

DRS

Disaster
Recovery
Server



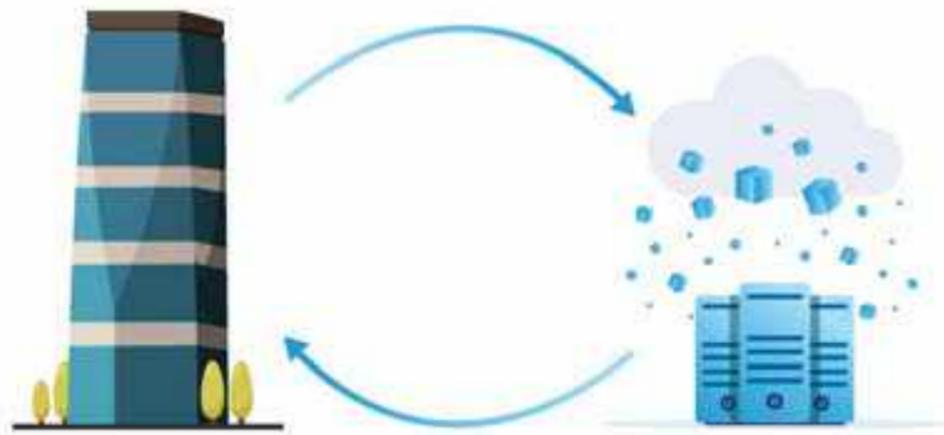
clouds7[®]
seguridad y gestión en la nube



Disaster Recovery Server

¿Qué es DRS?

Disaster Recovery Server (recuperación ante desastres de servidores): un servicio de Clouds7 que proporciona un servicio de recuperación ante desastres (DRaaS) orientado sobre todo a los clientes de SMB. Este servicio se integra sobre el servicio de copias de seguridad. Disaster Recovery Server es una solución rápida y estable para iniciar las copias exactas de sus equipos en el sitio en el cloud y trasladar la carga de trabajo de los equipos originales dañados a los equipos de recuperación en el cloud, en caso de desastre natural o causado por el ser humano.



La funcionalidad clave

- Gestionar el servicio Disaster Recovery Server Cloud desde una única consola.
- Ampliar hasta cinco redes locales al cloud mediante un túnel VPN seguro.
- Establecer la conexión al sitio en el cloud sin necesidad de implementar dispositivos VPN.
- Proteger su equipo con el uso de servidores de recuperación en el cloud.
- Proteger aplicaciones y dispositivos con el uso de servidores principales en el cloud.
- Realizar operaciones de recuperación ante desastres automáticas para copias de seguridad cifradas.
- Realizar una prueba de conmutación por error en la red aislada.

Requerimientos de software: Sistemas operativos compatibles

La protección con un servidor de recuperación se ha probado para los siguientes sistemas operativos:

- Centos 6.6, 7.1, 7.2, 7.3, 7.4, 7.5 y 7.6
- Debian 9
- Ubuntu 16.04, 18.04
- Windows Server 2008/2008 R2
- Windows Server 2012/2012 R2

Windows Server 2016: todas las opciones de instalación, excepto Nano Server.

Los sistemas operativos de los equipos de escritorio Windows no son compatibles con las condiciones de los productos de Microsoft.

Es posible que este software funcione con otros sistemas operativos de Windows y distribuciones Linux, pero no se lo podemos asegurar.

Plataformas de virtualización compatibles

La protección de equipos virtuales con un servidor de recuperación se ha probado para las siguientes plataformas de virtualización:

- VMware ESXi 5.1, 5.5, 6.0, 6.5
- Windows Server 2008 R2 con Hyper-V
- Windows Server 2012/2012 R2 con Hyper-V
- Microsoft Hyper-V Server 2012/2012 R2
- Windows Server 2016 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Microsoft Hyper-V Server 2016
- Equipos virtuales basados en Kernel (KVM)
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2
- Equipos virtuales de Azure

El dispositivo VPN se ha probado para las siguientes plataformas de virtualización:

- VMware ESXi 5.1, 5.5, 6.0, 6.5
- Windows Server 2008 R2 con Hyper-V
- Windows Server 2012/2012 R2 con Hyper-V
- Microsoft Hyper-V Server 2012/2012 R2
- Windows Server 2016 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Microsoft Hyper-V Server 2016

Puede que este software funcione con otras plataformas de virtualización y versiones distintas, pero no se lo podemos asegurar.

Limitaciones

Las siguientes plataformas y configuraciones no son compatibles con Disaster Recovery Cloud:

1. Plataformas no compatibles:

- Agentes para Virtuozzo.
- macOS.

2. Configuraciones no compatibles:

Microsoft Windows:

- Los discos dinámicos no son compatibles.
- Los sistemas operativos de los equipos de escritorio Windows no son compatibles (debido a las condiciones de los productos de Microsoft).
- El servicio Active Directory no es compatible con la replicación FRS.
- Los dispositivos extraíbles sin formato GPT o MBR (también llamado "superfloppy") no son compatibles.

Linux:

- Equipos Linux con volúmenes lógicos (LVM) o volúmenes formateados con el sistema de archivos XFS.
- Sistema de archivos sin tabla de partición.
- Un servidor de recuperación tiene una interfaz de red. Si el equipo original tiene varias interfaces de red, solo se emula una.
- Los servidores en la cloud no se cifran.

Configuración de la funcionalidad de recuperación ante desastres





Creación de un servidor principal

Requisitos previos

Se debe establecer uno de los tipos de conectividad en el sitio en el cloud.

Pasos para crear un servidor principal

1. Vaya a **Recuperación ante desastres > Servidores**.
2. Haga clic en **Crear servidor principal**.
3. Seleccione una plantilla para el nuevo equipo virtual.
4. Seleccione el número de núcleos virtuales y el tamaño de la RAM. Preste atención a los puntos del equipo que se encuentran junto a cada opción. El número de puntos del equipo indican el coste de funcionamiento del servidor principal por hora.
5. [Opcional] Cambie el tamaño de las unidades de discos virtuales. Si necesita más de un disco rígido, haga clic en **Agregar disco** y a continuación, especifique el nuevo disco.
6. Especifique la red de cloud en la que se incluirá el servidor principal.
7. Especifique la dirección IP que tendrá el servidor en la red de producción. La primera dirección IP libre de su red de producción se establece de forma predeterminada.
Nota: Si usa un servidor DHCP, agregue esta dirección IP a la lista de exclusión de servidores para evitar conflictos con la dirección IP.
8. [Opcional] Marque la casilla de verificación de acceso a Internet. De esta forma, el servidor principal tendrá **acceso a Internet**.
9. [Opcional] Marque la casilla de verificación de dirección **IP pública**. El hecho de que el servidor principal cuente con una dirección IP pública conlleva que se pueda acceder a él desde Internet. Si deja la casilla de verificación desmarcada, el servidor solo estará disponible en su red de producción. La dirección IP pública se mostrará cuando finalice la configuración. Los siguientes puertos se abren para realizar conexiones de entrada a direcciones IP públicas: TCP: 80, 443, 8088, 8443, UDP: 1194. Si necesita que se abran otros puertos, póngase en contacto con el equipo de soporte técnico.

10. [Opcional] Seleccione Establecer el **umbral de RPO**.

El umbral de RPO determina el intervalo temporal máximo permitido entre el último punto de recuperación y el momento presente. El valor se puede establecer entre 15 y 60 minutos, 1 y 24 horas y 1 y 14 días.

11. Defina el nombre del servidor principal.

12. [Opcional] Especifique una descripción para el servidor principal.

13. Haga clic en **Crear**.

El servidor principal estará disponible en la red de producción. Puede gestionar el servidor mediante su consola, el escritorio remoto, SSH o TeamViewer.

Operaciones con un servidor principal

El servidor de principal aparece en la sección de la consola de copias de seguridad **Recuperación ante desastres > Servidores**.

Para iniciar o detener el servidor, haga clic en **Iniciar** o **Detener** en el panel derecho.

Para editar la configuración del servidor primario, deténgalo, haga clic en **Información** y, luego, en **Editar**.

Para aplicar un plan de copias de seguridad al servidor principal, haga clic en **Copia de seguridad**. Verá un plan de copias de seguridad predefinido en el que puede cambiar únicamente la planificación y las reglas de retención. Para obtener más información, consulte "Realización de copias de seguridad de servidores en la cloud".



