Cyber Disaster Recovery Cloud

25.10

Guía del administrador

REVISIÓN:10/11/2025

Contenido

Acerca de Acronis Disaster Recovery

Acronis Disaster Recovery forma parte de Cyber Protection, que ofrece recuperación ante desastres como servicio (DRaaS). Disaster Recovery es una solución rápida y estable que, en caso de desastre natural o provocado por el hombre, activa servidores de recuperación (copias exactas de sus servidores locales) en el sitio de recuperación ante desastres (DR).

El sitio de DR es una ubicación secundaria que garantiza que las operaciones de TI se restauren y continúen si el sitio principal falla. En tal caso, DR cambia las cargas de trabajo de los equipos originales dañados a los servidores de recuperación en el sitio de DR. El sitio de DR incluye los servidores en la nube y la conexión a la nube (redes en la nube).

La ubicación del sitio de DR puede estar en Acronis Cyber Protect Cloud o en Microsoft Azure. La disponibilidad de las ubicaciones del sitio de DR depende de los elementos de la oferta que estén habilitados para su inquilino.

El sitio de DR se encuentra en Acronis Cyber Protect Cloud.

Nota
Solo se admite una ubicación por inquilino de cliente. Si desea cambiar la ubicación de su sitio de DR, primero debe eliminar la configuración existente y, a continuación, crear una nueva con la nueva ubicación.

Para obtener más información sobre Disaster Recovery en Acronis Cyber Protect Cloud, consulte "Disaster Recovery para Cyber Protect Cloud" (p. 7).

Para obtener más información sobre Disaster Recovery en Microsoft Azure, consulte "Disaster Recovery para Microsoft Azure" (p. 104).

Disaster Recovery para Cyber Protect Cloud

Disaster Recovery para Cyber Protect Cloud tiene las siguientes características:

- La ubicación del sitio de DR es Cyber Protect Cloud.
- Las copias de seguridad (puntos de recuperación) de los servidores protegidos se almacenan en Cyber Protect Cloud.

La funcionalidad clave

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

- Gestionar el servicio Disaster Recovery desde una única consola
- Ampliar hasta 23 redes locales a la nube mediante un túnel VPN seguro
- Establecer la conexión al sitio en la nube sin necesidad de implementar dispositivos VPN[1] (el modo solo en la nube)
- Establecer la conexión de punto a sitio[2] en sus sitios locales[3] y en la nube[4]
- Proteger su equipo con el uso de servidores de recuperación[5] en la nube
- Proteger aplicaciones y dispositivos con el uso de servidores principales[6] en la nube
- Realizar operaciones de recuperación ante desastres automáticas para copias de seguridad cifradas
- Realizar una prueba de conmutación por error en la red aislada
- Utilice runbooks[7] para automatizar el despliegue en el entorno de producción en la nube

[1] Un equipo virtual especial que permite la conexión entre la red local y el sitio en el cloud mediante un túnel de VPN seguro. El dispositivo VPN se implementa en el sitio local.
[2] Una conexión VPN segura desde el exterior hacia los sitios locales y el cloud mediante sus dispositivos endpoint (como un ordenador de sobremesa o un portátil).
[3] La infraestructura local implementada en las instalaciones de su empresa.
[4] Sitio remoto alojado en el cloud, usado para la ejecución de infraestructuras de recuperación en caso de desastres.
[5] Una réplica en equipo virtual del equipo original basada en las copias de seguridad del servidor protegido almacenadas en el cloud. Los servidores de recuperación se utilizan para trasladar cargas de trabajo desde los servidores originales en caso de desastre.
[6] Un equipo virtual que no tiene un equipo enlazado en el sitio local (como un servidor de recuperación). Los servidores principales se utilizan para proteger una aplicación o para ejecutar varios servicios auxiliares (como un servidor web).
[7] Escenario planificado que consiste en pasos configurables que automatizan las acciones de recuperación ante desastres.

Requisitos de software para Disaster Recovery para Cyber Protect Cloud

Sistemas operativos compatibles

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

- CentOS 6.6, 7.x, 8.x
- Debian 9.x, 10.x, 11.x
- Red Hat Enterprise Linux 6.6, 7.x, 8.x
- Ubuntu 18.04, 20.x, 21.x, 22.04, 22.10
- Oracle Linux 7.3 and 7.9 with Unbreakable Enterprise Kernel
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019: todas las opciones de instalación, excepto Nano Server
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server
- AlmaLinux 8.x, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5
- Rocky Linux 9.x, 8.x

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

Nota
La protección con un servidor de recuperación se ha probado para máquinas virtuales de Microsoft Azure con los siguientes sistemas operativos:

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019: todas las opciones de instalación, excepto Nano Server
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server
- Servidor Ubuntu 20.04 LTS - 2.ª generación (canónico). Para obtener más información sobre el acceso a la consola del servidor de recuperación, consulte este artículo de la base de conocimientos.

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, 6.7, 7.0
- Windows Server 2008 R2 con Hyper-V
- Windows Server 2012/2012 R2 con Hyper-V
- Windows Server 2016 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Windows Server 2022 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Máquinas virtuales basadas en Kernel (KVM): solo invitados completamente virtualizados (HVM). No se admiten invitados paravirtualizados (PV).
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2
- Nutanix Acropolis Hypervisor (AHV) con Sistema Operativo Nutanix Acropolis (AOS): 6.5, 6.6, 6.7, 6.8, 6.10

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

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 con Hyper-V
- Windows Server 2012/2012 R2 con Hyper-V
- Windows Server 2016 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Windows Server 2022 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

Se admite las cargas de trabajo de Linux que tienen copias de seguridad sin agente desde un SO invitado y tienen volúmenes con las configuraciones de Logical Volume Manager (LVM).

Se admite las cargas de trabajo de Windows que tienen copias de seguridad sin agente desde un SO invitado y tienen configuraciones de discos dinámicos (LDM).

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

Limitaciones

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

1. Plataformas no compatibles:
   - Agentes para Virtuozzo.
   - macOS
   - Los sistemas operativos de los equipos de escritorio Windows no son compatibles con las condiciones de los productos de Microsoft.
   - Windows Server Azure Edition

     Azure Edition es una versión especial de Windows Server que fue creada específicamente para ejecutarse ya sea como una máquina virtual (MV) de Azure IaaS en Azure o como una máquina virtual en un clúster de Azure Stack HCI. A diferencia de las ediciones Standard y Datacenter, Azure Edition no tiene licencia para ejecutarse en hardware sin sistema operativo, Hyper-V de cliente de Windows, Hyper-V de Windows Server, hipervisores de terceros o nubes de terceros.
2. Configuraciones no compatibles:

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

   Linux
   - Sistemas de archivos sin tabla de partición.
   - Cargas de trabajo de Linux de las que se realiza una copia de seguridad con un agente de desde un SO invitado y que tienen volúmenes con las siguientes configuraciones avanzadas de Logical Volume Manager (LVM): Volúmenes segmentados, volúmenes replicados o volúmenes RAID 0, RAID 4, RAID 5, RAID 6 o RAID 10.

   Nota
   Las cargas de trabajo con varios sistemas operativos instalados no son compatibles.
3. Modos de inquilino no compatibles:
   - La recuperación ante desastres no está disponible cuando el modo de cumplimiento está habilitado para el inquilino.
4. Tipos de copias de seguridad no compatibles:

- Los puntos de recuperación de Protección continua de datos (CDP) no son compatibles.

  Importante
  Si crea un servidor de recuperación a partir de una copia de seguridad que tenga un punto de recuperación CDP, perderá los datos incluidos en este punto de recuperación durante la conmutación por recuperación o al crear una copia de seguridad de un servidor de recuperación.

- Las copias de seguridad de datos forenses no se pueden usar para crear servidores de recuperación.

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.

Producto de prueba de Disaster Recovery

Puede utilizar una versión de prueba de Acronis Disaster Recovery durante un período de 30 días. En este caso, Disaster Recovery tiene las siguientes limitaciones para los inquilinos de los partners:

- Sin acceso a Internet público para la recuperación y los servidores principales. No puede asignar direcciones IP públicas a los servidores.
- La VPN multisitio IPsec no está disponible.

Operaciones con máquinas virtuales de Microsoft Azure

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

Puede ejecutar la conmutación por error de las máquinas virtuales de Microsoft Azure para Acronis Cyber Protect Cloud. Para obtener más información, consulte "Realización de una conmutación por error" (p. 80).

Después de eso, puede ejecutar la conmutación tras recuperación desde Acronis Cyber Protect Cloud y de vuelta a las máquinas virtuales de Azure. Para obtener más información, consulte "Conmutación tras recuperación desde Cyber Protect Cloud a una máquina virtual de Azure" (p. 96).

Puede configurar una conectividad VPN multisitio IPsec entre Acronis Cyber Protect Cloud y la puerta de enlace VPN de Azure. Para obtener más información, consulte "Configuración de VPN de IPsec de varios sitios" (p. 33).

Limitaciones al usar el almacenamiento en la nube con redundancia geográfica

El almacenamiento en la nube con redundancia geográfica proporciona una ubicación secundaria para los datos de copias de seguridad. La ubicación secundaria es una región geográficamente distinta a la ubicación de almacenamiento primaria. La separación geográfica de las regiones garantiza que, en caso de que se produzca un desastre que afecte a una de las regiones e impida que se recuperen los datos de copias de seguridad, la otra región no se verá afectada y no se interrumpirán las operaciones.

Importante
El servicio de Disaster Recovery no se puede utilizar si se cambia la ubicación primaria de almacenamiento de copia de seguridad por una secundaria con redundancia geográfica.

Eliminación automática de entornos de clientes que no se usan en el sitio en la nube

El servicio de Disaster Recovery realiza el seguimiento del uso de entornos de cliente creados para la recuperación ante desastres y los elimina automáticamente si no se utilizan.

Los siguientes criterios se utilizan para definir si un inquilino cliente está activo:

- Actualmente, hay al menos un servidor en la nube o ha habido algún servidor en la nube en los últimos siete días.
  O
- La opción **Acceso mediante VPN al sitio local** está habilitada y, o bien se ha establecido el túnel OpenVPN de sitio a sitio, o bien se han reportado datos desde el dispositivo VPN en los últimos 7 días.

El resto de inquilinos se considera inquilinos inactivos. El sistema realiza lo siguiente para estos inquilinos:

- Se elimina la puerta de enlace de VPN, así como todos los recursos en la nube relacionados con el inquilino.
- Se elimina el registro del dispositivo VPN.

Los inquilinos inactivos se restauran al estado en el que no se había configurado la conectividad.

Trabajo con Disaster Recovery a Cyber Protect Cloud

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

El flujo de trabajo básico para utilizar la recuperación ante desastres es el siguiente:

1. Cree un servidor de recuperación de la carga de trabajo que desee proteger de una de las siguientes maneras:
   - a. Cree un plan de protección que incluya el módulo de **recuperación ante desastres** y el módulo de **copia de seguridad** con la configuración **Qué copiar** establecida en **Todo el equipo** o **Sistema y volúmenes de arranque**.
     b. Aplique el plan a sus dispositivos. Esto configurará automáticamente la infraestructura de recuperación ante desastres predeterminada. Para obtener más información, consulte Crear un plan de protección de recuperación ante desastres.

     Nota
     Los administradores de unidades no pueden crear, modificar ni aplicar planes de protección de recuperación ante desastres.

   - Configure la infraestructura en la nube de recuperación ante desastres manualmente y controle cada paso. Consulte "Creación de un servidor de recuperación" (p. 59).
2. Configure la conectividad con el sitio en la nube.
   - Modo solo en la nube
   - Conexión OpenVPN de sitio a sitio
   - Conexión VPN de IPsec de varios sitios
   - Conexión de punto a sitio
3. Configure la conmutación por error de prueba automatizada.
4. Ejecute una prueba de conmutación por error.
5. [Si ocurre un desastre] Realice una conmutación por error de producción.
6. [Después del desastre] Realice una conmutación tras recuperación al sitio local.
7. [Opcional] Configurar runbooks.

Creación de un plan de protección de recuperación ante desastres

El plan de protección de recuperación ante desastres es un plan de protección en el que el módulo **Recuperación ante desastres** está habilitado.

Al habilitar la función de recuperación ante desastres y aplicar el plan a sus dispositivos, automáticamente se crea la infraestructura de red en la nube (sitio en la nube). Para obtener más información, consulte "Infraestructura de red en la nube predeterminada" (p. 16).

Nota

- Al aplicar un plan de protección de recuperación ante desastres, se crea la infraestructura de red en la nube de recuperación únicamente en el caso de que no exista. Las redes existentes en la nube no se cambian ni se vuelven a crear.
- Después de configurar la recuperación ante desastres podrá realizar una prueba o la conmutación por error de producción desde cualquier punto de recuperación generado después de la creación del servidor de recuperación del dispositivo. Los puntos de recuperación (copias de seguridad) que se generaron antes de que el dispositivo estuviese protegido con la recuperación ante desastres (antes de crear el servidor de recuperación) no se pueden usar para la conmutación por error.
- No se puede habilitar un plan de protección para la recuperación ante desastres si no se puede detectar la dirección IP de un dispositivo. Por ejemplo, cuando se realizan copias de seguridad sin agente de máquinas virtuales y no se les asigna una dirección IP.
- Cuando aplica un plan de protección, se asignan las mismas redes y direcciones IP al sitio en la nube. La conectividad VPN de IPsec requiere que los segmentos de red en la nube y los sitios locales no se superpongan. Si se configura una conectividad VPN de IPsec de varios sitios y, a continuación, aplica un plan de protección a uno o varios dispositivos, debe actualizar de forma adicional las redes en la nube y reasignar las direcciones IP de los servidores en la nube. Para obtener más información, consulte "Reasignación de direcciones IP" (p. 52).

Para crear un plan de protección de recuperación ante desastres

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione los equipos que quiera proteger.
3. Haga clic en **Proteger** y, a continuación, en **Crear plan**.
   Se abre la configuración predeterminada del plan de protección.
4. Configure las opciones de copia de seguridad.
   Para usar la funcionalidad de recuperación ante desastres, el 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 la nube.
5. Active el interruptor que se encuentra junto al nombre del módulo para habilitar el módulo **Recuperación ante desastres**.
6. En el campo **Ubicación**, seleccione dónde crear la infraestructura de recuperación ante desastres.
7. Haga clic en **Crear**.
   El plan se crea y se aplica a los equipos seleccionados. Se crea la infraestructura de red predeterminada y los servidores de recuperación con parámetros predeterminados. Para obtener más información, consulte "Edición de la configuración predeterminada de un servidor de recuperación" (p. 15) y "Infraestructura de red en la nube predeterminada" (p. 16).

Qué hacer a continuación

- Puede editar la configuración predeterminada del servidor de recuperación. Para obtener más información, consulte "Edición de la configuración predeterminada de un servidor de recuperación" (p. 15).
- Puede editar la configuración predeterminada del servidor de red. Para obtener más información, consulte "Conectividad y redes" (p. 17).

Edición de la configuración predeterminada de un servidor de recuperación

Cuando cree y aplique un plan de protección de recuperación ante desastres, se creará un servidor de recuperación con la configuración predeterminada. Puede editar esta configuración predeterminada cuando sea necesario.

El siguiente procedimiento se aplica a los servidores de recuperación que se encuentran en Cyber Protect Cloud. Si desea configurar los ajustes de un servidor de recuperación que está ubicado en Microsoft Azure, siga los pasos que se describen en "Creación de servidores de recuperación en Microsoft Azure" (p. 123).

Nota
Se crea un servidor de recuperación únicamente en caso de que no exista. Los servidores de recuperación que ya existan no se cambian ni se vuelven a crear.

Pasos para editar la configuración predeterminada del servidor de recuperación

1. Vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione un dispositivo y haga clic en **Recuperación ante desastres**.
3. Pasos para editar la configuración predeterminada del servidor de recuperación.
   La configuración del servidor de recuperación se describe en la siguiente tabla.

Configuración	Valor predeterminado	Descripción
CPU y RAM	automático	El número de CPU virtuales y la cantidad de RAM del servidor de recuperación. La configuración predeterminada se determinará automáticamente según la configuración de la CPU y la RAM del dispositivo original.
Red en la nube	automático	Red en la nube a la que se conectará el servidor. Para obtener datos sobre cómo se configuran las redes en la nube, consulte Infraestructura de red en la nube.
Dirección IP en la	automático	Dirección IP que tendrá el servidor en la red

red de producción		productiva. La dirección IP del equipo original se establece de forma predeterminada.
Dirección IP de prueba	inválido	La dirección IP de prueba 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 VPN sustituirá la dirección IP de prueba por la dirección IP de producción mediante el protocolo NAT. La dirección IP de prueba no aparece especificada. La consola será la única forma de acceder al servidor durante una conmutación por error de prueba.
Acceso a Internet	habilitado	Habilite el servidor de recuperación para acceder a Internet durante una conmutación por error de prueba o real. De forma predeterminada, el puerto TCP 25 está denegado para las conexiones de salida.
Usar dirección pública	inválido	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 no usa una dirección IP pública, el servidor solo estará disponible en su red productiva. Para usar una dirección IP pública, debe habilitar el acceso a Internet. La dirección IP pública se mostrara cuando finalice la configuración. De forma predeterminada, el puerto TCP 443 está abierto para las conexiones de entrada.
Establecer el umbral de RPO	inválido	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.

Infraestructura de red en la nube predeterminada

La infraestructura de red en la nube que se crea automáticamente cuando aplica un plan de protección de recuperación ante desastres a recursos informáticos consta de los siguientes componentes:

- Un servidor de recuperación para cada dispositivo protegido.

  El servidor de recuperación es una máquina virtual en la nube que constituye una copia del dispositivo seleccionado.

  Para cada uno de los dispositivos seleccionados se crea un servidor de recuperación con la configuración predeterminada en el estado **En espera** (máquina virtual que no está en ejecución). El tamaño del servidor de recuperación se ajusta automáticamente según la CPU y la RAM del dispositivo protegido.
- Puerta de enlace VPN en el sitio de la nube.
- Redes en la nube a las que están conectados los servidores de recuperación.

El sistema comprueba la dirección IP de cada dispositivo y crea automáticamente redes en la nube adecuadas si no hay redes en la nube a las que se pueda adaptar una dirección IP. Si ya ha tiene redes en la nube existentes a las que se puedan adaptar las direcciones IP de los servidores de recuperación, las redes en la nube existentes no cambiarán ni se volverán a crear.

- Si no tiene ninguna red en la nube o ha configurado los ajustes de la recuperación ante desastres por primera vez, la entidad IANA configurará las redes en la nube con rangos máximos recomendados para uso privado (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) según el rango de direcciones IP de su dispositivo. Puede editar la máscara de red para reducir su red.
- Si tiene dispositivos en varias redes locales, la red del sitio en la nube puede convertirse en un superconjunto de redes locales. Puede volver a configurar las redes en la sección **Conectividad**. Consulte "Gestión de redes para OpenVPN de sitio a sitio" (p. 26).
- Si tiene que configurar la conectividad OpenVPN de sitio a sitio, descargue el dispositivo VPN y configúrelo. Consulte "Configuración de OpenVPN de sitio a sitio" (p. 24). Asegúrese de que los rangos de las redes en la nube coinciden con los de sus redes locales conectadas al dispositivo VPN.
- Para cambiar la configuración de red predeterminada, vaya a **Disaster Recovery** > **Conectividad**, o en el módulo **Recuperación ante desastres** del plan de protección, haga clic en **Ir a conectividad**.

Si revoca, elimina o desconecta el módulo **Recuperación ante desastres** de un plan de protección, los servidores de recuperación y las redes en la nube no se eliminarán automáticamente. Puede eliminar la infraestructura de recuperación ante desastres manualmente, en caso necesario.

Conectividad y redes

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

Disaster Recovery le permite definir los siguientes tipos de conectividad al sitio en la nube:

- **Modo solo en la nube**

  Este tipo de conexión no requiere la implementación de un dispositivo VPN en el sitio local.

Las redes locales y en el cloud son independientes. Este tipo de conexión implica la conmutación por error de todos los servidores protegidos del sitio local o bien la conmutación por error parcial de los servidores independientes que no necesitan comunicarse con el sitio local.

Los servidores en el cloud en el sitio en el cloud son accesibles a través de VPN de punto a sitio y de direcciones IP públicas (si están asignadas).

- **Conexión OpenVPN de sitio a sitio**

  Este tipo de conexión requiere la implementación de un dispositivo VPN en el sitio local.

  La conexión de OpenVPN de sitio a sitio le permite extender sus redes a la nube y conservar las direcciones IP.

  Su sitio local se conecta al sitio en el cloud por medio de un túnel VPN seguro. Este tipo de conexión es adecuado en caso de que sus servidores dependan en gran medida del sitio local, como puede suceder con un servidor web o un servidor de bases de datos. En caso de una conmutación por error parcial, al recrear uno de estos servidores en el sitio en el cloud mientras el otro se queda en el sitio local, podrán seguir comunicándose mediante un túnel VPN.

  Los servidores en el cloud en el sitio en el cloud son accesibles a través de la red local, de VPN de punto a sitio y de direcciones IP públicas (si están asignadas).

- **Conexión VPN de IPsec de varios sitios**

  Este tipo de conexión requiere un dispositivo VPN local compatible con IPsec IKE v2.

  Cuando inicie la configuración de la conexión VPN de IPsec de varios sitios, Disaster Recovery creará automáticamente una puerta de enlace de Cloud VPN con una dirección IP pública.

  Con la VPN de IPsec de varios sitios, sus sitios locales se conectan al sitio en la nube por medio de un túnel VPN de IPsec seguro.

  Este tipo de conexión es adecuada para los escenarios de Disaster Recovery cuando tiene uno o varios sitios locales que alojan cargas de trabajo críticas o servicios estrechamente dependientes.

  En caso de una conmutación por error parcial de uno de los servidores, se recreará dicho servidor en el sitio en la nube mientras que el resto se mantendrán en el sitio local, por lo que podrán seguir comunicándose mediante un túnel VPN de IPsec.

  En caso de una conmutación por error parcial de uno de los sitios locales, el resto seguirá operativo, por lo que podrán seguir comunicándose mediante un túnel VPN de IPsec.

- **Acceso de VPN remoto de punto a sitio**

  Un acceso remoto y seguro de la VPN de punto a sitio a sus cargas de trabajo de sitio local y en la nube desde fuera mediante su dispositivo de punto final.

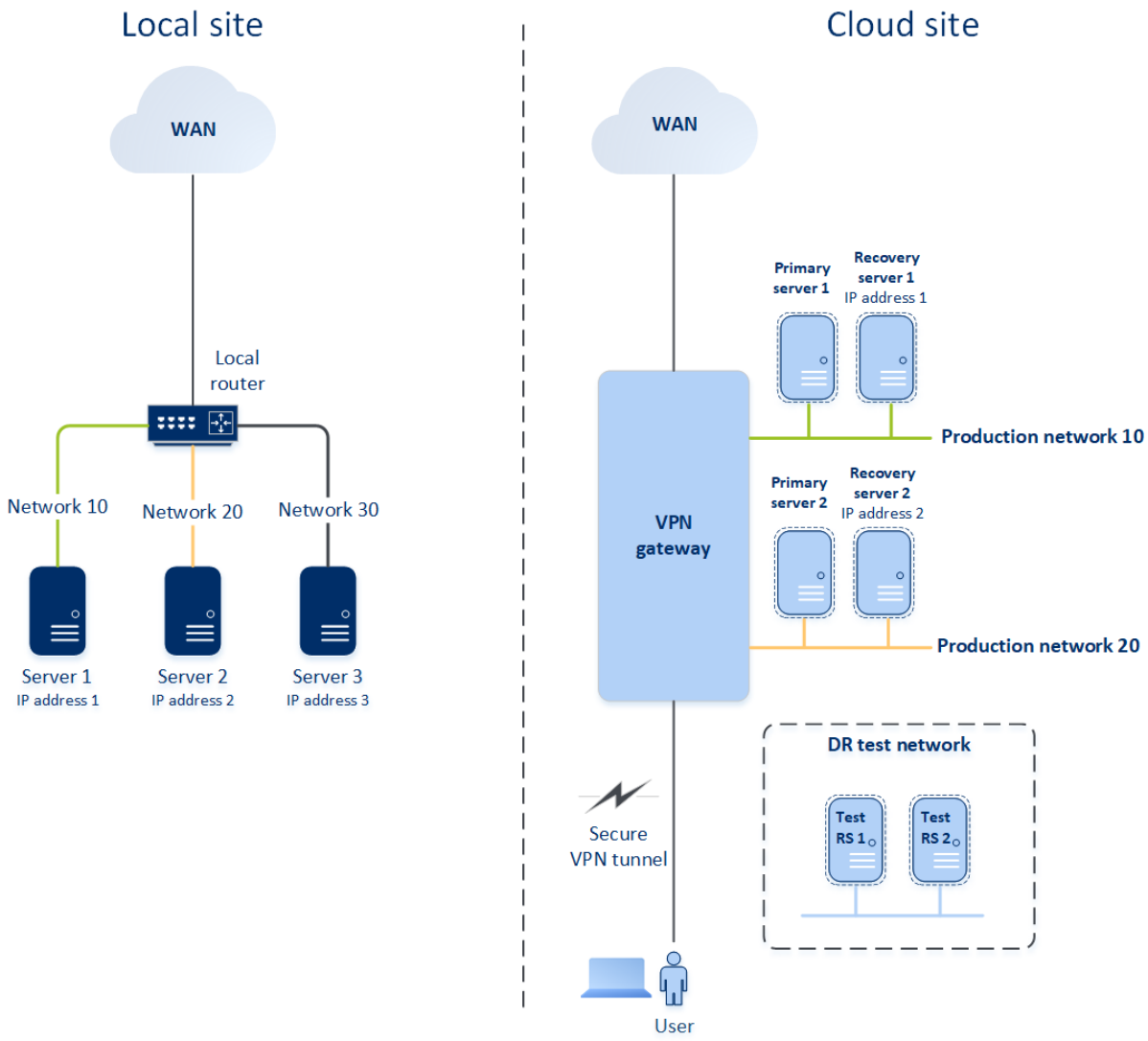
  Para el acceso en un sitio local, este tipo de conexión requiere la implementación de un dispositivo VPN en el sitio local.

Modo solo en la nube

El modo solo en el cloud no requiere la implementación de un dispositivo VPN en el sitio local. Implica que tiene dos redes independientes: una en el sitio local y otra en el sitio en el cloud. La enrutación se realiza con el enrutador en el sitio de la nube.

Cómo funciona el enrutamiento

Si se establece el modo solo en la nube, el enrutamiento se realiza con el enrutador en el sitio de la nube, de forma que los servidores de diferentes redes en la nube puedan comunicarse entre ellos.



Configuración del modo solo en la nube

El modo "Solo en la nube" es el tipo de conectividad predeterminado que se crea automáticamente cuando aplica un plan de recuperación ante desastres a un recurso informático.

Para configurar una conexión en el modo "Solo en la nube"

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Seleccione **Solo en la nube** y haga clic en **Configurar**.
   Como resultado, la puerta de enlace de VPN y la red de la nube con la dirección y la máscara definidas se despliegan en el sitio en la nube.

Gestión de redes en el modo Solo en la nube

Puede añadir y gestionar hasta 23 redes en la nube.

Añadir red

Para agregar una nueva red al cloud:

1. Vaya a **Disaster Recovery** > **Conectividad**.
2. En el **Sitio en la nube**, pulse **Añadir red en la nube**.
3. Defina los parámetros de red en la nube: la máscara y dirección de red, y haga clic en **Listo**.

Como resultado, la red en la nube adicional se creará en el sitio de la nube con la máscara y la dirección definidas.

Eliminar red

Requisitos previos

Se eliminarán todos los servidores de nube de la red que desea eliminar.

Para eliminar una red en la nube

1. Vaya a **Disaster Recovery** > **Conectividad**.
2. En **Sitio en el cloud**, haga clic en la dirección de red que desea eliminar.
3. Haga clic en **Eliminar** y confirme la operación.

Cambiar parámetros

Para cambiar los parámetros de la red en el cloud:

1. Vaya a **Disaster Recovery** > **Conectividad**.
2. En **Sitio en el cloud**, haga clic en la dirección de red que desea editar.
3. Haga clic en **Editar**.
4. Defina la máscara y dirección de red y haga clic en **Listo**.

Conexión OpenVPN de sitio a sitio

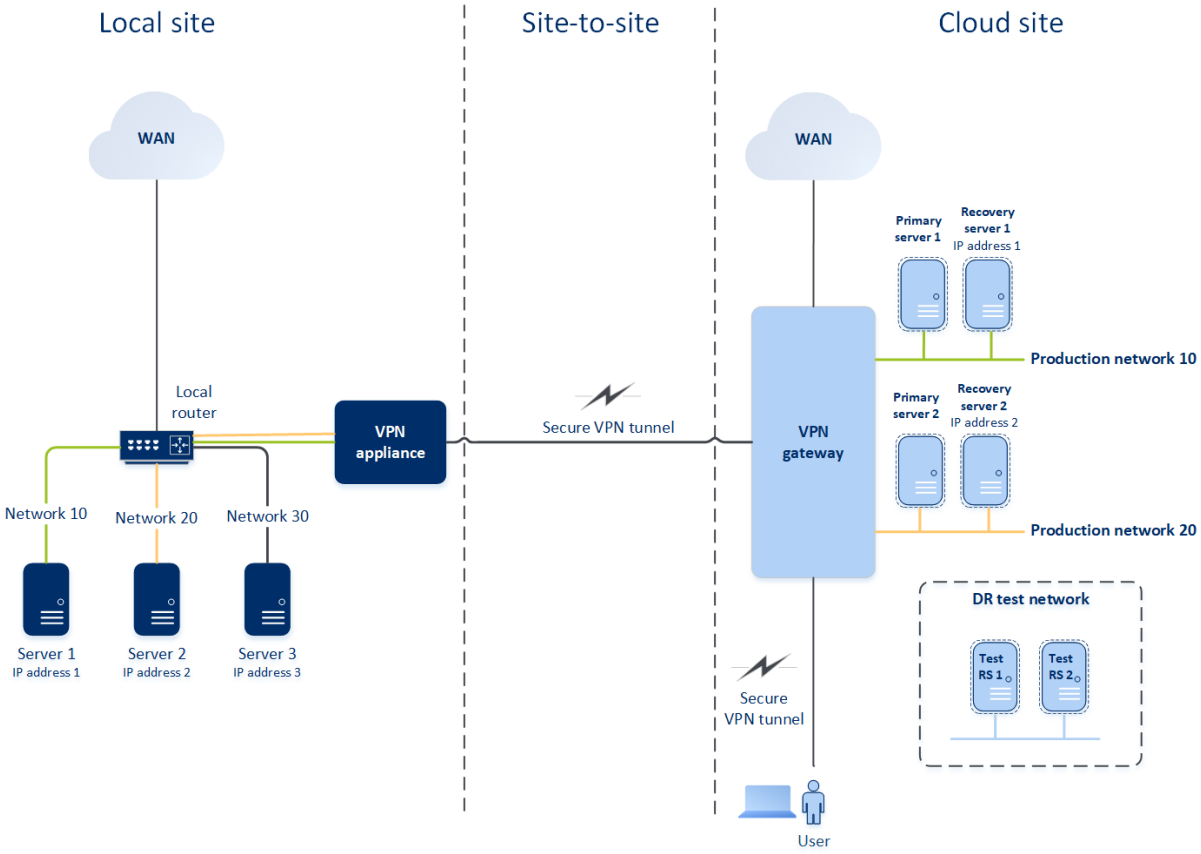
Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Para entender cómo funcionan las redes en Disaster Recovery, pensaremos en un caso en el que tiene tres redes, cada una con un equipo en el sitio local. Va a configurar la protección frente a desastres para dos redes, Red 10 y Red 20.

En el siguiente diagrama, puede ver el sitio local donde se alojan sus equipos y el sitio en la nube donde se inician los servidores en la nube en caso de desastre.

La solución Disaster Recovery le permite realizar una conmutación por error de toda la carga de trabajo de los equipos dañados en el sitio local a los servidores de nube que se encuentran en la nube.

Puede añadir y gestionar hasta 23 redes en la nube.



Para establecer una conectividad OpenVPN de sitio a sitio entre el sitio local y el sitio en la nube, se usa un **dispositivo VPN** y una **puerta de enlace de VPN**.

Cuando comience a configurar la conexión OpenVPN de sitio a sitio en la consola de Cyber Protect, se desplegará automáticamente la puerta de enlace de VPN en el sitio de la nube.

Después del despliegue de la puerta de enlace de VPN, debe hacer lo siguiente:

- Despliegue el dispositivo VPN en su sitio local.
- Añada las redes que desee proteger.
- Registre el dispositivo VPN en la nube.

Disaster Recovery creará una réplica de su red local en la nube. Se establecerá un túnel VPN seguro entre el dispositivo VPN y la puerta de enlace VPN. Este túnel VPN proporcionará la extensión de su red local a la nube. Las redes de producción en la nube se conectarán con sus redes locales. Los

servidores locales y de nube se comunicarán a través de este túnel VPN como si estuvieran en el mismo segmento de Ethernet. El enrutamiento se realizará a través de su router local.

Para que cada equipo de origen quede protegido, debe crear un servidor de recuperación en el sitio en la nube. Se queda en estado **En espera** hasta que ocurre un evento de conmutación por error. Si sucede un desastre e inicia un proceso de conmutación por error (en el **modo de producción**), el servidor de recuperación que representa la copia exacta de su equipo protegido se inicia en la nube. Puede tener la misma dirección IP asignada que el equipo de origen e iniciarse en el mismo segmento de Ethernet. Sus clientes pueden seguir trabajando con el servidor sin notar ningún cambio en segundo plano.

También puede iniciar un proceso de conmutación por error en el **modo de prueba**. Esto quiere decir que el equipo de origen continúa funcionando y, al mismo tiempo, se inicia en la nube el servidor de recuperación correspondiente con la misma dirección IP. Para evitar conflictos debido a la dirección IP, se crea una red virtual especial en la nube, la **red de prueba**. La red de prueba se aísla para evitar que se duplique la dirección IP del equipo de origen en un segmento de Ethernet. Para acceder al servidor de recuperación en el modo de prueba de conmutación por error, debe asignar la **Dirección IP de prueba** al servidor de recuperación al crearlo. Se pueden especificar otros parámetros para el servidor de recuperación que también puede configurar.

Cómo funciona el enrutamiento

Cuando se establece una conexión de sitio a sitio, el enrutamiento entre redes en la nube se realiza con su enrutador local. El servidor VPN no lleva a cabo enrutamientos entre los servidores en la nube localizados en diferentes redes. Si un servidor de nube de una red quiere comunicarse con un servidor de otra red en la nube, el tráfico pasará a través del túnel VPN del enrutador local del sitio local. Después, el enrutador local lo enruta hacia otra red y vuelve a través del túnel al servidor de destino del sitio en la nube.

Puerta de enlace de VPN

Un componente importante que permite la comunicación entre los sitios locales y en la nube es la puerta de enlace del VPN. Es una máquina virtual en la nube en el que está instalado software especial y la red se configura de forma específica. La puerta de enlace del VPN realiza las siguientes funciones:

- Conecta los segmentos de Ethernet de su red local y de producción en la nube en el modo L2.
- Proporciona reglas de tablas de IP y EB.
- Funciona como enrutador y NAT predeterminados para los equipos en las redes de prueba y producción.
- Funciona como servidor DHCP. Todos los equipos en las redes de producción y prueba obtienen la configuración de red (direcciones IP, configuración del DNS) por medio de DHCP. Un servidor en la nube obtendrá cada vez la misma dirección IP del servidor DHCP. Si necesita establecer la configuración de DNS personalizada, póngase en contacto con el equipo de soporte técnico.
- Funciona como DNS para almacenar archivos en la memoria caché.

Configuración de red de la puerta de enlace de VPN

La puerta de enlace de VPN tiene varias interfaces de red:

- Interfaz externa, conectada a Internet.
- Interfaces de producción, conectadas a las redes de producción.
- Interfaz de prueba, conectada a la red de prueba.

Además, se añaden dos interfaces virtuales para las conexiones de punto a sitio y de sitio a sitio.

Cuando se implementa e inicializa la puerta de enlace de VPN, se crean los puentes: uno para la interfaz externa y otro para las interfaces de cliente y producción. Aunque el puente entre cliente y producción y la interfaz de prueba usen las mismas direcciones IP, la puerta de enlace de VPN puede enrutar paquetes correctamente mediante una técnica específica.

Dispositivo VPN

El **dispositivo VPN** es una máquina virtual en el sitio local en el que se instala Linux, software especial y una configuración de red especial. Permite la comunicación entre los sitios local y en la nube.

Habilitación de la conectividad de sitio a sitio

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede habilitar la conectividad de sitio a sitio en los siguientes casos:

- Si necesita que los servidores en el cloud en el sitio en el cloud se comuniquen con los servidores en el sitio local.
- Si, después de una conmutación por error al cloud, la infraestructura local se recupera y quiere realizar una conmutación por recuperación de sus servidores al sitio local.

Para habilitar la conectividad de sitio a sitio

1. Vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades** y luego habilite la opción **Conexión de sitio a sitio**.

Como resultado, se habilita la conexión de sitio a sitio VPN entre los sitios local y en la nube. El servicio Disaster Recovery obtiene la configuración de red del dispositivo VPN y extiende las redes locales al sitio en la nube.

Configuración de OpenVPN de sitio a sitio

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Requisitos del dispositivo VPN

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 una conexión OpenVPN de sitio a sitio

El dispositivo VPN amplía su red local a la nube mediante un túnel de VPN seguro. Este tipo de conexión se suele llamar conexión "de sitio a sitio" (S2S). Puede seguir el procedimiento siguiente o ver el tutorial en vídeo.

Para configurar una conexión mediante el dispositivo VPN

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Seleccione **Conexión OpenVPN de sitio a sitio** y haga clic en **Configurar**.
   El sistema empieza a implementar la puerta de enlace de VPN en la nube. Este procedimiento tardará un tiempo. mientras tanto, puede continuar con el siguiente paso.

   Nota
   La puerta de enlace de VPN se proporciona sin ningún cargo adicional. Se eliminará si la funcionalidad de Disaster Recovery no se usa, es decir, si no hay ningún servidor principal ni de recuperación en la nube durante siete días.

3. En el bloque **Dispositivo VPN**, pulse 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. Asimismo, le recomendamos que habilite la **Memoria dinámica** para el 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 Cyber Protection.

   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 Cyber Protect 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 VPN y comienza a transmitir información sobre las redes de todas las interfaces activas al servicio Disaster Recovery. La consola de Cyber Protect muestra las interfaces basándose en la información del dispositivo VPN.

Gestión de la configuración del dispositivo VPN

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

En la pestaña **Disaster Recovery** > **Conectividad**, puede:

- Descargar archivos de registro.
- Cancelar el registro del dispositivo (si necesita restablecer la configuración del dispositivo VPN o cambiar al modo Solo en la nube).

Para acceder a esta configuración, haga clic en el icono **i** del bloque **Dispositivo VPN**.

En la consola del dispositivo VPN, puede hacer lo siguiente:

- Cambiar la contraseña del dispositivo.
- Ver o cambiar la configuración de red y definir la interfaz que utilizará como WAN para la conexión a Internet.
- Registrar la cuenta o cambiar su registro (repitiéndolo).
- Reiniciar el servicio VPN.
- Reiniciar el dispositivo VPN.
- Ejecutar el comando del shell de Linux (solo en casos avanzados de resolución de problemas).

Gestión de redes para OpenVPN de sitio a sitio

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

Puede añadir y gestionar hasta 23 redes en la nube.

Adición de redes

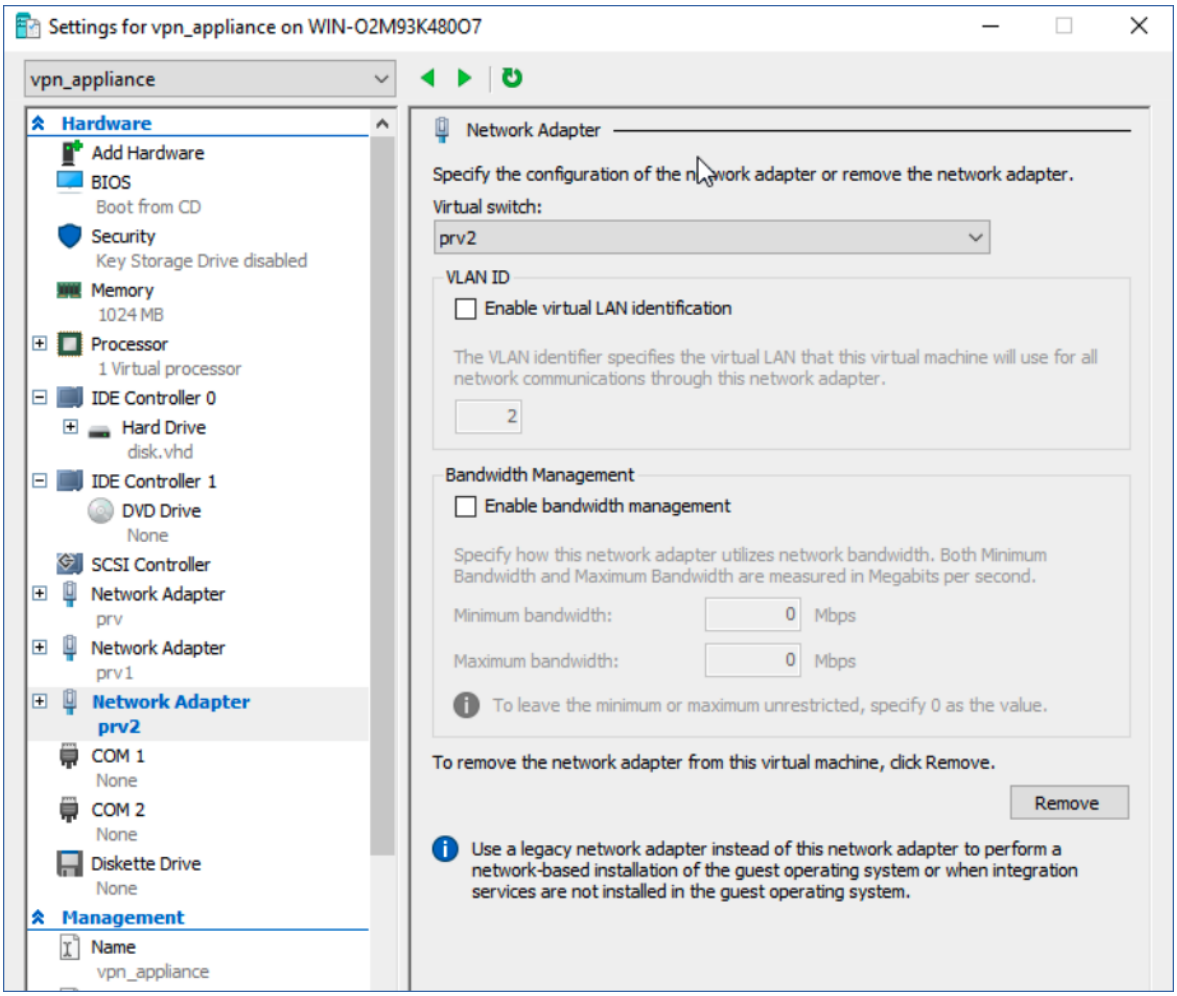
Requisitos previos

La conectividad Open VPN de sitio a sitio está configurada, según se indica en "Configuración de OpenVPN de sitio a sitio" (p. 24).

