, haga clic en el punto de montaje del punto de recuperación que quiere desmontar y haga clic en **Dismount (Desmontar)**.
- En la ventana **Dismounting the Recovery Point (Desmontaje del punto de recuperación)**, haga clic en **Yes (Sí)** para confirmar.

Desmontaje de todos los puntos de recuperación

Para desmontar todos los puntos de recuperación:

- Navigue a la Core Console y haga clic en **Tools** → **Mounts (Herramientas > Montajes)**.
- En la página **Local Mounts (Montajes activos)**, haga clic en **Dismount All (Desmontar todo)**.
- En la ventana **Dismounting the Recovery Point (Desmontaje del punto de recuperación)**, haga clic en **Yes (Sí)** para confirmar.

Montaje de un punto de recuperación para una máquina Linux

Mediante la utilidad **aaamount** de AppAssure, puede montar un volumen de forma remota desde un punto de recuperación como volumen local, en una máquina Linux.

- Cree un nuevo directorio para montar el punto de recuperación (por ejemplo, puede usar el comando **mkdir**).
- Verifique que el directorio existe (por ejemplo, mediante el comando **ls**).
- Ejecute la utilidad **aaamount** de AppAssure como raíz o como el superusuario, por ejemplo: **sudo aaamount**
- En la solicitud de montaje de AppAssure, introduzca el siguiente comando para enumerar las máquinas protegidas. **lm**
- Cuando se le solicite, introduzca la dirección IP o nombre del host del servidor del Core.
- Introduzca las credenciales de inicio de sesión para el servidor del Core, es decir, el nombre de usuario y la contraseña.

Se mostrará una lista de las máquinas que están protegidas por el servidor de AppAssure. Cada máquina se identifica con los datos siguientes: número de elemento de línea, dirección de host/IP y un número de identificación para la máquina. Por ejemplo:

```
293cc667-44b4-48ab-91d8-44bc74252a4f
```

- Introduzca el comando siguiente para listar los puntos de recuperación que están disponibles para una máquina especificada: **lr <line_number_of_machine>**

8. Introduzca el siguiente comando para seleccionar y montar el punto de recuperación especificado en el punto/ruta de acceso de montaje especificados. **m <volume_recovery_point_ID_number> <path>**
9. Para verificar que el montaje ha sido correcto, introduzca el comando siguiente, que deberá listar el volumen remoto conectado: **l**

Eliminación de puntos de recuperación

Puede fácilmente eliminar puntos de recuperación de una máquina específica desde el repositorio. Al eliminar puntos de recuperación en AppAssure, puede especificar una de las siguientes opciones:

| Cuadro de texto | Descripción |
|--|--|
| Delete All Recovery Points | Elimina todos los puntos de recuperación para la máquina Agent seleccionada del repositorio. |
| Delete a Range of Recovery Points | Elimina todos los puntos de recuperación de un rango especificado antes del actual, hasta e incluida la imagen base, que son todos los datos de la máquina, así como todos los puntos de recuperación después del actual hasta la imagen base siguiente. |


 **NOTA:** No podrá recuperar los puntos de recuperación que haya eliminado.

Para eliminar puntos de recuperación:

1. En el área de navegación izquierda de la Core Console, seleccione la máquina para la que desea ver los puntos de recuperación y, a continuación, haga clic en la pestaña **Recovery Points (Puntos de recuperación)**.
2. Haga clic en el menú **Actions (Acciones)**.
3. Seleccione una de las opciones siguientes:
 - Para eliminar todos los puntos de recuperación actualmente almacenados, haga clic en **Delete All (Eliminar todos)**.
 - Para eliminar un conjunto de puntos de recuperación en un rango de datos específico, haga clic en **Delete Range (Eliminar rango)**. Se muestra el cuadro de diálogo **Delete (Eliminar)**. En el cuadro de diálogo **Delete Range (Eliminar rango)**, especifique el rango de puntos de recuperación que desea eliminar utilizando una fecha y hora de inicio y una fecha y hora de finalización; a continuación, haga clic en **Delete (Eliminar)**.


Eliminación de una cadena de puntos de recuperación huérfanos

Un punto de recuperación huérfano es una instantánea incremental que no está asociada a ninguna imagen base. Las instantáneas posteriores siguen creándose en este punto de recuperación. Sin la imagen base, los puntos de recuperación que se originan están incompletos y es poco probable que contengan los datos necesarios para realizar una recuperación. Se considera que estos puntos de recuperación forman parte de la cadena de puntos de recuperación huérfanos. En caso de producirse esta situación, la mejor solución consiste en eliminar la cadena y crear una imagen base nueva. Para obtener más información sobre cómo forzar una imagen base, consulte [Cómo forzar una instantánea](#).

 **NOTA:** La capacidad para eliminar una cadena de puntos de recuperación huérfanos no está disponible para los puntos de recuperación replicados en un Core de destino.

Para eliminar una cadena de puntos de recuperación huérfanos:

1. En la Core Console, seleccione la máquina protegida para la que desea eliminar la cadena de puntos de recuperación huérfanos.
2. Haga clic en la pestaña **Recovery Points (Puntos de recuperación)**.
3. En **Recovery Points (Puntos de recuperación)**, expanda el punto de recuperación huérfano. En la columna **Type (Tipo)**, este punto de recuperación aparece como **Incremental Orphaned (Huérfano incremental)**.
4. Junto a **Actions (Acciones)**, haga clic en **Delete (Eliminar)**. Aparece la ventana **Delete Recovery Points (Eliminar puntos de recuperación)**.
5. En la ventana **Delete Recovery Points (Eliminar puntos de recuperación)**, haga clic en **Yes (Sí)**.

 **PRECAUCIÓN:** Al eliminar este punto de recuperación se elimina toda la cadena de puntos de recuperación, incluidos los puntos incrementales situados antes o después de la cadena, hasta la imagen base siguiente. Esta operación no se puede deshacer.

Cómo forzar una instantánea

Forzar una instantánea le permite forzar una transferencia de datos para la máquina protegida actual. Cuando se fuerza una instantánea, la transferencia se inicia inmediatamente o se agrega a la cola. Solo se transfieren los datos que hayan cambiado desde un punto de recuperación anterior. Si no existe ningún punto de recuperación anterior, se transfieren todos los datos en los volúmenes protegidos, que se denominan imagen base.

Para forzar una instantánea:

1. En la Core Console, seleccione la máquina o clúster con el punto de recuperación para el que quiera forzar una instantánea.
2. Haga clic en la pestaña **Summary (Resumen)** de la sección **Volumes (Volúmenes)** y, a continuación, seleccione una de las opciones que se describen a continuación:
 - **Force Snapshot (Forzar instantánea):** toma una instantánea incremental de los datos actualizados desde que se tomó la última instantánea.
 - **Force Base Image (Forzar imagen base):** toma una instantánea completa de los datos de los volúmenes de la máquina.
3. Cuando aparezca una notificación en el cuadro de diálogo **Transfer Status (Estado de transferencia)** de que la instantánea se ha puesto en cola, haga clic en **OK (Aceptar)**. Aparecerá una barra de progreso junto a la máquina en la pestaña **Machines (Máquinas)** que mostrará el progreso de la instantánea.

Restablecimiento de datos

Con AppAssure, puede recuperar o restaurar al instante datos en sus máquinas físicas (para máquinas Windows o Linux) o en máquinas virtuales a partir de puntos de recuperación almacenados para máquinas Windows. Los temas de esta sección describen cómo puede exportar un punto de recuperación específico para máquinas Windows a una máquina virtual o revertir una máquina a un punto de recuperación anterior.

Si ha configurado la replicación entre dos Cores (origen y destino), solo podrá exportar datos del Core de destino después de que la replicación inicial se haya completado.

Acerca de la exportación de datos protegidos de máquinas de Windows a máquinas virtuales

AppAssure es compatible con la exportación puntual o continua (para admitir máquinas en espera virtuales) de información de copias de seguridad de Windows a una máquina virtual. La exportación de los datos a una máquina en espera virtual proporciona una copia de alta disponibilidad de los datos. Si una máquina protegida deja de funcionar, puede iniciar la máquina virtual para realizar la recuperación.

El siguiente diagrama muestra una implementación típica para la exportación de datos a una máquina virtual.

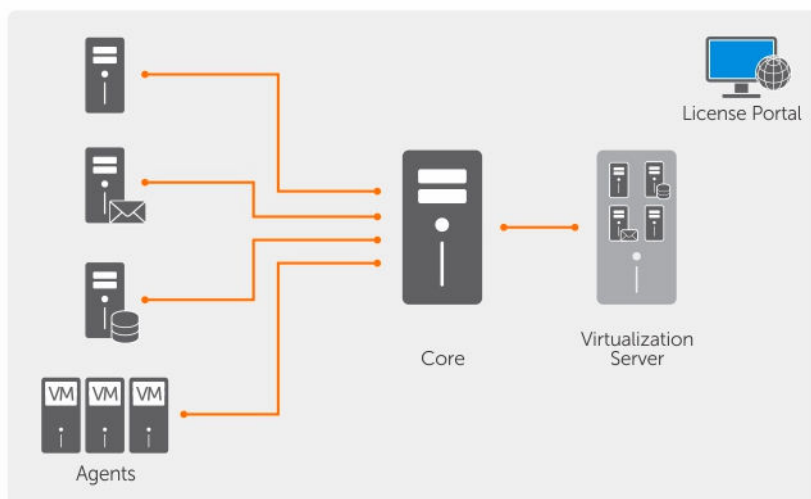




Ilustración 4. Exportación de datos a una máquina virtual

Cree una espera virtual exportando datos protegidos de manera continua desde la máquina de Windows a una máquina virtual. Cuando se exporta a una máquina virtual, se exportan los datos de copia de seguridad de un punto de recuperación, así como los parámetros definidos en el programa de protección de la máquina.

Puede realizar una exportación virtual de puntos de recuperación protegidos para máquinas Windows o Linux, VMware, ESXi, Hyper-V y Oracle VirtualBox.

-  **NOTA:** La pestaña Appliance muestra todas las máquinas virtuales, pero sólo es compatible con la administración de máquinas virtuales Hyper-V y ESXi. Para administrar las otras máquinas virtuales, utilice las herramientas de administración de hipervisores.
-  **NOTA:** La máquina virtual a la que exporte deberá tener una versión con licencia de ESXi, estación de trabajo de VMWare o Hyper-V, en lugar de las versiones gratuitas o de prueba.


Limitaciones de compatibilidad de volúmenes básicos y dinámicos

Dell AppAssure admite la toma de instantáneas de todos los volúmenes básicos y dinámicos. AppAssure también admite la exportación de los volúmenes dinámicos simples que están en un único disco físico. Los volúmenes dinámicos simples no son volúmenes seccionados, reflejados ni distribuidos.

Los discos dinámicos (excepto los discos dinámicos simples, como se ha descrito más arriba) no están disponibles para la selección en el asistente Export Wizard (Asistente de exportación). Los volúmenes dinámicos que no son simples disponen de una geometría de disco arbitraria que no se puede interpretar por completo. Por lo tanto, AppAssure no admite la exportación de volúmenes dinámicos complejos o que no son simples.


Administración de exportaciones

En la pestaña **Virtual Standby (En espera virtual)** de la Core Console, puede ver el estado de las exportaciones que ha configurado, incluidas exportaciones de una sola vez y exportaciones continuas para la espera virtual. En esta pestaña puede administrar las exportaciones y ponerlas en pausa o detenerlas, eliminar las exportaciones o ver una cola de las próximas exportaciones.

 **NOTA:** Solo Dell DL1000, de 3 TB con configuración de 2 máquinas virtuales (VM), es compatible con la exportación de una vez y la exportación continua (en espera virtual).

1. En la Core Console, navegue a la pestaña **Virtual Standby (En espera virtual)**.

En la pestaña **Virtual Standby (En espera virtual)** puede ver una tabla de la configuración guardada de la exportación, que incluye la información que se describe en la tabla siguiente.

| Menú | Descripción |
|---------------------|--|
| Status | <p> NOTA: El estado de la configuración de espera virtual se define mediante el color del icono.</p> <p>Verde: el estado de espera virtual está configurado correctamente, está activo y no está en pausa. La próxima exportación Virtual Standby (En espera virtual) se realizará después de la próxima instantánea.</p> <p>Amarillo: la espera virtual se encuentra en pausa y el Core sigue guardándola. Sin embargo, después de una transferencia nueva, la tarea de exportación no se iniciará automáticamente y no habrá nuevas exportaciones Virtual Standby (En espera virtual) para este Agent.</p> |
| Machine Name | El nombre de la máquina origen. |
| Destination | La máquina virtual y la ruta de acceso a los datos que se están exportando. |
| Export Type | El tipo de plataforma de máquina virtual para la exportación, como, por ejemplo, ESXi, VMware, Hyper-V o VirtualBox. |
| Last Export | La fecha y la hora de la última exportación. Si acaba de agregarse una exportación pero no se ha completado, aparecerá un mensaje indicando que la exportación aún no se ha realizado. Si una exportación ha fallado o se ha cancelado, también se mostrará el mensaje correspondiente. |

2. Para administrar la configuración de exportación guardada, seleccione una exportación y, a continuación, haga clic en una de las opciones siguientes:
 - **Pause (Pausa):** Para pausar la exportación.
 - **Resume (Reanudar):** Para reiniciar una exportación en pausa.
 - **Force (Forzar):** Para forzar una nueva exportación. Esta opción puede ser útil cuando la espera virtual está en pausa y, a continuación, se reanuda, lo que significa que la tarea de exportación se reiniciará solamente después de una nueva transferencia. Si no desea esperar la transferencia nueva, puede forzar una exportación.
3. Para eliminar una exportación del sistema, haga clic en **Remove (Quitar)**. Al eliminar una exportación, se suprimirá permanentemente del sistema y no podrá volver a iniciarla.


4. Para ver detalles acerca de las exportaciones activas actualmente en cola para completarse, haga clic en **Show Export Queue (Mostrar cola de exportación)**.

Se mostrará la tabla siguiente:

| Menú | Descripción |
|---------------|---|
| Machine Name | El nombre de la máquina origen. |
| Destination | El estado de espera virtual está configurado correctamente, está activo y no está en pausa. La próxima exportación Virtual Standby (En espera virtual) se realizará después de la próxima instantánea. |
| Export Type | La espera virtual se encuentra en pausa y el Core sigue guardándola. Sin embargo, después de una transferencia nueva, la tarea de exportación no se iniciará automáticamente y no habrá nuevas exportaciones Virtual Standby (En espera virtual) para este Agent. |
| Schedule Type | El tipo de exportación es One-time (Una vez) o Continuous (Continua). |
| Status | El progreso de la exportación, que se muestra como un porcentaje en la barra de progreso. |

Exportación de información de copia de seguridad de una máquina Windows a una máquina virtual

Puede exportar datos desde sus máquinas Windows a una máquina virtual (VMWare, ESXi e Hyper-V) mediante la exportación de toda la información de copia de seguridad desde un punto de recuperación, así como de los parámetros definidos para el programa de protección de la máquina.

 **NOTA:** Solo Dell DL1000, de 3 TB con configuración de 2 máquinas virtuales (VM), es compatible con la exportación de una vez y la exportación continua (en espera virtual).

Para exportar la información de copia de seguridad de Windows a una máquina virtual:

1. En la Core Console, haga clic en la pestaña **Protected Machines (Máquinas protegidas)**.
2. En la lista de máquinas protegidas, seleccione la máquina o clúster con el punto de recuperación para el que quiera exportar.
3. En el menú desplegable **Actions (Acciones)** para la máquina, haga clic en **Export (Exportar)** y, a continuación, seleccione el tipo de exportación que desee realizar. Puede elegir entre las siguientes opciones:
 - One-time (Una vez)
 - Virtual Standby (En espera virtual)

Aparecerá el cuadro de diálogo **Export Wizard (Asistente de exportación)**.

Exportación de datos de Windows mediante exportación ESXi

En AppAssure, puede elegir exportar datos mediante la exportación ESXi realizando una exportación única o continua.

Cómo realizar una exportación ESXi única

Para realizar una exportación ESXi única:

1. En la Core Console, navegue a la máquina que desee exportar.
2. En la pestaña **Summary (Resumen)**, haga clic en **Actions (Acciones)** → **Export (Exportar)** → **One-time (Único)**.

