Quest

Rapid Recovery 6.2

Guía del usuario

Índice

Leyenda

WARNING: Un icono de AVISO indica la posibilidad de daños en la propiedad, lesiones personales o la muerte.

CAUTION: Un icono de PRECAUCIÓN indica un posible daño en el equipo o una pérdida de datos si no se siguen las instrucciones.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: Un icono de información indica información complementaria.

Introducción a Rapid Recovery

Rapid Recovery es una solución de copia de seguridad, replicación y recuperación que ofrece objetivos de punto de recuperación y objetivos con un tiempo de recuperación casi inexistente. Rapid Recovery ofrece protección de datos, recuperación ante desastres, migración de datos y administración de datos. Tiene la flexibilidad de realizar una restauración bare metal (hardware similar o diferente) y puede restaurar las copias de seguridad de máquinas virtuales físicas, independientemente del origen. Rapid Recovery también puede archivar en la nube, en un dispositivo de recuperación y copia de seguridad de la serie DL o en un sistema compatible de su elección. Con Rapid Recovery, puede replicar en uno o más destinos para obtener mayor redundancia y seguridad.

Rapid Recovery ofrece:

- **Flexibilidad.** Puede realizar una recuperación universal en varias plataformas, incluida la restauración de físico a virtual, de virtual a físico, de virtual a virtual y de físico a físico.
- **Integración de la nube**. Puede exportar una máquina virtual, archivar y replicar en la nube y realizar una restauración Bare Metal Restore de archivos en la nube. Entre los servicios en la nube compatibles se incluyen Microsoft Azure, Amazon Web Services (AWS), cualquier proveedor basado en OpenStack (incluido Rackspace) y Google Cloud. Las plataformas específicas del gobierno de los EE. UU. incluyen AWS GovCloud (US) y Azure Government.
- **Desduplicación inteligente**. Puede reducir los requisitos de almacenamiento almacenando los datos una vez y haciendo referencia a ellos en lo sucesivo (una vez por repositorio o dominio de cifrado).
- **Recuperación instantánea**. Nuestra función Live Recovery le permite acceder en primer lugar a los datos importantes, mientras que, en paralelo, se completan las operaciones de restauración restantes.
- **Recuperación a nivel de archivos**. Puede recuperar datos a nivel de archivo en las instalaciones, desde una ubicación remota o desde la nube.
- **Búsqueda a nivel de archivos**. Puede especificar criterios para buscar un intervalo de puntos de recuperación para uno o varios archivos. En los resultados de búsqueda puede seleccionar y restaurar los archivos que desee en el equipo del Core local directamente desde la Core Console.
- **Soporte virtual**. Rapid Recovery admite la exportación virtual puntual, lo que le permite generar una máquina virtual de arranque desde un punto de recuperación; y la espera virtual, en la que la máquina virtual de arranque que generó se actualiza continuamente después de cada copia de seguridad. Puede incluso realizar exportaciones virtuales a volúmenes compartidos del clúster de Microsoft Hyper-V.
- **Asistencia de Rapid Snap for Virtual**. La asistencia mejorada para la virtualización incluye la protección sin agentes de máquinas virtuales vCenter/ESXi e Hyper-V. Rapid Snap for Virtual incluye la protección y la detección automática para VMware ESXi 5.5 y posteriores sin un software Agent instalado. La protección basada en hosts admite la instalación de Rapid Recovery Agent únicamente en un host Microsoft Hyper-V, lo que le permite proteger sin agentes a todas las máquinas virtuales invitadas.
- **Asistencia de la aplicación**. Rapid Recovery Agent está integrado con asistencia para las aplicaciones Microsoft Exchange, SQL Server y Oracle. Cuando protege estos servidores de aplicación en su Core, las instantáneas de copia de seguridad ofrecen automáticamente reconocimiento por parte de la aplicación, es decir, los registros de transacciones abiertas y transacciones en marcha se completan y las memorias caché se vacían antes de crear la instantánea. Se admiten funciones específicas de aplicaciones, incluidas la conectabilidad SQL (de SQL Server) y la comprobación de la integridad de la base de datos DBVERIFY (de Oracle). El reconocimiento de aplicaciones también se aplica a la protección sin agentes de SQL Server y Exchange Server.

Consulte los siguientes recursos para obtener más información acerca de Rapid Recovery.

- El sitio web de soporte del producto Rapid Recovery en https://support.quest.com/rapid-recovery/.
- El sitio web de documentación en https://support.quest.com/rapid-recovery/technical-documents/.

Core Console

Esta sección describe los diversos elementos de la interfaz de usuario (IU) de la Core Console de Rapid Recovery.

Acceso a la Core Console de Rapid Recovery

Complete los pasos siguientes para acceder a la Core Console de Rapid Recovery.

- Realice una de las siguientes acciones para acceder a la Core Console de Rapid Recovery:
    1. Inicie sesión localmente en el servidor del Core de Rapid Recovery y haga doble clic en el icono Core Console.
    2. O bien, escriba una de las URL siguientes en el navegador web:
    - https://<NombreServidorCore>:8006/apprecovery/admin/ o
    - https://<DirecciónIPServidorCore>:8006/apprecovery/admin/

> **NOTE:** Como la interfaz de usuario de la Core Console de Rapid Recovery depende de JavaScript, el navegador web que utiliza para acceder a Core Console debe tener JavaScript habilitado.
>
> **NOTE:** Si ha cambiado el puerto predeterminado del servicio Rapid Recovery, actualice el puerto en la URL anterior según corresponda.

Comprensión de la Guía de inicio rápido

La Guía de inicio rápido es una función que indica un recorrido guiado de tareas sugeridas para configurar y utilizar el Rapid Recovery Core.

La Guía de inicio rápido aparece automáticamente la primera vez que instala o actualiza el Rapid Recovery Core y accede a la Core Console. Haga clic en **Iniciar guía** en la **página de bienvenida** para ver las distintas tareas de configuración sugeridas. Consulte la guía usando las opciones **Omitir paso** y **Atrás**. Cuando haya visto la última tarea sugerida, haga clic en **Finalizar** para cerrar la guía.

Puede volver a iniciar la guía de inicio rápido en cualquier momento desde el menú de ayuda de la Core Console. También puede optar por ocultar la página de **bienvenida** en la Guía de inicio rápido.

A no ser que la oculte, la Guía de inicio rápido aparece cada vez que inicia sesión en la Rapid Recovery Core Console y que accede a la página **Inicio**. Para obtener más información, consulte Cómo ocultar la Guía de inicio rápido.

No es necesario que realice los pasos sugeridos en la guía. Simplemente puede consultar las tareas sugeridas utilizando las opciones **Omitir paso** y **Atrás**. También puede ocultar la guía en cualquier momento y hacer clic en **Salir de la guía**.

Si elige realizar cualquier tarea de configuración sugerida en la Guía de inicio rápido, siga las indicaciones que aparecen en cualquier paso de la guía para mostrar el asistente o área correspondiente de la interfaz de usuario. Los procedimientos necesarios para completar todas las tareas sugeridas en la guía se describen en este documento, tal y como se indica en la siguiente tabla.

NOTE: No todos los usuarios necesitan realizar todas las tareas de configuración sugeridas en la Guía de inicio rápido. Debe entender qué tareas quiere cumplir según sus necesidades concretas.

La Guía de inicio rápido soluciona todas las siguientes tareas de configuración:

Tabla 1. Tareas de configuración de la Guía de inicio rápido

Función	Descripción corta	Resultado de seleccionar la tarea, enlace a procedimiento
Protección	Protección de un único equipo, protección de un clúster de servidor o protección de varios equipos usando la protección masiva	Haga clic en Proteger o seleccione **Proteger equipo** en el menú desplegable para abrir el Asistente para proteger un equipo. Para obtener más información sobre cómo completar el Asistente para proteger un equipo, consulte Protección de un equipo. Seleccione **Proteger clúster** en el menú desplegable para abrir el cuadro de diálogo Conectarse al clúster. Para obtener más información sobre cómo proteger un clúster, consulte Protección de un clúster. Seleccione **Protección masiva** en el menú desplegable para abrir el Asistente para proteger varios equipos. Para obtener más información sobre cómo completar el Asistente para proteger varios equipos, consulte Acerca de la protección de varios equipos.
Replicación	Configuración de una replicación de un Core primario (origen) a uno secundario (destino)	Haga clic en **Replicación** para abrir la página Replicación. Le solicita que agregue un Core de destino mediante el asistente Replicación. Para obtener información sobre cómo usar el asistente Replicación para configurar la replicación en un Core administrado automáticamente, consulte Replicación en un Core de destino administrado automáticamente. Para obtener más información sobre la replicación, consulte Configuración de la replicación.
Exportación virtual	Realización de una exportación puntual o establecimiento de una exportación continua desde un equipo protegido a una máquina virtual	Haga clic en **Exportar** para realizar una exportación de datos de su equipo protegido a una máquina virtual. Puede realizar una única exportación puntual o establezca una espera virtual para la exportación continua a una máquina virtual. Para obtener información sobre la exportación virtual, consulte Exportación a máquinas virtuales con Rapid Recovery.
Administrar y configurar	Le permite establecer la configuración adicional del Rapid Recovery Core	Haga clic en **Más** para ver las funciones adicionales que puede administrar o configurar. Las funciones incluyen archivos comprimidos, montajes, CD de inicio, repositorios, claves de cifrado, cuentas de la nube, búsqueda de archivos, políticas de retención, notificaciones, informes, registros, etc.
Configurar cifrado	Agregar o importar claves de cifrado que puede utilizar para uno o varios equipos protegidos	Haga clic en **Claves de cifrado** para gestionar la seguridad de los datos protegidos agregando o importando claves de cifrado. Puede aplicar claves de cifrado a uno o varios

Función	Descripción corta	Resultado de seleccionar la tarea, enlace a procedimiento
		equipos protegidos. El cifrado se describe en el tema Cifrado.
Configurar notificaciones	Configuración de las notificaciones para los eventos, advertencias y alertas.	Haga clic en **Eventos** para especificar grupos de notificación de eventos, advertencias y alertas. Para enviarlos por correo electrónico, también deberá establecer los ajustes del servidor SMTP. Para obtener más información sobre cómo administrar eventos, consulte el tema Eventos, incluidos los temas Configuración de grupos de notificación y Configuración de un servidor de correo electrónico.
Administrar retención	Permite consultar o cambiar la política de retención predeterminada para el Core	Haga clic en **Política de retención** para abrir la página Política de retención para el Core. Desde aquí puede definir cuánto tiempo conservar un punto de recuperación antes de consolidarlo. Para obtener información sobre los conceptos de las políticas de retención, consulte el tema Administración de datos anteriores. Para obtener información sobre los procedimientos, consulte Administración de políticas de retención.
Restaurar	Restauración de datos desde un punto de recuperación del Core	Haga clic en **Restaurar** para abrir el Asistente para restaurar un equipo. Para obtener información sobre cómo restaurar datos, consulte el tema Acerca de la restauración de volúmenes desde un punto de recuperación.

Cómo ocultar la Guía de inicio rápido

La Guía de inicio rápido aparece automáticamente la primera vez que instala o actualiza el Core de Rapid Recovery.

También aparece cuando selecciona Guía de inicio rápido en el menú desplegable Ayuda y cada vez que accede a la página Inicio de la Consola de Core.

Utilice el siguiente procedimiento para ocultar la Guía de inicio rápido.

- En la Core Console de Rapid Recovery, si está consultando la página **Bienvenido** de la Guía de inicio rápido, haga lo siguiente:
  - Si quiere ocultar la página **Bienvenido** de la Guía de inicio rápido, seleccione **No volver a mostrar**.

    NOTE: Esta opción ocultará la página **Bienvenido** la próxima vez que se abra la Guía de inicio rápido y después hasta que actualice el Core de Rapid Recovery.

    NOTE: Si selecciona ocultar esta página y desea acceder a las opciones avanzadas de la función, seleccione **Atrás** en el asistente para ver esta página oculta.
  - Si quiere ocultar la Guía de inicio rápido para esta sesión, a continuación haga clic en **Cerrar**.

    Se cierra la Guía de inicio rápido. La siguiente vez que acceda a la página Inicio en la Consola de Core, volverá a aparecer la Guía de inicio rápido.
    También puede abrir la Guía de inicio rápido desde el menú Ayuda.
- En cualquier página de la Guía de inicio rápido, haga clic en **Salir de la guía**.

  Se cierra la Guía de inicio rápido. Aunque seleccione esta opción, podrá seguir abriendo la Guía de inicio rápido desde el menú Ayuda.

Desplazarse hasta la Rapid Recovery Core Console

Cuando inicia sesión en la Core Console y cada vez que hace clic en el icono **Inicio** , aparece la página **Inicio**. La página **Inicio** le brinda una vista del Rapid Recovery Core con dos opciones. En el área de visualización principal, el contenido predeterminado es el nuevo panel del Core, que muestra un conjunto de informes en tiempo real en el sistema. Los informes predeterminados del panel incluyen el estado reciente del trabajo de transferencia, las transferencias por equipo, una descripción general del repositorio y el estado de la conectividad de equipos protegidos, replicados y con puntos de recuperación únicamente. También puede cambiar a la clásica vista Tablas de resumen. En esta vista, el título de la página muestra el nombre para mostrar del Rapid Recovery Core y puede ver tablas de resumen que muestran los equipos protegidos, repositorios y alertas recientes. Para obtener más información, consulte Funcionamiento de la página Inicio (vista de tablas de resumen) y Funcionamiento de los informes del panel del Core, respectivamente.

En la página **Inicio** (y en cada página de la Core Console), el área de navegación de la izquierda muestra los elementos que están protegidos en el Core. Puede navegar a otras páginas en la IU mediante uno de estos procedimientos:

- Hacer clic en el icono correspondiente de la barra de iconos en el área de navegación de la izquierda.

  Las opciones a las que se puede acceder desde la barra de iconos incluyen Replicar, En espera virtual, Eventos, Configuración y Más.
- Expandir el menú (Más) en la barra de iconos y, a continuación, seleccionar un destino.
- Hacer clic en un botón u opción de menú de la barra de botones. Los botones incluyen Proteger, Restaurar, Archivo y Replicar.

Cuando selecciona un elemento en el área de navegación izquierda, el enfoque de la Core Console cambia para mostrar información de resumen sobre dicho elemento. Por ejemplo, si hace clic en el nombre de un equipo protegido, la Core Console muestra información únicamente sobre dicho equipo, en lugar de sobre el Core. En este ejemplo, el nombre para mostrar del equipo protegido figura como el título de la página. Aparecerá un submenú a la derecha en el que puede ver información específica sobre el equipo protegido. Las opciones del menú incluyen: Resumen, Puntos de recuperación, Eventos, Configuración, Informes y Más.

Para volver a la visualización de la información sobre el Core, incluyendo los informes del panel o una vista de resumen de varios equipos protegidos o duplicados, haga clic en el icono **Inicio** de la parte superior derecha de la UI. En la página **Inicio**, puede alternar entre la vista de panel y la de página de resumen haciendo clic en el enlace rojo de la parte superior derecha de la página.

Puede utilizar el título de la parte superior de la Core Console con el fin de proporcionar contexto para la información que está viendo en el Core. Por ejemplo:

- Cada vez que vea el nombre para mostrar o la dirección IP del Core como título de la página, lo que está viendo es información de resumen del Core.
- Si el título es "Panel", lo que ve es el panel del Core.
- Si aparece el nombre para mostrar o la dirección IP de un equipo protegido, o un panel Resumen en la parte superior de una página, quiere decir que está viendo información acerca de un solo equipo protegido por o replicado en el Core.
- Si aparece el título "Equipos protegidos", significa que se está viendo información acerca de todos los equipos protegidos en el Rapid Recovery Core.
- Si aparece el título "Equipos replicados de...", es que está viendo información sobre todos los equipos replicados en el Rapid Recovery Core.
- Si aparece el título de página "Solo puntos de recuperación", quiere decir que está viendo información acerca de todos los equipos con puntos de recuperación únicamente en este Core.

Para obtener información sobre las características y funciones disponibles en cada página, consulte la sección apropiada a continuación.

Para obtener más información sobre la visualización de equipos protegidos, consulte Visualización del menú Equipos protegidos. Para obtener más información sobre la administración de equipos protegidos, consulte Administración de equipos protegidos.

Para obtener más información sobre la visualización de equipos replicados, consulte Visualización de la replicación entrante y saliente.

Para obtener más información sobre la visualización de equipos con puntos de recuperación únicamente, consulte Visualización en el menú Solo puntos de recuperación.

Comprensión del área de navegación izquierda

El área de navegación izquierda aparece en Core Console, en el lado izquierdo de la interfaz de usuario. El contenido de esta área de navegación puede ser diferente según el tipo de objetos protegidos en el Rapid Recovery Core.

El área de navegación izquierda siempre contiene lo siguiente:

- **Barra de iconos.** Para navegar entre las páginas principales de Core Console.
- **Filtro de texto.** El filtro de texto es un campo de texto que le permite filtrar los elementos que se muestran en los distintos menús que aparecen debajo del mismo. Al hacer clic en la flecha situada a la derecha del filtro de texto se expande y contrae cada uno de los menús que aparecen.

Al seguir estos elementos, el área de navegación izquierda muestra los menús para ayudarle a navegar, filtrar y ver los objetos protegidos en el Core. Esto incluye equipos protegidos y equipos replicados, entre otros.

Cada menú es contextual, es decir, el menú solo aparece en Core Console si es pertinente. Por ejemplo, si protege al menos un equipo, aparece el menú Equipos protegidos, y así sucesivamente.

Para obtener más información, consulte las tablas que figuran en el área de navegación de la izquierda Visualización de la interfaz para el usuario de la Core Console.

See also: Visualización de información de resumen de un equipo protegido
See also: Ver información de resumen para un host
See also: Replicación
See also: Comprensión de los grupos personalizados

Visualización de la página Inicio de la Rapid Recovery Core Console

Cada vez que inicie sesión en Rapid Recovery Core Console o cada vez que haga clic en el icono **Inicio**  de la barra de iconos, aparece la página **Inicio**. La página **Inicio** ofrece una vista del **panel** y una vista conocida de las **tablas de resumen**. Las tablas de resumen es la vista predeterminada.

Puede alternar entre las vistas de la página **Inicio** haciendo clic en el icono de alternar la vista de panel  en la parte superior derecha de la página **Inicio**.

En la página **Inicio**, y cada dos páginas de Core Console, puede desplazarse hacia las funciones que desee utilizando el área de navegación izquierda.

Para obtener más información, consulte los siguientes temas:

- Comprensión del área de navegación izquierda
- Funcionamiento de los informes del panel del Core
- Funcionamiento de la página Inicio (vista de tablas de resumen)
- Visualización de la interfaz para el usuario de la Core Console

Funcionamiento de la página Inicio (vista de tablas de resumen)

La página **Inicio** solo se aplica al Core. En la vista de panel, muestra informes gráficos en tiempo real. Cuando cambia a la vista Tablas de resumen, la página **Inicio** muestra todos los equipos o réplicas que protege el Core, los repositorios asociados al Core y las alertas para equipos de este Core.

La vista de cada panel en la página **Inicio** se puede ampliar o contraer. Por ejemplo, si hace clic en el icono  (contraer vista) que se encuentra en la parte superior derecha del panel Equipos protegidos, se contrae la vista de equipos protegidos y solo es visible el nombre del panel. Para expandir la vista para volver a ver todos los equipos protegidos, haga clic en el icono  (expandir vista).

La siguiente tabla describe los diversos elementos en la página **Inicio** cuando se encuentra en la vista de tablas de resumen.

Tabla 2. Opciones de la página Inicio

Elemento de la IU	Descripción
Equipos protegidos	El panel Equipos protegidos enumera los equipos que protege el Core. Este panel aparece independientemente de que se haya agregado algún equipo al Core para su protección o no.

Elemento de la IU	Descripción
	Esta sección incluye la siguiente información para cada equipo protegido: • **Tipo de equipo.** Un icono muestra si se trata de un equipo físico, de una máquina virtual o de un clúster protegido. • **Estado.** Los círculos de color en la columna Estado muestran si se puede acceder al equipo protegido, si se encuentra en pausa, fuera de línea o si no se puede contactar con él. • **Nombre para mostrar.** El nombre que se muestra o la dirección IP del equipo protegido. • **Nombre del repositorio.** El nombre del repositorio que almacena los puntos de recuperación de ese equipo. • **Última instantánea.** La fecha y la hora a la que Rapid Recovery tomó la instantánea del punto de recuperación más reciente de ese equipo. • **Puntos de recuperación.** El número de puntos de recuperación almacenados en el repositorio y el uso de espacio para cada equipo protegido. • Versión. La versión del software Rapid Recovery Agent instalado en ese equipo. Si hace clic en un nombre de equipo específico que se muestra en este panel, aparece una página Resumen, que muestra la información de resumen del equipo seleccionado. Para obtener más información sobre lo que puede realizar en la página Resumen, consulte Visualización de información de resumen de un equipo protegido.
Equipos replicados	El panel Equipos replicados indica los equipos que este Core replica de otro Core. Este panel no aparece a menos que su Core replique equipos de otro Core. Esta sección incluye la siguiente información para cada equipo replicado: • **Tipo de equipo.** Un icono muestra si se trata de un equipo físico, de una máquina virtual o de un clúster protegido. • **Estado.** Los círculos de color en la columna Estado muestran si se puede acceder al equipo replicado, si se encuentra en pausa, fuera de línea o si no se puede contactar con él. • **Nombre para mostrar.** El nombre que se muestra o la dirección IP del equipo replicado. • **Nombre de replicación.** El nombre para mostrar del Core de origen de los equipos que replica en este Core de destino. Puede definir este nombre cuando configure la replicación. • **Nombre del repositorio.** El nombre del repositorio que almacena los puntos de recuperación de ese equipo. • **Última instantánea replicada.** La fecha y la hora a la que Rapid Recovery Rapid Recovery realizó la réplica más reciente del equipo protegido original. • **Puntos de recuperación.** El número de puntos de recuperación almacenados en el repositorio y el uso de espacio para cada equipo replicado. • Versión. La versión del software Rapid Recovery Agent instalado en ese equipo. Si hace clic en un nombre de equipo específico que aparezca en este panel, se muestra la página Resumen, donde se enumera información de resumen de ese equipo replicado.
Equipos con puntos de	El panel Equipos con puntos de recuperación únicamente enumera los equipos que muestran las máquinas que se retiran de la protección o replicación, si se han

Elemento de la IU	Descripción
recuperación únicamente	conservado los puntos de recuperación. Estos equipos pueden utilizarse para la recuperación a nivel de archivos, pero no pueden utilizarse para una recuperación Bare Metal Restore, para restaurar volúmenes completos, o para agregar datos de instantáneas. Este panel no aparecerá a menos que tenga algún equipo que cumpla esta definición. Esta sección incluye la siguiente información para cada equipo con solo puntos de recuperación: • **Tipo de equipo.** Un icono muestra si se trata de un equipo físico, de una máquina virtual o de un clúster protegido. • **Estado.** Los círculos de color en la columna Estado muestran si se puede acceder al equipo con puntos de recuperación únicamente, si se encuentra en pausa, fuera de línea o si no se puede contactar con él. • **Nombre para mostrar.** El nombre para mostrar o dirección IP del equipo para el que mantuvo puntos de recuperación. • **Nombre del repositorio.** El nombre del repositorio que almacena el resto de puntos de recuperación de ese equipo. • **Puntos de recuperación.** El número de puntos de recuperación almacenados en el repositorio y el uso de espacio para cada equipo de puntos de recuperación únicamente. Si hace clic en un nombre de equipo específico que aparezca en este panel, se muestra la página Resumen para este equipo con puntos de recuperación únicamente.
Repositorios DVM	Este panel aparece para la configuración DL1000, independientemente de que se hayan creado repositorios Administrador de volúmenes de desduplicación (DVM). Este panel no aparece a menos que el Core tenga uno o más repositorios DVM. Incluye la siguiente información para cada repositorio DVM: • **Tipo.** Un icono muestra un repositorio. • **Estado.** Los círculos coloreados en la columna Estado muestran si un repositorio está montado y puede aceptar transferencias de puntos de recuperación, o si no se puede contactar con él o tiene un estado de error. • **Nombre del repositorio.** El nombre para mostrar del repositorio. • **Uso del espacio.** La cantidad total de espacio utilizado en el repositorio y el tamaño del volumen de almacenamiento o su ampliación. • **Datos protegidos.** La cantidad de espacio utilizada en el repositorio. • **Equipos.** El número de equipos para los que el repositorio almacena puntos de recuperación. • **Puntos de recuperación.** El número de puntos de recuperación almacenados en el repositorio. • **Tasa de compresión.** El índice al que el repositorio comprime los datos protegidos para ahorrar espacio. Para obtener más información, consulte Comprensión de los repositorios.

Elemento de la IU	Descripción
Alertas	Esta sección enumera las alertas importantes para el Core y cada equipo que protege. La sección incluye la siguiente información: • **Iconos.** La columna de iconos indica la naturaleza de la alerta. Estas alertas incluyen mensajes informativos y errores. • **Fecha.** Muestra la fecha y la hora a las que Rapid Recovery emitió la alerta. • **Mensaje.** Describe la alerta. También puede ver estos detalles en la página Eventos del Core. Para obtener más información, consulte Visualización de eventos mediante las páginas de tareas, alertas y del diario.

Funcionamiento de los informes del panel del Core

El panel del Core muestra un conjunto de informes gráficos en tiempo real de datos relevantes para el Core, los equipos que protege y las instantáneas guardadas en el repositorio. Los informes del panel incluyen:

- Informes del sistema Core
  - **Supervisor de problemas**. Este informe muestra la actividad de trabajo, las conexiones con el portal de licencias y la actividad de transferencia para detectar antes problemas en el sistema. Haga clic en el widget de reloj para borrar toda la actividad a la que se le ha realizado un seguimiento y supervisar los eventos nuevos.
  - **Repositorio**. Este informe muestra los repositorios asociados con el Core. Muestra el número de repositorios, cuántos equipos están protegidos en cada uno, el número de puntos de recuperación y el porcentaje de compresión o desduplicación. Este informe se actualiza cada minuto.
- Informes del equipo
  - **Conectividad de equipo**. Este informe muestra el estado de la conectividad de los equipos protegidos y replicados en el Core. También muestra la conectividad de datos en un puntos de recuperación-solo equipo.
- Informes de instantáneas
  - **Trabajo de transferencia**. Este informe muestra todas las transferencias de datos de instantáneas (incluidas las imágenes base e instantáneas incrementales) que se han completado en las últimas 24 horas. Las instantáneas incluyen imágenes base e instantáneas incrementales. Este informe del panel aparece como un gráfico de círculos.
  - **Trabajo de transferencia por equipo**. Este trabajo indica, por equipo protegido, el número de operaciones correctas y trabajos de transferencia con fallos en las últimas 24 horas. Este informe del panel aparece como un gráfico de líneas.

En la parte superior del recuadro Panel, puede hacer clic en el widget  (Expandir) para mostrar una lista de informes que aparecen en el panel en las tres categorías descritas anteriormente. Cada categoría de informes, y cada informe, tiene una casilla. Si la casilla está seleccionada, el informe o la categoría aparecerán en el panel. Si desactiva esta opción, el informe no se mostrará. De esta manera, puede cambiar fácilmente la visualización de los informes en el panel. Si hace clic en  (Contrato), el menú desaparece.

También puede contraer o ampliar la vista de los informes en el panel al hacer clic en la flecha hacia arriba o hacia abajo en el encabezado del informe. Algunos informes del panel (conectividad de equipo y de repositorio) tienen un signo más junto a la flecha, desde la que se puede agregar otro equipo protegido u otro repositorio, respectivamente.

También puede arrastrar y soltar para mover la ubicación de uno de los informes a otro lugar en el panel, para solicitar los informes de una forma más eficaz para su uso.

Visualización del menú Equipos protegidos

En la interfaz de usuario de Rapid Recovery, aparece un menú Equipos protegidos en el área de navegación izquierda. Al igual que con todas las etiquetas de menú en el área de navegación, la etiqueta de este menú aparece en todas las letras mayúsculas. Este menú está ampliado completamente de forma predeterminada, y muestra una lista de todos los equipos que están protegidos por este Core. Si tiene clústeres de servidores protegidos, estos también se incluyen en esta lista.

Puede contraer o ampliar la vista de cualquiera de estos equipos protegidos y clústeres de servidores en su Core haciendo clic en la fecha del lado izquierdo de este menú.

El menú Equipos protegidos incluye un menú desplegable en el lado derecho que muestra las funciones que se pueden realizar en todos los equipos protegidos. Haga clic en la flecha situada a la derecha de **Equipos protegidos** para ver el menú.

Todos los equipos que aparecen en el menú Equipos protegidos tienen un menú desplegable que controla las funciones de ese equipo exclusivamente.

Si está gestionando clústeres de servidores desde el Core de Rapid Recovery, el clúster también aparece en el menú de navegación de la izquierda. En el menú desplegable de cualquier clúster, también puede ir a la página **Nodos protegidos** del clúster seleccionado.

Si hace clic en la flecha de la izquierda del menú Equipos protegidos, se contrae la lista de equipos protegidos y clústeres de servidores y dejan de mostrarse los equipos. Si vuelve a hacer clic en esta flecha, la lista de equipos vuelve a abrirse.

Si hace clic en cualquier nombre de equipo del menú Equipos protegidos, se abre la ficha Resumen de ese equipo. Para obtener más información sobre lo que puede realizar en la página Resumen, consulte Visualización de información de resumen de un equipo protegido.

Por último, al hacer clic directamente en el menú **Equipos protegidos**, la página **Equipos protegidos** aparece en el área de contenido principal con un único panel que muestra los equipos protegidos en este Core. Para obtener más información sobre lo que puede hacer en el panel **Equipos protegidos** de la página Equipos protegidos, consulte .

NOTE: Desde la página **Equipos protegidos**, puede volver a una vista desde la perspectiva del Core haciendo clic en el icono **Inicio** de la barra de iconos.

Visualización de información de resumen de un equipo protegido

Si hace clic en el nombre de un equipo protegido en la Core Console, aparecerá la página **Resumen**. Esta página contiene, como mínimo, un panel Resumen y un panel Volúmenes. Si se agrega un equipo a la replicación, también aparecerá un panel Replicación.

Si dispone de uno o más servidores Exchange protegidos, también verá un panel Información de Exchange Server, que contiene información sobre sus Exchange Servers protegidos.

Si dispone de uno o más SQL Servers protegidos, también verá un panel Información de SQL Server, que contiene información sobre sus SQL Servers protegidos.

En la parte superior de esta página, hay un menú con acciones que puede realizar en el equipo protegido. Debajo, como mínimo, aparece un panel Resumen y un panel Volúmenes. Si se agrega un equipo a la replicación, también aparecerá un panel Replicación.

Cuando se muestra información de un equipo protegido (en la página Resumen y en el resto de vistas), aparece un menú situado en la parte superior de la página con las funciones que puede llevar a cabo. Dicho menú aparece justo debajo del nombre del equipo protegido.

See also: Visualización en el panel Resumen
See also: Visualización de volúmenes en un equipo protegido
See also: Visualización de la información de replicación
See also: Visualización del panel Información de Exchange Server
See also: Visualización del panel Información de SQL Server
c_Viewing_summary_information_for_a_host.xml

Visualización en el panel Resumen

El panel **Resumen** contiene información de resumen sobre el equipo protegido, incluyendo el nombre de host, la fecha y la hora de la última instantánea, la fecha y la hora de la próxima instantánea programada, la información de la clave de cifrado y la información de la versión del software Rapid Recovery Agent. También existe un vínculo a una página detallada sobre información del sistema para el equipo.

Visualización de volúmenes en un equipo protegido

Puede realizar las siguientes acciones para cualquiera de los volúmenes enumerados desde la página Resumen en el panel Volúmenes para cualquier equipo protegido:

- Establezca una programación de protección de un volumen seleccionado. Las programaciones de protección se establecen normalmente cuando protege por primera vez un equipo. Para obtener más información sobre la modificación de la programación para protección, consulte Creación de un programa de protección personalizado en el modo simple.
- Forzar una imagen base o instantánea. Las instantáneas se realizan normalmente en base a la programación de protección. Sin embargo, puede forzar la realización de una imagen base o una instantánea incremental de los volúmenes seleccionados siempre que quiera. Para obtener más información, consulte Cómo forzar una instantánea.

Visualización de la información de replicación

El panel **Replicación** contiene información de resumen sobre el equipo replicado, incluidos el nombre de replicación, el estado de la replicación, el progreso y el espacio disponible.

Visualización del panel Información de Exchange Server

El panel **Información de Exchange Server** solo aparece en los equipos protegidos que son Exchange Server.

Este panel contiene información de resumen sobre el Exchange Server protegido, incluida la versión instalada de Microsoft Exchange, la ruta de acceso en la que está instalado Exchange y la ruta de acceso definida en los datos de correo de Exchange.

La cuadrícula de almacenes de correo muestra el nombre de la Base de datos de Exchange (EDB), la ruta de acceso del archivo EDB, la ruta de acceso en la que los archivos de registro están almacenados, el prefijo de registro, la ruta de acceso del sistema, el Grupo de disponibilidad de base de datos (DAG) y el tipo de almacén de correo.

Visualización del panel Información de SQL Server

El panel **Información de SQL Server** solo aparece para los equipos protegidos que sean servidores SQL Server.

Este panel contiene información de resumen sobre los servidores SQL Server protegidos. Puede ampliar la información de la base de datos para ver la información detallada de cada tabla en dicha base de datos. También puede ver la base de datos o el nombre de tabla y la ruta de acceso a la base de datos.

Ver información de resumen para un host

Si hace clic en el nombre de un hipervisor o equipo host del clúster en la Core Console, aparecerá la página **Resumen**. Esta página contiene, como mínimo, una barra de acciones de función, el panel Resumen y el panel Procesadores. La barra de acciones se muestra en la parte superior de todas las páginas del host. El panel Resumen incluye información como el nombre del host y el software de virtualización. El panel Procesadores incluye una tabla que enumera la arquitectura, el número de Cores, el número de hilos, la velocidad del reloj y una descripción de cada procesador.

Dependiendo del tipo de host que sea el equipo, también se pueden mostrar los siguientes paneles:

- **Servidor SMB.** Si un host Hyper-V utiliza uno o más servidores SMB, esta sección muestra el nombre de host de cada servidor SMB.
- **Nodos.** La página de **Resumen** de un host de clúster incluye la sección para mostrar el nombre de host y el número de versión de Rapid Recovery de cada nodo.
- **Volúmenes.** Cuando utilice una protección sin agentes, la página **Resumen** de un host de Hyper-V incluye esta sección para mostrar el nombre, el sistema de archivos, el uso de espacio. la programación actual y la siguiente instantánea de cada volumen protegido.
- **Discos compartidos.** Si un host de Hyper-V que utiliza una protección sin agentes tiene uno o más VHDX compartidos, esta sección muestra el nombre y la ruta de acceso de cada disco duro virtual.

Para obtener más información acerca de clústeres de CSV, consulte "Soporte para volúmenes compartidos de clúster" en la *Rapid Recovery System Requirements Guide (Guía de requisitos del sistema de Rapid Recovery)*. Para obtener información acerca de otros temas relacionados, consulte los siguientes enlaces:

- Visualización de información de resumen de un equipo protegido
- Comprensión de Rapid Snap for Virtual

Visualización de los puntos de recuperación para un equipo

En la página Puntos de recuperación se muestra una lista de los puntos de recuperación recopilados para ese equipo protegido, así como los datos pertinentes de equipo y repositorio. En esta página puede montar, exportar y restaurar puntos de recuperación específicos, así como eliminar puntos de recuperación.

La página se divide en dos paneles: Resumen de puntos de recuperación y Puntos de recuperación. El panel Resumen no incluye ningún vínculo para el usuario. Muestra los siguientes datos del equipo.

Tabla 3. Datos del panel Resumen de puntos de recuperación

Elemento de la IU	Descripción
Total de puntos de recuperación	El número de puntos de recuperación recopilados para este equipo protegido en particular.

Elemento de la IU	Descripción
Total de datos protegidos	La cantidad de datos de este equipo protegido que están almacenados en el repositorio.
Repositorio	El nombre del repositorio en el que Rapid Recovery almacena los puntos de recuperación de este equipo protegido.
Estado del repositorio	La barra de progreso muestra el porcentaje del espacio total utilizado en el repositorio. La cantidad de datos utilizada y el tamaño total del repositorio aparecen debajo de la barra de progreso.

Para obtener más información, consulte .

Visualización de eventos de un equipo protegido

En la página **Eventos**, puede ver los trabajos que se han realizado o que están en curso en el equipo protegido que seleccionó. Los botones de la parte superior de la página le permiten navegar a listas de trabajos en cada una de las tres categorías de actividades:

- **Tareas.** Un trabajo que Rapid Recovery debe realizar para funcionar correctamente.
- **Alertas.** Una notificación relacionada con una tarea o evento que incluye errores y advertencias.
- **Diario.** Un compuesto de todas las tareas y alertas del equipo protegido.

La siguiente tabla incluye las descripciones de cada elemento de la página **Eventos**.

Tabla 4. Elementos de la página Eventos

Elemento de la IU	Descripción
Palabra clave de la búsqueda	Le permite buscar un elemento específico dentro de cada categoría. Solo disponible para tareas.
De	Para restringir los resultados, puede introducir una fecha en la que empezar la búsqueda. Solo disponible para tareas.
A	Para restringir los resultados, puede introducir una fecha en la que detener la búsqueda. Solo disponible para tareas.
Iconos de estado	Cada icono representa un estado de trabajo diferente. En el caso de alertas y tareas, al hacer clic en uno de los iconos podrá filtrar la lista por ese estado, generando

Elemento de la IU	Descripción
	básicamente un informe. Al hacer clic en el icono una segunda vez elimina el filtro para ese estado. Puede filtrar por más de un estado. Los estados incluyen: • **Activo.** Un trabajo que está en curso. • **En cola.** Un trabajo que está esperando que otro trabajo finalice antes de poder iniciarse. • **Esperando.** Un trabajo que está esperando su aprobación o finalización, como una unidad de inicialización. (Para obtener más información acerca de las unidades de inicialización, consulte Replicación.) • **Finalizado.** Un trabajo que se ha realizado correctamente. • **Con fallo.** Un trabajo que ha fallado y no se completó.
Icono de servicio	Este botón agrega trabajos de servicios a la lista de trabajos. Cuando hace clic en este icono, aparece un icono de servicio más pequeño en cada icono de estado, que le permite filtrar por trabajos de servicio que tienen esos estados (si los hubiera). Los ejemplos de trabajos de servicios incluyen la eliminación de archivos de índice o retirar un equipo de la protección.
Lista desplegable Tipo de exportación	La lista desplegable incluye los formatos con los que puede exportar el informe del evento. Solo disponible para tareas. Incluye los siguientes formatos: • PDF • HTML • CSV • XLS • XLSX
(icono Exportar)	Convierte el informe del evento al formato que seleccionó. Solo disponible para tareas.
Selección de página	Los informes de eventos pueden incluir varios trabajos en múltiples páginas. Los números y las flechas de la parte inferior de la página **Eventos** permiten navegar a las páginas adicionales del informe.

La página **Eventos** muestra todos los eventos de una tabla. La siguiente tabla enumera la información que se muestra para cada elemento.

Tabla 5. Información detallada para la tabla de resumen de los eventos

Elemento de la IU	Descripción
Estado	Muestra el estado de la tarea, alerta o el elemento diario. Está disponible para las alertas o los elementos diario; haga clic en el encabezado para filtrar los resultados por estado.
Nombre	Nombre está disponible solo para las tareas. Este campo de texto enumera el tipo de tarea que se ha completado para este equipo protegido. Algunos ejemplos incluyen la transferencia de volúmenes, el mantenimiento del repositorio, la consolidación, la realización de comprobaciones de la capacidad de montaje, la realización de comprobaciones de suma de comprobación, y así sucesivamente.

Elemento de la IU	Descripción
Hora de inicio	Disponible para las tareas, alertas y los elementos diario. Muestra la fecha y la hora en las que se inició el trabajo o la tarea.
Hora de finalización	Solo disponible para tareas. Muestra la fecha y la hora en las que se completó la tarea.
Detalles del trabajo	Solo disponible para tareas. Se abre el cuadro de diálogo **Supervisar tarea activa** por lo que puede ver los detalles de un trabajo específico o una tarea. Estos detalles incluyen una ID para el trabajo, la velocidad a la que el Core transfirió los datos (si corresponde), el tiempo transcurrido para que el trabajo se complete, el trabajo total en cantidad de gigabytes y cualquier tarea secundaria relacionada con el trabajo.
Mensaje	Disponible para las alertas y los elementos diario. Este campo de texto proporciona un mensaje descriptivo de la alerta o el elemento diario.

Visualización de informes de un equipo protegido

El menú desplegable **Informes** permite generar informes a petición para el equipo protegido seleccionado.

- El informe de trabajos proporciona un informe del estado de trabajos correctos y de trabajos con fallos del equipo seleccionado. Los trabajos con fallos pueden verse más adelante en un informe de error. Para obtener más información sobre este tipo de informe, consulte Descripción del informe de trabajo.
- El informe de errores proporciona información sobre los trabajos del Core cancelados y con fallos del equipo especificado. Para obtener más información sobre este tipo de informe, consulte Comprensión del informe de error.

Para obtener más información sobre cómo generar estos informes, consulte Generación de un informa del Core a petición.

Visualización de equipos replicados en el menú de navegación

Si el Core replica equipos desde otro Rapid Recovery Core, el nombre para mostrar del Core de origen aparece como un menú que puede contraerse en el área de navegación izquierda de Core Console. Al igual que con todas etiquetas de menú del área de navegación, este nombre de menú de los equipos replicados aparece con todas las letras mayúsculas, debajo del menú Equipos protegidos. De manera predeterminada, el menú de los equipos replicados se expande completamente y muestra en una lista todos los equipos que derivan del Core de origen y que se replican en el Core de destino.

Puede contraer o expandir la vista de cualquiera de los equipos replicados del Core de origen haciendo clic en la fecha del lado izquierdo de este menú.

Cada menú de equipos replicados incluye un menú desplegable en el lado derecho que incluye las funciones que se pueden realizar de forma simultánea en todos los equipos replicados derivados de dicho Core. Haga clic en la

flecha situada a la derecha del menú de equipos replicados para visualizar una lista desplegable de las funciones que puede realizar. Estas acciones incluyen lo siguiente:

- Realiza una pausa en la replicación. Si la replicación está activa en este momento, detiene la acción hasta que la reanuda.
- Reanuda la replicación. Si la replicación se ha puesto en pausa, comienza a replicar nuevamente.
- Forzar replicación. Replica a petición, en lugar de en una hora programada.
- Quitar replicación. Elimina la relación de replicación entre el Core de origen y el Core de destino. De forma opcional, puede eliminar los puntos de recuperación almacenados en este Core. Para obtener más información, consulte Eliminar la replicación saliente del Core de inicio o Eliminar la replicación entrante del Core de destino.

Si se hace clic directamente en el nombre del Core de origen en el menú de navegación, la página **Equipos replicados de [nombre del Core de origen]** aparece en el área de contenido principal. Para obtener más información sobre lo que puede realizar en dicha página, consulte Visualización de la replicación entrante y saliente.

Pausa y reanudación de la replicación
Forzado de la replicación
Eliminar la replicación saliente del Core de inicio
Eliminar la replicación entrante del Core de destino

Visualización en el menú Solo puntos de recuperación

El menú Solo puntos de recuperación aparece en el área de navegación izquierda si se cumple una de las siguientes condiciones:

- Si su Rapid Recovery Core conserva algunos puntos de recuperación de un equipo que estaba protegido previamente.
- si ha eliminado la replicación pero conserva los puntos de recuperación.

Al igual que con todas las etiquetas de menú en el área de navegación, la etiqueta de este menú aparece en todas las letras mayúsculas.

Puede contraer o ampliar la vista de los equipos con solo puntos de replicación haciendo clic en la fecha del lado izquierdo de este menú.

El menú incluye un menú desplegable en el lado derecho que muestra las funciones que se pueden realizar en todos los equipos solo con puntos de recuperación de forma simultánea. En este caso, la única función que puede realizar es eliminar puntos de recuperación desde el Core.

CAUTION: Esta acción elimina todos equipos con solo puntos de recuperación de su Core de Rapid Recovery**, eliminándolos permanentemente y evitando que pueda restaurar información de esos puntos de recuperación desde este Core.**

Visualización en el menú Grupos personalizados

El menú Grupos personalizados aparece en el área de navegación izquierda únicamente si ha definido uno o más grupos personalizados. Al igual que con todas las etiquetas de menú en el área de navegación, la etiqueta de este menú aparece en todas las letras mayúsculas.

Puede contraer o ampliar la vista de los elementos de este menú haciendo clic en la fecha del lado izquierdo de este menú.

El menú Grupos personalizados incluye un menú desplegable en el lado derecho que muestra las funciones que se pueden realizar de forma simultánea en todos los elementos parecidos de ese grupo.

Para obtener más información, consulte Comprensión de los grupos personalizados.

Uso del cuadro de diálogo Error

Cuando se produce un error en la interfaz de usuario de la Core Console de Rapid RecoveryRapid Recovery, como al intentar introducir un parámetro no válido, se abre un cuadro de diálogo Error. El cuadro de diálogo normalmente indica la causa del error, incluye algunos vínculos para proporcionar más información sobre el error, e incluye un botón Cerrar. Debe cerrar el cuadro de diálogo Error antes de continuar, pero es posible que desee ver más información sobre el error.

En el cuadro de diálogo Error, seleccione entre las siguientes opciones:

Los errores de la interfaz de usuario que hacen que aparezca el cuadro de diálogo Error no se siguen en la página Eventos de Rapid Recovery, ya que son simplemente errores de validación o de entrada de datos. Sin embargo, cuando hace clic en la opción Buscar base de conocimiento por cualquier error, el vínculo de URL que se proporciona para ese error se registra en el archivo Core AppRecovery.log. Puede buscar en el registro la cadena de texto “KB article url generated” para ver la URL de cada error que se vio en un navegador. Para obtener más información sobre la descarga o visualización de registros de error del Core, consulte los temas Descarga y visualización del archivo de registro del Core o Acceso a los registros del Core, respectivamente.

Configuración del Core

Esta sección describe cómo administrar y cambiar la configuración de su Rapid Recovery Core, y los botones y herramientas de las funciones clave disponibles en la Core Console.

El Rapid Recovery Core dispone de configuraciones ajustables que se configuran por defecto para ofrecer un rendimiento óptimo a la mayoría de los usuarios. Estas configuraciones afectan a la información de la pantalla en la Core Console o al rendimiento delRapid Recovery Core. Desde la barra de iconos, haga clic en (Configuración) para acceder a la configuración del Core.

Se muestra un conjunto de funciones clave como botones en la parte superior de la página, de forma horizontal. Para acceder a una de estas funciones, haga clic en el botón correspondiente. Para obtener más información acerca de estos botones, consulte Funciones clave de configuración del Core.

Bajo los botones de funciones clave se encuentran los ajustes configurables del Core. Para ver todas las opciones de configuración de cualquier ajuste, haga clic en un vínculo de acceso directo en la parte izquierda del panel Configuración o desplácese hacia abajo en la parte derecha de la página. Para obtener más información acerca de todo el conjunto de ajustes del Core, consulte Configuración del Rapid Recovery Core.

También puede acceder a las herramientas del Core, por ejemplo, la visualización de un resumen de la información del sistema o la descarga de los archivos de registro del Core. Para obtener más información, consulte Herramientas de nivel del Core.

Funciones clave de configuración del Core

Se muestra un conjunto de funciones clave como botones organizados horizontalmente en la parte superior de la página (Configuración). Para acceder a una de estas funciones, haga clic en el botón correspondiente.

En la siguiente tabla se describen los botones de funciones a los que se puede acceder en la página Configuración.

Tabla 6. Funciones clave de configuración del Core

Botón de función clave	Descripción
Configuración de copia de seguridad	Realiza una copia de seguridad de los ajustes de configuración del Core en un archivo XML con el nombre que escoja. Especifique una ruta de acceso completa local en el servidor Core.
Configuración de restauración	Si tiene un archivo XML de copia de seguridad de su configuración del Core, esta opción le permite especificar el nombre y la ruta local del archivo desde el que restaura la configuración de Core. Utilice esta función para restaurar la configuración del Core o migrar desde otro Core. De manera opcional, también puede restaurar los repositorios.
Reiniciar el servicio del Core	Esta opción apaga gradualmente el servicio del Core y después vuelve a iniciarlo.

Botón de función clave	Descripción
Apagar el servicio del Core	Esta opción apaga gradualmente el servicio del Core.

Para obtener más información acerca de cómo realizar una copia de seguridad y restauración de la configuración del Core, consulte Copia de seguridad y restauración de la configuración del Core.

Para obtener más información sobre el apagado y reinicio del servicio del Core, consulte Reinicio o apagado del servicio del Core.

Copia de seguridad y restauración de la configuración del Core

Puede realizar una copia de seguridad de la información de la configuración del Core en un archivo, para luego restaurar dicha configuración si tiene problemas con el equipo del Core o si desea migrar esta configuración a un equipo diferente. La información que se incluye en la copia de seguridad incluye los metadatos de repositorios (como el nombre del repositorio, la ruta de acceso de los datos y la ruta de acceso de los metadatos); los equipos protegidos en el Core; las relaciones de replicación (orígenes y destinos); qué equipos están configurados para la espera virtual, así como información sobre las claves de cifrado.

Este proceso restaura solo los parámetros de configuración, no los datos. La información de seguridad (como las credenciales de autenticación) no se almacenan en el archivo de configuración. No hay riesgo de seguridad al guardar un archivo de configuración del Core.

NOTE: Debe realizar primero una copia de seguridad de la información de la configuración del Core antes de poder utilizar este proceso para restaurar configuraciones del Core.

Utilice este procedimiento para realizar una copia de seguridad y restaurar la configuración del Core.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración).

   Aparecerá la página **Valores**. En la parte superior del panel Configuración, sobre las categorías de la configuración, verá las opciones **Configuración de copia de seguridad** o **Configuración de restauración**.
3. Si desea realizar una copia de seguridad de la configuración del Core, vaya al paso 4. Si desea restaurar la configuración del Core, vaya al paso 6.
4. Para realizar una copia de seguridad de la **configuración** actual en un archivo XML, haga clic en **Configuración de copia de seguridad** en la parte superior de la página Configuración.

   Aparece el cuadro de diálogo Configuración de copia de seguridad del Core.
5. En el cuadro de texto Ruta de acceso local, introduzca una ruta de acceso de un directorio accesible localmente del equipo del Core donde desea almacenar la configuración del Core como un archivo XML y, a continuación, haga clic en **Realizar copia de seguridad**.

   Por ejemplo, escriba `C:\Users\Your_User_Name\Documents\RRCoreSettings` y, a continuación, haga clic en **Realizar copia de seguridad**.

   Se guardará un archivo denominado AppRecoveryCoreConfigurationBackup.xml en el destino local que especifique.
6. Para restaurar la configuración del Core desde un archivo XML de copia de seguridad guardado anteriormente empleando este método, realice los pasos siguientes.

   NOTE: Cuando restaura los parámetros de configuración del Core, se reinicia el servicio del Core de Rapid Recovery.

a. En la parte superior de la página **Configuración**, haga clic en **Configuración de restauración**.

Aparece el cuadro de diálogo **Restaurar configuración de Core**.

b. En el cuadro de texto **Ruta de acceso local**, introduzca la ruta de acceso local de la ubicación donde almacenó los parámetros de configuración del Core.

Por ejemplo, escriba `C:\Users\Your_User_Name\Documents\RRCoreSettings`.

c. Si no desea restaurar la información de repositorios, vaya al paso g.

d. De forma opcional, si desea restaurar la información de repositorios según se haya configurado en el archivo de copia de seguridad, seleccione **Restaurar repositorios** y después haga clic en **Restaurar**.

Aparece el cuadro de diálogo **Restaurar repositorios**.

Si selecciona restaurar información de repositorios desde los datos de configuración en copia de seguridad, los repositorios configurados cuando se guardó la configuración del Core aparecerán para su verificación. Todos los repositorios existentes están seleccionados de forma predeterminada.

e. Verifique la información de los repositorios que desea restaurar. Si aparecen varios repositorios en las listas para su verificación y solo desea restaurar la información de algunos de ellos, anule la selección de cada repositorio que no desee.

f. Cuando esté satisfecho con la selección de repositorios que desea restaurar, haga clic en **Guardar**.

El cuadro de diálogo **Restaurar repositorios** se cierra.

g. En el cuadro de diálogo **Restaurar repositorios**, haga clic en **Restaurar**.

El cuadro de diálogo **Restaurar repositorios** se cierra y empieza el proceso de restauración. Aparecerá una alerta indicando que ha cambiado la configuración del servicio de repositorios.

h. Si no se puede restaurar cualquier parámetro de la configuración, verá un mensaje de error. Revise los detalles del error para ver si se requiere alguna acción por su parte. Para obtener más información, consulte Visualización de eventos mediante las páginas de tareas, alertas y del diario. Para continuar, haga clic en **Cerrar** para abandonar el cuadro de diálogo de error.

i. Después de restaurar la configuración, verifique lo siguiente:

- Desbloquee todas las claves de cifrado. Para obtener más información, consulte Desbloqueo de una clave de cifrado.
- Si el estado en espera virtual está configurado para actualizar continuamente una VM a un destino de red, debe especificar las credenciales de red en la configuración del estado en espera virtual antes de realizar una sincronización satisfactoria. Para obtener más información, consulte Exportación de la MV.
- Si el archivo programado está configurado para archivar en una cuenta de en la nube, debe especificar las credenciales para que el Core pueda conectarse a la cuenta en la nube. Para obtener más información sobre la vinculación del Core a una cuenta en la nube, consulte Incorporación de una cuenta de nube.
- Si se ha establecido la replicación y desea restaurar en un Core de destino, verifique la configuración del Core (especialmente del host) de destino en el Core de origen. Para obtener más información, si administra su propio Core, consulte Replicación en un Core de destino administrado automáticamente. Si está replicando a un Core administrado por un tercero, consulte Replicación en un Core de destino externo.
- Si la comprobación de capacidad de conectabilidad de SQL está configurada y si la instancia de SQL Server que realiza la comprobación está en el equipo del Core, especifique las credenciales de SQL en la configuración Conectabilidad. Para obtener más información, consulte Administración de la configuración de conectabilidad de SQL del Core.

Compruebe que la configuración del motor de reproducción se ha restaurado y actualice la configuración si no se garantizó una comunicación eficaz. Para obtener más información, consulte Configuración de los parámetros del motor de Replay.

Reinicio o apagado del servicio del Core

Sistemáticamente, un equipo en el que se ejecuta Rapid Recovery Core se apaga o debe reiniciarse. En versión 6.2,Rapid Recovery Core se ha mejorado para aumentar su capacidad para apagar y reiniciar los servicios del Core gradualmente.

La IU del Core ahora ofrece características de IU para reiniciar o apagar el servicio del Core con un solo clic. Esta característica es útil cuando es necesario el mantenimiento planificado del servidor del Core (incluido el reinicio). Los usuarios reciben notificaciones cuando los servicios correspondientes han terminado de apagarse. Se puede acceder a estas características desde la parte superior de la página Configuración del Core.

NOTE: Otra característica útil que respalda el cierre estable es la capacidad de suspender al Core de la programación de futuras tareas. Para obtener más información, consulte el tema Suspensión o reanudación de tareas programadas.

Utilice este procedimiento para reiniciar o apagar el servicio del Core.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración).

   Aparece la página **Configuración**. En la parte superior del panel Configuración, sobre las categorías de la configuración, verá las opciones **Reiniciar el servicio del Core** o **Apagar el servicio del Core**.
3. Si desea reiniciar el servicio del Core, en la parte superior del panel Configuración, haga clic en **Reiniciar el servicio del Core**.

   Aparece una lista de cada tarea que debe completarse antes del reinicio, incluida una visualización del progreso de la tarea.
4. De manera opcional, puede realizar uno de los siguientes métodos:
   a. Para forzar el reinicio, (un proceso menos ordenado en el que se detienen las tareas explícitamente antes de la finalización), haga clic en **Forzar reinicio**.
   b. Para cancelar el reinicio del Core, haga clic en **Cancelar**.
5. Si desea apagar el servicio del Core sin reiniciarlo de inmediato, en la parte superior del panel Configuración, haga clic en **Apagar el servicio del Core**.
6. De manera opcional, puede realizar uno de los siguientes métodos:
   a. Para forzar el apagado, (un proceso menos ordenado en el que se detienen las tareas explícitamente antes de la finalización), haga clic en **Forzar apagado**.
   b. Para cancelar el reinicio del Core, haga clic en **Cancelar**.

Tareas relacionadas

See also: Suspensión o reanudación de tareas programadas

Configuración del Rapid Recovery Core

El panel Configuración contiene una columna de navegación en el lado izquierdo, que enumera cada configuración del Core. Haga clic en cualquier enlace de esta lista o desplácese hacia abajo en el lado derecho de la página para ver todas las opciones de configuración de cada ajuste del Core.

Cuando haga clic en una opción que desee cambiar, ese valor se volverá editable. Realice uno de los siguientes pasos:

- Si el control es un menú desplegable, haga clic en la flecha hacia abajo para ver una lista de opciones y seleccione la opción deseada en el menú.
- Si el control es un campo de texto, introduzca un valor.
- Si la opción muestra Sí o No, haga clic en el valor, que se convertirá en una casilla de verificación. Para Sí, marque la casilla. Para No, desmarque la casilla.
- Si la opción muestra un valor de tiempo (por ejemplo, horas, minutos y segundos), puede hacer clic en cada componente y escribir un valor nuevo o utilizar las flechas hacia arriba y hacia abajo para seleccionar nuevos valores.

Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para confirmar, guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

La configuración de Rapid Recovery Core que puede configurar se describe en la siguiente tabla. Cada configuración tiene un enlace a un tema relevante con más información.

Tabla 7. Opciones configurables del Rapid Recovery Core

Parámetro de Configuración	Descripción
General	La configuración general incluye las opciones de configuración que se aplican generalmente a Rapid Recovery Core, incluyendo opciones de visualización y puertos para el servidor web y para el servicio Rapid Recovery. Para obtener más información acerca de la configuración general de Rapid Recovery Core, incluyendo cómo configurar esta configuración, consulte Configuración de los parámetros generales del Core.
Actualizaciones	La configuración de actualización controla el aspecto de la función Actualización automática, que comprueba si existen versiones actualizadas del software de Rapid Recovery. Para obtener más información acerca de la configuración para actualizar Rapid Recovery Core, incluyendo cómo configurar estos parámetros, consulte Configuración de los parámetros de actualización.
Trabajos nocturnos	La configuración Trabajos nocturnos son tareas automatizadas que realiza el Core diariamente. Puede configurar la hora en la que comienzan los trabajos y qué trabajos se realizan. Quest recomienda programar los trabajos fuera de las horas laborales normales para reducir la carga en el sistema cuando la demanda de recursos es alta. Para obtener más información, consulte Comprensión de los trabajos nocturnos, Configuración de trabajos nocturnos para el Core y Personalización de trabajos nocturnos para un equipo protegido.
Cola de transferencia	La configuración de Cola de transferencia controla el número de veces que se intentan las operaciones de transferencia si los trabajos fallan debido a la no disponibilidad de los recursos. Puede establecer el número máximo de transferencias simultáneas y el número máximo de reintentos para transferir datos. Para obtener más información acerca de la configuración de la cola de transferencia, consulte Modificación de la configuración de la cola de transferencias.
Tiempo de espera del cliente	La configuración de tiempo de espera del cliente determina la cantidad de tiempo que ha de transcurrir antes que se intenten esas solicitudes de conexión específicas u operaciones de lectura y escritura antes de que se agote el tiempo de espera.

Parámetro de Configuración	Descripción
	Para obtener más información acerca de la configuración del tiempo de espera del cliente, consulte Ajuste de la configuración del tiempo de espera de clientes.
Caché de desduplicación de DVM	La desduplicación garantiza que bloques únicos de información se almacenen solo una vez en su repositorio, creando referencias a bloques de datos repetidos. Las referencias se almacenan en una caché de desduplicación. Si se utilizan claves de cifrado, la desduplicación se produce dentro de cada dominio de cifrado. La configuración de la caché de desduplicación de DVM le permite configurar el tamaño y especificar las ubicaciones para la caché principal y secundaria, así como la ubicación de la caché de metadatos. Para obtener más información sobre la caché de desduplicación, consulte Funcionamiento de la caché de desduplicación y las ubicaciones de almacenamiento. Para obtener más información sobre el ajuste de la configuración, consulte Configuración de los valores de caché de la desduplicación de DVM.
Replay Engine	La configuración de Replay Engine controla la información relacionada con el canal de comunicación de Replay Engine, como las direcciones IP y los valores de tiempo, para ayudar a ajustar el rendimiento específico a sus necesidades de red. Para obtener más información sobre de la configuración del motor para Rapid Recovery, consulte Configuración de los parámetros del motor de Replay.
Implementar	Los parámetros de implementación le permiten establecer las opciones para implementar el software Rapid Recovery Agent desde su Core en los equipos que desea proteger. Para obtener más información acerca de la configuración de los parámetros de implementación, consulte Configuración de los parámetros de implementación.
Conexión de base de datos	Rapid Recovery almacena la información de transacciones en una base de datos de servicio MongoDB que se instala localmente de forma predeterminada en el equipo del Core. Puede configurar estos parámetros para cambiar la cantidad de tiempo que se retiene la información en la base de datos, o para cambiar el tamaño del grupo de conexión para permitir más o menos conexiones simultáneas. Para obtener más información acerca del establecimiento o modificación de parámetros de conexión de bases de datos para la base de datos de servicio, consulte Configuración de los parámetros de conexión con la base de datos.
Parámetros de base de datos local	Rapid Recovery muestra información sobre las tareas, eventos y alertas del Core en la página Eventos. Rapid Recovery almacena esta información de transacciones en una base de datos de servicio MongoDB que se instala localmente en el mismo equipo que el Rapid Recovery Core. Puede configurar la información de credenciales (nombre de usuario y contraseña) para la base de datos de servicio MongoDB utilizando los parámetros de la base de datos local. Para obtener más información sobre el ajuste de la configuración de la base de datos local, consulte Modificación de la configuración de la conexión con la base de datos local.
Servidor SMTP	Configure los ajustes del servidor de protocolo sencillo de transferencia de correo (SMTP) para el Core, también podrá enviar la información de eventos del Core por correo electrónico. Para obtener más información acerca de la configuración de un servidor de correo electrónico SMTP, consulte Configuración de un servidor de correo electrónico.

Parámetro de Configuración	Descripción
	NOTE: Para enviar información de eventos por correo electrónico, también deberá configurar los parámetros del grupo de notificación. Para obtener más información sobre la especificación de eventos para recibir alertas de correo electrónico, consulte Configuración de grupos de notificación.
Cuentas en la nube	La configuración Cuentas en la nube le permite especificar los valores de la configuración de las cuentas de almacenamiento en la nube compatibles. Estos parámetros no crean cuentas de nube. En su lugar, asocia el almacenamiento en la nube externo existente o las cuentas del proveedor de servicios de la nube con el Rapid Recovery Core para facilitar acciones como el archivado de la información de Rapid Recovery. Para obtener información sobre el establecimiento de la configuración del tiempo de expiración de las cuentas en la nube, consulte Configuración de ajustes de conexión de cuentas de la nube. Para obtener más información sobre la administración de las cuentas en la nube en la Rapid Recovery Core Console, consulte Cuentas en la nube.
Certificados de administración de Azure	Para obtener información sobre las suscripciones de Azure, para poder acceder a la Core Console, debe cargar el certificado de administración de Azure para asociarlo con el Core. Desde la Core Console puede cargar nuevos certificados, actualizar la vista de los certificados actualmente asociados con el Core o eliminar el certificado de Azure que está asociado con el Core. Para obtener más información sobre el uso de los certificados de administración de Azure, consulte Trabajar con certificados de administración de Azure asociados con el Core.
Informes	La configuración de informes incluye parámetros de configuración que le permiten seleccionar el tipo de fuente que se utiliza cuando se genera un informe a partir del Rapid Recovery Core. También puede establecer el tamaño del papel y la orientación de la página de los informes. Para obtener más información acerca de cómo cambiar la configuración de los informes, consulte Administración de la configuración de informes.
conectividad	Los valores de conectabilidad le permiten especificar si llevar a cabo las comprobaciones de capacidad de conectabilidad de SQL en el equipo protegido, o si utilizar la instancia de SQL Server en el Core. Si se especifica SQL en el Core, deberá proporcionar la información de las credenciales. Para obtener más información acerca de cómo administrar la configuración de conectabilidad de SQL para el Core, consulte Administración de la configuración de conectabilidad de SQL del Core.
Trabajos	Los trabajos del Core se crean automáticamente cada vez que inicia operaciones como la replicación. Puede especificar la configuración de cada trabajo mediante la configuración del Core de los trabajos. Puede configurar el número de trabajos que hay que ejecutar a la vez. En caso de que se produzcan errores de red o de comunicación que eviten que se complete un trabajo la primera vez, puede establecer el número de veces que se debe intentar realizar un trabajo a través de la configuración Recuento de intentos. Para obtener información acerca de los trabajos del Core, qué trabajos están disponibles y cómo configurarlos, consulte Configuración de trabajo de Core.

Parámetro de Configuración	Descripción
Licencias	Desde la Core Console, Rapid Recovery le permite cambiar la licencia asociada con su Core, limitar el número de instantáneas diarias, ver la información del grupo de licencias y ponerse en contacto con el servidor de licencias. Para obtener más información acerca de cómo administrar licencias desde el Core, consulte Administración de licencias. Para obtener más información sobre la administración de licencias, consulte la *Rapid Recovery License Portal User Guide (Guía del usuario del Portal de licencias de Rapid Recovery)*. **NOTE:** El Portal de licencias de Rapid Recovery tiene un ciclo de versión diferente al del software Rapid Recovery. Para obtener la documentación del producto más reciente, consulte el sitio web de documentación técnica de Quest.
Configuración de SNMP	Simple Network Management Protocol (SNMP) es un protocolo para administrar dispositivos en un red IP. Puede configurar el Rapid Recovery Core como un agente SNMP. El Core puede informar sobre alertas, estado de repositorios y equipos protegidos. Para obtener más información sobre el uso de SNMP con Rapid Recovery, consulte Comprensión de la configuración de SNMP.
vSphere	La configuración del Core de VSphere se aplica solo a los usuarios de la protección sin agentes de las máquinas virtuales. Si se utiliza un host vSphere, estos valores incluyen las opciones de conexión que se aplican a las máquinas virtuales. Para obtener más información sobre la configuración de vSphere para la protección sin agentes de VMware o ESXi, consulte Configuración de los valores de vSphere.
Proxy de VMware	Un servicio de proxy de VMware instalado con el Core le permite a los usuarios establecer tiempos de expiración del servicio asociados con el almacenamiento del disco de VMware. Para obtener más información acerca de esta configuración, consulte Administración de la configuración del proxy VMware.
Portal de protección de datos	Si administra de dos o más Cores, puede integrar el servidor del Core con el Portal de protección de datos de Quest. Esta función, que resulta especialmente útil para los proveedores de servicios administrados, permite administrar varios Cores; acceder a un panel de supervisión de tareas y eventos, ver el estado del repositorio y comprobar la Condición del sistema; generar informes; y realizar una lista creciente de funciones desde una única interfaz de usuario basada en web. Para habilitar o deshabilitar el acceso al portal, utilice esta configuración.
vFoglight	Quest Foglight for Virtualization (vFoglight) ayuda a los administradores a supervisar, analizar y optimizar hipervisores en los entornos de VMware, Hyper-V y OpenStack. Para los clientes que administran máquinas virtuales con vFogLight y las protegen en la consola de Rapid Recovery, esta configuración del Core les permite integrar la navegación de los dos productos. Después de introducir correctamente la configuración de vFoglight, haciendo clic en la URL de vFoglight en la página **Resumen** de la máquina virtual en la Core Console, los usuarios navegan a la página correspondiente para esa máquina virtual en vFoglight. Para obtener más información sobre la configuración del Core de vFoglight, consulte Configuración de valores de vFoglight. Para obtener más información sobre vFoglight, consulte la página de producto vFoglight en el sitio web de Quest.

También puede acceder a las herramientas del Core, por ejemplo, la visualización de un resumen de la información del sistema o la descarga de los archivos de registro del Core. Para obtener más información, consulte Herramientas de nivel del Core.

Configuración de los parámetros generales del Core

La configuración general del Rapid Recovery Core incluye el ID del Core, el nombre para mostrar del Core, el puerto del servidor web, el puerto de servicio, la configuración regional (el idioma de visualización de la Core Console) y el tema del color de visualización.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core, en el lado izquierdo de la página Configuración, haga clic en **General**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta poder ver el encabezado General.
3. Haga clic en la configuración general que desea cambiar.

   La configuración seleccionada se convierte en editable, como un campo de texto o un menú desplegable.
4. Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 8. Información de configuración general

Cuadro de texto	Descripción
ID de Core	Cada núcleo tiene un ID de Core único. Este ID se utiliza, por ejemplo, para integrar su Core con el Portal de protección de datos para proporcionar informes o administración de dos o más Cores. El ID del Core aparece ahora en Configuración general. **NOTE:** Este campo no es configurable.
Nombre para mostrar	Introduzca un nombre para mostrar nuevo para el Core. Este es el nombre que se mostrará en la Rapid Recovery Core Console y (si está activado) en el Portal de protección de datos. Puede introducir hasta 64 caracteres.
Puerto del servidor Web	Introduzca un número de puerto para el servidor Web. El puerto predeterminado es 8006. **NOTE:** Quest recomienda que se utilice el puerto predeterminado.
Puerto de servicio	Introduzca un número de puerto para el servicio Rapid Recovery Core. El puerto predeterminado es 8006. **NOTE:** Quest recomienda que se utilice el puerto predeterminado.
Configuración regional	En la lista desplegable **Configuración regional**, seleccione el idioma que desea mostrar.

Cuadro de texto	Descripción
	Puede elegir entre inglés, francés, alemán, japonés, coreano, portugués, chino simplificado y español. **NOTE:** Si cambia el idioma, confirme el mensaje que indica que el servicio Rapid Recovery Core debe reiniciarse antes de que el idioma actualizado se pueda mostrar en la Core Console. Puede reiniciar este servicio utilizando el botón **Reiniciar el servicio del Core** en la parte superior de la página Configuración del Core.
Tema	En la lista desplegable **Tema**, seleccione el estilo que desee aplicar a la Core Console. Hay disponibles tres temas: • **Oscuro**. Este tema presenta el fondo gris oscuro sólido en toda la interfaz (menú de navegación izquierdo, barra de botones superior y panel principal). Los elementos y los botones de texto sin enfocar aparecen en blanquecino o en blanco cuando están enfocados. Los vínculos seleccionables aparecen en azul medio. Los botones ocasionales presentan el texto blanco sobre un fondo azul medio. • **Híbrido**. Este tema presenta el fondo gris oscuro familiar para el menú de navegación izquierdo y la barra de botones de la parte superior de la Core Console. Los elementos de texto en estas áreas son blancos. El panel principal tiene un fondo blanco con información destacada blanquecina y elementos de texto y botones de texto en negro. Los vínculos seleccionables aparecen en azul oscuro. Los botones ocasionales presentan el texto blanco sobre un fondo azul. • **Claro**. Este tema presenta un fondo blanco puro en toda la interfaz (menú de navegación izquierdo, barra de botones superior y panel principal). El logotipo de Quest y algunos elementos de diseño son naranjas. Los elementos de texto son de color gris oscuro, con títulos en negro. Los vínculos seleccionables aparecen en azul medio al pasar el ratón por encima. Los botones ocasionales presentan el texto blanco sobre un fondo azul medio.
Acepto el uso de datos personales	Para cambiar la configuración que permite a la aplicación utilizar información personal, en la lista desplegable **Acepto el uso de datos personales**, seleccione **Sí** o **No** según corresponda. En el cuadro de diálogo, seleccione y registre el archivo de licencia correspondiente. Al actualizar o instalar Rapid Recovery Core, tiene la opción de establecer el uso compartido de información personal. Si acepta compartir información con Quest, puede utilizar funciones como la actualización automática y el Portal de protección de datos (que en ese caso se activa de manera predeterminada). Si rechaza compartir información con Quest durante la instalación, se le pedirá que registre una licencia sin llamada a la central. Debe tener acceso a la licencia sin llamada a la central para guardar y confirmar el cambio. Independientemente de la opción que haya seleccionado durante la instalación, puede cambiar la configuración **Acepto el uso de datos personales** en la configuración general del Core. Asegúrese de que dispone de acceso a la licencia sin llamada a la central, ya que esta acción le solicitará que la cargue. En versión 6.2, cuando cambia esta configuración de "Sí" a "No", se aplica lo siguiente: a. Se le solicitará que cargue el archivo de licencia sin llamada a la central.

Cuadro de texto	Descripción

b. Después de confirmar la licencia sin llamada a la central, la configuración de actualizaciones del Core se ajusta automáticamente para nunca buscar ni instalar actualizaciones del Core.

c. El ajuste del portal de protección de datos "Habilitar la conexión con el portal de protección de datos" está establecido en "No".

Sin embargo, no ocurre así al revés. Al cambiar esta configuración de "No" a "Sí", otorga permiso al Core para compartir su información, pero no se comparte la información hasta que cambie de forma explícita la licencia al modo con llamada a la central y actualice la configuración pertinente del Core. Por ejemplo:

a. La clave sin llamada a la central sigue registrada hasta que cargue explícitamente una clave estándar con llamada a la central (que puede obtener del portal de licencias).

b. Para utilizar la actualización automática, cambie "Comprobar nuevas actualizaciones" de "Nunca" a "Cada día", "Cada semana" o "Cada mes". De manera opcional, cambie "Instalar actualizaciones" para recibir o no notificaciones para instalar actualizaciones automáticas.

c. Para compartir información con el Portal de protección de datos, establezca "Habilitar la conexión con el portal de protección de datos" en "Sí".

NOTE: Si realiza esta configuración por primera vez, se le solicitará cargar una licencia con llamada a la central.

Para comprender el efecto de compartir su información personal, consulte Administración de la privacidad, incluido el tema Cómo utiliza Rapid Recovery la información personal.

Para obtener más información sobre las funciones de las que no dispone al utilizar el modo sin llamada a la central, consulte el tema Restricciones de la licencia sin llamada a la central.

Para solicitar una licencia del **modo con llamada a la central**, consulte Obtención y uso de licencias sin llamada a la central.

5. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

Configuración de los parámetros de actualización

Rapid Recovery incluye la función Actualización automática. Al instalar el Rapid Recovery Core, puede elegir si desea actualizar automáticamente el software del Rapid Recovery Core cuando haya nuevas actualizaciones disponibles y la frecuencia con la que el sistema debe buscarlas.

NOTE: La función de actualización automática requiere una licencia del modo estándar con llamada a la central. Si utiliza una licencia de software en modo sin llamada a la central, el Core no tiene permiso para comunicarse con el Portal de licencias de Rapid Recovery y no puede actualizar el Core ni notificar las actualizaciones disponibles. Para obtener más información, consulte Administración de la privacidad.

Los números de versión de Rapid Recovery, normalmente, incluyen cuatro fragmentos de información, separados por puntos decimales: el número de la versión primaria, el número de la versión secundaria, el número de revisión y el número de compilación. Por ejemplo, el primer nombre de la versión de Rapid Recovery era 6.0.1.609. La versión siguiente era 6.0.2.142.

La función de actualización automática compara todos los dígitos de un número de versión. Si activa la actualización automática, el software del Core solo se actualiza sin intervención cuando los números de la versión primaria y secundaria son idénticos. Por ejemplo, la actualización automática se iniciaría de la versión del Core 6.0.1.609 a la 6.0.2.142 (ambas empiezan por 6.0). En el mismo equipo, el Core no se actualizaría automáticamente de 6.0.2.142 a 6.1.1.XXX, porque los dígitos siguientes al primer decimal no son iguales. En su lugar, aparecerá una notificación (en un banner en la parte superior de la Core Console) de que hay una actualización del software del Core disponible. Esta notificación le da la oportunidad de consultar las notas de la versión y determinar si actualizar el software a la última versión del Core es adecuado para sus necesidades.

NOTE: Para obtener información sobre la instalación del software Rapid Recovery Core, consulte la *Guía de instalación y actualización de Rapid Recovery*.

Puede ver y cambiar los ajustes que utiliza el sistema para buscar actualizaciones en cualquier momento.

CAUTION: Cuando utilice la replicación, la configuración de su sistema para instalar las actualizaciones automáticamente puede dar como resultado la actualización de su Core de origen antes que el Core de destino, lo que puede provocar fallos de replicación o la imposibilidad de configurar nuevas replicaciones entre Cores. Para los usuarios de la replicación, Quest **recomienda que los administradores apliquen actualizaciones automáticas únicamente en el Core de destino, y luego actualizar manualmente el Core de origen, actualizando por último los equipos protegidos.**

Complete los pasos de este procedimiento para configurar los ajustes de actualización.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página **Configuración**, haga clic en **Actualizaciones**.
   - Desplácese hacia abajo en el lado derecho de la página **Configuración** hasta que pueda ver el encabezado Actualizaciones.
3. Haga clic en la opción que desee cambiar.

   La opción seleccionada se volverá editable.
4. Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 9. Información de configuración de actualizaciones

Cuadro de texto	Descripción
Comprobar nuevas actualizaciones	Seleccione la frecuencia con la que Rapid Recovery debe buscar e instalar actualizaciones. Puede seleccionar las opciones siguientes: • Nunca • Diariamente • Semanalmente • Mensualmente Si elige las actualizaciones automáticas, una vez que se supere el umbral temporal, si hay una actualización disponible, la función se instalará cuando se hayan completado los trabajos nocturnos.

Cuadro de texto	Descripción
Instalar actualizaciones	Especifique cómo se administran las actualizaciones disponibles eligiendo una de las siguientes opciones: • No comprobar actualizaciones nunca • Notificarme acerca de las actualizaciones, pero no instalarlas automáticamente • Instalar automáticamente actualizaciones
Estado	El estado indica si hay nuevas actualizaciones disponibles.
Última comprobación	El campo Última comprobación indica la fecha y la hora a la que se comprobó por última vez si había actualizaciones. Haga clic en **Comprobar ahora** para verificar inmediatamente si hay disponible una actualización de software. Esta comprobación se produce independientemente de la frecuencia que haya establecido.

5. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

Comprensión de los trabajos nocturnos

Los trabajos nocturnos son tareas automatizadas diarias que se realizan a una hora predeterminada fuera del horario laboral normal. Estos trabajos utilizan mucha memoria, e incluyen varias comprobaciones de integridad y tareas de consolidación de datos que se realizan mejor cuando el Rapid Recovery Core está menos activo.

Todos los trabajos nocturnos y el ámbito en el que se pueden aplicar están descritos en la siguiente tabla. Los trabajos nocturnos se pueden administrar en el nivel del Core (que se aplica a todos los equipos protegidos en el Core). Aquellos trabajos nocturnos que se pueden aplicar también a un equipo protegido específico registran el ámbito como "Equipo protegido".

Tabla 10. Información de los trabajos nocturnos

Nombre de trabajo	Ámbito	Descripción
Cambiar	N/A	Este control abre el cuadro de diálogo **Trabajos nocturnos**, donde se puede activar, desactivar o cambiar la configuración de cada trabajo nocturno.
Hora de trabajos nocturnos	Todos	Este valor representa la hora a la que se programan la ejecución de los trabajos nocturnos. Quest recomienda configurar el Core para ejecutar trabajos nocturnos durante una hora de escasa actividad. La hora predeterminada es las 12:00 horas.
Comprobar la conectabilidad de bases de datos SQL	Equipo protegido	Comprueba la integridad de los puntos de recuperación que contienen bases de datos SQL. Para obtener más información, consulte Administración de la configuración de conectabilidad de SQL del Core.
Comprobar suma de comprobación	Equipo protegido	Comprueba la integridad de los puntos de recuperación que contienen archivos de bases de datos de Exchange (EDB).

Nombre de trabajo	Ámbito	Descripción
de bases de datos de Exchange		**NOTE:** Esta opción no aparece si no está protegiendo un Exchange Server en su Core.
Comprobar integridad de bases de datos de Oracle	Core o equipo protegido	Comprueba la integridad de las bases de datos de Oracle que utilizan la utilidad DBVERIFY. Proceso: • Montar el punto de recuperación más reciente para cada grupo de protección. • Enumerar los archivos y carpetas de cada volumen. • Examina los puntos de recuperación para garantizar que los archivos de datos son válidos y que los bloques de datos no están dañados. • Desmontar el punto de recuperación.
Comprobar integridad de puntos de recuperación	Core o equipo protegido	Comprueba la integridad de los puntos de recuperación de cada equipo protegido. De forma predeterminada, la opción `Check integrity of recovery points` no está activada. Proceso: • Montar el punto de recuperación más reciente para cada grupo de protección. • Enumerar los archivos y carpetas de cada volumen. • Examinar los puntos de recuperación para garantizar que son válidos. • Desmontar el punto de recuperación.
Limpiar claves de registro huérfanas de los Agents de Hyper-V		Para los hosts Hyper-V que utilizan la protección sin agentes de Rapid Recovery versión 6.1.x, el trabajo nocturno limpia las claves huérfanas creadas en el registro de Windows para cada operación de conexión y desconexión. Las entradas de registro son inofensivas, pero con el tiempo pueden acumularse danto lugar a un rendimiento más lento. **NOTE:** A partir de Rapid Recovery versión 6.2, un enfoque mejorado para obtener metadatos de almacenamiento para la protección sin agentes de Hyper-V impide la creación de entradas de registro.
Consolidar instantáneas de VMware para máquinas virtuales protegidas	Core o equipo protegido	Este trabajo nocturno es relevante si utilizan API nativas de VMware para proteger equipos sin el software Rapid Recovery Agent. Debe consolidar periódicamente las instantáneas de VMware. La activación de este trabajo nocturno le permitirá llevar a cabo estas consolidaciones todos los días. Este trabajo nocturno contiene el parámetro, Consolidaciones máximas simultáneas, que se debe configurar en un número entre 1 y 100.
Eliminación aplazada	Core	Esta configuración le permite aplazar la eliminación de los puntos de recuperación del repositorio hasta la hora especificada en el Core para realizar trabajos nocturnos. Cuando está activada, después de que se ejecuten otros trabajos nocturnos, el procesamiento del Core se dedica a ejecutar el trabajo "Eliminar los registros previamente marcados para borrarse". Este trabajo elimina los puntos de recuperación marcados del repositorio hasta que se han eliminado todos, o hasta que han pasado

Nombre de trabajo	Ámbito	Descripción
		cuatro horas desde la hora de ejecución de los trabajos nocturnos. Los trabajos nocturnos terminan y se reanudan otros trabajos en cola. Las eliminaciones restantes se realizan en segundo plano, al mismo tiempo que otras tareas, hasta que se ejecutan los trabajos nocturnos del día siguiente. De forma predeterminada, la opción `Deferred Delete` no está activada. Quest recomienda desactivar este trabajo nocturno a menos que se produzcan problemas de rendimiento de transferencias relacionados con las eliminaciones de puntos de recuperación con copia de seguridad. Si activa esta opción, Quest recomienda revisar los trabajos del Core para asegurarse de que la mayoría de puntos de recuperación marcados para eliminarse se eliminen del repositorio antes de una semana. Esta estrategia ayuda a equilibrar el rendimiento máximo de las transferencias con una reclamación máxima de espacio del repositorio.
Eliminar sucesos y trabajos antiguos	Core	Mantiene la escala de la base de datos de eventos eliminando eventos antiguos. El número de días es configurable, con un valor predeterminado de 30 días.
Truncamiento del registro para Exchange	Equipo protegido	Mantiene el tamaño de los registros de Exchange truncando el registro de transacciones de base de datos de Exchange para que coincida con el punto de recuperación más reciente. **NOTE:** Esta opción no aparece si no está protegiendo un Exchange Server en su Core.
Truncamiento de registro de Oracle	Equipo protegido	Controla el truncamiento de los registros de Oracle. A menos que se haya desactivado, el truncamiento se produce una vez al día, cuando se ejecutan los trabajos nocturnos. • Puede seguir la directiva de eliminación **Automática** (activada de forma predeterminada), que trunca todos los registros de Oracle almacenados localmente cuando se ejecutan los trabajos nocturnos. Los registros para el día actual aún persisten en las instantáneas de copia de seguridad que preceden a la ejecución del trabajo nocturno. • Puede seleccionar una directiva de eliminación personalizada para un servidor protegido de Oracle específico. La directiva **Mantener más reciente** le permite especificar el tiempo antes de que se trunquen los registros de Oracle, y la directiva **Mantener número especificado** le permite mantener un número especificado de archivos de registro antes de truncar los más antiguos. • Puede desactivar el trabajo nocturno, lo que dará como resultado una acumulación considerable de archivos de registro. En estos casos, los usuarios también pueden truncar los archivos de registro manualmente, como se describe en el tema Truncamiento manual de registros de la base de datos de Oracle.
Truncamiento del registro para SQL	Equipo protegido	Mantiene el tamaño de los registros de SQL Server truncando el registro de transacciones de base de datos para que coincida con el punto de recuperación más reciente. **NOTE:** Esta opción no aparece si no está protegiendo un SQL Server en su Core.

Nombre de trabajo	Ámbito	Descripción
Consolidación	Core o equipo protegido	Aplica la política de retención a los datos a los que se ha realizado una copia de seguridad mediante la combinación o "consolidación" de los puntos de recuperación en el calendario dictados en la política. Puede personalizar la política en el Core, la cual se aplicará de forma predeterminada a todos los equipos protegidos. De manera predeterminada, el trabajo de compilación se ejecuta en todo el Core; también puede hacer clic en [Expandir] para expandir la vista de los equipos protegidos. A continuación, puede definir el conjunto de equipos protegidos que desea acumular utilizando la directiva del Core. Para obtener más información acerca de cómo utilizar una política de retención en un equipo protegido que difiera de la política predeterminada establecida en el Core, consulte Personalización de la configuración de la política de retención de un equipo protegido.

Configuración de trabajos nocturnos para el Core

Cuando se activa una opción de trabajo nocturno en el Rapid Recovery Core, el trabajo seleccionado se ejecuta una vez al día a la hora especificada en todos los equipos que están protegidos por el Core. A la inversa, si desactiva cualquier trabajo nocturno a nivel del Core, el trabajo especificado ya no se ejecuta para todos los equipos que están protegidos por el Core.

NOTE: Si el ámbito de un trabajo nocturno, tal como se describe en el tema Comprensión de los trabajos nocturnos, incluye equipos protegidos, puede configurar ese trabajo nocturno únicamente para uno o más equipos protegidos específicos de forma individual. Para obtener más información sobre la aplicación de parámetros de trabajos nocturnos específicos para equipos protegidos, consulte Personalización de trabajos nocturnos para un equipo protegido.

Debido a que los trabajos nocturnos utilizan gran cantidad de memoria, Quest recomienda configurar el Core para ejecutarlos durante un periodo de baja actividad. La programación predeterminada para la ejecución de trabajos nocturnos es las 12:00 am. Si alguna otra hora es más adecuada, cambie este parámetro en el campo Hora de trabajos nocturnos utilizando este procedimiento.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página **Configuración** haga clic en **Trabajos nocturnos**.
   - Desplácese hacia abajo en el lado derecho de la página **Configuración** hasta que pueda ver el encabezado Trabajos nocturnos.
3. Para cambiar cualquier trabajo nocturno o para cambiar la hora a la que empiezan a ejecutarse los trabajos nocturnos, haga clic en **Cambiar**.

   Se abrirá el cuadro de diálogo **Trabajos nocturnos**.
4. Si desea cambiar la hora de ejecución de los trabajos nocturnos, introduzca una nueva hora en el cuadro de texto **Horas de trabajos nocturnos**.
5. En la primera columna, haga clic para seleccionar cada opción de los trabajos nocturnos que desee configurar para el Core. Haga clic en cualquier opción seleccionada para borrarla.
6. Haga clic en **Aceptar**.

   El cuadro de diálogo **Trabajos nocturnos** se cerrará y su configuración de trabajos nocturnos para el Core se guardará.

Modificación de la configuración de la cola de transferencias

La configuración de la cola de transferencias son ajustes a nivel de Core que establecen el número máximo de transferencias simultáneas y el número máximo de reintentos para transferir datos.

Complete los pasos de este procedimiento para modificar la configuración de la cola de transferencias.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Cola de transferencia**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Cola de transferencia.
3. Haga clic en la opción que desee cambiar.

   La opción seleccionada se volverá editable.
4. Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 11. Información de configuración de la cola de transferencias

Cuadro de texto	Descripción
Número máximo de transferencias simultáneas	Introduzca un valor para actualizar el número de transferencias simultáneas. Establezca un número del 1 al 60. Cuanto más pequeño sea el número, más pequeña será la carga en la red y en otros recursos del sistema. Conforme el número de Agents procesados aumenta, también lo hace la carga en el sistema.
Número máximo de reintentos	Introduzca un valor para establecer el número máximo de intentos antes de que la operación de transferencia se cancele. Establezca un número del 1 al 60.

5. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en para guardar los cambios y salir del modo edición, o haga clic en para salir del modo sin guardar.

Ajuste de la configuración del tiempo de espera de clientes

La configuración del tiempo de espera de clientes controla la cantidad de tiempo en las que se intentan varias operaciones antes de que se agote el tiempo de espera.

NOTE: Quest recomienda no alterar la configuración predeterminada del tiempo de espera a no ser que se produzcan problemas específicos en su entorno, y que el servicio de asistencia técnica de Quest aconseje modificar dicha configuración.

Complete los pasos de este procedimiento para ajustar la configuración del tiempo de espera del cliente.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Tiempo de espera del cliente**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Tiempo de espera del cliente.
3. Haga clic en la opción que desee cambiar.

   La opción seleccionada se volverá editable.
4. Introduzca la información de configuración según se describe en la tabla siguiente.
5.

Tabla 12. Información de configuración del tiempo de espera del cliente

Configuración	Descripción
Tiempo de espera de la conexión	Controla el tiempo de espera de una conexión entre el Core y los equipos protegidos cuando se envían datos mediante el protocolo de transferencia de hipertexto (http). Introduzca la cantidad de tiempo que desea que transcurra antes de que se agote el tiempo de espera de conexión. Utiliza el formato HH:MM:SS. **NOTE:** El valor predeterminado es 0:05:00 o cinco minutos.
Tiempo de espera de lectura y escritura	Controla el tiempo de espera de una conexión entre el Core y los equipos protegidos cuando se leen o se escriben secuencias de datos mediante http. Un ejemplo es recibir bloques de datos cambiados de un equipo protegido al Core en una instantánea incremental. Introduzca la cantidad de tiempo que desea que transcurra antes de que se agote el tiempo de espera máximo durante un evento de lectura o escritura. Utiliza el formato HH:MM:SS. **NOTE:** El valor predeterminado es 0:05:00 o cinco minutos.
Tiempo de espera de conexión de la interfaz de usuario	Controla el tiempo de espera de una conexión entre la interfaz gráfica de usuario y el servicio del Core de Rapid Recovery mediante http. Introduzca la cantidad de tiempo que desea que transcurra antes de que se agote el tiempo de espera de IU de conexión. Utiliza el formato HH:MM:SS. **NOTE:** El valor predeterminado es 0:05:00 o cinco minutos.
Tiempo de espera de lectura/escritura de la interfaz de usuario	Controla el tiempo de espera de una conexión para leer y escribir secuencias de datos entre la interfaz gráfica de usuario y el servicio del Core de Rapid Recovery mediante http. Introduzca la cantidad de tiempo que desea que transcurra antes de que se agote el tiempo de espera máximo durante los eventos de lectura o escritura. Utiliza el formato HH:MM:SS.

Configuración	Descripción

NOTE: El valor predeterminado es 0:05:00 o cinco minutos.

6. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

Funcionamiento de la caché de desduplicación y las ubicaciones de almacenamiento

La desduplicación global reduce la cantidad de espacio de almacenamiento en disco necesario para los datos de los cuales el Core realiza copias de seguridad. Cada repositorio se desduplica, almacenando cada bloque exclusivo una vez de forma física en disco, y empleando las referencias virtuales o punteros a esos bloques en copias de seguridad posteriores. Para identificar los bloques duplicados, Rapid Recovery incluye una caché de desduplicación para los repositorios del administrador de volúmenes de desduplicación (DVM). La caché mantiene las referencias a bloques exclusivos.

De manera predeterminada, la caché de desduplicación para repositorios DVM es de 1,5 GB. Este tamaño es suficiente para numerosos repositorios. Se desduplicarán sus datos en todo el repositorio hasta que se supere el tamaño de esta memoria caché. Si la cantidad de información redundante fuera tan grande que se llenara la caché de desduplicación, su repositorio dejaría de aprovechar todas las ventajas de la desduplicación para los datos recién añadidos. La cantidad de datos almacenados en su repositorio antes de que se llene la memoria caché de desduplicación varía dependiendo del tipo de datos que se incluyen en copia de seguridad y es diferente para cada usuario.

Puede aumentar el tamaño de la caché de desduplicación de DVM cambiando la configuración de la caché de desduplicación en el Rapid Recovery Core. Para obtener información acerca de cómo aumentar el tamaño de la caché, consulte el tema Configuración de los valores de caché de la desduplicación de DVM.

Cuando aumenta el tamaño de la caché de desduplicación de DVM hay dos factores a tener en cuenta: el espacio en disco y el uso de memoria RAM.

Espacio en disco. Se almacenan en disco dos copias de la caché de desduplicación de DVM: una memoria caché principal y una memoria caché secundaria que es una copia en paralelo. Por lo tanto, en el caso de utilizar el tamaño de la memoria caché predeterminada de 1,5 GB para un repositorio DVM, se utilizarán 3 GB de almacenamiento en disco en el sistema. A medida que aumenta el tamaño de la memoria caché, la cantidad de espacio en disco utilizada se mantiene proporcionalmente el doble del tamaño de la memoria caché. Para garantizar un rendimiento adecuado y resistente a los fallos, el Core cambia dinámicamente la prioridad de estas cachés. Ambas son necesarias, la única diferencia radica en que la memoria caché designada como principal se guarda primero.

Uso de memoria RAM. Cuando se inicia el Rapid Recovery Core, carga la caché de desduplicación en la RAM. El tamaño de la caché, por lo tanto, afecta al uso de la memoria para el sistema. La cantidad total de RAM que utiliza el Core depende de muchos factores. Entre estos factores se incluyen qué operaciones se están ejecutando, el número de usuarios, el número de equipos protegidos y el tamaño de la caché de desduplicación. Cada operación realizada por el Core (transferencia, replicación, consolidación, etc.) consume memoria RAM. Una vez finalizada una operación, el consumo de memoria se ve reducido en consecuencia. Sin embargo, los administradores deberían tener en cuenta el requisito de carga de memoria RAM más alto para realizar operaciones de forma eficaz.

La configuración predeterminada para el Rapid Recovery Core coloca la caché principal, la caché secundaria y la caché de metadatos para repositorios DVM en el directorio de AppRecovery. Esta carpeta está instalada en el equipo del Core.

NOTE: Dependiendo de su configuración, es posible que el directorio de AppRecovery no esté visible en el Rapid Recovery Core. Para ver este directorio es posible que tenga que cambiar el panel de control de opciones de carpeta para que muestre archivos, carpetas y unidades ocultos.

Presuponiendo que el Rapid Recovery Core esté instalado en la unidad C, estas ubicaciones son normalmente las siguientes:

Tabla 13. Ubicaciones de almacenamiento predeterminadas para la configuración de la caché de desduplicación de DVM

Configuración	Ubicación de almacenamiento predeterminada
Ubicación de la memoria caché principal	C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache
Ubicación de la memoria caché secundaria	C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
Ubicación de la memoria caché de metadatos	C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata

Puede cambiar la ubicación de almacenamiento de estas memorias caché. Por ejemplo, para aumentar la tolerancia a fallos, puede cambiar la ubicación de su caché secundaria a una unidad física diferente a la principal, presuponiendo que el Rapid Recovery Core tenga acceso a dicha ubicación.

Para obtener más información acerca del cambio de las ubicaciones de almacenamiento para cualquiera de estas configuraciones, consulte el tema Configuración de los valores de caché de la desduplicación de DVM.

Quest recomienda planificar el almacenamiento de desduplicación por separado. La desduplicación solo se produce en un único repositorio (no en varios). Si se utiliza cifrado basado en el Core, la desduplicación se limita a los datos protegidos por una clave única, ya que por motivos de seguridad cada clave sirve para un único dominio de cifrado.

Para obtener más información acerca de la desduplicación, consulte Desduplicación en Rapid Recovery.

Configuración de los valores de caché de la desduplicación de DVM

Complete los pasos de este procedimiento para configurar los parámetros de la caché de desduplicación para repositorios DVM.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Caché de desduplicación de DVM**. Esta opción solo aparece si el Core tiene uno o más repositorios DVM.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Caché de desduplicación de DVM.
3. Si desea restaurar los valores predeterminados de la caché de desduplicación de DVM en cualquier momento, haga lo siguiente:
   a. En la parte superior del área de configuración de la caché de desduplicación, haga clic en **Restaurar valores predeterminados**.

   Aparecerá el cuadro de diálogo Restaurar valores predeterminados.

   b. Haga clic en **Sí** para confirmar la restauración.
4. Haga clic en la opción de configuración que desee cambiar.

La opción seleccionada se volverá editable.

5. Para cambiar opciones de configuración individuales de la caché de desduplicación, introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 14. Información de configuración de la caché de desduplicación de DVM

Configuración	Descripción
Restaurar valores predeterminados	Este control restablece las ubicaciones de la caché DVM a las ubicaciones predeterminadas del sistema, que se describen para cada parámetro.
Ubicación de la caché principal	Si desea cambiar la ubicación de la memoria caché principal para repositorios DVM, en el cuadro de texto Ubicación de la memoria caché principal introduzca la ruta de acceso para una ubicación de almacenamiento accesible para el Core. La ubicación predeterminada es: `C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache` Ya que las memorias caché principal y secundaria son del mismo tamaño, el almacenamiento colectivo de estas dos memorias caché requiere el doble de espacio que la cantidad asignada para el tamaño de la memoria caché de desduplicación. Por ejemplo, si especifica 1,5 GB para el tamaño de desduplicación de la memoria caché de desduplicación, asegúrese de que cada una de las dos ubicaciones de almacenamiento cuenta con 1,5 GB como mínimo. En particular, si ambas ubicaciones pertenecen a la misma unidad (por ejemplo, la unidad C), debe haber al menos 3,0GB de espacio libre en el disco.
Ubicación de la caché secundaria	Si desea cambiar la ubicación de la memoria caché secundaria para repositorios DVM, en el cuadro de texto Ubicación de la memoria caché secundaria introduzca la ruta de acceso para una ubicación de almacenamiento accesible para el Core. La ubicación predeterminada es: `C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache`
Ubicación de metadatos de la caché	Si desea cambiar la ubicación de metadatos de la caché para repositorios DVM, en el cuadro de texto Ubicación de metadatos de la caché introduzca la ruta de acceso para una ubicación de almacenamiento accesible para el Core. La ubicación predeterminada es: `C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata`
Tamaño de la caché de desduplicación (GB)	Si desea cambiar el tamaño de la memoria caché de desduplicación para repositorios DVM, en el cuadro de texto Tamaño de caché de desduplicación introduzca una nueva cantidad (en GB). La ubicación predeterminada es: `C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache` El ajuste mínimo de tamaño de caché es 1,5GB. Además, el tamaño de la memoria caché no puede superar el 50% de la memoria RAM instalada.

6. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

Configuración de los parámetros del motor de Replay

Puede configurar información referente al Replay Engine, que es el canal de comunicación de Rapid Recovery. Estos parámetros determinan la configuración del Core para que proporcione una comunicación eficaz.

En general, Quest recomienda el uso de la configuración predeterminada. En algunos casos, es posible que el servicio de asistencia técnica de Quest le indique modificar estos parámetros para ayudar a ajustar el rendimiento a sus necesidades de red.

Complete los pasos de este procedimiento para configurar los parámetros del motor de Replay.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Replay Engine**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Replay Engine.
3. Haga clic en la opción que desee cambiar.

   La opción seleccionada se volverá editable.
4. Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 15. Información de la configuración de Replay Engine

Cuadro de texto	Descripción
Dirección IP	El Core utiliza esta dirección IP cuando realiza el montaje y la restauración de un punto de recuperación para permitir reacciones entre los equipos protegidos y el Core. La dirección IP de Replay Engine se rellena automáticamente con la dirección IP del equipo del Core. Si introduce manualmente la dirección IP del servidor, este valor se utilizará en caso de que el equipo protegido no pueda resolver automáticamente la dirección IP facilitada. No hace falta establecer este valor manualmente a menos que los equipos protegidos tengan problemas para comunicarse con el Core.
Puerto de preferencia	Escriba 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 de Replay.
Puerto en uso	Representa el puerto que se utiliza para la configuración del motor de Replay.
Permitir autoasignación de puerto	Haga clic para permitir la autoasignación del puerto TCP.
Grupo de administración	Escriba un nuevo nombre para Grupo de administración. El nombre predeterminado es BUILTIN\Administrators.

Cuadro de texto	Descripción
Longitud de E/S asíncrona mínima	Escriba un valor o elija el valor predeterminado. Describe la longitud mínima de entrada y salida asíncrona. El valor predeterminado es 65536.
Tiempo de espera de lectura	Escriba un valor de tiempo máximo de espera de lectura o elija el valor predeterminado. El valor predeterminado es 0:05:00.
Tiempo de espera de escritura	Escriba un valor de tiempo máximo de espera de escritura o elija el valor predeterminado. El valor predeterminado es 0:05:00.
Tamaño del búfer de recepción	Escriba el tamaño del búfer de recepción o acepte el valor predeterminado. El valor predeterminado es 8192.
Tamaño del búfer de envío	Escriba el tamaño del búfer de salida o acepte el valor predeterminado. El valor predeterminado es 8192.
Sin retraso	Se recomienda dejar esta casilla de verificación sin marcar, ya que, de lo contrario, la eficacia de la red podría verse afectada. Si desea modificar este ajuste, póngase en contacto con el servicio de asistencia técnica de Quest para que le asesoren.

5. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

Configuración de los parámetros de implementación

Rapid Recovery le permite descargar instaladores desde el Rapid Recovery Core en los equipos que desee proteger.

Puede configurar los parámetros relacionados con la implementación del software Rapid Recovery Agent desde el Core en los equipos que desee proteger.

Complete los pasos de este procedimiento para configurar los parámetros de implementación.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en ⚙ (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Implementar**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Implementar.
3. Haga clic en la opción que desee cambiar.

   La opción seleccionada se volverá editable.
4. Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 16. Información de configuración de implementaciones

Cuadro de texto	Descripción
Nombre de instalador de Agent	El nombre de archivo predeterminado es Agent-Web.exe. Si desea cambiar el nombre de este archivo por cualquier motivo, puede utilizar este parámetro para especificar un nuevo nombre del archivo ejecutable del instalador web del Core. Este archivo transmite una descarga de la última versión del instalador del Core de Rapid Recovery, que se inicia directamente desde Internet y le permite realizar una pausa y reanudar el proceso según lo necesite.
Dirección del Core	Introduzca la dirección de su servidor Core. Normalmente consta del protocolo, el nombre de su servidor Core y el puerto, así como el directorio donde residen los archivos del Core. Por ejemplo, si su servidor es Muestra, el parámetro es https://muestra:8006/apprecovery/admin/Core
Error de tiempo de espera de recepción	La cantidad de tiempo que la implementación del software Agent debe intentarse antes de agotar el tiempo de espera. El valor predeterminado es 00:25:00 o veinticinco minutos. Si desea cambiar este parámetro, introduzca la cantidad de tiempo que desea que el sistema pase intentando implementar el software Agent antes de que se agote el tiempo de espera máximo durante los eventos de lectura o escritura. Utiliza el formato HH:MM:SS.
Número máximo de instalaciones paralelas	Este parámetro controla el número máximo de implementaciones del software Agent que debe intentar el Core al mismo tiempo. El valor predeterminado es 100.

5. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

Configuración de los parámetros de conexión con la base de datos

Rapid Recovery muestra información sobre las tareas del Core, eventos y alertas en la página Eventos.Rapid Recovery almacena esta información transaccional en una base de datos del servicio MongoDB que se instala localmente de forma predeterminada en el equipo del Core. Puede configurar estos parámetros para cambiar la cantidad de tiempo que se retiene la información en la base de datos, o para cambiar el tamaño del grupo de conexión para permitir más o menos conexiones simultáneas.

Si está utilizando un segundo Rapid Recovery Core, puede configurar los parámetros de conexión de la base de datos en el primer Core para que apunten al segundo equipo del Core. De esta manera, los datos de eventos de ambos Cores se almacenarán en MongoDB en el segundo Core.

También puede configurar los parámetros de conexión de la base de datos del Core para que apunten a otro equipo que tenga instalado MongoDB de forma separada y que esté accesible desde la red al Rapid Recovery Core. Los datos de transacciones de eventos de su Core se guardan en esa base de datos de servicio, no de forma local. Para obtener más información acerca del establecimiento o modificación de parámetros de conexión de bases de datos para la base de datos de servicio, consulte Configuración de los parámetros de conexión con la base de datos.

NOTE: Para obtener más información sobre la visualización de información de eventos desde el Rapid Recovery Core, consulte Visualización de eventos mediante las páginas de tareas, alertas y del diario.

Los clientes pueden elegir especificar la instalación de la base de datos de servicio MongoDB en otro equipo que sea accesible para el Rapid Recovery Core en la red. Si la base de datos de servicio para su Rapid Recovery Core se instala en otro equipo que no sea el que aloja el Rapid Recovery Core, debe proporcionar credenciales para la base de datos (un nombre de usuario y una contraseña) en esta configuración.

Complete los pasos de este procedimiento para modificar los parámetros de conexión de base de datos de la base de datos de servicio que utiliza el Rapid Recovery Core.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Conexión de base de datos**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Conexión de base de datos.
3. En la parte superior del área de configuración de la conexión de base de datos, puede hacer lo siguiente:
   - Haga clic en **Probar conexión** para verificar la configuración.

     Se recomienda probar la conexión si cambia alguno de los valores de conexión de la base de datos.
   - Haga clic en **Restaurar valores predeterminados** para restaurar todas las opciones de configuración de la base de datos a sus valores predeterminados.

     Se le solicitará que confirme esta acción y, si lo hace, los valores personalizados de configuración de la conexión de la base de datos se descartarán.
4. Haga clic en la opción que desee cambiar.

   La opción seleccionada se volverá editable.
5. Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 17. Información de configuración de la conexión de la base de datos

Descripciones de la configuración de la conexión disponibles en la página Configuración del Rapid Recovery Core.

Cuadro de texto	Descripción
Nombre de host	Escriba un nombre de host para la conexión de la base de datos. **NOTE:** Cuando localhost es el parámetro especificado como host, MongoDB se instala de forma local en el equipo que aloja al Core.
Puerto	Especifique un número de puerto para la conexión de la base de datos. **NOTE:** El valor predeterminado es 27017.
Nombre de usuario	Introduzca un nombre de usuario con privilegios administrativos para la base de datos de servicio MongoDB. **NOTE:** Si el parámetro de nombre de host es localhost, no se requiere este campo.
Contraseña	Introduzca la contraseña asociada con el nombre de usuario que haya especificado.

Cuadro de texto	Descripción
	NOTE: Si el parámetro de nombre de host es localhost, no se requiere este campo.
Periodo de retención (día)	Introduzca el número de días que se conservará el historial de eventos y trabajos en la base de datos de servicio.
Tamaño máximo de grupo de conexiones	Establece el número máximo de conexiones de base de datos en caché para permitir la reutilización dinámica. **NOTE:** El valor predeterminado es 100.
Tamaño mínimo de grupo de conexiones	Establece el número mínimo de conexiones de base de datos en caché para permitir la reutilización dinámica. **NOTE:** El valor predeterminado es 0.

6. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

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

Puede ver eventos del sistema relacionados con el Rapid Recovery Core en la página Eventos. El Rapid Recovery Core almacena esta información de transacciones en una base de datos de servicio MongoDB. De manera predeterminada, esta base de datos está instalada localmente en el equipo del Core y el nombre de host en la configuración de conexión de base de datos tiene los valores predeterminados del localhost. En esta situación, la interfaz de loopback omite el hardware de la interfaz de red local y no son necesarias las credenciales de la base de datos.

De manera opcional y para aumentar la seguridad, puede especificar explícitamente credenciales de base de datos (un nombre de usuario y una contraseña) para la base de datos MongoDB que utiliza el Rapid Recovery Core.

NOTE: Para obtener más información sobre la visualización de información de eventos desde el Rapid Recovery Core, consulte Visualización de eventos mediante las páginas de tareas, alertas y del diario. Para obtener más información sobre la configuración de conexión de base de datos, consulte Configuración de los parámetros de conexión con la base de datos.

Complete los pasos de este procedimiento para modificar la configuración de la conexión con la base de datos local con el fin de especificar credenciales de base de datos.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en ⚙ (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Parámetros de base de datos local**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Parámetros de base de datos local.
3. Haga clic en la opción que desee cambiar.

La opción seleccionada se volverá editable.

4. Introduzca las credenciales correspondientes para la conexión a la base de datos de servicio, tal como se describe en la tabla siguiente.

Tabla 18. Información de configuración de la base de datos local

Cuadro de texto	Descripción
Nombre de usuario	Introduzca un nombre de usuario con privilegios administrativos para la base de datos de servicio MongoDB.
Contraseña	Introduzca la contraseña asociada con el nombre de usuario que haya especificado.

5. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

Administración de la configuración del servidor SMTP

Si configura los parámetros del servidor de protocolo sencillo de transferencia de correo (SMTP) para el Core, podrá enviar notificaciones de tareas, eventos y alertas por correo electrónico.

Puede encontrar información sobre cómo configurar un servidor de correo electrónico SMTP en el tema Configuración de un servidor de correo electrónico.

NOTE: Para enviar información de eventos por correo electrónico, también deberá configurar los parámetros del grupo de notificación. Para obtener más información sobre cómo especificar eventos para recibir alertas de correo electrónico, consulte Configuración de grupos de notificación.

Configuración de ajustes de conexión de cuentas de la nube

La configuración de conexión de cuentas en la nube permite determinar cuánto tiempo debe transcurrir entre que Rapid Recovery intenta conectarse a su cuenta en la nube antes de que se agote el tiempo de la operación. Realice los pasos del procedimiento siguiente para configurar los ajustes de conexión para su cuenta de nube.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en **Configuración**.

Aparecerá la página Configuración.

3. En el menú izquierdo, haga clic en **Cuentas de nube**.
4. En la tabla Cuentas en la nube, haga clic en el menú desplegable junto a la cuenta en la nube que desee configurar y, a continuación, complete una de las siguientes acciones:
   - Para restablecer los siguientes valores predeterminados a partir de cualquier configuración personalizada de la nube, haga clic en **Restablecer**.
     - **Tiempo de espera agotado de la solicitud** 01:30 (minutos y segundos)
     - **Tamaño del búfer de escritura** 8388608 (bytes)
     - **Tamaño del búfer de lectura** 8388608 (bytes)
   - Para cambiar la configuración de la conexión de la cuenta de nube, haga clic en **Editar** y, en el cuadro de diálogo **Configuración de la nube**, realice cualquiera de las siguientes acciones:
     - En **Tiempo de espera agotado de la solicitud**, utilice las flechas hacia arriba y hacia abajo para determinar la cantidad de tiempo en minutos y segundos que Rapid Recovery debe invertir en cada intento de conexión con la cuenta de nube cuando hay un retraso. Los intentos de conexión cesarán transcurrida la cantidad de tiempo introducida.
     - En **Tamaño del búfer de escritura**, introduzca el tamaño del búfer que desea reservar para escribir los datos archivados en la nube.
     - En **Tamaño del búfer de lectura**, introduzca el tamaño del bloque que desea reservar para leer los datos archivados desde la nube.

Trabajar con certificados de administración de Azure asociados con el Core

Desde la configuración del Rapid Recovery Core, puede asociar los certificados de administración de Azure con su Core. Este proceso permite al Core acceder a la información acerca de las suscripciones de Azure, haciendo que la información esté disponibles desde la Core Console.

Por ejemplo, cuando se realiza una exportación virtual a Azure, después de cargar la información del certificado, puede seleccionar la suscripción de Azure apropiada desde el cuadro desplegable. Los objetos asociados con esa suscripción pasan a ser accesibles a otros controles de la interfaz de usuario de Core Console, como las cuentas de almacenamiento, contenedores, etc.

La información del certificado de administración de Azure se almacena en un archivo de configuración de publicación generado en Microsoft Azure. Puede agregar uno o más certificados de administración a su Core. El Core obtiene las credenciales de manera segura.

Trabajar con certificados de administración de Azure desde la configuración del Core incluye las siguientes tareas:

- Obtención del archivo de configuración de publicación de su cuenta de Azure
- Carga de un certificado de administración de Azure
- Actualización o eliminación de certificados de administración de Azure

Obtención del archivo de configuración de publicación de su cuenta de Azure

Para realizar esta tarea, debe utilizar un equipo de Windows en el que se haya habilitado PowerShell. También debe tener acceso a una cuenta de Azure a la que se le haya concedido el rol de administrador o coadministrador de servicios.

El archivo de configuración de publicación es un documento XML generado en Azure. Este archivo contiene la definición de la API AzureServiceManagement e información sobre su suscripción de Azure, incluidas las credenciales codificadas seguras, su tipo de suscripción y un certificado de administración de Azure. El archivo contiene una extensión de archivo de `.publishsettings`, de donde se deriva la descripción. Sin el archivo de configuración de publicación, no puede conectar Core a una cuenta de Azure.

Puede obtener una copia del archivo de configuración de publicación desde un equipo de Windows registrado en su cuenta de Azure.

CAUTION: Puesto que el archivo de configuración de publicación contiene sus credenciales e información sobre su cuenta de Azure, Microsoft recomienda almacenar este archivo en una ubicación segura. Una vez que haya cargado el certificado, puede eliminar el archivo desde su sistema local.

Microsoft impone un límite de 100 certificados de administración por suscripción, con un límite máximo adicional de 100 certificados de administración para todas las suscripciones con un ID de usuario de administrador de servicios específico. Si tiene que acceder a la misma cuenta de Azure desde varios Cores, puede generar el archivo de configuración de publicación una sola vez y volver a utilizar el mismo archivo para cargar el certificado de administración en varios Cores. De esta manera, puede evitar superar el límite de generación de certificados.

NOTE: Para obtener más información sobre este límite, consulte la sección "Limitaciones" del artículo de Knowledge Base "Certificates overview for Azure Cloud Services" (Descripción general de certificados para los servicios en la nube de Azure) en https://docs.microsoft.com/es-es/azure/cloud-services/cloud-services-certs-create.

Realice los pasos de este procedimiento para obtener el archivo de configuración de publicación.

1. En un equipo de Windows, inicie sesión en el panel de Azure.
2. Mientras esté conectado a Azure, abra otra ventana del explorador.
3. Ejecute un script de PowerShell para descargar el archivo introduciendo la siguiente dirección en la URL del explorador: `https://manage.windowsazure.com/publishsettings/index?client=powershell`.

   Si todo va bien, el archivo de configuración de publicación se guarda en su directorio de descarga predeterminado.
4. Traslade este archivo a un equipo al que pueda acceder la Core Console.

Para asociar la información de suscripción de Azure con su Rapid Recovery Core, consulte el tema de *Guía del usuario de Rapid Recovery* "Loading an Azure management certificate" (Carga de un certificado de administración de Azure).

Carga de un certificado de administración de Azure

Para realizar esta tarea, debe disponer de un archivo de configuración de publicación de la correspondiente cuenta de Azure. Para obtener información sobre el acceso a este archivo, consulte Obtención del archivo de configuración de publicación de su cuenta de Azure.

Cuando se carga un certificado de administración de Azure en su Core, se le da acceso a la Core Console a la información de suscripción de su cuenta de Azure. A continuación, podrá ver los objetos asociados con su suscripción de Azure en la Core Console.

Complete los pasos de este procedimiento para cargar un certificado de administración de Azure en el Core.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Certificados de administración de Azure**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Certificados de administración de Azure.
3. Debajo del encabezado Certificados de administración de Azure, haga clic en **Cargar certificado**.

   Se mostrará el cuadro de diálogo **Cargar certificado**.
4. En el cuadro de diálogo **Cargar certificado**, haga clic en **Examinar**.

   Se mostrará la ventana **Carga de archivo**.
5. Vaya a la ubicación en la que se encuentre el archivo de configuración de publicación, selecciónelo y haga clic en **Abrir**.

   Se cerrará la ventana **Carga de archivo** y el certificado de administración de Azure se cargará en la Core Console.

Actualización o eliminación de certificados de administración de Azure

Para eliminar un certificado de administración de Azure de la Core Console, debe cargarse el certificado y asociarse al Core. Para obtener información sobre la asociación de certificados al Core, consulte Carga de un certificado de administración de Azure.

Complete los pasos de este procedimiento para actualizar la visualización de los certificados de administración de Azure con el Core o elimine el certificado del Core.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Certificados de administración de Azure**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Certificados de administración de Azure.
3. Para actualizar la visualización de certificados disponibles en la Core Console, debajo del encabezado Certificados de administración de Azure, haga clic en **Actualizar**.

   Se actualizará la página **Configuración del Core** y mostrará la información actualizada sobre los certificados asociados al Core.
4. Para eliminar un certificado del Core, en el certificado adecuado, haga clic en y seleccione **Eliminar**.
5. Haga clic en el cuadro de diálogo de confirmación para confirmar la eliminación del certificado.

   Se cerrará el cuadro de diálogo y el certificado de administración de Azure seleccionado se eliminará del Core.

Administración de la configuración de informes

Puede generar informes para el Rapid Recovery Core o para equipos protegidos. Para obtener información sobre los informes que puede generar, consulte Emisión de informes.

Complete los pasos de este procedimiento para administrar la configuración de informes de los informes de Core.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Informes**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Informes.

     Aparece la configuración del Core de **Informes**. La configuración de informes se describe en la siguiente tabla.

Opción	Descripción
Restaurar valores predeterminados	Esta opción restaura la configuración de informes a sus valores predeterminados. Los valores predeterminados se enumeran a continuación para cada parámetro.
Tipo de letra	Esta opción controla el tipo de letra predeterminado que se utiliza para los informes. El tipo de letra predeterminado es Trebuchet MS. Puede cambiar esta fuente por cualquier tipo de letra disponible para el sistema.
Tamaño del papel	Esta opción controla el tamaño del papel predeterminado utilizado para imprimir informes. El predeterminado es de carta. Puede seleccionar los siguientes tamaños de papel: • A3 • A4 • B4 • Ejecutivo • Libro de contabilidad • Legal • Carta • Periódico
Orientación de página	Esta opción controla la orientación de la página para informes exportados. La orientación predeterminada es Horizontal. Puede seleccionar las opciones de diseño siguientes: • Horizontal • Vertical

3. Para cambiar cualquiera de los parámetros de los informes, haga clic en el campo de configuración pertinente.

   El campo de configuración aparece como un menú desplegable configurable.
4. Haga clic en el menú desplegable y seleccione uno de los valores disponibles.

Por ejemplo, en el campo Tipo de letra, haga clic en **Times New Roman.**

5. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

   La opción seleccionada aparece ahora como la nueva configuración del parámetro Informes seleccionado.

Administración de la configuración de conectabilidad de SQL del Core

Las comprobaciones de conectabilidad SQL se realizan como parte de los trabajos nocturnos de Rapid Recovery. Con el fin de reducir los costos de licencia, Rapid Recovery propone dos opciones para realizar las comprobaciones de conectabilidad: utilizar una instancia de SQL Server con licencia instalada en el equipo del Core de Rapid Recovery o emplear la instancia de SQL Server que ya está instalada en el equipo protegido. Esta segunda opción es ahora el valor predeterminado. Sin embargo, si el equipo protegido ya se utiliza mientras se realizan los trabajos nocturnos, se recomienda realizar las comprobaciones con una instancia de SQL Server en el Core.

La capacidad de realizar comprobaciones de conectabilidad mediante la instancia de SQL Server en un equipo protegido es una función del software Rapid Recovery Agent. Esta función no funciona si el SQL Server está protegido sin agentes. Por tanto, si utiliza una protección sin agentes en el equipo SQL, configure este ajuste del Core en **Utilizar SQL Server en el Core**, como se muestra en el paso 3 de este procedimiento.

En resumen, el proceso de administración de la configuración de conectibilidad SQL del Core consta de las áreas siguientes:

- Montar el punto de recuperación más reciente para grupos de protección que contienen bases de datos.
- Conectar con la base de datos desde SQL Server.
- Abrir la base de datos.
- Cerrar la base de datos.
- Desmontar el punto de recuperación.

  Para activar esta comprobación nocturna, especifique una instancia de SQL Server que haya que utilizar para realizar comprobaciones de conectabilidad de las bases de datos SQL Server en equipos protegidos.

  NOTE: Esta opción no aparece si no está protegiendo un SQL Server en su Core.

Para configurar el Core con tal de realizar comprobaciones de la conectibilidad SQL como parte de las tareas nocturnas, realice los pasos siguientes.

NOTE: Si selecciona la opción predeterminada para utilizar la instancia de SQL Server instalada en el equipo protegido, esa instancia de SQL Server administrará la conectabilidad de SQL de todos los equipos protegidos de SQL. Si no desea que este parámetro se aplique a todos los equipos SQL protegidos, seleccione Usar SQL Server en el Core. Para realizar comprobaciones de conectabilidad en el Core, debe instalar o utilizar una versión de SQL Server con licencia en el equipo del Core.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Conectabilidad**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Conectabilidad.
3. Para utilizar la instancia de SQL Server instalada en el equipo protegido de SQL Server, seleccione **Utilizar SQL Server en el equipo protegido**. Esta es la opción predeterminada.
4. Para utilizar la instancia de SQL Server instalada en el Core de Rapid Recovery, seleccione **Utilizar SQL Server en el Core** y, a continuación, introduzca la información de autenticación tal como se describe en la tabla siguiente.

Tabla 19. Información de credenciales de SQL Server

Descripciones de la información necesaria para autenticar una conexión a SQL Server.

Cuadro de texto	Descripción
SQL Server	Desde el menú desplegable de SQL Server, seleccione la opción apropiada de la instancia de SQL Server desde el servidor del Core.
Tipo de credencial	Elija el método de autenticación pertinente para sus credenciales entre las siguientes opciones: • Windows • SQL
Nombre de usuario	Especifique un nombre de usuario para acceder a SQL Server en el Core según el tipo de credencial seleccionado.
Contraseña	Especifique una contraseña para acceder a SQL Server en el Core según el tipo de credencial seleccionado.

5. Haga clic en **Probar conexión**.

   NOTE: Si no ha especificado las credenciales correctamente, aparece un mensaje que le indica que las credenciales son incorrectas. Corrija la información de credenciales y vuelva a probar la conexión.
6. Si está satisfecho con los cambios, haga clic en **Aplicar**.

Funcionamiento de los trabajos de Core

Los trabajos son procesos que el Core de Rapid Recovery realiza para dar soporte a sus operaciones, incluida la copia de seguridad en puntos de recuperación, la replicación de datos, el archivado de datos, la exportación de datos a máquinas virtuales, el manteniendo de repositorios, etc. Los trabajos de Core se inician automáticamente

para algunas operaciones, como la replicación o el archivado según un calendario de programación establecido. También puede abrir algunos trabajos a petición desde varios componentes en la Core Console.

- Al visualizar o editar la configuración del trabajo del Core, cada trabajo tendrá dos parámetros: N.º máximo de trabajos simultáneos y Recuento de intentos.
  - El parámetro N.º máximo de trabajos simultáneos determina cuántos trabajos de ese tipo se pueden ejecutar al mismo tiempo.
  - El parámetro Recuento de intentos determina el número de veces que un trabajo se debe intentar ejecutar antes de abandonarlo si un error de red u otro error de comunicación impide que el trabajo tenga éxito la primera vez.
- En la tabla de trabajos de Core, la columna Configuración indica si el trabajo que aparece está incluido en la configuración de trabajos de Core de manera predeterminada o si es necesario agregarlo explícitamente.

La siguiente tabla describe los trabajos del Core principal disponibles y sus funciones.

Tabla 20. Trabajos de Core

Nombre de trabajo	Descripción	N.º máximo de trabajos simultáneos	Recuento de intentos	Configuración
Comprobar la conectabilidad de bases de datos SQL en instantáneas	Permite al Core comprobar la coherencia de las bases de datos SQL y garantiza que todos los archivos MDF (datos) y LDF (registro) compatibles están disponibles en la instantánea de copia de seguridad. Proceso: • Montar el punto de recuperación más reciente para grupos de protección que contienen bases de datos SQL. • Montar la base de datos. Si se está realizando la conectabilidad desde el servidor SQL protegido, realice el montaje mediante la ruta de acceso UNC. • Conectar con la base de datos desde SQL Server. • Realizar la comprobación de conectabilidad. • Realizar operaciones de limpieza. • Cerrar la base de datos. • Desmontar la base de datos. • Desmontar el punto de recuperación.	1	0	Predeterminado
Comprobar suma de comprobación de bases de datos de Exchange	Comprueba la integridad de los puntos de recuperación que contienen bases de datos de Exchange. Proceso: • Montar el punto de recuperación más reciente para grupos de	1	0	Predeterminado

Nombre de trabajo	Descripción	N.º máximo de trabajos simultáneos	Recuento de intentos	Configuración
	protección que contienen bases de datos SQL. • Conectar con la base de datos desde SQL Server. • Abrir la base de datos. • Cerrar la base de datos. • Desmontar el punto de recuperación.			
Comprobar la capacidad de montaje de bases de datos de Exchange	Comprueba que las bases de datos de Exchange se pueden montar.	1	0	Predeterminado
Replicar datos de equipos protegidos desde origen remoto	Transfiere una copia de puntos de recuperación de un equipo protegido desde un Core de origen a un Core de destino. Este trabajo se ejecuta en el Core de destino y recibe los puntos de recuperación replicados entrantes.	3	0	Predeterminado
Replicar datos de equipos protegidos en destino remoto	Transfiere una copia de puntos de recuperación de un equipo protegido desde un Core de origen (en el que se guardaron originariamente) a un Core de destino. Este trabajo se ejecuta en el Core de origen y controla la replicación saliente.	1	3	Predeterminado
Consolidar puntos de recuperación	Aplica la política de retención a sus datos de copia de seguridad combinando la "consolidación" de puntos de recuperación en el programa definido en la política de retención.	1	0	Predeterminado
Comprobar puntos de recuperación	Comprueba la integridad de los puntos de recuperación.	1	0	Agregar
Eliminar todos los puntos de recuperación	Elimina el conjunto completo de puntos de recuperación en un equipo protegido.	1	0	Agregar
Eliminar cadena de puntos de recuperación	Elimina una cadena de puntos de recuperación completa en un equipo protegido.	1	0	Agregar
Eliminar intervalo de puntos de recuperación	Elimina un conjunto de puntos de recuperación en un equipo protegido, por identificador de punto de recuperación o por intervalo de fechas.	1	0	Agregar

Nombre de trabajo	Descripción	N.º máximo de trabajos simultáneos	Recuento de intentos	Configuración
Implementar software de Agent en equipos	Implementa el software Rapid Recovery Agent en el equipo o equipos especificados.	1	0	Agregar
Descargue bibliotecas de Exchange	Descarga las bibliotecas de Microsoft Exchange desde el equipo protegido al equipo del Core en la ruta de acceso `C:\ProgramData\AppRecovery\ExchangeLibraries`.	1	0	Agregar
Exportar a archivo comprimido	Crea una copia de seguridad en la ruta de acceso especificada con un archivo de los puntos de recuperación seleccionados. Proceso: • Puntos de recuperación de montaje. • Escribir datos en copias de seguridad. • Desmontar el punto de recuperación.	1	0	Agregar
Exportar a máquina virtual	Exporta los datos del punto de recuperación especificado del equipo protegido a la ruta de destino como una máquina virtual. Proceso: • Montar punto de recuperación. • Crear una máquina virtual a partir de los datos del punto de recuperación en la ruta de destino. • Desmontar el punto de recuperación.	1	0	Agregar
Importar archivos	Importa el punto de recuperación a partir de la copia de seguridad especificada en un archivo comprimido del Core previamente creado.	1	0	Agregar
Mantener repositorio	Realiza una comprobación del repositorio. Proceso: • Comprobar el sistema de archivos de repositorio. • Montar punto de recuperación. • Volver a calcular el caché de desduplicación para el repositorio. • Cargar los puntos de recuperación del repositorio.	1	0	Agregar

Nombre de trabajo	Descripción	N.º máximo de trabajos simultáneos	Recuento de intentos	Configuración
Montar instantáneas de puntos de recuperación	Realiza el montaje del punto de recuperación en la ruta de acceso especificada.	1	0	Agregar
Proteger máquinas virtuales ESX®	Agrega todas las máquinas virtuales especificadas a la protección sin agente. El trabajo se realiza inmediatamente después de agregar la protección sin agente de una o más máquinas virtuales al Core mediante el asistente para proteger varios equipos. El trabajo establece el número de identificación para cada máquina virtual especificada, escribe información sobre el Core en un archivo de configuración y recupera los metadatos del archivo.	1	0	Agregar
Restaurar desde punto de recuperación	Realiza una restauración a partir de un punto de recuperación en un equipo de destino especificado. Proceso: • Montar punto de recuperación. • Escribir todos los datos del punto de recuperación en el equipo especificado. • Desmontar el punto de recuperación.	1	0	Agregar
Carga de registros	Carga los registros al servidor especificado.	1	0	Agregar

Algunos trabajos de Core se incluyen en Configuración. La configuración de los trabajos le permite especificar cuántos trabajos simultáneos del mismo tipo puede ejecutar el Core y cuántos reintentos se deben realizar si falla el primer intento del trabajo.

Para obtener más información acerca de estos ajustes, consulte Configuración de trabajo de Core.

Para obtener información sobre cómo agregar trabajos a la Configuración del Core, consulte Incorporación de trabajos del Core a la configuración.

Para obtener más información sobre la edición de la configuración de los trabajos en la lista Configuración, consulte Modificación de los parámetros de los trabajos del Core.

Configuración de trabajo de Core

Cuando selecciona (Configuración) de la barra de iconos, puede acceder a la configuración de algunos trabajos del Core. El área **Trabajos** en la página Configuración del Core permite determinar dos valores para cada tipo de trabajo enumerado:

1. El número máximo de trabajos de este tipo que el Core puede intentar al mismo tiempo. Se debe establecer en un valor entre 1 y 50.
2. El número de veces que un trabajo se debe intentar si un error de red u otro error de comunicación impide que el trabajo tenga éxito la primera vez. Se debe establecer en un valor entre 0 y 10.

Varios trabajos se incluyen automáticamente en la configuración del Core. Estos trabajos incluyen un valor de "Predeterminado" en la columna Configuración (tal como se muestra en el tema Funcionamiento de los trabajos de Core).

Puede agregar algunos otros trabajos en la configuración si desea ajustar dichos valores para controlar el número máximo de trabajos o reintentos para esas funciones. Estos trabajos incluyen un valor de "Agregar" en la columna Configuración. Para obtener información sobre cómo agregar estos trabajos a la tabla Configuración, consulte Incorporación de trabajos del Core a la configuración.

Los trabajos del Core que no están disponibles en Configuración no proporcionan la capacidad de establecer estos dos parámetros.

Para los trabajos que se enumeran en Configuración, puede editar los valores existentes. Esto le permite personalizar los dos parámetros, eliminar un tipo de trabajo de la lista de configuración de trabajo o restaurar la configuración predeterminada. Para obtener información detallada, consulte el tema Modificación de los parámetros de los trabajos del Core.

Incorporación de trabajos del Core a la configuración

La configuración de los trabajos del Core le permite definir, para cada tipo de trabajo, el número máximo de trabajos para el Core que pueden intentarse a la vez y cuántas veces se debe reintentar ese trabajo si falla el primer intento.

Cada tipo de trabajo del Core tiene valores predeterminados para estos dos parámetros, tal como se describe en el tema Configuración de trabajo de Core. Esta lista también indica los tipos de trabajo que se incluyen en la configuración del Core de manera predeterminada.

Agregar un trabajo del Core a la configuración le permite cambiar estos parámetros para el tipo de trabajo que ha agregado.

Realice los pasos del procedimiento siguiente para agregar un trabajo a la configuración del Core.

1. Desplácese hasta la Core Console de Rapid Recovery.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Trabajos**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Trabajos.

   Aparece la configuración del Core de Trabajos.
3. En la página Configuración del Core, en Trabajos, haga clic en **Agregar**.

   Aparece el cuadro de diálogo Configuración de trabajo.
4. En el cuadro de diálogo **Configuración de trabajo**, en el campo **Trabajos**, seleccione el nombre del trabajo que desea agregar a la configuración del Core.

   Estos trabajos se describen en el tema Configuración de trabajo de Core.
5. Para establecer el número máximo de trabajos que el Core puede intentar al mismo tiempo, en el cuadro de texto **N.º máximo de trabajos simultáneos**, introduzca un nuevo valor entre 1 y 50.
6. Para establecer el número de intentos que el Core debe realizar antes de abandonar el trabajo, en el cuadro de texto **Recuento de intentos**, introduzca un nuevo valor entre 0 y 10.
7. Haga clic en **Guardar**.

   Se cerrará el cuadro de diálogo Configuración de trabajo y se aplicarán sus nuevos parámetros del trabajo.

Modificación de los parámetros de los trabajos del Core

La configuración de los trabajos del Core le permite definir, para cada tipo de trabajo, el número máximo de trabajos para el Core que pueden intentarse a la vez y cuántas veces se debe reintentar ese trabajo si falla el primer intento.

Cada tipo de trabajo del Core tiene valores predeterminados para estos dos parámetros, tal como se describe en el tema Funcionamiento de los trabajos de Core. Esta lista también indica los tipos de trabajo que se incluyen en la configuración del Core de manera predeterminada. Al editar la configuración de los trabajos del Core, puede conseguir lo siguiente:

- Puede personalizar la configuración de cada tipo de trabajo del Core.
- Puede eliminar un tipo de trabajo de la lista de configuración del Core. Esta función no está disponible si el tipo de trabajo está incluido en la configuración de manera predeterminada.

  NOTE: Eliminar un trabajo de la configuración del Core no hace más que quitar el tipo de trabajo de esa lista. Para volver a editar la configuración del Core para ese tipo de trabajo en el futuro, puede agregarlo a la lista tal como se describe en el tema Incorporación de trabajos del Core a la configuración.

- Puede restablecer la configuración de cualquier tipo de trabajo a sus valores predeterminados.

  NOTE: Aunque solo puede utilizar esta función para los tipos de trabajo incluidos en la configuración del Core de manera predeterminada, sí que puede establecer otros tipos de trabajo en sus valores predeterminados si los elimina de la lista y los vuelve a agregar.

Realice los pasos del procedimiento siguiente para editar la configuración de un trabajo.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página **Configuración**, haga clic en **Trabajos**.
   - Desplácese hacia abajo en el lado derecho de la página **Configuración** hasta que pueda ver el encabezado Trabajos.

   Aparece la configuración del Core de Trabajos.
3. Desde la cuadrícula Trabajo, seleccione el trabajo que desee quitar de la lista. Desde el menú desplegable de ese trabajo, seleccione **Eliminar**.

   El trabajo se eliminará de la lista.
4. Desde la cuadrícula Trabajo, seleccione en la lista el trabajo para el que desea restablecer la configuración. Desde el menú desplegable de ese trabajo, seleccione **Restablecer los valores predeterminados**.

   La configuración de trabajo de este trabajo se restablecerá a sus valores predeterminados.
5. En la cuadrícula Trabajo, seleccione el trabajo que desee cambiar. Desde el menú desplegable de ese trabajo, seleccione **Editar**.
6. La configuración del trabajo: Se abre el cuadro de diálogo [JobName].
7. Para cambiar el número máximo de trabajos que el Core puede intentar al mismo tiempo, en el cuadro de texto Número máximo de trabajos simultáneos, introduzca un nuevo valor entre 1 y 50.
8. Para cambiar el parámetro del número de intentos adicionales que el Core debe realizar antes de abandonar el trabajo, en el cuadro de texto Recuento de intentos, introduzca un nuevo valor entre 0 y 10.
9. Haga clic en **Guardar**.

   Se cerrará el cuadro de diálogo Configuración de trabajo y se aplicarán sus nuevos parámetros del trabajo.

Administración de licencias

Existen tres tipos de licencias de software de Rapid Recovery:

- **Prueba,** que deja de realizar instantáneas después de 14 días,
- **Suscripción,** que tiene fecha de caducidad y
- **Perpetua,** que no tiene fecha de caducidad.

Muchos usuarios de Rapid Recovery Core comienzan con una licencia de prueba, que tiene capacidades limitadas. Tras 14 días, si las circunstancias lo requieren, un administrador de grupo puede ampliar la licencia de prueba a 28 días. De lo contrario, puede adquirir y registrar una licencia de suscripción o perpetua.

NOTE: Para obtener información sobre cómo introducir la clave de licencia o la información del archivo (por ejemplo, para actualizar o cambiar una licencia de prueba por una licencia a largo plazo), consulte Actualización o cambio de una licencia.

Rapid Recovery ofrece licencias en un archivo. Un archivo de licencias de Rapid Recovery contiene un grupo de licencias que puede distribuir a los equipos que desea proteger. Este grupo se refleja en el Portal de licencias de Rapid Recovery. Para cada tipo de licencia de los enumerados anteriormente, existen dos tipos de grupos de licencias:

- **Enterprise.** Cada licencia de este grupo puede aplicarse en una instalación de Rapid Recovery Agent o un socket en un host hipervisor utilizando protección sin agentes, independientemente del espacio utilizado.
- **Capacity.** Estas licencias se aplican a la cantidad de datos que tenga previsto proteger, medida en terabytes (TB), independientemente del número de agentes de Rapid Recovery instalados o del número de sockets de los que disponga. Si excede la cantidad de espacio asignado a la licencia que ha adquirido, debe adquirir otra. Para licencias Capacity:
  - Los dispositivos DL utilizan un modelo de licencia Capacity back-end en el que la capacidad especificada en la licencia limita el tamaño del repositorio (en TB) que puede utilizar en el dispositivo.
  - Las instalaciones de software utilizan un modelo de licencia Capacity front-end en el que la capacidad especificada en la licencia limita la cantidad de datos (en TB) de los equipos que desea proteger que puede guardar en el repositorio. La capacidad front-end se mide previamente a la compresión y la desduplicación.

En versión 6.2, un Core solo puede utilizar un tipo de grupo de licencias. Por ejemplo, si su Core utiliza un grupo de licencias Capacity, no puede utilizar también un grupo de licencias Enterprise. Lo mismo ocurre en sentido inverso.

Los tipos de grupos de licencias no se pueden combinar en un único archivo de licencias. Por ejemplo, no puede incluir un grupo de licencias Enterprise y un grupo de licencias Capacity en la misma licencia perpetua.

Los **archivos de licencia** son archivos de texto que terminan con la extensión de archivo `.lic` . Algunos ejemplos de archivos de licencia son:

- Los archivos de licencia pueden aparecer con una longitud de nueve caracteres, que consiste en tres grupos de números separados entre sí por un guion; por ejemplo, `123-456-789.lic`.
- Las licencias basadas en software pueden aparecer con formato Software-<nombre de grupo>.lic, y el grupo tendrá el nombre del cliente o de la cuenta; por ejemplo, `Software-YourCompany.lic`.
- Las licencias de dispositivos de la serie DL pueden aparecer con formato <Serie de dispositivo>-<Nombre de grupo>.lic, y el grupo tendrá el nombre del cliente o de la cuenta; por ejemplo, `DL4X00 Series-YourCompany.lic`.

Rapid Recovery admite estos tipos de licencia en dos modos: el modo estándar con llamada a la central y el modo sin llamada a la central, que tiene varias limitaciones. Las licencias de suscripción siempre son del modo con llamada a la central. Las licencias de prueba y perpetua pueden ser del modo con llamada a la central o del modo sin llamada a la central. Para ver cómo afecta este modo al uso de datos personales en Rapid Recovery, consulte el tema "Administración de la privacidad". Para conocer las restricciones de las licencias sin llamada a

la central o recibir información acerca de cómo obtener una licencia de este modo, consulte "Obtener y utilizar licencias sin llamada a la central". Estos temas se encuentran en la *Guía del usuario de Rapid Recovery*.

Rapid Recovery le permite administrar licencias o ponerse en contacto con el servidor de licencias directamente desde la Core Console seleccionando (Configuración) de la barra de iconos y haciendo clic en **Licencias**.

La configuración de Licencias incluye la información siguiente:

Detalles de la licencia:

- **Cambiar licencia**. Le permite cargar un archivo de licencia o introducir una clave de licencia para cambiar una licencia existente asociada con el Core.
- **Agregar licencia**. Esta opción solo está disponible para dispositivos de copia de seguridad de la serie DL y le permite cargar un archivo de licencia o introducir una clave de licencia.
- **Grupo de portal de licencias**. Esta opción abre el portal de licencias para la administración del grupo.
- **Tipo de licencia**. Los tipos de licencia incluyen Prueba, Suscripción y Empresa. Para obtener más información, consulte el tema "Descripción de los tipos de licencia de software" en la *Rapid Recovery License Portal User Guide (Guía del usuario del Portal de licencias de Rapid Recovery)*.
- **Estado de la licencia**. Indica el estado de la licencia. Un estado activo garantiza que las instantáneas pueden proseguir como está programado. Si la licencia está bloqueada o caducada, o si el Core no ha podido comunicarse con el Portal de licencias de Rapid Recovery pasado el periodo de gracia, se realiza una pausa en las instantáneas hasta que se corrige el estado de la licencia.
- **La clave de licencia caduca dentro de**. Esta opción solo está disponible cuando se usa una licencia de suscripción, y muestra el tiempo restante para la caducidad de la suscripción en días.

Restricciones de licencia:

- **Máximo de instantáneas por día**. Indica el número de copias de seguridad, que está limitado por la licencia específica.

Grupo de licencias:

- **Tamaño de grupo**. El grupo de licencias es el número de licencias que no son de prueba disponibles para asignar en todos los grupos y subgrupos del Portal de licencias de Rapid Recovery. El tamaño del grupo determina cuántas licencias se pueden asignar. Para obtener más información, consulte el tema "Descripción de los grupos de licencias" en la *Rapid Recovery License Portal User Guide (Guía del usuario del Portal de licencias de Rapid Recovery)*.
- **Usado por este Core**. Indica el número de equipos del grupo de licencias que están protegidos por este Core.
- **Total usado en grupo**. Indica el número total de equipos protegidos dentro del mismo grupo de licencias que este Core.
- **Envío de datos a la central deshabilitado**. Si es visible, este estado indica que el Core no se comunica con el Portal de licencias de Rapid Recovery ni con el Portal de protección de datos. La actualización automática está deshabilitada y no se produce intercambio de información personal entre el Core y Quest Software Inc. o cualquier otra entidad, de conformidad con las políticas del GDPR.

Servidor de licencias. Estos parámetros se aplican a licencias estándar (llamada a casa). Estos parámetros no son aplicables a dispositivos y otras licencias que no son de llamada a casa:

- **Dirección del servidor de licencias**. Muestra una URL activa del servidor de licencias asociado con este Core.
- **Última respuesta del servidor de licencias**. Indica si la comunicación que se intentó por última vez con el portal del servidor de licencias fue correcta.
- **Último contacto con el servidor de licencias**. Muestra la fecha y la hora del último contacto correcto con el servidor de licencias.
- **Siguiente intento para ponerse en contacto con el servidor de licencias**. Indica las próximas fecha y hora programadas para intentar la comunicación con el servidor de licencias.
- **Póngase en contacto ahora**. Este botón entra en contacto con el servidor de licencias a petición. Utilice esta opción después de realizar cambios en la configuración de la licencia para registrar cambios inmediatamente en lugar de esperar al siguiente intento programado.

Para obtener más información sobre las licencias, consulte la *Rapid Recovery License Portal User Guide (Guía del usuario del Portal de licencias de Rapid Recovery)*.