Pasos para añadir una red en el sitio local y extenderla a la nube

1. En el dispositivo VPN, configure la nueva interfaz de red con la red local que desea extender al cloud.
2. [Opcional] Si desea añadir una o más redes, por cada red adicional, añada una interfaz de red virtual (adaptador de red) a la máquina virtual en la que se está ejecutando el dispositivo virtual.

   El siguiente ejemplo muestra cómo hacerlo en el caso de una máquina virtual que se está ejecutando en un hipervisor de Hyper-V.



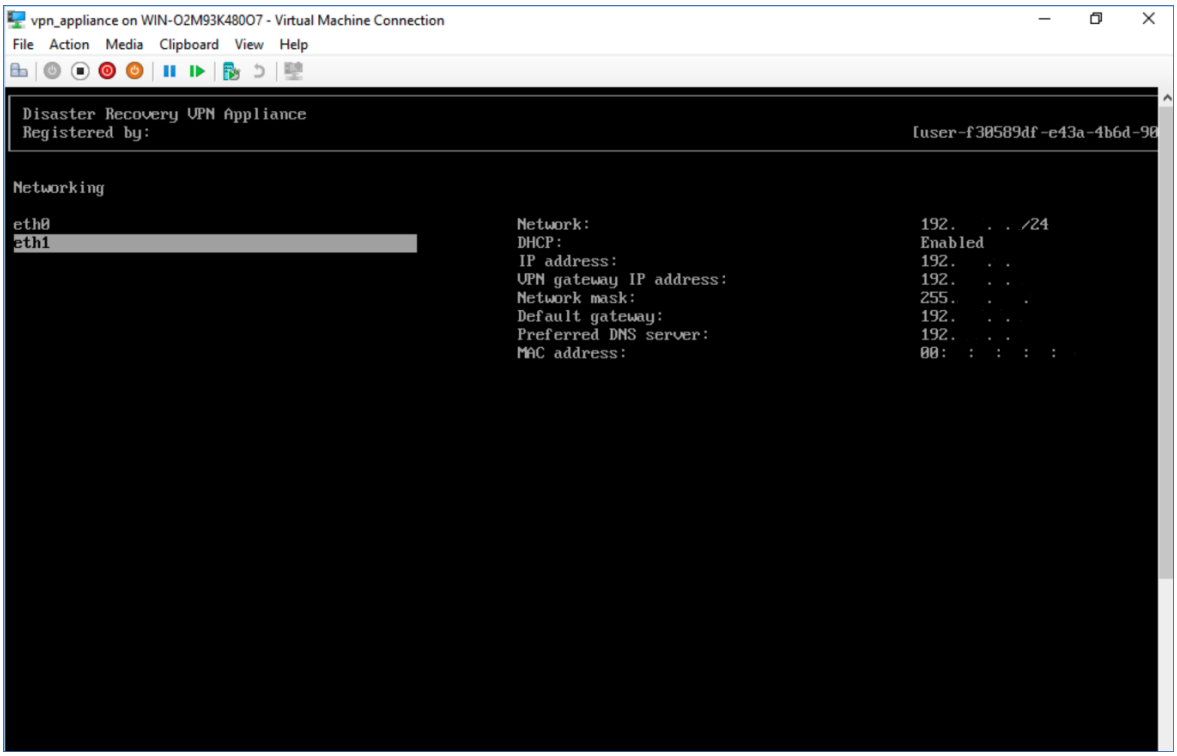
Nota

Los nuevos adaptadores de red virtuales deben configurarse con la red virtual local que desea extender a la nube.

3. Inicie sesión en la consola del dispositivo VPN y, a continuación, en la sección **Conexión a redes virtuales**, configure los ajuste de red para una de las interfaces (adaptadores).

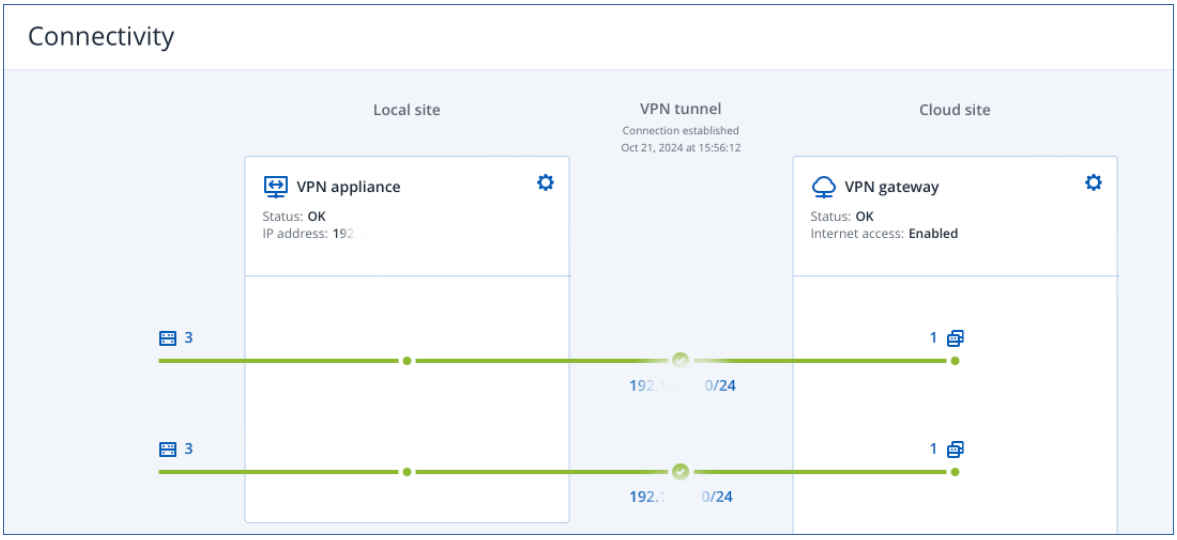
Nota

- La configuración de la dirección IP es obligatoria únicamente para una de las interfaces de red virtuales para habilitar el acceso a Internet. Puede omitir la configuración de la dirección IP para las otras interfaces de red.
- El modo promiscuo y las transmisiones falsificadas o suplantación de direcciones MAC deben estar habilitados para cada adaptador. Para obtener más información, consulte este artículo de la base de conocimientos.



El dispositivo VPN comienza automáticamente a transmitir información sobre las redes de todas las interfaces activas a Disaster Recovery.

4. Inicie sesión en la consola de Cyber Protect y vaya a **Recuperación ante desastres** > **Conectividad**.



Todas las redes locales se extienden automáticamente al sitio en la nube.

Eliminar red

Para eliminar una red extendida al cloud:

1. Inicie sesión en la consola del dispositivo VPN.
2. En la sección **Redes**, seleccione la interfaz que desea eliminar y haga clic en **Borrar**

configuración de red.

3. Confirme la operación.

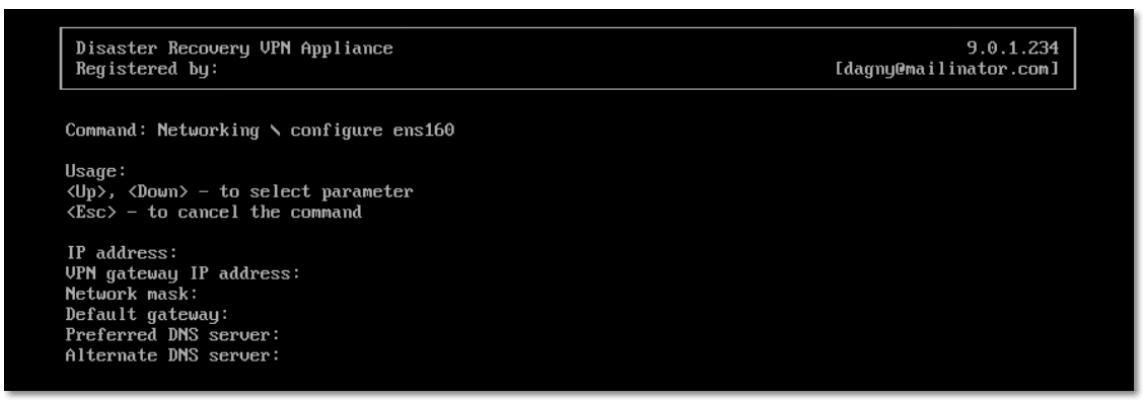
Como resultado, se detendrá la extensión de red local al la nube mediante un túnel de VPN seguro. Esta red funcionará como un segmento independiente de la nube. Si esta interfaz se usa para pasar el tráfico hacia o desde el sitio en el la nube, todas sus conexiones de red hacia o desde el sitio en la nube se desconectarán.

Cambiar parámetros

Para cambiar los parámetros de red:

1. Inicie sesión en la consola del dispositivo VPN.
2. En la sección **Redes**, seleccione la interfaz que desea editar.
3. Haga clic en **Editar configuración de red**.
4. Seleccione una de las opciones:
   - Para la configuración automática de la red mediante DHCP, haga clic en **Usar DHCP** y confirme la operación.
   - Para configurar la red manualmente, haga clic en **Establecer dirección IP estática**, establezca la configuración y, a continuación, haga clic en **Introducir**.

Configuración	Descripción
Dirección IP	Dirección IP de la interfaz en la red local.
Dirección IP de la puerta de enlace de VPN	Dirección IP especial que se reserva para el segmento en la nube de la red con el fin de que el servicio de Disaster Recovery funcione correctamente.
Máscara de red	Máscara de red de la red local.
Puerta de enlace predeterminada	Entrada predeterminada en el sitio local.
Servidor DNS preferido	Servidor DNS principal del sitio local.
Servidor DNS alternativo	Servidor DNS secundario del sitio local.



Permitir tráfico DHCP a través de VPN L2

Si los dispositivos de su sitio local obtienen su dirección IP de un servidor DHCP, puede proteger dicho servidor con Disaster Recovery, conmutarlo por error a la nube y, a continuación, permitir que el tráfico DHCP circule por una VPN L2. De este modo, su servidor DHCP se ejecutará en la nube, pero continuará asignando direcciones IP a sus dispositivos locales.

Requisitos previos

Se debe establecer un tipo de conectividad VPN L2 de sitio a sitio para el sitio en la nube.

Para permitir el tráfico DHCP a través de la conexión VPN L2

1. Vaya a **Disaster Recovery** > pestaña **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Habilite el conmutador **Permitir tráfico DHCP a través de VPN L2**.

Cambio de VPN de sitio a sitio OpenVPN a VPN IPsec de varios sitios

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede cambiar fácilmente de una conexión OpenVPN de sitio a sitio a una conexión VPN de IPsec de varios sitios y al contrario.

Cuando cambia el tipo de conectividad, las conexiones VPN activas se eliminan, pero la configuración de la red y de los servidores en la nube se conservan. Sin embargo, puede que necesite reasignar las direcciones IP de las redes y los servidores en la nube.

La siguiente tabla compara las características básicas de la conexión OpenVPN de sitio a sitio y la conexión VPN de IPsec de varios sitios.

	OpenVPN de sitio a sitio	**VPN de IPsec de varios sitios**
Soporte técnico del sitio local	Único	Único, múltiple
Modo de puerta de enlace de VPN	L2 Open VPN	L3 IPsec VPN
Segmentos de red	Amplía la red local a la red en la nube	Las redes locales y los segmentos de las redes en la nube no deben superponerse
Compatible con el acceso de	Sí	No

	OpenVPN de sitio a sitio	VPN de IPsec de varios sitios
punto a sitio al sitio local		
Compatible con el acceso de punto a sitio al sitio en la nube	Sí	Sí
Requiere un elemento de oferta de IP pública	No	Sí

Para cambiar de una conexión OpenVPN de sitio a sitio a una conexión VPN de IPsec de varios sitios

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Haga clic en **Cambiar a VPN de IPsec de varios sitios**.
4. Haga clic en **Reconfigurar**.
5. Reasigne las direcciones IP de la red y los servidores en la nube.
6. Configurar los ajustes de conexión de IPsec de varios sitios.

Deshabilitación de la conexión de sitio a sitio

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Si no necesita que los servidores de nube del sitio en la nube se comuniquen con los servidores del sitio local, puede deshabilitar la conexión de sitio a sitio.

Pasos para deshabilitar la conectividad de sitio a sitio

1. Vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades** y luego deshabilite la opción **Conexión de sitio a sitio**.

El sitio local se desconectará del sitio en el cloud.

Solucionar problemas en la conectividad Open VPN de sitio a sitio

Cuando experimente problemas de conectividad con su sitio Open VPN de sitio a sitio, puede solucionar problemas y, a continuación, corregir los errores informados o enviar la información al equipo de soporte para su análisis y asistencia.

Para solucionar problemas de conectividad Open VPN de sitio a sitio

1. Abra la interfaz gráfica del dispositivo VPN.
2. En **Comandos**, seleccione **Resolución de problemas** y, a continuación, pulse **Intro**.
3. En la interfaz de línea de comandos, en la línea **¿Desea ejecutar el diagnóstico para la conexión de sitio a sitio [S/N]**, escriba **S** y, a continuación, pulse **Intro**.
   Se inicia la herramienta de diagnóstico. Si se detecta un problema, verá un error correspondiente y una descripción detallada. Puede copiar el texto que aparece o tomar una captura de pantalla y enviarla al equipo de soporte para obtener asistencia.

Conexión VPN de IPsec de varios sitios

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede utilizar la conectividad VPN de IPsec de varios sitios para conectar un solo sitio local o varios sitios locales a Disaster Recovery mediante una conexión VPN de IPsec L3 segura.

Este tipo de conectividad es útil para escenarios de Disaster Recovery si tiene uno de los siguientes casos:

- Tiene un sitio local con cargas de trabajo críticas.
- tiene varios sitios locales con cargas de trabajo críticas. Por ejemplo, oficinas en diferentes ubicaciones.
- utiliza sitios de software de terceros o sitios de proveedor de servicios gestionados y se conecta a ellos mediante un túnel VPN IPsec.

Para establecer una comunicación VPN de IPsec de varios sitios entre el sitio local y el sitio en la nube, se usa una **puerta de enlace de VPN**. Cuando comience a configurar la conexión VPN de IPsec de varios sitios en la consola de Cyber Protect, se implementará la puerta de enlace de VPN automáticamente en el sitio de la nube. Debe configurar los segmentos de red en la nube y asegurarse de que no se superpongan con los segmentos de la red local. Se establece un túnel VPN seguro entre los sitios locales y el sitio en la nube. Los servidores locales y en la nube pueden comunicarse mediante este túnel VPN si se encuentran todos en el mismo segmento de Ethernet.

Nota
Cuando se utiliza una conexión VPN de IPsec de varios sitios, la puerta de enlace VPN se asigna automáticamente una dirección IP pública.

Para que cada equipo de origen quede protegido, debe crear un servidor de recuperación en el sitio en la nube. Se queda en estado **En espera** hasta que sucede un evento de conmutación por error. Si sucede un desastre e inicia un proceso de conmutación por error (en el **modo de producción**), el servidor de recuperación que representa la copia exacta de su equipo protegido se inicia en la nube. Sus clientes pueden seguir trabajando con el servidor sin notar ningún cambio en segundo plano.

También puede iniciar un proceso de conmutación por error en el **modo de prueba**. Esto quiere decir que el equipo de origen continúa funcionando y, al mismo tiempo, se inicia en la nube el servidor de recuperación correspondiente en una red virtual especial que se crea en la nube, la **red de prueba**. La red de prueba se aísla para evitar que se dupliquen las direcciones IP en el resto de los segmentos de red en la nube.

Puerta de enlace de VPN

El principal componente que permite la comunicación entre los sitios locales y el sitio en la nube es la **puerta de enlace de VPN**. Es un equipo virtual en el cloud en el que se instala software especial, y la red se configura de forma específica. La puerta de enlace de VPN realiza las siguientes funciones:

- Conecta los segmentos de Ethernet de su red local y de producción en la nube en el modo IPsec L3.
- Funciona como enrutador y NAT predeterminados para los equipos en las redes de prueba y producción.
- Funciona como servidor DHCP. Todos los equipos en las redes de producción y prueba obtienen la configuración de red (direcciones IP, configuración del DNS) por medio de DHCP. Un servidor en la nube obtendrá cada vez la misma dirección IP del servidor DHCP.

  Si lo prefiere, puede establecer una configuración de DNS personalizada. Para obtener más información, consulte "Configuración de servidores DNS personalizados" (p. 53).
- Funciona como DNS para almacenar archivos en la memoria caché.

Cómo funciona el enrutamiento

El enrutamiento entre las redes en la nube se realiza con el enrutador en el sitio en la nube, de forma que los servidores de diferentes redes en esta puedan comunicarse entre ellos.

Configuración de VPN de IPsec de varios sitios

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede configurar la conexión VPN de IPsec de varios sitios de dos formas:

- Desde la pestaña **Disaster Recovery** > **Conectividad**.
- Aplicar un plan de protección en uno o varios dispositivos y luego cambiar de forma manual de la conexión OpenVPN de sitio a sitio creada de forma automática a una conexión VPN de IPsec de varios sitios, configurando los ajustes de VPN de IPsec de varios sitios y reasignando las direcciones IP.

Pestaña Conectividad

Pasos para configurar una conexión VPN de IPsec de varios sitios desde la pestaña Conectividad

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. En la sección **Conexión VPN de varios sitios**, haga clic en **Configurar**.
   Una puerta de enlace de VPN se implementa en el sitio en la nube.
3. Configure los ajustes de VPN de IPsec de varios sitios.

Plan de protección

Pasos para configurar una conexión VPN de IPsec de varios sitios desde un plan de protección

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Aplique un plan de protección a uno o varios dispositivos de la lista.
   El servidor de recuperación y los ajustes de infraestructura en la nube se configuran de manera automática para la conectividad OpenVPN de sitio a sitio.
3. Vaya a **Disaster Recovery** > **Conectividad**.
4. Haga clic en **Mostrar propiedades**.
5. Haga clic en **Cambiar a VPN de IPsec de varios sitios**.
6. Configure los ajustes de VPN de IPsec de varios sitios.
7. Reasigne las direcciones IP de la red y los servidores en la nube.

Configuración de los ajustes de VPN de IPsec de varios sitios

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Después de configurar una VPN de IPsec de varios sitios, debe configurar los ajustes del sitio en la nube y los sitios locales en la pestaña **Disaster Recovery** > **Conectividad**.

Requisitos previos

- Se ha configurado la conectividad VPN de IPsec de varios sitios. Para obtener más información sobre la configuración de la conectividad VPN de IPsec de varios sitios, consulte "Configuración de VPN de IPsec de varios sitios" (p. 33).
- Cada puerta de enlace de VPN de IPsec local tiene una dirección IP pública.
- Su red en la nube tiene suficientes direcciones IP para los servidores en la nube que son copias de sus equipos protegidos (en la red de producción) y para los servidores de recuperación (con una o dos direcciones IP, según sus necesidades).
- [Si usa un cortafuegos entre los sitios locales y el sitio en la nube] Los siguientes protocolos IP y puertos UDP se admiten en los sitios locales: Protocolo IP ID 50 (ESP), Puerto UDP 500 (IKE) y Puerto UDP 4500.
- Se ha deshabilitado la configuración de NAT-T en el sitio local.

Para configurar una conexión VPN de IPsec de varios sitios

1. Añada una o más redes al sitio en la nube.
   a. Haga clic en **Añadir red**.

   Nota
   Cuando añada una red en la nube, se añadirá automáticamente la red de prueba correspondiente con la misma dirección y máscara de red para realizar conmutaciones por error de prueba. Los servidores en la nube de la red de prueba tendrán las mismas direcciones IP que en la red productiva en la nube. Si necesita acceder a un servidor en la nube desde la red productiva durante una conmutación por error de prueba, asigne una segunda dirección IP de prueba cuando cree un servidor de recuperación.

   b. En el campo **Dirección de red**, escriba la dirección IP de la red.

   Nota
   Asegúrese de que las redes de la nube no se solapen con ninguna red local en su entorno. De lo contrario, no se podrá establecer un túnel.

   c. En el campo **Máscara de red**, escriba la máscara de la red.
   d. Haga clic en **Agregar**.
2. Configure los ajustes de cada sitio local que quiera conectar al sitio en la nube, de acuerdo con las recomendaciones de los sitios locales. Para obtener más información sobre estas recomendaciones, consulte "Recomendaciones generales para sitios locales" (p. 36).
   a. Haga clic en **Añadir conexión**.
   b. Introduzca un nombre para la puerta de enlace de VPN local.
   c. Introduzca la dirección IP pública de la puerta de enlace de VPN local.
   d. [Opcional] Introduzca una descripción de la puerta de enlace de VPN local.
   e. Haga clic en **Siguiente**.
   f. En el campo **Clave compartida previamente**, escríbala o haga clic en **Generar nueva clave compartida previamente** para utilizar un valor generado automáticamente.

   Nota
   Utilice la misma clave compartida previamente para las puertas de enlace de VPN locales y en la nube.

   g. Haga clic en **Configuración de seguridad de IPsec o IKE** para configurar los ajustes. Para obtener más información acerca de los ajustes que puede configurar, consulte "Configuración de seguridad de IPsec o IKE" (p. 37).

Nota
Puede utilizar los ajustes predeterminados, que se completan automáticamente, o valores personalizados. Solo se admiten las conexiones del protocolo IKEv2. La **acción de inicio** predeterminada cuando se establece la VPN es **Agregar** (su puerta de enlace de VPN local iniciará la conexión). Sin embargo, puede cambiarla a **Iniciar** (la puerta de enlace de la VPN en la nube iniciará la conexión) o **Dirigir** (adecuada para cortafuegos compatibles con la opción dirigir).

h. Configurar las **directivas de red**.
   Las directivas de red especifican las redes a las que se conecta la VPN IPsec. Escriba la dirección IP y la máscara de la red con el formato CIDR. Los segmentos de las redes locales y en la nube no deben superponerse.
i. Haga clic en **Guardar**.

Recomendaciones generales para sitios locales

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Cuando configure los sitios locales para la conectividad VPN de IPsec de varios sitios, tenga en cuenta las siguientes recomendaciones:

- En cada fase de IKE, establezca al menos uno de los valores que están configurados en el sitio en la nube para los siguientes parámetros: Algoritmo de cifrado, algoritmo de hash y números de grupo Diffie-Hellman.
- Habilite el secreto perfecto hacia adelante con al menos uno de los valores para los números de grupo Diffie-Hellman configurados en el sitio en la nube para la fase 2 de IKE.
- Configure los mismos valores para la **vida útil** de las fases 1 y 2 de IKE que los del sitio en la nube.
- No se admiten las configuraciones con NAT traversal (NAT-T). Deshabilite la configuración de NAT-T en el sitio local. Si no, no se podrá negociar la encapsulación de UDP adicional.
- La configuración **Acción de inicio** define qué lado inicia la conexión. El valor predeterminado **Agregar** significa que la conexión se inicia en el sitio local y que el sitio en la nube está esperando que se inicie la conexión. Cambie el valor a **Iniciar** si desea que la conexión se inicie en el sitio en la nube, o a **Dirigir** si desea que ambos lados puedan iniciar la conexión (adecuado para cortafuegos que son compatibles con la opción dirigir).

Para obtener más información y ejemplos de configuración para distintas soluciones, consulte:

- Esta serie de artículos de la base de conocimientos:
- Este vídeo de ejemplo:

Configuración de seguridad de IPsec o IKE

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La siguiente tabla proporciona más información sobre los parámetros de seguridad Psec/IKE.

Parámetro	Descripción
Algoritmo de cifrado	El algoritmo de cifrado que se utilizará para asegurarse de que los datos no se puedan ver mientras estén en tránsito. De manera predeterminada, se seleccionarán todos los algoritmos. Al menos uno de los algoritmos seleccionados debe estar configurado en su puerta de enlace local para cada fase de IKE.
Algoritmo de hash	El algoritmo de hash que se utilizará para verificar la integridad y la autenticidad de los datos. De manera predeterminada, se seleccionarán todos los algoritmos. Al menos uno de los algoritmos seleccionados debe estar configurado en su puerta de enlace local para cada fase de IKE.
Números de grupo Diffie-Hellman	Los números de grupo Diffie-Hellman definen la fuerza de la clave utilizada en el proceso de Internet Key Exchange (IKE). Los números de grupo más altos son más seguros, pero requieren más tiempo para que la clave se calcule. De manera predeterminada, se seleccionarán todos los grupos. Al menos uno de los grupos seleccionados debe estar configurado en su puerta de enlace local para cada fase de IKE.
Vida útil (segundos)	El valor de la vida útil determina la duración de una instancia de conexión con un conjunto de claves de cifrado o autenticación para paquetes de usuario, desde la compleción de la negociación hasta el vencimiento. Intervalo de la fase 1:De 900 a 28 800 segundos, con 28 800 como valor predeterminado. Intervalo de la fase 2: De 900 a 3600 segundos, con 3600 como valor predeterminado.

Parámetro	Descripción
	La vida útil de la fase 2 debe ser inferior a la de la fase 1. La conexión se renegocia a través del canal de codificación antes de que venza. Consulte **Tiempo de margen para cambiar la clave**. Si el lado local y el remoto no tienen la misma vida útil, las conexiones remplazadas estarán desordenadas en el lado con la vida útil más larga. Consulte también **Tiempo de margen para cambiar la clave** y **Difusión de cambio de clave**.
Tiempo de margen para cambiar la clave (segundos)	Tiempo de margen antes de la expiración de la conexión o la expiración del canal de claves durante el cual el lado local de la conexión VPN intenta negociar un reemplazo. El tiempo exacto para cambiar la clave se selecciona de manera aleatoria según el valor de la **Difusión de cambio de clave**. Es relevante solo a nivel local; el lado remoto no necesita estar de acuerdo. Intervalo: 900-3600 segundos. El valor predeterminado es 3600.
Tamaño del período de reproducción (paquete)	Tamaño del período de reproducción de IPsec para esta conexión. El valor predeterminado -1 utiliza el valor configurado con charon.replay_window en el archivo strongswan.conf. Los valores superiores a 32 solo son compatibles cuando se utiliza el backend Netlink. Un valor igual a 0 deshabilita la protección de reproducción de IPsec.
Difusión de cambio de clave (%)	Porcentaje máximo que los valores de marginbytes, marginpackets y margintime aumentan aleatoriamente para distribuir al azar los intervalos de cambio de clave (importante para servidores con muchas conexiones). El valor de difusión de cambio de clave puede exceder el 100 %. Después del aumento aleatorio, el valor de marginTYPE no debe exceder lifeTYPE, donde TYPE es bytes, paquetes o tiempo. El valor 0 % deshabilita la distribución aleatoria. Es relevante solo a nivel local; el lado remoto no

Parámetro	Descripción
	necesita estar de acuerdo.
Tiempo de espera de DPD (segundos)	Tiempo tras el que tiene lugar la acción del tiempo de espera de la detección de pares inactivos (DPD). Puede especificar un valor igual o mayor que 30. El valor predeterminado es 30.
Acción del tiempo de espera de la detección de pares inactivos (DPD)	Acción que debe realizarse después de que se agote el tiempo de espera de la detección de pares inactivos (DPD). **Reiniciar**: Reinicia la sesión cuando se agota el tiempo de espera de DPD. **Borrar**: Finaliza la sesión cuando se agote el tiempo de espera de DPD. **Ninguna**: No realiza ninguna acción cuando se agota el tiempo de espera de DPD.
Acción de inicio	Determina qué lado inicia la conexión y establece el túnel para la conexión VPN. **Agregar**: La puerta de enlace de su VPN local iniciará la conexión. **Iniciar**: La puerta de enlace de la VPN en la nube iniciará la conexión. **Dirigir**: Adecuado para puertas de enlace de VPN compatibles con la opción dirigir. el túnel estará activo solo cuando haya tráfico iniciado desde la puerta de enlace de VPN local o la puerta de enlace de Cloud VPN.

Cambio de VPN IPsec de varios sitios a OpenVPN de sitio a sitio

Puede cambiar fácilmente de una conexión VPN de IPsec de varios sitios a una conexión OpenVPN de sitio a sitio.

Cuando cambia el tipo de conectividad, las conexiones VPN activas se eliminan, pero la configuración de la red y de los servidores en la nube se conservan. Sin embargo, puede que necesite reasignar las direcciones IP de las redes y los servidores en la nube.

La siguiente tabla compara las características básicas de la conexión OpenVPN de sitio a sitio y la conexión VPN de IPsec de varios sitios.

	OpenVPN de sitio a sitio	VPN de IPsec de varios sitios
Soporte técnico del sitio local	Único	Único, múltiple
Modo de puerta de enlace de VPN	L2 Open VPN	L3 IPsec VPN
Segmentos de red	Amplía la red local a la red en la nube	Las redes locales y los segmentos de las redes en la nube no deben superponerse
Compatible con el acceso de punto a sitio al sitio local	Sí	No
Compatible con el acceso de punto a sitio al sitio en la nube	Sí	Sí
Requiere un elemento de oferta de IP pública	No	Sí

Para cambiar de una conexión VPN de IPsec de varios sitios a una conexión OpenVPN de sitio a sitio

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Haga clic en **Cambiar a OpenVPN de sitio a sitio**.
4. Haga clic en **Reconfigurar**.
5. Reasigne las direcciones IP de la red y los servidores en la nube.
6. Configure los ajustes de la conexión de sitio a sitio.

Solución de problemas de configuración de VPN de IPsec

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Cuando configure o use la conexión VPN de IPsec, puede experimentar problemas.

Puede obtener más información sobre los problemas que puede encontrar en los archivos de registro de IPsec y comprobar el tema Solución de problemas de configuración de VPN IPsec para conocer las posibles soluciones a algunos de los problemas comunes que pueden ocurrir.

Solución de problemas de configuración de VPN de IPsec

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La siguiente tabla describe los problemas de configuración de VPN de IPsec más frecuentes y explica cómo resolverlos.

Problema	Posible solución
Aparece el siguiente mensaje de error: **Error de negociación de la fase 1 de IKE. Compruebe la configuración de IPsec IKE en los sitios locales y en la nube.**	Haga clic en **Reintentar** y compruebe si aparece algún mensaje de error más específico. Por ejemplo, un mensaje de error más específico podría ser uno sobre una discrepancia de algoritmos o una clave compartida previamente incorrecta. **Nota** Por motivos de seguridad, las siguientes restricciones se aplican a la conectividad VPN de IPsec: • IKEv1 está obsoleto en RFC8247 y no se admite debido a que supone riesgos de seguridad. Solo se admiten las conexiones del protocolo IKEv2. • Los siguientes algoritmos de cifrado no se consideran seguros y no son compatibles: DES y 3DES. • Los siguientes algoritmos de hash no se consideran seguros y no son compatibles: SHA1 y MD5. • El número 2 de grupo de Diffie-Hellman no se considera seguro y no es compatible.
El estado de la conexión entre mi sitio local y en la nube sigue siendo **Conectando**.	Compruebe: • Si el puerto UDP 500 está abierto (cuando use un cortafuegos). • La conectividad entre el sitio local y el sitio en la nube. • Si la dirección IP del sitio local es correcta.
El estado de la conexión entre mi sitio local y en la nube sigue siendo **Esperando una conexión**.	Este estado aparece cuando se establece **Agregar** como **Acción de inicio** para el sitio en la nube, lo que significa que el sitio en la nube está esperando que se inicie la conexión desde el sitio local.

Problema	Posible solución
	Inicie la conexión desde el sitio local.
El estado de la conexión entre mi sitio local y en la nube sigue siendo **Esperando el tráfico**.	Verá este estado cuando la **acción de inicio** para el sitio local sea **Dirigir**. Si está esperando una conexión desde el sitio local, haga lo siguiente: • Desde el sitio local, intente hacer ping en la máquina virtual del sitio en la nube. Se trata de un comportamiento estándar necesario para establecer un túnel para algunos dispositivos, por ejemplo, Cisco ASA. (Modo Dirigir) • Asegúrese de que el sitio local haya establecido un túnel al configurar **Iniciar** como **Acción de inicio** del sitio local.
El estado de la conexión entre mi sitio local y en la nube se ha establecido, pero una o más directivas de red no funcionan.	Esto puede deberse a las siguientes razones: • La asignación de red en el sitio IPsec en la nube es distinta de la asignación de red del sitio local. Asegúrese de que las asignaciones de red y la secuencia de las directivas de red de los sitios local y en la nube coinciden exactamente. • Este estado es correcto cuando se establece **Dirigir** como **Acción de inicio** del sitio local o en la nube (por ejemplo, en dispositivos Cisco ASA), y no hay tráfico en ese momento. Puede intentar hacer ping para asegurarse de que se ha establecido el túnel. Si el ping no funciona, compruebe la asignación de red del sitio local y en la nube.
Quiero reiniciar una conexión IPsec específica.	Para reiniciar una conexión IPsec específica: 1. En la pantalla **Recuperación ante desastres** > **Conectividad**, haga clic en la conexión IPsec. 2. Haga clic en **Deshabilitar conexión**. 3. Haga clic en la conexión de IPsec de nuevo. 4. Haga clic en **Habilitar conexión**.

Descarga de archivos de registro de VPN de IPsec

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede obtener más información sobre la conectividad IPsec en los archivos de registro del servidor VPN. Los archivos de registro están comprimidos en un archivo .zip que puede descargar y extraer.

Requisitos previos

Se ha configurado la conectividad VPN de IPsec de varios sitios.

Para descargar el archivo .zip con los archivos de registro

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en el icono de engranaje que se encuentra junto a la puerta de enlace de VPN del sitio en la nube.
3. Haga clic en **Descargar registro**.
4. Haga clic en **Listo**.
5. Cuando el archivo .zip esté listo para descargarse, haga clic en **Descargar registro** y guárdelo de forma local.

Archivos de registro de VPN de IPsec de varios sitios

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La siguiente lista describe los archivos de registro de VPN de IPsec que son parte del archivo .zip y sobre la información que contienen.

- `ip.txt`: El archivo contiene los registros de la configuración de las interfaces de red. Deben aparecer dos direcciones IP: una pública y una local. Si no ve estas direcciones IP en el registro, hay un problema. Comuníquese con el equipo de soporte.

  Nota
  El valor de la máscara de la dirección IP pública debe ser 32.

- `swanctl-list-loaded-config.txt`: El archivo contiene información sobre todos los sitios de IPsec. Si no ve algún sitio en el archivo, no se habrá aplicado la configuración de IPsec. Intente actualizar la configuración y guardarla o comuníquese con el equipo de soporte.
- `swanctl-list-active-sas.txt`: El archivo contiene conexiones y políticas en estado activo o conectado.

Acceso de VPN remoto de punto a sitio

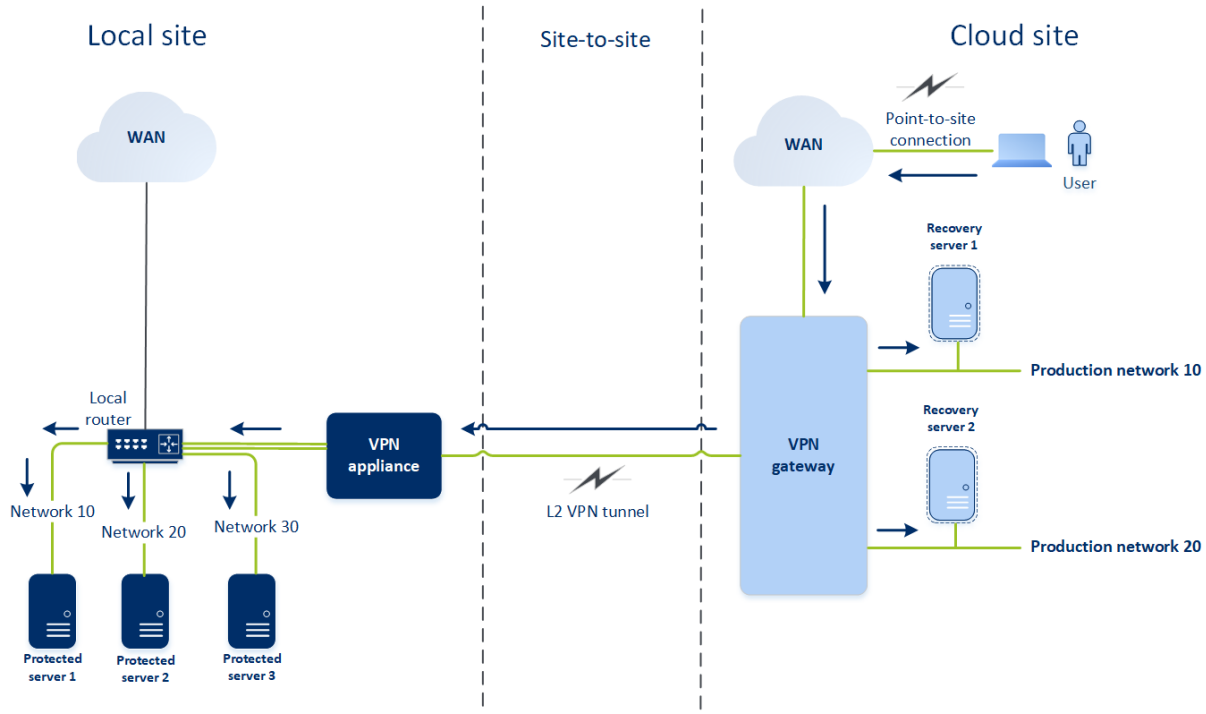
Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La conexión de punto a sitio es una conexión VPN segura desde el exterior que usa sus dispositivos de endpoint (como un ordenador o portátil) a los sitios en la nube y locales mediante un VPN. Está disponible después de establecer una conexión OpenVPN de sitio a sitio al sitio de recuperación de desastres. Este tipo de conexión es útil en los casos siguientes:

- En muchas empresas, los servicios corporativos y los recursos web solo están disponibles desde la red de la empresa. Puede utilizar la conexión de punto a sitio para conectarse al sitio local de forma segura.
- En caso de desastre, al trasladar una carga de trabajo al sitio en la nube mientras la red local está desactivada, puede necesitar acceder directamente a sus servidores en el cloud. Esto es posible gracias a la conexión de punto a sitio al sitio en la nube.

Para la conexión de punto a sitio en el sitio local, debe instalar el dispositivo VPN en el sitio local, configurar la conexión de sitio a sitio y después la conexión de punto a sitio del sitio local. Así, sus empleados remotos tendrán acceso a la red corporativa mediante L2 VPN.

El siguiente esquema muestra el sitio local, el sitio del cloud y las comunicaciones entre servidores están marcadas en verde. El túnel L2 VPN conecta el sitio local con el de la nube. Cuando un usuario establece una conexión de punto a sitio, las comunicaciones al sitio local se realizan a través del sitio en la nube.



La configuración de punto a sitio usa certificados para autenticar el cliente de VPN. También se usan las credenciales de usuario para la autenticación. Tenga en cuenta lo siguiente acerca de la conexión de punto a sitio al sitio local:

- Los usuarios deben usar sus credenciales de Cyber Protect Cloud para autenticarse en el cliente VPN. Deben tener los roles de usuario "Administrador de la empresa" o "Ciberprotección".

- Si ha vuelto a generar la configuración OpenVPN, debe proporcionar la configuración actualizada a todos los usuarios que estén utilizando la conexión de punto a sitio para acceder al sitio en la nube.

Configuración de acceso de VPN remoto de punto a sitio

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Si necesita conectar su sitio local de forma remota, puede configurar la conexión de punto a sitio del sitio local. Puede seguir el procedimiento siguiente o ver el tutorial en vídeo.

Requisitos previos

- La conectividad OpenVPN de sitio a sitio está configurada.
- El dispositivo VPN está instalado en el sitio local.

Para configurar la conexión de punto a sitio al sitio local

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Habilite la opción **Acceso mediante VPN al sitio local**.
4. Asegúrese de que el usuario que debe establecer la conexión de punto a sitio en el sitio local tiene:
   - Una cuenta de usuario en Cyber Protect Cloud. Estas credenciales se usan para la autenticación en el cliente VPN. De lo contrario, cree una cuenta de usuario en Cyber Protect Cloud.
   - Un rol de usuario de "Administrador de la empresa" o "Ciberprotección".
5. Configurar el cliente OpenVPN:
   a. Descargue el cliente OpenVPN versión 2.4.0 o posterior de la siguiente ubicación https://openvpn.net/community-downloads/.

      Nota
      El cliente OpenVPN Connect no es compatible.

   b. Instale el cliente OpenVPN en el equipo desde el que quiera conectarse al sitio local.
   c. Haga clic en **Descargar configuración para OpenVPN**. El archivo de configuración es válido para los usuarios de su organización con el rol de usuario "Administrador de la empresa" o "Ciberprotección".
   d. Importe la configuración descargada al cliente OpenVPN.
   e. Inicie sesión en el cliente OpenVPN con sus credenciales de usuario de Cyber Protect Cloud (vea el paso 4 anterior).

f. [Opcional] Si la autenticación de doble factor está habilitada en su organización, debe proporcional el código TOTP de generación única.

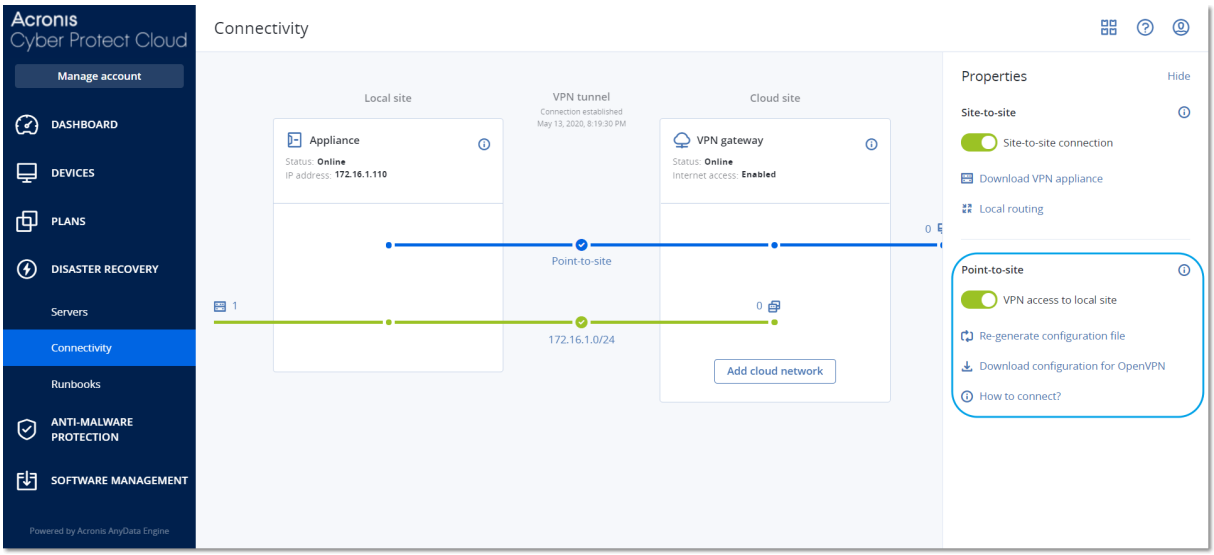
Importante
Si ha habilitado la autenticación de doble factor para su cuenta, tiene que volver a generar el archivo de configuración y renovarlo para sus clientes OpenVPN existentes. Los usuarios deben volver a iniciar sesión en Cyber Protect Cloud para configurar la configurar la autenticación de doble factor en sus cuentas.

Como resultado, podrá conectarse a las máquinas en el sitio local.

