Cyber Disaster Recovery Cloud

24.03

Guía del administrador

REVISIÓN:11/04/2024

Contenido

Acerca de Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR): parte de Cyber Protection que proporciona un servicio de recuperación ante desastres (DRaaS). Cyber Disaster Recovery Cloud es una solución rápida y estable para iniciar las copias exactas de sus equipos en el sitio en la nube y trasladar la carga de trabajo de los equipos originales dañados a los servidores de recuperación en la nube, en caso de desastre natural o causado por el ser humano.

Puede configurar la recuperación ante desastres de las siguientes maneras:

- Cree un plan de protección que incluya el módulo de recuperación ante desastres y aplíquelo a sus dispositivos. Así se configurará automáticamente la infraestructura predeterminada de recuperación ante desastres. Consulte Crear un plan de protección de recuperación ante desastres.
- Configure la infraestructura en la nube de recuperación ante desastres manualmente y controle cada paso. Consulte "Configuración de servidores de recuperación" (p. 58).

La funcionalidad clave

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

- Gestionar el servicio Cyber Disaster Recovery Cloud 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 en sus ubicaciones locales y en la nube
- Proteger su equipo con el uso de servidores de recuperación en el cloud
- Proteger aplicaciones y dispositivos con el uso de servidores principales en el cloud
- Realizar operaciones de recuperación ante desastres automáticas para copias de seguridad cifradas
- Realizar una prueba de conmutación por error en la red aislada
- Use runbooks para iniciar 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.

Requerimientos de software

Sistemas operativos compatibles

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

- CentOS 6.6, 7.x, 8.x
- Debian 9.x, 10.x, 11.x
- Red Hat Enterprise Linux 6.6, 7.x, 8.x
- Ubuntu 16.04, 18.04, 20.x, 21.x
- 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

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 https://kb.acronis.com/content/71616.

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

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

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

Limitaciones

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

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 discos dinámicos no son compatibles.
   - Los sistemas operativos de los equipos de escritorio Windows no son compatibles (debido a las condiciones de los productos de Microsoft).
   - El servicio Active Directory no es compatible con la replicación FRS.
   - Los dispositivos extraíbles sin 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. 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 Cyber Disaster Recovery Cloud

Puede utilizar una versión de prueba de Acronis Cyber Disaster Recovery Cloud durante un periodo de 30 días. En este caso, la recuperación ante desastres 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.

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 recuperación ante desastres no se puede utilizar si se cambia la ubicación primaria de almacenamiento de copia de seguridad por una secundaria con redundancia geográfica.

Compatibilidad de la recuperación ante desastres 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.

Puntos de cálculo

En Disaster Recovery, 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 la nube Acronis 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 cobrarán 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 la recuperación ante desastres 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.

Crear un plan de protección de recuperación ante desastres

Cree un plan de protección que incluya el módulo Recuperación ante desastres y aplíquelo a sus dispositivos.

De forma predeterminada, el módulo Recuperación ante desastres se deshabilita al crear un nuevo plan de protección. Al habilitar la funcionalidad de recuperación ante desastres y aplicar el plan a sus dispositivos, se crea la infraestructura de red en la nube, incluido 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 en estado En espera (máquina virtual que no está en ejecución) con la configuración predeterminada. El tamaño del servidor de recuperación se establece automáticamente en función de la CPU y la RAM del dispositivo protegido. La infraestructura de red en la nube predeterminada también se crea automáticamente: Las redes y la puerta de enlace de VPN del sitio en la nube a las que se conectarán los servidores de recuperación.

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 eliminan automáticamente. Puede eliminar la infraestructura de recuperación ante desastres manualmente, en caso necesario.

Nota

- Después de configurar la recuperación ante desastres, podrá realizar una prueba o la conmutación por error de producción desde cualquier punto de recuperación creado después de crear el servidor de recuperación del dispositivo. Los puntos de recuperación que se generaron antes de que el dispositivo estuviese protegido con la recuperación ante desastres (por ejemplo, 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. 46).

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. Haga clic en el interruptor que se encuentra junto al nombre del módulo para habilitar el módulo de recuperación ante desastres.
6. Haga clic en **Crear**.
   Se crea el plan y se aplica a los equipos seleccionados.

Qué hacer a continuación

- Puede editar la configuración predeterminada del servidor de recuperación. Para obtener más información, consulte "Configuración de servidores de recuperación" (p. 58).
- Puede editar la configuración predeterminada del servidor de red. Para obtener más información, consulte "Configuración de conectividad" (p. 18).
- Puede obtener más información sobre los parámetros predeterminados del servidor de recuperación y la infraestructura de las redes en la nube. Para obtener más información, consulte "Edición de los parámetros predeterminados del servidor de recuperación" (p. 15) y "Infraestructura de red en la nube" (p. 17).

Edición de los parámetros predeterminados del servidor de recuperación

Al crear y aplicar un plan de protección de recuperación ante desastres, se crea un servidor de recuperación con parámetros predeterminados. Puede editar estos parámetros predeterminados más adelante.

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.

Para editar los parámetros predeterminados del servidor de recuperación

1. Vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione un dispositivo y haga clic en **Recuperación ante desastres**.
3. Edite los parámetros predeterminados del servidor de recuperación.
   Los parámetros del servidor de recuperación se describen en la siguiente tabla.

Servidor de recuperación parámetro	**Predeterminado valor**	**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 el cloud	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 red de producción	automático	Dirección IP que tendrá el servidor en la red 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

La infraestructura de red en la nube consta de la puerta de enlace de VPN del sitio en la nube y de las redes en la nube a las que se conectarán los servidores de recuperación.

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.

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" (p. 39).
- 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. 29). 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 redes predeterminada, haga clic en el enlace **Ir a Conectividad** del módulo de recuperación ante desastres del plan de protección o acceda a **Recuperación ante desastres** > **Conectividad**.

Configuración de conectividad

Esta sección explica los conceptos de red que debe conocer para comprender el funcionamiento de Cyber Disaster Recovery Cloud. Aprenderá a configurar distintos tipos de conectividad al sitio en el cloud, según sus necesidades. Por último, aprenderá a gestionar las redes en el cloud y la configuración del dispositivo VPN y la puerta de enlace de VPN.

Conceptos de redes

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

Cyber Disaster Recovery Cloud 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, Cyber Disaster Recovery Cloud 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 recuperación ante desastres 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.

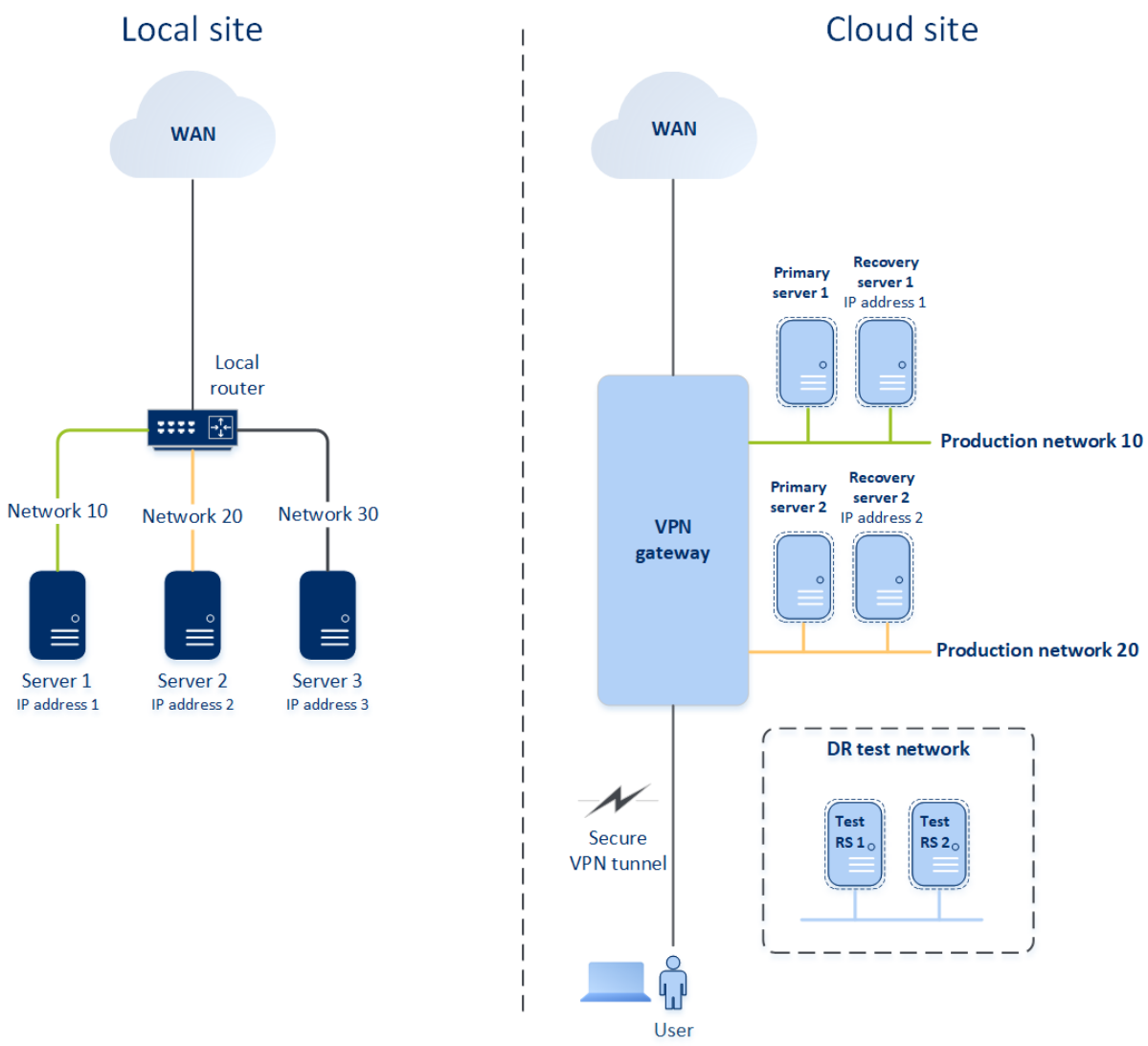
  Para el acceso en un sitio local, este tipo de conexión requiere la implementación de un dispositivo VPN en el sitio local.