Para obtener más información sobre cómo actualizar o cambiar una clave o archivo de licencia, consulte Actualización o cambio de una licencia.

Si es necesario, los usuarios de dispositivos de copia de seguridad de la serie DL también pueden agregar licencias a la Core. Para obtener más información, consulte Adición de una licencia.

Para obtener más información sobre cómo ponerse en contacto con el servidor del portal de licencias, consulte Contacto con el servidor del Portal de licencias de Rapid Recovery.

También puede ver información de licencia para un único equipo protegido. Para obtener más información, consulte Visualización de la información de licencia en un equipo.

Actualización o cambio de una licencia

Cuando haya actualizado o adquirido una licencia de Rapid Recovery de largo plazo, recibirá un archivo o una clave de licencia por correo electrónico.

Realice los pasos de este procedimiento para actualizar la licencia de prueba o cambiar la licencia existente, y asóciela con la Rapid Recovery Core Console.

NOTE: Si es necesario, los usuarios de dispositivos de copia de seguridad de la serie DL también pueden agregar licencias a la Core. Para obtener más información, consulte Adición de una licencia.

NOTE: Para obtener información sobre cómo obtener una clave de licencia o para conocer los detalles del uso del portal de licencias para descargar el software, registrar dispositivos, administrar suscripciones de licencia y grupos de licencias, y para generar informes del portal de licencias, consulte la *Rapid Recovery License Portal User Guide (Guía del usuario del Portal de licencias de Rapid Recovery)*.

Si acaba de instalar un nuevo Core y se visualiza un mensaje en la Core Console que le pide que elija un archivo o clave de licencia, pase al paso 5.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración).
3. Desplácese hacia abajo en el lado derecho de la página **Configuración** hasta que pueda ver el encabezado **Servidor de licencias**.

   Aparece la configuración del Core para las licencias.
4. Para actualizar o cambiar la licencia existente asociada con su Core, en la parte superior del área de configuración del Core Detalles de la licencia, haga clic en **Cambiar licencia**.

Aparecerá el cuadro de diálogo **Cambiar licencia**.

5. Si desea introducir manualmente la clave de licencia, vaya al paso 6. Si desea cargar un archivo de licencia, haga lo siguiente:
    a. Para actualizar un archivo de licencia, desde el campo **Seleccionar archivo de licencia o introducir clave de licencia**, haga clic en **Seleccionar archivo**.

    En el cuadro de diálogo **Carga de archivo**, desplácese por el sistema de archivos y localice el nuevo archivo de licencia que desea utilizar. Por ejemplo, busque `Software-YourCompany.lic`.

    b. Haga clic en el archivo de licencia y, a continuación, haga clic en **Abrir**.

    El cuadro de diálogo **Carga de archivo** se cerrará. El archivo de licencia que ha seleccionado aparece en el campo de texto de licencias.

    c. En el cuadro de diálogo **Cambiar licencia**, haga clic en **Continuar**.

    El archivo de licencia que ha seleccionado se autentica y esa licencia se asocia a su Core.

    d. Vaya al paso 7.
6. Para introducir manualmente la clave de licencia, en el campo de texto **Seleccionar archivo de licencia o introducir clave de licencia**, introduzca la clave de licencia con cuidado y, a continuación, haga clic en **Continuar**.

    El cuadro de diálogo se cierra, el archivo de licencia seleccionado se autentica y esa licencia se asocia a su Core.
7. Si observa la página principal de la **Quick Start Guide** (Guía de inicio rápido), puede iniciar la guía o cerrar la herramienta. Este es el último paso requerido para este procedimiento.

    NOTE: Para obtener más información sobre la Guía de inicio rápido, consulte "Explicación de la guía de inicio rápido" en *Guía del usuario de Rapid Recovery*.
8. Si realiza estos pasos en la página **Configuración** del Core, desplácese por el lado derecho de la página **Configuración** hasta que vea el encabezado Servidor de licencias.
9. En el área Servidor de licencias, haga clic en **Ponerse en contacto ahora**.

    Una vez aplicada la licencia en el servidor de licencias, cualquier equipo protegido asociado se actualiza con la nueva licencia de manera automática.

Si observa mensajes de error en la parte superior de la Rapid Recovery Core Console (como servicios específicos no iniciados), siga la guía del mensaje de error para resolver estos errores.

Adición de una licencia

Los propietarios de dispositivos de copias de seguridad de la serie DL pueden agregar una o más licencias a la Rapid Recovery Core Console.

Cuando haya actualizado la licencia de Rapid Recovery o haya adquirido una, recibirá un archivo o una clave de licencia por correo electrónico.

También puede actualizar o cambiar una licencia existente en la Core Console. Para obtener más información, consulte Actualización o cambio de una licencia.

NOTE: Únicamente los usuarios de servidores de copias de seguridad de la serie DL pueden ver el botón **Agregar servidor**.

NOTE: Para obtener información sobre cómo obtener una clave de licencia, consulte la *Rapid Recovery License Portal User Guide (Guía del usuario del Portal de licencias de Rapid Recovery)*.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración).
3. Desplácese hacia abajo en el lado derecho de la página **Configuración** hasta que pueda ver el encabezado Licencias.

Aparece la configuración del Core para las licencias.

4. Para agregar una licencia y asociarla con su Core, en la parte superior del área de configuración del Core Detalles de licencia, haga clic en **Agregar licencia**. En el cuadro de diálogo resultante, realice una de las siguientes acciones:

    a. Si desea introducir manualmente la clave de licencia, escriba cuidadosamente la clave y, a continuación, haga clic en **Continuar**.

    El cuadro de diálogo se cierra, el archivo de licencia seleccionado se autentica y esa licencia se asocia a su Core.

    b. Si desea cargar un archivo de licencia, haga clic en **Seleccionar archivo**.

    En el cuadro de diálogo **Carga de archivo**, desplácese por el sistema de archivos y localice el nuevo archivo de licencia que desea utilizar. Por ejemplo, busque `Software-YourCompany.lic`.

    c. Haga clic en el archivo de licencia y, a continuación, haga clic en **Abrir**.

    El cuadro de diálogo Carga de archivo se cerrará. El archivo de licencia seleccionado aparece en el cuadro de diálogo actual.

    d. En el cuadro de diálogo, haga clic en **Continuar**.

    El cuadro de diálogo se cierra, el archivo de licencia seleccionado se autentica y esa licencia se asocia a su Core.

5. Desplácese hacia abajo en el lado derecho de la página **Configuración** hasta que pueda ver el encabezado Servidor de licencias.

    Aparece la configuración del Core de Licencias.

6. En el área Servidor de licencias, haga clic en **Ponerse en contacto ahora**.

    Una vez aplicada la licencia en el servidor de licencias, cualquier equipo protegido asociado se actualiza con la nueva licencia de manera automática.

Contacto con el servidor del Portal de licencias de Rapid Recovery

La Rapid Recovery Core Console se pone frecuentemente en contacto con el servidor del Portal de licencias de Rapid Recovery para mantenerse actualizada de cualquier cambio que se realice en el portal de licencias.

Para licencias que no son de prueba, el Rapid Recovery Core contacta con el portal de licencias cada hora. Si el Core no puede contactar con el portal de licencias tras un periodo de gracia de 10 días, el Core deja de tomar instantáneas.

Por lo general, la comunicación con el servidor del portal de licencias se produce de forma automática, en los intervalos establecidos; no obstante, puede iniciar la comunicación bajo demanda.

Complete los pasos de este procedimiento para establecer contacto con el servidor del portal de licencias.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en **Configuración** y, a continuación, desplácese hacia abajo en la parte derecha de la página **Configuración** hasta que vea el encabezado Servidor de licencias.
3. En el área Servidor de licencias, haga clic en **Ponerse en contacto ahora**.

Comprensión de la configuración de SNMP

Simple Network Management Protocol (SNMP) es un protocolo para administrar dispositivos en un red IP. SNMP se utiliza principalmente para supervisar dispositivos en una red buscando condiciones que requieren atención. Este protocolo utiliza componentes de software (agentes) para remitir información a sistemas administrativos (gestores). Un agente SNMP administra las solicitudes del gestor para obtener o establecer ciertos parámetros. El agente SNMP puede enviar capturas (notificaciones sobre eventos específicos) al gestor.

Los objetos de datos que administran los agentes SNMP se organizan en un archivo de Base de información de administración (MIB) que contiene Identificadores de objetos (OID). Cada OID identifica una variable que se puede leer o establecer utilizando SNMP.

Rapid Recovery incluye compatibilidad con la versión de SNMP 1.0.

Puede configurar el Core de Rapid Recovery como un agente SNMP. El Core puede informar sobre alertas, estado de repositorios y equipos protegidos. Un host SNMP puede leer esta información mediante una aplicación independiente denominada explorador SNMP. Puede instalar el explorador SNMP en cualquier equipo que esté accesible para el Core de Rapid Recovery a través de la red.

Para garantizar que el explorador SNMP puede recibir las notificaciones de eventos del Core SNMP, compruebe que las opciones de notificación de un grupo de notificación están correctamente configuradas para notificar mediante captura de SNMP.

NOTE: Puede utilizar el grupo predeterminado o crear un grupo de notificación personalizada. El proceso es el mismo.

Abra el grupo de notificación, seleccione la pestaña **Opciones de notificación** y compruebe que la opción **Notificar por captura de SNMP** está activada. El grupo de notificación especifica el número de captura 1 de manera predeterminada. Si fuera necesario, puede cambiar el número de captura para garantizar que coincide con el valor que espera el explorador SNMP.

Para obtener más información y detalles específicos sobre opciones de notificación de configuración, consulte Configuración de grupos de notificación.

De forma alternativa, puede descargar un archivo MIB del Core de Rapid Recovery. Este archivo se puede leer con un explorador SNMP de forma más sencilla para el usuario que con los datos que recibe directamente desde el Core.

Esta sección incluye los siguientes temas:

- Configuración de los valores SNMP
- Descarga del archivo MIB de SNMP

Configuración de los valores SNMP

Utilice los parámetros de SNMP para controlar la comunicación, como las alertas, entre el Rapid Recovery Core y un explorador SNMP. La configuración disponible incluye el puerto de SNMP, el puerto receptor de capturas y el nombre de host del receptor de capturas.

NOTE: Las compilaciones de Rapid Recovery anteriores a la versión 6.1 no incluyen la capacidad para cambiar la configuración **Cadena de comunidad**.

Utilice este procedimiento para configurar los parámetros de SNMP para el Core.

1. Desplácese hasta la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Configuración de SNMP**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Configuración de SNMP.

     Se muestran los ajustes de Configuración de SNMP.
3. Modifique la configuración de SNMP según se describe en la tabla siguiente.

Tabla 21. Información de configuración de la conexión SNMP

Cuadro de texto	Descripción
Gestionar solicitud entrante	Para permitir que el Core reconozca los protocolos SNMP entrantes, seleccione esta opción. Para bloquear los protocolos SNMP entrantes, borre la opción. **NOTE:** La selección de la opción para gestionar las solicitudes entrantes permite editar la configuración de la cadena de comunidad.
Cadena de comunidad	Introduzca un nombre para la comunidad. **NOTE:** Solo puede cambiar esta configuración si la configuración **Gestionar solicitud entrante** se establece en **Sí**.
Puerto entrante	Especifique un número de puerto para la conexión SNMP. **NOTE:** El valor predeterminado es 8161.
Enviar capturas	Para permitir que se envíen alertas (capturas) mediante el protocolo SNMP, seleccione esta opción. Para bloquear las alertas, borre la opción.
Puerto de receptor de captura	Introduzca un número de puerto para la alerta entrante. El valor predeterminado es 162.
Nombre de host de receptor de captura	Introduzca un nombre de host para la conexión SNMP. **NOTE:** El nombre de host predeterminado es localhost.

4. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

Descarga del archivo MIB de SNMP

El protocolo Simple Network Management Protocol se utiliza para controlar si existen condiciones que requieran su atención en los dispositivos de una red. Cuando el Core de Rapid Recovery se establece como un agente SNMP, el Core comunica información como alertas, el estado del repositorio y los equipos protegidos. Esta información la puede leer un host SNMP utilizando una aplicación autónoma denominada explorador SNMP.

Los objetos de datos administrados por los agentes SNMP se organizan en un archivo Base de información de administración (MIB) que contiene Identificadores de objetos (OID). Cada OID identifica una variable que se puede leer o establecer utilizando SNMP.

Puede descargar un archivo MIB del Core de Rapid Recovery. Un explorador SNMP puede entonces leer este archivo, llamado quest-rapid-recovery.mib, de forma más sencilla para el usuario que con los datos que recibe directamente desde el Core.

Siga este procedimiento para descargar el archivo MIB de SNMP del Core de Rapid Recovery.

1. Desplácese hasta la Core Console de Rapid Recovery.
2. En la barra de iconos, haga clic en ••• (Más) y, a continuación, haga clic en **Descargas**.

Aparece la página **Descargas**.

3. Desplácese hacia abajo al panel Otros archivos.
4. Para descargar el archivo MIB, haga clic en el vínculo de descarga **Archivo MIB de SNMP**.

   Aparecen los valores de Configuración de SNMP.

5. En el cuadro de diálogo **Apertura de quest-rapid-recovery-core.mib**, realice una de las siguientes acciones:

   - Para abrir el archivo de registro, seleccione **Abrir con y**, a continuación, elija una aplicación de explorador SNMP para ver el archivo de texto MIB, y por último haga clic en **Aceptar**.

     Se abre el archivo MIB en la aplicación seleccionada.

   - Para guardar el archivo localmente, seleccione **Guardar archivo** y haga clic en **Aceptar**.

     El archivo quest-rapid-recovery-core.mib se guardará en su carpeta Descargas. Puede abrirse mediante un explorador SNMP o un editor de texto.

Configuración de los valores de vSphere

VMware vSphere es una suite de software de virtualización desde la que puede administrar las máquinas virtuales ESXi o vCenter Server. Si utiliza vSphere, no es necesario cargar el software Rapid Recovery Agent en máquinas virtuales individuales para protegerlas. Esto se denomina la función de protección sin agente, que solo se aplica en máquinas virtuales.

Utilice este procedimiento para configurar los parámetros de vSphere para el Core.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:

   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **vSphere**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado vSphere.

3. Modifique la configuración de vSphere según se describe en la tabla siguiente.

Tabla 22. Información de configuración de VSphere Core

Elemento de la IU	Tipo de módulo de la IU	Descripción
Duración de la conexión	Cuadro de rotación	Establece la duración antes de que se agote el tiempo de espera para la conexión con el servidor ESXi. Utiliza el formato HH:MM:SS. **NOTE:** El valor predeterminado es 00:10:00 o diez minutos.
Consolidaciones máximas simultáneas	Campo de texto	Establece el número máximo de consolidaciones simultáneas para las máquinas virtuales protegidas. **NOTE:** El valor predeterminado es 0.
Número máximo de reintentos	Campo de texto	Establece el número máximo de intentos para la conexión a un disco virtual o a las operaciones de lectura y escritura antes de que se agote el tiempo de espera.

Elemento de la IU	Tipo de módulo de la IU	Descripción
		NOTE: El valor predeterminado es 10.
Permitir restauración en paralelo	Boolean (casilla de verificación)	Cuando esta opción está seleccionada, se activa una restauración paralela para una máquina virtual sin agente. Cuando esta opción está demarcada, la función está desactivada. **NOTE:** El valor predeterminado es No (desmarcada).

4. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

Administración de la configuración del proxy VMware

La configuración del proxy VMWare está diseñada para los equipos VMWare ESXi que requieren API del Kit de desarrollo de disco virtual (VDDK) para acceder al almacenamiento del disco de VMware. Rapid Recovery trata este acceso y los posibles tiempos de espera asociados con este mediante un proceso llamado el proxy de VMWare. Este servicio se instala automáticamente junto con el Rapid Recovery Core y solo se ejecuta cuando es necesario. La página Configuración del Core permite ajustar la configuración de tiempo de espera del servicio cuando lo vea apropiado.

1. En la barra de iconos de la Rapid Recovery Core Console, haga clic en ⚙ (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Proxy VMware**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado **Proxy VMware**.
2. En **Proxy VMware**, modifique la configuración de tiempo de espera que se describe en la tabla siguiente.

Tabla 23. Información de la configuración del proxy VMware

Elemento de la IU	Descripción
Tiempo de espera de la conexión	La cantidad máxima de tiempo que debe transcurrir antes de que el proxy VMware pare de intentar conectarse al almacenamiento del disco de VMware, expresada como hh:mm:ss. **NOTE:** El valor predeterminado es 5 minutos (00:05:00).
Tiempo de espera de lectura y escritura	La cantidad máxima de tiempo que debe transcurrir antes de que el proxy VMware pare de intentar leer o escribir en el almacenamiento del disco de VMware, expresada como hh:mm:ss. **NOTE:** El valor predeterminado es 5 minutos (00:05:00).

Elemento de la IU	Descripción
Tiempo de espera de inicio del servicio	La cantidad máxima de tiempo que debe transcurrir antes de que Rapid Recovery deba parar de intentar iniciar el servicio del proxy VMware, expresada como hh:mm:ss. **NOTE:** El valor predeterminado es 5 minutos (00:05:00).
Tiempo de espera de detención del servicio	La cantidad máxima de tiempo que debe transcurrir antes de que Rapid Recovery deba parar de intentar detener el servicio del proxy VMware, expresada como hh:mm:ss. **NOTE:** El valor predeterminado es 1 minuto (00:01:00).

3. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en la marca de verificación para guardar los cambios y salir del modo edición, o haga clic en **X** para salir del modo sin guardar.

Configuración de valores de vFoglight

Si proporciona información sobre vFoglight en la configuración del Core, la Core Console muestra una URL de vFoglight para cada máquina virtual en su página Resumen. Haciendo clic en esta URL se abre información sobre la máquina virtual en vFogLight.

Complete los siguientes pasos para integrar su servidor vFoglight con el servidor de Rapid Recovery Core.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Configuración de vFoglight**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado vFoglight.

     Se muestran los ajustes de configuración de vFoglight.
3. Modifique la configuración de vFoglight según se describe en la tabla siguiente.

Tabla 24. Información de configuración de la conexión de vFoglight

Cuadro de texto	Descripción
Uso de https	Habilita o deshabilita el protocolo seguro de transferencia de hipertexto (HTTPS). El valor predeterminado es HTTPS seguro.
Host	Introduzca un nombre de host o una dirección IP de su servidor vFoglight. Para obtener detalles, consulte a su administrador del servidor vFoglight.
Puerto	Especifique el puerto apropiado. El puerto predeterminado es 32896. Para obtener detalles, consulte a su administrador del servidor vFoglight.

Cuadro de texto	Descripción
Token de autenticación	Proporciona la autenticación adecuada para permitir que el Core se comunique con su servidor vFoglight. Para obtener detalles, consulte a su administrador del servidor vFoglight.

4. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

Herramientas de nivel del Core

Además de configurar las opciones del Core, también puede utilizar las herramientas a nivel del Core que se describen en la tabla siguiente.

Tabla 25. Otras herramientas a nivel del Core

Elemento de la IU	Descripción
Información del sistema	Rapid Recovery permite ver información sobre el Rapid Recovery Core, que incluye información del sistema, volúmenes locales y montados, así como conexiones del motor de Replay. Para obtener más datos sobre la información que se muestra en la página Información del sistema, consulte Funcionamiento de la información del sistema para el Core. Para obtener más información sobre cómo acceder a la información del sistema, consulte Visualización de la información del sistema del Core.
Descarga de archivos de registro del Core	La información sobre diversas actividades del Rapid Recovery Core se guarda en el archivo de registro del Core. Para diagnosticar posibles problemas, puede descargar y ver los registros de su Rapid Recovery Core. Para obtener más información sobre cómo acceder y ver los registros del Core, consulte Acceso a los registros del Core. Cada equipo protegido también guarda un registro de actividad. Este registro se puede cargar en el Core si selecciona el trabajo nocturno denominado Descargando los registros desde los equipos protegidos. Para obtener más información acerca de los trabajos nocturnos, consulte Comprensión de los trabajos nocturnos. Para obtener más información sobre cómo configurar los parámetros de este trabajo nocturno para el Core, consulte Configuración de trabajos nocturnos para el Core. Para obtener más información sobre cómo configurar los trabajos nocturnos para equipos protegidos específicos, consulte Personalización de trabajos nocturnos para un equipo protegido.

Funcionamiento de la información del sistema para el Core

Rapid Recovery le permite ver información sobre el Rapid Recovery Core. Puede ver la información general, información sobre volúmenes locales e información sobre volúmenes montados.

En el panel **General**, puede ver la información como se describe en la tabla siguiente.

Tabla 26. Información del sistema

Elemento de la IU	Descripción
Nombre de host	El nombre del equipo de su Rapid Recovery Core.
Versión del sistema operativo	La versión del sistema operativo instalado en el Rapid Recovery Core.
Arquitectura del sistema operativo	Enumera la estructura y el diseño subyacentes del equipo que aloja su Rapid Recovery Core. También puede incluir el chipset y el sistema de 64 bits. El Rapid Recovery Core solo es compatible con sistemas de 64 bits.
Memoria (física)	Enumera la cantidad de memoria de acceso aleatorio (RAM) instalada en el equipo del Core.
Nombre para mostrar	Muestra el nombre para mostrar del Core, que es configurable (consulte Configuración de los parámetros generales del Core).
Nombre de dominio totalmente cualificado	Muestra el nombre de dominio totalmente cualificado del equipo del Core.
Ubicación de la memoria caché de metadatos	Muestra la ruta de acceso de la ubicación de la caché de metadatos. Para obtener más información, consulte Funcionamiento de la caché de desduplicación y las ubicaciones de almacenamiento.
Ubicación de la memoria caché principal	Muestra la ruta de acceso de la ubicación de la caché de desduplicación principal. Para obtener más información, consulte Funcionamiento de la caché de desduplicación y las ubicaciones de almacenamiento.
Ubicación de la memoria caché secundaria	Muestra la ruta de acceso de la ubicación de la caché de desduplicación secundaria. Para obtener más información, consulte Funcionamiento de la caché de desduplicación y las ubicaciones de almacenamiento.

El panel **Volúmenes** incluye la siguiente información sobre los volúmenes de almacenamiento para el equipo del Core: Nombre, ID de dispositivo, sistema de archivos, capacidad bruta, capacidad formateada, capacidad utilizada y puntos de montaje.

El panel **Conexiones del motor de reproducción** muestra información sobre los puntos de recuperación montados en estos momentos. Puede ver el Extremo local, el Extremo remoto, el Id. de Agent de la imagen montada, el Id. de imagen montada y el Nombre para mostrar de la imagen montada. Puede ver si el montaje es escribible, ver el usuario autenticado, los bytes leídos y los bytes escritos.

Puede desmontar puntos de recuperación que estén montados localmente en un Core desde la página Montajes. Para obtener más información sobre el desmontaje de los puntos de recuperación, consulte Desmontaje de puntos de recuperación.

Para obtener más información, consulte Visualización de la información del sistema del Core.

Visualización de la información del sistema del Core

La información del sistema del Core incluye información general, información sobre volúmenes locales e información sobre los volúmenes montados en el Core. Para obtener una descripción detallada de la información disponible en esta página, consulte Funcionamiento de la información del sistema para el Core.

Complete los pasos de este procedimiento para ver la información del sistema del Core.

NOTE: También puede ver la información del sistema de un equipo protegido específico. Para obtener más información, consulte Visualización de la información del sistema de un equipo protegido.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más) y, a continuación, haga clic en **Información del sistema**.

   Aparece la página **Información del sistema**.

Acceso a los registros del Core

La información sobre diversas actividades del Core de Rapid Recovery se guarda en el archivo de registro del Core. Este archivo, **AppRecovery.log**, se almacena de forma predeterminada en la ruta `C:\ProgramData\AppRecovery\Logs`.

NOTE: Dependiendo de su configuración, es posible que el directorio de AppRecovery no esté visible en el Core de Rapid Recovery. Para ver este directorio es posible que tenga que cambiar el panel de control de opciones de carpeta para que muestre archivos, carpetas y unidades ocultos. Si esta configuración incluye la opción de ocultar extensiones de tipos de archivos conocidos, es posible que el archivo de registro del Core aparezca como AppRecovery sin la extensión `.log`.

El registro del Core incluye información sobre los trabajos completados del Core, fallos de conexión, los resultados de intentos por parte del Core para ponerse en contacto con el portal de licencias y otra información. Cada declaración almacenada en el archivo de registro del Core va precedida por uno de los cuatro calificadores: INFORMACIÓN, DEPURAR, ERROR y ADVERTENCIA. Estos calificadores ayudan a organizar por categorías la naturaleza de la información almacenada en el registro a la hora de diagnosticar un problema.

NOTE: De igual manera, un archivo de registro también se almacena en cada equipo protegido con información relativa a sus intentos de comunicarse con el Core. Para obtener más información acerca de los registros de equipos, consulte Descarga y visualización del archivo de registro de un equipo protegido.

La capacidad de acceder a registros puede ser útil al solucionar un problema o trabajar con el soporte técnico de Quest Rapid Recovery. Para acceder a los registros, consulte los siguientes procedimientos:

See also: Descarga y visualización del archivo de registro del Core
See also: Descarga y visualización del archivo de registro de un equipo protegido

Descarga y visualización del archivo de registro del Core

Si se produce algún error o problema con el Core, puede descargar los registros del Core para verlos o consultarlos con su representante de Quest Support.

1. En la Rapid Recovery Core Console, en la barra de iconos, haga clic en  (Más) y, a continuación, haga clic en  **Registro del Core**.
2. En la página **Descargar registro del Core**, haga clic en  **Haga clic aquí para iniciar la descarga**.
3. Si se le solicita que abra o guarde el archivo `Core AppRecovery.log`, haga clic en **Guardar**.
4. Si observa el cuadro de diálogo **Apertura de Core AppRecovery.log**, realice una de las siguientes acciones:
   - Para abrir el archivo de registro, seleccione **Abrir con** y, a continuación, seleccione una aplicación (como Bloc de notas) para visualizar el archivo de registro basado en texto y haga clic en **Aceptar**.

     Se abre el archivo **Core AppRecovery.log** en la aplicación seleccionada.
   - Para guardar el archivo localmente, seleccione **Guardar archivo** y haga clic en **Aceptar**.

     El archivo **Core AppRecovery.log** se guardará en su carpeta **Descargas**. Se puede abrir con un editor de texto.

See also: Descarga y visualización del archivo de registro del Core
See also: Descarga y visualización del archivo de registro de un equipo protegido

Repositorios

En esta sección se describe cómo trabajar con repositorios compatibles con Rapid Recovery. Se abordan las características y atributos del tipo de repositorio principal (Administrador de volúmenes de desduplicación o DVM) y del tipo secundario (un repositorio por capas). Describe los tipos de desduplicación que se utilizan en Rapid Recovery y cómo se utilizan las desduplicaciones en la aplicación. A continuación, en esta sección se describe cómo administrar DVM y repositorios por capas, incluido crear un repositorio, ver y editar sus detalles y eliminar un repositorio. También puede conocer cómo se abre un repositorio de un Core en otro Core.

Los temas incluyen:

- Comprensión de los repositorios
- Desduplicación en Rapid Recovery
- Administración de un repositorio DVM
- Administración de un repositorio por capas
- Comprobación de un repositorio
- Cambio de la configuración de un repositorio
- Conexión a un repositorio existente
- Ver o modificar los detalles de repositorio
- Eliminación de un repositorio

Comprensión de los repositorios

Un repositorio es una estructura de datos que se utiliza para almacenar y administrar datos de Rapid Recovery. Las instantáneas de copia de seguridad se guardan en un repositorio en forma de puntos de recuperación. Para poder proteger máquinas, replicar o restaurar datos en Rapid Recovery, necesita al menos un repositorio.

Un administrador de Rapid Recovery crea explícitamente un repositorio dentro de una ubicación de almacenamiento (un volumen de disco) asociado con un Core determinado. Puede crear un repositorio desde la IU o desde la línea de comandos. Desde la Rapid Recovery Core Console, puede crear un nuevo repositorio DVM primario o un repositorio por capas secundario. Al proteger un equipo, también puede definir un repositorio DVM como un paso avanzado en flujo de trabajo del asistente.

Desde la página **Repositorios** de la Rapid Recovery Core Console puede crear un nuevo repositorio o conectar el Core a un repositorio existente (utilizado por otro Core en ese momento). En general, puede ver los detalles de un repositorio, la configuración del repositorio, realizar una comprobación del mismo o eliminarlo. Los repositorios DVM le permiten agregar una ubicación de almacenamiento u optimizar un repositorio. Los repositorios por capas le permiten desconectarse del equipo que aloja el repositorio. Para obtener más información acerca de la administración de un tipo de repositorio específico, consulte Administración de un repositorio DVM o Administración de un repositorio por capas, respectivamente.

Un repositorio se puede encontrar en diferentes tecnologías de almacenamiento, incluidos dispositivos de almacenamiento conectados directamente (DAS), de red de área de almacenamiento (SAN) o de almacenamiento conectado a la red (NAS).

NOTE: Almacene los repositorios de Rapid Recovery en dispositivos de almacenamiento principales. La velocidad para el volumen de almacenamiento es el factor más crítico. No se admiten dispositivos de almacenamiento de archivado, como Data Domain, debido a limitaciones de rendimiento. De forma similar, los repositorios no deben almacenarse en filtros NAS que se conectan a la nube, puesto que estos dispositivos suelen tener limitaciones de rendimiento cuando se utilizan como almacenamiento primario.

DAS ofrece el más alto ancho de banda de datos y la velocidad de acceso más rápida, y es fácil de implementar. Para obtener resultados óptimos, utilice DAS con el almacenamiento 6 de la Matriz redundante de discos independientes (RAID). Para obtener más información, consulte el artículo 118153 de la base de conocimientos de Quest, Opciones de repositorio: Almacenamiento conectado directamente, Red de área de almacenamiento o Almacenamiento conectado a la red.

La ubicación de almacenamiento para cualquier repositorio DVM principal debe estar siempre en el subdirectorio que especifique (por ejemplo, `E:\Repository`), nunca en la raíz de un volumen (por ejemplo, `E:\`). Al crear un repositorio por capas, no puede especificar un directorio, pero sí un contenedor. Puede seleccionar el contenedor predeterminado o crear uno nuevo.

Los repositorios DVM se utilizan para el almacenamiento principal, en el que el Core guarda los puntos de recuperación directamente en los dispositivos de almacenamiento especificados.

Los repositorios por capas se utilizan para el almacenamiento secundario. En este modelo, los puntos de recuperación se reubican desde un repositorio DVM principal a un volumen de almacenamiento secundario que especifique. Una vez copiados y verificados, los puntos de recuperación se eliminan del repositorio principal, dejando espacio para más datos de copia de seguridad.

NOTE: Para versión 6.2, los repositorios por capas solo son compatibles en los servidores de desduplicación y de copia de seguridad de la serie Quest DR.

Puede utilizar cualquier combinación de repositorios DVM o por capas definida para un único Core. Si se han agregado los dos tipos de repositorios al Core, la página **Repositorios** muestra un panel independiente donde se enumera cada tipo de repositorio por separado. Los repositorios principales aparecen primero, seguidos de los repositorios por capas (secundarios).

En la siguiente sección se describen las características de cada tipo de repositorio compatible con Rapid Recovery.

Repositorio DVM. El formato de este repositorio heredado utiliza el Administrador de volúmenes de desduplicación (DVM).

- DVM es una tecnología de repositorio principal utilizada para el almacenamiento de los puntos de recuperación.
- Los repositorios DVM se crean y administran desde la Rapid Recovery Core Console.
- Los repositorios DVM admiten varios volúmenes, hasta 255 repositorios en un único Core.
- Puede especificar el tamaño de un repositorio DVM tras la creación y puede agregar extensiones más tarde.
- Puede crear repositorios DVM en máquinas que cuentan únicamente con sistemas operativos Windows.
- El volumen de repositorio DVM puede ser local (en el almacenamiento conectado al servidor del Core), o en una ubicación de almacenamiento en una ubicación compartida del Sistema de archivos de Internet comunes (CIFS).
- Puede utilizar este tipo de repositorio al actualizar las instalaciones de AppAssure existentes, y al utilizar las instalaciones de Rapid Recovery nuevas.
- Los repositorios DVM pueden distribuirse entre diferentes tecnologías de almacenamiento.
- Los tipos de almacenamiento admitidos incluyen la Red de área de almacenamiento (SAN), el Almacenamiento conectado directamente (DAS) o el Almacenamiento conectado a la red (NAS)
- Requiere 8 GB de RAM, preferiblemente memoria de Verificación y corrección de errores (ECC)
- Requiere un procesador de cuatro núcleos en el equipo del Core
- Admite varios repositorios DVM por host
- No es obligatorio ningún servicio adicional; el repositorio DVM utiliza servicios de Core nativos para la comunicación con el Core y para eventos de seguimiento
- Cada repositorio DVM admite hasta 4096 extensiones adicionales (también llamadas ubicaciones de almacenamiento)
- Tamaño fijo; en el repositorio DVM es obligatorio que especifique el tamaño del repositorio en un volumen. El tamaño que especifique no puede superar el tamaño del volumen. Cada volumen que define como una ubicación de almacenamiento debe tener un mínimo de 1 GB de espacio libre disponible en él.
- La ubicación del almacenamiento de un repositorio puede ser un disco simple o dinámico, con la velocidad como el factor más importante
- Puede utilizar las claves de cifrado estándar creadas y administradas en la Core Console (Cifrado basado en Core)
- Desduplica los datos a lo largo de todo el repositorio (o a lo largo de dominios de cifrado dentro de cada repositorio, si se utilizan las claves de cifrado)
- Utiliza una caché de desduplicación de DVM dedicada y redimensionable, con una ubicación de almacenamiento completamente configurable en la configuración del Core
- Optimizado para escribir los datos, almacenar los datos de la instantánea en un repositorio local para el Core, con todos los datos procesados a través del Core
- No se puede cambiar el nombre tras la creación
- Los nuevos repositorios de este tipo se pueden crear con las API de REST, la utilidad Command Line Management de Rapid Recovery (cmdutil.exe) o los cmdlet de Windows PowerShell

Cuando se crea un repositorio DVM, el Rapid Recovery Core preasigna el espacio de almacenamiento obligatorio para los datos y los metadatos en la ubicación especificada. El tamaño del repositorio DVM mínimo es de 1 GB, que por razones prácticas es demasiado pequeño, excepto para la prueba.

Como la desduplicación DVM requiere una caché secundaria y primaria, asegúrese de que el espacio de almacenamiento que reserva es dos veces el tamaño de la caché de desduplicación. Por ejemplo, si tiene 1,5 GB reservados en la configuración de la caché de desduplicación de DVM en el Core, reserve 3GB en el volumen

de la caché. La ruta de acceso de la instalación predeterminada para la caché se encuentra en la unidad C. Para obtener más información, consulte Funcionamiento de la caché de desduplicación y las ubicaciones de almacenamiento.

Repositorio por capas. Los repositorios por capas se introdujeron en Rapid Recovery versión 6.1.

- La tecnología de repositorios por capas solo se utiliza para almacenamiento secundario.
- Los puntos de recuperación existentes (con 1 semana o más antiguos) que aún no se han designado para archivar se pueden reubicar desde el repositorio DVM de Rapid Recovery principal. Esta característica se habilita a través del periodo de retención.
- Los repositorios por capas se crean y administran desde la Rapid Recovery Core Console.
- Actualmente, los repositorios por capas solo son compatibles en los servidores de desduplicación y de copia de seguridad de la serie Quest DR versión 4.0.
- Los puntos de recuperación asociados al almacenamiento secundario continúan estando protegidos con el cifrado y están sujetos a la consolidación. El Core sigue siendo el encargado de controlar la directiva de retención y la consolidación en la nueva ubicación.
- Dado que la consolidación continúa de forma nocturna, los puntos de recuperación se asocian constantemente. Al visualizar los puntos de recuperación por equipo protegido, aquellos puntos asociados aparecen marcados con un icono de la base de datos dorado .

En cuanto a la interoperabilidad, los puntos de recuperación guardados en repositorios DVM principales se pueden asociar a un repositorio secundario. Debido a que los servidores DR compatibles con los repositorios por capas utilizan un sistema operativo CentOS, no se admiten los repositorios DVM en ellos.

Uso de servidores físicos o virtuales para almacenamiento de repositorios

Si utiliza Rapid Recovery en un dispositivo de copia de seguridad y recuperación Quest DL4300, puede crear repositorios DVM y por capas. En la versión 6.2, el repositorio por capas debe estar almacenado en un dispositivo de copia de seguridad y desduplicación DR con un sistema operativo 4.0.

Los repositorios por capas administrados en los dispositivos DL utilizan licencias Capacity. Por tanto, mientras es posible asociar puntos de recuperación de su repositorio DVM relacionados con un dispositivo DL a un almacenamiento secundario en un dispositivo DR, el espacio ocupado para esos puntos de recuperación va en detrimento de la capacidad de DL. Por esta razón, resulta más rentable archivar puntos de recuperación de un dispositivo DL y almacenar los archivos en el dispositivo DR.

Ningún otro dispositivo de almacenamiento, copia de seguridad, recuperación o desduplicación se ha probado de manera explícita para su uso con Rapid Recovery. Proceda bajo su propio riesgo.

El Virtual DR2000v se puede utilizar para un repositorio por capas, siempre que tenga instalados los servicios RDS correctos y se ejecute el sistema operativo 4.0. Otros dispositivos virtuales aún no son compatibles con el Core Rapid Recovery versión 6.2.

See also: Administración de un repositorio DVM
See also: Administración de un repositorio por capas

Desduplicación en Rapid Recovery

La desduplicación es una técnica de compresión de datos que reduce tanto los requisitos de almacenamiento como los de carga de la red. El proceso implica almacenar físicamente bloques exclusivos de datos solo una vez en el disco. En Rapid Recovery, cuando cualquier bloque de datos exclusivo se produce por segunda vez en un repositorio principal, en lugar de almacenar los datos de nuevo, el Core almacena una referencia virtual de los datos en el repositorio.

La desduplicación se produce en las instantáneas de copia de seguridad capturadas por el Rapid Recovery Core..

- La información de las copias de seguridad se desduplica en un repositorio único. No se puede desduplicar en varios repositorios .
- Los repositorios DVM utilizan un cifrado basado en el destino. Por motivos de seguridad, el cifrado se realiza antes que la desduplicación. La desduplicación se limita a los datos protegidos con una única clave de cifrado.

Si se llena la caché de desduplicación, la desduplicación no es óptima. En este caso, la desduplicación se puede ejecutar como un proceso posterior (también conocido como reclamación de bloques). Después de aumentar el tamaño de la caché de desduplicación, ejecute el trabajo de optimización de repositorio. Desde ese momento, el Core reclamará bloques, lo que proporciona más espacio en su repositorio.

Para obtener más información sobre el trabajo de optimización de repositorio, consulte Acerca de la optimización del repositorio DVM. Para obtener más información sobre la realización de esta tarea, consulte Optimización de un repositorio DVM.

Por lo tanto, Rapid Recovery aprovecha todos los tipos de desduplicación que se describen aquí: desduplicación basada en destino, desduplicación en línea y desduplicación posprocesamiento.

Para obtener más información acerca de dónde se almacenan las referencias a bloques exclusivos en repositorios DVM, consulte Funcionamiento de la caché de desduplicación y las ubicaciones de almacenamiento. Para obtener información sobre la configuración de la memoria caché de desduplicación de DVM, consulte Configuración de los valores de caché de la desduplicación de DVM.

Administración de un repositorio DVM

La administración de un repositorio DVM implica las siguientes operaciones:

1. **Creación de un repositorio DVM**. Antes de crear un repositorio, tenga en cuenta el tipo de tecnología apropiado.

   Para obtener información acerca de los distintos tipos de repositorios, consulte Comprensión de los repositorios.
   Para obtener más información sobre cómo crear un repositorio DVM, consulte Creación de un repositorio DVM.
2. **Conexión a un repositorio**. Para obtener más información sobre la conexión a un repositorio existente actualmente administrado por otro Core, consulte Conexión a un repositorio existente.
3. **Adición de una nueva ubicación de almacenamiento.** Para obtener más información sobre cómo agregar una nueva ubicación de almacenamiento a un repositorio DVM, consulte Cómo agregar una ubicación de almacenamiento a un repositorio DVM existente.
4. **Comprobación de un repositorio.** Para obtener más información sobre cómo comprobar un repositorio DVM, consulte Comprobación de un repositorio.
5. **Modificación de la configuración del repositorio.** Para obtener más información sobre la visualización de los detalles del repositorio o la modificación de la configuración de un repositorio, consulte Ver o modificar los detalles de repositorio
6. **Ejecución de la optimización del repositorio DVM**. Para obtener más información sobre el trabajo de optimización de repositorio, consulte Acerca de la optimización del repositorio DVM. Para obtener información sobre los pasos para optimizar un repositorio DVM existente, consulte Optimización de un repositorio DVM.
7. **Eliminación de un repositorio**. Para obtener más información sobre cómo eliminar un repositorio, consulte Eliminación de un repositorio.

Para obtener información sobre la administración de un repositorio por capas, consulte Administración de un repositorio por capas.

Creación de un repositorio DVM

En este proceso se describe cómo crear un repositorio en el Core con la tecnología de repositorios Deduplication Volume Manager (DVM).

- Debe tener acceso administrativo al equipo en el que quiere crear un repositorio DVM.
- Este tipo de repositorio requiere un mínimo de 1 GB de espacio de almacenamiento disponible en el volumen que defina como la ubicación de almacenamiento.
- La ubicación de almacenamiento de un repositorio DVM debe estar en una unidad local conectada al servidor del Core o en un recurso compartido CIFS.
- El servidor del Core puede ser cualquier dispositivo DL Series (incluido el DL1000) o cualquier servidor de Windows basado en software que cumpla los requisitos del sistema.

NOTE: Los repositorios DVM no son compatibles con los servidores de desduplicación y de copia de seguridad del disco de la serie DR. Los servidores DR utilizan su propia desduplicación. Esta desduplicación no es compatible con la desduplicación que el Rapid Recovery Core aplica a un repositorio DVM.

Si desea crear un repositorio por capas para almacenamiento secundario de puntos de recuperación guardados originalmente en su repositorio DVM, consulte el tema Creación de un repositorio por capas.

Complete los pasos siguientes para crear un repositorio DVM.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Repositorios**.

   Aparecerá la página **Repositorios**.
3. En la parte superior de la página, en el título de página Repositorios, haga clic en la flecha desplegable junto a **Crear** y, a continuación, seleccione **Repositorio DVM**.

   Se mostrará el cuadro de diálogo **Agregar repositorio nuevo**.
4. Introduzca la información según se describe en la tabla siguiente.

Tabla 27. Parámetros de Agregar repositorio nuevo

Cuadro de texto	Descripción
Nombre del repositorio	Introduzca el nombre para mostrar del repositorio. De manera predeterminada, este cuadro de texto incluye el término Repositorio y un número, que se corresponde con el número de repositorios de este Core. Por ejemplo, si se trata del primer repositorio, el nombre predeterminado es Repositorio 1. Cambie el nombre según sea necesario. Los nombres del repositorio contienen entre 1 y 40 caracteres alfanuméricos, incluidos los espacios. No utilice caracteres prohibidos ni frases prohibidas.
Operaciones simultáneas	Defina el número de solicitudes simultáneas que desee que admita el repositorio. De manera predeterminada, el valor es 64.
Comentarios	Opcionalmente, escriba una nota descriptiva sobre este repositorio. Puede introducir hasta 254 caracteres. Por ejemplo, escriba **Repositorio DVM 2.**

5. Haga clic en **Agregar ubicación de almacenamiento** para definir la ubicación de almacenamiento o el volumen específicos para este repositorio. Utilice una unidad de almacenamiento principal rápida con suficiente espacio de almacenamiento. La ubicación de almacenamiento para un repositorio DVM

puede ser local (en almacenamiento adjunto al servidor del Core) o encontrarse en una ubicación con red compartida de un sistema de archivos de Internet comunes (CIFS). No puede especificar ambas para una única ubicación de almacenamiento.

CAUTION: Defina una carpeta específica en la raíz para la ubicación de almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice `E:\Repository\`, no `E:\`. Si el repositorio que está creando en este paso se elimina más adelante, se eliminarán todos los archivos en la ubicación de almacenamiento de su repositorio. Si define la ubicación de almacenamiento en la raíz, el resto de archivos del volumen (p. ej., `E:\`) se eliminan, lo que podría derivar en una pérdida grave de datos.

Aparecerá el cuadro de diálogo **Agregar ubicación de almacenamiento**.

6. Haga clic en **Agregar ubicación de almacenamiento** para definir la ubicación de almacenamiento o el volumen específicos para el repositorio. Este volumen debe ser la ubicación de almacenamiento principal.
7. En el área **Ubicación del almacenamiento**, especifique cómo agregar el archivo para la ubicación de almacenamiento. Puede elegir si desea agregar un volumen de almacenamiento conectado de forma local (como un almacenamiento de conexión directa, una red de área de almacenamiento o un almacenamiento conectado a la red). También podría especificar un volumen de almacenamiento en una ubicación compartida de CIFS.
   - Seleccione **Agregar el archivo en disco local** para especificar un equipo local y, a continuación, introduzca la información según se describe en la siguiente tabla.

Tabla 28. Parámetros de Disco local

Cuadro de texto	Descripción
Ruta de acceso a datos	Introduzca la ubicación para almacenar los datos protegidos. Por ejemplo, introduzca `X:\Repository\Data`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
Ruta de acceso a metadatos	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, introduzca `X:\Repository\Metadata`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.

   - O, seleccione **Agregar archivo en recurso compartido CIFS** para especificar una ubicación de uso compartido de red y, a continuación, introduzca la información según se describe en la siguiente tabla.

Tabla 29. Credenciales de recurso compartido CIFS

Cuadro de texto	Descripción
Ruta de acceso UNC	Introduzca la ruta de acceso de la ubicación de uso compartido de red. Si esta ubicación está en la raíz, defina un nombre de carpeta específico (por ejemplo, `Repository`). La ruta de acceso debe comenzar por \\. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.

Cuadro de texto	Descripción
Nombre de usuario	Especifique un nombre de usuario para el acceso a la ubicación compartida de red.
Contraseña	Especifique una contraseña para acceder a la ubicación de uso compartido de red.

8. En el área **Configuración de almacenamiento**, haga clic en **Más detalles** e introduzca los detalles para la ubicación de almacenamiento según se describen en la siguiente tabla.

Tabla 30. Detalles de configuración de almacenamiento

Cuadro de texto	Descripción
Tamaño	Defina el tamaño o la capacidad de la ubicación del archivo. El tamaño mínimo es de 1 GB. El valor predeterminado es 250 GB. Puede elegir entre las siguientes opciones: • GB • TB **NOTE:** El tamaño que especifique no puede superar el tamaño del volumen. Si la ubicación de almacenamiento es un volumen New Technology File System (NTFS) que utiliza Windows 8 o posterior, o bien Windows Server 2012 o posterior, el límite de tamaño del archivo es 256 TB. **NOTE:** Para que Rapid Recovery pueda validar el sistema operativo, el Instrumental de administración de Windows (WMI) debe estar instalado en la ubicación de almacenamiento deseada.
Política de almacenamiento en caché de escritura	La política de almacenamiento en caché de escritura controla cómo se utiliza el Administrador de caché de Windows en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: • Activado • Desactivado • Sincronización Si se establece como Activado, que es el valor predeterminado, Windows controla el almacenamiento en caché. Es adecuado para Windows 10 y para versiones de Windows Server 2012 y posteriores. **NOTE:** si se establece la política de escritura en caché en Activado, se mejora el rendimiento; no obstante, el valor recomendado es Desactivada. Si utiliza Windows Server 2008 SP2 o Windows Server 2008 R2 SP2, la configuración recomendada es Desactivado. Si se establece en Desactivado, Rapid Recovery controla el almacenamiento en caché. Si se establece en Sincronización, Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.
Bytes por sector	Especifique el número de bytes que desea que incluya cada sector. El valor predeterminado es 512.

Cuadro de texto	Descripción
Promedio de bytes por registro	Especifique el promedio del número de bytes por registro. El valor predeterminado es 8192.

9. Haga clic en **Guardar**.

   Se cierra el cuadro de diálogo **Agregar ubicación de almacenamiento** y se guarda la configuración. El cuadro de diálogo **Agregar repositorio nuevo** muestra la nueva ubicación de almacenamiento.
10. De forma opcional, repita del paso 6 al paso 9 para agregar más ubicaciones de almacenamiento para el repositorio.
11. Cuando se han definido todas las ubicaciones de almacenamiento que quiere crear para el repositorio en este momento, pulse **Agregar repositorio nuevo** en el cuadro de diálogo **Crear**.

    Se cierra el cuadro de diálogo **Agregar repositorio nuevo** y se aplican los cambios. Aparece la página **Repositorios** que muestra el repositorio agregado recientemente en la tabla de resumen Repositorios DVM.

Cómo agregar una ubicación de almacenamiento a un repositorio DVM existente

Debe existir un repositorio DVM en su repositorio para realizar este procedimiento.

Agregar una ubicación de almacenamiento a un repositorio DVM permite definir dónde se almacenará el repositorio o volumen.

Complete los pasos del procedimiento siguiente para especificar la ubicación de almacenamiento para el repositorio o volumen.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Repositorios**.

   Aparecerá la página **Repositorios**.

   Aparece el panel Repositorios DVM.
3. En la tabla de resumen de los repositorios, en la fila que representa el repositorio DVM para el que desea agregar una ubicación de almacenamiento, haga clic en el menú desplegable (Más opciones) y, a continuación, seleccione **Agregar ubicación de almacenamiento**.

   Aparece el cuadro de diálogo **Agregar ubicación de almacenamiento**.
4. Especifique cómo agregar el archivo a la ubicación de almacenamiento. Puede elegir agregar el archivo en el disco local o en un recurso compartido CIFS.
   - Seleccione **Agregar el archivo en disco local** para especificar un equipo local y, a continuación, introduzca la información según se describe en la siguiente tabla.

Tabla 31. Parámetros de Disco local

Cuadro de texto	Descripción
Ruta de acceso a datos	Introduzca la ubicación para almacenar los datos protegidos. Por ejemplo, introduzca `X:\Repository\Data`.

Cuadro de texto	Descripción
	Se aplican las mismas limitaciones en la ruta de acceso; utilice solo caracteres alfanuméricos, guiones o puntos, sin espacios ni caracteres especiales.
Ruta de acceso a metadatos	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, introduzca `X:\Repository\Metadata`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.

- O, seleccione **Agregar archivo en recurso compartido CIFS** para especificar una ubicación de uso compartido de red y, a continuación, introduzca la información según se describe en la siguiente tabla.

Tabla 32. Credenciales de recurso compartido CIFS

Cuadro de texto	Descripción
Ruta de acceso UNC	Introduzca la ruta de acceso de la ubicación de uso compartido de red. Si esta ubicación está en la raíz, defina un nombre de carpeta específico (por ejemplo, `Repository`). La ruta de acceso debe comenzar por \\. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
Nombre de usuario	Especifique un nombre de usuario para el acceso a la ubicación compartida de red.
Contraseña	Especifique una contraseña para acceder a la ubicación de uso compartido de red.

5. En el panel Configuración de almacenamiento, haga clic en **Más detalles** e introduzca los detalles para la ubicación de almacenamiento según se describen en la siguiente tabla.

Tabla 33. Detalles de ubicación de almacenamiento

Cuadro de texto	Descripción
Tamaño	Defina el tamaño o la capacidad de la ubicación del archivo. El tamaño predeterminado es de 250 GB. Puede elegir entre las siguientes opciones: • GB • TB **NOTE:** El tamaño mínimo es de 1 GB. El tamaño que especifique no puede superar el tamaño del volumen. Si la ubicación del almacenamiento es un volumen NTFS que utiliza Windows 8, 8.1 o Windows Server 2012, 2012 R2 o 2016, el límite de tamaño del archivo es 256 TB.

Cuadro de texto	Descripción
	NOTE: Para que Rapid Recovery pueda validar el sistema operativo, el Instrumental de administración de Windows (WMI) debe estar instalado en la ubicación de almacenamiento deseada.
Política de almacenamiento en caché de escritura	La política de almacenamiento en caché de escritura controla cómo se utiliza el Administrador de caché de Windows en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: • Activado • Desactivado • Sincronización Si se establece como Activado, que es el valor predeterminado, Windows controla el almacenamiento en caché. Es adecuado para Windows 10 y para versiones de Windows Server 2012 y posteriores. **NOTE:** si se establece la política de escritura en caché en Activado, se mejora el rendimiento; no obstante, el valor recomendado es Desactivada. Si utiliza Windows Server 2008 SP2 o Windows Server 2008 R2 SP2, la configuración recomendada es Desactivado. Si se establece en Desactivado, Rapid Recovery controla el almacenamiento en caché. Si se establece en Sincronización, Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.
Bytes por sector	Especifique el número de bytes que desea que incluya cada sector. El valor predeterminado es 512.
Promedio de bytes por registro	Especifique el promedio del número de bytes por registro. El valor predeterminado es 8192.

6. De manera opcional, si desea realizar el trabajo de optimización de repositorio para el repositorio seleccionado, seleccione **Ejecutar trabajo de optimización de repositorio para [nombre del repositorio]**.

   Quest recomienda que realice el trabajo de optimización de repositorio al agregar ubicaciones de almacenamiento a un repositorio existente. Este trabajo optimiza el espacio libre aplicando la desduplicación a los datos almacenados en el repositorio.

   En función de varios factores, como el tamaño del repositorio, la cantidad de datos en el repositorio, el ancho de banda de red disponible y la carga existente en la entrada y salida del sistema, realizar un trabajo de optimización de repositorio podría tardar una cantidad considerable de tiempo y consumir gran parte del ancho de banda en su entorno.

   Para obtener más información sobre el trabajo de optimización de repositorio, consulte Acerca de la optimización del repositorio DVM.

7. Haga clic en **Guardar**.

   El cuadro de diálogo se cierra y la ubicación del almacenamiento se guarda. En la tabla de resumen de los repositorios, la ubicación de almacenamiento que ha creado es visible si expande los detalles de un repositorio.

Acerca de la comprobación de la integridad de los repositorios DVM

En la AppAssure versión 5.3.6 y versiones anteriores, la replicación incluía el proceso de copiar puntos de recuperación del Core de origen al Core de destino con regularidad. Consolidación de puntos de recuperación antiguos que solo se han realizado en el Core de origen. Los puntos de recuperación más antiguos combinados se sincronizaron a diario al ejecutar el trabajo nocturno.

Empezando con la AppAssure versión 5.4.1 y en versiones actuales de Rapid Recovery Core, los usuarios pueden establecer políticas de retención dispares entre los Cores de origen y destino. Para que la replicación funcione correctamente con diferentes políticas de retención, el Core de destino debe tener la misma versión de software (o más reciente) que el Core de origen.

Los administradores pueden configurar la consolidación del Core de destino en una velocidad diferente al Core de origen. De forma similar, puede definir una política de retención personalizada para cualquier equipo replicado. Por ejemplo, puede consolidar puntos de recuperación en el Core de destino a una velocidad más rápida y con menos granularidad que en el Core de origen, con lo que se ahorra espacio. O puede consolidar puntos de recuperación de cualquier equipo replicado seleccionado a una velocidad más lenta en el Core de destino, manteniendo más granularidad, lo que puede ser útil para los fines de cumplimiento. Para obtener más información sobre el uso de la política de retención que difiere de la predeterminada en el Core, consulte Personalización de la configuración de la política de retención de un equipo protegido.

Algunos clientes han experimentado incoherencias en los puntos de recuperación que se replicaron en un Core de destino antes de la AppAssure versión 5.3.6. Para solucionar este problema, AppAssure versión 5.4.1 y posteriores incluyen un trabajo de Core que se ejecuta en el repositorio DVM. Quest recomienda realizar el trabajo Comprobación de integridad en un solo momento en cada repositorio DVM de un Core de destino replicado si el repositorio se creó antes de la versión 5.4.x (si se creó en la versión 5.3.x o anterior).

Si desea instrucciones sobre cómo realizar esta comprobación, consulte el procedimiento Realizar una comprobación de integridad en un repositorio DVM.

El trabajo de comprobación de integridad **no** estará disponible:

- En un nuevo repositorio DVM en un Core de destino creado en la AppAssure versión 5.4.1 o posterior o creado en Rapid Recovery.
- En un Core de origen.
- Si ya ha ejecutado el trabajo de comprobación de integridad (o trabajo de comprobación de repositorio) en este repositorio.
- Si no ha usado la replicación.

Si el Core se ha actualizado en cualquier momento en AppAssure 5.3.x y ha utilizado la replicación, debe ejecutar este trabajo antes de configurar las políticas de retención diferentes entre el Core de origen y el Core de destino, o configurar una política de retención personalizada en un equipo replicado.

No podrá ver o ejecutar este trabajo a menos que tenga uno o más repositorios seleccionables (creados antes de la versión 5.4.x y que todavía no se han realizado).

Al ejecutar este trabajo se verifica la integridad de todos los datos almacenados en el repositorio especificado, lo que garantiza que pueda recuperar los datos de cada instantánea o imagen base. Si la comprobación de integridad descubre cualquier problema con los datos de su repositorio, el trabajo se detiene de inmediato. Los detalles de evento de ese trabajo en el Core le indican que contacte con el Asistencia para la protección de datos de Quest para que pueda programar tiempo de trabajo con un representante de Dell para realizar procedimientos adicionales para identificar y solucionar las incoherencias de los datos.

CAUTION: La ejecución de este trabajo puede tardar un largo periodo de tiempo. La cantidad de tiempo varía en función la cantidad y el tipo de datos que haya en el repositorio y en el sistema subyacente de almacenamiento. Mientras el trabajo se está ejecutando, no es posible realizar ninguna otra transacción en ese repositorio, incluyendo las transferencias (instantáneas, copias de seguridad de imagen base y replicación), trabajos nocturnos, etc.

Puede realizar otras operaciones en otros repositorios mientras el trabajo se ejecuta.

NOTE: Este trabajo comprueba la integridad de todo el contenido de un repositorio. Si desea obtener información sobre el trabajo de `Checking repository` que puede usar para comprobar que un repositorio puede montarse y usarse, consulte Comprobación de un repositorio.

Realizar una comprobación de integridad en un repositorio DVM

Hay una comprobación de integridad disponible para repositorios DVM. La finalidad de este procedimiento es comprobar la integridad de todo el repositorio DVM. Se recomienda para Cores de destino replicados cuando actualice de AppAssure 5.3.x a la versión 5.4. Durante la ejecución de la comprobación de integridad, que puede tardar cierto tiempo, no es posible realizar otras acciones en el repositorio.

Si tiene múltiples repositorios DVM para un Core de destino, realice este proceso una vez para cada repositorio.

NOTE: Si tiene otro repositorio DVM en el Core de destino para el que ya se ha completado el trabajo de comprobación de repositorio o si crea un nuevo repositorio adicional para este Core de destino, puede realizar operaciones en ese repositorio secundario mientras el trabajo de comprobación de repositorio se ejecuta en el repositorio DVM especificado.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Repositorios**.

   Se mostrará la página **Repositorios**.
3. En la tabla de resumen de repositorios DVM, en la fila que representa el repositorio DVM que quiere comprobar, haga clic en (Más opciones) y, en el menú desplegable, seleccione **Comprobación de integridad**.

   Aparecerá un mensaje de confirmación.

   CAUTION: Antes de confirmar que desea realizar el trabajo, debe considerar con cuidado la duración de tiempo necesaria. Mientras el trabajo se está ejecutando, no es posible realizar ninguna otra transacción en ese repositorio, incluyendo las transferencias (instantáneas, copias de seguridad de imagen base y replicación), trabajos nocturnos, etc.
4. Para realizar la comprobación de integridad haga clic en **Sí** en el cuadro de diálogo **Comprobación de repositorio**.

   El cuadro de diálogo se cierra. Cualquier trabajo que esté en cola o en progreso se cancelará y comenzará el trabajo de comprobación de integridad.
5. Para supervisar el progreso del trabajo Comprobación de integridad de un repositorio, incluyendo la determinación de si es necesario realizar pasos adicionales tras la comprobación, en la barra de iconos, haga clic en (Eventos).
6. En la página **Tareas**, haga clic en **Detalles del trabajo** del trabajo para ver más información sobre el estado del trabajo.
   - Si ve un error en las tareas secundarias de este trabajo, anote el error y proporcione la información a un representante del servicio de asistencia técnica de Quest.
   - Si el trabajo Comprobación de integridad termina todas las tareas secundarias con éxito, podrá establecer una directiva de retención personalizada para este repositorio.

Acerca de la optimización del repositorio DVM

Cuando se utiliza un repositorio DVM, los datos que capture en cada instantánea se desduplican. Esta desduplicación se produce de manera gradual, a medida que las instantáneas se guardan en el repositorio. Se guarda una aparición de cada cadena de información en el repositorio. Cuando una cadena de información se desduplica, se utiliza una referencia a la cadena original en la caché de desduplicación, ahorrando así espacio en el repositorio.

Si la caché de desduplicación de DVM se llena, solo se desduplican los datos de instantánea que ya se han referenciado en la caché. A medida que se produce la desduplicación, la caché continúa la actualización con los nuevos valores exclusivos y sobrescribe los valores más antiguos de la caché. Esto da lugar a una menor desduplicación óptima.

Para obtener más información acerca de la desduplicación, consulte Funcionamiento de la caché de desduplicación y las ubicaciones de almacenamiento.

Puede elegir aumentar la caché de desduplicación de DVM antes de que se llene, lo que garantiza la continuidad de una desduplicación óptima de los datos del repositorio. Para obtener más información, consulte Configuración de los valores de caché de la desduplicación de DVM.

También puede aumentar la caché de desduplicación después de que se llene. Si desea reclamar espacio en el repositorio después de aumentar la caché, puede optimizar el repositorio. Esta acción fuerza una comparación de los datos en sus instantáneas con la información de la caché de desduplicación. Si hubiera cadenas repetidas en el repositorio, los datos se sustituyen con referencias a los datos, lo que ahorra espacio de almacenamiento en el repositorio. Este proceso se denomina a veces como desduplicación sin conexión, ya que el proceso de desduplicación se produce bajo solicitud, en lugar de gradualmente a medida que se transfieren los datos de instantánea.

El proceso de optimización hace un uso intensivo del procesador. La cantidad de tiempo que tarda en ejecutarse este trabajo depende de varios factores. Entre estos factores se incluye el tamaño del repositorio, la cantidad de datos en el repositorio, el ancho de red disponible y la carga existente en la entrada y salida del sistema. Cuantos más datos haya en el repositorio, más tardará el trabajo en ejecutarse.

Las siguientes acciones se sustituyen o cancelan cuando se produce un trabajo de optimización de repositorio.

- Trabajo de eliminación de todos los puntos de recuperación
- Trabajo de eliminación de cadena de puntos de recuperación
- Trabajo de mantenimiento de repositorio
- Trabajo base de eliminación de puntos de recuperación
- Trabajo de optimización de repositorio

Para obtener información sobre los pasos del proceso de optimización de un repositorio DVM existente, consulte Optimización de un repositorio DVM.

Puede interrumpir el trabajo de optimización de repositorio durante un tiempo limitado si es necesario. Para obtener más información, consulte Interrupción o reanudación de la optimización de un repositorio DVM.

Optimización de un repositorio DVM

Debe tener un repositorio DVM en el Core para realizar este procedimiento.

Puede realizar desduplicación sin conexión de datos guardados en un repositorio DVM existente. Esto se consigue mediante el inicio del Trabajo de optimización de repositorio.

NOTE: Quest recomienda que realice el trabajo Optimizar repositorio solo después de aumentar el tamaño de la caché de desduplicación. Esta acción le permite recuperar espacio de repositorio y utilizar de forma más eficaz la caché de desduplicación de DVM.

Lleve a cabo los pasos de este procedimiento para optimizar un repositorio DVM.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Repositorios**.

   Aparecerá la página **Repositorios**.
3. En el panel Repositorios DVM, en la fila que representa el repositorio que quiere actualizar, haga clic en (Más opciones) y, a continuación, seleccione **Optimizar**.

   Aparece un mensaje de aviso que le pide que confirme la optimización.
4. Haga clic en confirmar la optimización.

   El trabajo de optimización tiene prioridad sobre la mayoría de los otros trabajos. Si es necesario, puede interrumpir un trabajo de optimización en progreso. Para obtener más información sobre la interrupción o reanudación de este trabajo, consulte Interrupción o reanudación de la optimización de un repositorio DVM.

Interrupción o reanudación de la optimización de un repositorio DVM

Esta tarea requiere un repositorio DVM existente en su Core, con un trabajo de optimización de repositorio en ejecución.

Al iniciar el Trabajo de optimización de repositorio, el repositorio DVM seleccionado se desduplica. Esta optimización de la desduplicación es un trabajo intensivo del procesador para ahorrar espacio en el repositorio. Para obtener más información, consulte Acerca de la optimización del repositorio DVM.

Una vez que este trabajo se ha iniciado, puede interrumpir el trabajo mediante el procedimiento siguiente. Esto pausa la desduplicación. Si ya ha interrumpido una optimización, puede reanudar el proceso mediante este procedimiento.

NOTE: Este procedimiento se aplica solo a repositorios DVM y solo cuando el trabajo de optimización de repositorio se ha iniciado.

Complete los pasos de este procedimiento para interrumpir o reanudar un trabajo de optimización de repositorio.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más), y, a continuación, seleccione **Repositorios**.

   Aparecerá la página **Repositorios**.

   Aparece el panel Repositorios DVM.
3. Si desea interrumpir un trabajo de optimización, haga lo siguiente:
   a. En la tabla de resumen de repositorios, en la fila que represente el repositorio adecuado, haga clic en (Más opciones) y, a continuación, seleccione **Interrumpir la optimización de trabajos**.

   Aparece un mensaje de aviso que le pide que confirme la interrupción.
   b. Haga clic en confirmar la interrupción.
4. Si desea reanudar un trabajo de optimización interrumpido, haga lo siguiente:
   a. En la tabla de resumen de repositorios, en la fila que represente el repositorio adecuado, haga clic en (Más opciones) y, a continuación, seleccione **Optimizar**.

   Aparece un mensaje de aviso que le pide que confirme la optimización.
   b. En el cuadro de diálogo, seleccione la opción **Continuar trabajo desde el punto de interrupción** y, a continuación, haga clic en **Sí**.

   El cuadro de diálogo se cierra y el trabajo de optimización de repositorio se reanuda desde el punto donde se interrumpió por última vez.

Administración de un repositorio por capas

Un repositorio por capas es un repositorio secundario definido en su Core en el que los puntos de recuperación pueden reubicarse desde un repositorio DVM principal.

Una vez que se mueven, los puntos de recuperación se eliminan de su repositorio DVM principal. El Core sigue administrando los puntos de recuperación reubicados hasta que finalmente se consolidan y se eliminan.

Para nivelar los datos de la copia de seguridad, debe definir la antigüedad a la que los puntos de recuperación de su repositorio DVM deberían comenzar a nivelarse. Puede hacer esto en la página del periodo de retención.

Antes de que pueda reubicar los puntos de recuperación en un repositorio por capas, debe crear el repositorio secundario en su Rapid Recovery Core.

Administrar un repositorio por capas implica las siguientes operaciones:

1. **Creación de un repositorio por capas**. Para nivelar los puntos de recuperación obsoletos en un almacenamiento secundario, primero debe definir el repositorio por capas en la Rapid Recovery Core Console. En versión 6.2, la nivelación solo es compatible en servidores de desduplicación de DR Series que ejecutan el SO 4.0. El repositorio requiere servicios RDS nativos en el servidor DR. Para obtener más información, consulte Comprensión de los repositorios. Para obtener más información sobre la creación de un repositorio por capas, consulte Creación de un repositorio por capas.
2. **Conexión a un repositorio**. Para obtener más información sobre la conexión a un repositorio por capas existente, consulte Conexión a un repositorio existente.
3. **Definir periodo de retención.** Después de haber agregado un repositorio por capas a su Core, defina en el periodo de retención la antigüedad de los puntos de recuperación para empezar a nivelarlos desde el repositorio DVM al repositorio por capas. Debe configurar la nivelación utilizando una directiva de retención personalizada para equipos protegidos específicos. Para obtener información acerca de cómo configurar su política de retención para nivelar puntos de recuperaciónen determinadas máquinas protegidas, consulte Personalización de la configuración de la política de retención de un equipo protegido.
4. **Modificación de la configuración del repositorio.** Para obtener más información sobre la modificación de la configuración del repositorio para un repositorio por capas, consulte Ver o modificar los detalles de repositorio.
5. **Comprobación de un repositorio.** Para obtener más información sobre la comprobación de un repositorio, consulte Comprobación de un repositorio.
6. **Eliminación de un repositorio**. Para obtener más información sobre cómo eliminar un repositorio, consulte Eliminación de un repositorio.

Para obtener información sobre la administración de un repositorio DVM, consulte Administración de un repositorio DVM.

Creación de un repositorio por capas

Este proceso describe cómo crear un repositorio por capas desde la Rapid Recovery Core Console, que puede utilizarse como almacenamiento secundario solo para copias de seguridad de equipos protegidos en su Core.

NOTE: En la versión 6.2, la única ubicación física compatible para los repositorios por capas es el servidor de desduplicación de la serie DR que ejecuta el SO 4.0. Al configurar su directiva de retención para nivelar, puede especificar una hora tras la cual los puntos de recuperación se reubicarán desde su repositorio DVM hasta el repositorio por capas de su servidor DR. El servidor DR incluye los servicios de almacenamiento rápido de datos (RDS).

Si desea crear un repositorio DVM principal, consulte el tema Creación de un repositorio DVM.

- Para fines de planificación, se reservan 128 GB del volumen de almacenamiento de forma predeterminada para el diccionario de desduplicación.
- El servidor del Core puede ser un servidor Windows basado en software y con el tamaño adecuado que cumpla con los requisitos del sistema de archivos y del sistema operativo de Rapid Recovery. También puede ser cualquier servidor de copia de seguridad DL distinto a DL1000 o a DL4000. Estos modelos de servidor solo son compatibles actualmente con repositorios DVM.

  NOTE: Para obtener más información sobre requisitos del sistema, consulte la *Rapid Recovery System Requirements Guide (Guía de requisitos del sistema de Rapid Recovery)*.
- Debe tener acceso administrativo al servidor DR en el que desea crear el repositorio por capas.
- Debe especificar el nombre de host del servidor DR.

En un volumen de almacenamiento con aprovisionamiento reducido, el volumen de repositorio muestra la cantidad de espacio consumido del sistema operativo. Un volumen con aprovisionamiento grueso puede mostrar el contenido entero de la unidad que se va a consumir con los datos. Puede supervisar los repositorios con regularidad con este informe de repositorios, que le ayuda a evitar llenar el volumen de un repositorio. Para obtener información sobre cómo generar un informe de repositorios manualmente, consulte Generación de un informa del Core a petición. Para obtener más información sobre la automatización de la generación de informes de forma continua, consulte Programación de un informe.

Lleve a cabo los pasos de este procedimiento para crear un repositorio por capas.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Repositorios**.

   Aparecerá la página **Repositorios**.
3. En la parte superior de la página, en el título de página Repositorios, haga clic en la flecha desplegable junto a **Crear** y, a continuación, seleccione **Repositorio por capas**.

   Se muestra el **Asistente para crear repositorio**.
4. En la página **Conexión**, en el campo de texto Servidor, introduzca la dirección IP o el nombre del servidor de la red para el equipo al que desea conectarse y agregue un repositorio. A continuación, haga clic en **Siguiente**.

   Los servicios RDS están preinstalados en los servidores DR. Si el equipo contiene un servidor RDS y ejecuta el sistema operativo 4.0, se conectará a él. De lo contrario, póngase en contacto con el administrador del servidor DR para obtener asistencia, actualizar a la versión correcta del servidor RDS y volver a este paso.
5. En la página **Configuración**, introduzca la información de configuración del repositorio como se describe en la tabla siguiente y, a continuación, haga clic en **Siguiente**.

Tabla 34. Ajustes de la página Configuración

Descripciones de la configuración disponible para configurar el repositorio.

Cuadro de texto	Descripción
Nombre	Introduzca un nombre para mostrar para el repositorio. De manera predeterminada, este cuadro de texto incluye el término Repositorio y un número. El nombre sugerido se corresponde con el número de repositorios que existen actualmente para este Core. Por ejemplo, para el primer repositorio, el nombre sugerido es Repositorio 1 y para el segundo repositorio, el nombre sugerido es Repositorio 2, etc. Si se emplean repositorios de más de un tipo de tecnología, debe incluir el tipo en el nombre, por ejemplo, `TieringRepository1`.

Cuadro de texto	Descripción
	Los nombres del repositorio contienen entre 1 y 40 caracteres alfanuméricos, incluidos los espacios. No utilice caracteres prohibidos ni frases prohibidas.
Comentarios	Esta información es opcional. Se puede utilizar para describir el tipo de información que se guardará en este repositorio. Por ejemplo, "este repositorio contiene los puntos de recuperación desactualizados de todos los servidores de SQL y Exchange Server en el dominio de cuenta". Esta información puede modificarse en cualquier momento.
Grupo de almacenamiento y opciones de contenedor	Seleccione las opciones de su repositorio por capas de la siguiente manera: • Seleccione **Utilizar el grupo de almacenamiento y el contenedor predeterminados** para crear la estructura del repositorio en ubicaciones predeterminadas. La mayoría de los usuarios pueden seleccionar esta opción predeterminada. • Seleccione **Elegir un grupo de almacenamiento y un contenedor existentes** si desea especificar la estructura para su repositorio por capas y seleccione los objetos adecuados. Esta opción es para usuarios avanzados que conocen el grupo de almacenamiento y las opciones de contenedor.

6. En la página **Opciones de seguridad**, realice una de las acciones siguientes:

   • Para restringir el acceso del Core que está creando e impedir que otros usuarios de su red accedan a la información de este repositorio, seleccione **Proteger este repositorio con su licencia única**. A continuación, haga clic en **Finalizar**.

   Este paso es una precaución opcional. El repositorio ya está seguro; sin embargo, el acceso al Rapid Recovery Core requiere una autenticación. Estas opciones de seguridad se aplican cuando un usuario intenta abrir este repositorio desde un Rapid Recovery Core diferente. Para obtener seguridad adicional, también puede aplicar claves de cifrado a las copias de seguridad para cualquier equipo protegido.

   • Para completar el proceso de creación de un repositorio por capas sin también asegurar el repositorio con su licencia, desactive la opción **Asegurar este repositorio con su licencia exclusiva**, haga clic en **Finalizar** y, en el cuadro de diálogo **Advertencia de repositorio no seguro**, haga clic en **Sí**.

   Se cierra el **Asistente para crear** repositorio. La información del repositorio que especificó genera un trabajo Crear repositorio, que empieza de forma inmediata. Este trabajo y la creación del repositorio resultante tarda varios minutos en completarse. Al finalizar el trabajo, aparece un panel **Repositorios por capas** en la parte inferior de la página **Repositorio**, que muestra el nuevo repositorio por capas que acaba de agregar.
7. De forma opcional, puede realizar un seguimiento del progreso de la tarea de creación del repositorio por capas. Para obtener más información, consulte Visualización de tareas.

Comprobación de un repositorio

Rapid Recovery permite realizar una comprobación de diagnóstico de un volumen del repositorio cuando se producen errores en el Core. Los errores podrían ser el resultado del apagado incorrecto del Core, del fallo de un repositorio al montar o desmontar, de un error de hardware o de otros factores ambientales, de menor pila IP que puedan exponerse en la funcionalidad de Rapid Recovery.

Para todos los tipos de tecnologías de repositorios, la comprobación realiza las tareas siguientes:

- Comprobar repositorio
- Montar repositorio
- Cargar los puntos de recuperación del repositorio

Solo para los repositorios DVM, la comprobación también realiza la tarea "Recalcular la caché de desduplicación del repositorio".

NOTE: Este procedimiento se debe realizar únicamente con fines de diagnóstico. Por ejemplo, ejecute esta comprobación en el caso de un error de hardware, apagado incorrecto del Core o error de importación de un repositorio.

1. Desplácese hasta la Core Console de Rapid Recovery.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Repositorios**.

   Aparecerá la página **Repositorios**.
3. Para comprobar un repositorio, en cualquier fila de la tabla de resumen de cualquier tipo de tecnología de repositorio, haga clic en (Más opciones) y, a continuación, seleccione **Comprobar**.

   Aparecerá el cuadro de diálogo **Check Repository (Comprobar repositorio)**.
4. En el cuadro de diálogo **Comprobar repositorio** confirme que entiende que se cancelan todas las tareas activas asociadas con este repositorio y que desea continuar.

   Los trabajos activos se cancelan y el trabajo de comprobación de repositorio se inicia.
5. De manera opcional, para realizar un seguimiento del estado del trabajo, haga clic en el menú desplegable **Tareas en ejecución** en la barra de botones y, a continuación, haga clic en el trabajo Mantener repositorio.

Cambio de la configuración de un repositorio

Este procedimiento asume que su Core tiene un repositorio R3que funciona. Para ver o cambiar la configuración de un repositorio DVM, consulte Ver o modificar los detalles de repositorio.

En la configuración del repositorio por capas, puede cambiar el nombre para mostrar, los comentarios y las opciones de seguridad.

1. En la barra de iconos Rapid Recovery Core Console, haga clic en (Más) y, a continuación, seleccione **Repositorios**.
2. En la página **Repositorios**, desplácese hacia abajo hasta el panel **Repositorios por capas**.
3. En la fila que representa el repositorio que desea actualizar, haga clic en (Más opciones) y, a continuación, seleccione **Configuración**.

   Se muestra el asistente **Editar la configuración del repositorio**.
4. En la página **Configuración**, puede cambiar la configuración descrita en la siguiente tabla.

Opción	Descripción
Nombre	El nombre para mostrar del repositorio. Por ejemplo, Repositorio 1.

Opción	Descripción
Comentarios	Notas o una descripción que desee asociar a este repositorio.

5. Haga clic en **Siguiente**.
6. En la página **Opciones de seguridad**, para establecer la seguridad para hacer que solo un Core con el mismo número de licencia que este Core permita comunicarse con el repositorio, seleccione **Proteger este repositorio con su licencia única**.

   NOTE: Este paso es una precaución opcional. El repositorio ya está seguro; sin embargo, el acceso al Rapid Recovery Core requiere una autenticación. Estas opciones de seguridad se aplican cuando un usuario intenta abrir este repositorio desde un Rapid Recovery Core diferente. Para obtener seguridad adicional, también puede aplicar claves de cifrado a las copias de seguridad para cualquier equipo protegido.
7. Haga clic en **Finalizar**.

   Se aplican los cambios al repositorio.
8. Si elige no agregar seguridad adicional a su repositorio en el paso anterior, aparece el cuadro de diálogo **Advertencia de repositorio no seguro**. Haga clic en **Sí** para confirmar que no desea proteger el repositorio mediante clave de licencia.

   Se cierra el asistente **Editar la configuración del repositorio**. Los cambios realizados en la configuración del repositorio se aplican inmediatamente.

Conexión a un repositorio existente

Para realizar este procedimiento, debe disponer de las credenciales adecuadas para el Core de origen y debe contar con la ruta de acceso local o de red, la dirección IP o el nombre del servidor.

CAUTION: Realice este procedimiento solo para repositorios y datos para los que tenga permiso de acceso legal.

Si se conecta a un repositorio R3 o por capas, dicho repositorio debe desconectarse del Core que lo utilizó previamente. Para obtener más información acerca de la desconexión de un repositorio, consulte el tema Desconexión de un repositorio.

Si se conecta a un repositorio DVM que no esté asociado actualmente con otro Core, no se aplicará ningún otro requisito previo.

Si se conecta a un repositorio DV; que actualmente pertenece a otro Core en funcionamiento, primero debe preparar la inminente transferencia de propiedad. Se aplican los siguientes requisitos previos:

- Si el Core de origen que contiene el repositorio está en funcionamiento, detenga temporalmente la protección de los equipos en ese Core.
- A continuación, detenga el servicio de Core del Core de origen mientras transfiere la propiedad.
- Tras conectar el repositorio al nuevo Core como se describe en este procedimiento, vuelva al Core de origen. Asegúrese de que todos los equipos que sigue protegiendo disponen de un repositorio asociado a ellos.
- Después, reinicie los servicios de Core en el Core de origen.

Para obtener más información sobre la puesta en pausa de la protección, consulte Puesta en pausa y reanudación de la protección. Para obtener más información sobre el apagado y reinicio del servicio del Core, consulte Reinicio o apagado del servicio del Core.

Desde su Rapid Recovery Core Console, puede conectarse a un repositorio existente que actualmente está administrado en un Core diferente. Al finalizar esta conexión cambia la propiedad del repositorio del Core original a su Core actual. Tras conectarse al repositorio, se puede acceder a la información solo en el segundo Core, no

en el original. El repositorio al que se conecta debe ser accesible en una ubicación de red compartida o en un dispositivo de almacenamiento accesible para el segundo Core.

Este proceso resulta útil si su Core de origen está fuera de servicio y desea activar un Core de sustitución. Si, más adelante, desea cambiar de nuevo la propiedad del segundo Core a un tercer Core (o al de origen), puede hacerlo. Se aplicarán las mismas reglas.

El Core de origen que pierde el repositorio no debe estar en uso. Por ejemplo, el equipo debe estar apagado, no se puede acceder a la red o los servicios de Core deben estar detenidos.

Los repositorios por capas pueden asegurarse con una única licencia. Al seleccionar esta configuración de seguridad adicional se impide que individuos no autorizados puedan arrebatarle el control de su repositorio a otro repositorio. Si asegura su repositorio mediante su licencia única, solo los administradores con acceso a su clave de licencia podrán conectarse a su repositorio. Para obtener más información acerca de la actualización de la configuración de su repositorio, consulte el procedimiento Cambio de la configuración de un repositorio.

Realice el procedimiento siguiente para conectarse a un repositorio existente.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más), y, a continuación, seleccione **Repositorios**.

   Se mostrará la página **Repositorios**.
3. Para conectarse a un repositorio DVM existente, haga clic en el menú desplegable junto a **Conectarse al existente** y, a continuación, seleccione **Repositorio DVM**.

   Se abre el cuadro de diálogo **Conectarse al repositorio DVM existente**.
4. Continúe en el paso 6.
5. Para conectarse a un repositorio por capas existente, haga clic en el menú desplegable junto a **Conectarse al existente** y, a continuación, seleccione **Repositorio por capas**. Continúe en el paso 7.
6. En el cuadro de diálogo **Conectarse al repositorio DVM existente**, introduzca la siguiente información para el repositorio que desea abrir y, a continuación, haga clic en **Conectar**.

Tabla 35. Opciones de Abrir repositorio DVM existente

Cuadro de texto	Descripción
Ruta de acceso	La ruta de acceso del repositorio (por ejemplo, `D:\work\machine` de una ruta de acceso local, o `\\10.10.99.155\repositories` por dirección IP, o \\servername \sharename de una ruta de red).
Nombre de usuario	Si el repositorio tiene una ruta de acceso de red, introduzca el nombre de usuario para iniciar sesión en el recurso compartido de red.
Contraseña	Si el repositorio tiene una ruta de acceso de red, introduzca la contraseña para iniciar sesión en el recurso compartido de red.

   El cuadro de diálogo se cierra y el repositorio seleccionado se agrega al Core actual.
7. En el **Asistente de conexión a repositorios**, en la página **Conexión**, introduzca el nombre del servidor i la dirección IP del equipo que aloja el repositorio que desea conectar a este Core y, a continuación, haga clic en **Siguiente**.
8. En la página **Cores** del asistente, haga clic para seleccionar el Core apropiado y, a continuación, haga clic en **Siguiente**.
9. En la página **Detalles** del asistente, revise los detalles para garantizar que el Core seleccionado es apropiado. Para conectarse al Core seleccionado, haga clic en **Finalizar**.

   Si observa un error que indique que el repositorio seleccionado está en uso, inicie sesión en ese Core y prepárelo para la transferencia de propiedad de su repositorio a este Core. Pause cualquier protección existente; pause cualquier replicación existente; espere a que se completen los trabajos en cola o cancélelos. Apague los servicios del Core o apague gradualmente el servidor del Core y, a continuación,

repita este procedimiento. Para obtener más información sobre la puesta en pausa de la protección, consulte Puesta en pausa y reanudación de la protección. Para obtener más información sobre la puesta en pausa de la replicación, consulte Pausa y reanudación de la replicación. Para obtener más información sobre el apagado y reinicio del servicio del Core, consulte Reinicio o apagado del servicio del Core.

Ver o modificar los detalles de repositorio

Para ver los detalles del repositorio, el Core debe contener primero un repositorio. Para obtener más información sobre cómo crear un repositorio DVM o por capas, consulte Creación de un repositorio DVM o Creación de un repositorio por capas, respectivamente.

En el panel **Repositorios DVM**, se muestra cada repositorio DVM agregado al Core.

- Si hace clic en (Expandir), las filas secundarias muestran las ubicaciones de los datos y metadatos del repositorio DVM.
- También puede (Contraer) la vista.

En el panel **Repositorios por capas** se utilizan al menos tres filas de datos para representar cada repositorio existente:

- La fila superior es el servidor RDS . Puede conectarse a un máximo de tres servidores RDS por Core.
- La segunda fila muestra el grupo de almacenamiento . Cada servidor RDS puede incluir un máximo de cinco grupos de almacenamiento.
- La tercera fila muestra el repositorio por capas.

Puede (Expandir) y (Contraer) la vista en lospaneles **Repositorios por capas** para ahorrar espacio.

Los detalles del repositorio varían en función del tipo de tecnología del repositorio. Para ver o modificar los detalles del repositorio, utilice el siguiente procedimiento:

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Repositorios**.

   Se muestra la página **Repositorios**.
3. Las siguientes acciones generales están disponibles:

Opción	Descripción
+ Crear	En el menú desplegable, seleccione el tipo de repositorio adecuado para crear un repositorio. Puede elegir entre: • Repositorio DVM • Repositorio por capas
Conectarse al existente	En el menú desplegable, seleccione un tipo de repositorio para abrir un repositorio desde otro Core.

Opción	Descripción
	Este proceso convierte al Core en el propietario del repositorio. Puede elegir entre: • Repositorio DVM • Repositorio por capas Para obtener más información, consulte Conexión a un repositorio existente.
Actualizar	Actualiza la lista de repositorios que se muestran en la página.

4. En el panel **Repositorios DVM**, en el menú desplegable (Más opciones) de cualquier repositorio DVM, puede realizar las acciones siguientes:

Opción	Descripción
Agregar ubicación de almacenamiento	Ampliar el repositorio existente agregando una ubicación del almacenamiento **NOTE:** Al ampliar un volumen de repositorio DVM, primero pause la protección. A continuación, amplíe el volumen y, finalmente, reanude la protección. Esta acción evita los errores extraños que pueden producirse solo al ampliar un volumen de forma simultánea con una fase de transferencia específica.
Comprobar	Realizar una comprobación de repositorio.
Configuración	Ver o modificar la configuración del repositorio. Esta configuración incluye: • Ver el nombre de repositorio • Ver o cambiar el número máximo de operaciones simultáneas • Ver o cambiar una descripción del repositorio • Activar o desactivar alertas • Activar o desactivar la compresión para los datos guardados en el repositorio
Optimizar	Realizar un trabajo de optimización de repositorio. Para obtener más información, consulte Acerca de la optimización del repositorio DVM.
Eliminar	Eliminar un repositorio. **CAUTION: Esta opción elimina completamente el repositorio DVM seleccionado y todos los datos que contiene.**

5. En el panel **Repositorios por capas**, en el menú desplegable (Más opciones) de cualquier servicio de RDS, puede realizar las acciones siguientes:

Opción	Descripción
Cambiar credenciales	Le permite cambiar la contraseña asociada con el host seleccionado actualmente. Esta acción resulta útil al cambiar la propiedad de un repositorio para mantener la seguridad. **NOTE:** Confirme la nueva contraseña y haga clic en **Guardar** para actualizar sus credenciales.

6. No hay acciones disponibles para los grupos de almacenamiento.
7. En elpanel **Repositorios por capas**, en el menú desplegable (Más opciones) de cualquier repositorio por capas, puede realizar las siguientes acciones:

Opción	Descripción
Configuración	Abre el asistente Editar la configuración del repositorio, en el que puede ver o modificar la configuración del repositorio. Esta configuración incluye: • Ver el servidor o el host • Ver o cambiar el nombre de repositorio • Ver o cambiar los comentarios del repositorio
Comprobar	Cancela todas las tareas activas del repositorio seleccionado y después realiza una comprobación del repositorio.
Desconectar	Desmonta el repositorio seleccionado. **NOTE:** Después de desconectarse, puede volver a conectarse al repositorio más tarde utilizando la función **Conectarse al existente** en la parte superior de la página Repositorios.
Eliminar	Eliminar un repositorio. **CAUTION: Esta opción elimina completamente el repositorio seleccionado y todos los datos que contiene.**

Desconexión de un repositorio

Este procedimiento asume que su Core tiene un repositorio R3 que funciona.

En la página **Repositorios**, puede desconectar un repositorio existente. Este proceso no elimina los datos del repositorio. Simplemente interrumpe la conexión actual con el repositorio y su contenido. Esto es útil, por ejemplo, en una situación en la que desee conectarse al repositorio desde un Core diferente.

Realice este procedimiento para desconectar un repositorio por capas.

1. En la Rapid Recovery Core Console, en la barra de iconos, haga clic en el menú (Más) y, a continuación, haga clic en **Repositorios**.
2. En la página **Repositorios**, en la fila que representa el repositorio que desea desconectar, haga clic en (Más opciones) y, a continuación, seleccione **Desconectar**.

   Se abre el cuadro de diálogo **Desconectar repositorio**.
3. Haga clic para confirmar la acción y desconectar el repositorio existente.

   El repositorio se desconecta y la página **Repositorios** se actualiza. El repositorio ya no aparece en la lista de repositorios disponibles actualmente.

Para volver a conectar el repositorio, consulte el procedimiento Conexión a un repositorio existente.

Eliminación de un repositorio

Lleve a cabo los pasos de este procedimiento para eliminar un repositorio.

1. Vaya a Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Repositorios**.

   Se muestra la página **Repositorios**.
3. En la tabla de resumen de los repositorios adecuados, en la fila que representa el repositorio que desea eliminar, haga clic en (Más opciones) para expandir el menú desplegable y, a continuación, seleccione **Eliminar**.

   Aparece un mensaje de advertencia para confirmar la eliminación.

   CAUTION: Cuando se elimina un repositorio los datos del mismo se descartan y no se pueden recuperar.
4. Haga clic en **Sí** para confirmar la eliminación del repositorio.

Administración de la privacidad

Esta sección describe la información personal que Rapid Recovery puede recopilar, para qué se utiliza y cómo se controla la privacidad de dichos datos.

Los temas incluyen:

- Cumplimiento del Reglamento General de Protección de Datos
- Cómo utiliza Rapid Recovery la información personal
- Restricciones de la licencia sin llamada a la central
- Obtención y uso de licencias sin llamada a la central

Cumplimiento del Reglamento General de Protección de Datos

El Reglamento General de Protección de Datos (GDPR) es una normativa creada para reforzar y unificar la protección de datos de todos los individuos de la Unión Europea (UE). También afecta a la exportación de datos personales fuera de la Unión Europea, por lo que resulta relevante para la creación de software en EE. UU. y en otros países. Actualiza normas acerca de la manipulación de datos personales de individuos. El GDPR se está adoptando ampliamente en todo el sector del software.

Para cumplir el GDPR, se ha estudiado cuidadosamente la recopilación de cualquier información de identificación personal (PII) por parte de Rapid Recovery Core. Se ha simplificado la recopilación de datos, y la información recogida está claramente documentada.

Al instalar el Rapid Recovery Core y ejecutar la Recovery and Update Utility (RUU) o la herramienta de recopilación de información, recibirá una descripción de la información que recopila Rapid Recovery y de nuestros propósitos para recopilar dicha información.

Si acepta dicho uso de datos personales, puede asociar una licencia (en el modo estándar con llamada a la central) con su Core. Si decide rechazar el uso de los datos personales descrito en la política de privacidad, debe solicitar una licencia especial sin llamada a la central. Tras recibir dicha licencia y asociarla con su Core, no se utilizarán sus PII, y ciertas funciones (actualización automática y habilitación de la integración entre el Core y el Portal de protección de datos) estarán deshabilitadas.

Independientemente de la opción de privacidad que seleccionó durante la instalación, puede cambiarla en la configuración general del Core **Acepto el uso de datos personales**. Para alternar entre los modos con y sin llamada a la central, debe tener acceso a la licencia adecuada.

Para obtener más información acerca del GDPR, consulte el sitio web del Reglamento General de Protección de Datos de la UE en http://www.eugdpr.org/eugdpr.org.html.

Para obtener más información sobre la gestión de su privacidad, consulte los siguientes temas en la *Guía del usuario de Rapid Recovery*:

- Se aplican ciertas reglas de negocios al cambiar entre los modos con y sin llamada a la central mediante la configuración general **Acepto el uso de datos personales**. Para obtener más información, consulte el tema "Configuración de los parámetros generales del Core".
- Para ver qué información recopila Rapid Recovery, en qué circunstancias y por qué, consulte "Cómo utiliza Rapid Recovery la información personal."
- Para ver qué funciones no puede utilizar al utilizar una licencia sin llamada a la central, consulte el tema "Restricciones de licencia sin llamada a la central".
- Para descargar una licencia con llamada a la central, inicie sesión en el Portal de licencias de Rapid Recovery. En el menú de navegación, haga clic en **Licencias**, y en el menú desplegable situado arriba a la derecha, seleccione **Clave de licencia.**
- Para saber cómo obtener una licencia en el modo sin llamada a la central, consulte el tema "Obtener y utilizar claves de licencia sin llamada a la central".

Cómo utiliza Rapid Recovery la información personal

Como se describe en Administración de licencias, Rapid Recovery utiliza tres tipos de licencias de software: de suscripción, perpetua y de prueba.

Las licencias se pueden utilizar de dos modos diferentes:

- **Modo con llamada a la central.** Todas las licencias se emiten en el modo con llamada a la central a menos que se solicite lo contrario. Si registra una licencia con llamada a la central mediante el Portal de licencias de Rapid Recovery, Rapid Recovery recopila información de identificación personal (PII). A continuación se describe qué información se recopila y cómo se utiliza.
- **Modo sin llamada a la central.** Aunque esté conectado a Internet, si obtiene y registra una licencia sin llamada a la central, Rapid Recovery no compartirá su PII. Este modo le impide realizar ciertas funciones, tal y como se describe en el tema Obtención y uso de licencias sin llamada a la central.

Las licencias de suscripción solo pueden utilizarse en el modo con llamada a la central. Las licencias de prueba y perpetua pueden utilizarse en el modo con llamada a la central o en el modo sin llamada a la central.

Si registra una licencia con llamada a la central, usted concede permiso a Rapid Recovery para recopilar la siguiente PII:

- Las direcciones IP y nombres de hosts que se ejecutan que se ejecutan en o interactúan con Rapid Recovery Core y Agent.
- Las direcciones de correo electrónico asociadas con licencias Rapid Recovery y
- El consumo de licencias con respecto a la cantidad de licencias del grupo.

Esta información se envía a Quest Software Inc. con los siguientes propósitos:

- Aplicar adecuadamente los términos de licencia apropiados para el producto;
- Proporcionar asistencia al cliente; por ejemplo, cuando ejecuta la herramienta de recopilación de información, los registros y los datos de diagnóstico que especifica se recopilan en una carpeta local que

se envía a Quest, o puede cargarse en Amazon, y solo es accesible para Asistencia para la protección de datos de Quest.

- Para notificar a los usuarios de las actualizaciones disponibles (si la configuración de actualización de su Core especifica una opción diferente a **No comprobar actualizaciones nunca**); y
- Para permitir la comunicación entre el Core y el Portal de protección de datos. Esta comunicación se puede habilitar o deshabilitar utilizando la configuración **Portal de protección de datos** en el Core. Este portal permite a los usuarios con licencia y con un contrato de asistencia vigente supervisar el estado de Cores y máquinas protegidas, administrar varios Cores y generar informes a petición para los Cores y máquinas protegidas pertinentes.

Tiene derecho a decidir si desea o no compartir esta información con Quest. En primer lugar, al instalar o actualizar el Rapid Recovery Core, puede decidir si compartir esta información en la página **Política de Privacidad** del instalador. Además, si decide no compartir información con Quest, puede cambiar la configuración general del Core **Acepto el uso de datos personales**. Al cambiar esta configuración se le pide que introduzca una licencia. Si introduce una licencia sin llamada a la central, se deshabilitan las actualizaciones automáticas, así como su conexión al Portal de protección de datos.

Para ver más recursos sobre este tema, consulte los siguientes enlaces relacionados.

- Para obtener más información sobre las funciones de las que no dispone al utilizar el modo sin llamada a la central, consulte el tema Restricciones de la licencia sin llamada a la central.
- Para recibir más información sobre cómo obtener una licencia en el modo sin llamada a la central, contacte con el equipo de licencias Quest mediante un formulario web, como se describe en el tema Obtención y uso de licencias sin llamada a la central.
- Para obtener más información acerca de cómo cambiar su configuración general, incluido el uso compartido de PII, consulte el tema Configuración de los parámetros generales del Core.
- Para obtener más información sobre cómo ver la información de licencia para un solo equipo protegido, consulte Visualización de la información de licencia en un equipo.
- Para obtener información acerca de cómo introducir la clave de licencia o la información del archivo (por ejemplo, para actualizar una licencia perpetua con llamada a la central a una licencia perpetua sin llamada a la central), consulte Actualización o cambio de una licencia.
- Para obtener información acerca de los tipos de licencia disponibles, consulte Administración de licencias.
- Para obtener más información sobre cómo ponerse en contacto con el servidor del portal de licencias, consulte Contacto con el servidor del Portal de licencias de Rapid Recovery.
- Para consultar otros temas relacionados con la administración de licencias, consulte la *Rapid Recovery License Portal User Guide (Guía del usuario del Portal de licencias de Rapid Recovery)*.

Restricciones de la licencia sin llamada a la central

Registrar una licencia de Rapid Recovery en modo sin llamada a la central impide que el Core comparta su información personal. Esta información incluye dirección de correo electrónico, direcciones IP e información de consumo de licencias.

Después de registrar una licencia sin llamada a la central, no podrá realizar las siguientes acciones:

- Visualizar información del servidor de licencias en la página **Configuración** de la Core Console (debido a que su Core no tiene permiso para comunicarse con el Portal de licencias de Rapid Recovery).
- Administrar el consumo de licencias desde la Core Console.
- Enviar información a Asistencia para la protección de datos de Quest desde la herramienta de recopilación de información de Rapid Recovery.
- Supervisar el estado de los Cores y equipos protegidos, administrar varios Cores y generar informes a petición para los equipos pertinentes en varios Cores en el Portal de protección de datos.
- Utilizar la función de actualización automática para actualizar a una nueva versión de Rapid Recovery Core (no se notifica a su Core de las nuevas versiones disponibles).
- Utilizar la función de actualización automática para actualizar directamente equipos protegidos de Linux utilizando administradores de paquetes como yum, zypper o apt (pero puede descargar un paquete de instalación desde una máquina Linux con acceso a internet y mover archivos de instalación al equipo protegido de forma manual).

Obtención y uso de licencias sin llamada a la central

Si obtiene la licencia sin llamada a la central antes de actualizar o instalar Rapid Recovery Core versión 6.2, transfiera la licencia al servidor del Core. Al ejecutar el instalador, en la página **Política de Privacidad**, seleccione la opción de rechazar compartir datos y, cuando se le solicite, registre la licencia sin llamada a la central.

Si ya ha registrado su Rapid Recovery Core versión 6.2 con una clave con llamada a la central, acceda a la configuración general del Core, seleccione la opción de rechazar compartir datos y, cuando se le solicite, registre la clave sin llamada a la central.

Para obtener más información o instrucciones paso a paso para cambiar la configuración general del Core, consulte el tema Configuración de los parámetros generales del Core.

Para obtener más información acerca de cómo administrar licencias desde el Rapid Recovery Core, consulte Administración de licencias.

Complete los pasos de este procedimiento para ponerse en contacto con el equipo de licencias de Quest para obtener una licencia sin llamada a la central.

1. En un navegador web, vaya al sitio web de Asistencia con las licencias de Quest en https://support.quest.com/contact-us/licensing.
2. En el menú desplegable **¿Cómo podemos ayudarle?**, seleccione **Obtener una licencia para mi producto**.
3. En el menú desplegable **Seleccionar producto**, seleccione **Rapid Recovery**.
4. Desde el menú desplegable **Versión del producto**, seleccione la opción adecuada.

   Por ejemplo, seleccione **6.2**.
5. En la sección Información de contacto del formulario, agregue información tal como se describe en la siguiente tabla.

Nombre de campo	Descripción	Campo obligatorio
Correo electrónico empresarial	Introduzca la dirección de correo electrónico a la que desea que le responda el equipo de licencias de Quest. Si tiene acceso a la cuenta	Sí

Nombre de campo	Descripción	Campo obligatorio
	de correo electrónico asociada a su licencia de Rapid Recovery, utilice esa dirección para recibir una respuesta más rápida.	
Nombre del contacto	Introduzca su nombre de pila.	Sí
Apellidos del contacto	Introduzca sus apellidos.	Sí
Nombre de la compañía	Introduzca el nombre de la empresa asociada con su licencia de Rapid Recovery.	
Federal de los EE. UU.	Seleccione esta opción si su licencia está relacionada con una organización federal de los Estados Unidos.	No
País	Seleccione su país.	Sí
Número de teléfono	Introduzca su número de teléfono, incluido el código de área. Si el teléfono no pertenece a Estados Unidos, incluya el código de país.	Sí
Número de licencia (si está disponible)		No
Clave de licencia (si está disponible)	Las claves de licencia se utilizaron en AppAssure 5.4.1 y versiones anteriores. En general es una cadena de 30 caracteres (6 grupos de 5 números y letras mayúsculas del alfabeto, separados por guiones).	No
ID de equipo	Nombre del equipo registrado como Core.	No
Etiqueta de servicio (si está disponible)	Introduzca la etiqueta de servicio si está disponible.	No
Detalles de la solicitud de licencia	Indique en este campo que, de acuerdo con el GDPR, desea reemplazar su licencia con llamada a la central por una licencia sin llamada a la central para proteger su PII. **NOTE:** Al realizar esta solicitud, acepta que eliminará la clave de licencia con llamada a la central al recibir y registrar la clave de licencia sin llamada a la central. También acepta que no compartirá esta clave.	Sí
Archivo de licencia	Si dispone de una licencia con llamada a la central, puede adjuntar el archivo de licencia.	No

6. Para validar su solicitud y enviar el formulario, seleccione **No soy un robot** y, a continuación, haga clic en **Siguiente**.

   Cuando envíe el formulario, recibirá un mensaje de correo electrónico con un número de solicitud de servicio.

Cuando reciba el archivo de licencia con llamada a la central, cárguelo en el servidor del Core para registrar la licencia. Para obtener más información, consulte Actualización o cambio de una licencia.

Cifrado

Esta sección describe el proceso de asegurar datos en su entorno utilizando claves de cifrado y configuración de cifrado de instantáneas a nivel de equipo.

Comprensión de las claves de cifrado

El Core de Rapid Recovery puede cifrar datos de instantáneas para todos los volúmenes de cualquier repositorio utilizando claves de cifrado que usted define y administra.

En vez de cifrar el repositorio completo, Rapid Recovery permite especificar una clave de cifrado para uno o más equipos protegidos en un único Core de Rapid Recovery. Cada clave de cifrado activa crea un dominio de cifrado. No hay límite en el número de claves de cifrado que pueden crearse en el Core.

En un entorno multiusuario (cuando un único Core aloja múltiples dominios de cifrado), los datos se particionan y se desduplican dentro de cada dominio de cifrado. Como resultado, Quest recomienda el uso de una única clave de cifrado para equipos protegidos múltiples si desea maximizar los beneficios de la desduplicación entre un conjunto de equipos protegidos.

También puede compartir claves de cifrado entre Cores empleando uno de los tres métodos. Un método es exportar una clave de cifrado como un archivo desde un Core de Rapid Recovery e importarlo en otro Core. Un segundo método es archivar datos asegurados con una clave de cifrado y luego importar esos datos archivados en otro Core de Rapid Recovery. El tercer método es replicar puntos de recuperación desde un equipo protegido utilizando una clave de cifrado. Después de replicar equipos protegidos, las claves de cifrado empleadas en el Core de origen aparecen como las claves de cifrado replicadas en el Core de destino.

En todos los casos, una vez importadas, las claves de cifrado aparecen en el Core con un estado de bloqueo. Para acceder a los datos desde una clave de cifrado bloqueada, debe desbloquearla. Para obtener información sobre la importación, exportación, bloqueo o desbloqueo de claves de cifrado, consulte el tema Administración de las claves de cifrado.

Los conceptos y consideraciones clave de la seguridad incluyen:

- El cifrado se realiza mediante el estándar de cifrado avanzado (AES) de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) que cumple el estándar SHA-3.
- La desduplicación funciona en el dominio de cifrado para garantizar la privacidad.
- El cifrado se realiza sin afectar al rendimiento.
- Puede aplicar una única clave de cifrado a cualquier número de equipos protegidos, pero un equipo protegido solo puede tener aplicada una clave de cifrado a la vez.
- Puede agregar, quitar, importar, exportar, modificar y eliminar las claves de cifrado que se han configurado en el Core de Rapid Recovery.

> **CAUTION:** Rapid Recovery **realiza una nueva instantánea siempre que aplique una clave de cifrado en un equipo protegido. También se desencadena una nueva instantánea después de desasociar una clave de cifrado de un equipo protegido.**

Las claves de cifrado generadas desde el Core de Rapid Recovery son archivos de texto que contienen cuatro parámetros que se describen en la siguiente tabla:

Tabla 36. Componentes de una clave de cifrado

Componente	Descripción
Nombre	Este valor es equivalente al nombre de la clave que se asigna cuando se agrega una clave en la Core Console de Rapid Recovery.
Clave	Este parámetro consta de 107 caracteres latinos alfabéticos, numéricos y matemáticos generados de forma aleatoria.
Id.	El Id. de clave consta de 26 caracteres latinos en mayúsculas y minúsculas generados de forma aleatoria.
Comentario	El comentario contiene el texto de la descripción de la clave que se introdujo cuando se creó la clave.

Cifrado de los datos en transporte en una red

Rapid Recovery Coreversión 6.2 incluye una nueva característica de cifrado: ahora se pueden cifrar todos los datos en transporte en una red entre Quest recomienda activar esta configuración de cifrado cuando los datos entre el Core y las máquinas protegidas (o entre dos Cores, como ocurre durante la replicación) deben pasar por redes públicas o no fiables como Internet.

Aunque solo hay una pequeña pérdida de rendimiento al activar este cifrado, si sus Cores y máquinas protegidas están dentro de los límites de una red de área local privada, puede desactivar esta opción con confianza.

Lea la siguiente información y ajuste su entorno en consecuencia.

De manera predeterminada, al proteger una máquina con el Asistente para proteger un equipo o el Asistente para proteger varios equipos, el cifrado de los datos en transporte en una red está activado. Si selecciona opciones avanzadas para el asistente, podrá ver las opciones de Cifrado. En la página Cifrado del asistente, si lo prefiere, puede desactivar la opción **Cifrar los datos en transporte en una red**.

NOTE: Si no selecciona las opciones avanzadas en el asistente, el cifrado de datos en transporte se activa igualmente.

Después de completar el Asistente de protección pertinente, siempre puede activar o desactivar el cifrado de datos de instantánea cambiando la configuración de transferencia a nivel de máquina. Seleccione la máquina protegida, haga clic en **Configuración** y, en Configuración de transferencia, en el valor **Cifrar datos de instantánea**, seleccione **Sí** para activar el cifrado o seleccione **No** para desactivar el cifrado durante el transporte. Para obtener detalles específicos, consulte Visualización y modificación de la configuración de equipos protegidos en la *Guía del usuario de Rapid Recovery*.

Aplicación o eliminación de claves de cifrado

Puede asegurar los datos protegidos en su Core en cualquier momento definiendo una clave de cifrado y aplicándola a uno o más equipos protegidos de su repositorio. Puede aplicar una única clave de cifrado a

cualquier número de equipos protegidos, pero un equipo protegido solo puede tener aplicada una clave de cifrado a la vez.

El ámbito de desduplicación de Rapid Recovery se limita a los equipos protegidos con el mismo repositorio y clave de cifrado. Por lo tanto, para potenciar al máximo el valor de la desduplicación, Quest recomienda aplicar una única clave de cifrado al máximo número de equipos protegidos posible. Sin embargo, no hay límite en el número de claves de cifrado que pueden crearse en el Core. Por ello, si el cumplimiento normativo, las reglas de seguridad, las políticas de privacidad u otras circunstancias lo requieren, puede agregar y administrar cualquier número de claves de cifrado. Luego podrá aplicar cada clave a un único equipo protegido o a cualquier conjunto de equipos de su repositorio.

En el momento que aplica una clave de cifrado a un equipo protegido o disocia una clave de cifrado de un equipo protegido, Rapid Recovery toma una nueva imagen base para ese equipo en la siguiente instantánea programada o forzada. Los datos que se almacenan en esa imagen de base (y todas las instantáneas incrementales posteriores que se tomen mientras se aplica una clave de cifrado) están protegidos por un estándar de cifrado avanzado de 256 bits. No existen métodos conocidos para poner en peligro este método de cifrado.

Si cambia el nombre de la frase de contraseña por una clave de cifrado existente y que se usa actualmente para proteger un equipo, a continuación, en la siguiente instantánea programada o forzada, Rapid Recovery Core captura y refleja las propiedades actualizadas de la clave. Los datos que se almacenan en esa imagen (y todas las instantáneas incrementales posteriores que se tomen mientras se aplica una clave de cifrado) están protegidos por un estándar de cifrado avanzado de 256 bits. No existen métodos conocidos para poner en peligro este método de cifrado.

Una vez que se crea y se aplica una clave de cifrado a un equipo protegido, existen dos conceptos que se aplican para retirar ese cifrado. El primero es desasociar la clave del equipo protegido. Opcionalmente, una vez que se desasocia la clave de cifrado de todos los equipos protegidos, puede eliminarse del Rapid Recovery Core.

Esta sección incluye los siguientes temas:

- Asociación de una clave de cifrado con un equipo protegido
- Aplicación de una clave de cifrado desde la página Equipos protegidos
- Desasociación de una clave de cifrado de un equipo protegido

Asociación de una clave de cifrado con un equipo protegido

Puede aplicar una clave de cifrado a un equipo protegido empleando uno de los dos métodos siguientes:

- **Como parte de la protección de un equipo.** Cuando se utiliza este método, puede aplicar el cifrado a uno o varios equipos de forma simultánea. Este método le permite agregar una nueva clave de cifrado o aplicar una clave existente al equipo o equipos seleccionados.

  Para utilizar el cifrado cuando se define inicialmente la protección de un equipo, debe seleccionar las opciones avanzadas en el Asistente para proteger equipo relevante. Esta selección agrega una página Cifrado al flujo de trabajo del asistente. Desde esta página, seleccione **Activar cifrado** y, a continuación, seleccione una clave de cifrado existente o especifique parámetros para una nueva clave. Para obtener más información, consulte Protección de un equipo o Acerca de la protección de varios equipos, respectivamente.

- **Modificando los parámetros de configuración de un equipo.** Este método aplica una clave de cifrado a un equipo protegido a la vez. Existen dos enfoques para modificar los parámetros de configuración de un equipo en la interfaz de usuario de Rapid Recovery:

  - Modificar los parámetros de configuración de un equipo protegido específico. La clave de cifrado que desee utilizar para este enfoque debe existir en el Core de Rapid Recovery, ser un tipo de clave universal y estar en un estado de desbloqueo. El cifrado forma parte de la configuración general.

Para obtener más información, consulte Visualización y modificación de la configuración de equipos protegidos.

- Haga clic en el icono **No cifrado** en la página Equipos protegidos. Empleando este enfoque puede crear y aplicar una nueva clave de cifrado, o asignar una clave existente desbloqueada existente al equipo protegido especificado. Para obtener más información, consulte Aplicación de una clave de cifrado desde la página Equipos protegidos.

Aplicación de una clave de cifrado desde la página Equipos protegidos

Una vez se ha agregado una clave de cifrado a un Core de Rapid Recovery, puede utilizarse para cualquier número de equipos protegidos.

Si selecciona una clave de cifrado durante la protección inicial de uno o más equipos, esa clave se aplica automáticamente a cualquier equipo que proteja utilizando ese asistente. En dichos casos, no se requiere este procedimiento.

Realice este procedimiento:

- Si desea aplicar una clave de cifrado existente, universal, desbloqueada para cualquier equipo protegido en el Core.
- Si acaba de agregar una nueva clave de cifrado mediante el proceso que se describe en el tema Incorporación de una clave de cifrado y desea aplicar esa clave a un equipo protegido.
- Si el cifrado ya se aplica a un equipo protegido en el Core, pero desea cambiar la clave a una clave universal desbloqueada diferente disponible en el Core.

CAUTION: Después de aplicar una clave de cifrado a un equipo protegido, Rapid Recovery **toma una nueva imagen de base para ese equipo en la siguiente instantánea programada o forzada.**

1. Desplácese hasta el Core de Rapid Recovery y haga clic en **Equipos protegidos**.

   Aparece la página **Equipos protegidos** enumerando todos los equipos protegidos por este Core. Aparece un Candado abierto para todos los equipos que no tienen aplicada una clave de cifrado. Un candado cerrado indica que un equipo protegido tiene el cifrado aplicado.

2. En el panel Equipos protegidos, haga clic en el icono de candado del equipo protegido que desee configurar.

   Aparece el cuadro de diálogo **Configuración de cifrado**.

3. Realice uno de los siguientes pasos:

   - Si desea aplicar una clave de cifrado existente a esa máquina, seleccione **Cifrar los datos mediante un cifrado basado en Core con una clave existente** y en el menú desplegable, seleccione la clave adecuada. Haga clic en **Aceptar** para confirmar.
   - Si desea cambiar una clave de cifrado existente a una clave universal, desbloqueada diferente seleccione **Cifrar los datos mediante un cifrado basado en Core con una clave nueva** y en el menú desplegable, seleccione la clave adecuada. Haga clic en **Aceptar** para confirmar.
   - Si desea crear una nueva clave de cifrado y aplicarla a este equipo protegido, haga clic en **Cifrar los datos mediante un cifrado basado en Core con una clave nueva**. A continuación, introduzca los detalles para la clave según se describe en la tabla siguiente.

Tabla 37. Detalles de la nueva clave de cifrado

Cuadro de texto	Descripción
Nombre	Escriba un nombre para la clave de cifrado. Los nombres de las claves de cifrado contienen entre 1 y 64 caracteres alfanuméricos. No utilice caracteres no permitidos o frases no permitidas.
Descripción	Escriba un comentario descriptivo para la clave de cifrado. Esta información aparece en el campo Descripción cuando al visualizar una lista de claves de cifrado en la Rapid Recovery Core Console. Las descripciones pueden contener hasta 254 caracteres. La práctica recomendada es evitar el uso de caracteres no permitidos y frases no permitidas.
Frase de contraseña	Introduzca una frase de contraseña usada para controlar el acceso. La práctica recomendada es evitar el uso de caracteres no permitidos. Registre la frase de contraseña en lugar seguro. El servicio de asistencia técnica de Quest no puede recuperar una frase de contraseña. Una vez cree una clave de cifrado y la aplique a uno o más equipos protegidos no podrá recuperar los datos si pierde la frase de contraseña.
Confirmar frase de contraseña	Como confirmación, vuelva a escribir la Frase de contraseña. Se utiliza para confirmar la entrada de frase de contraseña.

4. Haga clic en **Aceptar**.

   El cuadro de diálogo se cierra. La clave de cifrado que especificó se ha aplicado a copias de seguridad futuras en este equipo protegido, y el candado ahora aparece como cerrado.

   De forma opcional, si desea que se aplique una clave de cifrado de forma inmediata, fuerce una instantánea. Para obtener más información, consulte Cómo forzar una instantánea.

   CAUTION: Rapid Recovery **utiliza cifrado AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) con claves de 256 bits. Si bien el uso de cifrado es opcional,** Quest **recomienda que establezca una clave de cifrado y que proteja la frase de contraseña que defina. Almacene la frase de contraseña en una ubicación segura, dado que es clave para la recuperación de datos. Sin una frase de contraseña, la recuperación de datos no es posible.**

Desasociación de una clave de cifrado de un equipo protegido

Una vez se aplica una clave de cifrado a un equipo protegido, se cifran todos los datos de instantáneas posteriores que se almacenan en el Core de Rapid Recovery.

Puede desasociar una clave de cifrado de un equipo protegido. Esta acción no descifra los datos de copia de seguridad existentes, pero da como resultado una nueva imagen de base para ese equipo en el momento de que se realice la siguiente instantánea programada o forzada.

NOTE: Si desea retirar una clave de cifrado del Core, según se describe en el tema Eliminación de una clave de cifrado, debe desasociar primero esa clave de cifrado de todos los equipos protegidos.

Realice este procedimiento para desasociar una clave de cifrado de un equipo protegido específico.

1. Desplácese hasta el Core de Rapid Recovery y haga clic en **Equipos protegidos**.

Aparece la página Equipos protegidos enumerando todos los equipos protegidos por este Core. Aparece un Candado abierto  para todos los equipos que no tienen aplicada una clave de cifrado. Un candado cerrado  indica que un equipo protegido tiene el cifrado aplicado.

2. En el panel Equipos protegidos, haga clic en el icono  **Cifrado** del equipo protegido que quiere configurar.

   Aparece el cuadro de diálogo **Configuración de cifrado**.

3. Seleccione **Cifrar datos mediante un cifrado basado en el Core con una clave existente** y, desde el menú desplegable, seleccione **(Ninguno)** y, a continuación, haga clic en **Aceptar**.
4. Si desea retirar esta clave de cifrado del Core de Rapid Recovery, primero repita este procedimiento para todos los equipos protegidos que utilicen esta clave. A continuación, realice el procedimiento que se describe en el tema Eliminación de una clave de cifrado.

Administración de las claves de cifrado

Para administrar las claves de cifrado del Rapid Recovery Core, en la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Claves de cifrado**. Aparece la página **Claves de cifrado**. Para cada clave de cifrado que se haya agregado al Rapid Recovery Core (si ya se ha definido alguna), verá la información que se describe en la siguiente tabla.

Tabla 38. Información sobre cada clave de cifrado

Elemento de la IU	Descripción
Select Item (Seleccionar elemento)	Para cada clave de cifrado, puede seleccionar la casilla de verificación para realizar acciones de la lista de opciones del menú situada encima de la tabla.
Nombre	El nombre asociado con la clave de cifrado.
Huella digital	Este parámetro es una cadena alfabética de 26 caracteres de caracteres latinos en mayúsculas y minúsculas generado aleatoriamente que ayuda a identificar de forma exclusiva cada clave de cifrado.
Tipo	El tipo describe el punto de origen de una clave de cifrado y su capacidad de aplicarse. Una clave de cifrado puede contener uno de los dos tipos posibles: **Universal**. El tipo Universal es la condición predeterminada cuando crea una clave de cifrado. Una clave con un tipo de Universal, combinado con un estado Desbloqueado, indica que la clave puede aplicarse a un equipo protegido. No es posible bloquear un tipo de clave universal manualmente; en su lugar, debe primero cambiar su tipo según se describe en el procedimiento Cambio de los tipos de clave de cifrado. **Replicación**. Cuando un equipo protegido en un Core de origen tiene activado el cifrado, y los puntos de recuperación de ese equipo se replican en un Core de destino, cualquier clave de cifrado empleada en el origen aparece automáticamente en el Core de destino con un tipo de Replicación. El estado predeterminado después de recibir una clave replicada es bloqueado. Puede desbloquear una clave de cifrado con un tipo de Replicación proporcionando la frase de contraseña. Si una clave tiene un tipo de desbloqueo, puede bloquearla manualmente. Para obtener más información, consulte el tema Desbloqueo de una clave de cifrado.

Elemento de la IU	Descripción
Estado	El estado indica si se puede utilizar una clave de cifrado. Los dos estados posibles incluyen: • Desbloqueado. Un estado Desbloqueado indica que la clave puede utilizarse de forma inmediata. Por ejemplo, puede cifrar instantáneas de un equipo protegido, o realizar una recuperación de los datos desde un punto de recuperación replicado en el Core de destino. • Bloqueado. Un estado Bloqueado indica que la clave no puede utilizarse hasta que se desbloquee proporcionando la frase de contraseña. Bloqueado es el estado predeterminado de una nueva clave de cifrado importada o replicada. Si el estado de una clave de cifrado es Bloqueado, debe desbloquearse antes de poder utilizarse. Si ha desbloqueado previamente una clave de cifrado bloqueada, y la duración para permanecer desbloqueada ha transcurrido, el estado cambia de Desbloqueado a Bloqueado. Después de que la clave se bloquee automáticamente, debe desbloquear la clave de nuevo para utilizarla. Para obtener más información, consulte el tema Desbloqueo de una clave de cifrado.
Descripción	La descripción es un campo opcional que se recomienda para proporcionar información útil sobre la clave de cifrado, como su destino o una pista de la frase de contraseña.

En el nivel superior del panel Claves de cifrado puede agregar una clave de cifrado o importar una clave utilizando un archivo exportado desde otro Rapid Recovery Core. También puede eliminar las claves seleccionadas en la tabla de resumen.

Una vez haya una clave de cifrado para un Core, puede administrar las claves existentes modificando el nombre o las propiedades de descripción, cambiando la frase de contraseña, desbloqueando una clave de cifrado bloqueada o bien eliminando la clave del Rapid Recovery Core. También puede exportar una clave a un archivo, que puede importarse en otro Rapid Recovery Core.

Cuando agrega una clave de cifrado desde la página **Claves de cifrado**, la clave aparece en la lista de claves de cifrado, pero no se aplica a un equipo protegido específico. Para obtener información sobre cómo aplicar una clave de cifrado que cree desde el panel **Claves de cifrado**, o para eliminar una clave completamente del Rapid Recovery Core, consulte Aplicación o eliminación de claves de cifrado.

Desde el panel **Claves de cifrado** puede administrar la seguridad para los datos de copia de seguridad guardados en el Core de cualquier equipo protegido de su repositorio realizando lo siguiente:

- Incorporación de una clave de cifrado
- Importación de una clave de cifrado
- Desbloqueo de una clave de cifrado
- Modificación de una clave de cifrado
- Cambio de la frase de contraseña de la clave de cifrado
- Exportación de una clave de cifrado
- Eliminación de una clave de cifrado
- Cambio de los tipos de clave de cifrado

Incorporación de una clave de cifrado

Rapid Recovery utiliza cifrado AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) con claves de 256 bits. Si bien el uso de cifrado es opcional, Quest recomienda que establezca una clave de cifrado y que proteja la frase de contraseña que defina.

CAUTION: Guarde la frase de contraseña en un lugar seguro. Sin una frase de contraseña, no podrá recuperar los datos de los puntos de recuperación cifrados.

Tras definir una clave de cifrado, puede utilizarla para salvaguardar sus datos. Las claves de cifrado pueden utilizarse en cualquier número de equipos protegidos.

Este paso describe cómo agregar una clave de cifrado desde la Core Console de Rapid Recovery. Este proceso no aplica la clave a ningún equipo que se esté protegiendo en esos momentos en el Core. También puede agregar una clave de cifrado durante el proceso de protección de un equipo. Para obtener más información sobre la incorporación del cifrado como parte de la protección de un equipo, consulte Protección de un equipo. Para obtener más información sobre la incorporación del cifrado a dos o más equipos protegiéndolos inicialmente, consulte Acerca de la protección de varios equipos.

Complete los pasos de este procedimiento para agregar una clave de cifrado.

1. Desplácese hasta la Core Console de Rapid Recovery.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Claves de cifrado**.

   Aparece la página **Claves de cifrado**.
3. Haga clic en **Agregar clave de cifrado**.

   Se abrirá el cuadro de diálogo **Crear clave de cifrado**.
4. En el cuadro de diálogo **Crear clave de cifrado**, escriba los detalles para la clave según se describe en la tabla siguiente.

Tabla 39. Detalles de Crear clave de cifrado

Cuadro de texto	Descripción
Nombre	Escriba un nombre para la clave de cifrado. Los nombres de las claves de cifrado contienen entre 1 y 64 caracteres alfanuméricos. No utilice caracteres no permitidos o frases no permitidas.
Descripción	Escriba un comentario para la clave de cifrado. Esta información aparece en el campo Descripción cuando se ven claves de cifrado desde la Core Console. Puede introducir hasta 254 caracteres. La práctica recomendada es evitar el uso de caracteres no permitidos y frases no permitidas.
Frase de contraseña	Introduzca una frase de contraseña usada para controlar el acceso. La práctica recomendada es evitar el uso de caracteres no permitidos. **CAUTION: Registre la frase de contraseña en lugar seguro.**Quest**El soporte técnico de no puede recuperar frases de contraseña. Una vez cree una clave de cifrado y la aplique a uno o más equipos protegidos no podrá recuperar los datos si pierde la frase de contraseña.**

Cuadro de texto	Descripción
Confirmar la frase de contraseña	Como confirmación, vuelva a escribir la Frase de contraseña. Se utiliza para confirmar la entrada de frase de contraseña.

5. Haga clic en **Aceptar**.

   El cuadro de diálogo se cierra y la clave de cifrado creada aparece en la página Claves de cifrado.

6. Si desea aplicar la clave de cifrado a un equipo protegido, consulte Aplicación de una clave de cifrado desde la página Equipos protegidos.

Importación de una clave de cifrado

Puede importar una clave de cifrado desde otro Core de Rapid Recovery y utilizar esa clave para cifrar los datos de un equipo protegido en su Core. Para importar la clave debe primero poder acceder a ella desde el equipo del Core, ya sea localmente o a través de la red. También debe saber la frase de contraseña de la clave de cifrado.

Complete los pasos de este procedimiento para importar una clave de cifrado.

NOTE: Este proceso no aplica la clave a ningún equipo protegido. Para obtener más información sobre la aplicación de la clave, consulte Aplicación de una clave de cifrado desde la página Equipos protegidos.

1. Vaya al Core de Rapid Recovery.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Claves de cifrado**.

   Aparece la página **Claves de cifrado**.

3. Haga clic en **Importar**.

   Aparece el cuadro de diálogo **File Upload** (Carga de archivos).

4. En el cuadro de diálogo **File Upload** (Carga de archivos), vaya a la red o al directorio local que contiene la clave de cifrado que quiere importar.

   Por ejemplo, vaya a la carpeta **Descargas** del usuario que ha iniciado sesión.

   El nombre de archivo de la clave comienza por "EncryptionKey-," seguido del Id. de la clave, y termina con la extensión de archivo .key. Por ejemplo, un nombre de clave de cifrado de muestra es EncryptionKey-CaracteresAlfabeticosAleatorios.key.

5. Seleccione la clave que desea importar y luego haga clic en **Abrir**.
6. En el cuadro de diálogo **Importar clave**, haga clic en **Aceptar**.

   El cuadro de diálogo se cierra y la clave de cifrado importada aparece en la página **Claves de cifrado**. Si la clave de cifrado se utilizó para proteger un volumen antes de exportarla, el estado de la clave es Bloqueado.

Desbloqueo de una clave de cifrado

Las claves de cifrado pueden contener un estado de bloqueo o desbloqueo. Puede aplicarse una cable de cifrado desbloqueada a un equipo protegido para asegurar los datos de copia de seguridad guardados para ese equipo en el repositorio. También puede recuperar datos de un punto de recuperación desde un Rapid Recovery Core que utiliza una clave de cifrado desbloqueada.

Cuando importa una clave de cifrado a un Rapid RecoveryCore, su estado predeterminado es bloqueado. Esto es así sin que sea relevante si importó explícitamente la clave o si la clave de cifrado se agregó al Rapid

Recovery Core replicando equipos protegidos cifrados o importando un archivo comprimido de puntos de recuperación cifrados.

Para claves de cifrado agregadas al Rapid Recovery Core solo por replicación, cuando desbloquea una clave, puede especificar una duración de tiempo (en horas, días o meses) para que la clave de cifrado permanezca desbloqueada. Cada día tiene un periodo de 24 horas, a contar desde la hora que se guardó la solicitud de desbloqueo en el Rapid Recovery Core. Por ejemplo, si se desbloquea la clave a las 11:24 AM del martes y la duración seleccionada es 2 días, la clave se volverá a bloquear automáticamente a las 11:24 AM del jueves.

NOTE: No es posible utilizar una clave de cifrado bloqueada para recuperar datos o para aplicarla a un equipo protegido. Primero debe proporcionar la frase de contraseña, lo que desbloqueará la clave.

También puede bloquear una clave de cifrado desbloqueada, lo que garantiza que no podrá aplicarse a ningún equipo protegido hasta que se desbloquee. Para bloquear una clave de cifrado con estado Universal, debe cambiar primero su tipo a Replicada.

Si una clave de cifrado desbloqueada se está utilizando en ese momento para proteger un equipo en el Core, primero debe desasociar esa clave de cifrado del equipo protegido antes de que pueda bloquearla.

Complete los pasos de este procedimiento para desbloquear una clave de cifrado bloqueada.

1. Vaya al Rapid Recovery Core.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Claves de cifrado**.

   Aparece la página **Claves de cifrado**. La columna Estado indica qué claves de cifrado están bloqueadas.
3. Localice la clave de cifrado que desea desbloquear, haga clic en el menú desplegable y seleccione **Desbloquear**.

   Aparecerá el cuadro de diálogo **Desbloquear clave de cifrado**.
4. En el cuadro de diálogo, en el campo Frase de contraseña, introduzca la frase de contraseña para desbloquear esta clave.
5. Para especificar la cantidad de tiempo que la clave permanece desbloqueada, en la opción Duración, realice una de las acciones siguientes:
   - Para especificar que la clave permanezca desbloqueada hasta que la bloquee explícitamente en Rapid Recovery, seleccione **Hasta que se bloquee manualmente**.
   - Para especificar que la clave permanezca bloqueada durante el tiempo que configure en horas, días o meses, haga lo siguiente:
     - Seleccione el campo de número e introduzca un valor entre 1 y 999.
     - Especifique la duración en horas, días o meses, respectivamente.
     - A continuación, haga clic en **Aceptar**.

     Esta opción está disponible para claves de cifrado que se incorporaron por replicación.
     El cuadro de diálogo se cierra y los cambios de la clave de cifrado seleccionada aparecen en la página Claves de cifrado.
   - Para especificar que la clave permanezca bloqueada hasta una fecha y hora que especifique, haga lo siguiente:
     - Seleccione la opción **Hasta**.
     - En el campo de texto o a través de los widgets de calendario y reloj, especifique explícitamente los datos y la hora a la que desee que se bloquee la clave de cifrado.
     - A continuación, haga clic en **Aceptar**.

     Esta opción está disponible para claves de cifrado que se incorporaron por replicación.
     El cuadro de diálogo se cierra y los cambios de la clave de cifrado seleccionada aparecen en la página Claves de cifrado.

Bloqueo de una clave de cifrado

Cuando el estado de una clave de cifrado está bloqueado, no se pude aplicar a ningún equipo protegido hasta que se desbloquee. Para bloquear una clave de cifrado con el tipo Universal, debe cambiar primero su tipo a Replicado.

Complete los pasos de este procedimiento para bloquear una clave de cifrado.

1. Vaya al Rapid Recovery Core.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Claves de cifrado**.

   Aparece la página **Claves de cifrado**. La columna Estado indica qué claves de cifrado están desbloqueadas y muestra el tipo de cada clave.
3. Localice la clave de cifrado que desea bloquear. Si el tipo es Universal, a continuación, haga clic en el menú desplegable y seleccione **Cambiar el tipo a Replicado**.

   Aparece el cuadro de diálogo **Cambiar tipo de clave de cifrado**.
4. En el cuadro de diálogo, confirme que desea cambiar el tipo de clave a **Replicado**.
5. Si ha cambiado correctamente el estado de la clave de cifrado a Replicado, haga clic en su menú desplegable y seleccione **Bloquear**.

   Aparece el cuadro de diálogo **Bloquear clave de cifrado**.
6. En el cuadro de diálogo, confirme que quiere bloquear la clave.

   Se cerrará el cuadro de diálogo y el estado de la clave de cifrado seleccionada será ahora Bloqueado.

NOTE: Esta opción está disponible para claves de cifrado que se incorporaron por replicación.

Modificación de una clave de cifrado

Después de definir una clave de cifrado, puede modificar el nombre de la clave de cifrado o la descripción de la clave. Estas propiedades están visibles cuando ve la lista de claves de cifrado del panel Claves de cifrado.

Complete los pasos de este procedimiento para editar el nombre o la descripción de una clave de cifrado desbloqueada existente.

CAUTION: Después de modificar el nombre o la descripción de una clave de cifrado que se utiliza para proteger a uno o más equipos, Rapid Recovery toma una nueva imagen base. La instantánea de la imagen base se produce en ese equipo en la siguiente instantánea programada o forzada.

1. Vaya al Rapid Recovery Core.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Claves de cifrado**.

   Aparece la página **Claves de cifrado**.
3. Ubique la clave de cifrado que desea editar y, haga lo siguiente:
   - Si la clave está bloqueada, primero debe desbloquearla. Consulte Desbloqueo de una clave de cifrado.
   - Si la clave está desbloqueada, continúe como se describe a continuación.
4. Haga clic en el menú desplegable para la clave de cifrado especificado, y seleccione **Editar**.

   Aparecerá el cuadro de diálogo **Editar clave de cifrado**.
5. En el cuadro de diálogo, edite el nombre o la descripción de la clave de cifrado y, a continuación, haga clic en **Aceptar**.

El cuadro de diálogo se cierra y los cambios de la clave de cifrado seleccionada aparecen en la página **Claves de cifrado**.

Cambio de la frase de contraseña de la clave de cifrado

Para mantener el máximo de seguridad, puede cambiar la frase de contraseña de cualquier clave de cifrado. Complete los pasos de este procedimiento para cambiar la frase de contraseña de una clave de cifrado.

> **CAUTION: Después de modificar la frase de contraseña de una clave de cifrado que se utiliza para proteger a uno o más equipos, el Core de Rapid Recovery captura una instantánea incremental para ese equipo en la siguiente instantánea programada o forzada.**

1. Vaya al Core de Rapid Recovery.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Claves de cifrado**.

   Aparece la página **Claves de cifrado**.
3. Localice la clave de cifrado que desea actualizar, haga clic en el menú desplegable y seleccione **Cambiar frase de contraseña**.

   Aparecerá el cuadro de diálogo **Cambiar frase de contraseña**.
4. En el cuadro de diálogo, en el campo **Frase de contraseña**, introduzca la nueva frase de contraseña para el cifrado.
5. En el campo **Confirmar la frase de contraseña**, vuelva a escribir la misma frase de contraseña.
6. Haga clic en **Aceptar**.

   El cuadro de diálogo se cierra y la frase de contraseña se actualiza.
7. De manera opcional, si utiliza una sugerencia en el campo Descripción, edite la clave de cifrado para actualizar la sugerencia. Para obtener más información, consulte Modificación de una clave de cifrado.

> **CAUTION: Rapid Recovery utiliza cifrado AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) con claves de 256 bits. Quest recomienda que guarde la frase de contraseña en un lugar seguro y mantenga esta información actualizada. El servicio de asistencia técnica de Quest no puede recuperar una frase de contraseña. Sin la frase de contraseña, no podrá recuperar información de los puntos de recuperación cifrados.**

Exportación de una clave de cifrado

Puede exportar una clave de cifrado desde cualquier Core de Rapid Recovery con el propósito expreso de utilizarla en otro Core. Cuando realiza este procedimiento, la clave se guarda en la carpeta **Descargas** de la cuenta de usuario activa de Windows.

Complete los pasos de este procedimiento para exportar una clave de cifrado.

1. Vaya al Core de Rapid Recovery.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Claves de cifrado**.

   Aparece la página **Claves de cifrado**.
3. Localice la clave de cifrado que desea exportar, haga clic en el menú desplegable y seleccione **Exportar**.

Aparece el cuadro de diálogo **Abrir clave de cifrado-[name.key]**.

4. En el cuadro de diálogo, seleccione **Guardar archivo** para guardar y almacenar las claves de cifrado en una ubicación segura y, a continuación, haga clic en **Aceptar**.

   La clave de cifrado se descarga como un archivo de texto en la ubicación predeterminada, como la carpeta **Descargas** de la cuenta de usuario de Windows activa.

5. De forma opcional, si desea importar esta clave en un Core diferente, copie el archivo en una ubicación accesible desde ese Core.

Eliminación de una clave de cifrado

Al eliminar una clave de cifrado de la página claves de cifrado, la clave se borra del Core de Rapid Recovery.

NOTE: La eliminación de una clave de cifrado no descifra los puntos de recuperación ya guardados con la clave. Todavía debe conservar y proporcionar la frase de contraseña de la clave para recuperar los datos para los puntos de recuperación encriptados existentes.

No es posible eliminar una clave de cifrado que ya esté asociada con cualquier equipo protegido. Primero debe ver la configuración del cifrado de cada equipo protegido que utilice la clave, y desasociar la clave de cifrado que desea eliminar. Para obtener más información, consulte el tema Desasociación de una clave de cifrado de un equipo protegido.

Complete los pasos de este procedimiento para quitar una clave de cifrado.

1. Vaya al Core de Rapid Recovery.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Claves de cifrado**.

   Aparece la página **Claves de cifrado**.
3. Localice la clave de cifrado que desea quitar. Haga clic en el menú desplegable y seleccione **Eliminar**.

   Se abrirá el cuadro de diálogo **Eliminar clave de cifrado**. Verá un mensaje que confirma la acción para quitar la clave de cifrado.
4. En el cuadro de diálogo, confirme que desea quitar la clave de cifrado.

   NOTE: La eliminación de una clave de cifrado no descifra los puntos de recuperación ya guardados con la clave. Todavía debe conservar y proporcionar la clave para recuperar los datos para los puntos de recuperación encriptados existentes.

   El cuadro de diálogo se cierra y la clave de cifrado quitada deja de aparecer en la página **Claves de cifrado**.

Cambio de los tipos de clave de cifrado

Las claves de cifrado enumeran uno de los dos tipos posibles en el panel Claves de cifrado: Universal o Replicación. El tipo indica que origen probable de la clave de cifrado y determina si puede cambiar sus detalles o la frase de contraseña. Puede modificar estos atributos únicamente si el tipo es Universal. Si necesita modificar estos atributos para una clave con el tipo Replicación, debe cambiar su tipo a Universal mediante este procedimiento. Cuando cambia el tipo de una clave de cifrado a Universal, se desbloquea manualmente y puede utilizarse para cifrar otros equipos protegidos.

NOTE: Debe conocer la frase de contraseña para cambiar el tipo de Replicación a Universal.

Las claves de cifrado también tienen dos posibles estados: Bloqueado o Desbloqueado. El estado controla su capacidad de aplicar una clave de cifrado a un equipo protegido, o para restaurar datos desde un punto de

recuperación con cifrado. Puede cambiar el tipo de una clave de cifrado manualmente únicamente si el estado es Desbloqueado.

Cuando crea por primera vez una clave de cifrado, su tipo es Universal y su estado Desbloqueado. Puede utilizar dicha clave inmediatamente (por ejemplo, para cifrar copias de seguridad de un equipo protegido). Sin embargo, una clave de tipo Universal no se puede bloquear manualmente. Si desea bloquear manualmente una clave de cifrado con el tipo Universal, deberá cambiar el tipo a Replicación mediante este procedimiento.

No se puede cambiar una clave de cifrado tipo si ya está en uso cifrando puntos de recuperación para uno o más equipos protegidos.

Siga este procedimiento para cambiar el tipo de una clave de cifrado.

1. Vaya al Core de Rapid Recovery.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Claves de cifrado**.

   Aparece la página **Claves de cifrado**. Todas las claves de cifrado accesibles al Core aparecen en una tabla de resumen. Cada una muestra un tipo de Universal o Replicación.
3. Localice la clave de cifrado que quiere actualizar.
4. Si quiere cambiar una clave de cifrado de Universal a Replicación, haga lo siguiente:
   a. Haga clic en el menú desplegable y seleccione **Cambiar el tipo a Replicación**.

   Aparece el cuadro de diálogo **Cambiar tipo de clave de cifrado**. Se muestra un mensaje que confirma que desea cambiar el tipo a Replicación.

   - En el cuadro de diálogo, confirme que desea cambiar el tipo a Replicación.

   El cuadro de diálogo se cierra y se actualiza el tipo de clave de cifrado a Replicación.
5. Si quiere cambiar una clave de cifrado de Replicación a Universal, haga lo siguiente:
   a. Haga clic en el menú desplegable y seleccione **Cambiar el tipo a Universal**

   Aparece el cuadro de diálogo **Cambiar tipo de clave de cifrado**. Se muestra un mensaje que confirma que desea cambiar el tipo a Universal.

   - En el cuadro de diálogo, en el campo **Frase de contraseña**, introduzca la frase de contraseña y, a continuación, haga clic en **Aceptar** para confirmar que desea cambiar el tipo a Universal.

   El cuadro de diálogo se cierra y se actualiza el tipo de clave de cifrado a Universal.

Protección de máquinas

Esta sección describe cómo proteger, configurar y administrar los equipos protegidos en su entorno de Rapid Recovery.

Acerca de la protección de los equipos con Rapid Recovery

Para proteger sus datos mediante Rapid Recovery, debe añadir las estaciones de trabajo, servidores, equipos de escritorio y portátiles que desea proteger a su Rapid Recovery Core.

En la Rapid Recovery Core Console, mediante uno de los asistentes para proteger un equipo, puede identificar los equipos que desea proteger. Puede hacer lo siguiente:

- Proteja un solo equipo con el asistente para proteger un equipo, que se conecta al equipo que utiliza un nombre de host de red o dirección IP. Para obtener más información sobre cómo proteger un único equipo, consulte Protección de un equipo.
- Proteja un clúster de red con el asistente Proteger clúster, que se conecta al clúster y sus nodos mediante un nombre de host de red o dirección IP. Para obtener más información sobre cómo proteger un clúster, consulte Protección de un clúster.
- Proteja varios equipos de forma simultánea mediante el asistente para proteger varios equipos. Este asistente le permite conectarse a los equipos asociados con un servidor Microsoft Active Directory, a equipos en un host ESXi o vCenter o a equipos en un host o clúster Hyper-V. También puede introducir manualmente la información de conexión (nombre de host de red o dirección IP, nombre de usuario y contraseña) para varios equipos. Para obtener más información sobre cómo proteger varios equipos, consulte Acerca de la protección de varios equipos.

NOTE: Quest recomienda limitar el número de equipos para proteger de manera simultánea a 50 o menos para evitar experimentar restricciones de recursos que puedan provocar que falle la operación de protección.

Cuando identifique los requisitos de protección de un equipo individual en el asistente, puede especificar qué volúmenes desea proteger. Al proteger varios equipos, todos los volúmenes se protegen de manera predeterminada. (Puede cambiar esto más adelante en base al equipo individual).

Al proteger una máquina virtual en un host vCenter/ESXi o Hyper-V, debe definir si protegerla mediante la función Rapid Snap for Virtual o instalando Rapid Recovery Agent. Para obtener más información, consulte Factores para elegir la protección con o sin agente.

El asistente también le permite definir un programa personalizado de protección (o volver a utilizar un programa existente).

Mediante las opciones avanzadas, puede agregar medidas de seguridad adicionales al especificar o aplicar una clave de cifrado a las copias de seguridad de los equipos que desea proteger.

Finalmente, si no hay ninguno, puede definir un repositorio utilizando el asistente.

Después de instalar el software Agent, cada máquina debe reiniciarse tras la instalación.

Para obtener más información sobre cómo proteger las estaciones de trabajo y los servidores, consulte Protección de un equipo.

Factores para elegir la protección con o sin agente

La función Rapid Snap for Virtual de Rapid Recovery es compatible en vCenter/ESXi o en hipervisores Hyper-V. Esta función, también conocida como protección sin agente, le permite proteger máquinas virtuales en su Core sin instalar el software Rapid Recovery Agent en cada máquina invitada.