Gestión de la configuración de la conexión de punto a sitio:

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad** y pulse en **Mostrar propiedades** en la esquina superior derecha.



Acceso mediante VPN al sitio local

Esta opción se utiliza para administrar el acceso VPN al sitio local. Está habilitada por defecto. Si está deshabilitada, entonces no se permitirá el acceso de punto a sitio al sitio local.

Descargar configuración para OpenVPN

Así se descargará el archivo de configuración del cliente OpenVPN, El archivo es necesario para establecer una conexión de punto a sitio al sitio en la nube.

Volver a generar la configuración

Puede volver a generar el archivo de configuración del cliente OpenVPN.

Esta acción es obligatoria en los siguientes casos:

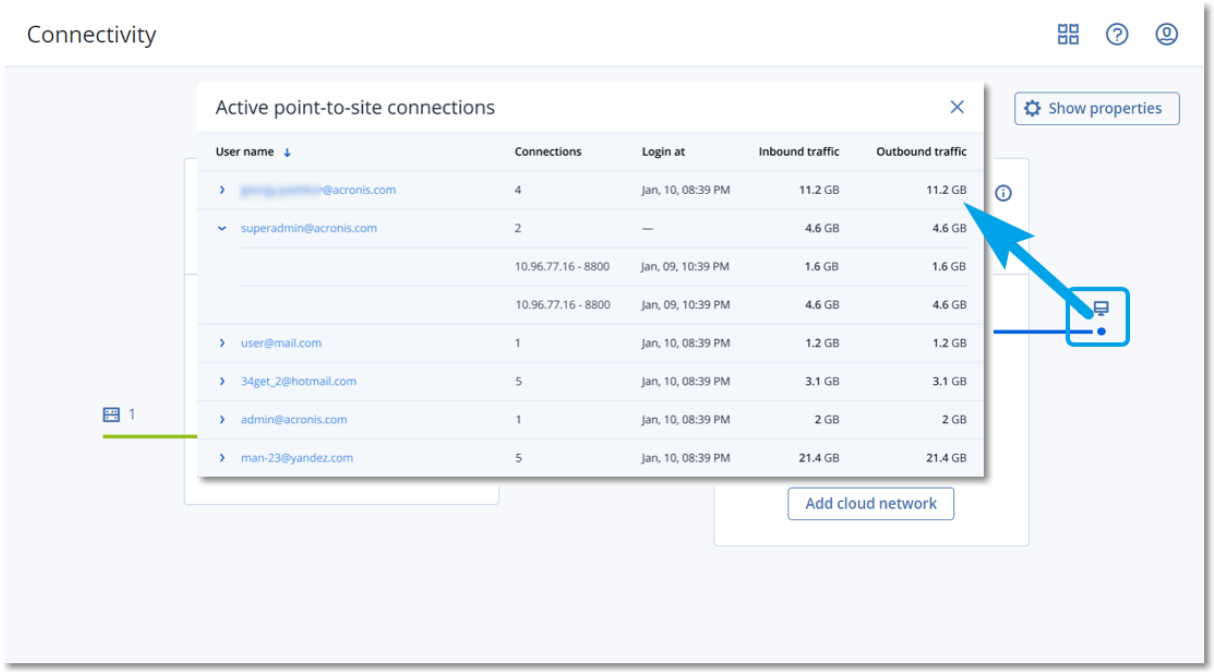
- Si cree que el archivo de configuración está en riesgo.
- Si la autenticación de doble factor estaba habilitada en su cuenta.

En cuanto se actualice el archivo de configuración, no se podrá llevar a cabo la conexión a través del archivo de configuración anterior. Asegúrese de distribuir el nuevo archivo entre los usuarios a los que se les permita usar la conexión de punto a sitio.

Conexiones activas de punto a sitio

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede ver todas las conexiones de punto a sitio activas en **Recuperación ante desastres** > **Conectividad**. Pulse en el icono del equipo en la línea azul de **De punto a sitio** y verá información detallada sobre las conexiones de punto a sitio activas agrupadas por su nombre de usuario.



Recomendaciones para la disponibilidad de servicios de dominio de Active Directory

Si tiene que autenticar sus cargas de trabajo protegidas en un controlador de dominio, le recomendamos que disponga de una instancia de controlador de dominio de Active Directory (AD DC) en el sitio de Disaster Recovery.

Controladores de dominio de Active Directory para conectividad OpenVPN L2

Con la conectividad OpenVPN L2, las direcciones IP de las cargas de trabajo protegidas se conservan en el sitio en la nube durante una conmutación por error de prueba o de producción. Por ello, la instancia de AD DC tiene la misma dirección IP que en el sitio local durante una conmutación por error de prueba o de producción.

Con DNS personalizados podrá establecer su propio servidor DNS personalizado para todos los servidores en la nube. Para obtener más información, consulte "Configuración de servidores DNS personalizados" (p. 53).

Controladores de dominio de Active Directory para conectividad VPN de IPsec L3

Con la conectividad VPN de IPsec L3, las direcciones IP de las cargas de trabajo protegidas no se conservan en el sitio en la nube. Por ello, recomendamos tener una instancia de AD DC dedicada adicional como un servidor principal en el sitio en la nube antes de llevar a cabo la conmutación por error de producción.

Estas son las recomendaciones para una instancia de AD DC dedicada que esté configurada como un servidor principal en el sitio en la nube:

- Apague el cortafuegos de Windows.
- Una el servidor principal al servicio de Active Directory.
- Asegúrese de que el servidor principal tenga acceso a Internet.
- Añada la función de Active Directory.

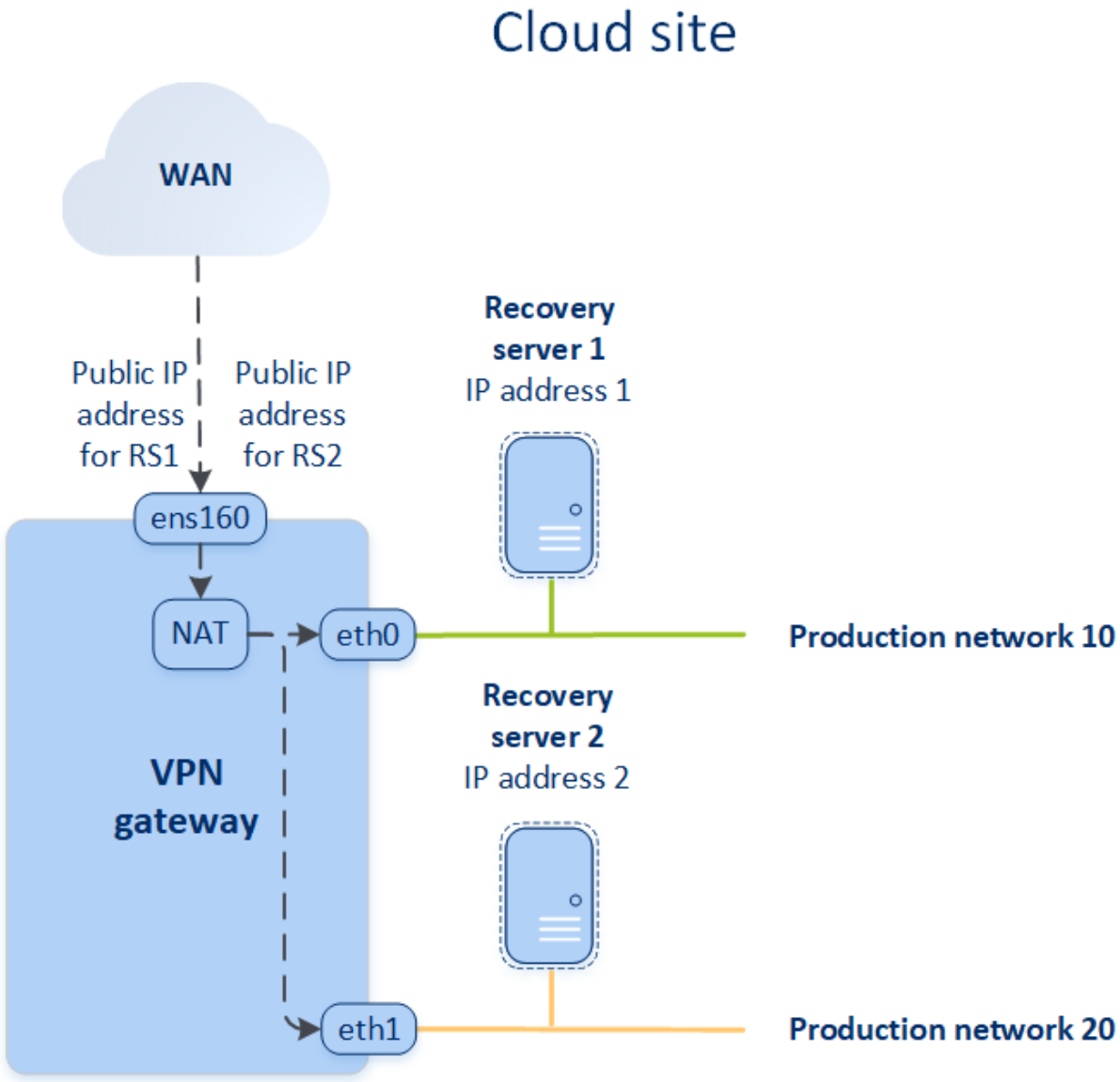
Con DNS personalizados podrá establecer su propio servidor DNS personalizado para todos los servidores en la nube. Para obtener más información, consulte "Configuración de servidores DNS personalizados" (p. 53).

Gestión de redes

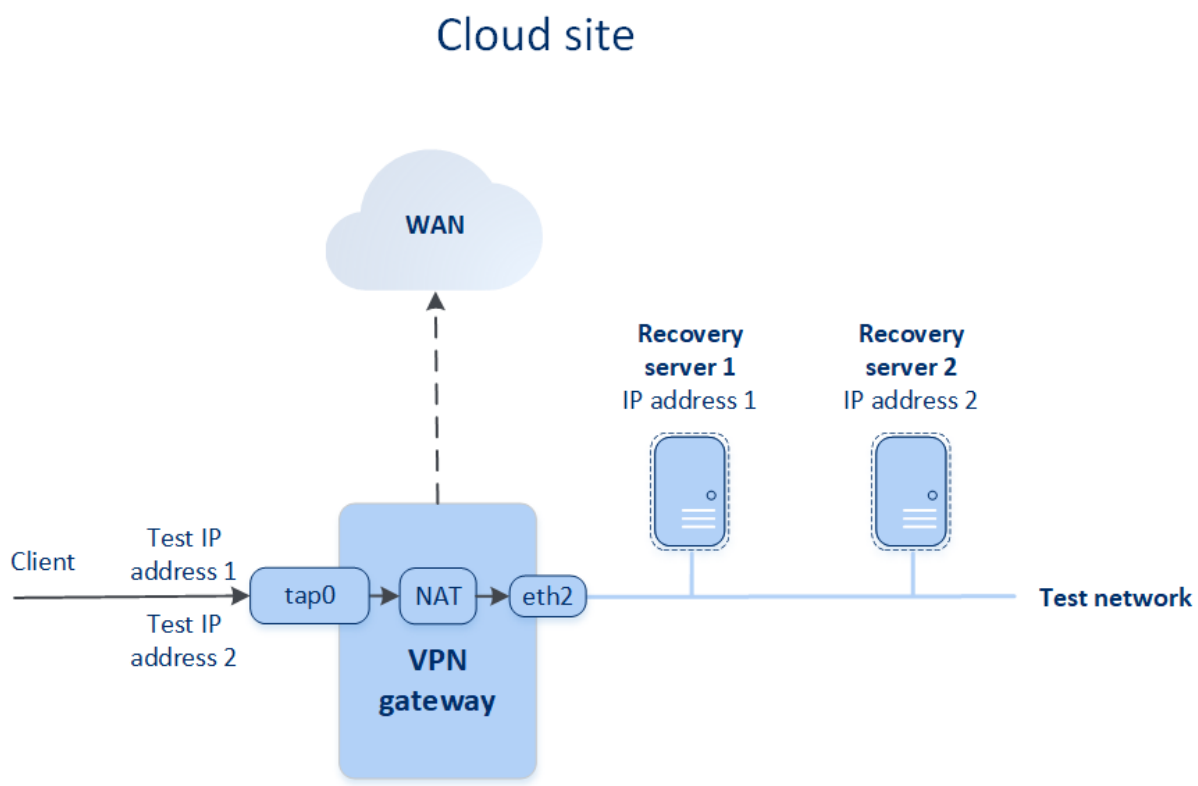
Esta sección describe escenarios de gestión de redes.

Direcciones IP de prueba y públicas

Si asigna la dirección IP pública al crear un servidor de recuperación, este pasará a estar disponible desde Internet a través de dicha dirección IP. Cuando llega un paquete de Internet con la dirección IP pública de destino, la puerta de enlace de VPN la vuelve a asignar a la dirección IP de producción correspondiente mediante NAT y la envía al servidor de recuperación correspondiente.



Si asigna la dirección IP de prueba al crear un servidor de recuperación, este pasará a estar disponible desde la red de prueba a través de dicha dirección IP. Al realizar la prueba de conmutación por error, el equipo de origen continuará funcionando mientras el servidor de recuperación con la misma dirección IP se inicia en la red de prueba en la nube. No se produce ningún conflicto de dirección IP, ya que la red de prueba está aislada. Se puede acceder a los servidores de recuperación en la red de prueba con sus direcciones IP de prueba que se vuelven a asignar a las direcciones IP de producción mediante NAT.



Para obtener más información sobre OpenVPN de sitio a sitio, consulte "OpenVPN de sitio a sitio: información adicional" (p. 162).

Volver a configurar la dirección IP

Para garantizar el rendimiento adecuado de la recuperación ante desastres, las direcciones IP asignadas a los servidores local y en el cloud deben ser coherentes. Si hay alguna incoherencia en las direcciones IP o estas no coinciden, verá un signo de exclamación junto a la red correspondiente en **Disaster Recovery** > **Conectividad**.

A continuación, se enumeran algunas de las razones más conocidas de la incoherencia de direcciones IP:

1. Se ha migrado un servidor de recuperación de una red a otra o se ha cambiado la máscara de red de la red en la nube. Como resultado, los servidores de nube tienen las direcciones IP de redes a las que no están conectados.
2. El tipo de conectividad se cambió de sin conexión de sitio a sitio a conexión de sitio a sitio. Como resultado, un servidor local se encuentra en una red distinta de aquella que se creó para el servidor de recuperación en el sitio en el cloud.
3. El tipo de conectividad se cambió de OpenVPN de sitio a sitio a VPN de IPsec de varios sitios, o de VPN de IPsec de varios sitios a OpenVPN de sitio a sitio. Para obtener más información sobre estos escenarios, consulte Cambio de conexiones, "Cambio de VPN IPsec de varios sitios a OpenVPN de sitio a sitio" (p. 39) y Reasignación de direcciones IP.
4. Editar los siguientes parámetros de red en el sitio del dispositivo VPN:

- Agregar una interfaz mediante la configuración de red.
- Editar manualmente la máscara de red mediante la configuración de interfaz.
- Editar la máscara de red mediante DHCP.
- Editar manualmente la máscara y dirección de red mediante la configuración de interfaz.
- Editar la máscara y dirección de red mediante DHCP.

El resultado de las anteriores acciones es que la red en el sitio en el cloud puede convertirse en un subconjunto o un superconjunto de la red local, o bien la interfaz del dispositivo VPN puede informar de que distintas interfaces tienen la misma configuración de red.

Para resolver el problema con la configuración de red:

1. Haga clic en la red cuya dirección IP debe volver a configurar.
   Verá una lista de servidores en la red seleccionada, sus estados y sus direcciones IP. Los servidores cuyas configuraciones de red sean incoherentes se marcan con un signo de exclamación.
2. Para cambiar la configuración de red de un servidor, haga clic en **Ir al servidor**. Para cambiar la configuración de red de todos los servidores a la vez, haga clic en **Modificar**, en el bloque de notificaciones.
3. Cambie las direcciones IP según sea necesario definiéndolas en los campos **IP nueva** y **Nueva IP de prueba**.
4. Haga clic en **Confirmar** cuando tenga todo a punto.

Mover servidores a una red adecuada

Al crear un plan de protección con recuperación ante desastres y aplicarlo a los dispositivos seleccionados, el sistema comprueba la dirección IP de cada dispositivo y crea automáticamente redes en la nube si no hay redes en la nube que existentes a las que se pueda adaptar la dirección IP. De forma predeterminada, la entidad IANA configura las redes con rangos máximos recomendados en la nube para uso privado (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Puede editar la máscara de red para reducir su red.

En el caso de que los dispositivos seleccionados estén en varias redes locales, la red del sitio en la nube puede convertirse en un superconjunto de redes locales. En este caso, siga estos pasos para volver a configurar redes en la nube:

1. Haga clic en la red en la nube cuyo tamaño tenga que volver a configurar y luego en **Editar**.
2. Vuelva a configurar el tamaño de la red con los ajustes correctos.
3. Cree otras redes requeridas.
4. Haga clic en el icono de notificación que se encuentra junto al número de dispositivos conectados a la red.
5. Haga clic en **Mover a una red adecuada**.
6. Seleccione los servidores que desea mover a las redes adecuadas y, a continuación, haga clic en **Mover**.

Reasignación de direcciones IP

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Debe reasignar las direcciones IP de las redes y los servidores en la nube para completar la configuración en los siguientes casos:

- Tras cambiar de OpenVPN de sitio a sitio a VPN de IPsec de varios sitios, o al contrario.
- Tras aplicar un plan de protección (si se ha configurado la conectividad VPN de IPsec de varios sitios).

Red en el cloud

Para reasignar la dirección IP de una red en la nube

1. En la pestaña **Conectividad**, haga clic en la dirección IP de la red en la nube.
2. En la ventana emergente **Red**, haga clic en **Editar**.
3. Escriba la dirección y la máscara de red nuevas.
4. Haga clic en **Listo**.

Después de reasignar la dirección IP de una red en la nube, deberá reasignar los servidores en la nube que pertenecen a la red en la nube reasignada.

Servidor en la nube

Para reasignar la dirección IP de un servidor

1. En la pestaña **Conectividad**, haga clic en la dirección IP del servidor de la red en la nube.
2. En la ventana emergente **Servidores**, haga clic en **Cambiar la dirección IP**.
3. En la ventana emergente **Cambiar la dirección IP**, escriba la nueva dirección IP del servidor o utilice la dirección IP generada automáticamente que forma parte de la red en la nube reasignada.

   Nota
   Disaster Recovery asigna automáticamente direcciones IP de la red en la nube a todos los servidores en la nube que son parte de esta antes de reasignar la dirección IP de la red. Puede utilizar las direcciones IP sugeridas para reasignar las direcciones IP de todos los servidores en la nube a la vez.

4. Haga clic en **Confirmar**.

Reinstalación de la puerta de enlace de VPN

Si ocurre un problema con la puerta de enlace de VPN que no puede resolver, puede que quiera volver a instalarla. Los posibles problemas incluyen los siguientes:

- El estado de la puerta de enlace de la VPN es **Error**.
- El estado de la puerta de enlace de la VPN aparece como **Pendiente** durante un periodo prolongado.
- El estado de la puerta de enlace de la VPN no se ha determinado durante un periodo prolongado.

El proceso de reinstalación de la puerta de enlace de VPN incluye las siguientes acciones automáticas: eliminación por completo de la máquina virtual de la puerta de enlace de VPN, instalación de una nueva máquina virtual a partir de la plantilla y aplicación de la configuración de la puerta de enlace de VPN anterior a la nueva máquina virtual.

Requisitos previos

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

Pasos para volver a instalar la puerta de enlace de VPN

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en el icono de engranaje de la puerta de enlace de VPN y seleccione **Reinstalar la puerta de enlace de la VPN**.
3. En el cuadro de diálogo **Reinstalar la puerta de enlace de la VPN**, ingrese sus credenciales de inicio de sesión.
4. Haga clic en **Reinstalar**.

Configuración de servidores DNS personalizados

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Cuando configura una conectividad, Disaster Recovery crea su infraestructura de red en la nube. El servidor DHCP en la nube asigna de forma automática los servidores DNS predeterminados a los servidores de recuperación y servidores principales. Sin embargo, puede cambiar los ajustes predeterminados y configurar los servidores DNS personalizados. La nueva configuración de DNS se aplicará en el momento de la próxima solicitud al servidor DHCP.

Requisitos previos

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

Para configurar un servidor DNS personalizado

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Haga clic en **Predeterminado (proporcionado por Cloud Site)**.
4. Seleccione **Servidores personalizados**.
5. Escriba la dirección IP del servidor DNS.
6. [Opcional] Si desea agregar otro servidor DNS, haga clic en **Agregar** y escriba la dirección IP del servidor DNS.

   Nota
   Cuando haya añadido los servidores DNS personalizados, también podrá añadir los servidores DNS predeterminados. De ese modo, si los servidores DNS personalizados no están disponibles, Disaster Recovery utilizará los servidores DNS predeterminados.

7. Haga clic en **Listo**.

Eliminación de servidores DNS personalizados

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede eliminar servidores DNS desde la lista de DNS personalizados.

Requisitos previos

Se han configurado los servidores DNS personalizados.

Para eliminar un servidor DNS personalizado

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Haga clic en **Servidores personalizados**.
4. Haga clic en el icono de eliminar que hay junto al servidor DNS.

   Nota
   La operación de eliminación está deshabilitada cuando solo hay disponible un servidor DNS personalizado. Si desea eliminar todos los servidores DNS personalizados, seleccione **Predeterminado (proporcionado por Cloud Site)**.

5. Haga clic en **Listo**.

Configuración de enrutación local

Además de sus redes locales que se extienden a la nube mediante el dispositivo VPN, puede tener otras redes locales que no estén registradas en dicho dispositivo y cuyos servidores deban comunicarse con servidores en la nube. Para establecer la conectividad entre estos servidores locales y los servidores en el cloud, debe configurar los ajustes de enrutación local.

Para configurar la enrutación local:

1. Vaya a **Disaster Recovery** > **Conectividad**.
2. Pulse en **Mostrar propiedades** y luego pulse en **Enrutamiento local**.
3. Especifique las redes locales en la notación del CIDR.
4. Haga clic en **Guardar**.

Como resultado, los servidores de las redes locales especificadas podrán comunicarse con los servidores en la nube.

Descarga de direcciones MAC

Puede descargar una lista de direcciones MAC para extraerlas e importarlas en la configuración de su servidor DHCP personalizado.

Requisitos previos

- Se debe establecer uno de los tipos de conectividad en el sitio en el cloud.
- Se debe configurar al menos un servidor de recuperación o principal con una dirección MAC.

Cómo descargar la lista de direcciones MAC

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Haga clic en **Descargar la lista de direcciones MAC** y guarde el archivo CSV.

Trabajar con registros

Disaster Recovery recopila registros para el dispositivo VPN y la puerta de enlace VPN. Los registros se guardan como archivos .txt, que se comprimen en un archivo .zip. Puede descargar y extraer el archivo comprimido y utilizar la información para resolver problemas o supervisar objetivos.

La siguiente lista describe los archivos de registro que son parte del archivo .zip y la información que contienen.

`dnsmasq.config.txt`: El archivo contiene información sobre la configuración del servicio que proporciona direcciones DNS y DHCP.

`dnsmasq.leases.txt`: El archivo contiene información sobre los alquileres actuales de direcciones DHCP.

`dnsmasq_log.txt`: El archivo contiene registros del servicio dnsmasq.

`ebtables.txt`: El archivo contiene información sobre las tablas del cortafuegos.

`free.txt`: El archivo contiene información sobre la memoria disponible.

`ip.txt`: El archivo contiene los registros de la configuración de las interfaces de red, incluidos los nombres que pueden utilizarse en la configuración de **Capturar paquetes de red**.

`NetworkManager_log.txt`: El archivo contiene registros del servicio NetworkManager.

`NetworkManager_status.txt`: El archivo contiene información sobre el estado del servicio NetworkManager.

`openvpn@p2s_log.txt`: El archivo contiene los registros del servicio OpenVPN.

`openvpn@p2s_status.txt`: El archivo contiene información sobre el estado de los túneles de VPN.

`ps.txt`: El archivo contiene información sobre los procesos que se ejecutan actualmente en la puerta de enlace VPN o en el dispositivo VPN.

`resolf.conf.txt`: El archivo contiene información sobre la configuración de los servidores DNS.

`routes.txt`: El archivo contiene información sobre las rutas de conexión a redes virtuales.

`uname.txt`: El archivo contiene información sobre la versión actual del kernel del sistema operativo.

`uptime.txt`: El archivo contiene información sobre la longitud del periodo para el que el sistema operativo no se ha reiniciado.

`vpnserver_log.txt`: El archivo contiene los registros del servicio VPN.

`vpnserver_status.txt`: El archivo contiene información sobre el estado del servidor VPN.

Para obtener más información sobre los archivos de registro que son específicos de la conectividad VPN de IPsec, consulte "Archivos de registro de VPN de IPsec de varios sitios" (p. 43).

Descarga de registros del dispositivo VPN

Puede descargar y extraer el archivo comprimido que contiene los registros del dispositivo VPN y utilizar la información para resolver problemas o supervisar objetivos.

Pasos para descargar los registros del dispositivo VPN

1. En la página **Conectividad**, haga clic en el icono de engranaje junto al dispositivo VPN.
2. Haga clic en **Descargar registro**.
3. [Opcional] Seleccione **Capturar paquetes de red** y configure los ajustes. Para obtener más información, consulte "Capturar paquetes de red" (p. 57).
4. Haga clic en **Listo**.
5. Cuando el archivo .zip esté listo para descargarse, haga clic en **Descargar registro** y guárdelo de forma local.

Descarga de registros de la puerta de enlace VPN

Puede descargar y extraer el archivo comprimido que contiene los registros de la puerta de enlace VPN y utilizar la información para resolver problemas o supervisar objetivos.

Pasos para descargar los registros de la puerta de enlace VPN

1. En la página **Conectividad**, haga clic en el icono de engranaje junto a la puerta de enlace VPN.
2. Haga clic en **Descargar registro**.
3. [Opcional] Seleccione **Capturar paquetes de red** y luego configure los ajustes. Para obtener más información, consulte "Capturar paquetes de red" (p. 57).
4. Haga clic en **Listo**.
5. Cuando el archivo .zip esté listo para descargarse, haga clic en **Descargar registro** y guárdelo de forma local.

Capturar paquetes de red

Para solucionar problemas y analizar la comunicación entre el sitio de producción local y un servidor principal o de recuperación, puede elegir recopilar paquetes de red en la puerta de enlace VPN o en el dispositivo VPN.

Cuando se recopilan 32 000 paquetes de red o se llega al límite de tiempo, la captura de paquetes de red se detiene y los resultados se escriben en un archivo .libpcap que se añade al archivo ZIP de registros.

La siguiente tabla proporciona más información sobre los ajustes de **Capturar paquetes de red** que puede configurar.

Configuración	Descripción
Nombre de la interfaz de red	Interfaz de red en la que capturar paquetes de red. Si desea capturar paquetes de red en todas las interfaces de red, seleccione **Cualquiera**.
Límite temporal (segundos)	El límite temporal para capturar paquetes de red. El valor máximo que puede establecer es 1800.
Filtrado	Un filtro extra para aplicar a los paquetes de red capturados. Puede introducir una cadena con protocolos, puertos, direcciones, y sus combinaciones, separada por un espacio, como "and", "or", "not", " (", ") ", "src", "dst", "net", "host", "port", "ip", "tcp", "udp", "icmp", "arp", y "esp". Si desea utilizar paréntesis, ponga espacios antes y después. También puede introducir direcciones IP y de red, por ejemplo: "icmp o arp" y "puerto 67 o 68". Para obtener más información acerca de los valores que puede introducir, consulte la ayuda tpcdump de Linux.

Servidores de nube

Con Disaster Recovery a Cyber Protect Cloud, puede utilizar dos tipos de servidores de nube: principal y de recuperación.

Un servidor principal es una máquina virtual que no está vinculada a un equipo en el sitio local. Puede utilizar servidores principales para proteger una aplicación específica o ejecutar varios servicios auxiliares (como un servidor web).

Un servidor de recuperación es una máquina virtual réplica del equipo original (servidor protegido). El servidor de recuperación se basa en las copias de seguridad del servidor protegido que se almacenan en la nube. En caso de un desastre, los servidores de recuperación se utilizan para cambiar los recursos informáticos de los servidores originales.

Configuración de servidores de recuperación

Servidor de recuperación: réplica del equipo original basada en las copias de seguridad del servidor protegido almacenadas en el cloud. Los servidores de recuperación se utilizan para trasladar cargas de trabajo desde los servidores originales en caso de desastre.

Al crear un servidor de recuperación, debe especificar los siguientes parámetros de red:

Parámetro	Descripción
Red en la nube	(Obligatorio) La red en la nube a la que se conectará un servidor de recuperación.
Dirección IP en la red de producción	(Obligatorio) La dirección IP con la que se inicia una máquina virtual para un servidor de recuperación. Esta dirección se usa tanto para la red de producción como para la de prueba. Antes de iniciar la máquina virtual, esta se configura para obtener la dirección IP mediante DHCP.
Dirección IP de prueba	(Opcional) La dirección IP para acceder a un servidor de recuperación desde la red de cliente-producción durante la prueba de conmutación por error, para evitar que la dirección IP de producción se duplique en la misma red. Esta dirección IP es distinta de la de la red de producción. Los servidores en el sitio local pueden alcanzar el servidor de recuperación durante la prueba de conmutación por error a través de la dirección IP, pero el acceso en la dirección contraria no está disponible. El servidor de recuperación en la red de prueba dispone de acceso a Internet si se seleccionó la opción **Acceso a Internet** durante la creación de dicho servidor.
Dirección IP pública	(Opcional) La dirección IP para acceder a un servidor de recuperación desde Internet. Si un servidor no tiene dirección IP pública, solo es alcanzable desde la red local.

Parámetro	Descripción
Acceso a Internet	(Opcional) Permite que un servidor de recuperación acceda a Internet (tanto en el caso de producción como en el de la prueba de conmutación por error).

Creación de un servidor de recuperación

Para crear un servidor de recuperación que será una copia de su carga de trabajo, siga el procedimiento que aparece a continuación. También puede ver el vídeo tutorial que muestra el proceso.

Importante
Cuando realice una conmutación por error, puede seleccionar solo los puntos de recuperación que se crearon después de crear el servidor de recuperación.

Requisitos previos

- Se debe aplicar un plan de protección 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 la nube.
- 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 dispositivos**, seleccione la máquina que desea proteger.
2. Haga clic en **Recuperación ante desastres** y, luego, en **Crear servidor de recuperación**.
3. En el asistente **Crear servidor de recuperación**, en la pestaña **Configuración del servidor**, haga lo siguiente:
   a. Seleccione el número de núcleos virtuales y el tamaño de la RAM.

      Nota
      Puede ver los puntos de cálculo para cada opción. El número de puntos de cálculo indican el coste de funcionamiento del servidor de recuperación por hora. Para obtener más información, consulte "Puntos de cálculo" (p. 73).

   b. [Opcional] Cambie el nombre predeterminado del servidor de recuperación.
   c. [Opcional] Agregue una descripción.
4. En la pestaña **Red**, haga lo siguiente:
   a. Especifique la red en el cloud a la que se conectará el servidor.
   b. Seleccione la opción **DHCP**.

Opción DHCP	Descripción
Proporcionado	Esta es la configuración predeterminada. Un servidor DHCP en la

Opción DHCP	Descripción
por Cloud Site	nube configurado automáticamente proporcionará la dirección IP del servidor.
Personalizado	Su propio servidor DHCP en la nube proporcionará la dirección IP del servidor.

c. Especifique la **dirección MAC**.

La dirección MAC es un identificador único asignado al adaptador de red del servidor. Si usa un DHCP personalizado, puede configurarlo para que siempre asigne una dirección IP específica a una dirección MAC concreta. Así, se garantiza que el servidor de recuperación siempre tenga la misma dirección IP. Puede ejecutar aplicaciones con licencias registradas con la dirección MAC.

d. 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.

Si usa un servidor DHCP personalizado, deberá especificar la misma dirección IP en la **Dirección IP en la red de producción** que la configurada en el servidor DHCP. De lo contrario, la conmutación por error de prueba no funcionará correctamente y no será posible alcanzar el servidor mediante una dirección IP pública.

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

Si selecciona esta configuración, podrá probar una conmutación por error en la red de prueba aislada y conectarse al servidor de recuperación mediante escritorio remoto o SSH durante una conmutación por error de prueba. Durante una conmutación por error de prueba, la puerta de enlace de VPN sustituirá la dirección IP de prueba por la dirección IP de producción mediante el protocolo NAT.

Si no selecciona la configuración, la consola será la única forma de acceder al servidor durante una conmutación por error de prueba.

Nota

Si utiliza 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 introducir otra.

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

Si selecciona esta configuración, el servidor de recuperación tendrá acceso a Internet durante una conmutación por error de prueba o de producción. De forma predeterminada, el puerto TCP 25 está abierto para las conexiones de salida a direcciones IP públicas.

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

Con una dirección IP pública, el servidor de recuperación se vuelve accesible desde Internet durante una conmutación por error o una conmutación por error de prueba. Si no selecciona esta configuración, el servidor solo estará disponible en su red de producción.

La opción **Usar dirección IP pública** requiere que esté seleccionada la opción **Acceso a Internet**.

La dirección IP pública se mostrara cuando finalice la configuración. De forma predeterminada, el puerto TCP 443 está abierto para las conexiones de entrada a direcciones IP públicas.

Nota
Si borra la casilla de verificación **Usar dirección IP pública** o elimina el servidor de recuperación, su dirección IP pública no se reservará.

5. En la pestaña **Configuración**, seleccione **Establecer el umbral de RPO** y, a continuación, establezca el valor.

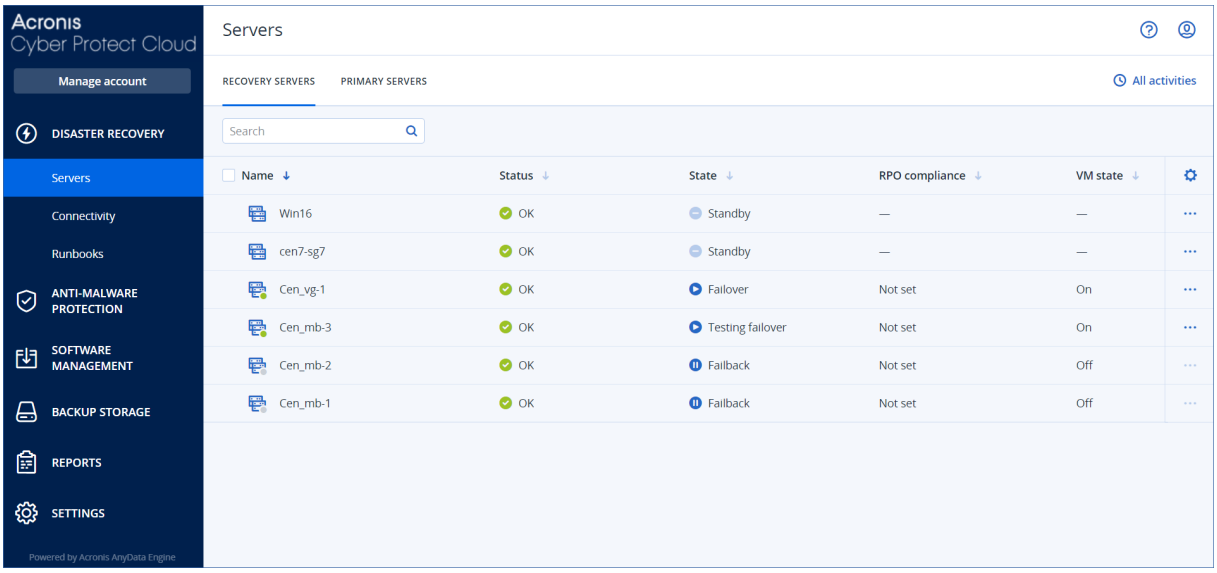
   El umbral de RPO define el intervalo temporal máximo entre el último punto de recuperación viable para una conmutación por error y el momento presente. El valor se puede establecer entre 15 y 60 minutos, 1 y 24 horas y 1 y 14 días.
6. [Opcional] [Si las copias de seguridad del equipo seleccionado están cifradas utilizando el cifrado como una propiedad del equipo], especifique la contraseña que se utilizará automáticamente al crear una máquina virtual para el servidor de recuperación a partir de la copia de seguridad cifrada.
   a. Haga clic en **Introducir contraseña**, introduzca la contraseña de la copia de seguridad cifrada y defina un nombre para las credenciales.

      De forma predeterminada, verá la copia de seguridad más reciente en la lista.
   b. Para ver todas las copias de seguridad, seleccione **Mostrar todas las copias de seguridad**.
   c. Haga clic en **Guardar**.

Nota
Tenga en cuenta que, aunque la contraseña que especifique se guardará en un almacén de credenciales seguro, es posible que incumpla sus obligaciones legales si la guarda.

7. En la pestaña **Reglas del cortafuegos de la nube**, edite las reglas de firewall predeterminadas. Para obtener más información, consulte "Configuración de reglas de cortafuegos para servidores en la nube" (p. 70).
8. Haga clic en **Crear**.

En la consola de Cyber Protect, el servidor de recuperación aparece en la pestaña **Disaster Recovery** > **Servidores** > **Servidores de recuperación**.



Operaciones con servidores de recuperación

En la consola de Cyber Protect, los servidores principales se muestran en la pestaña **Disaster Recovery** > **Servidores** > **Servidores de recuperación**.

Encender

Para encender un servidor de recuperación

1. En la pestaña **Servidores de recuperación**, haga clic en el servidor de recuperación.
2. Haga clic en **Encender**.

Apagar

Para apagar un servidor de recuperación

1. En la pestaña **Servidores de recuperación**, haga clic en el servidor de recuperación.
2. Haga clic en **Apagar**.
3. En la pantalla **Apagar servidor**, haga clic en **Apagar**.

Apagado forzoso

Para forzar el apagado de un servidor de recuperación

1. En la pestaña **Servidores de recuperación**, haga clic en el servidor de recuperación.
2. Haga clic en **Apagar**.
3. En la pantalla **Apagar servidor**, seleccione **Forzar apagado del servidor** y, a continuación, haga clic en **Apagar**.

Detener

Pasos para parar un servidor de recuperación

1. En la pestaña **Servidores de recuperación**, haga clic en el servidor de recuperación.
2. Haga clic en **Detener**.

Editar configuración

Para editar la configuración de un servidor de recuperación

1. En la pestaña **Servidores de recuperación**, haga clic en el servidor de recuperación.
2. Haga clic en **Detener**.
3. Haga clic en **Editar** y, a continuación, edite la configuración.

Aplicar plan de protección

Pasos para aplicar un plan a un servidor principal

1. En la pestaña **Servidores principales**, haga clic en el servidor principal.
2. En la pestaña **Plan**, haga clic en **Crear**.
   Verá un plan de protección predefinido en el que solo puede cambiar las reglas de programación y retención. Para obtener más información, consulte "Copia de seguridad de los servidores de nube".

Configuración de servidores principales

Un **servidor principal** es una máquina virtual que no tiene un equipo enlazado en el sitio local, en comparación con un servidor de recuperación. Los servidores principales se utilizan para proteger una aplicación por replicación o para ejecutar varios servicios auxiliares (como un servidor web).

Normalmente, se usa un servidor principal para la replicación de datos en tiempo real en servidores que ejecuten aplicaciones fundamentales. La replicación la configura usted mismo con herramientas nativas de la aplicación. Por ejemplo, la replicación de Active Directory o de SQL se puede configurar entre los servidores locales y el principal.

Como alternativa, un servidor principal se puede incluir en un grupo de disponibilidad AlwaysOn (AGG) o un grupo de disponibilidad de base de datos (DAG).

Ambos métodos requieren un profundo conocimiento de la aplicación y los derechos del administrador. Un servidor principal consume constantemente recursos informáticos y espacio del almacenamiento rápido de recuperación ante desastres. Necesita mantenimiento por su parte, como el control de la replicación, la instalación de actualizaciones de software y la realización de copias de seguridad. Las ventajas son los RPO y RTO mínimos con una carga mínima del entorno de producción (en comparación con la realización de copias de seguridad de servidores completos en la cloud).

Los servidores principales solo se inician en la red de producción y tienen los siguientes parámetros de red:

Parámetro	Descripción
Red en la nube	(Obligatorio) La red en la nube a la que se conectará un servidor principal.
Dirección IP en la red de producción	(Obligatorio) La dirección IP que tendrá el servidor principal en la red de producción. La primera dirección IP libre de su red de producción se establece de forma predeterminada.
Dirección IP pública	(Opcional) La dirección IP para acceder a un servidor principal desde Internet. Si un servidor no tiene dirección IP pública, solo se podrá acceder a él desde la red local y no desde Internet.
Acceso a Internet	(Opcional) Permite que un servidor principal tenga acceso a Internet.

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 la pestaña **Disaster Recovery** > **Servidores** > **Servidores principales**.
2. Haga clic en **Crear**.
3. En el asistente **Crear servidor principal**, en la pestaña **Configuración del servidor**, haga lo siguiente:
   a. Seleccione una plantilla para el nuevo equipo virtual.
   b. Seleccione la variante de la configuración (el número de núcleos virtuales y el tamaño de la RAM).
   La siguiente tabla muestra la cantidad total máxima de espacio en el disco (GB) para cada variante.

Tipo	vCPU	RAM (GB)	Cantidad total máxima de espacio en el disco (GB)
F1	1	2	500
F2	1	4	1,000
F3	2	8	2,000
F4	4	16	4,000
F5	8	32	8,000
F6	16	64	16,000
F7	16	128	32,000
F8	16	256	64,000

c. [Opcional] Cambie el tamaño de los discos virtuales. Si necesita más de un disco duro, haga clic en **Agregar disco** y, a continuación, especifique el nuevo tamaño de disco. Puede añadir hasta 10 discos en un servidor principal.

d. Cambie el nombre predeterminado del servidor de recuperación.

e. Agregue una descripción.

4. En la pestaña **Red**, haga lo siguiente:

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

b. Seleccione la opción **DHCP**.

Opción DHCP	Descripción
Proporcionado por Cloud Site	Esta es la configuración predeterminada. Un servidor DHCP en la nube configurado automáticamente proporcionará la dirección IP del servidor.
Personalizado	Su propio servidor DHCP en la nube proporcionará la dirección IP del servidor.

c. Especifique la **dirección MAC**.

La dirección MAC es un identificador único que se asigna al adaptador de red del servidor. Si usa un DHCP personalizado, puede configurarlo para que siempre asigne una dirección IP específica a una dirección MAC concreta. Así se garantiza que el servidor principal siempre tenga la misma dirección IP. Puede ejecutar aplicaciones con licencias que se registran en la dirección MAC.

d. 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.

Si usa un servidor DHCP personalizado, deberá especificar la misma dirección IP en la **Dirección IP en la red de producción** que la configurada en el servidor DHCP. De lo contrario, la conmutación por error de prueba no funcionará correctamente y no será posible alcanzar el servidor mediante una dirección IP pública.

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

Si selecciona esta opción, el servidor principal tendrá acceso a Internet. De forma predeterminada, el puerto TCP 25 está abierto para las conexiones de salida a direcciones IP públicas.