Gestión de servidores en el cloud

Para gestionar servidores en el cloud, vaya a **Recuperación ante desastres > Servidores**. Puede encontrar la siguiente información acerca de cada servidor. Para mostrar todas las columnas opcionales en la tabla, haga clic en el icono de engranaje.

Nombre de la columna	Descripción
Nombre	Un nombre de servidor de cloud que ha definido usted
Tipo de servidor	Un tipo de servidor de cloud puede ser: <ul style="list-style-type: none"> • Recuperación • Principal
Rango	El rango que refleja el problema más grave con un servidor de cloud (en función de las alertas activas)
Estado	El estado de un servidor de cloud de acuerdo con su ciclo de vida
Umbral de RPO	El intervalo temporal máximo permitido entre el último punto de recuperación viable para una conmutación por error y el momento presente. El valor puede establecerse entre 5-60 minutos, 1-24 horas y 1-14 días.

Nombre de la columna	Descripción
Cumplimiento de RPO	<p>El Cumplimiento de RPO es la proporción entre los RPO reales y el Umbral de RPO. El Cumplimiento de RPO se muestra si se ha definido el Umbral de RPO.</p> <p>Se calcula de la siguiente forma:</p> <p>Cumplimiento de RPO = RPO reales / Umbral de RPO donde RPO reales = hora actual – último tiempo de punto de recuperación</p> <p>Rangos de cumplimiento de RPO Dependiendo del valor de la proporción entre los RPO reales y el Umbral de RPO, se usan los siguientes rangos:</p> <ul style="list-style-type: none"> • Dentro del umbral. El Cumplimiento de RPO es < 1x. Un servidor cumple el Umbral de RPO. • Superado. El Cumplimiento de RPO es <= 2x. Un servidor infringe el Umbral de RPO. • Superado en gran medida. El Cumplimiento de RPO es <= 4x. Un servidor infringe el Umbral de RPO más de 2 veces. • Superado severamente. El Cumplimiento de RPO es > 4x. Un servidor infringe el Umbral de RPO más de 4 veces. • Pendiente (no hay copias de seguridad). El servidor está protegido con el plan de copias de seguridad, pero la copia de seguridad está en proceso de creación y no se ha completado aún.
RPO reales	Tiempo transcurrido desde la creación del último punto de recuperación
Último punto de recuperación	La fecha y la hora en las que se creó el último punto de recuperación.

Realización de copias de seguridad de servidores en la cloud

Realización de copias de seguridad de servidores en la cloud

Agent para VMware, que se instala en el sitio en el cloud, realiza copias de seguridad de los servidores principales y de recuperación. En su versión inicial, las funcionalidades de esta copia de seguridad se ven ligeramente restringidas en comparación con una copia de seguridad realizada por agentes locales. Estas limitaciones son temporales y se eliminarán en futuras versiones.

- La única ubicación de copia de seguridad es el almacenamiento en la cloud.
- No se puede aplicar un plan de copias de seguridad a varios servidores. Cada servidor debe tener su propio plan de copias de seguridad, incluso si todos los planes de copias de seguridad tienen la misma configuración.
- Solo se puede aplicar un plan de copias de seguridad a un servidor.
- No es compatible con la copia de seguridad compatible con la aplicación.
- El cifrado no está disponible.
- Las opciones de copia de seguridad no están disponibles.

Cuando elimina un servidor principal, las copias de seguridad también se eliminan.

Se realiza una copia de seguridad de un servidor de recuperación únicamente en estado de conmutación por error. Sus copias de seguridad siguen la secuencia de copia de seguridad del servidor original. Cuando se lleva a cabo una conmutación por recuperación, el servidor original puede continuar esta secuencia de copia de seguridad. Por lo tanto, las copias de seguridad del servidor de recuperación solo se pueden eliminar manualmente o como resultado de la aplicación de reglas de retención. Cuando se elimina un servidor de recuperación, sus copias de seguridad se conservan siempre.

Nota: los planes de copias de seguridad para servidores en el cloud se realizan en hora UTC.

Configuración de servidores principales





Configuración de la funcionalidad de recuperación ante desastres

Para configurar la funcionalidad de recuperación ante desastres:

Configure el tipo de conectividad en el sitio en el cloud:

1. Conexión de sitio a sitio

Requisitos del dispositivo VPN y Requisitos del sistema:

- 1 CPU
- 1 GB DE RAM
- 8 GB de espacio de disco

Puertos

- TCP 443 (salida): para conexión VPN
- TCP 80 (salida): para actualizar el dispositivo automáticamente.

Asegúrese de que sus cortafuegos y otros componentes del sistema de seguridad de la red permiten las conexiones a través de estos puertos a cualquier dirección IP.

Configuración de la conexión de sitio a sitio

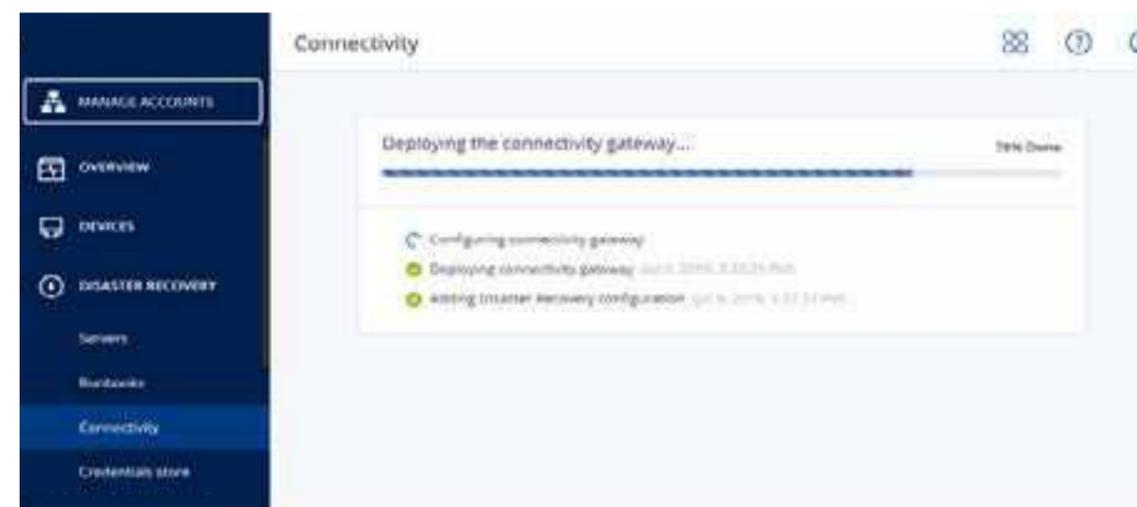
El dispositivo VPN amplía su red local a la cloud mediante un túnel de VPN seguro. Este tipo de conexión se suele llamar conexión "de sitio a sitio" (S2S).

Pasos para configurar una conexión mediante el dispositivo VPN

1. En la consola de copias de seguridad, vaya a **Recuperación ante desastres** > **Conectividad** y haga clic en **Configurar**. Se abrirá el asistente de configuración de conectividad.

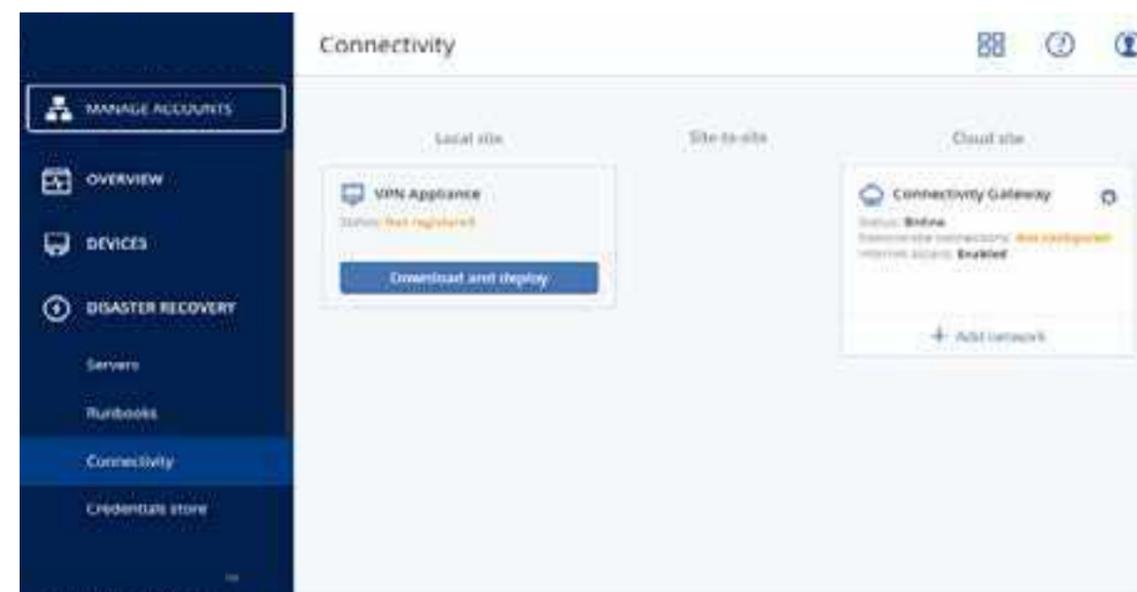
2. Seleccione **Conexión de sitio a sitio** y haga clic en **Iniciar**.