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.



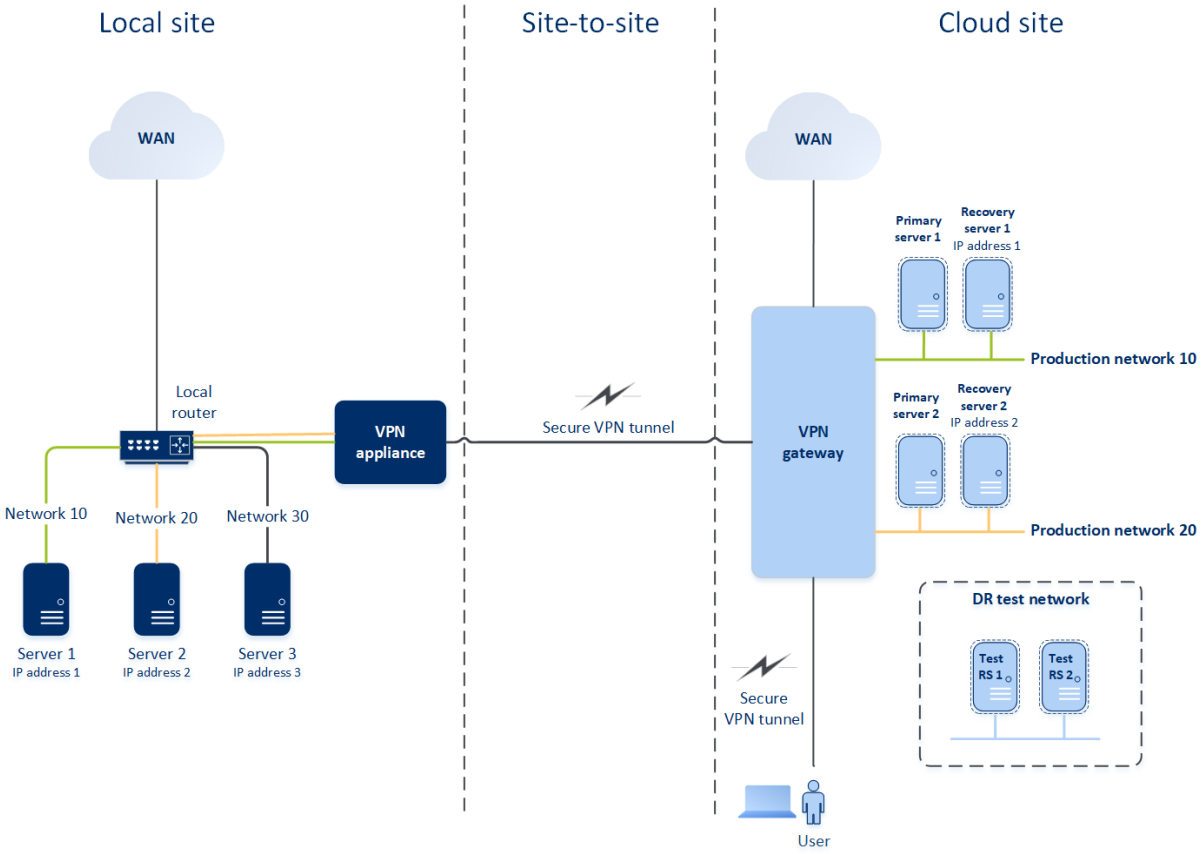
Conexión OpenVPN de sitio a sitio

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

Para entender cómo funcionan las redes en Cyber Disaster Recovery Cloud, 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 Cyber Disaster Recovery Cloud le permite realizar una conmutación por error de toda la carga de trabajo de los equipos dañados en el sitio local a los servidores en la nube que se encuentran en la nube. Puede proteger hasta 23 redes con Cyber Disaster Recovery Cloud.



Para establecer una comunicación 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 implementará automáticamente la puerta de enlace de VPN en el sitio de la nube. Después, debe implementar el dispositivo VPN en su sitio local, añadir las redes que desea proteger y registrar el dispositivo en la nube. Cyber Disaster Recovery Cloud crea una réplica de su red local en la nube. Se establece un túnel VPN seguro entre el dispositivo VPN y la puerta de enlace de VPN. Permite extender su red local al cloud. Las redes de producción en el cloud están conectadas con sus redes locales. Los servidores locales y en la nube pueden comunicarse mediante este túnel VPN si se encuentran todos en el mismo segmento de Ethernet. La enrutación se realiza con su enrutador 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 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. 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 el cloud 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 el cloud, 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 se tratarán en sus respectivas secciones, a continuación.

Cómo funciona el enrutamiento

Cuando se establece la 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 en la nube de una red quiere comunicarse con un servidor de otra red en la nube, el tráfico pasa 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 local y en el cloud es la **puerta de enlace de VPN**. Es una máquina virtual en la nube 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 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 el cloud.

Servidores de recuperación

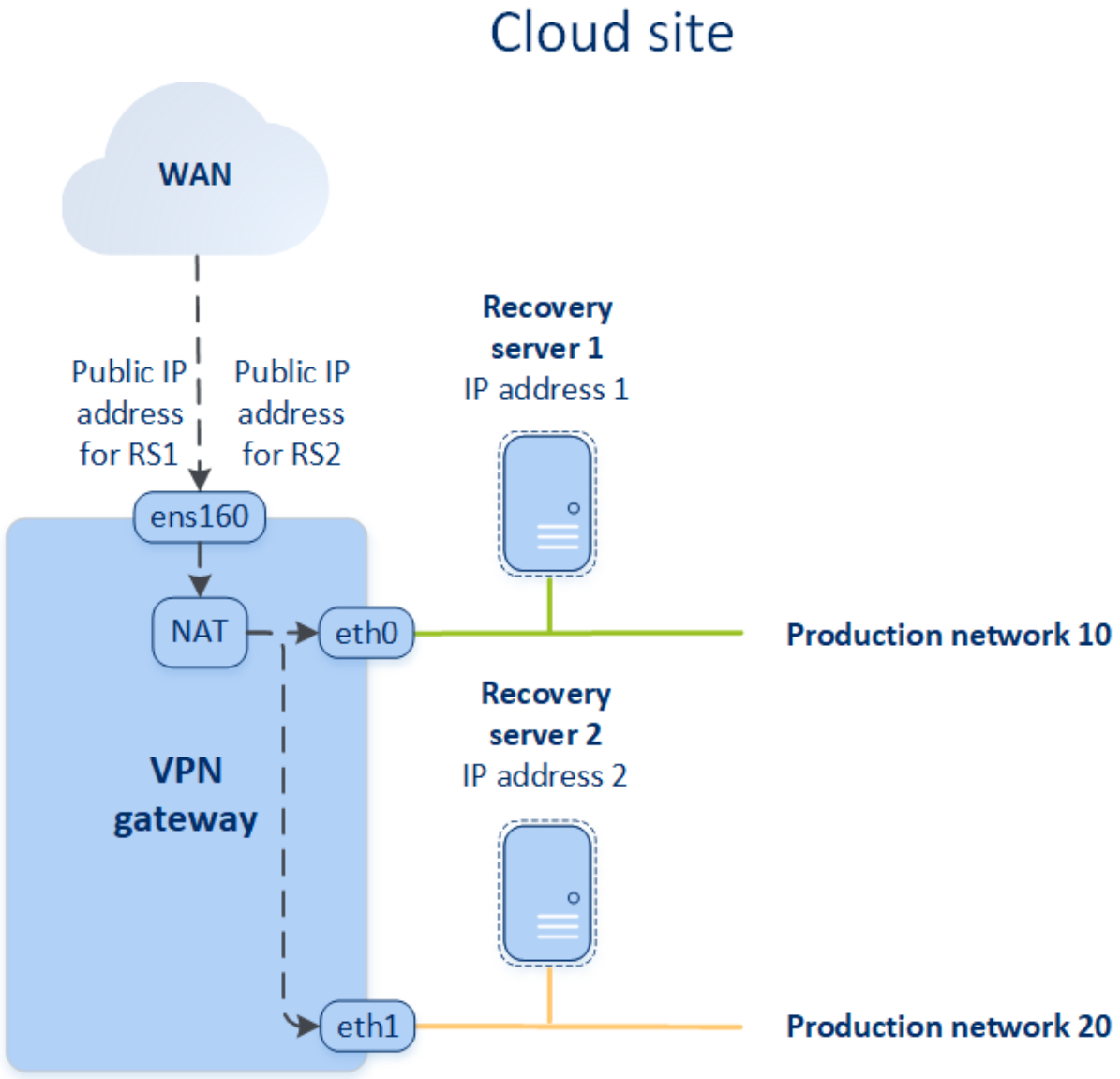
Servidor de recuperación: réplica del equipo original basada en las copias de seguridad del servidor protegido almacenadas en el cloud. Los servidores de recuperación se utilizan para trasladar cargas de trabajo desde los servidores originales en caso de desastre.