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

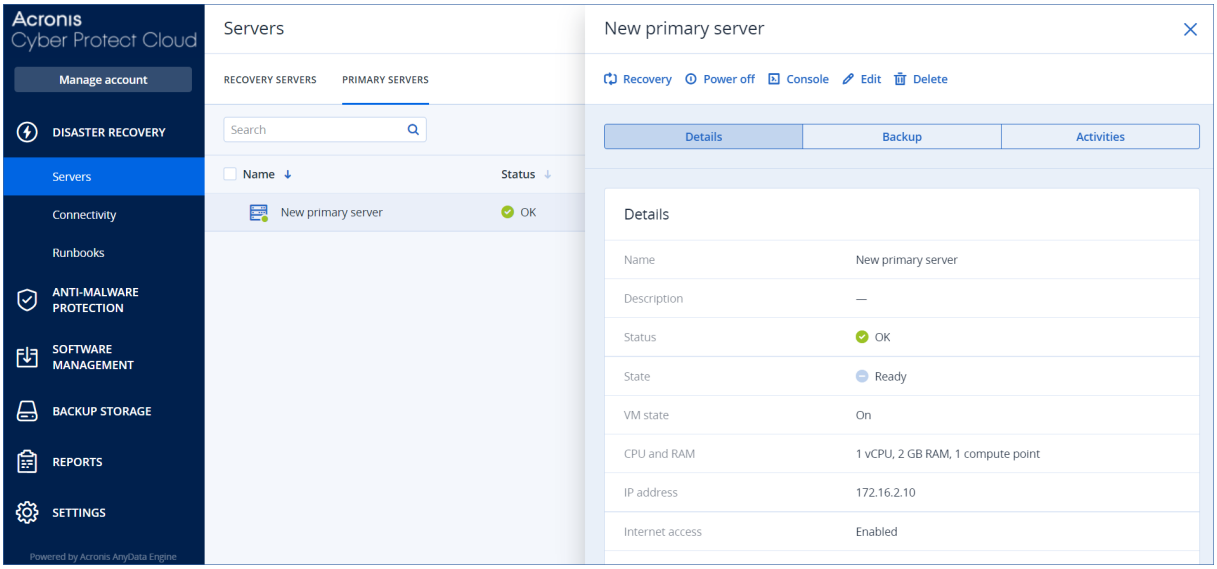
Con una dirección IP pública, el servidor principal se vuelve accesible desde Internet. Si no selecciona esta configuración, el servidor solo estará disponible en su red de producción.

La dirección IP pública se mostrara cuando finalice la configuración. De forma predeterminada, el puerto TCP 443 está abierto para las conexiones de entrada a direcciones IP públicas.

Nota
Si borra la casilla de verificación **Usar dirección IP pública** o elimina el servidor de recuperación, su dirección IP pública no se reservará.

5. [Opcional] En la pestaña **Configuración**, seleccione **Establecer el umbral de RPO** y, a continuación, establezca el valor.
   El umbral de RPO determina el intervalo temporal máximo 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.
6. [Opcional] En la pestaña **Reglas de cortafuegos de la nube**, edite las reglas de firewall predeterminadas. Para obtener más información, consulte "Configuración de reglas de cortafuegos para servidores en la nube" (p. 70).
7. 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 servidores principales

En la consola de Cyber Protect, los servidores principales se muestran en la pestaña **Disaster Recovery** > **Servidores** > **Servidores principales**.

Encender

Pasos para encender un servidor principal

1. En la pestaña **Servidores principales**, haga clic en el servidor principal.
2. Haga clic en **Encender**.

Apagar

Pasos para apagar un servidor principal

1. En la pestaña **Servidores principales**, haga clic en el servidor principal.
2. Haga clic en **Apagar**.
3. En la pantalla **Apagar servidor**, haga clic en **Apagar**.

Apagado forzoso

Pasos para forzar el apagado de un servidor principal

1. En la pestaña **Servidores principales**, haga clic en el servidor principal.
2. Haga clic en **Apagar**.
3. En la pantalla **Apagar servidor**, seleccione **Forzar apagado del servidor** y, a continuación, haga clic en **Apagar**.

Detener

Pasos para parar un servidor principal

1. En la pestaña **Servidores principales**, haga clic en el servidor principal.
2. Haga clic en **Detener**.

Editar configuración

Pasos para editar la configuración de un servidor principal

1. En la pestaña **Servidores principales**, haga clic en el servidor principal.
2. Haga clic en **Detener**.
3. Haga clic en **Editar** y, a continuación, edite la configuración.

Aplicar plan de protección

Pasos para aplicar un plan a un servidor principal

1. En la pestaña **Servidores principales**, haga clic en el servidor principal.
2. En la pestaña **Plan**, haga clic en **Crear**.
   Verá un plan de protección predefinido en el que solo puede cambiar las reglas de programación y retención. Para obtener más información, consulte "Copia de seguridad de los servidores de nube".

Vista de detalles sobre servidores e la nube

Para ver los detalles de los servidores de nube, vaya a **Disaster Recovery** > **Servidores**. Allí encontrará dos pestañas: **Servidores de recuperación** y **Servidores principales**. Para mostrar

todas las columnas opcionales de la tabla, haga clic en el icono de engranaje.

Puede encontrar la siguiente información acerca de cada servidor si lo selecciona.

Nombre de la columna	Descripción
Nombre	Un nombre de servidor de cloud que ha definido usted
Rango	El rango que refleja el problema más grave con un servidor de cloud (en función de las alertas activas)
Estado	Estado de un servidor en la nube
Estado del equipo virtual	El estado de energía de un equipo virtual asociado con un servidor de cloud.
Ubicación activa	Ubicación en la que se aloja un servidor en la nube. Por ejemplo, **Nube**.
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 15-60 minutos, 1-24 horas y 1-14 días.
Cumplimiento de RPO	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. Se calcula de la siguiente forma: **Cumplimiento de RPO = RPO reales / Umbral de RPO** donde **RPO reales = hora actual – último tiempo de punto de recuperación** **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: • **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 protección, 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

Copias de seguridad de servidores de nube

Se realiza una copia de seguridad sin agente de la nube de los servidores principales y de recuperación. Estas copias de seguridad tienen las siguientes restricciones.

- La única ubicación de copia de seguridad posible es el almacenamiento en la nube. Las copias de seguridad de los servidores principales se realizan en el almacenamiento de **copias de seguridad de los servidores principales**.

  Nota
  No se admiten ubicaciones de copia de seguridad de Microsoft Azure.

- 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 de la nube se realizan en hora UTC.

Reglas de cortafuegos para servidores en la nube

Puede configurar las reglas de cortafuegos para controlar el tráfico de entrada y de salida del servidor principal y el de recuperación en su sitio de la nube.

Puede configurar las reglas de entrada después de suministrar una dirección IP pública para el servidor de la nube. De forma predeterminada, el puerto TCP 443 está habilitado y el resto de las conexiones de entrada están denegadas. Puede cambiar las reglas de cortafuegos predeterminadas

y añadir o eliminar excepciones de entrada. Si no se ha suministrado una IP pública, solo podrá ver las reglas de entrada, pero no configurarlas.

Puede configurar las reglas de salida después de suministrar acceso a Internet para el servidor de la nube. De forma predeterminada, el puerto TCP 25 está denegado y el resto de las conexiones de salida están permitidas. Puede cambiar las reglas de cortafuegos predeterminadas y añadir o eliminar excepciones de salida. Si no se ha suministrado acceso a Internet, solo podrá ver las reglas de salida, pero no configurarlas.

Nota
Por motivos de seguridad, hay reglas de cortafuegos predeterminadas que no puede cambiar.

Para las conexiones de entrada y de salida:

- Permiso ping: Solicitud de eco ICMP (tipo 8, código 0) y respuesta de eco ICMP (tipo: 0, código: 0)
- Permiso ICMP necesario para fragmentar (tipo 3, código 4)
- Permiso TTL excedido (tipo 11, código 0)

Solo para conexiones de entrada:

- Parte no configurable: Rechazar todos

Solo para conexiones de salida:

- Parte no configurable: Rechazar todo

Configuración de reglas de cortafuegos para servidores en la nube

Puede editar las reglas de cortafuegos predeterminadas para los servidores primarios y de recuperación en la nube.

Pasos para editar las reglas de cortafuegos de un servidor de su sitio en la nube

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores**.
2. Si desea editar las reglas de cortafuegos de un servidor de su sitio en la nube, haga clic en la pestaña **Servidores de recuperación**. De manera alternativa, si desea editar las reglas de cortafuegos de un servidor principal, haga clic en la pestaña **Servidores principales**.
3. Haga clic en el servidor y después haga clic en **Editar**.
4. Haga clic en la pestaña **Reglas de cortafuegos de la nube**.
5. Si desea cambiar la acción predeterminada para las conexiones de entrada:

a. En el campo desplegable **Entrada**, seleccione la acción predeterminada.

Acción	Descripción
Rechazar todo	Rechaza cualquier tráfico de entrada. Puede añadir excepciones y permitir el tráfico desde direcciones IP específicas, protocolos y puertos.
Permitir todo	Permite todo el tráfico TCP y UDP de entrada. Puede añadir excepciones y rechazar el tráfico desde direcciones IP específicas, protocolos y puertos.

Nota
Al cambiar la acción predeterminada se invalida y elimina la configuración de las reglas de entrada existentes.

b. [Opcional] Si desea guardar las excepciones existentes, seleccione **Guardar excepciones completadas** en la ventana de confirmación.

c. Haga clic en **Confirmar**.

6. Si desea añadir una excepción:

a. Haga clic en **Agregar Excepción**.

b. Especifique los parámetros del cortafuegos.

Parámetro de cortafuegos	Descripción
Protocolo	Seleccione el protocolo para la conexión. Se admiten las siguientes opciones: • **TCP** • **UDP** • **TCP+UDP**
Puerto del servidor	Seleccione los puertos a los que se aplica la regla. Puede especificar lo siguiente: • un número de puerto específico (por ejemplo, `2298`) • un intervalo de números de puerto (por ejemplo, `6000-6700`) • cualquier número de puerto. Utilice `*` si desea que la regla se aplique a cualquier número de puerto.
Dirección IP del cliente	Seleccione las direcciones IP a las que se aplica la regla. Puede especificar lo siguiente: • una dirección IP específica (por ejemplo, `192.168.0.0`) • un intervalo de direcciones IP que utilicen la notación CIDR (por ejemplo, `192.168.0.0/24`) • cualquier dirección IP. Utilice `*` si desea que la regla se aplique a cualquier dirección IP.

7. Si desea eliminar una excepción de entrada existente, haga clic en el icono de la papelera junto a la excepción.
8. Si desea cambiar la acción predeterminada para las conexiones de salida:
   a. En el campo desplegable **Salida**, seleccione la acción predeterminada.

Acción	Descripción
Rechazar todo	Rechaza cualquier tráfico de salida. Puede añadir excepciones y permitir el tráfico a direcciones IP específicas, protocolos y puertos.
Permitir todo	Deniega todo el tráfico de salida. Puede añadir excepciones y rechazar el tráfico desde direcciones IP específicas, protocolos y puertos.

Nota
Al cambiar la acción predeterminada se invalida y elimina la configuración de las reglas de salida existentes.

   b. [Opcional] Si desea guardar las excepciones existentes, seleccione **Guardar excepciones completadas** en la ventana de confirmación.
   c. Haga clic en **Confirmar**.
9. Si desea añadir una excepción:
   a. Haga clic en **Agregar Excepción**.
   b. Especifique los parámetros del cortafuegos.

Parámetro de cortafuegos	Descripción
Protocolo	Seleccione el protocolo para la conexión. Se admiten las siguientes opciones: • **TCP** • **UDP** • **TCP+UDP**
Puerto del servidor	Seleccione los puertos a los que se aplica la regla. Puede especificar lo siguiente: • un número de puerto específico (por ejemplo, `2298`) • un intervalo de números de puerto (por ejemplo, `6000-6700`) • cualquier número de puerto. Utilice `*` si desea que la regla se aplique a cualquier número de puerto.
Dirección IP del cliente	Seleccione las direcciones IP a las que se aplica la regla. Puede especificar lo siguiente: • una dirección IP específica (por ejemplo, `192.168.0.0`) • un intervalo de direcciones IP que utilicen la notación CIDR (por

Parámetro de cortafuegos	Descripción
	ejemplo, `192.168.0.0/24`) • cualquier dirección IP. Utilice `*` si desea que la regla se aplique a cualquier dirección IP.

10. Si desea eliminar una excepción de salida existente, haga clic en el icono de la papelera junto a la excepción.
11. Haga clic en **Guardar**.

Comprobación de las actividades del cortafuegos de la nube

Después de actualizar la configuración de las reglas del cortafuegos de un servidor de la nube, un registro de la actividad de actualización estará disponible en la consola de Cyber Protect. Puede ver el registro y comprobar la siguiente información:

- nombre del usuario que actualizó la configuración
- fecha y hora de la actualización
- configuración de cortafuegos para conexiones de entrada y de salida
- acciones predeterminadas para conexiones de entrada y de salida
- protocolos, puertos y direcciones IP de las excepciones para conexiones de entrada y de salida

Pasos para ver la información sobre el cambio de configuración de las reglas de un cortafuegos de la nube

1. En la consola de Cyber Protect, haga clic en **Supervisión** > **Actividades**.
2. Haga clic en la actividad correspondiente y en **Todas las propiedades**.
   La descripción de la actividad debe ser **Actualizando configuración del servidor en la nube**.
3. En el campo **contexto**, inspeccione la información que le interese.

Puntos de cálculo

En Disaster Recovery a Cyber Protect Cloud, los puntos de cálculo se utilizan para los servidores principales y los servidores de recuperación durante fallos en las pruebas y en la producción. Los puntos de cálculo reflejan los recursos de cálculo utilizados para ejecutar los servidores (máquinas virtuales) en la nube.

El consumo de los puntos de cálculo durante la recuperación ante desastres depende de los parámetros del servidor y la duración del periodo de tiempo durante el que el servidor se encuentra en el estado de conmutación por error. Cuanto más potente sea el servidor y más largo el periodo de tiempo, más puntos de cálculo se consumirán. Y cuantos más puntos de cálculo se consuman, mayor será el precio que se cobrará.

Todos los servidores que estén funcionando en Cyber Protect Cloud se cobrarán por puntos de cálculo en función de su configuración de variante e independientemente de su estado (encendido o apagado).

Los servidores de recuperación en estado de espera no consumen puntos de cálculo y no se cobrará por ellos.

En la siguiente tabla puede ver un ejemplo de ocho servidores en la nube con diferentes variantes y los puntos de cálculo correspondientes que consumirán por hora. Las variantes de los servidores se pueden cambiar en la pestaña **Detalles**.

Tipo	CPU	RAM	Puntos de cálculo
F1	1 vCPU	2 GB	1
F2	1 vCPU	4 GB	2
F3	2 vCPU	8 GB	4
F4	4 vCPU	16 GB	8
F5	8 vCPU	32 GB	16
F6	16 vCPU	64 GB	32
F7	16 vCPU	128 GB	64
F8	16 vCPU	256 GB	128

Con la información que figura en la tabla, puede estimar fácilmente cuántos puntos de cálculo consumirá un servidor (máquina virtual).

Por ejemplo, si quiere proteger una máquina virtual con 4 vCPU* de 16 GB de RAM con Disaster Recovery y una máquina virtual con 2 vCPU y 8 GB de RAM, la primera máquina virtual consumirá 8 puntos de cálculo por hora, y la segunda máquina virtual 4 puntos de cálculo por hora. Si ambas máquinas virtuales están en una conmutación por error, el consumo total será de 12 puntos de cálculo por hora o 288 puntos de cálculo por todo el día (12 puntos de cálculo x 24 horas = 288 puntos de cálculo).

* vCPU se refiere a una unidad central de procesamiento (CPU) física que se asigna a una máquina virtual y es una entidad dependiente del tiempo.

Nota
Si se alcanza el exceso de la cuota de **Puntos de cálculo**, todos los servidores principales y de recuperación se apagarán. No será posible utilizar estos servidores hasta el comienzo del siguiente período de facturación o hasta que aumente la cuota. El período de facturación predeterminado es un mes calendario completo.

Conmutación por error de prueba

Realizar una conmutación por error de prueba implica iniciar un servidor de recuperación en una VLAN de prueba aislada de su red productiva. Puede probar varios servidores de recuperación a la vez y 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 las cargas de trabajo de su red local.

Durante la conmutación por error de prueba, la máquina virtual (servidor de recuperación) no se apaga. El agente lee el contenido de los discos virtuales directamente desde la copia de seguridad y accede aleatoriamente a varias partes de ella. Esto podría hacer que el rendimiento del servidor de recuperación en el estado de conmutación por error de prueba sea más lento de lo normal.

Ejecución de una prueba de conmutación por error

Aunque la realización de una conmutación por error de prueba 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.

Importante
Tiene que crear un servidor de recuperación antes para proteger sus dispositivos en caso de desastre.

Puede realizar una conmutación por error solo desde los puntos de recuperación (copias de seguridad) que se crearon después de crear el servidor de recuperación del dispositivo.

Se debe crear por lo menos un punto de recuperación antes de llevar a cabo una conmutación por error en un servidor de recuperación. Solo se permiten 100 puntos de recuperación como máximo.

Pasos para llevar a cabo una conmutación por error de prueba

1. Seleccione el equipo original o el servidor de recuperación que quiera probar.
2. Haga clic en **Disaster Recovery**.
   Se abre la descripción del servidor de recuperación.
3. Haga clic en **Conmutación por error**.
4. Seleccione el tipo de conmutación por error **Conmutación por error de prueba**.
5. Seleccione el punto de recuperación (copia de seguridad) y haga clic en **Iniciar**.
6. Si la copia de seguridad que ha seleccionado está cifrada usando el cifrado como una propiedad del equipo:

a. Introduzca la contraseña de cifrado para la copia de seguridad establecida.

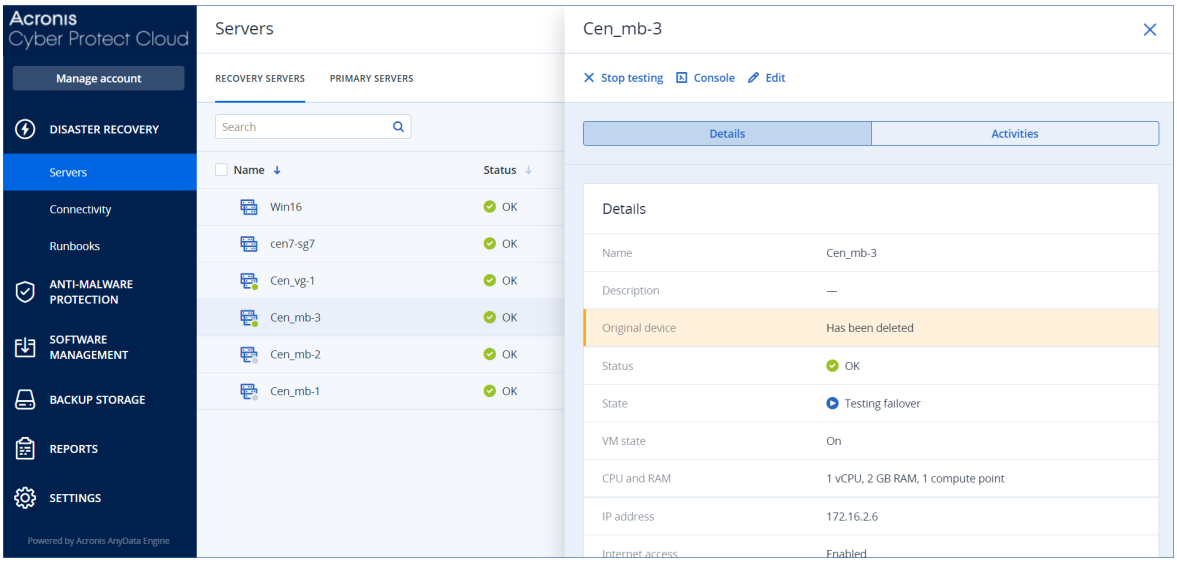
> **Nota**
> Solo se guardará la contraseña temporalmente y se utilizará para la operación de prueba de conmutación por error actual. La contraseña se eliminará automáticamente del almacén de credenciales si se detiene la prueba de conmutación por error o una vez que esta se haya completado.

b. [Opcional] Para guardar la contraseña de la copia de seguridad establecida y utilizarla en las siguientes operaciones de conmutación por error, seleccione la casilla de verificación **Almacenar la contraseña en un almacén de credenciales seguro...** e introduzca un nombre para las credenciales en el campo **Nombre de las credenciales**.

> **Importante**
> La contraseña se almacenará en un almacén de credenciales seguro y se aplicará automáticamente en las siguientes operaciones de conmutación por error. No obstante, es posible que incumpla sus obligaciones legales si guarda las contraseñas.

c. Haga clic en **Listo**.

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



7. Use uno de los siguientes métodos para probar el servidor de recuperación:
   - En **Disaster Recovery** > **Servidores**, seleccione el servidor de recuperación y, a continuación, haga clic en **Consola**.
   - 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.

8. Cuando la prueba haya terminado, haga clic en **Detener comprobación**.
   El servidor de recuperación se detiene. Todos los cambios realizados en el servidor de recuperación durante la prueba de conmutación por error se pierden.

Conmutación por error de prueba automatizada

Con la conmutación por error de prueba automatizada, el servidor de recuperación se prueba automáticamente una vez al mes sin ninguna interacción manual.

El proceso de conmutación por error de prueba automatizada está formado por las siguientes partes:

1. creación de una máquina virtual desde el último punto de recuperación
2. captura de pantalla de la máquina virtual
3. análisis de si el sistema operativo de la máquina virtual empieza correctamente
4. notificación acerca del estado de la conmutación por error de prueba

Nota
La conmutación por error de prueba automatizada consume puntos de cálculo.

Puede configurar la conmutación por error de prueba automatizada en la configuración del servidor de recuperación. Para obtener más información, consulte "Configuración de la conmutación por error de prueba automatizada" (p. 78).

Tenga en cuenta que, en casos muy excepcionales, la conmutación por error de prueba automatizada podría omitirse y no ejecutarse a la hora planificada. Esto se debe a que la conmutación por error de producción tiene mayor prioridad que la conmutación por error de prueba automatizada, de manera que los recursos de hardware (CPU y RAM) asignados para la conmutación por error de prueba automatizada podrían estar limitados temporalmente para garantizar que hay suficientes recursos para una conmutación por error de producción simultánea.

Si, por algún motivo, la conmutación por error de prueba se omite, se emitirá una alerta.

Nota
La conmutación por error de prueba automatizada fallará si las copias de seguridad del equipo original están cifradas utilizando el cifrado como una propiedad del equipo, y la contraseña de cifrado no se especifica al crear el servidor de recuperación. Para obtener más información sobre cómo especificar la contraseña de cifrado, consulte "Creación de un servidor de recuperación" (p. 59).

Configuración de la conmutación por error de prueba automatizada

Al configurar la conmutación por error de prueba automatizada, puede probar el servidor de recuperación de forma mensual sin ejecutar ninguna acción manual.

Pasos para configurar la conmutación por error de prueba automatizada

1. En la consola, vaya a **Recuperación ante desastres** > **Servidores** > **Servidores de recuperación** y seleccione el servidor de recuperación.
2. Haga clic en **Editar**.
3. En la pestaña **Conmutación por error de prueba automatizada**, en el campo **Planificación**, seleccione **Mensual**.
4. [Opcional] En **Tiempo de espera de las capturas de pantalla**, cambia el valor predeterminado del periodo de tiempo máximo (en minutos) para que el sistema intente realizar la prueba de conmutación por error automatizada.
5. [Opcional] Si desea guardar el valor **Tiempo de espera de las capturas de pantalla** como predeterminado y que se rellene automáticamente cuando habilite la conmutación por error de prueba automatizada para el resto de servidores de recuperación, seleccione **Establecer como tiempo de espera predeterminado**.
6. Haga clic en **Guardar**.

Ver el estado de la conmutación por error de prueba automatizada

Puede ver la información de una conmutación por error de prueba automatizada completada, como el estado, la hora de inicio, la hora de finalización, la duración y la captura de pantalla de la máquina virtual.

Nota
La captura de pantalla de la máquina virtual se conserva hasta que la conmutación por error de la prueba automatizada se ejecuta de nuevo y genera una nueva captura de pantalla.

Pasos para ver el estado de la conmutación por error de prueba automatizada de un servidor de recuperación

1. En la consola, vaya a **Recuperación ante desastres** > **Servidores** > **Servidores de recuperación** y seleccione el servidor de recuperación.
2. En la sección **Conmutación por error de prueba automatizada**, compruebe la información de la última conmutación por error de prueba automatizada.
3. [Opcional] Para ver la captura de pantalla de la máquina virtual, haga clic en **Mostrar captura de pantalla**.

Deshabilitación de la conmutación por error de prueba automatizada

Puede deshabilitar la conmutación por error de prueba automatizada si desea ahorrar recursos o no necesita que se ejecute en determinado servidor de recuperación.

Pasos para deshabilitar la conmutación por error de prueba automatizada

1. En la consola, vaya a **Disaster Recovery** > **Servidores** > **Servidores de recuperación** y seleccione el servidor de recuperación.
2. Haga clic en **Editar**.
3. En el asistente, haga clic en la pestaña **Conmutación por error de prueba automatizada**.
4. Desactive el interruptor **Conmutación por error de prueba automática**.
5. Haga clic en **Guardar**.

Conmutación por error de producción

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

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

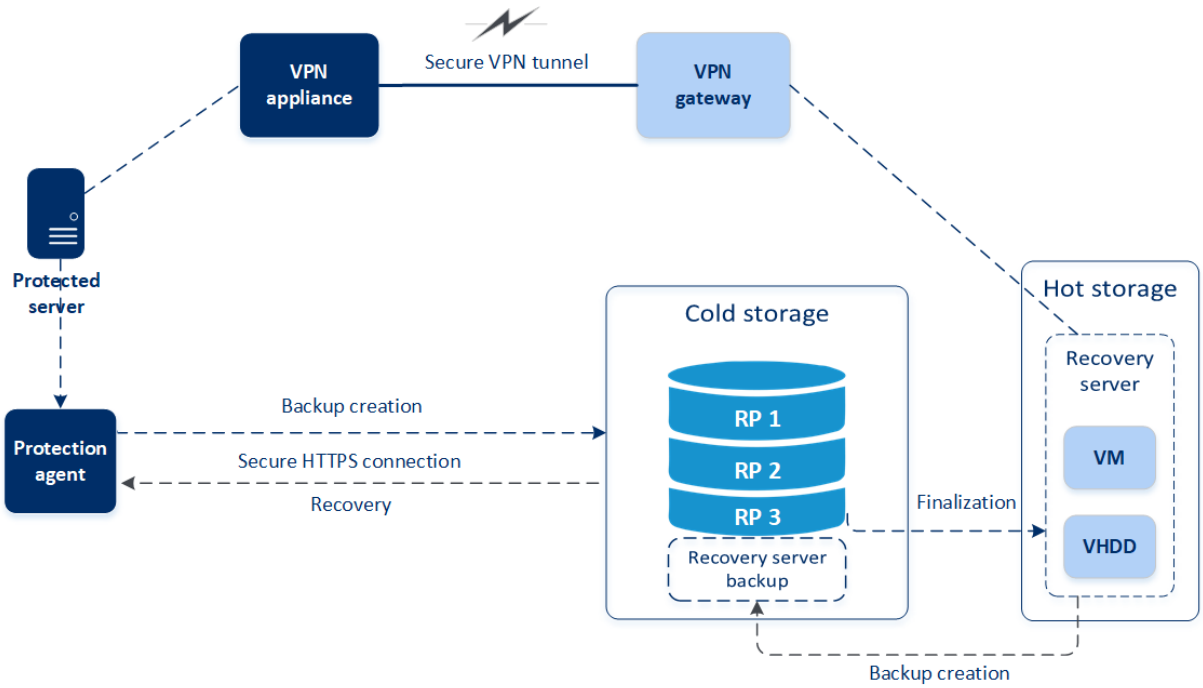
Al iniciar el proceso de conmutación por error, seleccione el punto de recuperación (copia de seguridad) del equipo original a partir del cual se creará una máquina virtual con los parámetros predefinidos. La operación de conmutación por error usa la funcionalidad "ejecutar equipo virtual a partir de una copia de seguridad". El servidor de recuperación obtiene el estado de transición **Finalización**. Este proceso consiste en transferir los discos virtuales del servidor desde el almacenamiento de copia de seguridad (almacenamiento "inactivo") hasta el almacenamiento de recuperación ante desastres (almacenamiento "de acceso frecuente").

Nota
Durante el estado **Finalización**, el servidor es accesible y funcional, aunque su rendimiento será menor de lo normal. Puede abrir la consola del servidor haciendo clic en el enlace **La consola está lista**. El enlace está disponible en la columna **Estado de la máquina virtual** en la pantalla **Disaster Recovery** > **Servidores** y en la vista **Detalles** del servidor.

Cuando se complete el estado **Finalización**, el rendimiento del servidor alcanzará 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 la nube.

Si el servidor de recuperación cuenta con un agente de protección 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 componente de copia de seguridad).

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



Realización de una conmutación por error

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

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 conmutación por error, el servidor de recuperación se inicia en la red de producción. Para evitar interferencias y problemas no deseados, asegúrese de que la carga de trabajo original no está en línea ni se puede acceder a ella a través de la VPN.

Para evitar una interferencia de la copia de seguridad en el mismo archivo comprimido de la nube, revoque de forma manual el plan de protección de la carga de trabajo que se encuentra en el estado **Conmutación por error**. Para obtener más información sobre la revocación de planes, consulte Revocación de un plan de protección.

Importante
Tiene que crear un servidor de recuperación antes para proteger sus dispositivos en caso de desastre.

Puede realizar una conmutación por error solo desde los puntos de recuperación (copias de seguridad) que se crearon después de crear el servidor de recuperación del dispositivo.

Se debe crear por lo menos un punto de recuperación antes de llevar a cabo una conmutación por error en un servidor de recuperación. Solo se permiten 100 puntos de recuperación como máximo.

Puede seguir el procedimiento siguiente o ver el tutorial en vídeo.

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 Cyber Protect, vaya a **Disaster Recovery** > **Servidores** > **Servidores de recuperación** y seleccione el servidor de recuperación.
3. Haga clic en **Conmutación por error**.
4. Seleccione **Conmutación por error en producción**.
5. Seleccione el punto de recuperación (copia de seguridad) y haga clic en **Iniciar**.
6. [Si la copia de seguridad que ha seleccionado está cifrada usando el cifrado como una propiedad del equipo]
   a. Introduzca la contraseña de cifrado para la copia de seguridad establecida.

      Nota
      Solo se guardará la contraseña temporalmente y se utilizará para la operación de conmutación por error actual. La contraseña se eliminará automáticamente del almacén de credenciales una vez que se complete la operación de conmutación por error y el servidor vuelva al estado **En espera**.

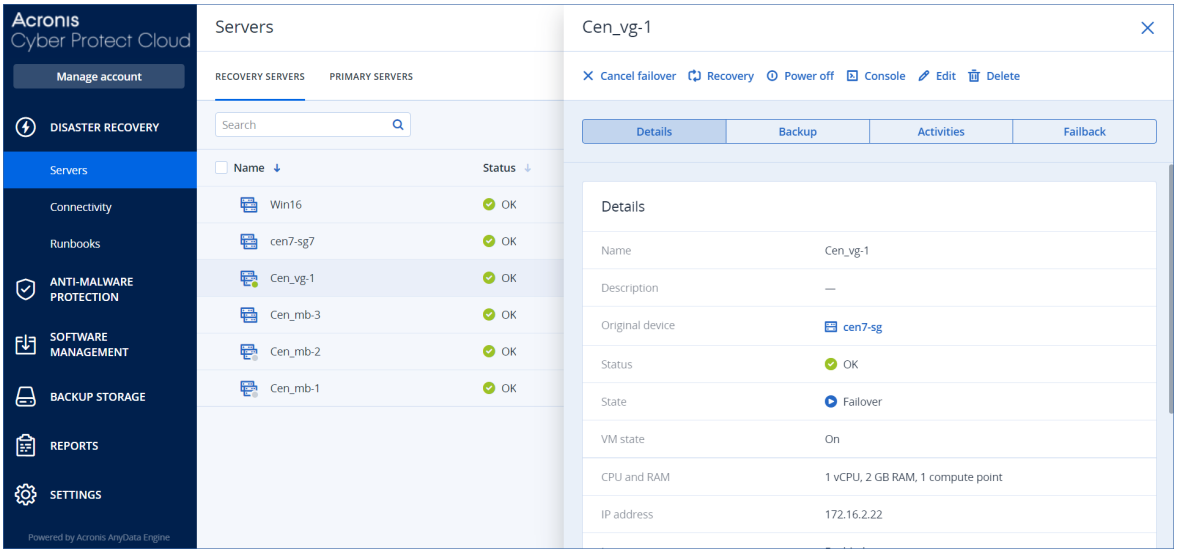
   b. [Opcional] Para guardar la contraseña de la copia de seguridad establecida y utilizarla en las siguientes operaciones de conmutación por error, seleccione la casilla de verificación **Almacenar la contraseña en un almacén de credenciales seguro...** e introduzca un nombre para las credenciales en el campo **Nombre de las credenciales**.

      Importante
      La contraseña se almacenará en un almacén de credenciales seguro y se aplicará automáticamente en las siguientes operaciones de conmutación por error. No obstante, es posible que incumpla sus obligaciones legales si guarda las contraseñas.

   c. Haga clic en **Listo**.

   Cuando el servidor de recuperación se inicia, su estado cambia a **Finalización** y, después de un tiempo, cambia a **Conmutación por error**.

Importante
Es importante saber que el servidor sigue estando disponible durante los estados **Finalización** y **Conmutación por error**. Durante el estado **Finalización**, puede acceder a la consola del servidor haciendo clic en el enlace **La consola está lista**. El enlace está disponible en la columna **Estado de la máquina virtual** en la pantalla **Disaster Recovery** > **Servidores** y en la vista **Detalles** del servidor.



7. Mire la consola del servidor de recuperación para asegurarse de que se ha iniciado. Haga clic en **Disaster Recovery** > **Servidores**, seleccione el servidor de recuperación y, a continuación, haga clic en **Consola**.
8. 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 protección. Este plan de protección 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".

Cómo realizar una conmutación por error de servidores mediante DNS local

Si su sitio local utiliza servidores DNS para resolver los nombres de los equipos, es posible que los servidores de recuperación no consigan comunicarse después de una conmutación por error. Esto sucede porque los servidores DNS de la nube son diferentes a los del sitio local. De manera predeterminada, los servidores de la nube recién creados utilizan los servidores DNS del sitio de la nube, pero puede configurar ajustes de DNS personalizados. Para obtener más información, consulte "Configuración de servidores DNS personalizados" (p. 53).

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 VPN 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 VPN 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 del 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 VPN).

Nota
Las instrucciones no serán válidas si su servidor DHCP en la nube se ha configurado con la opción **DHCP personalizado** y algunos de los servidores principales o de recuperación obtienen su dirección IP de dicho servidor DHCP.

Detener una conmutación por error

Puede detener una conmutación por error de producción en cualquier momento, durante cada fase del proceso.

Nota
Al detener una conmutación por error, se revierten todos los cambios que se realizaron desde el momento en que se inició, excepto las copias de seguridad del servidor de recuperación.

Pasos para detener una conmutación por error

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores** > **Servidores de recuperación**.
2. Seleccione el servidor de recuperación cuyo estado sea **Conmutación por error**.
3. Haga clic en el servidor de recuperación.
4. Haga clic en **Detener conmutación por error**.
5. En la ventana de confirmación que aparece, seleccione la casilla de verificación y, a continuación, haga clic en **Detener conmutación por error**.
   Se ha detenido la conmutación por error. El servidor de recuperación vuelve al estado **Espera**.

Conmutación por recuperación

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La conmutación por recuperación es un proceso que consiste en mover la carga de trabajo desde la nube a la máquina física o virtual en su sitio local. Puede realizar una conmutación tras recuperación en un servidor de recuperación en estado de **Conmutación por error** y seguir usando el servidor en su sitio local.

Puede ejecutar una conmutación por error automatizada en una máquina virtual o un equipo físico en su sitio local. Durante la conmutación tras recuperación, mientras la máquina virtual funciona en la nube, puede transferir los datos de la copia de seguridad al sitio local. Esta tecnología le ayuda a obtener un tiempo de inactividad muy breve, que se calcula y aparece en la consola de Cyber Protect. Puede verlo y usar esta información para planificar sus actividades y, si fuese necesario, advertir a sus clientes sobre un próximo tiempo de inactividad. Si realiza conmutación tras recuperación basada en agente con un dispositivo de arranque, el tiempo de inactividad aún será menor, porque los cambios delta se transferirán al sitio local.

Para una conmutación tras recuperación a un equipo físico de destino, puede utilizar la conmutación tras recuperación basada en agente a través de un dispositivo de arranque. Para obtener más información, consulte "Realización de conmutación tras recuperación basada en agente mediante dispositivo de arranque" (p. 86).

Para una conmutación tras recuperación a una máquina virtual de destino, puede utilizar la conmutación tras recuperación basada en agente a través de un dispositivo de arranque o la conmutación tras recuperación sin agente a través del agente de hipervisor. Para obtener más información, consulte "Realización de conmutación tras recuperación basada en agente mediante dispositivo de arranque" (p. 86) y "Realización de conmutación tras recuperación sin agente a través de un agente de hipervisor" (p. 91).

En casos específicos en los que no pueda usar el procedimiento de conmutación tras recuperación automatizada, puede realizarla de forma manual. Para obtener más información, consulte "Conmutación tras recuperación manual" (p. 94).

Nota
Las operaciones de runbook solo admiten la conmutación tras recuperación en el modo manual. Esto significa que, si inicia el proceso de conmutación tras recuperación mediante la ejecución de un runbook que incluya un paso **Servidor de conmutación tras recuperación**, el procedimiento requerirá una interacción manual: deberá recuperar el equipo de forma manual y confirmar o cancelar el proceso de conmutación tras recuperación desde la pestaña **Disaster Recovery** > **Servidores**.

Conmutación tras recuperación basada en agente mediante dispositivo de arranque

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

El proceso de conmutación tras recuperación basada en agente mediante dispositivos de arranque está optimizado para realizar una conmutación tras recuperación a la máquina física o virtual original. Durante este proceso, solo se transfieren los cambios delta al sitio local.

El proceso de conmutación tras recuperación basada en el agente a través de un dispositivo de arranque a una máquina física o virtual de destino consta de las siguientes fases:

1. **Planificación**. Durante esta fase, restaure la infraestructura de TI en su sitio local (como los servidores y las configuraciones de red), configure los parámetros de la conmutación tras recuperación y planifique el inicio de la transferencia de datos.
2. **Transferencia de datos**. Durante esta fase, la máquina virtual en la nube sigue funcionando mientras se transfieren los datos del sitio en la nube al sitio local. Puede iniciar la siguiente fase de cambio en cualquier momento durante la transferencia de datos, pero deberá tener en cuenta la siguientes relaciones.
   Cuanto más tiempo pase en la fase de transferencia de datos,
   - más tiempo se seguirá ejecutando la máquina virtual en la nube;
   - mayor será la cantidad de datos transferidos a su sitio local;
   - mayor será el coste que pagará (gasta más en puntos de cálculo);
   - menor será el tiempo de inactividad que experimente durante la fase de cambio.

   Si desea reducir el tiempo de inactividad, inicie la fase de cambio cuando se haya transferido más del 90 % de los datos al sitio local.
   Si no puede permitirse tener un tiempo de inactividad más largo y no desea gastar más puntos de cálculo para ejecutar la máquina virtual en la nube, puede empezar la fase de cambio antes.

   Nota
   El proceso de transferencia de datos utiliza una tecnología flashback. Esta tecnología compara los datos disponibles en el equipo de destino con los de la máquina virtual en la nube. Si parte de los datos ya están disponibles en el equipo de destino, no se transferirán de nuevo. Esta tecnología agiliza la fase de transferencia de datos.
   Por ese motivo, le recomendamos que restaure el servidor en el equipo original en el sitio local.
3. **Cambio**. Durante esta fase, la máquina virtual en la nube se apagará y los datos restantes, incluido el incremento de la última copia de seguridad, se transferirán al sitio local. Si no se aplica ningún plan de copias de seguridad en el servidor de recuperación, se ejecutará

automáticamente una copia de seguridad durante la fase de cambio y ralentizará el proceso.

4. **Validación**. Durante esta fase, el equipo del sitio local estará listo y podrá reiniciarlo con un dispositivo de arranque basado en Linux. Compruebe que la máquina virtual funciona correctamente y:
   - Si todo funciona según lo esperado, confirme la conmutación por recuperación. Tras la confirmación de la conmutación por recuperación, se eliminará la máquina virtual en la nube y el servidor de recuperación volverá al estado **En espera**. El proceso de conmutación por recuperación habrá terminado.
   - Si algo va mal, puede cancelar la conmutación por error y volver a la fase de planificación.

Nota
Una vez que se haya reiniciado el dispositivo de arranque, no podrá volver a utilizarlo. Si descubre que algo va mal durante la fase de validación, debe registrar un nuevo dispositivo de arranque y volver a iniciar el proceso de conmutación tras recuperación.

Sin embargo, al utilizarse la tecnología flashback, no se volverán a transferir los datos que ya estén en el sitio local y el proceso de conmutación tras recuperación será mucho más rápido.

Realización de conmutación tras recuperación basada en agente mediante dispositivo de arranque

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede ejecutar una conmutación tras recuperación basada en agente mediante dispositivo de arranque en un equipo físico o una máquina virtual de destino en su sitio local.

Nota
El proceso de transferencia de datos utiliza una tecnología flashback. Esta tecnología compara los datos disponibles en el equipo de destino con los de la máquina virtual en la nube. Si parte de los datos ya están disponibles en el equipo de destino, no se transferirán de nuevo. Esta tecnología agiliza la fase de transferencia de datos.

Por ese motivo, le recomendamos que restaure el servidor en el equipo original en el sitio local.

Requisitos previos

- El agente que utilizará para ejecutar la conmutación por recuperación está en línea y no se está utilizando actualmente en otra operación de conmutación por recuperación.
- Su conexión a Internet es estable.
- Hay un dispositivo de arranque registrado disponible. Para obtener más información, consulte "Creación de dispositivos de arranque para recuperar sistemas operativos" en la guía del usuario de Cyber Protection.

- El equipo de destino es el equipo original en su sitio local o tiene el mismo firmware que el equipo original.
- Existe al menos una copia de seguridad completa de la máquina virtual en la nube.

Pasos para llevar a cabo una conmutación por recuperación de un equipo físico

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores**.
2. Seleccione un servidor de recuperación cuyo estado sea **Conmutación por error**.
3. Haga clic en la pestaña **Conmutación por recuperación**.
4. En el campo **Tipo de conmutación tras recuperación**, seleccione **Basada en agente a través de dispositivo de arranque**.
5. En el campo **Dispositivo de arranque de destino**, haga clic en **Especificar**, seleccione el dispositivo de arranque y haga clic en **Listo**.

   Nota
   Le recomendamos que utilice un dispositivo de arranque listo porque ya estará configurado. Para obtener más información, consulte "Creación de dispositivos de arranque para recuperar sistemas operativos" en la guía del usuario de Cyber Protection.