El sistema empieza a implementar la puerta de enlace de conectividad en el cloud. Este procedimiento tardará un tiempo. mientras tanto, puede continuar con el siguiente paso.



Nota: La puerta de enlace de conectividad se proporciona sin ningún cargo adicional. Se eliminará si la funcionalidad de recuperación ante desastres no se usa, es decir, si no hay ningún servidor principal ni de recuperación en la cloud durante siete días.

3. Haga clic en **Descargar e implementar**. En función de la plataforma de virtualización que use, descargue el dispositivo VPN de VMware vSphere o Microsoft Hyper-V.





4. Implemente el dispositivo y conéctelo a las redes de producción. En vSphere, asegúrese de que esté activado el **modo Promiscuous** y **Transmisiones falsificadas** y establezca en **Aceptar** todos los conmutadores virtuales que conecten el dispositivo VPN a las redes de producción. Para acceder a esta configuración, en vSphere Client, seleccione el host > **Resumen** > **Red** y, a continuación, seleccione el conmutador > Editar **configuración...** > **Seguridad**.

En Hyper-V, cree un equipo virtual de **1.ª generación** con 1024 MB de memoria. También le recomendamos habilitar la **memoria dinámica** del equipo. Cuando haya creado el equipo, vaya a **Configuración** > **Hardware** > **Adaptador de red** > **Funciones avanzadas** y marque la casilla de verificación **Habilitar el redireccionamiento de direcciones MAC**.

5. Encienda el dispositivo.

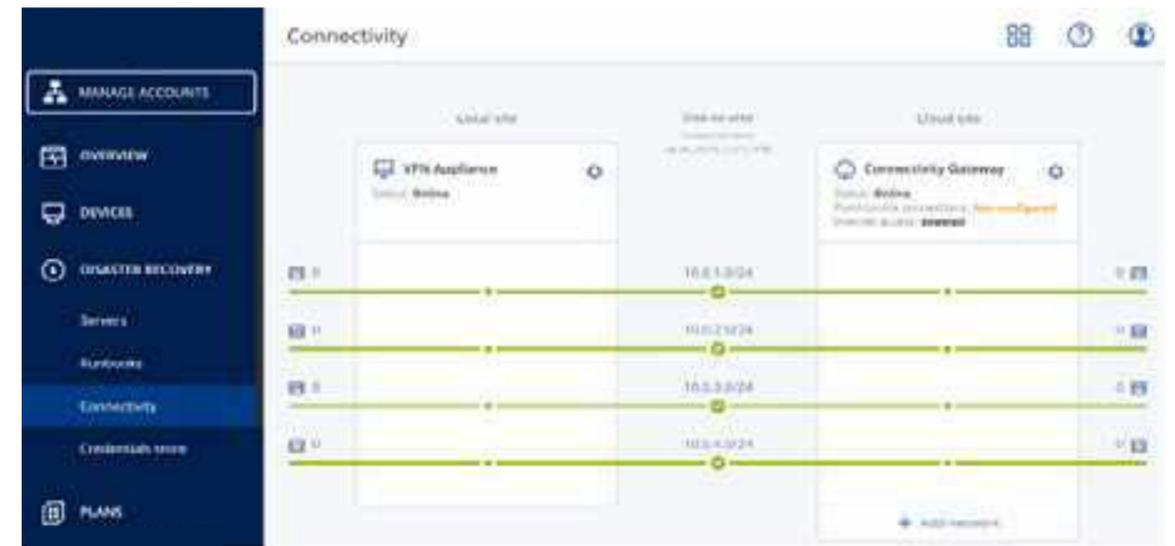
6. Abra la consola del dispositivo e inicie sesión con el nombre de usuario y la contraseña "admin"/"admin".

7. [Opcional] Cambie la contraseña.

8. [Opcional] Cambie la configuración de red si así lo precisa. Defina la interfaz que se usará como WAN para la conexión a Internet.

9. Use las credenciales del administrador de la empresa para registrar el dispositivo en el servicio de copias de seguridad. Estas credenciales solo se usan una vez para recuperar el certificado. La URL del centro de datos viene predefinida.

Nota: Si se ha configurado la autenticación de doble factor para su cuenta, también se le solicitará el código TOTP. Si se ha habilitado, pero no se ha configurado la autenticación de doble factor para su cuenta, no puede registrar el dispositivo VPN. Primero, debe ir a la página de inicio de sesión de la consola de copias de seguridad y completar la configuración de la autenticación de doble factor para su cuenta. Para obtener más información acerca de la autenticación de doble factor, vaya a la Guía del administrador del portal de gestión. Cuando haya completado la configuración, el dispositivo mostrará el estado En línea. El dispositivo se conecta a la puerta de enlace de conectividad y comienza a transmitir información sobre las redes de todas las interfaces activas al servicio Disaster Recovery Cloud. La consola de copias de seguridad muestra las interfaces basándose en la información del dispositivo VPN.



Pasos para probar la conexión VPN

1. Vaya a **Recuperación ante desastres** > **Conectividad**.

2. En el bloque **Dispositivo VPN**, haga clic en el icono de engranaje.

3. Asegúrese de que el dispositivo VPN y la puerta de enlace de conectividad muestren el estado **En línea**.

4. Haga clic en **Probar conexión**.

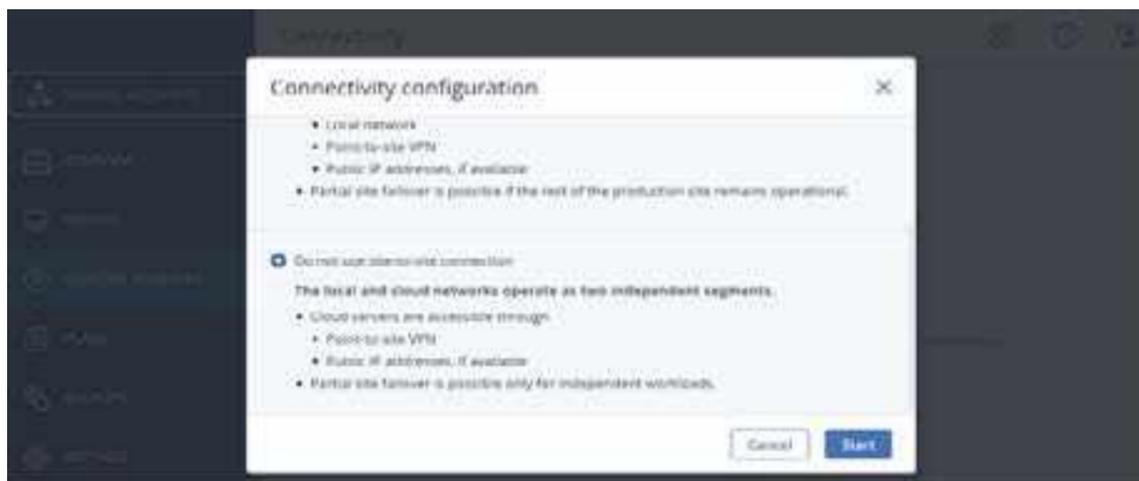
El dispositivo VPN comprueba la conexión a la puerta de enlace de conectividad. Aparecerá la lista de pruebas que se están realizando y sus resultados.