Recomendaciones generales

Con versión 6.2, la función Rapid Snap for Virtual de Rapid Recovery casi ha logrado la paridad con la protección proporcionada al instalar el software Rapid Recovery Agent. Como regla general, Quest recomienda utilizar la protección sin agente en máquinas virtuales ESXi o Hyper-V. Si el software Agent está instalado en máquinas virtuales ESXi o Hyper-V, a menos que haya una razón convincente para proteger explícitamente su máquina virtual utilizando Rapid Recovery Agent, Quest recomienda eliminar el software Agent y proteger sus máquinas virtuales sin agente.

La protección sin agente tiene algunas ventajas y algunas limitaciones. Esto se describe con claridad en el tema Comprensión de Rapid Snap for Virtual.

Las excepciones a la recomendación de utilizar protección sin agente son las siguientes:

- Recopilar metadatos para máquinas sin agente es más lento que para máquinas protegidas por el software Rapid Recovery Agent. Si experimenta problemas de rendimiento relacionados con los metadatos (específicamente para máquinas de Exchange Server o SQL Server protegidas sin agente), Asistencia para la protección de datos de Quest puede sugerir la instalación del Agent basado en software en servidores de aplicaciones específicos para solucionar problemas.
- Si protege solo una o dos máquinas virtuales en un hipervisor con varios sockets, puede consumir menos licencias instalando Agent directamente en las máquinas virtuales en lugar de hacerlo en el host.
- Si necesita funciones exclusivas de Rapid Recovery Agent, instale el software Agent en las máquinas virtuales pertinentes.

Algunas funciones son exclusivas en la protección instalando el software Rapid Recovery Agent. Esto se aplica a los siguientes ejemplos:

- Realizar una comprobación de conectabilidad de SQL es una capacidad del software Rapid Recovery Agent. Si protege su máquina SQL Server sin agente, debe realizar comprobaciones de conectabilidad de SQL utilizando una instancia de SQL Server instalada en el servidor de Core. Para realizar esta comprobación, debe ajustar la configuración de conectabilidad de su Core a **Utilizar SQL Server en el Core**.
- Los volúmenes dinámicos protegidos sin agente están protegidos al nivel de disco, no de volumen.
- Live Recovery es una función del software Rapid Recovery Agent. No puede utilizar esta función al restaurar volúmenes protegidos utilizando Rapid Snap for Virtual.

Si necesita cualquiera de las características descritas en la lista anterior para una máquina virtual específica, Quest recomienda instalar Agent en lugar de proteger la máquina virtual sin agente.

Para obtener más información, consulte el tema Comprensión de Rapid Snap for Virtual.

Conceptos de consumo de licencia de la versión 6.2

Rapid Recoveryversión 6.2 interrumpe el uso de determinados grupos de licencias aplicables para Windows Server, hosts Hyper-V, sockets VMware, servidores Exchange, servidores SQL Server, servidores Linux, etc. El nuevo modelo está considerablemente simplificado.

Como se describe en el tema Administración de licencias, Rapid Recovery versión 6.2 solo utiliza dos grupos de licencias: Capacity y Enterprise. Si la concesión de licencias de su Core está configurada para utilizar un grupo de licencias Capacity, no puede utilizar otro tipo de grupo.

NOTE: En el futuro, Quest añadirá grupos de licencias basados en otras unidades de medida. Los grupos Capacity y Enterprise seguirán existiendo.

Los dispositivos DL utilizan la concesión de licencias Capacity y no se ven afectados por las restricciones de grupo de licencias. De igual modo, los entornos Rapid Recovery basados en software que utilizan concesión de licencias Capacity front-end no reciben beneficios de licencia por utilizar protección sin agente. Otras ventajas de utilizar la protección sin agente son relevantes incluso con grupos de licencias Capacity en uso.

Si su entorno Rapid Recovery versión 6.2 utiliza un grupo de licencias Enterprise, se aplican las siguientes reglas:

- Los hosts de hipervisor Hyper-V o vCenter/ESXi protegidos con Rapid Recovery Agent consumen una licencia del grupo por cada uno de los sockets de procesador. Si su host de hipervisor tiene seis sockets de CPU, consume 6 licencias del grupo Enterprise.
- Cualquier otra máquina (física o virtual) protegida en su Core con Rapid Recovery Agent consume una licencia de ese grupo. Esto se aplica incluso a los servidores de aplicaciones (como Exchange Server, SQL Server o base de datos de Oracle 12c) con varios sockets de CPU.

Ventajas de licencia de utilizar la protección sin agente

Puede proteger máquinas virtuales invitadas en un host de hipervisor vCenter/ESXi ejecutando el Asistente para proteger varios equipos. En la página **Conexión** de este asistente, si especifica **Proteger VM seleccionadas sin agentes**, las máquinas virtuales invitadas del host se protegen sin agente. Estas máquinas virtuales no consumen licencias de su grupo de licencias. Si Rapid Recovery Agent no está instalado en el host, añadir este host a su Core consume una licencia por cada socket de CPU.

Cuando protege un servidor Hyper-V, Rapid Recovery Agent se instala en el host. Por cada socket de CPU de dicho host de hipervisor, se consume una licencia de su grupo Enterprise. Si especifica que desea proteger el servidor Hyper-V sin agente, las máquinas virtuales invitadas se protegen sin agente y no consumen licencias de su grupo de licencias disponible.

Cuando protege un clúster Hyper-V, Rapid Recovery Agent se instala en cada nodo del clúster. Solo consume una licencia de su grupo de licencias. Se consumen el número total de sockets de CPU del clúster. Si especifica que desea proteger el clúster Hyper-V sin agente, las máquinas virtuales invitadas se protegen sin agente y no consumen licencias de su grupo de licencias disponible del clúster.

La principal ventaja de utilizar Rapid Snap for Virtual consiste en una reducción del consumo de licencias de su grupo de licencias Enterprise para las máquinas virtuales que protege. Si especifica una protección sin agente para un host de hipervisor ESXi o un servidor o clúster Hyper-V, las nuevas máquinas virtuales creadas en el host se protegen sin agente automáticamente, y no consumen licencias de su grupo de licencias Enterprise.

Si algunas de las máquinas virtuales de dicho host de hipervisor tenía Rapid Recovery Agent previamente instalado y su Core tiene Rapid Recovery versión 6.2, debería realizar una de las siguientes acciones:

- Eliminar el software Agent para proteger la máquina virtual sin agente. No se consumen licencias de su grupo.
- Añadir manualmente la máquina a la protección sin agente.
- Si necesita que la máquina esté protegida por Agent y el host está añadido al Core, asociar la máquina virtual con su host primario. Así obtiene la ventaja de la protección basada en Agent y no se consume licencia.
- No cambiar nada. La máquina virtual está protegida mediante las API de Rapid Recovery Agent y solo se consume una licencia.

Cada máquina virtual de un hipervisor añadida a su Core se protege sin agente y sin consumir licencia. Para obtener esta ventaja, debe hacer lo siguiente:

La principal ventaja de utilizar Rapid Snap for Virtual consiste en una reducción del consumo de licencias de su grupo de licencias Enterprise para las máquinas virtuales que protege. Cada máquina virtual de un hipervisor

añadida a su Core se protege sin agente y sin consumir licencia. Para obtener esta ventaja, debe hacer lo siguiente:

- **Proteger VM sin Agent.** Puede proteger máquinas virtuales de forma explícita mediante el asistente para proteger varios equipos. Al proteger un host de hipervisor, también puede seleccionar la opción **Protección automática de las nuevas máquinas virtuales**, que protege de forma implícita las nuevas máquinas virtuales en cuanto se crean.
- **Asociar la máquina virtual invitada con su host de hipervisor protegido.** Si está instalado Rapid Recovery Agent, sus API (y no las nativas del hipervisor) se utilizan para proteger la máquina virtual. Sin embargo, puede reducir el consumo de licencias asociando la máquina virtual con el host añadido al Core. Esta asociación se realiza a nivel de máquinas virtuales por cada máquina virtual. El proceso de vinculación de la máquina virtual invitada con su host de hipervisor primario se describe en el paso 3 del procedimiento Visualización y modificación de la configuración de equipos protegidos.
- **Desinstalar Agent.** A menos que se recomiende lo contrario, elimine todas las copias del software Agent de la máquina virtual.

Para ver una explicación de las ventajas y limitaciones de la protección sin agente, los softwares adicionales recomendados, los requisitos mínimos del host y mucho más, consulte el tema Comprensión de Rapid Snap for Virtual.

Acerca de la protección de equipos Linux con Rapid Recovery

El software Rapid Recovery Agent es compatible con varios sistemas operativos basados en Linux (para obtener más detalles, consulte los requisitos del sistema definidos ahora en la *Rapid Recovery System Requirements Guide (Guía de requisitos del sistema de Rapid Recovery)*). El Rapid Recovery Core solo es compatible con equipos Windows. Aunque puede administrar equipos protegidos Linux desde la Rapid Recovery Core Console, varios procedimientos para equipos Linux tienen pasos que difieren de sus equivalentes Windows. También puede realizar algunas acciones directamente en equipos protegidos Linux mediante la utilidad de la línea de comandos local_amount.

NOTE: Anteriormente, la utilidad local_amount se llamaba aamount.

Si desea proteger un único equipo Linux, ahora puede utilizar el Asistente para proteger un equipo. Consulte el tema "Protección de un equipo". Para proteger varios equipos Linux de forma simultánea utilizando el asistente desde la Core Console, consulte el tema Protección de varios equipos manualmente.

Para implementar o instalar el software Agent en un equipo Linux desde la Core Console, debe contar con lo siguiente:

- La cuenta de usuario debe disponer de privilegios SUDO.
- El equipo Linux que desea proteger debe disponer de acceso a un servidor SSH.

Si un equipo Linux que desea proteger no cumple estos requisitos previos, consúltelo con un administrador de Linux. Cuando cumpla con estos requisitos podrá completar el asistente pertinente para implementar e instalar el software Agent.

Acerca de la protección de servidores de bases de datos de Oracle

Rapid Recoveryversión 6.2 amplía la asistencia de la aplicación para que incluya protección basada en Agent de los servidores de bases de datos relacionales de Oracle 12c. Puede proteger un servidor de bases de datos de Oracle y todas sus bases de datos, y realizar las tareas relacionadas.

En esta versión, se aplican las siguientes restricciones:

- Oracle 12c es la única versión probada y compatible con la protección en el Rapid Recovery Core. Utilice cualquier otra versión de Oracle bajo su propia responsabilidad.
- Los servidores de bases de datos de Oracle protegidos deben ejecutar las versiones de 64 bits de Windows Server 2012 R2 x64 o Windows Server 2016.
- Debe instalar el software del Agent de Rapid Recovery (versión 6.2 o posterior) en el servidor de Oracle. La protección sin agentes se planifica para una versión futura.
- La protección de las bases de datos de Oracle 12c se limita al uso de Volume Snapshot Service (VSS) (Servicio de instantánea de volumen) en el modo ARCHIVELOG.

  NOTE: La asistencia para NOARCHIVELOG (el modo de registro de la base de datos de Oracle predeterminado) se planifica para una versión futura. Las bases de datos de Oracle con el modo ARCHIVELOG habilitado también deben estar establecidas para archivar todos los registros de repetición en línea con el proceso ARCH (archivar). Un administrador de base de datos (DBA) pueda cambiar el modo y establecer el archivado de los registros de repetición con Oracle SQL*Plus u Oracle Enterprise Manager. Para obtener más información sobre la habilitación del modo ARCHIVELOG y el archivado, consulte la documentación de Oracle o a un DBA de Oracle 12c cualificado.

Para proteger por completo los servidores Orable, realice las siguientes tareas:

- Instale el software del Agent deRapid Recovery (versión 6.2 o posterior) en el servidor de Oracle e inicie la protección. Utilice el asistente de protección del equipo para ubicar el servidor Oracle en su red, implementar el software del Agent y establecer una programación para protección. Para obtener más información, consulte Acerca de la protección de los equipos con Rapid Recovery.
- Introduzca sus credenciales para cada base de datos en la Rapid Recovery Core Console. El Core obtiene de manera segura las credenciales y le permite acceder a los metadatos desde la interfaz de usuario. Antes de introducir las credenciales, no puede ver los detalles de las bases de datos sobre el servidor de Orable protegido. Para obtener más información, consulte Introducción o edición de credenciales para las bases de datos de Oracle.
- Active el modo de registro de archivo del servidor protegido de Orable y compruebe el escritor de Oracle VSS, en la Core Console. Para obtener más información, consulte Activación del modo de registro de archivo y adición de VSS Writer en las bases de datos de Oracle protegidas.
- Revise la directiva de truncamiento del registro y configúrelo según sea necesario. Cuando una base de datos de Oracle está establecida en el modo de registro, los registros se acumulan rápidamente y consumen un espacio en disco considerable. Por esta razón, un trabajo nocturno está establecido de manera predeterminada para truncar automáticamente los registro de Oracle. Puede configurar tres opciones de eliminación para este trabajo nocturno, o puede desactivarlo. Para obtener más información, consulte Acerca del truncamiento de los registros de Oracle.

  También puede truncar manualmente los registros de la base de datos de Oracle a petición. Para obtener más información acerca de este procedimiento, consulte Truncamiento manual de registros de la base de datos de Oracle.

Una vez haya instalado el Agent, protegido el equipo en el Core y configurado los ajustes de manera adecuada, puede realizar lo siguiente:

- **Ver los metadatos.** Desde la página **Resumen** del equipo protegido, puede ver los metadatos de cada base de datos en el servidor de Oracle, incluida la conexión y el estado de cada archivo de registro, archivo de control y archivo de datos.
- **Comprobar integridad de la base de datos.** Puede realizar comprobaciones de integridad desde la Core Console utilizando la utilidad DBVERIFY.
- **Truncar registros de archivo**, utilizando una de las tres políticas de eliminación.
- **Restaurar base de datos.** Restaurar volúmenes completos, o volúmenes que contienen bases de datos seleccionadas. Una vez haya activado el modo de registro de archivo, las instantáneas de la base de datos de Oracle son coherentes con bloqueos desde el punto de vista del servicio de Oracle.
- **Realizar la exportación virtual.** Puede realizar una exportación única o configurar una máquina virtual en espera que actualice continuamente la máquina virtual con información nueva, a medida que las copias de seguridad de las bases de datos se capturan.

  Si inicia una máquina virtual de una base de datos de Oracle, puede iniciar de manera manual los servicios de la base de datos y deshabilitar manualmente el modo de copia de seguridad de los archivos de datos de la base de datos.

Introducción o edición de credenciales para las bases de datos de Oracle

Antes de realizar este procedimiento, primero debe añadir un servidor de bases de datos de Oracle para la protección en su Core.

Para introducir o editar las credenciales de la base de datos de Oracle:

- La cuenta de usuario de Windows del usuario de Rapid Recovery que efectúa este procedimiento debe contar con privilegios SYSDBA en el servidor de bases de datos protegidas.
- El servidor del Rapid Recovery Core deberá poder acceder a la base de datos y se deberá establecer con éxito una conexión.

NOTE: SYSDBA es un privilegio administrativo de bases de datos de sistemas de Oracle necesario para realizar operaciones administrativas de alto nivel. Estas funciones incluyen la creación, el inicio, el apagado, la realización de copias de seguridad o la recuperación de una base de datos de Oracle.

Tras proteger el servidor de bases de datos de Oracle, no podrá acceder a los metadatos de la base de datos o ver los detalles de la base de datos hasta que introduzca las credenciales de cada base de datos. Este paso único copia en caché las credenciales de la base de datos de forma segura y proporciona a la Core Console acceso a la información de estado de todos los archivos de registro de transacciones protegidos, los archivos de control y los archivos de datos que integran las bases de datos de Oracle.

Por ejemplo, en la página **Resumen** del equipo de Oracle protegido, antes de introducir las credenciales, no podrá ampliar los detalles de cualquiera de las bases de datos protegidas del panel Información de servidor de Oracle.

NOTE: El siguiente paso es un paso único necesario en cada nueva base de datos de Oracle protegida.

Complete los pasos de este procedimiento para proporcionar a la Rapid Recovery Core Console acceso a los metadatos necesarios de las bases de datos de Oracle protegidas.

1. Vaya al equipo Oracle protegido en la Rapid Recovery Core Console.

Aparece la página **Resumen** para el equipo protegido.

2. En la página **Resumen**, desplácese hacia abajo hasta el panel **Información del servidor de Oracle**.
3. En la primera base de datos de la tabla, haga clic en la lista desplegable (Más opciones) y seleccione **Editar credenciales**.

   Se mostrará el cuadro de diálogo **Editar credenciales de instancia**.
4. Se admiten dos tipos de conexión: básica y Transparent Network Substrate (TNS, una tecnología de sistemas de red exclusiva de Oracle). Realice uno de los siguientes pasos:
   - Para conectarse con una conexión básica, introduzca la información de la siguiente tabla:

Opción	Descripción
Tipo de conexión	Básico
Nombre de host	Introduzca el nombre del host o la dirección IP.
Puerto	Introduzca el puerto correspondiente. El puerto predeterminado abierto para este fin es 1521.
SID o nombre del servicio	Seleccione el método de conexión correspondiente. Puede utilizar uno de los siguientes métodos: • **SID.** El identificador del sistema de Oracle (SID) es un identificador exclusivo que identifica de forma única la instancia de base de datos. • **Nombre del servicio.** El nombre del servicio es el alias de TNS utilizado para conectarse de forma remota a su base de datos. **NOTE:** El nombre del servicio se puede encontrar en el archivo TNSNAMES.ORA.
Nombre del servicio	El nombre del servicio es el alias de TNS que introduce al conectarse de forma remota a su base de datos y a este servicio.

   - Para conectarse con TNS, introduzca la información de la siguiente tabla:

Opción	Descripción
Tipo de conexión	TNS
Alias de red	Seleccione este menú desplegable para ver los alias de las bases de datos disponibles en la red y seleccione el alias correspondiente.

5. Se admiten dos tipos de credencial: Oracle y sistema operativo. Realice uno de los siguientes pasos:
   - Para conectarse con las credenciales de Oracle, introduzca el nombre de usuario y la contraseña de la base de datos de Oracle en los campos de texto correspondientes.

     NOTE: Su cuenta de usuario de Windows debe disponer de privilegios SYSDBA.
   - Para conectarse con las credenciales copiadas en caché del sistema operativo, seleccione **Sistema operativo**.

NOTE: Su cuenta de usuario de Windows debe ser miembro del grupo local ORA_DBA, con lo que se garantiza que el usuario cuenta con privilegios SYSDBA.

6. Para comprobar las credenciales, haga clic en **Comprobar**.

   Aparecerá un cuadro de diálogo, en el que se indicará si la prueba de conexión se ha realizado con éxito.
7. Realice uno de los siguientes pasos:
   - Si se efectúa la verificación correctamente, haga clic en **Aceptar** para cerrar el cuadro de diálogo de mensaje.
   - Si no se realiza correctamente, cierre el cuadro de diálogo y revise las credenciales de la instancia hasta que se verifique la conexión. Consulte con el administrador de su sistema si tiene preguntas acerca de las credenciales.
8. En el cuadro de diálogo **Editar credenciales de instancia**, tras la verificación correcta, haga clic en **Aceptar**.

   El cuadro de diálogo se cerrará y la Rapid Recovery Core Console aplicará y copiará en caché las credenciales de forma inmediata. Muy poco después, los metadatos estarán disponibles en la Core Console y el indicador de estado de la base de datos seleccionada mostrará un estado verde (con conexión).
9. Repita los pasos 3 a 8 en todas las bases de datos que aparezcan en el panel Información de servidor de Oracle.

Después de introducir y copiar en caché las credenciales de todas las bases de datos de este equipo de Oracle protegido, realice los procedimientos que se describen en el tema Activación del modo de registro de archivo y adición de VSS Writer en las bases de datos de Oracle protegidas.

Activación del modo de registro de archivo y adición de VSS Writer en las bases de datos de Oracle protegidas

Antes de realizar este procedimiento, primero debe añadir un servidor de bases de datos de Oracle para la protección de su Core e introducir las credenciales de cada base de datos en la Core Console.

Las aplicaciones de base de datos requieren la presencia de una combinación de archivos específicos (tales como archivos de configuración, registro y control), cada uno de ellos configurados en un estado específico, para que sean coherentes con la aplicación. En versión 6.2, las bases de datos de Oracle requieren que se habilite el modo de registro de archivo. Hasta que lleve a cabo este procedimiento, las instantáneas que realice del servidor de bases de datos serán coherentes con el bloqueo, pero no coherentes con la aplicación.

Oracle VSS Writer se utiliza para capturar instantáneas con el Servicio de instantáneas de volumen. Este escritor debe estar habilitado.

NOTE: Los siguientes pasos son pasos únicos necesarios en cada nueva base de datos de Oracle protegida.

Complete los pasos de este procedimiento para comprobar si está habilitado el modo de registro de archivo, para habilitar este modo si es necesario y para añadir VSS Writer a su Core.

1. Vaya al equipo Oracle protegido en la Rapid Recovery Core Console.

   Aparece la página **Resumen** para el equipo protegido.
2. En la página **Resumen**, desplácese hacia abajo hasta el panel **Información del servidor de Oracle**.
3. En el panel **Información de servidor de Oracle**, si observa una notificación de advertencia que indica que el modo de registro de archivo está deshabilitado, haga clic en **Habilitar el modo de registro de archivo en estas bases de datos** y, a continuación, haga clic para confirmar el reinicio de las instancias de base de datos.

NOTE: Al habilitar el modo de archivado, las instancias de base de datos pertinentes se reinician. Esta operación podría tardar unos minutos.

4. En el panel **Información de servidor de Oracle**, si observa una notificación de advertencia que indica que Oracle VSS Writer está excluido de las instantáneas, haga clic en **Incluir Oracle VSS Writer** y, a continuación, haga clic para confirmar.

   El mensaje de advertencia se cerrará y VSS Writer se añadirá a su Core.

5. De manera opcional, puede seguir el progreso para la activación del modo de registro de archivo o la adición de VSS Writer. Para obtener más información, consulte Visualización de tareas.

Acerca del truncamiento de los registros de Oracle

El modo de registro de archivo, que se necesita para la asistencia de Oracle enversión 6.2, provoca que un gran número de archivos de registro se acumulen en el servidor de bases de datos, utilizando un valioso espacio de almacenamiento. Los archivos de registro relevantes se incluyen en las copias de seguridad del servidor de Oracle cada vez que una instantánea de punto de recuperación se captura, representando así los registros locales superfluos. Por esta razón, el Rapid Recovery Core incluye varios métodos para truncar los registros de Oracle.

1. El Rapid Recovery Core incluye configuración de trabajos nocturnos para truncar los registros de Oracle. El truncamiento de registros de Oracle está habilitado de manera predeterminada como trabajo nocturno utilizando la directiva de eliminación **Automática**. En este modelo, los registros se truncan una vez al día, cuando se ejecutan los trabajos nocturnos.

   Esta configuración está diseñada para satisfacer las necesidades de la mayoría de los usuarios. Si está satisfecho con este enfoque, no necesita cambiar la configuración. Está habilitada de forma predeterminada.

2. Puede personalizar la configuración del trabajo nocturno del truncamiento del registro de Oracle para un servidor de Oracle específico. Puede elegir entre otras dos directivas de eliminación:

   - La directiva de eliminación **Mantener más reciente** le permite especificar la duración (n días, semanas, meses o años) para retener los registros de Oracle antes del truncamiento. Cuando el plazo expira, los archivos de registro pasan el umbral y se truncan una vez al día cuando se ejecutan los trabajos nocturnos.
   - La directiva de eliminación **Mantener número especificado** le permite especificar un número determinado de archivos de registro para conservarlos. Después de alcanzar el umbral, los registros más recientes se conservan y los más antiguos se trunca una vez al día, cuando se ejecuten los trabajos nocturnos.

   Para obtener más información sobre el truncamiento de trabajos como trabajos nocturnos, consulte el tema Comprensión de los trabajos nocturnos.

3. También puede truncar registros manualmente a petición en cualquier momento. Para obtener más información sobre el tema, consulte Truncamiento manual de registros de la base de datos de Oracle.

El truncamiento de los registros de Oracle, por trabajos nocturnos o manualmente a petición, se produce sin requerir un trabajo de transferencia.

Truncamiento manual de registros de la base de datos de Oracle

Procedimiento adecuado solo para servidores de base de datos de Oracle protegidos en el Core.

Para admitir la protección de las bases de datos de Oracle en Rapid Recovery versión 6.2, se activa un trabajo nocturno para truncar los registros de archivo de Oracle de manera predeterminada. Puede desactivar este trabajo nocturno, que resultará en la acumulación de archivos de registro sustanciales en el servidor de bases de datos local.

En cualquier servidor protegido de Oracle puede truncar de forma manual los registros de la base de datos de Oracle a petición, en cualquier momento. El truncamiento eliminará los registros de archivo del servidor local.

En cada punto de recuperación guardado del repositorio, los registros de la base de datos siguen reflejando el estado de la base de datos en el momento en el que se capturó la instantánea de copia de seguridad.

Complete los pasos de este procedimiento para truncar de forma manual los archivos de registro de Oracle.

1. Vaya al equipo Oracle protegido en la Rapid Recovery Core Console.

   Aparece la página **Resumen** para el equipo protegido.
2. En la página **Resumen**, desplácese hacia abajo hasta el panel **Información del servidor de Oracle**.
3. En la fila de la tabla que representa la instancia de base de datos de Oracle para la que desea truncar los registros, haga clic en la lista desplegable (Más opciones) y seleccione **Forzar truncamiento de registro**.

   Aparece el cuadro de diálogo **Forzar truncamiento de registro**.
4. Si desea eliminar todos los registros de Oracle en el servidor de bases de datos local, desde el menú desplegable **Directiva de eliminación**, seleccione **Automático** y haga clic en **Forzar**.

   Un trabajo de truncamiento de registros se pone en cola. Si el sistema no está ocupado, el trabajo se ejecuta inmediatamente y los registros se truncan.
5. Si desea eliminar todos los registros almacenados localmente desde el servidor de Oracle (copias de lo almacenado en el punto de recuperación más reciente), realice lo siguiente:
   a. En el menú desplegable **Directiva de eliminación**, seleccione **Mantener más reciente**.
   b. En el campo de texto **Mantener registros para**, introduzca un número y, a continuación, desde el menú desplegable del periodo de tiempo, seleccione el periodo de tiempo relevante (**días, semanas, meses** o **años**).
   c. Haga clic en **Forzar**.

   Un trabajo de truncamiento de registros se pone en cola. Si el sistema no está ocupado, el trabajo se ejecuta inmediatamente y los registros se truncan.
6. Si desea conservar un número específico de archivos de registro de Oracle y truncar los registros restantes, realice lo siguiente:
   a. En el menú desplegable **Directiva de eliminación**, seleccione **Mantener número especificado**.
   b. En el campo de texto **Número de archivos archivados**, introduzca un número que represente la cantidad de registros recientes de la base de datos que desea retener.
   c. Haga clic en **Forzar**.

   Un trabajo de truncamiento de registros se pone en cola. Si el sistema no está ocupado, el trabajo se ejecuta inmediatamente y los registros se truncan.
7. Si desea truncar los registros de otras instancias de base de datos en este servidor, repita el paso 3 hasta el paso 6 en cada base de datos relevante enumerada en el panel de información del servidor de Oracle.

Acerca de la administración de servidores de aplicaciones protegidos en el Rapid Recovery Core

Rapid Recovery admite servidores de aplicaciones como SQL Server, Exchange Server y Oracle. Para obtener información acerca de las versiones específicas admitidas por Rapid Recovery, consulte la *Rapid Recovery System Requirements Guide (Guía de requisitos del sistema de Rapid Recovery)*.

Las opciones específicas para estas aplicaciones admitidas aparecen en la Rapid Recovery Core Console cuando se detecta una instancia del software y los archivos en servidores protegidos. En esos casos, hay disponibles opciones adicionales al seleccionar el equipo protegido en Core Console.

Si selecciona un SQL Server protegido en el menú de navegación izquierdo, las opciones de menú que aparecen para ese equipo protegido incluyen la opción del menú desplegable **SQL**.

Por ejemplo: si selecciona un Exchange Server protegido en el menú de navegación izquierdo, las opciones de menú que aparecen para ese equipo protegido incluyen la opción del menú desplegable **Exchange**.

Si selecciona un servidor de Oracle protegido, en la parte inferior de la página de **Resumen** de esa máquina protegida, busque el panel de información del servidor de Oracle, de uso exclusivo para servidores de bases de datos de Oracle protegidos.

Aunque estas opciones funcionen de forma diferente, hay algunas características comunes. Entre las funciones que se pueden realizar únicamente para servidores de SQL Server, Exchange y Oracle se incluyen:

- **Forzado de truncamiento de registros.** El servidor de SQL Server, los servidores de correo de Exchange mail servers y los servidores de bases de datos de Oracle incluyen registros de servidor. El proceso para truncar registros de SQL Server identifica el espacio disponible en el servidor. Cuando trunca registros de un servidor Exchange, además de la identificación del espacio disponible, el proceso también libera más espacio en el servidor. Lo mismo se aplica a Oracle; el truncamiento del registro elimina archivos de registro de archivación del servidor de Oracle para liberar espacio en el servidor protegido.
- **Establecimiento de credenciales para el servidor apropiado.** Los servidores SQL Server permiten establecer credenciales para un equipo SQL Server protegido por separado, o establecer las credenciales predeterminadas para todos los servidores SQL Server protegidos. Los servidores Exchange y Oracle le permiten establecer las credenciales para el equipo protegido en la página **Resumen** del servidor protegido.
- **Visualización del estado de las comprobaciones en los puntos de recuperación de SQL Server, Exchange Server u Oracle Server.** Los puntos de recuperación capturados del SQL Server, Exchange Server u Oracle Server protegido se corresponden con los indicadores de estado de color. Los colores indican el éxito o el error de las diversas comprobaciones relevantes para estos servidores de aplicaciones.

Los siguientes temas tratan la administración de SQL Server, Exchange Server o equipos protegidos de Oracle:

- Comprensión de los indicadores de estado de puntos de recuperación
- Configuración y funciones en servidores SQL Server protegidos
- Configuración y funciones en servidores de Exchange protegidos
- Acerca de la protección de servidores de bases de datos de Oracle

Acerca de la protección de clústeres de servidor

En Rapid Recovery, la protección de clúster de servidor está asociada con los equipos protegidos de Rapid Recovery instalados en nodos de clúster individuales (esto es, equipos individuales en el clúster), y el Rapid Recovery Core, que protege dichos equipos, todo ello como si fueran un único equipo compuesto.

Puede configurar fácilmente un Rapid Recovery Core para proteger y administrar un clúster. En la Core Console, un clúster está organizado como una entidad aparte, que actúa como un contenedor, para incluir los nodos relacionados. Por ejemplo, en el área de navegación izquierda, en el menú **Equipos protegidos**, se enumeran los clústeres protegidos. Justo debajo de cada clúster, aparecen los equipos Agent o los nodos individuales asociados. Cada uno de estos es un equipo protegido en el que está instalado el software Rapid Recovery Agent. Si hace clic en el clúster, aparece la página **Resumen** de la Core Console.

En los niveles de Core y clúster, puede ver información sobre el clúster, como la lista de nodos relacionados y volúmenes compartidos. Al mostrar la información de un clúster en la Core Console, puede hacer clic en **Nodos protegidos**, en la parte superior del menú, para ver una tabla de resumen de los nodos individuales del clúster. En la tabla de resumen, en cada nodo, puede realizar funciones como forzar una instantánea, realizar una exportación única o configurar un servidor virtual en espera, montar o visualizar puntos de recuperación, realizar una restauración desde un punto de recuperación, convertir el nodo de clúster en su propio equipo protegido o eliminar el nodo de la protección. Si el nodo es un servidor Exchange o SQL Server, podrá ver las opciones de los registros de truncamiento.

A nivel de clúster, también puede ver los metadatos correspondientes del clúster de Exchange y SQL para los nodos del clúster. Puede especificar la configuración de todo el clúster y los volúmenes compartidos de dicho clúster.

Si hace clic en cualquier nodo del clúster en el menú de navegación izquierdo, la información que se muestra en la Core Console es específica de ese nodo del clúster. Aquí puede ver la información específica de ese nodo o establecer la configuración solo de ese nodo.

Para obtener información acerca de las configuraciones de clúster y versiones de aplicación admitidas, y acerca de la compatibilidad para volúmenes compartidos de clústeres, consulte la *Rapid Recovery System Requirements Guide (Guía de requisitos del sistema de Rapid Recovery)*.

Comprensión de Rapid Snap for Virtual

La función Rapid Snap for Virtual de Rapid Recovery también se llama "protección sin agente" porque permite proteger máquinas virtuales (VM) en el Core sin instalar el Rapid Recovery Agent en cada máquina virtual.

CAUTION: Quest **recomienda que limite la iniciación de protección sin agentes a no más de 200 máquinas virtuales a la vez. No seleccione más de 200 VM mientras utiliza el Asistente para proteger varios equipos. Intentar iniciar la protección de más de 200 VM reduce el rendimiento de la IU. No existe un límite de VM que un Core pueda proteger sin agentes a lo largo del tiempo. Por ejemplo, hoy podría proteger 200 VM y mañana 200 más.**

Para obtener más información, consulteProtección de máquinas virtuales VMware vCenter/ESXi y Protección de máquinas virtuales en clústeres y servidores Hyper-V.

Protección de máquinas virtuales VMware vCenter/ESXi

Rapid Recovery permite proteger máquinas virtuales vCenter/ESXi sin instalar el Rapid Recovery Agent en la VM o el host ESXi, logrando la protección completa sin agentes. Rapid Recovery utiliza el cliente ESXi y la interfaz de programación de aplicaciones (API) nativos de VMware para detectar y proteger las VM seleccionadas en un solo host. A continuación, el Rapid Recovery Core se comunica con el disco de la máquina virtual (VMDK) para determinar los detalles necesarios de los volúmenes protegidos. Debido a que Rapid Recovery crea puntos de recuperación basados en volúmenes, no VMDK, cada volumen se puede montar, restaurar y exportar por separado.

Técnicamente, Rapid Recovery no protege un host de hipervisor VMware vCenter/ESXi. Cuando se selecciona un host vCenter/ESXi utilizando el Asistente para proteger varios equipos, se añade el host como entidad primaria en el Rapid Recovery Core. Las instantáneas del Core no incluyen archivos de datos ni datos del propio host. Sin embargo, se pueden proteger las VM invitadas en el host. Las VM protegidas se representan en la GUI del Core como secundarias del host primario. Si selecciona la protección sin agente de máquinas virtuales ESXi, el icono de la VM protegida () se muestra diferente al icono de una VM ESXi protegida utilizando Rapid Recovery Agent (por ejemplo, ).

NOTE: Quest recomienda que se instalen las herramientas de VMware en las máquinas virtuales (VM) que quiere proteger en los hosts vSphere o ESXi. Cuando las herramientas de VMware se instalan en una máquina virtual mediante el sistema operativo Windows (SO), las copias de seguridad que recupera el Rapid Recovery Core utilizan Microsoft Volume Shadow Copy Services (VSS) (Servicios de instantáneas de volumen de Microsoft). Esto proporciona capacidad para las copias de seguridad coherentes con la aplicación. Para obtener más información sobre el comportamiento de las VM sin agentes, con o sin herramientas de VMware, consulte Beneficios de instalar herramientas de hipervisor para la protección sin agentes y Comprensión de las copias de seguridad coherentes con el bloqueo y coherentes con la aplicación.

Cuando se instalan las herramientas de VMware, la protección sin agente utiliza el seguimiento de bloqueo cambiado (CBT) de VMware para reducir el tiempo necesario para las instantáneas incrementales. CBT determina qué bloques se han cambiado en el archivo del VMDK, lo que permite a Rapid Recovery realizar copias de seguridad solo de las porciones del disco que han cambiado desde la última instantánea. Este método

de copia de seguridad, a menudo, da como resultado operaciones de copia de seguridad más cortas y un consumo de recursos reducido en los elementos de almacenamiento y de red.

Utilizar la protección sin agentes ofrece varias ventajas. Algunos de los atributos más útiles incluyen las características siguientes:

- No se requiere un software adicional en el equipo host.
- La protección sin agentes le permite optar por proteger automáticamente las nuevas VM agregadas al host ESXi o Hyper-V.
- No es necesario un reinicio durante el proceso de protección.
- Las credenciales no son necesarias para cada una de las VM.
- La protección sin agentes le permite proteger una máquina virtual incluso si está apagada.
- La protección sin agentes le permite restaurar en los discos.
- La protección sin agentes es compatible con todos los sistemas operativos invitados.
- Si asocia una VM invitada con su host de hipervisor primario protegido, no se consume una licencia Enterprise al proteger la VM en el Core.
- De manera opcional, puede proteger y recopilar metadatos deSQL Server y Exchange.
- El Core (no Agent) puede realizar comprobaciones de conectividad, truncamientos de registros y comprobaciones de capacidades de montaje en los puntos de recuperación capturados desde los servidores deSQL y Exchange protegidos.
- La protección sin agentes permite exportar discos o volúmenes dinámicos.

  NOTE: Si los volúmenes dinámicos son complejos (seccionados, en espejo, extendidos o RAID), los exportan como imágenes de disco y transforman los volúmenes después de que la operación de exportación se haya completado en la VM exportada.

Si bien son muchas las razones para utilizar la protección sin agentes para las VM de ESXi, opte por el método de protección que mejor se adapte a sus entornos y necesidades empresariales. Junto con las ventajas mencionadas anteriormente, también debe tener en cuenta las consideraciones siguientes al elegir la protección sin agentes:

- La protección sin agente de los servidores de bases de datos de Oracle no recopila metadatos relacionados con Oracle. Aunque se realicen instantáneas de copia de seguridad de los archivos y del sistema operativo, no se admiten funciones relacionadas con Oracle. Para que exista compatibilidad con la aplicación de base de datos de Oracle, proteja su servidor utilizando Rapid Recovery Agent.
- La protección sin agentes no admite la protección de volúmenes dinámicos (por ejemplo, los volúmenes seccionados, en espejo, extendidos o RAID) a nivel de volumen. Los protege a nivel de disco.
- La protección sin agentes no admite Live Recovery. Para obtener más información acerca de esta función, consulte Descripción de Live Recovery.
- Durante el proceso de restauración de un único volumen en la VM protegida, la VM se reinicia automáticamente.
- La protección sin agentes no muestra la cantidad real de espacio utilizado en una VM si el tipo de disco virtual es "Thick Provision Eager Zeroed".

Si opta por utilizar la protección sin agentes para sus VM de ESXi, el host debe cumplir los requisitos mínimos siguientes para que la protección sin agentes sea correcta.

- El equipo host debe ejecutar la versión de ESXi 5.0.0 compilación 623860 o posterior.
- El equipo host debe cumplir los requisitos mínimos del sistema que se mencionan en la *Rapid Recovery System Requirements Guide (Guía de requisitos del sistema de Rapid Recovery)*.
- Para la protección a nivel de volumen, los VMDK deben incluir las tablas de partición de Master Boot Record (MBR) o de GUID (GPT). Los VMDK sin estas tablas de partición están protegidos como discos enteros, en lugar de como volúmenes individuales.
- Cada máquina virtual de VMware debe tener las herramientas de VMware instaladas para garantizar la coherencia de las instantáneas.

Protección de máquinas virtuales en clústeres y servidores Hyper-V

Para proteger máquinas virtuales de Hyper-V sin agentes, no necesita instalar el Rapid Recovery Agent en cada máquina virtual. Solo tiene que instalarlo en el equipo host o los nodos de clúster. El Agent protege el disco duro virtual del host y convierte los cambios en los archivos del disco duro e una imagen de volumen o una imagen de disco, en función del sistema de archivos. Un nuevo controlador proporciona suporte a nivel de archivos para las máquinas virtuales de hosts y volúmenes compartidos de clúster (CSV).

La compatibilidad sin agente con Hyper-V depende del sistema operativo del host. Hay una lista completa de los sistemas operativos y de los componentes de Rapid Recovery que admite cada uno en la *Rapid Recovery System Requirements Guide (Guía de requisitos del sistema de Rapid Recovery)*. Para obtener más información, consulte el tema "Matriz de compatibilidad e instalación del sistema operativo para la versión 6.2 de Rapid Recovery" en dicho documento.

Quest recomienda que se instalen los servicios de integración de Hyper-V en las máquinas virtuales (VM) que quiere proteger en los hosts Hyper-V. Al instalar los servicios de integración de Hyper-V en una VM con el sistema operativo Windows, las copias de seguridad realizadas por el Rapid Recovery Core utilizan Microsoft VSS. Esto proporciona capacidad para las copias de seguridad coherentes con la aplicación. Para obtener más información sobre el comportamiento de las VM sin agentes, con o sin servicios de integración de Hyper-V, consulte Beneficios de instalar herramientas de hipervisor para la protección sin agentes y Comprensión de las copias de seguridad coherentes con el bloqueo y coherentes con la aplicación.

NOTE: Rapid Recovery admite el formato de archivos de disco VHDx. No admite el formato VHD.

Para proteger máquinas virtuales en un CSV, el Rapid Recovery Agent y el controlador deben estar instalados en cada nodo de clúster mediante la función de implementación automática del Asistente para proteger varios equipos. En los nodos, el Agent puede proteger todas las máquinas virtuales en funcionamiento en los CSV creando dos tipos de cambios para cada archivo. El primer tipo de cambio solo se guarda antes o después de una instantánea o una restauración del sistema de limpieza. El segundo tipo de cambio reside en el disco, lo que hace que haya disponible una instantánea incremental incluso si hay un fallo de alimentación o un apagado con errores. El Agent instalado en el nodo fusiona todos los cambios en uno antes de transferir los datos.

Cuando un host o un nodo están en ejecución, Rapid Recovery crea una copia de seguridad. Si el host no está en ejecución, no se puede crear ninguna copia de seguridad; no obstante, si uno de los nodos no está en ejecución, Rapid Recovery puede continuar tomando instantáneas de las máquinas virtuales en el clúster.

NOTE: Para obtener un mejor rendimiento, se recomienda que el número máximo de transferencias simultáneas del nodo o host de Hyper-V se establezca en 1, que es el valor predeterminado.

La protección de Hyper-V sin agentes tiene las mismas capacidades que la protección tradicional en que el Agent está instalado en cada VM, entre las que se incluyen:

- Archivado
- Comprobaciones de integridad de puntos de recuperación
- Montaje de puntos de recuperación
- Detección automática de las nuevas máquinas virtuales (exclusivo en la protección sin agentes)
- Protecciónde los servidores de SQL y Exchange y recopilación de los metadatos
- Comprobación de la capacidad de montaje de Exchange
- Comprobaciónde conectividad de SQL
- Replicación
- Restauración de máquinas virtuales, incluida la restauración a CSV o a carpetas compartidas CIF
- Restauración de archivos en un formato VHDX de invitados
- Consolidación
- Exportación virtual a máquinas virtuales Hyper-V y otros hipervisores, incluidos ESXi, VMware Workstation y VirtualBox

Sin embargo, hay limitaciones que hay que tener en cuenta al elegir la protección de Hyper-V sin agentes. Las capacidades que no se realizan incluyen:

- Live Recovery
- La restauración de máquinas virtuales en CIFS con el formato VHD
- La restauración de archivos en un formato VHD (.vhd) de invitados
- La restauración de archivos en un formato VHD Set (.vhds) de invitados

NOTE: Para una instantánea coherente con la aplicación, debe tener la controladora SCSI instalada en cada máquina virtual. Sin esta controladora, el resultado es siempre una instantánea coherente con bloqueo.

Asistencia de la aplicación

Rapid Snap for Virtual le permite habilitar una protección sin agentes para lasaplicaciones de SQL Server y Exchange que se ejecutan en las máquinas virtuales de Hyper-V y ESXi. Esta funcionalidad opcional está disponible para las máquinas virtuales que ejecutan sistemas operativos Windows.

NOTE: La asistencia de la aplicación no incluye a las aplicaciones instaladas en las máquinas virtuales Linux.

Después de habilitar la asistencia de la aplicación, se muestran los metadatos de esta en la página **Resumen** de la máquina virtual, así como un icono junto al nombre de la máquina virtual en la página **Equipos**. Si se produce un error que impide la asistencia de la aplicación satisfactoria, el icono cambia de verde a rojo.

Antes de optar por la protección sin agentes de unSQL Server o Exchange Server, tenga en cuenta los siguientes puntos:

- Para proteger la aplicación, la máquina virtual debe estar encendida. El Core no recupera metadatos de equipos apagados.
- Las VM que desea proteger deben tener instaladas las utilidades de herramientas de VMware o de servicios de integración de Hyper-V.
- En una máquina virtual con Exchange Server y SQL Server instalados, no es posible truncar los registros por separado. Si ambas aplicaciones están instaladas, los registros se truncan juntos.
- Las comprobaciones de conectividad de SQL Server están disponibles solo en el Core y no se pueden llevar a cabo en el equipo protegido.
- Para ejecutar el truncamiento del registro en una máquina virtual ESXi, el host debe utilizar la versión de ESXi 6.5 o posterior.

Beneficios de instalar herramientas de hipervisor para la protección sin agentes

Al proteger máquinas virtuales (VM) sin utilizar el Agent Rapid Recovery, Quest recomienda instalar herramientas de VMware en las VM protegidas en hosts vSphere o ESXi. Del mismo modo, Quest recomienda instalar servicios de integración Hyper-V en las VM que desee proteger en hosts Hyper-V.

Instalar estas utilidades de hipervisor nativo permite que Rapid Recovery saque el máximo provecho de la funcionalidad del Servicio de instantáneas de volumen (VSS) de Microsoft.

Cuando se instalan estas utilidades en máquinas virtuales con el sistema operativo Windows, las copias de seguridad que captura el Rapid Recovery Core también pueden utilizar VSS. Cuando no se instalan estas herramientas, Rapid Recovery recopila instantáneas, pero solo en un estado coherente con el bloqueo. Para obtener más información, consulte Comprensión de las copias de seguridad coherentes con el bloqueo y coherentes con la aplicación.

Las siguientes condiciones se aplican en función de si las herramientas de VMware o los servicios de integración Hyper-V están o no instalados y si la VM está encendida:

Tabla 40. Condiciones del tipo de copia de seguridad para las VM

Herramienta de hipervisor	VM encendida	Tipo de copia inteligente
No instalado	Sí	Coherentes con el bloqueo
No instalado	No (cierre con errores)	Coherentes con el bloqueo
No instalado	No (cierre correcto)	Coherente con la aplicación
Instalada	Sí	Coherente con la aplicación
Instalada	No (cierre con errores)	Coherentes con el bloqueo
Instalada	No (cierre correcto)	Coherente con la aplicación

Comprensión de las copias de seguridad coherentes con el bloqueo y coherentes con la aplicación

Al proteger máquinas virtuales sin agente utilizando la función Rapid Snap for Virtual, los datos de las instantáneas de copia de seguridad que se realizaron pueden encontrarse en uno de estos dos estados:

- Coherente con el bloqueo. Como mínimo, todas las copias de seguridad sin agente realizadas por el Rapid Recovery Core son coherentes con el bloqueo. La copia de seguridad es una instantánea de todos los datos y archivos del sistema operativo en cada volumen protegido, tal y como se encontraban en el momento en que se realizó la misma. Si restaura desde un punto de recuperación coherente con el bloqueo, el sistema operativo de la máquina virtual se inicia y puede leer y entender el sistema de archivos y todos los archivos que contenga.

  Si recupera una aplicación transaccional a partir de un estado coherente con el bloqueo, la base de datos vuelve al último estado válido. El estado válido más reciente puede ser desde el momento del bloqueo o anterior al bloqueo. Si es anterior al bloqueo, la base de datos debe actualizar algunos trabajos para que los archivos de datos coincidan con la información de los registros. Este proceso tarda un tiempo cuando abre la base de datos por primera vez, lo que provoca un retraso al iniciar el equipo.
- **Coherente con la aplicación**. Las copias de seguridad coherentes con la aplicación utilizan Microsoft Volume Shadow Copy Service (VSS) para garantizar la coherencia de los datos de aplicaciones cuando se crea una instantánea. Al utilizar escritores VSS, las operaciones de entrada y salida pendientes se completan y los archivos de registro se confirman antes de que se realice la instantánea. Como resultado, si restaura a partir de un punto de sistema coherente con la aplicación, el sistema operativo de la máquina virtual se inicia y puede leer y entender el sistema de archivos. Además, los archivos para aplicaciones transaccionales como SQL Server o Exchange Server se encuentran en estado coherente. Por ejemplo, los registros de SQL Server coinciden con los archivos de datos, y la base de datos se abre rápidamente sin necesidad de reparaciones.

Funcionamiento del instalador del software Rapid Recovery Agent

Rapid Recovery le permite descargar instaladores del Core de Rapid Recovery. En la página **Descargas**, puede elegir entre descargar Agent Installer, Local Mount Utility (LMU) o un archivo MIB de SNMP. Para obtener más información acerca de la LMU, consulte Local Mount Utility. Para obtener más información acerca de la SNMP, consulte Comprensión de la configuración de SNMP.

NOTE: Para acceder a Agent Installer, consulte Descarga del instalador de Rapid Recovery Agent. Para obtener más información sobre la implementación de Agent Installer, consulte la Rapid Recovery Installation and Upgrade Guide (Guía de instalación y actualización de Rapid Recovery).

Agent Installer se utiliza para instalar la aplicación Rapid Recovery Agent en los equipos que el Core de Rapid Recovery debe proteger. Si determina que tiene un equipo que necesita el Agent Installer, puede descargar el instalador web desde la página Descargas de la Core Console de Rapid Recovery.

NOTE: La descarga del Core se realiza desde el Portal de licencias de Rapid Recovery. Para descargar el instalador del Core de Rapid Recovery, visite https://licenseportal.com. Para obtener más información, consulte la Rapid Recovery License Portal User Guide (Guía del usuario del Portal de licencias de Rapid Recovery).

Descarga del instalador de Rapid Recovery Agent

Descargue el instalador de Rapid Recovery Agent e impleméntelo en cualquier equipo que desee proteger en el Rapid Recovery Core. Complete los pasos de este procedimiento para descargar el instalador web.

1. Para descargar el instalador web de Agent directamente desde el equipo que desea proteger, haga lo siguiente:
    a. En un navegador web, abra el Portal de licencias de Rapid Recovery en https://licenseportal.com.
    b. En el menú de navegación izquierdo, haga clic en **Descargas**.
    c. Desde el panel **Aplicaciones basadas en Windows**, desplácese hasta la fila **Windows Agent** y haga clic en **Descargar** según el instalador apropiado (sistemas de 32 bits o de 64 bits).

    El archivo del instalador, por ejemplo, `Agent-X64-6.0.1.xxxx.exe`, se guarda en la carpeta de destino de descargas.
2. Para descargar el instalador web desde el Core, en la barra de iconos de la Core Console, haga clic en el icono **Más** y, a continuación, seleccione **Descargas**.
3. En la página **Descargas**, en el panel **Agent**, haga clic en **Descargar instalador web**.
4. En el cuadro de diálogo **Abrir Agent-Web.exe**, haga clic en **Guardar archivo**.

    El archivo del instalador, por ejemplo, `Agent-X64-6.0.1.xxxx.exe`, se guarda en la carpeta de destino de descargas.
5. Mueva el instalador al equipo adecuado e instale el software Rapid Recovery Agent.

    Para obtener más información acerca de la instalación del software Rapid Recovery Agent, consulte la Installation and Upgrade Guide (Guía de actualización y de instalación) de Rapid Recovery.

Implementación de Agent en varios equipos simultáneamente desde la Core Console

Puede implementar el software Rapid Recovery Agent de forma simultánea en varios equipos de Windows. Los equipos pueden formar parte de un dominio de Active Directory, vCenter o host virtual ESXi o un host virtual de Hyper-V; o bien pueden ser equipos que ya estén protegidos por el Rapid Recovery Core local, como en el caso de una actualización del software Rapid Recovery Agent. También tiene la opción de implementar manualmente el software en equipos que no estén necesariamente asociados a un dominio o host específico.

También puede implementar manualmente el software Rapid Recovery Agent en uno o varios equipos Linux desde la Core Console.

CAUTION: Si el Agent de AppAssure se instaló previamente en un equipo Linux, antes de instalar el Rapid Recovery Agent, elimine el Agent de AppAssure del equipo que utiliza una secuencia de comandos de Shell. Para obtener información sobre la eliminación del Agent de un equipo Linux, consulte el tema Desinstalar el software Agent de AppAssure de un equipo Linux en el *Guía de instalación y actualización de Rapid Recovery.* Para implementar correctamente el software Agent en equipos Linux, consulte los requisitos previos en el tema "Acerca de instalar el software Agent en equipos Linux" en el mismo documento.

La implementación del software Rapid Recovery Agent no protege automáticamente los equipos. Después de la implementación debe seleccionar la opción **Proteger varios equipos** en la barra de botones de la Core Console.

NOTE: La función con la que se lleva a cabo la implementación en varios equipos simultáneamente antes se denominaba implementación masiva. La función que protege varios equipos simultáneamente antes se denominaba protección masiva.

Para implementar y proteger varios equipos a la vez, realice las tareas siguientes:

- Implemente Rapid Recovery Agent en varios equipos. Consulte Implementación de Agent en varios equipos simultáneamente desde la Core Console.
- Supervise la implementación. Consulte Verificación de la implementación en varios equipos.
- Proteger varios equipos. Consulte Acerca de la protección de varios equipos.

  NOTE: Si ha seleccionado la opción Proteger equipo tras la instalación durante la implementación, omita este paso.
- Supervise la actividad de la protección masiva. Consulte Supervisión de la protección de varios equipos.

Uso del asistente para implementar el software Agent para implementar en uno o varios equipos

Puede simplificar la tarea de implementar el software Rapid Recovery Agent en uno o más equipos empleando el asistente para implementar el software Agent.

Si realiza la implementación en equipos Linux, este método es adecuado.

NOTE: En el pasado, esta función se denominaba "implementación masiva".

Al utilizar el asistente para implementar el software Agent, Rapid Recovery Core puede:

1. Detectar equipos Windows en un dominio de Active Directory e insertar el software Agent en los equipos que seleccione.
2. Conéctese a un host de VMware vCenter o ESXi, detecte los invitados e inserte el software Agent en los equipos que seleccione.
3. Conéctese a un Rapid Recovery Core local e implemente el software Agent actual (más reciente) en equipos Windows protegidos por el Core. (Para equipos Linux, utilice la opción de implementación manual).
4. Conéctese a un clúster o servidor de Hyper-V, detecte los invitados e inserte el software Agent en los equipos que seleccione.
5. Especifique manualmente los equipos Windows o Linux, mediante las credenciales y las direcciones IP e inserte el software Agent en los equipos que seleccione.

Desde el interior de la Core Console, puede completar cualquiera de las siguientes tareas:

- Implementación en equipos de un dominio de Active Directory
- Implementación en equipos de un host virtual VMware vCenter/ESXi
- Implementación de una actualización de software de Agent Rapid recovery para los equipos protegidos
- Implementación en equipos manualmente

NOTE: Quest recomienda limitar el número de equipos en los que implementa de forma simultánea a 50 o menos para evitar sufrir limitaciones de recursos que pueden provocar el fracaso de la operación de implementación.

NOTE: Los equipos de destino deben tener acceso a Internet para descargar e instalar bits, ya que Rapid Recovery utiliza la versión web del instalador de Rapid Recovery Agent para implementar los componentes de instalación. Si el acceso a Internet no está disponible, utilice la Core Console para descargar el instalador en un medio de almacenamiento como una unidad USB. A continuación, instale físicamente el software en los equipos que quiera proteger. Para obtener más información, consulte Descarga del instalador de Rapid Recovery Agent.

Implementación en equipos de un dominio de Active Directory

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

Utilice este procedimiento para implementar simultáneamente el software Rapid Recovery Agent en uno o más equipos en un dominio Active Directory.

1. En la Rapid Recovery Core Console, haga clic en el menú desplegable **Proteger** y luego haga clic en **Implementar el software Agent**.

   Se abre el asistente para implementar el software Agent.
2. En la página **Conexión** del asistente, en la lista desplegable **Origen**, seleccione **Active Directory**.
3. Introduzca la información de dominio y las credenciales de inicio de sesión según se describe en la tabla siguiente.

Tabla 41. Información y credenciales de dominio

Cuadro de texto	Descripción
Host	Nombre de host o dirección IP del dominio de Active Directory.
Nombre de usuario	El nombre de usuario utilizado para conectarse con el dominio; por ejemplo, Administrator (o, si el equipo se encuentra en un dominio, [nombre de dominio]\Administrator).
Contraseña	La contraseña segura que se utiliza para conectar con el dominio.

4. Haga clic en **Siguiente**.
5. En la página **Equipos**, seleccione los equipos en los que quiere implementar el software Rapid Recovery Agent.
6. De manera opcional, para reiniciar automáticamente los equipos protegidos una vez que Agent está instalado, seleccione **Después de la instalación del Agent, reiniciar el equipo automáticamente**.
7. Haga clic en **Finalizar**.

   El sistema comprueba de forma automática cada uno de los equipos que haya seleccionado.

   Si Rapid Recovery detecta cualquier laguna durante la verificación automática, el asistente avanza a la página Avisos, donde puede borrar los equipos de la selección y comprobar manualmente los equipos seleccionados. Si los equipos que ha agregado pasan la verificación automática, aparecerán en el panel Implementar Agent en los equipos.
8. Si ha aparecido la página Advertencia pero está satisfecho con la selección de repositorios, haga clic de nuevo en **Finalizar**.

El software Rapid Recovery Agent se implementa en los equipos especificados. Los equipos todavía no están protegidos. La protección se inicia una vez que se haya completado Protección de varios equipos en un dominio de Active Directory.

Implementación en equipos de un host virtual VMware vCenter/ESXi

Utilice este procedimiento para implementar simultáneamente el software Rapid Recovery Agent en uno o más equipos en un host virtual VMware vCenter/ESXi.

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

- Las credenciales de inicio de sesión para el host virtual VMware vCenter/ESXi.
- La ubicación del host.
- Las credenciales de inicio de sesión para cada uno de los equipos que desee proteger.

NOTE: Todas las máquinas virtuales deben tener herramientas de VMware instaladas; de lo contrario, Rapid Recovery no podrá detectar el nombre de host de la máquina virtual en la que se realizará la implementación. En lugar del nombre de host, Rapid Recovery utiliza el nombre de máquina virtual, lo cual puede causar problemas si el nombre de host es diferente del nombre de la máquina virtual.

1. En la Rapid Recovery Core Console, haga clic en el menú desplegable **Proteger** y luego haga clic en **Implementar el software Agent**.

   Se abre el asistente para **implementar el software Agent**.
2. En la página **Conexión** del asistente, en la lista desplegable **Origen**, seleccione **vCenter/ESXi**.
3. Introduzca la información de host y las credenciales de inicio de sesión según se describe en la tabla siguiente.

Tabla 42. Información de configuración de la conexión vCenter/ESXi

Cuadro de texto	Descripción
Host	Nombre o dirección IP del host virtual de VMware vCenter Server/ESXi.
Puerto	Número de puerto usado para conectar con el host virtual. El valor predeterminado es 443.
Nombre de usuario	El nombre de usuario utilizado para conectarse con el host virtual; por ejemplo, Administrator o, si el equipo se encuentra en un dominio, [nombre de dominio]\Administrator.
Contraseña	La contraseña segura que se utiliza para conectarse con este host virtual.

4. Haga clic en **Siguiente**.
5. En la página **Equipos** del asistente, seleccione una de las opciones siguientes en el menú desplegable:
   - Hosts y clústeres
   - Máquinas virtuales y plantillas
6. Expanda la lista de equipos y, a continuación, seleccione las máquinas virtuales en las que desea implementar el software.

Aparece una notificación si Rapid Recovery detecta que un equipo está fuera de línea o que las herramientas de VMware no están instaladas.

7. Si desea reiniciar los equipos automáticamente después de la implementación, seleccione **Después de la instalación, reiniciar el equipo automáticamente (recomendado)**.
8. Haga clic en **Siguiente**.

   Rapid Recovery comprueba de forma automática cada uno de los equipos que haya seleccionado.
9. En la página **Ajustes** del asistente, escriba las credenciales de cada equipo en el siguiente formato: `hostname::username::password`.

   NOTE: Introduzca un equipo por línea.
10. Haga clic en **Finalizar**.

    El sistema comprueba de forma automática cada uno de los equipos que haya seleccionado.

    Si Rapid Recovery detecta cualquier laguna durante la verificación automática, el asistente avanza a la página Avisos, donde puede borrar los equipos de la selección y comprobar manualmente los equipos seleccionados. Si los equipos que ha agregado pasan la verificación automática, aparecerán en el panel Implementar Agent en los equipos.
11. Si ha aparecido la página Advertencia pero está satisfecho con la selección de repositorios, haga clic de nuevo en **Finalizar**.

El software Rapid Recovery Agent se implementa en los equipos especificados. Los equipos todavía no están protegidos. La protección se inicia una vez que se haya completado Protección de varios equipos en un host virtual VMware vCenter/ESXi.

Implementación de una actualización de software de Agent Rapid recovery para los equipos protegidos

Puede utilizar el Asistente de implementación del software Agent para realizar una actualización del software Rapid Recovery Agent a equipos Windows que ya están protegidos por el Rapid Recovery Core local.

NOTE: Para los usuarios de Linux, si la versión anterior de Agent es de la marca AppAssure (versión 5.4.3 o posteriores), primero debe eliminar el software Agent con la secuencia de comandos de Shell adecuada para su versión de Agent de AppAssure específica. Eliminar el Agent de AppAssure después de instalar el Rapid Recovery Agent puede interrumpir la conexión entre el equipo Linux y el Core. Para obtener más información sobre cómo desinstalar el Agent de AppAssure de un equipo Linux, consulte Desinstalar el software Agent de AppAssure de un equipo Linux en *Rapid Recovery Installation and Upgrade Guide* (Guía de instalación y actualización de Rapid Recovery).

1. En la Core Console de Rapid Recovery, haga clic en el menú desplegable **Proteger** y luego haga clic en **Implementar el software de Agent**.

   Se abre el asistente para **implementar el software de Agent**.
2. En la página del asistente **Conexión**, de la lista desplegable **Origen**, seleccione **Core local**.
3. Haga clic en **Siguiente**.
4. En la página **Equipos** del asistente, seleccione los equipos protegidos en los que desea implementar una actualización del software de Agent Rapid Recovery.

   NOTE: En este momento, no puede utilizar este proceso para actualizar equipos Linux protegidos.
5. La práctica recomendada es restaurar cada equipo después de instalar o actualizar el software Agent. Si desea reiniciar los equipos automáticamente después de la implementación, deje la opción predeterminada

Después de la instalación del Agent, reiniciar el equipo automáticamente (recomendado). Desmarque la opción si no desea restaurar los equipos actualizados inmediatamente.

6. Haga clic en **Finalizar**.

   El sistema comprueba de forma automática cada uno de los equipos que haya seleccionado.

   Si Rapid Recovery detecta cualquier laguna durante la verificación automática, el asistente avanza a la página **Avisos**, donde puede borrar los equipos de la selección y comprobar manualmente los equipos seleccionados. Si los equipos que ha agregado pasan la verificación automática, aparecerán en el panel **Implementar Agent** en los equipos.

7. Si apareció la página **Aviso** y sigue satisfecho con las selecciones, haga clic en **Finalizar** otra vez.

Implementación en equipos manualmente

Utilice el siguiente procedimiento para implementar el Rapid Recovery Agent en varios equipos en cualquier tipo de host distinto del Core local, Active Directory, vCenter/ESXi o Hyper-V.

> **CAUTION: Si el Agent de AppAssure se instaló previamente en un equipo Linux, antes de instalar el Rapid Recovery Agent, elimine el Agent de AppAssure del equipo que utiliza una secuencia de comandos de Shell. Para obtener información sobre la eliminación del Agent de un equipo Linux, consulte el tema Desinstalar el software Agent de AppAssure de un equipo Linux en el *Guía de instalación y actualización de Rapid Recovery.* Para implementar correctamente el software Agent en equipos Linux, consulte los requisitos previos en el tema "Acerca de instalar el software Agent en equipos Linux" en el mismo documento.**

1. En la Rapid Recovery Core Console, haga clic en el menú desplegable **Proteger** y, a continuación, seleccione **Implementar el software de Agent**.

   Se abre el asistente para **implementar el software de Agent**.

2. En la página del asistente **Conexión**, de la lista desplegable **Origen**, seleccione **Manualmente**.
3. Haga clic en **Siguiente**.
4. En la página **Equipos** del asistente, introduzca los detalles del equipo en el cuadro de diálogo para todos los equipos en los que desea implementar Agent. Pulse **Intro** para separar la información de cada equipo. Utilice el formato `hostname::username::password::port`. Para los equipos Windows, la configuración del puerto es opcional. Para los equipos Linux, incluya siempre el puerto SSH, que es 22 de manera predeterminada. Los ejemplos incluyen:

   ```
   10.255.255.255::administrator::&11@yYz90z
   abc-host-00-1::administrator::99!zU$o83r::8006
   Linux-host-00-2::administrator::p@$$w0rD::22
   ```

5. Si desea reiniciar los equipos automáticamente después de la implementación, seleccione **Después de la instalación, reiniciar el equipo automáticamente (recomendado)**.
6. Haga clic en **Finalizar**.

   El sistema comprueba de forma automática cada uno de los equipos que haya seleccionado.

   Si Rapid Recovery detecta cualquier laguna durante la verificación automática, el asistente avanza a la página **Avisos**, donde puede borrar los equipos de la selección y comprobar manualmente los equipos seleccionados. Si los equipos que ha agregado pasan la verificación automática, aparecerán en el panel **Implementar Agent** en los equipos.

7. Si apareció la página **Aviso** y sigue satisfecho con las selecciones, haga clic en **Finalizar** otra vez.

El software Rapid Recovery Agent se implementa en los equipos especificados. Los equipos todavía no están protegidos. La protección se inicia una vez que se haya completado Protección de varios equipos manualmente.

Verificación de la implementación en varios equipos

Una vez haya implementado de forma simultánea el software Rapid Recovery Agent en dos o más equipos, podrá verificar si se ha hecho correctamente visualizando cada equipo indicado en el menú Equipos protegidos.

También puede ver información relativa al proceso de implementación masiva desde la página Eventos. Realice los pasos de este procedimiento para verificar la implementación.

1. Vaya a la Rapid Recovery Core Console, haga clic en (Eventos) y, a continuación, haga clic en **Alertas**.

   Los eventos de alerta aparecerán en la lista, mostrando el tiempo en que se inició el evento y un mensaje. Por cada implementación correcta del software Agent, verá una alerta indicando que el equipo protegido se ha agregado.
2. También puede hacer clic en cualquier enlace de un equipo protegido.

   Aparece la pestaña **Resumen** del equipo seleccionado, que muestra la información pertinente, entre la que se incluye:

   - El nombre de host del equipo protegido.
   - La última instantánea, si es aplicable.
   - La hora de la siguiente instantánea programada, basada en el calendario de programación de protección del equipo seleccionado.
   - La clave de cifrado, si la hubiera, utilizada para este equipo protegido.
   - La versión del software Agent.

Modificación de la configuración de implementación

Complete los pasos de este procedimiento para modificar la configuración de implementación.

1. Desde la Rapid Recovery Core Console, haga clic en (Configuración).
2. En la página **Configuración**, en la columna izquierda, haga clic en **Implementar** para ir a la sección Implementar.
3. Modifique cualquiera de las opciones siguientes haciendo clic en la configuración que quiere cambiar para que se pueda editar como un cuadro de texto o una lista desplegable y, a continuación, haga clic en para guardar la configuración.

Tabla 43. Opciones de implementación

Opción	Descripción
Agent Installer Name	Escriba el nombre del archivo ejecutable del agente. El valor predeterminado es Agent-web.exe.
Core Address	Introduzca la dirección para el Core.

Opción	Descripción
Error de tiempo de espera de recepción	Especifique el número de minutos que hay que esperar sin actividad antes del tiempo de espera.
Número máximo de instalaciones paralelas	Especifique un número para el máximo de instalaciones que quiere instalar de forma simultánea. El valor predeterminado y límite es 100.
Reinicio automático después de la instalación	Marque la casilla de verificación para Sí o desmárquela para No.
Proteger tras implementación	Marque la casilla de verificación para Sí o desmárquela para No.

Comprensión del calendario de programación de protección.

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

La primera transferencia de copia de seguridad de cualquier equipo añadido a la protección en el Core se denomina una instantánea de imagen base. Todos los datos de todos los volúmenes especificados (incluidos el sistema operativo, las aplicaciones y la configuración) se guardan en el repositorio, lo que puede tardar una cantidad de tiempo considerable en función de la cantidad de datos que se transfieran. En lo sucesivo, las instantáneas incrementales (copias de seguridad más pequeñas, compuestas únicamente por datos cambiados en el equipo protegido desde la última copia de seguridad) se guardarán en el repositorio con regularidad, basándose en el intervalo definido (por ejemplo, cada 60 minutos). Este tipo de copia de seguridad contiene menos datos que una imagen base y, por tanto, tarda menos tiempo en transferirse.

Los calendarios de programación de protección se definen inicialmente mediante el Asistente para proteger un equipo o el Asistente para proteger varios equipos. Al utilizar un asistente, puede personalizar los calendarios de programación de protección (seleccionando períodos o una hora de protección diaria) para ajustarse a sus necesidades empresariales. Es posible modificar el calendario de programación existente o crear un nuevo calendario de programación en cualquier momento en el cuadro de diálogo Calendario de programación de protección de la página de resumen en un equipo protegido específico.

Rapid Recovery proporciona un calendario de programación de protección predeterminado, que incluye un único periodo que abarca todos los días de la semana, con un único periodo de tiempo definido (desde las 12:00 hasta las 23:59). El intervalo predeterminado (el período de tiempo entre instantáneas) es de 60 minutos. La primera vez que habilita la protección también está activando el calendario de programación. De este modo, cuando se utiliza la configuración predeterminada, independientemente de la hora del día actual, la primera copia de seguridad se producirá cada hora, a la hora en punto (12:00, 13:00, 14:00, etc.).

La selección de periodos le permite ver el calendario de programación de protección predeterminado y realizar los ajustes pertinentes. Seleccionar una hora de protección diaria hace que el Rapid Recovery Core cree una copia de seguridad de los equipos protegidos indicados una vez a diario a la hora que especifique.

Es posible personalizar el calendario de programación para definir las horas punta y no punta utilizando los periodos disponibles de días laborables y fines de semana. Por ejemplo, si utiliza mayormente sus equipos protegidos los días laborables, podría disminuir el intervalo del periodo de días laborables a 20 minutos, dando lugar a tres instantáneas cada hora. También puede incrementar el intervalo del periodo de los fines de semanas

de 60 minutos a 180 minutos, con lo que obtendrá instantáneas una vez cada tres horas cuando el tráfico sea reducido.

También puede cambiar la programación predeterminada para definir horas pico y no pico diariamente. Para hacerlo, cambie la hora de inicio y la hora de finalización predeterminadas a un rango de tiempo menor (por ejemplo, de las 12:00 hasta las 16:59) y establezca un intervalo adecuado (por ejemplo, 20 minutos). Esto hará que se realicen copias de seguridad frecuentes durante el período de horas pico. A continuación puede añadir un intervalo de tiempo adicional para los días laborables para el periodo de tiempo restante (desde las 17:00 hasta las 23:59) y establezca un intervalo apropiado (posiblemente mayor, como por ejemplo, 180 minutos). Estos parámetros definen un periodo fuera de las horas de pico que incluye desde las 17:00 hasta la media noche todos los días. Esta personalización da como resultado instantáneas cada tres horas desde las 17:00 hasta las 23:59, e instantáneas cada 20 minutos desde las 12:00 hasta las 16:59.

Al modificar o crear un calendario de programación de protección por medio del cuadro de diálogo Calendario de programación de protección, Rapid Recovery le ofrece la opción de guardar ese calendario de programación como una plantilla reutilizable que puede aplicar después a otros equipos protegidos.

Otras opciones del asistente de protección incluyen el ajuste de una hora de protección diaria. El resultado es una única copia de seguridad diaria en el período definido (el ajuste predeterminado es 00:00).

Al proteger uno o varios equipos utilizando un asistente, puede realizar pausa en la protección inicialmente, lo cual define el calendario de programación de protección sin proteger los equipos. Cuando esté listo para empezar a proteger sus equipos basándose en el calendario de programación de protección establecido, deberá reanudar la protección de manera explícita. Para obtener más información sobre cómo reanudar la protección, consulte Pausa y reanudación de la replicación. Asimismo, si quiere proteger un equipo inmediatamente, puede forzar una instantánea. Para obtener más información, consulte Cómo forzar una instantánea.

See also: Creación de un programa de protección personalizado en el modo simple
See also: Creación de varios periodos de programación para protección en el modo avanzado

Protección de un equipo

Si ya ha instalado el software Rapid Recovery Agent en el equipo que quiere proteger, pero todavía no ha reiniciado el equipo, reinícielo ahora.

Este tema describe cómo iniciar la protección de los datos de un único equipo que especifique mediante el Asistente para proteger un equipo. Para proteger varios equipos utilizando uno proceso simultáneamente, consulte Acerca de la protección de varios equipos.

NOTE: A menos que se utilice una protección sin agentes en un host ESXi, VMware o Hyper-V, el equipo que desea proteger debe tener el software Rapid Recovery Agent instalado para poder protegerse. Puede decidir instalar el software Agent antes de este procedimiento o implementar el software en el equipo de destino como parte del Asistente para proteger un equipo. Para obtener más información sobre la protección sin Agent y sus restricciones, consulte Comprensión de Rapid Snap for Virtual.

NOTE: Para obtener más información acerca de la instalación del software Agent , consulte "Instalación del software Rapid Recovery Agent" en la *Rapid Recovery Installation and Upgrade Guide* (Guía de instalación y actualización de Rapid Recovery). Si el software Agent no está instalado antes de proteger un equipo, no podrá seleccionar volúmenes específicos para su protección como parte de este asistente. En este caso, de forma predeterminada, todos los volúmenes del equipo protegido sin agente estarán protegidos. Rapid Recovery es compatible con la protección y recuperación de equipos configurados con particiones EISA. La compatibilidad también se amplía a equipos con Windows 8 y 8.1 y Windows 2012 y 2012 R2 que utilicen Windows Recovery Environment (Windows RE).

Cuando agrega protección, debe definir información de conexión, como la dirección IP y el puerto, así como proporcionar credenciales para el equipo que quiera proteger. También puede proporcionar un nombre para mostrar que aparecerá en la Core Console en lugar de la dirección IP. Si cambia esto, no verá la dirección IP del equipo protegido cuando vea los detalles en la Core Console. También definirá el calendario de programación de protección del equipo.

Este proceso de protección incluye pasos opcionales a los que puede acceder si selecciona una configuración avanzada. Las opciones avanzadas incluyen las funciones de repositorio y el cifrado. Por ejemplo, puede

especificar un repositorio de Rapid Recovery existente para guardar instantáneas o crear un nuevo repositorio. También puede especificar una clave de cifrado existente (o agregar una nueva clave de cifrado) para aplicarla a los datos guardados en el Core para este equipo. Para obtener más información sobre las claves de cifrado, consulte Cifrado.

El flujo de trabajo del asistente de protección puede variar ligeramente según su entorno. Por ejemplo, si el software Rapid Recovery Agent está instalado en el equipo que desea proteger, no se le pedirá que lo instale desde el asistente. Del mismo modo, si ya existe un repositorio en el Core, no se le pedirá que cree uno.

CAUTION: Rapid Recovery no admite restauración Bare Metal Restore (R) de equipos Linux con particiones de arranque EXT2. Cualquier BMR realizada en un equipo con este tipo de partición dará como resultado un equipo que no puede iniciarse. Si desea realizar una BMR en este equipo en el futuro, tendrá que convertir cualquier partición ext2 a ext3 o ext4 antes de iniciar la protección y la copia de seguridad del equipo.

1. Realice uno de los siguientes pasos:
   - Si inicia desde el Asistente para proteger un equipo, continúe con el paso 2.
   - Si inicia desde la Rapid Recovery Core Console, en la barra de botones, haga clic en **Proteger**.

   Aparece el **Asistente para proteger un equipo**.
2. En la página **Bienvenido**, seleccione las opciones de instalación adecuadas:
   - Si no necesita definir un repositorio o establecer cifrado, seleccione **Típica**.
   - Si necesita crear un repositorio, necesita definir un repositorio diferente para copias de seguridad del equipo seleccionado o quiere establecer cifrado mediante el asistente, seleccione **Avanzada (mostrar pasos opcionales)**.
   - Opcionalmente, si no desea ver la página de **bienvenida** del Asistente para proteger un equipo en el futuro, seleccione la opción **Omitir esta página de bienvenida la próxima vez que se abra el asistente**.
3. Cuando esté satisfecho con sus opciones en la página de bienvenida, haga clic en **Siguiente**.

   Aparecerá la página **Conexión**.
4. En la página **Conexión**, introduzca la información acerca del equipo con el que desea conectarse según se describe en la tabla siguiente y, a continuación, haga clic en **Siguiente**.

Tabla 44. Configuración de conexión del equipo

Cuadro de texto	Descripción
Sistema operativo	Seleccione Windows o Linux, según el sistema operativo del equipo que desee proteger.
Host	El nombre de host o la dirección IP del equipo que desea proteger.
Puerto	El número de puerto por el que el Rapid Recovery Core se comunica con el Agent en el equipo. El número de puerto predeterminado es 8006.
Nombre de usuario	El nombre de usuario utilizado para conectarse con este equipo; por ejemplo, Administrator (o, si el equipo se encuentra en un dominio, [nombre de dominio]\Administrator).
Contraseña	La contraseña que se utiliza para conectar a ese equipo.

Si la página **Instalar Agent** aparece junto al Asistente para proteger un equipo, significa que Rapid Recovery no detecta el Rapid Recovery Agent en el equipo e instalará la versión actual del software. Vaya al paso 6.

Si aparece la página **Actualizar Agent** a continuación en el asistente, esto significa que hay una versión anterior del software Agent en el equipo que desea proteger.

NOTE: El software Agent debe instalarse en el equipo que quiera proteger y ese equipo deberá reiniciarse antes de que pueda hacer una copia de seguridad en el Core. Para que el instalador reinicie el equipo protegido, seleccione la opción **Después de la instalación, reiniciar el equipo automáticamente (recomendado)** antes de hacer clic en Siguiente.

5. En la página **Actualizar Agent**, realice una de las acciones siguientes:
   - Para implementar la nueva versión del software Agent (que coincide con la versión del Rapid Recovery Core), seleccione **Actualizar el software Rapid Recovery Agent a la última versión** .
   - Para seguir protegiendo el equipo sin actualizar la versión del software Agent, borre la opción **Actualizar el software Rapid Recovery Agent a la última versión**.
6. Haga clic en **Siguiente**.

   Aparecerá la página **Protección**.
7. De manera opcional, en la página **Protección**, si quiere que aparezca un nombre distinto a la dirección IP en la Rapid Recovery Core Console de este equipo protegido, en el campo **Nombre para mostrar**, escriba un nombre en el cuadro de diálogo.

   Puede introducir hasta 64 caracteres. No utilice los caracteres especiales descritos en el tema caracteres prohibidos. Tampoco el nombre para mostrar debe comenzar por cualquiera de las combinaciones de caracteres descritas en el tema frases prohibidas.
8. Seleccione la configuración de programación para protección adecuada tal como se describe a continuación:
   - Para utilizar la programación para protección predeterminada, en la opción **Configuración de programación**, seleccione **Protección predeterminada (instantáneas de todos los volúmenes cada hora)**.

     Con un calendario de programación de protección predeterminado, el Core tomará instantáneas de todos los volúmenes del equipo protegido una vez cada hora. Para cambiar la configuración de protección en cualquier momento después de cerrar el asistente, incluida la selección de qué volúmenes proteger, vaya a la página **Resumen** del equipo protegido específico.
   - Para definir un calendario de programación de protección diferente, en la opción **Configuración de calendario de programación**, seleccione **Protección personalizada**.

     Las opciones de programación se incluyen en el flujo de trabajo del asistente.
9. En la parte inferior de la página **Protección**, si está volviendo a proteger un equipo previamente protegido en este Core y desea especificar otro repositorio que no sea el repositorio original, seleccione la opción **Seleccionar un nuevo repositorio para este equipo**.

Las opciones avanzadas (incluidas Repositorio y Cifrado) se incluyen en el flujo de trabajo del asistente.

10. Continúe con su configuración del modo siguiente:

    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo en el paso 2 y ha especificado una protección predeterminada, y si existe un repositorio, haga clic en **Finalizar** para confirmar sus opciones, cierre el asistente y proteja el equipo que ha especificado.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si no existe un repositorio, haga clic en **Siguiente** y continúe en el paso 13 para crear un repositorio.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe con el paso 11 para seleccionar qué volúmenes se van a proteger.
    - Si ha seleccionado una configuración avanzada para el Asistente para proteger un equipo en el paso 2, así como la protección predeterminada, haga clic en **Siguiente** y continúe en el paso 13 para ver las opciones de repositorio y cifrado.
    - Si ha seleccionado Configuración avanzada para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe con el paso 11 para seleccionar qué volúmenes se van a proteger.

    La primera vez que se agrega protección a un equipo, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio del Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

11. En la página **Volúmenes de protección**, seleccione los volúmenes que desea proteger. Si se indican volúmenes que no quiera incluir en la protección, haga clic en la columna Comprobar para borrar la selección. A continuación, haga clic en **Siguiente**.

    NOTE: Por lo general, es recomendable proteger, como mínimo, el volumen reservado para el sistema y el volumen con el sistema operativo (normalmente la unidad C).

12. En la página **Calendario de programación de protección**, defina un calendario de programación de protección personalizado y luego haga clic en **Siguiente**. Para obtener información detallada sobre cómo definir un calendario de programación de protección personalizado, consulte Creación de un programa de protección personalizado en el modo simple.

    Si ya ha configurado la información del repositorio, no ha indicado que desee cambiar el repositorio y ha seleccionado la opción Avanzada en el paso 2, aparecerá la página **Cifrado**. Continúe en el paso 16.

    Si ya ha configurado la información del repositorio y ha seleccionado la opción Avanzada en el paso 2, o si ha indicado que desea cambiar el repositorio, aparecerá la página **Repositorio**. Continúe en el paso 13.

13. En la página **Repositorio**, realice los siguientes pasos:

    - Si ya tiene un repositorio y desea almacenar los datos de este equipo para la protección del repositorio existente, realice una de las acciones siguientes:

      1. Seleccione **Usar un repositorio existente**.
      2. Seleccione un repositorio existente de la lista.
      3. Haga clic en **Siguiente**.

      Se abrirá la página de **Cifrado**. Vaya al paso 15 para definir el cifrado de manera opcional.

    - Si desea crear un repositorio, en la página **Repositorio**, introduzca la información que se describe en la tabla siguiente y haga clic en **Siguiente** o **Finalizar** según corresponda.

Tabla 45. Configuración del repositorio

Cuadro de texto	Descripción
Nombre	Introduzca el nombre para mostrar del repositorio.

Cuadro de texto	Descripción
	De manera predeterminada, este cuadro de texto incluye el término Repositorio y un número, que se corresponde con el número de repositorios de este Core. Por ejemplo, si se trata del primer repositorio, el nombre predeterminado es Repositorio 1. Cambie el nombre según sea necesario. Los nombres del repositorio contienen entre 1 y 40 caracteres alfanuméricos, incluidos los espacios. No utilice caracteres prohibidos ni frases prohibidas.
Ubicación	Introduzca la ubicación para almacenar los datos protegidos. Este volumen debe ser la ubicación de almacenamiento principal. La ubicación puede ser local (una unidad en el equipo Core) o una unidad de red de uso compartido de CIFS. Si es de uso compartido de CIFS, la ruta debe comenzar por \\. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación. **CAUTION: Defina una carpeta específica en la raíz para la ubicación de almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice `E:\Repository\`, no `E:\`. Si el repositorio que está creando en este paso se elimina más adelante, se eliminarán todos los archivos en la ubicación de almacenamiento de su repositorio. Si define la ubicación de almacenamiento en la raíz, el resto de archivos del volumen (p. ej., `E:\`) se eliminan, lo que podría derivar en una pérdida grave de datos.** Por ejemplo, introduzca `X:\Repository\Data`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
Nombre de usuario	Introduzca un nombre de usuario para un usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.
Contraseña	Introduzca la contraseña para el usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.
Ruta de acceso a metadatos	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, introduzca `X:\Repository\Metadata`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.

14. En la página **Configuración del repositorio**, configure la cantidad de espacio en disco que desea asignar en el repositorio. Quest recomienda reservar un 20 % del volumen a los metadatos, que es el valor predeterminado. De manera opcional, utilizando el control deslizante o el campo **Tamaño**, puede asignar más o menos espacio de volumen para el repositorio.
15. De manera opcional, si desea visualizar e introducir información detallada acerca de la configuración de la ubicación de almacenamiento, seleccione **Mostrar opciones avanzadas** y ajuste la configuración como se describe en la siguiente tabla. Para ocultar estas opciones, desactive la opción **Mostrar opciones avanzadas**. Cuando haya completado la configuración del repositorio, haga clic en **Siguiente** o en **Finalizar**, según proceda.

Tabla 46. Detalles de configuración de almacenamiento

Cuadro de texto	Descripción
Bytes por sector	Especifique el número de bytes que desea que incluya cada sector. El valor predeterminado es 512.
Bytes por registro	Especifique el promedio del número de bytes por registro. El valor predeterminado es 8192.
Política de almacenamiento en caché de escritura	La política de almacenamiento en caché de escritura controla cómo se utiliza el Administrador de caché de Windows en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: • Activado • Desactivado • Sincronización Si se establece como Activado, que es el valor predeterminado, Windows controla el almacenamiento en caché. Es adecuado para Windows 10 y para versiones de Windows Server 2012 y posteriores. **NOTE:** si se establece la política de escritura en caché en Activado, se mejora el rendimiento; no obstante, el valor recomendado es Desactivada. Si utiliza Windows Server 2008 R2 SP2, la configuración recomendada es Desactivado. Si se establece en Desactivado, Rapid Recovery controla el almacenamiento en caché. Si se establece en Sincronización, Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.

Si ha seleccionado la opción **Avanzada** en el paso 1, aparece la página **Cifrado**.

16. De manera opcional, en la página **Cifrado**, si desea utilizar claves de cifrado para los datos almacenados en el repositorio, seleccione **Cifrar los datos en reposo en un repositorio** y, a continuación, realice una de las acciones siguientes:
    - Para seleccionar una clave de cifrado existente y aplicarla a todos los nuevos datos almacenados en el repositorio, seleccione **Cifrar los datos utilizando un cifrado basado en Core con una clave existente**, y, en el menú desplegable **Seleccionar clave de cifrado** seleccione la clave de cifrado.
    - Para definir una nueva clave de cifrado en este momento y aplicarla a todos los futuros datos almacenados en el repositorio, seleccione **Cifrar datos mediante un cifrado basado en el Core con una clave nueva** y, a continuación, introduzca información sobre la clave como se describe en la siguiente tabla:

Tabla 47. Definir nueva clave de cifrado

Cuadro de texto	Descripción
Nombre	Escriba un nombre para la clave de cifrado. Los nombres de las claves de cifrado contienen entre 1 y 64 caracteres alfanuméricos. No utilice caracteres no permitidos o frases no permitidas.

Cuadro de texto	Descripción
Descripción	Escriba un comentario descriptivo para la clave de cifrado. Esta información aparece en el campo Descripción cuando al visualizar una lista de claves de cifrado en la Rapid Recovery Core Console. Las descripciones pueden contener hasta 254 caracteres. La práctica recomendada es evitar el uso de caracteres no permitidos y frases no permitidas.
Frase de contraseña	Introduzca una frase de contraseña usada para controlar el acceso. La práctica recomendada es evitar el uso de caracteres no permitidos. Registre la frase de contraseña en lugar seguro. Asistencia para la protección de datos de Quest no puede recuperar frases de contraseña. Una vez cree una clave de cifrado y la aplique a uno o más equipos protegidos no podrá recuperar los datos si pierde la frase de contraseña.
Confirmar la frase de contraseña	Como confirmación, vuelva a escribir la Frase de contraseña. Se utiliza para confirmar la entrada de frase de contraseña.

17. De manera opcional, en la página **Cifrado**, si desea cifrar todos los datos de transporte a través de una red, seleccione **Cifrar los datos de transporte a través de una red**. Esta opción está habilitada de manera predeterminada. Si no desea cifrar los datos de esta manera, desactive esta opción.
18. Haga clic en **Finalizar** para guardar y aplicar sus ajustes.

    La primera vez que se agrega protección para una máquina, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

Protección de un clúster

En este tema se describe cómo agregar un clúster para protección en Rapid Recovery. Cuando agregue un clúster a la protección, debe especificar el nombre de host o dirección IP del clúster, la aplicación del clúster o uno de los nodos o equipos de clúster que incluye el software Rapid Recovery Agent.

NOTE: Se utiliza un repositorio para almacenar las instantáneas de datos que se capturan desde sus nodos protegidos. Para poder empezar a proteger datos en su clúster, debe tener configurado al menos un repositorio que esté asociado al Rapid Recovery Core.

Para obtener información sobre la configuración de repositorios, ver Comprensión de los repositorios.

1. Desde la Rapid Recovery Core Console, haga clic en el menú desplegable del botón **Proteger** y, a continuación, haga clic en **Proteger clúster**.
2. En la página de **bienvenida** del asistente, seleccione una de las opciones siguientes:
   - Típicas
   - Avanzado (mostrar pasos opcionales)
3. Haga clic en **Siguiente**.
4. En la página **Conexión** del asistente, introduzca la información siguiente:

Tabla 48. Configuración de Conectarse al clúster

Cuadro de texto	Descripción
Host	El nombre de host o dirección IP del clúster, la aplicación de clúster o uno de los nodos de clúster.
Puerto	El número de puerto del equipo en el que el Rapid Recovery Core se comunica con el Agent. El puerto predeterminado es 8006.
Nombre de usuario	El nombre de usuario del administrador de dominio utilizado para conectar a este equipo; por ejemplo, domain_name\administrator. **NOTE:** El nombre de dominio es obligatorio. No puede conectar con el clúster mediante el nombre de usuario de administrador local.
Contraseña	La contraseña que se utiliza para conectar a ese equipo.

5. Haga clic en **Siguiente**.

   NOTE: Si los nodos de clúster ya tienen una versión anterior del Rapid Recovery Agent instalada, aparecerá una página de Actualización en el asistente y le ofrecerá la oportunidad de actualizar el agente.

6. En la página **Nodos** del asistente, seleccione los nodos que desea proteger.

   El sistema verifica automáticamente todos los equipos que seleccione.

7. Haga clic en **Siguiente**.

   Si a continuación aparece la página **Protección** en el Asistente Proteger clúster, vaya al paso 11.

   Si el software Agent todavía no se ha implementado en los equipos que desee proteger o si alguno de los equipos que especificó no puede protegerse por cualquier otro motivo, los equipos seleccionados aparecerán en la página Advertencias.

8. Opcionalmente, en la página **Advertencias** del asistente, puede verificar cualquier equipo seleccionando el equipo y, a continuación, haciendo clic en **Verificar** en la barra de herramientas.
9. Opcionalmente, en la página **Advertencias**, seleccione **Tras la instalación de Agent, reinicie los equipos automáticamente**.

   NOTE: Quest recomienda esta opción. Debe reiniciar los equipos Agent antes de poder protegerlas.

10. Si el estado indica que puede llegarse al equipo, haga clic en **Siguiente** para instalar el software Rapid Recovery Agent.

    Aparecerá la página **Protección**.

11. De manera opcional, en la página **Protección**, si quiere que aparezca un nombre distinto a la dirección IP en la Rapid Recovery Core Console de este equipo protegido, en el campo **Nombre para mostrar**, escriba un nombre en el cuadro de diálogo.

    Puede introducir hasta 64 caracteres. No utilice los caracteres especiales descritos en el tema . Tampoco el nombre para mostrar debe comenzar por cualquiera de las combinaciones de caracteres descritas en el tema .

12. Seleccione la configuración de programación para protección adecuada tal como se describe a continuación:

    - Para utilizar la programación para protección predeterminada, en la opción Configuración de programación, seleccione **Protección predeterminada (instantáneas de todos los volúmenes cada hora)**.

Con un calendario de programación de protección predeterminado, el Core tomará instantáneas de todos los volúmenes del equipo protegido una vez cada hora. Para cambiar la configuración de protección en cualquier momento después de cerrar el asistente, incluida la selección de qué volúmenes proteger, vaya a la página **Resumen** del equipo protegido específico.

- Para definir un calendario de programación de protección diferente, en la opción Configuración de calendario de programación, seleccione **Protección personalizada**.

13. Continúe con su configuración del modo siguiente:
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si existe un repositorio, haga clic en **Finalizar** para confirmar sus opciones, cierre el asistente y proteja el equipo que ha especificado.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si no existe un repositorio, haga clic en **Siguiente** y continúe en el paso 16 para crear un repositorio.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe con el siguiente paso para seleccionar qué volúmenes se van a proteger.
    - Si ha seleccionado una configuración avanzada para el Asistente para proteger un equipo, así como la protección predeterminada, haga clic en **Siguiente** y continúe en el paso 16 para ver las opciones de repositorio y cifrado.
    - Si ha seleccionado Configuración avanzada para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe en el siguiente paso para seleccionar qué volúmenes se van a proteger.

    La primera vez que se agrega protección a un equipo, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio del Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.
14. En la página **Volúmenes de protección**, seleccione los volúmenes que desea proteger. Si se indican volúmenes que no quiera incluir en la protección, haga clic en la columna Comprobar para borrar la selección. A continuación, haga clic en **Siguiente**.

    NOTE: Por lo general, es recomendable proteger, como mínimo, el volumen reservado para el sistema y el volumen con el sistema operativo (normalmente la unidad C).
15. En la página **Calendario de programación de protección**, defina un calendario de programación de protección personalizado y luego haga clic en **Siguiente**. Para obtener información detallada sobre cómo definir un calendario de programación de protección personalizado, consulte Creación de un programa de protección personalizado en el modo simple.

    Si ya ha configurado la información del repositorio y ha seleccionado Opciones avanzadas en el paso 1, aparece la página Cifrado. Continúe en el paso 19.
16. En la página **Repositorio**, realice los siguientes pasos:
    - Si ya tiene un repositorio y desea almacenar los datos de este equipo para la protección del repositorio existente, realice una de las acciones siguientes:
        1. Seleccione **Usar un repositorio existente**.
        2. Seleccione un repositorio existente de la lista.
        3. Haga clic en **Siguiente**.

        Se abrirá la página de **Cifrado**. Vaya al paso 19 para definir el cifrado de manera opcional.
    - Si desea crear un repositorio, en la página **Repositorio**, introduzca la información que se describe en la tabla siguiente y haga clic en **Siguiente** o **Finalizar** según corresponda.

Tabla 49. Configuración del repositorio

Cuadro de texto	Descripción
Nombre	Introduzca el nombre para mostrar del repositorio. De manera predeterminada, este cuadro de texto incluye el término Repositorio y un número, que se corresponde con el número de repositorios de este Core. Por ejemplo, si se trata del primer repositorio, el nombre predeterminado es Repositorio 1. Cambie el nombre según sea necesario. Los nombres del repositorio contienen entre 1 y 40 caracteres alfanuméricos, incluidos los espacios. No utilice caracteres prohibidos ni frases prohibidas.
Ubicación	Introduzca la ubicación para almacenar los datos protegidos. Este volumen debe ser la ubicación de almacenamiento principal. La ubicación puede ser local (una unidad en el equipo Core) o una unidad de red de uso compartido de CIFS. Si es de uso compartido de CIFS, la ruta debe comenzar por \\. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación. **CAUTION: Defina una carpeta específica en la raíz para la ubicación de almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice `E:\Repository\`, no `E:\`. Si el repositorio que está creando en este paso se elimina más adelante, se eliminarán todos los archivos en la ubicación de almacenamiento de su repositorio. Si define la ubicación de almacenamiento en la raíz, el resto de archivos del volumen (p. ej., `E:\`) se eliminan, lo que podría derivar en una pérdida grave de datos.** Por ejemplo, introduzca `X:\Repository\Data`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
Nombre de usuario	Introduzca un nombre de usuario para un usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.
Contraseña	Introduzca la contraseña para el usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.
Ruta de acceso a metadatos	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, introduzca `X:\Repository\Metadata`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.

17. En la página **Configuración del repositorio**, configure la cantidad de espacio en disco que desea asignar en el repositorio. Quest recomienda reservar un 20 % del volumen a los metadatos, que es el valor predeterminado. De manera opcional, utilizando el control deslizante o el campo **Tamaño**, puede asignar más o menos espacio de volumen para el repositorio.
18. De manera opcional, si desea visualizar e introducir información detallada acerca de la configuración de la ubicación de almacenamiento, seleccione **Mostrar opciones avanzadas** y ajuste la configuración como se describe en la siguiente tabla. Para ocultar estas opciones, desactive la opción **Mostrar opciones**

avanzadas. Cuando haya completado la configuración del repositorio, haga clic en **Siguiente** o en **Finalizar**, según proceda.

Tabla 50. Detalles de configuración de almacenamiento

Cuadro de texto	Descripción
Bytes por sector	Especifique el número de bytes que desea que incluya cada sector. El valor predeterminado es 512.
Bytes por registro	Especifique el promedio del número de bytes por registro. El valor predeterminado es 8192.
Política de almacenamiento en caché de escritura	La política de almacenamiento en caché de escritura controla cómo se utiliza el Administrador de caché de Windows en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: • Activado • Desactivado • Sincronización Si se establece como Activado, que es el valor predeterminado, Windows controla el almacenamiento en caché. Es adecuado para Windows 10 y para versiones de Windows Server 2012 y posteriores. **NOTE:** si se establece la política de escritura en caché en Activado, se mejora el rendimiento; no obstante, el valor recomendado es Desactivada. Si utiliza Windows Server 2008 R2 SP2, la configuración recomendada es Desactivado. Si se establece en Desactivado, Rapid Recovery controla el almacenamiento en caché. Si se establece en Sincronización, Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.

Si ha seleccionado la opción **Avanzada** en el paso 1, aparece la página **Cifrado**.

19. De manera opcional, en la página **Cifrado**, si desea utilizar claves de cifrado para los datos almacenados en el repositorio, seleccione **Cifrar los datos en reposo en un repositorio** y, a continuación, realice una de las acciones siguientes:
    - Para seleccionar una clave de cifrado existente y aplicarla a todos los nuevos datos almacenados en el repositorio, seleccione **Cifrar los datos utilizando un cifrado basado en Core con una clave existente**, y, en el menú desplegable **Seleccionar clave de cifrado** seleccione la clave de cifrado.
    - Para definir una nueva clave de cifrado en este momento y aplicarla a todos los futuros datos almacenados en el repositorio, seleccione **Cifrar datos mediante un cifrado basado en el Core con una clave nueva** y, a continuación, introduzca información sobre la clave como se describe en la siguiente tabla:

Tabla 51. Definir nueva clave de cifrado

Cuadro de texto	Descripción
Nombre	Escriba un nombre para la clave de cifrado. Los nombres de las claves de cifrado contienen entre 1 y 64 caracteres alfanuméricos. No utilice caracteres no permitidos o frases no permitidas.

Cuadro de texto	Descripción
Descripción	Escriba un comentario descriptivo para la clave de cifrado. Esta información aparece en el campo Descripción cuando al visualizar una lista de claves de cifrado en la Rapid Recovery Core Console. Las descripciones pueden contener hasta 254 caracteres. La práctica recomendada es evitar el uso de caracteres no permitidos y frases no permitidas.
Frase de contraseña	Introduzca una frase de contraseña usada para controlar el acceso. La práctica recomendada es evitar el uso de caracteres no permitidos. Registre la frase de contraseña en lugar seguro. Asistencia para la protección de datos de Quest no puede recuperar frases de contraseña. Una vez cree una clave de cifrado y la aplique a uno o más equipos protegidos no podrá recuperar los datos si pierde la frase de contraseña.
Confirmar la frase de contraseña	Como confirmación, vuelva a escribir la Frase de contraseña. Se utiliza para confirmar la entrada de frase de contraseña.

20. De manera opcional, en la página **Cifrado**, si desea cifrar todos los datos de transporte a través de una red, seleccione **Cifrar los datos de transporte a través de una red**. Esta opción está habilitada de manera predeterminada. Si no desea cifrar los datos de esta manera, desactive esta opción.
21. Haga clic en **Finalizar** para guardar y aplicar sus ajustes.

    La primera vez que se agrega protección para una máquina, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

Protección de los nodos de un clúster

Esta tarea requiere que primero proteja un clúster. Para obtener más información, consulte Protección de un clúster.

En este tema se describe cómo proteger los datos en un nodo o equipo que tiene un Rapid Recovery Agent instalado. Este procedimiento permite agregar nodos individuales a la protección que haya omitido al proteger un clúster.

1. En la Core Console de Rapid Recovery, en Equipo protegido, haga clic en el clúster con los nodos que desea proteger.
2. En la página Resumen del clúster, haga clic en los **Nodos protegidos**.
3. En la página Nodos protegidos, haga clic en **Proteger nodo de clúster**.
4. En el cuadro de diálogo Proteger nodo de clúster, seleccione o introduzca la información siguiente según corresponda.

Tabla 52. Configuración de Proteger nodo de clúster

Cuadro de texto	Descripción
Host	Una lista desplegable de nodos en el clúster disponibles para su protección.
Puerto	El número de puerto por el que el Core de Rapid Recovery se comunica con el Agent en el nodo.

Cuadro de texto	Descripción
Nombre de usuario	El nombre de usuario del administrador de dominio utilizado para conectar a este nodo; por ejemplo, example_domain\administrator o administrator@example_domain.com.
Contraseña	La contraseña que se utiliza para conectar a ese equipo.

5. Para agregar el nodo, haga clic en **Conectar**.
6. Para iniciar la protección de este nodo con la configuración de protección predeterminada, vaya al Paso 13.

   NOTE: La configuración predeterminada garantiza que todos los volúmenes de este equipo están protegidos con un calendario de programación predeterminado cada 60 minutos.
7. En el cuadro de diálogo Proteger [nombre del nodo], si desea utilizar un repositorio que no sea el valor predeterminado, utilice la lista desplegable para seleccionar un repositorio.
8. Si desea asegurar los puntos de recuperación para este clúster utilizando cifrado basado en Core, utilice la lista desplegable para seleccionar una clave de cifrado.
9. Si no desea que la protección comience de inmediato tras completar este procedimiento, seleccione **Pausar protección inicialmente**.
10. Para introducir una configuración personalizada (por ejemplo, para personalizar el programa de protección para los volúmenes compartidos), haga lo siguiente:
    a. Para personalizar la configuración de un volumen individual, haga clic en **Función** junto al volumen que desea personalizar, y, a continuación, haga clic al lado del volumen pertinente.
    b. Consulte Creación de un programa de protección personalizado en el modo simple.
11. Haga clic en **Protect (Proteger)**.

Creación de un programa de protección personalizado en el modo simple

El procedimiento para crear un programa de protección personalizado desde un asistente de protección es idéntico al de crear un programa de protección para un equipo existente en el modo simple. Los programas de protección creados en un asistente o en el modo simple no se guardan como plantillas. Para crear plantillas o varios programas de protección, consulte Creación de varios periodos de programación para protección en el modo avanzado. Complete los pasos de este procedimiento para crear programas personalizados para utilizar Rapid Recovery para realizar copias de seguridad de datos de equipos protegidos.

1. Complete una de las siguientes tareas:
   - Si utiliza un asistente de protección (Proteger equipo, Proteger varios equipos, Proteger un clúster), en la página **Protección** del asistente, seleccione **Protección personalizada** y, a continuación, haga clic en **Siguiente**.
   - Si crea un programa de protección para un equipo que ya está protegido, en la página Resumen del equipo protegido, expanda los volúmenes del equipo protegido, seleccione los volúmenes aplicables y, a continuación, haga clic en **Establecer un programa**.

Aparece la página o el cuadro de diálogo **Programa de protección**.

2. En la página o el cuadro de diálogo **Programa de protección**, complete una de las opciones siguientes:

   - Para establecer un periodo de protección que se ejecute los días establecidos y en las horas especificadas, seleccione **Periodos** y, a continuación, vaya al paso 3.
   - Para establecer una hora específica para realizar copias de seguridad del equipo cada día, seleccione **Hora de protección diaria** y, a continuación, vaya al paso 7.

3. Para cambiar el intervalo de programación de cualquier periodo, complete los pasos siguientes:
   a. Cree un lapso de tiempo seleccionado una hora **de inicio** y una hora **de finalización**.
   b. Para cada periodo, haga clic en el cuadro de texto del intervalo e introduzca un intervalo adecuado en minutos.

   Por ejemplo, resalte el intervalo predeterminado de 60 y sustitúyalo por el valor 20 para realizar instantáneas cada 20 minutos durante este período.

4. Para personalizar las instantáneas en el horario laboral en las horas pico y fuera de horas pico, complete los pasos siguientes: establezca un intervalo óptimo para el intervalo pico, seleccione **Tomar instantáneas durante el tiempo restante** y, a continuación, establezca un intervalo fuera de horas pico siguiendo los pasos siguientes:
   a. Seleccione **Días laborables**.
   b. Establezca las horas **de inicio** y **de finalización** para crear un lapso de tiempo durante las horas laborales pico.
   c. En el cuadro **Cada X minutos**, introduzca un intervalo en minutos de la frecuencia con la que Rapid Recovery debe crear puntos de recuperación durante este lapso de horas laborales pico.

   Por ejemplo, resalte el intervalo existente de 60 y sustitúyalo por el valor 20 para realizar instantáneas cada 20 minutos durante el rango de tiempo que seleccionó para este período.
   d. Para programar las instantáneas durante las horas laborables fuera de las horas pico, seleccione **Tomar instantáneas durante el resto de tiempo**.
   e. En el cuadro **Cada X minutos**, introduzca un intervalo en minutos de la frecuencia con la que Rapid Recovery debe crear puntos de recuperación durante este lapso de horas laborales fuera de las horas pico.

   Por ejemplo, debido a que hay menos actividad empresarial durante estas horas y menos cambios en las copias de seguridad, puede decidir tomar menos instantánea y mantener el intervalo predeterminado de 60 minutos.

5. Continúe con el paso 7.
6. Para establecer que se realice a diario una única copia de seguridad a una sola hora del día, seleccione **Hora de protección diaria** y, a continuación, introduzca una hora con el formato HH:MM AM. Por ejemplo, para realizar una copia de seguridad diaria a las 21:00, introduzca 09:00 PM.
7. Para definir el calendario de programación sin comenzar copias de seguridad, seleccione **Pausar protección inicialmente**.

   Después de que haya realizado una pausa en la protección desde el asistente, permanecerá en pausa hasta que no la reanude de manera explícita. Una vez reanude la protección, las copias de seguridad se realizarán basándose en la programación que establezca. Para obtener más información sobre reanudar la protección, consulte Puesta en pausa y reanudación de la protección.

8. Cuando esté satisfecho con los cambios realizados en su calendario de programación de protección, haga clic en **Finalizar** o **Siguiente**, según sea adecuado.

   Si está utilizando un asistente, continúe con el paso siguiente del el asistente. Consulte el procedimiento para que el asistente adecuado cumpla los requisitos restantes.

See also: Comprensión del calendario de programación de protección.
See also: Creación de un programa de protección personalizado en el modo simple
See also: Creación de varios periodos de programación para protección en el modo avanzado

Creación de varios periodos de programación para protección en el modo avanzado

El programa de protección define cuándo se transfieren las copias de seguridad desde los equipos protegidos al Rapid Recovery Core. Los calendarios de programación de protección se definen inicialmente mediante el Asistente para proteger un equipo o el Asistente para proteger varios equipos.

Puede modificar una programación de protección existente en cualquier momento desde la página Resumen para un equipo protegido específico.

NOTE: Para obtener información sobre los conceptos de los calendarios de programación de protección, consulte Comprensión del calendario de programación de protección.. Para obtener información sobre cómo proteger un único equipo, consulte Protección de un equipo. Para obtener información sobre la protección masiva (la protección de varios equipos), consulte Acerca de la protección de varios equipos. Para obtener información sobre cómo personalizar periodos de protección al proteger un Agent mediante uno de estos asistentes, consulte Creación de un programa de protección personalizado en el modo simple. Para obtener información sobre cómo modificar un calendario de programación de protección existente, consulte Creación de varios periodos de programación para protección en el modo avanzado.

Realice los pasos que se indican en este procedimiento para modificar un calendario de programación de protección existente para volúmenes en un equipo protegido.

1. En la Core Console, en la lista de equipos protegidos, haga clic en el nombre del equipo que tiene la programación de protección que quiere cambiar.
2. En la página Resumen del equipo que haya seleccionado, en el panel Volúmenes, expanda los volúmenes del equipo protegido, seleccione los volúmenes aplicables y, a continuación, haga clic en **Establecer una programación**.

   Inicialmente, todos los volúmenes comparten una programación de protección.

   Para seleccionar todos los volúmenes a la vez, haga clic en la casilla de verificación de la fila del encabezado. Haga clic en (Grupo de protección) para expandir los volúmenes que se vayan a proteger, de manera que puede ver todos los volúmenes y seleccionar uno o varios.

   NOTE: Por lo general, es recomendable proteger, como mínimo, el volumen reservado para el sistema y el volumen con el sistema operativo (normalmente la unidad C).

Aparece el cuadro de diálogo **Programación de protección**.

3. En el cuadro de diálogo **Programación de protección**, realice una de las siguientes acciones:
   - Para modificar el periodo de programación existente en la página inicial del cuadro de diálogo, que se denomina Modo simple, consulte el procedimiento para Creación de varios periodos de programación para protección en el modo avanzado.
   - Si ha creado previamente una plantilla de programación de protección y quiere aplicarla a este equipo protegido, haga clic en **Modo avanzado**, seleccione la plantilla de la lista desplegable **Plantillas**, haga clic en **Aceptar** para confirmar y, a continuación, vaya al paso 7.
   - Si desea eliminar un periodo de tiempo de una programación, desmarque la casilla de verificación junto a cada opción de periodo de tiempo y, a continuación, vaya al paso 7. Las opciones incluyen las siguientes:
     - Días laborables (Lun-Vie): este intervalo de tiempo se refiere a una semana laboral típica de cinco días.
     - Fines de semana (Sáb, Dom): este intervalo de tiempo indica un fin de semana típico.
   - Si desea guardar una nueva programación de protección como una plantilla, haga clic en **Modo avanzado** y, a continuación, vaya al paso 4.
4. Un periodo es un lapso de tiempo especificado durante el cual determina cuántos minutos deben pasar entre cada instantánea tomada. Cuando las horas de inicio y finalización del día de la semana sean desde las 12:00 hasta las 23:59, solo existe un periodo. Para cambiar la hora de inicio o de finalización de un período definido, haga lo siguiente:
   a. Seleccione el período de tiempo adecuado.
   b. Para cambiar la hora de inicio de este periodo, utilice el icono del reloj en **Hora de inicio**.

   Por ejemplo, utilice las flechas para mostrar las 08:00.

   c. Para cambiar la hora de finalización de este periodo, utilice el icono del reloj en **Hora de finalización**.

   Por ejemplo, utilice las flechas para mostrar las 18:00.

   d. Cambie el intervalo de acuerdo con sus requisitos. Por ejemplo, si está definiendo un periodo de horas pico, cambie el intervalo de 60 minutos a 20 minutos para tomar instantáneas tres veces cada hora.

   Una barra azul proporciona una representación visual de este intervalo.
5. Si se ha definido un periodo distinto al de las 12:00 a las 23:59 en el paso 7 y 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. En la categoría adecuada, haga clic en **Agregar periodo**.
   b. Haga clic en el icono del reloj y seleccione la hora de inicio y la hora de finalización deseadas, según corresponda.

   Por ejemplo, establezca la hora de inicio a las 12:00 y la hora de finalización a las 07:59.

   c. Cambie el intervalo de acuerdo con sus requisitos. Por ejemplo, si está definiendo un periodo fuera de horas pico, cambie el intervalo de 60 minutos a 120 minutos para tomar instantáneas cada dos horas.
6. Si fuera necesario, continúe para crear periodos adicionales y configure las horas de inicio y finalización y los intervalos según corresponda.

   NOTE: Si desea eliminar un periodo que ha agregado, haga clic en el icono de la papelera del extremo derecho de ese periodo y, a continuación, haga clic en **Sí** para confirmar.
7. Para crear una plantilla desde el calendario de programación que ha establecido, haga clic en **Guardar como plantilla**.
8. En el cuadro de diálogo Guardar plantilla, introduzca un nombre para la plantilla y, a continuación, haga clic en **Guardar**.
9. Cuando el programa de protección cumpla sus requisitos, haga clic en **Aplicar**.

El cuadro de diálogo Calendario de programación de protección se cerrará.

See also: Comprensión del calendario de programación de protección.
See also: Creación de un programa de protección personalizado en el modo simple
See also: Creación de varios periodos de programación para protección en el modo avanzado

Puesta en pausa y reanudación de la protección

Cuando se pausa la protección, se detienen temporalmente todas las transferencias de datos del equipo seleccionado al Core de Rapid Recovery. Cuando reanuda la protección, el Core de Rapid Recovery sigue los requisitos del calendario de programación de protección, creando copias de seguridad de sus datos con regularidad basándose en ese calendario de programación.

Puede pausar la protección para cualquier equipo protegido de Rapid Recovery:

- Al establecer la protección mediante el Asistente para proteger un equipo o el Asistente para proteger varios equipos.
- Desde el menú desplegable Equipos protegidos que se encuentra en el área de navegación izquierda del Core de Rapid Recovery (puesta en pausa de la protección para todos los equipos protegidos).
- Desde la página Equipos protegidos (accesible cuando hace clic en el menú Equipos protegidos).
- Desde un equipo protegido específico del menú desplegable Equipos protegidos.
- Desde la parte superior de cada página para un equipo protegido específico.

Si pausa la protección mediante el Asistente para proteger un equipo o el Asistente para proteger varios equipos, la protección se pausará hasta que se reanude de manera explícita.

Si pausa la protección fuera de un asistente, puede elegir entre pausar la protección hasta que se reanude o pausarla durante una cantidad de tiempo indicada (especificada en cualquier combinación de días, horas y minutos). Si la pausa durante un período de tiempo, cuando venza ese tiempo, el sistema reanudará la protección basándose en el calendario de programación de protección automáticamente.

Puede reanudar la protección para cualquier equipo protegido de Rapid Recovery en pausa:

- Desde el menú desplegable Equipos protegidos que se encuentra en el área de navegación izquierda del Core de Rapid Recovery (reanudación de la protección para todos los equipos protegidos).
- Desde un equipo protegido específico del menú desplegable Equipos protegidos.
- Desde la página Equipos protegidos (accesible cuando hace clic en el menú Equipos protegidos).
- Desde la parte superior de cada página para un equipo protegido específico.

Utilice el procedimiento siguiente para pausar o reanudar la protección, según sea adecuado.

1. En la Core Console de Rapid Recovery, para pausar la protección en todos los equipos, haga clic en el menú desplegable Equipos protegidos del área de navegación izquierda y, a continuación, haga lo siguiente:
    a. Seleccione **Pausar la protección**.

    Aparecerá el cuadro de diálogo Pausar la protección.

b. Seleccione el ajuste adecuado utilizando una de las opciones descritas a continuación y, a continuación, haga clic en **Aceptar**.

- Si desea pausar la protección hasta que la reanude de manera explícita, seleccione **Pausar hasta reanudación**.
- Si desea pausar la protección durante un período especificado, seleccione **Pausar durante** y, a continuación, en los controles Días, Horas y Minutos, escriba o seleccione el período de pausa que sea adecuado.

2. Para reanudar la protección en todos los equipos, haga lo siguiente:
   a. Seleccione **Reanudar la protección**.

   Aparecerá el cuadro de diálogo Reanudar la protección.

   b. En el cuadro de diálogo Reanudar la protección, seleccione **Sí**.

   El cuadro de diálogo Reanudar la protección se cerrará y la protección se reanudará para todos los equipos.
3. Para pausar la protección de un solo equipo, a continuación, en el área de navegación izquierda, haga clic en el menú desplegable que se encuentra a la derecha del equipo cuya protección quiere modificar y haga lo siguiente:
   a. Seleccione **Pausar la protección**.

   Aparecerá el cuadro de diálogo Pausar la protección.

   b. Seleccione el ajuste adecuado utilizando una de las opciones descritas a continuación y, a continuación, haga clic en **Aceptar**.

   - Si desea pausar la protección hasta que la reanude de manera explícita, seleccione **Pausar hasta reanudación**.
   - Si desea pausar la protección durante un período especificado, seleccione **Pausar durante** y, a continuación, en los controles Días, Horas y Minutos, escriba o seleccione el período de pausa que sea adecuado.
4. Para reanudar la protección de un solo equipo, haga lo siguiente:
   a. Seleccione **Reanudar la protección**.

   Aparecerá el cuadro de diálogo Reanudar la protección.

   b. En el cuadro de diálogo Reanudar la protección, seleccione **Sí**.

   El cuadro de diálogo Reanudar la protección se cerrará y la protección se reanudará para el equipo seleccionado.
5. Para pausar la protección de un único equipo desde la página Equipo, desplácese hasta el equipo cuya protección quiere modificar.

   Aparecerá la página Resumen para el equipo seleccionado.

   a. En la parte superior de la página, haga clic en **Pausar**.

   Aparecerá el cuadro de diálogo Pausar la protección.

   b. Seleccione el ajuste adecuado utilizando una de las opciones descritas a continuación y, a continuación, haga clic en **Aceptar**.

   - Si desea pausar la protección hasta que la reanude de manera explícita, seleccione **Pausar hasta reanudación**.
   - Si desea pausar la protección durante un período especificado, seleccione **Pausar durante** y, a continuación, en los controles Días, Horas y Minutos, escriba o seleccione el período de pausa que sea adecuado.
6. Si desea reanudar la protección, haga lo siguiente:
   a. En la parte superior de la página, haga clic en **Reanudar**.
   b. En el cuadro de diálogo Reanudar la protección, haga clic en **Sí**.

   El cuadro de diálogo Reanudar la protección se cierra y la protección se reanuda para el equipo seleccionado.

Acerca de la protección de varios equipos

Puede agregar dos o más equipos con Windows para su protección en el Rapid Recovery Core simultáneamente mediante el Asistente para proteger varios equipos. Para proteger sus datos mediante Rapid Recovery, debe agregar las estaciones de trabajo y los servidores para la protección en la Rapid Recovery Core Console; por ejemplo, su Exchange Server, SQL Server, servidor Linux, etc.

Al igual que al proteger equipos individuales, la protección de varios equipos simultáneamente requiere la instalación del software Rapid Recovery Agent en todos los equipos que desee proteger.

NOTE: Como excepción a la regla, si protege máquinas virtuales en un host VMware/ESXi o Hyper-V, puede utilizar protección sin agentes. Para obtener más información, incluidas las restricciones para la protección sin agentes, consulte Comprensión de Rapid Snap for Virtual.

Los equipos protegidos se deben configurar con una política de seguridad que permita que la instalación remota sea posible.

Para conectarse a los equipos, tienen que ser accesibles y estar encendidos.

Hay más de un método para implementar el software Agent en varios equipos simultáneamente. Por ejemplo:

- Puede instalar el software Rapid Recovery Agent en varios equipos utilizando el Asistente para implementar el software Agent. Para obtener más información, consulte Uso del asistente para implementar el software Agent para implementar en uno o varios equipos.
- Puede implementar el software Rapid Recovery Agent como parte del Asistente para proteger varios equipos.

El proceso de protección de varios equipos incluye pasos opcionales a los que puede acceder si selecciona una configuración avanzada. Las opciones avanzadas incluyen las funciones de repositorio y el cifrado. Por ejemplo, puede especificar un repositorio de Rapid Recovery existente para guardar instantáneas o puede crear un nuevo repositorio. También puede especificar una clave de cifrado existente (o agregar una nueva clave de cifrado) para aplicarla a los datos guardados en el Core para los equipos que protege.

El flujo de trabajo del Asistente para proteger varios equipos puede variar ligeramente según su entorno. Por ejemplo, si el software Rapid Recovery Agent está instalado en los equipos que desea proteger, no se le pedirá que lo instale desde el asistente. Del mismo modo, si ya existe un repositorio en el Core, no se le pedirá que cree uno.

Al proteger varios equipos, siga los procedimientos adecuados en función de su configuración. Consulte las siguientes opciones para proteger varios equipos:

- Protección de varios equipos en un dominio de Active Directory
- Protección de varios equipos en un host virtual VMware vCenter/ESXi
- Protección de varios equipos en un host virtual Hyper-V
- Protección de varios equipos manualmente

Protección de varios equipos en un dominio de Active Directory

Utilice este procedimiento para proteger de forma simultánea uno o varios equipos de un dominio de Active Directory.

1. En la Rapid Recovery Core Console, haga clic en el menú desplegable **Proteger** y, a continuación, haga clic en **Proteger varios equipos**.

   Se abre el Asistente para proteger varios equipos.
2. En la página de **bienvenida** del asistente, seleccione una de las opciones siguientes:
   - Típicas
   - Avanzado (mostrar pasos opcionales)
3. Haga clic en **Siguiente**.
4. En la página **Conexión** del asistente, en la lista desplegable **Origen**, seleccione **Active Directory**.
5. Introduzca la información de dominio y las credenciales de inicio de sesión según se describe en la tabla siguiente.

Tabla 53. Información y credenciales de dominio

Cuadro de texto	Descripción
Host	Nombre de host o dirección IP del dominio de Active Directory.
Nombre de usuario	El nombre de usuario utilizado para conectarse con el dominio; por ejemplo, Administrator (o, si el equipo se encuentra en un dominio, [nombre de dominio]\Administrator).
Contraseña	La contraseña segura que se utiliza para conectar con el dominio.

6. Haga clic en **Siguiente**.
7. En la página **Seleccionar equipos** del asistente, seleccione los equipos que desea proteger.

   El sistema verifica automáticamente todos los equipos que seleccione.
8. Haga clic en **Siguiente**.

   Si a continuación aparece la página **Protección** en el Asistente para proteger varios equipos, vaya al paso 12.

   Si el software Agent todavía no se ha implementado en los equipos que desee proteger o si alguno de los equipos que especificó no puede protegerse por cualquier otro motivo, los equipos seleccionados aparecerán en la página Advertencias.
9. Opcionalmente, en la página **Advertencias** del asistente, puede verificar cualquier equipo seleccionando el equipo y, a continuación, haciendo clic en **Verificar** en la barra de herramientas.
10. Opcionalmente, en la página **Advertencias**, seleccione **Tras la instalación de Agent, reinicie los equipos automáticamente**.

    NOTE: Quest recomienda esta opción. Debe reiniciar los equipos Agent antes de poder protegerlas.
11. Si el estado indica que puede llegarse al equipo, haga clic en **Siguiente** para instalar el software Rapid Recovery Agent.

Aparecerá la página **Protección**.

12. De manera opcional, en la página **Protección**, si quiere que aparezca un nombre distinto a la dirección IP en la Rapid Recovery Core Console de este equipo protegido, en el campo **Nombre para mostrar**, escriba un nombre en el cuadro de diálogo.

    Puede introducir hasta 64 caracteres. No utilice los caracteres especiales descritos en el tema . Tampoco el nombre para mostrar debe comenzar por cualquiera de las combinaciones de caracteres descritas en el tema .

13. Seleccione la configuración de programación para protección adecuada tal como se describe a continuación:

    - Para utilizar la programación para protección predeterminada, en la opción Configuración de programación, seleccione **Protección predeterminada (instantáneas de todos los volúmenes cada hora)**.

    Con un calendario de programación de protección predeterminado, el Core tomará instantáneas de todos los volúmenes del equipo protegido una vez cada hora. Para cambiar la configuración de protección en cualquier momento después de cerrar el asistente, incluida la selección de qué volúmenes proteger, vaya a la página **Resumen** del equipo protegido específico.

    - Para definir un calendario de programación de protección diferente, en la opción Configuración de calendario de programación, seleccione **Protección personalizada**.

14. Continúe con su configuración del modo siguiente:

    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si existe un repositorio, haga clic en **Finalizar** para confirmar sus opciones, cierre el asistente y proteja el equipo que ha especificado.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si no existe un repositorio, haga clic en **Siguiente** y continúe en el paso 17 para crear un repositorio.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe con el siguiente paso para seleccionar qué volúmenes se van a proteger.
    - Si ha seleccionado una configuración avanzada para el Asistente para proteger un equipo, así como la protección predeterminada, haga clic en **Siguiente** y continúe en el paso 17 para ver las opciones de repositorio y cifrado.
    - Si ha seleccionado Configuración avanzada para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe en el siguiente paso para seleccionar qué volúmenes se van a proteger.

    La primera vez que se agrega protección a un equipo, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio del Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

15. En la página **Volúmenes de protección**, seleccione los volúmenes que desea proteger. Si se indican volúmenes que no quiera incluir en la protección, haga clic en la columna Comprobar para borrar la selección. A continuación, haga clic en **Siguiente**.

    NOTE: Por lo general, es recomendable proteger, como mínimo, el volumen reservado para el sistema y el volumen con el sistema operativo (normalmente la unidad C).

16. En la página **Calendario de programación de protección**, defina un calendario de programación de protección personalizado y luego haga clic en **Siguiente**. Para obtener información detallada sobre cómo definir un calendario de programación de protección personalizado, consulte Creación de un programa de protección personalizado en el modo simple.

Si ya ha configurado la información del repositorio y ha seleccionado Opciones avanzadas en el paso 1, aparece la página Cifrado. Continúe en el paso 20.

17. En la página **Repositorio**, realice los siguientes pasos:

    - Si ya tiene un repositorio y desea almacenar los datos de este equipo para la protección del repositorio existente, realice una de las acciones siguientes:

      1. Seleccione **Usar un repositorio existente**.
      2. Seleccione un repositorio existente de la lista.
      3. Haga clic en **Siguiente**.

      Se abrirá la página de **Cifrado**. Vaya al paso 20 para definir el cifrado de manera opcional.

    - Si desea crear un repositorio, en la página **Repositorio**, introduzca la información que se describe en la tabla siguiente y haga clic en **Siguiente** o **Finalizar** según corresponda.

Tabla 54. Configuración del repositorio

Cuadro de texto	Descripción
Nombre	Introduzca el nombre para mostrar del repositorio. De manera predeterminada, este cuadro de texto incluye el término Repositorio y un número, que se corresponde con el número de repositorios de este Core. Por ejemplo, si se trata del primer repositorio, el nombre predeterminado es Repositorio 1. Cambie el nombre según sea necesario. Los nombres del repositorio contienen entre 1 y 40 caracteres alfanuméricos, incluidos los espacios. No utilice caracteres prohibidos ni frases prohibidas.
Ubicación	Introduzca la ubicación para almacenar los datos protegidos. Este volumen debe ser la ubicación de almacenamiento principal. La ubicación puede ser local (una unidad en el equipo Core) o una unidad de red de uso compartido de CIFS. Si es de uso compartido de CIFS, la ruta debe comenzar por \\. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación. **CAUTION: Defina una carpeta específica en la raíz para la ubicación de almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice `E:\Repository\`, no `E:\`. Si el repositorio que está creando en este paso se elimina más adelante, se eliminarán todos los archivos en la ubicación de almacenamiento de su repositorio. Si define la ubicación de almacenamiento en la raíz, el resto de archivos del volumen (p. ej., `E:\`) se eliminan, lo que podría derivar en una pérdida grave de datos.** Por ejemplo, introduzca `X:\Repository\Data`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
Nombre de usuario	Introduzca un nombre de usuario para un usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.
Contraseña	Introduzca la contraseña para el usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.

Cuadro de texto	Descripción
Ruta de acceso a metadatos	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, introduzca `X:\Repository\Metadata`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.

18. En la página **Configuración del repositorio**, configure la cantidad de espacio en disco que desea asignar en el repositorio. Quest recomienda reservar un 20 % del volumen a los metadatos, que es el valor predeterminado. De manera opcional, utilizando el control deslizante o el campo **Tamaño**, puede asignar más o menos espacio de volumen para el repositorio.
19. De manera opcional, si desea visualizar e introducir información detallada acerca de la configuración de la ubicación de almacenamiento, seleccione **Mostrar opciones avanzadas** y ajuste la configuración como se describe en la siguiente tabla. Para ocultar estas opciones, desactive la opción **Mostrar opciones avanzadas**. Cuando haya completado la configuración del repositorio, haga clic en **Siguiente** o en **Finalizar**, según proceda.

Tabla 55. Detalles de configuración de almacenamiento

Cuadro de texto	Descripción
Bytes por sector	Especifique el número de bytes que desea que incluya cada sector. El valor predeterminado es 512.
Bytes por registro	Especifique el promedio del número de bytes por registro. El valor predeterminado es 8192.
Política de almacenamiento en caché de escritura	La política de almacenamiento en caché de escritura controla cómo se utiliza el Administrador de caché de Windows en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: • Activado • Desactivado • Sincronización Si se establece como Activado, que es el valor predeterminado, Windows controla el almacenamiento en caché. Es adecuado para Windows 10 y para versiones de Windows Server 2012 y posteriores. **NOTE:** si se establece la política de escritura en caché en Activado, se mejora el rendimiento; no obstante, el valor recomendado es Desactivada. Si utiliza Windows Server 2008 R2 SP2, la configuración recomendada es Desactivado. Si se establece en Desactivado, Rapid Recovery controla el almacenamiento en caché. Si se establece en Sincronización, Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.

Si ha seleccionado la opción **Avanzada** en el paso 1, aparece la página **Cifrado**.

20. De manera opcional, en la página **Cifrado**, si desea utilizar claves de cifrado para los datos almacenados en el repositorio, seleccione **Cifrar los datos en reposo en un repositorio** y, a continuación, realice una de las acciones siguientes:
    - Para seleccionar una clave de cifrado existente y aplicarla a todos los nuevos datos almacenados en el repositorio, seleccione **Cifrar los datos utilizando un cifrado basado en Core con una clave existente**, y, en el menú desplegable **Seleccionar clave de cifrado** seleccione la clave de cifrado.
    - Para definir una nueva clave de cifrado en este momento y aplicarla a todos los futuros datos almacenados en el repositorio, seleccione **Cifrar datos mediante un cifrado basado en el Core con una clave nueva** y, a continuación, introduzca información sobre la clave como se describe en la siguiente tabla:

Tabla 56. Definir nueva clave de cifrado

Cuadro de texto	Descripción
Nombre	Escriba un nombre para la clave de cifrado. Los nombres de las claves de cifrado contienen entre 1 y 64 caracteres alfanuméricos. No utilice caracteres no permitidos o frases no permitidas.
Descripción	Escriba un comentario descriptivo para la clave de cifrado. Esta información aparece en el campo Descripción cuando al visualizar una lista de claves de cifrado en la Rapid Recovery Core Console. Las descripciones pueden contener hasta 254 caracteres. La práctica recomendada es evitar el uso de caracteres no permitidos y frases no permitidas.
Frase de contraseña	Introduzca una frase de contraseña usada para controlar el acceso. La práctica recomendada es evitar el uso de caracteres no permitidos. Registre la frase de contraseña en lugar seguro. Asistencia para la protección de datos de Quest no puede recuperar frases de contraseña. Una vez cree una clave de cifrado y la aplique a uno o más equipos protegidos no podrá recuperar los datos si pierde la frase de contraseña.
Confirmar la frase de contraseña	Como confirmación, vuelva a escribir la Frase de contraseña. Se utiliza para confirmar la entrada de frase de contraseña.

21. De manera opcional, en la página **Cifrado**, si desea cifrar todos los datos de transporte a través de una red, seleccione **Cifrar los datos de transporte a través de una red**. Esta opción está habilitada de manera predeterminada. Si no desea cifrar los datos de esta manera, desactive esta opción.
22. Haga clic en **Finalizar** para guardar y aplicar sus ajustes.

    La primera vez que se agrega protección para una máquina, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

El software Rapid Recovery Agent se implementa en los equipos especificados y, si es necesario, se añaden los equipos a la protección en el Core.

Protección de varios equipos en un host virtual VMware vCenter/ESXi

Utilice este procedimiento para proteger simultáneamente uno o más equipos de un host virtual VMware vCenter/ESXi.

CAUTION: Si utiliza la protección sin agentes, Quest **recomienda limitar la protección a no más de 200 VM a la vez. Por ejemplo, no seleccione más de 200 VM mientras utiliza el Asistente para proteger varios equipos. La protección de más de 200 VM puede dar lugar a un rendimiento más lento. No existe un límite de VM que un Core pueda proteger sin agentes a lo largo del tiempo. Por ejemplo, hoy podría proteger 200 VM y mañana 200 más.**

1. En la Rapid Recovery Core Console, haga clic en el menú desplegable **Proteger** y, a continuación, haga clic en **Proteger varios equipos**.

   Se abre el Asistente para proteger varios equipos.
2. En la página de **bienvenida**, seleccione una de las opciones siguientes:
   - Típicas
   - Avanzado (mostrar pasos opcionales)
3. Haga clic en **Siguiente**.
4. En la página **Conexión** del asistente, en la lista desplegable **Origen**, seleccione **vCenter/ESXi**.
5. Introduzca la información de host y las credenciales de inicio de sesión según se describe en la tabla siguiente.

Tabla 57. Información de configuración de la conexión vCenter/ESXi

Cuadro de texto	Descripción
Host	Nombre o dirección IP del host virtual de VMware vCenter Server/ESXi.
Puerto	Número de puerto usado para conectar con el host virtual. El valor predeterminado es 443.
Nombre de usuario	El nombre de usuario utilizado para conectarse con el host virtual; por ejemplo, Administrator o, si el equipo se encuentra en un dominio, [nombre de dominio]\Administrator.
Contraseña	La contraseña segura que se utiliza para conectarse con este host virtual.

   - Para utilizar la protección sin agentes, seleccione **Proteger VM seleccionadas sin agentes** y, a continuación, consulte Proteger máquinas virtuales vCenter/ESXi mediante la protección sin agentes.
6. Haga clic en **Siguiente**.
7. En la página **Seleccionar equipos**, realice una de las acciones siguientes:
   - En la lista de VM, seleccione las VM que desea proteger.
   - Para desplazarse por la estructura de árbol para encontrar más máquinas virtuales, haga clic en **Ver árbol** y seleccione **Hosts y clústeres** o **VM y plantillas**. Seleccione las VM que desea proteger.

Aparece una notificación si Rapid Recovery detecta que un equipo no tiene conexión o que las herramientas de VMware no están instaladas.

8. Haga clic en **Siguiente**.
9. En la página **Ajustes**, escriba las credenciales de cada equipo con el siguiente formato: `hostname::username::password`.

   NOTE: Introduzca un equipo por línea.

10. Haga clic en **Siguiente**.

    Si a continuación aparece la página **Protección** en el Asistente para proteger varios equipos, vaya al paso 14.

    Si el software Agent todavía no se ha implementado en los equipos que desee proteger o si alguno de los equipos que especificó no puede protegerse por cualquier otro motivo, los equipos seleccionados aparecerán en la página **Advertencias**.

11. Opcionalmente, en la página **Advertencias**, puede verificar cualquier equipo seleccionando el equipo y, a continuación, haciendo clic en **Verificar** en la barra de herramientas.
12. Opcionalmente, en la página **Advertencias**, seleccione **Tras la instalación de Agent, reinicie los equipos automáticamente**.

    NOTE: Quest recomienda esta opción. Debe reiniciar los equipos Agent antes de poder protegerlas.

13. Si el estado indica que puede llegarse al equipo, haga clic en **Siguiente** para instalar el software Agent.

    Aparecerá la página **Protección**.

14. De manera opcional, en la página **Protección**, si quiere que aparezca un nombre distinto a la dirección IP en la Rapid Recovery Core Console de este equipo protegido, en el campo **Nombre para mostrar**, escriba un nombre en el cuadro de diálogo.

    Puede introducir hasta 64 caracteres. No utilice los caracteres especiales descritos en el tema . Tampoco el nombre para mostrar debe comenzar por cualquiera de las combinaciones de caracteres descritas en el tema .

15. Seleccione la configuración de programación para protección adecuada tal como se describe a continuación:

    - Para utilizar la programación para protección predeterminada, en la opción Configuración de programación, seleccione **Protección predeterminada (instantáneas de todos los volúmenes cada hora)**.

    Con un calendario de programación de protección predeterminado, el Core tomará instantáneas de todos los volúmenes del equipo protegido una vez cada hora. Para cambiar la configuración de protección en

cualquier momento después de cerrar el asistente, incluida la selección de qué volúmenes proteger, vaya a la página **Resumen** del equipo protegido específico.

- Para definir un calendario de programación de protección diferente, en la opción Configuración de calendario de programación, seleccione **Protección personalizada**.

16. Continúe con su configuración del modo siguiente:
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si existe un repositorio, haga clic en **Finalizar** para confirmar sus opciones, cierre el asistente y proteja el equipo que ha especificado.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si no existe un repositorio, haga clic en **Siguiente** y continúe en el paso 19 para crear un repositorio.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe con el siguiente paso para seleccionar qué volúmenes se van a proteger.
    - Si ha seleccionado una configuración avanzada para el Asistente para proteger un equipo, así como la protección predeterminada, haga clic en **Siguiente** y continúe en el paso 19 para ver las opciones de repositorio y cifrado.
    - Si ha seleccionado Configuración avanzada para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe en el siguiente paso para seleccionar qué volúmenes se van a proteger.

    La primera vez que se agrega protección a un equipo, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio del Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.
17. En la página **Volúmenes de protección**, seleccione los volúmenes que desea proteger. Si se indican volúmenes que no quiera incluir en la protección, haga clic en la columna Comprobar para borrar la selección. A continuación, haga clic en **Siguiente**.

    NOTE: Por lo general, es recomendable proteger, como mínimo, el volumen reservado para el sistema y el volumen con el sistema operativo (normalmente la unidad C).
18. En la página **Calendario de programación de protección**, defina un calendario de programación de protección personalizado y luego haga clic en **Siguiente**. Para obtener información detallada sobre cómo definir un calendario de programación de protección personalizado, consulte Creación de un programa de protección personalizado en el modo simple.

    Si ya ha configurado la información del repositorio y ha seleccionado Opciones avanzadas en el paso 1, aparece la página Cifrado. Continúe en el paso 22.
19. En la página **Repositorio**, realice los siguientes pasos:
    - Si ya tiene un repositorio y desea almacenar los datos de este equipo para la protección del repositorio existente, realice una de las acciones siguientes:
        1. Seleccione **Usar un repositorio existente**.
        2. Seleccione un repositorio existente de la lista.
        3. Haga clic en **Siguiente**.

        Se abrirá la página de **Cifrado**. Vaya al paso 22 para definir el cifrado de manera opcional.
    - Si desea crear un repositorio, en la página **Repositorio**, introduzca la información que se describe en la tabla siguiente y haga clic en **Siguiente** o **Finalizar** según corresponda.

Tabla 58. Configuración del repositorio

Cuadro de texto	Descripción
Nombre	Introduzca el nombre para mostrar del repositorio.

Cuadro de texto	Descripción
	De manera predeterminada, este cuadro de texto incluye el término Repositorio y un número, que se corresponde con el número de repositorios de este Core. Por ejemplo, si se trata del primer repositorio, el nombre predeterminado es Repositorio 1. Cambie el nombre según sea necesario. Los nombres del repositorio contienen entre 1 y 40 caracteres alfanuméricos, incluidos los espacios. No utilice caracteres prohibidos ni frases prohibidas.
Ubicación	Introduzca la ubicación para almacenar los datos protegidos. Este volumen debe ser la ubicación de almacenamiento principal. La ubicación puede ser local (una unidad en el equipo Core) o una unidad de red de uso compartido de CIFS. Si es de uso compartido de CIFS, la ruta debe comenzar por \\. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación. **CAUTION: Defina una carpeta específica en la raíz para la ubicación de almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice `E:\Repository\`, no `E:\`. Si el repositorio que está creando en este paso se elimina más adelante, se eliminarán todos los archivos en la ubicación de almacenamiento de su repositorio. Si define la ubicación de almacenamiento en la raíz, el resto de archivos del volumen (p. ej., `E:\`) se eliminan, lo que podría derivar en una pérdida grave de datos.** Por ejemplo, introduzca `X:\Repository\Data`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
Nombre de usuario	Introduzca un nombre de usuario para un usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.
Contraseña	Introduzca la contraseña para el usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.
Ruta de acceso a metadatos	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, introduzca `X:\Repository\Metadata`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.

20. En la página **Configuración del repositorio**, configure la cantidad de espacio en disco que desea asignar en el repositorio. Quest recomienda reservar un 20 % del volumen a los metadatos, que es el valor predeterminado. De manera opcional, utilizando el control deslizante o el campo **Tamaño**, puede asignar más o menos espacio de volumen para el repositorio.
21. De manera opcional, si desea visualizar e introducir información detallada acerca de la configuración de la ubicación de almacenamiento, seleccione **Mostrar opciones avanzadas** y ajuste la configuración como se describe en la siguiente tabla. Para ocultar estas opciones, desactive la opción **Mostrar opciones avanzadas**. Cuando haya completado la configuración del repositorio, haga clic en **Siguiente** o en **Finalizar**, según proceda.

Tabla 59. Detalles de configuración de almacenamiento

Cuadro de texto	Descripción
Bytes por sector	Especifique el número de bytes que desea que incluya cada sector. El valor predeterminado es 512.
Bytes por registro	Especifique el promedio del número de bytes por registro. El valor predeterminado es 8192.
Política de almacenamiento en caché de escritura	La política de almacenamiento en caché de escritura controla cómo se utiliza el Administrador de caché de Windows en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: • Activado • Desactivado • Sincronización Si se establece como Activado, que es el valor predeterminado, Windows controla el almacenamiento en caché. Es adecuado para Windows 10 y para versiones de Windows Server 2012 y posteriores. **NOTE:** si se establece la política de escritura en caché en Activado, se mejora el rendimiento; no obstante, el valor recomendado es Desactivada. Si utiliza Windows Server 2008 R2 SP2, la configuración recomendada es Desactivado. Si se establece en Desactivado, Rapid Recovery controla el almacenamiento en caché. Si se establece en Sincronización, Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.

Si ha seleccionado la opción **Avanzada** en el paso 1, aparece la página **Cifrado**.

22. De manera opcional, en la página **Cifrado**, si desea utilizar claves de cifrado para los datos almacenados en el repositorio, seleccione **Cifrar los datos en reposo en un repositorio** y, a continuación, realice una de las acciones siguientes:
    - Para seleccionar una clave de cifrado existente y aplicarla a todos los nuevos datos almacenados en el repositorio, seleccione **Cifrar los datos utilizando un cifrado basado en Core con una clave existente**, y, en el menú desplegable **Seleccionar clave de cifrado** seleccione la clave de cifrado.
    - Para definir una nueva clave de cifrado en este momento y aplicarla a todos los futuros datos almacenados en el repositorio, seleccione **Cifrar datos mediante un cifrado basado en el Core con una clave nueva** y, a continuación, introduzca información sobre la clave como se describe en la siguiente tabla:

Tabla 60. Definir nueva clave de cifrado

Cuadro de texto	Descripción
Nombre	Escriba un nombre para la clave de cifrado. Los nombres de las claves de cifrado contienen entre 1 y 64 caracteres alfanuméricos. No utilice caracteres no permitidos o frases no permitidas.

Cuadro de texto	Descripción
Descripción	Escriba un comentario descriptivo para la clave de cifrado. Esta información aparece en el campo Descripción cuando al visualizar una lista de claves de cifrado en la Rapid Recovery Core Console. Las descripciones pueden contener hasta 254 caracteres. La práctica recomendada es evitar el uso de caracteres no permitidos y frases no permitidas.
Frase de contraseña	Introduzca una frase de contraseña usada para controlar el acceso. La práctica recomendada es evitar el uso de caracteres no permitidos. Registre la frase de contraseña en lugar seguro. Asistencia para la protección de datos de Quest no puede recuperar frases de contraseña. Una vez cree una clave de cifrado y la aplique a uno o más equipos protegidos no podrá recuperar los datos si pierde la frase de contraseña.
Confirmar la frase de contraseña	Como confirmación, vuelva a escribir la Frase de contraseña. Se utiliza para confirmar la entrada de frase de contraseña.