6. [Opcional] Para cambiar la asignación de discos predeterminada, en el campo **Asignación de discos**, haga clic en **Especificar**, asigne los discos de la copia de seguridad a los discos del equipo de destino y haga clic en **Listo**.
7. Haga clic en **Iniciar transferencia de datos** y, en la ventana de confirmación, haga clic en **Iniciar**.

   Nota
   Si no hay una copia de seguridad de la máquina virtual en la nube, el sistema realizará una copia de seguridad automáticamente antes de la fase de transferencia de datos.

   Se iniciará la fase de transferencia de datos. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra cuántos datos se han transferido ya al sitio local y la cantidad total de datos que se transferirán. La cantidad total de datos incluye los de la copia de seguridad más reciente antes de que se iniciase la fase de transferencia de datos y las copias de seguridad de los datos recién generados (incrementos de copia de seguridad), mientras que la máquina virtual sigue ejecutándose en la fase de transferencia de datos. Por este motivo, los valores de **Progreso** aumentarán con el paso del tiempo. Como el sistema utiliza una tecnología flashback durante la transferencia de datos y no transfiere los datos que están disponibles en el equipo de destino, puede que el progreso sea más rápido de lo que ha calculado inicialmente la consola.

Campo	Descripción
Estimación del tiempo de inactividad	Este parámetro muestra cuánto tiempo dejará de estar disponible la máquina virtual en la nube si inicia la fase de cambio ahora. El valor se calcula según los valores del parámetro **Progreso** y disminuye con el paso del tiempo. Como el sistema utiliza una tecnología flashback durante la transferencia de datos y no transfiere los datos que están disponibles en el equipo de destino, puede que el tiempo de inactividad sea mucho menor que el valor que ha mostrado inicialmente la consola.

8. Haga clic en **Cambio** y en la ventana de confirmación vuelva a hacer clic en **Cambio**.
   Se iniciará la fase de cambio. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra el progreso de restauración del equipo en el sitio local.
Tiempo estimado para finalizar	Este parámetro muestra el tiempo aproximado en el que se completará la fase de cambio y tras el que podrá encender el equipo en el sitio local.

Nota
Si no se aplica ningún plan de copias de seguridad en la máquina virtual de la nube, se ejecutará automáticamente una copia de seguridad durante la fase de cambio, lo cual ralentizará el proceso.

9. Cuando se complete la fase de **cambio**, reinicie el dispositivo de arranque y compruebe que el equipo físico de su sitio local funciona según lo esperado.
   Para obtener más información, consulte "Recuperar discos usando dispositivos de arranque" en la guía del usuario de Cyber Protection.
10. Para finalizar el proceso, haga clic en **Confirmar la conmutación tras recuperación** y, en la ventana de confirmación, haga clic en **Confirmar**.
    Se eliminará el equipo virtual en la nube y el servidor de recuperación volverá al estado **En espera**.

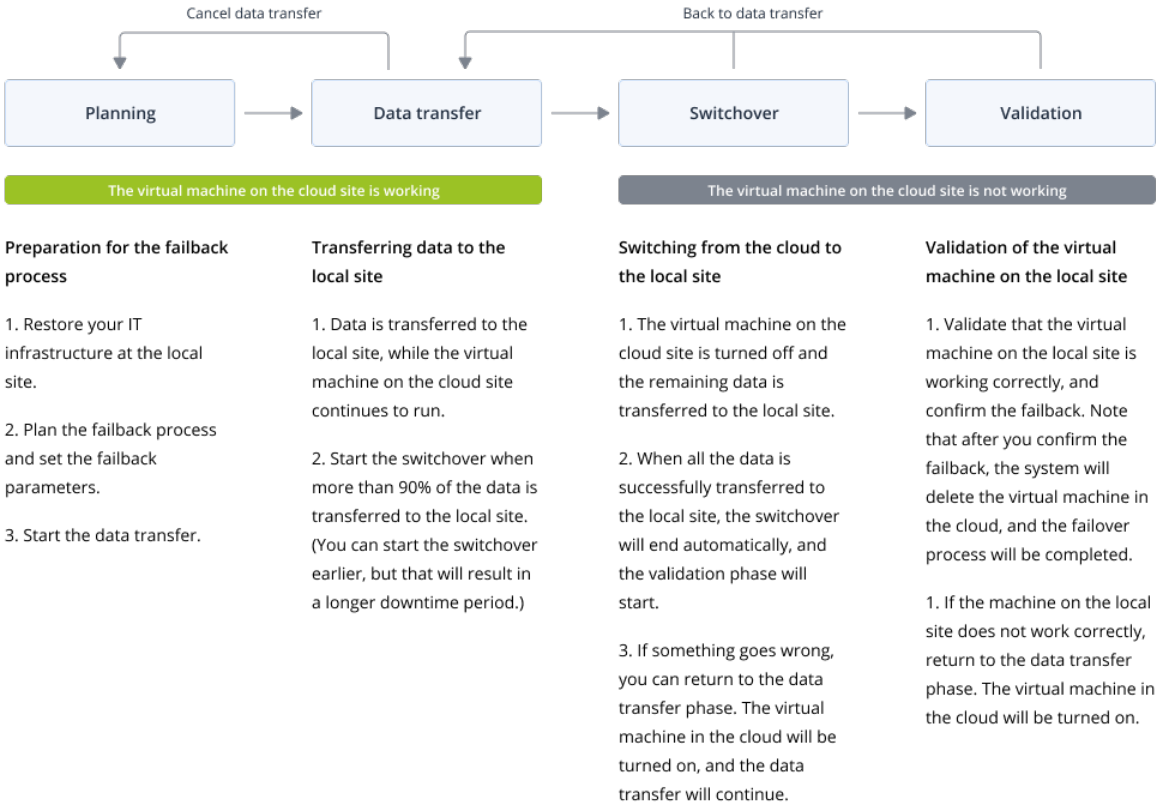
Nota
Aplicar un plan de protección en el servidor recuperado no forma parte del proceso de conmutación por recuperación. Una vez que finalice este proceso, aplique un plan de protección en el servidor recuperado para asegurarse de que vuelve a estar protegido. Puede aplicar el mismo plan de protección que se aplicó al servidor original o un nuevo plan que tenga habilitado el módulo **Recuperación ante desastres**.

Conmutación tras recuperación sin agente a través de un agente de hipervisor

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La conmutación tras recuperación sin agente a través de un proceso de agente de hipervisor está optimizada para realizar una conmutación tras recuperación a una nueva máquina virtual. Si desea realizar una conmutación tras recuperación a la máquina virtual original, siga el procedimiento para la conmutación tras recuperación basada en agente mediante un dispositivo de arranque.

La conmutación tras recuperación sin agente mediante un agente de hipervisor consta de cuatro fases.



1. **Planificación**. Durante esta fase, restaure la infraestructura de TI en su sitio local (como los servidores y las configuraciones de red), configure los parámetros de la conmutación tras recuperación y planifique el inicio de la transferencia de datos.

Nota
Para minimizar el tiempo total del proceso de conmutación tras recuperación, le recomendamos que inicie la fase de transferencia de datos inmediatamente después de configurar sus servidores locales y, a continuación, continúe con la configuración de la red y del resto de la infraestructura local durante la fase de transferencia de datos.

2. **Transferencia de datos**. Durante esta fase, la máquina virtual en la nube sigue funcionando mientras se transfieren los datos del sitio en la nube al sitio local. Puede iniciar la siguiente fase de cambio en cualquier momento durante la transferencia de datos, pero deberá tener en cuenta la siguientes relaciones.

   Cuanto más tiempo pase en la fase de transferencia de datos,

   - más tiempo se seguirá ejecutando la máquina virtual en la nube;
   - mayor será la cantidad de datos transferidos a su sitio local;
   - mayor será el coste que pagará (gasta más en puntos de cálculo);
   - menor será el tiempo de inactividad que experimente durante la fase de cambio.

   Si desea reducir el tiempo de inactividad, inicie la fase de cambio cuando se haya transferido más del 90 % de los datos al sitio local.

   Si no puede permitirse tener un tiempo de inactividad más largo y no desea gastar más puntos de cálculo para ejecutar la máquina virtual en la nube, puede empezar la fase de cambio antes.

   Si cancela el proceso de conmutación por recuperación durante la fase de transferencia de datos, los datos transferidos no se eliminarán del sitio local. Para evitar posibles problemas, elimine de forma manual los datos transferidos antes de iniciar un nuevo proceso de conmutación por recuperación. El posterior proceso de transferencia de datos se iniciará desde el principio.
3. **Cambio**. Durante esta fase, la máquina virtual en la nube se apagará y los datos restantes, incluido el incremento de la última copia de seguridad, se transferirán al sitio local. Si no se aplica ningún plan de copias de seguridad en el servidor de recuperación, se ejecutará automáticamente una copia de seguridad durante la fase de cambio y ralentizará el proceso.

   Puede ver el tiempo estimado de finalización (tiempo de inactividad) de esta fase en la consola de Cyber Protect. Cuando todos los datos se han transferido al sitio local (no hay pérdida de datos y la máquina virtual en el sitio local es una copia exacta de la máquina virtual en la nube), se completa la fase de cambio. Se recuperará la máquina virtual en el sitio local y se iniciará la fase de validación automáticamente.
4. **Validación**. Durante esta fase, la máquina virtual en el sitio local está lista y se inicia automáticamente. Puede verificar si la máquina virtual está funcionando correctamente, y:
   - Si todo funciona según lo esperado, confirme la conmutación por recuperación. Tras la confirmación de la conmutación por recuperación, se eliminará la máquina virtual en la nube y el servidor de recuperación volverá al estado **En espera**. El proceso de conmutación por recuperación habrá terminado.
   - Si algo va mal, puede cancelar el cambio y volver a la fase de transferencia de datos.

Realización de conmutación tras recuperación sin agente a través de un agente de hipervisor

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede realizar una conmutación tras recuperación sin agente a una máquina virtual de destino en su sitio local a través de un agente de hipervisor.

Requisitos previos

- El agente que utilizará para ejecutar la conmutación por recuperación está en línea y no se está utilizando actualmente en otra operación de conmutación por recuperación.
- Su conexión a Internet es estable.
- Existe al menos una copia de seguridad completa de la máquina virtual en la nube.

Pasos para realizar una conmutación tras recuperación sin agente a una máquina virtual a través de un agente de hipervisor

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores**.
2. Seleccione un servidor de recuperación cuyo estado sea **Conmutación por error**.
3. Haga clic en la pestaña **Conmutación por recuperación**.
4. En la sección **Parámetros de la conmutación por recuperación**, en el campo **Tipo de conmutación tras recuperación**, seleccione **Sin agente a través del hipervisor** y, a continuación, configure los demás parámetros.
   Tenga en cuenta que, de manera predeterminada, algunos **Parámetros de la conmutación por recuperación** se establecen automáticamente con los valores sugeridos, pero puede cambiarlos.
   La siguiente tabla proporciona más información sobre los **Parámetros de la conmutación por recuperación**.

Parámetro	Descripción
Tamaño de la copia de seguridad	La cantidad de datos que se transferirán a su sitio local durante el proceso de conmutación por recuperación. Tras iniciar el proceso de conmutación por recuperación a un equipo virtual de destino, el **Tamaño de la copia de seguridad** aumentará durante la fase de transferencia de datos debido a que el equipo virtual en la nube seguirá funcionando y generando nuevos datos. Para calcular una estimación del período de inactividad durante el proceso de conmutación por recuperación a un equipo virtual de

Parámetro	Descripción
	destino, tome el 10 % del valor del **Tamaño de la copia de seguridad** (puesto que recomendamos iniciar la fase de cambio tras haberse transferido el 90 % de los datos a su sitio local) y divídalo entre el valor de la velocidad de su conexión a Internet. **Nota** El valor de la velocidad de su conexión a Internet se reducirá si realiza varios procesos de conmutación por recuperación al mismo tiempo.
Ubicación del equipo de destino	Ubicación de la conmutación por recuperación: un servidor de VMware ESXi o de Microsoft Hyper-V. Puede elegir entre todos los servidores que tienen un agente registrado en el servicio de ciberprotección.
Agente	Agente que ejecutará la operación de conmutación por recuperación. Solo puede utilizar un agente para llevar a cabo una operación de conmutación por recuperación al mismo tiempo. Puede seleccionar un agente que esté en línea y no se esté utilizando para otro proceso de conmutación por recuperación y que tenga una versión que admita la funcionalidad de conmutación por recuperación y derechos para acceder a la copia de seguridad. Tenga en cuenta que puede instalar varios agentes en servidores VMware ESXi e iniciar un proceso de conmutación por recuperación independiente con cada uno de ellos. Puede llevar a cabo estos procesos de conmutación por recuperación a la vez.
Configuración del equipo de destino	Configuración del equipo virtual: • **Procesadores virtuales**. Seleccione el número de procesadores virtuales. • **Memoria**. Seleccione cuánta memoria tendrá el equipo virtual. • **Unidades**. Seleccione las unidades para la memoria. • [Opcional] **Adaptadores de red**. Para añadir un adaptador de red, haga clic en **Agregar** y seleccione una red en el campo **Red**. Cuando haya acabado de hacer cambios, haga clic en **Listo**.
Ruta	(Para servidores de Microsoft Hyper-V) Carpeta en el servidor en el que se almacenará su máquina. Asegúrese de que hay suficiente espacio de memoria libre en el servidor para la máquina.
Almacén de datos	(Para servidores de VMware ESXi) Almacén de datos en el servidor en el que se almacenará su máquina.

Parámetro	Descripción
	Asegúrese de que hay suficiente espacio de memoria libre en el servidor para la máquina.
Modo de aprovisionamiento	Método de asignación del disco virtual. Para servidores de Microsoft Hyper-V: • **Expansión dinámica** (valor predeterminado). • **Tamaño fijo**. Para servidores de Microsoft Hyper-V: • **Ligero** (valor predeterminado). • **Grueso**.
Nombre del equipo de destino	Nombre de la máquina de destino. De forma predeterminada, el nombre de la máquina de destino es el mismo que el del servidor de recuperación. El nombre del equipo de destino debe ser único en la **Ubicación del equipo de destino** seleccionada.

5. Haga clic en **Iniciar transferencia de datos** y, en la ventana de confirmación, haga clic en **Iniciar**.

Nota
Si no hay una copia de seguridad de la máquina virtual en la nube, el sistema realizará una copia de seguridad automáticamente antes de la fase de transferencia de datos.

Se iniciará la fase de **transferencia de datos**. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra cuántos datos se han transferido ya al sitio local y la cantidad total de datos que se transferirán. La cantidad total de datos incluye los de la copia de seguridad más reciente antes de que se iniciase la fase de transferencia de datos y las copias de seguridad de los datos recién generados (incrementos de copia de seguridad), mientras que la máquina virtual sigue ejecutándose en la fase de transferencia de datos. Por este motivo, ambos valores del parámetro **Progreso** aumentarán con el paso del tiempo.
Estimación del tiempo de inactividad	Este parámetro muestra cuánto tiempo dejará de estar disponible la máquina virtual en la nube si inicia la fase de cambio ahora. El valor se calcula según los valores del parámetro **Progreso** y disminuye con el paso del tiempo.

6. Haga clic en **Cambio** y en la ventana de confirmación vuelva a hacer clic en **Cambio**.
Se iniciará la fase de cambio. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra el progreso de restauración del equipo en el sitio local.
Tiempo estimado para finalizar	Este parámetro muestra el tiempo aproximado en el que se completará la fase de cambio y tras el que podrá encender el equipo en el sitio local.

Nota
Si no se aplica ningún plan de copias de seguridad en la máquina virtual de la nube, se ejecutará automáticamente una copia de seguridad durante la fase de cambio, lo cual ralentizará el proceso.

7. Después de que se complete la fase de **Cambio** y se inicie automáticamente la máquina virtual en el sitio local, verifique que esté funcionando correctamente.
8. Para finalizar el proceso, haga clic en **Confirmar la conmutación por recuperación** y, en la ventana de confirmación, haga clic en **Confirmar**.
   Se eliminará el equipo virtual en la nube y el servidor de recuperación volverá al estado **En espera**.

Nota
Aplicar un plan de protección en el servidor recuperado no forma parte del proceso de conmutación por recuperación. Una vez que finalice este proceso, aplique un plan de protección en el servidor recuperado para asegurarse de que vuelve a estar protegido. Puede aplicar el mismo plan de protección que se aplicó al servidor original o un nuevo plan que tenga habilitado el módulo **Recuperación ante desastres**.

Conmutación tras recuperación manual

Nota
Le recomendamos que utilice el proceso de conmutación tras recuperación en un modo manual solo cuando se lo indique el equipo de soporte.

También puede iniciar un proceso de conmutación tras recuperación en un modo manual. En este caso, la transferencia de datos desde la copia de seguridad en la nube al sitio local no se llevará a cabo de forma automática. Se debe hacer de forma manual cuando la máquina virtual en la nube esté apagada. Esto hace que el proceso de conmutación tras recuperación en un modo manual sea mucho más lento y probablemente el tiempo de inactividad también sea mayor.

El proceso de conmutación tras recuperación en un modo manual consta de las siguientes fases:

1. **Planificación**. Durante esta fase, restaure la infraestructura de TI en su sitio local (como los servidores y las configuraciones de red), configure los parámetros de la conmutación tras recuperación y planifique el inicio de la transferencia de datos.

2. **Cambio**. Durante esta fase, la máquina virtual en la nube se apagará y se hará una copia de seguridad de los datos recién generados. Si no se aplica ningún plan de copias de seguridad en el servidor de recuperación, se ejecutará automáticamente una copia de seguridad durante la fase de cambio y ralentizará el proceso. Cuando la copia de seguridad haya finalizado, restaure la máquina en el sitio local de forma manual. Puede recuperar el disco mediante un dispositivo de arranque o toda la máquina desde el almacenamiento de la copia de seguridad en la nube.
3. **Validación**. Durante esta fase, verifique que el equipo físico o la máquina virtual en el sitio local funciona correctamente y confirme la conmutación tras recuperación. Tras la confirmación, se eliminará la máquina virtual en el sitio en la nube y el servidor de recuperación volverá al estado **En espera**.

Realización de una conmutación tras recuperación manual

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede ejecutar una conmutación tras recuperación en un equipo físico o una máquina virtual de destino en su sitio local.

Pasos para llevar a cabo una conmutación tras recuperación manual

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores**.
2. Seleccione un servidor de recuperación cuyo estado sea **Conmutación por error**.
3. Haga clic en la pestaña **Conmutación por recuperación**.
4. En el campo **Destino**, seleccione **Equipo físico**.
5. Haga clic en el icono de engranaje y habilite el conmutador **Usar el modo manual**.
6. [Opcional] Calcule una estimación del período de inactividad durante el proceso de conmutación por recuperación mediante la división del valor del **Tamaño de la copia de seguridad** entre el valor de la velocidad de su conexión a Internet.

   Nota
   El valor de la velocidad de su conexión a Internet se reducirá si realiza varios procesos de conmutación por recuperación al mismo tiempo.

7. Haga clic en **Cambio** y en la ventana de confirmación vuelva a hacer clic en **Cambio**.
   Se apagará la máquina virtual en el sitio en la nube.

   Nota
   Si no se aplica ningún plan de copias de seguridad en la máquina virtual de la nube, se ejecutará automáticamente una copia de seguridad durante la fase de cambio, lo cual ralentizará el proceso.

8. Recupere el servidor desde una copia de seguridad en la nube al equipo físico o a la máquina virtual en su sitio local. Para obtener más información, consulte "Recuperar un equipo" en la guía del usuario de Cyber Protection.
9. Asegúrese de que la recuperación se complete y de que la máquina recuperada funcione correctamente y haga clic en **Se ha restaurado el equipo**.
10. Si todo funciona según lo esperado, haga clic en **Confirmar la conmutación por recuperación** y en la ventana de confirmación vuelva a hacer clic en **Confirmar**.

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

    Nota
    Aplicar un plan de protección en el servidor recuperado no forma parte del proceso de conmutación por recuperación. Una vez que finalice este proceso, aplique un plan de protección en el servidor recuperado para asegurarse de que vuelve a estar protegido. Puede aplicar el mismo plan de protección que se aplicó al servidor original o un nuevo plan que tenga habilitado el módulo **Recuperación ante desastres**.

Conmutación tras recuperación desde Cyber Protect Cloud a una máquina virtual de Azure

Puede realizar una conmutación tras recuperación desde Cyber Protect Cloud al equipo virtual de Azure original siguiendo el procedimiento para "Realización de una conmutación tras recuperación manual" (p. 95) y utilizando una de las siguientes opciones de recuperación en el paso 8.

Opciones de recuperación

- Recuperación sin agente

  Soporta la recuperación solo a una nueva máquina virtual de Microsoft Azure que se crea automáticamente.

  Configure la conexión de Azure en la consola de Cyber Protect (**Dispositivos** > **Agregar** > **Máquina virtual de Microsoft Azure**).

  Se despliega una máquina virtual de dispositivo de copia de seguridad en la suscripción de Azure para gestionar la recuperación.

  Flujo de recuperación:

  1. En la pantalla de **Almacenamiento de la copia de seguridad**, seleccione una copia de seguridad.
  2. Recupere como una máquina virtual de Azure.

  Puede utilizar el mismo flujo para copias de seguridad físicas, virtuales o basadas en agente.

  Para reducir los costes incurridos, la máquina virtual del dispositivo, cuando se utiliza solo para la recuperación, se puede encender solo durante la recuperación y luego se puede apagar manualmente.
- Recuperación basada en agente

Admite la recuperación en la misma máquina virtual de Azure (si la máquina virtual original con el agente está disponible) o en una nueva máquina virtual de Azure que tenga un nuevo agente instalado.

El proceso consiste en los siguientes pasos:

1. Cree manualmente una máquina virtual limpia de Windows o Linux en Azure.
2. Instale el agente de protección.
3. Utilice el agente para examinar y recuperar copias de seguridad de Acronis Cloud Storage.

Para obtener más información, consulte Recuperación de máquinas de Microsoft Azure y Amazon EC2.

Organización (runbooks)

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

Un runbook es un conjunto de instrucciones que describe cómo iniciar el entorno de producción en la nube. Puede crear runbooks en la consola de Cyber Protect.

Con los runbooks, puede:

- Automatizar la conmutación por error de uno o varios servidores.
- Hacer ping en la dirección IP del servidor y comprobar la conexión al puerto que especifique para poder comprobar automáticamente el resultado de la conmutación por error.
- Establecer la secuencia de operaciones de los servidores mediante la ejecución de aplicaciones distribuidas.
- Incluir operaciones manuales en el flujo de trabajo.
- Verifique la integridad de su solución de recuperación ante desastres mediante la ejecución de runbooks en modo de prueba.

Para acceder a la pantalla **Runbooks**, seleccione **Disaster Recovery** > **Runbooks**.

Creación de un runbook

Un runbook consiste en pasos que se ejecutan consecutivamente. Un paso consiste en acciones que comienzan simultáneamente.

Para crear un runbook, siga las instrucciones del siguiente procedimiento o del tutorial en vídeo.

Para crear un runbook

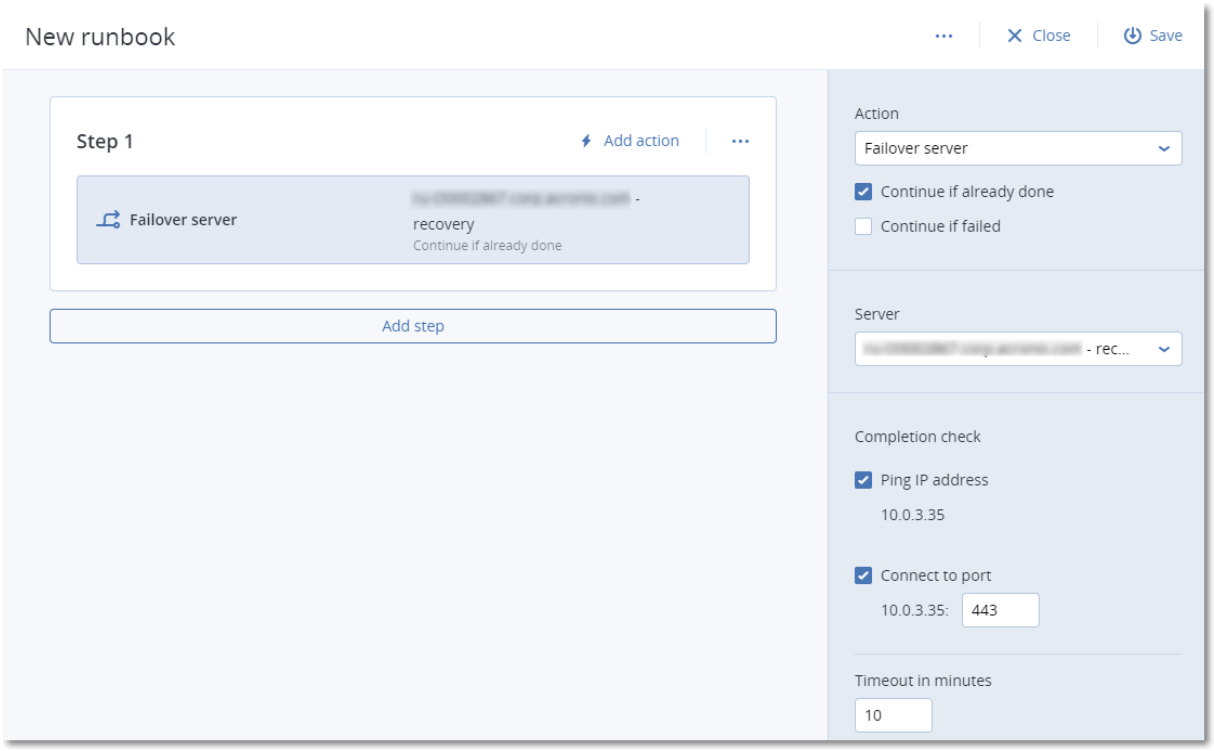
1. En la consola de Cyber Protection, vaya a **Disaster Recovery** > **Runbooks**.
2. Haga clic en **Crear runbook**.

3. Haga clic en **Añadir paso**.
4. Haga clic en **Añadir acción** y seleccione la acción que quiere añadir al paso.

Acción	Descripción
Conmutar por error el servidor	Realiza una conmutación por error de un servidor de la nube. Para definir esta acción, debe seleccionar un servidor de la nube y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estos parámetros, consulte "Parámetros de runbook" (p. 100). **Nota** Si la copia de seguridad del servidor que selecciona está cifrada utilizando el cifrado como una propiedad del equipo, la acción de **Conmutar por error el servidor** se detendrá y cambiará automáticamente a **Se requiere interacción**. Para continuar con la ejecución del runbook, tendrá que proporcionar la contraseña de la copia de seguridad cifrada.
Conmutar por recuperación el servidor	Realiza una conmutación tras recuperación de un servidor de la nube. Para definir esta acción, debe seleccionar un servidor de la nube y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estas configuraciones, consulte "Parámetros de runbook" (p. 100). **Nota** Las operaciones de runbook solo admiten la conmutación tras recuperación en el modo manual. Esto significa que, si inicia el proceso de conmutación tras recuperación mediante la ejecución de un runbook que incluya un paso **Conmutar por recuperación el servidor**, el procedimiento requerirá una interacción manual: deberá recuperar el equipo de forma manual y confirmar o cancelar el proceso de conmutación tras recuperación desde la pestaña **Disaster Recovery** > **Servidores**.
Iniciar servidor	Inicia un servidor de la nube. Para definir esta acción, debe seleccionar un servidor de la nube y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estas configuraciones, consulte "Parámetros de runbook" (p. 100). **Nota** La acción de **Iniciar servidor** no es aplicable para operaciones de conmutación por error de prueba en runbooks. Si intenta ejecutar dicha acción, fallará con el mensaje de error siguiente: Error: La acción no se aplica al estado actual del servidor.
Detener servidor	Detiene un servidor de la nube. Para definir esta acción, debe seleccionar un servidor de la nube y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estas configuraciones, consulte "Parámetros de runbook" (p. 100).

Acción	Descripción
	Nota La acción **Detener servidor** no es aplicable para operaciones de conmutación por error de prueba en runbooks. Si intenta ejecutar dicha acción, fallará con el mensaje de error siguiente: Error: La acción no se aplica al estado actual del servidor.
Operación manual	Una operación manual requiere una interacción de un usuario. Para definir esta acción, debe ingresar una descripción. Cuando una secuencia de runbook llega a una operación manual, el runbook se detendrá y no procederá hasta que un usuario realice la operación manual requerida, como hacer clic en el botón de confirmación.
Ejecutar runbook	Ejecuta otro runbook. Para definir esta acción, debe elegir un runbook. Un runbook puede estar formado únicamente por una ejecución de un runbook determinado. Por ejemplo, si añade la acción "ejecutar Runbook A", puede incluir la acción "ejecutar Runbook B", pero no puede añadir otra acción "ejecutar Runbook A".

5. Defina los parámetros del runbook para la acción. Para obtener más información sobre estos parámetros, consulte "Parámetros de runbook" (p. 100).
6. [Opcional] Para añadir una descripción del paso:
   a. Haga clic en el icono de puntos suspensivos y, luego, en **Descripción**.
   b. Introduzca una descripción del paso.
   c. Haga clic en **Listo**.
7. Repita los pasos del 3 al 6 hasta que cree la secuencia de pasos y acciones deseada.
8. [Opcional] Para cambiar el nombre predeterminado del runbook:
   a. Haga clic en el icono de puntos suspensivos.
   b. Introduzca el nombre del runbook.
   c. Introduzca una descripción del runbook.
   d. Haga clic en **Listo**.
9. Haga clic en **Guardar**.
10. Haga clic en **Cerrar**.



Parámetros de runbook

Los parámetros de runbook son configuraciones específicas que debe configurar para definir una acción del runbook. Hay dos categorías de parámetros de runbook: parámetros de acción y parámetros de comprobación de si los archivos están completos.

Los parámetros de acción definen el comportamiento del runbook dependiendo del estado inicial de la acción o el resultado.

Los parámetros de comprobación de si los archivos están completos aseguran que el servidor esté disponible y ofrezca los servicios necesarios. Si una comprobación de si los archivos están completos falla, se considera que la acción ha fallado.

En la tabla a continuación se describen los parámetros configurables del runbook para cada acción.

Parámetro de runbook	Categoría	Disponible para actuar	Descripción
Continuar si ya se ha realizado	Parámetro de acción	• **Conmutar por error el servidor** • **Iniciar servidor** • **Detener servidor** • **Conmutar por recuperación el servidor**	Este parámetro define el comportamiento del runbook cuando la acción requerida ya se ha realizado (por ejemplo, ya se ha realizado una conmutación por error o un servidor ya está en funcionamiento). Cuando está habilitado, el runbook emite un aviso y continúa. Cuando está deshabilitado, la acción falla y luego el runbook también falla.

Parámetro de runbook	Categoría	Disponible para actuar	Descripción
			Por defecto, este parámetro está habilitado.
Continuar si falla	Parámetro de acción	• **Conmutar por error el servidor** • **Iniciar servidor** • **Detener servidor** • **Conmutar por recuperación el servidor**	Este parámetro define el comportamiento del runbook cuando la acción requerida falla. Cuando está habilitado, el runbook emite un aviso y continúa. Cuando está deshabilitado, la acción falla y luego el runbook también falla. Por defecto, este parámetro está desactivado.
Hacer ping a la dirección IP	Verificación de finalización	• **Iniciar servidor**	El software hará ping a la dirección IP de producción del servidor en el cloud hasta que este responda o expire el tiempo de espera, lo que ocurra primero.
Conectar a puerto (443 de forma predeterminada)	Verificación de finalización	• **Conmutar por error el servidor** • **Iniciar servidor**	El software usará la dirección IP de producción del servidor en el cloud y el puerto que usted especifique para intentar conectarse a él hasta que se establezca la conexión o expire el tiempo de espera, lo que ocurra primero. De esta forma, puede comprobar si la aplicación que se detecta en el puerto especificado se encuentra en funcionamiento.
Tiempo de espera en minutos	Verificación de finalización	• **Conmutar por error el servidor** • **Iniciar servidor**	El tiempo de espera predeterminado es de 10 minutos.

Operaciones con runbooks

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Para acceder a la lista de operaciones, mueva el ratón sobre un runbook y haga clic en el icono de puntos suspensivos. Cuando un runbook no funciona, puede llevar a cabo las siguientes operaciones:

- **Ejecutar**
- **Editar**
- **Clonar**
- **Eliminar**

Ejecución de un runbook

Cada vez que haya clic en **Ejecutar**, se le pedirá que establezca los parámetros de la ejecución. Estos parámetros se aplicarán a todas las operaciones de conmutación por error y por recuperación incluidas en el runbook. Los runbooks especificados en las operaciones **Ejecutar runbook** heredan estos parámetros del runbook principal.

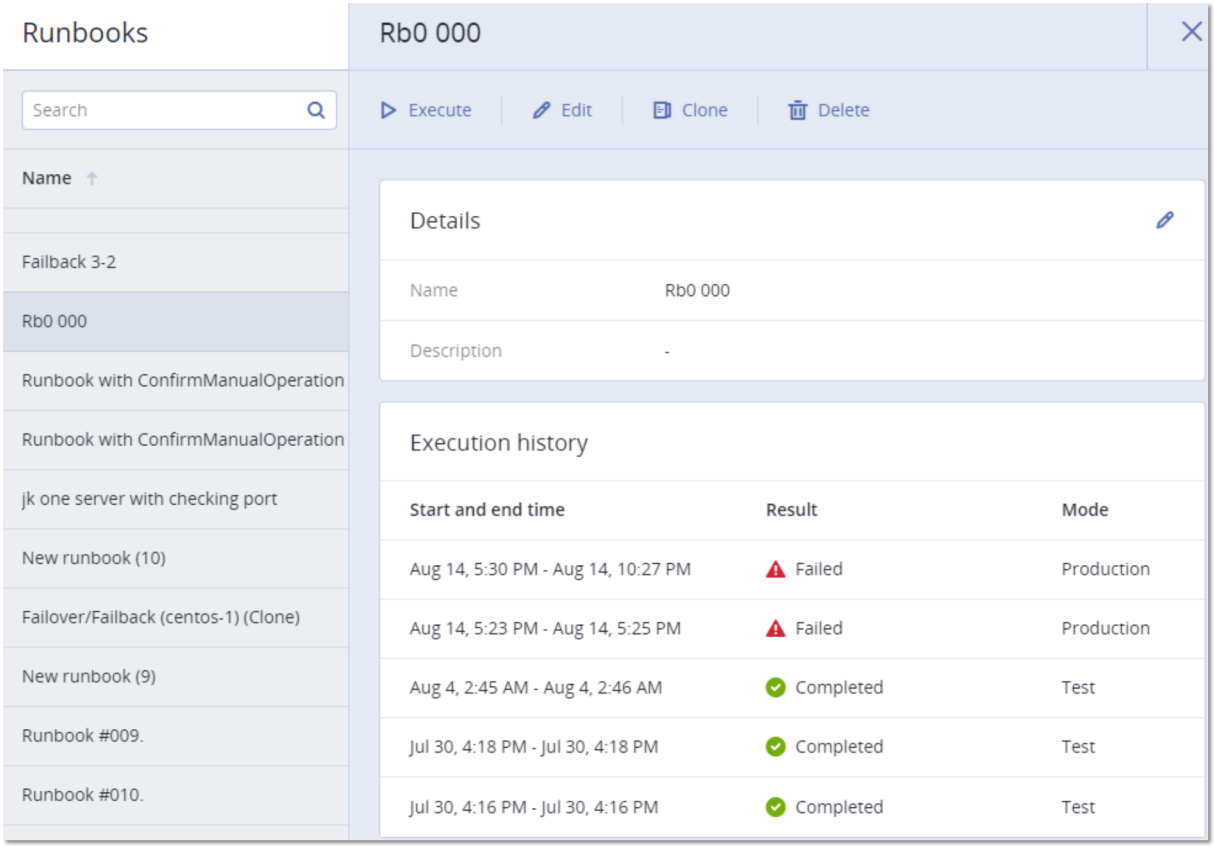
- **Modo conmutación por error y conmutación por recuperación**
  Elija si quiere ejecutar una conmutación por error de prueba (opción predeterminada) o una real (producción). El modo de conmutación por recuperación se corresponderá con el modo de conmutación por error elegido.
- **Punto de recuperación de conmutación por error**
  Elija el punto de recuperación más reciente (opción predeterminada) o seleccione un momento específico del pasado. Si elige la segunda opción, se seleccionarán los puntos de recuperación más cercanos a la fecha y la hora especificadas para cada servidor.

Detención de la ejecución de un runbook

Durante la ejecución de un runbook, puede seleccionar la opción **Detener** en la lista de operaciones. El software completará todas las acciones que ya se hayan iniciado excepto aquellas que requieran interacción del usuario.

Visualización del historial de ejecuciones

Al seleccionar un runbook de la pestaña **Runbooks**, el software muestra información sobre él y el historial de ejecuciones. Haga clic en la línea que corresponda a una ejecución específica para ver el registro de ejecuciones.



Eliminar el sitio de recuperación ante desastres

Puede eliminar el sitio de recuperación ante desastres. Esta acción eliminará automáticamente la puerta de enlace de VPN, las conexiones de VPN y todos los runbooks que se configuraron en el sitio.

Requisitos previos

No hay servidores en la nube disponibles en el sitio de recuperación de desastres.

Pasos para eliminar el sitio de recuperación ante desastres

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Haga clic en **Eliminar el sitio de recuperación ante desastres**.
4. En la ventana de confirmación, haga clic en **Eliminar**.

Disaster Recovery para Microsoft Azure

Disaster Recovery para Microsoft Azure es una solución de recuperación ante desastres asequible e integrada con el servicio Acronis Cyber Protection. Aprovecha la potencia y flexibilidad de la plataforma de nivel empresarial de Microsoft Azure como destino del sitio de DR. Esta solución utiliza copias de seguridad en frío (puntos de recuperación), que se pueden almacenar en Microsoft Azure, Acronis Cyber Protect Cloud o en un almacenamiento en la nube alojado por un partner. La configuración y orquestación del sitio de recuperación ante desastres se gestionan de forma centralizada desde la consola de Cyber Protect. Se utiliza su propia suscripción de Microsoft Azure como destino del sitio de DR.

La automatización y la orquestación incluyen las siguientes capacidades:

- Configuración inicial del sitio de DR
- Prueba de conmutación por error automatizada con verificación de captura de pantalla impulsada por IA
- Conmutación por error orquestada
- Conmutación tras recuperación automatizada a equipos físicos y máquinas virtuales, con un tiempo de inactividad casi nulo
- Runbooks para automatizar los escenarios clave de recuperación ante desastres
- Trabajadores bajo demanda (agentes temporales) que eliminan la necesidad de dispositivos virtuales permanentes
- DR en frío: las copias de seguridad se almacenan en el almacenamiento, pero no se ejecutan recursos de procesamiento (máquinas virtuales) hasta que se produce un desastre. DR en frío proporciona una recuperación rentable con un uso mínimo de la infraestructura de Azure.
- DR en caliente (disponible en futuras versiones): las copias de seguridad se replican de forma incremental en el almacenamiento intermedio de Azure y, en caso de desastre, están listas para ejecutarse como máquinas virtuales de Azure. El DR en caliente proporciona un RTO casi nulo.

Usted mantiene el control total sobre la infraestructura subyacente y las capacidades de Microsoft Azure, con la flexibilidad de utilizar los servicios nativos de Azure o integrar soluciones personalizadas, como firewalls de terceros y dispositivos SD-WAN, conectándolos a las redes de recuperación seleccionadas en el sitio de DR. Esta solución también admite la conmutación por error de escritorios de Windows que ejecutan Windows 10 o Windows 11.

Nota
Para utilizar Disaster Recovery en Microsoft Azure, debe tener una suscripción activa a Microsoft Azure.

Requisitos de software para Disaster Recovery en Microsoft Azure

Sistemas operativos compatibles

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

- Ubuntu 20.x, 21.x, 22.10, 23.04
- Debian 10.x, 11.x
- Red Hat Enterprise Linux 8.x, 9.x
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019: todas las opciones de instalación, excepto Nano Server
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server
- Windows Server 2025: todas las opciones de instalación, excepto Nano Server
- Windows 10
- Windows 11

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, 6.7, 7.0
- Windows Server 2008 R2 con Hyper-V
- Windows Server 2012/2012 R2 con Hyper-V
- Windows Server 2016 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Windows Server 2022 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Máquinas virtuales basadas en Kernel (KVM): solo invitados completamente virtualizados (HVM). No se admiten invitados paravirtualizados (PV).

Se admite las cargas de trabajo de Linux que tienen copias de seguridad sin agente desde un SO invitado y tienen volúmenes con las configuraciones de Logical Volume Manager (LVM).

Se admite las cargas de trabajo de Windows que tienen copias de seguridad sin agente desde un SO invitado y tienen configuraciones de discos dinámicos (LDM).

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

Limitaciones

Las siguientes plataformas y configuraciones no son compatibles con Disaster Recovery en Microsoft Azure:

1. Plataformas no compatibles:
   - Agentes para Virtuozzo.
   - macOS
2. Configuraciones no compatibles:

   Microsoft Windows
   - El servicio de Active Directory no es compatible con la replicación FRS.
   - Los dispositivos extraíbles sin formateo GPT o MBR (también llamado "superfloppy") no son compatibles.

   Linux
   - Sistemas de archivos sin tabla de partición.
   - Cargas de trabajo de Linux de las que se realiza una copia de seguridad con un agente de desde un SO invitado y que tienen volúmenes con las siguientes configuraciones avanzadas de Logical Volume Manager (LVM): Volúmenes segmentados, volúmenes replicados o volúmenes RAID 0, RAID 4, RAID 5, RAID 6 o RAID 10.

   Nota
   Las cargas de trabajo con varios sistemas operativos instalados no son compatibles.
3. Modos de inquilino no compatibles:
   - La recuperación ante desastres no está disponible cuando el modo de cumplimiento está habilitado para el inquilino.
4. Tipos de copias de seguridad no compatibles:
   - Los puntos de recuperación de Protección continua de datos (CDP) no son compatibles.

   Importante
   Si crea un servidor de recuperación a partir de una copia de seguridad que tenga un punto de recuperación CDP, perderá los datos incluidos en este punto de recuperación durante la conmutación por recuperación o al crear una copia de seguridad de un servidor de recuperación.

- Las copias de seguridad de datos forenses no se pueden usar para crear servidores de recuperación.

Los servidores en la cloud no se cifran.

Licencia de Disaster Recovery para Microsoft Azure

Para habilitar Disaster Recovery en Microsoft Azure, el elemento de oferta **DR y copia de seguridad directa en Azure** debe estar habilitado para su inquilino. Este elemento de oferta habilita:

- Disaster Recovery (DR) a Azure que utiliza la suscripción de Azure del cliente.
- Copia de seguridad directa en Azure que no requiere Advanced Backup.

Se consume una cuota del elemento de la oferta cuando se crea un servidor de recuperación o se habilita la copia de seguridad directa en Azure. Se utiliza solo una cuota por carga de trabajo, incluso si tanto DR como la copia de seguridad directa están activas.

La cuota para este elemento de oferta que se asigna a su inquilino representa el número máximo de cargas de trabajo que se pueden proteger. Un dispositivo que utiliza tanto Disaster Recovery a Azure como la protección de copia de seguridad directa en Azure consume una cuota.