2. Sin conexión de sitio a sitio

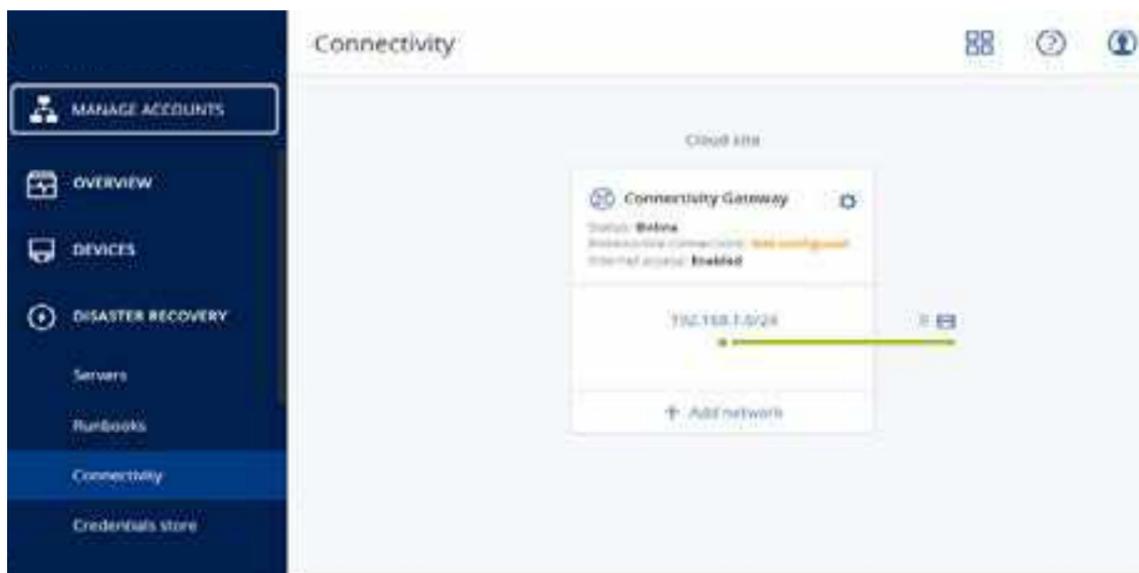
Requisitos del dispositivo VPN y Requisitos del sistema:

1. En la consola de copias de seguridad, vaya a **Recuperación ante desastres** > **Conectividad** y haga clic en **Configurar**. Se abrirá el asistente de configuración de conectividad.

2. Seleccione **No usar conexión de sitio a sitio** y haga clic en **Iniciar**.



3. Como resultado, la puerta de enlace de conectividad y la red en el cloud con la dirección y máscara definidas se implementarán en el sitio del cloud.



Para aprender a gestionar sus redes en el cloud y establecer la configuración de la puerta de enlace de conectividad, consulte "Gestión de redes en el cloud".

3. Conexión de punto a sitio

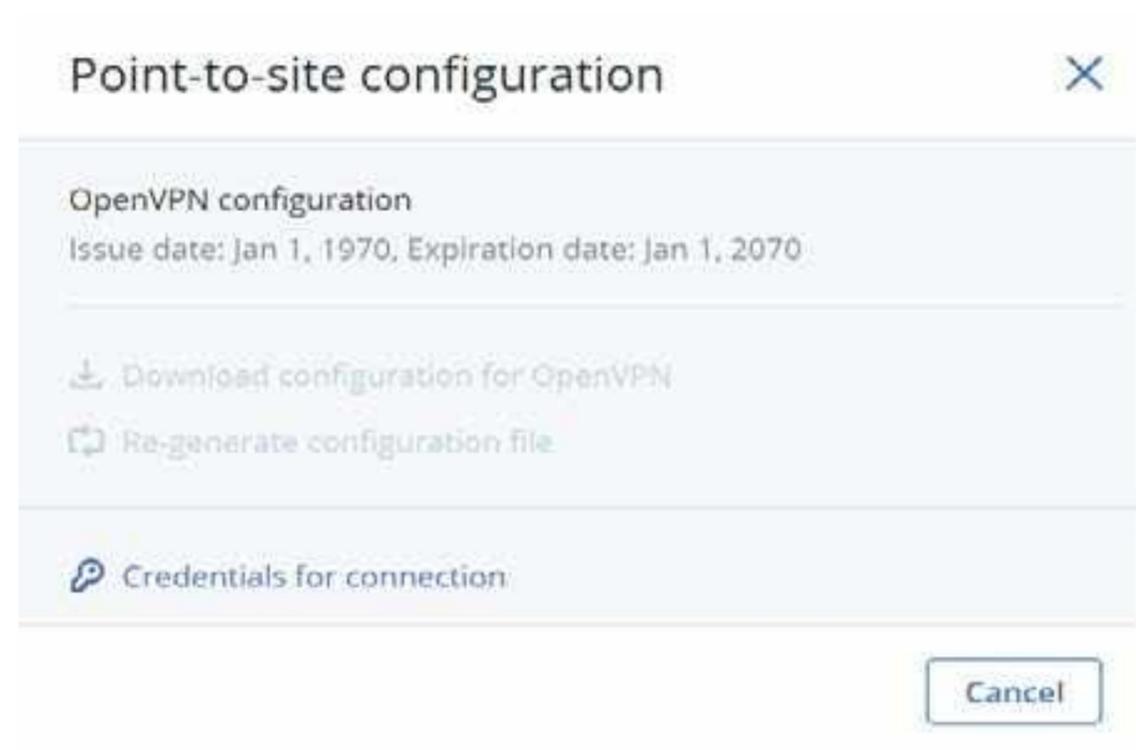
En el caso de que la red local esté caída, podrá conectarse directamente al sitio en el cloud. Este tipo de conexión se suele llamar conexión "de punto a sitio" (P2S), en comparación con la conexión "de sitio a sitio" (S2S).

Para establecer el nombre de usuario y la contraseña de la conexión de punto a sitio:

1. En la consola de copias de seguridad, vaya a **Recuperación ante desastres > Conectividad** y haga clic en el icono de engranaje en el bloque **Puerta de enlace de conectividad**.

2. Haga clic en Configuración de punto a sitio.

3. Haga clic en Credenciales para establecer la conexión.



4. Seleccione el nombre de usuario y contraseña.

5. Confirme la contraseña

6. Haga clic en Listo cuando tenga todo a punto.



3. Pasos para establecer la conexión de punto a sitio.

1. Instale el cliente OpenVPN en el equipo que quiera conectar al sitio en el cloud. Las versiones del cliente OpenVPN admitidas son la 2.4.0 y posteriores.
2. En la consola de copias de seguridad, vaya a **Recuperación ante desastres > Conectividad** y haga clic en el icono de engranaje en el bloque **Puerta de enlace de conectividad**.
3. Haga clic en **Descargar configuración para OpenVPN**.
4. Importe la configuración descargada a OpenVPN.
5. Cuando se inicie la conexión, introduzca el nombre de usuario y la contraseña que haya establecido como se ha descrito anteriormente.

2. Cree un plan de copias de seguridad completo para el equipo y aplíquelo a los servidores locales para protegerlos. Se debe crear por lo menos un punto de recuperación antes de crear servidores de recuperación.

3. Cree los servidores de recuperación para cada uno de los servidores locales que desee proteger.

Creación de un servidor de recuperación: Requisitos previos

- Se debe aplicar un plan de copias de seguridad al equipo original que quiera proteger. Este plan debe realizar copias de seguridad de todo el equipo o solo de los discos. Estas son necesarias para arrancar y proporcionar los servicios necesarios a un almacenamiento en el cloud. Se debe crear por lo menos un punto de recuperación para el equipo original.
- Se debe establecer uno de los tipos de conectividad en el sitio en el cloud.

Pasos para crear un servidor de recuperación

1. En la pestaña Todos los equipos, seleccione el equipo que desea proteger.
2. Haga clic en **Recuperación ante desastres** y, luego, en **Crear recuperar servidor**.
3. Seleccione el número de núcleos virtuales y el tamaño de la RAM. Tenga en cuenta los puntos del equipo que se encuentran junto a cada opción. El número de puntos del equipo indican el coste de funcionamiento del servidor de recuperación por hora.
4. Especifique la red en el cloud a la que se conectará el servidor.
5. Especifique la dirección IP que tendrá el servidor en la red de producción. La dirección IP del equipo original se establece de forma predefinida.