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

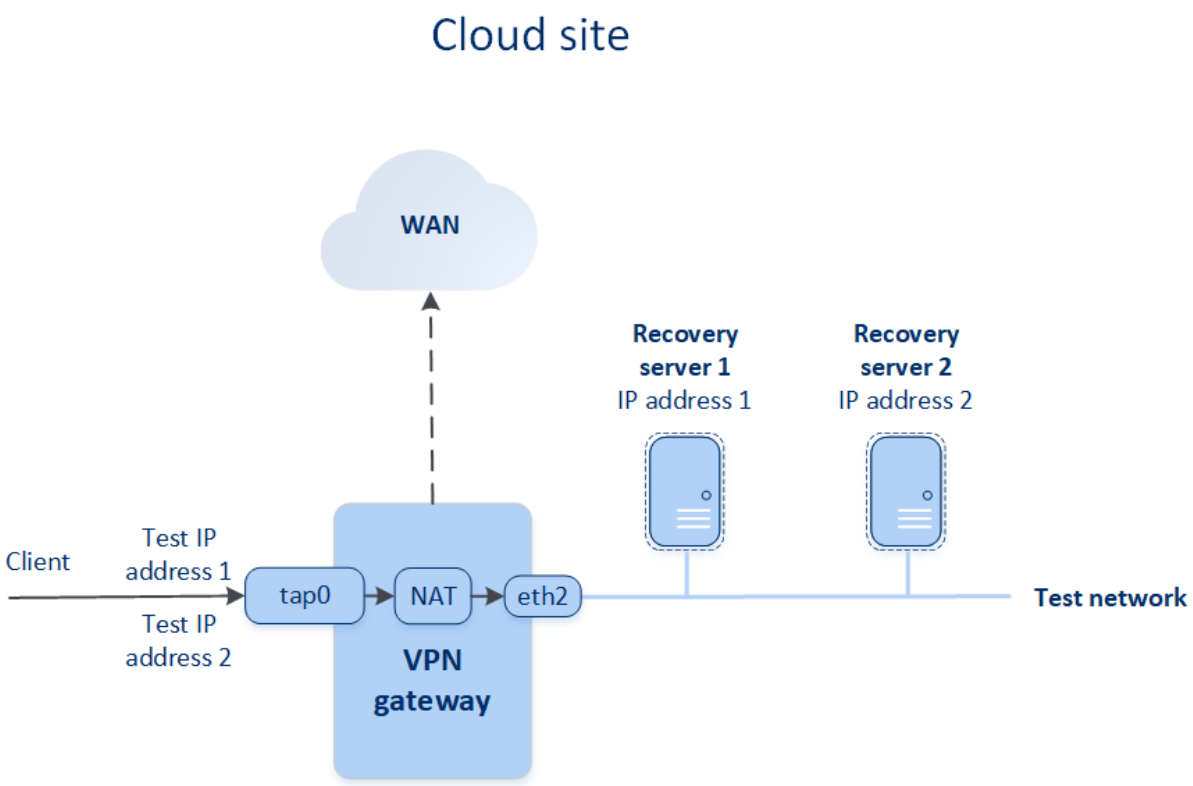
- **Red en el cloud** (obligatoria): una red en el cloud a la que se conecta un servidor de recuperación.
- **Dirección IP en la red de producción** (obligatoria): una dirección IP con la que se inicia un equipo virtual para un servidor de recuperación. Esta dirección se usa tanto para la red de producción como para la de prueba. Antes de iniciar el equipo virtual, este se configura para obtener la dirección IP mediante DHCP.
- **Dirección IP de prueba** (opcional): Una 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): Una 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.
- **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).

Dirección IP de prueba y pública

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 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 continúa funcionando mientras el servidor de recuperación con la misma dirección IP se inicia en la red de prueba en el cloud. 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 a través de 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. 101).

Servidores principales

Servidor principal: 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:

- **Red en el cloud** (obligatoria): una red en el cloud a la que se conecta un servidor principal.
- **Dirección IP en la red de producción** (obligatoria): 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): Una dirección IP para acceder a un servidor principal desde Internet. Si un servidor no tiene dirección IP pública, solo es alcanzable desde la red local y no desde Internet.
- **Acceso a Internet** (opcional): permite que el servidor principal tenga acceso a Internet.

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 Cyber Disaster Recovery Cloud mediante una conexión VPN de IPsec L3 segura.

Este tipo de conectividad es útil para escenarios de recuperación ante desastres si tiene uno de los siguientes casos de uso:

- 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 están conectados a ellos mediante un túnel VPN de 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.

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. 47).
- 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.

Acceso de VPN remoto de punto a sitio

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

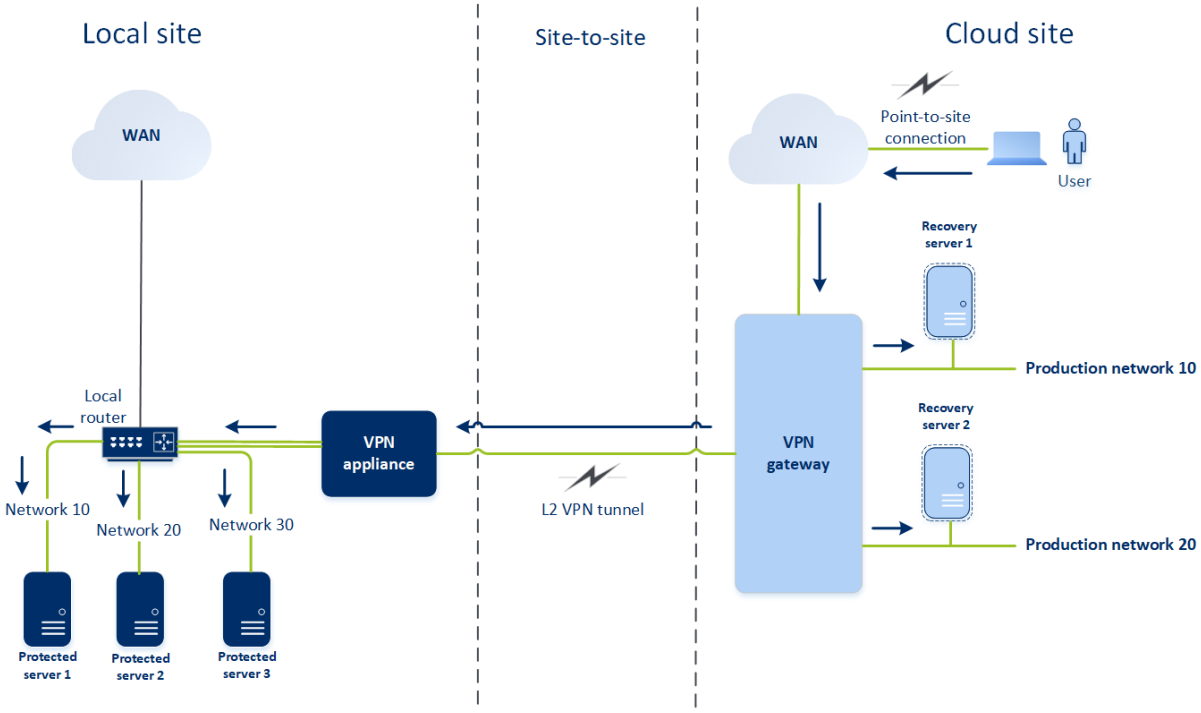
La conexión de punto a sitio es una conexión VPN segura desde el exterior que usa sus dispositivos de endpoint (como un ordenador o portátil) a los sitios en la nube y locales mediante un VPN. Está disponible después de establecer una conexión OpenVPN de sitio a sitio al sitio de Cyber Disaster Recovery Cloud. 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.