23. De manera opcional, en la página **Cifrado**, si desea cifrar todos los datos de transporte a través de una red, seleccione **Cifrar los datos de transporte a través de una red**. Esta opción está habilitada de manera predeterminada. Si no desea cifrar los datos de esta manera, desactive esta opción.
24. Haga clic en **Finalizar** para guardar y aplicar sus ajustes.

    La primera vez que se agrega protección para una máquina, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

El software Rapid Recovery Agent se implementa en los equipos especificados y, si es necesario, se añaden los equipos a la protección en el Core.

Proteger máquinas virtuales vCenter/ESXi mediante la protección sin agentes

Lleve a cabo el siguiente procedimiento para proteger máquinas virtuales ESXi sin agentes.

NOTE: Rapid Recovery recomienda que se instalen las herramientas de VMware en las máquinas virtuales (VM) que quiere proteger en los hosts vSphere o ESXi. Cuando las herramientas de VMware se instalan en una máquina virtual mediante el sistema operativo Windows (SO), las copias de seguridad que recupera el Rapid Recovery Core utilizan Microsoft Volume Shadow Services (VSS) (Servicios de instantáneas de volumen de Microsoft). Para obtener más información sobre el comportamiento de las VM sin agentes, con o sin herramientas de VMware, consulte Beneficios de instalar herramientas de hipervisor para la protección sin agentes.

CAUTION: Quest **recomienda que limite la protección sin agentes a no más de 200 máquinas virtuales a la vez. Por ejemplo, no seleccione más de 200 VM mientras utiliza el Asistente para proteger varios equipos. La protección de más de 200 VM puede dar lugar a un rendimiento más lento. No existe un límite de VM que un Core pueda proteger sin agentes a lo largo del tiempo. Por ejemplo, hoy podría proteger 200 VM y mañana 200 más.**

1. En la Rapid Recovery Core Console, haga clic en el menú desplegable **Proteger** y, a continuación, haga clic en **Proteger varios equipos**.

Se abre el Asistente para proteger varios equipos.

2. En la página de **bienvenida**, seleccione una de las opciones siguientes:
   - Típicas
   - Avanzado (mostrar pasos opcionales)
3. Haga clic en **Siguiente**.
4. En la página **Conexión** del asistente, en la lista desplegable **Origen**, seleccione **vCenter/ESX(i)**.
5. Introduzca la información de host y las credenciales de inicio de sesión según se describe en la tabla siguiente.

Tabla 61. Configuración de conexión vCenter/ESX(i)

Cuadro de texto	Descripción
Host	Nombre o dirección IP del host virtual.
Puerto	Número de puerto usado para conectar con el host virtual. El valor predeterminado es 443.
Nombre de usuario	El nombre de usuario utilizado para conectarse con el host virtual; por ejemplo, Administrator o, si el equipo se encuentra en un dominio, [nombre de dominio]\Administrator.
Contraseña	La contraseña segura que se utiliza para conectarse con este host virtual.

6. Asegúrese de que la opción **Proteger VM seleccionadas sin agentes** está seleccionada. (Esta opción se selecciona de forma predeterminada).
7. En la página **Seleccionar equipos**, realice una de las acciones siguientes:
   - En la lista de VM, seleccione las VM que desea proteger.
   - Para desplazarse por la estructura de árbol para encontrar más máquinas virtuales, haga clic en **Ver árbol** y seleccione **Hosts y clústeres** o **VM y plantillas**. Seleccione las VM que desea proteger.
8. Si desea proteger automáticamente las VM nuevas cuando se añaden al host, seleccione **Proteger equipos nuevos automáticamente** y, a continuación, haga clic en **Siguiente**.

   NOTE: El seguimiento de bloqueo cambiado (CBT) de VMware debe estar habilitado en cada una de las VM que desee proteger. Si el CBT no está activado, Rapid Recovery lo activa automáticamente para garantizar la protección.

   a. En la página **Protección automática**, seleccione el contenedor en el que desea que se añadan los nuevos equipos.
9. Haga clic en **Siguiente**.

   Si a continuación aparece la página **Protección** en el Asistente para proteger varios equipos, vaya al paso 12.

   Si el software Agent todavía no se ha implementado en los equipos que desee proteger o si alguno de los equipos que especificó no puede protegerse por cualquier otro motivo, los equipos seleccionados aparecerán en la página **Advertencias**.
10. Opcionalmente, en la página **Advertencias**, puede verificar cualquier equipo seleccionando el equipo y, a continuación, haciendo clic en **Verificar** en la barra de herramientas.
11. Haga clic en **Siguiente**.

Aparece **Protección**.

12. Seleccione la configuración de programación para protección adecuada tal como se describe a continuación:

    - Para utilizar la programación para protección predeterminada, en la opción Configuración de programación, seleccione **Protección predeterminada (instantáneas de todos los volúmenes cada hora)**.

    Con un calendario de programación de protección predeterminado, el Core tomará instantáneas de todos los volúmenes del equipo protegido una vez cada hora. Para cambiar la configuración de protección en cualquier momento después de cerrar el asistente, incluida la selección de qué volúmenes proteger, vaya a la página **Resumen** del equipo protegido específico.

    - Para definir un calendario de programación de protección diferente, en la opción Configuración de calendario de programación, seleccione **Protección personalizada**.

13. Continúe con su configuración del modo siguiente:

    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si existe un repositorio, haga clic en **Finalizar** para confirmar sus opciones, cierre el asistente y proteja el equipo que ha especificado.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si no existe un repositorio, haga clic en **Siguiente** y continúe en el paso 15 para crear un repositorio.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe con el siguiente paso para seleccionar qué volúmenes se van a proteger.
    - Si ha seleccionado una configuración avanzada para el Asistente para proteger un equipo, así como la protección predeterminada, haga clic en **Siguiente** y continúe en el paso 15 para ver las opciones de repositorio y cifrado.
    - Si ha seleccionado Configuración avanzada para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe en el siguiente paso para seleccionar qué volúmenes se van a proteger.

    La primera vez que se agrega protección a un equipo, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio del Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

14. En la página **Calendario de programación de protección**, defina un calendario de programación de protección personalizado y luego haga clic en **Siguiente**. Para obtener información detallada sobre cómo definir un calendario de programación de protección personalizado, consulte Creación de un programa de protección personalizado en el modo simple.

    Si ya ha configurado la información del repositorio y ha seleccionado Opciones avanzadas en el paso 1, aparece la página Cifrado. Continúe en el paso 18.

15. En la página **Repositorio**, realice los siguientes pasos:

    - Si ya tiene un repositorio y desea almacenar los datos de este equipo para la protección del repositorio existente, realice una de las acciones siguientes:

      1. Seleccione **Usar un repositorio existente**.
      2. Seleccione un repositorio existente de la lista.
      3. Haga clic en **Siguiente**.

      Se abrirá la página de **Cifrado**. Vaya al paso 18 para definir el cifrado de manera opcional.

    - Si desea crear un repositorio, en la página **Repositorio**, introduzca la información que se describe en la tabla siguiente y haga clic en **Siguiente** o **Finalizar** según corresponda.

Tabla 62. Configuración del repositorio

Cuadro de texto	Descripción
Nombre	Introduzca el nombre para mostrar del repositorio. De manera predeterminada, este cuadro de texto incluye el término Repositorio y un número, que se corresponde con el número de repositorios de este Core. Por ejemplo, si se trata del primer repositorio, el nombre predeterminado es Repositorio 1. Cambie el nombre según sea necesario. Los nombres del repositorio contienen entre 1 y 40 caracteres alfanuméricos, incluidos los espacios. No utilice caracteres prohibidos ni frases prohibidas.
Ubicación	Introduzca la ubicación para almacenar los datos protegidos. Este volumen debe ser la ubicación de almacenamiento principal. La ubicación puede ser local (una unidad en el equipo Core) o una unidad de red de uso compartido de CIFS. Si es de uso compartido de CIFS, la ruta debe comenzar por \\. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación. **CAUTION: Defina una carpeta específica en la raíz para la ubicación de almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice `E:\Repository\`, no `E:\`. Si el repositorio que está creando en este paso se elimina más adelante, se eliminarán todos los archivos en la ubicación de almacenamiento de su repositorio. Si define la ubicación de almacenamiento en la raíz, el resto de archivos del volumen (p. ej., `E:\`) se eliminan, lo que podría derivar en una pérdida grave de datos.** Por ejemplo, introduzca `X:\Repository\Data`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
Nombre de usuario	Introduzca un nombre de usuario para un usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.
Contraseña	Introduzca la contraseña para el usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.
Ruta de acceso a metadatos	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, introduzca `X:\Repository\Metadata`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.

16. En la página **Configuración del repositorio**, configure la cantidad de espacio en disco que desea asignar en el repositorio. Quest recomienda reservar un 20 % del volumen a los metadatos, que es el valor predeterminado. De manera opcional, utilizando el control deslizante o el campo **Tamaño**, puede asignar más o menos espacio de volumen para el repositorio.
17. De manera opcional, si desea visualizar e introducir información detallada acerca de la configuración de la ubicación de almacenamiento, seleccione **Mostrar opciones avanzadas** y ajuste la configuración como se describe en la siguiente tabla. Para ocultar estas opciones, desactive la opción **Mostrar opciones**

avanzadas. Cuando haya completado la configuración del repositorio, haga clic en **Siguiente** o en **Finalizar**, según proceda.

Tabla 63. Detalles de configuración de almacenamiento

Cuadro de texto	Descripción
Bytes por sector	Especifique el número de bytes que desea que incluya cada sector. El valor predeterminado es 512.
Bytes por registro	Especifique el promedio del número de bytes por registro. El valor predeterminado es 8192.
Política de almacenamiento en caché de escritura	La política de almacenamiento en caché de escritura controla cómo se utiliza el Administrador de caché de Windows en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: • Activado • Desactivado • Sincronización Si se establece como Activado, que es el valor predeterminado, Windows controla el almacenamiento en caché. Es adecuado para Windows 10 y para versiones de Windows Server 2012 y posteriores. **NOTE:** si se establece la política de escritura en caché en Activado, se mejora el rendimiento; no obstante, el valor recomendado es Desactivada. Si utiliza Windows Server 2008 R2 SP2, la configuración recomendada es Desactivado. Si se establece en Desactivado, Rapid Recovery controla el almacenamiento en caché. Si se establece en Sincronización, Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.

Si ha seleccionado la opción **Avanzada** en el paso 1, aparece la página **Cifrado**.

18. De manera opcional, en la página **Cifrado**, si desea utilizar claves de cifrado para los datos almacenados en el repositorio, seleccione **Cifrar los datos en reposo en un repositorio** y, a continuación, realice una de las acciones siguientes:
    - Para seleccionar una clave de cifrado existente y aplicarla a todos los nuevos datos almacenados en el repositorio, seleccione **Cifrar los datos utilizando un cifrado basado en Core con una clave existente**, y, en el menú desplegable **Seleccionar clave de cifrado** seleccione la clave de cifrado.
    - Para definir una nueva clave de cifrado en este momento y aplicarla a todos los futuros datos almacenados en el repositorio, seleccione **Cifrar datos mediante un cifrado basado en el Core con una clave nueva** y, a continuación, introduzca información sobre la clave como se describe en la siguiente tabla:

Tabla 64. Definir nueva clave de cifrado

Cuadro de texto	Descripción
Nombre	Escriba un nombre para la clave de cifrado. Los nombres de las claves de cifrado contienen entre 1 y 64 caracteres alfanuméricos. No utilice caracteres no permitidos o frases no permitidas.

Cuadro de texto	Descripción
Descripción	Escriba un comentario descriptivo para la clave de cifrado. Esta información aparece en el campo Descripción cuando al visualizar una lista de claves de cifrado en la Rapid Recovery Core Console. Las descripciones pueden contener hasta 254 caracteres. La práctica recomendada es evitar el uso de caracteres no permitidos y frases no permitidas.
Frase de contraseña	Introduzca una frase de contraseña usada para controlar el acceso. La práctica recomendada es evitar el uso de caracteres no permitidos. Registre la frase de contraseña en lugar seguro. Asistencia para la protección de datos de Quest no puede recuperar frases de contraseña. Una vez cree una clave de cifrado y la aplique a uno o más equipos protegidos no podrá recuperar los datos si pierde la frase de contraseña.
Confirmar la frase de contraseña	Como confirmación, vuelva a escribir la Frase de contraseña. Se utiliza para confirmar la entrada de frase de contraseña.

19. De manera opcional, en la página **Cifrado**, si desea cifrar todos los datos de transporte a través de una red, seleccione **Cifrar los datos de transporte a través de una red**. Esta opción está habilitada de manera predeterminada. Si no desea cifrar los datos de esta manera, desactive esta opción.
20. Haga clic en **Finalizar** para guardar y aplicar sus ajustes.

    La primera vez que se agrega protección para una máquina, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

Protección de varios equipos en un host virtual Hyper-V

Utilice este procedimiento para proteger simultáneamente uno o más equipos de un host virtual Hyper-V.

> **CAUTION: Si utiliza la protección sin agentes, Quest recomienda limitar la protección a no más de 200 máquinas virtuales a la vez. Por ejemplo, no seleccione más de 200 VM mientras utiliza el Asistente para proteger varios equipos. La protección de más de 200 VM puede dar lugar a un rendimiento más lento. No existe un límite de VM que un Core pueda proteger sin agentes a lo largo del tiempo. Por ejemplo, hoy podría proteger 200 VM y mañana 200 más.**

1. En la Rapid Recovery Core Console, haga clic en el menú desplegable **Proteger** y, a continuación, haga clic en **Proteger varios equipos**.

Se abre el Asistente para proteger varios equipos.

2. En la página de bienvenida, seleccione una de las opciones siguientes:
   - Típicas
   - Avanzado (mostrar pasos opcionales)
3. Haga clic en **Siguiente**.
4. En la página **Conexión** del asistente, en la lista desplegable **Origen**, seleccione una de las siguientes opciones:
   - Servidor Hyper-V
   - Clúster Hyper-V
5. Introduzca la información de host y las credenciales de inicio de sesión según se describe en la tabla siguiente.

Tabla 65. Configuración de la conexión Hyper-V

Cuadro de texto	Descripción
Host	Nombre o dirección IP del host virtual.
Puerto	Número de puerto usado para conectar con el host virtual. El valor predeterminado es 8006.
Nombre de usuario	El nombre de usuario utilizado para conectarse con el host virtual; por ejemplo, Administrator o, si el equipo se encuentra en un dominio, [nombre de dominio]\Administrator.
Contraseña	La contraseña segura que se utiliza para conectarse con este host virtual.

6. De manera opcional, si desea utilizar protección sin agentes, seleccione **Proteger el servidor Hyper-V sin necesidad un Agent en las VM invitadas**, y, a continuación, consulte Proteger máquinas virtuales Hyper-V mediante la protección sin agentes.
7. Haga clic en **Siguiente**.
8. En la página **Equipos**, seleccione las VM que desea proteger.
9. De forma opcional, si desea proteger automáticamente nuevas máquinas virtuales cuando se agreguen al host, seleccione **Proteger automáticamente nuevas máquinas virtuales**.
10. Haga clic en **Siguiente**.
11. En la página **Ajustes**, escriba las credenciales de cada equipo con el siguiente formato: `hostname::username::password`.

    NOTE: Introduzca un equipo por línea.
12. Haga clic en **Siguiente**.

    Si a continuación aparece la página **Protección** en el Asistente para proteger varios equipos, vaya al paso 15.

    Si el software Agent está presente en los equipos que desea proteger o los equipos que especificó no pueden protegerse por cualquier otro motivo, los equipos seleccionados aparecerán en la página **Advertencias**.
13. Opcionalmente, en la página **Advertencias**, puede verificar cualquier equipo seleccionando el equipo y, a continuación, haciendo clic en **Verificar** en la barra de herramientas.
14. Opcionalmente, en la página **Advertencias**, seleccione **Tras la instalación de Agent, reinicie los equipos automáticamente**.

NOTE: Quest recomienda esta opción. Debe reiniciar los equipos Agent antes de poder protegerlas.

15. Si el estado indica que puede llegarse al equipo, haga clic en **Siguiente** para instalar el software Agent.

    Aparecerá la página **Protección**.

16. De manera opcional, en la página **Protección**, si quiere que aparezca un nombre distinto a la dirección IP en la Rapid Recovery Core Console de este equipo protegido, en el campo **Nombre para mostrar**, escriba un nombre en el cuadro de diálogo.

    Puede introducir hasta 64 caracteres. No utilice los caracteres especiales descritos en el tema . Tampoco el nombre para mostrar debe comenzar por cualquiera de las combinaciones de caracteres descritas en el tema .

17. Seleccione la configuración de programación para protección adecuada tal como se describe a continuación:

    - Para utilizar la programación para protección predeterminada, en la opción Configuración de programación, seleccione **Protección predeterminada (instantáneas de todos los volúmenes cada hora)**.

    Con un calendario de programación de protección predeterminado, el Core tomará instantáneas de todos los volúmenes del equipo protegido una vez cada hora. Para cambiar la configuración de protección en cualquier momento después de cerrar el asistente, incluida la selección de qué volúmenes proteger, vaya a la página **Resumen** del equipo protegido específico.

    - Para definir un calendario de programación de protección diferente, en la opción Configuración de calendario de programación, seleccione **Protección personalizada**.

18. Continúe con su configuración del modo siguiente:

    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si existe un repositorio, haga clic en **Finalizar** para confirmar sus opciones, cierre el asistente y proteja el equipo que ha especificado.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si no existe un repositorio, haga clic en **Siguiente** y continúe en el paso 20 para crear un repositorio.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe con el siguiente paso para seleccionar qué volúmenes se van a proteger.
    - Si ha seleccionado una configuración avanzada para el Asistente para proteger un equipo, así como la protección predeterminada, haga clic en **Siguiente** y continúe en el paso 20 para ver las opciones de repositorio y cifrado.
    - Si ha seleccionado Configuración avanzada para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe en el siguiente paso para seleccionar qué volúmenes se van a proteger.

    La primera vez que se agrega protección a un equipo, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio del Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

19. En la página **Volúmenes de protección**, seleccione los volúmenes que desea proteger. Si se indican volúmenes que no quiera incluir en la protección, haga clic en la columna Comprobar para borrar la selección. A continuación, haga clic en **Siguiente**.

    NOTE: Por lo general, es recomendable proteger, como mínimo, el volumen reservado para el sistema y el volumen con el sistema operativo (normalmente la unidad C).

20. En la página **Calendario de programación de protección**, defina un calendario de programación de protección personalizado y luego haga clic en **Siguiente**. Para obtener información detallada sobre cómo definir un calendario de programación de protección personalizado, consulte Creación de un programa de protección personalizado en el modo simple.

Si ya ha configurado la información del repositorio y ha seleccionado Opciones avanzadas en el paso 1, aparece la página Cifrado. Continúe en el paso 23.

21. En la página **Repositorio**, realice los siguientes pasos:

    - Si ya tiene un repositorio y desea almacenar los datos de este equipo para la protección del repositorio existente, realice una de las acciones siguientes:

      1. Seleccione **Usar un repositorio existente**.
      2. Seleccione un repositorio existente de la lista.
      3. Haga clic en **Siguiente**.

      Se abrirá la página de **Cifrado**. Vaya al paso 23 para definir el cifrado de manera opcional.

    - Si desea crear un repositorio, en la página **Repositorio**, introduzca la información que se describe en la tabla siguiente y haga clic en **Siguiente** o **Finalizar** según corresponda.

Tabla 66. Configuración del repositorio

Cuadro de texto	Descripción
Nombre	Introduzca el nombre para mostrar del repositorio. De manera predeterminada, este cuadro de texto incluye el término Repositorio y un número, que se corresponde con el número de repositorios de este Core. Por ejemplo, si se trata del primer repositorio, el nombre predeterminado es Repositorio 1. Cambie el nombre según sea necesario. Los nombres del repositorio contienen entre 1 y 40 caracteres alfanuméricos, incluidos los espacios. No utilice caracteres prohibidos ni frases prohibidas.
Ubicación	Introduzca la ubicación para almacenar los datos protegidos. Este volumen debe ser la ubicación de almacenamiento principal. La ubicación puede ser local (una unidad en el equipo Core) o una unidad de red de uso compartido de CIFS. Si es de uso compartido de CIFS, la ruta debe comenzar por \\. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación. **CAUTION: Defina una carpeta específica en la raíz para la ubicación de almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice `E:\Repository\`, no `E:\`. Si el repositorio que está creando en este paso se elimina más adelante, se eliminarán todos los archivos en la ubicación de almacenamiento de su repositorio. Si define la ubicación de almacenamiento en la raíz, el resto de archivos del volumen (p. ej., `E:\`) se eliminan, lo que podría derivar en una pérdida grave de datos.** Por ejemplo, introduzca `X:\Repository\Data`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
Nombre de usuario	Introduzca un nombre de usuario para un usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.
Contraseña	Introduzca la contraseña para el usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.

Cuadro de texto	Descripción
Ruta de acceso a metadatos	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, introduzca `X:\Repository\Metadata`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.

22. En la página **Configuración del repositorio**, configure la cantidad de espacio en disco que desea asignar en el repositorio. Quest recomienda reservar un 20 % del volumen a los metadatos, que es el valor predeterminado. De manera opcional, utilizando el control deslizante o el campo **Tamaño**, puede asignar más o menos espacio de volumen para el repositorio.
23. De manera opcional, si desea visualizar e introducir información detallada acerca de la configuración de la ubicación de almacenamiento, seleccione **Mostrar opciones avanzadas** y ajuste la configuración como se describe en la siguiente tabla. Para ocultar estas opciones, desactive la opción **Mostrar opciones avanzadas**. Cuando haya completado la configuración del repositorio, haga clic en **Siguiente** o en **Finalizar**, según proceda.

Tabla 67. Detalles de configuración de almacenamiento

Cuadro de texto	Descripción
Bytes por sector	Especifique el número de bytes que desea que incluya cada sector. El valor predeterminado es 512.
Bytes por registro	Especifique el promedio del número de bytes por registro. El valor predeterminado es 8192.
Política de almacenamiento en caché de escritura	La política de almacenamiento en caché de escritura controla cómo se utiliza el Administrador de caché de Windows en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: • Activado • Desactivado • Sincronización Si se establece como Activado, que es el valor predeterminado, Windows controla el almacenamiento en caché. Es adecuado para Windows 10 y para versiones de Windows Server 2012 y posteriores. **NOTE:** si se establece la política de escritura en caché en Activado, se mejora el rendimiento; no obstante, el valor recomendado es Desactivada. Si utiliza Windows Server 2008 R2 SP2, la configuración recomendada es Desactivado. Si se establece en Desactivado, Rapid Recovery controla el almacenamiento en caché. Si se establece en Sincronización, Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.

Si ha seleccionado la opción **Avanzada** en el paso 1, aparece la página **Cifrado**.

24. De manera opcional, en la página **Cifrado**, si desea utilizar claves de cifrado para los datos almacenados en el repositorio, seleccione **Cifrar los datos en reposo en un repositorio** y, a continuación, realice una de las acciones siguientes:
    - Para seleccionar una clave de cifrado existente y aplicarla a todos los nuevos datos almacenados en el repositorio, seleccione **Cifrar los datos utilizando un cifrado basado en Core con una clave existente**, y, en el menú desplegable **Seleccionar clave de cifrado** seleccione la clave de cifrado.
    - Para definir una nueva clave de cifrado en este momento y aplicarla a todos los futuros datos almacenados en el repositorio, seleccione **Cifrar datos mediante un cifrado basado en el Core con una clave nueva** y, a continuación, introduzca información sobre la clave como se describe en la siguiente tabla:

Tabla 68. Definir nueva clave de cifrado

Cuadro de texto	Descripción
Nombre	Escriba un nombre para la clave de cifrado. Los nombres de las claves de cifrado contienen entre 1 y 64 caracteres alfanuméricos. No utilice caracteres no permitidos o frases no permitidas.
Descripción	Escriba un comentario descriptivo para la clave de cifrado. Esta información aparece en el campo Descripción cuando al visualizar una lista de claves de cifrado en la Rapid Recovery Core Console. Las descripciones pueden contener hasta 254 caracteres. La práctica recomendada es evitar el uso de caracteres no permitidos y frases no permitidas.
Frase de contraseña	Introduzca una frase de contraseña usada para controlar el acceso. La práctica recomendada es evitar el uso de caracteres no permitidos. Registre la frase de contraseña en lugar seguro. Asistencia para la protección de datos de Quest no puede recuperar frases de contraseña. Una vez cree una clave de cifrado y la aplique a uno o más equipos protegidos no podrá recuperar los datos si pierde la frase de contraseña.
Confirmar la frase de contraseña	Como confirmación, vuelva a escribir la Frase de contraseña. Se utiliza para confirmar la entrada de frase de contraseña.

25. De manera opcional, en la página **Cifrado**, si desea cifrar todos los datos de transporte a través de una red, seleccione **Cifrar los datos de transporte a través de una red**. Esta opción está habilitada de manera predeterminada. Si no desea cifrar los datos de esta manera, desactive esta opción.
26. Haga clic en **Finalizar** para guardar y aplicar sus ajustes.

    La primera vez que se agrega protección para una máquina, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

El software Rapid Recovery Agent se implementa en los equipos especificados y, si es necesario, se añaden los equipos a la protección en el Core.

Proteger máquinas virtuales Hyper-V mediante la protección sin agentes

La función Rapid Snap for Virtual permite proteger máquinas virtuales Hyper-V o clústeres sin agentes instalando el Rapid Recovery Agent solo en el host Hyper-V en lugar de en cada máquina virtual (VM).

CAUTION: Quest recomienda que limite la protección sin agentes a no más de 200 máquinas virtuales a la vez. Por ejemplo, no seleccione más de 200 VM mientras utiliza el Asistente para proteger varios equipos. La protección de más de 200 VM puede dar lugar a un rendimiento más lento. No existe un límite de VM que un Core pueda proteger sin agentes a lo largo del tiempo. Por ejemplo, hoy podría proteger 200 VM y mañana 200 más.

1. En la Rapid Recovery Core Console, haga clic en el menú desplegable **Proteger** y, a continuación, haga clic en **Proteger varios equipos**.

   Se abre el Asistente para proteger varios equipos.
2. En la página de **bienvenida**, seleccione una de las opciones siguientes:
   - Típicas
   - Avanzado (mostrar pasos opcionales)
3. Haga clic en **Siguiente**.
4. En la página **Conexión** del asistente, en la lista desplegable **Origen**, seleccione una de las siguientes opciones:
   - Servidor Hyper-V
   - Clúster Hyper-V
5. Introduzca la información de host y las credenciales de inicio de sesión según se describe en la tabla siguiente.

Tabla 69. Configuración de la conexión Hyper-V

Cuadro de texto	Descripción
Host	Nombre o dirección IP del host virtual.
Puerto	Número de puerto usado para conectar con el host virtual. El valor predeterminado es 8006.
Nombre de usuario	El nombre de usuario utilizado para conectarse con el host virtual; por ejemplo, Administrator o, si el equipo se encuentra en un dominio, [nombre de dominio]\Administrator.
Contraseña	La contraseña segura que se utiliza para conectarse con este host virtual.

6. Asegúrese de que la opción **Proteger el servidor Hyper-V sin necesidad de un Agent en las VM invitadas** o **Proteger el clúster Hyper-V sin necesidad de un Agent en las máquinas virtuales**

invitadas, según su elección en el paso 4, está seleccionada. (Esta opción se selecciona de forma predeterminada).

7. Haga clic en **Siguiente**.
8. En la página **Seleccionar equipos**, seleccione las VM que desea proteger.
9. De forma opcional, si desea proteger automáticamente nuevas máquinas virtuales cuando se agreguen al host, seleccione **Proteger automáticamente nuevas máquinas virtuales**.
10. Haga clic en **Siguiente**.
11. De manera opcional, en la página **Protección**, si quiere que aparezca un nombre distinto a la dirección IP en la Rapid Recovery Core Console de este equipo protegido, en el campo **Nombre para mostrar**, escriba un nombre en el cuadro de diálogo.

    Puede introducir hasta 64 caracteres. No utilice los caracteres especiales descritos en el tema caracteres prohibidos. Tampoco el nombre para mostrar debe comenzar por cualquiera de las combinaciones de caracteres descritas en el tema frases prohibidas.

12. Seleccione la configuración de programación para protección adecuada tal como se describe a continuación:

    - Para utilizar la programación para protección predeterminada, en la opción Configuración de programación, seleccione **Protección predeterminada (instantáneas de todos los volúmenes cada hora)**.

    Con un calendario de programación de protección predeterminado, el Core tomará instantáneas de todos los volúmenes del equipo protegido una vez cada hora. Para cambiar la configuración de protección en cualquier momento después de cerrar el asistente, incluida la selección de qué volúmenes proteger, vaya a la página **Resumen** del equipo protegido específico.

    - Para definir un calendario de programación de protección diferente, en la opción Configuración de calendario de programación, seleccione **Protección personalizada**.

13. Continúe con su configuración del modo siguiente:

    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si existe un repositorio, haga clic en **Finalizar** para confirmar sus opciones, cierre el asistente y proteja el equipo que ha especificado.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si no existe un repositorio, haga clic en **Siguiente** y continúe en el paso 16 para crear un repositorio.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe con el siguiente paso para seleccionar qué volúmenes se van a proteger.
    - Si ha seleccionado una configuración avanzada para el Asistente para proteger un equipo, así como la protección predeterminada, haga clic en **Siguiente** y continúe en el paso 16 para ver las opciones de repositorio y cifrado.
    - Si ha seleccionado Configuración avanzada para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe en el siguiente paso para seleccionar qué volúmenes se van a proteger.

    La primera vez que se agrega protección a un equipo, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio del Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

14. En la página **Volúmenes de protección**, seleccione los volúmenes que desea proteger. Si se indican volúmenes que no quiera incluir en la protección, haga clic en la columna Comprobar para borrar la selección. A continuación, haga clic en **Siguiente**.

    NOTE: Por lo general, es recomendable proteger, como mínimo, el volumen reservado para el sistema y el volumen con el sistema operativo (normalmente la unidad C).

15. En la página **Calendario de programación de protección**, defina un calendario de programación de protección personalizado y luego haga clic en **Siguiente**. Para obtener información detallada sobre cómo

definir un calendario de programación de protección personalizado, consulte Creación de un programa de protección personalizado en el modo simple.

Si ya ha configurado la información del repositorio y ha seleccionado Opciones avanzadas en el paso 1, aparece la página Cifrado. Continúe en el paso 19.

16. En la página **Repositorio**, realice los siguientes pasos:

- Si ya tiene un repositorio y desea almacenar los datos de este equipo para la protección del repositorio existente, realice una de las acciones siguientes:

  1. Seleccione **Usar un repositorio existente**.
  2. Seleccione un repositorio existente de la lista.
  3. Haga clic en **Siguiente**.

  Se abrirá la página de **Cifrado**. Vaya al paso 19 para definir el cifrado de manera opcional.

- Si desea crear un repositorio, en la página **Repositorio**, introduzca la información que se describe en la tabla siguiente y haga clic en **Siguiente** o **Finalizar** según corresponda.

Tabla 70. Configuración del repositorio

Cuadro de texto	Descripción
Nombre	Introduzca el nombre para mostrar del repositorio. De manera predeterminada, este cuadro de texto incluye el término Repositorio y un número, que se corresponde con el número de repositorios de este Core. Por ejemplo, si se trata del primer repositorio, el nombre predeterminado es Repositorio 1. Cambie el nombre según sea necesario. Los nombres del repositorio contienen entre 1 y 40 caracteres alfanuméricos, incluidos los espacios. No utilice caracteres prohibidos ni frases prohibidas.
Ubicación	Introduzca la ubicación para almacenar los datos protegidos. Este volumen debe ser la ubicación de almacenamiento principal. La ubicación puede ser local (una unidad en el equipo Core) o una unidad de red de uso compartido de CIFS. Si es de uso compartido de CIFS, la ruta debe comenzar por \\. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación. **CAUTION: Defina una carpeta específica en la raíz para la ubicación de almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice `E:\Repository\`, no `E:\`. Si el repositorio que está creando en este paso se elimina más adelante, se eliminarán todos los archivos en la ubicación de almacenamiento de su repositorio. Si define la ubicación de almacenamiento en la raíz, el resto de archivos del volumen (p. ej., `E:\`) se eliminan, lo que podría derivar en una pérdida grave de datos.** Por ejemplo, introduzca `X:\Repository\Data`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
Nombre de usuario	Introduzca un nombre de usuario para un usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.

Cuadro de texto	Descripción
Contraseña	Introduzca la contraseña para el usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.
Ruta de acceso a metadatos	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, introduzca `X:\Repository\Metadata`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.

17. En la página **Configuración del repositorio**, configure la cantidad de espacio en disco que desea asignar en el repositorio. Quest recomienda reservar un 20 % del volumen a los metadatos, que es el valor predeterminado. De manera opcional, utilizando el control deslizante o el campo **Tamaño**, puede asignar más o menos espacio de volumen para el repositorio.
18. De manera opcional, si desea visualizar e introducir información detallada acerca de la configuración de la ubicación de almacenamiento, seleccione **Mostrar opciones avanzadas** y ajuste la configuración como se describe en la siguiente tabla. Para ocultar estas opciones, desactive la opción **Mostrar opciones avanzadas**. Cuando haya completado la configuración del repositorio, haga clic en **Siguiente** o en **Finalizar**, según proceda.

Tabla 71. Detalles de configuración de almacenamiento

Cuadro de texto	Descripción
Bytes por sector	Especifique el número de bytes que desea que incluya cada sector. El valor predeterminado es 512.
Bytes por registro	Especifique el promedio del número de bytes por registro. El valor predeterminado es 8192.
Política de almacenamiento en caché de escritura	La política de almacenamiento en caché de escritura controla cómo se utiliza el Administrador de caché de Windows en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: • Activado • Desactivado • Sincronización Si se establece como Activado, que es el valor predeterminado, Windows controla el almacenamiento en caché. Es adecuado para Windows 10 y para versiones de Windows Server 2012 y posteriores. **NOTE:** si se establece la política de escritura en caché en Activado, se mejora el rendimiento; no obstante, el valor recomendado es Desactivada. Si utiliza Windows Server 2008 R2 SP2, la configuración recomendada es Desactivado. Si se establece en Desactivado, Rapid Recovery controla el almacenamiento en caché. Si se establece en Sincronización, Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.

Si ha seleccionado la opción **Avanzada** en el paso 1, aparece la página **Cifrado**.

19. De manera opcional, en la página **Cifrado**, si desea utilizar claves de cifrado para los datos almacenados en el repositorio, seleccione **Cifrar los datos en reposo en un repositorio** y, a continuación, realice una de las acciones siguientes:
    - Para seleccionar una clave de cifrado existente y aplicarla a todos los nuevos datos almacenados en el repositorio, seleccione **Cifrar los datos utilizando un cifrado basado en Core con una clave existente**, y, en el menú desplegable **Seleccionar clave de cifrado** seleccione la clave de cifrado.
    - Para definir una nueva clave de cifrado en este momento y aplicarla a todos los futuros datos almacenados en el repositorio, seleccione **Cifrar datos mediante un cifrado basado en el Core con una clave nueva** y, a continuación, introduzca información sobre la clave como se describe en la siguiente tabla:

Tabla 72. Definir nueva clave de cifrado

Cuadro de texto	Descripción
Nombre	Escriba un nombre para la clave de cifrado. Los nombres de las claves de cifrado contienen entre 1 y 64 caracteres alfanuméricos. No utilice caracteres no permitidos o frases no permitidas.
Descripción	Escriba un comentario descriptivo para la clave de cifrado. Esta información aparece en el campo Descripción cuando al visualizar una lista de claves de cifrado en la Rapid Recovery Core Console. Las descripciones pueden contener hasta 254 caracteres. La práctica recomendada es evitar el uso de caracteres no permitidos y frases no permitidas.
Frase de contraseña	Introduzca una frase de contraseña usada para controlar el acceso. La práctica recomendada es evitar el uso de caracteres no permitidos. Registre la frase de contraseña en lugar seguro. Asistencia para la protección de datos de Quest no puede recuperar frases de contraseña. Una vez cree una clave de cifrado y la aplique a uno o más equipos protegidos no podrá recuperar los datos si pierde la frase de contraseña.
Confirmar la frase de contraseña	Como confirmación, vuelva a escribir la Frase de contraseña. Se utiliza para confirmar la entrada de frase de contraseña.

20. De manera opcional, en la página **Cifrado**, si desea cifrar todos los datos de transporte a través de una red, seleccione **Cifrar los datos de transporte a través de una red**. Esta opción está habilitada de manera predeterminada. Si no desea cifrar los datos de esta manera, desactive esta opción.
21. Haga clic en **Finalizar** para guardar y aplicar sus ajustes.

    La primera vez que se agrega protección para una máquina, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

Protección de varios equipos manualmente

Utilice este procedimiento para especificar manualmente los detalles de varios equipos que desee proteger simultáneamente mediante el software Agent. Los detalles identifican cada equipo en la red de forma exclusiva e incluyen información de la conexión y las credenciales. Este enfoque suele utilizarse cuando se protegen equipos

Linux. Sin embargo, utilizando este proceso, puede proteger solo equipos Windows, solo equipos Linux o una combinación de ambos.

1. En la Rapid Recovery Core Console, haga clic en el menú desplegable **Proteger** y, a continuación, haga clic en **Proteger varios equipos**.

   Se abre el Asistente para proteger varios equipos.
2. En la página de **bienvenida**, seleccione una de las opciones siguientes:

   - Típicas
   - Avanzado (mostrar pasos opcionales)
3. Haga clic en **Siguiente**.
4. En la página del asistente **Conexión**, de la lista desplegable **Origen**, seleccione **Manualmente**.
5. Haga clic en **Siguiente**.
6. En la página **Seleccionar equipos**, para cada equipo que desee proteger, introduzca los detalles del equipo en el cuadro de diálogo. Pulse **Intro** para separar la información de cada equipo que desee agregar. Utilice el formato `hostname::username::password::port`. La configuración de puertos es opcional. El puerto predeterminado para instalar Agent en equipos Windows o Linux es 8006. Los ejemplos incluyen:

   ```
   10.255.255.255::administrator::&11@yYz90z
   Linux-host-00-2::administrator::p@$$w0rD::8006
   ```
7. Haga clic en **Siguiente**.

   Si a continuación aparece la página **Protección** en el Asistente para proteger varios equipos, vaya al paso 11.

   Si el software Agent todavía no se ha implementado en los equipos que desee proteger o si alguno de los equipos que especificó no puede protegerse por cualquier otro motivo, los equipos seleccionados aparecerán en la página **Advertencias**.
8. Opcionalmente, en la página **Advertencias de equipos**, puede verificar cualquier equipo seleccionando el equipo y, a continuación, haciendo clic en **Verificar** en la barra de herramientas.
9. Opcionalmente, en la página **Advertencias de equipos**, seleccione **Tras la instalación de Agent, reinicie los equipos automáticamente**.

   NOTE: Quest recomienda esta opción. Debe reiniciar los equipos Agent antes de poder protegerlas. Reiniciarlos garantiza que el servicio de Agent esté en ejecución y que el módulo del kernel adecuado se utilice para proteger el equipo, si corresponde.
10. Si el estado indica que puede llegarse al equipo, haga clic en **Siguiente** para instalar el software Agent.

    Aparecerá la página **Protección**.
11. De manera opcional, en la página **Protección**, si quiere que aparezca un nombre distinto a la dirección IP en la Rapid Recovery Core Console de este equipo protegido, en el campo **Nombre para mostrar**, escriba un nombre en el cuadro de diálogo.

    Puede introducir hasta 64 caracteres. No utilice los caracteres especiales descritos en el tema . Tampoco el nombre para mostrar debe comenzar por cualquiera de las combinaciones de caracteres descritas en el tema .
12. Seleccione la configuración de programación para protección adecuada tal como se describe a continuación:

    - Para utilizar la programación para protección predeterminada, en la opción Configuración de programación, seleccione **Protección predeterminada (instantáneas de todos los volúmenes cada hora)**.

    Con un calendario de programación de protección predeterminado, el Core tomará instantáneas de todos los volúmenes del equipo protegido una vez cada hora. Para cambiar la configuración de protección en

cualquier momento después de cerrar el asistente, incluida la selección de qué volúmenes proteger, vaya a la página **Resumen** del equipo protegido específico.

- Para definir un calendario de programación de protección diferente, en la opción Configuración de calendario de programación, seleccione **Protección personalizada**.

13. Continúe con su configuración del modo siguiente:
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si existe un repositorio, haga clic en **Finalizar** para confirmar sus opciones, cierre el asistente y proteja el equipo que ha especificado.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, y si no existe un repositorio, haga clic en **Siguiente** y continúe en el paso 16 para crear un repositorio.
    - Si ha seleccionado la configuración Típica para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe con el siguiente paso para seleccionar qué volúmenes se van a proteger.
    - Si ha seleccionado una configuración avanzada para el Asistente para proteger un equipo, así como la protección predeterminada, haga clic en **Siguiente** y continúe en el paso 16 para ver las opciones de repositorio y cifrado.
    - Si ha seleccionado Configuración avanzada para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** y continúe en el siguiente paso para seleccionar qué volúmenes se van a proteger.

    La primera vez que se agrega protección a un equipo, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio del Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.
14. En la página **Volúmenes de protección**, seleccione los volúmenes que desea proteger. Si se indican volúmenes que no quiera incluir en la protección, haga clic en la columna Comprobar para borrar la selección. A continuación, haga clic en **Siguiente**.

    NOTE: Por lo general, es recomendable proteger, como mínimo, el volumen reservado para el sistema y el volumen con el sistema operativo (normalmente la unidad C).
15. En la página **Calendario de programación de protección**, defina un calendario de programación de protección personalizado y luego haga clic en **Siguiente**. Para obtener información detallada sobre cómo definir un calendario de programación de protección personalizado, consulte Creación de un programa de protección personalizado en el modo simple.

    Si ya ha configurado la información del repositorio y ha seleccionado Opciones avanzadas en el paso 1, aparece la página Cifrado. Continúe en el paso 19.
16. En la página **Repositorio**, realice los siguientes pasos:
    - Si ya tiene un repositorio y desea almacenar los datos de este equipo para la protección del repositorio existente, realice una de las acciones siguientes:
        1. Seleccione **Usar un repositorio existente**.
        2. Seleccione un repositorio existente de la lista.
        3. Haga clic en **Siguiente**.

        Se abrirá la página de **Cifrado**. Vaya al paso 19 para definir el cifrado de manera opcional.
    - Si desea crear un repositorio, en la página **Repositorio**, introduzca la información que se describe en la tabla siguiente y haga clic en **Siguiente** o **Finalizar** según corresponda.

Tabla 73. Configuración del repositorio

Cuadro de texto	Descripción
Nombre	Introduzca el nombre para mostrar del repositorio.

Cuadro de texto	Descripción
	De manera predeterminada, este cuadro de texto incluye el término Repositorio y un número, que se corresponde con el número de repositorios de este Core. Por ejemplo, si se trata del primer repositorio, el nombre predeterminado es Repositorio 1. Cambie el nombre según sea necesario. Los nombres del repositorio contienen entre 1 y 40 caracteres alfanuméricos, incluidos los espacios. No utilice caracteres prohibidos ni frases prohibidas.
Ubicación	Introduzca la ubicación para almacenar los datos protegidos. Este volumen debe ser la ubicación de almacenamiento principal. La ubicación puede ser local (una unidad en el equipo Core) o una unidad de red de uso compartido de CIFS. Si es de uso compartido de CIFS, la ruta debe comenzar por \\. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación. **CAUTION: Defina una carpeta específica en la raíz para la ubicación de almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice `E:\Repository\`, no `E:\`. Si el repositorio que está creando en este paso se elimina más adelante, se eliminarán todos los archivos en la ubicación de almacenamiento de su repositorio. Si define la ubicación de almacenamiento en la raíz, el resto de archivos del volumen (p. ej., `E:\`) se eliminan, lo que podría derivar en una pérdida grave de datos.** Por ejemplo, introduzca `X:\Repository\Data`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
Nombre de usuario	Introduzca un nombre de usuario para un usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.
Contraseña	Introduzca la contraseña para el usuario con acceso administrativo. Esta información solo es necesaria si la ubicación especificada del repositorio es una ruta de red.
Ruta de acceso a metadatos	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, introduzca `X:\Repository\Metadata`. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guion y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.

17. En la página **Configuración del repositorio**, configure la cantidad de espacio en disco que desea asignar en el repositorio. Quest recomienda reservar un 20 % del volumen a los metadatos, que es el valor predeterminado. De manera opcional, utilizando el control deslizante o el campo **Tamaño**, puede asignar más o menos espacio de volumen para el repositorio.
18. De manera opcional, si desea visualizar e introducir información detallada acerca de la configuración de la ubicación de almacenamiento, seleccione **Mostrar opciones avanzadas** y ajuste la configuración como se describe en la siguiente tabla. Para ocultar estas opciones, desactive la opción **Mostrar opciones avanzadas**. Cuando haya completado la configuración del repositorio, haga clic en **Siguiente** o en **Finalizar**, según proceda.

Tabla 74. Detalles de configuración de almacenamiento

Cuadro de texto	Descripción
Bytes por sector	Especifique el número de bytes que desea que incluya cada sector. El valor predeterminado es 512.
Bytes por registro	Especifique el promedio del número de bytes por registro. El valor predeterminado es 8192.
Política de almacenamiento en caché de escritura	La política de almacenamiento en caché de escritura controla cómo se utiliza el Administrador de caché de Windows en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: • Activado • Desactivado • Sincronización Si se establece como Activado, que es el valor predeterminado, Windows controla el almacenamiento en caché. Es adecuado para Windows 10 y para versiones de Windows Server 2012 y posteriores. **NOTE:** si se establece la política de escritura en caché en Activado, se mejora el rendimiento; no obstante, el valor recomendado es Desactivada. Si utiliza Windows Server 2008 R2 SP2, la configuración recomendada es Desactivado. Si se establece en Desactivado, Rapid Recovery controla el almacenamiento en caché. Si se establece en Sincronización, Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.

Si ha seleccionado la opción **Avanzada** en el paso 1, aparece la página **Cifrado**.

19. De manera opcional, en la página **Cifrado**, si desea utilizar claves de cifrado para los datos almacenados en el repositorio, seleccione **Cifrar los datos en reposo en un repositorio** y, a continuación, realice una de las acciones siguientes:
    - Para seleccionar una clave de cifrado existente y aplicarla a todos los nuevos datos almacenados en el repositorio, seleccione **Cifrar los datos utilizando un cifrado basado en Core con una clave existente**, y, en el menú desplegable **Seleccionar clave de cifrado** seleccione la clave de cifrado.
    - Para definir una nueva clave de cifrado en este momento y aplicarla a todos los futuros datos almacenados en el repositorio, seleccione **Cifrar datos mediante un cifrado basado en el Core con una clave nueva** y, a continuación, introduzca información sobre la clave como se describe en la siguiente tabla:

Tabla 75. Definir nueva clave de cifrado

Cuadro de texto	Descripción
Nombre	Escriba un nombre para la clave de cifrado. Los nombres de las claves de cifrado contienen entre 1 y 64 caracteres alfanuméricos. No utilice caracteres no permitidos o frases no permitidas.

Cuadro de texto	Descripción
Descripción	Escriba un comentario descriptivo para la clave de cifrado. Esta información aparece en el campo Descripción cuando al visualizar una lista de claves de cifrado en la Rapid Recovery Core Console. Las descripciones pueden contener hasta 254 caracteres. La práctica recomendada es evitar el uso de caracteres no permitidos y frases no permitidas.
Frase de contraseña	Introduzca una frase de contraseña usada para controlar el acceso. La práctica recomendada es evitar el uso de caracteres no permitidos. Registre la frase de contraseña en lugar seguro. Asistencia para la protección de datos de Quest no puede recuperar frases de contraseña. Una vez cree una clave de cifrado y la aplique a uno o más equipos protegidos no podrá recuperar los datos si pierde la frase de contraseña.
Confirmar la frase de contraseña	Como confirmación, vuelva a escribir la Frase de contraseña. Se utiliza para confirmar la entrada de frase de contraseña.

20. De manera opcional, en la página **Cifrado**, si desea cifrar todos los datos de transporte a través de una red, seleccione **Cifrar los datos de transporte a través de una red**. Esta opción está habilitada de manera predeterminada. Si no desea cifrar los datos de esta manera, desactive esta opción.
21. Haga clic en **Finalizar** para guardar y aplicar sus ajustes.

    La primera vez que se agrega protección para una máquina, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

El software Rapid Recovery Agent se implementa en los equipos especificados y, si es necesario, se añaden los equipos a la protección en el Core.

Supervisión de la protección de varios equipos

Puede supervisar el progreso a medida que Rapid Recovery aplica las políticas y calendarios de programación de protección a los equipos.

1. En la Rapid Recovery Core Console, navegue a la página Inicio de Rapid Recovery y, a continuación, haga clic en  (Eventos).

   Aparece la página **Eventos**, que se compone de los elementos Tareas, Alertas y Eventos. A medida que los volúmenes se transfieren, en el panel Tareas se muestra el estado y las horas de inicio y finalización.

   También puede filtrar tareas por estado (activas, en espera, completadas, en cola y fallidas). Para obtener más información, consulte Visualización de tareas.

   NOTE: Para ver únicamente las tareas que están a la espera de realizarse, asegúrese de seleccionar el icono Tareas en espera.

   A medida que se agrega cada equipo protegido, se registra una alerta, que indica si la operación ha sido correcta o si se han registrado errores. Para obtener más información, consulte Visualización de alertas.

   Para obtener información sobre cómo visualizar todos los eventos, consulte Visualización de un diario de todos los eventos registrados.

Activación de la asistencia de la aplicación

Después de que se haya puesto una máquina virtual bajo protección sin agentes, puede habilitar la asistencia de la aplicación de Exchange o SQL instalada en dicho equipo.

Antes de comenzar, se deben cumplir los siguientes requisitos previos.

- **Proteger la máquina virtual con Rapid Recovery Core.** La opción para habilitar la asistencia de la aplicación no está disponible durante el proceso de protección. El botón para habilitar esta función se muestra en varias páginas de la interfaz de usuario después de poner el equipo SQL o Exchange bajo protección. Para obtener más información, consulte Proteger máquinas virtuales vCenter/ESXi mediante la protección sin agentes o Proteger máquinas virtuales Hyper-V mediante la protección sin agentes.
- **Habilitar el acceso remoto de WMI.** Para permitir el acceso de WMI, debe instalar y configurar Administración remota de Windows en la máquina virtual (VM) de destino. Para obtener más información, consulte el artículo de Microsoft Knowledge Base en https://msdn.microsoft.com/en-us/library/aa384372(v=vs.85).aspx.
- **Conceder derechos administrativos de forma remota a los usuarios locales.** Configure LocalAccountTokenFilterPolicy ejecutando el siguiente símbolo del sistema administrativo:

  ```
  winrm quickconfig
  ```
- **Obtener la autorización de acceso del espacio de nombres raíz de WMI.** Para que el Core se conecte a las aplicaciones sin el Agent, la máquina virtual debe permitir el tráfico de red entrante en los puertos TCP 135 y 445, y a en los puertos 1024-1034 asignados de forma dinámica.
- **Permitir el acceso remoto a SQL Server y Exchange.** Este requisito previo varía en función de la aplicación en la que desee habilitar la asistencia.
  - **SQL:** Configure el Firewall de Windows abriendo los puertos 1433 y 1434.
  - **Exchange:** Abra los puertos TCP y UDP 389.
- **Integrar el invitado en el host.** La integración se lleva a cabo instalando el paquete de optimización específico para el hipervisor:
  - En las máquinas virtuales ESXi, utilice **VMware Tools,** herramientas necesarias para la protección de máquinas virtuales ESXi sin agentes.
  - En Hyper-V, utilice el paquete de **servicios de integración**, que viene preinstalado en la mayoría de los sistemas operativos Windows Server.

Complete los pasos siguientes para habilitar la asistencia de la aplicación en las máquinas virtuales protegidas sin agentes.

1. En la Core Console, vaya a la página **Equipos**.
2. Complete una de las siguientes acciones:
   - Para habilitar la asistencia de la aplicación en una única máquina virtual, haga clic en el menú **Acciones** de dicha máquina virtual y, a continuación, haga clic en **Habilitar la asistencia de la aplicación**.
   - Para habilitar la asistencia de la aplicación en varias máquinas virtuales de forma simultánea, seleccione las máquinas virtuales, haga clic en el menú desplegable **Asistencia de la aplicación** y, a continuación, haga clic en **Habilitar la asistencia de la aplicación**.
3. En el cuadro de diálogo **Editar la asistencia de la aplicación**, introduzca las credenciales de la máquina virtual.

Aparecerá un icono verde junto al nombre del equipo protegido en el que se ha habilitado la asistencia de la aplicación.

Si desea añadir las credenciales de la aplicación, puede hacerlo haciendo clic en **SQL** o **Exchange** en la parte superior de la página **Resumen** del equipo específico.

Configuración y funciones en servidores de Exchange protegidos

Si desea proteger un servidor Microsoft Exchange Server en su Core, puede configurar ajustes adicionales en la Rapid Recovery Core Console y realizar funciones adicionales.

Solo hay disponible un parámetro, **Habilitar comprobación de capacidad de montaje automático**, en la Core Console relacionada con Exchange Server. Si está activada, las comprobaciones de capacidad de montaje del Exchange Server se realizan automáticamente. Este parámetro está disponible cuando el estado del equipo protegido es verde (activo) o amarillo (en pausa).

Para obtener más información, consulte Acerca de las comprobaciones de capacidad de montaje de base de datos de Exchange.

También puede realizar una comprobación de la capacidad de montaje a petición, en el panel Puntos de recuperación de un equipo protegido del Exchange Server. Para obtener más información, consulte Forzado de una comprobación de capacidad de montaje de una base de datos de Exchange.

A continuación, se indican las funciones que puede realizar en un Exchange Server protegido por el Core.

- **Especificar credenciales de servidor Exchange**. El Rapid Recovery Core le permite establecer las credenciales para que el Core pueda autentificarse en el Exchange Server y obtener información.

  Para obtener más información acerca del establecimiento de credenciales para Exchange Servers, consulte Establecimiento de las credenciales para un equipo Exchange Server.

- **Truncar registros de Exchange**. Cuando fuerza el truncamiento de los registros del Exchange Server, este proceso identifica el espacio disponible y reclama espacio en el servidor protegido de Exchange.

  Para obtener más información acerca del truncamiento de los registros del Exchange Server a petición, consulte Forzado del truncamiento de registros para un equipo Exchange. Este proceso también puede llevarse a cabo como parte de los trabajos nocturnos.

- **Forzar una comprobación de la capacidad de montaje de una base de datos de Exchange**. Esta función comprueba que se puedan montar las bases de datos de Exchange, para detectar daños y alertar a los administradores para que todos los datos del servidor de Exchange se puedan recuperar correctamente.

  Para obtener más información acerca del forzado de una comprobación de la capacidad de montaje a petición, consulte Forzado de una comprobación de capacidad de montaje de una base de datos de Exchange.
  También puede forzar una comprobación de la capacidad de montaje para que se inicie automáticamente después de cada instantánea. Para obtener más información acerca de las comprobaciones de la capacidad de montaje, consulte Acerca de las comprobaciones de capacidad de montaje de base de datos de Exchange.

- **Forzar una comprobación de la suma de comprobación de puntos de recuperación de Exchange Server**. Esta función comprueba la integridad de los puntos de recuperación que contienen los archivos de la base de datos de Exchange.

  Para obtener más información acerca del forzado de una comprobación de la suma de comprobación a petición, consulte Forzado de comprobación de suma de comprobación de archivos de bases de datos de Exchange.

Puede truncar registros de Exchange y forzar una comprobación de la suma de comprobación como parte de los trabajos nocturnos. Para obtener más información acerca de las tareas que puede programar como trabajos nocturnos, consulte Comprensión de los trabajos nocturnos. Para obtener información sobre la configuración de trabajos nocturnos, consulte Configuración de trabajos nocturnos para el Core.

Establecimiento de las credenciales para un equipo Exchange Server

Para establecer las credenciales al iniciar sesión, debe haber un Exchange Server en un volumen protegido. Si Rapid Recovery no detecta la presencia de un Exchange Server, la función Establecer las credenciales no aparece en la Core Console.

Una vez que ha protegido datos en un servidor Microsoft Exchange, puede establecer credenciales de inicio de sesión en la Core Console de Rapid Recovery.

Complete los pasos de este procedimiento para definir las credenciales de cada Exchange Server.

1. En el área de navegación izquierda de la Core Console de Rapid Recovery, seleccione el equipo Exchange Server protegido para el que desea establecer las credenciales.

   La página **Resumen** se muestra en el Exchange Server protegido.

2. En la página **Resumen**, desde los vínculos de la parte superior de la página, haga clic en la flecha hacia abajo a la derecha del menú Exchange y, a continuación, en el menú desplegable resultante, seleccione **Establecer credenciales**.

   Aparece el cuadro de diálogo **Editar las credenciales de Exchange** para el Exchange Server.

3. En el cuadro de diálogo **Editar las credenciales de Exchange**, introduzca las credenciales, como se indica a continuación:
   a. En el campo de texto **Nombre de usuario**, introduzca el nombre de usuario de un usuario con permisos en el servidor de Exchange; por ejemplo, Administrador (o, si el equipo está en un dominio, [nombre de dominio]\Administrador).
   b. En el campo de texto **Contraseña**, introduzca la contraseña con el nombre que especificó para conectar con el Exchange Server.
   c. Haga clic en **Aceptar** para confirmar los ajustes y cerrar el cuadro de diálogo.

Forzado del truncamiento de registros para un equipo Exchange

Para forzar el truncamiento del log, debe haber una base de datos de Exchange en un volumen protegido. Si Rapid Recovery no detecta la presencia de una base de datos, la comprobación del truncamiento del log no aparece en la Consola de Core.

Cuando se fuerza un truncamiento del log para un servidor de Exchange protegido, el tamaño de los registros se reduce. Complete los pasos de este procedimiento para forzar el truncamiento del log bajo demanda.

1. En el área de navegación izquierda de la Core Console de Rapid Recovery, seleccione el servidor de Exchange protegido para el que desea forzar el truncamiento del log

   Aparece la página **Resumen** para el equipo protegido.

2. En la parte superior de la página, haga clic en el menú desplegable **Exchange** y seleccione **Forzar truncamiento del log**.
3. En el cuadro de diálogo resultante, haga clic para confirmar que desea forzar el truncamiento del log.

El cuadro de diálogo se cierra. El sistema empieza a truncar los registros de servidor de Exchange. Si las alertas del sistema están habilitadas para este tipo de evento, se muestra un mensaje que indica que empieza el proceso de truncamiento del log.

Acerca de las comprobaciones de capacidad de montaje de base de datos de Exchange

Cuando utiliceRapid Recovery para hacer copia de seguridad de archivos de servidores Microsoft Exchange, las comprobaciones de capacidad de montaje se pueden realizar en todas las bases de datos de Exchange tras cada instantánea. Esta función de detección de corrupción avisa a los administradores de posibles errores, y asegura que todos los datos en los servidores de Exchange se recuperarán correctamente en caso de error.

Para habilitar o deshabilitar esta función, vaya al menú **Configuración** del equipo protegido y establezca la opción **Habilitar comprobación de capacidad de montaje automática** en **Sí** o **No**, respectivamente. Para obtener más información acerca de la modificación de la configuración de un equipo protegido, consulte Visualización y modificación de la configuración de equipos protegidos.

Las comprobaciones de la capacidad de montaje no forman parte de la configuración nocturna. Sin embargo, si la comprobación de capacidad de montaje automática está habilitada, y si los trabajos nocturnos de Truncar registros de Exchange están habilitados, la comprobación de la capacidad de montaje se activa tras completar el truncamiento del registro.

También puede realizar una comprobación de la capacidad de montaje a petición, en el panel **Puntos de recuperación** de un equipo protegido del Exchange Server. Para obtener más información, consulte Forzado de una comprobación de capacidad de montaje de una base de datos de Exchange.

NOTE: Las comprobaciones de capacidad de montaje solo se aplican a Microsoft Exchange Server 2007, 2010, 2013 y 2016. Además, la cuenta de servicio de Rapid Recovery Agent debe estar asignada al rol Administrador organizativo en Exchange.

Forzado de una comprobación de capacidad de montaje de una base de datos de Exchange

Para forzar una comprobación de la capacidad de montaje, debe haber una base de datos de Exchange en un volumen protegido. Si Rapid Recovery no detecta la presencia de una base de datos, la función de comprobación de la capacidad de montaje no aparece en la Core Console.

Complete los pasos de este procedimiento para forzar que el sistema haga una comprobación de la capacidad de montaje para un punto de recuperación del servidor de Exchange a petición.

1. En el área de navegación izquierda de la Core Console de Rapid Recovery, seleccione el equipo Exchange Server protegido para el que quiere forzar la comprobación de la capacidad de montaje y, a continuación, haga clic en el menú **Puntos de recuperación**.
2. Desplácese hasta el panel **Puntos de recuperación**.
3. Navegue por los puntos de recuperación para encontrar el punto de recuperación en cuestión. De manera opcional, haga clic en la flecha ▸ a la derecha de un punto de recuperación de la lista para expandir la vista.

En la información del punto de recuperación expandido, puede ver los volúmenes incluidos en el punto de recuperación.

4. En el panel **Puntos de recuperación**, en la fila que represente el punto de recuperación correcto, haga clic en  y, en el menú desplegable, seleccione **Forzar comprobación de capacidad de montaje**.
5. En el cuadro de diálogo resultante, haga clic para confirmar que desea forzar la comprobación de la capacidad de montaje.

   El cuadro de diálogo se cierra. El sistema realiza la comprobación capacidad de montaje. Si las alertas del sistema están habilitadas para este tipo de evento, se muestra un mensaje que indica que empieza la comprobación de la capacidad de montaje.

Para obtener instrucciones sobre cómo ver el estado de la comprobación de la capacidad de montaje, consulte Visualización de eventos mediante las páginas de tareas, alertas y del diario.

Forzado de comprobación de suma de comprobación de archivos de bases de datos de Exchange

Para forzar una comprobación de suma de comprobación, debe haber una base de datos de Exchange en un volumen protegido. Si Rapid Recovery no detecta la presencia de una base de datos, la función de comprobación de suma de comprobación no aparece en la Core Console.

Complete los pasos de este procedimiento para forzar que el sistema haga una comprobación de suma de comprobación para un punto de recuperación del servidor de Exchange específico.

1. En el área de navegación izquierda de Core Console de Rapid Recovery, seleccione el servidor Exchange protegido para el que quiere forzar la comprobación de suma de comprobación y, a continuación, haga clic en el menú **Puntos de recuperación**.

   La página **Puntos de recuperación** se muestra en el servidor Exchange protegido.
2. Desplácese hasta el panel **Puntos de recuperación**.
3. Navegue por los puntos de recuperación para encontrar el punto de recuperación en cuestión. De manera opcional, haga clic en la flecha ▸ a la derecha de un punto de recuperación de la lista para expandir la vista.

   En la información del punto de recuperación expandido, puede ver los volúmenes incluidos en el punto de recuperación.
4. En el panel **Puntos de recuperación**, en la fila que represente el punto de recuperación correcto, haga clic en  y, en el menú desplegable, seleccione **Forzar comprobación de suma de comprobación**.
5. En el cuadro de diálogo resultante, haga clic para confirmar que desea forzar la comprobación de suma de comprobación.

   El cuadro de diálogo se cierra. El sistema realiza la comprobación de suma de comprobación. Si las alertas del sistema están habilitadas para este tipo de evento, se muestra un mensaje que indica que empieza la comprobación de suma de comprobación.

Para obtener instrucciones sobre cómo ver el estado de la comprobación de suma de comprobación, consulte Visualización de eventos mediante las páginas de tareas, alertas y del diario.

Configuración y funciones en servidores SQL Server protegidos

Si desea proteger un servidor Microsoft SQL Server en su Core, puede configurar parámetros adicionales en la Core Console de Rapid Recovery y realizar funciones adicionales.

Solo hay disponible un parámetro, **Conectabilidad**, en la Core Console relacionada con SQL Server.

El Core de Rapid Recovery le permite realizar una comprobación de conectabilidad de SQL para comprobar la integridad de los puntos de recuperación que contienen bases de datos de SQL. Esta acción comprueba la coherencia de bases de datos de SQL y garantiza que todos los archivos MDF (datos) y LDF (registro) compatibles están disponibles en la instantánea de copia de seguridad.

En versiones anteriores, las comprobaciones de conectabilidad de SQL requerían una versión con licencia de SQL Server en el equipo del Core. El Core de Rapid Recovery ahora ofrece la posibilidad de realizar las comprobaciones de conectabilidad de SQL desde una instancia de SQL Server en el Core o desde una versión con licencia en un equipo protegido de SQL Server.

Los parámetros de conectabilidad le permiten especificar qué versión con licencia de SQL Server se utiliza para llevar a cabo esta comprobación. Para obtener más información sobre la configuración de los parámetros de conectabilidad, consulte Administración de la configuración de conectabilidad de SQL del Core.

Para obtener más información sobre la conectabilidad de SQL, consulte Acerca de la conectabilidad de SQL.

A continuación, se indican las funciones que puede realizar en un servidor SQL protegido por el Core.

- **Especificar las credenciales de SQL Server.** El Rapid Recovery Core permite establecer las credenciales para que el Core pueda autentificarse en el SQL Server y obtener información. Puede establecer credenciales para un solo equipo protegido de SQL Server o establecer las credenciales predeterminadas para todos los servidores SQL Server protegidos.

  Para obtener más información acerca del establecimiento de credenciales para servidores de SQL, consulte Establecimiento de las credenciales para un equipo SQL Server.

- **Truncar registros de SQL.** Cuando fuerza el truncamiento de los registros del servidor de SQL, este proceso identifica el espacio disponible en el servidor protegido. Este proceso no reclama ningún espacio.

  Para obtener más información acerca del truncamiento de los registros de SQL Server a petición, consulte Forzado del truncamiento de registros para un equipo SQL.

- **Forzar una comprobación de conectabilidad de un servidor SQL**Server. Esta función comprueba la coherencia de bases de datos de SQL y garantiza que todos los archivos MDF (datos) y LDF (registro) compatibles están disponibles en la instantánea de copia de seguridad.

  Para obtener más información acerca del forzado de una comprobación de conectabilidad de servidores SQL Server a petición, consulte Forzado de una comprobación de conectabilidad de SQL Server.

Además de especificar las credenciales, cada una de las funciones descritas en la lista anterior pueden realizarse a petición, y también pueden configurarse para que se produzcan como parte de los trabajos nocturnos realizados para el Core. Para obtener más información acerca de las tareas que puede programar como trabajos nocturnos, consulte Comprensión de los trabajos nocturnos. Para obtener información sobre la configuración de trabajos nocturnos, consulte Configuración de trabajos nocturnos para el Core.

Establecimiento de las credenciales para un equipo SQL Server

Debe agregar el equipo SQL Server a la protección en el Core de Rapid Recovery antes de realizar este proceso. Para obtener más información sobre la protección de equipos, consulte Protección de un equipo.

Una vez proteja los datos en un equipo SQL Server de Microsoft, puede definir las credenciales de inicio de sesión para una única instancia o para todos los SQL Server, en la Core Console de Rapid Recovery.

Complete los pasos de este procedimiento para definir las credenciales de cada SQL Server.

1. En el área de navegación izquierda de la Core Console de Rapid Recovery, seleccione el equipo SQL Server protegido para el que desea establecer las credenciales.

   Aparece la página **Resumen** para el SQL Server protegido.
2. En la página **Resumen**, desde los vínculos de la parte superior de la página, haga clic en la flecha hacia abajo ▼ a la derecha del menú SQL y, a continuación, en el menú desplegable resultante, realice lo siguiente:

   - Si desea establecer credenciales para todas las instancias de bases de datos de SQL Server, haga clic en **Definir credenciales predeterminadas para todas las instancias** y, en el cuadro de diálogo **Editar credenciales predeterminadas**, haga lo siguiente:

     1. En el campo de texto **Nombre de usuario**, introduzca el nombre de usuario de un usuario con permisos para todos los servidores SQL asociados; por ejemplo, Administrador (o, si el equipo está en un dominio, [nombre de dominio]\Administrador).
     2. En el campo de texto **Contraseña**, introduzca la contraseña con el nombre que especificó para conectar con el SQL Server.
     3. Haga clic en **Aceptar** para confirmar los ajustes y cerrar el cuadro de diálogo.
   - Si desea definir unas credenciales para una única instancia de la base de datos de SQL Server, haga clic en el nombre de visualización del equipo SQL Server protegido y, a continuación, en el cuadro de diálogo **Editar credenciales de instancia**, haga lo siguiente:

     1. Seleccione el tipo de credencial (Predeterminada, Windows o SQL).
     2. En el campo de texto **Nombre de usuario**, introduzca el nombre de usuario de un usuario con permisos en el servidor SQL; por ejemplo, Administrador (o, si el equipo está en un dominio, [nombre de dominio]\Administrador).
     3. En el campo de texto **Contraseña**, introduzca la contraseña con el nombre que especificó para conectar con el SQL Server.
     4. Haga clic en **Aceptar** para confirmar los ajustes y cerrar el cuadro de diálogo.

Forzado del truncamiento de registros para un equipo SQL

El truncamiento de registros está disponible para equipos que usan SQL Server. Complete los pasos de este procedimiento para forzar el truncamiento del registro.

NOTE: Cuando se realiza para un equipo SQL, el truncamiento identifica el espacio libre en un disco, pero no reduce el tamaño de los registros.

1. En el área de navegación izquierda de la Core Console de Rapid Recovery, seleccione el equipo para el que desea forzar el truncamiento del registro.

Aparece la página **Resumen** para el equipo protegido.

2. Desde la página **Resumen** (o desde cualquier página de este equipo protegido), en la parte superior de la página, haga clic en el menú desplegable **SQL** y seleccione **Forzar truncamiento del registro**.
3. Haga clic en **Sí** para confirmar que desea forzar el truncamiento del registro.

Acerca de la conectabilidad de SQL

La función de conectabilidad de SQL permite que el Core de Rapid Recovery adjunte archivos de base de datos maestras de SQL (archivos .MDF) y archivos de base de datos de registro (archivos .LDF) a una instantánea de un SQL Server protegido. La instantánea se captura mediante una instancia local de Microsoft SQL Server.

Algunas cuestiones de importancia para los usuarios de Rapid Recovery que protejan equipos con SQL Server incluyen qué instancia de SQL Server realiza la conectabilidad y el método para realizar la conectabilidad SQL (a petición o como parte de los trabajos nocturnos).

La comprobación de conectabilidad permite que el Core compruebe la coherencia de las bases de datos de SQL y garantiza que todos los archivos MDF y LDF estén disponibles en la instantánea de copia de seguridad.

Las comprobaciones de conectabilidad se pueden ejecutar para puntos de recuperación específicos a petición, o bien como parte de un trabajo nocturno.

Para realizar la comprobación de conectabilidad de SQL a petición, consulte Forzado de una comprobación de conectabilidad de SQL Server. Para realizar la conectabilidad de SQL una vez al día, a la hora especificada para las operaciones de trabajos nocturnos, active la opción **Comprobar la conectabilidad de las bases de datos SQL** durante los trabajos nocturnos. Para obtener más información acerca de la configuración de los trabajos nocturnos para el Core, consulte Configuración de trabajos nocturnos para el Core. Para obtener más información acerca de la configuración de los trabajos nocturnos en un equipo específico (en este caso, un SQL Server protegido), consulte Personalización de trabajos nocturnos para un equipo protegido.

En versiones anteriores, la conectabilidad de SQL requería instalar y configurar una instancia local de Microsoft SQL Server en el equipo del Core. El Core de Rapid Recovery ahora le permite elegir realizar la comprobación de conectabilidad desde una instancia de SQL Server en el Core, o bien desde una instancia de SQL Server en un equipo protegido de SQL Server. La instancia que seleccione debe ser una versión con licencia completa de SQL Server proporcionada por Microsoft o mediante un distribuidor autorizado. Microsoft no permite el uso de licencias SQL pasivas.

La instancia de SQL Server que especifique se utilizará para todas las comprobaciones de conectabilidad. La conectabilidad se sincroniza entre la configuración del Core y los trabajos nocturnos. Por ejemplo, si especifica el uso de la instancia del Core de SQL Server para los trabajos nocturnos, las comprobaciones de conectabilidad a petición también utilizarán el Core. Por el contrario, si especifica el uso de la instancia de SQL Server en un equipo protegido específico, todas las comprobaciones de conectabilidad nocturna y a petición utilizarán la instancia local en el equipo protegido.

Seleccione la instancia de SQL Server que desea utilizar como parte de la configuración global del Core. Para obtener más información, consulte Administración de la configuración de conectabilidad de SQL del Core.

NOTE: Realizar la comprobación de conectabilidad desde un equipo protegido de SQL Server requiere que el software Rapid Recovery Agent esté instalado en dicho servidor. La protección sin agentes no es compatible con la conectabilidad de SQL.

La conectabilidad del Core de Rapid Recovery es compatible con SQL Server 2005, 2008, 2008 R2, 2012 y 2014. La cuenta que se utiliza para realizar las pruebas debe tener el rol sysadmin en la instancia de SQL Server.

el formato de almacenamiento en disco de SQL Server es el mismo en entornos de 32 y 64 bits, y la conectabilidad funciona entre ambas versiones. Una base de datos que se desconecta de una instancia de servidor que se ejecute en un entorno se puede adjuntar en una instancia de servidor que se ejecute en otro entorno.

NOTE: La versión de SQL Server en el Core tiene que ser igual o superior a la versión de SQL Server de todos los equipos protegidos con SQL Server instalado.

Forzado de una comprobación de conectabilidad de SQL Server

Para forzar una comprobación de capacidad de conexión, debe haber una base de datos de SQL en un volumen protegido. Si Rapid Recovery no detecta la presencia de una base de datos, la función de comprobación de capacidad de conexión no aparece en la Core Console.

Realice los pasos de este procedimiento para forzar que el sistema realice una comprobación de conectabilidad para un punto de recuperación del servidor SQL específico.

1. En el área de navegación izquierda de la Core Console de Rapid Recovery, seleccione el equipo SQL Server protegido para el que quiere forzar la comprobación de capacidad de conexión y, a continuación, haga clic en el menú **Puntos de recuperación**.
2. Desplácese hasta el panel **Puntos de recuperación**.
3. Navegue por los puntos de recuperación para encontrar el punto de recuperación en cuestión. De manera opcional, haga clic en la flecha a la derecha de un punto de recuperación de la lista para expandir la vista.

   En la información del punto de recuperación expandido, puede ver los volúmenes incluidos en el punto de recuperación.
4. En el panel **Puntos de recuperación**, en la fila que represente el punto de recuperación correcto, haga clic en  y, en el menú desplegable, seleccione **Forzar comprobación de conectabilidad**.
5. En el cuadro de diálogo resultante, haga clic para confirmar que desea forzar la comprobación de capacidad de conexión.

   El cuadro de diálogo se cierra. El sistema realiza la comprobación de conectabilidad.

Para obtener instrucciones sobre cómo ver el estado de las comprobación de capacidad de conexión, consulte Visualización de eventos mediante las páginas de tareas, alertas y del diario.

Administración de equipos protegidos

Esta sección describe cómo ver, configurar y administrar los equipos protegidos en su entorno de Rapid Recovery.

Acerca de la administración de equipos protegidos

Puede administrar los equipos protegidos desde la Rapid Recovery Core Console, incluidas las siguientes tareas:

- Puede ver los equipos protegidos en la Rapid Recovery Core Console utilizando las opciones descritas en el tema .
- Puede configurar los ajustes de un equipo determinado, que sustituyen a los ajustes predeterminados del Core. Algunas tareas de configuración incluyen el cambio de la configuración del host hipervisor o la máquina virtual, el acceso a la información del sistema, la modificación de la configuración de transferencia, la personalización de los trabajos nocturnos o la configuración de las notificaciones de eventos. Para obtener más información, consulte Configuración de los parámetros de equipos.
- Puede eliminar un equipo o un clúster de la protección, ver la información de licencia de un equipo protegido o diagnosticar problemas visualizando el archivo de registro del equipo protegido. Para obtener más información sobre esta y otras tareas, consulte Administración de equipos.
- Puede ver y administrar datos guardados en el Core. Para obtener más información, consulte Administración de instantáneas y puntos de recuperación.

Visualización de equipos protegidos

Desde la página **Inicio** de la Rapid Recovery Core Console, cuando observa la vista Tablas de resumen, puede ver información de resumen de cualquier equipo que proteja el Core en el panel Equipos protegidos.

NOTE: Un agente de software actúa por parte del usuario para realizar acciones específicas. Los equipos protegidos a veces se denominan Agents, ya que ejecutan el software Rapid Recovery Agent para facilitar las copias de seguridad y la replicación en el Rapid Recovery Core.

Puede ver el estado, el nombre para mostrar de cada equipo, qué repositorio utiliza, la fecha y la hora de la última instantánea, cuántos puntos de recuperación hay en el repositorio para el equipo, así como la cantidad total de espacio de almacenamiento que utilizan las instantáneas en el repositorio.

Para administrar aspectos de cualquier equipo protegido, empiece desplazándose hasta el equipo que desee ver, configurar o administrar. Desde la página **Inicio**, hay tres maneras de desplazarse hasta un equipo protegido:

- Puede hacer clic en la dirección IP o nombre para mostrar de cualquier equipo protegido del panel Equipos protegidos. Esta acción le llevará a la página Resumen del equipo protegido seleccionado.
- En el área de navegación de la izquierda, puede hacer clic en el título del menú **Equipos protegidos**. Aparecerá la página **Equipos protegidos**. En esta página puede ver información de resumen sobre cada

equipo. Para obtener una descripción detallada de esta página, consulte Visualización de información de resumen de un equipo protegido.

- En el menú Equipos protegidos del área de navegación de la izquierda, puede hacer clic en la dirección IP o en el nombre para mostrar de cualquier equipo protegido. Esta acción le llevará a la página **Resumen** del equipo protegido seleccionado. Para obtener una descripción detallada de esta página, consulte Visualización de información de resumen de un equipo protegido.

Visualización de información de resumen del clúster

Realice los pasos de este procedimiento para ver información de resumen sobre un clúster, incluyendo información sobre el quórum asociado para el clúster.

1. En la Core Console de Rapid Recovery, en Equipos protegidos, haga clic en el clúster que desea ver.

   Aparece la página Resumen para el equipo.
2. En la página Resumen, puede ver información como el nombre del clúster, tipo de clúster, tipo de quórum (si procede) y ruta de acceso de quórum (si procede). En esta página también se muestra información de un vistazo sobre los volúmenes de este clúster, que incluye el tamaño y la programación de protección. Si es aplicable, también puede ver información de SQL Server o Exchange Server para un clúster diferente.
3. Para ver la información más actual, haga clic en **Actualizar**.

Para obtener más información sobre la visualización de información de resumen y estado para una máquina o nodo individual del clúster, consulte .

Configuración de los parámetros de equipos

Una vez que haya protegido un equipo en su Rapid Recovery Core, puede ver y modificar fácilmente la configuración que rige el comportamiento de ese equipo protegido. Cuando modifica la configuración de un equipo específico, las nuevas opciones de configuración sustituyen el comportamiento establecido a nivel del Core.

Puede ver y configurar las siguientes las opciones del equipo en la Rapid Recovery Core Console:

- **General**. Los valores de configuración general del equipo incluyen el nombre para mostrar, el nombre de host, el puerto, la clave de cifrado, el repositorio y vínculos a un host de hipervisor. Para obtener información sobre la configuración de los valores generales de un equipo, consulte Visualización y modificación de la configuración de equipos protegidos.
- **Trabajos nocturnos**. El subconjunto de opciones de configuración de trabajo nocturno del Core que aparecen para un determinado equipo protegido le permiten sustituir el conjunto de opciones de configuración de trabajo nocturno establecidas a nivel del Core. Esto incluye la consolidación, que le permite administrar la política de retención. Algunos valores de configuración pueden diferir según el tipo de equipo que se proteja.
- **Configuración de transferencia.** Valores específicos de la administración de los procesos de transferencia de datos del equipo protegido seleccionado. Para obtener información sobre los tipos de transferencia de datos a los que afecta esta configuración, consulte Acerca de la modificación de la configuración de transferencias.
- **Escritores excluidos**. Estas opciones de configuración le permiten excluir escritores. Son específicos de cada equipo. Un escritor es una API específica que publica Microsoft para permitir que otros componentes de software participen en el uso de Microsoft Volume Shadow Services (VSS). Cada uno de los escritores en Rapid Recovery que participan en las instantáneas del volumen se muestra en la configuración de

Escritores excluidos. En el caso de que algún escritor interfiera con las transferencias correctas de copia de seguridad o las imposibilite, se podrán desactivar uno a uno. Quest recomienda no modificar estos valores a menos que un representante del Asistencia para la protección de datos de Quest indique lo contrario.

- **Detalles de la licencia**. Estos son los detalles de la licencia del equipo protegido específico. Estos valores contienen información del Core y del Portal de licencias de Rapid Recovery. Estas opciones de configuración son de solo lectura. Para modificarlas, actualice su información de licencia entre el Core y el portal de licencias. Para obtener más detalles, consulte a su administrador de licencias. Para obtener más información, consulte *Rapid Recovery License Portal User Guide (Guía del usuario del Portal de licencias de Rapid Recovery)*.

El procedimiento para ver o cambiar opciones de configuración a nivel de equipo es el mismo para la configuración general, los escritores excluidos y los detalles de la licencia. Para obtener más información, consulte Visualización y modificación de la configuración de equipos protegidos.

El procedimiento para modificar trabajos nocturnos para un equipo es diferente. Para obtener información sobre la configuración de los valores de trabajo nocturno de un equipo, consulte Personalización de trabajos nocturnos para un equipo protegido.

En algunos casos, es posible que desee ajustar la velocidad de transferencia de datos de un equipo protegido. Para obtener más información, consulte Acerca de la modificación de la configuración de transferencias.

Visualización y modificación de la configuración de equipos protegidos

La configuración de los equipos ayuda a determinar el comportamiento de un equipo protegido por el Core. Cuando modifica la configuración de un equipo específico, las nuevas opciones de configuración sustituyen el comportamiento establecido a nivel del Core.

De la misma forma, un host virtual de Hyper-V protegido tiene una configuración de equipo diferente a la de las máquinas virtuales que administra. Para obtener más información, consulte Ver información de resumen para un host.

Siga los pasos de este procedimiento para ver y modificar la configuración general, la configuración de transferencia, la configuración de escritores excluidos y la configuración de licencias de un equipo protegido.

NOTE: Para ver y modificar la configuración de un trabajo nocturno, consulte Personalización de trabajos nocturnos para un equipo protegido.

1. En la Rapid Recovery Core Console, en el menú Equipos protegidos, haga clic en la dirección IP o el nombre del equipo que desee visualizar o modificar.

   Se mostrará la página **Resumen** del equipo seleccionado.
2. Haga clic en el menú **Configuración**.

   Se muestra la página **Configuración**, que muestra los ajustes del equipo seleccionado. De manera opcional, para ver las categorías de configuración desde cualquier parte de la página, haga clic en el hipervínculo correspondiente del lado izquierdo de la página.

Cuando haga clic en una opción que desee cambiar, ese valor se volverá editable. Realice uno de los siguientes pasos:

- Si el control es un menú desplegable, haga clic en la flecha hacia abajo para ver una lista de opciones y seleccione la opción deseada en el menú.
- Si el control es un campo de texto, introduzca un valor.
- Si la opción muestra **Sí** o **No**, haga clic en el valor, que se convertirá en una casilla de verificación. Para Sí, marque la casilla. Para No, desmarque la casilla.
- Si la opción muestra un valor de tiempo (por ejemplo, horas, minutos y segundos), puede hacer clic en cada componente y escribir un valor nuevo o utilizar las flechas hacia arriba y hacia abajo para seleccionar nuevos valores.

Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para confirmar, guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

3. Para modificar la configuración general de un equipo protegido, haga clic en la opción pertinente y, a continuación, introduzca la información de configuración tal como se describe en la tabla siguiente.

Tabla 76. Configuración general de un equipo protegido

Cuadro de texto	Descripción
Nombre para mostrar	Escriba el nombre para mostrar del equipo. Es el nombre que aparece para un equipo protegido en la Rapid Recovery Core Console. Puede introducir hasta 64 caracteres. De manera predeterminada, es el nombre de host del equipo. Si fuera necesario, puede cambiarlo a otro de uso más fácil. No utilice caracteres prohibidos ni frases prohibidas.
Nombre de host	Es el nombre del equipo protegido tal y como aparece en los metadatos del equipo. **NOTE:** No cambie esta configuración, si lo hace podría interrumpir la conexión entre el equipo protegido y el Core.
Repositorio	Esta opción solo aparece para los clústeres Hyper-V protegidos, que admiten discos duros virtuales compartidos. Muestra el repositorio configurado en el Rapid Recovery Core en el que se almacenan los puntos de recuperación de discos duros virtuales compartidos para el clúster Hyper-V protegido.
Puerto	Especifique un número de puerto para el equipo. El puerto lo utiliza el servicio del Rapid Recovery Core para la comunicación con este equipo. El puerto predeterminado es 8006.
Clave de cifrado	Si desea que se aplique una clave de cifrado que ya esté definida para este Rapid Recovery Core a los datos de todos los volúmenes de este equipo protegido, puede especificarla aquí. Es necesario desbloquear la clave. Si no hay claves de cifrado, puede agregar una clave de cifrado. Para obtener más información sobre la administración de las claves de cifrado, consulte Administración de las claves de cifrado. Si los volúmenes de este equipo protegido están cifrados, puede cambiar a una clave de cifrado diferente. De forma alternativa, para desasociar una clave de cifrado, seleccione **(ninguno)** en el menú desplegable **Clave de cifrado**. **NOTE:** Después de aplicar una clave de cifrado, de cambiar una clave de cifrado o de desasociar una clave de cifrado para un equipo protegido, Rapid Recovery realiza una nueva imagen base en la siguiente instantánea programada o forzada.

Cuadro de texto	Descripción
Repositorio	Seleccione un repositorio para los puntos de recuperación. Muestra el repositorio configurado en el Rapid Recovery Core donde se almacenarán los datos de este equipo. El volumen del repositorio puede ser local (en almacenamiento conectado al servidor del Core) o encontrarse en un volumen en una ubicación CIFS compartida. **NOTE:** La configuración de repositorio en esta página solo se puede cambiar si no hay puntos de recuperación o si falta el repositorio anterior.
Hipervisor	Esta opción solo aparece para máquinas virtuales. El valor de este ajuste indica si la máquina virtual seleccionada está asociada como secundaria de un host de hipervisor protegido. • Si puede ver la dirección IP o el nombre para mostrar de un host protegido, significa que la asociación existe. Este resultado indica que el equipo protegido no consume innecesariamente una licencia de su grupo de licencias disponibles. • Si desea eliminar la asociación, haga clic en la dirección IP o nombre para mostrar del host de hipervisor, seleccione **Sin vincular** en el menú desplegable y haga clic en la marca de verificación para confirmar el cambio. Después, esta máquina virtual protegida consumirá una licencia de su grupo. • Si ve "Sin vincular", la máquina no está asociada actualmente en su Core como máquina virtual en un host protegido y consume una licencia de su grupo. Si desea guardar una licencia, y el host está protegido por Agent, puede asociarla haciendo clic en **Sin vincular** y seleccionando el host en el menú desplegable.
Versión del sistema operativo	Esta opción solo aparece para máquinas virtuales invitadas asociadas con un host de hipervisor protegido. Generalmente, Rapid Recovery detecta y muestra el sistema operativo de la máquina virtual protegida.

4. Para modificar la configuración de trabajo nocturno de un equipo protegido, consulte Personalización de trabajos nocturnos para un equipo protegido.
5. Para modificar la configuración de Exchange de un servidor Exchange protegido, en la sección Configuración de Exchange Server, haga clic en **Habilitar comprobación de capacidad de montaje automático** y realice lo siguiente:
   - Para activar las comprobaciones de capacidad de montaje automático, marque la casilla de verificación y, a continuación, haga clic en ✓.
   - Para desactivar las comprobaciones de capacidad de montaje automático, desmarque la casilla de verificación y, a continuación, haga clic en ✖.

   Para obtener más información sobre comprobaciones automáticas de capacidad de montaje, consulte Acerca de las comprobaciones de capacidad de montaje de base de datos de Exchange.
6. Para modificar la configuración de transferencia de un equipo protegido, haga clic en la opción pertinente y, a continuación, introduzca la información de configuración tal como se describe en la tabla siguiente.

   NOTE: Para obtener información sobre los conceptos de la configuración de transferencia, consulte Acerca de la modificación de la configuración de transferencias.

Tabla 77. Configuración de transferencia de un equipo protegido

Cuadro de texto	Descripción
Restaurar valores predeterminados	Este control restaura la configuración de transferencia a sus valores predeterminados.
Prioridad	Establece la prioridad de transferencia entre equipos protegidos. Le permite asignar prioridad por comparación con otros equipos protegidos. Seleccione un número del 1 al 10, siendo 1 la mayor prioridad. El valor predeterminado establece una prioridad de 5. **NOTE:** La prioridad se aplica a las transferencias que hay en la cola.
N.º máximo de flujos simultáneos	Establece el número máximo de enlaces de TCP que se envían al Core para procesarlos en paralelo por equipo protegido, para equipos protegidos en un repositorio DVM. **NOTE:** Quest recomienda establecer este valor como 8. Si se descartan paquetes, pruebe a incrementar este valor.
N.º máximo de escrituras simultáneas	Establece el número máximo de acciones de escritura en disco simultáneas por conexión de equipo protegido. **NOTE:** Quest recomienda establecer este valor igual que el valor que seleccionó para Número máximo de transmisiones simultáneas. Si se pierden paquetes, establezca un valor ligeramente menor: por ejemplo, si Número máximo de transmisiones simultáneas es 8, establezca este valor como 7.
Utilizar el número máximo predeterminado de reintentos del Core	Seleccione esta opción para utilizar el número predeterminado de reintentos para cada equipo protegido, si algunas de las operaciones no se pueden completar.
Tamaño máximo del segmento	Especifica la cantidad mayor de datos, en bytes, que un equipo puede recibir en un único segmento TCP. El valor predeterminado es 4194304. No cambie este valor predeterminado a menos que así se lo indique un representante de asistencia técnica de Quest.
Profundidad máxima de la cola de transferencia	Especifica la cantidad de comandos que pueden enviarse simultáneamente. El valor predeterminado es 64. Puede ajustar este valor con un número más alto si su sistema tiene un alto número de operaciones de entrada/salida simultáneas.
Lecturas pendientes por transmisión	Especifica cuántas operaciones de lectura en cola se almacenarán en el back-end. Este parámetro ayuda a controlar la puesta en cola de equipos protegidos. El valor predeterminado es 0.
Puerto de servidor de datos de transferencia	Establece el puerto de las transferencias. El valor predeterminado es 8009.

Cuadro de texto	Descripción
Tiempo de espera de la transferencia	Especifica en minutos y segundos la cantidad de tiempo que se permite a un paquete ser estático sin transferirlo.
Tiempo de espera de la instantánea	Especifica en minutos y segundos el tiempo máximo de espera para tomar una instantánea.
Tiempo de espera de limpieza de la instantánea	Especifica en minutos y segundos el tiempo máximo para procesar o eliminar una instantánea de VSS en un equipo protegido.
Tiempo de espera de lectura de red	Especifica en minutos y segundos el tiempo máximo de espera para una conexión de lectura. Si la lectura de red no se puede realizar en ese momento, se volverá a intentar realizar la operación.
Tiempo de espera de escritura de red	Especifica el tiempo máximo en segundos que se esperará para una conexión de escritura. Si la escritura de red no se puede realizar en ese momento, se volverá a intentar realizar la operación.
Cifrar datos de instantánea	Especifica si se cifran los datos transportados entre la máquina protegida y el Core. Esta opción está activada de manera predeterminada. Esta configuración se aplica a los datos de tránsito a través de una conexión de red. Si la opción está activada, se cifran todos los datos de instantáneas transportados a un repositorio DVM. **NOTE:** Quest recomienda activar esta opción cuando los datos entre el Core y las máquinas protegidas deben pasar por redes públicas o no fiables como Internet.

7. Para modificar la configuración de los escritores excluidos, haga clic en la configuración adecuada y, a continuación, seleccione un escritor si quiere excluirlo.

   NOTE: Como los escritores que aparecen en la lista son específicos del equipo que está configurando, no verá a todos los escritores de su lista.

8. Los detalles de la licencia de un equipo protegido son de solo lectura. La información de detalles de la licencia se describe en la tabla siguiente.

Tabla 78. Detalles de la licencia de un equipo protegido

Cuadro de texto	Descripción
Fecha de caducidad	Indica la fecha de caducidad de la licencia del equipo protegido seleccionado.
Estado de la licencia	Indica el estado actual de la licencia del equipo protegido seleccionado.
Tipo de licencia	Indica el tipo de licencia del equipo protegido seleccionado.
Tipo de Agent	Indica si el equipo protegido actual es un agente físico o virtual.

See also: Cambiar la configuración de un nodo o host de Hyper-V
See also: Cambiar la configuración de una máquina virtual protegida Hyper-V
See also: Cambiar la configuración de vSphere para una máquina virtual protegida VMware

Cambiar la configuración de un nodo o host de Hyper-V

Este procedimiento se aplica a los nodos o hosts de Hyper-V que usan la función Rapid Snap for Virtual (protección sin agentes) de Rapid Recovery para proteger las máquinas virtuales (VM).

Un host de Hyper-V que usa Rapid Snap for Virtual (protección sin agentes) para proteger máquinas virtuales se indica en el área de navegación de la izquierda con el icono de host  . La configuración de un host de Hyper-V con máquinas virtuales protegidas sin agentes no es la misma que la de un equipo protegido normal. Todos los cambios realizados en la configuración de un host se aplican a las máquinas virtuales de ese host.

1. En la Core Console, en Equipos protegidos en el área de navegación izquierda, haga clic en el host de Hyper-V cuya configuración quiera cambiar.

   Se abre la página **Resumen** del host.
2. En la barra de menú del host, haga clic en **Configuración**.

   Aparecerá la página **Configuración**.
3. En **General**, haga clic en la configuración que desea cambiar.

   La configuración seleccionada se convierte en editable, como un campo de texto o un menú desplegable.
4. Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 79. Información de configuración general

Cuadro de texto	Descripción
Nombre para mostrar	Nombre que aparece para un equipo protegido en la Rapid Recovery Core Console. Puede introducir hasta 64 caracteres. De manera predeterminada, es el nombre de host del equipo. Si fuera necesario, puede cambiarlo el nombre para mostrar a otro de uso más fácil. No utilice caracteres prohibidos ni frases prohibidas.
Nombre de host	Nombre del equipo protegido como aparece en los metadatos del equipo. **NOTE:** No cambie esta configuración, si lo hace podría interrumpir la conexión entre el equipo protegido y el Core.

5. En **Cola de transferencia**, para cambiar el número de trabajo de transferencia que pueden producirse en el host al mismo tiempo, haga clic en la configuración **Número máximo de transferencias simultáneas**.

   NOTE: Para obtener un mejor rendimiento, se recomienda que el número máximo de transferencias simultáneas del nodo o host de Hyper-V se establezca en 1, que es el valor predeterminado.
6. En **Trabajos nocturnos**, para cambiar la configuración de los trabajos nocturnos disponibles, haga clic en **Cambiar**.

   Aparece la ventana **Trabajos nocturnos**.
7. Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 80. Información de la configuración Trabajos nocturnos

Cuadro de texto	Descripción
Elimine las claves de registro huérfanas del	Elimina los archivos innecesarios del registro que surge de adjuntar y desasociar discos virtuales durante las transferencias de datos.

Cuadro de texto	Descripción
host Hyper-V protegido	
Comprobar integridad de puntos de recuperación	Realiza una comprobación de integridad de cada punto de recuperación creado para las máquinas virtuales en el host de Hyper-V.

8. Haga clic en **Aceptar**.
9. En **Protección automática**, para determinar si quiere proteger las nuevas máquinas virtuales automáticamente cuando se agregan al host de Hyper-V, haga clic en la configuración **Proteger automáticamente las nuevas máquinas virtuales**.

Cambiar la configuración de una máquina virtual protegida Hyper-V

Este procedimiento se aplica a máquinas virtuales Hyper-V (VM) protegidas mediante la función Rapid Snap for Virtual de Rapid Recovery (protección sin agentes).

Una VM Hyper-V que se protege mediante la función Rapid Snap for Virtual (protección sin agentes) se sindica en el área de navegación de la izquierda con el icono de host . La configuración de una VM Hyper-V sin agentes es la misma que la de un equipo protegido normal con la excepción de la sección Hyper-V que se encuentra en la parte inferior de la página Configuración. La siguiente tarea proporciona instrucciones solo para la configuración de la sección Hyper-V. Para ver la configuración de todos los demás equipos protegidos, consulte Visualización y modificación de la configuración de equipos protegidos.

1. En la Core Console, en el área de navegación izquierda en **Equipos protegidos**, haga clic en la VM Hyper-V cuya configuración quiere cambiar.

   Se abre la página **Resumen** para la VM.
2. En la barra de menú del host, haga clic en **Configuración**.

   Aparecerá la página **Configuración**.
3. En la lista de la izquierda, haga clic en **Hyper-V**.

   La configuración seleccionada se convierte en editable, como un campo de texto o un menú desplegable.
4. En **Hyper-V**, haga clic en **Configuración de instantáneas**.

   La configuración seleccionada se convierte en un menú desplegable editable.
5. En el menú desplegable, seleccione una de las opciones que se describen en la tabla siguiente.

Tabla 81. Información de la configuración de Hyper-V

Cuadro de texto	Descripción
Intente crear una instantánea VSS durante la primera transferencia, si falla, cree un punto de control	Si la instantánea VSS se realiza correctamente, el punto de recuperación estará en un estado coherente con la aplicación. Si la instantánea de VSS falla y se crea un punto de control, el punto de recuperación estará en un estado coherente con bloqueo.
No cree instantáneas VSS durante la transferencia.	Genera un punto de recuperación en un estado coherente con bloqueo.

Cuadro de texto	Descripción
Utilice únicamente instantáneas VSS durante las transferencias. Si la creación de instantáneas VSS falla, fallará toda la transferencia.	Genera solo puntos de recuperación coherentes con la aplicación. Si la instantánea VSS falla, no se genera ningún punto de recuperación.

Cambiar la configuración de vSphere para una máquina virtual protegida VMware

Este procedimiento se aplica a máquinas virtuales (VM) VMware ESXi que están protegidas mediante la función Rapid Snap for Virtual (protección sin agentes).

La configuración de una VM VMware que está protegida sin agentes incluye la misma configuración que se utiliza para una máquina protegida normal, con una excepción. En la sección **vSphere** de la página **Configuración** se incluye la configuración que se aplica solo a las VM VMware protegidas sin agentes. La siguiente tarea proporciona instrucciones solo de la sección **vSphere** de la página **Configuración**. Para ver la configuración de todos los demás equipos protegidos, consulte Visualización y modificación de la configuración de equipos protegidos.

1. En la Core Console, en Equipos protegidos en el área de navegación izquierda, haga clic en el host de Hyper-V cuya configuración quiera cambiar.

   Se abre la página **Resumen** del host.
2. En la barra de menú del host, haga clic en **Configuración**.

   Aparecerá la página **Configuración**.
3. En la lista de la izquierda, haga clic en **vSphere**.

   La configuración seleccionada se convierte en editable, como un campo de texto o un menú desplegable.
4. En **vSphere**, haga clic en la configuración que desea cambiar.

   La configuración seleccionada se convierte en editable, como un campo de texto o un menú desplegable.
5. Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 82. Información de la configuración de vSphere

Cuadro de texto	Descripción
Permitir a Rapid Recovery eliminar el usuario creado en VMware	El valor predeterminado es No.
Permitir la transferencia de volúmenes con capacidad utilizada no válida	El valor predeterminado es Sí.
Permitir instantáneas en modo inactivo	El valor predeterminado es Sí.

Acerca de la modificación de la configuración de transferencias

En Rapid Recovery, puede modificar la configuración para administrar los procesos de transferencia de datos de un equipo protegido. La configuración de las transferencias descrita en esta sección se establece en el nivel del equipo protegido. Para modificar la transferencia a nivel de Core, consulte Modificación de la configuración de la cola de transferencias.

Hay tres tipos de transferencias en Rapid Recovery:

- **Instantánea.** Realiza una copia de seguridad en su equipo protegido. Hay dos tipos de instantáneas posibles: una imagen base de todos los datos protegidos y una instantánea incremental de los datos actualizados desde la última instantánea. Este tipo de transferencia crea puntos de recuperación, que se almacenan en el repositorio asociado al Core. Para obtener más información, consulte Administración de instantáneas y puntos de recuperación.
- **Exportación de máquina virtual**. Crea una máquina virtual (VM) desde un punto de recuperación, que contiene todos los datos de la copia de seguridad del equipo protegido, así como el sistema operativo y los controladores y datos asociados para garantizar que la máquina virtual puede hacerse de inicio. Para obtener más información, consulte Exportación de la MV.
- Restaurar. Restaura la información de la copia de seguridad en un equipo protegido. Para obtener más información, consulte Acerca de la restauración de volúmenes desde un punto de recuperación.

  NOTE: Todo el volumen siempre se reescribe durante la restauración de sistemas Windows que utilicen particiones de sistema EFI.

La transferencia de datos en Rapid Recovery implica la transmisión de un volumen de datos a lo largo de una red desde equipos protegidos hasta el Core. En el caso de replicación, la transferencia también se produce desde el Core de origen al Core de destino.

La transferencia de datos se puede optimizar para su sistema a través de determinados ajustes de opciones de rendimiento. Estos parámetros controlan el uso de ancho de banda de datos durante el proceso de copia de seguridad de equipos protegidos, realizando una exportación de máquina virtual o una restauración. Estos son algunos de los factores que afectan al rendimiento de transferencia de datos:

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

Puede ajustar las opciones de rendimiento para cubrir mejor sus necesidades empresariales y ajustar el rendimiento basándose en su entorno. Para obtener más información, consulte Regulación de la velocidad de transferencia.

Regulación de la velocidad de transferencia

Cuando se transfieren datos de copia de seguridad o puntos de recuperación replicados entre equipos protegidos y Cores a través de la red, puede reducir deliberadamente la velocidad de transferencia. Este proceso se denomina regulación.

Cuando regula la velocidad de transferencia, está limitando la cantidad del ancho de banda de la red que dedica a las transferencias de archivos desde Rapid Recovery. Al configurar la replicación, por ejemplo, la regulación

puede reducir la probabilidad de que la transferencia de puntos de recuperación anteriores al Core replicado consuma todo el ancho de banda de la red.

> **CAUTION: No siempre es necesario o recomendable limitar la velocidad de transferencia. Esta información se facilita para indicar una posible solución a los problemas de rendimiento que puedan producirse en el entorno de Rapid Recovery. Por ejemplo, a veces, la regulación puede resolver los problemas relacionados con fallos de transferencia recurrentes o deceleraciones en la red debidos a la transferencia de una cantidad importante de datos a los Cores protegidos o replicados.**

Existen varios factores que determinan la mejor forma de abordar la regulación. El tipo de equipos que se protege es un elemento clave. Por ejemplo, un servidor de Microsoft Exchange ocupado tiene una velocidad de cambio mucho más elevada que la de un servidor web heredado que se utiliza poco.

Las capacidades de entrada y salida de los volúmenes de almacenamiento en los equipos protegidos también pueden contribuir a que la eficiencia sea mayor o menor.

La velocidad de la red también es otro factor fundamental, y tiene muchas variables. La red troncal implantada (por ejemplo, de 1 GbE frente a 10 GbE), la arquitectura, la configuración, el uso deliberado de grupos de NIC e incluso el tipo de cables que se utilizan pueden afectar a la velocidad de transferencia de la red. Si su entorno tiene una red de área amplia más lenta y si los trabajos de transferencia fallan para la copia de seguridad o la replicación, plantéese limitar la velocidad de transferencia utilizando algunas de estas opciones de configuración.

Por último, la regulación de la red implica un proceso de prueba y error. Quest recomienda ajustar y probar la configuración de transferencia y volver a examinar estas opciones periódicamente para garantizar que su configuración sigue satisfaciendo sus necesidades.

El ajuste de la velocidad de transferencia debe realizarse de manera individual equipo por equipo. En la Core Console, navegue hasta a un equipo específico, seleccione Configuración y ajuste la velocidad de transferencia. Para obtener información específica sobre cómo ver y cambiar estos valores, consulte Visualización y modificación de la configuración de equipos protegidos.

Ese tema también incluye descripciones de cada una de las opciones que se utilizan para la regulación transferencia. Estas descripciones pueden resultar útiles para determinar con qué opciones de configuración debe experimentar primero.

Las cuatro principales opciones que controlan la regulación de la velocidad se describen en la siguiente tabla:

Configuración a nivel del equipo	Configuración predeterminada	Configuración de limitación sugerida
N.º máximo de flujos simultáneos	8	4
N.º máximo de escrituras simultáneas	8	4
Tamaño máximo del segmento	4194304	2097152
Lecturas pendientes por transmisión	0	Empiece por 24.

Quest recomienda ajustar y probar el resto de opciones antes de cambiar la configuración predeterminada de las lecturas pendientes por transmisión, a menos que un representante del servicio de asistencia técnica de Quest indique lo contrario. A la hora de calibrar esta opción, empiece por un valor de 24.

Cuando especifique limitaciones para parámetros de transferencia de equipos protegidos, estas limitaciones se aplican por trabajo. Si dos trabajos de transferencia se producen simultáneamente o se superponen, se consume el doble de ancho de banda. Si cuatro trabajos de transferencia por la red se superponen, se usa el cuádruple de ancho de banda; y así sucesivamente.

Personalización de trabajos nocturnos para un equipo protegido

Los trabajos nocturnos pueden configurarse a nivel del Core o a nivel del equipo. Cuando los trabajos nocturnos se establecen a nivel de Core, los cambios se aplican a todos los equipos protegidos por ese Core. Los cambios realizados en trabajos nocturnos a nivel de equipo prevalecen sobre los cambios realizados a nivel de Core, y se aplican solo a los equipos especificados.

Para consultar una lista de todos los trabajos nocturnos, incluidos las descripciones y el ámbito disponibles para cada uno de ellos, consulte el tema Comprensión de los trabajos nocturnos.

Complete los pasos del procedimiento siguiente para realizar cambios en los trabajos nocturnos para un único equipo protegido.

1. En la Rapid Recovery Core Console, en el menú Equipos, haga clic en la dirección IP o el nombre del equipo para el que desee personalizar los trabajos nocturnos.

   Aparecerá la página **Resumen** del equipo seleccionado.
2. Haga clic en el menú **Configuración**.

   Aparece la página **Configuración**, que muestra los ajustes de configuración del equipo seleccionado.
3. De forma opcional, haga clic en el vínculo **Trabajos nocturnos** para desplazarse hasta la página **Configuración** para visualizar la configuración de los trabajos nocturnos.
4. En el encabezado Trabajos nocturnos, haga clic en **Cambiar**.

   Aparecerá el cuadro de diálogo **Trabajos nocturnos**.
5. En el cuadro de diálogo **Trabajos nocturnos**, seleccione los trabajos que desea incluir para que se ejecuten por la noche, o borre las opciones que desee omitir para este equipo.

   NOTE: Las opciones pueden variar de un equipo a otro. Por ejemplo, un equipo protegido que usa Exchange Server puede incluir Comprobar suma de comprobación de bases de datos de Exchange y Truncar registros de Exchange.

   NOTE: Para conocer más sobre la configuración de **Consolidación**, incluida la configuración de una política de retención personalizada, consulte Personalización de la configuración de la política de retención de un equipo protegido.
6. Haga clic en **Aceptar**.

   NOTE: Los resultados de este procedimiento se aplican únicamente al equipo protegido seleccionado. Para aplicar esta configuración en otro equipo, repita este procedimiento en el equipo que desee personalizar. Para cambiar la configuración de los trabajos nocturnos para todos equipos protegidos por un Core, consulte Configuración de trabajos nocturnos para el Core.

Visualización de la información del sistema de un equipo protegido

La Rapid Recovery Core Console le permite acceder fácilmente a la información del sistema sobre los equipos protegidos en el Core.

Cuando se visualiza la información del sistema de un equipo protegido específico, el panel **Información del sistema** muestra información general acerca del equipo protegido, incluida su relación con el Core y el repositorio. El panel **Volúmenes** muestra información sobre los volúmenes de almacenamiento en el equipo del

Core. El panel **Conexiones del motor de reproducción** muestra los volúmenes de todos los equipos que se están protegiendo.

Realice los pasos de este procedimiento para ver la información detallada del sistema de un equipo protegido.

1. Desplácese a la Rapid Recovery Core Console y, desde el menú de los equipos protegidos en el área de navegación izquierda, haga clic en el nombre de un equipo protegido.

   Aparece la página **Resumen** del equipo protegido seleccionado.
2. En la página **Resumen**, en la parte inferior del panel **Resumen**, haga clic en **Información del sistema**.
3. En la página **Información del sistema**, puede ver los siguientes detalles del equipo protegido seleccionado.
   - **Información del sistema.** Incluye el nombre de host, la versión del sistema operativo, la memoria física, el nombre para mostrar, el nombre de dominio completo y el tipo de máquina virtual (si corresponde).
   - **Volúmenes**. Incluye el nombre de volumen, la ID de dispositivo, el sistema de archivos, la capacidad formateada y la capacidad utilizada.
   - **Procesadores**. Incluye la arquitectura, el número de núcleos e hilos, la velocidad del reloj y la descripción.
   - **Adaptadores de red**. Incluye el tipo de adaptador de red y la velocidad.
   - **Direcciones IP**. Incluye la dirección IP y la familia.

Administración de equipos

Esta sección describe una variedad de tareas que puede realizar para administrar los equipos protegidos que administran sus equipos.

- Retirada de un equipo
- Retirada de un clúster de la protección
- Visualización de la información de licencia en un equipo
- Descarga y visualización del archivo de registro de un equipo protegido
- Conversión de un nodo de clúster protegido en un equipo protegido

Retirada de un equipo

Cuando retira un equipo de la protección en el Rapid Recovery Core, se le presentan dos opciones: puede mantener los puntos de recuperación guardados hasta ahora en el Core o bien puede eliminarlos.

Si mantiene los puntos de recuperación, tendrá lo que se conoce como un “equipo solo con puntos de recuperación”. Las operaciones de operación y montaje siguen estando disponibles en los puntos de recuperación capturados del equipo cuando se encontraba bajo protección. Sin embargo, las copias de seguridad de los equipos protegidos ya no siguen estando.

Si elimina los puntos de recuperación, esta acción elimina todos los datos de instantáneas del equipo que antes estaba protegido del Rapid Recovery Core.

Realice los pasos de este procedimiento para quitar un equipo de la protección de su entorno de Rapid Recovery.

1. Desde la Rapid Recovery Core Console, en el panel de navegación de la izquierda en Equipos protegidos, haga clic en el equipo desee quitar.
2. En la página **Resumen** del equipo en cuestión, haga clic en **Quitar equipo**.
3. En el cuadro de diálogo, si también desea eliminar todos los puntos de recuperación para este equipo del repositorio, seleccione **Quitar con puntos de recuperación**.
4. Para confirmar su decisión de quitar el equipo, haga clic en **Sí**.

   CAUTION: Si elimina los puntos de recuperación, ya no podrá restaurar datos para ese equipo.

   Rapid Recovery quitará la protección del equipo y cancelará todas las tareas activas del mismo.

Retirada de un clúster de la protección

Realice los pasos del procedimiento siguiente para quitar un clúster de la protección.

1. En la Rapid Recovery Core Console, en Equipos protegidos, haga clic en el clúster que desea eliminar.
2. En la página **Resumen** del clúster, haga clic en **Quitar clúster**.
3. Opcionalmente, en el cuadro de diálogo, para eliminar del repositorio todos los puntos de recuperación de este clúster almacenados actualmente, seleccione **Quitar con puntos de recuperación**.

   CAUTION: Si elimina los puntos de recuperación, ya no podrá restaurar datos para ese clúster.
4. En el cuadro de diálogo, haga clic en **Sí** para confirmar.

Retirada de nodos de clúster de la protección

Realice los pasos de los procedimientos siguientes para quitar los nodos de clúster de la protección.

Si solamente desea quitar un nodo del clúster, consulte Conversión de un nodo de clúster protegido en un equipo protegido.

1. En la Rapid Recovery Core Console, en Equipos protegidos, haga clic en el nodo de clúster que desea eliminar.
2. En la página **Resumen** del nodo, haga clic en **Quitar equipo**.

   Se abrirá el cuadro de diálogo Quitar nodo.
3. Opcionalmente, en el cuadro de diálogo, para eliminar del repositorio todos los puntos de recuperación de este clúster almacenados actualmente, seleccione **Quitar con puntos de recuperación**.

   CAUTION: Si elimina los puntos de recuperación, ya no podrá restaurar datos de los nodos de clúster.
4. En el cuadro de diálogo, haga clic en **Sí** para confirmar.

Retirada de todos los nodos de un clúster de la protección

Realice los pasos de este procedimiento para quitar todos los nodos de un clúster de la protección.

CAUTION: Si quita todos los nodos de un clúster, también se quita el clúster.

1. En la Rapid Recovery Core Console, en Equipos protegidos, haga clic en el clúster cuyos nodos desea eliminar.
2. En la página **Resumen** del clúster, haga clic en **Nodos protegidos**.
3. En la página **Nodos protegidos**, seleccione todos los nodos.
4. Haga clic en el menú desplegable **Quitar equipos** y, a continuación, seleccione una de las opciones que se describen en la siguiente tabla.

Tabla 83. Opciones de Quitar nodos

Opción	Descripción
Eliminar y mantener puntos de recuperación	Para mantener todos los puntos de recuperación actualmente almacenados para este clúster.
Quitar puntos de recuperación	Para quitar del repositorio todos los puntos de recuperación actualmente almacenados para este clúster. **CAUTION: Si elimina los puntos de recuperación, ya no podrá restaurar datos para ese clúster.**

5. En el cuadro de diálogo Eliminar nodos, haga clic en **Sí** para confirmar.

Visualización de la información de licencia en un equipo

Puede ver la información sobre el estado actual de la licencia del software Rapid Recovery Agent instalado en un equipo protegido.

1. En la Rapid Recovery Core Console, en Equipos protegidos, haga clic en el equipo que desea modificar.

   Aparece la página **Resumen** para el equipo seleccionado.
2. Haga clic en el menú **Configuración**.

   Aparece la página **Configuración**, que muestra los ajustes de configuración del equipo seleccionado.
3. Haga clic en el vínculo **Licencias** para desplazarse hasta la página Configuración para visualizar la configuración de licencias específica del equipo.

   Aparecerá la pantalla Estado, la cual mostrará detalles sobre las licencias del producto.

Descarga y visualización del archivo de registro de un equipo protegido

Si se produce algún error o problema con un equipo protegido, puede descargar los registros del equipo para verlos o consultarlos con su representante de Quest Support.

1. En el área de navegación izquierda de Core Console, bajo el menú Equipos protegidos, haga clic en la fecha para expandir el menú contextual de dicho equipo protegido. Desplácese hasta **Más**, expanda ese menú y, a continuación, seleccione **Agent Log**.

Aparece la página **Descargar el registro de agentes**.

2. En la página **Descargar registro de Agent**, haga clic en **Haga clic aquí para iniciar la descarga**.
3. En el cuadro de diálogo **Apertura de AgentAppRecovery.log**, realice una de las siguientes acciones:
   - Para abrir el archivo de registro, seleccione **Abrir con** y, a continuación, seleccione una aplicación (como Bloc de notas) para visualizar el archivo de registro basado en texto y haga clic en **Aceptar**.

     Se abre el archivo **AgentAppRecovery.log** en la aplicación seleccionada.
   - Para guardar el archivo localmente, seleccione **Guardar archivo** y después haga clic en **Aceptar**.

     El archivo **AgentAppRecovery.log** se guardará en su carpeta Descargas. Se puede abrir con un editor de texto.

See also: Descarga y visualización del archivo de registro del Core
See also: Descarga y visualización del archivo de registro de un equipo protegido

Conversión de un nodo de clúster protegido en un equipo protegido

En Rapid Recovery, puede convertir un nodo de clúster protegido en un equipo protegido de forma que aún siga administrado por el Core, pero que ya no sea parte del clúster. Esto es útil en el caso, por ejemplo, de que necesite quitar un nodo del clúster, pero quiera mantenerlo protegido.

1. En la Core Console de Rapid Recovery, desplácese hasta el clúster que contenga el equipo que quiera convertir y, a continuación, haga clic en **Nodos protegidos**.
2. En la página **Nodos protegidos**, desde el nodo específico que quiera convertir, haga clic en el menú desplegable Acciones y seleccione **Convertir en Agent**.
3. Para agregar el equipo nuevamente al clúster, selecciónelo y, a continuación, en la página Resumen, desde el menú Acciones, seleccione **Convertir en nodo de clúster** y, a continuación, haga clic en **Sí** para confirmar la acción.

Comprensión de los grupos personalizados

La Rapid Recovery Core Console muestra un menú de Equipos protegidos en el área de navegación izquierda. Esto incluye todos los equipos o los clústeres de servidor agregados a la protección del Rapid Recovery Core. Es posible que debajo aparezcan otros menús, en función de si incluye esos objetos en el Core. De la misma manera, puede crear un grupo personalizado, que se muestra como el último tipo de menú en el área de navegación de la izquierda.

La ventaja principal de un grupo personalizado es la capacidad de agrupar los objetos de Core en un contenedor lógico. Esto puede ayudarle a organizar y gestionar los objetos de Core para un fin específico (por ejemplo, por la organización, el centro de costes, el departamento, la región geográfica, etc.).

El acto de creación de un grupo siempre agrega un miembro del grupo (por ejemplo, un equipo protegido o un clúster de servidor, un equipo replicado o un equipo con solo puntos de recuperación) al nuevo grupo personalizado. El objeto agregado viene determinado por el punto de origen al crear el grupo. Idealmente, debería agregar entonces los miembros adicionales al grupo. De ahí en adelante, puede realizar acciones de grupo que se apliquen a todos los miembros de ese grupo personalizado, según se describe en Realización de acciones de grupo.

Los grupos personalizados pueden incluir equipos protegidos, clústeres de servidor, equipos replicados y equipos con solo puntos de recuperación. Los clústeres de servidor se comportan igual que los equipos protegidos, con la

excepción de que un clúster de servidor y sus nodos se comportan como una entidad única. Si intenta agregar un nodo desde un clúster de servidor a un grupo, se agrega todo el clúster.

Un grupo personalizado puede contener miembros similares o no similares. Con grupos de miembros similares, todas las acciones de grupo se aplican a todos los miembros del grupo. Por ejemplo, si fuerza una instantánea de un grupo personalizado de equipos protegidos, se realizará una copia de seguridad de todos los equipos. En los grupos con miembros no similares (por ejemplo, equipos protegidos y replicados), si aplica una acción de grupo, como el forzado de la replicación, esta solo se aplicará en los equipos replicados.

Puede crear uno o varios grupos. Un equipo protegido único o un equipo replicado se pueden incluir en uno o varios grupos. De esta forma, puede agrupar los equipos en su Core de la forma que quiera y puede realizar acciones en ese grupo en concreto.

Todos los grupos personalizados aparecen en el área de navegación izquierda, con la etiqueta que designe. Los grupos que tienen equipos protegidos estándar aparecen en primer lugar en el grupo personalizado y los equipos replicados aparecen debajo de los protegidos, según corresponda. Si hay algún equipo con solo puntos de recuperación, se enumerará debajo de los equipos replicados.

En el área de navegación de la izquierda, los objetos que están protegidos en el Core aparecen cada uno en su propio menú. De estos menús, los grupos personalizados aparecen al final.

Incluir un equipo en un grupo no lo quita de su ubicación original. Por ejemplo, si tiene tres equipos protegidos denominados Agent1, Agent2 y Agent3 y agrega Agent1 a CustomGroup1, el Agent1 aparecerá en ambas ubicaciones.

See also: Creación de grupos personalizados
See also: Modificación de nombres de grupo personalizados
See also: Eliminación de los grupos personalizados
See also: Realización de acciones de grupo
See also: Visualización de todos los equipos de un grupo personalizado en una página

Creación de grupos personalizados

Cuando desplace el cursor sobre el nombre de cualquier equipo de los menús Equipos protegidos o Equipos replicados, verá una flecha que abre el menú desplegable. En este menú, puede crear una etiqueta personalizada.

Utilice el siguiente procedimiento para crear un grupo personalizado.

1. Desplácese hasta la Core Console de Rapid Recovery.
2. Desde el menú Equipos protegidos, Equipos replicados o Equipos con puntos de recuperación únicamente, haga lo siguiente:
    a. Coloque el cursor sobre un equipo en el menú.
    b. Haga clic en el menú desplegable para ese equipo.
    c. Desplácese hacia abajo y seleccione **Etiquetar como** y, a continuación, haga clic en **Nueva etiqueta**.

    Aparece el cuadro de diálogo **Crear instantánea**.
3. En el campo **Nombre**, introduzca una etiqueta adecuada para su grupo personalizado.

    Utilice un nombre descriptivo que comunique el objetivo del grupo. Por ejemplo, para agrupar los equipos protegidos, replicados y con puntos de recuperación únicamente por departamento, escriba `Accounting Department`. Puede cambiar el nombre del grupo más adelante.

    NOTE: Las etiquetas deben tener 50 caracteres o menos. Puede incluir un espacio entre las palabras. Debe proporcionar una etiqueta para su grupo personalizado.
4. Cuando esté satisfecho con el nombre de la etiqueta, haga clic en **Aceptar**.

Se cierra el cuadro de diálogo y aparece el grupo personalizado como el último elemento en el área de navegación izquierda.

5. De forma opcional, pueden agregar otros equipos protegidos, replicados o con puntos de recuperación únicamente a este grupo. Vaya al nombre del equipo en el menú adecuado, haga clic en su menú desplegable, desplácese hacia abajo y seleccione **Etiquetar como** y, a continuación, haga clic en el nombre del grupo personalizado.

   Ahora puede realizar acciones grupo en este grupo. Para obtener más información, consulte Realización de acciones de grupo.

Modificación de nombres de grupo personalizados

Cuando modifica el nombre de un grupo personalizado, solo cambia la etiqueta. El nombre de equipo permanece igual.

Utilice el siguiente procedimiento para modificar un nombre de grupo personalizado.

1. Desplácese hasta la Core Console de Rapid Recovery.
2. En el menú Equipos protegidos, desplace el cursor sobre el grupo personalizado que desea modificar.
3. Haga clic en el menú desplegable del grupo y, a continuación, haga clic en **Editar**.

   Aparece el cuadro de diálogo **Modificar etiqueta**, que dentro del nombre del grupo personalizado se puede editar.
4. En el campo **Nombre**, actualice el texto o elimine el texto de la etiqueta existente y escriba una nueva etiqueta o su grupo personalizado.

   Utilice un nombre descriptivo que comunique el objetivo del grupo. Por ejemplo, para agrupar equipo protegidos, replicados y con puntos de recuperación únicamente por región geográfica, escriba `Tokyo`. Puede cambiar el nombre del grupo más adelante.

   NOTE: Las etiquetas deben tener 50 caracteres o menos. Puede incluir un espacio entre las palabras. Debe proporcionar una etiqueta para su grupo personalizado.
5. Cuando esté satisfecho con el nombre de la etiqueta, haga clic en **Aceptar**.

   Se cierra el cuadro de diálogo y aparece el grupo personalizado modificado como el último elemento en el área de navegación izquierda.
6. De forma opcional, pueden agregar otros equipos protegidos, replicados o con puntos de recuperación únicamente a este grupo. Vaya al nombre del equipo en el menú adecuado, haga clic en su menú desplegable, desplácese hacia abajo y seleccione **Etiquetar como** y, a continuación, haga clic en el nombre del grupo personalizado.

Eliminación de los grupos personalizados

Cuando quita un grupo personalizado, lo elimina del menú Equipos protegidos. Los equipos que estaban en el grupo no se quitan, sino que siguen en el menú estándar correspondiente.

Utilice el siguiente procedimiento para quitar un grupo personalizado.

1. Desplácese hasta la Core Console de Rapid Recovery.
2. En el menú Equipos protegidos, desplace el cursor sobre el grupo personalizado que desea quitar.
3. Haga clic en el menú desplegable del grupo y, a continuación, haga clic en **Quitar etiqueta**.

   Ve un mensaje que le pide confirmar que desea quitar el grupo.
4. Confirme la eliminación del grupo personalizado.

   Se cierra el cuadro de diálogo y el grupo personalizado se quita del área de navegación.

Realización de acciones de grupo

Puede realizar las acciones de grupo en cualquier grupo que aparece en el área de navegación izquierda de la Rapid Recovery Core Console. Si el grupo contiene miembros no similares (por ejemplo, equipos replicados y equipos con puntos de recuperación únicamente), las acciones que solicite solo se realizaran en los miembros del grupo relevantes.

Utilice el siguiente procedimiento para realizar acciones de grupo en un grupo personalizado.

1. Desplácese hasta la Rapid Recovery Core Console.
2. En el menú Equipos protegidos, desplace el cursor sobre el grupo personalizado sobre el que desee realizar una acción de grupo.
3. Haga clic en el menú desplegable de ese grupo y, a continuación, seleccione una acción de la siguiente forma:
   - Para forzar una instantánea incremental o una imagen de base para todos los equipos protegidos en el grupo, haga clic en **Forzar instantánea** o **Forzar imagen base**, como corresponda.
   - Para pausar la protección de todos los equipos protegidos en el grupo, haga clic en **Pausar la protección** y, a continuación, especifique los parámetros de reanudación.
   - Para reanudar la protección de todos los equipos protegidos en el grupo para el que se ha pausado la protección, haga clic en **Reanudar la protección** y, a continuación, confirme que quiere reanudarla.
   - Para actualizar la información de todos los objetos en el grupo, haga clic en **Actualizar los metadatos**.
   - Para pausar la replicación de todos los equipos protegidos en este grupo, debajo de Replicación, haga clic en **Pausar**.
   - Para reanudar la replicación de todos los equipos replicados en este grupo para el que se ha puesto en pausa la replicación, debajo de Replicación, haga clic en **Reanudar**.
   - Para forzar la replicación de todos los equipos replicados en este grupo, debajo de Replicación, haga clic en **Forzar**.
   - Para eliminar la replicación de todos los equipos replicados en este grupo, debajo de Replicación, haga clic en **Eliminar**.
   - Para eliminar los equipos con puntos de recuperación únicamente de este Core y descartar los puntos de recuperación, debajo de Solo puntos de recuperación, haga clic en **Quitar puntos de recuperación**.
   - Para modificar la etiqueta del grupo personalizado, solo en el caso de los grupos personalizados, seleccione **Editar**.
   - Para quitar el grupo personalizado del menú de navegación, solo en el caso de los grupos personalizados, seleccione **Quitar etiqueta**.

See also: Cómo forzar una instantánea
See also: Forzado de la replicación
See also: Pausa y reanudación de la replicación
See also: Puesta en pausa y reanudación de la protección
See also: Eliminar la replicación entrante del Core de destino
See also: Modificación de nombres de grupo personalizados
See also: Eliminación de los grupos personalizados

Visualización de todos los equipos de un grupo personalizado en una página

Si hace clic en el nombre de un grupo personalizado, accederá a la página Equipos que muestra todos los equipos de ese grupo personalizado. Ahí puede realizar algunas funciones del menú Acciones en todos los equipos o puede realizar acciones individuales seleccionando comandos de cada equipo concreto.

Instantáneas y puntos de recuperación

En esta sección se describe cómo utilizar y administrar las instantáneas y los puntos de recuperación generados mediante Rapid Recovery. Incluye información acerca del montaje, la visualización y el forzado, así como la migración y la eliminación de puntos de recuperación.

Administración de instantáneas y puntos de recuperación

Un punto de recuperación es un conjunto de instantáneas tomadas de volúmenes de discos individuales y almacenadas en el repositorio. Las instantáneas capturan y almacenan el estado de un volumen de disco en un punto determinado del tiempo mientras que las aplicaciones que generan los datos siguen utilizándose. En Rapid Recovery, puede forzar una instantánea, pausar temporalmente instantáneas y ver listas de puntos de recuperación actuales en el repositorio, así como eliminarlos si es necesario. Los puntos de recuperación se utilizan para restaurar equipos protegidos o para montar en un sistema de archivo local.

Las instantáneas que captura Rapid Recovery se realizan en el nivel del bloque y ofrecen reconocimiento de la aplicación. Esto significa que todos los registros de transacciones abiertas y transacciones en marcha se completan y que las memorias caché se vacían antes de crear la instantánea.

Rapid Recovery utiliza un controlador de filtro de volúmenes de bajo nivel que se adjunta a los volúmenes montados y, a continuación, realiza el seguimiento de todos los cambios de nivel de bloque para la próxima instantánea inminente. Los Microsoft Volume Shadow Services (VSS) (Servicios de instantáneas de volumen de Microsoft) se utilizan para facilitar instantáneas de la aplicación en estado coherente tras la interrupción.

Visualización de la página de puntos de recuperación de un equipo protegido

Realice los pasos del procedimiento siguiente para ver la lista completa de los puntos de recuperación para un equipo protegido.

NOTE: Si está protegiendo datos desde un clúster de servidor DAG o CCR, los puntos de recuperación asociados no aparecen a nivel de clúster. Sólo están visibles a nivel de nodo o de equipo.

1. En la Rapid Recovery Core Console, desplácese hasta el equipo protegido cuyos puntos de recuperación desee visualizar.
2. En el menú de la parte superior de la página, haga clic en **Puntos de recuperación**.

   Aparece la página **Puntos de recuperación** que muestra un panel de resumen los puntos de recuperación y un panel de puntos de recuperación.

Puede ver la información resumida sobre los puntos de recuperación del equipo como se describe en la tabla siguiente.

Tabla 84. Resumen de la información de punto de recuperación

Información	Descripción
Total de puntos de recuperación	Muestra el número total de puntos de recuperación guardados en el repositorio para este equipo.
Total de datos protegidos	Indica la cantidad de espacio de almacenamiento utilizado en el repositorio para estos puntos de recuperación.
Repositorio	Muestra el nombre del repositorio en el que se almacenan estos puntos de recuperación.
Estado del repositorio	Muestra de manera gráfica la cantidad de espacio consumido por los puntos de recuperación. Muestra el porcentaje del repositorio que se usa, la cantidad de espacio, y el espacio total del repositorio. Haga clic en el gráfico para ver la cantidad de espacio restante.

Puede ver la información sobre los puntos de recuperación del equipo como se describe en la tabla siguiente.

Tabla 85. Información de punto de recuperación

Información	Descripción
Icono	Representación gráfica de un punto de recuperación o, si se expande, un volumen en el punto de recuperación . Los puntos de recuperación muestran una flecha derecha que indica que se puede ampliar el detalle.
Cifrado	Indica si el punto de recuperación está cifrado.
Estado	Indica el estado actual del punto de recuperación.
Contenido	Lista los volúmenes incluidos en el punto de recuperación. • Haga clic en (Información) para ver el uso del espacio y el sistema de archivos. • Para los servidores Exchange, haga clic en para ver la información sobre el servidor.
Tipo	Define un punto de recuperación como una imagen base o una instantánea incremental (diferencial).
Fecha de creación	Muestra la fecha de creación del punto de recuperación.
Tamaño	Muestra la cantidad de espacio que el punto de recuperación consume en el repositorio.
•••	El menú desplegable [Más] le permite realizar ciertas funciones para el punto de recuperación seleccionado.

3. De manera opcional, expanda un punto de recuperación para ver los volúmenes protegidos.

Referencia relacionada

See also: Visualización de los puntos de recuperación para un equipo

Comprensión de los indicadores de estado de puntos de recuperación

Una vez que se obtiene un punto de recuperación para un Exchange Server o SQL Server protegido, la aplicación muestra un indicador de estado en color correspondiente en la tabla Puntos de recuperación. Esta tabla aparece en el panel **Puntos de recuperación** cuando se visualizan los puntos de recuperación de un equipo determinado. El color que muestra se basa en la configuración de comprobación del equipo protegido y en el éxito o fallo de esas comprobaciones, como se describe en las tablas siguientes.

NOTE: Para obtener más información sobre la visualización de los puntos de recuperación, consulte Visualización de la página de puntos de recuperación de un equipo protegido.

Colores de punto de estado de recuperación para bases de datos Exchange

En la siguiente tabla aparece una lista de los indicadores de estado que se muestran para las bases de datos Exchange.

Tabla 86. Indicadores de estado de bases de datos Exchange

Color de estado	Descripción
Blanco	Indica que no se detecta una base de datos de Exchange dentro del punto de recuperación, volumen o grupo de volúmenes.
Amarillo	Indica que las comprobaciones de capacidad de montaje de base de datos de Exchange aún no se han ejecutado.
Rojo	Indica que las comprobaciones de capacidad de montaje o de suma de comprobación han sido erróneas en al menos una base de datos.
Verde	Indica que el punto de recuperación contiene una o varias bases de datos, que las comprobaciones de capacidad están activadas y que la comprobación de capacidad o la comprobación de la suma de comprobación fueron correctas.

Colores de punto de estado de recuperación para bases de datos SQL

En la siguiente tabla aparece una lista de los indicadores de estado que se muestran para las bases de datos SQL.

Tabla 87. Indicadores de estado de bases de datos SQL

Color de estado	Descripción
Blanco	Indica que no se detecta una base de datos de SQL dentro del punto de recuperación, volumen o grupo de volúmenes.
Amarillo	La base de datos de SQL estaba fuera de línea, indicando que no fueron posibles las comprobaciones de conectabilidad y no se han ejecutado.
Rojo	Indica que la comprobación de conectabilidad ha fallado o que la base de datos de SQL está sin conexión.

Color de estado	Descripción
Verde	Indica que la comprobación de conectabilidad ha sido correcta.

NOTE: Los puntos de recuperación que no tienen una base de datos de SQL o Exchange asociadas aparecen con un indicador de estado en blanco. En las situaciones en las que existan tanto base de datos de Exchange como SQL para el punto de recuperación, se mostrarán los indicadores de estado más graves para el punto de recuperación.

Montaje de un punto de recuperación

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

NOTE: Para montar un punto de recuperación de Linux con la utilidad `local_mount`, consulte Montaje de un volumen de punto de recuperación en un equipo Linux.

NOTE: Al montar puntos de recuperación desde datos restaurados desde un equipo que tiene activada la desduplicación de datos, deberá activar también la desduplicación en el servidor de Core.

1. En la Rapid Recovery Core Console, desplácese hasta el equipo que quiera montar en un sistema de archivos local.

   Aparece la página **Resumen** del equipo protegido seleccionado.

2. Haga clic en el menú **Puntos de recuperación**.

   Aparecerá la página **Puntos de recuperación** del equipo seleccionado.

3. De manera opcional, en el panel **Puntos de recuperación**, desde la lista de puntos de recuperación, haga clic en el símbolo de flecha derecha para expandir los detalles del punto de recuperación que muestran los volúmenes que se incluyen en el punto de recuperación.

4. En la fila del punto de recuperación que desea montar, haga clic en y en el menú desplegable seleccione **Montar**.

   Aparecerá el **Asistente de montaje** y podrá ver la página **Volúmenes**.

5. En la página **Volúmenes**, seleccione cada volumen del punto de recuperación que desee montar y, a continuación, haga clic en **Siguiente**.

   Se mostrará la página **Opciones de montaje** del Asistente de montaje.

6. En la página **Opciones de montaje**, edite la configuración para montar un punto de recuperación como se describe en la tabla siguiente.

Tabla 88. Configuración de Opciones de montaje

Opción	Descripción
Carpeta local	Especifica la ruta de acceso que se utiliza para acceder al punto de recuperación montado. Por ejemplo, seleccione `C:\ProgramData\AppRecovery\MountPoints\MountPoint1`.

Opción	Descripción
Tipo de montaje	Especifica la forma para acceder a los datos para el punto de recuperación montado. • Solo lectura • Solo lectura con escrituras anteriores • Editable
Crear un recurso compartido de Windows para este montaje	De manera opcional, seleccione esta casilla para especificar si el punto de recuperación montado se puede compartir y, en ese caso, configurar los derechos de acceso, incluidos el nombre compartido y los grupos permitidos.

7. Haga clic en **Finalizar** para montar el punto de recuperación.

   NOTE: Si quiere copiar directorios o archivos desde un punto de recuperación montado a otro equipo con Windows, puede utilizar Windows Explorer para copiarlos con permisos predeterminados o permisos de acceso de archivo original. Para obtener información detallada, consulte desde Restauración de un directorio o archivo mediante Windows Explorer hasta Restauración de un directorio o archivo y conservación de permisos mediante Windows Explorer.

8. Opcionalmente, mientras la tarea está en curso, puede ver su progreso desde el menú desplegable **Tareas en ejecución** en la Core Console, o bien puede ver información detallada en la página **Eventos**. Para obtener más información sobre cómo supervisar eventos de Rapid Recovery, consulte Visualización de eventos mediante las páginas de tareas, alertas y del diario.

Desmontaje de puntos de recuperación

Realice los pasos de este procedimiento para desmontar los puntos de recuperación que están montados localmente en el Core.

NOTE: Cuando desmonte un punto de recuperación montado de forma remota, esta acción se denomina desconexión.

1. En la Rapid Recovery Core Console, en la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Montajes**.

   Aparecerá la página **Montajes**. Hay un panel para Montajes locales (puntos de recuperación montados en el Core) y otro para Montajes remotos (puntos de recuperación montados con Local Mount Utility). En cada panel, los puntos de recuperación montados correspondientes aparecen en una lista.

2. Para desmontar los montajes locales, en el panel **Montajes locales**, haga lo siguiente:

   a. Seleccione el punto o puntos de montaje local que desea desmontar.

   - Para desmontar todos los puntos de recuperación, haga clic en la casilla de verificación de la barra de título de la tabla Montajes locales para seleccionar todos los puntos de montaje.
   - Para desmontar uno o varios puntos de recuperación, haga clic en la casilla de verificación en la primera columna de cada fila que represente el punto de montaje que desea desconectar.

   b. Haga clic en **Desmontar**.

   Aparece un cuadro de diálogo de confirmación.

   c. Haga clic para confirmar que desea desmontar los puntos de recuperación seleccionados.

   Los puntos de recuperación locales se desmontan.

NOTE: Si las alertas del sistema están habilitadas, podría ver una alerta sobre que los puntos de montaje adecuados se están desmontando.

3. Para desconectar los puntos de recuperación montados de forma remota, haga lo siguiente en el panel **Montajes remotos**:
   a. Seleccione el punto o puntos de montaje remotos que desea desconectar.
   - Para desconectar todos los puntos de recuperación, haga clic en la casilla de verificación de la barra de título de la tabla Montajes remotos para seleccionar todos los puntos de montaje.
   - Para desconectar uno o varios puntos de recuperación, haga clic en la casilla de verificación en la primera columna de cada fila que represente el punto de montaje que desea desconectar.

   b. Haga clic en **Desconectar**.

   Aparece un cuadro de diálogo de confirmación.

   c. Haga clic para confirmar que desea desconectar los puntos de recuperación seleccionados.

   Los puntos de recuperación locales se desconectan.

   NOTE: Si las alertas del sistema están habilitadas, podría ver una alerta sobre que los puntos de montaje adecuados se están desconectando.

4. Confirme que los puntos de recuperación montados anteriormente ya no aparecen en las listas Montajes locales o Montajes remotos, según proceda.

Trabajo con puntos de recuperación de Linux

El método admitido y recomendado para montar y desmontar puntos de recuperación desde un equipo protegido con Linux es emplear la utilidad **local_mount**.

Estos procedimientos se dirigen específicamente al uso de local_mount para montar y desmontar puntos de recuperación de Linux.

NOTE: Para administrar los puntos de recuperación de Linux de cualquier otra forma, consulte Administración de instantáneas y puntos de recuperación, ya que cualquier otro tipo de administración se puede realizar desde la Core Console.

- Montaje de un volumen de punto de recuperación en un equipo Linux
- Desmontaje de un volumen de punto de recuperación en un equipo Linux

Montaje de un volumen de punto de recuperación en un equipo Linux

Mediante la utilidad local_mount de Rapid Recovery, puede montar un volumen de forma remota desde un punto de recuperación como volumen local, en un equipo con Linux.

NOTE: Al realizar este procedimiento, no intente montar puntos de recuperación en la carpeta /tmp, que contiene los archivos aavdisk.

1. Cree un nuevo directorio para montar el punto de recuperación (por ejemplo, puede utilizar el comando `mkdir`).
2. Verifique que el directorio existe (por ejemplo, utilizando el comando `ls`).
3. Ejecute la utilidad local_mount de Rapid Recovery como raíz, o como superusuario, por ejemplo:

   ```
   sudo local_mount
   ```
4. En la solicitud de montaje de Rapid Recovery, 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 Rapid Recovery Core.
6. Introduzca las credenciales de inicio de sesión para el servidor de Core, es decir, el nombre de usuario y la contraseña.

   Se mostrará una lista de los equipos protegidos por el servidor de Rapid Recovery. Cada equipo se identifica con lo siguiente: número de elemento de línea, host/dirección IP y número de ID del equipo.

   Por ejemplo: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba
7. Introduzca el siguiente comando para enumerar los puntos de recuperación disponibles actualmente para un equipo especificado:

   ```
   lr <número_línea_de_equipo>
   ```

   NOTE: Tenga en cuenta que también puede introducir el número de ID del equipo en este comando en lugar del número de elemento de línea.

   Aparecerá una lista con los puntos de recuperación base e incrementales de ese equipo. Esta lista incluye un número de elemento de línea, fecha y marca de tiempo, ubicación del volumen, tamaño del punto de recuperación y número de ID del volumen que incluye un número secuencial al final, que identifica al punto de recuperación.

   Por ejemplo, 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2
8. Introduzca el comando siguiente para seleccionar y montar el punto de recuperación especificado en el punto o la ruta de acceso de montaje que especifique.

   ```
   m <número_ID_punto_recuperación_volumen> <letra-volumen> [indicador]
   <ruta_de_acceso>
   ```

   El indicador en el comando determina cómo montar el punto de recuperación. Puede utilizar una de las siguientes opciones:

   - [r] - montar como solo lectura (predeterminado). Este indicador le permite montar un punto de recuperación pero no le permite realizar cambios en él.
   - [w] - montar como de lectura. Este indicador le permite montar el punto de recuperación y le permite realizar cambios en él.
   - [v] - montar con escrituras anteriores. Al montar con el indicador “v” le permite montar el punto de recuperación e incluir cualquier cambio que se realizara durante el anterior montaje de escritura pero que no están presentes en el punto de recuperación.
   - [n] - no montar nbd en <ruta_de_acceso>. Un nbd (dispositivo de bloque de red) realiza una conexión de socket entre el Core y el equipo protegido cuando realizar un montaje local. Este indicador le permite montar el punto de recuperación sin montar el nbd, lo que resulta útil si desea comprobar manualmente el sistema de archivos del punto de recuperación.

NOTE: También puede especificar un número de línea en el comando en lugar del número de ID del punto de recuperación para identificar al punto de recuperación. En ese caso, utilizaría el número de línea del equipo (desde la salida lm), seguido por el número de línea del punto de recuperación y la letra del volumen, seguido por la ruta de acceso, de este modo: m <número_de_línea_del_equipo> <número_de_línea_del_punto_de_recuperación> <letra_del_volumen> <ruta_de_acceso>. Por ejemplo, si la salida de `lm` enumera tres equipos protegidos, y especifica el comando `lr` para el número 2 y monta el volumen b del punto de recuperación número veintitrés en /tmp/mount_dir, el comando sería:

```
m 2 23 b /tmp/mount_dir
```

NOTE: Si desea montar un volumen BTRFS desde un sistema operativo compatible (consulte el tema "Matriz de compatibilidad e instalación del sistema operativo para la versión 6.1 de Rapid Recovery" en la Rapid Recovery Installation and Upgrade Guide [Guía de instalación y actualización de Rapid Recovery]), a continuación, debe incluir los parámetros siguientes:

```
mount -o nodatasum,device=/dev/xxx /dev/xxx /mnt/yyy
```

9. Para verificar que el montaje se ha realizado correctamente, introduzca el siguiente comando, que debería enumerar el volumen remoto adjunto:

   ```
   l
   ```

Desmontaje de un volumen de punto de recuperación en un equipo Linux

Realice los pasos de este procedimiento para ver la información detallada del sistema de un equipo Linux.