El asistente **Export Wizard (Asistente de exportación)** se muestra en la página **Protected Machines (Máquinas protegidas)**.

3. Seleccione una máquina para exportarla y, a continuación, haga clic en **Next (Siguiete)**.
4. En la página **Recovery Points (Puntos de recuperación)**, seleccione el punto de recuperación que desea exportar y, a continuación, haga clic en **Next (Siguiete)**.

Definición de la información de máquina virtual para realizar una exportación ESXi

Para definir la información de máquina virtual para realizar una exportación ESXi:


1. En la página **Destination (Destino)** del **Export Wizard (Asistente de exportación)**, en el menú desplegable **Recover to Virtual machine (Recuperar a máquina virtual)**, seleccione **ESXi(i)**.
2. Introduzca los parámetros para acceder a la máquina virtual, tal como se describe a continuación:

| Cuadro de texto | Descripción |
|------------------------|---|
| Host Name | Introduzca un nombre para la máquina host. |
| Port | Introduzca el puerto para la máquina host. El puerto predeterminado es 443. |
| User name | Introduzca las credenciales de inicio de sesión para la máquina host. |
| Password | Introduzca las credenciales de inicio de sesión para la máquina host. |

3. En la página **Virtual Machine Options (Opciones de máquina virtual)**, introduzca la información que se describe en la tabla siguiente.

| Cuadro de texto | Descripción |
|-----------------------------|---|
| Resource Pool | Seleccione una agrupación de recursos en la lista desplegable. |
| Data Store | Seleccione un almacén de datos en la lista desplegable. |
| Virtual Machine Name | Introduzca un nombre para la máquina virtual. |
| Memory | Especifique el uso de la memoria. |
| Disk Provisioning | Seleccione el tipo de aprovisionamiento de discos, como Thin (Ligero) o Thick (Grueso). |
| Disk Mapping | Especifique el tipo de asignación de discos, como Automatic (Automática) o Manual (Manual). |
| Version | Seleccione la versión de la máquina virtual. |

4. Haga clic en **Next (Siguiete)**.
5. En la página **Volumes (Volúmenes)**, seleccione los volúmenes que desea exportar y, a continuación, haga clic en **Next (Siguiete)**.
6. En la página **Summary (Resumen)**, haga clic en **Finish (Finalizar)** para completar el asistente e iniciar la exportación.

 **NOTA:** Para supervisar el estado y el progreso de la exportación, visualice **Virtual Standby (En espera virtual)** o la pestaña **Events (Eventos)**.

Cómo realizar una exportación ESXi continua (en espera virtual)

Para realizar una exportación ESXi continua (en espera virtual):

1. En la Core Console, realice una de las acciones siguientes:
 - En la pestaña Virtual Standby (En espera virtual), haga clic en **Add (Agregar)** para iniciar el asistente **Export Wizard (Asistente de exportación)**. En la página **Protected Machines (Máquinas protegidas)** del **Export Wizard (Asistente de exportación)**, seleccione la máquina protegida que desea exportar y, a continuación, haga clic en **Next (Siguiete)**.
 - Navegue a la máquina que desea exportar y, a continuación, haga clic en **Actions → Export → Virtual Standby (Acciones > Exportar > En espera virtual)**.
2. En la página **Destination (Destino)** del asistente **Export Wizard (Asistente de exportación)**, en el menú desplegable **Recover to a Virtual Machine (Recuperar a máquina virtual)**, seleccione **ESXi**.
3. Introduzca la información para acceder a la máquina virtual, tal como se describe en la tabla siguiente y, a continuación, haga clic en **Next (Siguiete)**.

| Cuadro de texto | Descripción |
|------------------|---|
| Host name | Introduzca un nombre para la máquina host. |
| Port | Introduzca el puerto para la máquina host. El predeterminado es 443. |
| User name | Introduzca las credenciales de inicio de sesión para la máquina host. |
| Password | Introduzca las credenciales de inicio de sesión para la máquina host. |

4. En la página **Virtual Machine Options (Opciones de máquina virtual)**, introduzca la información que se describe en la tabla siguiente.

| Cuadro de texto | Descripción |
|-----------------------------|--|
| Resource Pool | Seleccione una agrupación de recursos en la lista desplegable. |
| Data Store | Seleccione un almacén de datos en la lista desplegable. |
| Virtual Machine Name | Introduzca un nombre para la máquina virtual. |
| Memory | Haga clic en Use a specific amount of RAM (Utilizar una cantidad de RAM específica) para especificar la cantidad de RAM que utilizar. Por ejemplo, 4096 MB. La cantidad mínima permitida es 512 MB y la máxima viene determinada por la capacidad y las limitaciones de las máquinas host. (Recomendado) |
| Disk Provisioning | Seleccione el tipo de aprovisionamiento de discos, como Thin (Ligero) o Thick (Grueso). |
| Disk Mapping | Especifique el tipo de asignación de discos, como Automatic (Automática) o Manual (Manual). |
| Version | Seleccione la versión de la máquina virtual. |

5. Haga clic en **Next (Siguiete)**.
6. En la página **Volumes (Volúmenes)**, seleccione los volúmenes que desea exportar y, a continuación, haga clic en **Next (Siguiete)**.
7. En la página **Summary (Resumen)**, haga clic en **Finish (Finalizar)** para completar el asistente e iniciar la exportación.



NOTA: Para supervisar el estado y el progreso de la exportación, visualice **Virtual Standby (En espera virtual)** o la pestaña **Events (Eventos)**.

Exportación de datos de Windows mediante una exportación VMware Workstation

En AppAssure, puede seleccionar exportar datos mediante una exportación VMware Workstation al realizar una exportación única o continua. Complete los pasos que se indican en los siguientes procedimientos para exportar mediante una exportación VMware Workstation para el tipo de exportación adecuado.

Cómo realizar una exportación VMWare Workstation única


Para realizar una exportación VMWare Workstation única:


1. En la Core Console, navegue a la máquina que desee exportar.
2. En **Summary (Resumen)**, haga clic en **Actions** → **Export** → **One-time (Acciones > Exportar > Una vez)**.
El asistente **Export Wizard (Asistente de exportación)** se muestra en la página **Protected Machines (Máquinas protegidas)**.
3. Seleccione una máquina para exportarla y, a continuación, haga clic en **Next (Siguiete)**.
4. En la página **Recovery Points (Puntos de recuperación)**, seleccione el punto de recuperación que desea exportar y, a continuación, haga clic en **Next (Siguiete)**.

Definición de configuración única para realizar una exportación de estación de trabajo de VMware


Para definir la configuración única para realizar una exportación VMware Workstation:

1. En la página **Destination (Destino)** del asistente **Export Wizard (Asistente de exportación)**, en el menú desplegable **Recover to Virtual machine (Recuperar a máquina virtual)**, seleccione **VMware Workstation (Estación de trabajo VMware)** y, a continuación, haga clic en **Next (Siguiete)**.
2. En la página **Virtual Machine Options (Opciones de máquina virtual)**, introduzca los parámetros para acceder a la máquina virtual tal como se describen en la tabla siguiente.

| Cuadro de texto | Descripción |
|------------------|---|
| Location | Especifique la ruta de acceso de la carpeta local o recurso compartido de red en el que crear la máquina virtual.  NOTA: Si especificó una ruta de acceso de recurso compartido de red, tendrá que introducir las credenciales de inicio de sesión válidas para una cuenta que esté registrada en la máquina de destino. La cuenta debe tener permisos de lectura y escritura para el recurso compartido de red. |
| User Name | Introduzca las credenciales de inicio de sesión para la máquina virtual. <ul style="list-style-type: none"> • Si ha especificado una ruta de acceso de recurso compartido de red, debe introducir un nombre de usuario válido para una cuenta registrada en la máquina de destino. • Si ha especificado una ruta de acceso local, no hace falta nombre de usuario. |

| Cuadro de texto | Descripción |
|-----------------------------|--|
| Password | <p>Introduzca las credenciales de inicio de sesión para la máquina virtual.</p> <ul style="list-style-type: none"> • Si ha especificado una ruta de acceso de recurso compartido de red, debe introducir una contraseña válida para una cuenta registrada en la máquina de destino. • Si ha especificado una ruta de acceso local, no hace falta contraseña. |
| Virtual Machine Name | <p>Introduzca un nombre para la máquina virtual que se está creando, por ejemplo, VM-0A1B2C3D4.</p> <p> NOTA: El nombre predeterminado es el nombre de la máquina origen.</p> |
| Version | <p>Especifique la versión de VMware Workstation (Estación de trabajo VMware) para la máquina virtual. Puede elegir las opciones siguientes:</p> <ul style="list-style-type: none"> • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 |
| Memory | <p>Para especificar el uso de la memoria para la máquina virtual, haga clic en una de las opciones siguientes:</p> <ul style="list-style-type: none"> • Use the same amount of RAM as the source machine (Utilizar la misma cantidad de RAM que la máquina de origen), para especificar que la configuración de RAM es la misma que en la máquina de origen. • Use a specific amount of RAM (Utilizar una cantidad de RAM específica), para especificar la cantidad de RAM a utilizar, por ejemplo, 4096 Megabytes (MB). La cantidad mínima permitida es 512 MB y la cantidad máxima se determina mediante la capacidad y las limitaciones de la máquina host. (recomendado) |

3. Haga clic en **Next (Siguiente)**.
4. En la página **Summary (Resumen)**, haga clic en **Finish (Finalizar)** para completar el asistente e iniciar la exportación.



 **NOTA:** Para supervisar el estado y el progreso de la exportación, visualice **Virtual Standby (En espera virtual)** o la pestaña **Events (Eventos)**.

Cómo realizar una exportación de la estación de trabajo de VMware continua (en espera virtual)

Para realizar una exportación VMware Workstation continua (en espera virtual):

1. En la Core Console, realice una de las acciones siguientes:
 - En la pestaña Virtual Standby (En espera virtual), haga clic en **Add (Agregar)** para iniciar el asistente **Export Wizard (Asistente de exportación)**. En la página **Protected Machines (Máquinas protegidas)** del **Export Wizard (Asistente de exportación)**, seleccione la máquina protegida que desea exportar y, a continuación, haga clic en **Next (Siguiente)**.

- Navegue a la máquina que desea exportar y, en la pestaña **Summary (Resumen)** del menú desplegable **Actions (Acciones)** de esa máquina, haga clic en **Export** → **Virtual Standby (Exportar > En espera virtual)**.
2. En la página **Destination (Destino)** del asistente **Export Wizard (Asistente de exportación)**, haga clic en **Recover to a Virtual Machine** → **VMware Workstation (Recuperar en una máquina virtual > Estación de trabajo VMware)**.
 3. Haga clic en **Next (Siguiete)**.
 4. En la página **Virtual Machine Options (Opciones de máquina virtual)**, introduzca los parámetros para acceder a la máquina virtual tal como se describen en la tabla siguiente.

| Cuadro de texto | Descripción |
|------------------------|---|
| Target Path | <p>Especifique la ruta de acceso de la carpeta local o recurso compartido de red en el que crear la máquina virtual.</p> <p> NOTA: Si especificó una ruta de acceso de recurso compartido de red, introduzca credenciales de inicio de sesión válidas para una cuenta que esté registrada en la máquina de destino. La cuenta debe tener permisos de lectura y escritura para el recurso compartido de red.</p> |
| User Name | <p>Introduzca las credenciales de inicio de sesión para la máquina virtual.</p> <ul style="list-style-type: none"> • Si ha especificado una ruta de acceso de recurso compartido de red, debe introducir un nombre de usuario válido para una cuenta registrada en la máquina de destino. • Si ha especificado una ruta de acceso local, no hace falta nombre de usuario. |
| Password | <p>Introduzca las credenciales de inicio de sesión para la máquina virtual.</p> <ul style="list-style-type: none"> • Si ha especificado una ruta de acceso de recurso compartido de red, debe introducir una contraseña válida para una cuenta registrada en la máquina de destino. • Si ha especificado una ruta de acceso local, no hace falta contraseña. |
| Virtual Machine | <p>Introduzca un nombre para la máquina virtual que se está creando, por ejemplo, VM-0A1B2C3D4.</p> <p> NOTA: El nombre predeterminado es el nombre de la máquina origen.</p> |
| Version | <p>Especifique la versión de VMware Workstation (Estación de trabajo VMware) para la máquina virtual. Puede elegir las opciones siguientes:</p> <ul style="list-style-type: none"> • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 |
| Memory | <p>Para especificar la memoria para la máquina virtual, haga clic en una de las opciones siguientes:</p> <ul style="list-style-type: none"> • Use the same amount of RAM as the source machine (Utilizar la misma cantidad de RAM que la máquina de origen), para especificar que la configuración de RAM es la misma que en la máquina de origen. |

Cuadro de texto

Descripción

- Use a specific amount of RAM (Utilizar una cantidad de RAM específica), para especificar la cantidad de RAM a utilizar, por ejemplo, 4096 Megabytes (MB). La cantidad mínima permitida es 512 MB y la cantidad máxima se determina mediante la capacidad y las limitaciones de la máquina host.
5. Seleccione **Perform initial ad-hoc export (Realizar exportación ad hoc inicial)** para realizar la exportación virtual inmediatamente en lugar de después de la siguiente instantánea programada.
 6. Haga clic en **Next (Siguiendo)**.
 7. En la página **Volumes (Volúmenes)**, seleccione los volúmenes que se van a exportar; por ejemplo, C:\ y D:\, y haga clic en **Next (Siguiendo)**.
 8. En la página **Summary (Resumen)**, haga clic en **Finish (Finalizar)** para completar el asistente y para iniciar la exportación.



NOTA: Para supervisar el estado y el progreso de la exportación, visualice **Virtual Standby (En espera virtual)** o la pestaña **Events (Eventos)**.

Exportación de datos de Windows mediante exportación Hyper-V

En AppAssure, puede exportar datos mediante exportación de Hyper-V realizando una exportación única o continua. Lleve a cabo los pasos de los procedimientos siguientes para exportar mediante Hyper-V con el tipo adecuado de exportación.

Cómo realizar una exportación Hyper-V única

Para realizar una exportación Hyper-V única:

1. En la Core Console, navegue a la máquina que desee exportar.
2. En la ficha Summary (Resumen), haga clic en **Actions** → **Export** → **One-time** (Acciones > Exportar > Una vez).
El asistente **Export Wizard (Asistente de exportación)** se muestra en la página **Protected Machines (Máquinas protegidas)**.
3. Seleccione una máquina para exportarla y, a continuación, haga clic en **Next (Siguiendo)**.
4. En la página **Recovery Points (Puntos de recuperación)**, seleccione el punto de recuperación que desea exportar y, a continuación, haga clic en **Next (Siguiendo)**.