Cuota estricta excedida

Cuando se reduce la cuota estricta del elemento de la oferta, los servidores de recuperación existentes pueden quedar sin licencia. El número de servidores de recuperación sin licencia depende del exceso. Los servidores de recuperación que estaban en conmutación por error de prueba o de producción siguen siendo funcionales, pero quedan sin licencia. Los servidores de recuperación sin licencia en modo de espera tienen operaciones de DR limitadas. No puede encender los servidores sin licencia hasta que vuelvan a tener una.

Aumentar la cuota del elemento de oferta asigna automáticamente licencias a dispositivos no licenciados y elimina las alertas relacionadas.

Alertas generadas

Se generan las siguientes alertas cuando hay problemas causados por la falta de licencias.

- **El servidor de recuperación no tiene licencia**: esta alerta se genera cuando un servidor queda sin licencia.
- **La protección de Disaster Recovery se desactivó para una carga de trabajo**: esta alerta se genera cuando no hay licencias disponibles.
- **La conmutación por error de prueba automatizada ha fallado**: esta alerta se genera cuando se bloquea una conmutación por error debido a que falta una licencia.

Trabajar con Disaster Recovery en Microsoft Azure

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

El flujo de trabajo básico para utilizar la recuperación ante desastres es el siguiente:

1. Configure su sitio de DR en Microsoft Azure. Para obtener más información, consulte "Creación de un sitio de recuperación ante desastres en Microsoft Azure" (p. 114).
2. Cree un servidor de recuperación de la carga de trabajo que desea proteger. Para obtener más información, consulte "Creación de servidores de recuperación en Microsoft Azure" (p. 123).
3. [Opcional] Configure la conectividad desde su sitio local al sitio en la nube en Microsoft Azure mediante los servicios nativos de Azure, como la VPN de sitio a sitio de Azure o Azure ExpressRoute. Para obtener más información, consulte "Conectividad y redes en Microsoft Azure" (p. 117).
4. [Opcional] Configure los runbooks. Para obtener más información, consulte "Creación de un runbook en Microsoft Azure" (p. 150).
5. Configure la conmutación por error de prueba automatizada o realice una conmutación por error de prueba. Para obtener más información, consulte "Configuración de la conmutación por error de prueba automatizada en Microsoft Azure" (p. 133) y "Realización de una prueba de conmutación por error en Microsoft Azure" (p. 131).
6. [Cuando se produce un desastre] Realice una conmutación por error de producción. Para obtener más información, consulte "Realización de una conmutación por error de producción en Microsoft Azure" (p. 129).
7. [Después del desastre] Realice una conmutación tras recuperación al sitio local. Para obtener más información consulte "Conmutación tras recuperación en Microsoft Azure" (p. 136).

Gestionar el acceso a su suscripción de Microsoft Azure

Disaster Recovery a Microsoft Azure requiere que se conecte a una suscripción de Microsoft Azure en la consola de Cyber Protect.

Puede configurar las suscripciones de Microsoft Azure en la pantalla **Infraestructura** > **Nubes públicas**. Allí también puede gestionar sus suscripciones, realizando las siguientes tareas: renovar el acceso a la suscripción, ver las propiedades y actividades de la suscripción o eliminar la suscripción.

La siguiente tabla proporciona los enlaces al procedimiento correspondiente para la tarea que desea realizar.

Tarea	Enlace
Añadir acceso a una suscripción de	"Añadir el acceso a una suscripción de Microsoft

Tarea	Enlace
Microsoft Azure	Azure" (p. 109)
Renovar el acceso a una suscripción de Microsoft Azure	"Renovar el acceso a una suscripción de Microsoft Azure" (p. 110)
Eliminar el acceso a una suscripción de Microsoft Azure	"Eliminar el acceso a una suscripción de Microsoft Azure" (p. 111)

Añadir el acceso a una suscripción de Microsoft Azure

Al añadir una suscripción de Microsoft Azure en la consola de Cyber Protect, Acronis puede acceder de forma segura a su suscripción y hacer copias de seguridad directamente de las cargas de trabajo correspondientes en Microsoft Azure.

Pasos para añadir el acceso a una suscripción de Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Infraestructura > Nubes públicas**.
2. Haga clic en **Agregar**, y de la lista de opciones mostrada, seleccione **Microsoft Azure**.
3. En el diálogo mostrado, haga clic en **Iniciar sesión**. Se le redirigirá a la página de inicio de sesión de Microsoft.

   Nota
   Debe tener asignado uno de los siguientes roles en Microsoft Azure AD para poder completar la conexión con la suscripción: Administrador de aplicaciones en la nube, administrador de aplicaciones o administrador general. También debe tener asignado el rol Propietario para cada suscripción seleccionada.

4. En la pantalla de inicio de sesión de Microsoft, introduzca las credenciales de inicio de sesión y acepte los permisos solicitados. Se iniciará el proceso de conexión y puede tardar varios minutos.

   Para obtener más información sobre el acceso seguro a su suscripción de Microsoft Azure, consulte el artículo Auditoría y seguridad de conexión de Microsoft Azure (72684).
5. Cuando la conexión se haya completado, realice lo siguiente:
   a. En el campo **Suscripción de Microsoft Azure**, seleccione la suscripción correspondiente de la lista.
   b. [Opcional] En el campo **Región de Azure**, seleccione la región en la que desplegar los recursos del sistema.

      Nota
      El sistema preselecciona la región en la que se encuentran la mayoría de los grupos de recursos, pero puede cambiarla según su preferencia.

6. Haga clic en **Agregar suscripción**.

   Se añadirá la suscripción a la lista de nubes públicas.

Para renovar el certificado de acceso anual de la suscripción, consulte "Renovar el acceso a una suscripción de Microsoft Azure" (p. 110).

Para eliminar el acceso a la suscripción, consulte "Eliminar el acceso a una suscripción de Microsoft Azure" (p. 111).

Nota

Si la cuenta de Microsoft Azure en la que ha iniciado sesión incluye acceso a varios Microsoft Azure AD, incluidos aquellos en los que es un usuario invitado, solo se seleccionará el directorio del usuario predeterminado. Si quiere usar un directorio en el que es un usuario invitado, deberá crear un nuevo usuario en ese Microsoft Azure AD específico. A continuación, puede iniciar sesión en esa cuenta y conectar la suscripción correspondiente.

Renovar el acceso a una suscripción de Microsoft Azure

Cuando un usuario se registra en la consola de Cyber Protect, Acronis le asigna automáticamente el acceso a una suscripción de Microsoft Azure durante un año con un certificado de acceso único y gratuito. Cuando se acerque la fecha de caducidad del certificado, puede renovarlo de forma rápida y fácil.

Pasos para renovar el certificado de acceso de la suscripción de Microsoft Azure

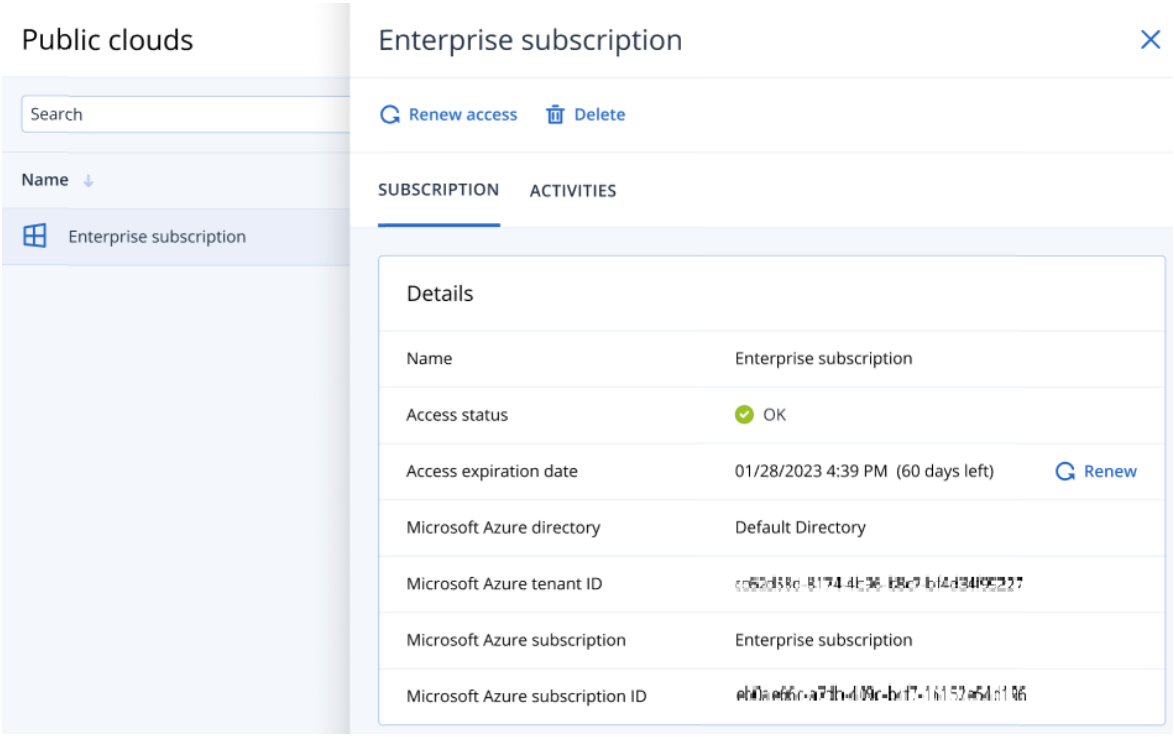
1. En la consola de Cyber Protect, vaya a **Infraestructura > Nubes públicas**.
2. Seleccione la suscripción correspondiente en la lista que se muestra.

   Nota

   La columna **Estado del acceso** indica el estado actual del certificado de acceso de cada suscripción y muestra uno de estos dos estados: **OK** o **Caducado**.

3. En el panel derecho, haga clic en **Renovar acceso**.

   Otra opción es hacer clic en la pestaña **Suscripción** y, a continuación, en **Renovar** en el campo **Fecha de caducidad del acceso**.



4. En la pantalla de inicio de sesión de Microsoft, introduzca las credenciales de inicio de sesión y acepte los permisos solicitados. Se iniciará el proceso de conexión y puede tardar varios minutos.
   Si la autenticación es correcta, el acceso se renovará automáticamente durante un año.
   Para obtener más información sobre los permisos necesarios, consulte el artículo Auditoría y seguridad de conexión de Microsoft Azure (72684).

Eliminar el acceso a una suscripción de Microsoft Azure

Es recomendable eliminar el acceso a la suscripción de Microsoft Azure si no se realizan copias de seguridad de cargas de trabajo en Microsoft Azure.

Pasos para eliminar el acceso a una suscripción de Microsoft Azure

Importante
No puede eliminar una suscripción si se está utilizando para hacer copias de seguridad en Microsoft Azure.

1. En la consola de Cyber Protect, vaya a **Infraestructura > Nubes públicas**.
2. Seleccione la suscripción correspondiente en la lista que se muestra.
3. En el panel derecho, haga clic en **Eliminar**.

Nota
Solo puede eliminar las suscripciones que haya añadido usted. También puede eliminar una suscripción si es un administrador de la empresa o de la unidad, o si tiene asignado el rol Administrador de cibernética o Administrador en el servicio de ciberprotección.

4. Haga clic en **Eliminar** en el mensaje de confirmación que se muestra.

Problemas de configuración entre suscripciones en Microsoft Azure

Si está utilizando dos suscripciones diferentes para Microsoft Azure: por ejemplo, una para la copia de seguridad directa en Microsoft Azure ("Suscripción 1") y otra para la configuración del sitio de DR en Microsoft Azure ("Suscripción 2"), pero elimina el acceso a "Suscripción 1", se producirán los siguientes problemas:

- La conmutación por error fallará
  No podrá iniciar una conmutación por error, ya que los datos de la copia de seguridad están almacenados en "Suscripción 1".
- La conmutación tras recuperación fallará
  Si se elimina el acceso a "Suscripción 1" después de realizar una conmutación por error, no será posible acceder a todos los datos de copia de seguridad que se almacenan en la suscripción. Por lo tanto, no será posible realizar operaciones de copia de seguridad de la máquina virtual en conmutación por error y conmutación tras recuperación. Mientras los datos de copia de seguridad permanezcan en "Suscripción 1", las operaciones de conmutación por error o recuperación dependen del acceso y los permisos válidos a la ubicación de almacenamiento original. La eliminación del acceso rompe esta dependencia, incluso si se inician operaciones de DR en una suscripción diferente.

Importante
No elimine ni revoque el acceso a la suscripción de Azure original si las copias de seguridad que se almacenan allí todavía se utilizan o se necesitan.

Creación de un plan de protección de recuperación ante desastres con Microsoft Azure

El plan de protección de recuperación ante desastres es un plan de protección en el que el módulo **Recuperación ante desastres** está habilitado.

Para Microsoft Azure, debe configurarse la ubicación del sitio de DR. No es posible aplicar un plan de protección con una ubicación de DR de Azure si no se ha configurado.

Nota

- La aplicación de un plan de protección de recuperación ante desastres crea servidores de recuperación en la nube. Las redes en la nube existentes no se modifican ni se vuelven a crear.
- Después de configurar la recuperación ante desastres podrá realizar una conmutación por error de prueba o de producción desde cualquier punto de recuperación (copias de seguridad) generado después de la creación del servidor de recuperación del dispositivo. No puede usar los puntos de recuperación que se generaron antes de que el dispositivo estuviese protegido con la recuperación ante desastres (antes de crear el servidor de recuperación).
- No se puede habilitar un plan de protección para la recuperación ante desastres si no se puede detectar la dirección IP de un dispositivo. Por ejemplo, cuando se realizan copias de seguridad sin agente de máquinas virtuales y no se les asigna una dirección IP. En este caso, recomendamos que cree un servidor de recuperación de forma manual.
- Cuando aplica un plan de protección, los servidores de recuperación se configuran en la subred que se configuró en las reglas de asignación durante la configuración de la ubicación del sitio de DR, en función de la dirección IP del dispositivo original. Si la dirección IP coincide con alguna de las redes locales de origen especificadas, el servidor de recuperación se creará en la red de recuperación de Azure y la subred correspondientes. El último octeto de la IP privada se tomará de la dirección IP del equipo original.

Para crear un plan de protección de recuperación ante desastres

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione los equipos que quiera proteger.
3. Haga clic en **Proteger** y, a continuación, en **Crear plan**.
   Se abre la configuración predeterminada del plan de protección.
4. Configure las opciones de copia de seguridad.
   Para usar la funcionalidad de recuperación ante desastres, el plan debe realizar copias de seguridad de todo el equipo o solo de los discos. Esto es necesario para arrancar y proporcionar los servicios necesarios a un almacenamiento en la nube o el almacenamiento de Microsoft Azure.
5. Active el interruptor que se encuentra junto al nombre del módulo para habilitar el módulo **Recuperación ante desastres**.
6. En el campo **Ubicación**, seleccione **Microsoft Azure**.
7. Haga clic en **Crear**.
   El plan se crea y se aplica a los equipos seleccionados. Se crean los servidores de recuperación con los parámetros predeterminados.

Gestión del sitio de recuperación ante desastres en Microsoft Azure

Puede crear y configurar su sitio de recuperación ante desastres (DR) en Microsoft Azure como parte de la creación del plan de protección de recuperación ante desastres o como un procedimiento separado, desde la pantalla **Disaster Recovery**.

Cuando se aplica un plan de protección de recuperación ante desastres, la infraestructura de red en la nube del servidor de recuperación se crea solo si no existe ya. Los servidores en la nube y las redes existentes no se cambian ni se vuelven a crear.

No se puede habilitar un plan de protección para la recuperación ante desastres si no se puede detectar la dirección IP de un dispositivo. Por ejemplo, cuando se realizan copias de seguridad sin agente de máquinas virtuales y no se les asigna una dirección IP. En este caso, recomendamos que cree un servidor de recuperación de forma manual.

Cuando aplica un plan de protección, los servidores de recuperación se configuran en la subred que hay configurada en las reglas de asignación durante la configuración de la ubicación del sitio de DR, y se basan en la dirección IP del dispositivo original. Si la dirección IP coincide con alguna de las redes locales de origen especificadas, el servidor de recuperación se creará en la red de recuperación de Azure y en la subred correspondientes. El último octeto de la IP privada se tomará de la dirección IP del equipo original.

Creación de un sitio de recuperación ante desastres en Microsoft Azure

Requisitos previos

- Tiene una suscripción a Microsoft Azure.
- Su cuenta de Microsoft tiene uno de los siguientes roles de Entra ID: Administrador de aplicaciones en la nube, Administrador de aplicaciones o Administrador global.
- Su cuenta de Microsoft tiene el rol de Propietario para la suscripción de Azure.
- El elemento de oferta de DR y copia de seguridad directa en Azure está habilitado para su inquilino.

Desde todos los dispositivos

Crear un sitio de DR en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione las cargas de trabajo que desea proteger.
3. En el menú **Acciones**, haga clic en **Proteger**.
4. Cree un plan de protección y configure los siguientes ajustes:

a. En el módulo **Copia de seguridad**, en el campo **Dónde guardar las copias de seguridad**, seleccione la ubicación de almacenamiento para las copias de seguridad de sus cargas de trabajo.
b. Active el módulo de **Recuperación ante desastres** y, a continuación, haga clic en el campo **Ubicación**.

Nota
Si solo está habilitado el elemento de oferta **DR y copia de seguridad directa en Azure** para su inquilino, la ubicación no se preseleccionará y verá un enlace para **Configurar**.
Si ambos elementos de oferta **DR en Acronis o en la nube híbrida** y **DR y copia de seguridad directa en Azure** están habilitados para su inquilino, Cyber Protect Cloud se preseleccionará como ubicación.

c. En el asistente de **Configuración del sitio de recuperación ante desastres**, en la pestaña **Ubicación del sitio**, seleccione **Microsoft Azure Cloud** y, a continuación, haga clic en **Siguiente**.
d. En la pestaña **Suscripción de Azure**, haga lo siguiente:
   - Si su suscripción de Microsoft Azure ya se había añadido a la consola de Cyber Protect, haga clic en ella y luego en **Siguiente**.
   - Si desea añadir una nueva suscripción de Microsoft Azure, haga clic en **Agregar suscripción**, añada la suscripción y luego pulse en ella y en **Siguiente**.
e. En la pestaña **Región de destino**, en el campo **Región de Azure**, seleccione la región de Azure para el sitio de DR.
f. En la pestaña **Red de recuperación**, configure las redes de recuperación para la conmutación por error de producción y prueba, y haga clic en **Siguiente**.

Opción	Descripción
Configuración predeterminada	Utilice esta opción si desea que las redes de producción y de prueba en Azure se creen automáticamente, con una red para cada entorno.
Configuración avanzada	Utilice esta opción si desea seleccionar sus redes de Azure existentes como redes de producción y prueba y configurar la asignación de redes.

g. En la pestaña **Resumen**, revise los parámetros de su sitio de DR y, a continuación, haga clic en **Configurar**.

El plan de protección se aplica correctamente a las cargas de trabajo seleccionadas. Se crea el sitio de DR en Azure, ubicado en la región de Azure seleccionada. En la pantalla **Disaster Recovery** > **Conectividad**, puede ver las redes de producción y prueba, así como los servidores de recuperación que se crearon, en **Modo de espera**.

Desde conectividad

Crear un sitio de DR en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery**.
2. Haga clic en **Configurar**.
3. En el asistente de **Configuración del sitio de recuperación ante desastres**, en la pestaña **Ubicación del sitio**, seleccione **Microsoft Azure Cloud** y, a continuación, haga clic en **Siguiente**.
4. En la pestaña **Suscripción de Azure**, haga lo siguiente:
   - Si su suscripción de Microsoft Azure ya se había añadido a la consola de Cyber Protect, haga clic en ella y luego en **Siguiente**.
   - Si desea añadir una nueva suscripción de Microsoft Azure, haga clic en **Agregar suscripción**, añada la suscripción y luego pulse en ella y en **Siguiente**.
5. En la pestaña **Región de destino**, en el campo **Región de Azure**, seleccione la región de Azure para el sitio de DR.
6. En la pestaña **Red de recuperación**, configure las redes de recuperación para la conmutación por error de producción y prueba, y haga clic en **Siguiente**.

Opción	Descripción
Configuración predeterminada	Utilice esta opción si desea que las redes de producción y de prueba en Azure se creen automáticamente, con una red para cada entorno.
Configuración avanzada	Utilice esta opción si desea seleccionar sus redes de Azure existentes como redes de producción y prueba y configurar la asignación de redes.

7. En la pestaña **Resumen**, revise los parámetros de su sitio de DR y, a continuación, haga clic en **Configurar**.
   El sitio de DR se crea en Azure, ubicado en la región de Azure seleccionada. En la pantalla **Disaster Recovery** > **Conectividad**, puede ver las redes de producción y prueba.

Eliminar el sitio de DR de Microsoft Azure

Puede eliminar el sitio de DR de Microsoft Azure si ya no lo necesita o si desea cambiar la ubicación del sitio de DR.

Requisitos previos

No hay servidores de recuperación en el sitio de DR.

Para eliminar el sitio de DR de Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Eliminar el sitio de recuperación ante desastres**.
3. En la ventana **Eliminar el sitio de recuperación ante desastres**, introduzca su credencial de inicio de sesión y haga clic en **Eliminar**.

Conectividad y redes en Microsoft Azure

Disaster Recovery en Microsoft Azure permite la orquestación de pruebas, conmutación por error y conmutación tras recuperación, así como la selección de redes de recuperación (subredes y redes virtuales de Azure) para los escenarios de conmutación por error de producción y de prueba. Puede configurar estas redes durante la configuración inicial del sitio de DR o más tarde: desde la pantalla de **Conectividad** o de forma individual para cada servidor de recuperación.

Mantiene el control total sobre la conexión a redes virtuales y la conectividad de Azure, y tiene la flexibilidad de aprovechar las capacidades nativas de la plataforma de Azure o de llevar soluciones personalizadas, como firewalls de terceros o dispositivos SD-WAN al sitio de DR, conectándolos a las redes de recuperación seleccionadas.

A continuación se presenta un resumen de los principales servicios de conexión a redes virtuales de Azure, su relevancia para los casos de uso de recuperación ante desastres y enlaces para obtener más información.

Azure Firewall

Azure Firewall proporciona un filtrado de tráfico de red centralizado y con estado en varias redes virtuales y subredes. Ayuda a hacer cumplir las reglas de seguridad entre cargas de trabajo después de una conmutación por error y admite escenarios en los que los entornos de DR deben cumplir con las políticas de cumplimiento o segmentación corporativas.

Puede utilizar Azure Firewall para controlar el tráfico saliente y entrante hacia y desde las máquinas virtuales con conmutación por error (por ejemplo, para limitar el acceso a Internet y permitir solo las fuentes de la lista de permitidos). Para la exposición administrada, coloque Azure Firewall entre la red in situ (a través de VPN) y las redes virtuales de DR de Azure.

Para obtener más información, consulte la Documentación de Microsoft Azure.

Grupos de seguridad de red (NSG)

Los NSG permiten definir reglas granulares para permitir o denegar el tráfico de red a las máquinas virtuales o subredes. Los NSG funcionan a nivel de la NIC de la máquina virtual y de la subred.

Puede aplicar los NSG para controlar el acceso a las máquinas virtuales de recuperación, garantizar el aislamiento de las conmutaciones por error de prueba o exponer solo los puertos necesarios (por ejemplo, RDP y HTTP). Los NSG son esenciales para habilitar de forma segura la conectividad en función de si la máquina virtual de recuperación está en modo de prueba o de producción.

Para obtener más información, consulte la Documentación de Microsoft Azure.

Servidores DNS

Las redes virtuales de Azure admiten configuraciones de servidor DNS personalizadas o integración con Azure DNS. Esto controla cómo funciona la resolución de nombres en el entorno de DR.

Asegúrese de que las máquinas virtuales de DR resuelvan los nombres correctamente, ya sea a otros servicios recuperados en Azure o a sistemas externos. El DNS personalizado es esencial al restaurar entornos integrados con AD o para el reenvío de DNS a sistemas locales.

Para obtener más información, consulte la Documentación de Microsoft Azure.

Enrutamiento de subredes (rutas definidas por el usuario)

Azure permite la creación de rutas personalizadas (UDR) para controlar el flujo de tráfico entre subredes y hacia redes in situ, anulando el enrutamiento predeterminado del sistema.

Cree rutas para dirigir el tráfico de las máquinas virtuales de recuperación a través de firewalls, a puertas de enlace de VPN o puntos de inspección. Esto ayuda a hacer cumplir las directivas de enrutamiento y garantizar la conectividad de vuelta a in situ a través de VPN o ExpressRoute.

Para obtener más información, consulte la Documentación de Microsoft Azure.

Direcciones IP públicas

Se pueden asignar direcciones IP públicas (estáticas o dinámicas) a las máquinas virtuales de Microsoft Azure para permitir el acceso directo a Internet cuando sea necesario. Esto es útil para exponer servicios o para el acceso remoto.

Asigne direcciones IP públicas a cargas de trabajo con conmutación por error que requieran acceso externo (por ejemplo, servidores web y administración remota). Evite hacerlo para cargas de trabajo sensibles. Utilice Bastion o un VPN en su lugar, si es posible.

Para obtener más información, consulte la Documentación de Microsoft Azure.

Azure Bastion

Azure Bastion permite el acceso seguro mediante RDP/SSH desde un navegador a las máquinas virtuales sin exponer las IP públicas. Funciona a través del portal de Azure y utiliza cifrado TLS.

Acceda a las máquinas virtuales recuperadas de forma segura para realizar diagnósticos o reconfiguraciones manuales tras la conmutación por error. Esto es especialmente útil en la conmutación por error de prueba, donde no se desea exponerlas a Internet.

Para obtener más información, consulte la Documentación de Microsoft Azure.

VPN de sitio a sitio de Azure

La VPN de sitio a sitio proporciona una conexión IPsec cifrada entre su red in situ y las redes virtuales de Azure, lo que permite la conectividad híbrida.

Garantiza el acceso fluido a las cargas de trabajo recuperadas desde las redes in situ. Resulta crítico para acceder a las apps internas o restaurar las dependencias cruzadas con los sistemas que aún se ejecutan in situ.

Para obtener más información, consulte la Documentación de Microsoft Azure.

Azure ExpressRoute

ExpressRoute ofrece conectividad privada dedicada entre su centro de datos y Azure, saltándose Internet para mejorar la velocidad, la fiabilidad y la seguridad.

Recomendado para DR de nivel empresarial con grandes conjuntos de datos o requisitos de baja latencia. Utilícelo para conectar sistemas in situ con máquinas virtuales de DR en Microsoft Azure sin depender de una VPN.

Para obtener más información, consulte la Documentación de Microsoft Azure.

Gestión de redes en Microsoft Azure

Las redes de recuperación son redes virtuales de Azure (VNet) y subredes donde se ejecutarán sus sistemas de copia de seguridad (servidores de recuperación) si sus sistemas principales fallan.

Hay dos tipos de redes de recuperación: redes de recuperación de producción y redes de recuperación de prueba.

Red de recuperación de producción

Las redes de recuperación de producción se utilizan durante un desastre real cuando necesita mover sus servicios a Azure. Las cargas de trabajo (VM) con conmutación por error están conectadas a estas redes de recuperación para que se reanuden las operaciones de la empresa.

Este es un ejemplo de una red de producción:

VNet: `dr-prod-vnet-91a4e5bf`

Subred: `subnet-one (10.0.10.0/24)`

Red de recuperación de prueba

Las redes de recuperación de prueba se utilizan durante las conmutaciones por error de prueba manuales o automatizadas para verificar que la recuperación ante desastres funciona sin afectar a sus sistemas de producción.

Para evitar conflictos de IP o filtraciones de datos, las redes de recuperación de prueba deben estar aisladas del entorno de producción. Para evitar la superposición con las redes de producción, la mejor práctica es utilizar una red virtual dedicada.

Para obtener más información sobre la planificación y el diseño de redes virtuales, consulte la documentación de Microsoft Azure.

Mejores prácticas para la configuración de red de Disaster Recovery

Cuando configure las redes de recuperación en Disaster Recovery a Microsoft Azure, le recomendamos que siga las siguientes mejores prácticas:

- Separe las redes virtuales y subredes de producción y de prueba

  Mantenga los entornos de prueba y producción aislados.
- Utilice etiquetas y convenciones de nomenclatura de Azure

  Etiquete claramente las redes (por ejemplo, `dr-prod` y `dr-test`) para facilitar la identificación y la automatización.
- Planifique cuidadosamente los rangos de IP

  Asegúrese de que las redes virtuales y las subredes no entren en conflicto con las redes in situ si hay conectividad entre el sitio de DR y el sitio in situ, por ejemplo, a través de una VPN IPsec o ExpressRoute.

  Mantenga esquemas de dirección coherentes para facilitar el enrutamiento y la integración de identidades.
- Preconfigure los recursos de red necesarios

  Las NSG, las tablas de rutas, el DNS personalizado y las IP públicas deben configurarse de antemano para las redes de recuperación de prueba y producción.

Recomendaciones para la disponibilidad de servicios de dominio de Active Directory

Si tiene que autenticar sus cargas de trabajo protegidas en un controlador de dominio, le recomendamos que disponga de una instancia de Controlador de dominio de Active Directory (AD DC) en el sitio de DR de Microsoft Azure.

Recomendaciones para la disponibilidad de AD DS en el sitio de DR en Azure

Las recomendaciones para una instancia AD DC dedicada en el sitio de DR son las siguientes:

- Apague el firewall de Windows.
- Una el AD DC al servicio de Active Directory.
- Asegúrese de que la máquina virtual de Microsoft Azure tenga acceso a Internet.
- Añada la función de Active Directory.
- Despliegue al menos un controlador de dominio en el sitio de DR de Azure

  Las cargas de trabajo recuperadas necesitan autenticarse, aplicar directivas de grupo y resolver nombres. Despliegue una máquina virtual de controlador de dominio adicional en Azure por adelantado, antes de la conmutación por error.
- Utilice un controlador de dominio replicado (que no sea de solo lectura)

  Los controladores de dominio de solo lectura (RODC) pueden no ser compatibles con todos los escenarios de autenticación después de una conmutación por error. Despliegue un controlador de dominio escribible y replíquelo con su bosque de AD in situ.
- Asegúrese de que la configuración de DNS sea correcta

  Las máquinas virtuales recuperadas deben resolver nombres de dominio y localizar controladores de dominio. Configure la red virtual de recuperación para usar la dirección IP del

controlador o de los controladores de dominio basado(s) en Azure como el servidor DNS personalizado.

- Replique SYSVOL y garantice la sincronización de tiempo

  Las directivas de grupo y las operaciones de dominio dependen de la replicación de SYSVOL y de la hora correcta. Asegúrese de que SYSVOL esté sincronizado y configure NTP o los ajustes de sincronización de hora para garantizar la coherencia entre Azure y los entornos in situ.

Agregar una red de recuperación de producción desde Microsoft Azure

Después de configurar el sitio de DR, puede agregar redes de recuperación de producción adicionales a partir de las que existen en Microsoft Azure.

Agregar una red de recuperación de producción desde Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. En el panel **Redes de producción**, haga clic en **Agregar red**.
3. En la ventana **Añadir red de producción**, en el campo **Red virtual**, seleccione una red virtual.
4. En el campo **Subred**, seleccione la subred.
5. [Opcional] Para establecer esta subred como predeterminada, seleccione **Establecer esta subred como "Predeterminada" para la asignación**.

   Al aplicar el plan de protección de recuperación ante desastres a los dispositivos originales, los servidores de recuperación se configuran en la subred predeterminada.
6. En el campo **Asignación a la red local**, haga clic en **Agregar**.

   Puede definir reglas de asignación introduciendo una o más redes locales de origen en formato CIDR. El servicio comparará la dirección IP del dispositivo original con las reglas de asignación. Si la dirección IP coincide con alguna de las redes locales de origen especificadas, el servidor de recuperación se creará en la red y la subred de recuperación de Azure correspondientes.
7. Introduzca una o más redes locales de origen en el formato CIDR.
8. Para añadir la red, haga clic en **Listo**.

Agregar una red de recuperación de prueba desde Microsoft Azure

Después de configurar el sitio de DR, puede añadir redes de recuperación de prueba adicionales a las que existen en Microsoft Azure.

Para agregar una red de recuperación de prueba desde Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. En el panel **Redes de prueba**, haga clic en **Agregar red**.
3. En la ventana **Añadir red de prueba**, en el campo **Red virtual**, seleccione una red virtual.
4. En el campo **Subred**, seleccione la subred.

5. [Opcional] Para establecer esta subred como predeterminada, seleccione **Establecer esta subred como "Predeterminada" para la asignación**.
   Al aplicar el plan de protección de recuperación ante desastres a los dispositivos originales, los servidores de recuperación se configuran en la subred predeterminada.
6. En el campo **Asignación a la red local**, haga clic en **Agregar**.
   Puede definir reglas de asignación introduciendo una o más redes locales de origen en formato CIDR. El servicio comparará la dirección IP del dispositivo original con las reglas de asignación. Si la dirección IP coincide con alguna de las redes locales de origen especificadas, el servidor de recuperación se creará en la red y la subred de recuperación de Azure correspondientes.
7. Introduzca una o más redes locales de origen en el formato CIDR.
8. Para añadir la red, haga clic en **Listo**.

Edición de redes de recuperación desde Microsoft Azure

Puede cambiar las redes de recuperación de prueba o de producción desde Microsoft Azure.

Para editar la configuración de una red de recuperación en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. En el panel de **Redes de producción** o **Red de prueba**, haga clic en la red que desea cambiar y luego en **Editar**.
3. Seleccione otra red entre las que están disponibles en Microsoft Azure.
4. Haga clic en **Listo**.

Servidores de recuperación en Microsoft Azure

Un servidor de recuperación es una réplica del equipo original que se crea a partir de la copia de seguridad (punto de recuperación) del servidor protegido que se almacena en la nube (Cyber Protect Cloud o Microsoft Azure). En caso de desastre, la carga de trabajo se cambia del servidor original al servidor de recuperación en Microsoft Azure.

Los servidores de recuperación se crean manualmente o automáticamente, cuando aplica un plan de protección de recuperación ante desastres a una carga de trabajo.

No se cobran puntos de cálculo por ejecutar sus servidores de recuperación en Microsoft Azure. Todos el uso de cálculo se factura directamente a su suscripción de Microsoft Azure.

La configuración de la dirección MAC para los servidores de recuperación no está disponible en Disaster Recovery para Microsoft Azure.

Administración de servidores de recuperación

Las siguientes operaciones con servidores de recuperación están disponibles en Disaster Recovery para Microsoft Azure:

Operación	Descripción
Encender	(Para servidores en el estado de conmutación por error) Encender la máquina virtual de Microsoft Azure (servidor de recuperación).
Apagar	[Para servidores en el estado de conmutación por error] Apagar la máquina virtual de Microsoft Azure (servidor de recuperación). La operación de apagado detiene la máquina virtual de Microsoft Azure, pero no desasigna recursos. La máquina virtual estará en el estado Detenida (Asignada). En este estado, una máquina virtual de Microsoft Azure sigue reservando CPU y memoria, incurriendo en cargos de cálculo como si estuviera en ejecución. Este estado preserva la dirección IP y la ubicación del servidor de la máquina virtual.
Apagado forzoso	[Para servidores en el estado de conmutación por error] Apagar forzosamente el servidor de recuperación.
Editar configuración	Modificar los ajustes del servidor de recuperación, como la configuración de la red o los umbrales de RPO desde la consola de Cyber Protect.
Conmutación por error de producción	Cambiar las cargas de trabajo al servidor de recuperación en la red de producción.
Conmutación por error de prueba	Probar el servidor de recuperación en la red de prueba aislada sin afectar la producción. Para evitar conflictos durante la conmutación por error, asegúrese de que redes de producción y de prueba estén configuradas correctamente. Pruebe regularmente las operaciones de conmutación por error para validar la funcionalidad del servidor de recuperación.
Conectar (a la consola)	[Para servidores en estado de conmutación por error] Después de hacer clic en **Conectar** y ser redirigido a Azure, puede conectarse a la máquina virtual de Azure utilizando las opciones nativas de Azure, como: • Asignar una dirección IP pública y conectarse mediante el protocolo de escritorio remoto (RDP) o SSH. • Usar Azure Bastion, un servicio seguro para conectarse a la máquina virtual sin una IP pública.

Creación de servidores de recuperación en Microsoft Azure

Los servidores de recuperación se crean automáticamente cuando aplica un plan de protección de recuperación ante desastres a una carga de trabajo. Si no se aplica un plan de protección de recuperación ante desastres a la carga de trabajo, puede crear un servidor de recuperación manualmente.

Requisitos previos

- Hay un plan de supervisión aplicado a la carga de trabajo.
- El sitio de DR en Microsoft Azure está configurado.

Para crear un servidor de recuperación en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo que desea proteger con Disaster Recovery y, a continuación, en el menú **Acciones**, pulse en **Recuperación ante desastres**.
3. Haga clic en **Crear servidor de recuperación**.
4. En el asistente **Crear servidor de recuperación**, en la pestaña **Configuración del servidor**, ajuste la configuración y pulse en **Siguiente**.

Configuración	Descripción
CPU y RAM	Tamaño de la máquina virtual de Microsoft Azure. El uso de recursos de cálculo se cobra directamente en su suscripción de Microsoft Azure por parte de Microsoft o su partner. Si algunos tamaños de máquina virtual de Microsoft Azure no están disponibles, consulte las limitaciones de su suscripción de Azure. Los siguientes tipos de máquina virtual de Microsoft Azure están excluidos de la selección: • Serie A (obsoleta en Microsoft Azure) • Tipos de máquina virtual que se basan en la arquitectura ARM CPU La configuración predeterminada se determina automáticamente en función de la configuración de CPU y RAM del dispositivo original. La RAM se ajusta redondeando al tamaño de máquina virtual de la familia B más cercano que cumpla o supere el valor de RAM original y seleccionando el número de núcleos de CPU más bajo disponible que satisfaga el requisito de RAM. Si no hay datos de RAM del equipo original (por ejemplo, para máquinas virtuales de Microsoft Azure que utilizan copias de seguridad sin agente), se selecciona un tamaño mínimo de máquina virtual de la familia B de forma predeterminada. Si la serie o el tamaño de máquina virtual seleccionados no están disponibles en la región o suscripción de destino, el sistema selecciona automáticamente el tamaño más cercano disponible de cualquier serie de la familia B dentro de esa región.
Tipo de disco	Tipo de disco de la máquina virtual de Microsoft Azure. El tipo de disco que seleccione se aplicará a todos los discos del servidor de recuperación. Solo están disponibles para su selección los tipos de disco de almacenamiento redundante local (LRS). No se puede seleccionar Premium SSD v2 ni Ultra SSD. Premium SSD v2 se asigna automáticamente durante una conmutación por error si se detectan discos de sector de 4K en la copia de seguridad de la carga de trabajo original.

Configuración	Descripción
Nombre	Nombre del servidor de recuperación que es visible en la consola de Cyber Protect. Este nombre no se utiliza para la máquina virtual de Microsoft Azure.
Descripción	Descripción del servidor de recuperación

5. En la pestaña **Red**, configure la red de producción y de prueba y, a continuación, haga clic en **Siguiente**.

Configuración	Descripción
Red	(Para red de producción) La red virtual de Azure (VNet) y la subred para la conmutación por error de producción. Durante una conmutación por error de producción, el servidor se conectará a esta red de Azure.
Dirección IP en la red de producción	(Para red de producción) De forma predeterminada, se deriva el último octeto de la dirección IP del equipo original en el rango de la red de producción, pero puede cambiar la dirección IP en cualquier momento antes de la conmutación por error. Cuando el servidor está en el estado de conmutación por error, puede modificar la dirección IP directamente en Azure.
Red	(Para red de prueba) La red virtual y la subred de Azure para la conmutación por error de prueba. Recomendamos que la red de prueba esté aislada dentro de una red virtual separada. Durante una conmutación por error de prueba, el servidor se conectará a esta red de Azure.
Dirección IP en la red de prueba	(Para red de prueba) De forma predeterminada, se deriva el último octeto del equipo original, en el rango de la red prueba, pero puede cambiar la dirección IP en cualquier momento antes de la conmutación por error. Cuando el servidor se encuentra en el estado de conmutación por error de prueba, puede modificar la dirección IP directamente en Azure.

Nota

- Por motivos de seguridad, no se asigna ninguna IP pública al servidor de recuperación por defecto. Sin una IP pública, el servidor de recuperación solo es accesible desde la red local. Si es necesario, asigne una IP pública directamente en el portal de Azure.
- Por defecto, el acceso a Internet está habilitado para los recursos en Azure. No se requiere ninguna configuración adicional para permitir el tráfico de salida a Internet. Si necesita restringir o aislar el acceso a Internet saliente en una red de prueba, debe configurar los controles de seguridad apropiados, como las reglas de grupo de seguridad de red (NSG), las rutas definidas por el usuario (UDR) o las directivas de Azure Firewall, según sus requisitos.

6. En la pestaña **Conmutación por error de prueba automatizada**, realice lo siguiente:
   a. [Opcional] Active el interruptor **Conmutación por error de prueba automatizada**.
   b. [Opcional] Configure de los ajustes.

Configuración	Descripción
Planificación	La conmutación por error de prueba automatizada se ejecuta una vez al mes.
Tiempo de espera de inicio de la MV / Minutos	El período máximo durante el cual el sistema intenta iniciar un equipo virtual en Azure y tomar una captura de pantalla para verificar si el sistema operativo se ha cargado correctamente. Este período de tiempo de espera no incluye el tiempo que se tarda en restaurar los datos de un archivo de copia de seguridad en frío, ya que esta duración depende del tamaño del archivo. Además, las horas de cálculo de las máquinas virtuales de Microsoft Azure no se cuentan durante el tiempo de restauración de datos.
Usar como tiempo de espera predeterminado	Seleccione esta casilla si desea guardar el valor de **Tiempo de espera de inicio de la MM / Minutos** como predeterminado. En este caso, el valor se rellenará automáticamente cuando active la conmutación por error de prueba automatizada para otros servidores de recuperación.

   c. Haga clic en **Siguiente**.
7. En la pestaña **Configuración**, haga lo siguiente:
   a. [Opcional] El umbral de RPO determina el intervalo temporal máximo permitido entre el último punto de recuperación y el momento presente. Puede establecer un valor de entre 15 y 60 minutos, 1 y 24 horas y 1 y 14 días.
   b. [Opcional] [Si las copias de seguridad del equipo seleccionado están cifradas utilizando el cifrado como una propiedad del equipo], especifique la contraseña que se utilizará automáticamente al crear una máquina virtual para el servidor de recuperación a partir de la copia de seguridad cifrada.
      a. Haga clic en **Introducir contraseña**, introduzca la contraseña de la copia de seguridad cifrada y defina un nombre para las credenciales.

De forma predeterminada, verá la copia de seguridad más reciente en la lista.

b. Para ver todas las copias de seguridad, seleccione **Mostrar todas las copias de seguridad**.

c. Haga clic en **Guardar**.

Nota
Tenga en cuenta que, aunque la contraseña que especifique se guardará en un almacén de credenciales seguro, es posible que incumpla sus obligaciones legales si la guarda.

8. Haga clic en **Crear**.

El servidor de recuperación se crea y está en estado de espera. No se cargan puntos de cálculo. Todo el uso de cálculo se factura directamente a su suscripción de Azure.