1. Ejecute la utilidad local_mount de Rapid Recovery como raíz, o como superusuario, por ejemplo:

   ```
   sudo local_mount
   ```

2. En la solicitud de montaje de Rapid Recovery, 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 del Rapid Recovery Core.
4. Introduzca las credenciales de inicio de sesión, es decir, el nombre de usuario y la contraseña, para este servidor Core.

   Se mostrará una lista de los equipos protegidos por el servidor de Rapid Recovery Core.

5. Introduzca el siguiente comando para enumerar los puntos de recuperación disponibles actualmente para un equipo especificado:

   ```
   lr <número_línea_de_equipo>
   ```

   NOTE: Tenga en cuenta que también puede introducir el número de ID del equipo en este comando en lugar del número de elemento de línea.

   Aparecerá una lista con los puntos de recuperación base e incrementales de ese equipo. Esta lista incluye: número de elemento de línea, fecha/marca de tiempo, ubicación del volumen, tamaño del punto de recuperación y número de identificación del volumen que incluye un número secuencial al final, que identifica al punto de recuperación.

   Por ejemplo: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2

6. Ejecute el comando `l or list` para obtener una lista de dispositivos NBD (Network Block Device, dispositivo de bloque de red) montados. Si monta cualquier punto de recuperación, obtendrá una ruta de acceso a un dispositivo NBD después de ejecutar el comando `l or list`.
7. Introduzca el siguiente comando para desmontar un punto de recuperación.

```
unmount <path_of_nbd-device>
```

8. Ejecute el comando `l or list` para comprobar que el desmontaje del punto de recuperación se realizó con éxito.

Cómo forzar una instantánea

Forzar una instantánea permite forzar una transferencia de datos para el equipo protegido actual. Cuando se fuerza una instantánea, la transferencia se inicia inmediatamente o se agrega a la cola si se están ejecutando otros trabajos.

Puede elegir entre dos tipos de instantáneas.

Si selecciona una instantánea incremental y no existe ningún punto de recuperación anterior, se captura una imagen base. Forzar una instantánea no cambia el calendario de las instantáneas de programación.

NOTE: Rapid Recovery admite Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016 tanto para transferencias base como para transferencias incrementales.

- Una imagen base es una instantánea de todos los datos en los volúmenes seleccionados del equipo.
- Una instantánea incremental captura todos los datos que se han modificado desde la última instantánea.

1. En la Core Console de Rapid Recovery, desplácese hasta el equipo o el clúster con el punto de recuperación para el que quiera forzar una instantánea.
2. En la página Resumen, haga clic en **Forzar instantánea**.

   Aparecerá el cuadro de diálogo Forzar instantánea.
3. En el cuadro de diálogo Forzar instantánea, en la casilla de verificación, haga clic en uno o más volúmenes, o grupos de protección.
4. Haga clic en **Forzar instantánea** o en Forzar imagen base, respectivamente.
5. Si ha seleccionado una imagen base, haga clic para confirmar que desea tomar una imagen base.

   Una imagen base puede tardar un tiempo considerable, en función de la cantidad de datos en los volúmenes de los que desea realizar una copia de seguridad.
   La instantánea que ha seleccionado se pone en cola y comienza en cuanto finalizan otros trabajos.

Eliminación de puntos de recuperación

Puede quitar fácilmente del repositorio los puntos de recuperación de un equipo concreto. Cuando elimine puntos de recuperación de Rapid Recovery, puede especificar una de las opciones siguientes.

- **Eliminar todos los puntos de recuperación**. Quita todos los puntos de recuperación para el equipo protegido del repositorio.
- **Eliminar un rango de puntos de recuperación**. Quita todos los puntos de recuperación de un rango especificado antes del actual, hasta e incluida la imagen base, que son todos los datos del equipo, así como todos los puntos de recuperación después del actual hasta la imagen base siguiente.

NOTE: No puede recuperar los puntos de recuperación que haya eliminado. Si necesita los datos almacenados en los puntos de recuperación, considere archivar primero los datos.

1. En la Rapid Recovery Core Console, bajo el menú **Equipos protegidos**, haga clic en el nombre o dirección IP del equipo del que desea ver y quitar los puntos de recuperación.

   Aparecerá la vista Resumen para el equipo protegido seleccionado.
2. Junto al nombre del equipo o la dirección IP, haga clic en el menú **Puntos de recuperación**.

Aparece la página **Puntos de recuperación** para el equipo seleccionado.

3. Desplácese hasta el panel **Puntos de recuperación**.

   Las opciones aparecen bajo el título del panel, incluidas Actualizar, Eliminar rango y Eliminar todo.

4. Para eliminar todos los puntos de recuperación almacenados actualmente, bajo el título del panel Puntos de recuperación, haga clic en **Eliminar todo** y, en el cuadro de diálogo de confirmación, haga clic en Confirmar eliminación.
5. Para eliminar un conjunto de puntos de recuperación en un rango de datos específico, haga lo siguiente:
   a. Bajo el título del panel Puntos de recuperación, haga clic en **Eliminar rango**.

   Aparece el cuadro de diálogo **Eliminar puntos de recuperación dentro del rango**.

   b. En el cuadro de diálogo **Eliminar puntos de recuperación dentro del rango**, seleccione en el campo **Desde** la fecha y la hora desde las que desea empezar a eliminar puntos de recuperación.
   c. En el campo **Hasta**, seleccione la fecha y la hora que definan el último punto de recuperación que desea eliminar.
   d. Haga clic en **Eliminar**.
   e. Haga clic en el cuadro de diálogo de confirmación para confirmar la eliminación.

Eliminación de una cadena de puntos de recuperación huérfanos

Un punto de recuperación huérfano es una instantánea incremental que no está asociada a una imagen base. Las instantáneas posteriores siguen generándose en este punto de recuperación; sin embargo, sin la imagen base, los puntos de recuperación resultantes están incompletos y es poco probable que contengan los datos necesarios para completar una recuperación. Estos puntos de recuperación se consideran parte de la cadena de puntos de recuperación huérfanos. Si se produce esta situación, la mejor solución es eliminar la cadena y crear una nueva imagen base.

Para obtener más información sobre cómo forzar una imagen base, consulte Cómo forzar una instantánea.

1. En la Rapid Recovery Core Console, desplácese hasta el equipo protegido cuya cadena de puntos de recuperación huérfanos quiera eliminar.
2. En el menú de la parte superior de la página, haga clic en **Puntos de recuperación**.
3. En el panel de Puntos de recuperación, amplíe el punto de recuperación huérfano.

   Este punto de recuperación está etiquetado en la columna Tipo como “Incremental, huérfano”.

4. Junto a Acciones, haga clic en **Eliminar**.

   Aparecerá la ventana Eliminar puntos de recuperación.

5. En la ventana Eliminar puntos de recuperación, haga clic en **Sí**.

> **CAUTION: Al eliminar este punto de recuperación se elimina toda la cadena de puntos de recuperación, incluidos los puntos de recuperación incrementales que se produzcan antes o después del mismo, hasta la siguiente imagen base. Esta operación no puede deshacerse.**
>
> **CAUTION: La cadena de puntos de recuperación huérfanos se eliminará.**

Migración de puntos de recuperación manual a un repositorio diferente

Si desea retirar los puntos de recuperación de un equipo protegido desde un repositorio sin eliminarlos, puede migrarlos a un repositorio diferente manualmente mediante este procedimiento. Este proceso implica archivar puntos de recuperación del repositorio de origen e importar el archivo al repositorio de destino.

Por ejemplo, puede realizar este procedimiento si su repositorio existente está completo o si sus necesidades cambian y quiere proteger un equipo con un Core y un repositorio diferentes.

CAUTION: Si su repositorio se ha actualizado previamente desde AppAssure **5.3 o 5.4 y ha utilizado la replicación,** Quest **recomienda que ejecute el trabajo Comprobación de repositorio en cada repositorio del Core de destino antes de la migración. Realizar este trabajo impedirá copiar las irregularidades de los datos al nuevo repositorio de destino. El trabajo de comprobación de repositorio solo está disponible en la UI si se puede aplicar a su Core y podría tardar una cantidad sustancial de tiempo en ejecutarse. Para obtener información sobre este trabajo, consulte Acerca de la comprobación de la integridad de los repositorios DVM. Para obtener información sobre cómo realizar este trabajo, consulte Realizar una comprobación de integridad en un repositorio DVM.**

1. En la Core Console de Rapid Recovery, pause la protección de los equipos protegidos cuyos puntos de recuperación quiere migrar. Para obtener más información, consulte Puesta en pausa y reanudación de la protección.
2. Cancele todas las operaciones en curso en los equipos protegidos cuyos puntos de recuperación quiere migrar o espere a que se hayan completado totalmente.
3. Archive los puntos de recuperación del equipo o equipos en los que ha realizado una pausa. Para obtener más información, consulte Creación de una archivación.
4. Tras archivar y verificar el archivo, elimine los puntos de recuperación existentes del equipo protegido que quiere migrar. Para obtener más información, consulte Eliminación de puntos de recuperación.

   NOTE: Si no elimina los puntos de recuperación existentes, no puede cambiar los repositorios de un equipo protegido.
5. Cree un repositorio nuevo para los puntos de recuperación migrados o asegúrese de que existe un nuevo repositorio de destino. Para obtener más información, consulte Creación de un repositorio DVM.
   - Si desea utilizar un repositorio existente, vaya al paso 6.
6. Cambie el repositorio de cada equipo en el que realizó una pausa completando los siguientes pasos:
   a. En la Core Console, haga clic en el equipo protegido en el árbol de navegación.
   b. En la página **Resumen** del equipo protegido, haga clic en **Configuración**.
   c. En la página **Configuración**, en el panel **General**, haga clic en la lista desplegable **Repositorio** y, a continuación, seleccione el nombre del repositorio que creó en el paso 4.
   - Si desea utilizar un repositorio existente, seleccione el nombre de un repositorio existente.

     NOTE: Cuando migre puntos de recuperación a un repositorio existente, asegúrese de que el repositorio existente tiene espacio libre suficiente para contener los puntos de recuperación migrados.

d. Haga clic en **Aceptar**.

7. Reanude la protección del equipo o equipos en los que realizó una pausa. Para obtener más información, consulte Puesta en pausa y reanudación de la protección.
8. Tome una nueva imagen base para cada equipo protegido que haya trasladado. Para obtener más información, consulte Cómo forzar una instantánea y utilice la opción Forzar imagen base.
9. Importe los datos archivados para los equipos que desee migrar. Para obtener más información, consulte Importación de un archivo.

Replicación

Esta sección describe cómo configurar y administrar la replicación de datos protegidos desde un Core de origen de Rapid Recovery en un Core de destino de Rapid Recovery para la recuperación de desastres.

Replicación con Rapid Recovery

En esta sección se proporciona información de conceptos y procedimientos que le ayudará a entender y configurar la replicación en Rapid Recovery.

La **replicación** es el proceso de copia de puntos de recuperación de un Rapid Recovery Core y de transmisión de los mismos a otro Rapid Recovery Core con fines de recuperación tras desastres. El proceso requiere la existencia de una relación de emparejamiento origen-destino entre dos o más Cores.

El Core de origen copia los puntos de recuperación de los equipos protegidos designados y, a continuación, transmite de forma asíncrona y continua los datos de la instantánea al Core de destino.

A menos que cambie el comportamiento predeterminado al configurar una programación de replicación, el Core debe iniciar un trabajo de replicación inmediatamente después de la finalización de cada copia de seguridad de la instantánea, comprobación de suma de comprobación, comprobación de capacidad de montaje y comprobación de capacidad de conexión. El truncamiento de registros de cualquier tipo también desencadena un trabajo de replicación, así como la comprobación de la integridad de puntos de recuperación o de una base de datos de Oracle. Si alguna de estas acciones está incluida en trabajos nocturnos, al finalizar dichos trabajos nocturnos también se desencadena un trabajo de replicación. Para obtener más información, consulte Programación de la replicación.

NOTE: Cuando replica datos para un clúster, debe replicar todo el clúster. Por ejemplo, si selecciona un nodo para replicar, el clúster se selecciona automáticamente. De forma similar, si selecciona el clúster, todos los nodos de dicho clúster también se seleccionan.

Para lograr una seguridad de los datos óptima, los administradores por lo general utilizan un Core de destino en un sitio de recuperación tras desastres remoto. Puede configurar la replicación de salida en un centro de datos de propiedad de la empresa o en un sitio de recuperación tras desastres remoto (es decir, un Core de destino administrado automáticamente). Otra opción es configurar la replicación de salida en un proveedor de servicio gestionado por terceros (MSP) o proveedor de Nube que aloja copias de seguridad y servicios de recuperación de desastres en una ubicación externa. Al replicar en 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 está gestionada por equipos protegidos. Se puede configurar cualquier equipo (o todos los equipos) protegido o replicado en un Core de origen para replicar en un Core de destino.

Estos son algunos de los posibles escenarios para replicación:

- **Replicación a una ubicación local.** El Core de destino está en un centro de datos local o una ubicación in situ, y la replicación se mantiene en todo momento. En esta configuración, la pérdida del Core no impediría una recuperación.
- **Replicación a una ubicación externa.** El Core de destino se ubica en un lugar externo de recuperación tras desastres remoto, en caso de pérdida.
- **Replicación mutua.** Dos centros de datos en dos ubicaciones distintas, cada una de ellas con un Core, y que son equipos de protección y sirven como copia de seguridad de recuperación externa entre sí, en caso

de desastre. En este caso, cada Core replica los equipos protegidos en el Core que se encuentra en el otro centro de datos.

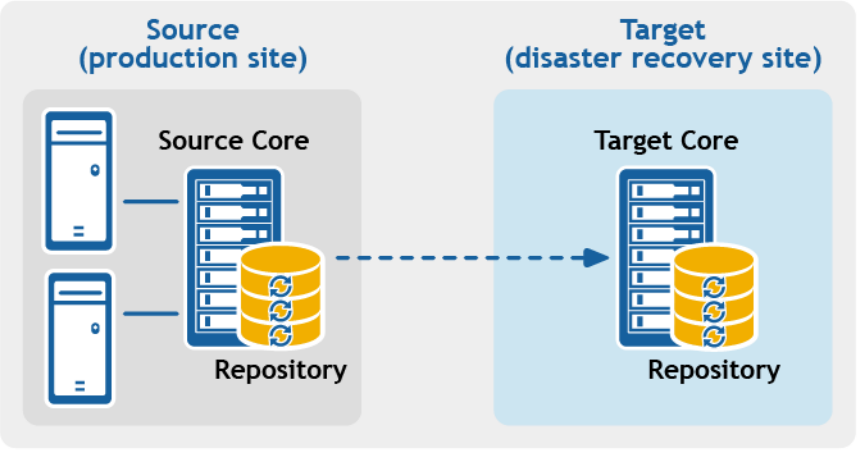
- **Replicación alojada y en nube.** Los socios de MSP de Rapid Recovery mantienen varios Cores de destino en un centro de datos o en una nube pública. En cada uno de estos Cores, el socio MSP permite a uno o más de sus clientes replicar puntos de recuperación desde un Core de origen del sitio del cliente en el Core del destino del MSP, siendo un servicio de pago.

  NOTE: En esta situación, los clientes solo tienen acceso a sus propios datos.

Estas son algunas de las configuraciones posibles de replicación:

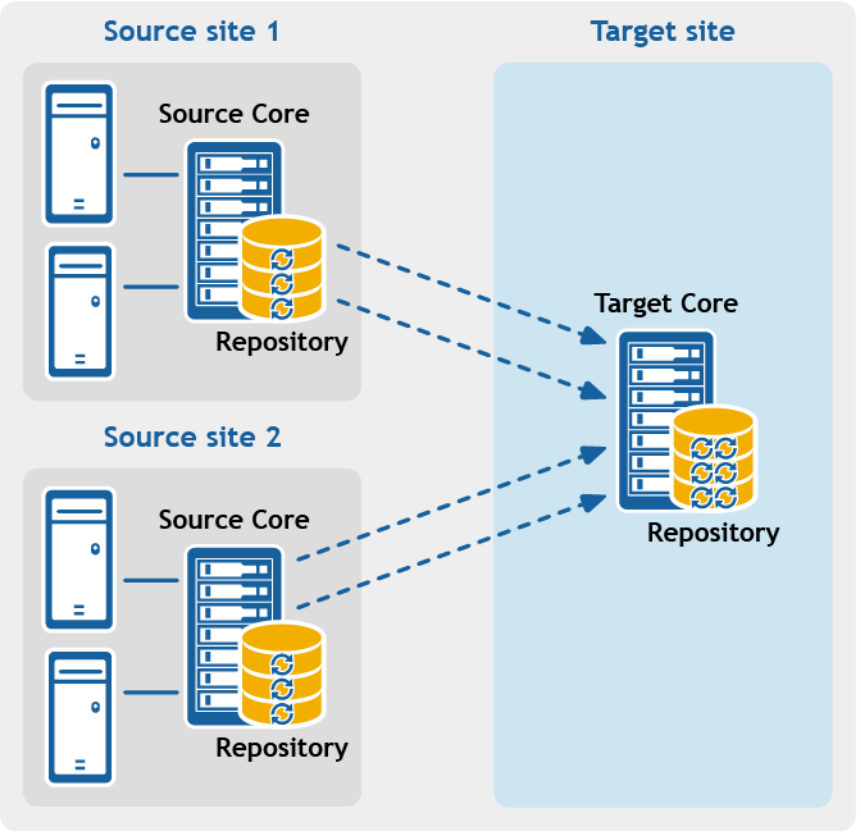
- **Replicación de punto a punto**. Replica uno o más equipos protegidos desde un Core de origen único a un Core de destino único.

Figura 1. Configuración de la replicación de punto a punto



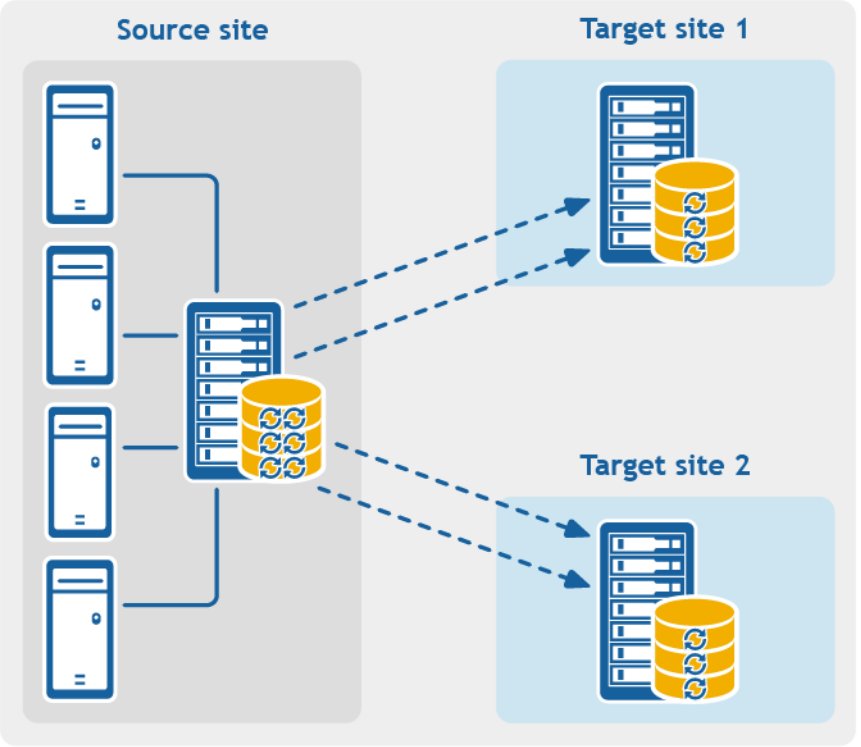
- **Replicación de multipunto a punto.** Replica los equipos protegidos de varios Cores de origen en un único Core de destino.

Figura 2. Configuración de la replicación de multipunto a punto.



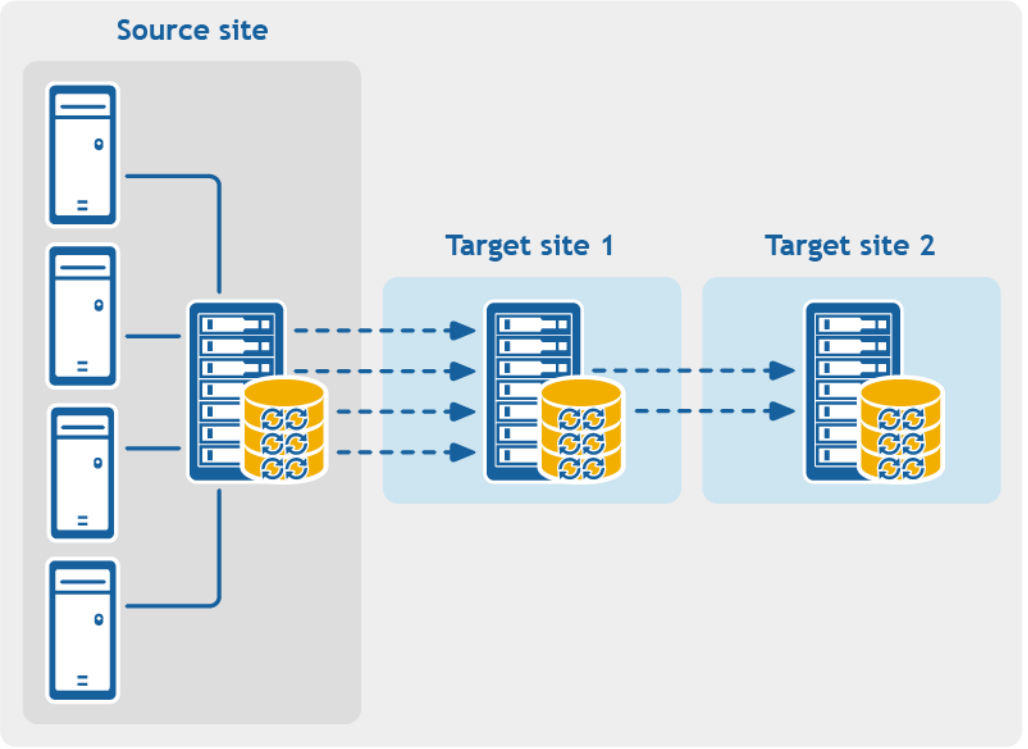
- **Replicación de punto a multipunto**. Replica uno o más equipos protegidos desde un Core de origen único a más de un Core de destino.

Figura 3. Configuración de la replicación de punto a multipunto



- **Replicación de salto múltiple.** Replica uno o más equipos protegidos desde un Core de destino a otro Core de destino, lo que produce opciones de conmutación por error o recuperación adicionales en el Core replicado.

Figura 4. Configuración de replicación de salto múltiple



Si se utilizan dispositivos de copia de seguridad de la serie DL, el Core de destino en el que replica debe disponer de una licencia de software válida configurada. Estos dispositivos de hardware incluyen una licencia de destino de replicación con la compra. Compruebe la clave de licencia en el mensaje de correo electrónico de bienvenida que recibió cuando adquirió el dispositivo. Para obtener ayuda, visite el sitio web de Asistencia con las licencias en https://support.quest.com/contact-us/licensing o envíe un correo electrónico a license@quest.com.

Cadenas del punto de recuperación y huérfanos

Rapid Recovery captura instantáneas de un equipo protegido y guarda los datos en un repositorio como punto de recuperación. El primer punto de recuperación guardado en el Core se denomina imagen base. La imagen base incluye el sistema operativo, las aplicaciones y las configuraciones de cada volumen que elija proteger, así como todos los datos de dichos volúmenes. Las copias de seguridad posteriores son instantáneas incrementales, que constan solo de datos modificados en los volúmenes protegidos desde la realización de la última copia de seguridad. La imagen base más todas las instantáneas incrementales forman una cadena de puntos de recuperación completa.

Desde una cadena de puntos de recuperación completa, podrá restaurar los datos con facilidad y confianza, mediante la utilización de la gama completa de opciones de recuperación disponible para Rapid Recovery. Estas opciones incluyen la restauración a nivel de archivos, a nivel de volumen y la restauración bare metal restore.

Debido a que lógicamente no puede realizar una restauración de datos que no existen, en el caso de una cadena de puntos de recuperación incompleta, no podrá restaurar los datos a nivel de volumen ni realizar una restauración bare metal restore. En tales casos, todavía podrá restaurar todos los datos que haya en un punto de recuperación a nivel de archivos.

Si la información que desea restaurar desde un punto de recuperación se encuentra en una copia de seguridad anterior que no está disponible en el Core (una instantánea incremental anterior o la imagen base), se dice que el punto de recuperación es huérfano. Los puntos de recuperación huérfanos son los típicos de algunos escenarios de replicación.

Por ejemplo, la primera vez que establece la replicación, las opciones para la restauración de datos desde los puntos de recuperación replicados son limitadas. Hasta que todos los datos de la copia de seguridad del Core de origen se transmitan al Core de destino, mediante la creación de cadenas de puntos de recuperación completas de los huérfanos, solo podrá realizar restauración a nivel de archivos.

Cuando comienza una replicación

De forma predeterminada, el Core pone automáticamente a los trabajos de transferencia de replicación en cola inmediatamente después de que se complete cada transferencia de copias de seguridad programadas con regularidad. Por lo tanto, a menos que el calendario de programación de replicación de un equipo protegido esté personalizado, se basará en su calendario de programación de instantáneas de copias de seguridad estándar.

La primera vez que configure la replicación, si hay uno o más puntos de recuperación en el Core de origen, el proceso de replicación se iniciará inmediatamente, a menos que:

- Seleccione la opción para pausar la replicación inicialmente o
- Seleccione la opción para utilizar una unidad de inicialización para realizar la transferencia inicial.

Si pausa la replicación inicialmente, esta se iniciará al reanudar explícitamente la replicación.

Si configura la replicación y especifica el uso de una unidad de inicialización, la replicación en el Core de destino se iniciará con la siguiente instantánea de copias de seguridad programadas con regularidad.

NOTE: Puede forzar una copia de seguridad del equipo protegido tras establecer la replicación. Esto hace que se inicie la replicación inmediatamente después de completarse la instantánea del equipo protegido.

Si especifica una unidad de inicialización al configurar la replicación, solo se replicarán las transferencias de copias de seguridad futuras. Si desea que haya puntos de recuperación existentes del equipo protegido en el Core de destino, deberá inicializar los datos desde el equipo protegido. Para inicializar datos, cree una unidad de inicialización desde el Core de origen y, a continuación, consuma la unidad de inicialización en el Core de destino.

También puede personalizar el calendario de programación de replicación de un equipo protegido. Por ejemplo, si utiliza el calendario de programación de protección predeterminado de una copia de seguridad por hora, podrá especificar que el Core de origen replique en el Core de destino en un calendario de programación diferente (por ejemplo, una vez al día a las 02:00).

Determinación de la estrategia y necesidades de inicialización

Los temas siguientes analizan la restauración a partir de datos replicados y la necesidad de inicializar datos del punto de recuperación desde el Core de origen.

Cuando es necesaria la inicialización de datos

La primera vez que establezca la replicación, a menos que especifique el uso de una unidad de inicialización, el Core de origen empezará a transmitir todos los puntos de recuperación de los equipos seleccionados al Core de destino. La transmisión de datos a través de la red puede tardar mucho tiempo. Los factores que intervienen incluyen la velocidad de la red, la solidez de la arquitectura de red y la cantidad de datos que se transmiten al

Core de destino. Por ejemplo, si los datos de la copia de seguridad son 10 GB y el enlace WAN transfiere a 24 Mbps, la transferencia podría tardar más de una hora en completarse.

En función de la cantidad de información que desee copiar en el Core de destino, la unidad de inicialización podría llegar a agregar hasta cientos o miles de gigabytes de datos. Muchas empresas deciden no consumir el ancho de banda de la red necesario y optan por definir y consumir una unidad de inicialización. Para obtener más información, consulte Consideraciones de rendimiento para la transferencia de datos replicados.

Si especifica el uso de una unidad de inicialización al definir la replicación, solo los puntos de recuperación guardados en el Core de origen después de haber establecido la replicación se replicarán en el Core de destino. Las copias de seguridad guardadas en el Core de origen antes de que se estableciera la replicación no estarán presentes en el Core de destino hasta que inicialice de forma explícita los datos, mediante el proceso siguiente.

Para evitar la ralentización de la red a causa de una transferencia intensiva de datos históricos, inicialice los datos de la copia de seguridad previa en el Core de destino mediante una **unidad de inicialización**. Una unidad de inicialización es un archivo de archivos comprimidos que **copia** un conjunto de imágenes base desduplicadas e instantáneas incrementales desde el Core de origen. El archivo de la unidad de inicialización contiene el conjunto completo de puntos de recuperación previos de los equipos protegidos que desee replicar desde el Core de origen al Core de destino.

Mueva el archivo de la unidad de inicialización a un volumen de almacenamiento que, posteriormente, pueda poner a disposición del Core de destino. A continuación, **consuma** la información de la unidad de inicialización. Para ello, es necesario adjuntar el volumen con imagen de la unidad de inicialización en el Core de destino e importar los datos en el repositorio de la Core Console. En este proceso se reparan los huérfanos mediante la unión de instantáneas incrementales replicadas al Core de destino con sus imágenes base, para formar una o más cadenas de puntos de recuperación completas. Este proceso a veces se denomina copiar-consumir.

Los datos de inicialización del Core de origen no siempre son necesarios. Por ejemplo:

- Si va a configurar la replicación para un nuevo Core de Rapid Recovery, no es necesaria la inicialización.
- Si los datos de instantáneas anteriores no son críticos para los datos replicados y solo necesita recuperar los datos guardados después de la configuración de la replicación, la inicialización no será necesaria.

  NOTE: En este caso, Quest recomienda capturar una nueva imagen base inmediatamente antes o después de configurar la replicación. Este paso asegura que haya una cadena de puntos de recuperación completa en el Core de destino desde el que poder restaurar los datos en el futuro.
- Si capturó una imagen base inmediatamente antes de configurar la replicación y solo tiene la necesidad de restaurar a partir de los datos capturados después de dicha fecha, no será necesaria la inicialización.
- Si configuró la replicación sin especificar una unidad de inicialización, los datos de la instantánea se transmitirán a través de la red desde el Core de origen al Core de destino.

Si se da alguna de estas situaciones, la inicialización de datos no será necesaria. En tales casos, la replicación se puede completar es su totalidad desde el Core de origen.

Si configuró la replicación de un Core con puntos de recuperación existentes y es posible que sea necesario restaurarla en el nivel del volumen, que desee realizar una restauración BMR o que desee restaurar los datos desde una imagen base o instantánea incremental anterior, la inicialización será necesaria. En estos casos, tenga en cuenta las necesidades de inicialización y la estrategia. Revise la información incluida en este tema y decida si va a inicializar en el Core de destino y qué método utilizará.

Métodos de inicialización de datos

Si desea que los equipos replicados en un Core de destino tengan acceso a los datos guardados previamente en el Core de origen, inicialice el Core de destino mediante uno de los métodos siguientes:

1. **Inicialización en el Core de destino a través de una conexión de red.** Especifique el uso de una unidad de inicialización cuando defina la replicación. A continuación, podrá compartir la carpeta que contiene la unidad de inicialización con el Core de destino y consumir el archivo de unidad de inicialización a través de la red. Para transferir grandes cantidades de datos o para conexiones lentas, este método de inicialización podría tardar una cantidad considerable de tiempo y consumir una cantidad importante de ancho de banda de la red.

NOTE: Quest no recomienda la inicialización de grandes cantidades de datos a través de una conexión de red. La primera inicialización puede llegar a implicar cantidades de datos muy grandes, que saturen una conexión WAN típica.

2. **Transferencia de datos de la copia de seguridad desde el Core de origen mediante medios de almacenamiento físicos.** Transfiera el archivo de unidad de inicialización a un dispositivo portátil, externo y extraíble de almacenamiento. Normalmente, este método es útil para grandes conjuntos de datos o lugares con conexiones de red lentas. La inicialización mediante este método requiere que se realicen los pasos siguientes:
   a. Crear un archivo de inicialización desde el Core de origen y guardarlo en los medios extraíbles.
   b. Transportar la unidad de inicialización a la ubicación física del Core de destino.
   c. Adjuntar la unidad al Core de destino.
   d. Consumir los datos de la unidad de inicialización en el repositorio del Core de destino.

   Si se replica en un Core de terceros, una vez el MSP haya recibido su medio, por lo general, un representante del centro de datos adjuntará dicho medio y le notificará cuando esté listo para que pueda consumir (o importar) los datos de inicialización en el Core.

   NOTE: Como hay que copiar grandes cantidades de datos al dispositivo de almacenamiento, se recomienda usar una conexión eSATA, USB 3.0 u otra de alta velocidad. Si el tamaño total del archivo de datos de inicialización es mayor que el espacio disponible en el medio extraíble, el archivo podrá exportarse a través de varios dispositivos.
3. **Transferencia de datos de una copia de seguridad mediante disco duro virtual en Cores de origen y de destino almacenados en hosts virtuales.** Si el Core de origen y de destino se encuentran en un host virtual, podrá definir y consumir una unidad de inicialización en un medio de almacenamiento virtual. La inicialización mediante este método requiere que se realicen los pasos siguientes:
   a. Cree un archivo de unidad de inicialización desde el Core de origen y guárdelo en un volumen de almacenamiento virtual.
   b. Desconecte el volumen del Core de origen y adjúntelo al Core de destino.
   c. Consumir los datos de la unidad de inicialización en el repositorio del Core de destino.

NOTE: Aunque se puede producir la replicación de instantáneas incrementales entre los Cores de origen y destino antes de que se complete la inicialización, las instantáneas replicadas que se transmiten del origen al destino quedarán huérfanas hasta que se consuman los datos iniciales y se combinen con las imágenes base replicadas.

Enlaces relacionados

- Para obtener información detallada sobre el proceso de consumo de la unidad de inicialización, consulte el tema Consumo de la unidad de inicialización en un Core de destino.
- Para obtener más información sobre los puntos de recuperación huérfanos, consulte Eliminación de una cadena de puntos de recuperación huérfanos.
- Para obtener más información sobre cómo preparar una unidad de inicialización, consulte Comprensión de unidades de inicialización y Consumo de la unidad de inicialización en un Core de destino.

See also: Consumo de la unidad de inicialización en un Core de destino
See also: Eliminación de una cadena de puntos de recuperación huérfanos

Consideraciones de rendimiento para la transferencia de datos replicados

Si el ancho de banda entre los Cores de origen y destino no puede dar servicio a la transferencia de puntos de recuperación almacenados, configure la replicación y especifique el uso de una unidad de inicialización. Este proceso inicia el Core de destino con imágenes base y puntos de recuperación de los servidores seleccionados

protegidos en el Core de origen. El proceso de inicialización se puede realizar en cualquier momento. La inicialización se puede realizar como parte de la transferencia inicial de datos, que sirve como base para la replicación programada regularmente. También puede inicializar datos para un equipo replicado anteriormente si la replicación se ha pausado o eliminado. En este caso, la opción "Crear cadenas de puntos de recuperación" permite copiar puntos de recuperación no replicados aún en una unidad de inicialización.

Cuando se prepare para la replicación, tenga en cuenta los factores siguientes:

- **Velocidad de cambio.** La velocidad de cambio es la velocidad a la que se acumula la cantidad de datos protegidos. La velocidad depende de la cantidad de datos que cambian en los volúmenes protegidos y el intervalo de protección de los volúmenes. Algunos tipos de máquinas, por lo general, tienen una mayor velocidad de cambio, como un servidor de correo electrónico Exchange. Una forma de reducir la velocidad de cambio es reducir el intervalo de protección.
- **Ancho de banda.** El ancho de banda es la velocidad de transferencia disponible entre el Core de origen y el Core de destino. Es fundamental que el ancho de banda sea mayor que la velocidad de cambio, para que la replicación pueda ajustarse a los puntos de recuperación creados por las instantáneas. En el caso de las transferencias de datos grandes de Core a Core, podrían ser necesarias varias secuencias en paralelo para que el rendimiento en velocidad pueda alcanzar la conexión Ethernet de 1GB Ethernet.

  NOTE: El ancho de banda que los ISP especifican es, por lo general, el ancho de banda disponible total. Todos los dispositivos en la red comparten el ancho de banda saliente. Asegúrese de que hay libre ancho de banda suficiente para que la replicación pueda dar servicio a la velocidad de cambios.
- **Número de equipos protegidos.** Es importante tener en cuenta el número de equipos protegidos por Core de origen, y cuántos tiene pensado replicar en el destino. No es obligatorio que se replique cada equipo protegido en el Core de origen; Rapid Recovery permite replicar según equipos protegidos, así que puede elegir replicar solo algunos equipos, si así lo desea. Si todos los equipos protegidos en un Core de origen se deben replicar, la velocidad de cambio es, por lo general, superior. Este factor es relevante si el ancho de banda entre los Cores de origen y destino no es suficiente para la cantidad y el tamaño de los puntos de recuperación que se están replicando.

La opción velocidad de cambios máxima para tipos de conexión WAN aparece en la tabla siguiente, con ejemplos del ancho de banda necesario por gigabyte para una velocidad de cambios razonable.

Tabla 89. Ejemplos de ancho de banda por gigabyte

Banda ancha	Ancho de banda	Velocidad máxima de cambios
DSL	768 Kbps y superior	330MB por hora
Cable	1 Mbps y superior	429MB por hora
T1	1,5 Mbps y superior	644MB por hora
Fibra	20 Mbps y superior	8,38GB por hora

NOTE: Cumpla las recomendaciones que se enumeran en la tabla anterior para obtener resultados óptimos.

Si un enlace falla durante la transferencia de datos, la replicación se reanuda desde el punto de fallo anterior de la transferencia (una vez que se restaura el enlace funcionalmente).

Según su configuración de red, la replicación puede ser un proceso muy largo. Asegúrese de que cuenta con suficiente ancho de banda para alojar la replicación, otras transferencias de Rapid Recovery como las copias de seguridad y cualquier otra de las aplicaciones importantes que debe ejecutar.

Si experimenta problemas al transferir correctamente datos a través de la red, sobre todo en algunos equipos protegidos o replicados, tenga en cuenta el ajuste de la velocidad de transferencia de datos en esos equipos. Para obtener más información, consulteAcerca de la modificación de la configuración de transferencias y Regulación de la velocidad de transferencia.

Acerca de la replicación y los puntos de recuperación cifrados

Aunque la unidad de inicialización no contiene copias de seguridad del registro de Core de origen y certificados, la unidad de inicialización no contiene claves de cifrado del Core de origen si los puntos de recuperación que se replican del origen al destino están cifrados. Los puntos de recuperación replicados permanecerán cifrados después de su transmisión al Core de destino. Los propietarios o administradores del Core de destino necesitan la frase de contraseña para recuperar los datos cifrados.

Acerca de las políticas de retención para replicación

Las políticas de retención en los Cores de destino y origen no están sincronizadas. La recuperación o eliminación a petición se realizan de forma independiente en cada Core con la acción inicial, así como durante la ejecución de los trabajos nocturnos.

Para obtener más información sobre las políticas de retención, consulte Administración de políticas de retención.

Visualización de la replicación entrante y saliente

Si hace clic en el icono **Replicación** de la barra de iconos, aparece la página **Replicación**. Esta página le proporciona una comprensión de la replicación desde el ámbito de este Core. Incluye dos paneles:

- En el panel **Replicación saliente** se muestran los equipos protegidos en este Core que se replican en otro Core.
- En el panel **Replicación entrante** se muestran los equipos replicados en este Core y el Core de origen del que se replican dichos equipos.

En esta sección se describe la información que se muestra en los paneles.

La información sobre la replicación saliente desde este Rapid Recovery Core se describe en la tabla siguiente.

Tabla 90. Información sobre replicación saliente

Elemento de la IU	Descripción
Seleccionar elemento	Para cada fila de la tabla de resumen, puede seleccionar la casilla de verificación para realizar acciones de la lista de opciones del menú situada encima de la tabla.
Tipo	Muestra el tipo de protección. Puede expandir un Core de destino para mostrar equipos replicados individuales.
Indicador de estado	El estado de la replicación. Los círculos coloreados de la columna Estado muestran si un equipo replicado dispone de conexión o no está accesible. Si pasa el cursor sobre el círculo coloreado, se muestra la condición de estado. Las condiciones de estado

Elemento de la IU	Descripción
	incluyen los colores verde (replicación establecida y con conexión), amarillo (replicación en pausa), rojo (error de autenticación) y gris (sin conexión o no accesible).
Nombre de replicación	El nombre mostrado del equipo de Core a los que los equipos de este Core de origen se replican.
Equipos	Muestra el número de equipos replicados en el Core de destino seleccionado.
Sincronización	La fecha y hora de la última transferencia de replicación al Core de destino.
•••	Al hacer clic en el menú desplegable Más de esta columna, verá una lista de acciones que podrá realizar para modificar la relación de replicación específica.

Puede realizar acciones sobre dos o más de los Cores enumerados en la cuadrícula de replicación saliente. Para realizar acciones en diversos Cores de destino, seleccione la casilla de verificación de cada Core en la cuadrícula y, a continuación, desde el menú de encima de dicha cuadrícula, puede seleccionar la acción que desee realizar. Puede realizar las acciones que se describen en la tabla siguiente.

Tabla 91. Acciones globales disponibles en el panel de replicación saliente

Elemento de la IU	Descripción
Agregar Core de destino	Le permite definir otro Core de destino para replicar equipos protegidos en este Core de origen.
Actualizar	Se actualiza la información mostrada en la tabla.
Forzar	Fuerza la replicación.
Realizar pausa	Se pausa la replicación establecida.
Reanudar	Se reanuda la replicación en pausa.
Copiar	Se abre el Asistente para replicación, que le permite copiar puntos de recuperación existentes de equipos protegidos seleccionados en una unidad de inicialización.
Eliminar	Se elimina la replicación saliente.
Unidades de inicialización	Esta opción de menú aparece si los datos se copiaron en una unidad de inicialización cuando se configuró la replicación. Se muestra la información sobre el archivo de unidad de inicialización, que incluye la fecha y hora en la que se guardó la unidad de inicialización. Los menús que pueden contraerse indican el Core de destino y los equipos protegidos desde los que se generaron los archivos de unidad de inicialización.
•••	Al hacer clic en el menú desplegable Más de esta columna, verá una lista de acciones que podrá realizar para modificar la relación de replicación específica.

La información sobre la replicación entrante desde otro Core se describe en la tabla siguiente.

Tabla 92. Información sobre la replicación entrante

Elemento de la IU	Descripción
Seleccionar elemento	Para cada fila de la tabla de resumen, puede seleccionar la casilla de verificación para realizar acciones de la lista de opciones del menú situada encima de la tabla.
Tipo	Muestra el tipo de protección. Puede expandir un Core de origen para mostrar equipos replicados individuales.
Indicador de estado	El estado de la replicación. Los círculos coloreados de la columna Estado muestran si un equipo replicado dispone de conexión o no está accesible. Si pasa el cursor sobre el círculo coloreado, se muestra la condición de estado. Las condiciones de estado incluyen los colores verde (replicación establecida y con conexión), amarillo (replicación en pausa), rojo (error de autenticación) y gris (sin conexión o no accesible).
Nombre de replicación	El nombre de visualización del equipo del Core de origen que contiene los equipos protegidos que se replican en este Core de destino. Este nombre se podrá especificar de manera opcional al establecer la replicación en el Core de origen mediante el Asistente para replicación.
Equipos	Se muestran el número de equipos protegidos en el Core de origen que se replican en este Core de destino.
Sincronización	La fecha y hora de la última transferencia de replicación del Core de origen.
	Al hacer clic en el menú desplegable Más de esta columna, verá una lista de acciones que podrá realizar para modificar la relación de replicación específica.

Puede realizar acciones sobre dos o más de los Cores de origen enumerados en la cuadrícula de replicación entrante. Para realizar acciones en diversos Cores de origen, seleccione la casilla de verificación de cada Core en la cuadrícula y, a continuación, desde el menú de encima de dicha cuadrícula, puede seleccionar la acción que desee realizar. Puede realizar las acciones que se describen en la tabla siguiente.

Tabla 93. Acciones globales disponibles en el panel replicación entrante

Elemento de la IU	Descripción
Actualizar	Se actualiza la información mostrada en la tabla.
Forzar	Fuerza la replicación.
Realizar pausa	Se pausa la replicación establecida.
Reanudar	Se reanuda la replicación en pausa.
Eliminar	Se elimina la replicación entrante.

Configuración de la replicación

Para replicar datos utilizando Rapid Recovery, debe configurar los Cores de origen y destino para la replicación. Después de configurar la replicación, puede replicar los datos del equipo protegido, monitorizar y administrar la replicación y realizar la recuperación.

NOTE: Cuando replica datos para un clúster, debe replicar todo el clúster. Por ejemplo, si selecciona un nodo para replicar, el clúster se selecciona automáticamente. De forma similar, si selecciona el clúster, todos los nodos de dicho clúster también se seleccionan.

La replicación en Rapid Recovery implica realizar las siguientes operaciones:

- Configurar un repositorio en el Core de destino. Para obtener más información sobre cómo agregar un repositorio al Core de destino, consulte Creación de un repositorio DVM.
- Configurar una replicación administrada automáticamente. Para obtener más información sobre cómo replicar en un Core de destino administrado automáticamente, consulte Replicación en un Core de destino administrado automáticamente.
- Configurar una replicación de terceros. Para obtener más información sobre cómo replicar en otro Core de destino, consulte Replicación en un Core de destino externo.
- Replicar un equipo protegido existente. Para obtener más información sobre cómo replicar un equipo protegido que ya está protegido por el Core de origen, consulte Cómo agregar un equipo a una replicación existente.
- Consumir la unidad de inicialización. Para obtener más información sobre cómo consumir los datos de la unidad de inicialización en el Core de destino, consulte Consumo de la unidad de inicialización en un Core de destino.
- Establecer la prioridad de replicación para un equipo protegido. Para obtener más información sobre cómo priorizar la replicación de equipos protegidos, consulte Cómo establecer la prioridad de replicación para un equipo protegido.
- Establecer la programación de replicación para un equipo protegido. Para obtener más información sobre cómo establecer un calendario de programación de replicación, consulte Programación de la replicación.
- Supervisar replicación según sea necesario. Para obtener más información sobre la supervisión de la replicación, consulte Visualización de la replicación entrante y saliente.
- Administrar las configuraciones de replicación según sea necesario. Para obtener más información sobre la administración de los ajustes de replicación, consulte Administración de configuraciones de replicación.
- Recuperar datos replicados en caso de desastre o pérdida de datos. Para obtener más información sobre la recuperación de datos replicados, consulte Recuperación de datos replicados.

Replicación en un Core de destino administrado automáticamente

Esta configuración se aplica a replicación a una ubicación externa y a replicación mutua. Los pasos siguientes son requisitos previos:

- El Rapid Recovery Core debe estar instalado en todos los equipos de origen y destino.
- Si configura Rapid Recovery para replicación multipunto a punto, debe realizar esta tarea en todos los Cores de origen y en el único Core de destino. Para ver las descripciones de estas configuraciones de replicación, consulte Replicación.
- Si necesita crear una unidad de inicialización y transferirla a un volumen de almacenamiento extraíble físico para realizar la transferencia inicial de puntos de recuperación existentes, debe tener un dispositivo de almacenamiento portátil adecuado preparado. También debe tener acceso físico al equipo del Core de origen, para adjuntar la unidad para copiar el archivo comprimido de la unidad de inicialización.
- Si utiliza una unidad de inicialización en un Core de destino administrado automáticamente, usted o el administrador de confianza deben tener acceso físico al Core de destino.

Un Core de destino administrado automáticamente es aquel al que tiene acceso. Por ejemplo, un Core administrado automáticamente a menudo está administrado por su compañía en una ubicación externa o está alojado en una ubicación geográfica distinta a la del Core de origen. La replicación se puede configurar completamente en un Core de origen, a no ser que elija inicializar sus datos con una unidad de inicialización. En esos casos, deberá crear una unidad de inicialización mediante este procedimiento y, posteriormente, adjuntar la unidad de inicialización en el Core de destino para consumir los datos del punto de recuperación archivado. Para obtener más información, consulte Determinación de la estrategia y necesidades de inicialización.

Complete los pasos del siguiente procedimiento para configurar su Core de origen, que se replicará en un Core de destino administrado automáticamente.

1. Vaya a la Rapid Recovery Core Console del Core de origen.
2. En la barra de botones, haga clic en **Replicar**.

   Aparece el **Asistente para replicación**.
3. En la página **Core de destino** del Asistente para replicación, si está estableciendo la replicación con un Core de destino que se ha emparejado anteriormente con este Core de origen, seleccione **Utilizar un Core de destino existente** y, a continuación, seleccione el Core de destino apropiado en la lista desplegable. Vaya al paso 5
4. En la página **Core de destino** del Asistente para replicación, si está estableciendo la replicación con un Core de destino de este Core de origen por primera vez, debe seleccionar **Tengo mi propio Core de destino** y, a continuación, introducir la información según se describe en la tabla siguiente.

Tabla 94. Información del Core de destino

Cuadro de texto	Descripción
Nombre de host	Escriba el nombre de host o dirección IP del equipo del Core en la que está replicando.
Puerto	Introduzca el número de puerto en el que el Rapid Recovery Core se comunicará con el equipo. El número de puerto predeterminado es 8006.

Cuadro de texto	Descripción
Nombre de usuario	Introduzca el nombre de usuario para acceder al equipo.
Contraseña	Escriba la contraseña para acceder al equipo.

5. Haga clic en **Siguiente**.

   NOTE: Si no hay ningún repositorio en el Core de destino, aparece un mensaje de advertencia que le indica que puede emparejar el Core de origen con el de destino, pero que no puede replicar los Agents (equipos protegidos) en esta ubicación hasta que no se establezca un repositorio. Para obtener más información acerca de cómo configurar un repositorio principal para un Core, consulte Creación de un repositorio DVM.

6. En la página **Solicitud**, introduzca un nombre para esta configuración de replicación; por ejemplo, SourceCore1. Este es el nombre para mostrar que se utiliza en el panel Replicación entrante en la página Replicación del Core de destino.
7. Haga clic en **Siguiente**.
8. En la página **Equipos protegidos**, seleccione los equipos protegidos que desea replicar y, a continuación, utilice las listas desplegables de la columna Repositorio para seleccionar un repositorio para cada equipo protegido.
9. Si desea realizar el proceso de inicialización para la transferencia de los datos de base, realice los siguientes pasos. Si no desea inicializar los datos, continúe con el paso siguiente.

   NOTE: Como hay que copiar grandes cantidades de datos al dispositivo de almacenamiento portátil, Quest recomienda el uso de una conexión eSATA, USB 3.0 u otra de alta velocidad con el dispositivo de almacenamiento portátil.

   a. En la página **Equipos protegidos** del Asistente para replicación, seleccione **Utilizar una unidad de inicialización para realizar la transferencia inicial**.

   - Si actualmente tiene uno o varios equipos protegidos replicando en un Core de destino, puede incluirlos en la unidad de inicialización seleccionando **Incluya los puntos de recuperación ya replicados en la unidad de inicialización**.
   - Si no desea que la replicación comience de inmediato tras completar este procedimiento, seleccione **Pausar replicación inicialmente**.

     NOTE: Si selecciona esta opción, la replicación no empezará hasta que se reanude explícitamente. Para obtener más información, consulte Pausa y reanudación de la replicación.

   b. Haga clic en **Siguiente**.
   c. En la página **Ubicación de la unidad de inicialización** del asistente para replicación, utilice la lista desplegable **Tipo de ubicación** para seleccionar los siguientes tipos de destino:

   - Local
   - Red
   - Nube

   d. En el campo Ubicación, introduzca los detalles para el archivo de la unidad de inicialización según se describen en la tabla siguiente en función del tipo de ubicación que haya seleccionado en el paso c.

Tabla 95. Detalles de archivación

Opción	Cuadro de texto	Descripción
Local	Ubicación de salida	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo

Opción	Cuadro de texto	Descripción
		comprimido de la unidad de inicialización; por ejemplo, `D:\work\archive`.
Red	Ubicación de salida	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo comprimido de la unidad de inicialización; por ejemplo, `\\servername\sharename`.
	Nombre de usuario	Escriba un nombre de usuario. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
	Contraseña	Escriba una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable. **NOTE:** Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de la carpeta	Introduzca un nombre para la carpeta en la que hay que guardar los datos archivados. El nombre predeterminado es Rapid-Recovery-Archive-[FECHA CREACIÓN]-[HORA CREACIÓN]

e. Haga clic en **Siguiente**.

f. En la página **Opciones de la unidad de inicialización** del Asistente para replicación, introduzca la información según lo descrito en la siguiente tabla.

Tabla 96. Opciones de la unidad de inicialización

Elemento	Descripción
Tamaño máximo	Los grandes archivos de datos se pueden dividir en varios segmentos. Seleccione el tamaño máximo del segmento que desea reservar para crear la unidad de inicialización realizando una de las siguientes acciones: • Seleccione **Destino completo** para reservar todo el espacio disponible en la ruta de acceso proporcionada en la página Ubicación de la unidad de inicialización para un uso futuro. Por ejemplo, si la ubicación es `D:\work\archive`, todo el espacio disponible en la unidad D: se reserva si es obligatorio copiar la unidad de inicialización, pero no se reserva inmediatamente después de iniciar el proceso de copia. • Seleccione el cuadro de texto, introduzca una cantidad y, a continuación, seleccione una unidad de medida en la lista desplegable para personalizar el espacio que desea reservar. El valor predeterminado es 250MB.

Elemento	Descripción
Acción de reciclaje	En el caso de que la ruta de acceso ya contenga una unidad de inicialización, seleccione una de las opciones siguientes: • **No reutilizar**. No sobrescribe ni borra datos de inicialización existentes de la ubicación. Si la ubicación no está vacía, la escritura en la unidad de inicialización fallará. • **Reemplazar este Core**. Sobrescribe los datos de inicialización que ya existan y que pertenezcan a este Core, pero deja intactos los datos del resto de Cores. • **Borrar completamente**. Borra todos los datos de inicialización del directorio antes de escribir en la unidad de inicialización.
Comentario	Introduzca un comentario que describa la unidad de inicialización.
Agregar todos los Agents a la unidad de inicialización	Seleccione esta opción para replicar todos los equipos protegidos en el Core de origen usando la unidad de inicialización. Esta opción se selecciona de forma predeterminada.
Crear cadenas de puntos de recuperación (reparar huérfanos)	Seleccione esta opción para replicar toda la cadena de puntos de recuperación en la unidad de inicialización. Con este proceso se agregan puntos de recuperación ya replicados a la unidad de inicialización, lo que evita que se creen huérfanos. Esta opción se selecciona de forma predeterminada. **NOTE:** La inicialización típica en AppAssure 5.4 replicaba únicamente el último punto de recuperación en la unidad de inicialización, lo que reducía la cantidad de tiempo y espacio necesarios para crear la unidad de inicialización. La opción para crear las cadenas del punto de recuperación en la unidad de inicialización necesita suficiente espacio en la unidad de inicialización como para almacenar los últimos puntos de recuperación desde los equipos protegidos especificados y puede llevar más tiempo.

g. Realice uno de los siguientes pasos:

- Si ha desactivado la casilla de verificación **Agregar todos los Agents a la unidad de inicialización**, haga clic en **Siguiente**.
- Si ha seleccionado **Agregar todos los Agents a la unidad de inicialización**, vaya al paso 10.

10. Haga clic en **Finalizar**.
11. Si ha creado una unidad de inicialización, envíela a su Core de destino.

    El emparejamiento del Core de origen y el de destino ha finalizado.

A menos que haya seleccionado la opción para realizar pausa en la protección inicialmente, el proceso de replicación se inicia inmediatamente.

1. Si ha seleccionado la opción para utilizar una unidad de inicialización, la replicación produce puntos de recuperación huérfanos en el Core de destino hasta que la unidad de inicialización se consume y proporciona las imágenes de base necesarias.
2. Si ha especificado el uso de una unidad, transfiera el archivo del archivo comprimido de la unidad de inicialización a un volumen (carpeta compartida, disco virtual o dispositivo de almacenamiento extraíble). A continuación, consuma la unidad de inicialización.

See also: Incorporación de una cuenta de nube
See also: Creación de un repositorio DVM
See also: Replicación con Rapid Recovery
See also: Determinación de la estrategia y necesidades de inicialización
See also: Replicación

Replicación en un Core de destino externo

Un Core de terceros es un Core de destino administrado y mantenido por un proveedor de servicios administrados (MSP). La replicación en un Core administrado por un tercero no exige que el cliente tenga acceso al Core de destino.

El proceso de replicación en un Core de terceros implica que el cliente lleve a cabo algunas tareas, así como la otra empresa. Después de que un cliente envíe una solicitud para la replicación del Core o Cores de origen, el proveedor de servicios administrados (MSP) debe completar la configuración en el Core de destino revisando la solicitud.

NOTE: Esta configuración se aplica a replicación alojada y en nube. El Core de Rapid Recovery debe estar instalado en todos los equipos de origen. Si configura Rapid Recovery para la replicación multipunto a punto, debe realizar esta tarea en todos los Cores de origen.

Para replicar en un Core de destino administrado por un tercero, complete las siguientes tareas:

- Envío de una solicitud de replicación a un proveedor de servicios de terceros
- Revisión de una solicitud de replicación de un cliente
- Cómo ignorar una solicitud de replicación de un cliente

Envío de una solicitud de replicación a un proveedor de servicios de terceros

Si usted es un usuario final que se suscribe a un Core administrado por un tercero, como un proveedor de servicios administrados (MSP), complete los pasos de este procedimiento para enviar una solicitud de replicación a su proveedor de servicios de terceros.

1. Vaya al Core de Rapid Recovery.
2. En barra de botones de iconos, haga clic en **Replicar**.

   Aparece el **Asistente para replicación**.
3. En la página **Target Core** (Core de destino) del Asistente para replicación, seleccione **Tengo una suscripción a un tercero que proporciona servicios de copia de seguridad y recuperación tras desastres remotos** y, a continuación, introduzca la información según se describe en la tabla siguiente.

Tabla 97. Información del Core de destino externo

Cuadro de texto	Descripción
Nombre de host	Escriba el nombre de host, dirección IP o FQDN para el equipo del Core de terceros.
Puerto	Escriba el número de puerto que le indicó el proveedor de servicios de terceros. El número de puerto predeterminado es 8006.

- Si el Core que desea agregar se ha emparejado con este Core de origen anteriormente, puede hacer lo siguiente:

  1. Seleccione **Utilizar un Core de destino existente**.

2. Seleccione el Core de destino de la lista desplegable.
3. Haga clic en **Siguiente**.
4. Vaya al Paso 7.

4. Haga clic en **Siguiente**.
5. En la página **Solicitud** del Asistente para replicación, introduzca la información según se describe en la tabla siguiente.

Tabla 98. Detalles del Core de destino externo

Cuadro de texto	Descripción
Dirección de correo electrónico	Introduzca la dirección de correo electrónico asociada con su suscripción de servicios de terceros.
Id. de cliente (opcional)	Escriba la dirección de correo electrónico de la suscripción y la Id. de cliente que le proporcionó el proveedor de servicios.

6. Haga clic en **Siguiente**.
7. En la página **Equipos protegidos** del Asistente para replicación, seleccione los equipos protegidos que desea replicar en el Core de terceros.
8. Si desea realizar el proceso de inicialización para la transferencia de los datos de base, realice los siguientes pasos.

NOTE: 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 **Equipos protegidos** del Asistente para replicación, seleccione **Use a seed drive to perform initial transfer** (Utilizar una unidad de inicialización para realizar la transferencia inicial).

- Si actualmente tiene uno o varios equipos protegidos replicando en un core de destino, puede incluirlos en la unidad de inicialización seleccionando la opción **Incluya los puntos de recuperación ya replicados en la unidad de inicialización**.

b. Haga clic en **Siguiente**.

c. En la página **Ubicación de la unidad de inicialización** del Asistente para replicación, utilice la lista desplegable tipo de **Ubicación** para seleccionar los tipos de destino siguientes:

- Local
- Red
- Nube

d. En función del tipo de ubicación que haya seleccionado en el Paso c, introduzca los detalles del archivo comprimido según se describe en la tabla siguiente.

Tabla 99. Detalles de archivación

Opción	Cuadro de texto	Descripción
Local	Ubicación de salida	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo comprimido de la unidad de inicialización; por ejemplo, `D:\trabajo\archivación`.
Red	Ubicación de salida	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida

Opción	Cuadro de texto	Descripción
		el archivo comprimido; por ejemplo, `\\nombreservidor\nombrerecursocompartido`.
	Nombre de usuario	Escriba un nombre de usuario. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
	Contraseña	Escriba una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable. **NOTE:** Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de la carpeta	Introduzca un nombre para la carpeta en la que hay que guardar los datos archivados. El nombre predeterminado es Rapid-Recovery-Archive-[FECHA CREACIÓN]-[HORA CREACIÓN]

e. Haga clic en **Siguiente**.

f. En la página **Opciones de la unidad de inicialización** del Asistente de replicación, introduzca la información según se describe en la tabla siguiente.

Tabla 100. Opciones de la unidad de inicialización

Elemento	Descripción
Tamaño máximo	Los grandes archivos de datos se pueden dividir en varios segmentos. Seleccione el tamaño máximo de espacio que desea reservar para crear la unidad de inicialización realizando una de las siguientes acciones: • Seleccione **Todo el destino** para reservar todo el espacio disponible en la ruta de acceso proporcionada en la página Ubicación de unidad de inicialización (por ejemplo, si la ubicación es D:\trabajo\archivo, se reserva todo el espacio disponible en la unidad D:). • 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 que desea reservar.
Acción de reciclaje	En el caso de que la ruta de acceso ya contenga una unidad de inicialización, seleccione una de las opciones siguientes: • **No reutilizar**. No sobrescribe ni borra datos de inicialización existentes de la ubicación. Si la ubicación no está vacía, la escritura en la unidad de inicialización fallará. • **Reemplazar este Core**. Sobrescribe los datos de inicialización que ya existan y que pertenezcan a este Core, pero deja intactos los datos del resto de Cores. • **Borrar completamente**. Borra todos los datos de inicialización del directorio antes de escribir en la unidad de inicialización.

Elemento	Descripción
Comentario	Introduzca un comentario que describa la unidad de inicialización.
Agregar todos los Agents a la unidad de inicialización	Seleccione esta opción para replicar todos los equipos protegidos en el Core de origen usando la unidad de inicialización. Esta opción se selecciona de forma predeterminada.
Crear cadenas de puntos de recuperación (reparar huérfanos)	Seleccione esta opción para replicar toda la cadena de puntos de recuperación en la unidad de inicialización. Esta opción se selecciona de forma predeterminada. **NOTE:** La inicialización típica en AppAssure 5.4 replicaba únicamente el último punto de recuperación en la unidad de inicialización, lo que reducía la cantidad de tiempo y espacio necesarios para crear la unidad de inicialización. La opción para crear las cadenas del punto de recuperación (RP) en la unidad de inicialización necesita suficiente espacio en la unidad de inicialización como para almacenar los últimos puntos de recuperación desde los equipos protegidos especificados y puede llevar más tiempo.

g. Realice uno de los siguientes pasos:

- Si ha desactivado la casilla de verificación **Agregar todos los Agents a la unidad de inicialización**, haga clic en **Siguiente**.
- Si ha seleccionado **Agregar todos los Agents a la unidad de inicialización**, vaya al Paso 9.

h. En la página **Equipos** del Asistente para replicación, seleccione los equipos protegidos que desea replicar en el Core de destino usando la unidad de inicialización.

9. Haga clic en **Finalizar**.
10. Si ha creado una unidad de inicialización, envíela tal y como se lo indique su proveedor de servicios de terceros.

Revisión de una solicitud de replicación de un cliente

Después de que un usuario complete el procedimiento Envío de una solicitud de replicación a un proveedor de servicios de terceros, se envía una solicitud de replicación desde el Core de origen al Core de destino de terceros. Como tercero, puede revisar la solicitud y, a continuación, aprobarla para iniciar la replicación para su cliente. También puede denegarla para evitar que se produzca.

Elija entre las siguientes opciones:

- Aprobación de una solicitud de replicación
- Denegación de una solicitud de replicación

Aprobación de una solicitud de replicación

Complete el siguiente procedimiento para aprobar una solicitud de replicación en un Core de destino de terceros.

1. En el Core de destino, navegue hacia la Rapid Recovery Core Console.
2. Desde la barra de iconos, haga clic en (Replicación).

   Aparece la página **Replicación**.
3. En la página **Replicación**, haga clic en **Solicitud (#)**.

Aparece la sección **Pending Replication Requests (Solicitudes de replicación pendientes)**.

4. En Solicitudes de replicación pendientes, haga clic en el menú desplegable junto a la solicitud que desea revisar y, a continuación, haga clic en **Revisar**.

   Aparecerá la ventana **Review Replication Request (Revisar solicitud de replicación)**.

   NOTE: La información que aparece en la sección Identidad del Core de origen de esta ventana viene determinada por la solicitud completada por el cliente.

5. En Identidad del Core de origen, realice una de las acciones siguientes:

   - Seleccione **Replace an existing replicated Core (Reemplazar un Core replicado existente)**y, a continuación, seleccione un Core en la lista desplegable.
   - Seleccione **Crear un nuevo Core de origen** y, a continuación, confirme que el nombre del Core, la dirección de correo electrónico y la Id. del cliente proporcionados son correctos. Edite la información como sea necesario.

6. En Agents, seleccione los equipos a los que se aplica la aprobación y, a continuación, utilice las listas desplegables de la columna Repositorio para seleccionar el repositorio correspondiente a cada equipo.
7. De forma optativa, en el cuadro de texto **Comentario**, introduzca una descripción o mensaje que se debe incluir en la respuesta al cliente.
8. Haga clic en **Enviar respuesta**.

   Se acepta la replicación.

Denegación de una solicitud de replicación

Complete los pasos en el siguiente procedimiento para denegar una solicitud de replicación a un Core de terceros de un cliente.

Para denegar una solicitud sin revisarla, consulte Cómo ignorar una solicitud de replicación de un cliente.

1. En el Core de destino, navegue hacia la Rapid Recovery Core Console.
2. Desde la barra de iconos, haga clic en (Replicación).

   Aparece la página **Replicación**.

3. En la página **Replicación**, haga clic en **Solicitud (#)**.

   Aparece la sección **Pending Replication Requests (Solicitudes de replicación pendientes)**.

4. En Solicitudes de replicación pendientes, haga clic en el menú desplegable junto a la solicitud que desea revisar y, a continuación, haga clic en **Revisar**.

   Aparecerá la ventana **Review Replication Request (Revisar solicitud de replicación)**.

5. Haga clic en **Denegar**.

   Se deniega la replicación. Aparece una notificación de denegación en Alertas en la pestaña Eventos del Core de origen.

Cómo ignorar una solicitud de replicación de un cliente

Como proveedor de servicios de terceros de un Core de destino, tiene la opción de ignorar una solicitud de replicación enviada por un cliente. Esta opción se puede utilizar si se ha enviado una solicitud por error o si desea denegar una solicitud sin revisarla.

Para obtener más información acerca de las solicitudes de replicación, consulte Revisión de una solicitud de replicación de un cliente.

Complete el siguiente procedimiento para ignorar una solicitud de replicación de un cliente.

1. En el Core de destino, navegue hacia la Rapid Recovery Core Console.
2. Desde la barra de iconos, haga clic en (Replicación).

   Aparece la página **Replicación**.
3. En la página **Replicación**, haga clic en **Solicitud (#)**.

   Aparece la sección **Pending Replication Requests (Solicitudes de replicación pendientes)**.
4. En Solicitudes de replicación pendientes, haga clic en el menú desplegable junto a la solicitud que desea ignorar y, a continuación, haga clic en **Omitir**.
5. En el cuadro de diálogo **Ignorando solicitud**, haga clic en **Sí** para confirmar el comando.

   Se envía la notificación de la omisión de la solicitud al Core de origen y la solicitud se quita de la pestaña Replicación en la pestaña Core.

Cómo agregar un equipo a una replicación existente

Después de que la replicación se haya establecido entre un Core de origen y otro de destino, es posible agregar nuevos equipos protegidos al destino. Complete los pasos del siguiente procedimiento en el Core de origen para agregar un nuevo equipo protegido a un Core de destino emparejado para la replicación.

Para obtener más información sobre la replicación, consulte Replicación y Replicación en un Core de destino administrado automáticamente.

1. Vaya a la Core Console de Rapid Recovery del Core de origen.
2. En la barra de botones, haga clic en **Replicar**.

   Se abre el Asistente para replicación en la página **Equipos protegidos**.
3. En la página **Equipos protegidos**, seleccione los equipos protegidos que desea replicar y, a continuación, utilice las listas desplegables de la columna Repositorio para seleccionar un repositorio para cada equipo protegido.
4. Si desea realizar el proceso de inicialización para la transferencia de los datos de base, realice los siguientes pasos:

   NOTE: 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 **Equipos protegidos** del Asistente para replicación, seleccione **Use a seed drive to perform initial transfer** (Utilizar una unidad de inicialización para realizar la transferencia inicial).

   - Si actualmente tiene uno o varios equipos protegidos replicando en un Core de destino, puede incluirlos en la unidad de inicialización seleccionando la opción **Incluya los puntos de recuperación ya replicados en la unidad de inicialización**.

   b. Haga clic en **Siguiente**.

c. En la página **Ubicación de unidad de inicialización** del asistente, utilice la lista desplegable Tipo de **ubicación** para seleccionar los siguientes tipos de destino:

- Local
- Red
- Nube

d. En función del tipo de ubicación que haya seleccionado en el Paso c, introduzca los detalles para el archivo según se describen en la tabla siguiente.

Tabla 101. Detalles de archivación

Opción	Cuadro de texto	Descripción
Local	Ubicación de salida	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo; por ejemplo, d:\trabajo\archivación.
Red	Ubicación de salida	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo; por ejemplo, \\nombreservidor\nombrerecursocompartido.
	Nombre de usuario	Escriba un nombre de usuario. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
	Contraseña	Escriba una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable. **NOTE:** Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de la carpeta	Introduzca un nombre para la carpeta en la que hay que guardar los datos archivados. El nombre predeterminado es Rapid-Recovery-Archive-[FECHA CREACIÓN]-[HORA CREACIÓN]

e. Haga clic en **Siguiente**.

f. En la página **Opciones de unidad de inicialización** del asistente, introduzca la información según lo descrito en la siguiente tabla.

Tabla 102. Opciones de la unidad de inicialización

Elemento	Descripción
Tamaño máximo	Los grandes archivos de datos se pueden dividir en varios segmentos. Seleccione el tamaño máximo de espacio que desea reservar para crear la unidad de inicialización realizando una de las siguientes acciones: • Seleccione **Todo el destino** para reservar todo el espacio disponible en la ruta de acceso proporcionada en la página Ubicación de unidad de inicialización

Elemento	Descripción
	(por ejemplo, si la ubicación es D:\trabajo\archivo, se reserva todo el espacio disponible en la unidad D:). • 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 que desea reservar.
Acción de reciclaje	En el caso de que la ruta de acceso ya contenga una unidad de inicialización, seleccione una de las opciones siguientes: • No reutilizar. No sobrescribe ni borra datos de inicialización existentes de la ubicación. Si la ubicación no está vacía, la escritura en la unidad de inicialización fallará. • Reemplazar este Core. Sobrescribe los datos de inicialización que ya existan y que pertenezcan a este Core, pero deja intactos los datos del resto de Cores. • Borrar completamente. Borra todos los datos de inicialización del directorio antes de escribir en la unidad de inicialización.
Comentario	Introduzca un comentario que describa la unidad de inicialización.
Agregar todos los Agents a la unidad de inicialización	Seleccione esta opción para replicar todos los equipos protegidos en el Core de origen usando la unidad de inicialización. Esta opción se selecciona de forma predeterminada.
Crear cadenas de puntos de recuperación (reparar huérfanos)	Seleccione esta opción para replicar toda la cadena de puntos de recuperación en la unidad de inicialización. Esta opción se selecciona de forma predeterminada. **NOTE:** La inicialización típica de Rapid Recovery 5.4 solo replica el último punto de recuperación en la unidad de inicialización, lo que reduce la cantidad de tiempo y espacio necesarios para crear la unidad de inicialización. La opción para crear las cadenas del punto de recuperación (RP) en la unidad de inicialización necesita suficiente espacio en la unidad de inicialización como para almacenar los últimos puntos de recuperación desde los equipos protegidos especificados y puede llevar más tiempo.

g. Realice uno de los siguientes pasos:

- Si ha desactivado la casilla de verificación **Agregar todos los Agents a la unidad de inicialización**, haga clic en **Siguiente**.
- Si ha seleccionado **Agregar todos los Agents a la unidad de inicialización**, vaya al Paso 5.

h. En la página **Equipos protegidos** del asistente, seleccione los equipos protegidos que desea replicar en el Core de destino usando la unidad de inicialización.

5. Haga clic en **Finalizar**.

Consumo de la unidad de inicialización en un Core de destino

Complete el siguiente procedimiento para consumir los datos del archivo de la unidad de inicialización en el Core de destino.

NOTE: Este procedimiento solo es necesario si se ha creado una unidad de inicialización como parte de las secciones Replicación en un Core de destino administrado automáticamente o Replicación en un Core de destino externo.

1. Si el archivo de la unidad de inicialización se ha guardado en un dispositivo de almacenamiento portátil, como una unidad USB, conecte la unidad al Core de destino.
2. En el Core de destino, abra la Rapid Recovery Core Console y, en la barra de iconos, haga clic en (Replicación).

   Aparece la página **Replicación**.
3. En la página **Replicación**, en Replicación entrante, haga clic en el menú desplegable para el Core de origen correcto y, a continuación, seleccione **Consumir**.

   Aparecerá el cuadro de diálogo **Consumir**.
4. En el campo **Tipo de ubicación**, seleccione una de las siguientes opciones de la lista desplegable:
   - Local
   - Red
   - Nube
5. Introduzca los detalles para el archivo comprimido de la unidad de inicialización según se describen en la tabla siguiente en función del tipo de ubicación que haya seleccionado en el paso 4.

Tabla 103. Detalles de archivación

Opción	Cuadro de texto	Descripción
Local	Ubicación	Introduzca la ruta de acceso para el archivo.
Red	Ubicación	Introduzca la ruta de acceso para el archivo.
	Nombre de usuario	Escriba el nombre de usuario. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
	Contraseña	Escriba una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable. **NOTE:** Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de la carpeta	Introduzca el nombre de la carpeta en la que se guardan los datos archivados; por ejemplo, Archivo-Rapid-Recovery-[FECHA CREACIÓN]-[HORA CREACIÓN]

6. Haga clic en **Comprobar archivo**.

   El Core busca el archivo.

   Después de encontrar el archivo, aparecen los siguientes cuadros de texto en la ventana Consumir prerrellenados con los datos recogidos del paso 4, paso 5, y el archivo. En Rango de fechas aparecen

las fechas del punto de recuperación más reciente y más antiguo contenido en la unidad de inicialización. Cualquier comentario introducido al crear la unidad de inicialización se importa automáticamente.

7. En el cuadro de diálogo **Consumir**, en Agents, seleccione los equipos en los que desea consumir datos.
8. Haga clic en **Consumir**.
9. Para supervisar el progreso del consumo de datos, vea la página Eventos.

Abandono de una unidad de inicialización

Si crea una unidad de inicialización con la intención de consumirla en el Core de destino, pero más tarde opta por no consumirla, puede abandonar la unidad de inicialización.

Hasta que abandona la unidad de inicialización o la consume, un vínculo a dicha unidad de inicialización pendiente permanecerá en el panel Replicación saliente en el Core de origen.

Hasta que transmita información de la unidad de inicialización, los puntos de recuperación huérfanos (que existen en el equipo protegido original, pero no en el Core de destino) no se pueden utilizar para restaurar los datos.

CAUTION: Si abandona la unidad de inicialización, los puntos de recuperación originales (definidos en el archivo de la unidad de inicialización) se transmiten por la red hasta el Core de destino durante el siguiente trabajo de replicación. La transmisión de los puntos de recuperación antiguos a través de la red podría ralentizar la red considerablemente, sobre todo si hay muchos puntos de recuperación.

Complete los pasos del procedimiento siguiente para abandonar una unidad de inicialización pendiente.

NOTE: El abandono de la unidad de inicialización en la Core Console no afecta al archivo de la unidad de inicialización desde su ubicación de almacenamiento.

1. En el Core de origen, abra la Rapid Recovery Core Console y, en la barra de iconos, haga clic en (Replicación).

   Aparece la página **Replicación**.
2. En la página **Replicación**, en el panel Replicación saliente, haga clic en **Unidades de inicialización (#)**.

   En el panel Replicación saliente, una sección aparece con información acerca de las unidades de inicialización pendientes.
3. De manera opcional, haga clic en la flecha para expandir el menú que puede contraerse.

   Aparecerá la información acerca de las unidades de inicialización pendientes, incluido el Core de destino y el rango de fechas de los puntos de recuperación incluidos en la unidad de inicialización.
4. Para el archivo de la unidad de inicialización que desea abandonar, haga clic en (Más opciones) y, a continuación, seleccione **Abandonar**.
5. En la ventana de confirmación, confirme que desea abandonar la unidad de inicialización.

   Se quita la unidad de inicialización.

   Si no existen más unidades de inicialización en el Core de origen, el enlace Unidades de inicialización (#) y la sección del mismo nombre se quitan del panel Replicación saliente.

Administración de configuraciones de replicación

Rapid Recovery le permite monitorizar, programar y ajustar la replicación en los niveles general, de Core y de equipo protegido.

Puede editar la siguiente configuración de replicación:

- Para configurar los siguientes trabajos de replicación, consulte Programación de la replicación.
- Para crear una unidad de inicialización de un equipo protegido que ya está emparejado para la replicación, consulte Uso de la función de copia para crear una unidad de inicialización
- Para supervisar el progreso de un trabajo de replicación, consulte Visualización de la replicación entrante y saliente.
- Para pausar o reanudar un trabajo de replicación, consulte Pausa y reanudación de la replicación.
- Para forzar la replicación de un equipo protegido saliente o entrante, consulte Forzado de la replicación.
- Para administrar la configuración de todos los Cores de destino y los procedimientos de replicación, consulte Administración de configuración para la replicación saliente.
- Para administrar la configuración de un Core de destino individual, consulte Cambio de la configuración del Core de destino.
- Para administrar la configuración de prioridad para un equipo protegido en concreto replicado en un Core de destino, consulte Cómo establecer la prioridad de replicación para un equipo protegido.

Programación de la replicación

A menos que cambie el comportamiento predeterminado al configurar una programación de replicación, el Core debe iniciar un trabajo de replicación inmediatamente después de la finalización de cada copia de seguridad de la instantánea, comprobación de suma de comprobación, comprobación de capacidad de conexión y los trabajos nocturnos.

Puede realizar cambios en el calendario de programación de replicación para reducir la carga de la red.

Complete los pasos del procedimiento siguiente para establecer un calendario de programación de replicación para cualquier equipo replicado.

1. En el Core de destino, abra la Rapid Recovery Core Console y, en la barra de iconos, haga clic en (Replicación).

   Aparece la página **Replicación**.

2. En el panel Replicación saliente, en el Core para el que desea programar la replicación, haga clic en (Más opciones) y, a continuación, seleccione **Programar**.

   Se abrirá el cuadro de diálogo **Calendario de programación de replicación de [NombreCore]**.

3. Seleccione una de las tres opciones siguientes:

   - **En todo momento**. Se replica después de cada nueva instantánea, de la comprobación de suma de comprobación y de la comprobación de conectabilidad y después de que se completen los trabajos nocturnos.
   - **Diario (solo inicia la replicación durante el periodo de tiempo especificado)**. Comienza a replicar únicamente durante el rango de tiempo proporcionado.

     1. En el cuadro de texto **Desde**, introduzca la hora más reciente en la que se puede producir la replicación.
     2. En el cuadro de texto **Hasta**, introduzca la hora más tardía en la que se puede producir la replicación.

        NOTE: Si la replicación está en curso cuando termine el tiempo programado, el trabajo de replicación se completará tras el periodo de tiempo asignado.

   - **Personalizado**. La replicación solo se inicia en el intervalo de tiempo proporcionado, lo que le permite establecer un intervalo de tiempo para los días laborables y otro para los fines de semana.

1. Junto a Días de la semana, en el cuadro de texto **Desde**, introduzca la hora más reciente en la que se puede realizar la replicación entre semana y, a continuación, en el cuadro de texto **Hasta**, introduzca la hora más tardía en la que se puede realizar la replicación entre semana.
2. Junto a Días de la semana, en el cuadro de texto **Desde**, introduzca la hora más reciente en la que se debe producir la replicación durante los fines de semana; a continuación, en el cuadro de texto **Hasta**, introduzca la hora más tardía en la que se debe producir la replicación durante los fines de semana.

4. Haga clic en **Guardar**.

   El calendario de programación se aplica a todas las replicaciones del Core de destino seleccionado.

Uso de la función de copia para crear una unidad de inicialización

Si seleccionó no crear una unidad de inicialización cuando configuró la replicación, puede crear una unidad de inicialización utilizando la función de copia en el menú desplegable del equipo protegido.

1. En el Core de origen, abra la Rapid Recovery Core Console y, en la barra de iconos, haga clic en (Replicación).

   Aparece la página **Replicación**.
2. En la página **Replicación**, en el panel Replicación saliente, haga clic en para expandir el Core que protege el equipo en el que desee crear una unidad de inicialización.

   La selección se expande para mostrar cada equipo protegido especificado en el Core.
3. Haga clic en la primera fila de la tabla para seleccionar cada una de las máquinas para las que desea crear una unidad de inicialización.
4. En el menú del panel Replicación saliente, haga clic en **Copiar**.

   Aparece el **Asistente para replicación**.
5. En la página **Ubicación de unidad de inicialización** del asistente, utilice la lista desplegable **Ubicación** para seleccionar los siguientes tipos de destino:
   - Local
   - Red
   - Nube
6. Introduzca los detalles para el archivo comprimido de la unidad de inicialización según se describen en la tabla siguiente en función del tipo de ubicación que haya seleccionado en el paso anterior.

Tabla 104. Detalles de archivación

Opción	Cuadro de texto	Descripción
Local	Ubicación de salida	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo; por ejemplo, d:\trabajo \archivación.
Red	Ubicación de salida	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo; por ejemplo, \ \nombreservidor\nombrerecursocompartido.
	Nombre de usuario	Escriba un nombre de usuario. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.

Opción	Cuadro de texto	Descripción
	Contraseña	Escriba una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable. **NOTE:** Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de la carpeta	Introduzca un nombre para la carpeta en la que hay que guardar los datos archivados. El nombre predeterminado es Rapid-Recovery-Archive-[FECHA CREACIÓN]-[HORA CREACIÓN]

7. Haga clic en **Siguiente**.
8. En la página Opciones de unidad de inicialización, introduzca la información según lo descrito en la siguiente tabla.

Tabla 105. Opciones de la unidad de inicialización

Elemento	Descripción
Tamaño máximo	Los grandes archivos de datos se pueden dividir en varios segmentos. Seleccione el tamaño máximo de espacio que desea reservar para crear la unidad de inicialización realizando una de las siguientes acciones: • Seleccione **Todo el destino** para reservar todo el espacio disponible en la ruta de acceso proporcionada en la página Ubicación de unidad de inicialización (por ejemplo, si la ubicación es D:\trabajo\archivo, se reserva todo el espacio disponible en la unidad D:). • 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 que desea reservar.
Acción de reciclaje	En el caso de que la ruta de acceso ya contenga una unidad de inicialización, seleccione una de las opciones siguientes: • **No reutilizar.** No sobrescribe ni borra datos de inicialización existentes de la ubicación. Si la ubicación no está vacía, la escritura en la unidad de inicialización fallará. • **Reemplazar este Core**. Sobrescribe los datos de inicialización que ya existan y que pertenezcan a este Core, pero deja intactos los datos del resto de Cores. • **Borrar completamente**. Borra todos los datos de inicialización del directorio antes de escribir en la unidad de inicialización.
Comentario	Introduzca un comentario que describa la unidad de inicialización.
Agregar todos los Agents a la unidad de inicialización	Seleccione esta opción para replicar todos los equipos protegidos en el Core de origen usando la unidad de inicialización. Esta opción se selecciona de forma predeterminada.

Elemento	Descripción
Crear cadenas de puntos de recuperación (reparar huérfanos)	Seleccione esta opción para replicar toda la cadena de puntos de recuperación en la unidad de inicialización. Esta opción se selecciona de forma predeterminada. **NOTE:** La inicialización típica de Rapid Recovery 5.4 solo replicaba el último punto de recuperación en la unidad de inicialización, lo que reducía la cantidad de tiempo y espacio necesarios para crear la unidad de inicialización. La opción para crear las cadenas del punto de recuperación en la unidad de inicialización necesita suficiente espacio en la unidad de inicialización como para almacenar los últimos puntos de recuperación desde los equipos protegidos especificados y puede llevar más tiempo.

9. Realice uno de los siguientes pasos:
   - Si ha desactivado la casilla de verificación **Agregar todos los Agents a la unidad de inicialización**, haga clic en **Siguiente**.
   - Si ha seleccionado **Agregar todos los Agents a la unidad de inicialización**, vaya al Paso 10.
10. En la página **Equipos protegidos** del asistente, seleccione los equipos protegidos para los que desea crear una unidad de inicialización.
11. Haga clic en **Finalizar**.

Supervisión de la replicación

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

1. En el Core de origen, abra la Rapid Recovery Core Console y, en la barra de iconos, haga clic en (Replicación).

   Aparece la página **Replicación**.
2. En esta página, puede ver información y supervisar el estado de las tareas de replicación según se describen en la tabla siguiente.

Tabla 106. Tareas de replicación

Sección	Descripción	Acciones disponibles
Unidades de inicialización (#)	Después de especificar el uso de una unidad de inicialización al definir la replicación, hasta que la abandone o consuma, el vínculo **Unidades de inicialización (#)** aparecerá en el panel Replicación saliente en el Core de origen. El número que se muestra indica cuántas unidades de inicialización están pendientes. **NOTE:** Este vínculo no aparecerá a menos que haya una unidad de inicialización pendiente. Haga clic en este vínculo para enumerar las unidades de inicialización que se han escrito pero aún no han sido consumidas por el Core de destino. Expanda aún más el menú contraíble para mostrar la información acerca de las unidades de inicialización pendientes, incluido el Core	En el menú desplegable, haga clic en **Abandonar** para abandonar o cancelar el proceso de inicialización.

Sección	Descripción	Acciones disponibles
	de destino y el rango de fechas de los puntos de recuperación incluidos en la unidad de inicialización.	
Replicación saliente	Enumera todos los Cores de destino en los que el Core de origen se está replicando. Incluye el nombre de indicador de estado, el nombre del Core de destino, el número de equipos que se replican y el progreso de una transmisión de replicación.	En un Core de origen, desde el menú desplegable ··· (Más), puede seleccionar las siguientes opciones: • **Detalles**: muestra Id., URL, nombre para mostrar, estado, Id. de cliente, dirección de correo electrónico y comentarios del Core replicado. • **Cambiar configuración.** Enumera el nombre mostrado y le permite editar el host y puerto para el Core de destino. • **Calendario de programación.** Le permite establecer un calendario de programación personalizado para la replicación en este Core de destino. • **Agregar equipos.** Le permite elegir un host de una lista desplegable, seleccionar equipos protegidos para replicación y crear una unidad de inicialización para la transferencia inicial del equipo protegido nuevo. Opcionalmente, puede elegir incluir los puntos de recuperación para los equipos de recuperación que ya ha agregado a la replicación. • **Eliminar.** Permite eliminar la relación de replicación entre los Cores de origen y destino. Si lo hace, cesa cualquier replicación en este Core.
Replicación entrante	Lista todos los equipos de origen desde los que el destino recibe datos replicados. Incluye el nombre, estado, equipos y progreso del Core remoto. Lista todos los Cores de origen desde los que el destino recibe datos replicados. El nombre de visualización para los Cores de origen que se enumeran se ocupan desde el valor en el Asistente para replicación al definir la replicación. Incluye el nombre de indicador de estado, el nombre del Core remoto y el progreso de una transmisión de replicación.	En un Core de destino, desde el menú desplegable ··· (Más), puede seleccionar las siguientes opciones: • **Detalles.** Enumera la Id., nombre de host, Id. de cliente, dirección de correo electrónico y comentarios para el Core replicado. • **Consumir.** Consume los datos iniciales de la unidad de inicialización y los guarda en el repositorio local. • **Eliminar.** Permite eliminar la relación de replicación entre los Cores de destino y origen. Si lo

Sección	Descripción	Acciones disponibles
		hace, cesa cualquier replicación de este Core.
Solicitudes de replicación pendientes	Esta información se aplica a los proveedores de servicios administrados solamente. Cuando un cliente hace clic en el vínculo **Solicitudes** en el panel Replicación entrante, la sección de una tabla de resumen aparece con una clasificación de los Id. de cliente, la dirección de correo electrónico y el nombre de host para la solicitud.	En el menú desplegable, haga clic en **Ignorar** para ignorar o rechazar la solicitud, o **Revisar** para revisar la solicitud pendiente.

Pausa y reanudación de la replicación

Puede realizar una pausa en la replicación de forma temporal para los Cores de origen (salida) o destino (entrada).

La opción para pausar la replicación solo está disponible si la replicación está activa. La opción para reanudar la replicación solo está disponible si la replicación está en pausa.

Realice los pasos del procedimiento siguiente para pausar o reanudar la replicación.

1. Abra laRapid Recovery Core Console y, desde la barra de icono, haga clic en (Replicación).

   Aparece la página **Replicación**.
2. Para pausar la replicación en todos los equipos replicados, haga lo siguiente:
   a. Haga clic en la casilla de verificación en la parte superior de la tabla de resumen para seleccionar el Core de origen y de destino.
   b. Haga clic en **Pausar** en el menú anterior a la tabla de resumen.

   La replicación de todos los equipos protegidos en el Core seleccionado está en pausa.
3. Para pausar la replicación de algunos equipos, haga lo siguiente:
   a. Haga clic en la flecha a la derecha de cualquier Core.

   La vista se expande para mostrar cada uno de los equipos protegidos del Core que se han replicado en el Core seleccionado.
   b. Haga clic en la primera columna para seleccionar cada máquina para la que desea pausar la replicación. Haga clic de nuevo en cualquier selección para borrar la casilla de verificación de los equipos que no desea pausar.
   c. Haga clic en **Pausar** en el menú anterior a la tabla de resumen.

   La replicación para los equipos protegidos seleccionados está en pausa.
4. Para reanudar la replicación en todos los equipos replicados, haga lo siguiente:
   a. Haga clic en la casilla de verificación en la parte superior de la tabla de resumen para seleccionar el Core de origen y de destino.
   b. Haga clic en **Reanudar** desde el menú de la parte superior de la tabla de resumen.

   La replicación de todos los equipos protegidos en el Core seleccionado se reanuda.
5. Para reanudar la replicación de algunos equipos, haga lo siguiente:
   a. Haga clic en la flecha a la derecha de cualquier Core.

   La vista se expande para mostrar cada uno de los equipos protegidos del Core que se han replicado en el Core seleccionado.

b. Haga clic en la primera columna para seleccionar cada máquina para la que desea reanudar la replicación. Haga clic de nuevo en cualquier selección para borrar la casilla de verificación de los equipos que no desea reanudar.

c. Haga clic en **Reanudar** desde el menú de la parte superior de la tabla de resumen.

Se reanuda la replicación para los equipos protegidos seleccionados.

Forzado de la replicación

Desde el Core de origen, puede forzar la replicación en cualquier momento, en lugar de esperar que un trabajo de replicación haga cola después de un evento específico, como una copia de seguridad o comprobación de capacidad de conexión.

Complete los pasos del siguiente procedimiento para forzar la replicación en el Core de origen o de destino.

1. En el Core de origen, abra la Rapid Recovery Core Console y, en la barra de iconos, haga clic en (Replicación).

   Aparece la página **Replicación**.

2. Realice uno de los siguientes pasos:

   - Para forzar la replicación en un Core de origen, desde el panel **Replicación saliente**, seleccione un Core y, desde el menú de la parte superior de la tabla de resumen, haga clic en **Forzar**.
   - Para forzar la replicación en un Core de destino, desde el panel **Replicación entrante**, seleccione un Core y, desde el menú de la parte superior de la tabla de resumen, haga clic en **Forzar**.

   Se abre el cuadro de diálogo Forzar replicación.

3. De manera opcional, si desea reparar cualquier de las cadenas huérfanas de los puntos de recuperación, seleccione **Restaurar cadenas de punto de recuperación huérfanas**.
4. Para confirmarlo, en el cuadro de diálogo Forzar la replicación, haga clic en **Sí**.

   El cuadro de diálogo se cierra y la replicación se fuerza.

Administración de configuración para la replicación saliente

Los cambios realizados en esta configuración afectan a la transferencia de datos a todos los Cores de destino asociados con este Core de origen.

1. En el Core de origen, abra la Rapid Recovery Core Console y, en la barra de iconos, haga clic en (Replicación).

   Aparece la página **Replicación**.

2. En el panel **Replicación saliente**, en la parte superior de la tabla de resumen, haga clic en (Configuración).

   Se muestra el cuadro de diálogo **Configuración de replicación**.

3. En el cuadro de diálogo **Configuración de replicación**, edite la configuración de replicación según se describe en la tabla siguiente.

Tabla 107. Configuración de replicación

Opción	Descripción
Duración de la caché (segundos)	Especifica el tiempo entre las solicitudes de estado de Core de destino realizadas por el Core de origen.

Opción	Descripción
Tiempo de espera de la sesión de imagen del volumen (minutos)	Especifica el tiempo que el Core de origen tarda en intentar transferir una imagen de volumen al Core de destino.
N.º máximo de flujos paralelos	Especifica el número de conexiones de red permitidas para su uso por parte de un equipo protegido único para la replicación de los datos de dicho equipo de una vez.
Velocidad máxima de transferencia (MB/s)	Especifique el límite de velocidad para la transferencia de los datos replicados.
Tamaño máximo de datos de transferencia (GB)	Especifique el tamaño máximo en GB para transferir los bloques de datos replicados.
Restaurar valores predeterminados	Seleccione esta opción para cambiar toda la configuración de replicación a los valores predeterminados del sistema. **NOTE:** Tome nota de cualquier configuración personalizada antes de seleccionar esta opción. No se le solicitará que confirme esta acción

4. Cuando esté satisfecho, haga clic en **Guardar** para guardar la configuración de replicación y cerrar el cuadro de diálogo.

Cambio de la configuración del Core de destino

Puede cambiar el host y la configuración de puertos en Cores de destino individuales desde el Core de origen.

1. En el Core de origen, abra la Rapid Recovery Core Console y, en la barra de iconos, haga clic en (Replicación). .

   Aparece la página **Replicación**.

   En el panel **Replicación saliente**, la tabla de resumen incluye una fila para cada Core de destino que se ha configurado para replicar puntos de recuperación desde este Core de origen.

2. Haga clic en el menú desplegable (Configuración) del Core de destino que desea modificar y, a continuación, seleccione **Cambiar la configuración**.

   Aparecerá el cuadro de diálogo **Configuración**.

3. Edite cualquiera de las opciones que se describen en la siguiente tabla.

Tabla 108. Configuración del Core de destino

Opción	Descripción
Host	Introduzca el host para el Core de destino.
Puerto	Introduzca un puerto para que el Core de destino lo utilice para la comunicación con el Core de origen. **NOTE:** El puerto predeterminado es 8006.

4. Haga clic en **Guardar**.

Cómo establecer la prioridad de replicación para un equipo protegido

La prioridad de replicación determina qué trabajos de replicación se envían en primer lugar al Core. La priorización se establece de manera ordinal, en una escala del 1 al 10, donde 1 es la primera prioridad y 10 la última. La primera vez que establezca la replicación de cualquier equipo, la prioridad se establece en 5. Puede ver y cambiar la prioridad en el nivel de equipo protegido del Core de origen.

En algunos casos, es posible que se abandonen algunos trabajos de replicación. Por ejemplo, los trabajos de replicación pueden abandonarse si el entorno está experimentando altas velocidades de cambios de manera excepcional o si la red no tiene suficiente ancho de banda. Es probable que se produzca esta situación si establece calendarios de programación que limitan las horas al realizarse la replicación en su entorno. Para obtener más información acerca de la configuración de la replicación de calendarios de programación, consulte Programación de la replicación.

Para garantizar la realización de la replicación de los equipos importantes primero, establezca una prioridad con un número bajo (entre 1 y 5) en los servidores críticos. Establezca una prioridad con un número alto (entre 6 y 10) en los equipos menos importantes.

La configuración del valor de prioridad de replicación de número 4 de cualquier equipo protegido garantiza que el trabajo de replicación se inicie antes que en un equipo con el valor de la prioridad de replicación predeterminada de 5. Los trabajos de replicación de equipos con un valor de prioridad de 3 se ponen en cola antes de los de 4 y así sucesivamente. Cuanto menor es el número de prioridad, antes se envían los trabajos de replicación. Es fácil de recordar que la prioridad 1 es la más importante. Los equipos con una prioridad de replicación de 1 se encuentran los primeros en la cola de replicación.

Complete los pasos siguientes para editar la configuración que será prioridad cuando un equipo protegido se replique.

1. En el Core de origen, abra la Rapid Recovery Core Console y, en la barra de iconos, haga clic en (Replicación).

   Aparece la página **Replicación**.
2. En el panel **Replicación saliente**, haga clic en la flecha a la derecha de cualquier Core de origen.

   La vista se expande para mostrar cada uno de los equipos protegidos del Core de destino que se han replicado en el Core de destino designado.
3. Haga clic en el menú desplegable (Más) en el equipo protegido al que quiere dar prioridad y, a continuación, haga clic en **Cambiar configuración**.

   Se muestra un cuadro de diálogo.
4. Haga clic en la lista desplegable **Prioridad** y seleccione la prioridad, desde **1 (más alto)** a **10 (más bajo)**, en función de sus necesidades.
5. Haga clic en **Guardar**.

   Se cerrará el cuadro de diálogo y la prioridad de replicación de las actualizaciones de los equipos seleccionados.

Eliminar la replicación saliente del Core de inicio

Complete los pasos de este procedimiento para eliminar uno o más equipos protegidos de la replicación en el Core de inicio.

1. En el Core de origen, abra la Rapid Recovery Core Console y, en la barra de iconos, haga clic en (Replicación).

   Aparece la página **Replicación**.

   En el panel **Replicación saliente**, la tabla de resumen incluye una fila para cada Core de destino que se ha configurado para replicar puntos de recuperación desde este Core de origen.

2. De manera opcional, haga clic en la flecha a la derecha de cualquier Core de destino.

   La vista se expande para mostrar cada uno de los equipos protegidos del Core de destino que se han replicado en el Core de destino designado.

3. Seleccione los equipos protegidos que desea eliminar de replicación saliente como se indica a continuación:

   - Para eliminar por completo la relación de replicación existente entre este Core de origen y cualquier Core de destino, haga clic en el menú desplegable (Más) de cualquier Core de destino y, a continuación, seleccione **Eliminar**.
   - Para eliminar replicación saliente de un subconjunto de equipos en el Core de destino especificado, amplíe la vista para mostrar todas las máquinas que se están replicando, y seleccione la casilla de verificación para cada equipo replicado que desea quitar. Borre la casilla de verificación de cualquier equipo que desee continuar replicando. A continuación, desde el menú que está por encima de la tabla de resumen, haga clic en **Eliminar**.

   Aparecerá un mensaje de confirmación que le preguntará si desea quitar las relaciones de replicación.

4. En el cuadro de diálogo resultante, haga clic en **Sí** para confirmar la eliminación.

Eliminar la replicación entrante del Core de destino

Complete los pasos de este procedimiento para eliminar uno o más equipos protegidos de la replicación en el Core de destino.

NOTE: También puede eliminar la replicación de equipos protegidos del panel Replicación saliente en la página Replicación del Core de origen. Para obtener más información, consulte Eliminar la replicación saliente del Core de inicio

1. En el Core de destino, abra la Rapid Recovery Core Console y, en la barra de iconos, haga clic en (Replicación).

Aparece la página **Replicación**. En el panel Replicación entrante, la tabla de resumen incluye una fila para cada Core de origen con los equipos protegidos que replica ese Core de destino.

2. Seleccione los equipos replicados para eliminaros de la siguiente manera:
   - Para eliminar todos los equipos replicados del Core de origen al Core de destino, en el panel Replicación entrante, seleccione la casilla de verificación de ese Core.
   - Para eliminar un subconjunto más pequeño de equipos del mismo Core de origen, haga lo siguiente:

     a. Haga clic en la flecha ▶ a la derecha del Core de origen.

     La vista se expande para mostrar cada uno de los equipos del Core de origen que se han replicado en el Core de destino.

     b. Seleccione la casilla de verificación de cada equipo replicado que desea quitar.

     c. En la fila principal del Core de origen seleccionado, haga clic en el menú desplegable ••• (Más) y, a continuación, seleccione **Eliminar**.

     Se abre el cuadro de diálogo **Quitar replicación**.
3. En el cuadro de diálogo **Quitar replicación**, haga lo siguiente:
   - Si desea dejar los puntos de recuperación replicados en el Core de destino, desmarque la opción **Eliminar puntos de recuperación existentes**.
   - Si desea eliminar todos los puntos de recuperación replicados recibidos de ese equipo, así como quitar el Core de origen de la replicación, seleccione **Eliminar puntos de recuperación existentes**.
4. Haga clic en **Sí** para confirmar la eliminación.

   WARNING: Si selecciona esta opción, se eliminarán todos los puntos de recuperación replicados en este Core.

   Los equipos protegidos seleccionados en el Core de origen se eliminan de la replicación en este Core de destino. De manera opcional, si ha seleccionado la opción para los eliminar puntos de recuperación, se eliminan del repositorio de este Core.

Recuperación de datos replicados

La funcionalidad de replicación 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 tras desastre.

Para la recuperación de desastres, el Core de destino puede utilizar los puntos de recuperación replicados para recuperar los equipos protegidos. Puede realizar las opciones de recuperación siguientes desde el Core de destino:

- Puntos de recuperación de montaje. Para obtener más información, consulte Montaje de un punto de recuperación.
- **Revertir a puntos de recuperación.** Para obtener más información, consulte Acerca de la restauración de volúmenes desde un punto de recuperación o Restauración de volúmenes para un equipo Linux mediante la línea de comandos.
- **Realizar una exportación de máquina virtual (VM).** Para obtener más información, consulte Exportación a máquinas virtuales con Rapid Recovery.
- **Realizar una bare metal restore (BMR).** Para obtener más información, consulte Realización de una restauración Bare Metal Restore para equipos con Windows.

Eventos

El Rapid Recovery Core incluye conjuntos predefinidos de eventos. Estos eventos se pueden utilizar para notificar a los administradores de los problemas críticos en el Core o sobre trabajos que pertenecen a copias de seguridad, a la exportación virtual, la replicación, etc.

En esta sección se describe cómo ver los eventos que se muestran en la Rapid Recovery Core Console. También puede obtener más información sobre los métodos y la configuración de la notificación de eventos, incluida la configuración de las notificaciones por correo electrónico. Por último, puede configurar las notificaciones para cambiar la cantidad de registros de eventos de tiempo que se conservan y reducir las notificaciones de eventos repetitivas.

Visualización de eventos mediante las páginas de tareas, alertas y del diario

En la Consola de Core, puede ver los eventos para el Core y puede ver los eventos de un equipo protegido o replicado específico.

En las páginas **Eventos** de la Core Console se muestra un registro de todos los eventos del sistema relacionados con Rapid Recovery Core. Para acceder a los eventos del Core y verlos, haga clic en (Eventos).

Las páginas **Eventos** para un equipo protegido o replicado específico muestran un registro de eventos relacionados con este equipo protegido. Para acceder y ver los eventos de un equipo seleccionado, haga clic en el nombre del equipo en el menú Equipos protegidos y, desde la página **Resumen**, haga clic en el menú **Eventos**.

Las páginas Eventos (del Core o de un equipo determinado) están disponibles en tres vistas: Tareas, Alertas y Diario.Todos los elementos que se muestran en cualquier categoría son un evento. Estas vistas permiten filtrar los detalles sobre diversos subconjuntos de eventos, según corresponda. La vista predeterminada es para mostrar tareas.

- Una **tarea** es un evento relacionado con un trabajo. Un **trabajo** es un proceso que el Rapid Recovery Core debe realizar. Cada trabajo tiene un estado actual y una fecha y hora de inicio y finalización. Algunas de las tareas se inician manualmente o las programa el usuario. Algunos ejemplos incluyen forzar una instantánea, programar una copia de seguridad o realizar una restauración a partir de un punto de recuperación. Otras tareas son funciones automáticas, como la ejecución los trabajos nocturnos o la consolidación mediante la política de retención predeterminada.
- Una **alerta** es un evento de prioridad, como un error, un aviso o un mensaje informativo importante. Si solicita notificaciones de eventos específicos, aparecen en el subconjunto Alertas.
- El **diario** muestra una lista completa de todos los eventos registrados (del Core o del equipo seleccionado, según corresponda). Esta lista es más completa, ya que muestra trabajos, eventos de prioridad alta y eventos de prioridad más baja. Esta categoría incluye eventos pasivos y eventos que no corresponden a trabajos (como el inicio del Core correctamente o los informes del estado del portal de licencias).

Realice los pasos de los procedimientos siguientes para ver tareas, alertas o un diario de todos los eventos:

- Visualización de tareas
- Visualización de alertas
- Visualización de un diario de todos los eventos registrados
- Visualización de tareas en ejecución desde cualquier página de la Core Console
- Navegar entre tareas, eventos y el diario de eventos

Visualización de tareas

Una tarea es un trabajo que el Rapid Recovery Core debe realizar, como transferir datos en una copia de seguridad programada con regularidad o realizar una restauración desde un punto de recuperación.

NOTE: Cuando una tarea se está ejecutando, se enumera en el menú desplegable **Tareas en ejecución** de la parte superior de Core Console. Al hacer clic en una tarea en ejecución, se abre el cuadro de diálogo **Supervisar tarea activa**. Aquí puede cancelar una o más tareas en ejecución. Para obtener más información, consulte el tema Visualización de tareas en ejecución desde cualquier página de la Core Console. También puede suspender la programación de futuras tareas en el Core. Esto resulta útil, por ejemplo, al actualizar el sistema operativo o realizar el mantenimiento del servidor. Para obtener más información acerca de esta función, consulte el tema Suspensión o reanudación de tareas programadas.

Realice los pasos siguientes para ver las tareas específicamente del Rapid Recovery Core o para ver las tareas asociadas con un equipo específico.

1. Para ver todas las tareas del Rapid Recovery Core, haga clic en (Eventos) en la barra de iconos. La vista predeterminada muestra todas las tareas del Core.

   Si desea ver las tareas de un equipo protegido específico, vaya a la página **Resumen** del equipo especificado y, a continuación, haga clic en el menú **Eventos**. La vista predeterminada muestra todas las tareas del equipo seleccionado.

2. Opcionalmente, para filtrar la lista de tareas por palabra clave, fecha de inicio, fecha de finalización o cualquier combinación, haga lo siguiente y, a continuación, pulse **Entrar**:

   a. Para filtrar por palabra clave, introduzca la palabra clave en el cuadro de texto **Palabra clave de la búsqueda**.

   Por ejemplo, puede filtrar por palabras clave como "consolidando", "archivo comprimido", "exportar" o "transferencia".

   b. Para filtrar por la fecha y hora de inicio, introduzca la fecha y hora de inicio mediante una de las siguientes opciones:

   - En el cuadro de texto **De**, escriba la fecha y hora con el formato MM/DD/AAAA HH:MM AM/PM. Por ejemplo, para buscar desde el 1 de enero de 2016 a las 8:00 AM, introduzca 1/1/2016 8:00 AM.
   - Para seleccionar la fecha y hora actuales, haga clic en el widget **Calendario** en el cuadro de texto **Desde** y, a continuación, haga clic en la fecha actual. La hora actual aparecerá automáticamente.
   - Haga clic en el widget **Calendario**, seleccione la fecha y, a continuación, haga clic en el widget Reloj y seleccione la hora que desea mediante los controles. Haga clic fuera del calendario para aceptar los cambios seleccionados.

   c. Para definir más la lista de tareas que aparece, también puede definir una fecha y hora de finalización con el mismo formato.

La lista de tareas se filtrará inmediatamente según los criterios que seleccione.

3. Opcionalmente, puede filtrar las tareas que aparecen en la lista de la manera siguiente:

Opción	Descripción
	Para ver únicamente las tareas activas, haga clic en el icono **Tarea activa**.
	Para ver únicamente las tareas que estén en cola para ser realizadas, haga clic en el icono **En cola**.
	Para ver únicamente las tareas que estén a la espera de ser realizadas, haga clic en el icono **Tareas en espera**.
	Para ver únicamente las tareas que se hayan completado, haga clic en el icono **Tareas completadas**.
	Para ver únicamente las tareas que hayan fallado, haga clic en el icono **Tareas con errores**.
	Para ver todos los eventos, incluidos los eventos de servicios del Core que no se muestran de forma predeterminada, haga clic en el icono **Servicio**.

4. Para exportar la lista de tareas, seleccione un formato de la lista y, a continuación, haga clic en  **Exportar**. En el cuadro de diálogo resultante, confirme la exportación y, a continuación, haga clic en **Aceptar**.

   Puede exportar utilizando los siguientes formatos:

Tabla 109. Formatos de exportación

Formatos de salida disponibles por medio de los cuales que puede descargar una exportación.

Formato	Descripción
PDF	Portable Document Format (formato de exportación predeterminado)
HTML	Formato de página web
CSV	Valores separados por comas
XLS	Libro de Microsoft Excel 1997 - 2003
XLSX	Libro de Excel

   El archivo del tipo que haya seleccionado se descarga en la ubicación predeterminada del servidor del Core.

5. Haga clic en el icono  **Detalles del trabajo** de cualquier tarea para abrir una nueva ventana con información detallada de la tarea.

Tareas relacionadas

See also: Visualización de tareas
See also: Suspensión o reanudación de tareas programadas
See also: Visualización de alertas

See also: Visualización de un diario de todos los eventos registrados
See also: Visualización de tareas en ejecución desde cualquier página de la Core Console
See also: Navegar entre tareas, eventos y el diario de eventos

Visualización de tareas en ejecución desde cualquier página de la Core Console

Para realizar este procedimiento, debe haber una tarea que esté actualmente en ejecución en el Rapid Recovery Core.

Rapid Recovery ofrece una forma rápida de ver las tareas que están actualmente en ejecución en el Core desde cualquier página de la Core Console.

En la parte derecha de la barra de botones se encuentra la cola **Tareas en ejecución** cola. En resoluciones de pantalla más bajas, o si la ventana del explorador no está completamente expandida, la cola puede aparecer como un icono  . Cuando uno o varias tareas están en ejecución, aparece un número que indica el número de tareas que están actualmente en ejecución junto a la cola y el icono se ve en animación. Puede hacer clic en la cola para mostrar una lista desplegable de las tareas en ejecución y completar las acciones que se describen en el procedimiento siguiente.

1. En la Core Console, mientras una tara está en ejecución, haga clic en **Tareas en ejecución** o en el icono de tareas en ejecución.

   Aparece un cuadro pequeño que muestra el tipo de tareas en ejecución y su progreso y presenta opciones para cancelar una o varias tareas o para ver más información.
2. Para cancelar una o varias tareas en ejecución, elija una de las opciones siguientes:
   - Para cancelar una única tarea, haga clic en **X** que se encuentra junto a la descripción de la tarea.
   - Para cancelar todas las tareas en ejecución, haga clic en **Cancelar todo**.
3. Para ver más información sobre una tarea en ejecución, haga clic en la descripción de la tarea.

   Se abre la ventana **Supervisar tarea activa** y muestra información como el progreso o la hora de inicio.

Tareas relacionadas

See also: Visualización de tareas
See also: Navegar entre tareas, eventos y el diario de eventos
See also: Suspensión o reanudación de tareas programadas

Suspensión o reanudación de tareas programadas

Para reanudar el programador del Core, primero debe pausarse, como se describe en el paso 3.

El Core realiza el seguimiento de las tareas basada en una programación. Las transferencias de copia de seguridad, replicación y archivado puede programarse; los informes se pueden generar semanal o mensualmente; y así sucesivamente. Cuando se acerca el momento de que se produzca una tarea programada, los trabajos se ponen en cola y se realizan consecutiva o simultáneamente, en función de la prioridad. Esta función se conoce como el programador del Core.

Los usuarios ahora pueden ordenar al Core que suspendan el programador Cuando se suspenden, los trabajos futuros que, de otro modo, se programarían automáticamente para ejecutarse en el Core, se conservan temporalmente en una cola y no se programan tareas nuevas. Esta función es útil en situaciones como la realización de actualizaciones al SO, instalaciones de software o para el mantenimiento del servidor del Core. Cuando se suspenden, los trabajos se acumulan en la cola, pero no empiezan hasta que la función de programador del Core se reanuda de manera explícita. Mientras, se muestra un banner en la Core Console que indica que el programador del Core esta pausado.

NOTE: Esta función evita que se ejecuten las tareas que se programarán pronto. Para visualizar o cancelar taras que ya están en cola sin suspender tareas futuras, consulte el tema Visualización de tareas en ejecución desde cualquier página de la Core Console.

Complete los siguientes pasos para suspender o reanudar la función del programador del Core.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Eventos).

   Aparecerá la página **Tareas**.
3. Para suspender la función del programador del Core, realice lo siguiente:
   a. Haga clic en **Suspender programador**.
   b. En el cuadro de diálogo, si desea cancelar que se ejecuten todas las tareas y suspender las tareas futuras, seleccione **Cancelar tareas activas y suspender**.
   c. Para solo suspender tareas futuras, haga clic en **Suspender**.

   Las tareas se suspenden y se muestra un banner en todas las páginas de la Core Console que indica que todas las tareas programadas se han suspendido.
4. Para reanudar las tareas suspendidas, en la página **Tareas**, haga clic en **Reanudar programador**.

NOTE: Cuando se suspenda el programador, puede hacer clic en **Reanudar** en el banner de la parte superior de la Core Console.

Tareas relacionadas

See also: Visualización de tareas en ejecución desde cualquier página de la Core Console
See also: Visualización de tareas
See also: Suspensión o reanudación de tareas programadas
See also: Visualización de alertas
See also: Visualización de un diario de todos los eventos registrados
See also: Navegar entre tareas, eventos y el diario de eventos

Visualización de alertas

Una alerta es una notificación con prioridad de un evento. Los eventos para los que solicitó notificaciones especialmente aparecen en la lista de alertas, con los errores, avisos o mensajes informativos importantes.

El Rapid Recovery Core se envía con un conjunto de eventos con prioridad predeterminado como alertas. Puede personalizar los eventos que aparecen como alertas editando el grupo de notificación predeterminado (o configurando un nuevo grupo de notificación). Además de estos eventos que aparecen en la página **Alertas**, puede cambiar los métodos que se utilizan para enviarle notificaciones cambiando las opciones de notificación. Para obtener más información sobre cómo cambiar los eventos que aparecen como alertas o las opciones de notificación, consulte el tema Comprensión de las notificaciones de eventos en Rapid Recovery.

Realice los pasos siguientes para ver las alertas específicamente del Rapid Recovery Core o para ver las alertas asociadas con un equipo específico.

1. Para ver las tareas del Rapid Recovery Core, en la barra de iconos, haga clic en (Eventos). Haga clic en el menú desplegable que se encuentra a la derecha del título de la página Tareas y seleccione **Alertas**.

   Si desea ver las alertas de un equipo protegido específico, vaya a la página **Resumen** del equipo especificado, haga clic en el menú **Eventos** y, a continuación, haga clic en **Alertas**.

   La lista de eventos se filtrará para mostrar únicamente las alertas importantes del Core o del equipo que seleccione.
2. De manera opcional, para filtrar la lista de alertas importantes por fecha de inicio, fecha de finalización, descripción del mensaje de alerta o cualquier combinación, haga lo siguiente:
   a. Para filtrar por categoría de alerta (errores, mensajes informativos o alertas), haga clic en el menú desplegable de estados y seleccione las condiciones del estado. Las opciones de filtro por categoría de alerta incluyen errores, mensajes informativos y avisos, o cualquier combinación de los tres.

b. Para filtrar por la fecha y hora de inicio, introduzca la fecha y hora de inicio mediante una de las siguientes opciones:

- En el cuadro de texto **De**, escriba la fecha y hora con el formato MM/DD/AAAA HH:MM AM/PM. Por ejemplo, para buscar desde el 1 de enero de 2016 a las 8:00 AM, introduzca 1/1/2016 8:00 AM.
- Para seleccionar la fecha y hora actuales, haga clic en el widget **Calendario** en el cuadro de texto **Desde** y, a continuación, haga clic en la fecha actual. La hora actual aparecerá automáticamente.
- Haga clic en el widget **Calendario**, seleccione la fecha y, a continuación, haga clic en el widget Reloj y seleccione la hora que desea mediante los controles. Haga clic fuera del calendario para aceptar los cambios seleccionados.

c. Para filtrar por descripción de alerta de mensaje, introduzca la descripción en el cuadro de texto **Buscar mensaje**.

Por ejemplo, para ver solo las alertas relacionadas con los Agents, introduzca "Agent"; para ver las alertas relacionadas con las transferencias, introduzca "transferencia", etc.

d. Para definir más la lista de alertas que aparece, también puede definir una fecha y hora de finalización con el mismo formato.

La lista de alertas se filtra inmediatamente según los criterios que seleccione.

3. De manera opcional, si quiere quitar todas las alertas, haga clic en **Descartar todo**.

Tareas relacionadas

See also: Configuración de grupos de notificación
See also: Visualización de tareas
See also: Suspensión o reanudación de tareas programadas
See also: Visualización de alertas
See also: Visualización de un diario de todos los eventos registrados
See also: Visualización de tareas en ejecución desde cualquier página de la Core Console
See also: Navegar entre tareas, eventos y el diario de eventos

Referencia relacionada

See also: Comprensión de las notificaciones de eventos en Rapid Recovery

Visualización de un diario de todos los eventos registrados

El diario muestra todos los eventos registrados. La lista es completa, incluye tanto los eventos relacionados como no relacionados con trabajos. Incluye eventos específicos para los que solicitaste notificaciones. El diario también muestra los eventos pasivos y los estados de los eventos del Core, el portal de licencias, etc.

NOTE: Si su entorno está establecido para que utilice la reducción de repeticiones, puede que algunos eventos repetidos no se registren cada vez que se produzca el evento. Para obtener más información acerca de esta función, consulte Acerca de la reducción de repeticiones

Realice los pasos siguientes para ver un diario de todos los eventos del Rapid Recovery Core o para ver un diario de todos los eventos de un equipo específico.

1. Para ver un diario de todos los eventos registrados para el Rapid Recovery Core, en la barra de iconos, haga clic en (Eventos). Haga clic en el menú desplegable que se encuentra a la derecha del título de la página Tareas y seleccione **Diario**.

Si desea ver un diario de todos los eventos de un equipo protegido, vaya a la página **Resumen** del equipo especificado, haga clic en el menú **Eventos** y, a continuación, haga clic en **Diario**.

2. De manera opcional, para filtrar la lista de todos los eventos por fecha de inicio, fecha de finalización, descripción del mensaje de alerta o cualquier combinación, haga lo siguiente:
    a. Para filtrar por categoría de evento (errores y mensajes informativos o avisos), haga clic en el menú desplegable de estados y seleccione las condiciones del estado. Las opciones de filtro por categoría de evento incluyen errores, mensajes informativos y avisos, o cualquier combinación de los tres.
    b. Para filtrar por la fecha y hora de inicio, introduzca la fecha y hora de inicio mediante una de las siguientes opciones:

    - En el cuadro de texto **De**, escriba la fecha y hora con el formato MM/DD/AAAA HH:MM AM/PM. Por ejemplo, para buscar desde el 1 de enero de 2016 a las 8:00 AM, introduzca 1/1/2016 8:00 AM.
    - Para seleccionar la fecha y hora actuales, haga clic en el widget **Calendario** en el cuadro de texto **Desde** y, a continuación, haga clic en la fecha actual. La hora actual aparecerá automáticamente.
    - Haga clic en el widget **Calendario**, seleccione la fecha y, a continuación, haga clic en el widget Reloj y seleccione la hora que desea mediante los controles. Haga clic fuera del calendario para aceptar los cambios seleccionados.

    c. Para filtrar por descripción de alerta de mensaje, introduzca la descripción en el cuadro de texto **Buscar mensaje**.

    Por ejemplo, para ver solo las alertas relacionadas con los Agents, introduzca "Agent"; para ver las alertas relacionadas con las transferencias, introduzca "transferencia".

    d. Para refinar más la lista de eventos que aparece, también puede definir una fecha y hora de finalización con el mismo formato.

    La lista de eventos se filtra inmediatamente según los criterios que seleccione.

Conceptos relacionados

See also: Acerca de la reducción de repeticiones

Tareas relacionadas

See also: Visualización de tareas
See also: Suspensión o reanudación de tareas programadas
See also: Visualización de alertas
See also: Visualización de un diario de todos los eventos registrados
See also: Visualización de tareas en ejecución desde cualquier página de la Core Console
See also: Navegar entre tareas, eventos y el diario de eventos

Navegar entre tareas, eventos y el diario de eventos

Los eventos registrados en el Core son visibles desde la Core Console y se dividen en tres categorías: tareas, alertas y un diario de todos los eventos registrados.

Independientemente de si visualiza eventos del Core de un equipo determinado, la vista predeterminada de eventos es la página **Tareas**. Si hace clic en el menú desplegable que se encuentra a la derecha del título de la página, puede seleccionar otra vista de eventos.

Realice los pasos siguientes para ver eventos y navegar entre tareas, alertas importantes y un diario de todos los eventos.

Para ver los eventos que pertenecen al Core, haga clic en (Eventos) en la barra de iconos.

Si primero accede a un equipo replicado o protegido y, a continuación, selecciona **Eventos** desde el menú que se encuentra en la parte superior de la página, puede ver eventos de un equipo determinado.

Independientemente de si visualiza eventos del Core de un equipo determinado, la vista predeterminada de eventos es la página **Tareas**. Si hace clic en el menú desplegable que se encuentra a la derecha del título de la página, puede seleccionar otra vista de eventos.

1. Para ver todas las tareas del Rapid Recovery Core, en la barra de iconos haga clic en (Eventos).

   La vista predeterminada muestra todas las tareas del Core. Continúe en el paso 3.
2. Si desea ver las tareas de un equipo protegido específico, vaya a la página **Resumen** del equipo especificado y, a continuación, haga clic en el menú **Eventos**.

   La vista predeterminada muestra todas las tareas del equipo seleccionado. Continúe en el paso 3.
3. En la parte superior izquierda del panel **Tareas**, haga clic en (flecha hacia abajo que aparece a la derecha del título Tareas).

   Aparece un menú desplegable.
4. Seleccione una de las siguientes opciones:

Opción	Descripción
Tarea	Una tarea es un trabajo que el Rapid Recovery Core debe realizar, como transferir datos en una copia de seguridad programada con regularidad o realizar una restauración desde un punto de recuperación.
Alerta	Una alerta es una notificación con prioridad relacionada con una tarea o un evento, como un error, un aviso o un mensaje informativo importante.
Diario	El diario muestra una lista completa de todos los eventos registrados. Esta lista es más completa que el conjunto que incluyen las alertas.

   Aparece la vista de eventos seleccionada. Por ejemplo, si ha seleccionado **Alertas**, aparece la página Alertas.
5. Para ver una vista diferente, vuelva al menú desplegable que se encuentra a la derecha del panel Tareas, Alertas o Diario y seleccione la opción de vista que quiere.

   La lista de eventos se filtra para mostrar solo el conjunto pertinente de eventos para la vista actual.

Tareas relacionadas

See also: Visualización de tareas
See also: Visualización de alertas
See also: Visualización de un diario de todos los eventos registrados
See also: Visualización de tareas en ejecución desde cualquier página de la Core Console

Comprensión de las notificaciones de eventos en Rapid Recovery

El Rapid Recovery Core sigue muchos eventos y registra la información con fines de funcionamiento y de diagnóstico.

Puede configurar las notificaciones de eventos específicos. Rapid Recovery permite elegir el método de notificación y el tiempo que el sistema debe conservar un registro de esos eventos. Con la función de reducción de repeticiones, podrá incluso ajustar la frecuencia con la que se le enviarán notificaciones sobre el mismo evento.

Los trabajos y los eventos que se siguen mediante el Core se guardan de manera predeterminada durante 30 días. Para cambiar el periodo de retención de seguimiento de eventos, consulte Configuración de la retención de eventos

Puede recibir notificaciones de eventos a través de diferentes métodos. Los métodos de notificación disponibles se enumeran en la tabla siguiente:

Tabla 110. Métodos de notificación de eventos compatibles

Tipo de opción	Descripción	Configuración predeterminada
Correo electrónico	Notifica al usuario especificado por correo electrónico, con los valores de configuración de SMTP del Core y según la plantilla de notificaciones de correo electrónico.	Desactivado
Registro de eventos de Windows	Registra eventos con la API Registro de eventos de Windows. Este registro se puede leer mediante el visor de eventos de Windows o aplicaciones personalizadas.	Activado
syslogd	Registra eventos que se pueden leer desde un servidor de registro de Linux que también admite el protocolo de mensajes syslog.	Desactivado
Alerta del sistema	Si se selecciona este método, los mensajes aparecen brevemente como un elemento emergente en la esquina inferior derecha de la Rapid Recovery Core Console.	Activado
Captura SNMP	Si configura el Rapid Recovery Core como un agente SNMP y se selecciona este método de notificación, los eventos se envían a un servidor de registro con el número de captura designado en el cuadro de diálogo Opciones de notificación.	Activado

Los grupos de notificación permiten especificar los tipos de eventos que quiere que se le notifiquen y establecer el método de notificación.

El Rapid Recovery Core requiere al menos un grupo de notificación y se envía con un grupo predeterminado que se aplica automáticamente. Puede utilizar la configuración predeterminada o puede editarla.

Opcionalmente, puede agregar y configurar grupos de notificación adicionales. Por ejemplo, puede usar el grupo predeterminado tal cual o puede configurar otro grupo que use notificaciones por correo electrónico.

Otro ejemplo, puede configurar un grupo de notificación personalizado para un tipo de evento (por ejemplo, Microsoft Exchange) y enviar todas las notificaciones relacionadas a un administrador de Exchange.

Para obtener más información, consulte Configuración de grupos de notificación.

Las notificaciones por correo electrónico están desactivadas de manera predeterminada. Para enviar notificaciones por correo electrónico, debe configurar un servidor de correo electrónico y editar o agregar un grupo de notificación con la opción **Notificar por correo electrónico** activada. Esta configuración requiere que introduzca la dirección de correo electrónico a la que se enviarán las notificaciones. Para obtener más información, consulte Configuración de un servidor de correo electrónico.

Si se utiliza un servidor de Exchange, debe configurar la transmisión en el servidor. De lo contrario, a pesar de las pruebas de correo electrónico correctas, no se envían notificaciones por correo electrónico. Para obtener más información, visite a su administrador de Exchange Server.

El Core usa una plantilla de notificaciones de correo electrónico. La plantilla incluye una línea de asunto y el contenido específico para el cuerpo del mensaje. Se incluye una plantilla de notificaciones de correo electrónico. La plantilla identifica el Core y el servidor host, la fecha y la hora del evento, el tipo de evento y los detalles del error si corresponde. De manera opcional, puede modificar la plantilla predeterminada o revertir las personalizaciones para restaurar los valores predeterminados. Para obtener más información, consulte Configuración de una plantilla de notificación por correo electrónico.

Puede reducir el número de eventos del mismo tipo y ámbito registrados y visibles en la Core Console mediante la función de reducción de repeticiones. Esta función está activada de forma predeterminada. Puede desactivar esta función o puede controlar el lapso de tiempo en el que se combinan los eventos en una única incidencia en el registro de eventos. Para obtener más información, consulte Acerca de la reducción de repeticiones.

Conceptos relacionados

See also: Acerca de la reducción de repeticiones

Tareas relacionadas

See also: Configuración de grupos de notificación
See also: Configuración de la retención de eventos

Referencia relacionada

See also: Comprensión de las notificaciones por correo electrónico

Configuración de grupos de notificación

NOTE: Primero debe configurar el protocolo simple de transferencia de correo (SMTP) si desea enviar alertas como mensajes de correo electrónico, según se describe en este procedimiento. Para obtener más información sobre cómo establecer la configuración del servidor de correo electrónico, consulte Configuración de un servidor de correo electrónico.

Los grupos de notificación le permiten definir conjuntos de eventos específicos en los que se alerta a los usuarios, y el modo en que esta notificación tiene lugar. Puede configurar alertas para que se envíen con los siguientes métodos:

- Por correo electrónico
- En el registro de eventos de Windows
- Utilizando syslogd
- Utilizando alertas de toast
- Utilizando alertas
- Utilizando captura SNMP

Rapid Recovery Core se envía con un grupo de notificación predeterminado para el Core. Puede editar ese grupo para que se adapte a sus necesidades. Como opción, puede configurar más de un grupo de notificaciones con diferentes parámetros de notificación.

Los grupos de notificación pueden establecerse al nivel del Core o para cada equipo protegido específico.

Realice los pasos de este procedimiento para configurar los grupos de notificación de las alertas.

1. Para establecer notificaciones a nivel de Core, en la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Notificaciones**.

   Aparecerá la página **Notificaciones**. Vaya al paso 3.
2. Para establecer notificaciones para un equipo protegido específico, haga lo siguiente:
   a. A partir del menú de los equipos protegidos, haga clic en el equipo para el que quiera especificar las notificaciones.

   Aparecerá la página **Resumen**.

   b. En la página **Resumen** del equipo protegido, en el menú desplegable **Más**, seleccione **Notificaciones**.

   Aparecerá la página **Grupos de notificación personalizada**.
3. Si desea agregar un nuevo grupo de notificación, haga clic en **Agregar grupo**. Vaya al Paso 5.

   Aparecerá el cuadro de diálogo **Agregar grupo de notificación** que muestra un área de descripción general y dos pestañas.
4. Si quiere editar el grupo de notificación predeterminado o un grupo de notificación existente, en el panel Grupos de notificación, haga clic en el menú desplegable (More) del grupo de notificación adecuado y seleccione **Editar**.

   El cuadro de diálogo **Editar grupo de notificación** contiene un área de descripción general y dos fichas.
5. En el área de descripción general, introduzca la información básica para el grupo de notificación, según se describe en la siguiente tabla.

Opción	Descripción
Nombre	Introduzca un nombre para el grupo de notificación de eventos. Esta información es obligatoria. **CAUTION: El valor que introduzca para el nombre del grupo de notificación se puede cambiar más tarde.**
Descripción	Introduzca una descripción que clarifique el propósito del grupo de notificación de eventos. Esta información es opcional

6. En la pestaña **Activar alertas**, configure el conjunto de eventos del sistema que genera alertas. Estas aparecen en la página **Alertas** cuando visualiza eventos en la Core Console. Puede seleccionar conjuntos de eventos como se describe en la tabla siguiente:

Opción	Descripción
Todas las alertas	Para crear alertas de todos los eventos, seleccione
Errores	Para crear alertas de errores, en el menú **Seleccionar tipos**, haga clic en **Error**. Esto se representa con una X roja.
Advertencia	Para crear alertas de errores, en el menú **Seleccionar tipos**, haga clic en **Aviso**. Esto se representa mediante un icono de signo de admiración amarillo.

Opción	Descripción
Información	Para crear alertas de mensajes informativos, en el menú **Seleccionar tipos**, haga clic en **Información**. Esto se representa con una i azul.
Restaurar valores predeterminados	o el grupo de notificación del Core predeterminado, para restaurar el conjunto de eventos para que aparezcan como alertas en el valor predeterminado, en el menú **Seleccionar tipos**, haga clic en **Restablecer valores predeterminados**. **NOTE:** Esta opción solo está disponible al editar el grupo de notificación del Core predeterminado. No está disponible para los nuevos grupos de notificación del Core o para las notificaciones de configuración de un equipo protegido específico.

7. Para crear alertas de un tipo de evento específico (error, aviso o mensaje informativo), haga lo siguiente:
    a. Si la opción **Todas las alertas** no muestra los grupos de alertas, haga clic en el símbolo mayor que **>** anterior a la etiqueta Todas las alertas. El símbolo cambia a una flecha hacia abajo y la vista se expande para mostrar los grupos.
    b. A continuación, haga clic en el símbolo mayor que **>** junto a cualquier grupo de alertas específico para visualizar los eventos relacionados en el grupo.

    - Para definir alertas para todos los eventos en cada grupo, seleccione la casilla de verificación para **Todas las alertas**.
    - Para definir alertas para todos los eventos de cualquier grupo de alerta, seleccione la casilla de verificación junto a ese grupo.
    - Para seleccionar solo algunos tipos de alerta dentro de un grupo de alertas, expanda el grupo y, a continuación, seleccione solo aquellos sucesos específicos para los que desea log, informes y establecer alertas.
8. Haga clic en la pestaña **Opciones de notificación**.
9. En la pestaña **Opciones de notificación**, especifique cómo se gestionará el proceso de notificación.

Opción	Descripción
Notificar por correo electrónico	Designar los receptores de la notificación por correo electrónico. Puede elegir separar varias direcciones de correo electrónico, así como copias y copias ocultas. **NOTE:** Si usa Exchange Server, se debe configurar la transmisión SMTP en el servidor. De lo contrario, notificaciones de eventos no se enviarán a las direcciones de correo electrónico designadas. Para obtener más información, consulte con el administrador de Exchange Server.
Notificar mediante registro de eventos de Windows	Seleccione esta opción si desea que las notificaciones se entreguen mediante el registro de eventos de Windows.
Notificar por syslogd.	Seleccione esta opción si desea que las notificaciones se entreguen mediante syslogd.

Opción	Descripción
	Especifique los detalles de syslogd en los cuadros de texto siguientes: • Host: • Puerto:
Notificar por alertas de Toast	Seleccione esta opción si desea que las notificaciones aparezcan como mensajes emergentes en la esquina inferior derecha de la pantalla.
Notificar por captura de SNMP	El Rapid Recovery Core Core sirve como agente SNMP, que envía capturas (notificaciones sobre eventos específicos) a un gestor SNMP. El resultado es que el Core informa sobre alertas, estado de repositorios y equipos protegidos. Seleccione esta opción si desea notificar eventos del Core por captura SNMP. También debe especificar un número de captura, que lo utiliza el administrador de SNMP.

10. Haga clic en **Aceptar**.

Si crea un grupo nuevo, verá un mensaje que indica que el nombre del grupo de notificación definido no puede cambiar después de crear el grupo. Puede cambiar otras propiedades del grupo de notificación en cualquier momento.

- Si está satisfecho con el nombre del grupo, confirme este mensaje y guarde su trabajo.
- Si desea cambiar el nombre del grupo, haga clic en **No** para volver a la ventana Crear grupo de notificación, actualice el nombre del grupo y cualquier otro ajuste del grupo de notificación y guarde su trabajo.

El grupo de notificación aparece en la tabla de resumen. Puede crear diferentes grupos de notificación por medio de cualquier conjunto de parámetros.

Comprensión de las notificaciones por correo electrónico

Puede configurar el Rapid Recovery Core para que le avise de eventos específicos mediante el envío de un mensaje de correo electrónico a la dirección de correo electrónico que ha especificado. Los eventos que desencadenan alertas y los métodos de notificación están definidos en el grupo de notificación.

NOTE: Deben establecerse grupos de notificación sin que importe que utilice el correo electrónico como método de notificación. Para obtener más información, consulte Configuración de grupos de notificación.

Rapid Recovery utiliza una plantilla de notificaciones de correo electrónico, que determina la información que se envía en cada notificación. La plantilla define la línea de asunto de los mensajes para cada alerta y el contenido del cuerpo del mensaje de correo electrónico. La plantilla tiene una configuración predeterminada; puede utilizarla como está o puede realizar pruebas y modificaciones que se ajusten a sus necesidades. En cualquier momento después de personaliza la plantilla de notificaciones, puede elegir la opción Restaurar valores predeterminados para volver a utilizar la plantilla predeterminada. Para obtener más información sobre la visualización o la personalización de la plantilla de correo electrónico, consulte Configuración de una plantilla de notificación por correo electrónico.

Si selecciona el correo electrónico como una de las opciones de notificación, primero deberá configurar un servidor SMTP de correo electrónico. El Rapid Recovery Core utiliza el servidor que defina para enviar alertas basadas en los parámetros del grupo de notificación.

Además, para recibir notificaciones por correo electrónico, debe activar la opción **Notificar por correo electrónico** en el grupo de notificación. Esta opción de notificación está desactivada de forma predeterminada. La opción **Notificar por correo electrónico** requiere que se defina como mínimo una dirección de destino. (Opcionalmente, puede agregar direcciones de copia y direcciones de copia oculta si lo desea).

Esta sección incluye los siguientes temas:

- Configuración de un servidor de correo electrónico
- Configuración de una plantilla de notificación por correo electrónico

Configuración de un servidor de correo electrónico

Complete los pasos de este procedimiento para configurar un servidor de correo electrónico.

NOTE: También debe configurar los ajustes del grupo de notificación, incluida la activación de la opción **Notificar por correo electrónico**, antes de que los mensajes de alerta por correo electrónico los envíe el sistema. Para obtener más información sobre cómo especificar eventos para recibir alertas de correo electrónico, consulte Configuración de grupos de notificación.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la configuración de la Lista de Cores del lado izquierdo de la página Configuración, haga clic en **Servidor SMTP**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado **Servidor SMTP**.
3. Haga clic en la opción que desee cambiar.

   La opción seleccionada se volverá editable.
4. Introduzca la información de configuración según se describe en la tabla siguiente.

Opción	Descripción
Servidor SMTP	Introduzca el nombre del servidor de correo electrónico que debe utilizar la plantilla de notificación de correo electrónico. La convención de asignación de nombres incluye el nombre de host, dominio y sufijo; por ejemplo, smtp.gmail.com.
De	Escriba una dirección de correo electrónico de remite. Se utiliza para especificar la dirección de correo electrónico de respuesta en la plantilla de notificaciones de correo electrónico; por ejemplo, noreply@localhost.com.
Nombre de usuario	Escriba un nombre de usuario para el servidor de correo electrónico.
Contraseña	Introduzca la contraseña asociada con el nombre de usuario necesaria para acceder al servidor de correo electrónico.

Opción	Descripción
Puerto	Escriba 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.
Tiempo de espera (segundos)	Introduzca un valor entero para especificar durante cuánto tiempo se debe intentar la conexión con el servidor de correo electrónico. Se utiliza para establecer el tiempo de espera en segundos. El valor predeterminado es 60 segundos.
TLS	Seleccione esta opción si el servidor de correo utiliza una conexión segura como Transport Layer Security (TLS) o Secure Sockets Layer (SSL).

5. Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en ✓ para guardar los cambios y salir del modo edición, o haga clic en ✕ para salir del modo sin guardar.

   CAUTION: Si no confirma cada cambio, la configuración no cambiará.

6. Haga clic en › **Enviar correo electrónico de prueba** y, a continuación, haga lo siguiente:
   a. En el cuadro de diálogo **Enviar correo electrónico de prueba**, introduzca una dirección de correo electrónico de destino para el mensaje de prueba y, a continuación, haga clic en **Enviar**.
   b. Si falla el mensaje de prueba, cierre el cuadro de diálogo de error y de **Enviar correo electrónico de prueba** y revise la configuración del servidor de correo electrónico. A continuación, envíe el mensaje de prueba otra vez.
   c. Una vez que el mensaje de prueba es correcto, haga clic en **Aceptar** para confirmar que la operación se ha realizado correctamente.
   d. Compruebe la cuenta de correo electrónico a la que ha enviado el mensaje de correo electrónico de prueba.

Configuración de una plantilla de notificación por correo electrónico

Cuando se habilitan las notificaciones de los eventos de Rapid Recovery por correo electrónico, se crea una plantilla predeterminada de forma predeterminada. El servidor de correo electrónico SMTP definido en el Core utiliza esta plantilla para enviar notificaciones de los eventos de Rapid Recovery por correo electrónico.

En este tema se describe el proceso de configuración de la plantilla de notificaciones del correo electrónico predeterminado o la personalización del contenido. Con la opción Restaurar valores predeterminados, puede restaurar los cambios en la plantilla de notificaciones predeterminada en cualquier momento.

CAUTION: Modifique la plantilla bajo su propia responsabilidad. Es responsable de probar las modificaciones realizadas en la plantilla. Solo se admite la plantilla predeterminada.

Complete los pasos de este procedimiento para configurar la plantilla de notificación de correo electrónico.

NOTE: También debe configurar un servidor de correo electrónico y ajustes del grupo de notificación, incluida la activación de la opción **Notificar por correo electrónico**, para poder enviar mensajes de alertas de correo electrónico. Para obtener más información sobre cómo configurar un servidor de correo electrónico para enviar alertas, consulte Configuración de un servidor de correo electrónico. Para obtener más información sobre cómo especificar eventos para recibir alertas de correo electrónico, consulte Configuración de grupos de notificación.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Notificaciones**.

   Aparecerá la página **Notificaciones**.
3. En el panel Configuración de correo electrónico, haga clic en **Cambiar**.

   Aparecerá el cuadro de diálogo **Editar configuración de notificación por correo electrónico**.
4. Seleccione **Activar notificaciones por correo electrónico**.

   La plantilla de correo electrónico se encuentra activada y también visible. Los valores de la plantilla de correo electrónico predeterminada se describen en el siguiente paso.
5. Revise el contenido en el cuadro de diálogo Editar configuración de notificación por correo electrónico y determine si el contenido predeterminado se adapta a sus necesidades.

Opción	Descripción
Habilitar notificaciones por correo electrónico	Esta configuración activa o desactiva la plantilla de notificaciones de correo electrónico. • Para habilitar las notificaciones por correo electrónico, seleccione esta opción. • Para desactivar las notificaciones por correo electrónico, borre esta opción.
Asunto del correo electrónico	El contenido de este campo de texto controla la línea de asunto para los mensajes de correo electrónico enviados como las notificaciones de eventos del sistema. La línea de asunto del correo electrónico predeterminado es la siguiente: `<hostName> <level>: <name> for <agentName>`

Correo electrónico	El contenido de esta área de texto controla el cuerpo para los mensajes de correo electrónico enviados como las notificaciones de eventos del sistema. El mensaje del cuerpo del correo electrónico predeterminado es el siguiente:
	`<shortCompanyName> <coreProductName> on <hostName> has reported the <level> event "<name>"`
	`Date/Time: <localTimestamp>`
	`<message>`
	`<if(details.errorDetails)>`
	`<details.ErrorDetails.Message>`
	`<details.ErrorDetails.Details>`
	`<endif>`
	`---`
	`About this event: <description>`
	`<coreAdminUrl>`

Opción	Descripción
Enviar correo electrónico de prueba	Al hacer clic en este botón se envía un mensaje de correo electrónico de prueba a la dirección de correo electrónico que se especifique en el cuadro de diálogo **Enviar correo electrónico de prueba**.
Restaurar valores predeterminados	Al hacer clic en este botón elimina los cambios personalizados de la plantilla de correo electrónico y restaura el asunto del correo electrónico y los campos del correo electrónico con el contenido predeterminado que se describe en esta tabla.
Aceptar	Al hacer clic en este botón confirma y guarda la configuración en el cuadro de diálogo Editar configuración de notificación por correo electrónico.
Cancelar	Al hacer clic en este botón se cancela cualquier cambio en el cuadro de diálogo Editar configuración de notificación por correo electrónico.

6. Si desea personalizar la plantilla de correo electrónico, realice los cambios en el texto o las variables descritas en el paso anterior. Las variables que se utilizan en los valores predeterminados se describen en la tabla siguiente.