Definición de configuración única para realizar una exportación Hyper-V

Para definir la configuración única para realizar una exportación Hyper-V:

1. En el cuadro de diálogo Hyper-V, haga clic en **Use local machine (Utilizar máquina local)** para realizar la exportación Hyper-V a una máquina local con la función Hyper-V asignada.
2. Haga clic en la opción **Remote host (Host remoto)** para indicar que el servidor de Hyper-V se encuentra en una máquina remota. Si ha seleccionado la opción Remote host (Host remoto), introduzca los parámetros del host remoto, según se describe a continuación:

Cuadro de texto

Descripción

Host Name


Introduzca una dirección IP o un nombre de host para el servidor de Hyper-V. Representa la dirección IP o el nombre de host del servidor de Hyper-V remoto.

| Cuadro de texto | Descripción |
|------------------|---|
| Port | Introduzca un número de puerto para la máquina. Representa el puerto a través del cuál el Core se comunica con esta máquina. |
| User Name | Introduzca el nombre de usuario para el usuario con privilegios administrativos para la estación de trabajo con el servidor de Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual. |
| Password | Introduzca la contraseña de la cuenta de usuario con privilegios administrativos en la estación de trabajo con el servidor de Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual. |

3. Haga clic en **Next (Siguiente)**.
4. En la página **Opciones de Máquinas Virtuales** en la **VM Machine Location (Ubicación de la caché de metadatos)**, especifique la ruta de acceso o la ubicación de la máquina virtual. Por ejemplo, **D:\export**. La ubicación de la VM debe tener suficiente espacio para retener las unidades virtuales y los metadatos de VM necesarios para la máquina virtual.
5. Escriba el nombre de la máquina virtual en el campo **Virtual Machine Name (Nombre de la máquina virtual)**.
El nombre que especifique aparece en la lista de máquinas virtuales en la consola Hyper-V Manager (Administrador de Hyper-V).
6. Haga clic en una de las opciones siguientes:
 - **Use the same amount of RAM as the source machine (Utilizar la misma cantidad de RAM que la máquina de origen)**, para identificar que el uso de RAM es idéntico entre la máquina virtual y la máquina de origen.
 - **Use a specific amount of RAM (Utilizar una cantidad específica de RAM)**, para especificar la cantidad de memoria que la máquina virtual debería tener tras la exportación; por ejemplo, 4096 MB (recomendado).
7. Para especificar el formato del disco, junto a **Disk Format (Formato de disco)**, haga clic en una de las opciones siguientes:
 - **VHDX**
 - **VHD**

 **NOTA:** La exportación Hyper-V admite formatos de disco VHDX si la máquina de destino ejecuta Windows 8 (Windows Server 2012) o superior. Si el formato VHDX no es compatible para su entorno, la opción estará desactivada.
8. En la página **Volumes (Volúmenes)**, seleccione los volúmenes a exportar. Para que la máquina virtual de modo sea una copia de seguridad efectiva de la máquina protegida, incluya la unidad de inicio de la máquina protegida. Por ejemplo, C:\.
Para VHD, los volúmenes seleccionados no deberían tener un tamaño superior a 2040 GB. Si los volúmenes seleccionados tienen un tamaño de más de 2040 GB y se selecciona el formato VHD, recibirá un mensaje de error.
9. En la página **Summary (Resumen)**, haga clic en **Finish (Finalizar)** para completar el asistente y para iniciar la exportación.

Cómo realizar una exportación Hyper-V continua (en espera virtual)

-  **NOTA:** Solo la configuración de 3 TB con 2 VM de DL1000 es compatible con la exportación puntual y continua (modo de espera virtual).


Para realizar una exportación Hyper-V continua (en espera virtual):

1. En la Core Console, en la pestaña **Virtual Standby (En espera virtual)**, haga clic en **Add (Agregar)** para iniciar el asistente **Export Wizard (Asistente de exportación)**. En la página **Protected Machines (Máquinas protegidas)** del **Export Wizard (Asistente de exportación)**.
2. Seleccione la máquina que desea exportar y, a continuación, haga clic en **Next (Siguiente)**.
3. En la pestaña **Summary (Resumen)**, haga clic en **Export (Exportar)** → **Virtual Standby (En espera virtual)**.
4. En el cuadro de diálogo Hyper-V, haga clic en **Use local machine (Utilizar máquina local)** para realizar la exportación Hyper-V a una máquina local con la función Hyper-V asignada.
5. Haga clic en la opción **Remote host (Host remoto)** para indicar que el servidor de Hyper-V se encuentra en una máquina remota. Si ha seleccionado la opción Remote host (Host remoto), introduzca los parámetros del host remoto, según se describe a continuación:

| Cuadro de texto | Descripción |
|------------------|---|
| Host Name | Introduzca una dirección IP o un nombre de host para el servidor de Hyper-V. Representa la dirección IP o el nombre de host del servidor de Hyper-V remoto. |
| Port | Introduzca un número de puerto para la máquina. Representa el puerto a través del cuál el Core se comunica con esta máquina. |
| User Name | Introduzca el nombre de usuario para el usuario con privilegios administrativos para la estación de trabajo con el servidor de Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual. |
| Password | Introduzca la contraseña de la cuenta de usuario con privilegios administrativos en la estación de trabajo con el servidor de Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual. |

6. En la página **Virtual Machines Options (Opciones de Máquinas Virtuales)** en la **VM Machine Location (Ubicación de la máquina de VM)**, especifique la ruta de acceso o la ubicación de la máquina virtual. Por ejemplo, D:\export. La ubicación de la VM debe tener suficiente espacio para retener las unidades virtuales y los metadatos de VM necesarias para la máquina virtual.
7. Escriba el nombre de la máquina virtual en el campo **Virtual Machine Name (Nombre de la máquina virtual)**.
El nombre que especifique aparece en la lista de máquinas virtuales en la consola Hyper-V Manager (Administrador de Hyper-V).
8. Haga clic en una de las opciones siguientes:
 - **Use the same amount of RAM as the source machine (Utilizar la misma cantidad de RAM que la máquina de origen)**, para identificar que el uso de RAM es idéntico entre la máquina virtual y la máquina de origen.
 - **Use a specific amount of RAM (Utilizar una cantidad específica de RAM)**, para especificar la cantidad de memoria que la máquina virtual debería tener tras la exportación; por ejemplo, 4096 MB.
9. Para especificar la generación, haga clic en una de las siguientes opciones:
 - Generation 1 (Generación 1) (recomendado)
 - Generation 2 (Generación 2)
10. Para especificar el formato del disco, junto a **Disk Format (Formato de disco)**, haga clic en una de las opciones siguientes:
 - **VHDX** (valor predeterminado)


- **VHD**

 **NOTA:** Hyper-V Export admite formatos de disco VHDX en caso de que la máquina de destino esté ejecutando Windows 8 (Windows Server 2012) o superior. Si el VHDX no es compatible para su entorno, la opción está desactivada. En la página Network Adapters (Adaptadores de red), seleccione el adaptador virtual para conectarse a un conmutador.

11. En la página **Volumes (Volúmenes)**, seleccione los volúmenes a exportar. Para que la máquina virtual de modo sea una copia de seguridad efectiva de la máquina protegida, incluya la unidad de inicio de la máquina protegida. Por ejemplo, C:\.

Para VHD, los volúmenes seleccionados no deberían tener un tamaño superior a 2040 GB. Si los volúmenes seleccionados tienen un tamaño de más de 2040 GB y se selecciona el formato VHD, recibirá un mensaje de error.


12. En la página **Summary (Resumen)**, haga clic en **Finish (Finalizar)** para completar el asistente y para iniciar la exportación.

 **NOTA:** Para supervisar el estado y el progreso de la exportación, visualice **Virtual Standby (En espera virtual)** o la pestaña **Events (Eventos)**.

Exportación de datos de Windows mediante exportación de VirtualBox de Oracle

En AppAssure, puede elegir exportar datos mediante una exportación de VirtualBox realizando una exportación única o continua mediante el establecimiento de una exportación continua (en espera virtual).

Realice los pasos de los procedimientos siguientes para el tipo de exportación adecuado.

 **NOTA:** Para realizar este tipo de exportación, debe tener VirtualBox de Oracle instalado en la máquina del Core. VirtualBox Versión 4.2.18 o superior se admite para hosts Windows.


Cómo realizar una exportación Oracle VirtualBox única

Para realizar una exportación Oracle VirtualBox única:

1. En la Core Console, navegue a la máquina Linux que desea exportar.
2. En la pestaña **Summary (Resumen)**, haga clic en **Actions (Acciones)** → **Export (Exportar)** → **One-time (Único)**.
El asistente **Export Wizard (Asistente de exportación)** se muestra en la página **Protected Machines (Máquinas protegidas)**.
3. Seleccione una máquina para exportarla y, a continuación, haga clic en **Next (Siguiente)**.
4. En la página **Recovery Points (Puntos de recuperación)**, seleccione el punto de recuperación que desea exportar y, a continuación, haga clic en **Next (Siguiente)**.
5. En la página **Destination (Destino)** del asistente **Export Wizard (Asistente de exportación)**, en el menú desplegable **Recover to Virtual machine (Recuperar a máquina virtual)**, seleccione **VirtualBox** y haga clic en **Next (Siguiente)**.
6. En la página **Virtual Machine Options (Opciones de máquina virtual)**, seleccione **Remote Linux Machine (Máquina Linux remota)**.
7. Introduzca los parámetros para acceder a la máquina virtual, como se indica a continuación:

| Cuadro de texto | Descripción |
|-----------------------------|--|
| VirtualBox Host Name | Introduzca una dirección IP o un nombre de host para el servidor de VirtualBox. Este campo representa la dirección IP o el nombre de host del servidor de VirtualBox remoto. |
| Port | Introduzca un número de puerto para la máquina. Este número representa el puerto a través del cuál el Core se comunica con esta máquina. |
| Virtual Machine Name | Especifique una ruta de destino para crear la máquina virtual. |
| User Name | El nombre de usuario de la cuenta en la máquina de destino, por ejemplo, root. |
| Password | Introduzca las credenciales de inicio de sesión para la máquina host. |
| Memory | Especifique la memoria para la máquina virtual. |


- En la página **Volumes (Volúmenes)**, seleccione los volúmenes de datos que desea exportar y, a continuación, haga clic en **Next (Siguiente)**.
- En la página **Summary (Resumen)**, haga clic en **Finish (Finalizar)** para completar el asistente y para iniciar la exportación.

 **NOTA:** Para supervisar el estado y el progreso de la exportación, visualice Virtual Standby (En espera virtual) o la pestaña Events (Eventos).

Cómo realizar una exportación VirtualBox de Oracle continua (en espera virtual)

Para realizar una exportación VirtualBox continua (en espera virtual):

- En la Core Console, realice una de las acciones siguientes:
 - En la pestaña **Virtual Standby (En espera virtual)**, haga clic en **Add (Agregar)** para iniciar el asistente **Export Wizard (Asistente de exportación)**. En la página **Protected Machines (Máquinas protegidas)** del asistente **Export Wizard (Asistente de exportación)**, seleccione la máquina protegida que desea exportar y, a continuación, haga clic en **Next (Siguiente)**.
 - Navegue a la máquina que desea exportar y, en la pestaña **Summary (Resumen)** del menú desplegable **Actions (Acciones)** de esa máquina, haga clic en **Export → Virtual Standby (Exportar > En espera virtual)**.
- En la página **Destination (Destino)** del **Export Wizard (Asistente de exportación)**, en el menú desplegable **Recover to Virtual machine (Recuperar a máquina virtual)**, seleccione **VirtualBox** y, a continuación, haga clic en **Next (Siguiente)**.
- En la página **Virtual Machine Options (Opciones de máquina virtual)**, seleccione **Use Windows machine (Usar máquina con Windows)**.
- Especifique los parámetros para acceder a la máquina virtual, según se describen en la tabla siguiente.

| Cuadro de texto | Descripción |
|-----------------------------|---|
| Virtual Machine Name | Introduzca un nombre para la máquina virtual que se está creando.  NOTA: El nombre predeterminado es el nombre de la máquina origen. |
| Target Path | Especifique una ruta de destino local o remoto para crear la máquina virtual. |

Cuadro de texto

Descripción



NOTA: La ruta de destino no debe ser un directorio raíz.

Si ha especificado una ruta de recurso compartido de red, tendrá que escribir credenciales de inicio de sesión válidas (nombre de usuario y contraseña) de una cuenta que esté registrada en la máquina de destino. La cuenta debe tener permisos de lectura y escritura en el recurso compartido de red.

Memory

Especifique la memoria para la máquina virtual.

- Haga clic en **Use the same amount of RAM as the source machine (Utilizar la misma cantidad de RAM que la máquina de origen)** para especificar que la configuración de RAM es la misma que en la máquina de origen.
 - Haga clic en **Use a specific amount of RAM (Utilizar una cantidad de RAM específica)** para especificar la cantidad de RAM a utilizar; por ejemplo, 4096 Megabytes (MB). La cantidad mínima permitida es 512 MB y la cantidad máxima se determina mediante la capacidad y las limitaciones de la máquina host.
5. Para especificar la cuenta de usuario de la máquina virtual, seleccione **Specify the user account for the exported virtual machine (Especificar la cuenta de usuario para la máquina virtual exportada)** y, a continuación, introduzca la información siguiente. Es información que hace referencia a una cuenta de usuario específica para la que se registrará la máquina virtual en el caso de que haya varias cuentas de usuario en la máquina virtual. Cuando se inicie una sesión con esta cuenta de usuario, solo este usuario verá esta máquina virtual en el administrador de VirtualBox. Si no se especifica ninguna cuenta, la máquina virtual se registrará para todos los usuarios existentes en la máquina de Windows con VirtualBox.
 - User name (Nombre de usuario): introduzca el nombre de usuario para el que se ha registrado la máquina virtual.
 - Password (Contraseña): escriba la contraseña para esta cuenta de usuario.
 6. Seleccione **Perform initial ad-hoc export (Realizar exportación ad hoc inicial)** para realizar la exportación virtual inmediatamente en lugar de después de la siguiente instantánea programada.
 7. Haga clic en **Next (Siguiente)**.
 8. En la página **Volumes (Volúmenes)**, seleccione los volúmenes que se van a exportar; por ejemplo, C:\ y D:\ y, a continuación, haga clic en **Next (Siguiente)**.
 9. En la página **Summary (Resumen)**, haga clic en **Finish (Finalizar)** para completar el asistente y para iniciar la exportación.




NOTA: Para supervisar el estado y el progreso de la exportación, visualice **Virtual Standby (En espera virtual)** o la pestaña **Events (Eventos)**.

Restauración de volúmenes desde un punto de recuperación


Puede restaurar los volúmenes en una máquina protegida desde los puntos de recuperación almacenados en el AppAssure Core. Para restaurar volúmenes desde un punto de recuperación:

1. En la Core Console, haga clic en la ficha **Restore (Restaurar)**.
Aparece el asistente **Restore Machine Wizard (Asistente de restaurar máquinas)**.
2. Desde la página **Protected Machines (Máquinas protegidas)**, seleccione la máquina protegida para la que desea restaurar datos y, a continuación, haga clic en **Next (Siguiente)**.

 **NOTA:** La máquina protegida debe tener el software del Agent instalado y debe tener los puntos de recuperación desde los cuales va a realizar la operación de restauración.

Se abrirá la página **Recovery Points (Puntos de recuperación)**.

3. En la lista de puntos de recuperación, busque la instantánea que desea restaurar en la máquina Agent.

 **NOTA:** Si es necesario, utilice los botones de navegación en la parte inferior de la página para ver los puntos de recuperación adicionales. O bien, si desea limitar la cantidad de puntos de recuperación que se muestran en la página Recovery Points (Puntos de recuperación) del asistente, puede filtrar por los volúmenes (si se han definido) o por la fecha de creación del punto de recuperación.

4. Haga clic en cualquier punto de recuperación para seleccionarlo y, a continuación, haga clic en **Next (Siguiente)**.

Se abrirá la página **Destination (Destino)**.

5. En la página **Destination (Destino)**, seleccione la máquina para la que desea restaurar datos de la manera siguiente:
 - Si desea restaurar datos desde el punto de recuperación seleccionado a la misma máquina Agent (por ejemplo, Machine1) y si los volúmenes que desea restaurar no incluyen el volumen del sistema, seleccione **Recover to a protected machine (only non-system volumes) (Recuperar a una máquina protegida (solamente volúmenes que no son del sistema))**, compruebe que la máquina de destino (Machine1) esté seleccionada y, a continuación, haga clic en **Next (Siguiente)**. Aparecerá la página **Volume Mapping (Asignación de volúmenes)**. Continúe en el paso 7.
 - Si desea restaurar datos desde el punto de recuperación seleccionado para una máquina protegida diferente (por ejemplo, para reemplazar el contenido de Machine2 con datos de Machine1), seleccione **Recover to a protected machine (only non-system volumes) (Recuperar a una máquina protegida (solamente volúmenes que no son del sistema))**, seleccione la máquina de destino (por ejemplo, Machine2) en la lista y, a continuación, haga clic en **Next (Siguiente)**. Aparecerá la página **Volume Mapping (Asignación de volúmenes)**. Continúe en el paso 7.
 - Si desea restaurar desde el punto de recuperación seleccionado a la misma máquina o una máquina diferente utilizando un CD de inicio y si los volúmenes que desea restaurar no incluyen el volumen del sistema, seleccione **Recover to any target machine using a boot CD (Recuperar a cualquier máquina de destino utilizando un CD de inicio)**.
 - Para continuar y crear el CD de inicio con información del punto de recuperación seleccionado, haga clic en **Next (Siguiente)** y continúe en el paso 10.
 - Si ya ha creado el CD de inicio y la máquina de destino se ha empezado a utilizar con el CD de inicio, continúe en el paso 17.
 - Si desea realizar una restauración a partir de un punto de recuperación en un volumen del sistema (por ejemplo, la unidad C de la máquina Agent llamada Machine1), debe realizar una restauración desde cero (BMR). Para obtener más información sobre el modo de llevar a cabo una restauración desde cero (BMR) para Windows, consulte [Cómo iniciar la restauración desde cero para máquinas Windows](#).
 - Para obtener más información sobre el modo de llevar a cabo una restauración desde cero (BMR) para Linux, consulte [Cómo iniciar una restauración desde cero para una máquina Linux](#), en el Plan para realizar una restauración desde cero para máquinas Linux.
6. Para conectarse a la Consola de recuperación universal (URC) en la máquina de destino, haga lo siguiente:
 - a. Seleccione **I already have a boot CD running on the target machine (Ya tengo un CD de inicio y se está ejecutando en la máquina de destino)**.
 - b. En el cuadro de texto IP Address (Dirección IP), introduzca la dirección IP de la máquina de destino con el CD de inicio.