Nota
Puede configurar reglas de firewall para la máquina virtual solo en el portal de Azure. De forma predeterminada, para las máquinas virtuales en conmutación por error de prueba y producción, se prohíben todas las conexiones entrantes y se permiten todas las conexiones salientes a Internet dentro de la red virtual de producción y prueba.

Edición de la configuración del servidor de recuperación

Cuando cree y aplique un plan de protección de recuperación ante desastres, se creará un servidor de recuperación con la configuración predeterminada. Puede editar esta configuración predeterminada cuando sea necesario.

Para editar la configuración de un servidor de recuperación en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores de recuperación**.
2. Haga clic en el servidor cuyos ajustes desea editar y luego en **Editar**.
3. Edite la configuración del servidor de recuperación.
4. Haga clic en **Guardar**.

Eliminación de un servidor de recuperación

Puede eliminar los servidores de recuperación que creó en Microsoft Azure.

Para eliminar un servidor de recuperación en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores de recuperación**.
2. Haga click en el servidor que quiera eliminar y, a continuación, pulse en **Eliminar**.
3. Haga clic en **Eliminar** en la ventana de confirmación.

Conmutación por error en Microsoft Azure

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Conmutación por error de producción

La conmutación por error es el proceso que cambia la carga de trabajo del servidor original en su sitio local al servidor de recuperación.

Al crear un servidor de recuperación, se queda en **Modo de espera**. La máquina virtual correspondiente no existe en Microsoft Azure hasta que inicie una conmutación por error. Antes de iniciar una conmutación por error, debe crear al menos una copia de seguridad de imagen de disco (con volumen de arranque) del equipo original.

Al iniciar una conmutación por error, seleccione el punto de recuperación (copia de seguridad) del equipo original a partir del cual se creará una máquina virtual con los parámetros predefinidos en Microsoft Azure.

Cuando la conmutación por error se completa, el estado del servidor de recuperación cambia a **Conmutación por error**. La carga de trabajo se cambia ahora del equipo original al servidor de recuperación en Microsoft Azure.

Si el servidor de recuperación tiene un agente de protección, para evitar interferencias (como iniciar una copia de seguridad o informar sobre estados obsoletos al componente de copia de seguridad), se detiene el servicio de agente.

Conmutación por error de prueba

La conmutación por error de prueba es un proceso de creación de una máquina virtual temporal en una red virtual (VNet) de Azure aislada y para probar los procedimientos de recuperación, configuraciones y la funcionalidad de las aplicaciones. Para obtener más información, consulte "Conmutación por error de prueba en Microsoft Azure" (p. 129).

Conmutación por error de prueba automatizada

La conmutación por error de prueba automatizada en Microsoft Azure valida la integridad de la copia de seguridad al arrancar una máquina virtual de servidor de recuperación desde la última copia de seguridad y hacer una captura de pantalla para confirmar que el sistema operativo se inició correctamente. Si está habilitada, la conmutación por error de prueba automatizada se inicia una vez al mes. Para obtener más información, consulte "Conmutación por error de prueba automatizada en Microsoft Azure" (p. 133).

Manejo de conflictos de direcciones IP en la conmutación por error

Si la dirección IP configurada en la red de producción ya está en uso en el momento de la conmutación por error de producción, se asignará automáticamente otra dirección IP disponible de la misma red.

Si la dirección IP de la red de prueba configurada ya está en uso en el momento de la conmutación por error de la prueba, se asignará otra dirección IP disponible de la red de prueba.

Recuperación del servidor de recuperación en conmutación por error a un momento dado anterior

Para recuperar un servidor en conmutación por error, inicie una nueva conmutación por error desde un punto de recuperación diferente para restaurar las operaciones.

Widgets de conmutación por error

Durante la conmutación por error de producción y prueba, puede ver información sobre el rendimiento de la conmutación por error (velocidad de recuperación) y los cuellos de botella o atascos en la pestaña **Actividades** de los detalles del servidor de recuperación. Para ver el widget **Atasco**, expanda la actividad **Creando equipo virtual** y, a continuación, en la subactividad **Copiar datos de la copia de seguridad a los discos del equipo virtual**, despliegue **Atasco**.

Realización de una conmutación por error de producción en Microsoft Azure

Cuando realiza una conmutación por error de producción, la carga de trabajo se cambia del equipo original al servidor de recuperación en Microsoft Azure.

Para realizar una conmutación por error de producción en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores de recuperación**.
2. Haga clic en el servidor que desea conmutar por error y luego en **Conmutación por error**.
3. En la ventana **Conmutación por error de servidor**, seleccione **Conmutación por error de producción** y, a continuación, seleccione el punto de recuperación (copia de seguridad) desde el que se iniciará el servidor de la nube.
4. Haga clic en **Iniciar**.

Cuando la conmutación por error se completa, el servicio comienza a ejecutarse en la máquina virtual en Azure. Al hacer clic en **Conectar**, se le redirigirá a la máquina virtual en Azure.

Conmutación por error de prueba en Microsoft Azure

Una conmutación por error de prueba es una parte vital de la estrategia de Disaster Recovery como servicio (DRaaS) en Microsoft Azure. Permite a las organizaciones validar los procesos de

recuperación sin afectar a los entornos de producción. Esto se realiza simulando la recuperación de una máquina virtual (MV) desde un punto de recuperación (copia de seguridad) seleccionado. El proceso crea una MV temporal en una red virtual (VNet) de Azure aislada para probar los procedimientos de recuperación, las configuraciones y la funcionalidad de las aplicaciones. Aunque son opcionales, se recomienda encarecidamente realizar pruebas de conmutación por error de forma regular para garantizar procesos de recuperación fiables y actualizados. Puede establecer una planificación de pruebas que se base en los requisitos de coste y salvaguarda de su organización.

Puede probar varios servidores de recuperación a la vez y comprobar su interacción. En la red de prueba, los servidores se comunican utilizando sus direcciones IP de producción, pero no pueden iniciar conexiones TCP o UDP con las cargas de trabajo de su red local.

Red de recuperación de prueba

Para asegurarse de que una prueba de conmutación por error no interfiera con las operaciones de producción, configure una red virtual (VNet) aislada en Azure para fines de prueba. Confirme que la VNet de prueba no tenga conexiones de enrutamiento o emparejamiento con la VNet de producción. Pruebe la conectividad desde una máquina virtual en la VNet de prueba para asegurarse de que no pueda acceder a los recursos de producción.

Proceso de la conmutación por error de prueba

El proceso de la conmutación por error de prueba consiste en las siguientes fases.

Iniciación

Durante esta fase, selecciona un punto de recuperación y comienza la conmutación por error de prueba.

Despliegue del trabajador (agente temporal)

Durante esta fase, se despliega automáticamente un trabajador que se utiliza para la operación de conmutación por error de prueba. El despliegue inicial del trabajador para una conmutación por error de prueba o producción puede tardar varios minutos. El inicio de los trabajadores para las conmutaciones por error posteriores debería ser más rápido.

Restauración de datos

Durante esta fase, los datos se copian desde el almacenamiento de copia de seguridad a un contenedor de Azure Blob Storage temporal. El tiempo que se tarda en copiar o restaurar los datos depende del tamaño de la carga de trabajo. Después de que se copien los datos, el contenido de Azure Blob Storage se convierte en un disco administrado, que se utiliza para iniciar la máquina virtual temporal.

Creación de máquina virtual de recuperación

La máquina virtual de recuperación está conectada a la red virtual aislada de Azure y a la subred preconfiguradas. De forma predeterminada, se asigna a la máquina virtual una dirección IP en la que el último octeto coincide con la dirección IP del equipo original. Puede modificar la dirección IP

antes de la conmutación por error de prueba en la configuración del servidor de recuperación. Durante la conmutación por error de prueba, puede hacerlo directamente en el portal de Azure.

Asegúrese de que la red virtual esté aislada de la red de producción para evitar interacciones no deseadas.

Verificación

Después de la creación de la máquina virtual, al hacer clic en el botón **Conectar** se le redireccionará a la máquina virtual específica en el portal de Azure.

Realice todas las pruebas necesarias para verificar el comportamiento de la aplicación, la conectividad y los objetivos de recuperación en el entorno aislado.

La conmutación por error de prueba no sobrescribe los puntos de recuperación existentes, lo que garantiza que sus copias de seguridad permanezcan intactas.

Deteniendo la conmutación por error de prueba

Al detener la conmutación por error de prueba, se eliminan la máquina virtual temporal, los recursos asociados y el trabajador. Si se utilizó una contraseña de cifrado, se elimina automáticamente del almacén de credenciales al detener o completar la conmutación por error de prueba.

Puede detener la prueba de conmutación por error en cualquier momento desde el portal de Azure.

Realización de una prueba de conmutación por error en Microsoft Azure

Aunque la realización de una conmutación por error de prueba es opcional, le recomendamos que lo haga habitualmente con la frecuencia que considere adecuada, teniendo en cuenta el coste y la seguridad.

Importante
Puede realizar una conmutación por error solo desde los puntos de recuperación (copias de seguridad) que se crearon después de crear el servidor de recuperación del dispositivo.

Se debe crear por lo menos un punto de recuperación antes de llevar a cabo una conmutación por error en un servidor de recuperación. Solo se permiten 100 puntos de recuperación como máximo.

Requisitos previos

- El servidor de recuperación está configurado en la ubicación de Azure y tiene al menos un punto de recuperación creado después de que se creó el servidor de recuperación.
- Una red virtual y una subred de Azure aisladas para la conmutación por error de prueba para garantizar que no haya interferencias con los entornos de producción.
- Las reglas del grupo de seguridad de red (NSG) están configuradas para cumplir con sus requisitos.

Para realizar una conmutación por error de prueba en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores de recuperación**.
2. Haga clic en el servidor que desea conmutar por error y luego en **Conmutación por error**.
3. En la ventana **Conmutación por error de servidor**, seleccione **Conmutación por error de prueba** y, a continuación, seleccione el punto de recuperación (copia de seguridad) desde el que se iniciará el servidor de la nube.
4. Haga clic en **Iniciar**.
5. Si la copia de seguridad que ha seleccionado está cifrada usando el cifrado como una propiedad del equipo:
   a. Introduzca la contraseña de cifrado para la copia de seguridad establecida.

      Nota
      Solo se guardará la contraseña temporalmente y se utilizará para la operación de prueba de conmutación por error actual. La contraseña se eliminará automáticamente del almacén de credenciales si se detiene la prueba de conmutación por error o una vez que esta se haya completado.

   b. [Opcional] Para guardar la contraseña de la copia de seguridad establecida y utilizarla en las siguientes operaciones de conmutación por error, seleccione la casilla de verificación **Almacenar la contraseña en un almacén de credenciales seguro...** e introduzca un nombre para las credenciales en el campo **Nombre de las credenciales**.

      Importante
      La contraseña se almacenará en un almacén de credenciales seguro y se aplicará automáticamente en las siguientes operaciones de conmutación por error. No obstante, es posible que incumpla sus obligaciones legales si guarda las contraseñas.

   c. Haga clic en **Listo**.

   Cuando el servidor de recuperación se inicia, su estado cambia a **Probando conmutación por error**.
6. Use uno de los siguientes métodos para probar el servidor de recuperación:
   - En **Disaster Recovery** > **Servidores de recuperación**, seleccione el servidor de recuperación y, a continuación, haga clic en **Conectar**.
   - 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.
   - 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.
7. Cuando la prueba haya terminado, haga clic en **Detener comprobación**.
   El servidor de recuperación se detiene. No se guardan los cambios realizados en el servidor de recuperación durante la conmutación por error de prueba.

Conmutación por error de prueba automatizada en Microsoft Azure

La conmutación por error de prueba automatizada en Microsoft Azure valida la integridad de la copia de seguridad al arrancar una máquina virtual de servidor de recuperación desde la última copia de seguridad y realizar una captura de pantalla para confirmar que el sistema operativo se inició correctamente.

Con la conmutación por error de prueba automatizada, el servidor de recuperación se prueba automáticamente una vez al mes sin ninguna interacción manual.

El proceso de conmutación por error de prueba automatizada está formado por las siguientes partes:

1. Creación de una máquina virtual en Microsoft Azure a partir del último punto de recuperación.
2. Tomar una captura de pantalla de la máquina virtual.
3. Análisis de si el sistema operativo de la máquina virtual arranca correctamente.
4. Notificación acerca del estado de la conmutación por error de prueba.

Nota
La conmutación por error de prueba automatizada consume horas de cálculo de la máquina virtual de Microsoft Azure.

Puede configurar la conmutación por error de prueba automatizada en la configuración del servidor de recuperación. Para obtener más información, consulte "Configuración de la conmutación por error de prueba automatizada en Microsoft Azure" (p. 133).

Si, por algún motivo, la conmutación por error de prueba se omite, se emitirá una alerta.

Nota
La conmutación por error de prueba automatizada fallará si las copias de seguridad del equipo original están cifradas utilizando el cifrado como una propiedad del equipo, y la contraseña de cifrado no se especifica al crear el servidor de recuperación. Para obtener más información sobre cómo especificar la contraseña de cifrado, consulte "Creación de servidores de recuperación en Microsoft Azure" (p. 123).

Configuración de la conmutación por error de prueba automatizada en Microsoft Azure

Al configurar la conmutación por error de prueba automatizada, puede probar el servidor de recuperación de forma mensual sin ejecutar ninguna acción manual.

Para configurar la conmutación por error de prueba automatizada de un servidor de recuperación en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Panel de control**.
2. En el widget **Conmutación por error de prueba automatizada**, haga clic en **Configurar**.
3. En el cuadro de diálogo **Configuración de la conmutación por error automátizada en modo de prueba**, seleccione uno o más servidores de recuperación para los que desee configurar la conmutación por error de prueba automatizada y, a continuación, haga clic en **Siguiente**.
4. Active el interruptor **Conmutación por error de prueba automatizada**.
5. En el campo **Planificación**, seleccione **Mensual**.
6. [Opcional] En **Tiempo de espera de inicio de la MV / Minutos**, cambie el valor predeterminado del período máximo durante el cual el sistema intenta iniciar la máquina virtual en Azure y tomar una captura de pantalla para verificar si el sistema operativo se cargó correctamente.

   Nota
   - Este tiempo de espera no incluye el tiempo necesario para restaurar datos desde un archivo de copia de seguridad en frío. El temporizador comienza cuando la máquina virtual empieza el arranque.
   - Durante la restauración de datos en frío, Azure crea temporalmente un almacenamiento Blob estándar, que posteriormente se convierte en un disco administrado para la máquina virtual.
   - Las horas de cálculo de la máquina virtual de Microsoft Azure no se contabilizan durante el proceso de restauración de datos.

7. [Opcional] Para guardar el valor **Tiempo de espera de inicio de la MV** como predeterminado y que se rellene automáticamente cuando habilite la conmutación por error de prueba automatizada para el resto de servidores de recuperación, seleccione **Establecer como tiempo de espera predeterminado**.
8. Haga clic en **Configurar**.

En la pestaña **Servidores de recuperación**, puede ver que se ha iniciado la conmutación por error de prueba automatizada. Después de que se complete, se eliminará la máquina virtual y podrá encontrar el enlace a la captura de pantalla del sistema operativo validado en los detalles del servidor de recuperación.

Ver el estado de la conmutación por error de prueba automatizada

Puede ver la información de una conmutación por error de prueba automatizada completada de un servidor de recuperación en Microsoft Azure, como el estado, la hora de inicio, la hora de finalización, la duración y la captura de pantalla de la máquina virtual.

Nota
La captura de pantalla de la máquina virtual se conserva hasta que la conmutación por error de la prueba automatizada se ejecuta de nuevo y genera una nueva captura de pantalla.

Pasos para ver el estado de la conmutación por error de prueba automatizada de un servidor de recuperación en Microsoft Azure

1. En la consola, vaya a **Disaster Recovery** > **Servidores de recuperación** y seleccione el servidor de recuperación.
2. En la sección **Conmutación por error de prueba automatizada**, compruebe la información de la última conmutación por error de prueba automatizada.
3. [Opcional] Para ver la captura de pantalla de la máquina virtual, haga clic en **Mostrar captura de pantalla**.

Deshabilitación de la conmutación por error de prueba automatizada

Puede deshabilitar la conmutación por error de prueba automatizada si desea ahorrar recursos o no necesita que se ejecute en un determinado servidor de recuperación en Microsoft Azure.

Para deshabilitar la conmutación por error de prueba automatizada para un servidor de recuperación en Microsoft Azure

1. En la consola, vaya a **Disaster Recovery** > **Servidores de recuperación** y seleccione el servidor de recuperación.
2. Haga clic en **Editar**.
3. En el asistente, haga clic en la pestaña **Conmutación por error de prueba automatizada**.
4. Desactive el interruptor **Conmutación por error de prueba automática**.
5. Haga clic en **Guardar**.

Requisitos y limitaciones para la conmutación por error de máquinas virtuales Linux a Microsoft Azure

Esta sección describe los principales requisitos y limitaciones para la conmutación por error de cargas de trabajo de Linux a Microsoft Azure, especialmente en entornos sin acceso a Internet.

Requisitos

Instalación del agente de máquina virtual de Microsoft Azure con acceso a Internet

El agente de la máquina virtual de Microsoft Azure se instala automáticamente durante la conmutación por error de prueba y producción.

Las herramientas de Linux necesarias (por ejemplo, **cloud-init**, controladores de red) se obtienen de repositorios públicos (por ejemplo, `archive.ubuntu.com` o `mirror.centos.org`).

Por motivos de seguridad, puede permitir la salida de HTTPS solo a repositorios específicos.

Instalación del Agente de máquina virtual de Microsoft Azure sin acceso a Internet

Debe instalar manualmente el Agente de máquina virtual de Microsoft Azure en el equipo Linux de origen antes de la conmutación por error.

Sin el agente, la conmutación por error puede fallar o resultar en una funcionalidad limitada de la máquina virtual.

Limitaciones

Dependencia de Internet

La falta de acceso a Internet en la máquina virtual de Microsoft Azure de destino requerirá que se preinstale un agente de Azure en la carga de trabajo original, lo que añade una sobrecarga de configuración.

La falta de acceso a Internet puede impedir las actualizaciones posteriores a la conmutación por error (por ejemplo, las herramientas de conexión a redes o de copia de seguridad).

Recomendaciones

- Permitir el acceso a Internet para la red virtual de producción y prueba antes de la conmutación por error. Este es un ajuste predeterminado.
- Restringir el acceso saliente a solo repositorios de Linux específicos si los conoce antes de una conmutación por error.
- Restringir el acceso a servicios de producción específicos durante las conmutaciones por error de prueba.
- Puede utilizar imágenes reflejadas internas o VPN para minimizar la dependencia de Internet.
- Ejecute pruebas de conmutación por error de forma regular para garantizar la disponibilidad del entorno.

Conmutación tras recuperación en Microsoft Azure

La conmutación tras recuperación es un proceso que consiste en mover la carga de trabajo desde la nube a la máquina física o virtual en su sitio local. Puede realizar una conmutación tras recuperación en un servidor de recuperación en estado de **Conmutación por error** y seguir usando el servidor en su sitio local.

Puede ejecutar una conmutación por error automatizada en una máquina virtual o un equipo físico en su sitio local. Durante la conmutación tras recuperación, mientras la máquina virtual funciona en la nube, puede transferir los datos de la copia de seguridad al sitio local. Esta tecnología le ayuda a obtener un tiempo de inactividad muy breve, que se calcula y aparece en la consola de Cyber Protect. Puede verlo y usar esta información para planificar sus actividades y, si fuese necesario, advertir a sus clientes sobre un próximo tiempo de inactividad. Si realiza conmutación tras

recuperación basada en agente con un dispositivo de arranque, el tiempo de inactividad aún será menor, porque los cambios delta se transferirán al sitio local.

Para una conmutación tras recuperación a un equipo físico de destino, puede utilizar la conmutación tras recuperación basada en agente a través de un dispositivo de arranque. Para obtener más información, consulte "Conmutación tras recuperación basada en agente mediante dispositivos de arranque de Microsoft Azure" (p. 137).

Para una conmutación tras recuperación a una máquina virtual de destino, puede utilizar la conmutación tras recuperación basada en agente a través de un dispositivo de arranque o la conmutación tras recuperación sin agente a través del agente de hipervisor. Para obtener más información, consulte "Realización de conmutación tras recuperación basada en agente mediante dispositivo de arranque desde Microsoft Azure" (p. 139) y "Realización de conmutación tras recuperación sin agente a través de un agente hipervisor desde Microsoft Azure" (p. 143).

Cuando no pueda usar el procedimiento de conmutación tras recuperación automatizada, puede realizarla de forma manual. Para obtener más información, consulte "Conmutación tras recuperación manual desde Microsoft Azure" (p. 147).

Nota
Las operaciones de runbook solo admiten la conmutación tras recuperación en el modo manual. Esto significa que, si inicia el proceso de conmutación tras recuperación mediante la ejecución de un runbook que incluya un paso de **Ejecutar una conmutación por recuperación del servidor**, el procedimiento requerirá una interacción manual: deberá recuperar el equipo de forma manual y confirmar o cancelar el proceso de conmutación tras recuperación desde la pestaña **Disaster Recovery** > **Servidores**.

Conmutación tras recuperación basada en agente mediante dispositivos de arranque de Microsoft Azure

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

El proceso de conmutación tras recuperación basada en agente mediante dispositivos de arranque está optimizado para realizar una conmutación tras recuperación a la máquina física o virtual original. Durante este proceso, solo se transfieren los cambios delta al sitio local.

El proceso de conmutación tras recuperación basada en el agente a través de un dispositivo de arranque a una máquina física o virtual de destino consta de las siguientes fases:

1. **Planificación**. Durante esta fase, restaure la infraestructura de TI en su sitio local (como los servidores y las configuraciones de red), configure los parámetros de la conmutación tras recuperación y planifique el inicio de la transferencia de datos.

2. **Transferencia de datos**. Durante esta fase, la máquina virtual en la nube sigue funcionando mientras se transfieren los datos del sitio en la nube al sitio local. Puede iniciar la siguiente fase de cambio en cualquier momento durante la transferencia de datos, pero deberá tener en cuenta la siguientes relaciones.

   Cuanto más tiempo pase en la fase de transferencia de datos,

   - más tiempo se seguirá ejecutando la máquina virtual en la nube;
   - mayor será la cantidad de datos transferidos a su sitio local;
   - mayor será el coste que pagará (gasta más en puntos de cálculo);
   - menor será el tiempo de inactividad que experimente durante la fase de cambio.

   Si desea reducir el tiempo de inactividad, inicie la fase de cambio cuando se haya transferido más del 90 % de los datos al sitio local.

   Si no puede permitirse tener un tiempo de inactividad más largo y no desea gastar más puntos de cálculo para ejecutar la máquina virtual en la nube, puede empezar la fase de cambio antes.

   Nota

   El proceso de transferencia de datos utiliza una tecnología flashback. Esta tecnología compara los datos disponibles en el equipo de destino con los de la máquina virtual en la nube. Si parte de los datos ya están disponibles en el equipo de destino, no se transferirán de nuevo. Esta tecnología agiliza la fase de transferencia de datos.

   Por ese motivo, le recomendamos que restaure el servidor en el equipo original en el sitio local.

3. **Cambio**. Durante esta fase, la máquina virtual en la nube se apagará y los datos restantes, incluido el incremento de la última copia de seguridad, se transferirán al sitio local. Si no se aplica ningún plan de copias de seguridad en el servidor de recuperación, se ejecutará automáticamente una copia de seguridad durante la fase de cambio y ralentizará el proceso.
4. **Validación**. Durante esta fase, el equipo del sitio local estará listo y podrá reiniciarlo con un dispositivo de arranque basado en Linux. Compruebe que la máquina virtual funciona correctamente y:
   - Si todo funciona según lo esperado, confirme la conmutación por recuperación. Tras la confirmación de la conmutación por recuperación, se eliminará la máquina virtual en la nube y el servidor de recuperación volverá al estado **En espera**. El proceso de conmutación por recuperación habrá terminado.
   - Si algo va mal, puede cancelar la conmutación por error y volver a la fase de planificación.

   Nota

   Una vez que se haya reiniciado el dispositivo de arranque, no podrá volver a utilizarlo. Si descubre que algo va mal durante la fase de validación, debe registrar un nuevo dispositivo de arranque y volver a iniciar el proceso de conmutación tras recuperación.

   Sin embargo, al utilizarse la tecnología flashback, no se volverán a transferir los datos que ya estén en el sitio local y el proceso de conmutación tras recuperación será mucho más rápido.

Realización de conmutación tras recuperación basada en agente mediante dispositivo de arranque desde Microsoft Azure

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede ejecutar una conmutación tras recuperación basada en agente mediante dispositivo de arranque desde Microsoft Azure a un equipo físico o una máquina virtual de destino en su sitio local.

Nota
El proceso de transferencia de datos utiliza una tecnología flashback. Esta tecnología compara los datos disponibles en el equipo de destino con los de la máquina virtual en la nube. Si parte de los datos ya están disponibles en el equipo de destino, no se transferirán de nuevo. Esta tecnología agiliza la fase de transferencia de datos.

Por ese motivo, le recomendamos que restaure el servidor en el equipo original en el sitio local.

Requisitos previos

- El agente que utilizará para ejecutar la conmutación por recuperación está en línea y no se está utilizando actualmente en otra operación de conmutación por recuperación.
- Su conexión a Internet es estable.
- Hay un dispositivo de arranque registrado disponible.
  Para obtener más información, consulte Creación de dispositivos de arranque para recuperar sistemas operativos.
- El equipo de destino es el equipo original en su sitio local o tiene el mismo firmware que el equipo original.
- Existe al menos una copia de seguridad completa de la máquina virtual en la nube.

Pasos para llevar a cabo una conmutación por recuperación de un equipo físico

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores**.
2. Seleccione un servidor de recuperación cuyo estado sea **Conmutación por error**.
3. Haga clic en la pestaña **Conmutación por recuperación**.
4. En el campo **Tipo de conmutación tras recuperación**, seleccione **Basada en agente a través de dispositivo de arranque**.
5. En el campo **Dispositivo de arranque de destino**, haga clic en **Especificar**, seleccione el dispositivo de arranque y haga clic en **Listo**.

Nota
Le recomendamos que utilice un dispositivo de arranque listo porque ya estará configurado. Para obtener más información, consulte Creación de dispositivos de arranque para recuperar sistemas operativos.

6. [Opcional] Para cambiar la asignación de discos predeterminada, en el campo **Asignación de discos**, haga clic en **Especificar**, asigne los discos de la copia de seguridad a los discos del equipo de destino y haga clic en **Listo**.
7. Haga clic en **Iniciar transferencia de datos** y, en la ventana de confirmación, haga clic en **Iniciar**.

Nota
Si no hay una copia de seguridad de la máquina virtual en la nube, el sistema realizará una copia de seguridad automáticamente antes de la fase de transferencia de datos.

Se iniciará la fase de transferencia de datos. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra cuántos datos se han transferido ya al sitio local y la cantidad total de datos que se transferirán. La cantidad total de datos incluye los de la copia de seguridad más reciente antes de que se iniciase la fase de transferencia de datos y las copias de seguridad de los datos recién generados (incrementos de copia de seguridad), mientras que la máquina virtual sigue ejecutándose en la fase de transferencia de datos. Por este motivo, los valores de **Progreso** aumentarán con el paso del tiempo. Como el sistema utiliza una tecnología flashback durante la transferencia de datos y no transfiere los datos que están disponibles en el equipo de destino, puede que el progreso sea más rápido de lo que ha calculado inicialmente la consola.
Estimación del tiempo de inactividad	Este parámetro muestra cuánto tiempo dejará de estar disponible la máquina virtual en la nube si inicia la fase de cambio ahora. El valor se calcula según los valores del parámetro **Progreso** y disminuye con el paso del tiempo. Como el sistema utiliza una tecnología flashback durante la transferencia de datos y no transfiere los datos que están disponibles en el equipo de destino, puede que el tiempo de inactividad sea mucho menor que el valor que ha mostrado inicialmente la consola.

8. Haga clic en **Cambio** y en la ventana de confirmación vuelva a hacer clic en **Cambio**.
Se iniciará la fase de cambio. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra el progreso de restauración del equipo en el sitio local.
Tiempo estimado para finalizar	Este parámetro muestra el tiempo aproximado en el que se completará la fase de cambio y tras el que podrá encender el equipo en el sitio local.

Nota
Si no se aplica ningún plan de copias de seguridad en la máquina virtual de la nube, se ejecutará automáticamente una copia de seguridad durante la fase de cambio, lo cual ralentizará el proceso.

9. Cuando se complete la fase de **cambio**, reinicie el dispositivo de arranque y compruebe que el equipo físico de su sitio local funciona según lo esperado.
   Para obtener más información, consulte Recuperar discos mediante dispositivos de arranque.
10. Para finalizar el proceso, haga clic en **Confirmar la conmutación tras recuperación** y, en la ventana de confirmación, haga clic en **Confirmar**.
    Se eliminará el equipo virtual en la nube y el servidor de recuperación volverá al estado **En espera**.

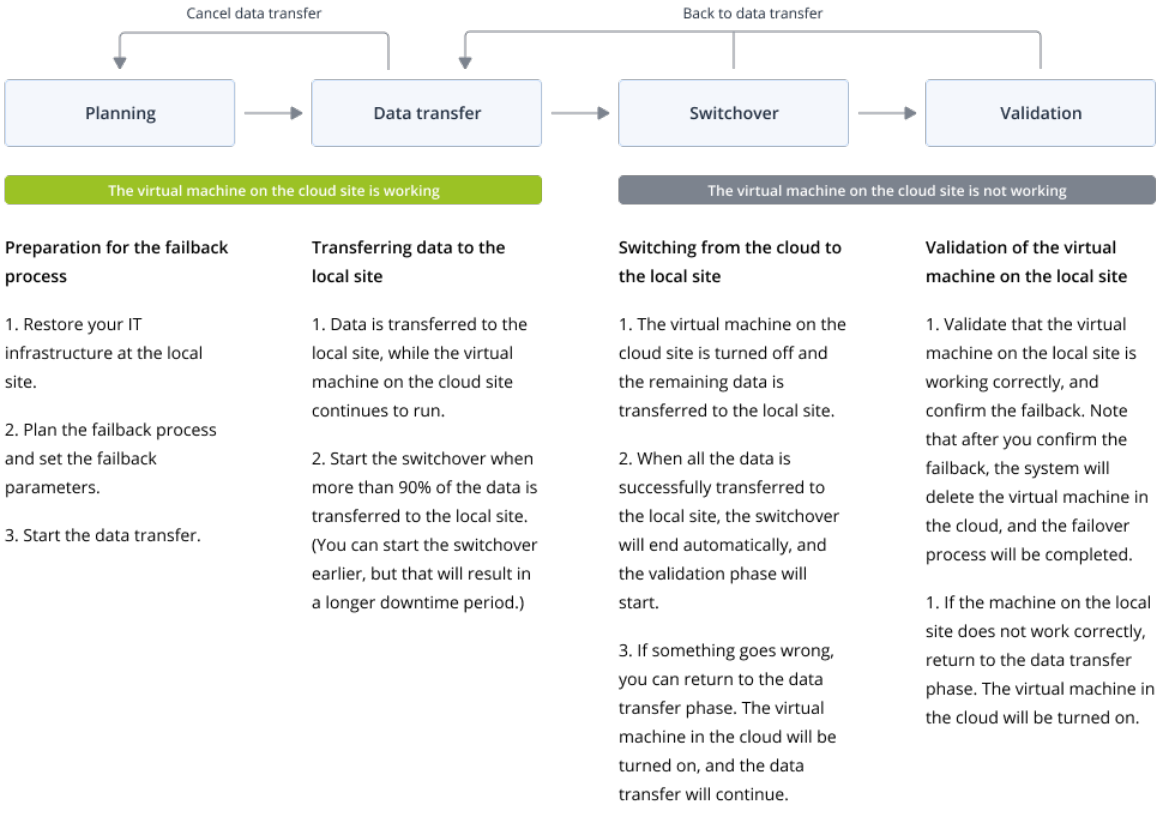
Nota
Aplicar un plan de protección en el servidor recuperado no forma parte del proceso de conmutación por recuperación. Una vez que finalice este proceso, aplique un plan de protección en el servidor recuperado para asegurarse de que vuelve a estar protegido. Puede aplicar el mismo plan de protección que se aplicó al servidor original o un nuevo plan que tenga habilitado el módulo **Recuperación ante desastres**.

Conmutación tras recuperación sin agente mediante un agente de hipervisor desde Microsoft Azure

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La conmutación tras recuperación sin agente mediante un proceso de agente de hipervisor está optimizada para realizar una conmutación tras recuperación desde Microsoft Azure a una nueva máquina virtual. Si desea realizar una conmutación tras recuperación a la máquina virtual original, siga el procedimiento para la conmutación tras recuperación basada en agente mediante dispositivos de arranque.

La conmutación tras recuperación sin agente mediante un agente de hipervisor consta de cuatro fases.



1. **Planificación**. Durante esta fase, restaure la infraestructura de TI en su sitio local (como los servidores y las configuraciones de red), configure los parámetros de la conmutación tras recuperación y planifique el inicio de la transferencia de datos.

   Nota
   Para minimizar el tiempo total del proceso de conmutación tras recuperación, le recomendamos que inicie la fase de transferencia de datos inmediatamente después de configurar sus servidores locales y, a continuación, continúe con la configuración de la red y del resto de la infraestructura local durante la fase de transferencia de datos.

2. **Transferencia de datos**. Durante esta fase, la máquina virtual en la nube sigue funcionando mientras se transfieren los datos del sitio en la nube al sitio local. Puede iniciar la siguiente fase de cambio en cualquier momento durante la transferencia de datos, pero deberá tener en cuenta la siguientes relaciones.

   Cuanto más tiempo pase en la fase de transferencia de datos,

   - más tiempo se seguirá ejecutando la máquina virtual en la nube;
   - mayor será la cantidad de datos transferidos a su sitio local;
   - mayor será el coste que pagará (gasta más en puntos de cálculo);
   - menor será el tiempo de inactividad que experimente durante la fase de cambio.

Si desea reducir el tiempo de inactividad, inicie la fase de cambio cuando se haya transferido más del 90 % de los datos al sitio local.

Si no puede permitirse tener un tiempo de inactividad más largo y no desea gastar más puntos de cálculo para ejecutar la máquina virtual en la nube, puede empezar la fase de cambio antes.

Si cancela el proceso de conmutación por recuperación durante la fase de transferencia de datos, los datos transferidos no se eliminarán del sitio local. Para evitar posibles problemas, elimine de forma manual los datos transferidos antes de iniciar un nuevo proceso de conmutación por recuperación. El posterior proceso de transferencia de datos se iniciará desde el principio.

3. **Cambio**. Durante esta fase, la máquina virtual en la nube se apagará y los datos restantes, incluido el incremento de la última copia de seguridad, se transferirán al sitio local. Si no se aplica ningún plan de copias de seguridad en el servidor de recuperación, se ejecutará automáticamente una copia de seguridad durante la fase de cambio y ralentizará el proceso.

   Puede ver el tiempo estimado de finalización (tiempo de inactividad) de esta fase en la consola de Cyber Protect. Cuando todos los datos se han transferido al sitio local (no hay pérdida de datos y la máquina virtual en el sitio local es una copia exacta de la máquina virtual en la nube), se completa la fase de cambio. Se recuperará la máquina virtual en el sitio local y se iniciará la fase de validación automáticamente.
4. **Validación**. Durante esta fase, la máquina virtual en el sitio local está lista y se inicia automáticamente. Puede verificar si la máquina virtual está funcionando correctamente, y:
   - Si todo funciona según lo esperado, confirme la conmutación por recuperación. Tras la confirmación de la conmutación por recuperación, se eliminará la máquina virtual en la nube y el servidor de recuperación volverá al estado **En espera**. El proceso de conmutación por recuperación habrá terminado.
   - Si algo va mal, puede cancelar el cambio y volver a la fase de transferencia de datos.

Realización de conmutación tras recuperación sin agente a través de un agente hipervisor desde Microsoft Azure

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede realizar una conmutación tras recuperación sin agente desde Microsoft Azure a una máquina virtual de destino en su sitio local a través de un agente hipervisor.

Requisitos previos

- El agente que utilizará para ejecutar la conmutación por recuperación está en línea y no se está utilizando actualmente en otra operación de conmutación por recuperación.
- Su conexión a Internet es estable.
- Existe al menos una copia de seguridad completa de la máquina virtual en la nube.

Pasos para realizar una conmutación tras recuperación sin agente a una máquina virtual a través de un agente de hipervisor

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores**.
2. Seleccione un servidor de recuperación cuyo estado sea **Conmutación por error**.
3. Haga clic en la pestaña **Conmutación por recuperación**.
4. En la sección **Parámetros de la conmutación por recuperación**, en el campo **Tipo de conmutación tras recuperación**, seleccione **Sin agente a través del hipervisor** y, a continuación, configure los demás parámetros.

   Algunos **Parámetros de la conmutación por recuperación** se establecen automáticamente con los valores sugeridos, pero puede cambiarlos.

   La siguiente tabla proporciona más información sobre los **Parámetros de la conmutación por recuperación**.

Parámetro	Descripción
Tamaño de la copia de seguridad	La cantidad de datos que se transferirán a su sitio local durante el proceso de conmutación por recuperación. Tras iniciar el proceso de conmutación por recuperación a un equipo virtual de destino, el **Tamaño de la copia de seguridad** aumentará durante la fase de transferencia de datos debido a que el equipo virtual en la nube seguirá funcionando y generando nuevos datos. Para calcular una estimación del período de inactividad durante el proceso de conmutación por recuperación a un equipo virtual de destino, tome el 10 % del valor del **Tamaño de la copia de seguridad** (puesto que recomendamos iniciar la fase de cambio tras haberse transferido el 90 % de los datos a su sitio local) y divídalo entre el valor de la velocidad de su conexión a Internet. **Nota** El valor de la velocidad de su conexión a Internet se reducirá si realiza varios procesos de conmutación por recuperación al mismo tiempo.
Ubicación del equipo de destino	Ubicación de la conmutación por recuperación: un servidor de VMware ESXi o de Microsoft Hyper-V. Puede elegir entre todos los servidores que tienen un agente registrado en el servicio de ciberprotección.
Agente	Agente que ejecutará la operación de conmutación por recuperación. Solo puede utilizar un agente para llevar a cabo una operación de conmutación por recuperación al mismo tiempo. Puede seleccionar un agente que esté en línea y no se esté utilizando para otro proceso de conmutación por recuperación y

Parámetro	Descripción
	que tenga una versión que admita la funcionalidad de conmutación por recuperación y derechos para acceder a la copia de seguridad. Puede instalar varios agentes en hosts VMware ESXi e iniciar un proceso de conmutación por recuperación independiente con cada uno de ellos. Puede llevar a cabo estos procesos de conmutación por recuperación a la vez.
Configuración del equipo de destino	Configuración del equipo virtual: • **Procesadores virtuales**. Seleccione el número de procesadores virtuales. • **Memoria**. Seleccione cuánta memoria tendrá el equipo virtual. • **Unidades**. Seleccione las unidades para la memoria. • [Opcional] **Adaptadores de red**. Para añadir un adaptador de red, haga clic en **Agregar** y seleccione una red en el campo **Red**. Cuando haya acabado de hacer cambios, haga clic en **Listo**.
Ruta	(Para servidores de Microsoft Hyper-V) Carpeta en el servidor en el que se almacenará su máquina. Asegúrese de que hay suficiente espacio de memoria libre en el servidor para la máquina.
Almacén de datos	[Para hosts VMware ESXi] Almacén de datos en el host en el que se almacenará su máquina. Asegúrese de que hay suficiente espacio de memoria libre en el servidor para la máquina.
Modo de aprovisionamiento	Método de asignación del disco virtual. Para servidores de Microsoft Hyper-V: • **Expansión dinámica** (valor predeterminado). • **Tamaño fijo**. Para servidores de Microsoft Hyper-V: • **Ligero** (valor predeterminado). • **Grueso**.
Nombre del equipo de destino	Nombre de la máquina de destino. De forma predeterminada, el nombre de la máquina de destino es el mismo que el del servidor de recuperación. El nombre del equipo de destino debe ser único en la **Ubicación del equipo de destino** seleccionada.

5. Haga clic en **Iniciar transferencia de datos** y, en la ventana de confirmación, haga clic en **Iniciar**.

Nota
Si no hay una copia de seguridad de la máquina virtual en la nube, el sistema realizará una copia de seguridad automáticamente antes de la fase de transferencia de datos.

Se iniciará la fase de **transferencia de datos**. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra cuántos datos se han transferido ya al sitio local y la cantidad total de datos que se transferirán. La cantidad total de datos incluye los de la copia de seguridad más reciente antes de que se iniciase la fase de transferencia de datos y las copias de seguridad de los datos recién generados (incrementos de copia de seguridad), mientras que la máquina virtual sigue ejecutándose en la fase de transferencia de datos. Por este motivo, ambos valores del parámetro **Progreso** aumentarán con el paso del tiempo.
Estimación del tiempo de inactividad	Este parámetro muestra cuánto tiempo dejará de estar disponible la máquina virtual en la nube si inicia la fase de cambio ahora. El valor se calcula según los valores del parámetro **Progreso** y disminuye con el paso del tiempo.

6. Haga clic en **Cambio** y en la ventana de confirmación vuelva a hacer clic en **Cambio**.
   Se iniciará la fase de cambio. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra el progreso de restauración del equipo en el sitio local.
Tiempo estimado para finalizar	Este parámetro muestra el tiempo aproximado en el que se completará la fase de cambio y tras el que podrá encender el equipo en el sitio local.

Nota
Si no se aplica ningún plan de copias de seguridad en la máquina virtual de la nube, se ejecutará automáticamente una copia de seguridad durante la fase de cambio, lo cual ralentizará el proceso.

7. Después de que se complete la fase de **Cambio** y se inicie automáticamente la máquina virtual en el sitio local, verifique que esté funcionando correctamente.
8. Para finalizar el proceso, haga clic en **Confirmar la conmutación por recuperación** y, en la ventana de confirmación, haga clic en **Confirmar**.
   Se eliminará el equipo virtual en la nube y el servidor de recuperación volverá al estado **En espera**.

Nota
Aplicar un plan de protección en el servidor recuperado no forma parte del proceso de conmutación por recuperación. Una vez que finalice este proceso, aplique un plan de protección en el servidor recuperado para asegurarse de que vuelve a estar protegido. Puede aplicar el mismo plan de protección que se aplicó al servidor original o un nuevo plan que tenga habilitado el módulo **Recuperación ante desastres**.

Conmutación tras recuperación manual desde Microsoft Azure

Nota
Le recomendamos que utilice el proceso de conmutación tras recuperación en un modo manual solo cuando se lo indique el equipo de soporte.

También puede iniciar un proceso de conmutación tras recuperación en un modo manual. En este caso, la transferencia de datos desde la copia de seguridad en la nube al sitio local no se llevará a cabo de forma automática. Se debe hacer de forma manual cuando la máquina virtual en la nube esté apagada. Esto hace que el proceso de conmutación tras recuperación en un modo manual sea mucho más lento y probablemente el tiempo de inactividad también sea mayor.