Nota: Si usa un servidor DHCP, agregue esta dirección IP a la lista de exclusión de servidores para evitar conflictos con la dirección IP.



6. [Opcional] Marque la casilla de verificación de **dirección IP de prueba** y, a continuación, especifique la dirección IP.

Esto le permitirá probar una conmutación por error en la red de prueba aislada y conectarse al servidor de recuperación mediante escritorio remoto o SSH durante una prueba de conmutación por error. En el modo de prueba de conmutación por error, la puerta de enlace de conectividad sustituirá la dirección IP de prueba por la dirección IP de producción mediante el protocolo NAT.

Si deja la casilla de verificación desmarcada, la consola será la única forma de acceder al servidor durante una conmutación por error de prueba.

Nota: Si usa un servidor DHCP, agregue esta dirección IP a la lista de exclusión de servidores para evitar conflictos con la dirección IP.

Puede seleccionar una de las direcciones IP propuestas o escribir otra.

7. [Opcional] Marque la casilla de verificación de **acceso a Internet**.

De esta forma, el servidor de recuperación tendrá acceso a Internet durante una conmutación por error de prueba o real.

8. [Opcional] Marque la casilla de verificación de **dirección IP pública**.

El hecho de que el servidor de recuperación cuente con una dirección IP pública conlleva que se pueda acceder a él desde Internet durante una conmutación por error de prueba o real. Si deja la casilla de verificación desmarcada, el servidor solo estará disponible en su red de producción. La dirección IP pública se mostrará cuando finalice la configuración. Los siguientes puertos se abren para realizar conexiones de entrada a direcciones IP públicas:

TCP: 80, 443, 8088, 8443

UDP: 1194

Si necesita que se abran otros puertos, póngase en contacto con el equipo de soporte técnico.

9. [Opcional] Establezca el **umbral de RPO**.

El umbral de RPO define el intervalo temporal máximo permitido entre el último punto de recuperación viable para una conmutación por error y el momento presente. El valor se puede establecer entre 15 y 60 minutos, 1 y 24 horas y 1 y 14 días.

10. [Opcional] Si las copias de seguridad del equipo seleccionado están cifradas, puede especificar la contraseña que se usará automáticamente al crear un equipo virtual para el servidor de recuperación a partir de las copias de seguridad cifradas. Haga clic en **Especificar** y defina el nombre y la contraseña de la credencial. De forma predeterminada, verá la copia de seguridad más reciente en la lista. Para ver todas las copias de seguridad, seleccione **Mostrar todas las copias de seguridad**.

11. [Opcional] Cambie el nombre del servidor de recuperación.

12. [Opcional] Escriba una descripción para el servidor de recuperación.

13. Haga clic en **Crear**.

El servidor de recuperación aparece en la sección de la consola de copias de seguridad **Recuperación ante desastres > Servidores**. También puede ver su configuración si selecciona el equipo original y hace clic en **Recuperación ante desastres**.

4. Realice una prueba de conmutación por error para comprobar cómo funciona.

Ejecución de una prueba de conmutación por error

Probar una conmutación por error implica iniciar un servidor de recuperación en una VLAN de prueba que está aislada de su red de producción. Puede probar varios servidores de recuperación a la vez para comprobar su interacción. En la red de prueba, los servidores se comunican mediante sus direcciones IP de producción, pero no pueden iniciar las conexiones TCP o UDP en los equipos de su red local.

Aunque el proceso de prueba de una conmutación por error es opcional, le recomendamos que lo haga habitualmente con la frecuencia que considere adecuada, teniendo en cuenta el coste y la seguridad. Una práctica recomendada es crear un runbook, que es un conjunto de instrucciones en las que se describe la forma de iniciar el entorno de producción en el cloud.

Pasos para ejecutar una conmutación por error de prueba

1. Seleccione el equipo original o el servidor de recuperación que quiera probar.

2. Haga clic en **Recuperación ante desastres**. Se abre la descripción del servidor de recuperación.

3. Haga clic en **Probar conmutación por error de prueba**.

4. Seleccione el punto de recuperación y haga clic en **Probar conmutación por error**.

Cuando el servidor de recuperación se inicia, su estado cambia a **Probando conmutación por error**.



5. Use uno de los siguientes métodos para probar el servidor de recuperación:

- En la consola de copias de seguridad, haga clic en **Recuperación ante desastres > Servidores**, seleccione el servidor de recuperación y a continuación, haga clic en **Consola** en el panel de la derecha.
- Use el equipo remoto o SSH para conectarse al servidor de recuperación y a la dirección IP de prueba que especificó al crear el servidor de recuperación. Pruebe la conexión tanto desde el interior como desde el exterior de la red de producción (como se describe en “Conexión de punto a sitio”).
- Ejecute una secuencia de comandos en el servidor de recuperación.
- El script puede comprobar la pantalla de inicio, si las aplicaciones se han iniciado, la conexión a Internet y la capacidad de otros equipos de conectarse al servidor de recuperación.
- Si el servidor de recuperación tiene acceso a Internet y una dirección IP pública, puede que quiera usar TeamViewer.

6. Cuando la prueba haya terminado, haga clic en Detener prueba en la consola de copia de seguridad.

El servidor de recuperación se detiene. Todos los cambios realizados en el servidor de recuperación durante la prueba de conmutación por error se pierden.

5. Creación de un servidor principal

Requisitos previos

Se debe establecer uno de los tipos de conectividad en el sitio en el cloud.

Pasos para crear un servidor principal

1. Vaya a Recuperación ante desastres > Servidores.
2. Haga clic en **Crear servidor principal**
3. Seleccione una plantilla para el nuevo equipo virtual.
4. Seleccione el número de núcleos virtuales y el tamaño de la RAM. Preste atención a los puntos del equipo que se encuentran junto a cada opción. El número de puntos del equipo indican el coste de funcionamiento del servidor principal por hora.

5. [Opcional] Cambie el tamaño de las unidades de discos virtuales. Si necesita más de un disco rígido, haga clic en **Agregar disco** y, a continuación, especifique el nuevo disco.

6. Especifique la red de cloud en la que se incluirá el servidor principal.

7. Especifique la dirección IP que tendrá el servidor en la red de producción. La primera dirección IP libre de su red de producción se establece de forma predeterminada.

Nota: Si usa un servidor DHCP, agregue esta dirección IP a la lista de exclusión de servidores para evitar conflictos con la dirección IP.

8. [Opcional] Marque la casilla de verificación de **acceso a Internet**. De esta forma, el servidor principal tendrá acceso a Internet.

9. [Opcional] Marque la casilla de verificación de dirección **IP pública**.

El hecho de que el servidor principal cuente con una dirección IP pública conlleva que se pueda acceder a él desde Internet. Si deja la casilla de verificación desmarcada, el servidor solo estará disponible en su red de producción.

La dirección IP pública se mostrará cuando finalice la configuración. Los siguientes puertos se abren para realizar conexiones de entrada a direcciones IP públicas:

TCP: 80, 443, 8088, 8443

UDP: 1194

Si necesita que se abran otros puertos, póngase en contacto con el equipo de soporte técnico.

10. [Opcional] Seleccione Establecer el umbral de RPO.

El umbral de RPO determina el intervalo temporal máximo permitido entre el último punto de recuperación y el momento presente. El valor se puede establecer entre 15 y 60 minutos, 1 y 24 horas y 1 y 14 días.

11. Defina el nombre del servidor principal.

12. [Opcional] Especifique una descripción para el servidor principal.

13. Haga clic en **Crear**.

El servidor principal estará disponible en la red de producción. Puede gestionar el servidor mediante su consola, el escritorio remoto, SSH o TeamViewer.

Como resultado, habrá configurado la funcionalidad de recuperación ante desastres que protegerá sus servidores locales de un desastre. Si se produce un desastre, puede realizar una conmutación por error de la carga de trabajo a los servidores de recuperación en el cloud. Cuando su sitio local se recupere del desastre, puede trasladar la carga de trabajo de vuelta a su sitio local.