- c. En el cuadro de texto Authentication Key (Clave de autenticación), introduzca la clave de autenticación del URC en la máquina de destino y, a continuación, haga clic en **Next (Siguiente)**. Aparecerá la página **Disk Mapping (Asignación de disco)**. Continúe en el paso 20.
7. En la página **Volume Mapping (Asignación de volumen)**, para cada volumen en el punto de recuperación que desea restaurar, seleccione el volumen de destino. Si no desea restaurar ningún volumen, en la columna Destination Volumes (Volúmenes de destino), seleccione **Do not restore (No restaurar)**.
8. Seleccione **Show advanced options (Mostrar opciones avanzadas)** y, a continuación, haga lo siguiente:
- Para restaurar en máquinas Windows, si desea utilizar Live Recovery, seleccione **Live Recovery**. El uso de la tecnología de recuperación instantánea Live Recovery en AppAssure, permite recuperar o restaurar instantáneamente datos a sus máquinas físicas o a máquinas virtuales a partir de puntos de recuperación almacenados de máquinas de Windows, que incluyen los espacios de almacenamiento de Microsoft Windows. Live Recovery no está disponible para máquinas Linux.
 - Si desea forzar el desmontaje, seleccione **Force Dismount (Forzar desmontaje)**. Si no fuerza un desmontaje antes de restaurar los datos, es posible que la restauración falle con un error de volumen en uso.
9. Continúe en el paso 20.
10. En la página Boot CD (CD de inicio), realice estos pasos:
- a. En el campo de texto **Output path (Ruta de salida)**, escriba la ruta de acceso en la que se debe almacenar la imagen ISO del CD de inicio.
 - b. En **Environment (Entorno)**, seleccione la arquitectura más adecuada para el hardware que está restaurando:
 - Para restaurar en cualquier máquina Windows con una arquitectura de 64 bits, seleccione **Windows 8 64-bit (Windows 8 de 64 bits)**.
 - Para restaurar en cualquier máquina Windows con una arquitectura de 32 bits (x86), seleccione **Windows 7 32-bit (Windows 7 de 32 bits)**.
11. Opcionalmente, para configurar los parámetros de red del Agent restaurado, o para usar UltraVNC, seleccione **Show advanced options (Mostrar opciones avanzadas)** y realice una de las acciones siguientes:
- Para establecer una conexión de red en la máquina que se ha restaurado, seleccione **Use the following IP address (Usar la siguiente dirección IP)** tal y como se describe en la tabla siguiente.

| Opción | Descripción |
|------------------------|---|
| IP Address | Especifique una dirección IP o un nombre de host para la máquina restaurada. |
| Subnet Mask | Especifique la máscara de subred para la máquina restaurada. |
| Default Gateway | Especifique la puerta de enlace predeterminada de la máquina restaurada. |
| DNS Server | Especifique el servidor de nombre de dominio para la máquina restaurada. |
| | <ul style="list-style-type: none"> • Para definir la información de UltraVNC, seleccione Add UltraVNC (Agregar UltraVNC) como se describe en la tabla siguiente. Utilice esta opción si necesita acceso remoto a la consola de recuperación. Mientras utiliza el CD de inicio, no podrá iniciar sesión en los servicios de Microsoft Terminal Server. |

| Opción | Descripción |
|-----------------|---|
| Password | Especifique una contraseña para esta conexión UltraVNC. |

| Opción | Descripción |
|--------|--|
| Port | Especifique un puerto para esta conexión UltraVNC. El puerto predeterminado es 5900. |


12. Haga clic en **Next (Siguiente)**.
13. Para insertar un controlador, haga lo siguiente:
 - a. Seleccione **Add an archive of drivers (Agregar un archivo de controladores)**.
 - b. Navegue al fichero ZIP que contiene el archivo, seleccione el fichero ZIP y haga clic en **Open (Abrir)**. El archivo se cargará y aparece en la página Driver Injection (Inserción de controlador).
 - c. A continuación, haga clic en **Next (Siguiente)**.
14. En la página ISO Image (Imagen ISO), puede ver el estado en el que se crea la imagen ISO del CD de inicio. Cuando el CD de inicio sea correcto, haga clic en **Next (Siguiente)**. Aparecerá la página **Connection (Conexión)**.
15. Inicie la máquina Agent para la que desea restaurar datos desde el CD de inicio.
 - Inicie la máquina Agent a partir de una imagen ISO, si es posible.
 - Si no lo es, copie la imagen ISO en medios físicos (un CD o un DVD), cargue el disco en la máquina Agent, configure la máquina que se cargará desde el CD de inicio y arranque desde el CD de inicio.

 **NOTA:** Quizá tenga que cambiar la configuración del BIOS de la máquina Agent para asegurarse de que el volumen que se carga primero es el CD de inicio.


Cuando se inicia desde el CD de inicio, la máquina Agent muestra la interfaz de la Consola de recuperación universal (URC). Este entorno se utiliza para restaurar la unidad del sistema o volúmenes seleccionados directamente desde AppAssure Core. Anote la dirección IP y las credenciales de la clave de autenticación de la URC, que se actualizan cada vez que se arranca desde el CD de inicio.

16. En la página **Connection (Conexión)** de la Core Console, introduzca la información de autenticación de la instancia URC de la máquina que desea restaurar, como se indica a continuación:
 - a. En el cuadro de texto IP Address (Dirección IP), introduzca la dirección IP de la máquina a la que va a restaurar desde un punto de recuperación.
 - b. En el cuadro de texto Authentication Key (Clave de autenticación), introduzca la información de la URC.
 - c. Haga clic en **Next (Siguiente)**.
Se abrirá la página **Disk Mapping (Asignación de disco)**.


17. Para asignar volúmenes manualmente, continúe en el paso 18. Para asignar volúmenes automáticamente, proceda del modo siguiente:
 - a. Seleccione **Automatic volume mapping (Asignación automática de volúmenes)**.
 - b. En el área **Automatic volume mapping (Asignación automática de volúmenes)**, seleccione los volúmenes que desea restaurar. Si no desea restaurar un volumen de la lista, desactive la opción.

 **NOTA:** Para realizar la restauración, se debe seleccionar como mínimo un volumen.

18. Si desea asignar volúmenes manualmente, proceda del modo siguiente:
 - a. Seleccione **Manual volume mapping (Asignación manual de volúmenes)**.
 - b. En el área **Manual volume mapping (Asignación manual de volúmenes)**, en la lista desplegable **Destination Volumes (Volúmenes de destino)** de cada volumen, seleccione el volumen que desee restaurar. Si no desea restaurar un volumen de la lista, desactive la opción.


 **NOTA:** Para realizar la restauración, se debe seleccionar como mínimo un volumen.

c. Haga clic en **Finish (Finalizar)**.

 **PRECAUCIÓN:** Si selecciona **Finish (Finalizar)**, todas las particiones y datos de la unidad de destino se eliminarán de manera permanente, y se reemplazarán por el contenido del punto de recuperación seleccionado, incluido el sistema operativo y los datos.

El **Restore Machine Wizard (Asistente para restaurar máquinas)** se cerrará y los datos se restaurarán desde los volúmenes seleccionados del punto de recuperación para la máquina de destino. Continúe en el paso 22.

19. En la página **Disk Mapping Preview (Vista previa de asignación de discos)**, revise los parámetros de la restauración de las acciones que haya seleccionado. Para realizar la restauración, haga clic en **Finish (Finalizar)**.

 **PRECAUCIÓN:** Si selecciona **Finish (Finalizar)**, todas las particiones y datos de la unidad de destino se eliminarán de manera permanente, y se reemplazarán por el contenido del punto de recuperación seleccionado, incluido el sistema operativo y los datos.

El **Restore Machine Wizard (Asistente para restaurar máquinas)** se cerrará y los datos se restaurarán desde los volúmenes seleccionados del punto de recuperación para la máquina de destino. Continúe en el paso 22.

20. Si los volúmenes que desea restaurar contienen bases de datos SQL o Microsoft Exchange, en la página **Dismount Databases (Desmontar bases de datos)**, se le solicitará que los desmonte. De manera opcional, si desea volver a montar estas bases de datos después de que se complete la restauración, seleccione **Automatically remount all databases after the recovery point is restored (Volver a montar automáticamente todas las bases de datos después de que se restaure el punto de recuperación)**. Haga clic en **Finish (Finalizar)**.

21. Haga clic en **OK (Aceptar)** para confirmar el mensaje de estado que indica que el proceso de restauración ha empezado.

22. Para supervisar el progreso de la acción de restauración, haga clic en **Events (Eventos)** en la Core Console.

Restauración de volúmenes para una máquina Linux mediante la línea de comandos

En AppAssure, puede restaurar volúmenes de sus máquinas Linux protegidas mediante la utilidad de línea de comandos `aamount`. Para restaurar volúmenes de una máquina Linux mediante la línea de comandos:

 **PRECAUCIÓN:** No debe intentar restaurar el sistema o el volumen raíz (/).

1. Ejecute la utilidad `aamount` de AppAssure como raíz, por ejemplo:

```
sudo aamount
```

2. En la solicitud de montaje de AppAssure, introduzca el siguiente comando para enumerar las máquinas protegidas:

```
lm
```

3. Cuando se le solicite, introduzca la dirección IP o nombre del host del servidor AppAssure Core.

4. Introduzca las credenciales de inicio de sesión, es decir, el nombre de usuario y la contraseña, para este servidor.

Se muestra una lista con las máquinas que el servidor de AppAssure protege. En la lista, aparecerán las máquinas de Agent encontradas por número de elemento de línea, host/dirección IP y el número de Id. de la máquina (por ejemplo: 293cc667-44b4-48ab-91d8-44bc74252a4f).

5. Introduzca el siguiente comando para enumerar los puntos de recuperación actualmente montados para la máquina especificada:

```
lr <machine_line_item_number>
```



NOTA: También puede introducir el número de Id. de la máquina en lugar del número de elemento de línea.

Aparece una lista que muestra los puntos de recuperación básicos e incrementales de dicha máquina. Esta lista incluye un número de elemento de línea, fecha/fecha y hora, ubicación de volumen, tamaño de punto de recuperación y un número de Id. para el volumen que incluye un número de secuencia al final (por ejemplo, "293cc667-44b4-48ab-91d8-44bc74252a4f:2"), que identifica el punto de recuperación.

6. Para seleccionar el punto de recuperación que se va a revertir, introduzca el siguiente comando:

```
r [volume_recovery_point_ID_number] [path]
```

Este comando revierte la imagen de volumen especificada por el Id. del Core en la ruta de acceso especificada. La ruta de acceso para la reversión es la ruta de acceso para el descriptor de archivo de dispositivo y no el directorio en el que está montado.



NOTA: Para identificar el punto de recuperación, también puede especificar un número de línea en el comando en lugar del número de Id. de punto de recuperación. En dicho caso, utilice el número de línea de máquina/Agent (en la salida de `lm`), seguido del número de línea de punto de recuperación y de la letra del volumen, seguido de la ruta de acceso, por ejemplo, `r [machine_line_item_number] [recovery_point_line_number] [volume_letter] [path]`. En este comando, `[path]` es el descriptor de archivo del volumen real.

Por ejemplo, si la salida de `lm` muestra tres máquinas de Agent, ha introducido el comando `lr` para el número 2 y desea revertir el volumen `b` del punto de recuperación 23 al volumen que se montó en el directorio `/mnt/data`, el comando será: `r2 23 b /mnt/data`.

7. Si se le solicita que continúe, escriba `y` para Sí.
Mientras continúe la reversión, aparecerán una serie de mensajes para notificarle el estado.
8. Tras una reversión satisfactoria, la utilidad `aamount` monta automáticamente el módulo de núcleo y vuelve a conectarlo al volumen revertido si el destino estaba previamente protegido y montado. Si no, monte el volumen de reversión en el disco local y, a continuación, verifique que los archivos estén restaurados.

Por ejemplo, puede usar el comando `sudo mount y`, a continuación, el comando `ls`.

Cómo iniciar la restauración desde cero para máquinas Windows

AppAssure ofrece la posibilidad de realizar una restauración desde cero (BMR) de las máquinas Windows, independientemente de que el hardware sea similar o distinto. Este proceso conlleva la creación de una imagen de CD de inicio, grabar la imagen en disco, iniciar el servidor de destino desde el disco, conectarse a la instancia de la consola de recuperación, asignar volúmenes, inicializar la recuperación y, a continuación, supervisar el proceso. Una vez terminada la restauración desde cero, podrá continuar con la tarea de cargar el sistema operativo y las aplicaciones de software en el servidor restaurado, seguida de sus valores y configuración únicos.

Otras circunstancias en las que puede decidir realizar una restauración desde cero incluyen una actualización de hardware o la sustitución del servidor.

La funcionalidad BMR también es compatible con las máquinas protegidas Linux gracias a la utilidad de línea de comandos `aaamount`. Para obtener más información, consulte [Cómo iniciar una restauración desde cero para una máquina Linux](#).

Plan para realizar una restauración desde cero para una máquina Windows


Para realizar una restauración desde cero -BMR para una máquina Windows:

1. Cree un CD de inicio.
2. Grabe la imagen en el disco.
3. Inicie el servidor de destino desde el CD de inicio.
4. Conéctese al disco de recuperación.
5. Asigne los volúmenes.
6. Inicie la recuperación.
7. Supervise el progreso.

Creación de la imagen ISO de un CD de inicio

Para realizar una restauración completa (BMR) en una máquina de Windows, cree primero una imagen de CD/ISO de inicio en la Core Console, que contenga la interfaz de la AppAssure Universal Recovery Console (Consola de recuperación universal de AppAssure). Esta Consola es un entorno que permite restaurar una unidad del sistema o todo el servidor directamente desde el AppAssure Core.

La imagen ISO que cree se adapta a la máquina que se va a restaurar; por lo tanto, debe incluir los controladores de almacenamiento masivo y red correctos. Si piensa que va a restaurar en un hardware diferente al de la máquina en la que creará el CD de inicio, deberá incluir una controladora de almacenamiento y otros controladores en el CD de inicio. Consulte [Inserción de controladores en un CD de inicio](#)

 **NOTA:** La Organización Internacional de Normalización (ISO) es un organismo internacional de representantes de diversas organizaciones nacionales que determinan y establecen los estándares de sistema de archivos. La ISO 9660 es un estándar de sistema de archivos que se utiliza con medios de disco óptico para el intercambio de datos y que admite diversos sistemas operativos, como por ejemplo, Windows. Una imagen ISO es el archivo de archivado o imagen de disco, que contiene datos de cada sector del disco, así como el sistema de archivos de disco.

Para crear una imagen ISO de un CD de inicio:


1. En la Core Console en la que se ubica el servidor que desea restaurar, seleccione el **Core** y, a continuación, haga clic en la ficha **Tools (Herramientas)**.
2. Haga clic en **Boot CDs (CD de inicio)**.
3. Seleccione **Actions (Acciones)** y, a continuación, haga clic en **Create Boot ISO (Crear ISO de inicio)**. Aparecerá el cuadro de diálogo **Create Boot CD (Crear CD de inicio)**. Para completar el cuadro de diálogo, realice los siguientes procedimientos.