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

El servicio de recuperación ante desastres 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.

Configuración de la conectividad inicial

Esta sección describe escenarios de configuración de la conectividad.

Configuración del modo solo en la nube

Para configurar una conexión en el modo solo en la nube

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

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

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 **Recuperación ante desastres** > **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 recuperación ante desastres 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 Cyber Disaster Recovery Cloud. La consola de Cyber Protect muestra las interfaces basándose en la información del dispositivo VPN.

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 **Recuperación ante desastres** > **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.

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

1. En la consola de Cyber Protect, vaya a **Recuperación ante desastres** > **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.

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 **Recuperación ante desastres** > **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 **Recuperación ante desastres** > **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. 31).
- 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 firewall 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.
   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. 34).
   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. 34).

      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 **Añadir** (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 **Añadir** 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. 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

Parámetro	Descripción
	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 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).

Parámetro	Descripción
	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. **Añadir**: 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.

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 recuperación ante desastres.

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. 47).

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. 47).

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

- Se ha configurado una conectividad OpenVPN de sitio a sitio.
- El dispositivo VPN se instala en el sitio local.

Para configurar la conexión de punto a sitio al sitio local

1. En la consola de Cyber Protect, vaya a **Recuperación ante desastres** > **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. Eestas 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/.
   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 compañía" o "Ciberprotección".
d. Importe la configuración descargada a 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, el usuario se podrá conectar al equipo en el sitio local.

Gestión de redes

Esta sección describe escenarios de gestión de redes.

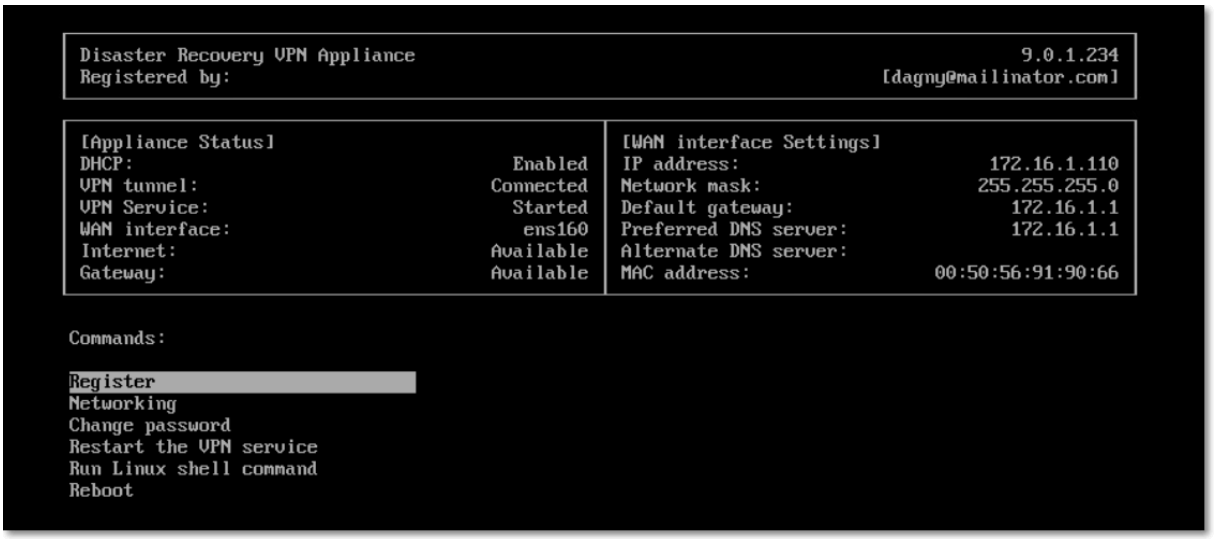
Gestión de redes

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

Conexión OpenVPN de sitio a sitio

Para añadir una red en el sitio local y extenderla al cloud:

1. En el dispositivo VPN, configure la nueva interfaz de red con la red local que desea extender al cloud.
2. Inicie sesión en la consola del dispositivo VPN.
3. En la sección **Redes**, establezca la configuración de red para la nueva interfaz.



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

Para eliminar una red extendida al cloud:

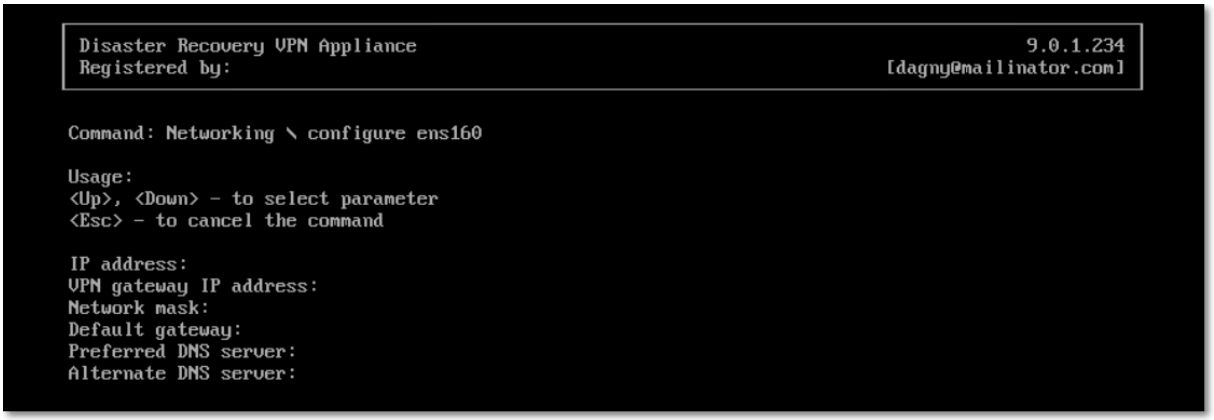
1. Inicie sesión en la consola del dispositivo VPN.
2. En la sección **Redes**, seleccione la interfaz que desea eliminar y haga clic en **Borrar configuración de red**.
3. Confirme la operación.

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

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 dos opciones disponibles:
   - Para la configuración automática de la red mediante DHCP, haga clic en **Usar DHCP**. Confirme la operación.
   - Para la configuración manual de la red, haga clic en **Definir dirección IP estática**. Se pueden editar as siguientes opciones de configuración:
     - **Dirección IP**: la dirección IP de la interfaz en la red local.
     - **Dirección IP de puertas de enlace de VPN**: la dirección IP específica que se reserva para el segmento en la nube de la red para que el servicio de Cyber Disaster Recovery Cloud funcione correctamente.

- **Máscara de red**: máscara de red de la red local.
- **Entrada por defecto**: entrada predeterminada en el sitio local.
- **Servidor DNS preferido**: servidor DNS principal del sitio local.
- **Servidor DNS alternativo**: servidor DNS secundario del sitio local.



- Realice los cambios necesarios y confírmelos al pulsar la tecla Entrar.

Modo solo en la nube

Puede tener hasta 23 redes en la nube.

Para agregar una nueva red al cloud:

1. Vaya a **Recuperación ante desastres** > **Conectividad**.
2. En el **Sitio en la nube**, pulse **Añadir red en la nube**.
3. Defina los parámetros de red en el cloud: la máscara y dirección de red. Haga clic en **Listo** cuando tenga todo a punto.

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

Para eliminar una red en el cloud:

Nota
No puede eliminar una red en la nube si hay al menos un servidor en la nube en ella. Primero elimine el servidor en el cloud y después, la red.

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

Para cambiar los parámetros de la red en el cloud:

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

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 **Recuperación ante desastres** > **Conectividad**.

A continuación se enumeran algunos motivos conocidos para la incoherencia entre direcciones IP:

1. Se migró un servidor de recuperación de una red a otra, o se modificó la máscara de la red en el cloud. Como resultado, los servidores en el cloud 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 este escenario, consulte Cambio de conexiones 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, su estado 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 **Cambiar**, 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 si no hay redes en la que existentes a los 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**.

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 consola de Cyber Protect (**Recuperación ante desastres** > **Conectividad**), puede hacer lo siguiente:

- 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** en el 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).

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 **Recuperación ante desastres** > **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**.

Habilitar y deshabilitar la conexión de sitio a sitio

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

Puede habilitar la conexión 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 conexión de sitio a sitio:

1. Vaya a **Recuperación ante desastres** > **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 Cyber Disaster Recovery Cloud obtiene la configuración de red del dispositivo VPN y extiende las redes locales al sitio en la nube.

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

Para deshabilitar la conexión de sitio a sitio:

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

Cambio de tipo de conexión de sitio a sitio

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

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

1. En la consola de Cyber Protect, vaya a **Recuperación ante desastres** -> **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.

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 **Recuperación ante desastres** -> **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.