Conmutación por error y conmutación por recuperación

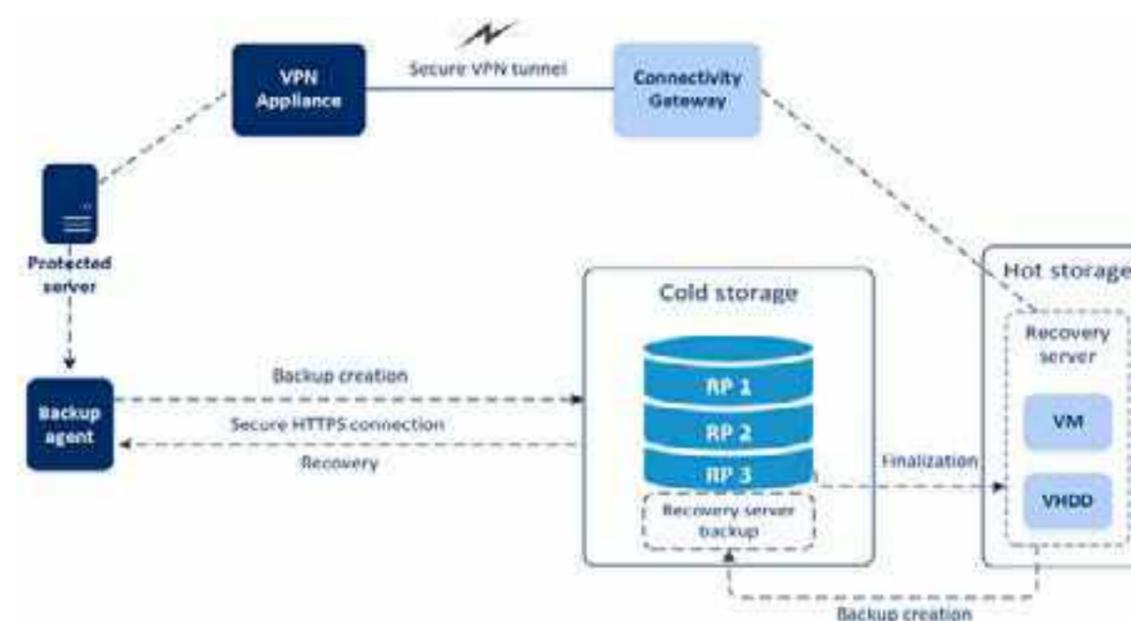
Cómo funcionan la conmutación por error y la conmutación por recuperación

Al crear un servidor de recuperación, se queda en estado **En espera**. El equipo virtual correspondiente no existe hasta que inicie la conmutación por error. Antes de iniciar el proceso de conmutación por error, debe crear al menos una copia de seguridad de imágenes de disco (con volumen de arranque) de su equipo original.

Al iniciar el proceso de conmutación por error, seleccione el punto de recuperación del equipo original a partir del que se crea un equipo virtual con los parámetros predefinidos. La operación de conmutación por error usa la funcionalidad "ejecutar equipo virtual a partir de una copia de seguridad". El servidor de recuperación obtiene el estado de transición **Finalización**. Este proceso consiste en transferir las unidades de disco virtual del servidor desde el almacenamiento de copias de seguridad (almacenamiento "estático") hasta el almacenamiento de recuperación ante desastres (almacenamiento "dinámico"). Durante la finalización, el servidor es accesible y funcional, aunque su rendimiento será menor de lo normal. Cuando la finalización se completa, el rendimiento del servidor alcanza su valor normal. El estado del servidor cambia a **Conmutación por error**. Ahora, la carga de trabajo se traslada del equipo original al servidor de recuperación en el sitio en el cloud.

Si el servidor de recuperación cuenta con un agente de copia de seguridad en su interior, el servicio de agente se detiene para evitar que se produzca una interferencia (como el inicio de una copia de seguridad o la creación de informes sobre estados desactualizados al servicio de copia de seguridad).

En el siguiente diagrama puede ver los procesos de conmutación por error y conmutación por recuperación.



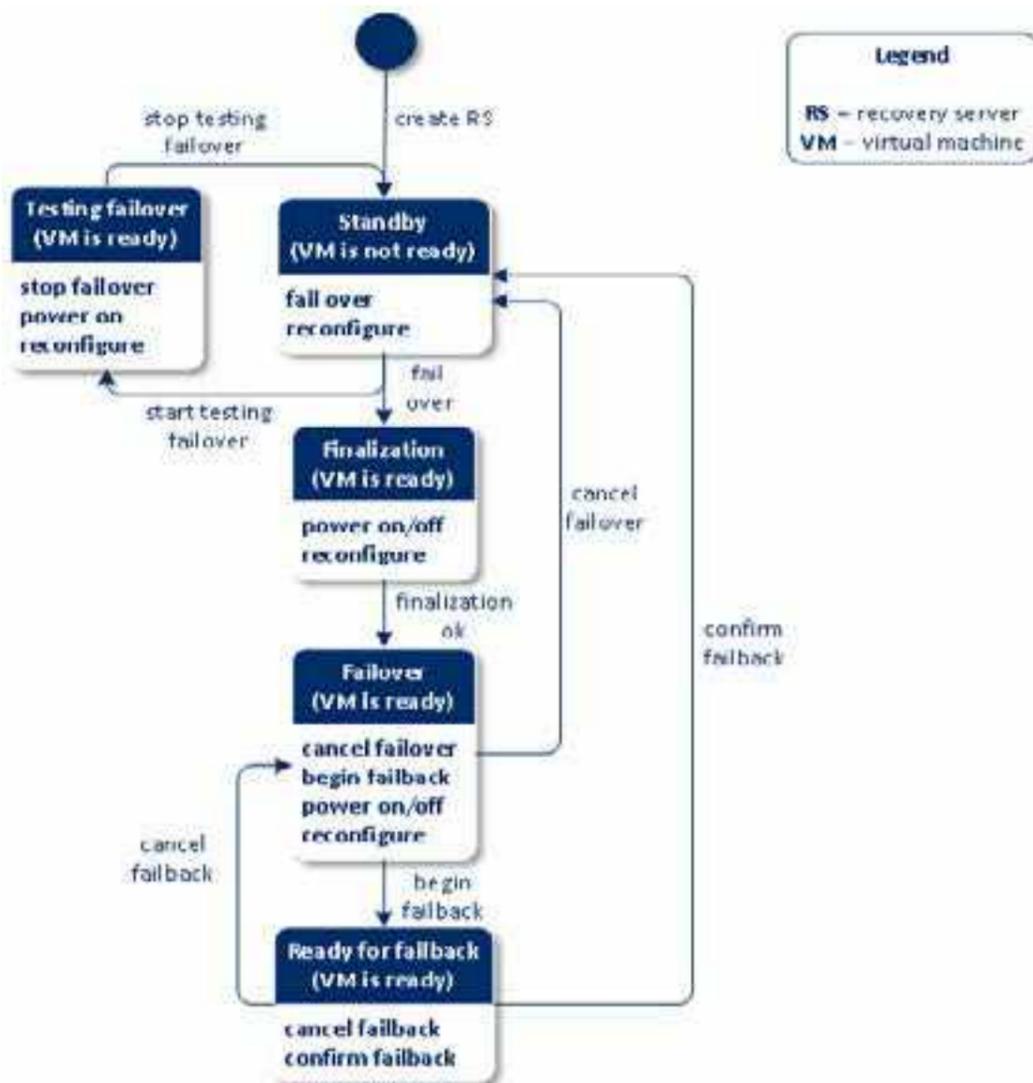


Probar conmutación por error

Durante una prueba de conmutación por error, el equipo virtual no se finaliza. Esto significa que el agente lee el contenido de los discos virtuales directamente desde la copia de seguridad, es decir, accede aleatoriamente a varias partes de ella.

Ciclo de vida del servidor de recuperación

En el siguiente diagrama puede observar el ciclo de vida del servidor de recuperación, que muestra estados permanentes y de transición. Cada bloque muestra un estado del servidor de recuperación, un estado del equipo virtual correspondiente y las acciones disponibles para el usuario en esta fase. Cada flecha es un evento o acción del usuario que lleva al siguiente estado.