Asignación de nombre del archivo del CD de inicio y configuración de la ruta de acceso

Para asignar un nombre al archivo del CD de inicio y configurar la ruta de acceso:

En el cuadro de diálogo **Create Boot CD (Crear CD de inicio)**, especifique la ruta ISO donde se almacenará la imagen de inicio en el servidor del Core.


Si al recurso compartido en el que desea almacenar la imagen le queda poco espacio, puede establecer la ruta de acceso según sea necesario; por ejemplo, D:\filename.iso.

 **NOTA:** La extensión del archivo debe ser .iso. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host de los dominios). Las letras de la "a" a la "z" no distinguen mayúsculas de minúsculas. No utilice espacios. No se admite ningún otro símbolo o caracteres de puntuación.

Creación de conexiones

Para crear conexiones:


1. En **Connection Options (Opciones de conexión)**, haga lo siguiente:
 - Para obtener la dirección IP de manera dinámica mediante el Protocolo de configuración dinámica de host (DHCP), seleccione **Obtain IP address automatically (Obtener dirección IP automáticamente)**.
 - De manera opcional, para especificar una dirección IP estática para la consola de recuperación, seleccione **Use the following IP address (Usar la siguiente dirección IP)** y escriba la dirección IP, la máscara de subred, la puerta de enlace predeterminada y el servidor DNS en los campos correspondientes. Deberá introducir todos los campos.
2. Si se le solicita, en **UltraVNC Options (Opciones de UltraVNC)**, seleccione **Add UltraVNC (Agregar UltraVNC)** y, a continuación, escriba las opciones UltraVNC. La configuración de UltraVNC permite administrar la consola de recuperación de manera remota mientras se usa.

 **NOTA:** Este paso es opcional. Si necesita acceso remoto a la consola de recuperación, deberá configurar y usar UltraVNC. No podrá iniciar sesión con Microsoft Terminal Services mientras utiliza el CD de inicio.

Inserción de controladores en un CD de inicio

La inserción del controlador se utiliza para facilitar la operabilidad entre la consola de recuperación, el adaptador de red y el almacenamiento en el servidor de destino.

Si piensa que va a restaurar en hardware diferente, deberá incluir una controladora de almacenamiento, un disco RAID, una interfaz AHCI, un conjunto de chips u otros controladores en el CD de inicio. Estos controladores permiten que el sistema operativo detecte todos los dispositivos y funcione correctamente en ellos.

 **NOTA:** Tenga en cuenta que el CD de inicio incluye controladores de Windows 7 PE de 32 bits de manera automática.

Para insertar controladores en un CD de inicio:

1. Descargue los controladores del sitio web del fabricante para el servidor y descomprímalos.
2. Comprima la carpeta que contiene los controladores mediante una utilidad de compresión de archivos, por ejemplo, WinZip.
3. En el cuadro de diálogo **Create Boot CD (Crear CD de inicio)**, en el panel **Drivers (Controladores)**, haga clic en **Add a Driver (Agregar un controlador)**.
4. Para buscar el archivo de controladores comprimido, vaya al sistema de archivos. Seleccione el archivo y haga clic en **Open (Abrir)**.


Los controladores insertados se resaltan en el panel **Drivers (Controladores)**.

Creación del CD de inicio

Para crear un CD de inicio, asígnele un nombre y especifique una ruta y, después, cree una conexión e inserte los controladores de manera opcional. En la pantalla **Create Boot CD (Crear CD de inicio)**, haga clic en **Create Boot CD (Crear CD de inicio)**. A continuación, se creará la imagen ISO.

Visualización del progreso de creación de la imagen ISO

Para ver el progreso de la creación de la imagen ISO, seleccione la pestaña **Events (Eventos)** y, a continuación en **Tasks (Tareas)**, puede supervisar el progreso para crear una imagen ISO.

 **NOTA:** También puede ver el progreso de la creación de la imagen ISO en el cuadro de texto **Monitor Active Task (Supervisar tarea activa)**.


Cuando la creación de la imagen ISO esté completada, estará disponible en la página **Boot CDs (CD de inicio)**, a la que se puede acceder desde el menú **Tools (Herramientas)**.

Acceso a la imagen ISO

Para acceder a la imagen ISO, navegue a la ruta de acceso de salida que ha especificado, o bien haga clic en el enlace para descargar la imagen en una ubicación desde la que podrá cargarla al nuevo sistema. Por ejemplo, una unidad de red.

Cómo cargar un CD de inicio

Cuando haya creado la imagen del CD de inicio, inicie el servidor de destino con el CD de inicio que acaba de crear.


 **NOTA:** Si ha creado el CD de inicio mediante DHCP, anote la dirección IP y la contraseña.

Para cargar un CD de inicio:

1. Vaya al nuevo servidor, cargue el CD de inicio e inicie la máquina.
2. Elija **Boot from CD-ROM (Iniciar desde el CD-ROM)**, que cargará lo siguiente:
 - Windows 7 PE
 - El software AppAssure Agent

Se inicia la AppAssure Universal Recovery Console (Consola de recuperación universal) y muestra la dirección IP y la contraseña de autenticación de la máquina.


3. Anote la dirección IP que aparece en el panel Network Adapters Settings (Configuración de adaptadores de red) y la contraseña de autenticación que se muestra en el panel Authentication (Autenticación). Necesitará esta información más adelante, durante el proceso de recuperación de datos, para volver a iniciar sesión en la consola.
4. Si desea cambiar la dirección IP, selecciónela y haga clic en **Change (Cambiar)**.

 **NOTA:** Si especificó una dirección IP en el cuadro de diálogo Create Boot CD (Crear CD de inicio), la Universal Recovery Console la utiliza y la muestra en la pantalla **Network Adapters Settings (Configuración de adaptadores de red)**.

Inserción de controladores en el servidor de destino

Si va a restaurar en hardware diferente, debe insertar una controladora de almacenamiento, un disco RAID, una interfaz AHCI, un conjunto de chips u otros controladores, en caso de que aún no estén incluidos en el CD de inicio. Estos controladores permiten que el sistema operativo funcione en todos los dispositivos del servidor de destino correctamente.

Si desconoce los controladores que requiere su servidor de destino, haga clic en la pestaña System Info (Información del sistema) en la Consola de recuperación universal. En esta pestaña se muestran todos los tipos de dispositivo y de hardware de sistema del servidor de destino que desea restaurar.

 **NOTA:** Tenga en cuenta que el servidor de destino incluye controladores de Windows 7 PE de 32 bits de manera automática.



Para insertar controladores en el servidor de destino:

1. Descargue los controladores del sitio web del fabricante para el servidor y descompríalos.
2. Comprima la carpeta que contiene los controladores mediante una utilidad de compresión de archivos (por ejemplo, Win Zip) y cópiela en el servidor de destino.
3. En la Consola de recuperación universal, haga clic en **Driver Injection (Inserción de controlador)**.
4. Para buscar el archivo de controladores comprimido, vaya al sistema de archivos y selecciónelo.
5. Si hizo clic en **Driver Injection (Inserción de controlador)** en el paso 3, haga clic en **Add Driver (Agregar controlador)**. Si eligió **Load driver (Cargar controlador)** en el paso 3, haga clic en **Open (Abrir)**.

Los controladores seleccionados se insertarán y se cargarán en el sistema operativo después de reiniciar el servidor de destino.

Cómo iniciar una restauración desde el Core

Para iniciar una restauración desde el Core:

1. Si las NIC de cualquier sistema que se estén restaurando están en equipo (asociadas), quite todas salvo una de los cables de red.
 **NOTA:** La restauración de AppAssure no reconoce NIC en equipo. El proceso no puede resolver qué NIC usar si está presente con más de una conexión activa.
2. Vuelva al servidor del Core y abra la Core Console.
3. En la pestaña **Machines (Máquinas)**, seleccione la máquina desde la que desea restaurar datos.
4. Haga clic en el menú **Actions (Acciones)** de la máquina, haga clic en **Recovery Points (Puntos de recuperación)** para ver una lista de todos los puntos de recuperación de esa máquina.
5. Expanda el punto de recuperación desde el que desea restaurar y, a continuación, haga clic en **Rollback (Revertir)**.
6. En el cuadro de diálogo **Rollback (Revertir)**, en **Choose Destination (Elegir destino)**, seleccione **Recovery Console Instance (Instancia de la consola de recuperación)**.
7. En los cuadros de texto **Host** y **Password (Contraseña)**, introduzca la dirección IP y la contraseña de autenticación del nuevo servidor en el que desea restaurar datos.
 **NOTA:** Los valores de Host y Password (Contraseña) son las credenciales que ha grabado en la tarea anterior. Para obtener más información, ver [Cómo cargar un CD de inicio](#).
8. Haga clic en **Load Volumes (Cargar volúmenes)** para cargar los volúmenes de destino en la nueva máquina.

Asignación de volúmenes


Puede asignar volúmenes a los discos del servidor de destino de forma automática o manual. Para alinear los discos automáticamente, el disco se debe limpiar y volver a particionar y todos los datos se eliminarán. La alineación se realiza en el orden en que aparecen los volúmenes, y éstos se asignan a los discos según convenga en función del tamaño, etc. Varios volúmenes pueden usar un disco. Si asigna unidades manualmente, no podrá usar el mismo disco dos veces.

Para la asignación manual, debe tener la máquina nueva con el formato correcto antes de restaurarla.

Para asignar volúmenes:

1. Para asignar volúmenes automáticamente, realice estos pasos:
 - a. En la página **Disk Mapping (Asignación de discos)** del asistente **Restore Machine Wizard (Asistente para restaurar máquina)**, seleccione la pestaña **Automatically Map Volumes (Asignar volúmenes automáticamente)**.

- b. En el área **Disk Mapping (Asignación de discos)**, en **Source Volume (Volumen de origen)**, compruebe que el volumen de origen está seleccionado y que los volúmenes adecuados aparecen debajo y están seleccionados.
 - c. Si el disco de destino que se asigna automáticamente es el volumen de destino correcto, seleccione **Destination Disk (Disco de destino)**.
 - d. Haga clic en **Restore (Restaurar)** y continúe en el paso 3.
2. Para asignar volúmenes manualmente, realice estos pasos:
 - a. En la página **Disk Mapping (Asignación de discos)** del asistente **Restore Machine Wizard (Asistente para restaurar máquina)**, seleccione la pestaña **Manually Map Volumes (Asignar volúmenes manualmente)**.
 - b. En el área **Volume Mapping (Asignación de volúmenes)**, en **Source Volume (Volumen de origen)**, compruebe que el volumen de origen está seleccionado y que los volúmenes adecuados aparecen debajo y están seleccionados.
 - c. En **Destination (Destino)**, en el menú desplegable, seleccione el destino adecuado que representará el volumen de destino para realizar la restauración desde cero del punto de recuperación seleccionado y, después, haga clic en **Rollback (Revertir)**.
 3. En el cuadro de diálogo de confirmación **RollbackURC**, revise la asignación del origen del punto de recuperación y el volumen de destino de la reversión. Para realizar la reversión, haga clic en **Restore (Restaurar)**.

 **PRECAUCIÓN:** Si selecciona **Begin Rollback (Iniciar reversión)**, todas las particiones y datos de la unidad de destino se eliminarán de manera permanente, y se reemplazarán por el contenido del punto de recuperación seleccionado, incluido el sistema operativo y los datos.


Visualización del progreso de la recuperación

Para ver el progreso de la recuperación:

1. Después de iniciar el proceso de reversión, aparece el cuadro de diálogo **Active Task (Tarea activa)**, que muestra que la acción de reversión se ha iniciado.

 **NOTA:** La aparición del cuadro de diálogo **Active Task (Tarea activa)** no significa que la tarea se haya completado correctamente.

2. De manera opcional, puede supervisar el progreso de la tarea desde el cuadro de diálogo **Active Task (Tarea activa)**. Para ello, haga clic en **Open Monitor Window (Abrir ventana del monitor)** y aparecerá el estado de la recuperación, así como la hora de inicio y de finalización en la ventana **Monitor Open Task (Supervisar tarea abierta)**.

 **NOTA:** Para volver a los puntos de recuperación de la máquina de origen, en el cuadro de diálogo **Active Task (Tarea activa)**, haga clic en **Close (Cerrar)**.

Inicio de un servidor de destino restaurado

Para iniciar un servidor de destino restaurado:

1. Vuelva al servidor de destino y, en la interfaz de la **AppAssure Universal Recovery Console (Consola de recuperación universal de AppAssure)**, haga clic en **Reboot (Reiniciar)** para iniciar la máquina.
2. Especifique que Windows se inicie normalmente.
3. Inicie la sesión en la máquina.

El sistema se restaurará a su estado anterior a la restauración desde cero.

Reparación de problemas de inicio

Tenga en cuenta que, si va a restaurar en hardware diferente, deberá insertar una controladora de almacenamiento, un disco RAID, una interfaz AHCI, un conjunto de chips u otros controladores, en caso de que aún no estén incluidos en el CD de inicio. Estos controladores permiten que el sistema operativo funcione en todos los dispositivos del servidor de destino correctamente.

Para reparar problemas de arranque:

1. Si detecta problemas al iniciar el servidor de destino restaurado, abra la Consola de recuperación universal volviendo a cargar el CD de inicio.
2. En la Consola de recuperación universal, haga clic en **Driver Injection (Inserción de controlador)**.
3. En el cuadro de diálogo Driver Injection (Inserción de controlador), haga clic en **Repair Boot Problems (Reparar problemas de inicio)**.
Los parámetros de inicio del registro de inicio del servidor de destino se repararán de forma automática.
4. En la Consola de recuperación universal, haga clic en **Reboot (Reiniciar)**.

Cómo iniciar una restauración desde cero para una máquina Linux

DL1000 puede realizar una Bare Metal Restore (Restauración desde cero - BMR) de una máquina Linux que incluya una reversión del volumen del sistema. Mediante la utilidad de línea de comandos de AppAssure, `aamount`, revierta a la imagen base del volumen de inicio. Antes de realizar una BMR para una máquina Linux, primero debe hacer lo siguiente:

- Obtenga un archivo de Live CD de BMR de la asistencia de AppAssure, que incluye una versión de inicio de Linux.
 - ✎ **NOTA:** También puede descargar el archivo de Live CD de Linux del portal de licencias, en la dirección <https://licenseportal.com>.
- Asegúrese de que hay espacio suficiente en el disco duro para crear particiones de destino en la máquina de destino que contengan los volúmenes de origen. Las particiones de destino deben tener un tamaño igual o superior a la partición de origen inicial.
- Identifique la ruta para la reversión, que será la ruta del descriptor de archivo de dispositivo. Para ello, use el comando `fdisk` desde una ventana de terminal.
 - ✎ **NOTA:** Antes de empezar a utilizar los comandos de AppAssure, instale la utilidad de pantalla. Esta utilidad le permite desplazarse por la pantalla para ver más datos, como una lista de puntos de recuperación.


Para realizar una restauración desde cero para una máquina Linux:

1. Con el archivo de Live CD que reciba de AppAssure, inicie la máquina Linux y abra una ventana de terminal.
2. Si fuera necesario, cree una nueva partición de disco, por ejemplo, ejecutando el comando `fdisk` como raíz y haga que esta partición se pueda iniciar mediante el comando `a`.
3. Ejecute la utilidad `aamount` de AppAssure como raíz, por ejemplo:

```
sudo aamount
```
4. En la solicitud de montaje de AppAssure, introduzca el siguiente comando para enumerar las máquinas protegidas:

```
lm
```
5. Cuando se le solicite, introduzca la dirección IP o nombre del host del servidor AppAssure Core.
6. Introduzca las credenciales de inicio de sesión, es decir, el nombre de usuario y la contraseña, para este servidor.
Aparece una lista que muestra las máquinas protegidas por este servidor AppAssure Core, y que enumera las máquinas encontradas por número de elemento de línea, dirección de host/IP y un número de Id. para la máquina (por ejemplo: `293cc667-44b4-48ab-91d8-44bc74252a4f`).
7. Para ver los puntos de recuperación montados actualmente para la máquina que desea restaurar, introduzca el siguiente comando:


lr <machine_line_item_number>

 **NOTA:** También puede introducir el número de Id. de la máquina en lugar del número de elemento de línea.


Aparece una lista que muestra los puntos de recuperación básicos e incrementales de dicha máquina. Esta lista incluye un número de elemento de línea, fecha/fecha y hora, ubicación de volumen, tamaño de punto de recuperación y un número de Id. para el volumen que incluye un número de secuencia al final (por ejemplo: "293cc667-44b4-48ab-91d8-44bc74252a4f:2"), que identifica el punto de recuperación.