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).

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.

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
   Cyber Disaster Recovery Cloud 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**.

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, Cyber Disaster Recovery Cloud 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 **Recuperación ante desastres** > **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 **Añadir** 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, Cyber Disaster Recovery Cloud 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 **Recuperación ante desastres** > **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**.

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 **Recuperación ante desastres** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Haga clic en **Descargar la lista de direcciones MAC** y guarde el archivo CSV.

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 **Recuperación ante desastres** > **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.

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 Recuperación ante desastres, 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.

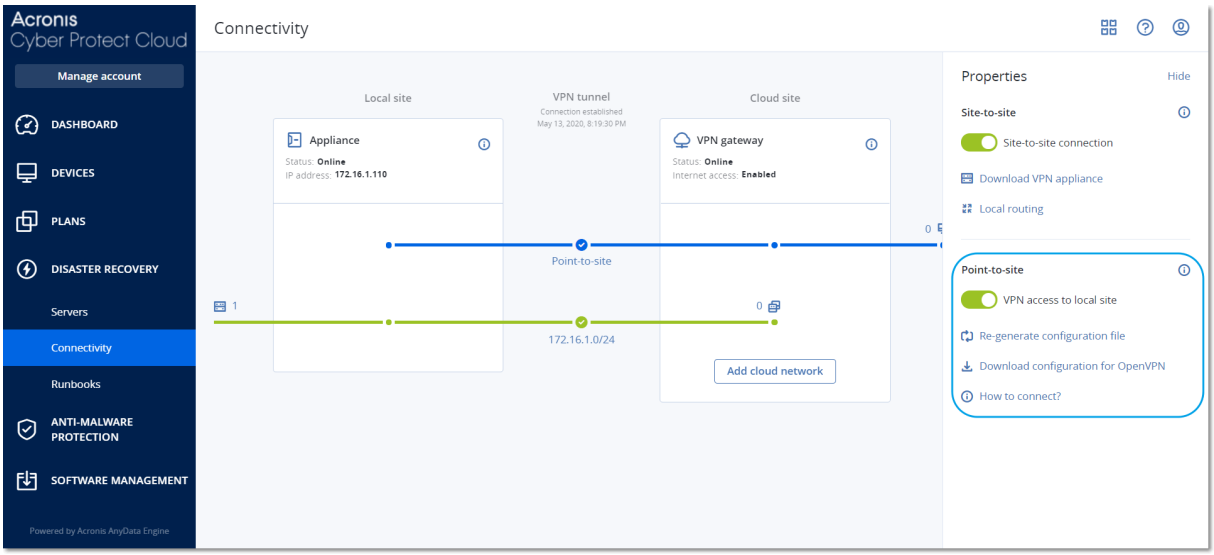
Para permitir el tráfico DHCP a través de la conexión VPN L2

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

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 **Recuperación ante desastres** > **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:

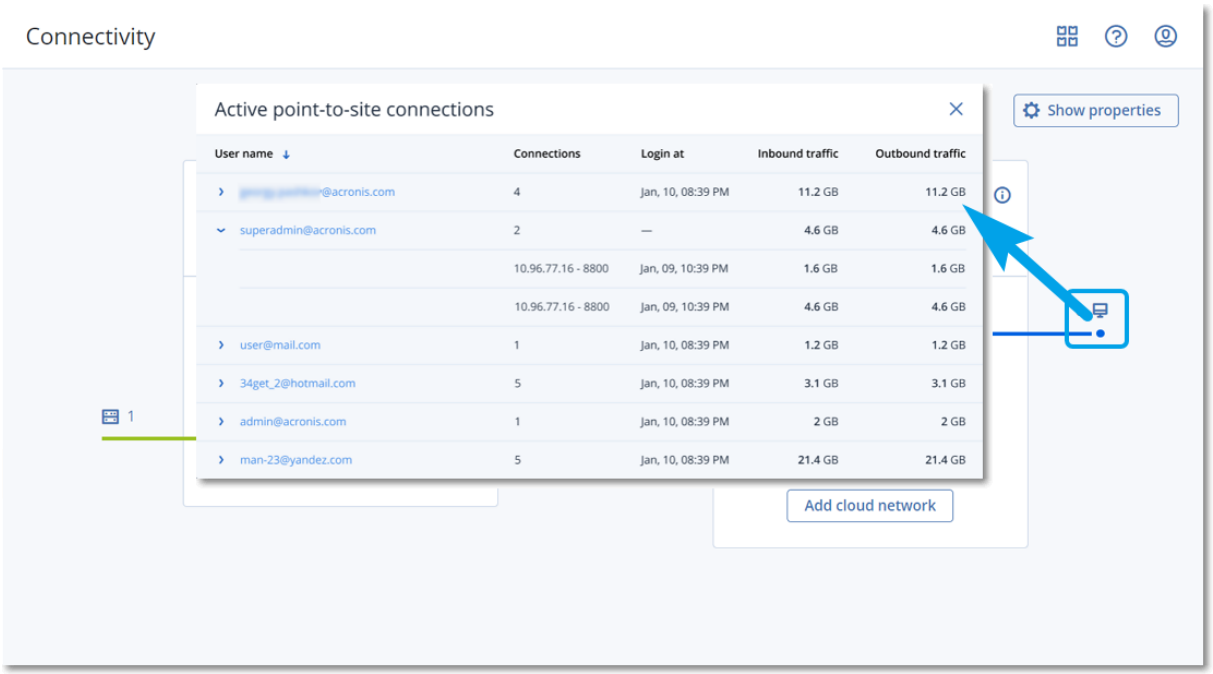
- Si cree que el archivo de configuración está en riesgo.
- Si la autenticación de doble factor estaba habilitada en su cuenta.

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.



Trabajar con registros

La recuperación ante desastres 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.

`dnsmsq.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 de firewall.

`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. 56).

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. 53).
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, a continuación, configure los ajustes. Para obtener más información, consulte "Capturar paquetes de red" (p. 53).
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.

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.

Problema	Posible solución
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 **Añadir** 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. 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** >

Problema	Posible solución
	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 **Recuperación ante desastres** > **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.

Configuración de servidores de recuperación

Esta sección describe los conceptos de conmutación por error y conmutación por recuperación, la creación de un servidor de recuperación y las operaciones de recuperación ante desastres.

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 el cloud.
- 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. 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. 12).

4. Especifique la red en el cloud a la que se conectará el servidor.
5. Seleccione la opción **DHCP**.

Opción DHCP	Descripción
Proporcionado por Cloud Site	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.

6. [Opcional] 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 de recuperación siempre tenga la misma dirección IP. Puede ejecutar aplicaciones con licencias que se registran en la dirección MAC.

7. 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.

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

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

   Puede seleccionar una de las direcciones IP propuestas o escribir otra.
9. [Opcional] Marque la casilla de verificación de **acceso a Internet**.
   De esta forma, el servidor de recuperación tendrá acceso a Internet durante una conmutación por error de prueba o real. De forma predeterminada, el puerto TCP 25 está abierto para las conexiones de salida a direcciones IP públicas.
10. [Opcional] Establezca el **umbral de RPO**.
    El umbral de RPO define el intervalo temporal máximo permitido entre el último punto de recuperación viable para una conmutación por error y el momento presente. El valor se puede establecer entre 15 y 60 minutos, 1 y 24 horas y 1 y 14 días.
11. [Opcional] Marque la casilla de verificación **Usar dirección IP pública**.
    El hecho de que el servidor de recuperación cuente con una dirección IP pública conlleva que se pueda acceder a él desde Internet durante una conmutación por error de prueba o real. Si deja la casilla de verificación desmarcada, el servidor solo estará disponible en su red de producción.

La opción **Usar dirección IP pública** requiere que esté habilitada 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.