Flujo de trabajo de conmutación por error y conmutación por recuperación

1. Acción del usuario: Crear un servidor de recuperación para proteger el equipo seleccionado.
2. Estado **En espera**. La configuración del servidor de recuperación se ha definido, pero el equipo virtual correspondiente no está listo.
3. Acción del usuario: Se inicia la conmutación por error en el modo de producción y el servidor de recuperación se está creando a partir del punto de recuperación seleccionado.
4. Estado **Finalización**. Los discos del equipo virtual se han finalizado a partir del punto de recuperación establecido y se trasladan al almacenamiento de alto rendimiento. El servidor de recuperación es funcional, aunque su rendimiento será menor de lo normal hasta que se complete la finalización.
5. Suceso: La finalización se completa correctamente.
6. Estado **Conmutación por error**. La carga de trabajo se traslada del equipo original al servidor de recuperación.
7. Acciones del usuario:
 - Iniciar una conmutación por recuperación. El servidor de recuperación se detendrá y se realizará una copia de seguridad en el almacenamiento en el cloud.
 - Si el usuario cancela la conmutación por error, la carga de trabajo se vuelve a trasladar al equipo original y el servidor de recuperación vuelve al estado **En espera**.
8. Estado **Listo para la conmutación por recuperación**. Se crea la copia de seguridad del servidor de recuperación. Debe recuperar el servidor local de esta copia de seguridad mediante el proceso de recuperación habitual.
9. Acciones del usuario:
 - Confirmar la conmutación por recuperación. Como resultado, los recursos en el cloud que se habían asignado al servidor de recuperación se liberan.
 - Cancelar conmutación por recuperación. Se cancela la conmutación por recuperación de acuerdo con su solicitud. El servidor de recuperación vuelve al estado **Conmutación por error**.



Flujo de trabajo de prueba de conmutación por error

1. Acción del usuario: Crear un servidor de recuperación para proteger el equipo seleccionado.
2. Estado **En espera**. La configuración del servidor de recuperación se ha definido, pero el equipo virtual correspondiente no está listo.
3. Acción del usuario: Iniciar la prueba de conmutación por error.
4. Estado **Probando conmutación por error**. En este estado, se creará un equipo virtual temporal para la prueba.
5. Acción del usuario: Detener la prueba de conmutación por error.

Creación de un servidor de recuperación

Requisitos previos

- Se debe aplicar un plan de copias de seguridad al equipo original que quiera proteger. Este plan debe realizar copias de seguridad de todo el equipo o solo de los discos. Estas son necesarias para arrancar y proporcionar los servicios necesarios a un almacenamiento en el cloud. Se debe crear por lo menos un punto de recuperación para el equipo original.
- Se debe establecer uno de los tipos de conectividad en el sitio en el cloud.

Pasos para crear un servidor de recuperación

1. En la pestaña **Todos los equipos**, seleccione el equipo que desea proteger.
2. Haga clic en Recuperación ante desastres y, luego, en **Crear recuperar servidor**.
3. Seleccione el número de núcleos virtuales y el tamaño de la RAM. Tenga en cuenta los puntos del equipo que se encuentran junto a cada opción. El número de puntos del equipo indican el coste de funcionamiento del servidor de recuperación por hora.
4. Especifique la red en el cloud a la que se conectará el servidor.
5. Especifique la dirección IP que tendrá el servidor en la red de producción. La dirección IP del equipo original se establece de forma predeterminada.

Nota: Si usa un servidor DHCP, agregue esta dirección IP a la lista de exclusión de servidores para evitar conflictos con la dirección IP.

6. [Opcional] Marque la casilla de verificación de **dirección IP de prueba** y, a continuación, especifique la dirección IP.

Esto le permitirá probar una conmutación por error en la red de prueba aislada y conectarse al servidor de recuperación mediante escritorio remoto o SSH durante una prueba de conmutación por error. En el modo de prueba de conmutación por error, la puerta de enlace de conectividad sustituirá la dirección IP de prueba por la dirección IP de producción mediante el protocolo NAT. Si deja la casilla de verificación desmarcada, la consola será la única forma de acceder al servidor durante una conmutación por error de prueba.

Nota: Si usa un servidor DHCP, agregue esta dirección IP a la lista de exclusión de servidores para evitar conflictos con la dirección IP. Puede seleccionar una de las direcciones IP propuestas o escribir otra.

7. [Opcional] Marque la casilla de verificación de **acceso a Internet**. De esta forma, el servidor de recuperación tendrá acceso a Internet durante una conmutación por error de prueba o real.

8. [Opcional] Marque la casilla de verificación de **dirección IP pública**. El hecho de que el servidor de recuperación cuente con una dirección IP pública conlleva que se pueda acceder a él desde Internet durante una conmutación por error de prueba o real. Si deja la casilla de verificación desmarcada, el servidor solo estará disponible en su red de producción.

La dirección IP pública se mostrará cuando finalice la configuración. Los siguientes puertos se abren para realizar conexiones de entrada a direcciones IP públicas: TCP: 80, 443, 8088, 8443 UDP: 1194 Si necesita que se abran otros puertos, póngase en contacto con el equipo de soporte técnico.

9. [Opcional] Establezca el **umbral de RPO**.

El umbral de RPO define el intervalo temporal máximo permitido entre el último punto de recuperación viable para una conmutación por error y el momento presente. El valor se puede establecer entre 15 y 60 minutos, 1 y 24 horas y 1 y 14 días.

10. [Opcional] Si las copias de seguridad del equipo seleccionado están cifradas, puede especificar la contraseña que se usará automáticamente al crear un equipo virtual para el servidor de recuperación a partir de las copias de seguridad cifradas. Haga clic en **Especificar** y defina el nombre y la contraseña de la credencial. De forma predeterminada, verá la copia de seguridad más reciente en la lista. Para ver todas las copias de seguridad, seleccione **Mostrar todas las copias de seguridad**.



11. [Opcional] Cambie el nombre del servidor de recuperación.

12. [Opcional] Escriba una descripción para el servidor de recuperación.

13. Haga clic en **Crear**.

El servidor de recuperación aparece en la sección de la consola de copias de seguridad **Recuperación ante desastres > Servidores**. También puede ver su configuración si selecciona el equipo original y hace clic en Recuperación ante desastres.

Ejecución de una prueba de conmutación por error

Probar una conmutación por error implica iniciar un servidor de recuperación en una VLAN de prueba que está aislada de su red de producción. Puede probar varios servidores de recuperación a la vez para comprobar su interacción. En la red de prueba, los servidores se comunican mediante sus direcciones IP de producción, pero no pueden iniciar las conexiones TCP o UDP en los equipos de su red local.

Aunque el proceso de prueba de una conmutación por error es opcional, le recomendamos que lo haga habitualmente con la frecuencia que considere adecuada, teniendo en cuenta el coste y la seguridad. Una práctica recomendada es crear un runbook, que es un conjunto de instrucciones en las que se describe la forma de iniciar el entorno de producción en el cloud.

Pasos para ejecutar una conmutación por error de prueba

1. Seleccione el equipo original o el servidor de recuperación que quiera probar.
2. Haga clic en Recuperación ante desastres.
Se abre la descripción del servidor de recuperación.
3. Haga clic en Probar conmutación por error de prueba.
4. Seleccione el punto de recuperación y haga clic en Probar conmutación por error.
Cuando el servidor de recuperación se inicia, su estado cambia a Probando conmutación por error.

5. Use uno de los siguientes métodos para probar el servidor de recuperación:

- En la consola de copias de seguridad, haga clic en Recuperación ante desastres > Servidores, seleccione el servidor de recuperación y, a continuación, haga clic en Consola en el panel de la derecha.
- Use el equipo remoto o SSH para conectarse al servidor de recuperación y a la dirección IP de prueba que especificó al crear el servidor de recuperación. Pruebe la conexión tanto desde el interior como desde el exterior de la red de producción (como se describe en "Conexión de punto a sitio").
- Ejecute una secuencia de comandos en el servidor de recuperación. El script puede comprobar la pantalla de inicio, si las aplicaciones se han iniciado, la conexión a Internet y la capacidad de otros equipos de conectarse al servidor de recuperación.
- Si el servidor de recuperación tiene acceso a Internet y una dirección IP pública, puede que quiera usar TeamViewer.

6. Cuando la prueba haya terminado, haga clic en Detener prueba en la consola de copia de seguridad.

El servidor de recuperación se detiene. Todos los cambios realizados en el servidor de recuperación durante la prueba de conmutación por error se pierden.

Realización de una conmutación por error

La conmutación por error es un proceso que consiste en mover una carga de trabajo a la cloud, además del estado en el que la carga de trabajo permanece en la cloud.