Opción	Descripción
hostName	Nombre de host del Core
details	Los objetos de detalles del evento específico.
agentName	El nombre del equipo protegido asociado a este evento, si el evento tiene un ámbito de un único equipo protegido.
repositoryName	El nombre del repositorio asociado a este evento, si el evento tiene un ámbito de repositorio.
jobSummary	El resumen del trabajo asociado a este evento, si el evento tiene un ámbito de trabajo.
remoteSlaveCoreName	El nombre del Core de destino remoto asociado a este evento, si el evento tiene un ámbito de Core de destino.
remoteMasterCoreName	El nombre del Core de origen remoto asociado a este evento, si el evento tiene un ámbito de Core de origen.
productName	El nombre del producto, por ejemplo "AppAssure Core" o "Rapid Recovery Core". Este nombre de producto puede cambiarse para las marcas que utilizan el etiquetado blanco.

Opción	Descripción
companyName	El nombre de la compañía que vende el producto.

7. En el cuadro de texto **Asunto del correo electrónico**, introduzca un asunto para la plantilla de correo electrónico.

   Esta opción se utiliza para definir el asunto de la plantilla de notificaciones de correo electrónico; por ejemplo, <hostname> - <level>: <name>.

8. En el cuadro de texto **Correo electrónico**, escriba la información para el texto de la plantilla que describe el evento, cuándo se ha producido y la gravedad.
9. Haga clic en **Enviar correo electrónico de prueba** y, a continuación, haga lo siguiente:
   a. En el cuadro de diálogo Enviar correo electrónico de prueba, introduzca una dirección de correo electrónico de destino para el mensaje de prueba y, a continuación, haga clic en **Enviar**.
   b. Si falla el mensaje de prueba, cierre el cuadro de diálogo de error y de Enviar correo electrónico de prueba, haga clic en **Aceptar** para guardar la configuración de la plantilla del correo electrónico actual. Y, a continuación, modifique la configuración del servidor de correo electrónico según se describe en el procedimiento Configuración de un servidor de correo electrónico. Asegúrese de que ha vuelto a introducir la contraseña de esa cuenta de correo electrónico. Guarde esa configuración y, a continuación, vuelva a este procedimiento.
   c. Una vez que el mensaje de prueba es correcto, haga clic en **Aceptar** para confirmar que la operación se ha realizado correctamente.
   d. Compruebe la cuenta de correo electrónico a la que ha enviado el mensaje de correo electrónico de prueba.

Una vez que esté satisfecho con los resultados de las pruebas, vuelva al cuadro de diálogo Editar configuración de notificación por correo electrónico y haga clic en **Aceptar** para cerrar el cuadro de diálogo y guardar los ajustes.

Configuración de valores de eventos

Puede configurar ciertos valores específicos de eventos.

Por ejemplo, puede establecer los valores de reducción de repeticiones para reducir la cantidad de notificaciones que ve de eventos repetidos idénticos.

También puede establecer la cantidad de tiempo, en días, que se conservan los registros de eventos en la base de datos.

Vea los temas siguientes para obtener información sobre la configuración de valores de eventos.

- Acerca de la reducción de repeticiones
- Configuración de la retención de eventos

Referencia relacionada

See also: Visualización de eventos mediante las páginas de tareas, alertas y del diario
See also: Comprensión de las notificaciones de eventos en Rapid Recovery

Acerca de la reducción de repeticiones

La capacidad de los administradores de recibir notificaciones sobre la periodicidad de ciertos eventos es de vital importancia. Sin embargo, en ciertas circunstancias, la recepción de una notificación repetida de eventos de los que ya está al tanto puede ser también frustrante e incómodo. Incluso si se genera una notificación debido a un error del entorno que desee conocer inmediatamente, es posible que el mismo estado de error genere cientos o miles de eventos en el mismo registro de eventos. Para reducir la repetición en el registro de eventos y reducir los inconvenientes de recibir alertas del sistema y notificaciones de correo electrónico repetidas para el mismo

evento en la Core Console, Rapid Recovery incluye una configuración de reducción de repeticiones que se habilita de forma predeterminada y se establece a los 5 minutos. Este parámetro puede ajustarse tan bajo como 1 minuto y tan alto como 60 minutos. También puede desactivarse completamente.

Cuando la reducción de repeticiones está desactivada, cada vez que se produzca un evento del mismo tipo y ámbito, se registrará en la base de datos. Sin importar la cantidad de tiempo que haya transcurrido desde que se produjo el evento anteriormente, cada nueva incidencia se mostrará en la parte Alertas de la página Eventos.

Cuando se habilita la reducción de repeticiones (por ejemplo, con el tiempo predeterminado de 5 minutos), la primera vez que se produzca ese evento específico, se registrará en la base de datos de eventos y se mostrará en el registro de alertas. Si más tarde se registra de nuevo un evento del mismo tipo y ámbito dentro del umbral de tiempo establecido, el recuento del evento en la base de datos aumentará en 1 por cada incidencia de repetición dentro de ese umbral. El registro se muestra en la parte Alertas de la página Eventos. Sin embargo, muestra el evento una única vez, con la fecha y la hora de la aparición más reciente. El registro de eventos no está actualizado con el mismo evento hasta que caduque el umbral de tiempo desde la primera aparición. Por ejemplo, si se establece en 5 minutos y el evento ocurre de nuevo 6 minutos más tarde, aparecerá en el registro y recibirá otra notificación.

Configuración de la reducción de repeticiones

Complete los pasos de este procedimiento para configurar la reducción de repeticiones de los eventos.

1. Vaya a la Rapid Recovery Core Console. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Notificaciones**.

   Aparecerá la página **Notificaciones**.
2. En el panel Reducción de repeticiones, verá la configuración existente.
3. Para activar, desactivar o cambiar el tiempo umbral de los eventos guardados, haga clic en **Cambiar**.

   Aparece el cuadro de diálogo **Editar reducción de repeticiones**
4. Realice uno de los siguientes pasos:
   - Para desactivar la reducción de repeticiones, desmarque la opción **Habilitar reducción de repeticiones**.
   - Para activar la reducción de repeticiones, seleccione la opción **Habilitar reducción de repeticiones**.
   - Para cambiar el umbral de tiempo (en minutos) para el que se ignoran los eventos idénticos repetidos, en el cuadro de texto **__ minutos**, introduzca un número entre 1 y 60.

   NOTE: La opción **Habilitar reducción de repeticiones** debe estar seleccionada para cambiar este valor.
5. Haga clic en **Aceptar** para guardar la configuración y cerrar el cuadro de diálogo.

Configuración de la retención de eventos

Los eventos y trabajos a los que se les realiza un seguimiento en el Core se guardan durante una cantidad de tiempo determinada. La configuración predeterminada es 30 días. Este número se puede establecer entre los 0 y 3652 días (aproximadamente 10 años).

Complete los pasos de este procedimiento para configurar la retención de los eventos.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Conexión de base de datos**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado **Conexión de base de datos**.

   Aparecerá la configuración de conexión de base de datos.
3. Para cambiar la cantidad de días durante los cuales la información de eventos se guarda en la base de datos, haga clic en el campo de texto **Periodo de retención (días)**, introduzca un valor entre 0 y 3652 y, a continuación, haga clic en para guardar el cambio.

   El periodo de retención de eventos se ajusta según lo especificado.

Emisión de informes

En esta sección se proporciona una descripción general de los informes disponibles en la Rapid Recovery Core Console.

Acerca de los informes de Rapid Recovery

Puede generar estos informes desde la Rapid Recovery Core Console. También se espera que otros informes estén disponibles desde el Portal de protección de datos.

Los informes disponibles desde la Core Console se describen en la siguiente tabla.

Tabla 111. Informes de Rapid Recovery

Tipo de informe	Descripción
Informe de trabajos	Ofrece un informe básico sobre el estado de los trabajos correctos, los trabajos con fallos y los trabajos con errores. Los trabajos con fallos pueden verse más adelante en un informe de error. • De manera predeterminada, el intervalo de tiempo es durante los últimos 31 días. Sin embargo, se puede personalizar. • Cuando se ejecuta desde el Core, este informe puede especificar los detalles de uno o más Cores.De manera predeterminada, este conjunto de información incluye los trabajos de todos los equipos: servidores de bases de datos, equipos protegidos, equipos replicados y equipos de puntos de recuperación únicamente de los Core especificados. Puede usar los parámetros de informe para personalizar el informe. Use los filtros para seleccionar o excluir equipos. También puede seleccionar o excluir los trabajos que son independientes del equipo, en cuyo caso el informe solo muestra el estado de los trabajos del Core. Para obtener más información sobre este tipo de informe, consulte Descripción del informe de trabajo.
Informe de resumen de trabajos	Proporciona un informe más detallado sobre el estado de los trabajos realizados correctamente, los trabajos con fallos y los trabajos con errores que muestra una línea independiente para cada tipo de trabajo, lo que permite un mejor diagnóstico de los posibles problemas. • De manera predeterminada, el intervalo de tiempo es durante los últimos 31 días. Sin embargo, se puede personalizar. • A diferencia del informe de trabajos, este informe no ofrece una selección de Cores como un parámetro. • De manera predeterminada, este conjunto de información incluye los trabajos de todos los equipos: servidores de bases de datos, equipos protegidos, equipos replicados y equipos de puntos de recuperación únicamente y trabajos dependientes de equipos, por tipo de trabajo. Puede personalizar el informe. Use los filtros para seleccionar o

Tipo de informe	Descripción
	excluir equipos. También puede seleccionar o excluir los trabajos independientes de equipos. • Cuando se ejecuta desde la perspectiva de un equipo protegido desde la Core Console, el informe resultante muestra el estado de los trabajos solo para ese equipo protegido. Para obtener más información sobre este tipo de informe, consulte Comprensión del informe de resumen de trabajos.
Informe de error	Proporciona información sobre los trabajos de Core con fallos para los criterios especificados. Este informe puede incluir detalles de equipos protegidos, o excluirlos. Como el informe de trabajos, este informe solo se puede ejecutar desde un equipo protegido seleccionado en el Core. El informe resultante muestra detalles sobre los trabajos con fallos solo para el equipo protegido seleccionado. Para obtener más información sobre este tipo de informe, consulte Comprensión del informe de error.
Informe de resumen	Proporciona información de resumen.De manera predeterminada, en esta información se incluyen los trabajos para todos los equipos protegidos: todos los equipos protegidos, equipos replicados y equipos de punto de recuperación únicamente de los Cores especificados. Puede usar los parámetros de informe para personalizar el informe. Use los filtros para seleccionar o excluir equipos. También puede seleccionar o excluir los trabajos que son independientes del equipo, en cuyo caso el informe solo muestra el estado de los trabajos del Core. Este informe no está disponible desde la perspectiva de cualquier equipo protegido único. Las categorías de la información de este informe incluyen el Core, la licencia y el repositorio. La información se muestra en forma de lista, gráfico y tabla Para obtener más información sobre este tipo de informe, consulte Comprensión del informe de resumen.
Informe de repositorio	Este tipo de informe le proporciona un informe de todos los repositorios en el Core o los Cores seleccionados. También puede seleccionar un único repositorio disponible en el Core. Este informe muestra solo la perspectiva del Core. Para obtener más información sobre este tipo de informe, consulte Descripción del informe del repositorio.
Informe de resumen clásico	Este informe proporciona una vista de resumen de estadísticas de éxito del trabajo, resúmenes de repositorios por GB, éxito de instantáneas, tendencia de uso de repositorios y un resumen de las máquinas protegidas en su Core. Los parámetros de informe incluyen rango de fechas y el Core pertinente.
Informe programado	También puede programar cualquiera de estos informes desde la Core Console. La programación de un informe hace que el informe que especifique se genere de forma repetida en el programa que defina. De forma opcional, puede establecer las notificaciones por correo electrónico cada vez que se genera un informe. Para obtener más información sobre la programación, modificación, pausa o eliminación de informes, consulte Administración de informes programados desde la Core Console.

En función del tipo de informe y los parámetros que haya seleccionado, puede generar un informe en uno o más Cores de Rapid Recovery o para uno o más equipos protegidos.

Generación de un informe desde la Core Console

Puede generar informes a petición desde la Core Console. Deben aplicarse las siguientes reglas:

- Todos los informes se pueden generar desde la perspectiva del Core.
- Además, se pueden generar dos tipos de trabajos (el informe de trabajos y el informe de error) desde la perspectiva de un equipo protegido. En estos informes, los datos se generan solo para que pertenezcan al equipo seleccionado.
- Los informes de error contienen datos solo si han fallado los trabajos seleccionado en los Cores seleccionados (o equipos protegidos).

El método para generar informes a petición es similar, si el informe se genera a partir del objetivo del Core o si se genera desde la perspectiva de un equipo protegido. Sin embargo, la navegación es algo diferente.

También puede programar informes para generarlos de forma repetida. Para obtener más información sobre la programación, modificación, pausa o eliminación de informes, consulte Administración de informes programados desde la Core Console.

Generación de un informa del Core a petición

Como se describe en el tema Acerca de los informes de Rapid Recovery, se pueden generar todos los informes disponibles desde la Core Console.

Realice los pasos del siguiente procedimiento para generar un informe desde la perspectiva del Rapid Recovery Core.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Informes**.

   Aparece la página **Informe de trabajos**. A la derecha del nombre del informe en el título de la página hay una flecha hacia abajo, con la que puede seleccionar otro tipo de informe.

   Si desea generar un informe de trabajos, continúe con el paso 6 para empezar a especificar los criterios del informe.
3. Para elegir otro tipo de informe, haga clic en la flecha situada a la derecha del nombre del informe para ver un menú con los informes disponibles.
4. Para definir informes programados, consulte Programación de un informe.
5. Para generar solo un informe de repositorio, vaya al paso 11.
6. Para generar un informe de trabajos, de resumen de trabajos, de fallos, de resumen o de Core (clásico), en el menú desplegable **Intervalo de fechas**, seleccione un intervalo de fechas.

   Si no se elige un rango de fechas, se usa la opción predeterminada, últimos 31 días. Puede elegir entre las opciones de la siguiente tabla.

Opción	Descripción
Últimas 24 horas	Actividad de los informes del último día, relativa a la hora el que generó el informe.
Últimos 7 días	Actividad de los informes de la última semana, relativa a la hora en que generó el informe.

Opción	Descripción
Últimos 31 días	Informe sobre la actividad de los 31 últimos días, en relación con la hora en que se genera el informe.
Últimos 90 días	Informe sobre la actividad de los 90 últimos días, en relación con la hora en que se genera el informe.
Últimos 365 días	Actividad de los informes del último año, relativa a la hora en que generó el informe.
Todo el tiempo	Este periodo de tiempo abarca la vida útil del Core.
Personalizado	Este periodo de tiempo requiere que especifique las fechas de inicio y finalización.
Mes hasta la fecha	Informe sobre la actividad desde el primer día del mes natural en curso hasta la fecha en que se genera el informe.
Año hasta la fecha	Informe sobre la actividad desde el primer día del año natural en curso hasta la fecha en que se genera el informe.

NOTE: En todos los casos, no hay datos para el informe anteriores a la implementación del Core, ni anteriores a la protección de los equipos en el Core.

7. En el caso de un informe de trabajos, de errores o de Core (clásico), en el menú desplegable **Cores de destino**, seleccione los Cores para los que desee generar el informe.

   La selección predeterminada incluye todos los Cores disponibles.

8. En el menú desplegable **Equipos protegidos**, seleccione los equipos para los que desea generar el informe.

   De manera predeterminada, en esta información se incluyen los trabajos para todos los equipos protegidos: todos los equipos protegidos, equipos replicados y equipos de punto de recuperación únicamente de los Cores especificados. Puede usar los parámetros de informe para personalizar el informe. Use los filtros para seleccionar o excluir equipos. También puede seleccionar o excluir los trabajos que son independientes del equipo, en cuyo caso el informe solo muestra el estado de los trabajos del Core.

   Puede elegir entre:

Opción	Descripción
Seleccionar todo	Esta opción le permite seleccionar todos los equipos protegidos de este Core. **NOTE:** Puede seleccionar todos los equipos y, a continuación, borrar algunos de ellos para especificar solo un subconjunto de la totalidad.
Independiente de equipo	Seleccione esta opción para generar un informe que incluya los trabajos de un Core pero no de equipos concretos. Trabajos como la creación o eliminación de un repositorio, o la creación de un CD de inicio, no están asociados a un equipo concreto. Si va a implementar el software Agent en un equipo

Opción	Descripción
	que aún no está protegido, este tipo de trabajo también se considera independiente del equipo. Estos trabajos no tienen un equipo protegido en la columna de equipo protegido del informe resultante. Por el contrario, si implementa el software Agent en un equipo ya protegido en el Core, el nombre del equipo protegido se incluye en el informe. No se considera independiente del equipo.
Equipos protegidos	Esta opción enumera todos los equipos protegidos de este Core. Puede seleccionarlos todos o solo algunos de los equipos protegidos.
Solo puntos de recuperación	Esta opción muestra los equipos que estuvieron protegidos, pero todavía tienen puntos de recuperación guardados en el repositorio.
[Cores de origen]	Si el Core es un Core de destino y replica puntos de recuperación de cualquier equipo protegido de un Core de origen, aparece el nombre de ese Core de origen (en mayúsculas). Esta opción enumera todos los equipos protegidos de ese Core de origen. Puede seleccionar todos los equipos replicados en este Core de destino o seleccionar solo algunos de ellos.
[Grupos personalizados]	Si tiene grupos personalizados creados en este Core, el nombre de cada grupo personalizado aparece como opción. Aparece cada objeto del grupo personalizado. Puede seleccionar todos los objetos en el grupo o solo algunos de ellos.

9. Si va a generar un informe de resumen, vaya al paso 12.
10. En el caso de informes de trabajos, errores o de resumen de trabajos, en el menú desplegable **Tipos de trabajo**, seleccione los tipos de trabajo que desee.

    De manera predeterminada, en esta información se incluyen todos los trabajos de los equipos protegidos seleccionados. Puede usar los parámetros de informe para personalizar el informe. Use los filtros para seleccionar o excluir los trabajos de la categoría de trabajos principales y todos los trabajos de la categoría de otros trabajos. También puede expandir cada una de estas categorías al definir parámetros de trabajo y seleccionar solo los tipos de trabajo de cada categoría que desea incluir en el informe. Active la casilla de cualquier tipo de trabajo para seleccionarlo o borrarlo. Puede seleccionar todos los trabajos de una u otra categoría, o solo algunos de ellos.

    Puede elegir entre los siguientes tipos de **otros** trabajos:
11. En el caso de un informe de repositorio, en el menú Repositorios, seleccione los repositorios que desea incluir en el informe.

    La selección predeterminada incluye todos los repositorios disponibles.
12. Haga clic en **Vista previa** para generar el informe con los criterios especificados.

Si no se encuentran los criterios de informe que ha seleccionado, el informe se genera, pero contiene una fila vacía. Por ejemplo, si no hay errores, el contenido de la columna Error es nulo en el informe.

13. Realice uno de los siguientes pasos:
    - Vea el informe generado en línea.
    - Actualice el informe dinámicamente cambiando los criterios; a continuación, vuelva a hacer clic en **Vista previa**.
    - Use el menú **Informes** para seleccionar un formato de exportación (incluido el formato predeterminado, PDF) y, a continuación, haga clic en  para exportar el informe. Para obtener más información sobre el menú Informes, consulte Uso del menú de informes.
    - Utilice la **barra de herramientas Informes** para ver, manipular o imprimir el informe. Para obtener más información sobre la barra de herramientas Informes, consulte Uso de la barra de herramientas de informes.

Generación de un informe de equipo protegido a petición

Puede generar un informe de trabajos o un informe de error para cualquier equipo protegido.

Realice los pasos del procedimiento siguiente para generar un informe para un equipo protegido.

1. Vaya a la Rapid Recovery Core Console.
2. Desde el menú Equipos protegidos, haga clic en el equipo protegido para el que quiere ver un informe.

   Aparece la página **Resumen** para el equipo protegido seleccionado.
3. En la parte superior de la página, desde las opciones del menú que se encuentran al lado del nombre del equipo protegido, haga clic en la flecha hacia abajo junto a Informes y, a continuación, seleccione un tipo de informe.
   - Si desea generar un informe de todos los trabajos que pertenecen a este equipo protegido, incluidos los trabajos con fallos, haga clic en **Informe de trabajos** y empiece especificado los criterios de su informe.
   - Si desea generar una lista de los trabajos con fallos que pertenece solo a este equipo protegido, haga clic en **Informe de error** y empiece especificando los criterios de su informe.
4. Para un informe de error o de trabajos, desde el menú desplegable **Rango de fechas**, seleccione un rango de fechas.

   Si no se elige un rango de fechas, se usa la opción predeterminada, últimos 31 días. Puede elegir entre las opciones de la siguiente tabla.

Opción	Descripción
Últimas 24 horas	Actividad de los informes del último día, relativa a la hora el que generó el informe.
Últimos 7 días	Actividad de los informes de la última semana, relativa a la hora en que generó el informe.
Últimos 31 días	Actividad de los informes de los últimos 31 días, relativa a la hora en que generó el informe.

Opción	Descripción
Últimos 90 días	Informe sobre la actividad de los 90 últimos días, en relación con la hora en que se genera el informe.
Últimos 365 días	Actividad de los informes del último año, relativa a la hora en que generó el informe.
Todo el tiempo	Este periodo de tiempo abarca la vida útil del Core.
Personalizado	Este periodo de tiempo requiere que especifique las fechas de inicio y finalización.
Mes hasta la fecha	Informe sobre la actividad desde el primer día del mes natural en curso hasta la fecha en que se genera el informe.
Año hasta la fecha	Informe sobre la actividad desde el primer día del año natural en curso hasta la fecha en que se genera el informe.

NOTE: En todos los casos, no hay datos para el informe anteriores a la implementación del Core, ni anteriores a la protección de los equipos en el Core.

5. Desde el menú desplegable **Tipos de trabajos**, seleccione los tipos de trabajos adecuados.

   De manera predeterminada, en esta información se incluyen todos los trabajos de los equipos protegidos seleccionados. Puede usar los parámetros de informe para personalizar el informe. Use los filtros para seleccionar o excluir los trabajos de la categoría de trabajos principales y todos los trabajos de la categoría de otros trabajos. También puede expandir cada una de estas categorías al definir parámetros de trabajo y seleccionar solo los tipos de trabajo de cada categoría que desea incluir en el informe. Active la casilla de cualquier tipo de trabajo para seleccionarlo o borrarlo. Puede seleccionar todos los trabajos de una u otra categoría, o solo algunos de ellos.

6. Haga clic en **Vista previa** para generar el informe con los criterios especificados.

   Si no se encuentran los criterios de informe que ha seleccionado, el informe se genera, pero contiene una fila vacía. Por ejemplo, si no hay errores, el contenido de la columna Error es nulo en el informe.

7. Realice uno de los siguientes pasos:

   - Vea el informe generado en línea.
   - Actualice el informe dinámicamente cambiando los criterios; a continuación, vuelva a hacer clic en **Vista previa**.
   - Utilice el **menú Informes** para seleccionar un formato de exportación y exportar el informe. Para obtener más información sobre el menú Informes, consulte Uso del menú de informes.
   - Utilice la **barra de herramientas Informes** para ver, manipular o imprimir el informe. Para obtener más información sobre la barra de herramientas Informes, consulte Uso de la barra de herramientas de informes.

Administración de informes programados desde la Core Console

Puede programar cualquiera de los informes disponibles desde la Core Console. La programación de un informe hace que éste se genere repetidamente en el futuro. El programa define si el informe se va a generar de forma diaria, semanal o mensual.

De manera opcional, Rapid Recovery permite enviar una notificación por correo electrónico a uno o más destinatarios cuando se genera cada informe. El correo electrónico especifica el tipo, el formato y el rango de fechas del informe e incluye el informe como un adjunto.

NOTE: Antes de que pueda enviar los informes por correo electrónico, debe configurar un servidor SMTP para el Core. Para obtener más información, consulte Configuración de un servidor de correo electrónico.

Si elige o no enviar notificaciones por correo electrónico, puede guardar los informes generados de forma local o en una ubicación de red accesible al servidor del Core.

Debe especificar la notificación y la entrega por correo electrónico o una ubicación para guardar los informes. También puede elegir ambas opciones.

Esta sección incluye los siguientes temas:

- Programación de un informe
- Modificación de una programación de informe
- Cómo pausar, reanudar o eliminar un informe programado

Conceptos relacionados

See also: Cómo pausar, reanudar o eliminar un informe programado

Tareas relacionadas

See also: Programación de un informe
See also: Modificación de una programación de informe

Programación de un informe

Puede programar un informe disponible desde la Core Console. El informe genera el programa que definió hasta que pause o elimine el informe.

Debe especificar la notificación y la entrega por correo electrónico o una ubicación para guardar los informes. También puede elegir ambas opciones.

Complete los pasos de este procedimiento para programar un informe.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Informes**.

   Aparece la página **Informe de trabajos**. Aparece una flecha hacia abajo a la derecha del nombre del informe actual.
3. Haga clic en la flecha situada a la derecha del nombre del informe y, en el menú desplegable, seleccione **Informes programados**.

   Aparece la página **Informes programados**.
4. Para programar la generación de un informe de forma repetida, haga clic en **Agregar**.

Aparece el **Definir Asistente de programación de informes**.

5. En la página **Configuración** del asistente, introduzca los detalles para el informe que quiere programar y, a continuación, haga clic en **Siguiente**. Estas opciones de configuración se describen en la tabla siguiente.

Tabla 112. Opciones de configuración del informe programado

Equipo	Informes disponibles
Nombre	Escriba el nombre de visualización que quiere asignar a este programa particular. El nombre predeterminado es Schedule report 1. Límite su nombre a 64 caracteres o menos. No utilice caracteres prohibidos ni frases prohibidas.
Formato de informe	Seleccione un formato de salida de informe. Si no selecciona un valor, se utiliza el formato predeterminado (pdf).
Tipo de informe	Seleccione el tipo de informe que desea generar de forma repetida.
Etiquetas	Seleccione las etiquetas que desea que aparezcan en el informe programado. Se requiere al menos una etiqueta. La función Grupos personalizados permite agrupar objetos de Core en un contenedor lógico, para el que define una etiqueta. Mediante el parámetro Etiquetas del asistente Definir Asistente de programación de informes, puede seleccionar un grupo personalizado para el que se ejecutan los informes programados. Si no hay etiquetas personalizadas, las opciones disponibles en el menú desplegable Etiquetas incluyen Seleccionar todo y Equipos protegidos. Si aparecen grupos personalizados, cada grupo aparece como una opción. Puede seleccionar o borrar cualquiera de las opciones para incluir o excluir esos objetos en el informe programado.
Equipo protegido	Seleccione uno o más equipos protegidos que se incluirán en el informe. Esta opción no está disponible para el informe de repositorio.
Tipos de trabajos	Seleccione los tipos de trabajo que desea que aparezcan en el informe. De manera predeterminada, en esta información se incluyen los trabajos para todos los equipos protegidos: todos los equipos protegidos, equipos replicados y equipos de punto de recuperación únicamente de los Cores especificados. Puede usar los parámetros de informe para personalizar el informe. Use los filtros para seleccionar o excluir equipos. También puede seleccionar o excluir los trabajos que son independientes del equipo, en cuyo caso el informe solo muestra el estado de los trabajos del Core. Los parámetros de Tipos de trabajos no están disponibles para los tipos de informes Resumen del Core y Repositorio programado.

6. En la página **Destino** del asistente, seleccione un destino para los informes que quiere programar. Debe seleccionar uno de los siguientes y es posible que seleccione ambos. Cuando esté satisfecho con el resultado, haga clic en **Siguiente**.

   - En el campo **Enviar a las direcciones de correo electrónico**, introduzca una o más direcciones de correo electrónico válidas para notificar a los usuarios por mensaje de correo electrónico cuando se genera un informe programado.

NOTE: Si no especifica las notificaciones por correo electrónico y la entrega, debe especificar una ubicación de almacenamiento.

- Seleccione **Guardar como archivo** para guardar los archivos del informe generado en una ubicación que especifique y, en el menú desplegable **Tipo de ubicación**, seleccione una opción de almacenamiento local, de red o de nube. A continuación, en el campo **Ubicación**, especifique información adicional de la ubicación como se describe en la tabla siguiente.

Tabla 113. Opciones de ubicación para los informes programados

Tipo de ubicación	Descripción del tipo de ubicación	Ubicación
Local	Seleccione el tipo de ubicación Local para guardar los informes generados en una ruta de acceso local accesible para el Core.	Especifique la ruta de acceso en el campo Ubicación. Escriba una ubicación accesible de forma local para el Core. Por ejemplo, para guardar los informes en la carpeta Informes en la unidad D, introduzca `D:\Reports\`.
Red	Seleccione el tipo de ubicación Red para guardar los informes generados en una ruta de acceso accesible para el Core en la red. Especifique la ruta de acceso en el campo Ubicación.	Especifique la ruta de acceso en el campo Ubicación. Escriba una ubicación accesible para el Core desde la red. Utilice el formato \\nombreServidor \nombreRecursoCompartido. Por ejemplo, para guardar los informes en el servidor Datos en la carpeta compartida denominada Informes, introduzca `\\Data\Reports\`. Especificar credenciales de red en los campos Nombre de usuario y Contraseña.
Nube	Seleccione el tipo de ubicación Nube para guardar los informes generados en una cuenta de almacenamiento de nube configurada en el Core. La cuenta de almacenamiento debe estar ya definida antes de realizar este paso. Para obtener información sobre cómo configurar una cuenta de almacenamiento de nube para trabajar con el Core, consulte Cuentas en la nube.	Desde el campo Cuenta, seleccione la cuenta de almacenamiento de nube adecuada que se va a utilizar para guardar los informes generados. Desde el campo Contenedor, especifique un contenedor adecuado en la cuenta de almacenamiento. Desde el campo Nombre de la carpeta, especifique una carpeta en la que se van a guardar los informes generados en el futuro.

7. Cuando esté satisfecho con sus opciones de destino, haga clic en **Siguiente**.
8. En la página del asistente de **calendario de programación**, desde el menú **Enviar datos**, seleccione una opción para determinar la frecuencia en la que se debe generar el informe que especificó. Puede generar informes diaria, semanal o mensualmente. Cada opción tiene sus propios parámetros, tal como se describe en la tabla siguiente.

Tabla 114. Opciones de frecuencia para generar informes programados

Frecuencia	Detalles de frecuencia	Parámetros de frecuencia
Diariamente	Genera y guarda o envía el informe especificado una vez al día a la hora especificada.	Para cambiar la hora predeterminada en la que se genera el informe, en el campo de texto Hora,

Frecuencia	Detalles de frecuencia	Parámetros de frecuencia
	La hora predeterminada para esta acción es las 12:00 AM (en función de la hora del servidor del Core).	escriba un valor nuevo o utilice los controles para cambiar la hora, los minutos y AM o PM.
Semanalmente	Genera y guarda o envía una vez por semana el informe especificado a una hora especificada del día especificado.	Para cambiar el día predeterminado en que se genera el informe, desde el menú Día de la semana, seleccione un día de la semana.
	La hora predeterminada para esta acción es las 12:00 del domingo (en función de la hora del servidor del Core).	Para cambiar la hora predeterminada en la que se genera el informe, en el campo de texto Hora, escriba un valor nuevo o utilice los controles para cambiar la hora, los minutos y AM o PM.
Mensualmente	Genera y guarda o envía una vez al mes el informe especificado en una fecha y hora específica del día.	Para cambiar la fecha predeterminada en que se genera el informe, desde el menú Día del mes, seleccione una fecha.
	La fecha predeterminada para esta acción es el primer día de cada mes a las 12:00 AM (en función de la hora del servidor del Core).	Para cambiar la hora predeterminada en la que se genera el informe, en el campo de texto Hora, escriba un valor nuevo o utilice los controles para cambiar la hora, los minutos y AM o PM.

9. De manera opcional, en la página del asistente **Programa**, si desea evitar que el informe programado se genere hasta que reanude los informes en pausa, seleccione **Realizar pausa en la creación de informes inicialmente**.

   Si quiere que este informe se genere según lo programado, desmarque esta opción.

10. Cuando esté satisfecho con el programa, haga clic en **Finalizar** para salir del asistente y guardar su trabajo.

    La nueva programación de un informe aparece en la tabla de resumen Informes de resumen.

Modificación de una programación de informe

Una vez que se ha programado un informe, puede modificar cualquiera de sus parámetros o en detalles. Puede editar la información de configuración del informe (nombre del informe, formato de salida, tipo de informe) incluidos los repositorios. También puede cambiar opciones de notificación por correo electrónico y el destino para guardar el informe generado. Por último, también puede cambiar la programación del informe.

Realice los pasos de este procedimiento para modificar los parámetros de un informe programado.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Informes**.

   Aparece la página **Informe de trabajos**. Aparece una flecha hacia abajo a la derecha del nombre del informe actual.

3. Haga clic en la flecha situada a la derecha del nombre del informe y, en el menú desplegable, seleccione **Informes programados**.

   Aparece la página **Informes programados**.

4. En la tabla de resumen Informes programados, en la fila del informe que desea modificar, haga clic en (Más opciones) y, a continuación, seleccione **Editar**.

Aparece el **Definir Asistente de programación de informes**.

5. Desplácese por las páginas del asistente y cambie los parámetros necesarios. Para obtener más información sobre los parámetros de este asistente, consulte el tema Programación de un informe.
6. En la página **Programa** página del asistente, haga clic en **Finalizar** para cerrar el asistente y guardar los cambios.

   El asistente se cierra y se modifica la programación del informe.

Cómo pausar, reanudar o eliminar un informe programado

Una vez se haya programado un informe, lo genera en el programa definido. Si quiere detener de forma temporal la generación de un informe programado, puede pausar el programa.

Si un informe programado se pone en pausa y desea reanudar la generación del informe, puede reanudar el informe tal como se describe en este procedimiento.

Si actualmente está generando un informe programado y ya no necesita generar ese informe, puede eliminarlo.

Para determinar si cualquier informe programado está en pausa, compruebe la columna de estado de la tabla de resumen de informes programados. Una esfera verde indica un informe programado activo; una esfera amarilla indica un programa pausado y una esfera roja indica un error.

Realice los pasos de este procedimiento para poner en pausa, reanudar o eliminar un programa para un informe.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Más) y, a continuación, seleccione **Informes**.

   Aparece la página **Informe de trabajos**. Aparece una flecha hacia abajo a la derecha del nombre del informe actual.
3. Haga clic en la flecha situada a la derecha del nombre del informe y, en el menú desplegable, seleccione **Informes programados**.

   Aparece la página **Informes programados**.
4. En la tabla de resumen Informes programados, vea el estado de todos los informes programados, mediante los indicadores de colores.
5. Para cada informe que desea pausar o reanudar, seleccione la casilla de verificación de la primera columna.
6. Desde las opciones Informes programados que se encuentran encima de la tabla de resumen, haga lo siguiente:
   - Para pausar la generación de los informes seleccionados, haga clic en **Pausar**.
   - Para reanudar la generación de informes programados que se ha pausado, haga clic en **Reanudar**.
   - Para eliminar los programas seleccionados de los informes programados existentes, haga clic en **Eliminar**.

     La eliminación de un informe programado solo impide la generación de informes futuros. Si se han guardado los informes programados anteriores, no se eliminan.

Uso del menú de informes

El menú Informes aparece en la parte superior de la página cuando se visualiza Informes. Este menú incluye un título del informe, que es también un menú desplegable que permite ver los tipos de informes disponibles. Debajo de este menú hay uno o varios filtros que le ayudarán a definir su criterios de informe.

Los filtros concretos disponibles dependen del tipo de informe. Para obtener información sobre los parámetros correspondientes a cada tipo de informe, consulte el tema en el que se describen los tipos de informe.

En la parte derecha del menú Informes hay ciertos controles. Estos controles, que se describen en la siguiente tabla, ayudan a generar y exportar el informe.

Tabla 115. Controles del menú Informes

Elemento de la IU	Descripción
Botón Vista previa	Haga clic en el botón Vista previa para generar un informe basado en el tipo de informe seleccionado y los parámetros de informe especificados en los filtros.
Menú desplegable de formato de exportación	El menú desplegable de exportación permite seleccionar un formato de salida del informe. Si no selecciona un valor, se utiliza el formato predeterminado (pdf).
Botón/icono Descargar	El botón Descargar permite exportar el informe generado en el tipo de formato seleccionado en el menú de exportación.

Los informes incluyen unidades de medida que permiten determinar más fácilmente si una columna se representa en GB, TB o segundos.

Si no le gusta el aspecto de un informe generado o exportado, puede cambiar la fuente utilizada en los informes. Para obtener más información, consulte Administración de la configuración de informes.

Una vez que se genera un informe, puede usar la barra de herramientas de informes.

See also: Descripción del informe de trabajo
See also: Comprensión del informe de error
See also: Comprensión del informe de resumen

Uso de la barra de herramientas de informes

Una vez lo haya creado en el menú Informes, el informe aparece debajo de una barra de herramientas Informes. La barra de herramientas puede ayudarle a manipular salida del informe, incluido el guardado y la impresión de los informes.

En la parte izquierda de la barra de herramientas, hay una opción de la barra lateral Alternar. Esta herramienta expande o contrae la barra lateral, lo que da acceso a algunas opciones de visualización más. A la derecha de la barra de herramientas, la opción Herramientas expande un menú desplegable que proporciona controles de navegación de informe. Los elementos de la barra de herramientas Informes se describen en la tabla siguiente.

Tabla 116. Icono de la barra de herramientas de informes

Icono	Descripción
	**Barra lateral Alternar.** Todas las páginas del informe se muestran como imágenes en miniatura. Otras opciones de la barra lateral no son compatibles.
	**Barra lateral: Mostrar miniaturas**. Esta es la vista predeterminada para todas las páginas de un informe generado.

Icono	Descripción
	**Barra lateral: Mostrar resumen del documento**. Esta función no es compatible.
	**Barra lateral: Mostrar archivos adjuntos**. No hay archivos adjuntos para los informes. Esta función no es compatible.
	**Buscar**. Permite buscar texto dentro del informe generado. Incluye las opciones para resaltar todo el texto que coincide con los criterios que ha introducido y también para hacer coincidir mayúsculas y minúsculas.
	**Página anterior**. Mover la vista del informe a la página anterior.
	**Página siguiente**. Pasar a la página siguiente en la vista del informe.
	**Introducir número de página.** Haga clic en el campo de texto del número de página, introduzca un número de página válido y pulse Entrar para pasar a esa página en la vista del informe.
	**Alejar.** Permite alejar la vista del informe generado. Cada vez que hace clic aleja más, hasta un mínimo del 25%.
	**Acercar**. Permite acercar la vista del informe generado. Cada vez que hace clic acerca más, hasta un máximo del 1000%.
	**Zoom automático**. Permite controlar la vista del zoom del informe generado, incluida la vista por tamaño real, ajuste de página, ancho completo o porcentaje, incluido el 50%, 75%, 100%, 125%, 150%, 200%, 300% o 400%.
	**Abrir archivo.** Permite navegar por el sistema de archivos para buscar y abrir un informe guardado.
	**Imprimir.** Permite imprimir el informe generado.
	**Herramientas.** El menú desplegable Herramientas se expande o contrae al hacer clic en este icono. Las opciones Herramientas se describen a continuación.
	**Herramientas: Ir a la primera página**. Permite navegar a la primera página del informe generado.
	**Herramientas: Ir a la última página**. Permite navegar a la última página del informe generado.
	**Herramientas: Girar hacia la derecha**. Esta opción rota el lienzo del informe generado en el sentido de las agujas del reloj.
	**Herramientas: Girar hacia la izquierda**. Esta opción rota el lienzo del informe generado en el sentido contrario a las agujas del reloj.

Icono	Descripción
	**Herramientas: Herramienta de mano**. Cuando se selecciona esta herramienta, permite mover el informe haciendo clic y arrastrándolo a lo largo de la pantalla.
	**Herramientas: Propiedades del documento**. Proporciona información sobre las propiedades del documento del informe generado. Haga clic en **Cerrar** para cerrar la ventana.

Para obtener información sobre cómo generar un informe, consulte Generación de un informe desde la Core Console.

Descripción del informe de trabajo

El informe de trabajos está disponible para el Rapid Recovery Core y los equipos protegidos en el Core. Este informe ofrece un método de ver el estado de los trabajos realizados por un Core o un equipo protegido seleccionado. Las filas o columnas que aparecen en el informe sin datos indican que el parámetro probado era nulo. Por ejemplo, si una columna (por ejemplo, Errores) aparece sin información, no se han producido errores para el registro seleccionado. Si el informe genera una fila en blanco, el trabajo del registro seleccionado refleja una actividad independiente de equipo.

Para obtener información sobre cómo generar un informe de trabajos del Core, consulte Generación de un informa del Core a petición. Para obtener información sobre cómo generar un informe de trabajos para un equipo protegido, consulte Generación de un informe de equipo protegido a petición.

Cuando genera un informe de trabajos, los detalles del informe incluyen lo siguiente:

- Criterios de selección del informe
- Una tabla de resumen que muestra una fila para cada trabajo en el rango de fechas que haya especificado. Además de incluir el Core, el equipo protegido y el tipo de trabajo adecuados, cada fila incluye:
  - Un resumen del trabajo
  - El estado del trabajo
  - Los errores relacionados con el trabajo
  - Las fechas de inicio y finalización del trabajo
  - La duración del trabajo en segundos
  - El trabajo total en MB

Si la información no es relevante para una categoría específica, la celda aparece sin información en el informe. Por ejemplo, si el Core para un equipo protegido especificado no tiene errores, la columna Error está en blanco en aquella fila del informe.

Comprensión del informe de resumen de trabajos

El informe de resumen de trabajos está disponible al realizar informes solo desde la perspectiva del Core; este informe no está disponible desde los informes de un equipo protegido. Este informe tiene un único resumen, que muestra información de resumen sobre todos los trabajos realizados en el Core, incluido un recuento de trabajos

con errores, pasados y cancelados. Muestra más información que el informe de trabajos, porque especifica cada trabajo en una línea independiente del informe.

Para obtener información sobre cómo generar un informe de resumen de trabajos, consulte Generación de un informe desde la Core Console.

Los parámetros de este tipo de informe incluyen:

- Rango de fechas
- Equipos protegidos
- Tipos de trabajo

Al generar un informe de resumen de trabajos, los detalles del informe incluyen los criterios de selección del informe, así como información sobre equipos protegidos, volúmenes y tipos de trabajos.

Información del Core

La parte del Core del informe de resumen incluye datos con respecto alRapid Recovery Core que se está reportando. Esta información incluye:

- El número de equipos protegidos delRapid Recovery Core
- El número de equipos con trabajos con fallos

Resumen de equipos protegidos

La parte de equipos protegidos del informe de resumen incluye datos de todos los equipos protegidos por el Rapid Recovery Core seleccionado y los volúmenes de esos equipos.

El gráfico muestra una línea para cada tipo de trabajo de cada equipo e incluye la proporción de trabajos realizados correctamente (de cualquier tipo), el número de trabajos pasados, el número de trabajos con errores y de trabajos cancelados. (Los trabajos cancelados no se tienen en cuenta para estas estadísticas).

Comprensión del informe de error

El informe de errores es un subconjunto del informe de trabajos y está disponible para el Rapid Recovery Core y los equipos protegidos en el Core. Un informe de error solo incluye los trabajos cancelados y con fallos indicados en el informe de trabajos y los compila en un único informe que se puede imprimir y exportar. Si el informe se genera con una fila en blanco, no hay errores en el rango de fechas especificado de los criterios de su informe.

NOTE: Los resultados de los parámetros de los equipos protegidos y de los Core de destino aparecen solo para el informe a nivel del Core.

Para obtener información sobre cómo generar un informe de trabajos del Core, consulte Generación de un informa del Core a petición. Para obtener información sobre cómo generar un informe de trabajos para un equipo protegido, consulte Generación de un informe de equipo protegido a petición.

Cuando se genera un informe de error, aparece una tabla de resumen que muestra una fila para cada trabajo en el rango de fechas especificado. Además de incluir el Core, el equipo protegido y el tipo de trabajo adecuados, cada fila incluye:

- Un resumen del trabajo
- El estado del trabajo
- Los errores relacionados con el trabajo
- Las fechas de inicio y finalización del trabajo
- La duración del trabajo en segundos
- El trabajo total en MB

Comprensión del informe de resumen

El informe de resumen está disponible para uno o más núcleos. Este informe no está disponible en los informes de un equipo protegido. El informe de resumen incluye información sobre los repositorios del Rapid Recovery Core seleccionado y sobre los equipos protegidos por ese Core. La información aparece como dos resúmenes dentro de un informe.

Para obtener información sobre cómo generar un informe de resumen, consulte Generación de un informe desde la Core Console.

Los parámetros de este tipo de informe incluyen:

- Rango de fechas
- Equipos protegidos

Al generar un informe de resumen, los detalles del informe incluyen los criterios de selección del informe, así como información sobre repositorios y equipos protegidos.

Información del Core

La parte del Core del informe de resumen incluye datos con respecto alRapid Recovery Core que se está reportando. Esta información incluye:

- La clave de licencia (identificador)
- La versión actual del software Rapid Recovery Core

Resumen de repositorios

La parte de repositorios del informe de resumen incluye datos de los repositorios ubicados en el Rapid Recovery Core seleccionado. Esta información incluye:

- El número de repositorios en el Core de Rapid Recovery
- Un resumen de repositorios en el Core.

Resumen de equipos protegidos

La parte de equipos protegidos del informe de resumen incluye datos de todos los equipos protegidos por los Cores o el Rapid Recovery Core seleccionados. Incluye un gráfico y una tabla de resumen.

El gráfico muestra los equipos protegidos por el índice de trabajos correctos (de cualquier tipo), comparado con los trabajos con fallos. (Los trabajos cancelados no se tienen en cuenta para estas estadísticas).

La X o eje horizontal muestra el número de equipos protegidos. La Y o eje vertical muestra los niveles de trabajos correctos. Específicamente, el eje Y muestra, por equipo protegido, cuántos de ellos habían:

- Trabajos no realizados
- Tasa de menos del 50% correctos
- Tasa del 50% o más correctos
- Tasa del 100% correctos

Debajo del gráfico aparece información sobre los equipos protegidos. Esta información incluye:

- La cantidad de equipos protegidos
- El número de equipos protegidos con trabajos con fallos
- Una tabla de resumen, por equipo protegido, que muestra lo siguiente:
  - Nombre del equipo protegido
  - Volúmenes protegidos por el equipo
  - Espacio protegido, en GB (total y actual)
  - Velocidad de cambio por día (promedio y mediana)
  - Estadísticas del trabajo (satisfactorio, completado, con fallos, cancelado)
  - Si se ha aplicado el cifrado
- La versión del Core

Descripción del informe del repositorio

El informe de repositorio incluye información sobre los repositorios del Rapid Recovery Core seleccionado y sobre los equipos protegidos por ese Core. La información aparece como dos resúmenes dentro de un informe.

Para obtener información sobre cómo generar un informe de repositorio del Core, consulte Generación de un informa del Core a petición.

Los parámetros de este tipo de informe solo incluyen repositorios.

Al generar un informe de repositorio, los detalles del informe de cada repositorio incluyen una lista de resumen de repositorios en el Core.

Comprensión del informe de resumen clásico

El informe de resumen clásico proporciona un resumen del periodo seleccionado de diversas métricas útiles para su Core.

En la parte superior se pueden ver tres gráficos circulares. El primero muestra estadísticas de trabajo (trabajos correctos, cancelados y con errores). El segundo muestra el espacio por repositorio en GB. El tercero muestra estadísticas de instantánea (trabajos correctos, cancelados y con errores).

A continuación hay un gráfico de tendencias que muestra el uso de los repositorios.

El informe concluye con un resumen de los equipos protegidos.

Los parámetros de informe de este tipo de informe incluyen intervalo de fechas y el Core pertinente.

Para obtener información sobre cómo generar este informe del Core, consulte Generación de un informa del Core a petición.

Exportación de la MV

Este capítulo describe cómo exportar un punto de recuperación para crear una máquina virtual.

Exportación a máquinas virtuales con Rapid Recovery

En el Rapid Recovery Core, puede exportar un punto de recuperación de un equipo Windows o Linux a una máquina virtual (VM) en uno de los varios formatos admitidos. Si el equipo protegido original del Core falla, puede iniciar la máquina virtual para sustituirlo rápidamente de manera temporal, lo que permite recuperar el equipo protegido original sin un tiempo de inactividad importante. Este proceso de exportación virtual crea una VM con toda la información de copia de seguridad de un punto de recuperación, así como del sistema operativo y de la configuración del equipo protegido. La máquina virtual se convierte en un clon de inicio de un equipo protegido.

NOTE: El punto de recuperación utilizado debe formar parte de una cadena de puntos de recuperación completa. Para obtener más información sobre las cadenas de puntos de recuperación, consulte el tema Cadenas del punto de recuperación y huérfanos.

Puede realizar una exportación virtual desde la página **En espera virtual** de la Core Console, desde un punto de recuperación específico que se muestre en el Core o seleccionando **Exportación de VM** en el menú desplegable  **Restaurar** de la barra de botones.

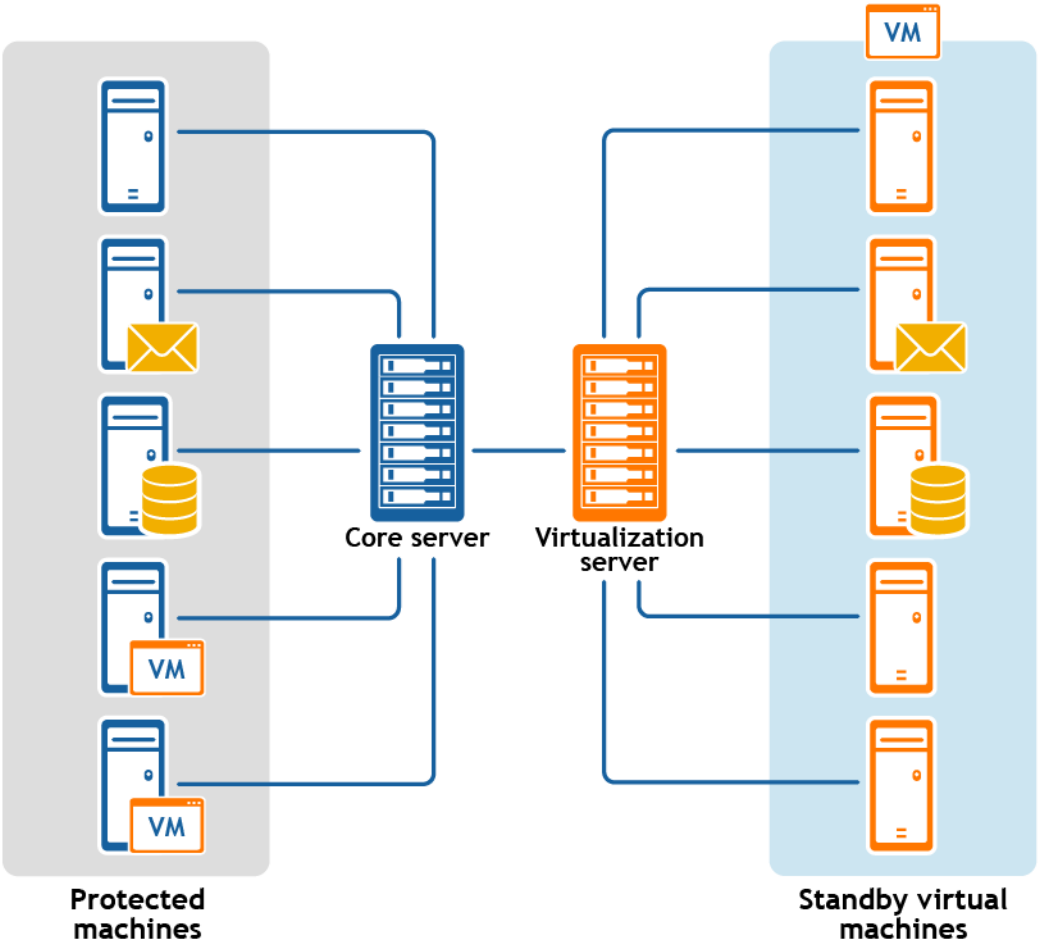
Cuando realiza una exportación virtual desde el Rapid Recovery Core, tiene dos opciones:

- Puede realizar una **única exportación virtual**, que crea una VM de inicio que representa una única instantánea en el tiempo de la información en el punto de recuperación. La tarea de exportación se pone en cola inmediatamente y, una vez finalizada la operación, la VM clonada se exporta a la ubicación especificada. La información de configuración que se utiliza para una exportación puntual no se guarda.
- Puede configurar **una exportación continua**. Este proceso crea una máquina virtual de inicio del punto de recuperación original que especificó, guardando la VM en la ubicación especificada. La información de configuración para realizar esa exportación virtual se guarda en la página **En espera virtual** en la Core Console. Posteriormente, cada vez que se capture una nueva instantánea del equipo protegido, el Core pone en cola un nuevo trabajo de exportación virtual y la VM de inicio se actualiza con la información actualizada. Debido a que este proceso crea un recurso de alta disponibilidad para la recuperación de datos, esta función también se llama **espera virtual**.

Entre el momento en que se pone en cola una exportación virtual y se completa, el trabajo se muestra en el panel Cola de exportación de la página Espera virtual en la Core Console.

El siguiente diagrama muestra una implementación típica para exportar datos a una máquina virtual.

Figura 5. Implementación en espera virtual



NOTE: En una configuración que implica replicación, el Core mostrado representa el Core de destino. 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.

Los hipervisores de VM compatibles incluyen vCenter/ESXi, VMware Workstation, Hyper-V, VirtualBox y Azure. Para obtener información acerca de las versiones compatibles de los hipervisores, consulte el tema "Requisitos de hipervisor" en el *Rapid Recovery System Requirements Guide (Guía de requisitos del sistema de Rapid Recovery)*.

Para ESXi, VMware Workstation o Hyper-V, la versión de la máquina virtual debe ser una versión con licencia de estas máquinas virtuales; no una versión de prueba o gratuita. La exportación a Azure requiere que tenga una cuenta en Azure, con otros requisitos previos.

NOTE: Para Azure, una implementación de eventos o eventual crea una VM mediante la gestión de VM clásica, no mediante el nuevo modelo de administrador de recursos. Trabajar con Azure conlleva aspectos únicos de ese proveedor de servicios en la nube. Para obtener más información, consulte Antes de la exportación virtual a Azure.

Conceptos relacionados

See also: Exportación de datos a una máquina virtual ESXi
See also: Exportación de datos a una máquina virtual VMWare Workstation
See also: Exportación de datos a una máquina virtual VirtualBox
See also: Exportación de datos a una máquina virtual Azure

Tareas relacionadas

See also: Administración de exportaciones

Referencia relacionada

See also: Exportación de datos a una máquina virtual Hyper-V

Exportación de datos a una máquina virtual ESXi

En Rapid Recovery, puede decidir exportar datos a ESXi realizando una exportación única o estableciendo una exportación continua (para el estado en espera virtual). Realice los pasos de los procedimientos siguientes para el tipo de exportación adecuado.

Cómo realizar una exportación de ESXi puntual

Realice los pasos de este procedimiento para realizar una exportación puntual a ESXi.

1. En la Core Console de Rapid Recovery, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, haga clic en **Exportación de la MV**.
2. En el Asistente de exportación de máquinas virtuales, seleccione **Exportación única**.
3. Haga clic en **Siguiente**.
4. En la página Equipos, seleccione el equipo protegido que desea exportar.
5. Haga clic en **Siguiente**.
6. En la página Puntos de recuperación, seleccione el punto de recuperación que desea utilizar para la exportación.
7. Haga clic en **Siguiente**.
8. En la página **Destino** del asistente Exportación, en el menú desplegable Exportar a una máquina virtual, seleccione **ESX(i)**.
9. Introduzca los parámetros para acceder a la máquina virtual según se describen en la tabla siguiente y, a continuación, haga clic en **Siguiente**.

Tabla 117. Parámetros de la máquina virtual

Opciones	Descripción
Nombre de host	Escriba un nombre para el equipo host.
Puerto	Escriba el puerto para el equipo host. El valor predeterminado es 443.
Nombre de usuario	Introduzca el nombre de usuario para iniciar sesión en el equipo host.
Contraseña	Introduzca la contraseña para iniciar sesión en el equipo host.

10. En la página Opciones de máquina virtual, introduzca la información como se describe en la tabla siguiente.

Tabla 118. Opciones de máquina virtual

Opción	Descripción
Grupo de recursos	Seleccione un bloque de recursos de la lista desplegable.

Opción	Descripción
Almacenamiento de configuración de la máquina virtual	Seleccione un almacén de datos de la lista desplegable.
Nombre de la máquina virtual	Introduzca un nombre para la máquina virtual.
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: • Utilizar la misma cantidad de RAM que el equipo de origen • Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.
Número de procesadores	El número de procesadores (CPU) que desea para la máquina virtual exportada. El mínimo es 1.
Núcleos por procesador	El número de núcleos que desea tener para cada procesador. El mínimo es 1.
Aprovisionamiento de discos	Seleccione el tipo de aprovisionamiento de discos a partir de las siguientes opciones: • Compacto. El aprovisionamiento compacto crea un disco virtual con el tamaño del espacio utilizado en los volúmenes originales, en lugar de con el tamaño de todo el volumen. Por ejemplo, si el volumen original es 1 TB, pero contiene solo 2 GB de espacio utilizado, Rapid Recovery crea un disco virtual de 2 GB. • Grueso. El aprovisionamiento grueso crea un nuevo disco o volumen del mismo tamaño que el volumen original del servidor protegido, incluso si solo se está utilizando una parte del volumen original. Por ejemplo, si el volumen es de 1 TB pero contiene solo 2 GB de espacio utilizado, Rapid Recovery crea un disco virtual de 1 TB.
Asignación de discos	Especifique el tipo de asignación de discos a partir de las siguientes opciones: • Automático • Manual • Con VM
Versión	En la lista desplegable, seleccione la versión de ESXi que se vaya a utilizar para crear la máquina virtual.

11. Haga clic en **Siguiente**.
12. En la página **Volúmenes**, seleccione los volúmenes que desee exportar y, a continuación, haga clic en **Siguiente**.
13. En la página **Resumen**, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

NOTE: Puede supervisar el estado y el progreso de la exportación visualizando las páginas **En espera virtual** o **Eventos**.

Configuración de la exportación continua a ESXi

Complete los pasos de este procedimiento para configurar la exportación continua a una máquina virtual ESXi (VM) mediante Rapid Recovery. Esto también se conoce como configuración de la espera virtual.

1. En la Rapid Recovery Core Console, realice una de las acciones siguientes:

   - En la Core Console, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, seleccione **Exportación de la MV**.

     1. En el Asistente de exportación de máquinas virtuales, seleccione **Continuo (servidor virtual en espera)**.
     2. Haga clic en **Siguiente.**

   - En la Core Console, en la barra de iconos, haga clic en (Espera virtual).

     - En la página **En espera virtual**, haga clic en **Agregar** para iniciar el Asistente de exportación de máquinas virtuales.

2. En la página **Equipos** del Asistente de exportación de máquinas virtuales, seleccione el equipo protegido que quiere exportar.
3. Haga clic en **Siguiente**.
4. En la página **Puntos de recuperación**, seleccione el punto de recuperación que quiere utilizar para la exportación.
5. Haga clic en **Siguiente**.
6. En la página **Destino** del Asistente de exportación, en el menú desplegable Recuperar en una máquina virtual, seleccione **ESXi**.
7. Introduzca la información para acceder a la máquina virtual según se describe en la tabla siguiente y, a continuación, haga clic en **Siguiente**.

Tabla 119. Credenciales de ESXi

Opción	Descripción
Nombre de host	Escriba un nombre para el equipo host.
Puerto	Escriba el puerto para el equipo host. El valor predeterminado es 443.
Nombre de usuario	Escriba las credenciales de inicio de sesión para el equipo host.
Contraseña	Escriba las credenciales de inicio de sesión para el equipo host.

8. En la página **Opciones de máquina virtual**, introduzca la información como se describe en la tabla siguiente.

Tabla 120. Opciones de máquina virtual

Opción	Descripción
Grupo de recursos	Seleccione un bloque de recursos de la lista desplegable.

Opción	Descripción
Almacén de datos	Seleccione un almacén de datos de la lista desplegable.
Nombre de la máquina virtual	Introduzca un nombre para la máquina virtual.
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: • Utilizar la misma cantidad de RAM que el equipo de origen • Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.
Número de procesadores	El número de procesadores (CPU) que desea para la máquina virtual exportada. El mínimo es 1.
Núcleos por procesador	El número de núcleos que desea tener para cada procesador. El mínimo es 1.
Aprovisionamiento de discos	Seleccione el tipo de aprovisionamiento de discos a partir de las siguientes opciones: • Compacto. El aprovisionamiento compacto crea un disco virtual con el tamaño del espacio utilizado en los volúmenes originales, en lugar de con el tamaño de todo el volumen. Por ejemplo, si el volumen original es 1 TB, pero contiene solo 2 GB de espacio utilizado, Rapid Recovery crea un disco virtual de 2 GB. • Grueso. El aprovisionamiento grueso crea un nuevo disco o volumen del mismo tamaño que el volumen original del servidor protegido, incluso si solo se está utilizando una parte del volumen original. Por ejemplo, si el volumen es de 1 TB, pero contiene 2 GB de espacio utilizado, Rapid Recovery crea un disco virtual de 1 TB.
Asignación de discos	Especifique el tipo de asignación de discos apropiado (Automática, Manual o con VM).
Versión	Seleccione la versión de la máquina virtual.
Realizar exportación única inicial	Seleccione para realizar la exportación virtual inmediatamente en lugar de hacerlo después de la próxima instantánea programada (opcional).

9. Haga clic en **Siguiente**.
10. En la página **Volúmenes**, seleccione los volúmenes que desee exportar y, a continuación, haga clic en **Siguiente**.
11. En la página **Resumen**, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

NOTE: Puede supervisar el estado y el progreso de la exportación visualizando las páginas En espera virtual o Eventos.

Exportación de datos a una máquina virtual VMWare Workstation

En Rapid Recovery puede exportar datos a VMware Workstation realizando una exportación puntual o estableciendo una exportación continua (para el estado en espera virtual). Realice los pasos de los procedimientos siguientes para el tipo de exportación adecuado.

Cómo realizar una exportación de VMWare Workstation puntual

Realice los pasos de este procedimiento para realizar una exportación puntual a VMware Workstation.

1. En la Core Console de Rapid Recovery, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, haga clic en **Exportación de la MV**.
2. En el Asistente de exportación de máquinas virtuales, seleccione **Exportación única**.
3. Haga clic en **Siguiente**.
4. En la página **Equipos**, seleccione el equipo protegido que quiere importar.
5. Haga clic en **Siguiente**.
6. En la página **Puntos de recuperación**, seleccione el punto de recuperación que quiere utilizar para la exportación.
7. Haga clic en **Siguiente**.
8. En la página **Destino** del asistente Exportación, en el menú desplegable Exportar a una máquina virtual, seleccione **VMware Workstation** y, a continuación, haga clic en **Siguiente**.
9. En la página **Opciones de máquina virtual**, introduzca los parámetros para acceder a la máquina virtual tal como se describen en la tabla siguiente.

Tabla 121. Parámetros de la máquina virtual

Opción	Descripción
Ubicación de VM	Especifique la ruta de acceso de la carpeta local o recurso compartido de red en el que crear la máquina virtual. **NOTE:** Si ha especificado una ruta de acceso compartida de red, tendrá que escribir credenciales de inicio de sesión válidas para una cuenta registrada en el equipo de destino. La cuenta debe tener permisos de lectura y escritura en el recurso compartido de red.
Nombre de usuario	Introduzca las credenciales de inicio de sesión de la ubicación de red de la exportación. • Si ha especificado una ruta de acceso compartida de red, debe especificar un nombre de usuario válido para una cuenta registrada en el equipo de destino. • Si ha especificado una ruta de acceso local, no hace falta nombre de usuario.
Contraseña	Introduzca las credenciales de inicio de sesión de la ubicación de red de la exportación. • Si ha especificado una ruta de acceso compartida de red, tendrá que especificar una contraseña válida para una cuenta registrada en el equipo de destino. • Si ha especificado una ruta de acceso local, no hace falta contraseña.

Opción	Descripción
Nombre de VM	Escriba un nombre para la máquina virtual que se está creando; por ejemplo, VM-0A1B2C3D4. **NOTE:** el nombre predeterminado es el nombre del equipo de origen.
Versión	Especifique la versión de VMware Workstation para la máquina virtual. Puede elegir entre: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0
Cantidad de RAM (MB)	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: • Utilizar la misma cantidad de RAM que el equipo de origen • Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.
Número de procesadores	El número de procesadores (CPU) que desea para la máquina virtual exportada. El mínimo es 1.
Núcleos por procesador	El número de núcleos que desea tener para cada procesador. El mínimo es 1.

10. Haga clic en **Siguiente**.
11. En la página **Volúmenes**, seleccione los volúmenes que desee exportar, por ejemplo, C:\ y D:\, y, a continuación, haga clic en **Siguiente**.
12. En la página **Resumen**, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

NOTE: Puede supervisar el estado y el progreso de la exportación visualizando las páginas **En espera virtual**o **Eventos**.

Configuración de una exportación continua a VMware Workstation

Complete los pasos de este procedimiento para realizar una exportación continua a una máquina virtual (VM) VMware Workstation con Rapid Recovery. Esto también se conoce como configuración de la espera virtual.

1. En la Rapid Recovery Core Console, realice una de las acciones siguientes:
   - En la Core Console, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, seleccione **Exportación de la MV**.

1. En el Asistente de exportación de máquinas virtuales, seleccione **Continuo (servidor virtual en espera)**.
2. Haga clic en **Siguiente.**

- En la Core Console, en la barra de iconos, haga clic en (Espera virtual).
  - En la página **En espera virtual**, haga clic en **Agregar** para iniciar el Asistente de exportación de máquinas virtuales.

2. En la página **Equipos** del Asistente de exportación de máquinas virtuales, seleccione el equipo protegido que quiere exportar.
3. Haga clic en **Siguiente**.
4. En la página **Puntos de recuperación**, seleccione el punto de recuperación que quiere utilizar para la exportación.
5. Haga clic en **Siguiente**.
6. En la página **Destino** del Asistente de exportación de máquinas virtuales, en el menú desplegable Recuperar en una máquina virtual, seleccione **VMware Workstation** y, a continuación, haga clic en **Siguiente**.
7. En la página **Opciones de máquina virtual**, introduzca los parámetros para acceder a la máquina virtual tal como se describen en la tabla siguiente.

Tabla 122. Parámetros de la máquina virtual

Opción	Descripción
Ruta de acceso al destino	Especifique la ruta de acceso de la carpeta local o recurso compartido de red en el que crear la máquina virtual. **NOTE:** Si ha especificado una ruta de acceso compartida de red, tendrá que escribir credenciales de inicio de sesión válidas para una cuenta registrada en el equipo de destino. La cuenta debe tener permisos de lectura y escritura en el recurso compartido de red.
Nombre de usuario	Introduzca las credenciales de inicio de sesión de la ubicación de red de la exportación. • Si ha especificado una ruta de acceso compartida de red, debe especificar un nombre de usuario válido para una cuenta registrada en el equipo de destino. • Si ha especificado una ruta de acceso local, no hace falta nombre de usuario.
Contraseña	Introduzca las credenciales de inicio de sesión de la ubicación de red de la exportación. • Si ha especificado una ruta de acceso compartida de red, tendrá que especificar una contraseña válida para una cuenta registrada en el equipo de destino. • Si ha especificado una ruta de acceso local, no hace falta contraseña.
Máquina virtual	Escriba un nombre para la máquina virtual que se está creando; por ejemplo, VM-0A1B2C3D4. **NOTE:** el nombre predeterminado es el nombre del equipo de origen.

Opción	Descripción
Versión	Especifique la versión de VMware Workstation para la máquina virtual. Puede elegir entre: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: • Utilizar la misma cantidad de RAM que el equipo de origen • Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.
Número de procesadores	El número de procesadores (CPU) que desea para la máquina virtual exportada. El mínimo es 1.
Núcleos por procesador	El número de núcleos que desea tener para cada procesador. El mínimo es 1.

8. Seleccione **Realizar exportación única inicial** para realizar la exportación virtual inmediatamente en lugar de hacerlo después de la próxima instantánea programada.
9. Haga clic en **Siguiente**.
10. En la página **Volúmenes**, seleccione los volúmenes que desee exportar, por ejemplo, C:\ y D:\, y, a continuación, haga clic en **Siguiente**.
11. En la página **Resumen**, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

NOTE: Puede supervisar el estado y el progreso de la exportación visualizando las páginas En espera virtual o Eventos.

Exportación de datos a una máquina virtual Hyper-V

En Rapid Recovery, puede exportar datos a una exportación de Hyper-V realizando una exportación puntual o estableciendo una exportación continua (para el estado en espera virtual).

Para obtener información sobre sistemas operativos de host compatibles de primera generación y de segunda generación que Hyper-V exporta, consulte el tema "Requisitos de hipervisor" en la *Rapid Recovery System Requirements Guide (Guía de requisitos del sistema de Rapid Recovery)*.

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

Cómo realizar una exportación de Hyper-V puntual

Realice los pasos de este procedimiento para realizar una exportación puntual a Hyper-V.

1. En la Rapid Recovery Core Console, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, haga clic en **Exportación de la MV**.
2. En el Asistente de exportación de máquinas virtuales, seleccione **Exportación única**.
3. Haga clic en **Siguiente**.
4. En la página **Equipos**, seleccione el equipo protegido que quiere importar.
5. Haga clic en **Siguiente**.
6. En la página **Puntos de recuperación**, seleccione el punto de recuperación que quiere utilizar para la exportación.
7. Haga clic en **Siguiente**.
8. En la página **Destino**, en el menú desplegable Exportar a máquina virtual, seleccione **Hyper-V**.
9. Para exportar a un equipo local con el rol Hyper-V asignado, haga clic en **Utilizar equipo local**.
10. Para indicar que el servidor Hyper-V se encuentra en un equipo remoto, haga clic en **Host remoto** y, a continuación, introduzca la información del host remoto como se describe en la tabla siguiente.

Tabla 123. Información de host remoto

Cuadro de texto	Descripción
Nombre de host	Especifique la dirección IP o el nombre de host para el servidor Hyper-V. Representa la dirección IP o nombre de host del servidor Hyper-V remoto.
Puerto	Especifique un número de puerto para el equipo. Representa el puerto por el que el Core se comunica con este equipo.
Nombre de usuario	Especifique el nombre de usuario para el usuario con permisos administrativos para la estación de trabajo con el servidor Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.
Contraseña	Especifique la contraseña para la cuenta de usuario con permisos administrativos en la estación de trabajo con el servidor Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.

11. Haga clic en **Siguiente**.
12. En la página **Opciones de máquinas virtuales** del cuadro de texto **Ubicación de la máquina virtual**, introduzca la ruta de acceso de la máquina virtual; por ejemplo, `D:\export`. Esto se utiliza para identificar la ubicación de la máquina virtual.

    NOTE: Debe especificar la ubicación de la máquina virtual tanto para los servidores locales como remotos de Hyper-V. La ruta de acceso debe ser una ruta de acceso local válida para el servidor Hyper-V. Los directorios que no existan se crean automáticamente. No debería intentar crearlos manualmente. La exportación a carpetas compartidas (por ejemplo a `\\data\share`) no está permitida.
13. En el cuadro de texto **Nombre de la máquina virtual**, introduzca un nombre para la máquina virtual.

El nombre que especifique aparecerá en la lista de máquinas virtuales en la consola Administrador de Hyper-V.

14. Para especificar el uso de la memoria, haga clic en una de las opciones siguientes:
    - **Utilizar la misma cantidad de RAM que el equipo de origen**. Seleccione esta opción para identificar que el uso de RAM es idéntico entre los equipos virtuales y de origen.
    - **Utilizar una cantidad específica de RAM.** Seleccione esta opción si desea especificar la cantidad de RAM en MB.

      La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.
15. Para especificar el formato de disco, junto a Formato de disco, haga clic en una de las siguientes opciones:
    - VHDX
    - VHD

    NOTE: La exportación de Hyper-V admite formatos de disco VHDX si el equipo de destino ejecuta Windows 8 (Windows Server 2012) o posterior. Si VHDX no se admite para su entorno, la opción está desactivada.

    NOTE: Si está exportando a Hyper-V de segunda generación, solo se admite la operación de formato de disco VHDX.
16. Para especificar la generación de Hyper-V que hay que emplear para la exportación, haga clic en uno de los siguientes elementos:
    - Generación 1
    - Generación 2

    NOTE: Solo la segunda generación admite la opción de inicio seguro.
17. Especifique el adaptador de red apropiado para la VM exportada.
18. En la página **Volúmenes**, seleccione los volúmenes que se van a exportar, por ejemplo, C:\.

    NOTE: Si los volúmenes seleccionados tienen mayor capacidad que las asignaciones máximas apropiadas admitidas por la aplicación como se indica a continuación, o bien superan la cantidad de espacio disponible, aparecerá un error.
    - Para el formato de disco VHDX, sus volúmenes seleccionados no deben tener un tamaño superior a 64 TB.
    - Para el formato de disco VHD, sus volúmenes seleccionados no deben tener un tamaño superior a 2040 GB.
19. En la página **Volúmenes**, haga clic en **Finalizar** para completar el asistente y para iniciar la exportación.

    NOTE: Puede supervisar el estado y el progreso de la exportación visualizando las páginas **En espera virtual** o **Eventos**.

Configuración de la exportación continua a Hyper-V

Complete los pasos de este procedimiento para configurar la exportación continua a una máquina virtual Hyper-V (VM) mediante Rapid Recovery. Esto también se conoce como configuración de la espera virtual.

1. En la Rapid Recovery Core Console, realice una de las acciones siguientes:
   - En la Core Console, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, seleccione **Exportación de la MV**.
     1. En el Asistente de exportación de máquinas virtuales, seleccione **Continuo (servidor virtual en espera)**.
     2. Haga clic en **Siguiente.**
   - En la Core Console, en la barra de iconos, haga clic en (En espera virtual).
     - En la página **En espera virtual**, haga clic en **Agregar** para iniciar el Asistente de exportación de máquinas virtuales.
2. En la página **Equipos** del Asistente de exportación de máquinas virtuales, seleccione el equipo protegido que quiere exportar.
3. Haga clic en **Siguiente**.
4. En la página **Puntos de recuperación**, seleccione el punto de recuperación que quiere utilizar para la exportación.
5. Haga clic en **Siguiente**.
6. En la página **Destino**, en el menú desplegable Exportar a una máquina virtual, seleccione **Hyper-V** y después realice una de las siguientes opciones:
   - Para exportar a un equipo local con el rol Hyper-V asignado, haga clic en **Utilizar equipo local**.
   - Para indicar que el servidor Hyper-V se encuentra en un equipo remoto, haga clic en **Host remoto** y, a continuación, introduzca los parámetros del host remoto como se describe en la tabla siguiente.

Tabla 124. Información de host remoto

Cuadro de texto	Descripción
Nombre de host	Especifique la dirección IP o el nombre de host para el servidor Hyper-V. Representa la dirección IP o nombre de host del servidor Hyper-V remoto.
Puerto	Especifique un número de puerto para el equipo. Representa el puerto por el que el Core se comunica con este equipo.
Nombre de usuario	Especifique el nombre de usuario para el usuario con permisos administrativos para la estación de trabajo con el servidor Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.

Cuadro de texto	Descripción
Contraseña	Especifique la contraseña para la cuenta de usuario con permisos administrativos en la estación de trabajo con el servidor Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.

7. Haga clic en **Siguiente**.
8. En la página **Opciones de máquinas virtuales** del cuadro de texto **Ubicación de la máquina virtual**, introduzca la ruta de acceso de la máquina virtual; por ejemplo, `D:\export`. Esto se utiliza para identificar la ubicación de la máquina virtual.

   NOTE: Debe especificar la ubicación de la máquina virtual tanto para los servidores locales como remotos de Hyper-V. La ruta de acceso debe ser una ruta de acceso local válida para el servidor Hyper-V. Los directorios que no existan se crean automáticamente. No debería intentar crearlos manualmente. La exportación a carpetas compartidas (por ejemplo a `\\data\share`) no está permitida.
9. En el cuadro de texto **Nombre de la máquina virtual**, introduzca el nombre de la máquina virtual.

   El nombre que especifique aparecerá en la lista de máquinas virtuales en la consola Administrador de Hyper-V.
10. Para especificar el uso de la memoria, haga clic en una de las opciones siguientes:
    - **Utilizar la misma cantidad de RAM que el equipo de origen**. Seleccione esta opción para identificar que el uso de RAM es idéntico entre los equipos virtuales y de origen.
    - **Utilizar una cantidad específica de RAM.** Seleccione esta opción si desea especificar la cantidad de RAM en MB.

      La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.
11. Para especificar el formato de disco, junto a Formato de disco, haga clic en una de las siguientes opciones:
    - VHDX
    - VHD

    NOTE: La exportación de Hyper-V admite formatos de disco VHDX si el equipo de destino ejecuta Windows 8 (Windows Server 2012) o posterior. Si VHDX no se admite para su entorno, la opción está desactivada.

    NOTE: Si está exportando a Hyper-V de segunda generación, solo se admite la operación de formato de disco VHDX.
12. Para especificar la generación de Hyper-V que hay que emplear para la exportación, haga clic en uno de los siguientes elementos:
    - Generación 1
    - Generación 2

    NOTE: Solo la segunda generación admite la opción de inicio seguro.
13. Especifique el adaptador de red apropiado para la VM exportada.
14. En la página **Volúmenes**, seleccione los volúmenes que se van a exportar, por ejemplo, C:\.

NOTE: Si los volúmenes seleccionados tienen mayor capacidad que las asignaciones máximas apropiadas admitidas por la aplicación como se indica a continuación, o bien superan la cantidad de espacio disponible, aparecerá un error.

- Para el formato de disco VHDX, sus volúmenes seleccionados no deben tener un tamaño superior a 64 TB.
- Para el formato de disco VHD, sus volúmenes seleccionados no deben tener un tamaño superior a 2040 GB.

15. Seleccione **Realizar exportación única inicial** para realizar la exportación virtual inmediatamente en lugar de hacerlo después de la próxima instantánea programada.
16. En la página **Volúmenes**, haga clic en **Finalizar** para completar el asistente y para iniciar la exportación.

NOTE: Puede supervisar el estado y el progreso de la exportación visualizando las páginas **En espera virtual** o **Eventos**.

Exportación de datos a una máquina virtual VirtualBox

En Rapid Recovery, puede decidir exportar datos a VirtualBox realizando una exportación única o estableciendo una exportación continua (para el estado en espera virtual).

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

NOTE: Para realizar este tipo de exportación a una máquina virtual VirtualBox en un host de Windows, debería tener VirtualBox instalado en el equipo Core. Las máquinas virtuales alojadas en Linux no comparten este requisito.

Cómo realizar una exportación de VirtualBox puntual

Para exportar a una máquina virtual VirtualBox en un host de Windows remoto, debe tener VirtualBox instalado en el equipo del Core. Este requisito no se aplica a las máquinas virtuales alojadas en Linux.

Realice los pasos de este procedimiento para realizar una exportación puntual a VirtualBox.

1. En la Rapid Recovery Core Console, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, haga clic en **Exportación de la MV**.
2. En el Asistente de exportación de máquinas virtuales, seleccione **Exportación única**.
3. Haga clic en **Siguiente**.
4. En la página **Equipos**, seleccione el equipo protegido que quiere importar.
5. Haga clic en **Siguiente**.
6. En la página **Puntos de recuperación**, seleccione el punto de recuperación que quiere utilizar para la exportación.
7. Haga clic en **Siguiente**.
8. En la página **Destino** del asistente Exportación , en el menú desplegable Exportar a una máquina virtual, seleccione **VirtualBox** y, a continuación, haga clic en **Siguiente**.
9. En la página **Opciones de máquina virtual**, seleccione **Utilizar equipo con Windows**.
10. Especifique los parámetros para acceder a la máquina virtual, según se describe en la tabla siguiente.

Tabla 125. Parámetros de la máquina virtual

Opción	Descripción
Nombre de la máquina virtual	Introduzca un nombre para la máquina virtual que se está creando. **NOTE:** el nombre predeterminado es el nombre del equipo de origen.
Ruta de acceso al destino	Especifique una ruta de acceso de destino local o remota para crear la máquina virtual. **NOTE:** La ruta de acceso de destino no debería ser un directorio raíz. Si especifica una ruta de acceso compartida de red, tendrá que especificar credenciales de inicio de sesión válidas (nombre de usuario y contraseña) para una cuenta registrada en el equipo de destino. La cuenta debe tener permisos de lectura y escritura en el recurso compartido de red.
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: • Utilizar la misma cantidad de RAM que el equipo de origen • Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.

11. Para especificar una cuenta de usuario para la máquina virtual, seleccione **Especificar la cuenta de usuario para la máquina virtual exportada** y, a continuación, introduzca la información siguiente. Esto 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 esta cuenta de usuario esté registrada, solamente este usuario verá esta máquina virtual en el administrador de VirtualBox. Si no se especifica una cuenta, la máquina virtual se registrará para todos los usuarios existentes en el equipo con Windows con VirtualBox.
    - Nombre de usuario: Introduzca el nombre de usuario para el que está registrada la máquina virtual.
    - Contraseña: Introduzca la contraseña para esta cuenta de usuario.
12. Haga clic en **Siguiente**.
13. En la página **Volúmenes**, seleccione los volúmenes que desee exportar, por ejemplo, C:\ y D:\, y, a continuación, haga clic en **Siguiente**.
14. En la página **Resumen**, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

    NOTE: Puede supervisar el estado y el progreso de la exportación visualizando las páginas **En espera virtual** o **Eventos**.

Configuración de una exportación continua a VirtualBox

Para exportar a una máquina virtual VirtualBox en un host de Windows remoto, debe tener VirtualBox instalado en el equipo del Core. Este requisito no se aplica a las máquinas virtuales alojadas en Linux.

Complete los pasos de este procedimiento para realizar una exportación continua a una máquina virtual (VM) de VirtualBox mediante Rapid Recovery.

1. En la Rapid Recovery Core Console, realice una de las acciones siguientes:
   - En la Core Console, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, seleccione **Exportación de la MV**.
     1. En el Asistente de exportación de máquinas virtuales, seleccione **Continuo (servidor virtual en espera)**.
     2. Haga clic en **Siguiente.**
   - En la Core Console, en la barra de iconos, haga clic en (En espera virtual).
     - En la página **En espera virtual**, haga clic en **Agregar** para iniciar el Asistente de exportación de máquinas virtuales.
2. En la página **Equipos** del Asistente de exportación de máquinas virtuales, seleccione el equipo protegido que quiere exportar.
3. Haga clic en **Siguiente**.
4. En la página **Puntos de recuperación**, seleccione el punto de recuperación que quiere utilizar para la exportación.
5. Haga clic en **Siguiente**.
6. En la página **Destino** del Asistente de exportación, en el menú desplegable **Recuperar en una máquina virtual**, seleccione **VirtualBox**.
7. En la página **Opciones de máquina virtual**, seleccione **Equipo remoto Linux**.
8. Introduzca información sobre la máquina virtual según se describe en la tabla siguiente.

Tabla 126. Configuración del equipo Linux remoto

Opción	Descripción
Nombre de host de VirtualBox	Introduzca una dirección IP o un nombre de host para el servidor VirtualBox. Este campo representa la dirección IP o el nombre de host del servidor VirtualBox remoto.
Puerto	Especifique un número de puerto para el equipo. Este número representa el puerto por el que el Core se comunica con este equipo.
Nombre de la máquina virtual	Introduzca un nombre para la máquina virtual que se está creando. **NOTE:** el nombre predeterminado es el nombre del equipo de origen.
Ruta de acceso al destino	Especifique una ruta de acceso de destino para crear la máquina virtual. **NOTE:** Se recomienda que cree una carpeta raíz desde la raíz para que la máquina virtual se ejecute desde la raíz. Si no utiliza la raíz, deberá crear la carpeta de destino manualmente en el equipo de destino antes de configurar la exportación. También deberá vincular o cargar manualmente la máquina virtual después de la exportación.
Nombre de usuario	Nombre de usuario de la cuenta del equipo de destino, por ejemplo, raíz.
Contraseña	Contraseña de la cuenta de usuario del equipo de destino.

Opción	Descripción
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: • Utilizar la misma cantidad de RAM que el equipo de origen • Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.

9. Seleccione **Realizar exportación única inicial** para realizar la exportación virtual inmediatamente en lugar de hacerlo después de la próxima instantánea programada.
10. Haga clic en **Siguiente**.
11. En la página **Volúmenes**, seleccione los volúmenes de datos que desea exportar y, a continuación, haga clic en **Siguiente**.
12. En la página **Resumen**, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

NOTE: Puede supervisar el estado y el progreso de la exportación visualizando las páginas En espera virtual o Eventos.

Exportación de datos a una máquina virtual Azure

En Rapid Recovery, puede decidir exportar datos a Azure realizando una exportación única o estableciendo una exportación continua (para el estado en espera virtual). La exportación puntual a Azure incluye la implementación en el flujo de trabajo. Si se utiliza una exportación continua, más tarde también puede implementar los archivos exportados en una VM de inicio.

Para obtener más información acerca de cómo trabajar con Azure, consulte .

Para obtener los requisitos previos de la exportación virtual a Azure, consulte Antes de la exportación virtual a Azure.

Para obtener una descripción detallada de aspectos exclusivos de la exportación virtual para Azure, consulte Exportar e implementar VM de Azure.

Para obtener más información sobre precios y configuraciones, consulte la página de precios de las máquinas virtuales en el sitio web de Azure.

Para consultar vínculos a otras referencias útiles en páginas web de Microsoft, consulte .

Para conocer los procedimientos relacionados con la exportación o implementación de máquinas virtuales en Azure, consulte los vínculos relacionados siguientes.

Conceptos relacionados

See also: Exportación de datos a una máquina virtual VirtualBox

Tareas relacionadas

See also: Configuración de una exportación continua a Azure
See also: Implementación de una máquina virtual en Azure
See also: Realizar una exportación de Azure puntual

Trabajar con Microsoft Azure

Microsoft Azure es una plataforma de informática en la nube basada en suscripciones. La información siguiente se proporciona a los clientes de Rapid Recovery para facilitar el uso de Azure con nuestro producto.

- Declinación de responsabilidades de la interfaz de Azure
- Creación de un contenedor en una cuenta de almacenamiento de Azure
- Exportar e implementar VM de Azure
- Documentación de Microsoft Azure

Declinación de responsabilidades de la interfaz de Azure

La interfaz de Microsoft Azure está sujeta a cambios.

La información que se proporciona en este documento está relacionada con los pasos necesarios de Azure actualizados en la fecha de publicación. Esta información se proporciona como un servicio a nuestros clientes para ayudarles con los requisitos previos de Azure.

Sin embargo, al trabajar con Azure, tenga en cuenta esos pasos específicos, direcciones URL e, incluso, la interfaz de Azure puede cambiar en cualquier momento, lo cual no está bajo nuestro control.

Si tiene dificultades para realizar los pasos relacionados con su cuenta de Azure, busque el asesoramiento de un representante de Microsoft Azure.

Creación de un contenedor en una cuenta de almacenamiento de Azure

- Debe tener acceso administrativo a una cuenta en Azure.
- Debe tener una cuenta de almacenamiento definida en su cuenta de Azure.

Al realizar una exportación virtual, la información se almacena en un contenedor de una cuenta de almacenamiento de Azure. Puede definir el contenedor desde su cuenta de Azure antes de realizar la exportación virtual, mediante el procedimiento siguiente. O puede definir el contenedor como parte del proceso de exportación desde la página **Destino** del asistente.

Complete los pasos de este procedimiento para crear un contenedor en una cuenta de almacenamiento de Azure.

1. Abra el panel de Microsoft Azure.
2. En el área de navegación izquierda, haga clic en **Todos los recursos**.
3. En el panel **Todos los recursos**, haga clic en el nombre de la cuenta de almacenamiento en la que quiere almacenar datos de las exportaciones virtuales de Rapid Recovery.
4. En el panel **Configuración**, haga clic en **Blobs**.
5. En la parte superior del panel **Servicio BLOB**, en el encabezado, haga clic en **+ contenedor**.
6. En el panel **Nuevo contenedor**, en el campo **Nombre**, escriba el nombre del nuevo contenedor.

   NOTE: Escriba un nombre que contenga entre 3 y 63 caracteres, solo con letras minúsculas, números y guiones.
7. En el panel **Nuevo contenedor**, en el menú desplegable **Tipo de acceso**, seleccione el tipo de contenedor adecuado, que define si se puede acceder al contenedor de forma pública. Utilice los pasos siguientes como guía.

Opción	Descripción
Privado	Esta opción restringe el contenedor al propietario de la cuenta.
Blob	Esta opción permite el acceso de lectura público a los objetos binarios grandes (Blobs).
Contenedor	Esta opción permite el acceso de lista y lectura público a todo el contenedor.

Por ejemplo, seleccione **Contenedor**.

8. Haga clic en **Crear**.

   Si las alertas del sistema están activas, debería ver un mensaje que indique que el contenedor se creó correctamente.

   La página **Servicio BLOB** se actualiza, con el nuevo nombre del contenedor que se muestra en la lista.

Documentación de Microsoft Azure

Microsoft tiene bastante documentación sobre cómo usar Azure en su centro de documentación.

Para obtener información sobre cómo crear una cuenta de Azure o configurar una máquina virtual para su uso con un Rapid Recovery Core o AppAssure Core, agregar una cuenta de almacenamiento, etc., consulte la documentación de Microsoft en https://azure.microsoft.com/en-us/documentation.

Por ejemplo, para ver información sobre el aprovisionamiento o la administración de máquinas virtuales Windows, consulte https://azure.microsoft.com/en-us/documentation/services/virtual-machines/windows/.

Para ver vídeos en línea sobre cómo usar Azure, consulte http://azure.microsoft.com/en-us/get-started/.

NOTE: El sitio web de Azure usa códigos de idioma y país para sus direcciones web, lo que afecta a la visualización del contenido. Por ejemplo, `https://azure.microsoft.com/[country-code]/[destination]/`.

NOTE: Las URL para Azure usadas en este documento incluyen el código de país para inglés de los Estados Unidos. Para el resto de idiomas, en función de la configuración de su equipo y el contenido que Microsoft ofrezca, las URL pueden variar según estos códigos.

Vínculos de Microsoft relevantes

Estos son algunos artículos relevantes incluidos en los sitios web de Microsoft:

- Página de inicio de sesión de Azure (EE. UU.)
- Página de inicio de Microsoft Azure
- Centro de Documentación de Microsoft
- Documentación sobre máquinas virtuales de Windows
- Vídeos: Primeros pasos con Azure
- Precios de máquinas virtuales Azure
- Servicios de Azure por región
- Acerca de las cuentas de almacenamiento de Azure
- Creación de una cuenta de almacenamiento en Azure
- Cómo añadir un disco de datos a una máquina virtual Windows en el portal Azure
- Uso del servicio de importación/exportación de Microsoft Azure para transferir datos al almacenamiento Blob
- Precios del servicio de importación/exportación
- Almacenamiento: Importación/exportación de unidades de disco duro a Windows Azure (blog)

Antes de la exportación virtual a Azure

Rapid Recovery permite realizar una exportación virtual (puntual o espera virtual) a Microsoft Azure.

Antes de realizar una exportación virtual de cualquier equipo protegido en Rapid Recovery, primero debe asociar su cuenta en la nube de Azure con su Core, como se describe en el tema Incorporación de una cuenta de nube.

Debe tener una cuenta de almacenamiento adecuada en Azure. Para obtener más información sobre cómo crear una cuenta de almacenamiento en Azure, consulte la información de soporte de Azure, a la cual se hace referencia en el tema .

En su cuenta de almacenamiento, puede crear de forma dinámica un contenedor para almacenar exportaciones o puede utilizar un contenedor existente. Para obtener más información sobre cómo crear un contenedor de almacenamiento, consulte Creación de un contenedor en una cuenta de almacenamiento de Azure.

A diferencia de otras formas de exportación virtual mediante Rapid Recovery, la exportación de máquinas virtuales de Azure incluye dos procesos, que se describen en detalle en el tema Exportar e implementar VM de Azure.

Exportar e implementar VM de Azure

A diferencia de la exportación virtual de otras plataformas, la exportación virtual de Azure consta de dos procesos: exportación e implementación.

Tenga en cuenta que los clientes de Microsoft Azure se harán responsables de las tarifas. Algunos aspectos de nuestra integración con Azure están diseñados con este sistema de tarifas en mente. Por ejemplo, Microsoft cobra una tarifa cuando implementa una VM en Azure y cuando se transmiten datos de Azure a otra fuente.

NOTE: Ya que Microsoft puede cambiar los requisitos previos, costes, etc., es aconsejable confirmar siempre por adelantado esta información con Azure. Para obtener más información, consulte el sitio web de Azure o a un representante de Azure.

Para evitar incurrir en gastos innecesarios, la exportación virtual a Azure consta de dos procesos independientes, para sufragar los costes que nos sean necesarios.

El proceso de **exportación** extrae el conjunto de archivos necesarios de Rapid Recovery, los valida y los carga un contenedor especificado en Azure. Estos archivos incluyen:

- Un archivo de disco duro virtual (VHD) para cada volumen del punto de recuperación.
- Un archivo XML, que contiene información de metadatos acerca de cada disco (una lista de archivos presentes en cada disco y una marca que indica si un volumen es un disco de sistema).
- Un archivo VHD que contiene la instantánea de copia de seguridad.

Los costes que no sean del almacenamiento necesario, por ejemplo, la exportación por sí misma no genera costes de Azure.

El proceso de **implementación** combina estos archivos en una máquina virtual de inicio. La implementación utiliza directamente las API de REST en la nube de Azure. El conjunto original de ficheros ubicados en Azure durante el proceso de exportación es de solo lectura en Azure y consume espacio, pero, de lo contrario, no genera gastos. Cuando implementa estos archivos, se crea una copia duplicada de ellos, se almacena en un contenedor independiente que especifique y se combinan en una máquina virtual de trabajo. Desde una perspectiva de una cuenta de Azure, después de implementarlos, se le cargarán gastos por la VM en sus servidores. Como la VM implementada es una copia de los archivos exportados, el proceso de implementación también dobla la cantidad de espacio de almacenamiento que se utiliza en Azure para esa exportación virtual.

Para una exportación virtual puntual, no existe ningún mecanismo para implementar VM como un proceso independiente. Por lo tanto, para que la exportación sea útil, debe implementar a Azure cuando cree la máquina virtual bajo petición. Como resultado, las exportaciones virtuales a Azure tienen un coste inmediato asociado con la VM que implemente.

Al establecer la espera virtual para un equipo protegido en Azure, para evitar el uso de espacio de almacenamiento adicional y cargos de VM, simplemente puede definir el proceso de exportación. El resultado es una exportación virtual inicial a Azure que se actualiza continuamente. Cada vez que se captura una instantánea en el Core, los archivos exportados se actualizan en su cuenta de Azure con información actualizada. Antes de la exportación virtual se pueda utilizar como una VM de inicio, debe implementarla, lo que genera costes de VM en Azure. Si no necesita convertir los archivos exportados de un equipo protegido a una VM de inicio, no se cargarán gastos en su cuenta de Azure.

Para obtener información sobre cómo realizar una exportación puntual a Azure, incluida la implementación, consulte el tema Realizar una exportación de Azure puntual.

Para obtener más información sobre cómo configurar la exportación continua en Azure, sin incluir la implementación, consulte el tema Configuración de una exportación continua a Azure.

Para obtener información acerca de implementar los archivos exportados más recientes para crear una VM en espera virtual de inicio en Azure, consulte el tema Implementación de una máquina virtual en Azure.

Realizar una exportación de Azure puntual

Antes de realizar una exportación puntual de Azure, necesita lo siguiente:

- Debe tener un equipo protegido con al menos un punto de recuperación en un Rapid Recovery Core que quiera exportar a Azure.
- Se debe activar el acceso remoto en el equipo protegido para que la VM implementada se inicie correctamente.
- Debe tener acceso administrativo a una cuenta en Azure.
- De manera opcional, antes de la exportación, puede crear un contenedor adecuado en su cuenta de almacenamiento de Azure en la que quiere que se almacenen los datos exportados. Para obtener más información, consulte el tema Creación de un contenedor en una cuenta de almacenamiento de Azure.

Tal como se describe en el tema Exportar e implementar VM de Azure, la exportación virtual a Azure consta de dos procesos: exportación e implementación.

El proceso de **exportación** extrae el conjunto de archivos necesarios de Rapid Recovery, los valida y los carga un contenedor especificado en Azure. Estos archivos incluyen:

- Un archivo de disco duro virtual (VHD) para cada volumen del punto de recuperación
- Un archivo XML, que contiene información de metadatos acerca de cada disco (una lista de archivos presentes en cada disco y una marca que indica si un volumen es un disco de sistema)
- Un archivo VHD que contiene la instantánea de copia de seguridad

El proceso de **implementación** combina estos archivos en una máquina virtual de inicio. La implementación utiliza directamente las API de REST en la nube de Azure. El conjunto original de ficheros ubicados en Azure durante el proceso de exportación es de solo lectura en Azure y consume espacio, pero, de lo contrario, no genera gastos adicionales de Azure. Cuando implementa estos archivos, se crea una copia duplicada de ellos, se almacena en un contenedor independiente que especifique y se combinan en una máquina virtual de trabajo. Desde una perspectiva de una cuenta de Azure, después de implementarlos, se le cargarán gastos por la VM en sus servidores. El proceso de implementación también dobla la cantidad de espacio de almacenamiento que se utiliza en Azure para esa exportación virtual.

Para una exportación virtual puntual, no existe ningún mecanismo para implementar como un proceso independiente; por lo tanto, para que la exportación sea útil, debe implementarlo al crear la máquina virtual a petición.

Al establecer la espera virtual en un equipo protegido en Azure, para evitar utilizar espacio de almacenamiento adicional y cargos de VM, puede exportar y actualizar continuamente el punto de recuperación automáticamente, sin la necesidad de implementarlo. A continuación, puede implementar en Azure solo si necesita utilizar la máquina virtual. Para obtener información acerca de implementar una espera virtual en Azure en una VM en funcionamiento, consulte el tema Implementar datos de la espera virtual en una VM en Azure.

Realice los pasos de este procedimiento para realizar una exportación puntual a Azure a petición, incluida la implementación en una VM.

1. En la Rapid Recovery Core Console, haga clic en el menú desplegable **Restaurar** y, a continuación, seleccione **Exportación VM**.

   Aparece el asistente Exportación de una máquina virtual.
2. En el asistente, en la página **Seleccionar tipo de exportación de VM**, seleccione **Exportación puntual** y, a continuación, haga clic en **Siguiente**.

   Aparece la página **Equipos** del asistente.
3. En la página **Equipos**, seleccione el equipo protegido que desea exportar y, a continuación, haga clic en **Siguiente**.
4. En la página **Puntos de recuperación**, desplácese por la lista de puntos de recuperación si es necesario y seleccione el punto de recuperación que quiere utilizar para la exportación. A continuación, haga clic en **Siguiente**.
5. En la página **Destino**, en el menú desplegable Exportar a máquina virtual, seleccione **Azure**.
6. Introduzca los parámetros para acceder a la máquina virtual según se describen en la tabla siguiente y, a continuación, haga clic en **Siguiente**.

Tabla 127. Credenciales de Azure

Opciones	Descripción
Archivo de configuración de publicación	El archivo de configuración de publicación es un documento XML generado en Azure que contiene certificados de administración para la información de suscripción de Azure. **NOTE:** La configuración de publicación solo se debe definir una vez por cuenta de Azure desde la UI del Core. Después, se almacena en la caché. Cuando se le solicite para este archivo, inicie sesión en su cuenta de Azure y descárguelo desde su VM en https://manage.windowsazure.com/publishsettings/index?client=powershell.

Opciones	Descripción
	El archivo define la API AzureServiceManagement e información sobre su suscripción de Azure, incluidas las credenciales seguras. Este archivo se debe definir en el Rapid Recovery Core antes de conectarse a su cuenta y realizar una exportación virtual. Por motivos de seguridad, guarde el archivo en una ubicación segura o elimínelo después de utilizarlo en este procedimiento.
Suscripción	Si acaba de agregar archivos de configuración de publicación, esta información se introduce automáticamente con información del archivo de configuración de publicación. **NOTE:** La configuración de publicación solo se debe definir una vez por cuenta de Azure desde la UI del Core. Después, se almacena en la caché. Si quiere utilizar un archivo de configuración de publicación previamente agregado, utilice esta lista desplegable para seleccionar un archivo. Si quiere agregar un archivo de configuración de publicación, utilice el botón + para abrir la ventana **Cargar certificado** y examinar el archivo. Cuando se le solicite para este archivo, inicie sesión en su cuenta de Azure y descárguelo desde su VM en https://manage.windowsazure.com/publishsettings/index?client=powershell. Por motivos de seguridad, guarde el archivo en una ubicación segura o elimínelo después de utilizarlo en este procedimiento.
Cuenta	Introducida automáticamente desde el archivo de suscripción, es la cuenta en la nube de Azure que se ha asociado con su Core. **NOTE:** Primero debe asociar la cuenta en la nube de Azure con su Core, como se describe en el tema Incorporación de una cuenta de nube.
Nombre de contenedor	En el menú desplegable, seleccione el nombre de un contenedor adecuado con su cuenta en la nube de Azure si ya existe uno. O introduzca un nombre para el nuevo contenedor. **NOTE:** Escriba un nombre que contenga entre 3 y 63 caracteres, solo con letras minúsculas, números y guiones.
Nombre de la carpeta	Especifique un nombre para la carpeta del contenedor para almacenar la máquina virtual exportada. **NOTE:** Una carpeta de Azure no puede contener ninguno de los caracteres siguientes: / \ : * ? " < > |

7. En la página **Implementar**, introduzca una descripción de la VM implementada, como se describe en la tabla siguiente y, a continuación, haga clic en **Siguiente**.

Tabla 128. Implementación en las opciones de Azure

Opción	Descripción
Nombre del servicio en la nube	El servicio en la nube de Azure es un contenedor de máquinas virtuales que utiliza el modelo de administración clásico. Si ya tiene un servicio en la nube existente, en el menú desplegable **Nombre del servicio en la nube**, seleccione el nombre del servicio en la nube adecuado. O, en el campo **Nombre del servicio en la nube**, escriba un nombre exclusivo y significativo para el servicio en la nube.

Opción	Descripción
	NOTE: Las suscripciones de Microsoft Azure tienen límites predeterminados sobre el número de servicio en la nube (normalmente 25). Asegúrese de no superar los límites de suscripción.
Nombre de la implementación	Si ha seleccionado un servicio en la nube con máquinas virtuales existentes, este campo se rellena automáticamente. Si ha seleccionado un servicio en la nube que no incluye máquinas virtuales, a continuación, introduzca un nombre para esta nueva implementación. **NOTE:** Escriba un nombre que contenga entre 3 y 63 caracteres, solo con letras minúsculas, números y guiones.
Contenedor de destino	Introduzca un nombre para el contenedor para almacenar las máquinas virtuales. **NOTE:** Escriba un nombre que contenga entre 3 y 63 caracteres, solo con letras minúsculas, números y guiones.

8. En la página **Opciones de máquina virtual**, introduzca la información como se describe en la tabla siguiente.

Tabla 129. Opciones de máquina virtual

Opción	Descripción
Nombre de la máquina virtual	Introduzca un nombre para la máquina virtual. **NOTE:** Escriba un nombre que contenga entre 3 y 15 caracteres, solo con letras minúsculas, números y guiones.
Tamaño de la máquina virtual	En el menú desplegable, seleccione un tamaño de VM adecuado. **NOTE:** Para obtener más información sobre precios y configuraciones, consulte la página de precios de las máquinas virtuales en el sitio web de Azure. Para consultar vínculos a otras referencias útiles en páginas web de Microsoft, consulte .
Extremo (configuración del acceso remoto)	Las opciones que aparecen a continuación son opciones de VM para la configuración del acceso remoto.
Nombre	Seleccione entre **RemoteDesktop** o **SSH**.
Protocolo	Seleccione entre **TCP** o **UDP**
Puertos	Los puertos públicos y privados utilizan 3389 de manera predeterminada. Cámbielo si es necesario.
Puertos del servidor de transferencia de datos	Los puertos públicos y privados utilizan 8009 de manera predeterminada. Cámbielo si es necesario.

Opción	Descripción
Puertos de Agent	Los puertos públicos y privados utilizan 8006 de manera predeterminada. Cámbielo si es necesario.

9. Haga clic en **Siguiente**.
10. En la página **Volúmenes**, seleccione los volúmenes que quiere exportar y, a continuación, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

> **NOTE:** Puede supervisar el estado y el progreso de la exportación visualizando la cola de exportaciones en la página **En espera virtual** o **Eventos**.

Configuración de una exportación continua a Azure

Antes de realizar una exportación virtual continua a Azure, necesita lo siguiente:

- Debe tener un equipo protegido con al menos un punto de recuperación en un Rapid Recovery Core que quiera exportar a Azure.
- Se debe activar el acceso remoto en el equipo protegido para que la VM implementada se inicie correctamente.
- Debe tener acceso administrativo a una cuenta en Azure.
- Para asociar su cuenta Azure con el Core, primero debe descargar un archivo de configuración de publicación desde Azure. Para obtener más información, consulte Obtención del archivo de configuración de publicación de su cuenta de Azure.
- De manera opcional, antes de la exportación, puede crear un contenedor adecuado en su cuenta de almacenamiento de Azure en la que quiere que se almacenen los datos exportados. Tenga en cuenta que los requisitos de almacenamiento incrementan a medida que el equipo protegido protege más datos. En su cuenta Azure, el contenedor que especifique debe estar asociado con una ubicación de almacenamiento con espacio suficiente para la máquina virtual. Para obtener más información, consulte el tema Creación de un contenedor en una cuenta de almacenamiento de Azure.

Complete los pasos de este procedimiento para realizar una exportación virtual continua de la máquina seleccionada a un contenedor especificado en una cuenta en la nube de Azure con Rapid Recovery.

> **NOTE:** Este proceso no incluye la implementación de los archivos exportados para crear una VM de inicio. Para ver los pasos sobre la implementación, consulte Implementación de una máquina virtual en Azure.

1. En la Core Console de Rapid Recovery, realice una de las acciones siguientes:
   - En la Core Console, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, seleccione **Exportación de la MV**.
     1. En el Asistente de exportación de máquinas virtuales, seleccione **Continuo (servidor virtual en espera)**.

2. Haga clic en **Siguiente.**

- En la Core Console, en la barra de iconos, haga clic en (Espera virtual).
  - En la página **En espera virtual**, haga clic en **+Agregar** para iniciar el asistente Exportación de máquinas virtuales.

2. En la página **Equipos** del Asistente de exportación de máquinas virtuales, seleccione el equipo protegido que quiere exportar.
3. Haga clic en **Siguiente**.
4. En la página **Puntos de recuperación**, seleccione el punto de recuperación que quiere utilizar para la exportación.
5. Haga clic en **Siguiente**.
6. En la página **Destino**, en el menú desplegable Exportar a máquina virtual, seleccione **Azure**. .
7. Introduzca los parámetros para acceder a la máquina virtual según se describen en la tabla siguiente y, a continuación, haga clic en **Siguiente**.

Tabla 130. Credenciales de Azure

Opciones	Descripción
Archivo de configuración de publicación	Esta opción solo aparece si aún no ha asociado la suscripción de Azure con el Core. Si visualiza esta opción, descargue el archivo tal y como se describe en el tema Obtención del archivo de configuración de publicación de su cuenta de Azure y asocie la suscripción con el Core. Esta asociación debe completarse antes de poder conectarse a la cuenta de Azure desde el Core y realizar una exportación virtual. **NOTE:** La configuración de publicación solo se debe definir una vez por cuenta de Azure desde la UI del Core. Después, se almacena en la caché. Por motivos de seguridad, guarde el archivo en una ubicación segura o elimínelo después de utilizarlo en este procedimiento.
Suscripción	Si acaba de agregar archivos de configuración de publicación, esta información se introduce automáticamente con información del archivo de configuración de publicación. **NOTE:** La configuración de publicación solo se debe definir una vez por cuenta de Azure desde la UI del Core. Después, se almacena en la caché. Si quiere utilizar un archivo de configuración de publicación previamente agregado, utilice esta lista desplegable para seleccionar un archivo. Si quiere agregar un archivo de configuración de publicación, utilice el botón + para abrir la ventana **Cargar certificado** y examinar el archivo.
Cuenta	Introducida automáticamente desde el archivo de suscripción, es la cuenta en la nube de Azure que se ha asociado con su Core. **NOTE:** Primero debe asociar la cuenta en la nube de Azure con el Core, como se describe en el tema. Incorporación de una cuenta de nube
Nombre de contenedor	En el menú desplegable, seleccione el nombre de un contenedor adecuado con su cuenta en la nube de Azure si ya existe uno. O introduzca un nombre para el nuevo contenedor. **NOTE:** Escriba un nombre que contenga entre 3 y 63 caracteres, solo con letras minúsculas, números y guiones.
Nombre de carpeta	Especifique un nombre para la carpeta del contenedor para almacenar la máquina virtual exportada.

Opciones	Descripción
	NOTE: Una carpeta de Azure no puede contener ninguno de los caracteres siguientes: / \ : * ? " < > |
Realizar exportación única inicial	Al definir la espera virtual, seleccione esta opción para poner en la cola el trabajo de exportación inmediatamente. Desactive esta opción si quiere que el Core espere hasta la próxima instantánea de copia de seguridad programada o forzada.

8. Haga clic en **Siguiente**.
9. En la página **Volúmenes**, seleccione los volúmenes que desee exportar y, a continuación, haga clic en **Siguiente**.
10. En la página **Resumen**, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

NOTE: Puede supervisar el estado y el progreso de la exportación visualizando las páginas En espera virtual o Eventos.

Los parámetros de espera virtual que defina en este procedimiento causan la exportación de los archivos necesarios para crear una VM en su cuenta de Azure. Después de cada instantánea (forzada o programada), estos archivos se actualizan en Azure con la nueva información de copia de seguridad. Antes de que inicie estos archivos como una VM, debe implementar la VM en Azure. Para ver los pasos sobre la implementación, consulte Implementación de una máquina virtual en Azure.

Implementación de una máquina virtual en Azure

Antes de implementar una máquina virtual en Azure, debe tener un equipo protegido en el Rapid Recovery Core con al menos un punto de recuperación y debe configurar la exportación continua (espera virtual) en la Core Console. Para obtener más información sobre la configuración de la exportación virtual, consulte Configuración de una exportación continua a Azure. Este proceso también requiere que tenga una cuenta de Azure con almacenamiento suficiente asociada con su Core.

Al configurar la espera virtual para un equipo protegido en Azure, la información de la copia de seguridad más reciente se exporta de forma continua desde el Core a su cuenta de Azure después de cada instantánea de copia de seguridad. Este proceso sobrescribe el conjunto anterior de archivos de exportación con la información de copia de seguridad actualizada. Antes de poder iniciar la exportación virtual como una VM (por ejemplo, si su equipo protegido original ha fallado), primero debe implementarla desde la Core Console. Este proceso genera una VM de inicio en un nuevo contenedor

Complete los pasos de este procedimiento para implementar sus archivos de exportación en espera virtual más recientes en una VM de inicio en Azure.

1. En la Rapid Recovery Core Console, en la barra de iconos, haga clic en (Espera virtual).
2. En el panel **Espera virtual**, identifique el equipo en el Rapid Recovery Core configurado para la exportación continua a Azure.
3. En la fila que representa el equipo en espera virtual que quiere implementar, haga clic en (Más opciones) y, a continuación, seleccione **Implementar una máquina virtual**.

Aparece el asistente **Implementar en Azure**.

4. En la página **Destino**, en el menú desplegable **Nombre del servicio en la nube**, seleccione el nombre del servicio en la nube adecuado de las opciones disponibles en su cuenta de Azure.
5. Haga clic en **Siguiente**.
6. En la página Puntos de recuperación, seleccione el punto de recuperación que desea utilizar para la exportación.
7. Haga clic en **Siguiente**.
8. En la página **Destino** del asistente Exportación, en el menú desplegable Exportar a una máquina virtual, seleccione **ESX(i)**.
9. Introduzca los parámetros para acceder a la máquina virtual según se describen en la tabla siguiente y, a continuación, haga clic en **Siguiente**.

Tabla 131. Parámetros de la máquina virtual

Opciones	Descripción
Nombre del servicio en la nube	Si ya tiene un servicio en la nube existente, en el menú desplegable **Nombre del servicio en la nube**, seleccione el nombre del servicio en la nube adecuado. O, en el campo **Nombre del servicio en la nube**, escriba un nombre exclusivo y significativo para el servicio en la nube. El nombre del servicio en la nube está asociado con su grupo de recursos en su cuenta de Azure. Si tiene privilegios administrativos de Azure, consulte la documentación de Azure para crear la cuenta adecuada. Si no ve una cuenta de servicio en la nube adecuada, solicite ayuda a su administrador de Azure. **NOTE:** Las suscripciones de Microsoft Azure tienen límites predeterminados sobre el número de servicio en la nube (normalmente 25). Asegúrese de no superar los límites de suscripción.
Nombre de la implementación	Si ha seleccionado un servicio en la nube con máquinas virtuales existentes, este campo se rellena automáticamente. Si ha seleccionado un servicio en la nube que no incluye máquinas virtuales, a continuación, introduzca un nombre para esta nueva implementación. **NOTE:** Escriba un nombre que contenga entre 3 y 63 caracteres, solo con letras minúsculas, números y guiones.
Contenedor de destino	Introduzca un nombre para el contenedor para almacenar las máquinas virtuales. **NOTE:** Escriba un nombre que contenga entre 3 y 63 caracteres, solo con letras minúsculas, números y guiones.

10. En la página Opciones de máquina virtual, introduzca la información como se describe en la tabla siguiente y, a continuación, haga clic en **Siguiente**.

Tabla 132. Opciones de máquina virtual

Opción	Descripción
Nombre de la máquina virtual	Introduzca un nombre para la máquina virtual. **NOTE:** Escriba un nombre que contenga entre 3 y 15 caracteres, solo con letras minúsculas, números y guiones.
Tamaño de la máquina virtual	En el menú desplegable, seleccione un tamaño de VM adecuado.

Opción	Descripción
	NOTE: Para obtener más información sobre precios y configuraciones, consulte la página de precios de las máquinas virtuales en el sitio web de Azure. Para consultar vínculos a otras referencias útiles en páginas web de Microsoft, consulte .
Extremo (configuración del acceso remoto)	
Nombre	Seleccione entre **RemoteDesktop** o **SSH**.
Protocolo	Seleccione entre **TCP** o **UDP**
Puertos	Los puertos públicos y privados utilizan 3389 de manera predeterminada. Cámbielo si es necesario.
Puertos del servidor de transferencia de datos	Los puertos públicos y privados utilizan 8009 de manera predeterminada. Cámbielo si es necesario.
Puertos de Agent	Los puertos públicos y privados utilizan 8006 de manera predeterminada. Cámbielo si es necesario.

11. En la página **Discos**, seleccione los volúmenes que quiere exportar y, a continuación, haga clic en **Finalizar** para cerrar el asistente e iniciar la implementación.

NOTE: Puede supervisar el progreso de la implementación visualizando tareas en la página **Eventos**.

Una vez haya finalizado la implementación, en su cuenta de Azure, puede ver la nueva VM en la vista **Ver equipos (clásica)** de Azure. Una vez que la VM esté disponible, también pagará tarifas. Para evitar los cargos continuos, elimine la VM implementada cuando no sea necesaria. Siempre puede implementar una VM desde el último conjunto de archivos de exportación virtual repitiendo este procedimiento.

Administración de exportaciones

Si el Core tiene la exportación continua configurada, los parámetros de configuración de cada exportación virtual aparecen como una fila en la página **En espera virtual**. Desde aquí puede ver el estado de las exportaciones continuas establecidas y administrar sus equipos en espera virtual. Puede agregar una espera virtual, forzar la exportación, pausar o reanudar la espera virtual o eliminar los requisitos de la exportación continua desde la Core Console.

Cuando se lleva a cabo una exportación única, el trabajo se incluye en la cola de exportación en la página **En espera virtual**. Durante este tiempo, puede pausar, reanudar o cancelar la operación de exportación puntual.

NOTE: Rapid Recovery admite exportación de Hyper-V a Windows 8, Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016.

La exportación virtual a una VM en espera virtual no se produce si la VM está encendida.

Complete los pasos de este procedimiento para gestionar las exportaciones virtuales.

1. En la Core Console, en la barra de iconos, haga clic en (En espera virtual).

Aparece la página **En espera virtual**. Aquí puede ver dos tablas de la configuración guardada de la exportación. Incluyen la información que se describe en la tabla siguiente.

Tabla 133. Información de espera virtual

Columna	Descripción
Seleccionar elemento	En cada fila de la tabla de resumen, puede seleccionar la casilla de verificación para llevar a cabo acciones de la lista de opciones de menú anterior a la tabla.
Indicador de estado	Las esferas de colores de la columna Estado muestran el estado de la espera virtual. Si pasa el cursor sobre el círculo coloreado, se muestra la condición de estado. • **Verde.** La espera virtual se ha configurado correctamente, está activa y no está en pausa. La exportación siguiente se lleva a cabo inmediatamente después de que se haya completado la instantánea siguiente. • **Amarillo.** Se pausa la espera virtual, pero los parámetros aún están definidos y guardados en el Core. Sin embargo, tras una nueva transferencia, el trabajo de exportación no se iniciará automáticamente y no habrá nuevas exportaciones para este equipo protegido hasta que cambie el estado.
Nombre del equipo	Nombre del equipo de origen.
Tipo de exportación	Haga clic en para ver el tipo de exportación. Muestra el tipo de plataforma de máquina virtual para la exportación, como ESXi, VMware Workstation, Hyper-V, VirtualBox o Azure.
Última exportación	Haga clic en para ver el tipo de exportación. Muestra la fecha y la hora de la última exportación. Si se acaba de agregar una exportación, pero no se ha completado, se muestra un mensaje que indica que la exportación todavía no se ha realizado. Si una exportación ha fallado o se canceló, también se muestra el mensaje correspondiente.
Destino	Máquina virtual y ruta de acceso a la que los datos se están exportando.
Configuración	El menú desplegable (Más opciones) permite realizar las siguientes funciones: • **Editar**. Permite editar la configuración de la espera virtual. • **Forzar**. Fuerza una exportación virtual. • **Pausar**. Pausa la exportación virtual. Solo está disponible cuando el estado está activo. • **Reanudar**. Reanuda la exportación virtual. Sólo está disponible cuando el estado está en pausa. • **Quitar**. Elimina el requisito de una exportación continua. No elimina la VM exportada actualizada más recientemente. • **Implementar una máquina virtual**. Solo para la exportación continua de Azure, convierte los archivos exportados de su cuenta de Azure en una máquina virtual de inicio.

Tabla 134. Información de la cola de exportación

Columna	Descripción
Seleccionar elemento	En cada fila de la tabla de resumen, puede seleccionar la casilla de verificación para llevar a cabo acciones de la lista de opciones de menú anterior a la tabla. Estas son algunas de las opciones: • **Cancelar**. Cancele la exportación virtual puntual actual. • **Configuración**. Permite actualizar el valor máximo de exportaciones simultáneas.
Indicador de estado	Muestra el estado de la exportación actual como un porcentaje. Cuando no hay ninguna exportación puntual en la cola, esta columna no tiene ningún valor.
Nombre del equipo	Nombre del equipo de origen.
Tipo de exportación	Haga clic en para ver el tipo de exportación. Muestra el tipo de plataforma de máquina virtual para la exportación, como ESXi, VMware, Hyper-V, VirtualBox o Azure.
Tipo de programa	Haga clic en para ver el tipo de programa. Muestra el tipo de exportación, ya sea Puntual o Continua.
Destino	Máquina virtual y ruta de acceso a la que los datos se están exportando.

2. Para gestionar los ajustes de exportación guardados, seleccione una exportación y, a continuación, haga clic en una de las siguientes opciones:
   - **Editar**. Se abre el **Asistente de exportación de máquinas virtuales** en la página **Opciones de VM**. Desde aquí puede cambiar la ubicación de la VM exportada, cambiar la versión del tipo de VM o especificar la RAM o los procesadores para la exportación. Para iniciar inmediatamente la exportación de VM, seleccione **Realizar exportación única inicial**.
   - **Forzar**. Fuerza una nueva exportación. Esta opción podría ser de utilidad cuando el estado en espera virtual esté pausado y luego se reanude, lo que significa que el trabajo de exportación se reiniciará solamente después de una nueva transferencia. Si no desea esperar a la nueva transferencia, puede forzar una exportación.
   - **Pausar**. Pausa una exportación activa.
   - **Reanudar**. Se reanuda el requisito de la exportación continua en la próxima instantánea forzada o programada.
3. Para eliminar una exportación del sistema, seleccione el exportar y, a continuación, haga clic en **Quitar**.

   La configuración de exportación se elimina de manera permanente del sistema. Al eliminar la configuración de espera virtual no se eliminan las máquinas virtuales exportadas como resultado de la configuración.
4. Para implementar una máquina virtual en Azure, seleccione **Implementar máquina virtual** y complete los detalles en el asistente Implementar en Azure.

Los datos de la exportación virtual más reciente guardados en su cuenta de Azure se implementan en su cuenta de Azure asociada como una VM de inicio.

5. Para gestionar el número de exportaciones que se ejecutan al mismo tiempo, haga lo siguiente:
   - Debajo de Cola de exportación, haga clic en **Configuración**.
   - En el cuadro de diálogo **N.º máximo de exportaciones simultáneas**, introduzca el número de exportaciones que quiere ejecutar de forma simultánea. El número predeterminado es 5.
   - Haga clic en **Guardar**.
6. Para cancelar una exportación única o continua que se incluye actualmente en la cola de exportación, seleccione la exportación y, a continuación, haga clic en **Cancelar**.
7. Para agregar una nueva exportación en espera virtual, puede hacer clic en **Agregar** para iniciar el Asistente de exportación. Completar el asistente resultante inicia una exportación continua del equipo protegido seleccionado. Para obtener más información sobre cómo configurar el estado en espera virtual para una máquina virtual específica, consulte uno de los temas siguientes:
   - Configuración de la exportación continua a ESXi
   - Configuración de una exportación continua a VMware Workstation
   - Configuración de la exportación continua a Hyper-V
   - Configuración de una exportación continua a VirtualBox
   - Configuración de una exportación continua a Azure

Restauración de datos

En esta sección se describe cómo restaurar datos de las copias de seguridad.

Acerca de la restauración de datos con Rapid Recovery

El Rapid Recovery Core puede restaurar datos al instante o realizar la recuperación de equipos en máquinas físicas o virtuales desde puntos de recuperación. Los puntos de recuperación contienen instantáneas del volumen del Agent capturadas en el nivel del bloque. Esas instantáneas ofrecen reconocimiento por parte de la aplicación, lo cual significa que todos los registros de transacciones abiertas y transacciones en marcha se completan y que las memorias caché se vacían antes de crear la instantánea. Mediante instantáneas con reconocimiento por parte de la aplicación, y junto con Verified Recovery, el Core puede 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 bare-metal, mediante Universal Recovery
- Recuperación bare-metal de hardware diferente, mediante Universal Recovery
- Exportación exclusiva a petición y continua a las máquinas virtuales

NOTE: Al restaurar datos o realizar una exportación virtual, el punto de recuperación utilizado debe formar parte de una cadena de puntos de recuperación completa. Para obtener más información sobre las cadenas de puntos de recuperación, consulte el tema Cadenas del punto de recuperación y huérfanos.

Descripción de Live Recovery

Live Recovery es una función de restauración de datos del Rapid Recovery Core. Si la máquina protegida experimenta fallos de datos de un volumen de Windows que no sea del sistema, puede restaurar datos a partir de un punto de recuperación del Rapid Recovery Core. Al seleccionar Live Recovery en Restore Wizard, permite a los usuarios continuar de inmediato las operaciones empresariales casi sin tiempo de inactividad. Live Recovery durante la restauración proporciona acceso inmediato a los datos, incluso aunque Rapid Recovery continúe restaurando datos en segundo plano. Esta función le permite un tiempo de recuperación prácticamente inexistente, incluso si la restauración implica terabytes de datos.

El Rapid Recovery Core utiliza la exclusiva tecnología de recuperación y copias de seguridad basada en bloques que le permite acceso completo de usuario a los servidores de destino durante el proceso de recuperación. Los bloques solicitados se restauran a petición para una recuperación sencilla.

Live Recovery se aplica a las máquinas físicas y virtuales protegidas por el Rapid Recovery Core, con las siguientes exclusiones:

- Live Recovery está accesible para volúmenes de Windows que no son del sistema. La unidad C:\ y la partición reservada al sistema no se pueden restaurar con Live Recovery.
- Live Recovery es accesible para volúmenes basados en Windows que utilizan Rapid Recovery Agent. Los volúmenes sin agentes o los volúmenes de Linux no pueden aprovecharse de Live Recovery.

Live Recovery le permite restaurar inmediatamente los servidores físicos o virtuales directamente desde el archivo de copia de seguridad. Cuando un volumen sin sistema está siendo restaurado, Rapid Recovery presenta los metadatos de volumen para el sistema operativo al instante, lo que hace que que los datos estén disponibles a petición. Por ejemplo, si el volumen de la base de datos de Microsoft Exchange está dañado, Live Recovery puede restaurar el volumen, la base de datos y los servicios de Exchange en minutos.

Esta función proporciona el método más rápido para recuperar grandes cantidades de datos con un tiempo de inactividad mínimo. Los usuarios pueden continuar inmediatamente las operaciones empresariales.

Una vez que Live Recovery se inicia, el volumen restaurado y su contenido vuelven a estar disponibles al instante. El Rapid Recovery Core continúa restaurando los datos en segundo plano, aunque el volumen, sus datos, aplicaciones y servicios estén ya en producción. Si se solicitan datos específicos, el proceso en segundo plano da preferencia a la restauración de dichos datos inmediatamente. Esta poderosa funcionalidad permite también cumplir los acuerdos de servicio más exigentes.

Una vez que ha iniciado Live Recovery, los metadatos (estructura del directorio, descriptores de seguridad, atributos de archivo NTFS, mapa de espacio libre, etc.) del volumen de destino se restauran rápidamente en la máquina protegida. A partir de entonces, el volumen y su contenido pasan a estar disponibles para el sistema. Rapid Recovery Agent comienza la restauración de los bloques de datos desde el servidor del Rapid Recovery Core, escribiendo los bloques en el volumen de destino.

Se responde de inmediato a las solicitudes de datos que todavía no se ha restaurado, con el programa de solicitud o sistema que ignoran que los bloques ya se han restaurado.

Restauración de datos desde puntos de recuperación

Rapid Recovery protege sus datos en equipos Windows y Linux. Las copias de seguridad de los equipos protegidos se guardan en el repositorio asociado con el Rapid Recovery Core como puntos de recuperación. Desde estos puntos de recuperación, puede restaurar los datos utilizando uno de los métodos siguientes.

- En la Rapid Recovery Core Console, puede restaurar volúmenes completos desde un punto de recuperación de un volumen sin sistema, reemplazando los volúmenes en el equipo de destino. Para obtener más información, consulte Acerca de la restauración de volúmenes desde un punto de recuperación.
- También puede restaurar todos los volúmenes en los equipos Linux a partir de los puntos de recuperación, utilizando la línea de comandos del Agent de Linux. Para obtener más información sobre el uso de la utilidad local_mount de la línea de comandos, consulte Restauración de volúmenes para un equipo Linux mediante la línea de comandos.

No puede restaurar un volumen que contenga el sistema operativo directamente desde un punto de recuperación, dado que el equipo en el que está realizando la restauración está utilizando el sistema operativo y controladores que se incluyen en el proceso de restauración. Si desea restaurar desde un punto de recuperación a un volumen del sistema (por ejemplo, la unidad C del equipo protegido), deberá realizar una restauración Bare Metal Restore (BMR). Esto implica crear una imagen de inicio desde el punto de recuperación, que incluye archivos del sistema operativo y de configuración, así como datos. Después, debe iniciar el equipo de destino desde esa imagen de inicio para completar la restauración. La imagen de inicio es diferente si el equipo que quiere restaurar utiliza un sistema operativo Windows o Linux. Si quiere restaurar desde un punto de recuperación en un volumen del sistema en un equipo con Windows, consulte Realización de una restauración

Bare Metal Restore para equipos con Windows. Si quiere restaurar desde un punto de recuperación en un volumen del sistema en un equipo con Linux, consulte Realización de una restauración Bare Metal Restore para equipos con Windows.

Si tiene un software RAID en un equipo Linux protegido por Rapid Recovery Agent versión 6.2, puede restaurar el software RAID desde un punto de recuperación.

NOTE: Esta característica apareció en versión 6.2, de modo que no es compatible con instantáneas realizadas en versiones de Agent anteriores. Si actualiza Rapid Recovery Agent a versión 6.2 o superior y a continuación realiza instantáneas en su Rapid Recovery Core, podrá restaurar el software RAID a partir de las nuevas instantáneas.

Por último, en contraste con la restauración de volúmenes enteros, puede montar un punto de recuperación desde un equipo con Windows y examinar las carpetas y los archivos individuales para recuperar únicamente un conjunto específico de archivos. Para obtener más información, consulte Restauración de un directorio o archivo mediante Windows Explorer. Si necesita realizar esta acción mientras conserva los permisos de archivo original (por ejemplo, al restaurar la carpeta de un usuario en un servidor de archivos), consulte Restauración de un directorio o archivo y conservación de permisos mediante Windows Explorer.

Los temas de esta sección describen información sobre cómo restaurar datos en equipos físicos. Para obtener más información sobre cómo exportar datos protegidos desde un punto de recuperación a una máquina virtual, consulte Exportación de la MV.

NOTE: Al recuperar datos en equipos con Windows, si el volumen que está restaurando tiene activada la desduplicación de datos de Windows, deberá asegurarse de que la desduplicación también está activada en el servidor del Core. Rapid Recovery admite Windows 8, Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016 para transferencias normales (tanto base como incrementales), así como con datos de restauración, restauración Bare Metal Restore y exportaciones virtuales. Para obtener más información acerca de los tipos de volúmenes admitidos y no admitidos para la copia de seguridad y la recuperación, consulte el tema "Limitaciones de compatibilidad de volúmenes básicos y dinámicos" en la *Rapid Recovery System Requirements Guide (Guía de requisitos del sistema de Rapid Recovery)*.

Acerca de la búsqueda de archivos y la función de restauración

La búsqueda de archivos y la función de restauración de Rapid Recovery le permite encontrar uno o varios archivos en los puntos de recuperación de un equipo protegido. De este modo, puede restaurar uno o más de los resultados en un disco local.

Pautas para la búsqueda

En la página de **búsqueda de archivos** de la Core Console, puede buscar un archivo en un conjunto de puntos de recuperación desde el equipo que seleccione. Los criterios de búsqueda se dividen en dos grupos: básicos y avanzados.

El grupo básicos incluye los siguientes parámetros:

- El equipo protegido con los puntos de recuperación que desea buscar.
- Un intervalo de tiempo que limita la búsqueda a únicamente los puntos de recuperación que se crearon entre la hora de inicio y de finalización.
- El nombre o la máscara del archivo que desea buscar. Puede utilizar el comodín "?" para reemplazar cualquier carácter individual y el "*" para reemplazar ninguno o varios caracteres; sin embargo, cuanto más específicos sean los nombres de los archivos, producirán resultados más específicos.
- Una lista de las rutas de acceso a los directorios en los que desea buscar.

NOTE: Todos los criterios básicos son necesarios. Si no se proporciona ningún directorio, Rapid Recovery busca todos los volúmenes del equipo protegido especificado.

El botón **Más opciones** revelará el grupo avanzado, que incluye los siguientes parámetros:

- La opción de buscar recursivamente en subdirectorios de la ubicación de búsqueda o solo en la ubicación especificada.
- La capacidad de ejecutar un algoritmo que aumenta la velocidad de las búsquedas en los volúmenes NTFS.
- La capacidad de limitar el número de resultados de la búsqueda a una suma más fácil de administrar.

NOTE: Los criterios de búsqueda específicos producen de manera más rápida y precisa los resultados de la búsqueda. Incluir subdirectorios (por ejemplo, `C:\work\documents\accounting` en lugar de `C:`), del mismo modo que proporcionar máscaras de archivo restrictivas (por ejemplo, `invoice*.pdf` en lugar de `in*.*`) reduce la cantidad de tiempo que tarda en realizar la búsqueda.

Debido a que la función continúa buscando en los puntos de recuperación y ubicaciones incluso después de encontrar el archivo requerido, puede pausar o detener una búsqueda antes de que finalice. Puede ejecutar varias las búsquedas simultáneamente, pero no puede iniciarlas al mismo tiempo. Por ejemplo, para encontrar otro archivo puede empezar una segunda búsqueda mientras la primera aún está en curso. Sin embargo, solo puede buscar en un equipo protegido a la vez.

NOTE: En el ejemplo anterior, al pausar la primera búsqueda proporciona más memoria disponible para la segunda búsqueda, lo que ayuda a que termine antes. Ejecutar múltiples búsquedas a la vez exige mucha memoria y aumenta la cantidad de tiempo que se tarda en realizar una búsqueda.

Cada búsqueda aparece como una pestaña en la página. Cuando haya terminado, puede cerrar las pestañas una a una o todas a la vez.

Pautas para la restauración

Después de haber **encontrado el archivo**, puede restaurarlo directamente desde la página de búsqueda.

La búsqueda de archivos y la función de restauración limita las capacidades de restauración solo para ubicaciones en el Core. No puede restaurar un archivo a un equipo protegido.

Tareas relacionadas

See also: Encontrar y restaurar un archivo

Encontrar y restaurar un archivo

Cuando desea restaurar un archivo en lugar de un volumen, puede utilizar Rapid Recovery para encontrar ese archivo entre los puntos de recuperación de su equipo protegido. Los criterios de búsqueda, como por ejemplo el intervalo de fechas y el directorio, le permiten restringir la búsqueda a un pequeño grupo de puntos de recuperación.

NOTE: Los criterios de búsqueda específicos producen de manera más rápida y precisa los resultados de la búsqueda y consumen menos memoria. Incluir subdirectorios (por ejemplo, `C:\work\documents\accounting` en lugar de `C:`), del mismo modo que proporcionar máscaras de archivo restrictivas (por ejemplo, `invoice*.pdf` en lugar de `in*.*`) reduce la cantidad de tiempo que tarda en realizar la búsqueda.

Después de haber encontrado el archivo, puede restaurarlo directamente desde la lista de resultados de la búsqueda.

1. En la barra de iconos Rapid Recovery Core Console, haga clic en el menú desplegable **Más**, y seleccione **Búsqueda de archivos**.

Se abre la página **Búsqueda de archivos**.

2. En la página **Búsqueda de archivos**, para buscar un archivo entre los puntos de recuperación de un equipo protegido específico, complete la información que se describe en la tabla que aparece a continuación.

Tabla 135. Criterios de búsqueda de archivos

Criterios de búsqueda para encontrar un archivo entre los puntos de recuperación de un equipo protegido.

Cuadro de texto	Descripción
Equipo	Seleccione en la lista desplegable el equipo protegido que desea buscar. **NOTE:** Puede buscar en los puntos de recuperación de un solo equipo protegido al mismo tiempo.
Intervalo de fechas de los puntos de recuperación	Especifique la fecha y la hora del punto de recuperación más antiguo y del nuevo punto de recuperación que desea buscar. Solo se buscarán los puntos de recuperación creados en este periodo. **NOTE:** El periodo de tiempo predeterminado es el mes anterior. Por ejemplo, si está buscando el martes, 22 de agosto de 2017 a las 14:04, el intervalo de fechas predeterminado es del 22/07/2017 a las 14:04 al 22/08/2017 a las 14:04.
Nombre de archivo (pueden utilizarse los caracteres comodín * y ?)	Introduzca el nombre del archivo o una máscara de archivo para el archivo que desea encontrar y restaurar. Los comodines pueden utilizarse como sustitutos de caracteres desconocidos. **NOTE:** Puede utilizar el comodín "?" para reemplazar cualquier carácter individual y el "*" para reemplazar cero o varios caracteres.
Directorios de búsqueda	Enumera uno o varios directorios del equipo protegido para limitar la búsqueda solo a estas ubicaciones. **NOTE:** Si no se proporciona ningún directorio, Rapid Recovery busca todos los volúmenes del equipo protegido especificado.

3. De manera opcional, haga clic en **Más opciones** y, a continuación, complete la información que se describe en la tabla siguiente.

Tabla 136. Más opciones de búsqueda de archivos

Más criterios de búsqueda para buscar un archivo en los puntos de recuperación de un equipo protegido.

Cuadro de texto	Descripción
Incluir subdirectorios	Busca todos los subdirectorios de los directorios que se enumeran en el paso 3. Habilitado de manera predeterminada.
Usar el algoritmo de búsqueda rápida para volúmenes NTFS	Busca volúmenes NTFS sin montarlos analizando las estructuras de los datos del sistema de archivos, que es más rápido y consume menos memoria durante la búsqueda. Habilitado de manera predeterminada. **NOTE:** Si se produce un problema durante una búsqueda de un volumen NTFS, intente realizar la búsqueda de nuevo sin la opción seleccionada.

Cuadro de texto	Descripción
Limitar resultados de la búsqueda a	Introduzca el número máximo de resultados que desea que aparezcan. El valor predeterminado es 1000.

4. Haga clic en **Iniciar búsqueda**.

   Comienza la búsqueda. Cada búsqueda aparece como una pestaña en **Resultados de la búsqueda**. Puede utilizar los botones de cada pestaña para pausar o detener una búsqueda o puede hacer clic en **X** en la pestaña para eliminar la búsqueda. Se pueden ejecutar varias búsquedas simultáneamente.
5. En los resultados de la búsqueda, seleccione el archivo que desea restaurar.
6. Haga clic en **Restaurar**.

   Se abre el cuadro de diálogo **Restaurar archivos**.
7. Para **Ubicación**, introduzca una ruta de destino para el archivo restaurado en el equipo en que el Core está instalado y en ejecución.
8. Haga clic en **Restaurar**.

   El archivo que ha seleccionado se restaura en la ruta de destino especificada con el árbol de directorio original en que el archivo aparecía en el equipo protegido.

Conceptos relacionados

See also: Acerca de la búsqueda de archivos y la función de restauración

Acerca de la restauración de volúmenes desde un punto de recuperación

Puede restaurar los volúmenes de un equipo protegido desde los puntos de recuperación almacenados en el Rapid Recovery Core mediante el asistente para restaurar un equipo.

NOTE: En versiones anteriores, este proceso se denominaba realizar una reversión.

NOTE: Rapid Recovery es compatible con la protección y recuperación de equipos configurados con particiones EISA. La compatibilidad también se amplía a equipos con Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016 que utilicen Windows Recovery Environment (Windows RE).

Puede comenzar una restauración desde cualquier ubicación de la Rapid Recovery Core Console haciendo clic en el icono **Restaurar** de la barra de botones de Rapid Recovery. Cuando inicia una restauración de esta manera, debe especificar cuál de los equipos protegidos en el Core desea restaurar y, a continuación, desplazarse hasta el volumen que desee restaurar.

También puede ir a la **página de puntos** de recuperación de un equipo específico, hacer clic en el menú desplegable de un punto de recuperación específico y, a continuación, seleccionar **Restaurar**. Si comienza una restauración de esta manera, comience por el paso 5 del tema Restauración de volúmenes desde un punto de recuperación.

También puede restaurar un punto de recuperación en un equipo Linux desde la línea de comandos. Para obtener más información, consulte el tema Restauración de volúmenes para un equipo Linux mediante la línea de comandos.

Si desea restaurar desde un punto de recuperación a un volumen del sistema, o bien restaurar desde un punto de recuperación utilizando un CD de inicio, deberá realizar una restauración Bare Metal Restore (BMR). Para obtener más información sobre BMR, consulte Restauración Bare Metal Restore para equipos con Windows,

y para consultar la información de requisitos previos para los sistemas operativos Windows o Linux, consulte Requisitos previos para realizar una restauración Bare Metal Restore para un equipo con Windows y Requisitos previos para realizar una restauración Bare Metal Restore para un equipo Linux, respectivamente. Puede acceder a funciones BMR de la Core Console como se describen en las directrices de cada sistema operativo. También puede realizar una BMR desde el Asistente para restaurar un equipo. El procedimiento le dirigirá al punto apropiado en el asistente al procedimiento Restauración Bare Metal Restore con el Asistente para restaurar un equipo.

Restauración de volúmenes desde un punto de recuperación

Para restaurar volúmenes desde un punto de recuperación, el equipo debe estar protegido en el Core al nivel de volumen y el Core debe contener puntos de recuperación desde los que realizar la operación de restauración.

Realice el procedimiento siguiente para restaurar volúmenes desde un punto de recuperación.

1. Para restaurar un volumen en un equipo protegido, desplácese hasta la Core Console y haga clic en **Restaurar** en la barra de botones de Rapid Recovery.

   Aparecerá el Asistente para restaurar un equipo.

2. Desde la página **Equipos protegidos**, seleccione el equipo protegido para el que desee restaurar datos y, a continuación, haga clic en **Siguiente**.

   Aparecerá la página **Puntos de recuperación**.

3. Desde la lista de puntos de recuperación, busque la instantánea que quiera restaurar en el equipo protegido.

   - Si es necesario, utilice los botones de la parte inferior de la página para mostrar más páginas de puntos de recuperación.
   - Opcionalmente, para limitar la cantidad de puntos de recuperación que aparecen en la página **Puntos de recuperación** del asistente, puede filtrar por volúmenes (si está definido) o por fecha de creación del punto de recuperación.

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

   Aparecerá la página **Destino**.

5. En la página **Destino**, seleccione el equipo en el que quiera restaurar datos de la manera siguiente:

   - Para restaurar datos desde el punto de recuperación seleccionado al mismo equipo y si los volúmenes que quiere restaurar no incluyen el volumen del sistema, seleccione **Recuperar en un equipo protegido (solamente volúmenes que no sean del sistema)**, verifique que el equipo de destino está seleccionado y, a continuación, haga clic en **Siguiente**.

     Aparecerá la página **Asignación de volúmenes**. Continúe en el paso 9.

   - Para restaurar datos desde el punto de recuperación seleccionado a un equipo protegido diferente (por ejemplo, sustituir el contenido de Equipo2 por datos de Equipo1), seleccione **Recuperar en un equipo protegido (solamente volúmenes que no sean del sistema)**, seleccione el equipo de destino en la lista y, a continuación, haga clic en **Siguiente**.

     Aparecerá la página **Asignación de volúmenes**. Continúe en el paso 9.

   - Si desea restaurar desde un punto de recuperación al mismo equipo o a un equipo diferente utilizando un CD de inicio, este proceso se considera una restauración Bare Metal Restore (BMR). Para obtener información acerca de la restauración BMR, consulte Bare Metal Restore.

NOTE: La realización de una BMR tiene requisitos específicos, en base al sistema operativo del equipo que desea restaurar. Para conocer los requisitos previos, consulte Requisitos previos para realizar una restauración Bare Metal Restore para un equipo con Windows y Requisitos previos para realizar una restauración Bare Metal Restore para un equipo Linux, respectivamente.

NOTE: Si los volúmenes que desea restaurar incluyen el volumen del sistema, seleccione **Recupere en cualquier máquina de destino usando un CD de inicio**. Esta opción le pide que cree un CD de inicio.

- Para continuar y crear el CD de inicio con información del punto de recuperación seleccionado empleando el Asistente para restaurar un equipo, haga clic en **Siguiente** y vaya al Realización de una restauración Bare Metal Restore para equipos con Windows.
- Si ya ha creado el CD de inicio y el equipo de destino se ha iniciado con el CD de inicio, vaya alpaso 8 del tema Realización de una restauración Bare Metal Restore para equipos con Windows.