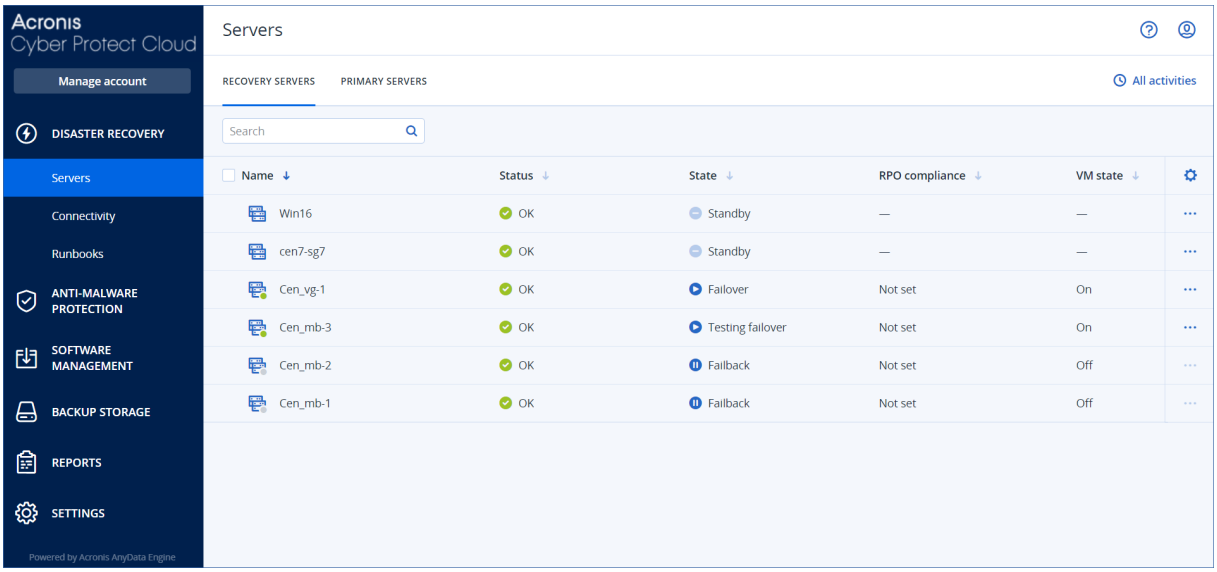
Nota
Si borra la casilla de verificación **Usar dirección IP pública** o elimina el servidor de recuperación, su dirección IP pública no se reservará.

12. [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 **Especificar**, 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. [Opcional] Para ver todas las copias de seguridad, seleccione **Mostrar todas las copias de seguridad**.
    c. Haga clic en **Listo**.

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.

13. [Opcional] Cambie el nombre del servidor de recuperación.
14. [Opcional] Escriba una descripción para el servidor de recuperación.
15. [Opcional] Haga clic en la pestaña **Reglas de cortafuegos de la nube** para editar las reglas de cortafuegos predeterminadas. Para obtener más información, consulte "Configuración de reglas de cortafuegos para servidores en la nube" (p. 89).
16. Haga clic en **Crear**.

En la consola de Cyber Protect, el servidor de recuperación aparece en la pestaña **Recuperación ante desastres** > **Servidores** > **Servidores de recuperación**. Puede ver su configuración si selecciona el equipo original y hace clic en **Recuperación ante desastres**.



Cómo funciona la conmutación por error

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.

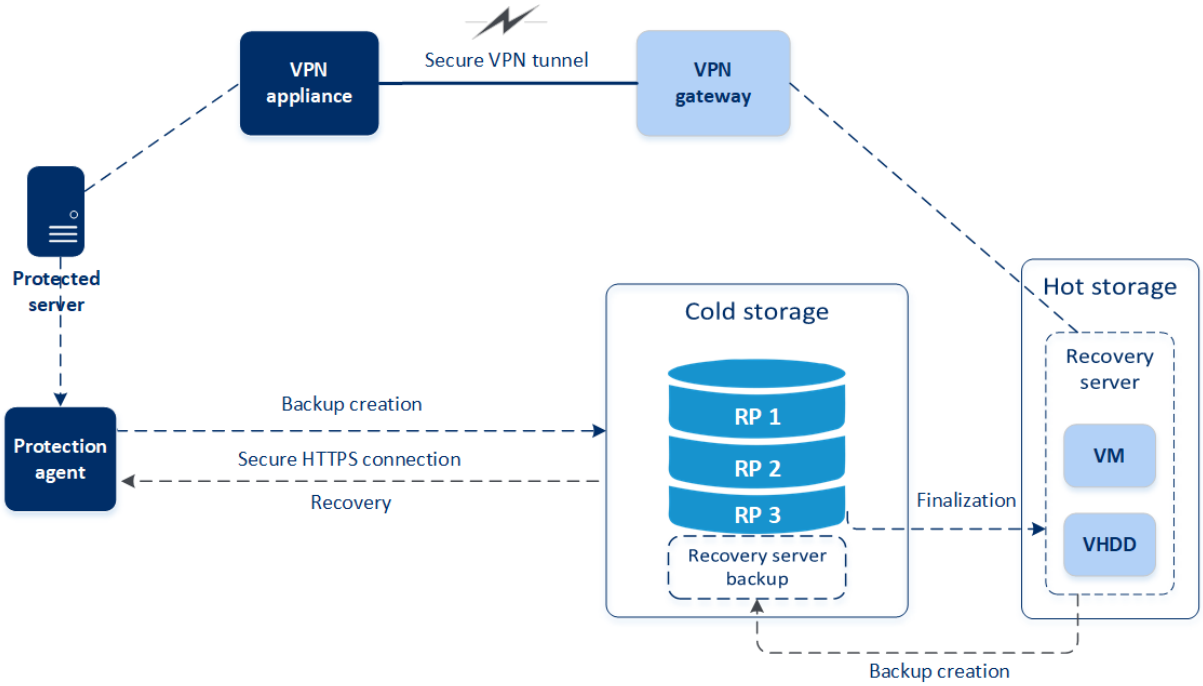
Al iniciar el proceso de conmutación por error, seleccione el punto de recuperación (copia de seguridad) del equipo original a partir del cual se creará una máquina virtual con los parámetros predefinidos. La operación de conmutación por error usa la funcionalidad "ejecutar equipo virtual a partir de 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 del equipo virtual** en la pantalla **Recuperación ante desastres** > **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.



Probar conmutación por error

Durante una **conmutación por error de prueba**, el equipo virtual no se apaga. Esto significa que el agente lee el contenido de los discos virtuales directamente desde la copia de seguridad, es decir, accede aleatoriamente a distintas partes de ella, y su rendimiento puede ser más lento de lo normal. Para obtener más información sobre el proceso de conmutación por error de prueba, consulte "Ejecución de una prueba de conmutación por error" (p. 63).

Conmutación por error de prueba automatizada

Cuando se configura la conmutación por error de prueba automatizada, se ejecuta una vez al mes sin ninguna interacción manual. Para obtener más información, consulte "Conmutación por error de prueba automatizada" (p. 65) y "Configuración de la conmutación por error de prueba automatizada" (p. 66).

Ejecución de una prueba de conmutación por error

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.

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 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 **Recuperación ante desastres**.
   Se abre la descripción del servidor de recuperación.
3. Haga clic en **Conmutación por error**.
4. Seleccione el tipo de conmutación por error **Probar conmutación por error**.
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.

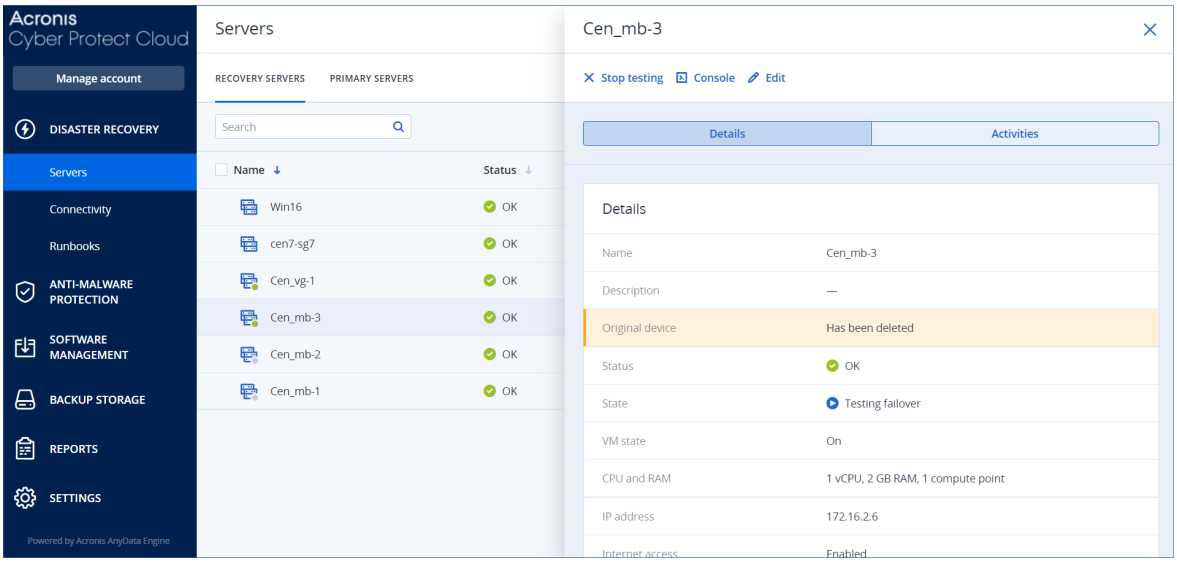
> **Nota**
> Solo se guardará la contraseña temporalmente y se utilizará para la operación de prueba de conmutación por error actual. La contraseña se eliminará automáticamente del almacén de credenciales si se detiene la prueba de conmutación por error o una vez que esta se haya completado.

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 **Recuperación ante desastres** > **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.