8. Para seleccionar el punto de recuperación de la imagen base que se va a revertir, introduzca el siguiente comando:


```
r <volume_base_image_recovery_point_ID_number> <path>
```


 **PRECAUCIÓN:** Asegúrese de que el volumen del sistema no esté montado.

Este comando revierte la imagen de volumen especificada por el Id. del Core en la ruta de acceso especificada. La ruta de acceso para la reversión es la ruta de acceso para el descriptor de archivo de dispositivo y no el directorio en el que está montado.

 **NOTA:** También puede especificar un número de línea en el comando en lugar del número de Id. de punto de recuperación para identificar el punto de recuperación. Utilice el número de línea de máquina/Agent (en la salida de lm), seguido del número de línea de punto de recuperación y de la letra de volumen, seguido de la ruta de acceso, por ejemplo, **r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>**. En este comando, <path> está el descriptor de archivo del volumen real.

9. Si se le solicita que continúe, escriba **y** para Sí.
Mientras continúe la reversión, aparecerán una serie de mensajes para notificarle el estado.
10. Tras una reversión satisfactoria, actualice el registro de inicio principal con el cargador de inicio restaurado.

 **NOTA:** La reparación o configuración del cargador de inicio solo es necesaria si el disco es nuevo. Si se trata de una reversión simple en el mismo disco, la configuración del cargador de inicio no será necesaria.

 **PRECAUCIÓN:** No desmonte un volumen Linux protegido manualmente. En caso de que necesite hacerlo, ejecute el siguiente comando antes de desmontar el volumen: **bsctl -d <path to volume>**.

En este comando, <path to volume> no se hace referencia al punto de montaje del volumen sino al descriptor de archivo del volumen; debe tener un formato similar al de este ejemplo: **/dev/sda1**.

Instalación de la utilidad de pantalla

Antes de empezar a utilizar los comandos de AppAssure, instale la utilidad de pantalla. Esta utilidad le permite desplazarse por la pantalla para ver más datos, como una lista de puntos de recuperación.


Para instalar la utilidad de pantalla:

1. Utilice el archivo de Live CD para iniciar la máquina Linux.
Se abrirá una ventana de terminal.
2. Introduzca el siguiente comando: `sudo apt-get install screen`
3. Para iniciar la utilidad de pantalla, escriba `screen` en el símbolo del sistema.

Creación de particiones de inicio en una máquina Linux

Para crear particiones de inicio en una máquina Linux mediante la línea de comandos:


1. Conecte todos los dispositivos mediante la utilidad **bsctl** con el siguiente comando como raíz: `sudo bsctl --attach-to-device /dev/<restored volume>`

 **NOTA:** Repita este paso para cada volumen restaurado.

2. Utilice los siguientes comandos para montar los volúmenes restaurados:

```
mount /dev/<restored volume> /mnt
```

```
mount /dev/<restored volume> /mnt
```

 **NOTA:** Puede que algunas configuraciones del sistema incluyan el directorio de inicio como parte del volumen raíz.

3. Utilice los siguientes comandos para montar los metadatos de instantáneas de los volúmenes restaurados:

```
sudo bsctl --reset-bitmap-store /dev/<restored volume>
```

```
sudo bsctl --map-bitmap-store /dev/<restored volume>
```

4. Compruebe que el identificador único universal (UUID) contiene volúmenes nuevos mediante el comando `blkid o ll /dev/disk/by-uuid`.

5. Compruebe que `/etc/fstab` contiene los UUID correctos para los volúmenes raíz y de inicio.

6. Instale el cargador de arranque unificado (GRUB) mediante los siguientes comandos:

```
mount --bind /dev/ /mnt/dev
```

```
mount --bind /dev/ /mnt/dev
```

```
chroot/mnt/bin/bash
```

```
grub-install/dev/sda
```

7. Compruebe que el archivo `/boot/grub/grub.conf` contiene el UUID correcto para el volumen raíz, o actualícelo según sea necesario con un editor de texto.

8. Extraiga el disco de Live CD de la unidad de CD-ROM y reinicie la máquina Linux.

Replicación de puntos de recuperación

Replicación

La replicación es el proceso de copiar puntos de recuperación y transmitirlos a una ubicación secundaria con el fin de la recuperación de desastres. El proceso requiere una relación de origen-destino emparejada entre dos Cores. La replicación se administra por máquina protegida, es decir, las instantáneas de copia de seguridad de una máquina protegida se replican en el Core de réplica de destino. Cuando la replicación está configurada, el Core de origen transmite de manera asíncrona y continua los datos de instantáneas incrementales al Core de destino. Puede configurar esta replicación de salida en el centro de datos propio de su compañía o en el sitio de recuperación de desastres remoto (es decir, un Core de destino administrado automáticamente) o en un proveedor de servicios administrado (MSP) que ofrezca servicios de recuperación de desastres y de copia de seguridad externos. Al realizar la replicación en un MSP, puede usar flujos de trabajo integrados que le permitan solicitar conexiones y recibir notificaciones de comentarios automáticas.

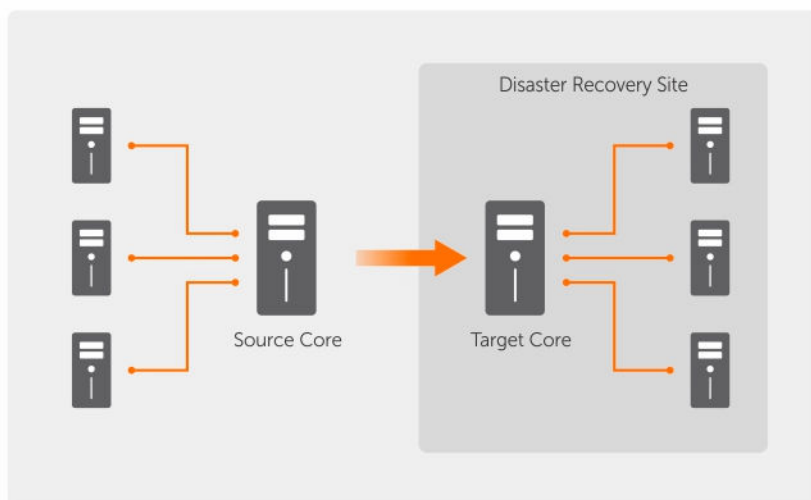


Ilustración 5. Arquitectura de replicación básica

La replicación comienza con la inicialización. La transferencia inicial de imágenes base desduplicadas e instantáneas incrementales de los Agents protegidos, que pueden sumar cientos o miles de gigabytes de datos. La replicación inicial se puede inicializar en el Core de destino mediante el uso de medios 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 desduplican. Si el tamaño total del archivo es mayor que el espacio disponible en el medio extraíble, el archivo podrá abarcar varios dispositivos, en función del espacio disponible en el medio. Durante el proceso de inicialización, los puntos de recuperación incrementales se replican en el sitio de destino. Después de que el Core de destino

consume el archivo de inicialización, los puntos de recuperación incrementales recién replicados se sincronizan de forma automática.

Plan para realizar la replicación


Para replicar los datos mediante AppAssure, debe configurar los Cores de origen y de destino para la replicación. Después de configurar la replicación, puede replicar los datos de las máquinas protegidas, supervisar y administrar la replicación y realizar la recuperación.

La replicación en AppAssure implica realizar las operaciones siguientes:

- Configurar la replicación administrada automáticamente. Para obtener más información acerca de cómo replicar a un Core de destino administrado automáticamente, consulte [Replicación a un Core administrado automáticamente](#).
- Configurar la replicación de terceros. Para obtener más información acerca de cómo replicar a un Core de destino de terceros, consulte [Replicación a un Core administrado por un tercero](#).
- Replique datos desde una máquina protegida nueva conectada al Core de origen. Para obtener más información sobre la replicación de una máquina protegida, consulte [Replicating A New Protected Machine \(Replicación de una máquina protegida nueva\)](#).
- Replicar una máquina protegida existente. Para obtener más información sobre la configuración de un Agent para la replicación, consulte [Replicación de los datos de un Agent en una máquina](#).
- Establecer la prioridad de replicación para un Agent. Para obtener más información sobre cómo priorizar la replicación de los Agents, consulte [Configuración de la prioridad de replicación para un Agent](#).
- Supervisar la replicación según sea necesario. Para obtener más información sobre cómo supervisar la replicación, ver [Monitoring Replication](#) (Supervisión de la replicación).
- Administrar la configuración de replicación según sea necesario. Para obtener más información acerca de cómo administrar la configuración de replicación, consulte [Administración de configuraciones de replicación](#).
- Recuperar los datos replicados ante situaciones de desastre o pérdida de datos. Para obtener más información acerca de cómo recuperar datos replicados, consulte [Recuperación de datos replicados](#).

Replicación a un Core administrado automáticamente

Un Core administrado automáticamente es aquel al que tiene acceso, generalmente porque lo administra su compañía en otra ubicación. La replicación se puede completar totalmente en el Core de origen, a menos que decida inicializar los datos. La inicialización requiere consumir la unidad de inicialización en el Core de destino después de configurar la replicación en el Core de origen.

 **NOTA:** Esta configuración se aplica a la replicación en una ubicación externa y a la replicación mutua. El Core se debe instalar en todas las máquinas de origen y de destino. Si está configurando su sistema para la replicación multipunto a punto, debe realizar esta tarea en todos los Cores de origen y en el Core de destino.

Configuración del Core de origen para replicar a un Core de destino administrado automáticamente

Para configurar el Core de origen para replicar a un Core de destino administrado automáticamente:

1. En la Core Console, haga clic en la pestaña **Replication (Replicación)**.
2. Haga clic en **Add Target Core (Agregar Core de destino)**.
Se abrirá el asistente **Replication (Replicación)**.
3. Seleccione **I have my own Target Core (Tengo mi propio Core de destino)** y, a continuación, introduzca la información según se describe en la tabla siguiente.

| Cuadro de texto | Descripción |
|------------------|---|
| Host Name | Introduzca el nombre de host o dirección IP de la máquina del Core en la que esté replicando. |
| Port | Introduzca el número de puerto con el que el AppAssure Core se comunica con la máquina. El número de puerto predeterminado es 8006. |
| User Name | Introduzca el nombre de usuario para acceder a la máquina. Por ejemplo, Administrator (Administrador) . |
| Password | Introduzca la contraseña para acceder a la máquina. |

Si el Core que desea agregar se ha emparejado anteriormente con este Core de origen, lleve a cabo los pasos siguientes:

- a. Seleccione **Use an existing target core (Usar un Core de destino existente)**.
 - b. En la lista desplegable, seleccione el Core de destino.
 - c. Haga clic en **Next (Siguiente)**.
 - d. Vaya al paso 7.
4. Haga clic en **Next (Siguiente)**.
 5. En la página **Details (Detalles)**, especifique un nombre para esta configuración de replicación; por ejemplo, SourceCore1. Si está volviendo a iniciar o reparando una configuración de replicación anterior, seleccione **My Core has been migrated and I would like to repair replication (Se ha migrado el Core y me gustaría reparar la replicación)**.
 6. Haga clic en **Next (Siguiente)**.
 7. En la página **Agents (Agentes)**, elija los Agents que desea replicar y, a continuación, utilice las listas desplegables de la columna **Repository (Repositorio)** y seleccione un repositorio para cada Agent.
 8. Si tiene pensado realizar el proceso de inicialización para la transferencia de los datos de la base, lleve a cabo los pasos siguientes:



NOTA: Como hay que copiar grandes cantidades de datos al dispositivo de almacenamiento portátil, se recomienda usar una conexión eSATA, USB 3.0 y otra de alta velocidad con el dispositivo de almacenamiento portátil.

- a. En la página **Agents (Agentes)**, seleccione **Use a seed drive to perform initial transfer (Utilizar una unidad de inicialización para realizar la transferencia inicial)**. Si actualmente se están replicando uno o más Agents en un Core de destino, para incluir esos Agents en la unidad de inicialización seleccione **With already replicated (Con los ya replicados)**.
- b. Haga clic en **Next (Siguiente)**.
- c. En la página **Seed Drive Location (Ubicación de la unidad de inicialización)**, utilice la lista desplegable **Location type (Tipo de ubicación)** para seleccionar una de las opciones siguientes:
 - Local: en el cuadro de texto **Location (Ubicación)**, especifique dónde desea guardar la unidad de inicialización; por ejemplo, D:\work\archive.
 - Network (Red): en el cuadro de texto **Location (Ubicación)**, especifique dónde desea guardar la unidad de inicialización y, a continuación, introduzca sus credenciales del recurso compartido de red en los cuadros de texto **User name (Nombre de usuario)** y **Password (Contraseña)**.
 - Cloud (Servicios en la nube): en el cuadro de texto **Account (Cuentas)**, seleccione la cuenta. Para seleccionar una cuenta de servicios en la nube, debe haberla agregado primero en la Core Console. Para obtener más información, consulte [Cómo agregar una cuenta de servicios en la nube](#). Seleccione el **Container (Contenedor)** asociado con su cuenta. Seleccione el **Folder Name (Nombre de la carpeta)** donde guardará los datos archivados.

d. Haga clic en **Next (Siguiete)**.

9. En el cuadro de diálogo **Seed Drive Option (Opciones de la unidad de inicialización)**, introduzca la información que se describe a continuación:

| Cuadro de texto | Descripción |
|--------------------------------------|--|
| Maximum Size | <p>Los grandes archivos de datos pueden dividirse en múltiples segmentos. Seleccione el tamaño máximo del segmento que desea reservar para crear la unidad de inicialización mediante una de las acciones siguientes:</p> <ul style="list-style-type: none">• Seleccione Entire Target (Todo el destino) para reservar todo el espacio disponible en la ruta de acceso proporcionada en la página Seed Drive Location (Ubicación de la unidad de inicialización) para su uso en el futuro (por ejemplo, si la ubicación es D:\work\archive, se reservará todo el espacio disponible en la unidad D: por si es necesario para copiar la unidad de inicialización, pero no se reserva inmediatamente después de iniciar el proceso de copia).• Seleccione el cuadro de texto en blanco, introduzca una cantidad y, a continuación, seleccione una unidad de medida en la lista desplegable para personalizar el espacio máximo que desea reservar. |
| Customer ID (optional) | <p>Opcionalmente, introduzca la Id. del cliente que le asignó el proveedor de servicio.</p> |
| Recycle action | <p>En el caso de que la ruta de acceso ya contenga una unidad de inicialización, seleccione una de las opciones siguientes:</p> <ul style="list-style-type: none">• Do not reuse (No reutilizar): no sobrescribe ni borra los datos existentes de la ubicación. Si la ubicación no está vacía, fallará la escritura de la unidad de inicialización.• Replace this core (Reemplazar este Core): sobrescribe los datos que ya existen y que pertenecen a este Core, pero deja intactos los datos de los otros Cores.• Erase completely (Borrar completamente): borra todos los datos del directorio antes de escribir la unidad de inicialización. |
| Comment | <p>Introduzca un comentario o una descripción del archivo.</p> |
| Add all Agents to Seed Drive | <p>Seleccione los Agents que desea replicar utilizando la unidad de inicialización.</p> |
| Build RP chains (fix orphans) | <p>Seleccione esta opción para replicar toda la cadena de puntos de recuperación (PR) en la unidad de inicialización. Esta opción está seleccionada de manera predeterminada.</p> <p>En AppAssure, la inicialización típica replica solo el último punto de recuperación a la unidad de inicialización, lo que reduce la cantidad de tiempo y espacio necesario para crear la unidad de inicialización. La opción para crear cadenas de punto de recuperación para la unidad de inicialización requiere el espacio suficiente en esa unidad para almacenar los puntos de recuperación más recientes desde uno o varios Agents especificados, lo cual puede llevar un tiempo adicional para completar la tarea.</p> |

| Cuadro de texto | Descripción |
|-----------------|-------------|
|-----------------|-------------|

| | |
|------------------------------|---|
| Use compatible format | Seleccione esta opción para crear la unidad de inicialización en un formato que sea compatible con las versiones nuevas y anteriores de AppAssure Core. |
|------------------------------|---|

10. En la página **Agents (Agentes)**, seleccione los Agents que desea replicar en el Core de destino usando la unidad de inicialización.
11. Haga clic en **Finish (Finalizar)**.
12. Si ha creado una unidad de inicialización, envíela al Core de destino.
El emparejamiento del Core de origen con el Core de destino ha finalizado. La replicación se inicia, pero produce puntos de recuperación huérfanos en el Core de destino hasta que la unidad de inicialización se consume y proporciona las imágenes base.