- Si desea restaurar desde un punto de recuperación a un volumen del sistema (por ejemplo, la unidad C del equipo Agent llamado Equipo1), este proceso también se considera una BMR. Seleccione **Recuperar en cualquier equipo de destino mediante un CD de inicio**. Esta opción le pide que cree un CD de inicio.
  - Para continuar y crear el CD de inicio con información del punto de recuperación seleccionado empleando el Asistente para restaurar un equipo, haga clic en **Siguiente** y vaya al Realización de una restauración Bare Metal Restore para equipos con Windows.
  - Si ya ha creado el CD de inicio, continúe en el paso 6.

6. Inicie el equipo que desea restaurar empleando el CD de inicio. Para obtener más información sobre BMR en un equipo con Windows, consulte Carga del CD de inicio e inicio del equipo de destino y para BMR en un equipo con Linux, consulte Carga del Live DVD e inicio del equipo de destino.
7. En el servidor Core, en la página **Destino** del Asistente para restaurar un equipo, seleccione **Ya tengo un CD de inicio ejecutándose en el equipo de destino** y, a continuación, introduzca la información sobre el equipo con el que desea conectar que está descrita en la siguiente tabla.

Tabla 137. Información del equipo

Cuadro de texto	Descripción
Dirección IP	Dirección IP del equipo que desea restaurar. Esta es idéntica a la dirección IP mostrada en la URC.
Clave de autenticación	Contraseña específica con la que conectarse al servidor seleccionado. Esta es idéntica a la clave de autenticación mostrada en la URC.

8. Haga clic en **Siguiente**.

   Si la información de conexión que introdujo coincide con la URC y si el Core y el servidor de destino pueden identificarse entre sí adecuadamente en la red, se cargarán los volúmenes para el punto de recuperación seleccionado. Aparecerá la página **Asignación de discos**.

   Para completar la restauración BMR desde el Asistente para restaurar un equipo, continúe en el paso 9 del tema Realización de una restauración Bare Metal Restore para equipos con Windows.

NOTE: Rapid Recovery es compatible con las particiones FAT32 y ReFS. Solo se admite la restauración completa y el BMR puesto que hay una limitación de controladores con el ReFS. La restauración se implementa en el modo usuario, exportación VM, etc. Si un Core está protegiendo al menos un volumen agente con el sistema de archivos ReFS, debería instalarse en equipos con Windows 8.1, Windows 10 (solo Enterprise o Pro), Windows Server 2012, Windows Server 2012 R2 o Windows Server 2016, ya que proporcionan compatibilidad nativa con ReFS. Si no es así, las funciones están limitadas y las operaciones de tipo montaje de una imagen de volumen no funcionan. La Rapid Recovery Core Console presenta los mensajes de error pertinentes en estas apariciones. La restauración Bare Metal Restore de la configuración de discos de espacios de almacenamiento tampoco se admite en esta versión. Para obtener más detalles, consulte la *Guía de instalación y actualización de Rapid Recovery*.

9. En la página **Asignación de volúmenes**, para cada volumen del punto de recuperación que quiera restaurar, seleccione el volumen de destino adecuado. Si no quiere restaurar un volumen, en la columna Volúmenes de destino, seleccione **No restaurar**.
10. Seleccione **Mostrar opciones avanzadas** y, a continuación, haga lo siguiente:
    - Para restaurar en máquinas con Windows, si desea utilizar Live Recovery, seleccione **Live Recovery**.

      Al utilizar la tecnología de recuperación instantánea de Live Recovery en Rapid Recovery, puede recuperar o restaurar datos instantáneamente en sus máquinas físicas o en máquinas virtuales desde puntos de recuperación almacenados de equipos Windows, lo cual incluye espacios de almacenamiento de Microsoft Windows. Live Recovery no está disponible para equipos con Linux ni máquinas virtuales que utilicen protección sin agentes.
    - Si desea forzar los volúmenes seleccionados para desmontar antes de que empiece la restauración, seleccione **Forzar desmontaje**.

      CAUTION: Si no fuerza un desmontaje antes de restaurar datos, puede que la restauración falle con un error que diga que el volumen está en uso.
11. Haga clic en **Siguiente.**
12. En la página **Desmontar bases de datos**, si los volúmenes que desea restaurar contienen bases de datos de Oracle, SQL o Microsoft Exchange, se le solicitará que las desmonte. Si desea volver a montar estas bases de datos automáticamente después de que la restauración se haya completado, seleccione **Volver a montar todas las bases de datos automáticamente después de que se haya restaurado el punto de recuperación**. De lo contrario, elimine la selección.

    NOTE: El escritor VSS adecuado captura las instantáneas de la base de datos en el modo de copia de seguridad. Si selecciona no volver a montar todas las bases de datos automáticamente (la opción predeterminada), después de restaurar debe iniciar manualmente las bases de datos.
13. Haga clic en **Siguiente.**

Es posible que aparezca la página Advertencia y le indique que cierre todos los programas en los volúmenes que desea restaurar. Si lo hace, haga clic en Siguiente de nuevo.

14. En la página **Resumen**, seleccione la opción **IMPORTANTE**. **Entiendo que esta operación sobrescribirá los volúmenes seleccionados con los datos del punto de recuperación seleccionado** para confirmar que entiende las consecuencias de una restauración de volúmenes.

    WARNING: Esta opción hace hincapié en la consecuencia de que los datos que se hayan guardado en el volumen seleccionado después de la fecha y la hora del punto de recuperación seleccionado se perderán después de la restauración.
15. Haga clic en **Finalizar**.

Restauración de un directorio o archivo mediante Windows Explorer

Puede utilizar Windows Explorer para copiar y pegar directorios y archivos desde un punto de recuperación montado en cualquier equipo con Windows. Esto puede ser de utilidad cuando solamente quiere distribuir una parte de un punto de recuperación a sus usuarios.

Cuando copie directorios y archivos, los permisos de acceso del usuario que esté realizando la operación de copia se utilizarán y aplicarán en los directorios y archivos pegados. Si quiere restaurar directorios y archivos para sus usuarios conservando los permisos de archivo original (por ejemplo, al restaurar la carpeta de un usuario en un servidor de archivos), consulte Restauración de un directorio o archivo y conservación de permisos mediante Windows Explorer.

1. Monte el punto de recuperación que contenga los datos que quiera restaurar. Para obtener información detallada, consulte Montaje de un punto de recuperación.
2. En Windows Explorer, desplácese hasta el punto de recuperación montado y seleccione los directorios y archivos que quiera restaurar. Haga clic con el botón secundario y seleccione **Copiar**.
3. En Windows Explorer, desplácese hasta la ubicación del equipo en el que quiera restaurar los datos. Haga clic con el botón secundario y seleccione **Pegar**.

Restauración de un directorio o archivo y conservación de permisos mediante Windows Explorer

Puede utilizar Windows Explorer para copiar y pegar directorios y archivos desde un punto de recuperación montado en cualquier equipo con Windows conservando los permisos de acceso de archivo.

Por ejemplo, si necesita restaurar una carpeta a la que solamente accedan usuarios específicos de un servidor de archivos, puede utilizar los comandos Copiar y Pegar con permisos para garantizar que los archivos restaurados conservan los permisos que restringen el acceso. De este modo, puede evitar tener que aplicar permisos manualmente a los directorios y archivos restaurados.

Algunos archivos tienen restricciones de acceso a archivos que requieren privilegios administrativos. Especialmente para Windows Server 2012 y sistemas operativos posteriores, el usuario que intenta la restauración debe tener los permisos de NTFS correctos para restaurar correctamente. Por ejemplo, para copiar todos los permisos de NTFS desde un punto de montaje, el usuario debe tener privilegios administrativos (con todos los permisos de NTFS).

NOTE: El comando Pegar con permisos se instala con el software Rapid Recovery Core y Agent. No está disponible en Local Mount Utility.

1. Monte el punto de recuperación que contenga los datos que quiera restaurar. Para obtener información detallada, consulte Montaje de un punto de recuperación.
2. En Windows Explorer, desplácese hasta el punto de recuperación montado y seleccione los directorios y archivos que quiera restaurar. Haga clic con el botón secundario y seleccione **Copiar**.
3. En Windows Explorer, desplácese hasta la ubicación del equipo en el que quiera restaurar los datos. Haga clic con el botón secundario y seleccione **Pegar con permisos**.

   NOTE: En este paso, si el comando Pegar con permisos está desactivado en el menú secundario, Windows Explorer no detecta los archivos que quiere copiar. Repita el Paso 2 para activar el comando Pegar con permisos en el menú secundario.

Restauración y nodos de clúster

Una restauración es el proceso de restaurar los volúmenes en un equipo a partir de puntos de recuperación. Para un clúster de servidor, realice una restauración a nivel de nodo o equipo. Esta sección proporciona directrices para realizar una restauración para volúmenes de clúster.

Realización de una restauración para clústeres de CCR y DAG (Exchange)

Realice los pasos de este procedimiento para efectuar una restauración para clústeres de CCR y DAG (Exchange).

1. Apague todos los nodos excepto uno.
2. Realice una restauración usando el procedimiento estándar de Rapid Recovery para el equipo, según se describe en Acerca de la restauración de volúmenes desde un punto de recuperación y Restauración de volúmenes para un equipo Linux mediante la línea de comandos.
3. Cuando la restauración haya finalizado, monte todas las bases de datos para los volúmenes de clúster.
4. Encienda el resto de nodos.
5. Para Exchange, acceda a la Consola de administración de Exchange y, para cada base de datos, realice la operación Actualizar copia de base de datos.

Realización de una restauración para clústeres de SCC (Exchange, SQL)

Realice los pasos de este procedimiento para efectuar una restauración para clústeres de SCC (Exchange, SQL).

1. Apague todos los nodos excepto uno.
2. Realice una restauración usando el procedimiento estándar de Rapid Recovery para el equipo, según se describe en Acerca de la restauración de volúmenes desde un punto de recuperación y Restauración de volúmenes para un equipo Linux mediante la línea de comandos.
3. Una vez terminada la restauración, monte todas las bases de datos a partir de los volúmenes de clúster.
4. Encienda el resto de nodos, de uno en uno.

> **NOTE:** No es necesario revertir el disco de quórum. Se puede generar automáticamente o usando la funcionalidad del servicio de clúster.

Restauración a partir de un archivo conectado

Hay dos maneras que usted puede restaurar datos desde un archivo: Puede utilizar un archivo como fuente para una restauración Bare Metal Restore (BMR); o puede conectar un archivo, montar un punto de recuperación desde el archivo y, a continuación, restaurar los datos archivados.

Cuando conecta un archivo, aparecerá bajo Archivo conectado en la página Archivos de la Core Console, mientras que se puede acceder al contenido del archivo desde el área de navegación de la izquierda. El contenido aparece bajo el nombre del archivo. Los equipos que fueron archivados aparecen como los equipos con punto de recuperación únicamente para que pueda acceder a los puntos de recuperación de la misma forma que lo haría para un equipo protegido: montando un punto de recuperación, localizando el elemento que desea recuperar y usando el Explorador de Windows para copiar y pegar el elemento en su destino.

Existen ventajas con respecto a la restauración a partir de un archivo en lugar de importar un archivo a un repositorio.

- La restauración a partir de un archivo conectado ahorra tiempo que puede emplear para importar un archivo completo a un repositorio.
- Además, cuando se importa un archivo, los puntos de recuperación archivados se agregan al repositorio.

  Debido a que los puntos de recuperación archivados son probablemente los elementos más antiguos del repositorio, es posible que se estén organizados de acuerdo a su política de retención durante el siguiente trabajo nocturno. (No obstante, esta acción no se borra del archivo; podría volver a importarlos al día siguiente).
- Por último, el Core recuerda la asociación de adjuntos con archivos, incluso después de desconectar un archivo, lo que hace que conectar el archivo de nuevo más tarde sea más rápido y fácil.

  Puede quitar la asociación mediante la eliminación del adjunto.

Para restaurar datos desde un archivo conectado, realice los pasos siguientes utilizando los vínculos relacionados:

NOTE: El procedimiento de restauración de un archivo conectado presupone que ya tiene un archivo de puntos de recuperación resumidos.

1. Conecte el archivo.
2. Monte el punto de recuperación que contiene el elemento que desea recuperar.
3. Restaure los datos mediante cualquiera de los métodos siguientes:
   - Restaure los datos, como archivo o carpeta, desde el punto de recuperación.
   - Restaure todo el punto de recuperación.
   - Exporte el punto de recuperación a una máquina virtual.

See also: Cómo funciona la archivación
See also: Adición de un archivo comprimido
See also: Importación de un archivo
See also: Montaje de un punto de recuperación
See also: Restauración de un directorio o archivo mediante Windows Explorer
See also: Restauración de volúmenes desde un punto de recuperación
See also: Exportación a máquinas virtuales con Rapid Recovery
See also: Llevar a cabo una BMR a partir de un archivo

Restauración de correo electrónico en Rapid Recovery

La función Restauración de correo electrónico enRapid Recovery le permite restaurar un buzón de correo, una carpeta o un elemento (como un mensaje, evento del calendario o contacto) del almacén de datos de un equipo protegido del Exchange Server. Puede restaurar su selección en una carpeta de recuperación, en la fuente original o en uno o más archivos PST.

Puede acceder a la página Restauración de correo electrónico desde el menú **Más** (...) de la Rapid Recovery Core Console. Desde ahí, puede completar las siguientes acciones:

- Abrir una base de datos de Exchange
- Restaurar un elemento a partir de la base de datos abierta
- Cerrar la base de datos
- Buscar un elemento en la base de datos abierta

Para obtener más información, consulteApertura de una base de datos de Exchange Rapid Recovery y Restauración de un elemento de correo electrónico en Rapid Recovery.

Requisitos previos de restauración de correo electrónico

Antes de poder restaurar los elementos de correo electrónico, debe cumplir los siguientes requisitos previos:

- Outlook 2007 o posterior debe estar instalado en el equipo del Core.
- Hay al menos un perfil configurado en Microsoft Outlook.
- El perfil de Outlook asociado debe tener permisos de control completo, incluidos los permisos Enviar como y Recibir como.Para obtener más información, consulte.
- La opción Modo de almacenamiento en caché Exchange de Outlook bajo el perfil de Outlook asociado con Rapid Recovery debe estar deshabilitada.
- El equipo del Core está en el mismo dominio que la base de datos de Exchange.
- La base de datos de Exchange está abierta y usted se encuentra en la página **Restauración de correo electrónico** de laRapid Recovery Core Console.Para obtener más información, consulteApertura de una base de datos de Exchange Rapid Recovery.

Sin los permisos adecuados y una instancia de Outlook instalada en el equipo del Core, no es posible realizar la recuperación de elementos de Exchange, aunque el servidor de Exchange esté protegido por un Rapid Recovery Core.

Apertura de una base de datos de Exchange Rapid Recovery

Antes de comenzar esta tarea, asegúrese de que se completan los siguientes requisitos previos:

- Outlook 2007 o posterior debe estar instalado en el equipo del Core.
- El equipo del Core está en el mismo dominio que la base de datos de Exchange.
- Los permisos adecuados establecidos en Exchange. Para obtener más información, consulte .

Rapid Recovery le permite restaurar elementos de correo electrónico sin abandonar la interfaz. Los elementos de correo electrónicos están en la base de datos de Exchange, en el punto de recuperación de un equipo de Exchange Server protegido, que puede abrir mediante el asistente Abrir bases de datos de Exchange.

1. Desde Rapid Recovery Core Console, haga clic en el menú Más (**...**) y, a continuación, haga clic en **Restauración de correo electrónico**.
2. En la página **Restauración de correo electrónico**, para acceder a la base de datos de Exchange en la que se almacena el elemento de correo electrónico, haga clic en **Abrir base de datos**.

El asistente Abrir bases de datos de Exchange se abrir.

3. En la página **Ubicación** del asistente, puede abrir una base de datos desde un equipo protegido o una ruta de acceso local, como el equipo actual o un recurso compartido de archivos:
   - **Abrir desde equipo protegido**: Haga clic en **Siguiente** y, a continuación, continúe al siguiente paso de la tarea.
   - **Abrir desde ruta de acceso local**: Introduzca la siguiente información de la ubicación y, a continuación, haga clic en **Finalizar**:
     - Ruta de acceso del archivo de base de datos
     - Ruta de acceso de registros
     - Ruta de acceso del sistema
4. En la página **Equipos**, seleccione el equipo protegido que alberga la base de datos de Exchange y, a continuación, haga clic en **Siguiente**.
5. En la página **Puntos de recuperación**, seleccione el punto de recuperación del momento temporal desde el que desea abrir la base de datos y, a continuación, haga clic en **Siguiente**.
6. En la página **Base de datos**, seleccione la base de datos de Exchange que desea abrir y, a continuación, haga clic en **Siguiente**.

   Rapid Recovery abre la base de datos seleccionada y se muestra en la página **Restauración de correo electrónico**, con los buzones de correo y las carpetas enumeradas a la izquierda, en un árbol de navegación ampliable. Los elementos de las carpetas se muestran a la derecha.

   NOTE: La cantidad de tiempo que tardaRapid Recovery en abrir la base de datos de Exchange depende del tamaño de la base de datos.

Para restaurar un elemento a partir de la base de datos abierta, consulte Restauración de un elemento de correo electrónico en Rapid Recovery.

Restauración de un elemento de correo electrónico en Rapid Recovery

Antes de comenzar con la tarea, asegúrese de que ha cumplido los requisitos previos para completar una tarea de restauración.Para obtener más información, consulteRequisitos previos de restauración de correo electrónico.

La función Restauración de correo electrónico deRapid Recovery le permite restaurar un buzón de correo, una carpeta o un elemento (como un mensaje, evento de calendario o contacto) desde el almacén de datos de un equipo Exchange Server protegido. Puede restaurar su selección en una carpeta de recuperación, en la fuente original o en uno o más archivos PST. Para restaurar un elemento de correo electrónico desde Rapid Recovery Core Console, complete los siguientes pasos.

1. Desde la base de datos de Exchange en la página **Restauración de correo electrónico**, seleccione el elemento que desea recuperar y, a continuación, en la barra de acciones **Restaurar correo electrónico**, haga clic en **Restaurar**.

Se abrirá el **Asistente de restauración de correo electrónico**.

2. En la página **Restaurar sesión**, complete una de las siguientes opciones y, a continuación, haga clic en **Siguiente**.
   - Si restaura elementos de correo electrónico por primera vez, introduzca un nombre para mostrar y las credenciales de Outlook de la sesión de restauración. Puede seleccionar esta sesión para una restauración futura.
   - Si ha creado previamente sesiones de restauración, seleccione una de las siguientes opciones:
     - Seleccione **Utilizar sesión de restauración existente** y, a continuación, seleccione una sesión de la lista desplegable.
     - Seleccione **Crear nueva sesión de restauración** y, a continuación, introduzca un nombre para mostrar y las credenciales de Outlook para la sesión de restauración.
3. En la página **Destino**, seleccione la ubicación de destino del elemento restaurado desde las siguientes opciones, y haga clic en **Siguiente**:

Tabla 138. Destinos de restauración de correo electrónico

Opción	Descripción
Restaurar a la carpeta de recuperación	Recupera los elementos seleccionados (incluida la jerarquía de carpetas) en una carpeta de recuperación de un buzón de correo en línea de su elección. Vaya al paso 4.
Restaurar a la ubicación original	Dirige el elemento seleccionado (incluida la jerarquía de carpetas) al buzón de correo electrónico del almacén de datos en línea en el que residía originariamente. Vaya al paso 5.
Restaurar al archivo PST	Guarda los elementos seleccionados (incluida la jerarquía de carpetas) creando un archivo PST (Personal Storage Table) o escribiendo en un archivo PST existente. Vaya al paso 6.
Restaurar a archivos PST (archivo individual para cada buzón de correo)	Guarda cada buzón de correo como un archivo PST (Personal Storage Table). Vaya al paso 6.

4. Si selecciona **Restaurar a la carpeta de recuperación**, en la página **Configuración**, seleccione un **Perfil** de la lista desplegable, examine y seleccione la libreta de direcciones de Outlook y, a continuación vaya al paso 7.

   De manera opcional, seleccione **Mostrar opciones avanzadas**, para personalizar más la restauración con las siguientes opciones:

Tabla 139. Opciones de restauración de correo electrónico avanzadas

Opción	Descripción
Gestión de errores	Determina la forma de abordar y gestionar cualquier error que se produzca durante el proceso de restauración. Seleccione una de las opciones siguientes: • **Registrar y continuar**. Recopila los mensajes de error en un registro y continúa con el proceso de restauración. • **Notificar al usuario**. Pausa la restauración y muestra un mensaje en el cuadro de diálogo Supervisar tarea activa cuando encuentra un error, y le da la opción de continuar o cancelar la restauración. • **Anular restauración**. Finaliza el proceso de restauración cuando se produce un error.
Restaurar objetos eliminados	Para una base de datos de Exchange 2010, 2013 y 2016, restaura los elementos eliminados de forma permanente. Para una base de datos de Exchange 2007, se restaura los elementos tachados de la carpeta actual.
Restaurar reglas de correo electrónico	Restaura cualquier regla que el usuario tuviera vigente en el momento en que se realizó la copia de seguridad de los datos.

5. Si selecciona **Restaurar a la ubicación original**, en la página **Configuración**, seleccione el **Perfil** de Outlook de destino, seleccione un **Tipo de restauración** de las siguientes opciones y, a continuación, vaya al paso 7:
   - **Restaurar únicamente diferencias**. Identifica si el elemento que se está restaurando ya está presente en la carpeta de destino y únicamente finaliza la restauración si no hay ningún elemento duplicado. También se conoce como restauración diferencial.
   - **Crear entradas duplicadas**. Restaura todos los elementos seleccionados sin sobrescribir los elementos existentes, con lo que se obtienen duplicados de los elementos previamente existentes.
   - **Sobrescribir si es más reciente**. Restaura los elementos más nuevos que no están presentes en el almacén de datos en línea. También restaura los elementos que están presentes en los almacenes de datos en línea pero que son más antiguos que los de la copia de la base de datos de Exchange.

   De manera opcional, seleccione **Mostrar opciones avanzadas**, para personalizar más la restauración con las siguientes opciones:

Tabla 140. Opciones de restauración de correo electrónico avanzadas

Opción	Descripción
Gestión de errores	Determina la forma de abordar y gestionar cualquier error que se produzca durante el proceso de restauración. Seleccione una de las opciones siguientes: • **Registrar y continuar**. Recopila los mensajes de error en un registro y continúa con el proceso de restauración. • **Notificar al usuario**. Pausa la restauración y muestra un mensaje en el cuadro de diálogo Supervisar tarea activa cuando encuentra un error, y le da la opción de continuar o cancelar la restauración. • **Anular restauración**. Finaliza el proceso de restauración cuando se produce un error.
Restaurar objetos eliminados	Para una base de datos de Exchange 2010, 2013 y 2016, restaura los elementos eliminados de forma permanente.

Opción	Descripción
	Para una base de datos de Exchange 2007, se restaura los elementos tachados de la carpeta actual.
Restaurar reglas de correo electrónico	Restaura cualquier regla que el usuario tuviera vigente en el momento en que se realizó la copia de seguridad de los datos.
Restaurar permisos de usuario	Restaura los permisos personalizados definidos para una carpeta pública. **NOTE:** Esta opción solo está disponible cuando se restaura una carpeta pública a su ubicación original. Si no selecciona la opción para restaurar permisos, los permisos de carpeta predeterminados se restauran con el contenido.

6. Si selecciona **Restaurar al archivo PST** o **Restaurar al archivo PST (archivo separado para cada buzón de correo)**, en la página **Configuración**, complete las siguientes selecciones y, a continuación, vaya al paso 7:
   a. **Perfil**. Seleccione un perfil de Outlook de la lista desplegable.
   b. **Almacenamiento de PST principal**. Para ubicar y seleccionar la carpeta de destino inicial para el archivo PST, introduzca la ruta o seleccione un archivo existente.
   c. **Almacenamiento de PST adicional (opcional)**. Si el destino principal no dispone de espacio suficiente para el archivo PST, seleccione un destino secundario para este.

   NOTE: No asigne la ubicación de contenido adicional al mismo disco que la ubicación principal.

   De manera opcional, seleccione **Mostrar opciones avanzadas**, para personalizar más la restauración con las siguientes opciones:

Tabla 141. Opciones de restauración de correo electrónico avanzadas

Opción	Descripción
Gestión de errores	Determina la forma de abordar y gestionar cualquier error que se produzca durante el proceso de restauración. Seleccione una de las opciones siguientes: • **Registrar y continuar**. Recopila los mensajes de error en un registro y continúa con el proceso de restauración. • **Notificar al usuario**. Pausa la restauración y muestra un mensaje en el cuadro de diálogo Supervisar tarea activa cuando encuentra un error, y le da la opción de continuar o cancelar la restauración. • **Anular restauración**. Finaliza el proceso de restauración cuando se produce un error.
Restaurar objetos eliminados	Para una base de datos de Exchange 2010, 2013 y 2016, restaura los elementos eliminados de forma permanente. Para una base de datos de Exchange 2007, se restaura los elementos tachados de la carpeta actual.

7. Haga clic en **Finalizar**.

   Los elementos se restauran en el destino seleccionado. Puede supervisar el progreso del trabajo en la página Eventos.

Bare Metal Restore

En esta sección se describe el método para restaurar en equipo protegido con Windows desde hardware igual o diferente con la restauración Bare Metal Restore.

Restauración Bare Metal Restore para equipos con Windows

Los servidores, cuando funcionan según lo esperado, realizan las tareas para las que están configurados. Esto cambia únicamente cuando fallan. Si se produce algún hecho catastrófico, que deje inoperable el servidor, deberán tomarse de inmediato pasos para restaurar todas las funciones de ese equipo.

Rapid Recovery ofrece la capacidad de realizar una restauración Bare Metal Restore (BMR) para equipos con Windows o Linux. BMR es un proceso que restaura toda la configuración de software de un sistema específico. Utiliza el término “Bare Metal” (reconstrucción completa) porque la operación de restauración no solamente recupera los datos del servidor, sino que también reformatea el disco duro y reinstala el sistema operativo y todas las aplicaciones de software. Para realizar una BMR, debe especificar un punto de recuperación desde un equipo protegido y revertir (realizar una restauración) a la máquina física o virtual designada. Si está realizando una restauración en un volumen del sistema, esto se considera una BMR. Si está realizando una restauración y requiere un CD de inicio, esto se considera una BMR. Otras circunstancias en las que puede elegir realizar una restauración completa incluyen una actualización de hardware o la sustitución de un servidor. En ambos casos, la restauración se realiza a partir de un punto de restauración en el hardware actualizado o sustituido.

Rapid Recovery admite los sistemas operativos Windows 8, 8.1 y Windows Server 2012, 2012 R2 que se inician desde particiones de EFI FAT32 disponibles para su protección o recuperación, así como volúmenes de Resilient File System (ReFS).

NOTE: La restauración Bare Metal Restore de la configuración de discos de espacios de almacenamiento (una función de Windows 8.1) tampoco se admite en esta versión. En la actualidad, solamente se admiten la restauración completa y la BMR dado que existe una limitación de controlador con ReFS, por lo que la restauración se implementa en modo de usuario, exportación de máquina virtual, etc. Si un Core está protegiendo al menos un volumen agente con el sistema de archivos ReFS, debería instalarse en un equipo bajo Windows 8, Windows 8.1, Windows Server 2012 o Windows Server 2012 R2, ya que estos sistemas operativos proporcionan compatibilidad nativa con ReFS. Si no es así, las funciones estarán limitadas y las operaciones de tipo montaje de una imagen de volumen no funcionarán. LaRapid Recovery Core Console presenta mensajes de error correspondientes en estos casos.

Solamente los sistemas operativos Linux compatibles están disponibles para su protección o recuperación. Se trata de los sistemas Ubuntu, Red Hat Enterprise Linux, CentOS y SUSE Linux Enterprise Server (SLES). Para obtener más detalles, consulte la *Guía de instalación y actualización de Rapid Recovery*.

Es posible realizar una BMR para máquinas físicas o virtuales. Como ventaja añadida, Rapid Recovery le permite realizar una restauración BMR independientemente de si el hardware es igual o distinto. Una restauración BMR en Rapid Recovery separa el sistema operativo de una plataforma específica, lo que ofrece portabilidad.

Ejemplos de la realización de una BMR para hardware similar incluyen la sustitución del disco duro del sistema existente o el intercambio del servidor con errores por un equipo idéntica.

Ejemplos de la realización de una BMR para hardware diferente incluyen la restauración de un sistema con errores con un servidor producido por un fabricante diferente o con una configuración diferente. Este proceso engloba crear una imagen de CD de inicio, grabar la imagen en el disco, iniciar el servidor de destino desde

la imagen de inicio, conectar con la instancia de la consola de recuperación, asignar volúmenes, iniciar la recuperación y, a continuación, supervisar el proceso. Cuando la restauración Bare Metal Restore finalice, puede continuar la tarea de carga del sistema operativo y las aplicaciones de software en el servidor restaurado, para luego establecer ajustes exclusivos necesarios para su configuración.

La restauración Bare Metal Restore no solamente se utiliza en casos de recuperación de desastres, sino también para migrar datos al actualizar o sustituir servidores.

Restauración de equipos virtuales

Si bien bare metal restore (BMR) es compatible con las máquinas virtuales (VM), hay que mencionar que es más fácil realizar una exportación virtual para una máquina virtual que realizar una BMR en un equipo físico. Para obtener más información sobre cómo realizar una exportación de máquina virtual, consulte Exportación a máquinas virtuales con Rapid Recovery.

Para realizar una BMR en un equipo con Windows, consulte el tema específico de Windows, incluidos los requisitos previos. Para obtener más información, consulte Realización de una restauración Bare Metal Restore para equipos con Windows.

También puede realizar una BMR desde el Asistente para restaurar un equipo. Para ello, empiece por el procedimiento Acerca de la restauración de volúmenes desde un punto de recuperación y, cuando se le indique en dicho procedimiento, pase a Realización de una restauración Bare Metal Restore para equipos con Windows.

Para realizar una BMR en un equipo Linux, consulte Realización de una restauración Bare Metal Restore para Linux. Además de realizar una BMR mediante la utilidad local_mount de la línea de comandos, ahora puede realizar una BMR desde dentro de la IU de la Core Console. Las directrices tiene en cuenta ambos enfoques.

Realización de una restauración Bare Metal Restore para equipos con Windows

Para realizar una restauración Bare Metal Restore para máquinas con Windows, realice las tareas siguientes.

- Creación de una imagen de inicio de Windows. Esta imagen ISO del CD de inicio se utilizará para arrancar la unidad de destino, desde la que puede acceder a la Universal Recovery Console para comunicarse con copias de seguridad del Core. Consulte Descripción de la creación del CD de inicio para equipos Windows.
  - Si necesita soportes físicos para iniciar el equipo de destino, debe transferir la imagen ISO del CD de inicio a un soporte. Consulte Transferencia de la imagen ISO del CD de inicio a soportes.
  - En cualquier caso, debe cargar la imagen de inicio en el servidor de destino e iniciar el servidor desde la imagen de inicio. Consulte Carga del CD de inicio e inicio del equipo de destino.

    NOTE: Este proceso describe el método para administrar una imagen de CD de inicio desde el cuadro de diálogo Crear CD de inicio. También puede realizar estos pasos desde el Asistente para restaurar un equipo, empezando desde la página CD de inicio del asistente. Puede acceder a esta acción cuando especifica Recupere en cualquier máquina de destino usando un CD de inicio desde la página Destino del asistente.
- Inicie una restauración Bare Metal Restore para Windows. Una vez se haya iniciado el equipo de destino desde el CD de inicio, puede iniciar la restauración BMR. Consulte Uso de la Universal Recovery Console para una BMR. Conlleva las siguientes tareas:
  - Iniciar una restauración desde un punto de recuperación del Core. Consulte Selección de un punto de recuperación e inicio de la BMR.
  - Asigne los volúmenes. Consulte Acerca de asignar discos para una restauración Bare Metal Restore.
  - Si está restaurando en hardware diferente y los controladores de almacenamiento y red necesarios no están presentes en el CD de inicio, puede que deba cargar los controladores desde un dispositivo

de soporte portátil. Para obtener más información, consulte Carga de controladores mediante la Universal Recovery Console.

- Realización de una BMR desde el Asistente para restaurar un equipo. Es posible realizar opcionalmente los procesos para administrar una imagen de inicio de Windows y para iniciar la BMR, incluyendo todas las subtareas, desde el Asistente para restaurar un equipo. Para obtener información sobre el inicio del asistente, consulte los pasos del 1 al 5 de Acerca de la restauración de volúmenes desde un punto de recuperación.
- Verifique una restauración Bare Metal Restore. Tras iniciar la restauración Bare Metal Restore, podrá verificar y supervisar su progreso. Consulte Comprobación de una restauración Bare Metal Restore.
  - Puede supervisar el progreso de su restauración. Consulte Visualización del progreso de recuperación.
  - Una vez completada, podrá iniciar el servidor restaurado. Consulte Inicio de un servidor de destino restaurado
  - Solucione los problemas del proceso de BMR. Consulte Solución de problemas de conexiones con la Universal Recovery Console y Reparación de problemas de inicio.

Requisitos previos para realizar una restauración Bare Metal Restore para un equipo con Windows

Antes de que pueda empezar el proceso de realizar una restauración Bare Metal Restore para un equipo con Windows, deberá asegurarse de que se cumplen las condiciones y criterios siguientes:

- Una unidad central de procesamiento (CPU) de 64 bits. El CD de inicio de Rapid Recovery contiene el sistema operativo Win PE 5.1. Las restauraciones BMR de Rapid Recovery no son compatibles con CPU basadas en x86. Solo se pueden realizar restauraciones BMR en CPU de 64 bits.

  NOTE: Se trata de un nuevo requisito a partir de la versión 6.0 .

- Copias de seguridad del equipo que quiere restaurar. Debe tener un Rapid Recovery Core en funcionamiento que contenga puntos de recuperación del servidor protegido que quiera restaurar.
- Hardware que se va a restaurar (nuevo o antiguo, similar o diferente). El equipo de destino debe cumplir los requisitos de instalación para un Agent. Para obtener información detallada, consulte la Guía de instalación y actualización de Rapid Recovery.
- Soportes y software de imagen. Debe tener un CD o DVD en blanco y software de grabación de discos, o bien software para crear una imagen ISO. Si gestiona máquinas remotamente mediante un software de Virtual Network Computing, como UltraVNC, deberá tener VNC Viewer.
- Controladores de almacenamiento y controladores de adaptador de red compatibles. Si restaura en hardware diferente, debe tener controladores de almacenamiento y controladores de adaptador de red compatibles para el equipo de destino, incluidos controladores RAID, AHCI y de chipset, según sea adecuado.
- Espacio de almacenamiento y particiones, según sea adecuado. Asegúrese de que hay suficiente espacio en el disco duro para crear particiones de destino en el equipo de destino para que contenga los volúmenes de origen. Cualquier partición de destino debería ser como mínimo igual de grande que la partición de origen original.
- Particiones compatibles. Los sistemas operativos Windows 8, Windows 8.1, Windows 10, Windows Server 2012 y Windows Server 2012 R2 que se inicien desde particiones de EFI FAT32 están disponibles para su protección o recuperación, así como volúmenes de Resilient File System (ReFS). Las particiones de UEFI se tratan como volúmenes FAT32 sencillos. Las transferencias incrementales tienen una compatibilidad y una protección completas. Rapid Recovery es compatible con sistemas UEFI para BMR, incluida la partición automática de discos GPT.

Restauración Bare Metal Restore con el Asistente para restaurar un equipo

Puede utilizar el asistente de restauración para crear un CD de inicio y para realizar una restauración Bare Metal Restore (BMR).

Antes de realizar una BMR, consulte Requisitos previos para realizar una restauración Bare Metal Restore para un equipo con Windows o Requisitos previos para realizar una restauración Bare Metal Restore para un equipo Linux, según proceda. Si está iniciando su BMR en un equipo con Windows desde la Core Console, consulte Realización de una restauración Bare Metal Restore para equipos con Windows.

El equipo protegido debe tener el software agente instalado y puntos de recuperación desde los que realizar la operación de restauración.

La administración de una imagen de inicio de Windows mediante el asistente conlleva las siguientes acciones:

- Iniciar la creación del CD de inicio.
- Definir la ruta de acceso para la imagen en el equipo Core.
- Seleccionar el entorno de recuperación adecuado para el hardware en el que se desea restaurar.
- Opcionalmente, definir parámetros de conexión del agente restaurado para usar la red o UltraVNC.
- Opcionalmente, insertar controladores para el hardware en el que se desea restaurar.
- Opcionalmente, transferir la imagen de inicio a medios físicos.
- Iniciar el equipo en el que se desean restaurar los datos del CD.
- Conectar con la Consola de recuperación universal.
- Asignar volúmenes.
- Iniciar la restauración Bare Metal Restore desde el punto de recuperación seleccionado en el Core.

> **NOTE:** Este proceso describe cómo administrar una imagen de CD de inicio desde el Asistente para restaurar un equipo, como parte del proceso de realización de una BMR empleando ese asistente. También puede administrar una imagen de inicio desde el cuadro de diálogo Crear CD de inicio. Para obtener información sobre la administración de una imagen de CD de inicio fuera del Asistente para restaurar un equipo, consulte Descripción de la creación del CD de inicio para equipos Windows.

1. Para restaurar un volumen en un equipo protegido, desplácese hasta la Core Console y haga clic en **Restaurar** en la barra de botones de Rapid Recovery.

   Aparecerá el Asistente para restaurar un equipo.
2. En la página Equipos, seleccione el equipo protegido que desea restaurar y, a continuación, haga clic en **Siguiente**.

Aparecerá la página Puntos de recuperación.

3. Seleccione el punto de recuperación que desea utilizar para restaurar el equipo.
   - Opcionalmente, si desea limitar el número de puntos de recuperación que se muestra, puede filtrar por volúmenes (si está definido) o por fecha de creación del punto de recuperación. También puede buscar un punto de recuperación concreto.
4. Haga clic en **Siguiente**.
5. En la página Destino, seleccione **Recuperar en cualquier equipo de destino mediante un CD de inicio**.
   - Si todavía no ha cargado un CD de inicio en el equipo que desea restaurar, haga clic en **Siguiente** y, a continuación, continúe con el paso 6.
   - Si ya ha cargado un CD de inicio en el equipo de destino de la BMR, seleccione **Ya tengo un CD de inicio ejecutándose en el equipo de destino**, haga clic en **Siguiente** y, a continuación, vaya al paso 16.
6. En la página CD de inicio, en el cuadro Ruta de salida, escriba la ruta de acceso en la que debe almacenarse la imagen ISO del CD de inicio.

   NOTE: Si en la unidad compartida en la que desea almacenar la imagen hay poco espacio, puede crear un disco en la ruta de acceso según sea necesario, por ejemplo, F:\filename.iso.

   NOTE: La extensión del archivo debe ser .iso. Cuando especifique la ruta de acceso, utilice solamente caracteres alfanuméricos, el guión, la barra diagonal inversa (solamente como delimitador de ruta de acceso) y el punto (solamente para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
7. Opcionalmente, para configurar parámetros de red para el equipo de destino o agregar capacidades de UltraVNC, seleccione **Mostrar opciones avanzadas** y realice las siguientes acciones:
   - Para establecer una conexión de red con el destino de la BMR, seleccione **Utilizar la siguiente dirección IP** y, a continuación, especifique la información que se describe en la tabla siguiente.

Tabla 142. Opciones de Conexión de red

Opción	Descripción
Dirección IP	Dirección IP del equipo restaurado.
Máscara de subred	Máscara de subred del equipo restaurado.
Puerta de enlace predeterminada	Especifique la puerta de enlace predeterminada para el equipo restaurado.
Servidor DNS	Especifique el servidor de nombre de dominio para el equipo restaurado.

   - Si tiene una cuenta UltraVNC y desea usarla para llevar a cabo la BMR, seleccione **Agregar UltraVNC** y, a continuación, especifique la información que se describe en la tabla siguiente.

Tabla 143. Credenciales de conexión de UltraVNC

Opción	Descripción
Contraseña	Contraseña de su cuenta UltraVNC.

Opción	Descripción
Puerto	Puerto que desea usar para conectarse al destino de la BMR. El puerto predeterminado es 5900.

8. Haga clic en **Siguiente**.
9.
   - Para establecer una conexión de red para el equipo restaurado, seleccione **Utilizar la dirección IP siguiente** como se describe en la tabla siguiente.
   - Para definir la información de UltraVNC, seleccione **Agregar UltraVNC** como se describe en la tabla siguiente.

     Utilice esta opción si requiere un acceso remoto en la consola de recuperación. No puede iniciar sesión mediante Microsoft Terminal Services mientras utilice el CD de inicio.

Tabla 144. Conexión UltraVNC

Opción	Descripción
Contraseña	Especifique una contraseña para esta conexión de UltraVNC.
Puerto	Especifique un puerto para esta conexión de UltraVNC. El puerto predeterminado es 5900.

10. Cuando esté satisfecho con sus selecciones en la página CD de inicio, haga clic en **Siguiente**.
11. Opcionalmente, en la página Inyección de controlador, si tiene pensado restaurar en hardware distinto, inserte los controladores de almacenamiento y demás controladores necesarios para el sistema de destino mediante los siguientes pasos:
    a. Descargue los controladores desde el sitio web del fabricante del servidor y descomprímalos.
    b. Comprima cada controlador en un archivo .zip mediante una utilidad de compresión adecuada (por ejemplo, WinZip).
    c. En la página Inyección de controlador del Asistente para restaurar un equipo, haga clic en **Agregar un archivo comprimido de controladores**.
    d. Desplácese por el sistema de archivos hasta el archivo del controlador comprimido, selecciónelo y, a continuación, haga clic en **Abrir**.
    e. Repita los pasos c y d, como corresponda, hasta que haya insertado todos los controladores necesarios.

    Para obtener más información acerca de la inserción de controladores, consulte Descripción de la inyección de controladores en un CD de inicio

    NOTE: No todas las versiones de Windows admiten la inyección automática de controladores. Si el sistema operativo no la admite, guarde los controladores de forma manual en `C:\Program Files\AppRecovery\Core\BootCdKit\Drivers\`.

    Rapid Recovery crea la imagen ISO del CD de inicio.
12. Haga clic en **Siguiente**.
13. Inicie el equipo de destino de la BMR y, a continuación, realice una de las acciones siguientes:
    - Si puede iniciar el equipo de destino desde la imagen ISO del CD de inicio, hágalo ahora.
    - Si no puede hacerlo, copie la imagen ISO en un soporte físico (un CD o DVD), introduzca el disco en el equipo de destino, configure el equipo para que se inicie desde el CD de inicio y reinícielo desde el CD.

      NOTE: Puede que tenga que cambiar la configuración de BIOS del equipo de destino para asegurarse de que el volumen que se carga primero es el CD de inicio.

El equipo de destino, cuando se inicia desde el CD de inicio, 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 el Rapid Recovery Core. Anote la dirección IP y las credenciales de clave de autenticación de la URC, que se actualizan cada vez que inicia desde el CD de inicio.

14. En la página Conexión del Asistente para restaurar un equipo, en la Core Console, introduzca la información de autenticación de la instancia de la URC del equipo que quiera restaurar, de la manera siguiente:

Tabla 145. Opciones de autenticación

Opción	Descripción
Dirección IP	Dirección IP que se proporciona en la URC en la máquina de destino.
Clave de autenticación	Clave de autenticación que se proporciona en la URC en la máquina de destino.

15. Haga clic en **Siguiente**.
16. En la página Asignación de discos, si desea asignar volúmenes manualmente, vaya al paso 10. Si desea asignar volúmenes automáticamente, realice los pasos siguientes:
    a. En el menú desplegable Asignación de volúmenes, seleccione **Automático**.
    b. En la lista de volúmenes, asegúrese de que los volúmenes que desea restaurar están seleccionados. Todos los volúmenes están seleccionados de forma predeterminada.

    Si no desea restaurar un volumen de la lista, desactive la opción.

    NOTE: Se debe seleccionar al menos un volumen para realizar la restauración.

    c. En el lado derecho, seleccione el disco de destino para la restauración.
    d. Haga clic en **Siguiente**.
    e. En la página Vista previa de asignación de discos, revise los parámetros de las acciones de restauración que seleccionó.
    f. Vaya al paso 18.
17. Para asignar volúmenes manualmente, en la página Asignación de discos, realice los pasos siguientes:
    a. En el menú desplegable Asignación de volúmenes, seleccione **Manual**.
    b. En la columna Destino, seleccione un volumen de destino que desea restaurar. Opcionalmente, si no desea restaurar un volumen enumerado, cancele la selección de la opción.

    NOTE: Se debe seleccionar al menos un volumen para realizar la restauración.

18. Haga clic en **Finalizar**.

    CAUTION: Todas las particiones y los datos de la unidad de destino se eliminarán de manera permanente, y se reemplazarán por el contenido del punto de recuperación seleccionado, incluidos el sistema operativo y todos los datos.

19. Si los volúmenes que quiere restaurar contienen bases de datos de Oracle, SQL Server o Microsoft Exchange y si está realizando una restauración en vivo, en la página Desmontar bases de datos, se le pedirá que las desmonte. Opcionalmente, si desea volver a montar estas bases de datos después de que la restauración se haya completado, seleccione **Volver a montar todas las bases de datos automáticamente después de que se haya restaurado el punto de recuperación**.
20. Haga clic en **Restaurar**.
21. En el mensaje de estado, haga clic en **Aceptar** para confirmar que el proceso de restauración ha empezado.

    Comienza la restauración. Puede ver el progreso en la página Eventos. Para obtener más información, consulte Visualización de eventos mediante las páginas de tareas, alertas y del diario.

Descripción de la creación del CD de inicio para equipos Windows

Una restauración Bare Metal Restore para Windows requiere una imagen de inicio denominada CD de inicio, que se crea definiendo parámetros en el Rapid Recovery Core. Esta imagen está adaptada a sus necesidades específicas. Utilizará la imagen para iniciar el equipo con Windows de destino. Basándose en las características específicas de su entorno, puede que necesite transferir esta imagen a un soporte físico, como un CD o DVD. A continuación, deberá cargar virtual o físicamente la imagen de inicio e iniciar el servidor Windows desde la imagen de inicio.

El primer paso al realizar una restauración Bare Metal Restore (BMR) para un equipo Windows es crear el archivo del CD de inicio en la Rapid Recovery Core Console. Se trata de una imagen ISO de inicio que contiene la interfaz de Universal Recovery Console (URC) de Rapid Recovery, un entorno que se utiliza para restaurar la unidad del sistema o todo el servidor directamente desde el Rapid Recovery Core.

La imagen ISO del CD de inicio que cree está personalizada para la máquina que se restaura; por lo tanto, debe contener los controladores correctos de red y almacenamiento masivo. Si anticipa que va a restaurar en hardware diferente del del equipo en el que se originó el punto de recuperación, deberá incluir una controladora de almacenamiento y otros controladores en el CD de inicio. Para obtener información sobre cómo insertar esos controladores en el CD de inicio, consulte Descripción de la inyección de controladores en un CD de inicio.

Descripción de la inyección de controladores en un CD de inicio

La imagen del CD de inicio requiere que los controladores de almacenamiento reconozcan las unidades del servidor y los controladores de adaptador de red para comunicarse con Rapid Recovery Core a través de la red.

Un conjunto genérico de controladores de controlador de almacenamiento y adaptador de red de Windows 8.1 x64 se incluye automáticamente al generar un CD de inicio para Windows. Esto satisface los requisitos de los sistemas más recientes. Los sistemas de otros fabricantes o sistemas más antiguos pueden requerir que inserte controladores de controladora de almacenamiento o adaptador de red al crear el CD de inicio. Si detecta que el CD de inicio que creó no contiene los controladores necesarios para realizar la restauración, también puede cargar controladores en el equipo de destino mediante la URC. Para obtener más información, consulte Carga de controladores mediante la Universal Recovery Console.

Cuando se está creando el CD de inicio, la inyección de controlador se utiliza para facilitar la interoperabilidad entre la consola de recuperación, el adaptador de red y el almacenamiento en el servidor de destino.

Los datos restaurados desde el punto de recuperación incluyen controladores para el hardware ya existente. Si está realizando una restauración Bare Metal Restore en hardware diferente, también debe insertar controladores de controladora de almacenamiento en el sistema operativo que se está restaurando mediante la URC después de que se hayan restaurado los datos en la unidad. Esto permite que el sistema operativo restaurado se inicie mediante el nuevo conjunto de hardware. Después de que el sistema operativo se inicie tras la restauración, podrá descargar e instalar los controladores adicionales que necesite el sistema operativo para interactuar con su nuevo hardware.

Creación de una imagen ISO de un CD de inicio

CD de inicio es el término que Rapid Recovery utiliza para referirse a la ubicación de almacenamiento portátil de la imagen ISO reservada para realizar una restauración Bare Metal Restore (BMR). La imagen incluye la Universal Recovery Console (URC) de Rapid Recovery.

Para realizar una restauración BMR en un equipo, debe iniciar el equipo desde el CD de inicio, lo que abre la consola. La consola es lo que permite conectar el destino de la restauración BMR en la ubicación del punto de recuperación que desea utilizar para llevar a cabo la restauración.

1. Desde la Rapid Recovery Core Console en la que está protegido el servidor que va a restaurar, en la barra de iconos, haga clic en el menú (Más) y, a continuación, haga clic en **CD de inicio**.
2. En la página de CD de inicio, haga clic en **CD de inicio**.

   Se abrirá el cuadro de diálogo Crear CD de inicio.
3. En el cuadro de diálogo Crear CD de inicio, en el cuadro de texto **Ruta de salida**, introduzca la ruta de acceso en la que quiera almacenar la imagen ISO del CD de inicio.

   NOTE: La extensión del archivo debe ser .iso. Cuando especifique la ruta de acceso, utilice solamente caracteres alfanuméricos, el guión, la barra diagonal inversa (solamente como delimitador de ruta de acceso) y el punto (solamente para separar nombres de host y dominios). En las letras de la a la z no se distingue entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
4. En Opciones de conexión, realice una de las acciones siguientes:
   - Para obtener la dirección IP dinámicamente mediante el protocolo Dynamic Host Configuration Protocol (DHCP), seleccione **Obtener dirección IP automáticamente**.
   - Para especificar una dirección IP estática para la URC, seleccione **Utilizar la siguiente dirección IP** y, a continuación, especifique la siguiente información:
     - Dirección IP
     - Máscara de subred
     - Puerta de enlace predeterminada
     - Servidor DNS

   NOTE: Debe especificar estos cuatro campos.
5. Si necesita acceso remoto a la consola de recuperación y tiene UltraVNC instalado, en Opciones de UltraVNC, realice los pasos siguientes:

   NOTE: UltraVNC permite administrar la URC de forma remota mientras está en uso. No puede iniciar sesión mediante Microsoft Terminal Services mientras utilice el CD de inicio.

   a. Seleccione **Agregar UltraVNC**.
   b. Introduzca su **Contraseña de UltraVNC**.
   c. Introduzca el **Puerto de UltraVNC**. El puerto predeterminado es 5900.

   NOTE: Las opciones de UltraVNC solo están disponibles si ya tiene UltraVNC instalado. Para hacer que estas opciones estén disponibles, vaya a http://www.uvnc.com/downloads/ultravnc/ para descargar UltraVNC versión 1.0.9.1 o posterior para arquitectura x64. Realice la instalación y guarde el archivo winvnc.exe en C:\Program Files\AppRecovery\Core\BootCdKit\UltraVnc_x64\.
6. Si tiene pensado restaurar en hardware distinto, insertar los controladores de almacenamiento y demás controladores necesarios para el sistema de destino mediante los siguientes pasos:

   NOTE: No todas las versiones de Windows admiten la inyección automática de controladores. Si el sistema operativo no la admite, guarde los controladores de forma manual en C:\Program Files \AppRecovery\Core\BootCdKit\Drivers\.

   a. Descargue los controladores desde el sitio web del fabricante del servidor y descomprímalos.
   b. Comprima cada controlador en un archivo .zip mediante una utilidad de compresión adecuada (por ejemplo, WinZip).
   c. En el cuadro de diálogo Crear CD de inicio, en el panel Controladores, haga clic en **Agregar un archivo comprimido de controladores**.

d. Desplácese por el sistema de archivos hasta el archivo del controlador comprimido, selecciónelo y, a continuación, haga clic en **Abrir**.

El archivo de controlador aparece en el panel Controladores del cuadro de diálogo Crear CD de arranque.

e. Repita los pasos c y d, como corresponda, hasta que haya agregado todos los controladores necesarios.

f. En el panel Controladores, seleccione los controladores que quiere insertar.

Para obtener más información acerca de la inserción de controladores, consulte Descripción de la inyección de controladores en un CD de inicio

7. Haga clic en **Crear CD de arranque**.

   Rapid Recovery crea el CD de inicio y lo guarda con el nombre de archivo que se ha proporcionado.

8. Para supervisar el progreso de esta tarea, vaya a la barra de iconos y haga clic en el icono de eventos.

   Para obtener más información sobre cómo supervisar eventos de Rapid Recovery, consulte Visualización de eventos mediante las páginas de tareas, alertas y del diario.

   Cuando termina la creación de la imagen ISO, aparece un registro de la imagen en la página de CD de inicio, a la que puede tener acceso desde el menú Más de la barra de iconos.

Para acceder a la imagen ISO, vaya a la ruta de salida que ha especificado, o bien haga clic en el enlace de la página de CD de inicio para descargar la imagen en una ubicación desde la que pueda cargarla en el nuevo sistema, por ejemplo, una unidad de red.

Transferencia de la imagen ISO del CD de inicio a soportes

Cuando cree el archivo del CD de inicio, se almacenará como imagen ISO en la ruta de acceso que especificó. Debe poder montar esta imagen como unidad en el servidor en el que esté realizando una restauración Bare Metal Restore.

Puede grabar la imagen ISO del CD de inicio en un disco compacto (CD) o disco de vídeo digital (DVD) accesible desde el arranque del sistema.

Cuando inicie la máquina desde el CD de inicio, la Universal Recovery Console se iniciará automáticamente.

Si realiza una BMR en una máquina virtual, este paso no es obligatorio. Sencillamente cargue la imagen ISO en una unidad y edite la configuración de esa máquina virtual para que se inicie desde esa unidad.

Carga del CD de inicio e inicio del equipo de destino

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

Para conectarse a la Rapid Recovery Core Console o usar Chromium para descargar controladores adicionales, primero debe cargar una controladora Ethernet y un adaptador de red. Para obtener más información, consulte Carga de controladores mediante la Universal Recovery Console.

NOTE: Si ha creado el CD de inicio con DHCP, tendrá que capturar la dirección IP y la contraseña.

1. En el nuevo servidor, cargue la imagen del CD de inicio desde la ubicación adecuada y, a continuación, inicie el servidor desde la imagen del CD de inicio para cargar el software Rapid Recovery Agent y Win PE 5.1.

El equipo de destino muestra una pantalla azul de Quest con tres botones de icono en la parte superior de la pantalla.

2. Para abrir la interfaz de usuario de la Universal Recovery Console (URC) de Rapid Recovery, haga clic en el icono de Quest en la parte superior de la pantalla.

   La dirección IP y la contraseña del equipo aparecen bajo autenticación.

   NOTE: Se generará una nueva contraseña temporal cada vez que la máquina se inicie con el CD de inicio. Anote la dirección IP que aparece en el panel Configuración de adaptadores de red y la contraseña de autenticación que aparece en el panel Autenticación. Necesitará esta información posteriormente, durante el proceso de recuperación de datos para volver a iniciar sesión en la consola.

   NOTE: Si no se ha proporcionado ninguna dirección IP, cargue la controladora Ethernet y el adaptador de red.

3. Si desea cambiar la dirección IP, selecciónela y haga clic en **Cambiar**.

   NOTE: Si especificó una dirección IP en el cuadro de diálogo Crear CD de inicio, la Universal Recovery Console la utiliza y la muestra en la pantalla Configuración de adaptadores de red.

El sistema está preparado para que pueda conectarse al Core, seleccionar un punto de recuperación, y continuar con el proceso de restauración bare metal restore.

Uso de la Universal Recovery Console para una BMR

Antes de iniciar una restauración Bare Metal Restore (BMR) para un equipo con Windows, es preciso que se den las siguientes condiciones:

- Para restaurar un punto de recuperación guardado en el Core, debe contar ya con el hardware adecuado. Para obtener más información, consulte Requisitos previos para realizar una restauración Bare Metal Restore para un equipo con Windows.
- El equipo con Windows de destino para la BMR debe iniciarse mediante la imagen del CD de inicio. Para obtener más información, consulte Descripción de la creación del CD de inicio para equipos Windows.

Una restauración Bare Metal Restore BMR inicia un equipo mediante un punto de recuperación seleccionado. El punto de recuperación incluye controladores del hardware anterior. Si está realizando una restauración en hardware diferente, debe insertar controladores de controlador de almacenamiento en el sistema operativo que se está restaurando mediante la URC después de que se hayan restaurado los datos en la unidad. Esto permite que el sistema operativo restaurado se inicie mediante el nuevo conjunto de hardware. Después de que se inicie el sistema operativo, puede descargar e instalar los controladores adicionales que necesita el sistema operativo para interactuar con el nuevo hardware.

Para iniciar una BMR desde la Rapid Recovery Core Console, realice las tareas siguientes.

- Selección de un punto de recuperación e inicio de la BMR
- Acerca de asignar discos para una restauración Bare Metal Restore
- Carga de controladores mediante la Universal Recovery Console

Este proceso es un paso en Realización de una restauración Bare Metal Restore para equipos con Windows.

Acerca de las herramientas de Universal Recovery Console

Universal Recovery Console (URC) incluye el acceso a las herramientas que pueden ayudarle a completar una restauración Bare Metal Restore (BMR).

Puede encontrar las siguientes herramientas haciendo clic en el icono central de la parte superior de la pantalla de presentación de Quest en un destino de BMR que se inicia en la URC.

- **Far Manager.** Esta herramienta es similar al Explorador de Windows. Proporciona una forma de navegar por los archivos del servidor hasta que haya finalizado la BMR e instalado un sistema operativo con su propia función de navegación, como el Explorador de Windows.
- **Chromium.** Este explorador de código abierto le permite acceder a Internet en un servidor que tenga una controladora de red cargada a través de la URC.
- **PuTTY.** Esta herramienta es un emulador de terminal de código abierto. En el contexto de una Rapid Recovery BMR, le permite conectarse a un dispositivo de almacenamiento NAS que no incluya una interfaz de usuario. Esta capacidad es posible que sea necesaria si desea realizar una restauración a partir de un archivo y el archivo se encuentra en un NAS.
- **Notepad.** Como en el sistema operativo Windows, esta herramienta le permite escribir notas sin formato y visualizar archivos de registro.
- **Administrador de tareas.** Como en el sistema operativo Windows, esta herramienta le permite administrar los procesos y supervisar el rendimiento del servidor mientras la restauración está en curso.
- **Editor de registros.** Como en el sistema operativo Windows, esta herramienta le permite cambiar el registro del sistema del destino de BMR.
- **Símbolo del sistema.** Esta herramienta le permite ejecutar comandos en el destino de BMR fuera de la URC hasta que instale una interfaz de usuario.

Carga de controladores mediante la Universal Recovery Console

Esta función le permite agregar los controladores que no se incluyeron en la imagen ISO pero que son necesarios para una restauración Bare Metal Restore correcta.

Esta tarea es un paso en Realización de una restauración Bare Metal Restore para equipos con Windows. Forma parte del proceso para Uso de la Universal Recovery Console para una BMR.

Al crear un CD de inicio, puede agregar los controladores necesarios a la imagen ISO. Después de iniciar el equipo de destino, también puede cargar controladores de almacenamiento o red desde la Universal Recovery Console (URC).

Si está restaurando en hardware diferente, debe insertar controladores de controlador de almacenamiento, RAID, AHCI, de chipset y de otro tipo si no están ya en el CD de inicio. Estos controladores permiten que el sistema operativo haga que todos los dispositivos funcionen correctamente en el servidor de destino una vez que haya reiniciado el sistema tras el proceso de restauración.

Realice los pasos del procedimiento siguiente para cargar controladores mediante la URC.

- Carga de controladores en la Consola de recuperación universal mediante multimedia portátiles
- Cómo cargar una controladora en la URC con Chromium

Carga de controladores en la Consola de recuperación universal mediante multimedia portátiles

Este procedimiento tiene los siguientes requisitos previos.

- Creación de una imagen ISO de un CD de inicio
- Transferencia de la imagen ISO del CD de inicio a soportes
- Carga del CD de inicio e inicio del equipo de destino

Lleve a cabo el siguiente procedimiento para utilizar un dispositivo multimedia portátil para cargar controladores en la Consola de recuperación universal (URC).

1. En un equipo con conexión a Internet, descargue los controladores del sitio web del fabricante para el servidor y descomprímalos.
2. Comprima cada controlador en un archivo .zip mediante una utilidad de compresión adecuada (por ejemplo, WinZip).
3. Copie y guarde el archivo .zip de controladores en un dispositivo multimedia portátil, por ejemplo, una unidad USB.
4. Quite el soporte del equipo conectado e insértelo en el servidor de destino de inicio.
5. En el servidor de destino, cargue el CD de inicio e inicie el equipo.

   Aparece la pantalla de presentación de Quest.
6. Para iniciar la URC, haga clic en el **icono de Quest**.

   La URC se abre en la pestaña del administrador de controladores de CD de inicio.
7. Expanda la lista **Otros dispositivos**.

   La lista muestra los controladores necesarios para el hardware pero no están en el CD de inicio
8. Haga clic con el botón derecho en un controlador de la lista y, a continuación, haga clic en **Cargar controlador**.
9. En la ventana Seleccionar modo de carga del controlador, seleccione una de las siguientes opciones:
   - Cargar paquete de único controlador (el controlador se cargará sin verificación para la compatibilidad de dispositivos)
   - Buscar paquetes de controlador en la carpeta (se buscarán controladores para el dispositivo seleccionado en la carpeta seleccionada)
10. Expanda la unidad del dispositivo multimedia portátil, seleccione el controlador (con la extensión de archivo .inf) y, a continuación, haga clic en **Aceptar**.

    El controlador se carga en el sistema operativo actual.
11. En la ventana Información, haga clic en **Aceptar** para confirmar que el controlador se ha cargado correctamente.
12. Repita esta acción las veces que sea necesario para cada controlador que desee cargar.

Cómo cargar una controladora en la URC con Chromium

Este procedimiento tiene los siguientes requisitos previos.

- Creación de una imagen ISO de un CD de inicio
- Transferencia de la imagen ISO del CD de inicio a soportes
- Carga del CD de inicio e inicio del equipo de destino

Lleve a cabo el siguiente procedimiento para utilizar el explorador Chromium que viene instalado en el CD de inicio para cargar controladoras mientras está en la URC.

1. En el servidor de destino, cargue el CD de inicio e inicie el equipo.

   Aparece la pantalla de presentación de Quest.
2. Para iniciar la URC, haga clic en el **icono de Quest**.

   La URC se abre en la pestaña del administrador de controladores de CD de inicio.
3. En el destino de BMR, haga clic en las herramientas (icono central) en la parte superior de la pantalla y, a continuación, haga clic en **Chromium**.
4. En el explorador Chromium, vaya a un sitio web donde pueda descargar los controladores necesarios.
5. Descargue el controlador o controladores en la ubicación que desee, como una carpeta local o un recurso compartido de archivo de red.
6. Expanda la lista **Otros dispositivos**.

   La lista muestra los controladores necesarios para el hardware pero no están en el CD de inicio
7. Haga clic con el botón derecho en un controlador de la lista y, a continuación, haga clic en **Cargar controlador**.
8. En la ventana Seleccionar modo de carga del controlador, seleccione una de las siguientes opciones:
   - Cargar paquete de único controlador (el controlador se carga sin verificación para la compatibilidad de dispositivos)
   - Buscar paquetes de controlador en la carpeta (se buscan controladores para el dispositivo seleccionado en la carpeta seleccionada)
9. Navegue a la ubicación en la que guardó el controlador, seleccione el controlador y, a continuación, haga clic en **Aceptar**.

   El controlador se carga en el sistema operativo actual.
10. En la ventana Información, haga clic en **Aceptar** para confirmar que el controlador se ha cargado correctamente.
11. Repita esta acción las veces que sea necesario para cada controlador que desee cargar.

Selección de un punto de recuperación e inicio de la BMR

Una vez que se puede acceder a la Universal Recovery Console en el equipo de destino de restauración Bare Metal Restore (BMR), debe seleccionar el punto de recuperación que desea restaurar.

Desplácese hasta la Core Console para seleccionar qué punto de recuperación quiere cargar y, a continuación, designe la consola de recuperación como el destino para los datos restaurados.

NOTE: Este paso es obligatorio para realizar una BMR en todos los equipos con Windows y opcional para realizar una BMR en las máquinas con Linux.

Esta tarea es un paso en Realización de una restauración Bare Metal Restore para equipos con Windows. Forma parte del proceso para Uso de la Universal Recovery Console para una BMR.

Si está realizando una BMR para un equipo con Linux desde la Core Console, esta tarea también es un paso de Realización de una restauración Bare Metal Restore para Linux. Forma parte del proceso de Inicio de una restauración Bare Metal Restore para un equipo Linux mediante la línea de comandos.

1. En la Rapid Recovery Core Console, en la lista de equipos protegidos, haga clic en el nombre del equipo protegido que desee restaurar.

Aparecerá la página Resumen del equipo seleccionado.

2. Haga clic en **Puntos de recuperación**.
3. Haga clic en el menú desplegable que hay junto al punto de recuperación que desea utilizar para BMR y, a continuación, haga clic en **Restaurar**.

   Aparecerá el Asistente para restaurar un equipo.
4. Seleccione **Recuperar en cualquier equipo de destino mediante un CD de inicio**.
5. Seleccione **Ya tengo un CD de inicio ejecutándose en el equipo de destino**.

   Los campos de texto de autenticación aparecen.
6. Introduzca la información sobre el equipo que quiera restaurar según se describe en la tabla siguiente.

Tabla 146. Información del equipo de destino

Cuadro de texto	Descripción
Dirección IP	Dirección IP del equipo que desea restaurar. Esta es idéntica a la dirección IP mostrada en la URC.
Clave de autenticación	Contraseña específica con la que conectarse al servidor seleccionado. Esta es idéntica a la clave de autenticación mostrada en la URC.

7. Haga clic en **Siguiente**.

   Si la información de conexión que introdujo coincide con la URC y si el Core y el servidor de destino pueden identificarse entre sí adecuadamente en la red, se cargarán los volúmenes para el punto de recuperación seleccionado y aparecerá la página Asignación de discos. En este caso, el siguiente paso es asignar volúmenes.
8. Continúe con Acerca de asignar discos para una restauración Bare Metal Restore para obtener más información acerca de las opciones de asignación de disco.

Acerca de asignar discos para una restauración Bare Metal Restore

Una vez conectado a la Universal Recovery Console, debe asignar volúmenes entre los indicados en el punto de recuperación y los volúmenes existentes en el hardware de destino.

Rapid Recovery trata de asignar volúmenes automáticamente. Si acepta la asignación predeterminada, el disco del equipo de destino se borrará y volverá a particionar, y todos los datos ya existentes se eliminarán. La alineación se realizará en el orden en que se enumeran los volúmenes en el punto de recuperación y los volúmenes se asignarán a los discos adecuadamente según su tamaño, etc. Suponiendo que haya suficiente espacio en la unidad de destino, no se necesitará ninguna partición al utilizar la alineación de discos automática. Recuerde que un disco se puede utilizar en varios volúmenes. Si asigna manualmente las unidades, recuerde que no puede utilizar el mismo disco dos veces.

Para la asignación manual, el nuevo equipo debe estar formateado correctamente antes de restaurarlo. El equipo de destino debe tener una partición separada para cada volumen en el punto de recuperación, incluido el volumen reservado para el sistema. Para obtener más información, consulte Uso de la Universal Recovery Console para una BMR.

Realice el procedimiento para una de las siguientes opciones de asignación de disco:

- Asignar discos virtuales a una restauración BMR automáticamente
- Asignar discos virtuales a una restauración BMR manualmente

CAUTION: Si bien Rapid Recovery admite particiones FAT32 y ReFS, en la actualidad solo se admiten las restauraciones completa y BMR, dado que existe una limitación de controlador con ReFS, por lo que la restauración se implementa en modo de usuario, exportación de máquina virtual, etc. Si un Core está protegiendo al menos un volumen agente con el sistema de archivos ReFS, debería instalarse en equipos con Windows 8.1, Windows 10 (solo Enterprise o Pro), Windows Server 2012, Windows Server 2012 R2 o Windows Server 2016, ya que proporcionan compatibilidad nativa con ReFS. Si no es así, las funciones están limitadas y las operaciones de tipo montaje de una imagen de volumen no funcionan. La Rapid Recovery **Core Console presenta los mensajes de error pertinentes en estas apariciones.**

CAUTION: La restauración Bare Metal Restore de la configuración de discos de espacios de almacenamiento tampoco se admite. Para obtener información detallada, consulte la *Guía de instalación y actualización de Rapid Recovery*

Esta tarea es un paso en Realización de una restauración Bare Metal Restore para equipos con Windows. Forma parte del proceso para Uso de la Universal Recovery Console para una BMR.

Si está realizando una BMR para un equipo con Linux desde la Core Console, esta tarea también es un paso de Realización de una restauración Bare Metal Restore para Linux. Forma parte del proceso para Inicio de una restauración Bare Metal Restore para Linux.

Asignar discos virtuales a una restauración BMR automáticamente

Este procedimiento permite asignar automáticamente los discos durante una restauración bare metal restore (BMR) mediante el asistente Restore Wizard.

Realice los pasos del siguiente procedimiento para seleccionar automáticamente los volúmenes que desea recuperar y dónde restaurarlos.

1. En la página Asignación de discos del Asistente para restaurar un equipo, al lado de Asignación de volúmenes, seleccione **Automático** en el menú desplegable.
2. En la tabla de la izquierda, compruebe que los volúmenes adecuados se enumeran y están seleccionados.

   NOTE: Normalmente, en el caso de una BMR, debería restaurar como mínimo el volumen reservado para el sistema y el volumen del sistema (por lo general, pero no siempre, el volumen C:\). Debe seleccionar al menos un volumen para realizar una BMR.
3. En la tabla de la derecha, seleccione el disco o discos a los que desea asignar volúmenes en la máquina de destino.
4. Haga clic en **Siguiente**.
5. En la página Vista previa de asignación, revise la asignación de los volúmenes de punto de recuperación y el volumen de destino de la restauración.
6. Para comenzar la restauración, haga clic en **Finalizar**.

   CAUTION: Si selecciona Iniciar restauración, 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.

Asignar discos virtuales a una restauración BMR manualmente

Este procedimiento describe cómo designar qué discos deben almacenarse en qué ubicaciones del equipo restaurado.

Para asignar discos manualmente, primero debe usar DiskPart en la línea de comandos en el equipo de destino de la restauración BMR para crear volúmenes de destino y aplicarles formato. Para obtener más información,

consulte la información sobre opciones de línea de comandos de DiskPart (Standard 7 SP1) en Microsoft Developer Network.

Realice los pasos del siguiente procedimiento para seleccionar manualmente los volúmenes que desea recuperar y dónde restaurarlos.

1. En la página Asignación de discos del Asistente para restaurar un equipo, al lado de Asignación de volúmenes, seleccione **Manual** en el menú desplegable.

   NOTE: Si no hay volúmenes en la unidad del equipo en el que está realizando una restauración Bare Metal Restore (BMR), no verá esta opción ni podrá asignar volúmenes manualmente.

2. En el área Asignación de volúmenes, bajo Volumen de origen, verifique que el volumen de origen esté seleccionado y que los volúmenes adecuados se enumeren debajo del mismo y estén seleccionados.
3. En Destino, desde el menú desplegable, seleccione el destino adecuado que sea el volumen de destino en el que realizar la restauración BMR del punto de recuperación seleccionado y, a continuación, haga clic en **Restaurar**.
4. En el cuadro de diálogo de confirmación, revise la asignación del origen del punto de recuperación y el volumen de destino para la restauración.
5. Para iniciar la restauración, haga clic en **Iniciar restauración**.

   CAUTION: Si selecciona Comenzar restauración, todas las particiones y los datos existentes de la unidad de destino se quitarán permanentemente y se sustituirán por el contenido del punto de recuperación seleccionado, incluido el sistema operativo y todos los datos.

Llevar a cabo una BMR a partir de un archivo

Rapid Recovery le permite restaurar un equipo desde cero mediante un punto de recuperación archivado.

Este procedimiento tiene los siguientes requisitos previos.

- Creación de una imagen ISO de un CD de inicio
- Carga del CD de inicio e inicio del equipo de destino

Desde la Universal Recovery Console (URC), se puede tener acceso a Rapid Recovery Core y recuperar un punto de recuperación para una restauración. También puede optar por restaurar su equipo sin sistema operativo desde un punto de recuperación almacenado en un archivo. La URC le permite llegar a este archivo si se encuentra en una unidad local, un recurso compartido de red o una cuenta en la nube.

1. En la URC, haga clic en la ficha **Restaurar a partir de archivo**.
2. En la lista desplegable **Tipo de ubicación**, seleccione la ubicación de su archivo. Puede seleccionar las opciones siguientes:
   - Local
   - Red
   - Nube
3. Introduzca las credenciales que se describen en la tabla siguiente según su selección de tipo de ubicación.

Tabla 147. Opciones de credenciales de tipo de ubicación

Tipo de ubicación	Opción	Descripción
Local	Ruta de acceso local	La ubicación actual del archivo.
Red	Ruta de red	La ubicación actual del archivo.
	Usuario	El nombre de usuario para el acceso de recurso compartido de red.

Tipo de ubicación	Opción	Descripción
	Contraseña	La contraseña para el acceso de recurso compartido de red.
Nube	Tipo de nube	El proveedor de su ubicación de almacenamiento de la nube. Seleccione una de las opciones siguientes: • Microsoft Azure • Amazon S3 • Nubes con tecnología OpenStack • Archivos de nube de Rackspace • Google Cloud

4. Si ha seleccionado un tipo de nube, complete las credenciales que pertenecen a su proveedor de nube.
   - Para Microsoft Azure, realice los pasos siguientes:
     1. Introduzca las siguientes credenciales:
        - Nombre de cuenta de almacenamiento
        - Clave de acceso
     2. Para el nombre del contenedor, de la lista desplegable, seleccione un contenedor.
     3. Para la ruta de acceso de la nube, de la lista desplegable, seleccione la ruta de acceso al archivo.
   - Para Amazon S3, lleve a cabo los siguientes pasos:
     1. Introduzca las siguientes credenciales:
        - Clave de acceso
        - Clave secreta
     2. Para el nombre del contenedor, de la lista desplegable, seleccione un contenedor.
     3. Para la ruta de acceso de la nube, de la lista desplegable, seleccione la ruta de acceso al archivo.
   - Para cuentas de archivos con tecnología OpenStack o Rackspace, realice los siguientes pasos:
     1. Introduzca la información siguiente:
        - Región
        - Usuario
     2. Seleccione una de las opciones siguientes:
        - Contraseña
        - Clave de API
     3. En el cuadro de texto, introduzca la información en función de su selección en el paso C.
     4. Introduzca la información siguiente:
        - Id. de inquilino
        - URL de autenticación
        - Nombre de contenedor
        - Ruta de la nube
   - Para las cuentas de Google Cloud, complete los siguientes pasos:
     1. Introduzca las siguientes credenciales:

- Archivo de certificado
- Clave privada

2. Introduzca la información siguiente:
   - ID de proyecto
   - Correo electrónico de la cuenta de servicio
3. En el campo Nombre del contenedor, de la lista desplegable, seleccione el contenedor adecuado.

   Para la ruta de acceso de la nube, de la lista desplegable, seleccione la ruta de acceso al archivo.

5. Haga clic en **Siguiente**.
6. En la página **Equipos**, seleccione el equipo protegido que desea restaurar y, a continuación, haga clic en **Siguiente**.
7. En la página **Equipos protegidos**, seleccione el punto de recuperación que desee utilizar para restaurar el equipo y, a continuación, haga clic en **Siguiente**.
8. En la página **Asignación**, seleccione una de las siguientes opciones y, a continuación, complete los pasos correspondientes:

   - En el menú desplegable **Asignación de volúmenes**, seleccione **Automático**.

     1. En la tabla de la izquierda, compruebe que los volúmenes adecuados se enumeran y están seleccionados.

        NOTE: Normalmente, en el caso de una BMR, debería restaurar como mínimo el volumen reservado para el sistema y el volumen del sistema (por lo general, pero no siempre, el volumen `C:\`). Debe seleccionar al menos un volumen para realizar una BMR.

     2. En la tabla de la derecha, seleccione el disco o discos a los que desea asignar volúmenes en la máquina de destino.

   - En el menú desplegable **Asignación de volúmenes**, seleccione **Manual**.

     NOTE: Para asignar discos manualmente, primero debe usar DiskPart en la línea de comandos para crear y dar formato a los volúmenes de destino. Para obtener más información, consulte la información sobre opciones de línea de comandos de DiskPart (Standard 7 SP1) en Microsoft Developer Network.

     NOTE: Si no hay volúmenes en la unidad del equipo en el que está realizando una restauración Bare Metal Restore (BMR), no verá esta opción ni podrá asignar volúmenes manualmente.

     - En **Volúmenes de destino**, en el menú desplegable, seleccione el volumen de destino adecuado para cada volumen en el punto de recuperación.

9. En el cuadro de texto **ruta de acceso para las asignaciones de montaje**, introduzca un destino para el almacenamiento temporal de los archivos de asignación.

   La ubicación predeterminada es `X:\ProgramData\AppRecovery\IndexEntriesMaps`.

   NOTE: Para asegurarse de que el destino tiene suficiente espacio libre, divida la capacidad de volumen de montaje total por 1,024. Por ejemplo, mediante la fórmula `(Mount volume total capacity) / 1024 = Free space` y, a continuación, `1 TB / 1024 = 1 GB`.

10. Haga clic en **Restaurar**.

    La URC asigna los volúmenes al nuevo disco o discos.

11. Haga clic en **Restaurar**.

    La URC restaura los datos en el equipo de destino. Puede ver el progreso en la ficha **Restaurar progreso**.

12. Una vez que se completa la restauración, extraiga el CD de inicio.
13. Para iniciar el equipo de destino BMR en Windows, reinicie el equipo.

Carga de controladores en el sistema operativo

Este procedimiento describe cómo cargar controladores en el sistema operativo en un destino de restauración Bare Metal Restore (BMR).

Para insertar controladores en el sistema operativo, ya ha realizado las tareas siguientes:

- Ha creado un CD de inicio mediante generador de CD de inicio en la Rapid Recovery Core Console. Para obtener más información, consulte Creación de una imagen ISO de un CD de inicio.
- Ha cargado el CD de inicio en destino de BMR. Para obtener más información, consulte Carga del CD de inicio e inicio del equipo de destino.
- Ha cargado los controladores necesarios para almacenamiento y redes. Para obtener más información, consulte Carga de controladores mediante la Universal Recovery Console.
- Ha realizado la restauración con el Asistente para restaurar un equipo de la Rapid Recovery Core Console o en un archivo comprimido desde la Universal Recovery Console (URC). Para obtener más información, consulteRestauración Bare Metal Restore con el Asistente para restaurar un equipo y Llevar a cabo una BMR a partir de un archivo.

Después de realizar una restauración, el proceso no está completo hasta que los controladores se insertan en el sistema operativo del destino de restauración Bare Metal Restore (BMR). Esta tarea es adicional a la carga de los controladores en la URC.

1. Después de hacer clic en Restaurar en el procedimiento BMR de su elección (consulte los requisitos previos), haga clic en la pestaña **Administrador de controladores de Windows existente**.
2. En el menú desplegable, seleccione un sistema operativo.

   La URC busca los controladores disponibles.
3. Para cargar más controladores, haga clic en **Forzar carga**.
4. Desplácese por el sistema de archivos hasta encontrar el archivo de controlador comprimido y, a continuación, selecciónelo.
5. Haga clic en **Aceptar**.

   La URC carga el controlador en el sistema operativo que seleccionó.
6. Repita los pasos 3 a 5 para cada controlador adicional que tenga que cargar.
7. Reinicie el equipo de BMR de destino.

   La restauración BMR ha finalizado. Si tiene un problema al reiniciar, consulte Reparación de problemas de inicio.

Realización de una restauración Bare Metal Restore para Linux

En Rapid Recovery puede realizar una restauración Bare Metal Restore (BMR) para un equipo con Linux, incluida una restauración del volumen del sistema. Las funciones de BMR son compatibles al utilizar la utilidad `local_mount` de la línea de comandos y desde dentro de la IU de la Core Console.

CAUTION: Rapid Recovery **es compatible con los tipos de partición ext2 solo si el kernel es 3.10 y superior. Si está usando un kernel anterior, convierta cualquier partición ext2 a ext3, ext4 o XFS antes de empezar a proteger y realizar copias de seguridad del equipo.**

CAUTION: Cuando inicia un equipo Linux restaurado por primera vez tras una BMR, Rapid Recovery **toma una imagen base del equipo restaurado. Dependiendo de la cantidad de datos del equipo, este proceso tarda más tiempo que al tomar una instantánea incremental. Para obtener más información sobre las imágenes base y las instantáneas incrementales, consulte Comprensión del calendario de programación de protección..**

Para realizar una restauración Bare Metal Restore para máquinas con Linux, realice las tareas siguientes.

- Gestione una imagen de inicio de Linux. Esta imagen ISO de inicio del Live DVD de Linux se utilizará para arrancar la unidad de destino, desde la que puede acceder a la Universal Recovery Console para comunicarse con copias de seguridad del Core. Consulte Administración de una imagen de inicio de Linux.
  - Para obtener la imagen de arranque de BMR, asegúrese de que la versión de LiveDVD coincide con la de su Core. Para obtener más información, consulte el tema Acerca de la imagen ISO de inicio para Linux y después Descarga de una imagen ISO de inicio para Linux.
  - Si necesita soportes físicos para arrancar el equipo con Linux de destino, deberá transferir la imagen ISO a un soporte. Consulte Almacenamiento de la imagen ISO del Live DVD en soportes.
  - En cualquier caso, deberá cargar la imagen de inicio en el servidor de destino e iniciar el servidor desde la imagen de inicio. Consulte Carga del Live DVD e inicio del equipo de destino.
  - Después de cargar el soporte, debe conectar el equipo Linux a Rapid Recovery Core. Consulte Conexión al destino de la restauración BMR desde el Rapid Recovery Core.
- Gestione particiones. Puede que deba crear o montar particiones antes de realizar una BMR en un equipo con Linux. Consulte Administración de particiones de Linux.
  - El sistema Linux en el que esté realizando una BMR debe tener las mismas particiones que los volúmenes de origen del punto de recuperación. Puede que necesite crear particiones adicionales en el sistema de destino, si es necesario. Consulte Creación de particiones en la unidad de destino.
  - Si está realizando una BMR manual, primero deberá montar particiones. Consulte Montaje de particiones desde la línea de comandos. Los pasos para montar particiones se incluyen en el proceso para realizar una BMR desde la línea de comandos. Consulte Inicio de una restauración Bare Metal Restore para un equipo Linux mediante la línea de comandos.

    Si está utilizando la partición automática de BMR en la Core Console, no tiene que montar particiones.Rapid Recovery restaurará las mismas particiones que las que se incluyen en los puntos de recuperación que se están restaurando.
- Inicie una restauración Bare Metal Restore para Linux. Una vez se haya iniciado el equipo de destino desde la imagen de inicio del Live DVD, podrá iniciar la BMR. Las tareas obligatorias dependen de si va a realizar esto desde la interfaz de usuario de Rapid Recovery o desde la línea de comandos mediante la utilidad local_mount. Consulte Inicio de una restauración Bare Metal Restore para Linux.
  - Si va a utilizar la Core Console, deberá iniciar una restauración desde un punto de recuperación del Core. Consulte Selección de un punto de recuperación e inicio de la BMR.
  - Si va a utilizar la Core Console, deberá asignar los volúmenes desde la IU. Consulte Acerca de asignar discos para una restauración Bare Metal Restore.
  - Opcionalmente, si realiza una restauración desde la línea de comandos, podrá usar la utilidad Pantalla para mejorar su capacidad de desplazarse y ver los comandos en la consola terminal. Esta

utilidad se abre de manera predeterminada. Si la cierra, puede iniciarla de nuevo. Para obtener más información, consulte Inicio de la utilidad Pantalla.

- Si va a utilizar local_mount, todas las tareas se realizarán en la línea de comandos. Para obtener más información, consulte Inicio de una restauración Bare Metal Restore para un equipo Linux mediante la línea de comandos.

- Verifique una restauración Bare Metal Restore. Tras iniciar la restauración Bare Metal Restore, podrá verificar y supervisar su progreso. Consulte Verificación de la restauración Bare Metal Restore desde la línea de comandos.
  - Puede supervisar el progreso de su restauración. Consulte Visualización del progreso de recuperación.
  - Una vez completada, podrá iniciar el servidor restaurado. Consulte Inicio de un servidor de destino restaurado.
  - Solucione los problemas del proceso de BMR. Consulte Solución de problemas de conexiones con la Universal Recovery Console y Reparación de problemas de inicio.

Requisitos previos para realizar una restauración Bare Metal Restore para un equipo Linux

Antes de que pueda empezar el proceso de realizar una restauración Bare Metal Restore para un equipo con Linux, deberá asegurarse de que se cumplen las condiciones y criterios siguientes:

- Copias de seguridad del equipo que quiere restaurar. Debe tener un Rapid Recovery Core en funcionamiento que contenga puntos de recuperación del servidor protegido que quiera restaurar.
- Hardware que se va a restaurar (nuevo o antiguo, similar o diferente). El equipo de destino debe cumplir los requisitos de instalación para un Agent. Para obtener información detallada, consulte la *Guía de instalación y actualización de Rapid Recovery*.
- Imagen de inicio del Live DVD. Obtenga la imagen ISO del Live DVD de Linux, que incluye una versión de inicio de Linux. Descárguela desde el Portal de licencias de Rapid Recovery enhttps://licenseportal.com. Si tiene algún problema al descargar el Live DVD, póngase en contacto con Asistencia para la protección de datos de Quest.
- Soportes y software de imagen. Si está utilizando soportes físicos, debe tener un CD o DVD en blanco y software de grabación de discos, o bien software para crear una imagen ISO.
- Controladores de almacenamiento y controladores de adaptador de red compatibles. Si restaura hardware diferente, debe tener controladores de almacenamiento y controladores de adaptador de red compatibles para el equipo de destino, incluidos controladores RAID, AHCI y de chipset para el sistema operativo de destino, según sea adecuado.
- Espacio de almacenamiento y particiones, según sea adecuado. Asegúrese de que hay suficiente espacio en el disco duro para crear particiones de destino en el equipo de destino para que contenga los volúmenes de origen. Cualquier partición de destino debería ser como mínimo igual de grande que la partición de origen original.
- Restaure la ruta de acceso. Identifique la ruta de acceso para la restauración, que es la ruta de acceso del descriptor del archivo del dispositivo. Para identificar la ruta de acceso del descriptor del archivo del dispositivo, utilice el comando `fdisk` desde una ventana del terminal.

Administración de una imagen de inicio de Linux

Una restauración Bare Metal Restore para Linux requiere una imagen de arranque del Live DVD, que puede descargar desde el Portal de licencias de Rapid Recovery. Utilizará la imagen para iniciar el equipo Linux de destino. Basándose en las características específicas de su entorno, puede que necesite transferir esta imagen a un soporte físico, como un CD o DVD. A continuación, deberá cargar virtual o físicamente la imagen de inicio e iniciar el servidor Linux desde la imagen de arranque.

NOTE: Anteriormente, el Live DVD se conocía como el Live CD.

La gestión de una imagen de inicio de Linux es un paso en Realización de una restauración Bare Metal Restore para Linux.

Puede realizar las siguientes tareas:

- Acerca de la imagen ISO de inicio para Linux
- Almacenamiento de la imagen ISO del Live DVD en soportes
- Carga del Live DVD e inicio del equipo de destino
- Conexión al destino de la restauración BMR desde el Rapid Recovery Core

Acerca de la imagen ISO de inicio para Linux

El primer paso al realizar una restauración Bare Metal Restore (BMR) para un equipo con Linux es descargar la imagen ISO del Live DVD de Linux desde el Portal de licencias de Rapid Recovery. El Live DVD funciona con todos los sistemas de archivos de Linux admitidos por Rapid Recovery e incluye una versión de arranque de Linux, la utilidad de pantalla y la interfaz de Universal Recovery Console (URC) de Rapid Recovery. La Universal Recovery Console de Rapid Recovery es un entorno que se utiliza para restaurar la unidad del sistema o todo el servidor directamente desde el Rapid Recovery Core.

NOTE: International Organization for Standardization (ISO) (Organización internacional de normalización) es un organismo internacional de representantes de diversas organizaciones nacionales que establecen los estándares del sistema de archivos. ISO 9660 es un sistema de archivos estándar que se utiliza para soportes de disco óptico para el intercambio de datos y que admite diversos sistemas operativos. Una imagen ISO es un archivo de archivado o imagen de disco que contiene datos por cada sector del disco, así como el sistema de archivos del disco.

Descarga de una imagen ISO de inicio para Linux

Para completar una restauración Bare Metal Restore de un equipo Linux, necesita una imagen ISO del Live DVD que coincida con su versión de Rapid Recovery. La versión actual de Live DVD está disponible en elPortal de licencias de Rapid Recovery en https://licenseportal.com. Si necesita una versión diferente, póngase en contacto con el Asistencia para la protección de datos de Quest.

NOTE: Para obtener más información acerca del Portal de licencias de Rapid Recovery, consulte la *Rapid Recovery License Portal User Guide (Guía del usuario del Portal de licencias de Rapid Recovery).*

Esta tarea es un paso en Realización de una restauración Bare Metal Restore para Linux. Forma parte del proceso para Administración de una imagen de inicio de Linux.

Para descargar la imagen ISO del Live DVD, complete los pasos de este procedimiento.

1. Inicie sesión en el Portal de licencias de Rapid Recovery en https://licenseportal.com.
2. En el menú de navegación izquierdo, haga clic en **Descargas**.

Se muestra la página **Descargas**.

3. Desplácese hasta Aplicaciones basadas en Linux y, desde la sección Live DVD de Linux, haga clic en **Descargar**.
4. Guarde la imagen ISO del Live DVD.

   NOTE: Cuando restaure una máquina virtual, guarde la imagen en una ubicación de la red y, a continuación, configure la VM para que se inicie desde una unidad de CD o DVD asociada con la imagen.

5. Si está realizando una restauración desde un equipo físico, grabe la imagen ISO del CD de inicio en un disco compacto (CD) o disco de vídeo digital (DVD) desde el que pueda iniciarse el equipo de destino. Para obtener más información, consulte Almacenamiento de la imagen ISO del Live DVD en soportes.

Almacenamiento de la imagen ISO del Live DVD en soportes

Cuando descarga el archivo del Live DVD de Linux, se almacena como una imagen ISO en la ruta que especificó. Debe poder iniciar el equipo con Linux de destino desde la imagen del Live DVD.

Esta tarea es un paso en Realización de una restauración Bare Metal Restore para Linux. Forma parte del proceso para Administración de una imagen de inicio de Linux.

1. Grabe la imagen ISO del CD de inicio en un disco compacto (CD) o disco de vídeo digital (DVD).

   Si realiza una BMR en una máquina virtual, este paso no es obligatorio. Solo cargue la imagen ISO en una unidad y edite la configuración del equipo de esa máquina virtual para que se inicie desde esa unidad. También puede utilizar la exportación virtual para restaurar una máquina virtual Linux. Para obtener más información, consulte Exportación de la MV.

Carga del Live DVD e inicio del equipo de destino

Después de obtener la imagen ISO del Live DVD, deberá iniciar el equipo con Linux desde el Live DVD recién creado.

Esta tarea es un paso en Realización de una restauración Bare Metal Restore para Linux. Forma parte del proceso para Administración de una imagen de inicio de Linux.

1. Desplácese hasta el nuevo servidor y cargue la imagen del Live DVD desde la ubicación adecuada. Especifique que el servidor se iniciará desde la imagen del Live DVD.
2. Inicie el equipo.

   Aparecerá una pantalla emergente de Rapid Recovery y se abrirá una ventana de terminal, que muestra la dirección IP y una contraseña de autenticación para el equipo.

   NOTE: Se generará una nueva contraseña temporal cada vez que el equipo se inicie con la imagen del Live DVD.

3. Anote la dirección IP y la contraseña de autenticación que aparecen en la pantalla de introducción. Necesitará esta información posteriormente, durante el proceso de recuperación de datos para volver a iniciar sesión en la consola.

Conexión al destino de la restauración BMR desde el Rapid Recovery Core

Una vez iniciado el equipo con Linux de destino con el Live DVD, este equipo está listo para que se conecte a él desde el Core e inicie el proceso de restauración Bare Metal Restore. Puede realizar este proceso utilizando cualquiera de estos dos métodos:

- Iniciando una restauración desde la Rapid Recovery Core Console. Para obtener más información, consulte Inicio de una restauración Bare Metal Restore para Linux.
- Iniciando una restauración desde la línea de comandos mediante la utilidad local_mount. Para obtener más información, consulte Inicio de una restauración Bare Metal Restore para un equipo Linux mediante la línea de comandos.

Administración de particiones de Linux

Al realizar una BMR, la unidad de destino en la que vaya a restaurar datos debe tener las mismas particiones que en el punto de recuperación que esté restaurando. Puede que necesite crear particiones para cumplir este requisito.

Puede iniciar la restauración desde la línea de comandos mediante la utilidad local_mount, o bien puede iniciar la restauración desde Rapid Recovery Core Console. Si restaura mediante la interfaz de usuario, primero deberá montar las particiones.

La gestión de particiones de Linux es un paso en Realización de una restauración Bare Metal Restore para Linux.

Puede realizar las siguientes tareas:

Tareas relacionadas

See also: Creación de particiones en la unidad de destino
See also: Formateo de particiones en la unidad de destino
See also: Montaje de particiones desde la línea de comandos

Creación de particiones en la unidad de destino

A menudo, al realizar una BMR, la unidad de destino es un nuevo volumen que puede estar compuesto por una única partición. La unidad del equipo de destino debe tener la misma tabla de partición que en el punto de recuperación, incluido el tamaño de los volúmenes. Si la unidad de destino no contiene las mismas particiones, deberá crearlas antes de realizar la restauración Bare Metal Restore. Utilice la utilidad fdisk para crear particiones en la unidad de destino iguales a las particiones de la unidad de origen.

CAUTION: El siguiente procedimiento es sólo un ejemplo. Los entornos del cliente son distintos. Debe cambiar los comandos que utiliza para que coincidan con las especificaciones de su entorno.

Esta tarea es un paso en Realización de una restauración Bare Metal Restore para Linux. Forma parte del proceso para Administración de particiones de Linux.

1. Opcionalmente, puede usar la utilidad Pantalla. Esta utilidad se inicia de manera predeterminada y permanece activa hasta que reinicia el equipo.

   NOTE: Si la cierra de forma explícita y desea volver a abrirla, consulte Inicio de la utilidad Pantalla.

2. Desde la línea de comandos, introduzca el siguiente comando y, a continuación, pulse **Intro** para cambiar los privilegios para ejecutar como administrador y, a continuación, enumere las particiones de disco existentes:

   ```
   sudo fdisk -l
   ```

   Aparecerá una lista de todos los volúmenes.

En este ejemplo se da por hecho que el volumen que quiere particionar es /dev/sda. Si su volumen es diferente (por ejemplo, en el caso de unidades anteriores, puede que vea /dev/hda), cambie los comandos de la manera correspondiente.

3. Para crear una nueva partición de inicio, introduzca el siguiente comando y, a continuación, pulse **Intro**:

   ```
   sudo fdisk /dev/sda
   ```

4. Para crear una nueva partición de inicio, introduzca el siguiente comando y, a continuación, pulse **Intro**:

   ```
   n
   ```

5. Para crear una nueva partición principal, introduzca el siguiente comando y, a continuación, pulse **Intro**:

   ```
   p
   ```

6. Para especificar el número de partición, introduzca el número de partición y, a continuación, pulse **Intro**. Por ejemplo, para especificar la partición 1, escriba 1 y, a continuación, pulse **Intro**.
7. Para utilizar el primer sector, 2048, pulse **Intro**.
8. Asigne una cantidad adecuada a la partición de inicio introduciendo el símbolo más y la cantidad de asignación y, a continuación, pulse **Intro**.

   Por ejemplo, para asignar 500 M para la partición de inicio, escriba lo siguiente y, a continuación, pulse **Intro**:

   ```
   +512000K
   ```

9. Para cambiar de un indicador de inicio a la partición de inicio (para que la partición sea de inicio), escriba el siguiente comando y, a continuación, pulse **Intro**:

   ```
   a
   ```

10. Para asignar un indicador de inicio a la partición adecuada, escriba el número de la partición y, a continuación, pulse **Intro**. Por ejemplo, para asignar un indicador de inicio a la partición 1, escriba 1 y, a continuación, pulse **Intro**.
11. Continúe realizando particiones en el disco duro según sea necesario.
12. Para guardar todos los cambios en la utilidad fdisk, escriba el siguiente comando y, a continuación, pulse **Intro**:

    w

Formateo de particiones en la unidad de destino

Después de crear particiones en un nuevo volumen en la unidad de destino para llevar a cabo la restauración bare metal restore, si no va a utilizar la partición automática, debe formatear las particiones antes de que se puedan montar. Si se da esta situación, siga este procedimiento para dar formato a particiones con formatos ext3, ext4 o XFS.

Para el resto de casos, no es necesario que formatee las particiones, tal y como se describe en este tema.

Esta tarea es un paso en Realización de una restauración Bare Metal Restore para Linux. Forma parte del proceso para Administración de particiones de Linux.

1. Opcionalmente, puede usar la utilidad Pantalla. Esta utilidad se inicia de manera predeterminada y permanece activa hasta que reinicia el equipo.

   NOTE: Si la cierra de forma explícita y desea volver a abrirla, consulte Inicio de la utilidad Pantalla.

2. Desde la línea de comandos, introduzca el siguiente comando y, a continuación, pulse **Intro** para cambiar los privilegios para ejecutar como administrador y, a continuación, enumere las particiones de disco existentes:

   ```
   sudo fdisk -l
   ```

   Aparecerá una lista de todos los volúmenes.

En este ejemplo, se da por hecho que la partición que quiere formatear es /dev/sda1. Si su volumen es diferente (por ejemplo, en el caso de unidades anteriores, puede que vea /dev/hda), cambie los comandos de la manera correspondiente.

3. Seleccione uno de los siguientes comandos en base al formato que desee usar para la partición de destino:

   - Para formatear una partición con formato ext3, introduzca el siguiente comando y, a continuación, pulse **Intro**:

     ```
     sudo mkfs.ext3 /dev/sda1
     ```

   - Para formatear una partición con formato ext4, introduzca el siguiente comando y, a continuación, pulse **Intro**:

     ```
     sudo mkfs.ext4 /dev/sda1
     ```

   - Para formatear una partición con formato XFS, introduzca el siguiente comando y, a continuación, pulse **Intro**:

     ```
     sudo mkfs.xfs /dev/sda1
     ```

     Se formateará la partición seleccionada con el formato elegido.

4. Si tiene que dar formato a otras particiones, repita este procedimiento.

Montaje de particiones desde la línea de comandos

Si está realizando una BMR mediante la Rapid Recovery Core Console, primero deberá montar las particiones adecuadas en el equipo de destino. Realice esta acción desde la línea de comandos de la Universal Recovery Console.

Esta tarea es un paso en Realización de una restauración Bare Metal Restore para Linux. Forma parte del proceso para Administración de particiones de Linux.

Realice los pasos de este procedimiento para montar particiones en el equipo con Linux antes de realizar una restauración.

1. Desde la línea de comandos, introduzca el siguiente comando y, a continuación, pulse **Intro** para cambiar los privilegios para ejecutar como administrador y, a continuación, enumere las particiones de disco existentes:

   ```
   sudo fdisk -l
   ```

   Aparecerá una lista de todos los volúmenes.

2. Dé formato a todas las particiones que necesite para realizar la BMR en el directorio de montaje. Estas deben coincidir con los volúmenes que hay en el punto de recuperación. Por ejemplo, si el volumen que quiere montar se denomina sda1 y el directorio de montaje, mnt, escriba el siguiente comando y, a continuación, pulse **Intro**:
3. Monte todas las particiones que necesite para realizar la BMR en el directorio de montaje. Estas deben coincidir con los volúmenes que hay en el punto de recuperación. Por ejemplo, si el volumen que quiere montar se denomina sda1 y el directorio de montaje, mnt, escriba el siguiente comando y, a continuación, pulse **Intro**:

   ```
   mount /dev/sda1 /mnt
   ```

4. Repita el Paso 3 según sea necesario hasta que haya montado todos los volúmenes requeridos.

   Una vez se hayan montado los volúmenes, podrá realizar una restauración en el equipo con Linux de destino desde la Rapid Recovery Core Console. Consulte Inicio de una restauración Bare Metal Restore para Linux.

Inicio de una restauración Bare Metal Restore para Linux

Antes de iniciar una restauración Bare Metal Restore (BMR) para un equipo con Linux, es preciso que se den las siguientes condiciones:

- Para restaurar un punto de recuperación guardado en el Core, debe contar ya con el hardware adecuado. Para obtener más información, consulte Requisitos previos para realizar una restauración Bare Metal Restore para un equipo Linux.
- El equipo con Linux de destino para la BMR debe iniciarse mediante la imagen de inicio del Live DVD. Para obtener más información, consulte Administración de una imagen de inicio de Linux.
- El número de volúmenes del equipo con Linux que va a restaurarse debe coincidir con el número de volúmenes del punto de recuperación. También debe decidir si va a restaurar desde la Rapid Recovery Core Console o desde la línea de comandos mediante local_mount. Para obtener más información, consulte Administración de particiones de Linux.
- Si va a restaurar desde la IU de la Core Console, el primer paso para iniciar una BMR es seleccionar el punto de recuperación adecuado y, a continuación, iniciar la restauración en el hardware especificando la dirección IP y la contraseña temporal que obtuvo de la Universal Recovery Console. A continuación, deberá asignar las unidades e iniciar la restauración.

Este proceso es un paso en Realización de una restauración Bare Metal Restore para Linux.

Para iniciar una BMR desde la Rapid Recovery Core Console, realice las tareas siguientes.

- Selección de un punto de recuperación e inicio de la BMR
- Acerca de asignar discos para una restauración Bare Metal Restore

Si está restaurando desde la línea de comandos mediante la utilidad local_mount, primero debe establecer los privilegios adecuados, montar volúmenes, ejecutar local_mount, obtener información sobre el Core de la lista de equipos, conectarse al Core, obtener una lista de puntos de recuperación, seleccionar el punto de recuperación que quiere revertir mediante una restauración Bare Metal Restore e iniciar la restauración.

Opcionalmente, puede que quiera iniciar la utilidad Pantalla.

Para iniciar una BMR desde la línea de comandos, realice las tareas siguientes.

- Inicio de la utilidad Pantalla
- Inicio de una restauración Bare Metal Restore para un equipo Linux mediante la línea de comandos

Inicio de la utilidad Pantalla

En el Live DVD se incluye Pantalla, una utilidad que está disponible cuando inicia desde el Live DVD en la Universal Recovery Console. Pantalla permite que los usuarios gestionen varios shells simultáneamente a través de una única sesión de shell seguro (SSH) o ventana de consola. Esto le permite realizar una tarea en una ventana de terminal (como verificar volúmenes montados) y, mientras se está ejecutando, abrir o cambiar a otra instancia de shell para realizar otra tarea (como ejecutar la utilidad local_mount).

La utilidad Pantalla también tiene su propio búfer de desplazamiento hacia atrás, que le permite desplazar la pantalla para ver mayores cantidades de datos, como una lista de puntos de recuperación.

NOTE: Esta utilidad se proporciona por comodidad; el uso de la utilidad Pantalla es opcional.

La utilidad Pantalla se inicia en el equipo iniciado con el Live DVD de forma predeterminada. Sin embargo, si ha cerrado esta aplicación, deberá iniciar la utilidad Pantalla desde el Live DVD mediante el procedimiento siguiente.

1. Si se inició el equipo desde el Live DVD, en la ventana de terminal introduzca screen y pulse **Intro**.

Se abrirá la utilidad Pantalla.

Inicio de una restauración Bare Metal Restore para un equipo Linux mediante la línea de comandos

Una vez que la imagen ISO del Live DVD sea accesible en el equipo en el que quiera realizar una BMR y el número y tamaño de los volúmenes coincidan entre el equipo de destino y el punto de recuperación en el que quiera realizar una restauración Bare Metal Restore, podrá iniciar una restauración desde la línea de comandos mediante la utilidad local_mount.

NOTE: Este componente anteriormente se denominaba `aamount`.

Si desea realizar una BMR mediante la IU de la Rapid Recovery Core Console, consulte Selección de un punto de recuperación e inicio de la BMR.

NOTE: Al realizar este procedimiento, no intente montar puntos de recuperación en la carpeta /tmp, que contiene los archivos de rapidrecovery-vdisk (anteriormente, aavdisk).

Esta tarea es un paso en Realización de una restauración Bare Metal Restore para Linux. Forma parte del proceso para Inicio de una restauración Bare Metal Restore para un equipo Linux mediante la línea de comandos.

Realice los pasos de este procedimiento para seleccionar un punto de recuperación en el Core para revertir al equipo de destino de BMR física o virtual.

1. Para ejecutar la utilidad local_mount de Rapid Recovery como raíz, escriba el siguiente comando y, a continuación, pulse **Intro**:

   ```
   sudo local_mount
   ```

2. Para enumerar los equipos protegidos, escriba el siguiente comando y, a continuación, pulse **Intro**

   ```
   lm
   ```

3. Cuando se le pida, introduzca la información de conexión para el Rapid Recovery Core como se describe en la tabla siguiente, pulsando **Intro** después de cada comando obligatorio:

Tabla 148. Información de conexión del Rapid Recovery Core

Cuadro de texto	Descripción	Obligatorio
Dirección IP o nombre de host del Rapid Recovery Core	Dirección IP o el nombre de host del Rapid Recovery Core.	Sí
Dominio	Dominio del Rapid Recovery Core. Esto es opcional.	No
Usuario	Nombre de usuario de un administrador en el Core.	Sí
Contraseña	Contraseña utilizada para conectar al usuario administrativo con el Core.	Sí

   Aparecerá una lista que muestra los equipos protegidos por este Rapid Recovery Core. Enumera los equipos encontrados por número de elemento de línea, el nombre mostrado del host o dirección IP y un número de ID del equipo.

4. Para enumerar los puntos de recuperación del equipo que quiere restaurar, escriba el comando de enumeración de puntos de recuperación mediante la sintaxis siguiente y, a continuación, pulse **Intro**:

   ```
   lr <número_de_elemento_de_línea_del_equipo>
   ```

NOTE: También puede introducir el número de ID del equipo en este comando en lugar del número de elemento de línea.

Aparecerá una lista con los puntos de recuperación base e incrementales de ese equipo. Esta lista incluye:

- Un número de elemento de línea
- Un sello de fecha y hora
- Una lista con letras de los volúmenes dentro del punto de recuperación
- La ubicación del volumen
- El tamaño del punto de recuperación
- Un número de ID del volumen que incluye un número de secuencia al final, que identifica el punto de recuperación

5. Para seleccionar el punto de recuperación para una restauración, introduzca el siguiente comando y, a continuación, pulse **Intro**:

   ```
   r <número_de_identificación_del_punto_de_recuperación> <ruta_de_acceso>
   ```

   CAUTION: Debe asegurarse de que el volumen del sistema no está montado.

   NOTE: Si inició el equipo desde el Live DVD, el volumen del sistema no está montado.

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

   NOTE: También puede especificar un número de línea en el comando en lugar del número de ID del punto de recuperación para identificar al punto de recuperación. En ese caso, utilice el número de línea del Agent o el equipo (desde la salida `lm`), seguido por el número de línea del punto de recuperación y la letra del volumen (de la lista con letras de los volúmenes dentro del punto de recuperación), seguido por la ruta de acceso. Por ejemplo:

   ```
   r <número_de_elemento_de_línea_del_equipo>
   <número_de_línea_del_punto_de_recuperación_de_la_imagen_de_base>
   <letra_del_volumen> <ruta_de_acceso>
   ```

   Por ejemplo, escriba: `r 1 24 a /dev/sda1`
   En este comando, `<ruta_de_acceso>` es el descriptor del archivo para el propio volumen.

6. Cuando se le pregunte si quiere continuar, introduzca s de Sí y, a continuación, pulse **Intro**.

   Después de que comience la restauración, aparecerá una serie de mensajes que le notificarán el estado de finalización de la restauración.

   NOTE: Si recibe un mensaje de excepción, la información detallada relativa a dicha excepción podrá encontrarse en el archivo local_mount.log. El archivo local_mount.log se encuentra en `/var/log/appassure`.

7. Tras una restauración correcta, salga de local_mount escribiendo `exit` y, a continuación, pulse **Intro**.
8. Su siguiente paso será verificar la restauración. Para obtener más información, consulte Verificación de la restauración Bare Metal Restore desde la línea de comandos.

Restauración de volúmenes para un equipo Linux mediante la línea de comandos

Antes de restaurar desde un punto de recuperación usando la línea de comandos, debe desmontar el disco en el que restaurará los datos.

En Rapid Recovery, puede restaurar volúmenes en sus equipos Linux protegidos mediante la utilidad de la línea de comandos `local_mount`.

NOTE: Este proceso se denominaba anteriormente una reversión. Al realizar este procedimiento, no intente montar puntos de recuperación en la carpeta /tmp, que contiene los archivos de rapidrecovery-vdisk (anteriormente, aavdisk). La restauración de volúmenes también es compatible para los equipos protegidos dentro de la Rapid Recovery Core Console. Consulte Acerca de la restauración de volúmenes desde un punto de recuperación para obtener más información.

CAUTION: Para restaurar el sistema o la partición raíz (/) o el sistema operativo completo, consulte Realización de una restauración Bare Metal Restore para Linux.

1. Ejecute la utilidad Rapid Recovery`local_mount` como raíz, por ejemplo:

   ```
   sudo local_mount
   ```

2. En la solicitud de montaje de Rapid Recovery, 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 del Rapid Recovery Core.
4. Introduzca las credenciales de inicio de sesión, es decir, el nombre de usuario y la contraseña, para este servidor.

   Aparecerá una lista que muestra los equipos protegidos por este servidor del Rapid Recovery Core. Enumera los equipos protegidos encontrados por número de elemento de línea, dirección IP/host y número de identificación del equipo (por ejemplo: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2).

5. Introduzca el siguiente comando para enumerar los puntos de recuperación montados actualmente para el equipo especificado:

   ```
   lr <número_de_elemento_de_línea_del_equipo>
   ```

   NOTE: Tenga en cuenta que también puede introducir el número de ID del equipo en este comando en lugar del número de elemento de línea.

   Aparecerá una lista que muestra los puntos de recuperación base e incrementales de ese equipo. Esta lista incluye un número de elemento de línea, fecha/marca de tiempo, ubicación del volumen, tamaño del punto de recuperación y número de ID del volumen que incluye un número secuencial al final (por ejemplo, "93cc667-44b4-48ab-91d8-44bc74252a4f:2"), que identifica al punto de recuperación.

6. Introduzca el siguiente comando para seleccionar un punto de recuperación para realizar la restauración:

   ```
   r <número_ID_punto_recuperación_volumen> <ruta de acceso de dispositivo>
   ```

   Este comando restaura la imagen del volumen especificada por la ID del Core a la ruta de acceso especificada. La ruta de acceso para la restauración es la ruta de acceso del descriptor del archivo del dispositivo y no es el directorio en el que está montado.

   - También puede especificar un número de línea en el comando en lugar del número de ID del punto de recuperación para identificar al punto de recuperación. En ese caso, utilizaría el número de línea del equipo protegido (desde la salida lm), seguido por el número de línea del punto de recuperación y la letra del volumen, seguido por la ruta de acceso, de este modo: r <número_de_elemento_de_línea_de_la_máquina> <número_de_línea_del_punto_de_recuperación> <letra_del_volumen> <ruta_de_acceso>. En este comando, <ruta_de_acceso> es el descriptor del archivo para el propio volumen.

Por ejemplo, si la salida de `lm` enumera tres equipos protegidos y especifica el comando `lr` para el equipo protegido número `2` y desea restaurar el punto de recuperación `23` volumen `b` en el volumen que estaba montado en el directorio `/dev/sda5`, el comando sería:
`r2 23 b /dev/sda5`

NOTE: Se puede restaurar en / si es necesario. Si realiza una restauración Bare Metal Restore mediante un Live DVD, se supone que desea restaurar en otro equipo. Para obtener más información, consulte Inicio de una restauración Bare Metal Restore para Linux.

7. Cuando se le pregunte si quiere continuar, introduzca `y` para Sí.

   Cuando continúe la restauración, aparecerá una serie de mensajes que le notificarán el estado.

8. Tras una restauración correcta, la utilidad `local_mount` montará y volverá a adjuntar automáticamente el módulo de kernel en el volumen restaurado si el destino se protegió y montó anteriormente. Si no es así, deberá montar el volumen restaurado en el disco local y, a continuación, debería verificar que los archivos se han restaurado (por ejemplo, puede utilizar el comando `sudo mount` y luego el comando `ls`).

Comprobación de una restauración Bare Metal Restore

Una vez que haya realizado una restauración Bare Metal Restore (BMR), puede comprobar el progreso de la restauración. Cuando la acción se haya realizado correctamente, podrá iniciar el servidor restaurado. Se incluyen algunos pasos de solución de problemas si encuentra dificultades al conectarse a la Universal Recovery Console para realizar la restauración y para reparar problemas de inicio con el equipo restaurado.

Puede realizar las siguientes tareas:

- Visualización del progreso de recuperación
- Inicio de un servidor de destino restaurado
- Solución de problemas de conexiones con la Universal Recovery Console
- Reparación de problemas de inicio

Visualización del progreso de recuperación

Realice los pasos de este procedimiento para ver el progreso de la restauración de los datos desde un punto de recuperación (incluida la restauración Bare Metal Restore) iniciado desde la Rapid Recovery Core Console.

1. Después de iniciar el proceso de restauración de datos desde un punto de recuperación, mientras la tarea está en curso, puede ver su progreso desde el menú desplegable  **Tareas en ejecución** en la Core Console.
2. Opcionalmente, puede ver información detallada en la página **Eventos**. Para obtener más información sobre la supervisión de eventos deRapid Recovery, consulte Visualización de eventos mediante las páginas de tareas, alertas y del diario.

Inicio de un servidor de destino restaurado

Realice los pasos de este procedimiento para iniciar el servidor de destino restaurado.

NOTE: Antes de iniciar el servidor de destino restaurado, debería verificar que la recuperación se haya realizado correctamente. Para obtener más información, consulte Visualización del progreso de recuperación.

Esta tarea es un paso en Realización de una restauración Bare Metal Restore para equipos con Windows. Forma parte del proceso para Comprobación de una restauración Bare Metal Restore.

1. En el servidor de destino, compruebe que la Rapid Recovery Universal Recovery Console está activa.
2. Expulse el CD de inicio (o desconecte el soporte físico con la imagen del CD de inicio) del servidor restaurado.
3. En la Universal Recovery Console, haga clic en el icono del menú de alimentación de la parte superior de la pantalla y, a continuación, haga clic en **Reiniciar**.
4. Especifique que el sistema operativo se inicie con normalidad.
5. Inicie la sesión en el equipo. El sistema debe restaurarse al estado capturado en el punto de recuperación.

Solución de problemas de conexiones con la Universal Recovery Console

A continuación se indican pasos de solución de problemas para conectarse a la imagen del CD de inicio como parte del proceso de Selección de un punto de recuperación e inicio de la BMR.

Si aparece un error que indique que el Core no se ha podido conectar al servidor remoto, es probable que la causa sea una de las distintas causas posibles.

- Verifique que la dirección IP y la contraseña actual que aparecen en la URC son idénticas a la información que introdujo en el cuadro de diálogo Instancia de la consola de recuperación.
- Para llegar al servidor en el que se restaurarán datos, el Core debe poder identificar al servidor en la red. Para determinar si la identificación del servidor es posible, puede abrir un símbolo del sistema en el Core y hacer ping en la dirección IP del servidor de BMR de destino. También puede abrir un símbolo del sistema en el servidor de destino y hacer ping en la dirección IP de Rapid Recovery Core.
- Verifique que la configuración del adaptador de red es compatible entre el Core y el servidor de BMR de destino.

Reparación de problemas de inicio

Este procedimiento tiene los siguientes requisitos previos.

- Creación de una imagen ISO de un CD de inicio
- Carga del CD de inicio e inicio del equipo de destino
- Carga de controladores mediante la Universal Recovery Console

Realice los pasos de este procedimiento para reparar problemas de arranque. Recuerde que si está restaurando en hardware diferente, debe insertar controladores de controladora de almacenamiento, RAID, AHCI, de chipset y de otro tipo si no están ya en el CD de inicio. Estos controladores permiten que el sistema operativo haga que todos los dispositivos funcionen correctamente en su servidor de destino. Para obtener más información, consulte Carga de controladores mediante la Universal Recovery Console. Realice el procedimiento siguiente para reparar problemas de arranque en su servidor de destino.

1. Desde la Universal Recovery Console, haga clic en la ficha **Administrador de controladores de Windows existente**.
2. Haga clic en **Reparar problemas de inicio**.

   Los parámetros de arranque del registro de inicio del servidor de destino se repararán automáticamente.

Verificación de la restauración Bare Metal Restore desde la línea de comandos

Quest recomienda realizar los siguientes pasos para verificar que una restauración Bare Metal Restore se ha realizado desde la línea de comandos.

Esta tarea es un paso en Realización de una restauración Bare Metal Restore para Linux.

- Realización de una comprobación del sistema de archivos en el volumen restaurado
- Uso de la línea de comandos para hacer que un equipo Linux pueda iniciarse

Realización de una comprobación del sistema de archivos en el volumen restaurado

Una vez que haya ejecutado una restauración Bare Metal Restore desde la línea de comandos, debería realizar una comprobación del sistema de archivos en el volumen restaurado para asegurarse de que los datos restaurados del punto de recuperación no están dañados.

Esta tarea es un paso en Realización de una restauración Bare Metal Restore para Linux. Forma parte del proceso para Verificación de la restauración Bare Metal Restore desde la línea de comandos.

Realice la tarea siguiente para realizar una comprobación del sistema de archivos en el volumen restaurado.

1. Desde la línea de comandos en la Universal Recovery Console del equipo con Linux que ha restaurado, para verificar si se han montado las particiones adecuadas, escriba el siguiente comando y, a continuación, pulse **Intro**:

   ```
   df
   ```

2. Si el volumen restaurado no está montado, vaya al Paso 3. Si el volumen restaurado está montado, desmóntelo escribiendo el siguiente comando y, a continuación, pulsando **Intro**:

   ```
   umount <punto de montaje>
   ```

3. Ejecute una comprobación del sistema de archivos en los volúmenes restaurados escribiendo el siguiente comando y, a continuación, pulse **Intro**:

   ```
   fsck -f <volumen>
   ```

   Si fsck devuelve un valor correcto, el sistema de archivos estará verificado.

4. Vuelva a montar los volúmenes adecuados escribiendo el siguiente comando con el formato `mount <volume> <folder>` y, a continuación, pulse **Intro**.

   Por ejemplo, si la ruta de acceso de los volúmenes es prod/sda1 y la carpeta en la que quiere montarlos es mnt, escriba lo siguiente y, a continuación, pulse **Intro**:

   ```
   mount /dev/sda1 /mnt
   ```

Uso de la línea de comandos para hacer que un equipo Linux pueda iniciarse

Una vez haya realizado una comprobación del sistema de archivos correcta en el volumen restaurado, deberá crear particiones de inicio.

GNU Grand Unified Bootloader (GRUB) es un cargador de inicio que permite que los administradores configuren qué sistema operativo o configuración de kernel específica se utiliza para iniciar el sistema. Después de una BMR, el archivo de configuración para GRUB debe modificarse para que el equipo utilice el identificador

universalmente único (UUID) adecuado para el volumen raíz. Antes de este paso, debe montar los volúmenes raíz y de inicio, así como comprobar los UUID de cada uno. Esto garantizará que pueda iniciar desde la partición.

NOTE: Este procedimiento se aplica a equipos Linux que utilizan GRUB1 o GRUB2. Cuando utilice este procedimiento, asegúrese de que la partición de inicio está en buen estado y protegida.

GRUB o GRUB2 normalmente se instala con los sistemas operativos Linux. Puede realizar este procedimiento utilizando la versión que viene con su distribución de Linux. Si una versión de GRUB no está instalada, tendrá que volver a instalar la versión predeterminada adecuada para su distribución de Linux.

CAUTION: Cuando inicia un equipo Linux restaurado por primera vez tras una BMR, Rapid Recovery **toma una imagen base del equipo restaurado. Dependiendo de la cantidad de datos del equipo, este proceso tarda más tiempo que al tomar una instantánea incremental. Para obtener más información sobre las imágenes base y las instantáneas incrementales, consulte Comprensión del calendario de programación de protección..**

Esta tarea es un paso en Realización de una restauración Bare Metal Restore para Linux. Forma parte del proceso para Verificación de la restauración Bare Metal Restore desde la línea de comandos.

Realice la tarea siguiente para crear particiones de inicio mediante la línea de comandos.

1. Primero deberá montar el volumen raíz y luego el volumen de inicio. Monte cada volumen restaurado utilizando el siguiente comando:
   a. Para montar el volumen raíz, escriba el siguiente comando y, a continuación, pulse **Intro**:
      `mount /<volumen restaurado[raíz]> /mnt`
      Por ejemplo, si /dev/sda2 es el volumen raíz, escriba mount /dev/sda2 /mnt y, a continuación, pulse **Intro**.
   b. Para montar el volumen de inicio, escriba el siguiente comando y, a continuación, pulse **Intro**:
      `mount /<volumen restaurado[arranque]> /mnt/boot`
      Por ejemplo, si /dev/sda1 es el volumen de arranque, escriba mount /dev/sda1 /mnt/boot y, a continuación, pulse **Intro**.

   NOTE: Algunas configuraciones del sistema pueden incluir el directorio de inicio como parte del volumen raíz.
2. Si el tamaño del volumen aumenta (es decir, si el volumen de destino en el nuevo equipo Linux es mayor que el volumen que tenía el punto de recuperación), deberá eliminar todos los archivos de datos de mapa de bits existentes.
3. Obtenga el identificador único universal (UUID) de los nuevos volúmenes utilizando el comando `blkid`. Escriba lo siguiente y, a continuación, pulse **Intro**:
   `blkid [volumen]`

   NOTE: También puede utilizar el comando `ls -l /dev/disk/by-uuid`.
4. Si realiza una BMR en un disco totalmente nuevo en el equipo de destino, comente la partición intercambiada en fstab en su volumen raíz.
5. La modificación de las rutas de acceso de fstab y mtab debería realizarse en el volumen restaurado, no en el Live DVD. No es necesario modificar rutas de acceso en el Live DVD. Prepárese para la instalación de Grand Unified Bootloader (GRUB) escribiendo los siguientes comandos. Después de cada comando, pulse **Intro**:
   ```
   mount --bind /dev /mnt/dev
   mount --bind /proc /mnt/proc
   mount --bind /sys /mnt/sys
   ```
6. Cambie el directorio raíz escribiendo el siguiente comando y, a continuación, pulsando **Intro**:
   `chroot /mnt /bin/bash`
7. Obtenga el UUID anterior de la partición o particiones del archivo `/etc/fstab` de los puntos de recuperación montados y compárelo con los UUID de las particiones raíz (para Ubuntu y CentOS), de arranque (para CentOS y RHEL) o de datos escribiendo el siguiente comando y, a continuación, pulsando **Intro**:

```
less /mnt/etc/fstab
```

8. Obtenga el UUID anterior de la partición o particiones del archivo `/etc/mtab` de los puntos de recuperación montados y compárelo con los UUID de las particiones raíz (para Ubuntu y CentOS), de arranque (para CentOS y RHEL) y de datos escribiendo el siguiente comando y, a continuación, pulsando **Intro**:

   ```
   less /mnt/etc/mtab
   ```

9. Si usa SLES 11, instale GRUB introduciendo los siguientes comandos, pulsando **Intro** en cada uno:

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

10. Si utiliza Ubuntu, CentOS 6.x, RHEL 6.x u Oracle Linux 6.x, instale GRUB; para ello, escriba el comando siguiente y, a continuación, pulse **Intro**:

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

11. Si utiliza SLES 12, CentOS 7, RHEL 7 u Oracle 7, instale GRUB2; para ello, escriba el comando siguiente y, a continuación, pulse **Intro**:

    ```
    grub2-install /dev/sda
    ```

12. Tras completar la instalación, ejecute una de las siguientes actualizaciones:

    - Para SLES:

      ```
      grub-install.unsupported --recheck /dev/sda
      grub-install.unsupported /dev/sda
      update-grub
      ```

      NOTE: Si no existe el comando `update-grub` en su distribución de Linux, omita esta opción.

    - Para otras distribuciones:

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

      NOTE: Si no existe el comando `update-grub` en su distribución de Linux, omita esta opción.

13. Quite el disco Live DVD de la unidad de CD-ROM o DVD y reinicie el equipo con Linux.

Administración de datos anteriores

En esta sección se describe cómo administrar los datos de las instantáneas de vencimientos guardados en su repositorio. Incluye información sobre la conservación de puntos de recuperación en su repositorio, las políticas de retención y el proceso resultado de consolidar puntos de recuperación para conservar espacio. Describe la capacidad de reubicar puntos de recuperación desde su repositorio a un servidor de desduplicación y de copia de seguridad de la serie DR de Quest.

En esta sección también se describe cómo administrar políticas de retención que controlan el consolidado y cómo forzar el consolidado a petición.

Retención de datos, niveles de almacenamiento secundario y archivado

Cada vez que su Core captura una instantánea, los datos se guardan como punto de recuperación en su repositorio. Los puntos de recuperación se van acumulando sistemáticamente a lo largo del tiempo. El Core utiliza una política de retención para determinar el tiempo durante el que se conservan los datos de instantáneas en el repositorio. Durante la ejecución de trabajos nocturnos (en particular, durante el proceso de consolidación), el Core aplica la política de retención para reducir la cantidad de espacio de almacenamiento consumido. Se compara la fecha de cada punto de recuperación con la fecha del punto de recuperación más reciente. A continuación, el Core consolida (combina) puntos de recuperación más antiguos. Con el tiempo, los puntos de recuperación más antiguos del repositorio se sustituyen de forma continua por los más recientes cuando los primeros llegan poco a poco a la mayor antigüedad definida en el periodo de retención.

A partir de la versión 6.1.1 de Rapid Recovery, también puede reubicar puntos de recuperación de su repositorio DVM principal en un repositorio por capas en una copia de seguridad DR de Quest y un dispositivo de desduplicación. Esto libera espacio de almacenamiento de su repositorio principal.

Para asociar puntos de recuperación con el almacenamiento secundario mediante este método, primero debe agregar el servidor DR como un repositorio en su Rapid Recovery Core. Para obtener más información acerca de cómo crear un nuevo repositorio por capas secundario en un DR, consulte Creación de un repositorio por capas.A continuación, en el nivel del equipo protegido, especifique en la directiva de retención la antigüedad a la que desea que se reubiquen los puntos de recuperación del repositorio principal al secundario. Para obtener más información, consulte Personalización de la configuración de la política de retención de un equipo protegido (especialmente los pasos 7 y 10).

NOTE: Independientemente de dónde se encuentran los puntos de recuperación (un repositorio DVM local principal o un repositorio por capas secundario en un servidor de copia de seguridad de DR), también están sujetos a la política de retención y, por lo tanto, se consolidarán. Si necesita conservar puntos de recuperación más antiguos, un método es archivarlos. El otro enfoque es desactivar la consolidación o extender el periodo de retención de los equipos protegidos correspondientes.

Para conservar puntos de recuperación que, de otro modo, se combinarían y, finalmente, eliminarían, puede crear un archivo comprimido desde Core Console. Un archivo comprimido es un archivo que contiene una copia del conjunto completo de puntos de recuperación de equipos protegidos en su Core en el punto temporal en el que se crearon. Más adelante, podrá acceder a la información archivada desde la Core Console. A diferencia de los puntos de recuperación del repositorio, los puntos de recuperación de archivos comprimidos no se consolidan.

Los archivos comprimidos son útiles para mantener los datos de cumplimiento; realizar copias de seguridad de su Core; inicializar datos de replicación en un Core de réplica remoto; y para ahorrar espacio en su Core para conservar las transacciones empresariales importantes manteniendo las copias de seguridad durante un periodo de tiempo mayor.

Para obtener más información sobre archivos, consulte Archivado.

Administración de políticas de retención

Una política de retención es un conjunto de reglas que determina el periodo de tiempo del que dispone el Core para retener los puntos de recuperación antes de consolidarlos. Las políticas de retención se pueden configurar para que se consoliden en base a horas, días, semanas, meses y años. Se pueden configurar hasta seis reglas (la política predeterminada establece cinco reglas).

Ya que puede realizar copias de seguridad con una frecuencia de 5 minutos (una vez cada hora para DL1000), la primera regla en la política de retención establece generalmente la duración de la retención de todos los puntos de recuperación. Por ejemplo, si realiza una copia una copia de seguridad de un equipo cada cuarto de hora, se guardan 96 puntos de recuperación en el repositorio de ese equipo por día, hasta que comience la consolidación. Sin administrar la política de retención, dicha cantidad de datos puede llenar rápidamente un repositorio.

NOTE: Los administradores deben tener en cuenta que la realización de copias de seguridad frecuentes puede afectar al tráfico de la red. Otros factores que afectan al tráfico de la red incluyen otras transferencias (como la replicación), la velocidad de cambio de los datos y el hardware de red, cables y conmutadores.

El Core está predefinido con una política de retención predeterminada. La política predeterminada conserva:

- Todos los puntos de recuperación durante tres días
- Un punto de recuperación por hora durante dos días
- Un punto de recuperación por día durante cuatro días
- Un punto de recuperación por semana durante tres semanas
- Un punto de recuperación por mes durante dos meses
- Un punto de recuperación al año durante X años (opción deshabilitada en la política predeterminada).

Después de esta política predeterminada, el punto de recuperación más antiguo es generalmente de 92 días de antigüedad. Los datos posteriores a la fecha de origen de una política predeterminada se eliminan.

Al configurar la política de retención a nivel del Core se aplica automáticamente a todos los equipos que proteja dicho Core. Puede cambiar la política predeterminada según sus necesidades.

También puede crear una política de retención personalizada para cualquier máquina. Al establecer la política a nivel de equipo se puede especificar una política de retención distinta a la política predeterminada del Core. Para obtener más información sobre la configuración de las políticas de retención, consulte Ajuste de la configuración de la política de retención predeterminada del Core y Personalización de la configuración de la política de retención de un equipo protegido.

Ajuste de la configuración de la política de retención predeterminada del Core

La política de retención del Core especifica durante cuánto tiempo se almacenan los puntos de recuperación de un equipo protegido en el repositorio.

La política de retención del Core se ejecuta mediante un proceso de consolidación que se realiza como un componente de trabajos nocturnos en ejecución. A continuación, los puntos de recuperación por encima del tiempo especificado en la política de retención se “consolidan” (combinan) en menos puntos de recuperación que cubren un período de tiempo menos detallado. La aplicación de la política de retención de forma nocturna da como resultado la constante consolidación de copias de seguridad que envejecen. Esto lleva aparejada la eliminación de los puntos de recuperación más antiguos, en base a los requisitos especificados en esa política de retención.

Se pueden configurar diferentes ajustes de retención para Cores de origen y destino.

NOTE: Este tema es específico para personalizar la configuración de la directiva de retención en el Rapid Recovery Core. Cuando guarda la configuración de la política de retención personalizada en el Core, establece la configuración de la política de retención predeterminada que puede aplicarse a todos los equipos protegidos por este Core. Para obtener más información sobre cómo personalizar la configuración de las políticas de retención de equipos protegidos individuales, consulte Personalización de la configuración de la política de retención de un equipo protegido.

1. Vaya a la Rapid Recovery Core Console.
2. En la barra de iconos, haga clic en (Configuración) y, a continuación, realice una de las acciones siguientes:
   - En la lista de configuración del Core del lado izquierdo de la página Configuración haga clic en **Trabajos nocturnos**.
   - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado **Trabajos nocturnos**.

   Aparece la configuración del Core de los trabajos nocturnos.
3. En **Trabajos nocturnos**, haga clic en **Cambiar**.

   Se abrirá el cuadro de diálogo **Trabajos nocturnos**.
4. Para especificar los intervalos de tiempo para conservar los datos de copia de seguridad según sea necesario, en el panel Trabajos nocturnos, seleccione **Consolidación** y, a continuación, haga clic en **Configuración**.

   Se mostrará el cuadro de diálogo **Configuración** para la directiva de retención predeterminada del Core.
5. Para restaurar la configuración de la política de retención del Core a los valores predeterminados en cualquier momento, en la parte inferior del cuadro de diálogo Configuración, haga clic en **Restaurar valores predeterminados** y, a continuación, haga clic en **Sí** para confirmar.

   La configuración se restaura a los valores predeterminados descritos en la tabla en el paso 6.
6. Introduzca la programación predeterminada para conservar los puntos de recuperación como se describe en la tabla siguiente. La primera configuración especifica el periodo de retención principal para todos los puntos de recuperación guardados en el repositorio. Cada configuración adicional, cuando está activada, proporciona un nivel más granular de retención especificando los intervalos entre los que los puntos de recuperación deben consolidarse. Estos valores definen la duración durante la cual se mantienen los puntos de recuperación.

   Las opciones de la política de retención se describen en la tabla siguiente.

Tabla 149. Opciones del calendario de programación para la política de retención predeterminada

Cuadro de texto	Descripción
Conserva todos los puntos de recuperación de n [periodo de tiempo de retención]...	Especifica el periodo de retención principal para todos los puntos de recuperación guardados en el repositorio. Escriba el número que represente el período de retención y seleccione el período de tiempo. El valor predeterminado es 3 días. Puede elegir entre: Días, semanas, meses y años

Cuadro de texto	Descripción
...y luego conservar un punto de recuperación por hora durante n [período de tiempo de retención]	Si se selecciona, esta configuración mantiene un punto de recuperación por hora durante el periodo de tiempo que se especifique. El valor predeterminado es 2 días. Puede elegir entre días, semanas, meses y años. Si no desea guardar al menos un punto de recuperación por hora, borre esta opción.
...y luego conservar un punto de recuperación por día durante n [período de tiempo de retención]	Si se selecciona, esta configuración mantiene un punto de recuperación por día durante el periodo de tiempo que se especifique. El valor predeterminado es 4 días. Puede elegir entre días, semanas, meses y años. Si no desea guardar al menos un punto de recuperación por día, borre esta opción.
...y luego conservar un punto de recuperación por semana durante n [período de tiempo de retención]	Si se selecciona, esta configuración mantiene un punto de recuperación por semana durante el periodo de tiempo que se especifique. El valor predeterminado es 3 semanas. Puede elegir entre semanas, meses y años. Si no desea guardar al menos un punto de recuperación por semana, borre esta opción.
...y luego conservar un punto de recuperación por mes durante n [período de tiempo de retención]	Si se selecciona, esta configuración mantiene un punto de recuperación por mes durante el periodo de tiempo que se especifique. El valor predeterminado es 2 meses. Puede elegir entre meses y años. Si no desea guardar al menos un punto de recuperación por mes, borre esta opción.
...y luego conservar un punto de recuperación por año durante n [período de tiempo de retención]	Si se selecciona, esta configuración mantiene un punto de recuperación por año durante el número de años que se especifique. El valor predeterminado (1 año) está deshabilitado de forma predeterminada. Si no desea guardar al menos un punto de recuperación por año, seleccione esta opción y especifique un número de años. Si no desea guardar al menos un punto de recuperación por año, borre esta opción.

El punto de recuperación más antiguo se determina con la configuración de la política de retención.

En el ejemplo siguiente se explica cómo se calcula el período de retención.

Conservar todos los puntos de recuperación durante tres días.

...y luego conservar un punto de recuperación por hora durante tres días

...y luego conservar un punto de recuperación por día durante cuatro días

...y luego conservar un punto de recuperación por semana durante tres semanas

...y luego conservar un punto de recuperación por mes durante dos meses

....y luego conservar un punto de recuperación por mes durante un año

En este ejemplo, el punto de recuperación más antiguo tendría un año y tres meses de antigüedad.

7. Cuando esté satisfecho con la configuración de la política de retención, haga clic en **Guardar**.

   El cuadro de diálogo **Configuración** se cierra.

8. En el cuadro de diálogo **Trabajos nocturnos**, haga clic en **Aceptar**.

   El cuadro de diálogo **Trabajos nocturnos** se cierra. La política de retención que definió se aplicará durante la consolidación nocturna.

   También puede aplicar esta configuración al especificar la política de retención de cualquier equipo protegido individual. Para obtener más información sobre cómo configurar políticas de retención para un

equipo protegido, consulte Personalización de la configuración de la política de retención de un equipo protegido.

Personalización de la configuración de la política de retención de un equipo protegido

Si desea reubicar puntos de recuperación para un equipo protegido específico desde un repositorio DVM principal en un repositorio por capas, el repositorio por capas ya debe existir. Para definir un repositorio por capas, consulte el tema Creación de un repositorio por capas.

La política de retención de un equipo protegido especifica durante cuánto tiempo se almacenan los puntos de recuperación en el repositorio. De forma predeterminada, cada equipo protegido usa la directiva de retención definida para el Core, a no ser que especifique una directiva de retención personalizada, como se describe en este procedimiento.

A partir de AppAssure versión 5.4.1, Rapid Recovery incluye la capacidad de definir directivas de retención distintas entre un equipo protegido en el Core de origen y el equipo replicado correspondiente en el Core de destino.

Siga este procedimiento para definir una política de retención personalizada para un equipo protegido, incluido un equipo replicado.

NOTE: Lo siguiente se aplica a los entornos que actualizan desde la versión 5.3.x de AppAssure a la versión 5.4.1 o cualquier versión del Rapid Recovery Core. Si desea personalizar una directiva de retención para cualquier equipo replicado, en primer lugar, deberá actualizar los Core de origen y destino a la versión 5.4.1 del AppAssure Core y, a continuación, realizar el trabajo Comprobar repositorio en cada repositorio en ese Core de destino. Es muy posible que la realización de este trabajo lleve una importante cantidad de tiempo, en función del tamaño de su repositorio y el sistema de almacenamiento subyacente. Para obtener información en segundo plano acerca de este trabajo, consulte Acerca de la comprobación de la integridad de los repositorios DVM. Para obtener información acerca de cómo realizar este trabajo, consulte Realizar una comprobación de integridad en un repositorio DVM.

1. En el menú Equipos de la Rapid Recovery Core Console, haga clic en el nombre del equipo que desea modificar.

   Se mostrará la página **Resumen** del equipo seleccionado.

2. Haga clic en el menú **Configuración**.

   Se muestra la página **Configuración**, que muestra los ajustes de configuración del equipo seleccionado.

3. De forma opcional, haga clic en el vínculo **Trabajos nocturnos** para desplazarse hasta la página Configuración para visualizar la configuración de los trabajos nocturnos.

4. En el encabezado Trabajos nocturnos, haga clic en **Cambiar**.

   Se abrirá el cuadro de diálogo **Trabajos nocturnos**.

5. Para especificar los intervalos de tiempo para conservar los datos de copia de seguridad según sea necesario, seleccione **Consolidación** y, a continuación, haga clic en **Configuración**.

   Se mostrará el cuadro de diálogo **Configuración** para la directiva de retención.

6. Si está personalizando los ajustes de la política de retención para un equipo replicado y ve un aviso que le notifica que debe realizar una comprobación de integridad en su repositorio, continúe con este paso. De lo contrario, vaya al paso 7.
   a. Si está preparado para realizar el trabajo, haga clic en **Comprobar integridad**
   b. Haga clic en **Sí** para confirmar el trabajo de comprobación de integridad.

NOTE: La ejecución de este trabajo puede tardar cierta cantidad de tiempo, en función del tamaño de su repositorio. Durante este tiempo, no podrá realizar ninguna otra acción (instantáneas, replicaciones ni exportaciones virtuales, entre otras) en el repositorio. Para obtener información sobre este trabajo, consulte Acerca de la comprobación de la integridad de los repositorios DVM.

- Cuando el trabajo Comprobar repositorio haya completado todos los trabajos secundarios con éxito, vuelva a este procedimiento y continúe con el siguiente paso.

7. En el cuadro de diálogo **Configuración**, haga lo siguiente:
   - Para usar la política de retención predeterminada con este equipo protegido, seleccione **Utilizar la política de retención predeterminada del Core** y haga clic en **Guardar**. La directiva predeterminada se aplica a este equipo protegido.
   - Para definir una política de retención predeterminada para este agente, seleccione **Utilizar la política de retención predeterminada** y continúe en el siguiente paso.

   El cuadro de diálogo **Configuración** se expande para mostrar información de la política de retención personalizada.
8. Introduzca el calendario de programación personalizado para conservar los puntos de recuperación como se describe en la tabla siguiente. La primera configuración especifica el periodo de retención principal para todos los puntos de recuperación guardados en el repositorio. Cada configuración adicional, cuando está activada, proporciona un nivel más granular de retención especificando los intervalos entre los que los puntos de recuperación deben consolidarse. Estos valores definen la duración durante la cual se mantienen los puntos de recuperación.

Tabla 150. Opciones del calendario de programación para la política de retención personalizada

Cuadro de texto	Descripción
Conserva todos los puntos de recuperación de n [periodo de tiempo de retención]...	Especifica el periodo de retención principal para todos los puntos de recuperación guardados en el repositorio. Escriba el número que represente el período de retención y seleccione el período de tiempo. El valor predeterminado es 3 días. Puede elegir entre: Días, semanas, meses y años
...y luego conservar un punto de recuperación por hora durante n [período de tiempo de retención]	Si se selecciona, esta configuración mantiene un punto de recuperación por hora durante el periodo de tiempo que se especifique. El valor predeterminado es 2 días. Puede elegir entre días, semanas, meses y años. Si no desea guardar al menos un punto de recuperación por hora, borre esta opción.
...y luego conservar un punto de recuperación por día durante n [período de tiempo de retención]	Si se selecciona, esta configuración mantiene un punto de recuperación por día durante el periodo de tiempo que se especifique. El valor predeterminado es 4 días. Puede elegir entre días, semanas, meses y años. Si no desea guardar al menos un punto de recuperación por día, borre esta opción.
...y luego conservar un punto de recuperación por semana durante n [período de tiempo de retención]	Si se selecciona, esta configuración mantiene un punto de recuperación por semana durante el periodo de tiempo que se especifique. El valor predeterminado es 3 semanas. Puede elegir entre semanas, meses y años. Si no desea guardar al menos un punto de recuperación por semana, borre esta opción.
...y luego conservar un punto de recuperación por mes durante n	Si se selecciona, esta configuración mantiene un punto de recuperación por mes durante el periodo de tiempo que se especifique. El valor predeterminado es 2 meses. Puede elegir entre meses y años.

Cuadro de texto	Descripción
[período de tiempo de retención]	Si no desea guardar al menos un punto de recuperación por mes, borre esta opción.
...y luego conservar un punto de recuperación por año durante n [período de tiempo de retención]	Si se selecciona, esta configuración mantiene un punto de recuperación por año durante el número de años que se especifique. El valor predeterminado (1 año) está deshabilitado de forma predeterminada. Si no desea guardar al menos un punto de recuperación por año, seleccione esta opción y especifique un número de años. Si no desea guardar al menos un punto de recuperación por año, borre esta opción.

En el ejemplo siguiente se explica cómo se calcula el período de retención.

Conservar todos los puntos de recuperación durante tres días.

...y luego conservar un punto de recuperación por hora durante tres días

...y luego conservar un punto de recuperación por día durante cuatro días

...y luego conservar un punto de recuperación por semana durante tres semanas

...y luego conservar un punto de recuperación por mes durante dos meses

....y luego conservar un punto de recuperación por mes durante un año

En este ejemplo, el punto de recuperación más antiguo tendría un año y tres meses de antigüedad.