Al iniciar una recuperación por error, el servidor de recuperación se inicia en la red de producción. Todos los planes de copias de seguridad se revocarán desde el equipo original. Se ha creado y aplicado automáticamente un nuevo plan de copias de seguridad al servidor de recuperación.



Pasos para llevar a cabo una conmutación por error

1. Asegúrese de que el equipo original no esté disponible en la red.
2. En la consola de copias de seguridad, seleccione el equipo original o el servidor de recuperación que corresponda al equipo.
3. Haga clic en **Recuperación ante desastres**. Se abre la descripción del servidor de recuperación.
4. Haga clic en **Conmutación por error**.

5. Seleccione el punto de recuperación y haga clic en **Conmutación por error**.

Cuando el servidor de recuperación se inicia, su estado cambia a **Finalización** y, después de un tiempo, cambia a **Conmutación por error**. Entender que el servidor está disponible en ambos estados es fundamental, a pesar de que el indicador de progreso cambie. Para obtener más información, consulte “Cómo funcionan la conmutación por error y la conmutación por recuperación”.

6. Mire la consola del servidor de recuperación para asegurarse de que se ha iniciado. Haga clic en **Recuperación ante desastres** > **Servidores**, seleccione el servidor de recuperación y, a continuación, haga clic en **Consola** en el panel de la derecha.

7. Asegúrese de que se pueda acceder al servidor de recuperación mediante la dirección IP de producción que haya especificado al crearlo. Cuando el servidor de recuperación se haya apagado, se crea y se aplica automáticamente un nuevo plan de copias de seguridad. Este plan de copias de seguridad se basa en el que se usó para crear el servidor de recuperación, con ciertas limitaciones. En este plan, puede cambiar únicamente la planificación y las reglas de retención. Para obtener más información, consulte “Realización de copias de seguridad de servidores en la cloud”. La única forma de salir del estado de conmutación por error es llevar a cabo una conmutación por recuperación.

Cómo realizar una conmutación por error de servidores mediante DNS local

Si usa los servidores DNS en el sitio local para resolver nombres de máquina, en ese caso, después de una conmutación por error los servidores de recuperación, correspondiente a las máquinas que dependen de DNS, no se comunicarán porque los servidores DNS usan en el cloud son distintos. De forma predeterminada, los servidores DNS del sitio de cloud se usan para los servidores de cloud recién creados. Si necesita aplicar configuración de DNS personalizada, póngase en contacto con el equipo de soporte técnico.

Cómo se realiza una conmutación por error de un servidor DHCP

Su infraestructura local puede tener el servidor DHCP ubicado en un host Windows o Linux. Cuando se produce una conmutación por error al sitio de cloud en este tipo de host, se produce el problema de duplicación del servidor DHCP porque la puerta de enlace en el cloud también realiza el rol DHCP. Para resolver este problema, realice uno de los siguientes procedimientos:

- Si solo se conmutó por error al cloud el host DHCP, mientras que el resto de los servidores locales siguen en el sitio local, deberá iniciar sesión en el host DHCP en el cloud y desactivar el servidor DHCP en él. De esta forma, no habrá conflictos y solo la puerta de enlace de conectividad funcionará como el servidor DHCP.
- Si los servidores de cloud ya tienen la dirección IP del host DHCP, deberá iniciar sesión en el host DHCP en el cloud y desactivar el servidor DHCP en él. También debería iniciar sesión en los servidores de cloud y renovar la concesión DHCP para asignar las nuevas direcciones IP asignadas desde el servidor DHCP correcto (hospedado en la puerta de enlace de conectividad).



Realización de una conmutación por recuperación

La conmutación por recuperación es un proceso que consiste en volver a mover la carga de trabajo desde la cloud a sus instalaciones. Durante este proceso, el servidor no está disponible. La duración de la ventana de mantenimiento es aproximadamente igual a la de una copia de seguridad y la posterior recuperación del servidor.

Pasos para llevar a cabo una conmutación por recuperación

1. Seleccione un servidor de recuperación cuyo estado sea **conmutación por error**.

2. Haga clic en **Recuperación ante desastres**.

Se abre la descripción del servidor de recuperación.

3. Haga clic en **Preparar conmutación por recuperación**.

El servidor de recuperación se detendrá y se realizará una copia de seguridad en el almacenamiento en la cloud. Espere hasta que el proceso de creación de la copia de seguridad termine.

En ese momento, puede llevar a cabo dos acciones: **Cancelar la conmutación por recuperación** y **Confirmar la conmutación por recuperación**. Si hace clic en **Cancelar conmutación por recuperación**, el servidor de recuperación se iniciará y la conmutación por error continuará.

4. Recupere el servidor desde esta copia de seguridad al hardware o a un equipo virtual situado en sus instalaciones.

- Al usar un dispositivo de arranque, proceda como se describe en “Recuperar discos usando dispositivos de arranque” en el Manual del usuario del servicio de recuperación. Asegúrese de que inicia sesión en la cloud usando la cuenta para la que se registró el servidor, así como de que haya seleccionado la copia de seguridad más reciente.

- Si el equipo de destino está en línea o es un equipo virtual, puede usar la consola de copia de seguridad. En la pestaña **Copias de seguridad**, seleccione el almacenamiento en la cloud. **En Equipo desde el cual examinar**, seleccione el equipo físico de destino, o bien el equipo que esté ejecutando el agente si el equipo de destino es virtual. El equipo seleccionado debe estar registrado para la misma cuenta para la que se registró el servidor. Busque la copia de seguridad más reciente del servidor, haga clic en **Recuperar todo el equipo** y configure otros parámetros de recuperación. Para obtener instrucciones detalladas, consulte la sección “Recuperación de un equipo” en el Manual del usuario del servicio de recuperación.

Asegúrese de que la recuperación se complete y de que el equipo recuperado funcione correctamente.

5. Vuelva al servidor de recuperación de la consola de copias de seguridad y, a continuación, haga clic en **Confirmar la conmutación por recuperación**.

El servidor de recuperación y los puntos de recuperación pasarán a estar disponibles para la conmutación por error. Para crear puntos de recuperación nuevos, aplique el plan de copias de seguridad a un nuevo servidor local.

Trabajando con copias de seguridad cifradas

Puede crear servidores de recuperación a partir de las copias de seguridad cifradas. Para su comodidad, puede configurar una aplicación de contraseña automática para una copia de seguridad cifrada durante la conmutación por error de un servidor de recuperación. Al crear un servidor de recuperación, puede especificar la contraseña para su uso para operaciones de recuperación ante desastres automáticas. Se guardará en el Almacén de credenciales, un almacenamiento seguro de credenciales que puede encontrarse en la sección **Recuperación ante desastres > Almacén de credenciales**. Una credencial puede estar vinculada a varias copias de seguridad.

Para gestionar las contraseñas guardadas en el Almacén de credenciales

1. Vaya a **Recuperación ante desastres > Almacén de credenciales**.

2. Para gestionar una credencial específica, haga clic en el icono en la última columna. Puede ver los elementos enlazados a esta credencial.

- Para desvincular la copia de seguridad de la credencial seleccionada, haga clic en el icono de papelera de reciclaje cerca de la copia de seguridad. Como resultado, tendrá que especificar la contraseña de forma manual durante la conmutación por error al servidor de recuperación.

- Para editar la credencial, haga clic en **Editar** y, a continuación, especifique el nombre o contraseña.

- Para eliminar la credencial, haga clic en **Eliminar**. Tenga en cuenta que tendrá que especificar la contraseña de forma manual durante la conmutación por error al servidor de recuperación.

Comunícate con un asesor comercial

MÉXICO - GUATEMALA - EL SALVADOR - HONDURAS - COSTA RICA - PANAMÁ- BELICE
- ECUADOR - PERÚ- CHILE - ARGENTINA - URUGUAY - PARAGUAY - NICARAGUA -
CURAZAO - BOLIVIA - ARUBA - VENEZUELA - PUERTO RICO - REPÚBLICA DOMINICANA

  310 415 1190 / 312 270 9069

USA: 7630 NW 25th St STE 2 Doral Miami, Florida 33122
+1 786 600 1400

COLOMBIA: Cl43#79-55 Oficina 201 Laureles Medellín, Antioquia, 050031
(4) 580 53 29

www.clouds7.com