Nota
Las acciones **Iniciar servidor** y **Detener servidor** no se aplican a las operaciones de conmutación por error de prueba ni en los runbooks ni cuando se inicia una conmutación por error de prueba manualmente. Si intenta ejecutar dichas acciones, fallarán y aparecerá el siguiente mensaje de error:
Error: La acción no es aplicable al estado actual del servidor.

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. 66).

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. 58).

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 sección **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.

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] Haga clic en **Mostrar captura de pantalla** para ver la captura de pantalla de la máquina virtual.

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 **Recuperación ante desastres** > **Servidores** > **Servidores de recuperación** y seleccione el servidor de recuperación.
2. Haga clic en **Editar**.
3. En la sección **Conmutación por error de prueba automatizada**, en el campo **Planificación**, seleccione **Nunca**.
4. Haga clic en **Guardar**.

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 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 las instrucciones siguientes 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 **Recuperación ante desastres** > **Servidores** > **Servidores de recuperación** y seleccione el servidor de recuperación.
3. Haga clic en **Conmutación por error**.
4. Seleccione el tipo de conmutación por error **Conmutación por error de 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**.

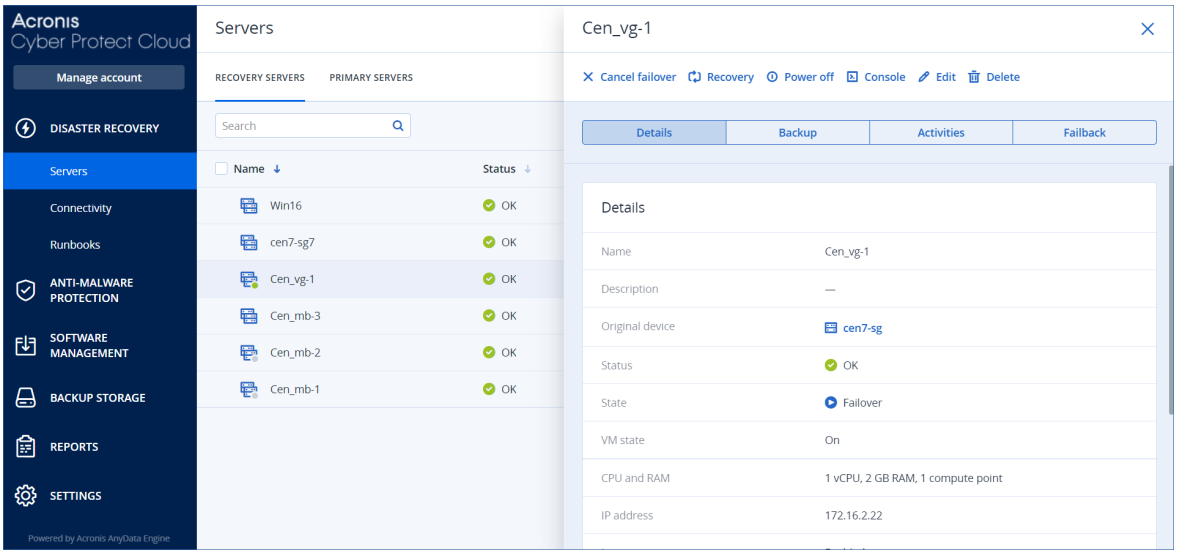
   b. [Opcional] Para guardar la contraseña de la copia de seguridad establecida y utilizarla en las siguientes operaciones de conmutación por error, seleccione la casilla de verificación **Almacenar la contraseña en un almacén de credenciales seguro...** e introduzca un nombre para las credenciales en 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 del equipo virtual** en la pantalla **Recuperación ante desastres** > **Servidores** y en la vista **Detalles** del servidor. Para obtener más información, consulte "Cómo funciona la conmutación por error" (p. 61).



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

Si quiere cancelar la conmutación por error, seleccione el servidor de recuperación y haga clic en **Cancelar conmutación por error**. Se perderán todos los cambios que se hayan realizado desde el momento de la conmutación por error, excepto las copias de seguridad de los servidores de recuperación. El servidor de recuperación volverá al estado **En espera**.

Si quiere llevar a cabo una conmutación tras recuperación, seleccione el servidor de recuperación y haga clic en **Conmutación tras recuperación**.

Cómo realizar una conmutación por error de servidores mediante DNS local

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

Cómo se realiza una conmutación por error de un servidor DHCP

Su infraestructura local puede tener el servidor DHCP ubicado en un host Windows o Linux. Cuando se produce una conmutación por error al sitio de cloud en este tipo de host, se produce el problema de duplicación del servidor DHCP porque la puerta de enlace 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.

Cómo funciona la 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 de destino en su sitio local. Durante la conmutación tras recuperación, la máquina virtual en la nube sigue funcionando mientras se transfieren los datos de la copia de seguridad al sitio local. Esta tecnología le ayuda a conseguir un tiempo de inactividad muy corto, que se estima 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 futuro tiempo de inactividad.

El proceso de conmutación tras recuperación es ligeramente diferente si el destino es una máquina virtual o un equipo físico. Para obtener más información sobre las fases del proceso de conmutación por recuperación, consulte "Conmutación por recuperación en una máquina virtual de destino" (p. 71) y "Conmutación por recuperación en una máquina física de destino" (p. 76).

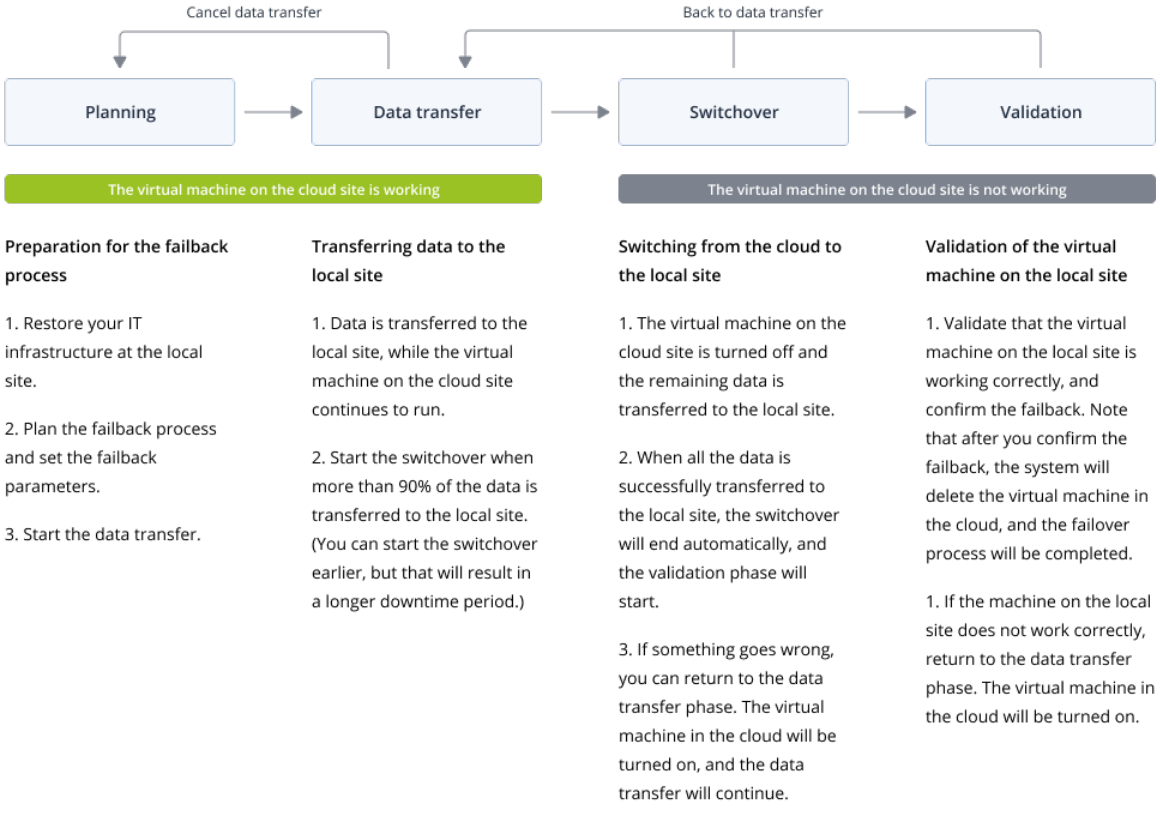
En casos específicos en los que no pueda usar el procedimiento de conmutación tras recuperación automatizada, puede realizarla de forma manual. Para obtener más información, consulte "Conmutación tras recuperación manual" (p. 80).

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 **Recuperación ante desastres** > **Servidores**.

Conmutación por recuperación en una máquina virtual de destino

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

El proceso de conmutación por recuperación de una máquina virtual de destino 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.