9. Si deseaconservar los puntos de recuperación en su repositorio DVM principal, salte al paso 11.
10. Si desea reubicar los puntos de recuperación de su repositorio DVM principal a un repositorio por capas secundarioalmacenado en un dispositivo de copia de seguridad de la serie DR de Quest, realice lo siguiente:
    a. Seleccione la opción **Reubicar los puntos de recuperación desactualizados en un repositorio por capas**.
    b. Seleccione la antigüedad en la cual quiere reubicar puntos de recuperación de su repositorio principal al repositorio por capas.

    Puede especificar la antigüedad por semanas, meses o años. El periodo más corto que puede establecer es 1 semana.

    c. En el menú desplegable **Seleccionar un repositorio**, seleccione el repositorio por capas en el que desea reubicar todos los puntos de recuperación del equipo especificado.

> **NOTE:** Independientemente de dónde se encuentran los puntos de recuperación (un repositorio DVM local principal o un repositorio por capas secundario en un servidor de copia de seguridad de DR), también están sujetos a la política de retención y, por lo tanto, se consolidarán. Si necesita conservar puntos de recuperación más antiguos, un método es archivarlos. El otro enfoque es desactivar la consolidación o extender el periodo de retención de los equipos protegidos correspondientes.

11. Haga clic en **Guardar**.

Forzar la consolidación en todos los equipos protegidos

Puede omitir la política de retención programada al forzar los puntos de recuperación para consolidar el nivel del equipo protegido.

1. A partir del menú de los equipos protegidos de la Core Console de Rapid Recovery, haga clic en el nombre de un equipo protegido específico.

Aparece la página **Resumen** para el equipo seleccionado.

2. Haga clic en el menú desplegable **Más** en la parte superior de la vista del equipo protegido y, a continuación, seleccione **Política de retención**.

   Aparece la página **Política de retención** del equipo especificado.

3. Haga clic en **Force Rollup** (Forzar consolidación).
4. En el cuadro de diálogo, haga clic en **Sí** para confirmar.

   Rapid Recovery inicia la consolidación para este equipo, independientemente del calendario de programación de la política de retención.

Archivado

Esta sección proporciona información conceptual sobre los archivos de Rapid Recovery, incluidos casos de negocio para crearlos, opciones de almacenamiento y usos. También describe cómo crear un archivo puntual o cómo crear un archivo que se actualiza continuamente conforme a una programación. Los temas describen cómo pausar o editar archivos programados, cómo forzar o comprobar un archivo y cómo adjuntar o importar un archivo.

Cómo funciona la archivación

El Rapid Recovery Core guarda los datos de las instantáneas en el repositorio. Mientras que un repositorio se puede encontrar en diferentes tecnologías de almacenamiento (como por ejemplo SAN, DAS, o NAS), el factor de rendimiento más importante es la velocidad. Los repositorios usan elementos multimedia a corto plazo (que son caros y rápidos). Para prevenir que un repositorio se llene demasiado rápido el Core impone una directiva de retención que, con el tiempo, consolida los puntos de recuperación y finalmente los reemplaza por las copias de seguridad nuevas.

Si necesita conservar los puntos de recuperación, ya sea por un significado histórico, por cumplimiento legal, para cumplir con las políticas de almacenamiento de datos externos, o por cualquier otra razón, puede crear un archivo comprimido. Un archivo comprimido es una copia de los puntos de recuperación desde el repositorio para los equipos especificados a través de un intervalo de fechas que haya designado. Archivar un conjunto de puntos de recuperación no elimina los puntos de recuperación original de su repositorio. En lugar de eso, el archivo comprimido inmoviliza la colección de puntos de recuperación en el momento en el que se creó el archivo, como una copia por separado en la ubicación de almacenamiento que haya especificado. A diferencia de los puntos de recuperación del repositorio, los datos de un archivo comprimido no están sujetos a consolidación.

Puede crear, importar y adjuntar archivos comprimidos desde la opción **Archivo** en la barra de botones, o desde la página **Archivos** que se puede acceder desde el icono (Más) en la Core Console.

See also: Opciones de creación y almacenamiento de archivos comprimidos
See also: Opciones de almacenamiento y archivado de Amazon
See also: Opciones de la cadena de puntos de recuperación para los archivos
See also: Métodos para obtener acceso a un archivo
See also: Usos de los archivos comprimidos
See also: Creación de una archivación

Opciones de creación y almacenamiento de archivos comprimidos

Puede crear un archivo temporal a petición en cualquier momento.

También puede definir los requisitos para el archivado continuo programado. Esta acción crea un archivo de puntos de recuperación para los equipos que seleccione, en la ubicación que haya designado. Los puntos de recuperación adicionales para esos equipos se anexan continuamente al archivo siguiendo la programación que defina (diariamente, semanalmente o mensualmente).

Cuando cree un archivo, debe especificar dónde desea guardarlo. Puede almacenar un archivo comprimido en un sistema de archivos (localmente o a través de la red) o en una cuenta de almacenamiento en la nube.

NOTE: Antes de archivar en una cuenta en la nube, debe agregar las credenciales a la cuenta de almacenamiento en el Rapid Recovery Core. Para obtener más información sobre la definición de una cuenta en la nube en el Core, consulte Incorporación de una cuenta de nube.

Si almacena su archivo en la cuenta de almacenamiento en la nube de Amazon, debe definir la clase de almacenamiento al crear la cuenta. Para archivar directamente en Amazon Glacier, puede especificar el almacenamiento Glacier al definir la ubicación en el asistente Archivos. Para obtener más información sobre las clases de almacenamiento de Amazon, consulte Opciones de almacenamiento y archivado de Amazon.

- Los archivos puntuales son de solo lectura. Cuando se crea un archivo puntual, la ubicación de destino que especifique debe estar vacía.
- Cuando se utiliza un archivo programado, el Core anexa los puntos de recuperación adicionales al archivo existente.
- Si el medio de almacenamiento que ha seleccionado se queda sin espacio, Rapid Recovery detiene el trabajo, lo que le permite especificar otra ubicación. El archivo se divide en segmentos que pueden encontrarse en diferentes lugares, como el espacio lo permita.

See also: Incorporación de una cuenta de nube

Opciones de almacenamiento y archivado de Amazon

Al archivar datos en una cuenta de Amazon Simple Storage Service (S3), puede elegir entre varias clases de almacenamiento. Cada una tiene diferentes costes, beneficios y restricciones de acceso asociados. Los precios pueden variar por región.Rapid Recoveryversión 6.2 amplía la asistencia de las cuentas de almacenamiento de Amazon a todas las clases de almacenamiento. Esto es útil cuando se planea almacenar archivos deRapid Recovery en la nube de Amazon.

La comprensión de las clases de almacenamiento disponibles y la diferencia en los tiempos de espera para acceder a esas clases es fundamental para controlar los costes de almacenamiento de manera eficaz, al mismo tiempo que se puede acceder a los archivos dentro de los plazos de tiempo aceptables.

NOTE: Quest proporciona esta información de cortesía a los clientes de Rapid Recovery para crear conciencia de los factores que influyen en los precios de almacenamiento. Estos conceptos pueden ayudarle a planificar y crear presupuesto en consecuencia. Usted es responsable de todos los costes de almacenamiento en Amazon o de cualquier otro proveedor de servicios de la nube. Desde que Amazon puede cambiar los requisitos previos, los requisitos, los costes, las definiciones de la capa de almacenamiento, etc., se recomienda utilizar el sitio web de Amazon como el origen de autoridad principal de dicha información.

En general, Amazon actualmente ofrece las siguientes clases de almacenamiento.

Estándar. Esta clase de almacenamiento es para los datos a los que planea acceder con frecuencia o rápidamente. Esta clase es la opción predeterminada de almacenamiento de todos los asistentes de Rapid Recovery, de Windows y de cuadros de diálogo. No hay ninguna tarifa independiente para recuperar información en la clase de almacenamiento estándar.

Acceso estándar poco frecuente (IA). Esta clase de almacenamiento es más económica que la estándar, y está pensada para los datos a los que no tiene intención de acceder con frecuencia. Hay una tarifa de recuperación asociada al acceso a los datos en la clase de almacenamiento. Sin embargo, la disponibilidad es inmediata. Amazon cobra una tarifa para los objetos eliminados del almacenamiento de acceso poco frecuente antes de los 30 días.

Glacier. Esta clase es para el almacenamiento a largo plazo de datos que no requieren acceso a tiempo real. Es más económico para el almacenamiento a largo plazo de datos que rara vez se recuperan. Hay una tarifa de recuperación asociada con el acceso a los datos en la clase de almacenamiento. Amazon cobra una tarifa para los objetos eliminados de Glacier antes de los 90 días. La recuperación de datos almacenados en Glacier no es inmediata. Los tiempos de recuperación estándar requieren de 3 a 5 horas; la recuperación masiva de grandes

cantidades datos puede tardar hasta 12 horas. Las recuperaciones inmediatas pueden tardar hasta 5 minutos. Se aplican tarifas para cada opción de recuperación.

NOTE: A diferencia de las otras clases de almacenamiento de Amazon,Rapid Recovery no admite la creación de una cuenta en la nube específica de Glacier. Para archivar datos en Glacier, elija una cuenta en la nube de Amazon y seleccione la opción **Utilizar almacenamiento de Glacier** en la página **Ubicación** del asistente Archivos.

Almacenamiento de redundancia reducido (RRS). Esta categoría es una clase de almacenamiento de bajo coste diseñada para datos reproducibles no críticos con menos redundancia que la clase de almacenamiento estándar. Hay una tarifa de recuperación mínima asociada con el acceso a los datos en la clase de almacenamiento. Se espera que un porcentaje fraccionario de objetos almacenados en esta clase (Amazon lo recoge como un 0,01 % como máximo) no pueda recuperarse.

Para obtener la información más reciente, revise siempre los materiales del sitio web de Amazon.

En general, se aplican las siguientes pautas:

- Si pretende restaurar datos de manera habitual desde el archivo de Rapid Recovery, Estándar es la mejor opción.
- Desde el punto de vista económico, si planea restaurar datos de manera ocasional, considere Acceso estándar poco frecuente.
- Glacier está diseñado para el almacenamiento en frío de puntos de recuperación archivados desde los que en raras ocasiones se espera realizar la restauración. Un buen ejemplo de cuándo utilizar el almacenamiento Glacier es cuando se guardan los datos para el cumplimiento normativo. Glacier está disponible como una opción de archivo del asistente Archivos.
- Para el almacenamiento de datos no críticos y reproducibles, considere RRS.

Opciones de la cadena de puntos de recuperación para los archivos

Antes de crear el archivo, debe decidir el enfoque adecuado para las cadenas de puntos de recuperación. Utilice la información siguiente para determinar qué opción selecciona de la página **Opciones** del asistente Archivos.

- **Compilar cadenas de puntos de recuperación completas, además de las imágenes de base referenciadas fuera del intervalo de fechas.** Si selecciona la opción de compilar cadenas de puntos de recuperación completas podrá realizar el intervalo completo de la restauración de acciones para cualquier punto de recuperación en el archivo. Este intervalo incluye la restauración a nivel de archivos, a nivel de volumen y la restauración bare metal restore. Cuando selecciona esta opción, las cadenas de puntos de recuperación completas se guardan con su archivo. Puede restaurar datos incluso si la imagen base correspondiente al punto de recuperación seleccionado es anterior al intervalo de fechas del archivo. Sin embargo, el tamaño de este archivo es mayor para asegurarse de que tiene acceso a los datos en toda la cadena de puntos de recuperación.
- **Incluir solo los puntos de recuperación en el intervalo de fechas. Esto ahorra espacio, pero el usuario es responsable de archivar las imágenes de base que sean necesarias.** Si incluye solo los puntos de recuperación en el intervalo de fechas especificado en el archivo, el tamaño del archivo del archivo es menor. Para los datos que la imagen de base se incluye en el intervalo de fechas que ha especificado, tiene acceso a la gama completa de las opciones de restauración. Sin embargo, si desea recuperar datos capturados en una imagen base de una fecha anterior al intervalo de fechas que ha especificado, puede quedar restringido solo al nivel del archivo de recuperación. Los datos que se queden fuera del intervalo de archivos quedarán huérfanos.

Para obtener más información de las cadenas de puntos de recuperación, consulte el tema Cadenas del punto de recuperación y huérfanos.

Conceptos relacionados

See also: Cadenas del punto de recuperación y huérfanos

Tareas relacionadas

See also: Creación de una archivación
See also: Modificación de una archivación programada

Métodos para obtener acceso a un archivo

Cuando es necesario obtener acceso a los datos archivados en un punto de recuperación, tiene dos opciones.

- Para los archivos creados con Rapid Recovery versión 6.0.1 y posteriores, puede adjuntar el archivo. El archivo adjunto se muestra en el menú de navegación que se encuentra a la izquierda de la Core Console. Puede examinar los puntos de recuperación en el archivo, y efectuar las mismas acciones en los datos que en cualquier otro punto de recuperación que se encuentre actualmente en el repositorio, sin tener que importarlos.
- Puede importar un archivo restaurando esos puntos de recuperación a su repositorio. A continuación, puede realizar las mismas acciones con los datos que con cualquier otro punto de recuperación de su Core.Rapid Recovery Core es compatible con versiones anteriores y admite la importación de archivos de todas las versiones de AppAssure yRapid Recovery.

CAUTION: Dado que el Core reconoce las fechas originales de los puntos de recuperación en un archivo, los puntos importados desde otro archivo se pueden resumir o eliminar durante el siguiente periodo trabajos nocturnos, si su antigüedad supera el periodo de retención. Si desea conservar los puntos de recuperación más antiguos importados a partir de un archivo, puede desactivar la consolidación o extender el periodo de retención de los equipos protegidos más relevantes.

Cuando necesite acceder a los datos de un punto de recuperación archivado, puede adjuntar (en Rapid Recovery 6.x y posteriores) o importar el archivo comprimido, para restaurar dichos puntos de recuperación en su repositorio.

Tareas relacionadas

See also: Adición de un archivo comprimido
See also: Importación de un archivo

Usos de los archivos comprimidos

Una vez se haya creado un archivo, puede utilizarse de las siguientes maneras:

- Se puede utilizar un archivo para mover datos entre repositorios.
- Un archivo comprimido puede adjuntarse a la Core Console y montarse como un sistema de archivos de recuperación simple de archivo o carpeta. Pueden aplicarse ciertas restricciones.
- Un archivo puede importarse a un repositorio. Si algún punto de recuperación del archivo ya se ha consolidado o eliminado del repositorio, esta acción lo restaura.
- Un archivo puede utilizarse como el origen de una restauración Bare Metal Restore o para exportar una máquina virtual.

Creación de una archivación

Puede utilizar este procedimiento para crear un archivo comprimido único o programado.

Si tiene pensado crear un archivo en una ubicación en la nube, primero se debe agregar su cuenta de nube a la Rapid Recovery Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.

Un archivo puntual es un archivo creado a petición para un equipo especificado. Un archivo comprimido programado un archivo comprimido que aparece automáticamente en la fecha y hora especificadas en el

asistente. Cuando programa un archivo periódico, satisface la necesidad de archivar datos procedentes de equipos protegidos con frecuencia sin el inconveniente de definir repetidamente un archivo puntual.

Al crear un archivo comprimido, debe decidir si va a incluir una cadena de puntos de recuperación completa en el archivo. Para obtener más información, consulte Opciones de la cadena de puntos de recuperación para los archivos.

1. En la barra de botones de la Core Console de Rapid Recovery, haga clic en **Archivo comprimido**.

   Se abre el Asistente de archivación.
2. En la página **Tipo de archivación** del asistente, seleccione una de las siguientes opciones:
   - Archivación única
   - Archivado continuo (por programación)
3. Haga clic en **Siguiente**.
4. En la página **Ubicación**, seleccione la opción de la lista desplegable **Tipo de ubicación** y, a continuación, introduzca la información tal y como se describe en la tabla siguiente.

Tabla 151. Opciones del tipo de ubicación del archivo comprimido

Opción	Cuadro de texto	Descripción
Local	Ubicación	Introduzca la ruta de acceso en la que desea que resida el archivo; por ejemplo, `d:\work\archive`.
Red	Ubicación	Introduzca la ruta de red en la que desea que resida el archivo; por ejemplo, `\\servername\sharename`.
	Nombre de usuario	Introduzca el nombre de usuario del usuario con acceso al recurso compartido de red.
	Contraseña	Introduzca la contraseña del usuario con acceso al recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable. **NOTE:** Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de carpeta	Introduzca un nombre para la carpeta en la que se guardan los datos archivados.
	Utilizar almacenamiento Glacier	Para almacenar su archivo en el almacenamiento Amazon Glacier, seleccione esta opción. Esta opción está pensada para el almacenamiento a largo plazo de los

Opción	Cuadro de texto	Descripción
		archivos. Para obtener más información, consulte Opciones de almacenamiento y archivado de Amazon.

5. Haga clic en **Siguiente**.
6. En la página **Equipos** del asistente, seleccione los equipos protegidos o equipos que desea archivar y, a continuación, haga clic en **Siguiente**.
7. Realice uno de los siguientes pasos:
   - Si elige crear un archivo comprimido puntual, omita el paso 14.
   - Si elige crear un archivo comprimido programado, continúe con el paso 8
8. En la página **Calendario de programación**, seleccione una de las siguientes opciones de la lista desplegable **Enviar datos**:
   - Diariamente
   - Semanalmente
   - Mensualmente
9. Introduzca la información que se describe en la siguiente tabla en base a lo que seleccionó en el paso 8.

Tabla 152. Opciones enviar datos

Opción	Cuadro de texto	Descripción
Diariamente	Una hora	Seleccione la hora del día a la que desea crear un archivo diario.
Semanalmente	Un día a la semana	Seleccione un día de la semana en el que crear automáticamente el archivo.
	Una hora	Seleccione la hora del día a la que desea crear una archivación.
Mensualmente	Un día al mes	Seleccione el día del mes en el que crear automáticamente el archivo.
	Una hora	Seleccione la hora del día a la que desea crear una archivación.

10. De manera opcional, si no desea que el trabajo de archivación empiece a la hora programada siguiente después de completar el asistente, seleccione **Realizar pausa en archivación inicial**.

    NOTE: Si desea realizar una pausa en un archivo programado si necesita más tiempo para preparar la ubicación de destino antes de que se reanude la archivación. Si no desea seleccionar esta opción, la archivación comenzará a la hora programada.
11. Haga clic en **Siguiente**.
12. En la página **Opciones**, seleccione una de las acciones de reciclaje descritas en la tabla siguiente.

Tabla 153. Opciones de reciclaje de archivos comprimidos continuos

Cuadro de texto	Descripción
Reemplazar este Core	Sobrescribe los datos archivados que ya existan y que pertenezcan a este Core, pero deja intactos los datos del resto de Cores.

Cuadro de texto	Descripción
Borrar completamente	Borra todos los datos archivados del directorio antes de escribir el nuevo archivo.
Incremental	Le permite añadir puntos de recuperación a un archivo existente. Compara los puntos de recuperación para evitar duplicar datos que hay en el archivo comprimido.

13. En la página **Opciones** de un archivo comprimido continuo, determine si desea incluir cadenas de puntos de recuperación completa en su archivo. Para obtener más información acerca de las opciones de las cadenas de puntos de recuperación, consulte Opciones de la cadena de puntos de recuperación para los archivos. Realice uno de los siguientes pasos:
    - Seleccione **Compilar cadenas de puntos de recuperación completas, además de las imágenes de base referenciadas fuera del intervalo de fechas** y, a continuación, omita el paso 17.
    - **Seleccione Incluir solo los puntos de recuperación en el intervalo de fechas. Esta opción ahorra espacio, pero el usuario es responsable de archivar las imágenes de base que sean necesarias** y, a continuación, vaya al paso 17.
14. En la página **Opciones** para una archivación única, introduzca la información que se describe en la tabla siguiente.

Tabla 154. Opciones de archivación única

Cuadro de texto	Descripción
Tamaño máximo	Los grandes archivos de datos se pueden dividir en varios segmentos. Seleccione el tamaño máximo de espacio que desea reservar para crear el archivo realizando una de las siguientes acciones: • Seleccione **Destino completo** para reservar todo el espacio disponible en la ruta de acceso que se introdujo en el destino del 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, introduzca la cantidad de espacio y, a continuación, seleccione una unidad de medida en la lista desplegable para personalizar el espacio que desea reservar. **NOTE:** Los archivos de la nube de Amazon se dividen automáticamente en segmentos de 50 GB. Los archivos de la nube de Microsoft Azure se dividen automáticamente en segmentos de 200 GB.
Acción de reciclaje	Seleccione una de las opciones de la acción de reciclaje siguientes: • **No reutilizar.** No sobrescribe ni borra datos archivados existentes de la ubicación. Si la ubicación no está vacía, Rapid Recovery permite seleccionar una ubicación diferente. • **Reemplazar este Core.** Sobrescribe los datos archivados que ya existan y que pertenezcan a este Core, pero deja intactos los datos del resto de Cores. • **Borrar completamente.** Borra todos los datos archivados del directorio antes de escribir el nuevo archivo. • **Incremental.** Le permite añadir puntos de recuperación a un archivo existente. Compara los puntos de recuperación para evitar duplicar datos que ya hay en el archivo comprimido.

Cuadro de texto	Descripción
Comentario	Escriba comentarios o información adicional que sea necesaria capturar para el archivo. El comentario aparece si importa el archivo comprimido más tarde.
Compilar cadenas de puntos de recuperación completas, además de las imágenes de base referenciadas fuera del intervalo de fechas.	Seleccione esta opción para archivar la cadena de punto de recuperación completa. Esta opción se selecciona de forma predeterminada.
Incluir solo los puntos de recuperación en el intervalo de fechas. Esto ahorra espacio, pero el usuario es responsable de archivar las imágenes de base que sean necesarias.	Seleccione esta opción para archivar solo los puntos de recuperación incrementales y las imágenes sin base. **NOTE:** Esta opción produce un archivo comprimido de puntos de recuperación huérfanos. No podrá usarlos para la recuperación hasta que archive sus imágenes base relacionadas. Para obtener más información acerca de las opciones de las cadenas de puntos de recuperación, consulte Opciones de la cadena de puntos de recuperación para los archivos.

15. Si seleccionó la opción de incluir solo los puntos de recuperación en el intervalo de fechas, haga clic en **Siguiente**. De lo contrario, haga clic en **Finalizar**.
16. En la página **Intervalo de fechas**, introduzca de forma manual la fecha de inicio y la de finalización de los puntos de recuperación que se van a archivar o seleccione la fecha y hora haciendo clic en el icono de calendario seguido por el icono de reloj después de la ventana calendario.
17. Haga clic en **Finalizar**.

    El Asistente se cerrará.

Archivar en la nube

Cuando los datos alcanzan la finalización de un periodo de retención, es posible que desee ampliar dicho plazo archivando los datos. Al archivar datos, siempre surge la cuestión de dónde almacenarlos. Rapid Recovery le permite cargar su archivo en una gran variedad de proveedores de nube directamente desde la Core Console. Las nubes compatibles incluyen Microsoft Azure, Amazon S3, cualquier proveedor basado en OpenStack, archivos de nube Rackspace y Google Cloud.

La exportación de un archivo a una nube empleando Rapid Recovery lleva aparejados los siguientes procedimientos:

- Añade una nueva cuenta de nube al Rapid Recovery Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.
- Archivar sus datos y exportarlos a su cuenta de nube. Para obtener más información, consulte Creación de una archivación.
- Recuperar los datos archivados adjuntando un archivo o importándolos desde la ubicación de nube. Para obtener más información, consulte Adición de un archivo comprimido o Importación de un archivo, respectivamente.

Modificación de una archivación programada

Rapid Recovery permite cambiar los detalles de un archivado programado. Para modificar una archivación programada, realice estos pasos en el procedimiento siguiente.

1. En la Rapid Recovery Core Console, haga clic en el menú desplegable **Más** en la barra de iconos y, a continuación, seleccione **Archivos**.
2. En la página **Archivos**, en Archivaciones programadas, haga clic en el menú desplegable junto al archivo que desea cambiar y, a continuación, haga clic en **Editar**.

   Se abre el **Asistente de archivación**.
3. En la página **Ubicación** del Asistente de archivación, seleccione una de las siguientes opciones de la lista desplegable **Tipo de ubicación**:
   - Local
   - Red
   - Nube
4. 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 155. Detalles de archivación

Opción	Cuadro de texto	Descripción
Local	Ubicación	Introduzca la ruta de acceso en la que desea que resida el archivo; por ejemplo, `d:\work\archive`.
Red	Ubicación	Introduzca la ruta de red en la que desea que resida el archivo; por ejemplo, `\\servername\sharename`.
	Nombre de usuario	Introduzca el nombre de usuario del usuario con acceso al recurso compartido de red.
	Contraseña	Introduzca la contraseña del usuario con acceso al recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable.

Opción	Cuadro de texto	Descripción
		NOTE: Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de carpeta	Introduzca un nombre para la carpeta en la que se guardan los datos archivados.
	Utilizar almacenamiento Glacier	Para almacenar su archivo en el almacenamiento Amazon Glacier, seleccione esta opción. Esta opción está pensada para el almacenamiento a largo plazo de los archivos. Para obtener más información, consulte Opciones de almacenamiento y archivado de Amazon/

5. Haga clic en **Siguiente**.
6. En la página **Equipos** del asistente, seleccione los equipos protegidos o equipos que contienen los puntos de recuperación que desea archivar. Borre los equipos que no desea archivar.
7. Haga clic en **Siguiente**.
8. En la página **Calendario de programación**, seleccione una de las siguientes opciones de la lista desplegable **Enviar datos**:
   - Diariamente
   - Semanalmente
   - Mensualmente
9. Introduzca la información que se describe en la siguiente tabla en base a lo que seleccionó en el paso 8.

Tabla 156. Opciones enviar datos

Opción	Cuadro de texto	Descripción
Diariamente	Una hora	Seleccione la hora del día a la que desea crear un archivo diario.
Semanalmente	Un día a la semana	Seleccione un día de la semana en el que crear automáticamente el archivo.
	Una hora	Seleccione la hora del día a la que desea crear un archivo diario.
Mensualmente	Un día al mes	Seleccione el día del mes en el que crear automáticamente el archivo.
	Una hora	Seleccione la hora del día a la que desea crear un archivo diario.

10. De manera opcional, para aplazar la archivación y que se reanude más tarde, seleccione **Realizar pausa en archivación inicial**.

    NOTE: Si desea realizar una pausa en un archivo programado si necesita más tiempo para preparar la ubicación de destino antes de que se reanude la archivación. Si no desea seleccionar esta opción, la archivación comenzará a la hora programada.
11. Haga clic en **Siguiente**.
12. En la página **Opciones**, utilice la lista desplegable **Acción de reciclaje** para seleccionar una de las opciones descritas en la tabla siguiente:

Tabla 157. Opciones de reciclar archivo comprimido

Cuadro de texto	Descripción
Incremental	Le permite añadir puntos de recuperación a un archivo existente. Compara los puntos de recuperación para evitar duplicar datos que ya hay en el archivo.
Reemplazar este Core	Sobrescribe los datos archivados que ya existan y que pertenezcan a este Core, pero deja intactos los datos del resto de Cores.
Borrar completamente	Borra todos los datos archivados del directorio antes de escribir el nuevo archivo.

13. En la página **Opciones** del asistente, determine si desea incluir cadenas de puntos de recuperación completa en su archivo. Para obtener más información acerca de las opciones de las cadenas de puntos de recuperación, consulte Opciones de la cadena de puntos de recuperación para los archivos. Realice uno de los siguientes pasos:
    - Seleccione **Compilar cadenas de puntos de recuperación completas, además de las imágenes de base referenciadas fuera del intervalo de fechas**.
    - **Seleccione Incluir solo los puntos de recuperación en el intervalo de fechas. Esto ahorra espacio, pero tiene la responsabilidad de archivar las imágenes de base que sean necesarias**.
14. Haga clic en **Finalizar**.

    Rapid Recovery se aplica a los cambios en el archivo comprimido.

Cómo realizar una pausa o reanudar un archivo programado

Si tiene un trabajo programado de archivado para que se repita, puede pausar o resumir esta acción según sea necesario.

Hay veces que es necesario realizar una pausa en un trabajo de archivación programado, como cuando tiene que cambiar la ubicación de archivación de destino. Del mismo modo, si estableció una pausa inicial en el archivado cuando realizó el procedimiento Creación de una archivación, es probable que desee reanudar el archivo comprimido programado más adelante. Realice los pasos del procedimiento siguiente para realizar una pausa o reanudar la archivación programada.

1. Desde laRapid Recovery Core Console, haga clic en el menú **Más** de la barra de iconos y, a continuación, en **Archivos**.
2. En la página **Archivos comprimidos**, en las archivaciones programadas, realice una de las acciones siguientes:
    - Seleccione el archivo que prefiera y, a continuación, haga clic en la acción que desee:
        - Realizar pausa
        - Reanudar
    - Junto al archivo que desee, haga clic en el menú desplegable y haga clic en una de las siguientes acciones:
        - Realizar pausa
        - Reanudar

El estado del archivo se muestra en la columna Programar.

Forzar un trabajo de archivación

Mediante este procedimiento, puede forzar Rapid Recovery para realizar el trabajo de archivado en un archivo comprimido programado en cualquier momento.

Para forzar un trabajo de archivación, debe tener un archivo programado en el Core.

1. Desde la Rapid Recovery Core Console, en la barra de iconos, haga clic en el menú **Más** de la barra de iconos y, a continuación, haga clic en **Archivos**.
2. En la página Archivos comprimidos, en Archivaciones programadas, haga clic en el menú desplegable junto al archivo comprimido que desea forzar y, a continuación, haga clic en **Forzar**.

   Rapid Recovery archiva los puntos de recuperación en función de la configuración que ha elegido para ese archivo comprimido, independientemente de la hora de archivo comprimido programado que estableció.

Comprobación de una archivación

La comprobación de un archivo comprimido verifica si un archivo comprimido y su contenido se encuentran lo suficientemente saludables para que se restauren.

Puede explorar un archivo comprimido para la integridad de su estructura, los segmentos de datos y archivos de índice al realizar una comprobación de archivo comprimido. La comprobación de archivo comprimido verifica la presencia de todos los archivos necesarios en el archivo y que los archivos se encuentran en buen estado. Para realizar una comprobación de archivo, realice los pasos del siguiente procedimiento.

1. Desde la Rapid Recovery Core Console, en la barra de iconos, haga clic en el menú **Más** de la barra de iconos y, a continuación, haga clic en **Archivos**.
2. En la página **Archivos**, haga clic en **Comprobar**.

   Aparecerá el cuadro de diálogo **Comprobar archivado**.
3. Para **Tipo de ubicación**, seleccione una de las opciones siguientes en la lista desplegable:
   - Local
   - Red
   - Nube
4. En función del tipo de ubicación que haya seleccionado en el paso 3, introduzca los detalles para el archivo comprimido según se describen en la siguiente tabla.

Tabla 158. Detalles de archivación

Opción	Cuadro de texto	Descripción
Local	Ubicación	Introduzca la ruta de acceso local para el archivo.
Red	Ubicación	Introduzca la ruta de acceso de red para el archivo.
	Nombre de usuario	Escriba el nombre de usuario. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.

Opción	Cuadro de texto	Descripción
	Contraseña	Escriba una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable. **NOTE:** Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de carpeta	Seleccione la carpeta en la que se guardan los datos archivados; por ejemplo, Archivo-Rapid Recovery-7-[FECHA CREACIÓN]-[HORA CREACIÓN]

5. Seleccione o borre las comprobaciones que se describen en la siguiente tabla. Todos están seleccionados de forma predeterminada.

   NOTE: No borre todas las comprobaciones. Debe seleccionar al menos una opción.

Opción	Descripción
Desplazamiento de asignación de archivos de índice	Esta opción comprueba que todos los datos de la estructura interna del archivo están en la ubicación correcta.
Integridad de estructura	Esta opción verifica la presencia de determinados archivos internos y las estructuras de las carpetas del archivo comprimido. Si faltan los archivos o las carpetas, la comprobación falla.
Integridad de suma de comprobación	Esta opción comprueba la integridad de los segmentos de datos en el archivo comprimido para asegurarse de que los segmentos se encuentran en buen estado.

6. Haga clic en **Comprobar archivo**.

   Rapid Recovery comprueba el archivo según las selecciones efectuadas.

Adición de un archivo comprimido

La adición de un archivo comprimido le permite ver los puntos de recuperación de dicho archivo.

Deberá tener un archivo ya existente creado en el Rapid Recovery Core versión 6.0.1 o posterior para completar este procedimiento. Para obtener más información, consulte Creación de una archivación.

Cuando adjunte un archivo comprimido, el nombre que le proporcione aparecerá como un archivo comprimido de menú en el menú de navegación que se encuentra a la izquierda de la Core Console. Cada equipo protegido con puntos de recuperación del archivo comprimido se muestra por separado debajo del menú de archivo. Puede hacer clic en cualquier nombre de equipo en el archivo comprimido y examinar sus puntos de recuperación. A continuación, puede realizar las mismas acciones que con cualquier otro punto de recuperación visible en el Core.

Al adjuntar el archivo comprimido también se almacenan las credenciales para acceder a la información. Hasta que elimine la definición del archivo comprimido adjunto, podrá volver a adjuntar o desvincular dicho archivo para hacer que se pueda acceder a sus puntos de recuperación con mayor facilidad.

Utilice este procedimiento para adjuntar un archivo comprimido.

1. En la Rapid Recovery Core Console, haga clic en el menú desplegable **Archivo** y, a continuación, seleccione **Adjuntar archivo**.

   Aparecerá el cuadro de diálogo **Adjuntar archivo comprimido**.
2. En el cuadro de texto **Nombre**, introduzca un nombre para dicho archivo comprimido.

   El valor que escriba en este campo aparecerá en el menú de navegación que se encuentra a la izquierda como el nombre del menú del archivo comprimido.

   Si se sigue la práctica recomendada de los nombres de visualización, el nombre del archivo comprimido debería contener entre 1 y 64 caracteres alfanuméricos, espacios incluidos. No utilice caracteres no permitidos o frases no permitidas.
3. En la lista desplegable **Tipo de ubicación**, seleccione el tipo de ubicación del archivo comprimido de entre las opciones siguientes:
   - Local
   - Red
   - Nube
4. 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 159. Detalles del tipo de ubicación

Opción	Cuadro de texto	Descripción
Local	Ubicación	Introduzca la ruta de acceso al archivo comprimido; por ejemplo, `D:\work\archive`.
Red	Ubicación	Introduzca la ruta de acceso al archivo comprimido; por ejemplo, `\\servername\sharename`.
	Nombre de usuario	Introduzca el nombre de usuario para iniciar sesión en el recurso compartido de red.
	Contraseña	Introduzca la contraseña para iniciar sesión en el recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable. **NOTE:** Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.
	Contenedor	En el menú desplegable, seleccione el contenedor del archivo comprimido asociado con su cuenta.
	Nombre de carpeta	Introduzca el nombre de la carpeta de los datos del archivo comprimido; por ejemplo, Rapid-Recovery-Archive-[FECHA CREACIÓN]-[HORA CREACIÓN].

5. Presione **Attach (Conectar)**.

El archivo comprimido se adjunta a este Core y monta el contenido como un sistema de archivos.

Importación de un archivo

Puede utilizar este procedimiento para importar un archivo comprimido una sola vez, o programar un archivo comprimido que se va a importar de manera recurrente.

Cuando desea recuperar datos archivados, puede importar el archivo completo en una ubicación específica.

CAUTION: Realice este paso solo después de una cuidadosa consideración. La importación de un archivo comprimido llena el repositorio con el contenido del archivo comprimido, sustituyendo los datos nuevos en el repositorio ya que se capturó el archivo comprimido.

Para importar un archivo, realice los pasos del siguiente procedimiento.

1. En la barra de menú de la Rapid Recovery Core Console, haga clic en el menú desplegable **Archivo** y, a continuación, seleccione **Importar archivo**.

   Se abre el **Asistente de importación de archivo comprimido**.
2. En la página **Tipo de importación** del Asistente, seleccione una de las siguientes opciones:
   - Importación única
   - Importación continua (por programación)
3. Haga clic en **Siguiente**.
4. En la página **Ubicación**, seleccione la ubicación del archivo que desea importar de la lista desplegable y, a continuación, introduzca la información tal y como se describe en la tabla siguiente:

Tabla 160. Opciones del tipo de ubicación del archivo comprimido importado

Opción	Cuadro de texto	Descripción
Local	Ubicación	Introduzca la ruta de acceso en la que desea que resida el archivo; por ejemplo, `d:\work\archive`.
Red	Ubicación	Introduzca la ruta de red en la que desea que resida el archivo; por ejemplo, `\\servername\sharename`.
	Nombre de usuario	Introduzca el nombre de usuario del usuario con acceso al recurso compartido de red.
	Contraseña	Introduzca la contraseña del usuario con acceso al recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable. **NOTE:** Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.

Opción	Cuadro de texto	Descripción
	Nombre de la carpeta	Introduzca un nombre para la carpeta en la que se guardan los datos archivados.

5. Haga clic en **Siguiente**.
6. En la página **Información de archivo comprimido** del asistente, si desea importar cada máquina incluida en el archivo, seleccione **Importar todos los equipos**.
7. Complete una de las siguientes opciones según su selección:
   - Si ha seleccionado **Importación única** en el paso 2, ha seleccionado **Importar todos los equipos** en el paso 6, y todos los equipos están presentes en el Core, como protegidos, replicados o como equipos con puntos de recuperación únicamente, vaya al paso 12.
   - Si ha seleccionado **Importación continua (por programación)** en el paso 2, ha seleccionado **Importar todos los equipos** en el paso 6, y al menos un equipo no está presente en el Core, como protegido, replicado o como un equipo con puntos de recuperación únicamente, haga clic en **Siguiente** y, a continuación, vaya a paso 9.
   - Si no importa todos los equipos en el paso 6, haga clic en **Siguiente**, y, a continuación, continúe con el paso 8.
8. En la página **Equipos**, seleccione los equipos que desea importar desde el archivo.
   - Si ha seleccionado **Importación única** en el paso 2, y al menos un equipo no está presente en el Core, como protegido, replicado o como un equipo con puntos de recuperación únicamente, utilice las listas desplegables para seleccionar un repositorio para cada una de las máquinas que desea importar y, a continuación, vaya al paso 12.
   - Si todos los equipos ya están presentes en el Core, como protegidos, replicados o como equipos con puntos de recuperación únicamente, vaya al paso 12.
9. Haga clic en **Siguiente**.
10. En la página **Repositorio**, complete una de las opciones siguientes:
    - Si un repositorio está asociado con el Core, seleccione una de las opciones de la siguiente tabla.

Tabla 161. Opciones de repositorio

Opción	Descripción
Usar un repositorio existente	Seleccione un repositorio actualmente asociado a este Core en la lista desplegable.
Crear un repositorio	En el cuadro de texto Servidor, introduzca el nombre del servidor en el que desea guardar el nuevo repositorio, por ejemplo, nombreservidor o localhost, y, a continuación, consulte Creación de un repositorio DVM.

    - Si no hay ningún repositorio asociado con el Core, introduzca el nombre del servidor en el que desea guardar el nuevo repositorio, por ejemplo, nombreservidor o localhost, y, a continuación, consulte Creación de un repositorio DVM.
11. Si elige **Importación continua (por programación)** en el paso 2, en la página **Calendario de programación**, seleccione las opciones descritas en la tabla siguiente.

Tabla 162. Opciones de importación del calendario de programación

Opción	Descripción
Diariamente	Haga clic en el icono del reloj y utilice las flechas hacia arriba y hacia abajo para seleccionar la hora en la que desea que el trabajo de archivación empiece.

Opción	Descripción
	Si está utilizando un sistema de 12 horas, haga clic en el botón AM/PM para especificar la hora del día.
Semanalmente	Seleccione el día de la semana y, a continuación, la hora a la que desea que el trabajo de archivación empiece. Si está utilizando un sistema de 12 horas, haga clic en el botón AM/PM para especificar la hora del día.
Mensualmente	Seleccione el día del mes y la hora a la que desea que el trabajo de archivación empiece. Si está utilizando un sistema de 12 horas, haga clic en el botón AM/PM para especificar la hora del día.
Realizar pausa en importación inicial	Seleccione esta opción si no desea que el trabajo de importación empiece a la hora programada siguiente después de completar el asistente. **NOTE:** Puede realizar una pausa en una importación programada si necesita más tiempo para preparar la ubicación de destino antes de que se reanude la archivación. Si no desea seleccionar esta opción, la importación comenzará a la hora programada.

12. Haga clic en **Finalizar**.

Cuentas en la nube

Rapid Recovery le permite definir conexiones entre almacenamiento en la nube existente o proveedores de servicio en la nube y su Rapid Recovery Core. Entre los servicios en la nube compatibles se incluyen Microsoft Azure, Amazon Web Services (AWS), cualquier proveedor basado en OpenStack (incluido Rackspace) y Google Cloud. Las plataformas específicas del gobierno de los EE. UU. incluyen AWS GovCloud (US) y Azure Government. Puede agregar cualquier número de cuentas en la nube a la Core Console, incluidas varias cuentas para el mismo proveedor.

El propósito de agregar cuentas en la nube a su Core Console es trabajar con ellas como se describe en el tema Acerca de las cuentas de servicios en la nube.

Una vez agregadas, puede gestionar la conexión entre el Core y las cuentas en la nube. De forma específica, puede editar el nombre para mostrar o la información de las credenciales, configurar las opciones de conexión de la cuenta o eliminar la cuenta de Rapid Recovery. Cuando edite o elimine cuentas en la nube en la Core Console, no podrá cambiar las cuentas en la nube en sí, solo la vinculación entre estas y su capacidad de acceder a ellas desde la Core Console.

Esta sección describe cómo definir vínculos entre cuentas de proveedores de almacenamiento en la nube o de proveedores de servicio en la nube y la Rapid Recovery Core Console. También describe cómo gestionar estas cuentas en la nube en Rapid Recovery.

Los temas incluyen:

- Acerca de las cuentas de servicios en la nube
- Consideración de las opciones de almacenamiento en la nube
- Incorporación de una cuenta de nube
- Modificación de una cuenta de nube
- Eliminación de una cuenta de nube

Acerca de las cuentas de servicios en la nube

Rapid Recovery funciona con cuentas en la nube de las siguientes formas:

- **Archivo.** Puede almacenar un archivo puntual o un archivo programado continuado en la nube. Esta función es compatible con todos los tipos de cuenta en la nube admitidos. Cuando archive en la nube, podrá acceder más tarde a la información en los puntos de recuperación archivados adjuntando el archivo (para archivos creados en la versión 6.0.1 o posterior). Para todos los archivos, también puede importar el archivo. También puede realizar la restauración Bare Metal Restore a partir de un archivo.
- **Exportación virtual.** Puede realizar la exportación virtual a una cuenta en la nube de Azure. Esto incluye la exportación puntual de una máquina virtual o la exportación continuada para una máquina virtual en modo de espera.

Para obtener información conceptual relativa a varias cuentas en la nube, consulte Consideración de las opciones de almacenamiento en la nube.

Para obtener información sobre la configuración de los ajustes de tiempo de expiración entre el Core y las cuentas en la nube, consulte Configuración de ajustes de conexión de cuentas de la nube.

Para obtener información sobre la realización de exportaciones virtuales a la nube de Azure, consulte Exportación de datos a una máquina virtual Azure.

Consideración de las opciones de almacenamiento en la nube

En este tema se describe el soporte para las cuentas de almacenamiento en la nube de la Administración Pública de EE. UU. También se analizan las compensaciones entre los costes y otros factores al seleccionar cuentas en la nube para archivar.

Seguridad de las cuentas en la nube para la Administración Pública de EE. UU.

Las agencias de la Administración Pública locales, estatales y federales de Estados Unidos y sus partners tienen acceso a cada vez más opciones de cuentas en la nube. Rapid Recovery es compatible con las siguientes ofertas para la Administración Pública y cuentas en la nube relacionadas:

- **AWS GovCloud (US).**Amazon Web Services ofrece un servicio llamado AWS GovCloud (US). Se trata de una región de AWS aislada diseñada para cumplir requisitos normativos y de cumplimiento específicos. El uso de este servicio permite que las agencias de la Administración Pública de Estados Unidos y los clientes se unan a empresas privadas para aprovechar las cuentas en la nube. Rapid Recovery es compatible con el archivado en cuentas de almacenamiento Amazon S3 en GovCloud de AWS.
- **Azure Government.** Azure Government es una plataforma en la nube puramente gubernamental de Estados Unidos exclusiva para las agencias de la Administración Pública federales, estatales, locales y tribales de Estados Unidos y sus partners. Rapid Recovery es compatible con Azure Government de la misma forma que ofrecemos soporte de Azure estándar. Por ejemplo:
  - Rapid Recovery es compatible con el archivado en Azure Government y las cuentas de almacenamiento Azure estándar.
  - Rapid Recovery admite la exportación virtual a una máquina virtual Azure (puntual o espera virtual) en plataformas públicas y de Azure Government.
  - Rapid Recovery es compatible con la replicación de Cores local en un destino de replicación en la plataforma en la nube pública o de Azure Government. Para cada plataforma, si ha iniciado sesión en Azure Marketplace, puede seleccionar el "Destino de replicación Rapid Recovery " desde el marketplace de Azure Government. Mediante esta máquina virtual, los servicios de proceso de Azure y el almacenamiento que agrega a la máquina virtual para el repositorio, los usuarios pueden configurar de forma rápida y sencilla un Core de destino que replica sus datos de copia de seguridad locales en la nube de Azure Government.

Equilibrio del tiempo de acceso, el coste y la comodidad para archivar en cuentas en la nube

Con el fin de ofrecer a nuestros usuarios opciones rentables de exportación virtuales y de archivado en la nube, Rapid Recovery continúa ampliando la asistencia de los proveedores de almacenamiento en la nube (y las clases de almacenamiento para los proveedores líderes que las ofrecen). Los usuarios formados pueden aprovechar las políticas para equilibrar la comodidad de los archivos de datos, el tiempo de acceso a estos y el coste.

A la hora de considerar estrategias para archivar o exportar a la nube, es recomendable que los usuarios de Rapid Recovery entiendan las compensaciones entre el coste inicial de almacenamiento de datos, la frecuencia con la que se espera que se utilicen los datos, la necesidad de acceder a ellos en un periodo de tiempo determinado y los costes asociados con la recuperación de los datos.

Algunos proveedores (como Amazon S3) ofrecen diferentes clases de almacenamiento. Elegir la clase de almacenamiento correcta puede ahorrarle dinero si sus hipótesis acerca de estos factores son acertadas. Quest recomienda que los usuarios de Rapid Recovery revisen las políticas de almacenamiento de datos al menos una vez al año para garantizar que se están usando los recursos de forma eficaz. Asimismo, los administradores

deben revisar los datos que se archivan o exportan a cuentas en la nube para que pueda actualizar las hipótesis de planificación y migrar datos según corresponda.

El coste que supone para algunos proveedores el almacenamiento de datos es muy bajo o, en algunos casos, inexistente. Sin embargo, los proveedores de servicios en la nube a menudo aplican cargos en su cuenta cuando accede o recupera esos datos. Normalmente, existen diferentes tarifas que se calculan basándose en la rapidez con la que necesite acceder a los datos. En algunos casos, utilizar un almacenamiento más caro (como el estándar de Amazon S3) resulta más rentable si pretende restaurar los datos a partir de los puntos de recuperación que si los almacena en Glacier y necesita restaurarlos.

Amazon le permite definir políticas de ciclo de vida de datos que mueven datos entre las clases de almacenamiento de Amazon S3 a lo largo del tiempo. Por ejemplo, podría almacenar datos cargados recientemente utilizando la clase de almacenamiento Estándar, moverlos a Estándar: acceso poco frecuente 30 días más tarde y después a Almacenamiento de redundancia reducido pasados otros 60 días. También puede archivar datos de forma explícita de cualquier tipo de cuenta en la nube de Amazon S3 en Glacier utilizando el asistente Archivos. Esto es recomendable si se espera que la recuperación de datos no se lleve a cabo con mucha frecuencia. Antes de seleccionar esta opción, es importante que conozca las tarifas relacionadas con el acceso, el vencimiento del almacenamiento, etc. Consulte el tema Opciones de almacenamiento y archivado de Amazon.

Algunas características de Rapid Recovery están especialmente diseñadas para la nube. Si realiza una exportación virtual a la nube mediante Azure, hágalo con la espera virtual. Este proceso le permite crear una máquina virtual completamente de arranque en la nube de Azure. Los archivos de la máquina virtual se actualizan de forma continua con los punto de recuperación recién capturados. A diferencia de la espera virtual realizada de forma local, los archivos de la máquina virtual no se implementan en una máquina virtual de arranque a menos que los necesite. El coste inicial de la espera virtual en Azure solo incluye el almacenamiento. Los costes de procesos (que en Azure pueden ser considerables a largo plazo) solo se producen si se implementa la máquina virtual, lo que es necesario hacerla girar y para realizar una operación de restauración.

También puede replicar un Core local en la nube de Azure utilizando el destino de replicación Rapid Recovery. Puede configurar de forma rápida y sencilla un Core de destino seleccionando "Replicación de destino de Rapid Recovery" desde Azure Marketplace. El Core de destino incurre en los costes de procesos. También debe planificar el almacenamiento del repositorio dentro de Azure. Una característica nueva de versión 6.2 es que ahora puede utilizar el destino de replicación en la nube de la Administración Pública. Para obtener información sobre la replicación en Azure, consulte el *Rapid Recovery Replication Target for Microsoft Azure Setup Guide (Guía de configuración de replicación de destino de Rapid Recovery para Microsoft Azure)*

Es recomendable que los usuarios de Rapid Recovery que utilizan estas opciones de almacenamiento en la nube entiendan las compensaciones entre el coste inicial de almacenamiento de datos, la necesidad de acceder a ellos en un periodo de tiempo determinado y los costes asociados con la recuperación de los datos.

Por ejemplo, el coste que supone para algunos proveedores el almacenamiento de datos es muy bajo o, en algunos casos, inexistente. Sin embargo, los proveedores de servicios en la nube a menudo aplican cargos en su cuenta cuando accede o recupera esos datos. Normalmente, existen diferentes tarifas que se calculan basándose en la rapidez con la que necesite acceder a los datos. En algunos casos, utilizar un almacenamiento más caro (como el estándar de Amazon S3) resulta más rentable si pretende restaurar los datos a partir de los puntos de recuperación que si los almacena en Glacier y necesita restaurarlos.

Amazon le permite definir políticas de ciclo de vida de datos que mueven datos entre las clases de almacenamiento de Amazon S3 a lo largo del tiempo. Por ejemplo, podría almacenar datos cargados recientemente utilizando la clase de almacenamiento Estándar, moverlos a Estándar: acceso poco frecuente 30 días más tarde y después a Amazon Glacier pasados otros 60 días.

Incorporación de una cuenta de nube

Antes de que pueda mover datos en ambas direcciones entre una cuenta en la nube y su Core, debe agregar información de la cuenta del proveedor de la nube a la Rapid Recovery Core Console. Esta información identifica la cuenta en la nube en la Core Console al mismo tiempo que almacena en la caché la información de la conexión de forma segura. Este proceso permite al Rapid Recovery Core conectarse a la cuenta en la nube para realizar las operaciones que especifique.

Para añadir una cuenta de nube, realice estos pasos en el procedimiento siguiente.

1. En la barra de iconos de la Rapid Recovery Core Console, haga clic en el icono **Más** y, a continuación, seleccione **Cuentas en la nube**.

   Aparece la página **Cuentas en la nube**.
2. En la página **Cuentas en la nube**, haga clic en **Agregar cuenta nueva**.

   Se abrirá el cuadro de diálogo **Agregar cuenta nueva**.
3. Seleccione un proveedor de nube compatible en la lista desplegable Tipo de nube.
4. Basándose en el tipo de nube que haya seleccionado en el paso 3, introduzca los detalles que se describen en la tabla siguiente.

Tabla 163. Detalles de cuenta de nube

Tipo de nube	Cuadro de texto	Descripción
Microsoft Azure	Nombre para mostrar	Introduzca un nombre para mostrar para que esta cuenta en la nube se muestre en la Rapid Recovery Core Console; por ejemplo, Cuenta en la nube de Azure 1.
	Nombre de cuenta de almacenamiento	Introduzca el nombre de su cuenta de almacenamiento de Microsoft Azure. **NOTE:** El nombre debe coincidir precisamente con el nombre de la cuenta de almacenamiento de Azure. Debe contener solo números y letras en minúsculas y tener entre 3 y 24 caracteres de longitud.
	Clave de acceso	Introduzca la clave de acceso para su cuenta. **NOTE:** Puede introducir la clave principal o secundaria. Para obtener la clave de acceso de su cuenta de Azure, consulte **Claves** en **Configuración**.
	Utilizar protocolo https	Seleccione esta opción para usar el protocolo https seguro, en lugar del protocolo http estándar.
Amazon S3	Nombre para mostrar	Introduzca un nombre para mostrar para que esta cuenta en la nube se muestre en la Rapid Recovery Core Console; por ejemplo, Cuenta en la nube de Amazon S3 1.
	Clave de acceso	Introduzca la clave de acceso para su cuenta en la nube de Amazon.
	Clave secreta	Introduzca la clave secreta para esta cuenta.
	Extremo de servicio	De manera opcional, si utiliza una cuenta de almacenamiento compatible con S3 distinta a la cuenta de almacenamiento de Amazon S3 estándar, introduzca la URL http o https completa de esa cuenta de almacenamiento.

Tipo de nube	Cuadro de texto	Descripción
	Clase de almacenamiento	Seleccione una clase de almacenamiento para la cuenta S3. Puede elegir entre: • Estándar • Estándar: acceso poco frecuente • Almacenamiento de redundancia reducido Si desea archivar en Glacier, puede definir su cuenta en la nube de Amazon mediante cualquier clase de almacenamiento que aparezca. A la opción de seleccionar el almacenamiento en Glacier se puede acceder desde el asistente Archivos. **NOTE:** Para obtener más información sobre las clases de almacenamiento, consulte el tema Consideración de las opciones de almacenamiento en la nube.
Nubes con tecnología OpenStack	Nombre para mostrar	Introduzca un nombre para mostrar para que esta cuenta en la nube se muestre en la Rapid Recovery Core Console; por ejemplo, Cuenta en la nube de OpenStack 1.
	Región	Introduzca la región para su cuenta de nube.
	Nombre de usuario	Introduzca el nombre de usuario para su cuenta en la nube basada en OpenStack.
	Contraseña o clave de API	Seleccione si quiere utilizar una contraseña o una clave de API y, a continuación, introduzca su selección para esta cuenta.
	Id. de inquilino	Introduzca la identificación de inquilino para esta cuenta.
	URL de autenticación	Introduzca la dirección URL de autenticación para esta cuenta. Esta es la URL base para la instancia de nube. Si no se proporciona, Rapid Recovery Core utiliza la URL predeterminada, https://identity.api.rackspacecloud.com.
Archivos de nube de Rackspace	Nombre para mostrar	Introduzca un nombre para mostrar para que esta cuenta en la nube se muestre en la Rapid Recovery Core Console; por ejemplo, Cuenta en la nube de Rackspace 1.
	Región	Utilice la lista desplegable para seleccionar la región para su cuenta.
	Nombre de usuario	Introduzca el nombre de usuario para su cuenta de nube de Rackspace.
	Contraseña o clave de API	Seleccione si quiere utilizar una contraseña o una clave de API y, a continuación, introduzca su selección para esta cuenta.
	Id. de inquilino	Introduzca la identificación de inquilino para esta cuenta.
	URL de autenticación	Introduzca la dirección URL de autenticación para esta cuenta. Esta es la URL base para la instancia de nube. Si no se proporciona,

Tipo de nube	Cuadro de texto	Descripción
		Rapid Recovery Core utiliza la URL predeterminada, https://identity.api.rackspacecloud.com.
Google Cloud	Nombre para mostrar	Introduzca un nombre para mostrar para que esta cuenta en la nube se muestre en la Rapid Recovery Core Console; por ejemplo, Cuenta en la nube de Google 1.
	Archivo de certificado	Examine y seleccione su archivo de certificado de Google para autenticar esta cuenta en la nube.
	Clave privada	Introduzca la clave privada para esta cuenta.
	ID de proyecto	Introduzca el ID del proyecto asociado a esta cuenta.
	Correo electrónico de la cuenta de servicio	Introduzca la dirección de correo electrónico registrada en Google Cloud como propietario de esta cuenta de servicio en la nube.

5. Haga clic en **Guardar**.

   Se cerrará el cuadro de diálogo y su cuenta aparecerá en la página **Cuentas en la nube** de la Core Console.

Modificación de una cuenta de nube

Si necesita cambiar la información para conectar con su cuenta de nube, como por ejemplo para actualizar la contraseña o modificar el nombre para mostrar, puede hacerlo en la página **Cuentas en la nube** de la Rapid Recovery Core Console. Complete los pasos del siguiente procedimiento para modificar una cuenta de nube.

1. En la barra de iconos de la Rapid Recovery Core Console, haga clic en el icono **Más** y, a continuación, seleccione **Cuentas en la nube**.

   Aparece la página **Cuentas en la nube**.

2. Haga clic en el menú desplegable que hay junto a la cuenta en la nube que desea modificar y, a continuación, seleccione **Editar**.

   Se abre la ventana **Editar cuenta**.

3. Modifique los detalles según sea necesario y, a continuación, vuelva a escribir la contraseña (o clave API, clave secreta, clave privada, etc.) necesaria para la conexión a la cuenta de nube. Después haga clic en **Guardar**.

   NOTE: No puede modificar el tipo de nube.

Eliminación de una cuenta de nube

Si deja de usar su servicio de nube o decide dejar de usarlo para un Core en particular, es posible que desee eliminar su cuenta de nube de la Core Console. Complete los pasos del siguiente procedimiento para eliminar una cuenta de nube.

1. En la barra de iconos de la Rapid Recovery Core Console, haga clic en el icono **Más** y, a continuación, seleccione **Cuentas en la nube**.

   Aparece la página **Cuentas en la nube**.

2. Haga clic en el menú desplegable que hay junto a la cuenta de nube que desea modificar y, a continuación, seleccione **Eliminar**.
3. En el cuadro de diálogo **Eliminar cuenta**, haga clic en **Sí** para confirmar que desea eliminar la cuenta.
4. Si la cuenta de nube está en uso en esos momentos, un segundo cuadro de diálogo le pedirá confirmación sobre la eliminación. Haga clic en **Sí** para confirmar.

   NOTE: La eliminación de una cuenta que está en uso hace que todos los trabajos de archivación para esta cuenta fallen.

   El cuadro de diálogo se cierra y las credenciales para acceder a la cuenta en la nube especificada se eliminan del Core.

Local Mount Utility

En esta sección se describe cómo descargar, instalar y utilizar la Utilidad de montaje local (LMU) de Rapid Recovery basada en Windows para montar puntos de recuperación y explorar el contenido de un nivel de archivos con un equipo que es el host del Rapid Recovery Core.

Acerca de Local Mount Utility

Local Mount Utility (LMU) es una aplicación basada en Windows que se puede descargar y que permite montar un punto de recuperación de Rapid Recovery en cualquiera de los tres modos disponibles en cualquier máquina Windows compatible. Esta utilidad ligera se puede instalar en los mismos sistemas operativos Windows de 32 y 64 bits que el software Rapid Recovery Agent, pero no puede estar instalado en la misma máquina que Agent. LMU incluye los controladores de rapidrecovery-vdisk (anteriormente aavdisk) y aavstor, pero no se ejecuta como un servicio. Cuando la instale, de manera predeterminada, se instala en el directorio `C:\Program Files\AppRecovery\Local Mount Utility` y coloca un acceso directo en el escritorio del equipo.

Aunque la utilidad ha sido diseñada para el acceso remoto a un Rapid Recovery Core, también puede instalar LMU en el mismo equipo que un Rapid Recovery Core. Cuando se ejecuta en un Core, la aplicación reconoce y muestra todos los montajes de ese Core, incluidos los montajes realizados por medio de la Rapid Recovery Core Console. De la misma forma, los montajes realizados en LMU también aparecerán en la Core Console.

Cuando LMU se instala en el mismo equipo que Mailbox Restore, LMU inicia automáticamente Mailbox Restore cuando se usa para abrir una base de datos de Exchange. Mailbox Restore es la aplicación de Quest Rapid Recovery que se utiliza para restaurar almacenes de datos y elementos de Microsoft Exchange. Puede instalarla después de instalar LMU o el Rapid Recovery Core. Para obtener más información sobre Mailbox Restore, consulte la *Guía del usuario de Mailbox Restore para Exchange.*

NOTE: En los equipos con Linux se usa una utilidad de línea de comandos, local_mount, para hacer consultas en el Core para equipos protegidos y sus puntos de recuperación correspondientes. De la misma forma, la herramienta permite a los usuarios montar un volumen de puntos de recuperación de forma remota, explorar el contenido del volumen en los niveles de archivo y restaurar archivos concretos o todo un volumen desde el punto de recuperación, incluida una restauración BMR del volumen del sistema. Para obtener más información, véase *Guía del usuario de Rapid Recovery.*

Cómo trabajar con equipos Rapid Recovery Core en la Local Mount Utility

La Local Mount Utility (LMU) le permite trabajar con un número ilimitado de equipos Core de forma local o remota. Si instala la LMU en un servidor Rapid Recovery Core, el equipo aparece automáticamente en la LMU como host local. Todos los demás Core remotos aparecen con sus nombres de equipo o direcciones IP, en

función de la información que se haya especificado al agregarlos. Con la LMU, puede agregar, modificar y eliminar equipos Core. Para obtener más información, consulte los siguientes procedimientos:

- Incorporación de un equipo Core a Local Mount Utility
- Cambio de las opciones de Local Mount Utility
- Edición de la configuración de conexión de un Core en Local Mount Utility
- Cómo volver a conectarse a un Core
- Eliminación de un equipo Rapid Recovery Core de Local Mount Utility

Tareas relacionadas

See also: Incorporación de un equipo Core a Local Mount Utility
See also: Cambio de las opciones de Local Mount Utility
See also: Edición de la configuración de conexión de un Core en Local Mount Utility
See also: Cómo volver a conectarse a un Core
See also: Eliminación de un equipo Rapid Recovery Core de Local Mount Utility

Incorporación de un equipo Core a Local Mount Utility

Para montar un punto de recuperación, debe agregar un equipo Core a la LMU. No hay límite en el número de Cores que puede agregar.

Realice el procedimiento siguiente para configurar LMU agregando un Core.

1. En el equipo en el que esté instalada la utilidad LMU, ejecútela haciendo doble clic en el icono del escritorio.
2. Realice uno de los siguientes pasos:
   - En el menú de Local Mount Utility en la esquina superior izquierda, haga clic en **Agregar Core**.
   - Haga clic con el botón derecho en el panel de la izquierda y, a continuación, haga clic en **Agregar Core**.

   Aparecerá el cuadro de diálogo **Agregar Core**.
3. En el cuadro de diálogo **Agregar Core**, escriba las credenciales solicitadas que se describen en la tabla siguiente:

Tabla 164. Credenciales del Rapid Recovery **Core**

Opción	Descripción
Nombre de host	El nombre o la dirección IP del Core desde el que quiere montar puntos de recuperación. **NOTE:** Si instala LMU en un equipo Rapid Recovery Core, LMU agrega automáticamente el equipo de host local.
Puerto	Número de puerto usado para comunicar con el Core. El número de puerto predeterminado es 8006.
Utilizar mis credenciales de usuario de Windows	Seleccione esta opción si las credenciales que utiliza para acceder al Core son las mismas que sus credenciales de Windows.

Opción	Descripción
Utilizar credenciales específicas	Seleccione esta opción si las credenciales que utiliza para acceder al Core son distintas de las credenciales de Windows.
Nombre de usuario	Nombre de usuario utilizado para acceder al equipo del Core. **NOTE:** Esta opción solo está disponible si elije usar credenciales específicas.
Contraseña	Contraseña utilizada para acceder al equipo del Core. **NOTE:** Esta opción solo está disponible si elije usar credenciales específicas.

4. Haga clic en **Conectar**.
5. Si agrega varios Cores, repita todos los pasos según sea necesario.

Cambio de las opciones de Local Mount Utility

Lleve a cabo el siguiente procedimiento para cambiar las opciones para todos los Rapid Recovery Core conectados a LMU.

1. Desde la interfaz de usuario de Local Mount Utility, haga clic en **Opciones**.
2. En el cuadro de diálogo **Opciones**, puede cambiar la configuración descrita en la siguiente tabla.

Tabla 165. Configuración del Core

Opción	Descripción
Ubicación	Utilice el botón **Examinar** o introduzca una ruta de acceso a la carpeta que desee utilizar para los puntos de recuperación de montaje.
Tipo de montaje	Especifica la forma para acceder a los datos para el punto de recuperación montado. • Solo lectura • Solo lectura con escrituras anteriores • Editable
Idioma	Seleccione el idioma en el que desea que LMU aparezca. Puede seleccionar las opciones siguientes: • Inglés • Francés • Alemán • Portugués • Español • Chino simplificado • Japonés • Coreano

Opción	Descripción
Actualización automática	Seleccione e introduzca la cantidad de tiempo tras el cual la LMU debe actualizar su conexión al Core para obtener la información más reciente.
Mostrar Core local	Si la LMU está instalada en un equipo del Core, seleccione mostrar este Core.
Mostrar notificaciones emergentes	Seleccione permitir que la LMU notifique los eventos y alertas mediante elementos emergentes en el escritorio.
Abra la carpeta de montaje en el explorador de Windows si el montaje se ha realizado correctamente.	Seleccione esta opción para poder examinar el contenido de un punto de recuperación montado.

3. Haga clic en **Guardar**.

Edición de la configuración de conexión de un Core en Local Mount Utility

Para editar la configuración que se ha establecido al agregar un Core a LMU, realice el siguiente procedimiento.

NOTE: Este procedimiento no se aplica al Core de host local. Sólo se aplica a las máquinas de Core remoto.

1. En la interfaz de usuario de Local Mount Utility, haga clic con el botón derecho en el Core para el que desee editar la configuración y, a continuación, haga clic en **Editar Core**.
2. En el cuadro de diálogo **Editar Core**, puede cambiar la configuración descrita en la siguiente tabla.

Tabla 166. Configuración del Core

Opción	Descripción
Nombre de host	El nombre del Core desde el que desee montar puntos de recuperación. **NOTE:** Si instala LMU en un equipo Rapid Recovery Core, LMU agrega automáticamente el equipo de host local.
Puerto	Número de puerto usado para comunicar con el Core. El número de puerto predeterminado es 8006.
Utilizar mis credenciales de usuario de Windows	Seleccione esta opción si las credenciales que utiliza para acceder al Core son las mismas que sus credenciales de Windows.
Utilizar credenciales específicas	Seleccione esta opción si las credenciales que utiliza para acceder al Core son distintas de las credenciales de Windows.

Opción	Descripción
Nombre de usuario	Nombre de usuario utilizado para acceder al equipo del Core. **NOTE:** Esta opción solo está disponible si elije usar credenciales específicas.
Contraseña	Contraseña utilizada para acceder al equipo del Core. **NOTE:** Esta opción solo está disponible si elije usar credenciales específicas.

3. Después de realizar los cambios, haga clic en **Aceptar**.

Cómo volver a conectarse a un Core

Si pierde la conexión con un equipo del Rapid Recovery Core , puede restablecerla haciendo clic en **Actualizar** en la pantalla de inicio de LMU.

Eliminación de un equipo Rapid Recovery Core de Local Mount Utility

Lleve a cabo el siguiente procedimiento para eliminar un Core de LMU.

NOTE: Esta opción no está disponible para un Rapid Recovery Core localizado en el host local y etiquetado como tal.

1. Desde la interfaz de usuario de la utilidad de Local Mount Utility, haga clic con el botón derecho en el Core que desee eliminar y, a continuación, haga clic en **Eliminar Core**.
2. Para confirmar el comando, haga clic en **Sí** en el cuadro de diálogo.

   LMU elimina el Core y sus equipos protegidos del árbol de navegación.

Cómo trabajar con equipos protegidos en Local Mount Utility

Con la Local Mount Utility, puede montar y examinar los puntos de recuperación de los equipos protegidos sin tener que haber iniciado sesión en la Rapid Recovery Core Console asociada a ese equipo. Para obtener más información, consulte los siguientes procedimientos:

- Montaje de un punto de recuperación mediante Local Mount Utility
- Exploración de un punto de recuperación montado mediante Local Mount Utility
- Actualización de los puntos de recuperación
- Desmontaje de puntos de recuperación en Local Mount Utility

Montaje de un punto de recuperación mediante Local Mount Utility

Con la LMU, puede montar cualquier punto de recuperación asociado a un equipo Core conectado, incluyendo equipos protegidos, equipos replicados y equipos con puntos de recuperación únicamente.

Antes de montar un punto de recuperación, Local Mount Utility (LMU) debe conectarse al Core en el que se almacena el punto de recuperación. Como se describe en el procedimiento Incorporación de un equipo Core a Local Mount Utility, el número de Cores que pueden agregarse a la LMU es ilimitado.

1. En la LMU, seleccione el equipo desde el que desea montar un punto de recuperación.
2. Seleccione el punto de recuperación que desee montar y seleccione una de las siguientes opciones:

Opción	Descripción
Montar	Esta opción le permite montar el punto de recuperación mediante la selección predeterminada de las opciones de la LMU. Para obtener más información, consulte. Cambio de las opciones de Local Mount Utility.
Montaje avanzado...	Esta opción abre el cuadro de diálogo **Montajes avanzados**.

3. Si ha seleccionado **Montaje avanzado**, complete las opciones que se describen en la siguiente tabla.

Tabla 167. Opciones de montaje avanzado

Opción	Descripción
Ruta de acceso de punto de montaje	Introduzca o busque la ubicación que desea utilizar para el montaje de los puntos de recuperación.
Tipo de montaje	Seleccione una de las opciones siguientes: • Montar de solo lectura • Montar como editable • Montaje de solo lectura con escrituras anteriores Para obtener descripciones de cada opción, consulte el Paso 4.

- Haga clic en **Montar**.

LMU abre automáticamente la carpeta que contiene el punto de recuperación montado. La columna Montaje local de la página Puntos de recuperación de la LMU indica cómo se montó el punto de recuperación.

Exploración de un punto de recuperación montado mediante Local Mount Utility

La exploración de un punto de recuperación abre los datos de copia de seguridad en una ventana del Explorador de Windows, y le permite buscar los volúmenes y las carpetas para el tema o los temas que desea recuperar.

A continuación, puede recuperar elementos copiándolos en la ubicación que desee por medio de un administrador de archivos, como por ejemplo, Explorador de Windows (o mediante programación con las API de Windows). Realice el procedimiento siguiente para examinar un punto de recuperación montado actualmente.

NOTE: este procedimiento no es necesario si está explorando un punto de recuperación justo después de montarlo, ya que la carpeta que contiene el punto de recuperación se actualiza automáticamente al completar el procedimiento de montaje.

1. Desde la interfaz de usuario de la utilidad de montaje local, haga clic en **Montajes activos**.

   Se abre la ventana Montajes activos y muestra todos los puntos de recuperación montados.
2. Expanda el árbol de navegación para mostrar los puntos de recuperación montados para cada equipo y sus volúmenes.
3. Haga clic en **Explorar** junto al volumen que desea explorar.

Actualización de los puntos de recuperación

Si la opción está habilitada, la Local Mount Utility (LMU) recibe actualizaciones en tiempo real del Core y de los equipos protegidos. Si esta opción está deshabilitada, para ver los últimos puntos de recuperación de un equipo debe hacer clic con frecuencia en **Actualizar** en la pantalla de inicio de LMU.

Desmontaje de puntos de recuperación en Local Mount Utility

Realice el procedimiento siguiente para desmontar los puntos de recuperación montados en Local Mount Utility (LMU).

1. En la interfaz de usuario de LMU, haga clic en el Core o equipo protegido asociado con el punto o los puntos de recuperación montados.
2. Complete una de las siguientes acciones:
   - Para desmontar al mismo tiempo todos los puntos de recuperación montados del Core o equipo protegido seleccionado, haga clic en **Desmontar todo** y después haga clic en **Sí** en el cuadro de diálogo.
   - Para desmontar un único punto de recuperación, seleccione el punto de recuperación en la lista y haga clic en **Desmontar**.

   El punto o los puntos de recuperación se desmontan.

Referencias de la Core Console

Este apéndice incluye tablas de referencia que describen muchas de las funciones e iconos disponibles en la Rapid Recovery Core Console. Actúa como un complemento al capítulo Core Console de la *Guía del usuario de Rapid Recovery*.

Visualización de la interfaz para el usuario de la Core Console

La Core Console es la IU principal con la que los usuarios interactúan con Rapid Recovery. Cuando inicia sesión en la Rapid Recovery Core Console, verá los siguientes elementos.

Tabla 168. Elementos de la IU incluidos en la Core Console

Descripciones de los menús y la información que aparece en la Core Console.

Elemento de la IU	Descripción
Área de marca	Para los entornos típicos, la parte superior izquierda de la Core Console es la marca con el nombre completo del producto, incluido el logotipo de Quest. Al hacer clic en cualquier parte de los resultados de área de la marca en la apertura de una nueva pestaña en el navegador web, se muestra documentación del producto en el sitio web de asistencia.
Barra de botones	La barra de botones, que aparece a la derecha del área de marca, contiene botones a los que se puede acceder desde cualquier parte de la Core Console. Estos botones inician asistentes para llevar a cabo tareas comunes, como la protección de un equipo; la realización de una restauración a partir de un punto de recuperación; la creación, conexión o importación de un archivo; o la replicación desde este Core de origen a un Core de destino. Cada botón de la barra de botones se describe en mayor detalle en la tabla Tabla 169.
Ejecución del recuento de tareas	Muestra el número de trabajos que se están ejecutando actualmente. Este valor es una dinámica basada en el estado del sistema. Cuando hace clic en el menú desplegable, verá un resumen del estado de todos los trabajos que se están ejecutando actualmente. Puede elegir la cancelación del trabajo haciendo clic en la **X** de cualquier trabajo.
Acciones (menú desplegable)	El menú **Ayuda** incluye las siguientes opciones: • **Ayuda**. Abre la ayuda del producto, que se abre en una ventana independiente del navegador. • **Documentación**. Vínculos a la documentación técnica de Rapid Recovery del sitio web de Quest. • **Soporte**. Vínculos al sitio web de Asistencia para la protección de datos de Quest, que proporcionan acceso a Chat en vivo, tutoriales de vídeo, artículos de la base de conocimientos de Rapid Recovery, preguntas frecuentes y más. • **Guía de inicio rápido**. La Guía de inicio rápido es una guía de tareas sugeridas para configurar y usar Rapid Recovery. La guía se abre automáticamente cada vez que inicia sesión en la Core Console, a no ser que desactive esta función. Puede abrir

Elemento de la IU	Descripción
	la Guía de inicio rápido en el menú Ayuda en cualquier momento. Para obtener más información acerca de esta función, consulte Comprensión de la Guía de inicio rápido. • **Enviar una idea**. Si tiene sugerencias acerca de las características o mejoras, seleccione esta opción para abrir el portal de ideación de Quest, donde puede describir sus ideas de forma rápida y fácil para que las revisen los administradores de productos y puedan considerar su inclusión en una futura versión de Rapid Recovery. • **Acerca de**. Abre el cuadro de diálogo Acerca de Rapid Recovery. La información de aquí incluye el componente de Rapid Recovery, información sobre la versión, el ID del Core, un hipervínculo para contribuciones de terceros y una descripción del software.
Fecha y hora del servidor	La hora actual del equipo que ejecuta el servicio del Rapid Recovery Core aparece en la parte superior derecha de la Core Console. Al pasar el ratónsobre la hora, también aparece la fecha del servidor. Se trata de la fecha y hora registrada por el sistema para eventos como la creación de registros, programaciones e informes. Por ejemplo, cuando se aplican planificaciones de protección, se utiliza la hora mostrada en la Core Console. Esto sucede incluso aunque la zona horaria sea distinta en el servidor de la base de datos o en el equipo cliente donde se esté ejecutando el navegador.
Barra de iconos	La barra de iconos incluye una representación gráfica para las funciones principales accesibles en la Core Console. Se muestra en el lateral izquierdo de la interfaz de usuario (UI), directamente por debajo del área de marca. Al hacer clic en el elemento apropiado de la barra de iconos le lleva a la sección correspondiente de la UI donde puede gestionar esa función. Cada icono de la barra de iconos se describe en mayor detalle en la tabla Tabla 170.
Área de navegación izquierda	El área de navegación izquierda se muestra en el lateral izquierdo de la interfaz de usuario, por debajo de la barra de iconos. • El área de navegación izquierda contiene el texto filtrar y el menú Equipos. • Si ha agregado replicación a este Core, este área contiene un menú Equipos replicados. • Si tiene algún equipo que se retirara de la protección pero que tenga guardados puntos de recuperación, entonces este área contiene un menú Solo puntos de recuperación. • Si agregó cualquier grupo personalizado, entonces este área contiene un menú Grupo personalizado. • Si ha conectado un archivo, a continuación, esta área contiene un menú de archivos conectados. Puede alternar la visualización del área de navegación izquierda. Esto resulta útil cuando tiene que ver más contexto en el área de navegación principal de la IU. Para ocultar esta sección, haga clic en el borde de color gris entre las áreas de navegación izquierda y principal. Para mostrar este elemento de la IU de nuevo, haga clic en el borde de color gris de nuevo. Cada elemento del área de navegación izquierda se describe en mayor detalle en la tabla Tabla 172.
Ayuda sensible al contexto	  Desde la Rapid Recovery Core Console, cada vez que haga clic en el icono Ayuda (un signo de interrogación azul), se abre una ventana de navegador cuyo tamaño se puede modificar con dos marcos. El marco izquierdo contiene un árbol de navegación que muestra los temas de la *Guía del usuario de Rapid Recovery*. El marco derecho muestra el contenido del tema de la ayuda seleccionado. Siempre es posible ampliar el árbol de navegación de la ayuda

Elemento de la IU	Descripción
	para mostrar la ubicación del tema seleccionado en su jerarquía. Puede explorar todos los temas de la *Guía del usuario* utilizando esta función de ayuda sensible al contexto. Cierre el navegador cuando haya terminado de explorar temas. También puede abrir la ayuda desde la opción **Ayuda** del menú **Ayuda**.

Barra de botones

Los detalles sobre la barra de botones aparecen en la tabla siguiente.

Tabla 169. Botones y menús de la barra de botones

Descripciones de las acciones disponibles para cada menú y un botones en la barra de botones de la Core Console.

Elemento de la IU	Descripción
Barra de botones: Botón y menú Proteger	El botón **Proteger** inicia el Asistente para proteger un equipo, desde el que puede proteger un único equipo en el Rapid Recovery Core. Para otras opciones de protección adicionales, podrá acceder al menú desplegable que hay junto a este botón, que incluye las opciones siguientes. • La opción **Proteger equipo** es otro método para iniciar el Asistente para proteger un equipo para proteger un único equipo. • La opción **Proteger clúster** le permite conectar con un clúster de servidores. • La opción **Proteger varios equipos** abre el Asistente para proteger varios equipos, que le permite proteger dos o más equipos de forma simultánea. • La opción **Implementar el software Agent** permite instalar el software Rapid Recovery Agent en uno o varios equipos al mismo tiempo. Esta función utiliza el asistente para implementar el software Agent.
Barra de botones: Botón y menú Restaurar	El botón **Restaurar** abre el Asistente para restaurar un equipo que le permite restaurar datos procedentes de puntos de recuperación guardados desde un equipo protegido. Para otras opciones de exportación y restauración adicionales, podrá acceder al menú desplegable que hay junto a este botón, que incluye las opciones siguientes. • La opción **Restaurar equipo** es otro método para iniciar el Asistente para restaurar un equipo para restaurar datos. • La opción **Montar punto de recuperación** inicia el Asistente de montaje, que permite montar puntos de recuperación desde un equipo protegido. • La opción **Exportación de la VM** abre el Asistente de exportación. Desde este asistente puede crear una máquina virtual a partir de puntos de recuperación guardados en el Rapid Recovery Core. Tiene la opción de crear una exportación única, o puede definir parámetros para una máquina virtual que se actualice continuamente después de cada instantánea de un equipo protegido.
Barra de botones: Botón	El botón **Archivo comprimido** abre el Asistente de archivación. Desde el asistente, puede crear una archivación única desde los puntos de recuperación

Elemento de la IU	Descripción
y menú Archivo	seleccionados o crear un archivo comprimido y guardarlo continuamente para que lo archive en función del programa que defina. Para otras opciones de archivo comprimido adicionales, podrá acceder al menú desplegable que hay junto a este botón, que incluye las opciones siguientes. • La opción **Crear archivo comprimido** es otro método para iniciar el asistente de creación de archivo comprimido para crear una archivación única o una archivación continua. • La opción **Importar archivo comprimido** inicia el Asistente de importación de archivo comprimido, que permite importar un archivo comprimido. • La opción **Adjuntar archivo comprimido** monta un archivo comprimido para poder leer el contenido como un sistema de archivos.
Barra de botones: Botón Replicar 	El botón **Replicar** abre el asistente Replicación. Desde el asistente, puede especificar un Core de destino, seleccionar equipos protegidos en el Core de origen y replicar puntos de recuperación desde los equipos seleccionados en el Core de destino en el repositorio que especifique. Puede pausar la replicación al definirla o puede comenzar la replicación inmediatamente. Además, puede especificar si una unidad de inicialización se utilizará para copiar los datos de puntos de recuperación en el Core de destino.

Barra de iconos

Los detalles sobre la barra de iconos aparecen en la tabla siguiente.

Tabla 170. Barra de iconos

Las descripciones de las acciones disponibles para cada menú en la barra de iconos de la Core Console.

Elemento de la IU	Descripción
Barra de iconos	La barra de iconos incluye una representación gráfica para las funciones principales accesibles en la Core Console. Al hacer clic en el elemento apropiado le lleva a la sección correspondiente de la interfaz de usuario donde puede gestionar esa función. Los iconos de la barra de iconos incluyen:
Barra de iconos: Icono de inicio 	**Inicio**. Haga clic en el botón Inicio para navegar hasta la página Inicio del Core.
Barra de iconos: Icono de replicación 	**Replicación**. Haga clic en el icono Replicación para ver o gestionar replicaciones entrantes o salientes.
Barra de iconos: Icono En espera virtual 	**Espera virtual**. Haga clic en el icono En espera virtual para exportar información desde un punto de recuperación a una máquina virtual arrancable.

Elemento de la IU	Descripción		
Barra de iconos: Icono de Eventos			**Eventos.** Haga clic en el icono Eventos para ver un registro de todos los eventos del sistema relacionados con el Rapid Recovery Core.
Barra de iconos: Icono Configuración			**Configuración**. Haga clic en el icono Configuración para ver o administrar la configuración del Rapid Recovery Core. Puede realizar una copia de seguridad o restaurar los valores de la configuración del Core. Puede establecer una configuración general para los puertos de control o mostrar los aspectos. Además, puede configurar los ajustes en las categorías siguientes: actualizaciones automáticas; trabajos nocturnos; configuración de la cola de transferencias; configuración del tiempo de espera del cliente; configuración de la caché de desduplicación de DVM; configuración de Replay Engine; e implementar la configuración. Puede ver o cambiar las conexiones de la base de datos; la configuración de un servidor SMTP; las cuentas de almacenamiento en la nube y cambiar la configuración del tipo de letra de los informes. Puede establecer la configuración de conectabilidad de SQL; la configuración de trabajo del Core; los ajustes de licencia; la configuración de SNMP; y la configuración de vSphere.
Barra de iconos: Icono Más			**Más**. Haga clic en el icono Más para acceder a otras características importantes. Cada una tiene un icono propio que se enumera a continuación.
Barra de iconos: Icono Más	Información del sistema		**Información del sistema**. Haga clic en Información del sistema para mostrar los datos acerca del servidor del Rapid Recovery Core. Puede ver el nombre de host, el SO, la arquitectura y la memoria del Core. Puede ver el nombre que se muestra en la Core Console. También puede ver el nombre de dominio completamente cualificado del Core de su red, así como la ruta de acceso para sus metadatos de caché y las cachés de desduplicación. Para obtener más información sobre cómo cambiar el nombre para mostrar, consulte Funcionamiento de la información del sistema para el Core. Para obtener más información sobre la caché de desduplicación, consulte Funcionamiento de la caché de desduplicación y las ubicaciones de almacenamiento. Para obtener más información sobre el ajuste de la configuración, consulte Configuración de los valores de caché de la desduplicación de DVM.
Barra de iconos: Icono Más	Archivos comprimidos		**Archivos comprimidos**. Rapid Recovery le permite administrar los archivos de información del Core. Puede ver información acerca de archivos programados o conectados, y puede agregar, comprobar o importar los archivos.
Barra de iconos: Icono Más	Montajes		**Montajes**. Permite ver y desmontar montajes locales, así como ver y desconectar montajes remotos.
Barra de iconos: Icono Más	CD de arranque		**CD de arranque**. Permite administrar los CD de arranque, que se utilizan normalmente para una restauración Bare Metal Restore (BMR). Puede crear una imagen ISO del CD

Elemento de la IU	Descripción		
			de arranque, eliminar una imagen existente o hacer clic en la ruta de acceso para abrir o guardar la imagen.
Barra de iconos: Icono Más	Repositorios		**Repositorios**. Permite ver y administrar los repositorios asociados con el Core.
Barra de iconos: Icono Más	Claves de cifrado		**Claves de cifrado**. Permite ver, administrar, importar o agregar las claves de cifrado que puede aplicar a los equipos protegidos. Si no se utiliza, puede eliminar las claves de cifrado.
Barra de iconos: Icono Más	Cuentas en la nube		**Cuentas en la nube**. Permite ver y administrar las conexiones entre el Core y las cuentas de almacenamiento en la Nube.
Barra de iconos: Icono Más	Búsqueda de archivos		**Búsqueda de archivos**. Permite buscar archivos específicos a través de los puntos de recuperación que posteriormente se pueden restaurar en el disco local.
Barra de iconos: Icono Más	Política de retención		**Política de retención**. Permite ver y modificar la política de retención del Core, incluidos el tiempo para conservar puntos de recuperación antes de consolidarlos y finalmente eliminarlos.
Barra de iconos: Icono Más	Notificaciones		**Notificaciones**. Permite configurar las notificaciones sobre los eventos del Core, definir la configuración de servidor SMTP para las notificaciones por correo electrónico y establecer la reducción de repeticiones para suprimir las notificaciones del mismo evento.
Barra de iconos: Icono Más	Restauración de correo		**Restauración de correo electrónico**. Permite la búsqueda en las base de datos del servidor Exchange para ubicar y restaurar los mensajes de correo electrónico.
Barra de iconos: Icono Más	Descargas		Descargas. Puede descargar el instalador web del software Agent, Local Mount Utility o los archivos MIB que contienen información de eventos para utilizarla en un navegador SNMP.
Barra de iconos: Icono Más	Informes		Informes. Permite acceder a los informes de Core o programar informes para generarlos en una base constante.
Barra de iconos: Icono Más	Core Log		Core Log. Permite descargar el archivo de Core log con fines de diagnóstico.

Menú de navegación izquierdo

El conjunto completo de menús que puede aparecer en el área de navegación izquierda se describe en la siguiente tabla:

Tabla 171. Opciones del menú de navegación izquierdo

Las descripciones de las opciones disponibles para los tipos de equipos que aparecen en el área de navegación izquierda.

Elemento de la IU	Descripción
Menú Equipos	El menú Equipos (anteriormente llamado menú Equipos protegidos) aparece como el primer menú del área de navegación izquierda si hay uno o más equipos protegidos en el Core. Si hace clic en un nombre de equipo específico que se muestre en el panel, aparece una página de resumen, que muestra la información de resumen del equipo seleccionado. Para obtener más información sobre lo que puede realizar en la página Resumen, consulte Visualización de información de resumen de un equipo protegido.
Menú Equipos replicados	Si aparece el nombre de otro Rapid Recovery Core como un menú de navegación de nivel superior, el Core en el que visualiza la Core Console es un Core de destino. El menú recibe el nombre después del Core de origen, y cada equipo que aparece debajo representa un equipo de ese Core de origen que se ha replicado en el destino. Si el Core de destino replica los puntos de recuperación de más de un Core de origen, cada Core de origen aparece como su propio menú de navegación en el área de navegación izquierda. Si hace clic en un nombre de equipo específico que se muestre en el menú de un equipo replicado, aparece una página de resumen, que muestra la información de resumen del equipo replicado seleccionado. Para obtener más información acerca de la replicación, consulte Replicación.
Menú Solo puntos de recuperación	Si aparece un menú SOLO PUNTOS DE RECUPERACIÓN, el Core conserva los puntos de recuperación de un equipo una vez se haya protegido o replicado. Mientras que el equipo no continúe con la captura de nuevas instantáneas, los puntos de recuperación previamente capturados permanecen en el Core. Estos puntos de recuperación pueden utilizarse para la recuperación a nivel de archivos, pero no pueden utilizarse para una recuperación Bare Metal Restore sin sistema operativo, para restaurar volúmenes completos, o para agregar datos de instantáneas.
Menú Grupos personalizados	Si ha creado un grupo personalizado, el menú Grupos personalizados aparece en el menú de navegación. Los grupos personalizados son contenedores lógicos que se utilizan para agrupar los equipos (por ejemplo, por función, organización o ubicación geográfica). Los grupos personalizados pueden contener objetos heterogéneos (equipos protegidos, equipos replicados, entre otros). Puede definir la etiqueta de un grupo personalizado; como ocurre en otros menús, el nombre aparece en letras mayúsculas. Puede realizar acciones para elementos similares en un grupo personalizado al hacer clic en la flecha derecha del título del grupo personalizado. Por ejemplo, puede forzar una instantánea de cada equipo protegido de un grupo personalizado. Para obtener más información sobre la creación y administración de grupos personalizados, consulte Comprensión de los grupos personalizados.
Menú archivos comprimidos adjuntos	 Si conecta los archivos al Core, cada archivo aparece en el menú de navegación izquierdo. La etiqueta es el nombre del archivo. Cada equipo que aparece en la lista se incluye en el archivo.

Los detalles acerca de los elementos en el área de navegación izquierda aparecen en la tabla siguiente.

Tabla 172. Área de navegación izquierda y menús

Las descripciones de los menús disponibles para los tipos de equipos que aparecen en el área de navegación izquierda.

Elemento de la IU	Descripción
Filtro de texto de los menús de los equipos 	El filtro de texto es un campo de texto que le permite filtrar los elementos que se muestran en los menús de los equipos, equipos replicados y equipos con puntos de recuperación únicamente. Si escribe los criterios en este tipo de filtro solo los equipos que cumplen los criterios se mostrarán en los menús correspondientes.
Expandir y contraer detalles 	Haga clic en la flecha situada a la derecha del filtro de texto para expandir y contraer los detalles de los menús de los equipos, equipos replicados y equipos con puntos de recuperación únicamente.
Menú Equipos 	El menú Equipos aparece en el área de navegación izquierda de la IU. En este menú puede ver todos los equipos protegidos, los clústeres protegidos o los equipos replicados configurados en su Core. Si tiene grupos protegidos o equipos con puntos de recuperación únicamente, también aparecerán como una parte de este menú. **NOTE:** Si un hipervisor ESXi/vSphere tiene máquinas bajo protección, el host también aparecerá en este menú, con sus máquinas virtuales como secundarias, aunque dicho host no esté protegido. Puede contraer o expandir la vista de cualquiera de estos equipos protegidos en su Core haciendo clic en la fecha del lado izquierdo de esta etiqueta del menú. El icono que se visualiza representa el tipo de equipo: • Un icono de equipo simple representa una máquina física o una máquina virtual protegida con el software Agent Rapid Recovery instalado. Se utiliza el mismo icono para mostrar un equipo con punto de recuperación únicamente. • Un icono de varios equipos representa un clúster protegido. • Un icono de equipo doble hueco representa un VMware de una MV con protección sin agentes. • Un icono de equipo triple hueco representa un host VMware vCenter. • Un icono que muestra dos servidores apilados representa un host Hyper-V. • Un icono que muestra un único servidor representa una máquina virtual Hyper-V protegida sin agentes. Si hace clic en la etiqueta del menú Equipos, se abrirá la página Equipos, que muestra todos los equipos protegidos de este Core en el panel Equipos. Para obtener más información, consulte Visualización del menú Equipos protegidos.
Menú Equipos replicados	Si está replicando equipos desde otro Rapid Recovery Core, el nombre de ese Core aparecerá como un menú separado en el menú Equipos. Cada una de los equipos replicados en este Core de destino desde el Core de origen enumerado aparecen en este menú. Para cada equipo replicado, el icono indica el tipo de equipo que se está replicando. Por ejemplo, si se replica un solo equipo, el icono muestra un equipo. Si se replica un clúster de servidor, el icono representa un clúster. Puede contraer o ampliar la vista de cualquiera de estos equipos replicados haciendo clic en la fecha del lado izquierdo de esta etiqueta del menú. Puede realizar acciones en todos los equipos replicados desde el menú Equipos replicados. Si hace clic en el menú Equipos replicados, aparece la página Equipos. Esta página muestra los equipos protegidos en otro Core (de origen) que se replican en este

Elemento de la IU	Descripción
	Core de destino. Para obtener más información, consulte Visualización de equipos replicados en el menú de navegación.
Menú Solo puntos de recuperación	Si se retiraron de la protección equipos protegidos anteriormente por el Core, pero no se eliminaron los puntos de recuperación, entonces aparece el menú Solo puntos de recuperación. No hay ningún icono de menú. Cada uno de los equipos protegidos anteriormente con puntos de recuperación conservados se muestra en esta lista. El equipo con punto de recuperación únicamente muestra un icono de equipo protegido estándar. Puede contraer o ampliar la vista de los equipos con puntos de recuperación únicamente haciendo clic en la fecha del lado izquierdo de esta etiqueta del menú. Puede eliminar los puntos de recuperación de todos los equipos con solo puntos de recuperación en este Core desde el menú Solo puntos de recuperación. Si hace clic en el menú Solo puntos de recuperación, se abrirá la página Equipos, que muestra todos los equipos en los que se guardaron puntos de recuperación. Para obtener más información, consulte Visualización en el menú Solo puntos de recuperación.
Menú Grupos personalizados	Si su Core incluye grupos personalizados, el área de navegación izquierda incluye un menú Grupos personalizados. Cada objeto de ese grupo personalizado se visualiza en esta lista. Puede contraer o expandir la vista de cualquiera de los grupos personalizados en su Core haciendo clic en la flecha del lado izquierdo de esta etiqueta del menú. Puede realizar acciones para elementos parecidos en el grupo desde el menú Grupos personalizados. Si hace clic en el menú Grupos personalizados, se abrirá la página Equipos, que muestra un panel para cada uno de los objetos de Rapid Recovery que aparecen en su grupo: equipos protegidos, equipos replicados y equipos con puntos de recuperación únicamente. Para obtener más información, consulte Visualización en el menú Grupos personalizados.
Menú archivos comprimidos adjuntos	Si adjunta los archivos comprimidos a su Core, el área de navegación izquierda incluye un menú para cada archivo comprimido adjunto. Se visualiza en esta lista cada una de los equipos protegidos incluidos en el archivo comprimido. La etiqueta del menú utiliza el nombre especificado al guardar el archivo. Puede contraer o expander la vista de cualquiera de los archivos comprimidos adjuntos a su Core haciendo clic en la fecha del lado izquierdo de esta etiqueta del menú. Puede realizar acciones para elementos parecidos en el grupo desde el menú archivos comprimidos adjuntos. Si hace clic en el menú archivos adjuntos, se abrirá la página Equipos, que muestra un panel para cada uno de los objetos de Rapid Recovery que aparecen en su grupo: equipos protegidos, equipos replicados y equipos con puntos de recuperación únicamente. Para obtener más información, consulte Visualización en el menú Grupos personalizados.

Visualización de equipos protegidos

Desde la página **Inicio** de la Rapid Recovery Core Console, cuando observa la vista Tablas de resumen, puede ver información de resumen de cualquier equipo que proteja el Core en el panel Equipos protegidos.

NOTE: Un agente de software actúa por parte del usuario para realizar acciones específicas. Los equipos protegidos a veces se denominan Agents, ya que ejecutan el software Rapid Recovery Agent para facilitar las copias de seguridad y la replicación en el Rapid Recovery Core.

Puede ver el estado, el nombre para mostrar de cada equipo, qué repositorio utiliza, la fecha y la hora de la última instantánea, cuántos puntos de recuperación hay en el repositorio para el equipo, así como la cantidad total de espacio de almacenamiento que utilizan las instantáneas en el repositorio.

Para administrar aspectos de cualquier equipo protegido, empiece desplazándose hasta el equipo que desee ver, configurar o administrar. Desde la página **Inicio**, hay tres maneras de desplazarse hasta un equipo protegido:

- Puede hacer clic en la dirección IP o nombre para mostrar de cualquier equipo protegido del panel Equipos protegidos. Esta acción le llevará a la página Resumen del equipo protegido seleccionado.
- En el área de navegación de la izquierda, puede hacer clic en el título del menú **Equipos protegidos**. Aparecerá la página **Equipos protegidos**. En esta página puede ver información de resumen sobre cada equipo. Para obtener una descripción detallada de esta página, consulte Visualización de información de resumen de un equipo protegido.
- En el menú Equipos protegidos del área de navegación de la izquierda, puede hacer clic en la dirección IP o en el nombre para mostrar de cualquier equipo protegido. Esta acción le llevará a la página **Resumen** del equipo protegido seleccionado. Para obtener una descripción detallada de esta página, consulte Visualización de información de resumen de un equipo protegido.

Visualización de eventos de un equipo protegido

En la página **Eventos**, puede ver los trabajos que se han realizado o que están en curso en el equipo protegido que seleccionó. Los botones de la parte superior de la página le permiten navegar a listas de trabajos en cada una de las tres categorías de actividades:

- **Tareas.** Un trabajo que Rapid Recovery debe realizar para funcionar correctamente.
- **Alertas.** Una notificación relacionada con una tarea o evento que incluye errores y advertencias.
- **Diario.** Un compuesto de todas las tareas y alertas del equipo protegido.

La siguiente tabla incluye las descripciones de cada elemento de la página **Eventos**.

Tabla 173. Elementos de la página Eventos

Elemento de la IU	Descripción
Palabra clave de la búsqueda	Le permite buscar un elemento específico dentro de cada categoría. Solo disponible para tareas.
De	Para restringir los resultados, puede introducir una fecha en la que empezar la búsqueda. Solo disponible para tareas.
A	Para restringir los resultados, puede introducir una fecha en la que detener la búsqueda. Solo disponible para tareas.
Iconos de estado	Cada icono representa un estado de trabajo diferente. En el caso de alertas y tareas, al hacer clic en uno de los iconos podrá filtrar la lista por ese estado, generando

Elemento de la IU	Descripción
	básicamente un informe. Al hacer clic en el icono una segunda vez elimina el filtro para ese estado. Puede filtrar por más de un estado. Los estados incluyen: • **Activo.** Un trabajo que está en curso. • **En cola.** Un trabajo que está esperando que otro trabajo finalice antes de poder iniciarse. • **Esperando.** Un trabajo que está esperando su aprobación o finalización, como una unidad de inicialización. (Para obtener más información acerca de las unidades de inicialización, consulte Replicación.) • **Finalizado.** Un trabajo que se ha realizado correctamente. • **Con fallo.** Un trabajo que ha fallado y no se completó.
Icono de servicio	Este botón agrega trabajos de servicios a la lista de trabajos. Cuando hace clic en este icono, aparece un icono de servicio más pequeño en cada icono de estado, que le permite filtrar por trabajos de servicio que tienen esos estados (si los hubiera). Los ejemplos de trabajos de servicios incluyen la eliminación de archivos de índice o retirar un equipo de la protección.
Lista desplegable Tipo de exportación	La lista desplegable incluye los formatos con los que puede exportar el informe del evento. Solo disponible para tareas. Incluye los siguientes formatos: • PDF • HTML • CSV • XLS • XLSX
(icono Exportar)	Convierte el informe del evento al formato que seleccionó. Solo disponible para tareas.
Selección de página	Los informes de eventos pueden incluir varios trabajos en múltiples páginas. Los números y las flechas de la parte inferior de la página **Eventos** permiten navegar a las páginas adicionales del informe.

La página **Eventos** muestra todos los eventos de una tabla. La siguiente tabla enumera la información que se muestra para cada elemento.

Tabla 174. Información detallada para la tabla de resumen de los eventos

Elemento de la IU	Descripción
Estado	Muestra el estado de la tarea, alerta o el elemento diario. Está disponible para las alertas o los elementos diario; haga clic en el encabezado para filtrar los resultados por estado.
Nombre	Nombre está disponible solo para las tareas. Este campo de texto enumera el tipo de tarea que se ha completado para este equipo protegido. Algunos ejemplos incluyen la transferencia de volúmenes, el mantenimiento del repositorio, la consolidación, la realización de comprobaciones de la capacidad de montaje, la realización de comprobaciones de suma de comprobación, y así sucesivamente.

Elemento de la IU	Descripción
Hora de inicio	Disponible para las tareas, alertas y los elementos diario. Muestra la fecha y la hora en las que se inició el trabajo o la tarea.
Hora de finalización	Solo disponible para tareas. Muestra la fecha y la hora en las que se completó la tarea.
Detalles del trabajo	Solo disponible para tareas. Se abre el cuadro de diálogo **Supervisar tarea activa** por lo que puede ver los detalles de un trabajo específico o una tarea. Estos detalles incluyen una ID para el trabajo, la velocidad a la que el Core transfirió los datos (si corresponde), el tiempo transcurrido para que el trabajo se complete, el trabajo total en cantidad de gigabytes y cualquier tarea secundaria relacionada con el trabajo.
Mensaje	Disponible para las alertas y los elementos diario. Este campo de texto proporciona un mensaje descriptivo de la alerta o el elemento diario.

Visualización del menú Más de un equipo protegido

El menú **Más** ofrece opciones adicionales para ayudar a administrar los equipos protegidos seleccionados. Para acceder a estas herramientas, haga clic en el menú desplegable Más y seleccione una de las opciones descritas en la tabla siguiente.

Tabla 175. Herramientas a las que se puede acceder desde la opción Más de un equipo protegido

Elemento de la IU	Descripción
Información del sistema	Muestra información sobre el equipo protegido, la información del sistema, los volúmenes, los procesadores, los adaptadores de red y las direcciones IP de este equipo. Para obtener más información, consulte Visualización de la información del sistema de un equipo protegido.
Montajes	Puede ver o desmontar volúmenes montados localmente desde el panel Montajes locales. Puede ver o desmontar volúmenes montados empleando Local Mount Utility desde el panel Montajes remotos. Para obtener información sobre cómo desmontar volúmenes, consulte Desmontaje de puntos de recuperación. Para obtener información sobre el montaje de un punto de recuperación de forma local, consulte Montaje de un punto de recuperación o Montaje de un volumen de punto de recuperación en un equipo Linux, respectivamente.
Política de retención	Le permite especificar una política de retención para el equipo seleccionado. Puede optar por utilizar la política predeterminada del Core o por diferenciar la política de retención únicamente de este equipo. Para obtener más información, consulte Personalización de la configuración de la política de retención de un equipo protegido.
Notificaciones	Le permite especificar un grupo de notificaciones personalizadas de eventos relacionados con el equipo seleccionado. Esto no modifica las notificaciones ya

Elemento de la IU	Descripción
	configuradas en el Core. Para obtener más información, consulte Configuración de grupos de notificación.
 Registro de agentes	Le permite descargar y visualizar el archivo de registro de un equipo protegido mediante el software Rapid Recovery Agent. Para obtener más información, consulte Descarga y visualización del archivo de registro de un equipo protegido.

Third-party contributions

This product contains the third-party components listed below. For third-party license information, go to http://quest.com/legal/license-agreements.aspx. Source code for components marked with an asterisk (*) is available at http://opensource.quest.com.

Table 176. List of third-party contributions

Component	License or acknowledgment	Notes
AlphaFS 2.0.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
AlphaVSS 1.2.4000	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ANTLR 3.3.3	BSD ANTLR 3	Copyright (c) 2003-2007, Terence Parr A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ANTLR 4.0.2	BSD ANTLR 4	Copyright (c) 2012 Terence Parr and Sam Harwell A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
AWS SDK for .NET 3.3.37	Apache 2.0	A copy of this license can be found at Apache 2.0.
Azure SDK for .NET 2.4	Apache 2.0	A copy of this license can be found at Apache 2.0
Bootstrap 3.0.0	Apache 2.0	Bootstrap.js by @fat & @mdo Copyright 2012 Twitter, Inc. A copy of this license can be found at Apache 2.0
Bundletransformer 1.9.138	Apache 2.0	Copyright (c) 2012-2015 Andrey Taritsyn A copy of this license can be found at Apache 2.0
Caliburn.Micro 2.0.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Castle Windsor 2.5.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
Chromium 43.0.2312	Chromium BSD License N/A	Copyright 2014 The Chromium Authors. All rights reserved. A copy of this license can be found at Chromium BSD License N/A.

Component	License or acknowledgment	Notes
CLAP 4.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Common Library for Hyak Code Generator 1.0.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
curlpp 0.7.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
EcmaScript.Net 1.0.1	Mozilla Public License (MPL) 1.1	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Far Manager 3.0.4242	Far Manager BSD License N/A	Copyright (c) 1996 Eugene Roshal Copyright (c) 2000 Far Group All rights reserved. A copy of this licenses can be found at Far Manager BSD License N/A.
fio 2.18*	GPL (GNU General Public License) 2.0	This component is not used in the application. It is provided with the product for customer convenience. A copy of this license can be found at GPL (GNU General Public License) 2.0.
FlotCharts 0.8.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Google APIs Client Library for .NET 1.9.2	Apache 2.0	Copyright 2011 Google Inc A copy of this license can be found at Apache 2.0.
HTML Renderer 1.5.0.6	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
html5-placeholder-shim.jquery.js 1.0.58	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ISOLINUX 4.05 20120131*	GPL (GNU General Public License) 2.0	A copy of this license can be found at GPL (GNU General Public License) 2.0.
JavaScriptEngineSwitcher 1.2.4	Apache 2.0	Copyright (c) 2013-2015 Andrey Taritsyn A copy of this license can be found at Apache 2.0.
jqGrid 4.4.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jqrowl 1.2.6	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
JQuery 1.8.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery File Upload Plugin 5	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery knob 1.2.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Templates 1.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Templates 1.0.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
JQuery UI 1.9.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Validation 1.9.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Viewport 1.0.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Viewport 1.0.0.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.fileDownload 1.3.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.hotkeys 0.7.9	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.mCustomScrollbar 3.0.7	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquerey.mousewheel 3.1.12	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.splitter 0.14.0	GNU LGPL Version 3, 29 June 2007	Copyright (C) 2010-2013 Jakub Jankiewicz A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.tagsinput 1.3.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Json.NET 4.5	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
jsTree 1.0-rc3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.11.3*	GNU LGPL Version 3, 29 June 2007	Copyright © 2006–2015 SUSE LLC and contributors. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.12*	GNU LGPL Version 3, 29 June 2007	Copyright © 2002 Red Hat, Inc. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.15*	GNU LGPL Version 3, 29 June 2007	Copyright © 2015 Canonical Ltd. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.17*	GNU LGPL Version 3, 29 June 2007	Copyright © 2002 Red Hat, Inc. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.19*	GNU LGPL Version 3, 29 June 2007	Copyright © 2006–2015 SUSE LLC and contributors. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Libc.so.6 2.7*	LGPL (GNU Lesser General Public License) 2.1	A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
libext2fs 1.42.12*	GNU Lesser General Public License 2.1	Copyright (C) 1993, 1994, 1995, 1996 Theodore Ts'o. A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
libssh2 1.4.3	BSD-style N/A	Portions Copyright 2002-2010 Atsuhiko Yamanaka, JCraft,Inc. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Log4Net 1.2.10	Apache 2.0	A copy of this license can be found at Apache 2.0.
MarkdownSharp 1.13	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
matchMedia 2.72	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
memtest86+ 4.20*	GPL (GNU General Public License) 2.0	A copy of this license can be found at GPL (GNU General Public License) 2.0.
Microsoft Azure Compute	Apache 2.0	A copy of this license can be found at Apache 2.0.

Component	License or acknowledgment	Notes
Management Library 12.0.0		
Microsoft Reactive Extensions for .NET 2.1	Apache 2.0	A copy of this license can be found at Apache 2.0.
Moment.js 2.6.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
MongoDB 2.0.6*	GNU Affero GPL 3.0	A copy of this license can be found at GNU AFFERO GENERAL PUBLIC LICENSE
MongoDB 10gen driver 2.4.1	Apache 2.0	A copy of this license can be found at Apache 2.0.
Mono 5.2*	LGPL (GNU Lesser General Public License) 2.1	Copyright (C) 1991, 1999 Free Software Foundation, Inc. A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
MsieJavaScriptEngine 1.4.3*	Mozilla Public License (MPL) 1.1	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
NBD various*	GPL (GNU General Public License) 2.0	This component is not used in the application. It is provided with the product for customer convenience. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
NDesk.Options 0.2.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Newtonsoft.Json.dll 6.0.8	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
NLog 4.4.12	BSD - Kowalski 2011	Copyright (c) 2004-2011 Jaroslaw Kowalski <jaak@jkowwalski.net>. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
OpenSSL 1.1.0e	OpenSSL 1.0	This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved. A copy of this license can be found at OpenSSL 1.0.
OpenStack.NET 1.4.0.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
PowerCollections 2007*	Eclipse Public License 1.0	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Prism 4.0	Microsoft patterns & practices license N/A	Contains software or other content adapted from Microsoft patterns & practices ObjectBuilder, © 2006 Microsoft Corporation. All rights reserved. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ProductionStackTrace 1.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Protobuf-net 2.0.0.627	Apache 2.0	A copy of this license can be found at Apache 2.0.
PuTTY 0.63	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Quartz.NET 2.1.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
Raphaël—JavaScript Library 2.1.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
RazorGenerator 2.1	Apache 2.0	A copy of this license can be found at Apache 2.0.
Resize Floating Popup Control Revision 3	Code Project Open License (CPOL) 1.02	A copy of this license can be found at Code Project Open License (CPOL) 1.02 .
respond.js 1.3.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
SignalR 1.2.2	Apache 2.0	Copyright (c) .NET Foundation. All rights reserved. A copy of this license can be found at Apache 2.0.
SimpleRestServices 1.2.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
SimpleRestServices 1.3.0.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Sparsehash 1.11	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
SSH.Net 2013.4.7	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
TextFileEncodingDetector 1.0	BSD TextFileEncodingDetector 1.0	Copyright 2002-2008 Xiph.org Foundation Copyright 2002-2008 Jean-Marc Valin Copyright 2005-2007 Analog Devices Inc. Copyright 2005-2008 Commonwealth Scientific and Industrial Research Organisation (CSIRO) Copyright 1993, 2002, 2006 David Rowe Copyright 2003 EpicGames Copyright 1992-1994 Jutta Degener, Carsten Bormann A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
trip 2.1.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Tri-state tree view Revision 9 (30-May-2011)	Code Project Open License (CPOL) 1.02	A copy of this license can be found at Code Project Open License (CPOL) 1.02 .
Virtual Box SDK 4.2.14*	LGPL (GNU Lesser General Public License) 2.1	c 2004-2015 Oracle Corporation A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
WebGrease 1.5.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
Yahoo! UI Library: YUI Compressor .Net 2.7.0	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
zlib 1.2.5	zlib 1.2.5	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Apache 2.0

License Text

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places:

within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Chromium BSD License N/A

License Text

Copyright 2014 The Chromium Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code Project Open License (CPOL) 1.02

License Text

Preamble

This License governs Your use of the Work. This License is intended to allow developers to use the Source Code and Executable Files provided as part of the Work in any application in any form.

The main points subject to the terms of the License are:

Source Code and Executable Files can be used in commercial applications;

Source Code and Executable Files can be redistributed; and

Source Code can be modified to create derivative works.

No claim of suitability, guarantee, or any warranty whatsoever is provided. The software is provided "as-is".

The Article(s) accompanying the Work may not be distributed or republished without the Author's consent

This License is entered between You, the individual or other entity reading or otherwise making use of the Work licensed pursuant to this License and the individual or other entity which offers the Work under the terms of this License ("Author").

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CODE PROJECT OPEN LICENSE ("LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HEREIN, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE AUTHOR GRANTS YOU THE RIGHTS CONTAINED HEREIN IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO ACCEPT AND BE BOUND BY THE TERMS OF THIS LICENSE, YOU CANNOT MAKE ANY USE OF THE WORK.

Definitions.

"Articles" means, collectively, all articles written by Author which describes how the Source Code and Executable Files for the Work may be used by a user.

"Author" means the individual or entity that offers the Work under the terms of this License.

"Derivative Work" means a work based upon the Work or upon the Work and other pre-existing works.

"Executable Files" refer to the executables, binary files, configuration and any required data files included in the Work.

"Publisher" means the provider of the website, magazine, CD-ROM, DVD or other medium from or by which the Work is obtained by You.

"Source Code" refers to the collection of source code and configuration files used to create the Executable Files.

"Standard Version" refers to such a Work if it has not been modified, or has been modified in accordance with the consent of the Author, such consent being in the full discretion of the Author.

"Work" refers to the collection of files distributed by the Publisher, including the Source Code, Executable Files, binaries, data files, documentation, whitepapers and the Articles.

"You" is you, an individual or entity wishing to use the Work and exercise your rights under this License.

Fair Use/Fair Use Rights. Nothing in this License is intended to reduce, limit, or restrict any rights arising from fair use, fair dealing, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

License Grant. Subject to the terms and conditions of this License, the Author hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

You may use the standard version of the Source Code or Executable Files in Your own applications.

You may apply bug fixes, portability fixes and other modifications obtained from the Public Domain or from the Author. A Work modified in such a way shall still be considered the standard version and will be subject to this License.

You may otherwise modify Your copy of this Work (excluding the Articles) in any way to create a Derivative Work, provided that You insert a prominent notice in each changed file stating how, when and where You changed that file.

You may distribute the standard version of the Executable Files and Source Code or Derivative Work in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution.

The Articles discussing the Work published in any form by the author may not be distributed or republished without the Author's consent. The author retains copyright to any such Articles. You may use the Executable Files and Source Code pursuant to this License but you may not repost or republish or otherwise distribute or make available the Articles, without the prior written consent of the Author.

Any subroutines or modules supplied by You and linked into the Source Code or Executable Files this Work shall not be considered part of this Work and will not be subject to the terms of this License.

Patent License. Subject to the terms and conditions of this License, each Author hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, import, and otherwise transfer the Work.

Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

You agree not to remove any of the original copyright, patent, trademark, and attribution notices and associated disclaimers that may appear in the Source Code or Executable Files.

You agree not to advertise or in any way imply that this Work is a product of Your own.

The name of the Author may not be used to endorse or promote products derived from the Work without the prior written consent of the Author.

You agree not to sell, lease, or rent any part of the Work. This does not restrict you from including the Work or any part of the Work inside a larger software distribution that itself is being sold. The Work by itself, though, cannot be sold, leased or rented.

You may distribute the Executable Files and Source Code only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy of the Executable Files or Source Code You distribute and ensure that anyone receiving such Executable Files and Source Code agrees that the terms of this License apply to such Executable Files and/or Source Code. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute the Executable Files or Source Code with any

technological measures that control access or use of the Work in a manner inconsistent with the terms of this License.

You agree not to use the Work for illegal, immoral or improper purposes, or on pages containing illegal, immoral or improper material. The Work is subject to applicable export laws. You agree to comply with all such laws and regulations that may apply to the Work after Your receipt of the Work.

Representations, Warranties and Disclaimer. THIS WORK IS PROVIDED "AS IS", "WHERE IS" AND "AS AVAILABLE", WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OR GUARANTEES. YOU, THE USER, ASSUME ALL RISK IN ITS USE, INCLUDING COPYRIGHT INFRINGEMENT, PATENT INFRINGEMENT, SUITABILITY, ETC. AUTHOR EXPRESSLY DISCLAIMS ALL EXPRESS, IMPLIED OR STATUTORY WARRANTIES OR CONDITIONS, INCLUDING WITHOUT LIMITATION, WARRANTIES OR CONDITIONS OF MERCHANTABILITY, MERCHANTABLE QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY OF TITLE OR NON-INFRINGEMENT, OR THAT THE WORK (OR ANY PORTION THEREOF) IS CORRECT, USEFUL, BUG-FREE OR FREE OF VIRUSES. YOU MUST PASS THIS DISCLAIMER ON WHENEVER YOU DISTRIBUTE THE WORK OR DERIVATIVE WORKS.

Indemnity. You agree to defend, indemnify and hold harmless the Author and the Publisher from and against any claims, suits, losses, damages, liabilities, costs, and expenses (including reasonable legal or attorneys' fees) resulting from or relating to any use of the Work by You.

Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL THE AUTHOR OR THE PUBLISHER BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK OR OTHERWISE, EVEN IF THE AUTHOR OR THE PUBLISHER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Termination.

This License and the rights granted hereunder will terminate automatically upon any breach by You of any term of this License. Individuals or entities who have received Derivative Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 6, 7, 8, 9, 10 and 11 will survive any termination of this License.

If You bring a copyright, trademark, patent or any other infringement claim against any contributor over infringements You claim are made by the Work, your License from such contributor to the Work ends automatically.

Subject to the above terms and conditions, this License is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, the Author reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

Publisher. The parties hereby confirm that the Publisher shall not, under any circumstances, be responsible for and shall not have any liability in respect of the subject matter of this License. The Publisher makes no warranty whatsoever in connection with the Work and shall not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. The Publisher reserves the right to cease making the Work available to You at any time without notice

Miscellaneous

This License shall be governed by the laws of the location of the head office of the Author or if the Author is an individual, the laws of location of the principal place of residence of the Author.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this License, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed herein. There are no understandings, agreements or representations with respect to the Work not specified herein. The Author

shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Author and You.

Far Manager BSD License N/A

License Text

Copyright (c) 1996 Eugene Roshal

Copyright (c) 2000 Far Group

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions

are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

EXCEPTION:

Far Manager plugins that use only the following header files from this distribution (none or any): farcolor.hpp, farkeys.hpp, plugin.hpp, farcolorW.pas, farkeysW.pas and pluginW.pas; can be distributed under any other possible license with no implications from the above license on them.

GNU AFFERO GENERAL PUBLIC LICENSE

Version 3, 19 November 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/> Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU Affero General Public License is a free, copyleft license for software and other kinds of works, specifically designed to ensure cooperation with the community in the case of network server software.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, our General Public Licenses are intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

Developers that use our General Public Licenses protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License which gives you legal permission to copy, distribute and/or modify the software.

A secondary benefit of defending all users' freedom is that improvements made in alternate versions of the program, if they receive widespread use, become available for other developers to incorporate. Many developers of free software are heartened and encouraged by the resulting cooperation. However, in the case of software used on network servers, this result may fail to come about. The GNU General Public License permits making a modified version and letting the public access it on a server without ever releasing its source code to the public.

The GNU Affero General Public License is designed specifically to ensure that, in such cases, the modified source code becomes available to the community. It requires the operator of a network server to provide the source code of the modified version running there to the users of that server. Therefore, public use of a modified version, on a publicly accessible server, gives the public access to the source code of the modified version.

An older license, called the Affero General Public License and published by Affero, was designed to accomplish similar goals. This is a different license, not a version of the Affero GPL, but Affero has released a new version of the Affero GPL which permits relicensing under this license.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU Affero General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component,

and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from

a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms. "Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available

network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Remote Network Interaction; Use with the GNU General Public License.

Notwithstanding any other provision of this License, if you modify the Program, your modified version must prominently offer all users interacting with it remotely through a computer network (if your version supports such interaction) an opportunity to receive the Corresponding Source of your version by providing access to the Corresponding Source from a network server at no charge, through some standard or customary means of facilitating copying of software. This Corresponding Source shall include the Corresponding Source for any work covered by version 3 of the GNU General Public License that is incorporated pursuant to the following paragraph.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the work with which it is combined will remain governed by version 3 of the GNU General Public License.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU Affero General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU Affero General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU Affero General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU Affero General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU Affero General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Affero General Public License for more details.

You should have received a copy of the GNU Affero General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If your software can interact with users remotely through a computer network, you should also make sure that it provides a way for users to get its source. For example, if your program is a web application, its interface could display a "Source" link that leads users to an archive of the code. There are many ways you could offer source, and different solutions will be better for different programs; see section 13 for the specific requirements.

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU AGPL, see <http://www.gnu.org/licenses/>.

GPL (GNU General Public License) 2.0

License Text

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its

contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS"

WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

LGPL (GNU Lesser General Public License) 2.1

License Text

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is

especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will

automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

OpenSSL 1.0

License Text

License

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

==========

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

/

Quiénes somos

Somos algo más que un nombre

Nos esforzamos constantemente para que la tecnología de la información funcione mejor para usted. Por eso creamos soluciones de software orientadas a la comunidad que le ayuden a reducir el tiempo dedicado a la administración de TI y a aumentar el dedicado a la innovación empresarial. Le ayudamos a modernizar su centro de datos y pasar a la nube con mayor celeridad; además, le ofrecemos la experiencia, seguridad y accesibilidad que necesita para hacer crecer una empresa basada en datos. En Quest invitamos a la comunidad global a formar parte de nuestras innovaciones y nos comprometemos firmemente a garantizar la satisfacción del cliente, por lo que continuamos ofreciendo soluciones de impacto real en nuestros clientes actuales y creando un legado del que nos sentimos orgullosos. Desafiamos el statu quo transformándonos en una nueva empresa de software. Y, con usted como asociado, trabajamos sin descanso para garantizar que su tecnología de la información esté diseñada por usted y para usted. Esta es nuestra misión, y estamos en esto juntos. Bienvenido al nuevo Quest. Está invitado: Join the Innovation™.

Nuestra marca, nuestra visión. Juntos.

Nuestro logotipo refleja nuestra historia: innovación, comunidad y asistencia. Una parte importante de esta historia comienza con la letra Q. Es un círculo perfecto que representa nuestro compromiso con la solidez y la precisión tecnológica. El espacio dentro de la Q simboliza nuestra necesidad de añadir la pieza faltante, la comunidad, al nuevo Quest.

Cómo ponerse en contacto con Quest

Para tratar cuestiones relacionadas con las ventas u otro tipo de preguntas, visite https://www.quest.com/contact.

Recursos de asistencia técnica

La asistencia técnica está disponible para los clientes de Quest con un contrato de mantenimiento válido y para clientes con versiones de prueba. Puede acceder al portal Quest Support en Https://support.quest.com.

El portal de asistencia proporciona herramientas de autoayuda que puede utilizar para resolver problemas de forma rápida e independiente, 24 horas, 365 días al año. El portal de asistencia le permite:

- Enviar y administrar una solicitud de servicio.
- Ver artículos de la base de conocimientos.
- Suscribirse a las notificaciones de productos.
- Descargar software y documentación técnica.
- Ver vídeos paso a paso.
- Participar en discusiones de comunidad.
- Chatear con los ingenieros de asistencia en línea.
- Ver servicios que le ayuden con nuestro producto

Glosario

Agent

Rapid Recovery Agent es un software instalado en un equipo físico o virtual que permite que se incorpore a la protección en el Rapid Recovery Core.

imagen base

La primera transferencia de copia de seguridad guardada en el Core se denomina una instantánea de imagen base. Todos los datos de todos los volúmenes especificados (incluido el sistema operativo, las aplicaciones y la configuración) se guardan en el Core. Para obtener más información, consulte Instantánea.

suma de comprobación

Una suma de comprobación es una función que crea bloques de datos que se utilizan para detectar errores accidentales que se crean durante la transmisión o almacenamiento.

clúster

Consulte Clúster de failover de Windows.

Cluster Continuous Replication (CCR)

Solución de clúster de failover de almacenamiento no compartido que utiliza la tecnología incluida de registro asíncrono incorporada para crear y mantener una copia de cada grupo de almacenamiento en un segundo servidor en un clúster de failover. CCR está diseñado para ser una solución de uno o dos centros de datos, proporcionando ambos alta disponibilidad y confianza del sitio. Es uno de los dos tipos de implementaciones de Servidor de buzón en clúster (CMS) disponibles en Exchange 2007.

nodo de clúster

Un equipo individual es parte de un clúster de failover de Windows.

compresión

La Storage Networking Industry Association (SNIA) define la compresión como el proceso de cifrado de datos para reducir su tamaño.

Core

El Rapid Recovery Core es el componente central de la arquitectura de Rapid Recovery. El Core proporciona los servicios esenciales de copia de seguridad, recuperación, retención, replicación, archivado y administración. En el contexto de la replicación, el Core también se denomina source core (Core de origen). El Core de origen es el Core que origina, y el Core de destino es el destino (otro Rapid Recovery Core en su propio servidor exclusivo, donde se replican equipos y clústeres protegidos).

Core Console

La Core Console de Rapid Recovery es una interfaz basada en web que permite administrar totalmente el Core de Rapid Recovery.

grupo de disponibilidad de base de datos (DAG)

Un conjunto de hasta 16 servidores Microsoft Exchange Server 2010 Mailbox que proporcionan recuperación a nivel de base de datos, automática, a partir de una base de datos, servidor o error de red. Los DAG utilizan replicación continua y un subconjunto de tecnologías de clústering de failover en Windows para proporcionar alta disponibilidad y fiabilidad del sitio. Servidores Mailbox en un monitor DAG entre ellos para errores. Cuando se añade un servidor Mailbox a un DAG, funciona con los otros servidores del DAG para proporcionar recuperación automática a nivel de base de datos frente a errores de bases de datos.

cifrado

Los datos se cifran para que sólo sean accesibles a los usuarios autorizados que tengan la clave de descodificación adecuada. Los datos se cifran mediante AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC). En CBC, a cada bloque de datos se le aplica la disyunción exclusiva (XOR) con el bloque de texto cifrado previo antes del cifrado, de modo que cada bloque de texto cifrado nuevo depende de todos los bloques de texto sin formato precedentes. Se utiliza una frase de contraseña como vector de inicialización.

evento

Un evento es un proceso que el Core ha registrado. Los eventos se pueden ver en la Core Console haciendo clic en el icono  (Eventos) de la barra de iconos. La vista predeterminada que aparece cuando hace clic en este icono muestra la página **Tareas**. Esta vista muestra los eventos relacionados con un trabajo. Los eventos por los que recibe una notificación se pueden ver en la página **Alertas**. En la página **Diario** aparece un registro de todos los eventos. Puede personalizar la notificación de cualquier evento si configura o modifica los grupos de notificación existentes. Esta acción aumenta la prioridad del evento al mostrarla en la página de **Alertas**. A los miembros de un grupo de notificaciones se les notificará de los eventos con el método de notificación que se ha establecido en las opciones de notificación del grupo.

desduplicación global

La Storage Networking Industry Association (SNIA) define la desduplicación de datos como la sustitución de varias copias de datos (en niveles variables de granularidad) con referencias a una copia compartida para ahorrar espacio de almacenamiento o ancho de banda. El administrador de volúmenes de Rapid Recovery realiza la desduplicación global de datos en un volumen lógico. El nivel de granularidad de la desduplicación es de 8 KB. El ámbito de desduplicación de Rapid Recovery se limita a los equipos protegidos con el mismo repositorio y clave de cifrado.

instantánea incremental

Las instantáneas incrementales son copias de seguridad que constan únicamente de datos cambiados en el equipo protegido desde la última copia de seguridad. Se guardan en el Core de forma habitual, en base al intervalo definido (por ejemplo, cada 60 minutos). Para obtener más información, consulte Instantánea.

clave de licencia

Una clave de licencia es un método que se utiliza para registrar su software o dispositivo de Rapid Recovery. (También puede utilizar un archivo de licencia). Puede obtener claves o archivos de licencia cuando se registre en el Portal de licencias de Rapid Recovery para una cuenta. Para obtener más información, consulte Portal de Licencias.

Portal de licencias

El Portal de licencias de Rapid Recovery es una interfaz web donde los usuarios y socios pueden descargar el software, registrar los dispositivos de Rapid Recovery y administrar las suscripciones de licencias. Los usuarios del Portal de licencias pueden registrar cuentas, descargar el software de Core y Agent de Rapid Recovery, administrar grupos, seguir la actividad de grupos, registrar dispositivos integrados, registrar equipos, invitar a usuarios y generar informes. Para obtener más información, consulte la *Rapid Recovery License Portal User Guide* (Guía de usuario del Portal de licencias de Rapid Recovery).

Live Recovery

Live Recovery de Rapid Recovery es una tecnología de recuperación instantánea para máquinas virtuales o servidores. Proporciona acceso casi continuo a volúmenes de datos en un servidor virtual o físico, y permite recuperar un volumen completo con RTO cercanos a cero y unos RPO de minutos.

Utilidad de montaje local

Local Mount Utility (LMU) es una aplicación descargable que permite montar un punto de recuperación en un Rapid Recovery Core desde cualquier equipo.

truncamiento del registro

El truncamiento del registro es una función que elimina registros del registro de transacciones. Para un equipo SQL Server, cuando fuerza el truncamiento de los registros de SQL Server, este proceso simplemente identifica el espacio libre en el servidor SQL. Para un servidor de base de datos de Oracle, cuando trunca registros (ya sea de forma programada o manual a petición), los registros de archivos se eliminan para liberar espacio. Del

mismo modo, cuando fuerza el truncamiento de los registros de Exchange Server, esta acción libera espacio en el servidor Exchange.

roles de administración

La Consola de administración central de Rapid Recovery introduce un nuevo concepto de roles de administración que permiten dividir la responsabilidad administrativa entre datos de confianza y administradores de servicio junto con el control de acceso para permitir una delegación de la administración segura y eficaz.

capacidad de montaje

La capacidad de montaje de Exchange es una función de detección de corrupción que alerta a los administradores de posibles errores y asegura que todos los datos en servidores Exchange se recuperan correctamente en el caso de un error.

Sistema de archivos de objeto

El almacén de objetos adaptable de Rapid Recovery es un componente de sistema de archivos de objeto. Trata a todos los bloques de datos, de los que se derivan las instantáneas, como objetos. Almacena, recupera, mantiene y replica esos objetos. Se ha diseñado para ofrecer rendimiento ampliable de entrada/salida (E/S) junto con desduplicación global de datos, cifrado y administración de retención. El Sistema de archivos de objeto interactúa directamente con tecnologías de almacenamiento estándar del sector.

frase de contraseña

Una frase de contraseña es una clave que se utiliza en el cifrado de datos. Si se pierde la frase de contraseña, los datos no se pueden recuperar.

caracteres prohibidos

Los caracteres prohibidos son caracteres que no deben utilizarse cuando se asigna un nombre a un objeto en la Rapid Recovery Core Console. Por ejemplo, cuando se define un nombre para mostrar para un equipo protegido, no utilice ninguno de los siguientes caracteres especiales:

Tabla 177. Caracteres prohibidos

Carácter	Nombre de carácter	Prohibido en
?	signo de interrogación	nombre para mostrar de equipo, clave de cifrado, repositorio, descripción de ruta de acceso
|	barra vertical	nombre para mostrar de equipo, clave de cifrado, repositorio, descripción de ruta de acceso
:	dos puntos	nombre para mostrar de equipo, clave de cifrado, repositorio El uso de este símbolo se admite cuando se especifica una ruta de acceso, como por ejemplo `c:\data`.
/	barra diagonal	nombre para mostrar de equipo, clave de cifrado, repositorio, descripción de ruta de acceso
\	barra diagonal inversa	nombre para mostrar de equipo, clave de cifrado, repositorio El uso de este símbolo se admite cuando se especifica una ruta de acceso local o de red, como, por ejemplo, `c:\data` o `\\ComputerName\SharedFolder\`
*	asterisco	nombre para mostrar de equipo, clave de cifrado, repositorio, descripción de ruta de acceso
"	comillas dobles	nombre para mostrar de equipo, clave de cifrado, repositorio, descripción de ruta de acceso

Carácter	Nombre de carácter	Prohibido en
<	cuña o paréntesis angular de apertura	nombre para mostrar de equipo, clave de cifrado, repositorio, descripción de ruta de acceso
>	cuña o paréntesis angular de cierre	nombre para mostrar de equipo, clave de cifrado, repositorio, descripción de ruta de acceso

frases prohibidas

Las frases prohibidas son frases (o conjuntos de caracteres) que no deben utilizarse para el nombre de ningún objeto en la Rapid Recovery Core Console porque están reservadas para el uso de sistemas operativos. La práctica recomendada es evitar el uso de estas frases siempre que sea posible. Por ejemplo, cuando se define un nombre para mostrar para un equipo protegido, no utilice ninguna de las siguientes frases:

Tabla 178. Frases prohibidas

Frase	Uso general	Prohibido en
con	consola	nombre para mostrar de equipo, clave de cifrado, repositorio, descripción de ruta de acceso
prn	puerto de impresora	nombre para mostrar de equipo, clave de cifrado
aux	puerto auxiliar	nombre para mostrar de equipo, clave de cifrado
nul	valor nulo	nombre para mostrar de equipo, clave de cifrado
com1, com2... a través de com9	puerto de comunicación	nombre para mostrar de equipo, clave de cifrado
lpt1, lpt2... a través de lpt9	puerto de terminal de impresión en línea	nombre para mostrar de equipo, clave de cifrado, repositorio, descripción de ruta de acceso

equipo protegido

Un equipo protegido, también llamado Agent, es un ordenador físico o una máquina virtual que está protegido en el Core de Rapid Recovery. Los datos de la copia de seguridad se transmiten del equipo protegido al repositorio especificado en el Core mediante un intervalo de protección predefinido. La imagen base transmite todos los datos a un punto de recuperación (incluido el sistema operativo, las aplicaciones y las configuraciones). Cada instantánea incremental posterior confirma solo los bloques cambiados en los volúmenes de disco especificados en el equipo protegido. Los equipos protegidos basados en software tienen el software Rapid Recovery Agent instalado. Algunas máquinas virtuales también pueden protegerse sin agentes con algunas limitaciones.

Rapid Recovery

Rapid Recovery establece un nuevo estándar para la protección de datos unificada gracias a que combina la copia de seguridad, la replicación y la recuperación en una única solución que se ha diseñado para que sea la

copia de seguridad más rápida y fiable de protección de máquinas virtuales (VM), así como de equipos físicos y entornos de nube.

quórum

Para un clúster de failover, el número de elementos debe estar en línea para que un clúster dado continúe la ejecución. Los elementos relevantes en este contexto son nodos de clúster. A este término también se le puede hacer referencia como recurso con capacidad para quórum seleccionado para mantener los datos de configuración necesarios para la recuperación del clúster. Estos datos contienen detalles de todos los cambios que se han aplicado a la base de datos de clústeres. El recurso de quórum suele ser accesible a otros recursos de clúster para que cualquier nodo de clúster tenga acceso a los cambios de base de datos más recientes. De forma predeterminada, sólo hay un recurso de quórum por clúster de servidor. Una configuración de quórum concreta (configuración para un clúster de failover) determina el punto en el que demasiados errores detendrán la ejecución del clúster.

puntos de recuperación

Los puntos de recuperación son una colección de instantáneas de varios volúmenes de disco. Por ejemplo, C:, D: y E:.

puntos de recuperación-solo equipo

Un equipo con puntos de recuperación únicamente es la representación en el Core de los puntos de recuperación de un equipo que anteriormente estaba protegido en el Core y se eliminó. Si quita la replicación, pero mantiene los puntos de recuperación, también da como resultado un equipo con puntos de recuperación únicamente. La información se puede ver y recuperar a nivel de archivos. No puede utilizar un equipo con puntos de recuperación únicamente para realizar una BMR o restaurar volúmenes completos, ni puede agregar más datos a un equipo con puntos de recuperación únicamente.

Core remoto

Un Core remoto representa un Core de Rapid Recovery al que se puede acceder a través de un equipo que no es de Core mediante Local Mount Utility o la Consola de administración central.

replicación

La replicación es el proceso de copia de puntos de recuperación de un Rapid Recovery Core y de transmisión de los mismos a otro Rapid Recovery Core con fines de recuperación tras desastres. El proceso requiere la existencia de una relación de emparejamiento origen-destino entre dos o más Cores. La replicación está gestionada por equipos protegidos. Se puede configurar cualquier equipo (o todos los equipos) protegido o replicado en un Core de origen para replicar en un Core de destino. Se trata de los puntos de recuperación que se copian al Core de destino.

repositorio

Un repositorio es una colección de imágenes base e instantáneas incrementales tomadas de los equipos protegidos de un Rapid Recovery Core. Los repositorios se deben crear en dispositivos de almacenamiento primarios rápidos. Los repositorios DVM se pueden almacenar en una ubicación local del equipo del Core, en cuyo caso solo está alojado en un sistema operativo Windows compatible. Se puede usar almacenamiento de conexión directa, una red de área de almacenamiento o un servidor conectado a la red con la capacidad adecuada.

API de REST

La transferencia de estado representativa (REST) es una arquitectura del software simple sin estado diseñada para la escalabilidad. Rapid Recovery utiliza esta arquitectura en sus interfaces de programación de aplicaciones (API) para automatizar y personalizar ciertas funciones y tareas. Hay un conjunto independiente de API de REST para la funcionalidad de CORE y de los equipos protegidos (Agent).

restaurar

El proceso de restaurar uno o más volúmenes de almacenamiento en un equipo a partir de puntos de recuperación guardados en el Rapid Recovery Core se conoce como realizar una restauración. Esto se conocía anteriormente como reversión.

retención

La retención define el tiempo durante el que las instantáneas de copia de seguridad de los equipos protegidos se almacenarán en el Rapid Recovery Core. La política de retención se ejecuta en los puntos de recuperación mediante el proceso de consolidación.

consolidación

El proceso de consolidación es un procedimiento de mantenimiento interno que se realiza de noche y que ejecuta la política de retención al reducir y eliminar los puntos de recuperación antiguos. Rapid Recovery reduce la consolidación solo a operaciones de metadatos.

inicialización

En la replicación, la transferencia inicial de las imágenes base desduplicadas e instantáneas incrementales de Agents protegidos, que pueden formar hasta cientos o miles de gigabytes de datos. La replicación inicial se puede inicializar en el Core de destino usando medios externos, lo que es útil para grandes conjuntos de datos o sitios con enlaces lentos.

clúster de servidor

Consulte Clúster de failover de Windows.

copia de seguridad de SharePoint

Una copia de seguridad de SharePoint es una copia de los datos que se utilizan para restaurar y recuperar los datos de un servidor SharePoint tras un fallo del sistema. Desde la copia de seguridad de SharePoint puede realizar la recuperación de la granja completa de SharePoint, o bien uno o más componentes de la granja.

clúster de copia única

Una solución de clúster de failover de almacenamiento, que utiliza una copia única de un grupo de almacenamiento en el almacenamiento que se comparte entre los nodos del clúster. Es uno de los dos tipos de implementaciones de Servidor de buzón en clúster (CMS) disponibles en Exchange 2007.

Smart Agent

El Rapid Recovery Smart Agent se instala en los equipos protegidos por el Rapid Recovery Core. El Smart Agent realiza el seguimiento de bloques cambiados en el volumen de discos y hace instantáneas de los bloques cambiados en un intervalo predefinido de protección.

instantánea

Una instantánea es un término habitual en el sector para referirse a la función de capturar y almacenar el estado de un volumen de disco en un punto determinado, mientras las aplicaciones se están ejecutando. La instantánea es crítica si se necesita recuperar el sistema debido a un corte de conexión o a un error del sistema. Las instantáneas de Rapid Recovery ofrecen reconocimiento por parte de la aplicación, lo cual significa que todos los registros de transacciones abiertas y transacciones en marcha se completan y que las memorias caché se vacían antes de crear la instantánea. Rapid Recovery utiliza Microsoft Volume Shadow Services (VSS) (Servicios de instantáneas de volumen de Microsoft) para facilitar instantáneas de la aplicación en estado coherente tras la interrupción.

conectabilidad SQL

La conectabilidad SQL es una ejecución de prueba dentro del Rapid Recovery Core para asegurarse de que todos los puntos de recuperación de SQL están libres de errores y disponibles para la copia de seguridad en caso de error.

copia de seguridad de SQL

Una copia de seguridad de SQL es una copia de los datos que se utilizan para restaurar y recuperar los datos de un servidor SQL tras un fallo del sistema. Desde la copia de seguridad de SQL puede realizar la recuperación de la base de datos completa de SQL, o bien uno o más componentes de la base de datos SQL.

copia de seguridad diferencial de SQL

Una copia de seguridad de la base de datos diferencial es una copia acumulativa de todos los cambios en los datos desde la última copia de seguridad completa de la base de datos SQL. Las copias de seguridad diferenciales son normalmente más rápidas de crear que las copias de seguridad completas de la base de datos, y reducen el número de registros de transacciones requeridos para recuperar la base de datos.

Core de destino

El Core de destino, que en ocasiones se denomina Core de réplica, es el Rapid Recovery Core que recibe los datos replicados (puntos de recuperación) desde el Core de origen.

Transport Layer Security

Transport Layer Security (TLS) es un moderno protocolo de red criptográfico diseñado para garantizar la seguridad de las comunicaciones a través de Internet. Este protocolo, definido por Internet Engineering Task Force, es el sucesor de Secure Sockets Layer (SSL). El término SSL sigue utilizándose de manera general, y los protocolos son interoperables (un cliente TLS puede degradar su nivel para comunicarse con un servidor SSL).

True Scale

True Scale es la arquitectura adaptable de Rapid Recovery.

Universal Recovery

La tecnología Rapid Recovery Universal Recovery ofrece una flexibilidad ilimitada para restaurar equipos. Permite realizar la recuperación monolítica para y desde cualquier plataforma física o virtual de su elección, así como actualizaciones de recuperación incrementales en máquinas virtuales desde cualquier origen físico o virtual. También permite realizar recuperaciones en el nivel de aplicación, elemento y objeto de archivos individuales, carpetas, correo electrónico, elementos de calendario, bases de datos y aplicaciones.

Verified Recovery

La tecnología Verified Recovery se utiliza para llevar a cabo pruebas automatizadas de recuperación y la verificación de copias de seguridad. Admite varios sistemas de archivos y servidores.

en espera virtual

El estado de espera virtual es un proceso que crea una copia idéntica en una máquina virtual de un equipo protegido. El equipo de origen original puede ser físico o virtual, pero el producto siempre es virtual. Puede crear un estado en espera virtual único a petición o puede definir requisitos para crear la VM arrancable y, constantemente, actualizarla después de capturar cada instantánea en el equipo protegido original.

Administrador de volúmenes

El administrador de volúmenes de Rapid Recovery administrada los objetos y los almacena y presenta como volumen lógico. Saca el máximo provecho de la arquitectura de canalización dinámica para ofrecer escalabilidad TruScale, paralelismo y modelo de entrada y salida (E/S) asíncrono para obtener un alto rendimiento con la mínima latencia de E/S.

etiquetado blanco

Rapid Recovery ofrece la posibilidad de que ciertos proveedores específicos de servicios de copia de seguridad y recuperación tras desastres utilicen Rapid Recovery como marca blanca o la personalicen con su propio logotipo. De ese modo, pueden llevarlo al mercado como un producto o un servicio propio.

La opción de utilizar Rapid Recovery como marca blanca solo está disponible para organizaciones cuyos acuerdos de licencia de Quest Software concedan explícitamente privilegios de cambio de marca. Igualmente, las opciones de licencia, sublicencia y/o redistribución de este software solo se conceden a las organizaciones con las que existe un acuerdo de licencia específico vigente que garantice dichos privilegios. Quest Software se reserva todos los derechos de Rapid Recovery. La opción de marca blanca no concede derechos de propiedad intelectual de Rapid Recovery a nadie. Para solicitar esta funcionalidad para su organización, póngase en contacto con su representante de Quest Software.

clúster de failover de Windows

Grupo de equipos independientes que funcionan de forma conjunta para aumentar la disponibilidad de las aplicaciones y servicios. Los servidores en clúster (denominados nodos) se conectan mediante cables físicos y también por software. Si falla uno de los nodos del clúster, otro nodo empezará a proporcionar servicio (este proceso se conoce como failover). El usuario detecta una serie de pequeñas caídas en el servicio. Rapid Recovery admite la protección de un número de tipos de clústeres de SQL Server y Exchange Server.