Consumo de la unidad de inicialización en un Core de destino

Este procedimiento solo es necesario si creó una unidad de inicialización durante la Configuración de la replicación de un Core administrado automáticamente.

Para consumir una unidad de inicialización en un Core de destino:

1. Si la unidad de inicialización se guardó en un dispositivo de almacenamiento portátil como una unidad USB, conecte la unidad al Core de destino.
2. Desde la Core Console en el Core de origen, seleccione la pestaña **Replication (Replicación)**.
3. En **Incoming Replication (Replicación entrante)**, seleccione el Core de origen correcto en el menú desplegable y, a continuación, haga clic en **Consume (Consumir)**.
Aparece la ventana Consume (Consumir).
4. Para **Location Type (Tipo de ubicación)**, seleccione una de las opciones siguientes en la lista desplegable:
 - Local
 - Network (Red)
 - Cloud (Nube)
5. Introduzca la información siguiente según sea necesario:

| Cuadro de texto | Descripción |
|-----------------|-------------|
|-----------------|-------------|

| | |
|-----------------------------|---|
| Location (Ubicación) | Introduzca la ruta de acceso de la unidad de inicialización, como una unidad USB o un recurso compartido de red (por ejemplo, D:\). |
|-----------------------------|---|

| | |
|-------------------------------------|--|
| Username (Nombre de usuario) | Introduzca el nombre de usuario de la carpeta o unidad compartida. El nombre de usuario solo se requiere para una ruta de acceso de red. |
|-------------------------------------|--|

| | |
|------------------------------|--|
| Password (Contraseña) | Introduzca la contraseña de la carpeta o unidad compartida. La contraseña solo se requiere para una ruta de acceso de red. |
|------------------------------|--|

| | |
|-------------------------|--|
| Account (Cuenta) | Seleccione una cuenta desde la lista desplegable. Para seleccionar una cuenta de servicios en la nube, debe haberla agregado primero en la Core Console. |
|-------------------------|--|

| | |
|-------------------------------|--|
| Container (Contenedor) | En el menú desplegable, seleccione un contenedor asociado con la cuenta. |
|-------------------------------|--|

Cuadro de texto

Descripción

Folder Name (Nombre de carpeta)

Introduzca el nombre de la carpeta en la que se guarda los datos archivados; por ejemplo, -Archivo- [FECHA DE CREACIÓN] - [TIEMPO DE CREACIÓN]

6. Haga clic en **Check File (Comprobar archivo)**.


Una vez que el Core comprueba el archivo, rellena automáticamente el campo **Date Range (Rango de fechas)** con las fechas de los puntos de recuperación más antiguos y más recientes incluidos en la unidad de inicialización. También importa los comentarios introducidos en Configuración de la replicación de un Core administrado automáticamente.

7. En **Agent Names (Nombres de Agent)** en la ventana **Consume (Consumir)**, seleccione las máquinas para las que desea consumir datos y, a continuación, haga clic en **Consume (Consumir)**.

 **NOTA:** Para supervisar el progreso de consumo de datos, seleccione la pestaña **Events (Eventos)**.

Abandono de una unidad de inicialización pendiente

Si crea una unidad de inicialización con la intención de consumirla en el Core de destino, pero decide no enviarla a la ubicación remota, el enlace a dicha unidad de inicialización pendiente permanecerá en la pestaña **Replication (Replicación)** del Core de origen. Puede abandonar la unidad de inicialización pendiente para dar prioridad a datos de inicialización diferentes o más actualizados.

 **NOTA:** Mediante este proceso, se elimina la unidad de inicialización pendiente de la Core Console en el Core de origen, pero no se elimina la unidad de la ubicación de almacenamiento en la que se guardó.

Para abandonar una unidad de inicialización pendiente:

1. En la Core Console en el Core de origen, seleccione la pestaña **Replication (Replicación)**.

2. Haga clic en **Outstanding Seed Drive (#) (N.º de unidades de inicialización pendientes)**.

Aparecerá la sección **Outstanding seed drives (Unidades de inicialización pendientes)**, que muestra el nombre del Core de destino remoto, la fecha y hora en las que se creó la unidad de inicialización y el intervalo de datos de los puntos de recuperación incluidos en la unidad.

3. Haga clic en el menú desplegable de la unidad que desea abandonar y elija **Abandon (Abandonar)**.


Aparecerá la ventana **Outstanding Seed Drive (Unidad de inicialización pendiente)**.

4. Haga clic en **Yes (Sí)** para confirmar la acción.

La unidad de inicialización se eliminará. Si no hay más unidades de inicialización en el Core de origen, la próxima vez que abra la pestaña **Replication (Replicación)**, no aparecerá el enlace **Outstanding Seed Drive (#) (N.º de unidades de inicialización pendientes)** ni la sección **Outstanding seed drives (Unidades de inicialización pendientes)**.

Replicación a un Core administrado por un tercero

Un Core de terceros es un Core de destino que un MSP se encarga de administrar y mantener. Para replicar a un Core administrado por terceros no es necesario tener acceso al Core de destino. Una vez que un cliente configura la replicación en el Core o los Cores de destino, el MSP finaliza la configuración en el Core de destino.

 **NOTA:** Esta configuración se aplica a la replicación alojada y en la nube. El AppAssure Core debe estar instalado en todas las máquinas Core de origen.

Replicación de un Agent nuevo

Cuando añada un AppAssure Agent para protección en un Core de origen, AppAssure le da la opción de replicar el Agent nuevo en un Core de destino existente.

Para replicar un Agent nuevo:

1. Vaya a la Core Console y seleccione la pestaña **Machines (Máquinas)**.
2. En el menú desplegable **Actions (Acciones)**, haga clic en **Protect Machine (Proteger máquina)**.
3. En el cuadro de diálogo **Protect Machine (Proteger máquina)**, introduzca la información como se describe en la tabla siguiente.

| Cuadro de texto | Descripción |
|-------------------------------------|---|
| Host | Introduzca el nombre de host o la dirección IP de la máquina que desea proteger. |
| Port (Puerto) | Introduzca el número de puerto por el que el AppAssure Core se comunicará con el Agent en la máquina. |
| Username (Nombre de usuario) | Introduzca el nombre de usuario que se utiliza para conectar a esa máquina. Por ejemplo, Administrador. |
| Password (Contraseña) | Introduzca la contraseña que se utiliza para conectarse a esta máquina. |


4. Haga clic en **Connect (Conectar)** para conectar a esa máquina.
5. Haga clic en **Show Advanced Options (Mostrar opciones avanzadas)** y edite la configuración siguiente, según sus necesidades.

| Cuadro de texto | Descripción |
|---|--|
| Display Name (Nombre de visualización) | Escriba un nombre para la máquina, que se mostrará en la Core Console. |
| Repository (Repositorio) | Seleccione el repositorio en el AppAssure Core donde se almacenarán los datos de esta máquina. |
| Encryption Key (Clave de cifrado) | Especifique si el cifrado debe aplicarse a los datos de cada volumen de esta máquina que se almacenarán en el repositorio. |



NOTA: La configuración del cifrado de un repositorio se define en la pestaña **Configuration (Configuración)** de la Core Console.

| | |
|---|--|
| Remote Core (Core remoto) | Especifique el Core de destino en el que desee replicar el Agent. |
| Remote Repository (Repositorio remoto) | El nombre del repositorio que desee en el Core de destino en el que se almacenarán los datos replicados para esta máquina. |

| Cuadro de texto | Descripción |
|--|---|
| Pause (Pausa) | Marque esta casilla de verificación si desea pausar la replicación; por ejemplo, para pausarla hasta después de que AppAssure tome una imagen base del Agent nuevo. |
| Schedule (Programa) | <p>Seleccione una de las opciones siguientes:</p> <ul style="list-style-type: none"> Protect all volumes with default schedule (Proteger todos los volúmenes con el programa predeterminado) Protect specific volumes with custom schedule (Proteger volúmenes específicos con programa personalizado) <p> NOTA: El programa predeterminado es cada 15 minutos.</p> |
| Initially pause protection (Pausar protección inicialmente) | Seleccione esta casilla de verificación si desea pausar la protección, por ejemplo, para evitar que AppAssure tome una imagen base, hasta que pasen las horas de máxima utilización. |

- Haga clic en **Protect (Proteger)**.

Replicación de los datos de Agent en una máquina

La replicación es la relación entre los Cores de origen y de destino en el mismo sitio o entre dos sitios con enlace lento por Agent. Si la replicación está configurada entre dos Cores, el Core de origen transmite de forma asíncrona los datos de instantánea incremental de los Agents seleccionados al Core de destino o de origen. La replicación de salida se puede configurar en un proveedor de servicio administrado que proporcione servicio de recuperación de desastres y copia de seguridad externos o en un Core administrado automáticamente. Para replicar datos del Agent en una máquina:

- En la Core Console, haga clic en la pestaña **Machines (Máquinas)**.
- Seleccione la máquina que desea replicar.
- En el menú desplegable **Actions (Acciones)**, haga clic en **Replication (Replicación)** y, a continuación, complete una de las siguientes opciones:
 - Si configura la replicación, haga clic en **Enable (Habilitar)**.
 - Si ya ha configurado una replicación existente, puede hacer clic en **Copy (Copiar)**.


Aparecerá el cuadro de diálogo **Enable Replications (Habilitar replicación)**.

- En el cuadro de texto **Host**, introduzca el nombre del host.
- En **Agents (Agents)**, seleccione la máquina que tiene el Agent y los datos que desea replicar.
- Si fuera necesario, seleccione la casilla de verificación **Use a seed drive to perform initial transfer (Utilizar una unidad de inicialización para realizar la transferencia inicial)**.
- Haga clic en **Add (Agregar)**.
- Para hacer una pausa o para reanudar la replicación, haga clic en **Replication (Replicación)** en el menú desplegable **Actions (Acciones)** y, a continuación, haga clic en **Pause (Pausar)** o en **Resume (Reanudar)** según proceda.

Configuración de la prioridad de replicación para un Agent

Para establecer la prioridad de replicación para un Agent:

1. En la Core Console, seleccione la máquina protegida para la que desee configurar la prioridad de replicación y haga clic en la pestaña **Configuration (Configuración)**.
2. Haga clic en **Select Transfer Settings (Seleccionar configuración de transferencia)** y, a continuación, utilice la lista desplegable **Priority (Prioridad)**, para seleccionar una de las opciones siguientes:
 - **Default (Predeterminado)**
 - **Highest (Más alto)**
 - **Lowest (Más bajo)**
 - **1**
 - **2**
 - **3**
 - **4**

 **NOTA:** La prioridad predeterminada es 5. Si un Agent recibe la prioridad 1 y otro Agent recibe la prioridad Highest (Más alto), se replica el Agent con prioridad más alta antes que el Agent con prioridad 1.

3. Haga clic en **OK (Aceptar)**.

Supervisión de la replicación

Cuando la replicación esté configurada, puede supervisar el estado de las tareas de replicación para los Cores de origen y destino. Puede actualizar la información del estado, ver detalles de replicación, etc.

Para supervisar la replicación

1. En la Core Console, haga clic en la pestaña **Replication (Replicación)**.
2. En esta pestaña, puede ver información y supervisar el estado de las tareas de replicación, según se describe a continuación:

Tabla 4. Supervisión de la replicación

| Sección | Descripción | Acciones disponibles |
|------------------------------|---|---|
| Pending Replication Requests | Muestra el Id. de cliente, la dirección de correo electrónico y el nombre del host cuando se envía una solicitud de replicación a un proveedor de servicios de terceros. Aparece en esta sección hasta que MSP acepta la solicitud. | En el menú desplegable, haga clic en Ignore (Ignorar) para ignorar o rechazar la solicitud. |
| Outstanding Seed Drives | Enumera las unidades de inicialización que se han escrito pero que el Core de destino aún no ha consumido. Incluye el nombre de Core remoto, la | En el menú desplegable, haga clic en Abandon (Abandonar) para abandonar o cancelar el proceso de inicialización. |

| Sección | Descripción | Acciones disponibles |
|----------------------|--|---|
| Outgoing Replication | <p>fecha de creación y el intervalo de fechas.</p> <p>Enumera todos los Cores de destino en los que se replica el Core de origen. Incluye el nombre del Core remoto, el estado de existencia, el número de máquinas protegidas a replicar y el progreso de una transmisión de replicación.</p> | <p>En un Core de origen, en el menú desplegable, puede seleccionar las opciones siguientes:</p> <ul style="list-style-type: none"> • Details (Detalles): muestra el Id., URI, nombre para mostrar, estado, Id. de cliente, dirección de correo electrónico y comentarios del Core replicado. • Change Settings (Cambiar configuración): muestra el nombre para mostrar y le permite editar el host y puerto para el Core de destino. • Add Agents (Agregar agentes): le permite elegir un host de una lista desplegable, seleccionar máquinas protegidas para replicación y crear una unidad de inicialización para la transferencia inicial de la máquina protegida. |
| Incoming Replication | <p>Enumera todas las máquinas de origen desde las que el destino recibe datos replicados. Incluye el nombre del Core remoto, estado, máquinas y progreso.</p> | <p>En un Core de destino, en el menú desplegable, puede seleccionar las opciones siguientes:</p> <ul style="list-style-type: none"> • Details (Detalles): muestra el Id., nombre de host, Id. de cliente, dirección de correo electrónico y comentarios del Core replicado. • Consume (Consumir): consume los datos iniciales de la unidad de inicialización y los guarda en el repositorio local. |

3. Haga clic en el botón **Refresh (Actualizar)** para actualizar las selecciones de esta pestaña con la información más reciente.

Administración de configuraciones de replicación

Puede ajustar una serie de configuraciones para la forma en la que se ejecuta la replicación en los Cores de origen y destino.

Para administrar las configuraciones de replicación:

1. En la Core Console, haga clic en la pestaña **Replication (Replicación)**.
2. En el menú desplegable **Actions (Acciones)**, haga clic en **Settings (Configuración)**.

3. En la ventana **Replication Settings (Configuración de replicación)**, edite la configuración de replicación, según se describe a continuación:


| Opción | Descripción |
|---|---|
| Cache lifetime | Especifica el tiempo entre las solicitudes de estado de Core de destino realizadas por el Core de origen. |
| Volume image session timeout | Especifica el tiempo que el Core de origen tarda en intentar transferir una imagen de volumen al Core de destino. |
| Max. concurrent replication jobs | Especifica el número de máquinas protegidas que tienen permiso para replicar a la vez en el Core de destino. |
| Max. parallel streams | Especifica el número de conexiones de red permitidas para su uso por parte de una máquina protegida única para la replicación de los datos de dicha máquina de una vez. |

4. Haga clic en **Save (Guardar)**.

Eliminación de replicación

Puede interrumpir la replicación y eliminar las máquinas protegidas de replicación de varias formas. Las opciones incluyen:

- [Eliminación de un Agent de la replicación en el Core de origen](#)
- [Eliminación de un Agent en el Core de destino](#)
- [Eliminación de un Core de destino de la replicación](#)
- [Eliminación de un Core de origen de la replicación](#)

 **NOTA:** La eliminación de un Core de origen tendrá como resultado la eliminación de todos los equipos replicados protegidos por dicho Core.

Extracción de una máquina protegida de la replicación en el Core de origen

Para quitar una máquina protegida de la replicación en el Core de origen:

1. Desde el Core de origen, abra la Core Console y haga clic en la pestaña **Replication (Replicación)**.
2. Expanda la sección **Outgoing Replication (Replicación saliente)**.
3. En el menú desplegable para la máquina protegida que desea eliminar de la replicación, haga clic en **Delete (Eliminar)**.
4. En el cuadro de diálogo **Outgoing Replication (Replicación saliente)**, haga clic en **Yes (Sí)** para confirmar la eliminación.