El proceso de conmutación tras recuperación en un modo manual consta de las siguientes fases:

1. **Planificación**. Durante esta fase, restaure la infraestructura de TI en su sitio local (como los servidores y las configuraciones de red), configure los parámetros de la conmutación tras recuperación y planifique el inicio de la transferencia de datos.
2. **Cambio**. Durante esta fase, la máquina virtual en la nube se apagará y se hará una copia de seguridad de los datos recién generados. Si no se aplica ningún plan de copias de seguridad en el servidor de recuperación, se ejecutará automáticamente una copia de seguridad durante la fase de cambio y ralentizará el proceso. Cuando la copia de seguridad haya finalizado, restaure la máquina en el sitio local de forma manual. Puede recuperar el disco mediante un dispositivo de arranque o toda la máquina desde el almacenamiento de la copia de seguridad en la nube.
3. **Validación**. Durante esta fase, verifique que el equipo físico o la máquina virtual en el sitio local funciona correctamente y confirme la conmutación tras recuperación. Tras la confirmación, se eliminará la máquina virtual en el sitio en la nube y el servidor de recuperación volverá al estado **En espera**.

Realización de una conmutación tras recuperación manual desde Microsoft Azure

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede ejecutar una conmutación tras recuperación manual desde Microsoft Azure en un equipo físico o virtual de destino en su sitio local.

Pasos para llevar a cabo una conmutación tras recuperación manual

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores**.
2. Seleccione un servidor de recuperación cuyo estado sea **Conmutación por error**.
3. Haga clic en la pestaña **Conmutación por recuperación**.
4. En el campo **Destino**, seleccione **Equipo físico**.
5. Haga clic en el icono de engranaje y habilite el conmutador **Usar el modo manual**.
6. [Opcional] Calcule una estimación del período de inactividad durante el proceso de conmutación por recuperación mediante la división del valor del **Tamaño de la copia de seguridad** entre el valor de la velocidad de su conexión a Internet.

   Nota
   El valor de la velocidad de su conexión a Internet se reducirá si realiza varios procesos de conmutación por recuperación al mismo tiempo.

7. Haga clic en **Cambio** y en la ventana de confirmación vuelva a hacer clic en **Cambio**.
   Se apagará la máquina virtual en el sitio en la nube.

   Nota
   Si no se aplica ningún plan de copias de seguridad en la máquina virtual de la nube, se ejecutará automáticamente una copia de seguridad durante la fase de cambio, lo cual ralentizará el proceso.

8. Recupere el servidor desde una copia de seguridad en la nube al equipo físico o a la máquina virtual en su sitio local.
   Para obtener más información, consulte Recuperación de máquinas virtuales y Recuperación de equipos físicos.

   Nota
   Si está realizando una conmutación tras recuperación desde una máquina virtual de Microsoft Azure a la máquina virtual de Azure original, utilice las opciones de recuperación que se describen en "Conmutación tras recuperación desde Microsoft Azure a una máquina virtual de Azure" (p. 149).

9. Asegúrese de que la recuperación se complete y de que la máquina recuperada funcione correctamente y haga clic en **Se ha restaurado el equipo**.
10. Si todo funciona según lo esperado, haga clic en **Confirmar la conmutación por recuperación** y en la ventana de confirmación vuelva a hacer clic en **Confirmar**.
    El servidor de recuperación y los puntos de recuperación pasarán a estar disponibles para la conmutación por error. Para crear puntos de recuperación, aplique un plan de protección al nuevo servidor local.

Nota
Aplicar un plan de protección en el servidor recuperado no forma parte del proceso de conmutación por recuperación. Una vez que finalice este proceso, aplique un plan de protección en el servidor recuperado para asegurarse de que vuelve a estar protegido. Puede aplicar el mismo plan de protección que se aplicó al servidor original o un nuevo plan que tenga habilitado el módulo **Recuperación ante desastres**.

Conmutación tras recuperación desde Microsoft Azure a una máquina virtual de Azure

Puede realizar una conmutación tras recuperación desde una máquina virtual de Microsoft Azure a la máquina virtual de Azure original siguiendo el procedimiento para "Realización de una conmutación tras recuperación manual desde Microsoft Azure" (p. 147) y utilizando una de las siguientes opciones de recuperación en el paso 8:

Opciones de recuperación

- Recuperación sin agente

  Soporta la recuperación solo a una nueva máquina virtual de Microsoft Azure que se crea automáticamente.

  Proceso: configure la conexión de Azure en la consola de Cyber Protect (**Dispositivos** > **Agregar** > **Máquina virtual de Microsoft Azure**).

  Se despliega una máquina virtual de dispositivo de copia de seguridad en la suscripción de Azure para gestionar la recuperación.

  Flujo de recuperación:

  En la pantalla **Almacenamiento de la copia de seguridad**, seleccione una copia de seguridad. Recupérela como una máquina virtual de Azure.

  Puede utilizar el mismo flujo para copias de seguridad físicas, virtuales o basadas en agente.

  Consideración de costes: la máquina virtual de dispositivo, cuando se utiliza solo para la recuperación, únicamente se puede encender durante la recuperación y luego se apaga manualmente.
- Recuperación basada en agente

  Admite la recuperación en la misma máquina virtual de Microsoft Azure (si la máquina virtual original con el agente está disponible) o en una nueva máquina virtual de Azure que tenga un nuevo agente instalado.

  Proceso: cree manualmente una máquina virtual limpia con Windows/Linux en Azure. Instale el agente de protección. Utilice el agente para examinar y recuperar copias de seguridad del almacenamiento en Acronis Cloud Storage.

  Para obtener más información, consulte Recuperación de máquinas de Microsoft Azure y Amazon EC2.

Runbooks en Microsoft Azure

Un runbook es un conjunto de instrucciones en las que se describe la forma de lanzar el entorno de producción en la nube.

Con los runbooks, puede:

- Automatizar la conmutación por error de uno o varios servidores.
- Hacer ping en la dirección IP del servidor y comprobar la conexión al puerto que especifique para poder comprobar automáticamente el resultado de la conmutación por error.
- Establecer la secuencia de operaciones de los servidores mediante la ejecución de aplicaciones distribuidas.
- Incluir operaciones manuales en el flujo de trabajo.
- Verifique la integridad de su solución de recuperación ante desastres mediante la ejecución de runbooks en modo de prueba.

Runbooks para automatizar la operación de conmutación por error y garantizar que sus sistemas se recuperen en el orden correcto para abordar las dependencias entre aplicaciones.

Los runbooks le permiten automatizar una conmutación por error de uno o varios servidores. Puede configurar la secuencia correcta de las operaciones de conmutación por error para los servidores ejecutando las aplicaciones distribuidas. Puede ejecutar runbooks en modo de producción o prueba para comprobar la integridad de su solución de recuperación ante desastres.

Creación de un runbook en Microsoft Azure

Un runbook consiste en pasos que se ejecutan consecutivamente. Un paso consiste en acciones que comienzan simultáneamente.

Para crear un runbook en Microsoft Azure

1. En la consola de Cyber Protection, vaya a **Disaster Recovery** > **Runbooks**.
2. Haga clic en **Crear runbook**.
3. Haga clic en **Añadir paso**.
4. Haga clic en **Añadir acción** y seleccione la acción que quiere añadir al paso.

Acción	Descripción
Conmutar por error el servidor	Realiza una conmutación por error de un servidor de recuperación. Para definir esta acción, debe seleccionar un servidor de recuperación y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estos parámetros, consulte "Parámetros de runbook en Microsoft Azure" (p. 152).

Acción	Descripción
	Nota Si la copia de seguridad del servidor que selecciona está cifrada utilizando el cifrado como una propiedad del equipo, la acción de **Conmutar por error el servidor** se detendrá y cambiará automáticamente a **Se requiere interacción**. Para continuar con la ejecución del runbook, tendrá que proporcionar la contraseña de la copia de seguridad cifrada.
Conmutar por recuperación el servidor	Realiza una conmutación tras recuperación de un servidor en la nube. Para definir esta acción, debe seleccionar un servidor en la nube y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estos parámetros, consulte "Parámetros de runbook en Microsoft Azure" (p. 152). **Nota** Las operaciones de runbook solo admiten la conmutación tras recuperación en el modo manual. Esto significa que, si inicia el proceso de conmutación tras recuperación mediante la ejecución de un runbook que incluya un paso **Conmutar por recuperación el servidor**, el procedimiento requerirá una interacción manual: deberá recuperar el equipo de forma manual y confirmar o cancelar el proceso de conmutación tras recuperación desde la pestaña **Disaster Recovery** > **Servidores**.
Iniciar servidor	Inicia un servidor de la nube. Para definir esta acción, debe seleccionar un servidor de la nube y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estas configuraciones, consulte "Parámetros de runbook en Microsoft Azure" (p. 152). **Nota** La acción de **Iniciar servidor** no es aplicable para operaciones de conmutación por error de prueba en runbooks. Si intenta ejecutar dicha acción, fallará con el mensaje de error siguiente: Error: La acción no se aplica al estado actual del servidor.
Detener servidor	Detiene un servidor en la nube. Para definir esta acción, debe seleccionar un servidor en la nube y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estos parámetros, consulte "Parámetros de runbook en Microsoft Azure" (p. 152). **Nota** La acción **Detener servidor** no es aplicable para operaciones de conmutación por error de prueba en runbooks. Si intenta ejecutar dicha acción, fallará con el mensaje de error siguiente: Error: La acción no se aplica al estado actual del servidor.
Operación manual	Una operación manual requiere una interacción de un usuario. Para definir esta acción, debe ingresar una descripción.

Acción	Descripción
	Cuando una secuencia de runbook llega a una operación manual, el runbook se detendrá y no procederá hasta que un usuario realice la operación manual requerida, como hacer clic en el botón de confirmación.
Ejecutar runbook	Ejecuta otro runbook. Para definir esta acción, debe elegir un runbook. Un runbook puede estar formado únicamente por una ejecución de un runbook determinado. Por ejemplo, si añade la acción "ejecutar Runbook A", puede incluir la acción "ejecutar Runbook B", pero no puede añadir otra acción "ejecutar Runbook A".

5. Defina los parámetros del runbook para la acción. Para obtener más información sobre estos parámetros, consulte "Parámetros de runbook" (p. 100).
6. [Opcional] Para añadir una descripción del paso:
   a. Haga clic en el icono de puntos suspensivos y, luego, en **Descripción**.
   b. Introduzca una descripción del paso.
   c. Haga clic en **Listo**.
7. Repita los pasos del 3 al 6 hasta que cree la secuencia de pasos y acciones deseada.
8. [Opcional] Para cambiar el nombre predeterminado del runbook:
   a. Haga clic en el icono de puntos suspensivos.
   b. Introduzca el nombre del runbook.
   c. Introduzca una descripción del runbook.
   d. Haga clic en **Listo**.
9. Haga clic en **Guardar**.
10. Haga clic en **Cerrar**.

Parámetros de runbook en Microsoft Azure

Los parámetros de runbook son configuraciones específicas que debe configurar para definir una acción de runbook. Definen el comportamiento del runbook dependiendo del estado inicial o resultado de la acción.

En la tabla a continuación se describen los parámetros configurables del runbook para cada acción.

Parámetro de runbook	Disponible para actuar	Descripción
Continuar si ya se ha realizado	• **Conmutar por error el servidor** • **Iniciar servidor** • **Detener servidor** • **Conmutar por**	Este parámetro define el comportamiento del runbook cuando la acción requerida ya se ha realizado (por ejemplo, ya se ha realizado una conmutación por error o un servidor ya está en funcionamiento). Cuando está habilitado, el runbook emite un aviso y continúa. Cuando está deshabilitado, la acción falla y luego el runbook

Parámetro de runbook	Disponible para actuar	Descripción
	recuperación el servidor	también falla. Por defecto, este parámetro está habilitado.
Continuar si falla	• **Conmutar por error el servidor** • **Iniciar servidor** • **Detener servidor** • **Conmutar por recuperación el servidor**	Este parámetro define el comportamiento del runbook cuando la acción requerida falla. Cuando está habilitado, el runbook emite un aviso y continúa. Cuando está deshabilitado, la acción falla y luego el runbook también falla. Por defecto, este parámetro está desactivado.

Operaciones con runbooks en Microsoft Azure

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Cuando un runbook no se está ejecutando, están disponibles las siguientes operaciones: ejecutar, editar, clonar, ver detalles y eliminar.

Ejecutar

Cada vez que haga clic en **Ejecutar**, se le pedirá que establezca los parámetros de la ejecución. Estos parámetros se aplicarán a todas las operaciones de conmutación por error y tras recuperación incluidas en el runbook. Si hay runbooks especificados en las operaciones de **Ejecutar runbook**, heredarán estos parámetros del runbook principal.

Para ejecutar un runbook

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Runbooks**.
2. Haga clic en el runbook que quiera ejecutar y luego en **Ejecutar**.

3. En la ventana **Parámetros de ejecución**, configure los parámetros.

Parámetro	Descripción
Modo conmutación por error y conmutación por recuperación	Elija si quiere ejecutar una conmutación por error de prueba (opción predeterminada) o una real (producción). El modo de conmutación tras recuperación se corresponderá con el modo de conmutación por error seleccionado.
Punto de recuperación de conmutación por error	Seleccione el punto de recuperación más reciente (por defecto) o seleccione un momento dado en el pasado. Si selecciona un momento dado en el pasado, se seleccionarán los puntos de recuperación más cercanos antes de la fecha y hora especificadas para cada servidor.

4. Haga clic en **Iniciar**.

   La ejecución del runbook comienza. Puede detener la ejecución del runbook. El software completará todas las acciones ya iniciadas, excepto las que requieran interacción del usuario.

   Editar

   Pasos para editar un runbook

   1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Runbooks**.
   2. Haga clic en el runbook que quiera ejecutar y luego en **Editar**.
   3. Edite el runbook.
   4. Haga clic en **Guardar**.

   Clonar

   Cuando clona un runbook, el historial del runbook original no se clona.

   Pasos para clonar un runbook

   1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Runbooks**.
   2. Haga clic en el runbook que quiera ejecutar y luego en **Clonar**.
   3. [Opcional] En la ventana de clonación, edite el nombre predeterminado y escriba una descripción.
   4. Haga clic en **Clonar**.

   Ver detalles

   Para ver los detalles de un runbook

   1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Runbooks**.
   2. Haga clic en el runbook cuyos detalles desea ver.
      Se muestran los detalles del runbook y el historial de ejecución.

3. [Opcional] Para ver el registro de ejecución de una ejecución en concreto, haga clic en la línea que le corresponda.

Eliminar

Para eliminar un runbook

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Runbooks**.
2. Haga click en el runbook que quiera eliminar y, a continuación, pulse en **Eliminar**.
3. Haga clic en **Eliminar** en la ventana de confirmación.

Trabajadores en Microsoft Azure

Los trabajadores (workers) son agentes temporales y bajo demanda que se ejecutan en su suscripción de Azure en el grupo de recursos del sistema (con el prefijo: "cyber-protect-rg*") durante las operaciones de recuperación ante desastres, como la conmutación por error, la copia de seguridad tras la conmutación por error y la conmutación tras recuperación. Se despliega un trabajador para cada operación y se elimina tras la finalización de la operación. Este modelo bajo demanda ayuda a reducir costes al desplegar automáticamente los trabajadores solo durante las operaciones de DR activas y eliminarlos después.

El despliegue inicial del trabajador para una conmutación por error de prueba o producción puede tardar varios minutos. Iniciar trabajadores para las conmutaciones por error posteriores debería ser más rápido.

Para supervisar el estado de los trabajadores activos, vaya a **Nubes públicas**, haga clic en la conexión a su suscripción de Microsoft Azure y luego pulse en la pestaña **Trabajadores**.

Si una operación de recuperación ante desastres falla debido a un error con el trabajador, puede generar un informe y ver más información sobre dicho error. Para ello, vaya a la pestaña **Trabajadores**, active el interruptor **Resolución de problemas**, haga clic en el enlace **Instrucciones** y siga las instrucciones.

Recursos de Azure que se crean durante la configuración del sitio de DR y la conmutación por error

Cuando añade una conexión a su suscripción de Azure, el sistema crea un grupo de recursos con el prefijo `cyber-protect-rg*` en la región de Azure que seleccionó durante la configuración de la conexión de Azure. Este grupo de recursos tiene la siguiente etiqueta: **Application:CyberProtect**. Para obtener más información, consulte Seguridad y auditoría de la conexión de Microsoft Azure (72684).

Cuando se completa la configuración del sitio de DR, se crea un grupo de recursos con el prefijo `dr-rg*` para agregar los recursos para la conmutación por error. Este grupo de recursos tiene la siguiente etiqueta: **Application:DisasterRecovery**.

Durante las operaciones de recuperación ante desastres, se despliegan trabajadores temporales (agentes) para orquestar la conmutación por error, la conmutación tras recuperación y las operaciones de copia de seguridad posteriores a la conmutación por error. Estas son máquinas virtuales de Microsoft Azure temporales que se ejecutan en el grupo de recursos `cyber-protect-rg*`. Todos los recursos de Azure que se requieren para una conmutación por error de recuperación ante desastres, como las cuentas de almacenamiento y las máquinas virtuales que han fallado, se crean en el grupo de recursos `dr-rg*`. Puede gestionar la región de Azure para el grupo de recursos de conexión de Azure, el grupo de recursos de DR y sus recursos asociados durante la configuración del sitio de DR.

Eliminación reversible de inquilinos que tienen un sitio de recuperación en Microsoft Azure

La función de eliminación reversible de inquilinos (papelera de reciclaje) es compatible con la configuración del sitio de DR de Microsoft Azure.

Para garantizar la continuidad de la actividad empresarial durante la eliminación reversible y definitiva, las máquinas virtuales de Microsoft Azure en conmutación por error no se detendrán ni se eliminarán.

Caso extremo

Si desactiva el elemento de oferta **DR y copia de seguridad directa en Azure** (ya sea intencionadamente o accidentalmente), se activa una eliminación reversible de la configuración de la recuperación ante desastres (DR) de Azure. Esto significa que la configuración se elimina, pero permanece en la papelera de reciclaje durante 30 días. Si durante este período configura un nuevo sitio de DR en una ubicación diferente (no en Microsoft Azure), para recuperar la configuración inicial de DR en Microsoft Azure, debe habilitar el elemento de oferta **DR y copia de seguridad directa en Azure**, eliminar la nueva configuración y, a continuación, recuperar la inicial.

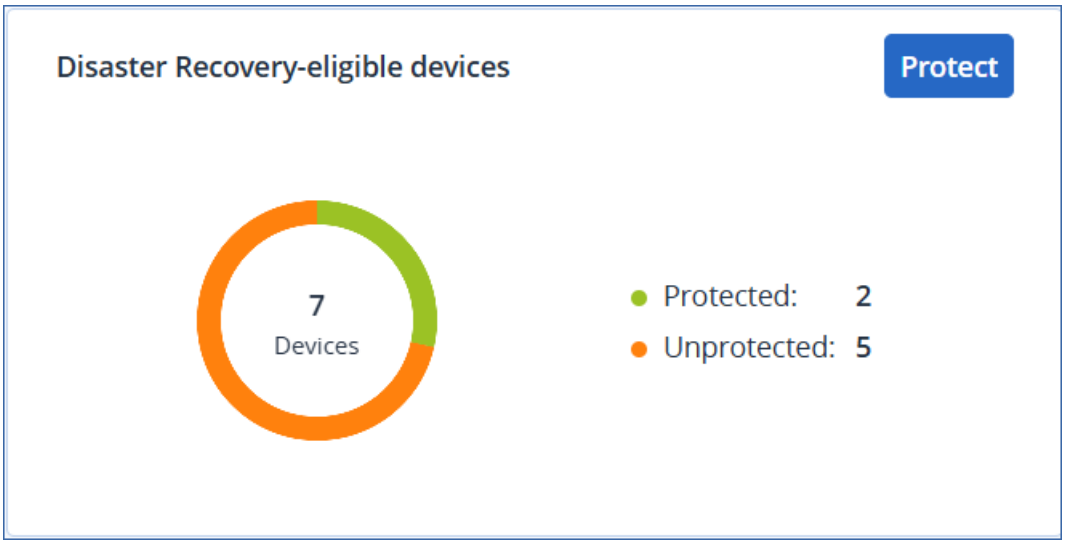
Panel de control de recuperación ante desastres

La página del **Panel de control** de Disaster Recovery contiene widgets que proporcionan un resumen en tiempo real y conocimientos prácticos para su sitio de recuperación ante desastres a lo largo de su ciclo de vida. Esto le ayuda a:

- Detecte y resuelva rápidamente los problemas mediante la supervisión del estado de los servidores de recuperación y principales.
- Evite el uso excesivo de puntos de cálculo al supervisar el número de servidores que los consumen.

Dispositivos elegibles para la recuperación ante desastres

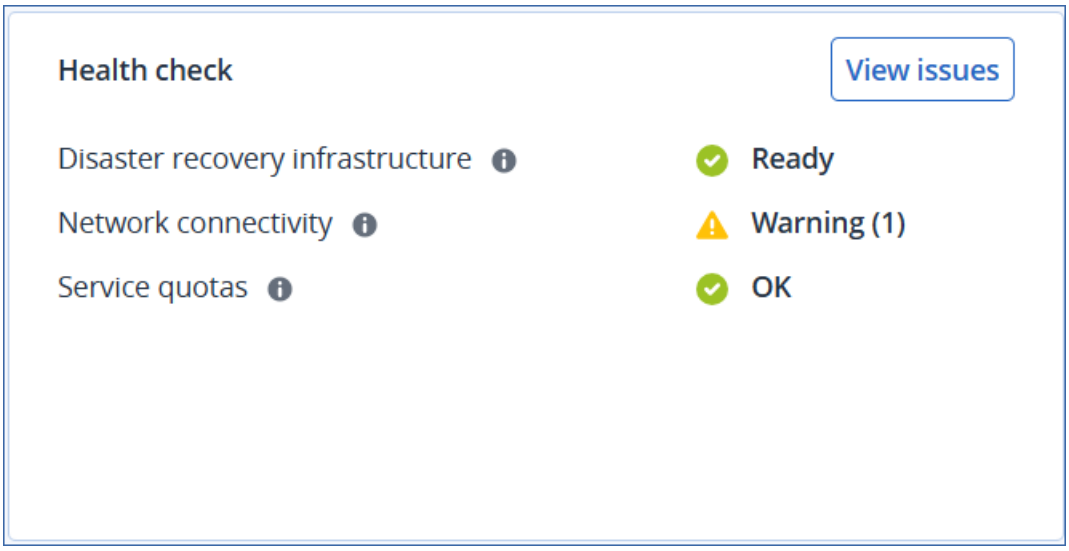
El widget muestra el número total de dispositivos que están protegidos por recuperación ante desastres (tienen un servidor de recuperación) y el número total de dispositivos que son elegibles para la protección por recuperación ante desastres.



Para ir a la página **Todos los dispositivos** donde puede configurar la recuperación ante desastres para los dispositivos elegibles, haga clic en **Proteger**.

Comprobación del estado

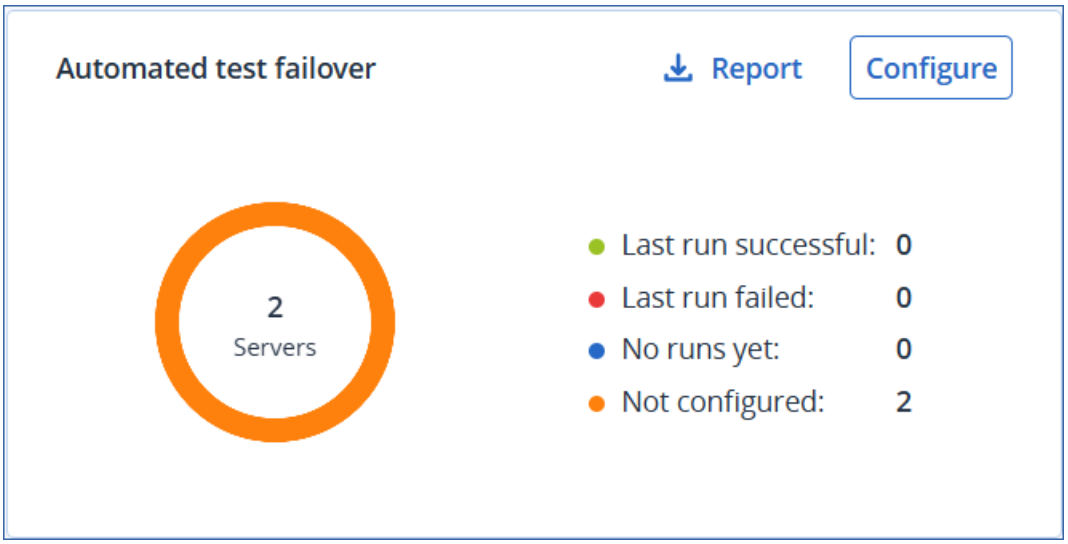
El widget muestra información sobre el estado de su infraestructura de recuperación ante desastres. Puede comprobar el estado de la configuración del sitio, la disponibilidad de la red (solo disponible para Disaster Recovery en Cyber Protect Cloud) y si hay cuotas de servicio que faltan.



Para ver más información acerca de los problemas detectados (avisos o errores), haga clic en **Ver problemas**.

Conmutación por error de prueba automatizada

El widget muestra información acerca de las operaciones de conmutación por error de prueba automatizada de sus servidores de recuperación.



Para comenzar a configurar la conmutación por error de prueba automatizada para sus servidores, haga clic en **Configurar**.

Para descargar los datos del widget, haga clic en **Informe**.

Servidores de recuperación en modo de conmutación por error

El widget muestra el número y el estado de los servidores de recuperación que están en producción o en conmutación por error en una prueba.

Si no hay servidores de recuperación en ejecución en la nube, verá un cero. Si hay un problema con algún servidor, verá un aviso o un estado de error.

El uso de puntos de cálculo por hora que se muestra es una instantánea en tiempo real, no un valor histórico. Esto significa que, si, por ejemplo, tiene dos servidores de recuperación y cada uno de ellos utiliza ocho puntos, verá un total de 16 puntos mostrados en el widget.

Puede utilizar esta información para estimar el coste de ejecución de estos servidores y también como recordatorio para detener la conmutación por error de un servidor que ya no necesita.

Servidores principales

El widget solo está disponible para Disaster Recovery en Cyber Protect Cloud. Muestra el número y el estado de los servidores principales en su entorno y su uso de puntos de cálculo por hora. Puede utilizar esta información para detectar y resolver rápidamente cualquier problema.

El uso de puntos de cálculo por hora que se muestra es una instantánea en tiempo real, no un valor histórico. Esto significa que, si, por ejemplo, tiene dos servidores de recuperación y cada uno de ellos utiliza ocho puntos, verá un total de 16 puntos mostrados en el widget.

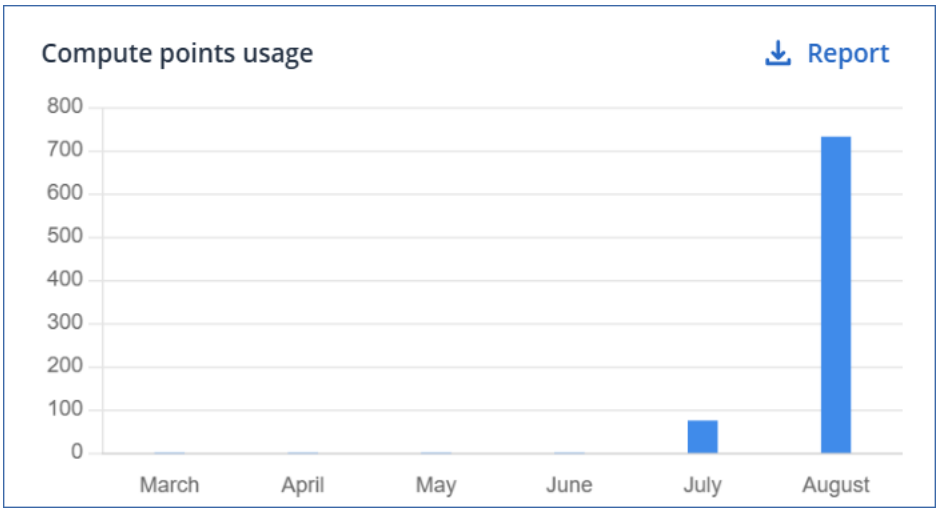
Puede utilizar esta información para estimar el coste de ejecución de estos servidores y también como recordatorio para detener la conmutación por error de un servidor que ya no necesita.

Alertas del servidor en la nube

El widget muestra las alertas más recientes por gravedad, para que pueda ver las alertas críticas de un vistazo. Los valores de **Tipo de alerta** y **Servidor de recuperación** en el widget son enlaces que abren los detalles de la alerta y los detalles del servidor de recuperación, respectivamente.

Uso de puntos de cálculo

Este widget muestra el número de puntos de cálculo que se han utilizado en su entorno durante los últimos 6 meses: el mes actual y cada uno de los cinco meses anteriores.



Puede descargar un informe detallado como un archivo CSV o PDF. El informe incluye la siguiente información sobre los servidores que usaron puntos de cálculo, para cada mes: nombre del servidor, tipo de servidor, estado, iniciado por, hora de inicio, hora de parada, horas activas durante el mes, uso de cálculo por hora y uso total de puntos de cálculo para el mes.

Para descargar los datos del widget, haga clic en **Informe** y, a continuación, seleccione el formato de archivo que prefiera.

Compatibilidad de Disaster Recovery con el software de cifrado

La recuperación ante desastres es compatible con el software de cifrado a nivel de disco siguiente:

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

Nota

- Para cargas de trabajo con cifrado a nivel de disco, recomendamos que instale el agente de protección en el sistema operativo invitado de la carga de trabajo y cree copias de seguridad basadas en agente.
- La conmutación por error y la conmutación tras recuperación no serán compatibles con copias de seguridad sin agente de recursos informáticos cifrados.

Para obtener más información sobre la compatibilidad con el software de cifrado, consulte la guía del usuario de Ciberprotección.

OpenVPN de sitio a sitio: información adicional

Cuando cree un servidor de recuperación, configure su **dirección IP en la red de producción** y su **dirección IP de prueba**.

Después de una conmutación por error (ejecutar la máquina virtual en la nube) y de iniciar sesión en la máquina virtual para comprobar la dirección IP del servidor, verá la **dirección IP en la red de producción**.

Cuando realice la conmutación por error de prueba, solo puede llegar al servidor de prueba usando la **dirección IP de prueba**, que solo es visible en la configuración del servidor de recuperación.

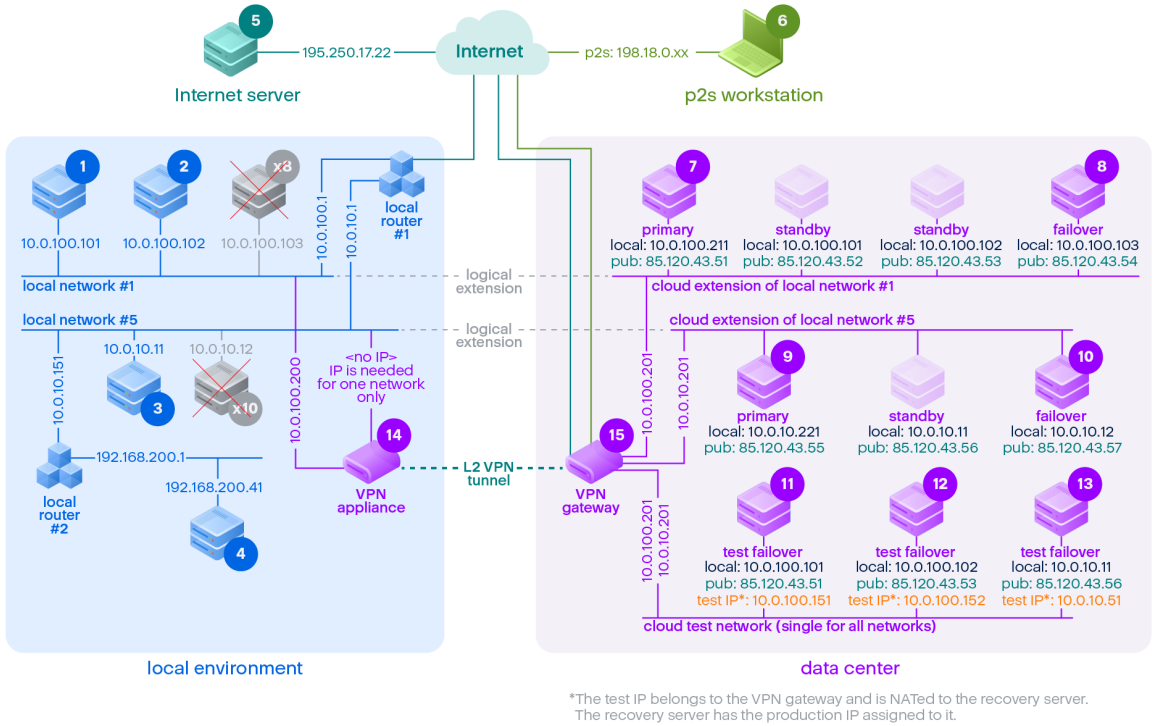
Para acceder a un servidor de prueba desde su sitio local, tiene que usar la **Dirección IP de prueba**.

Nota
La configuración de red del servidor siempre muestra la **dirección IP en la red de producción** (ya que el servidor de prueba refleja cómo se vería el servidor de producción). Esto ocurre porque la dirección IP de prueba no pertenece al servidor de prueba, sino a la puerta de enlace VPN, y se traduce a la dirección IP de producción utilizando NAT.

El siguiente diagrama presenta un ejemplo de la configuración de la conexión OpenVPN de sitio a sitio. Algunos de los servidores del entorno local se recuperan en la nube mediante la conmutación por error (mientras la infraestructura de la red funcione).

1. El cliente habilitó Disaster Recovery:
   a. mediante la configuración del dispositivo VPN (14) y su conexión al servidor VPN exclusivo de la nube (15)
   b. al proteger algunos de los servidores locales con Disaster Recovery (1, 2, 3, x8 y x10)
      Algunos servidores del sitio local (como el 4) están conectados a redes que no están conectadas al dispositivo VPN. Dichos servidores no están protegidos por Disaster Recovery.
2. Parte de los servidores (conectados a diferentes redes) funcionan en el sitio local: (1, 2, 3 y 4)
3. Los servidores protegidos (1, 2 y 3) se están probando con la conmutación por error de prueba (11, 12 y 13)
4. Algunos servidores del sitio local no están disponibles (x8 y x10). Después de ejecutar una conmutación por error, estarán disponibles en la nube (8 y 10)

5. Algunos servidores principales (7 y 9), conectados a diferentes redes, están disponibles en el entorno de la nube
6. (5) es un servidor en Internet con una dirección IP pública
7. (6) es una estación de trabajo conectada a la nube mediante una conexión VPN de punto a sitio (p2s)



En este ejemplo, está disponible la siguiente configuración de conexión (por ejemplo, "ping") desde un servidor en la fila **Desde:** a uno en la columna **Hasta:**.

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
De:		local	local	local	local	Internet	p2s	principal	conmutación por error	principal	conmutación por error	conmutación por error de prueba	conmutación por error de prueba	conmutación por error de prueba	dispositivo VPN	servidor VPN
1	local		directo	a través del enrutador local 1	a través del enrutador local 2	a través del enrutador local 1 y de Internet	no	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub	a través del túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub	a través del enrutador local 1 y del túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub	directo	no
2	local	directo		a través del enrutador local 1	a través del enrutador local 2	a través del enrutador local 1 y de Internet	no	a través del túnel: local a	a través del túnel: local a través del	a través del túnel: local a	a través del túnel: local a través del	a través del túnel: NAT (servidor VPN) a través	a través del túnel: NAT (servidor VPN) a través	a través del enrutador local 1 y del túnel: NAT (servidor	directo	no

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								través del enrutador local 1 y de Internet: pub	enrutador local 1 y de Internet: pub	través del enrutador local 1 y de Internet: pub	enrutador local 1 y de Internet: pub	del enrutador local 1 y de Internet: pub	del enrutador local 1 y de Internet: pub	VPN) a través del enrutador local 1 y de Internet: pub		
3	local	a través del enrutador local 1	a través del enrutador local 1		a través del enrutador local 2	a través del enrutador local 1 y de Internet	no	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub	a través del túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub	a través del enrutador local 1 y del túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub	a través del enrutador local	no
4	local	a través	a través	a través		a través del	no	a través	a través del	a través	a través del	a través del túnel:	a través del túnel:	a través del túnel:	a través	no

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		del enrutador 2 y del enrutador 1 locales	del enrutador 2 y del enrutador 1 locales	del enrutador local 2		enrutador 2 y del enrutador 1 locales y de Internet		del enrutador local 2 y del túnel: local a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	enrutador local 2 y del túnel: local a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	del enrutador local 2 y del túnel: local a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	enrutador local 2 y del túnel: local a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	NAT (servidor VPN) a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	NAT (servidor VPN) a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	NAT (servidor VPN) a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	del enrutador local 2	
5	Internet	no	no	no	no		n/d	a través de Internet: pub	a través de Internet: pub	a través de Internet: pub	a través de Internet: pub	a través de Internet: pub	a través de Internet: pub	a través de Internet: pub	no	no

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
6	p2s	no	no	no	no	a través de Internet		a través de VPN p2s (servidor VPN): local a través de Internet: pub	a través de VPN p2s (servidor VPN): local a través de Internet: pub	a través de VPN p2s (servidor VPN): local a través de Internet: pub	a través de VPN p2s (servidor VPN): local a través de Internet: pub	a través de VPN p2s: NAT (servidor VPN) a través de Internet: pub	a través de VPN p2s: NAT (servidor VPN) a través de Internet: pub	a través de VPN p2s: NAT (servidor VPN) a través de Internet: pub	no	no
7	principal	a través del túnel	a través del túnel	a través del túnel y del enrutador local 1	a través del túnel y del enrutador local 1 y 2	a través de Internet (mediante un servidor VPN)	no		directo de la nube: local	a través del túnel y del enrutador local 1: local	a través del túnel y del enrutador local 1: local	a través de un servidor VPN: NAT	a través de un servidor VPN: NAT	a través del túnel y del enrutador local 1: NAT	no	Solo protocolos DHCP y DNS
8	conmutación	a través	a través	a través	a través	a través de	no	directo de la		a través	a través del túnel	a través de un	a través de un	a través del túnel	no	Solo protoc

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	por error	del túnel	del túnel	del túnel y del enrutador local 1	del túnel y del enrutador local 1 y 2	Internet (mediante un servidor VPN)		nube: local		del túnel y del enrutador local 1: local	y del enrutador local 1: local	servidor VPN: NAT	servidor VPN: NAT	y del enrutador local 1: NAT		olos DHCP y DNS
9	principal	a través del túnel y del enrutador local 1	a través del túnel y del enrutador local 1	a través del túnel	a través del túnel	a través de Internet (mediante un servidor VPN)	no	a través del túnel y del enrutador local 1: local	a través del túnel y del enrutador local 1: local		directo de la nube: local	a través del túnel y del enrutador local 1: NAT	a través del túnel y del enrutador local 1: NAT	a través de un servidor VPN: NAT	no	Solo protocolos DHCP y DNS
10	conmutación por error	a través del túnel y del enrutador local 1	a través del túnel y del enrutador local 1	a través del túnel	a través del túnel	a través de Internet (mediante un servidor VPN)	no	a través del túnel y del enrutador local 1: local	a través del túnel y del enrutador local 1: local	directo de la nube: local		a través del túnel y del enrutador local 1: NAT	a través del túnel y del enrutador local 1: NAT	a través de un servidor VPN: NAT	no	Solo protocolos DHCP y DNS
11	conmut	no	no	no	no	a través	no	no	no	no	no		directo de	a través	no	Solo

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	ación por error de prueba					de Internet (mediante un servidor VPN)							la nube: local	de un servidor VPN: local (enrutamiento)		protocolos DHCP y DNS
12	conmutación por error de prueba	no	no	no	no	a través de Internet (mediante un servidor VPN)	no	no	no	no	no	directo de la nube: local		a través de un servidor VPN: local (enrutamiento)	no	Solo protocolos DHCP y DNS
13	conmutación por error de prueba	no	no	no	no	a través de Internet (mediante un servidor VPN)	no	no	no	no	no	a través de un servidor VPN: local (enrutamiento)	a través de un servidor VPN: local (enrutamiento)		no	Solo protocolos DHCP y DNS
14	dispositivo VPN	directo	directo	a través del enrutador local 1	a través del enrutador local 2	a través de Internet (enrutador local 1)	no	no	no	no	no	no	no	no		no

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
15	servidor VPN	no	no	no	no	no	no	no	no	no	no	no	no	no	no	

Glosario

C

Conexión de punto a sitio (P2S)

Una conexión VPN segura desde el exterior hacia los sitios locales y el cloud mediante sus dispositivos endpoint (como un ordenador de sobremesa o un portátil).

Conexión de sitio a sitio (S2S)

Conexión que amplía la red local al cloud mediante un túnel de VPN seguro.

Conmutación por recuperación

El proceso de restaurar servidores al sitio local después de haberlos cambiado al sitio en el cloud durante la conmutación por error.

D

Dirección IP de prueba

Una dirección IP necesaria en caso de una prueba de conmutación por error que evita que se duplique la dirección IP de producción.

Dirección IP pública

Una dirección IP necesaria para que los servidores en el cloud estén disponibles desde Internet.

Dispositivo VPN

Un equipo virtual especial que permite la conexión entre la red local y el sitio en el cloud mediante un túnel de VPN seguro. El dispositivo VPN se implementa en el sitio local.

F

Finalización

El estado intermedio para el proceso de recuperación o conmutación por error de producción del servidor en el cloud. 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.

O

Objetivo del punto de recuperación (RPO)

Cantidad de datos perdidos debido a una interrupción que se miden en la cantidad de tiempo transcurrido desde una interrupción planificada o un desastre. 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.

P

Puerta de enlace de VPN (anteriormente, servidor VPN o puerta de enlace de conectividad)

Un equipo virtual especial que proporciona una conexión entre las redes del sitio local y el sitio en el cloud mediante un túnel de VPN seguro. La puerta de enlace de VPN se implementa en el sitio en el cloud.

R

Recuperación de fallos

Cambiar la carga de trabajo o aplicación al sitio en el cloud en caso de desastre natural o causado por el ser humano en el sitio local.

Red de prueba

Red virtual aislada que se usa para probar el proceso de conmutación por error.

Red productiva

La red interna ampliada por túneles VPN que cubre sitios locales y en el cloud. Los servidores locales y en el cloud pueden comunicarse en la red de producción.

Runbook

Escenario planificado que consiste en pasos configurables que automatizan las acciones de recuperación ante desastres.

S

Servidor de recuperación

Una réplica en equipo virtual del equipo original basada en las copias de seguridad del servidor protegido almacenadas en el cloud. Los servidores de recuperación se utilizan para trasladar cargas de trabajo desde los servidores originales en caso de desastre.

Servidor en la nube

Referencia general a un servidor principal o de recuperación.

Servidor principal

Un equipo virtual que no tiene un equipo enlazado en el sitio local (como un servidor de recuperación). Los servidores principales se utilizan para proteger una aplicación o para ejecutar varios servicios auxiliares (como un servidor web).

Servidor protegido

Un equipo virtual o físico que pertenece a un cliente y está protegido con el servicio.

Sitio en el cloud (o sitio de recuperación ante desastres)

Sitio remoto alojado en el cloud, usado para la ejecución de infraestructuras de recuperación en caso de desastres.

Sitio local

La infraestructura local implementada en las instalaciones de su empresa.

Índice

D