Extracción de una máquina protegida en el Core de destino

Para quitar una máquina protegida en el Core de destino:

1. En el Core de destino, abra la Core Console y haga clic en la pestaña **Replication (Replicación)**.
2. Expanda la sección **Incoming Replication (Replicación entrante)**.
3. En el menú desplegable para la máquina protegida que desee eliminar de la replicación, haga clic en **Delete (Eliminar)** y, a continuación, seleccione una de las opciones siguientes.


| Opción | Descripción |
|----------------------------|--|
| Relationship Onl | Elimina la máquina protegida de la replicación pero mantiene los puntos de recuperación replicados. |
| With Recovery Point | Elimina la máquina protegida de la replicación y elimina todos los puntos de recuperación replicados de dicha máquina. |

Eliminación de un Core de destino de la replicación

Para eliminar un Core de destino de la replicación:

1. En el Core de origen, abra la Core Console y haga clic en la pestaña **Replication (Replicación)**.
2. En **Outgoing Replication (Replicación saliente)**, haga clic en el menú desplegable junto al Core remoto que desee eliminar y haga clic en **Delete (Eliminar)**.
3. En el cuadro de diálogo **Outgoing Replication (Replicación saliente)**, haga clic en **Yes (Sí)** para confirmar la eliminación.

Eliminación de un Core de origen de la replicación

 **NOTA:** Eliminar un Core de origen tendrá como resultado la eliminación de todos los Agents replicados protegidos por dicho Core.

Para eliminar un Core de origen de la replicación:

1. En el Core de destino, abra la Core Console y haga clic en la pestaña **Replication (Replicación)**.
2. Bajo **Incoming Replication (Replicación entrante)**, en el menú desplegable, haga clic en **Delete (Eliminar)** y, a continuación, seleccione una de las opciones siguientes.

| Opción | Descripción |
|--|---|
| Relationship Only (Sólo relación) | Elimina el Core de origen de la replicación pero mantiene los puntos de recuperación replicados. |
| With Recovery Points (Con puntos de recuperación) | Elimina el Core de origen de la replicación y elimina todos los puntos de recuperación replicados de dicha máquina. |

3. En el cuadro de diálogo **Incoming Replication (Replicación entrante)**, haga clic en **Yes (Sí)** para confirmar la eliminación.

Recuperación de datos replicados

La funcionalidad de replicación "Day-to-day" (Día a día) se mantiene en el Core de origen, mientras que solo el Core de destino es capaz de completar las funciones necesarias para la recuperación de desastres.

Para la recuperación de desastres, el Core de destino puede utilizar los puntos de recuperación replicados para recuperar los Agents protegidos y el Core.

Puede realizar las opciones de recuperación siguientes desde el Core de destino:

- Montar puntos de recuperación.
- Revertir a puntos de recuperación.

- Realizar una exportación de máquina virtual (VM).
- Realizar una restauración desde cero (BMR).
- Realizar conmutación por recuperación (en caso de que tenga configurado un entorno de replicación conmutación por error/conmutación por recuperación).

Comprensión de la conmutación por error y la conmutación por recuperación

AppAssure admite la conmutación por error y la conmutación por recuperación en entornos replicados, para casos en los que se produce una interrupción grave en la que el Core de origen y los Agents fallan. Conmutación por error hace referencia a la conmutación a un destino redundante o de espera (AppAssure Core) en el momento de la falla del sistema o de una finalización no esperada de un Core de origen y los Agents asociados. El objetivo principal de la conmutación por error es lanzar un Agent nuevo idéntico al Agent del fallo. El segundo objetivo es conmutar el Core de destino a un modo nuevo, para que el Core de destino proteja el Agent de conmutación por error de la misma forma que el Core de origen protegía al Agent inicial antes del error. El Core de destino puede recuperar instancias desde Agents replicados e iniciar inmediatamente la protección en las máquinas de conmutación por error. La conmutación por recuperación es el proceso de restaurar un Agent y un Core a sus estados originales (antes del fallo). El objetivo principal de la conmutación por recuperación es restaurar el Agent (en la mayoría de los casos, se trata de una nueva máquina que reemplaza a un Agent fallido) a un estado idéntico al último estado del nuevo Agent temporal. Al restaurarse, queda protegido por un Core de origen restaurado. La replicación también se restaura y el Core de destino actúa de nuevo como destino de replicación.

Cómo realizar una conmutación por error

Cuando encuentre una situación de desastre en la que su Core de origen y Agents asociados han fallado, puede habilitar la conmutación por error en AppAssure para cambiar la protección a su Core de conmutación por error (destino) idéntico. El Core de destino se convierte en el único Core que protege datos en su entorno y, a continuación, inicie un nuevo Agent para reemplazar temporalmente al Agent que ha fallado.

Para realizar una conmutación por error en el Core de destino:


1. Acceda a la Core Console en el Core de destino y haga clic en la pestaña **Replication (Replicación)**.
2. En **Incoming Replication (Replicación entrante)**, seleccione el Core de origen y, a continuación, expanda los detalles debajo del Agent individual.
3. En el menú **Actions (Acciones)** para dicho Core, haga clic en **Failover (Conmutación por error)**. Aparecerá el cuadro de diálogo **Fail Over (Conmutación por error)**, donde se listan los próximos pasos necesarios para completar una conmutación por error.
4. Haga clic en **Continue (Continuar)**.
5. En el área de navegación izquierda, bajo **Protected Machines (Máquinas protegidas)**, seleccione la máquina que tenga asociado el software Agent de AppAssure con puntos de recuperación.
6. Exporte la información del punto de recuperación de copia de seguridad en dicho Agent a una máquina virtual.
7. Exporte la información del punto de recuperación de copia de seguridad en dicho Agent a una máquina virtual.
8. Inicie la máquina virtual que ahora incluye la información de copia de seguridad exportada. Tiene que esperar a que el software del controlador de dispositivos se instale.
9. Reinicie la máquina virtual y espere a que el servicio de Agent se inicie.

10. Vuelva a la Core Console para el Core de destino y compruebe que el Agent nuevo aparece en la pestaña **Protected Machines (Máquinas protegidas)** y en la pestaña **Replication (Replicación)** bajo **Incoming Replication (Replicación entrante)**.
11. Fuerce varias instantáneas y compruebe que se completan correctamente.
Para obtener más información, consulte [Cómo forzar una instantánea](#).
12. Ahora puede continuar realizando la conmutación por recuperación.
Para obtener más información, consulte [Cómo realizar una conmutación por recuperación](#).

Cómo realizar una conmutación por recuperación

Después de reparar o sustituir el Core de origen que ha fallado y los Agents originales, debe mover los datos desde sus máquinas con conmutación por error para restaurar las máquinas de origen.

Para realizar conmutación por recuperación:

1. Acceda a la Core Console en el Core de destino y haga clic en la ficha **Replication (Replicación)**.
2. En **Incoming Replication (Replicación entrante)**, seleccione el Agent de conmutación por error y expanda los detalles.
3. En el menú **Actions (Acciones)**, haga clic en **Failback (Conmutación por recuperación)**.
Se abre el cuadro de diálogo **Fail Back (Conmutación por recuperación)** para describir los pasos que debe seguir antes de hacer clic en el botón **Continue (Continuar)** para completar la conmutación por recuperación.
4. Haga clic en **Cancel (Cancelar)**.
5. Si la máquina a la que se aplica conmutación por error ejecuta Microsoft SQL Server o Microsoft Exchange Server, detenga estos servicios.
6. Forzar una instantánea de la máquina. Para obtener más información, consulte [Cómo forzar una instantánea](#).
7. Apague la máquina de conmutación por error.
8. Cree un archivo del Agent de conmutación por error y envíelo como salida a un disco o ubicación de recurso compartido de red.
Para obtener más información acerca de cómo crear archivos, consulte [Creación de un archivo](#).
9. Cuando cree el archivo, acceda a la Core Console en el Core de origen recién reparado, y haga clic en la pestaña **Tools (Herramientas)**.
10. Importe el archivo que acaba de crear en el paso 8.
Para obtener más información, consulte [Importación de un archivo](#).
11. Regrese a la Core Console en el Core de destino y haga clic en la pestaña **Replication (Replicación)**.
12. En **Incoming Replication (Replicación entrante)**, seleccione el Agent de conmutación por error y expanda los detalles.
13. En el cuadro de diálogo **Failback (Conmutación por recuperación)**, haga clic en **Continue (Continuar)**.
14. Apague la máquina que tiene el Agent exportado que se ha creado durante la conmutación por error.
15. Realice una restauración desde cero (BMR) para el Core de origen y el Agent.
 **NOTA:** Cuando inicie la restauración, deberá usar los puntos de recuperación que se importaron desde el Core de origen hasta el Agent en la máquina virtual.
16. Espere a que se vuelva a iniciar la BMR y que se reinicie el servicio de Agent y, a continuación, revise y registre los detalles de conexión de red de la máquina.
17. Acceda a la Core Console en el Core de origen y, en la pestaña **Machines (Máquinas)**, modifique las configuraciones de protección de máquina para agregar los detalles de la conexión de red nueva.
Para obtener más información, consulte [Configuración de los valores de la máquina](#).

18. Vaya a la Core Console en el Core de destino y elimine el Agent de la pestaña **Replication (Replicación)**.
19. En la Core Console del Core de origen, vuelva a configurar la replicación entre el origen y el destino haciendo clic en la pestaña **Replication (Replicación)** y, a continuación, agregue el Core de destino para replicación.

Emisión de informes

Acerca de los informes





Su appliance DL le permite generar y ver información de resumen, de cumplimiento y de errores para varias máquinas Core y Agent.

Podrá elegir entre ver informes en línea, imprimir informes o exportarlos y guardarlos en uno de los diversos formatos admitidos. Los formatos entre los que puede elegir son:

- PDF
- XLS
- XLSX
- RTF
- MHT
- HTML
- TXT
- CSV
- Imagen

Acerca de la barra de herramientas de informes

La barra de herramientas para todos los informes le permite imprimir y guardar de dos maneras diferentes. La siguiente tabla describe las opciones para imprimir y guardar.

| Icono | Descripción |
|---|--|
|  | Imprimir el informe |
|  | Imprimir la página actual |
|  | Exportar un informe y guardarlo en el disco |
|  | Exportar un informe y mostrarlo en una nueva ventana Utilice esta opción para copiar, pegar y enviar por correo electrónico la URL para que otros vean el informe con un explorador de web. |

Acerca de los informes de cumplimiento

Los informes de cumplimiento están disponibles para el Core y AppAssure Agent. Le proporcionan una forma de ver el estado de los trabajos realizados por un determinado Core o Agent. Los trabajos fallidos aparecen en texto rojo. La información del informe de cumplimiento de Core que no esté asociada con un Agent aparece en blanco.

Los detalles sobre los trabajos se presentan en una vista de columnas que incluye las categorías siguientes:

- Core
- Agent protegido
- Tipo
- Resumen
- Estado
- Error
- Hora de inicio
- Hora de finalización
- Hora
- Trabajo total

Acerca de los informes de errores

Los informes de errores son subconjuntos de los informes de cumplimiento y están disponibles para los Cores y AppAssure Agents. Los informes de errores incluyen solo trabajos fallidos en informes de cumplimiento y los compilan en un único informe que se puede imprimir y exportar.

Los detalles sobre los errores se presentan en una vista de columnas, con las siguientes categorías:

- Core
- Agent
- Tipo
- Resumen
- Error
- Hora de inicio
- Hora de finalización
- Tiempo transcurrido
- Trabajo total

Acerca del informe de resumen del Core

El **Core Summary Report (Informe de resumen del Core)** incluye información sobre los repositorios del Core seleccionado y sobre los Agents protegidos por dicho Core. La información aparece como dos resúmenes en un informe.

Resumen de repositorios

La parte **Repositories (Repositorios)** del informe **Core Summary Report (Informe de resumen del Core)** incluye datos para los repositorios ubicados en el Core seleccionado. Los detalles sobre los repositorios se presentan en una vista de columnas con las siguientes categorías:

- Name (Nombre)
- Data Path (Ruta de acceso datos)
- Metadata Path (Ruta de acceso a metadatos)

- Allocated Space (Espacio asignado)
- Used Space (Espacio utilizado)
- Free Space (Espacio libre)
- Compression/Dedupe Ratio (Relación compresión/desdup.)

Resumen de Agents

La parte **Agents** del **Core Summary Report (Informe de resumen del Core)** incluye datos para todos los Agents protegidos por el Core seleccionado.

Los detalles sobre los Agents se presentan en vista de columnas, con las categorías siguientes:

- Name (Nombre)
- Protected Volumes (Volúmenes protegidos)
- Total protected space (Espacio total protegido)
- Current protected space (Espacio actual protegido)
- Change rate per day (**Average, Median**) (Velocidad de cambio por día [Promedio, Mediana])
- Jobs Statistic (**Passed, Failed, Canceled**) (Estadísticas de trabajos (Aprobado, Erróneo, Cancelado))

Cómo generar un informe para un Core o Agent

Para generar un informe para un Core o Agent:

1. Vaya a la Core Console y seleccione el Core o Agent para el que desee ejecutar el informe.
2. Haga clic en la pestaña **Tools (Herramientas)**.
3. En la pestaña **Tools (Herramientas)**, expanda **Reports (Informes)** en el área de navegación izquierda.
4. En el área de navegación, seleccione el informe que desee ejecutar. Los informes disponibles varían en función de la selección realizada en el paso 1 y se describen a continuación.

| Máquina | Informes disponibles |
|--------------|-------------------------|
| Core | Informe de cumplimiento |
| | Informe de resumen |
| | Informe de errores |
| Agent | Informe de cumplimiento |
| | Informe de errores |

5. En el calendario desplegable **Start Time (Hora de inicio)**, seleccione una fecha de inicio y, a continuación, introduzca una hora de inicio para el informe.



NOTA: No hay datos disponibles anteriores a la creación del Core o Agent.

6. En el calendario desplegable **End Time (Hora de finalización)**, seleccione una fecha de finalización y, a continuación, introduzca la hora de finalización para el informe.
7. Para un **Core Summary Report (Informe de resumen del Core)**, seleccione la casilla de verificación **All Time (Todo el tiempo)** si desea que la **Start Time (Hora de inicio)** y la **End Time (Hora de finalización)** abarquen toda la vida útil del Core.
8. Para un **Core Compliance Report (Informe de cumplimiento del Core)** o un **Core Errors Report (Informe de errores del Core)**, utilice la lista desplegable **Target Cores (Cores de destino)** para seleccionar el Core para el que desee ver datos.

9. Haga clic en **Generate Report (Generar informe)**.


Una vez que se haya generado el informe, puede usar la barra de herramientas para imprimirlo o exportarlo.

Acerca de los informes de Core de la Central Management Console (Consola de administración central)

Su appliance DL le permite generar y ver información de resumen, de cumplimiento y de errores de varios Cores. Los detalles sobre los Cores se presentan en vistas de columna con las mismas categorías descritas en esta sección.

Cómo generar un informe desde la Central Management Console (Consola de administración central)

Para generar un informe desde la Central Management Console (Consola de administración central):

1. En la pantalla **Central Management Console Welcome (Bienvenido a la Consola de administración central)**, haga clic en el menú desplegable en la esquina superior derecha.
2. En el menú desplegable, haga clic en **Reports (Informes)** y, a continuación, seleccione una de las siguientes opciones:
 - **Informe de cumplimiento**
 - **Informe de resumen**
 - **Informe de errores**
3. En el área de navegación izquierda, seleccione el Core o los Cores para los que desee ejecutar el informe.
4. En el calendario desplegable **Start Time (Hora de inicio)**, seleccione una fecha de inicio y, a continuación, introduzca una hora de inicio para el informe.
 **NOTA:** No hay datos disponibles antes del momento en el que se implementaron los Cores.
5. En el calendario desplegable **End Time (Hora de finalización)**, seleccione una fecha de finalización y, a continuación, introduzca la hora de finalización para el informe.
6. Haga clic en **Generate Report (Generar informe)**.
Una vez que se haya generado el informe, puede usar la barra de herramientas para imprimirlo o exportarlo.

Obtención de ayuda

Búsqueda de documentación y actualizaciones de software

Desde la Core Console, están disponibles enlaces directos a la documentación y actualizaciones de software de AppAssure y DL1000 Appliance.

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

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 para tratar cuestiones relacionadas con ventas, asistencia técnica o servicio 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.