Ejecución de la conmutación por recuperación en un equipo virtual

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

Puede ejecutar una conmutación por recuperación en un equipo virtual de destino en su 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.
- 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 virtual

1. En la consola de Cyber Protect, vaya a **Recuperación ante desastres** > **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** seleccione **Equipo virtual** como **Destino**, y configure el resto de 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 destino, tome el 10 % del valor del **Tamaño de la copia de seguridad** (puesto que recomendamos iniciar la fase de cambio

Parámetro	Descripción
	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.
Destino	Tipo de carga de trabajo en su sitio local en el que recuperará el servidor en la nube: **Equipo virtual** o **Equipo físico**.
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 por recuperación en una máquina física de destino

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

El proceso de conmutación tras recuperación automática en un equipo físico de destino consiste en las fases siguientes:

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 físico del sitio local estará listo y podrá reiniciarlo con un dispositivo de arranque basado en Linux. Verifique 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.

Ejecución de conmutación por recuperación en una máquina física

Nota

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

Puede ejecutar una conmutación tras recuperación automática en un equipo físico 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 físico 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 **Recuperación ante desastres** > **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. 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.
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 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 **Recuperación ante desastres** > **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**.

Trabajando con copias de seguridad cifradas

Puede crear servidores de recuperación a partir de las copias de seguridad cifradas. Para su comodidad, puede configurar una aplicación de contraseña automática para una copia de seguridad cifrada durante la conmutación por error de un servidor de recuperación.

Al crear un servidor de recuperación, puede especificar la contraseña para su uso para operaciones de recuperación ante desastres automáticas. Se guardará en el Almacén de credenciales, un almacenamiento seguro de credenciales que puede encontrarse en la sección **Configuración** > **Credenciales**.

Una credencial puede estar vinculada a varias copias de seguridad.

Para gestionar las contraseñas guardadas en el Almacén de credenciales

1. Vaya a **Configuración** > **Credenciales**.
2. Para gestionar una credencial específica, haga clic en el icono en la última columna. Puede ver los elementos enlazados a esta credencial.
   - Para desvincular la copia de seguridad de la credencial seleccionada, haga clic en el icono de papelera de reciclaje cerca de la copia de seguridad. Como resultado, tendrá que especificar la contraseña de forma manual durante la conmutación por error al servidor de recuperación.
   - Para editar la credencial, haga clic en **Editar** y, a continuación, especifique el nombre o contraseña.
   - Para eliminar la credencial, haga clic en **Eliminar**. Tenga en cuenta que tendrá que especificar la contraseña de forma manual durante la conmutación por error al servidor de recuperación.

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. 67).

Después de eso, puede ejecutar la conmutación tras recuperación de Acronis Cyber Protect Cloud a las máquinas virtuales de Azure. El proceso de conmutación tras recuperación es igual al de un equipo físico. Para obtener más información, consulte "Ejecución de conmutación por recuperación en una máquina física" (p. 77).

Nota
Para registrar una nueva máquina virtual de Azure para la conmutación tras recuperación, puede usar la extensión Acronis Backup VM disponible en Azure.

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. 31).

Configuración de servidores principales

En esta sección se describe cómo crear y administrar sus servidores principales.

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 **Recuperación ante desastres** > **Servidores** > **Servidores principales**.
2. Haga clic en **Crear**.
3. Seleccione una plantilla para el nuevo equipo virtual.
4. 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	1000
F3	2	8	2000
F4	4	16	4000
F5	8	32	8000
F6	16	64	16000
F7	16	128	32000
F8	16	256	64000

Nota
Puede ver los puntos de cálculo para cada opción. El número de puntos de cálculo indican el coste de funcionamiento del servidor principal por hora. Para obtener más información, consulte "Puntos de cálculo" (p. 12).

5. [Opcional] Cambie el tamaño de las unidades de discos virtuales. Si necesita más de un disco rígido, haga clic en **Agregar disco** y, a continuación, especifique el nuevo disco. Actualmente no puede añadir más de 10 discos en un servidor principal.
6. Especifique la red de cloud en la que se incluirá el servidor principal.
7. Seleccione la opción **DHCP**.

Opción DHCP	Descripción
Proporcionado por Cloud Site	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.

8. [Opcional] 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.
9. 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.

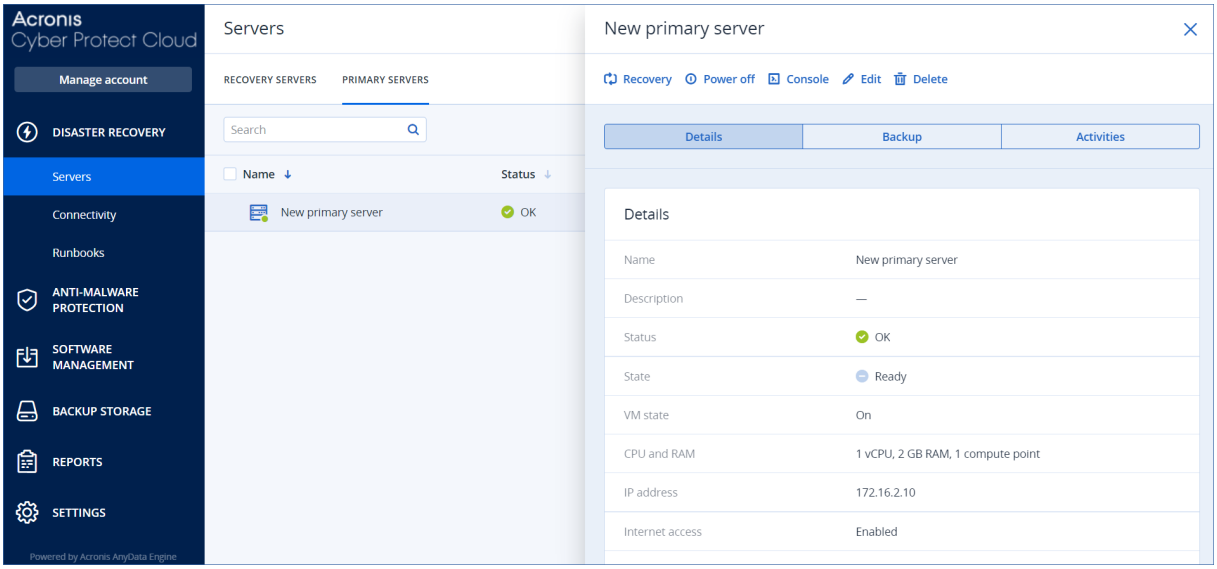
10. [Opcional] Marque la casilla de verificación de **acceso a Internet**.
    De esta forma, el servidor principal tendrá acceso a Internet. De forma predeterminada, el puerto TCP 25 está abierto para las conexiones de salida a direcciones IP públicas.
11. [Opcional] Marque la casilla de verificación **Usar dirección IP pública**.
    El hecho de que el servidor principal cuente con una dirección IP pública conlleva que se pueda acceder a él desde Internet. Si deja la casilla de verificación desmarcada, el servidor solo estará disponible en su red de producción.
    La dirección IP pública se 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.

12. [Opcional] Seleccione **Establecer el umbral de RPO**.
    El umbral de RPO determina el intervalo temporal máximo permitido entre el último punto de recuperación y el momento presente. El valor se puede establecer entre 15 y 60 minutos, 1 y 24 horas y 1 y 14 días.
13. Defina el nombre del servidor principal.

14. [Opcional] Especifique una descripción para el servidor principal.
15. [Opcional] Haga clic en la pestaña **Reglas de cortafuegos de la nube** para editar las reglas de cortafuegos predeterminadas. Para obtener más información, consulte "Configuración de reglas de cortafuegos para servidores en la nube" (p. 89).
16. Haga clic en **Crear**.

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



Operaciones con un servidor principal

El servidor principal aparece en la pestaña **Recuperación ante desastres** > **Servidores** > **Servidores principales** de la consola de Cyber Protect.

Para iniciar o detener el servidor, haga clic en **Encender** o **Apagar** en el panel del servidor principal.

Para editar la configuración del servidor principal, deténgalo y haga clic en **Editar**.

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

Gestión de servidores en el cloud

Para gestionar servidores en el cloud, vaya a **Recuperación ante desastres** > **Servidores**. Allí encontrará dos pestañas: **Servidores de recuperación** y **Servidores principales**. Para mostrar todas las columnas opcionales en 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.

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 **Recuperación ante desastres** > **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:

Parámetro de cortafuegos	Descripción
	• 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:

Parámetro de cortafuegos	Descripción
	• 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.

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 de firewall 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.

Realización de copias de seguridad de servidores en la cloud

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.

Organización (runbooks)

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

Un runbook es un conjunto de instrucciones que describen cómo iniciar el entorno de producción en la nube. Puede crear runbooks en la consola de Cyber Protect. Para acceder a la pantalla **Runbooks**, seleccione **Recuperación ante desastres** > **Runbooks**.

¿Por qué usar runbooks?

Con los runbooks, puede:

- Automatizar una 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.

Creación de un runbook

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

Puede seguir las instrucciones siguientes o ver el tutorial en vídeo.

Para crear un runbook

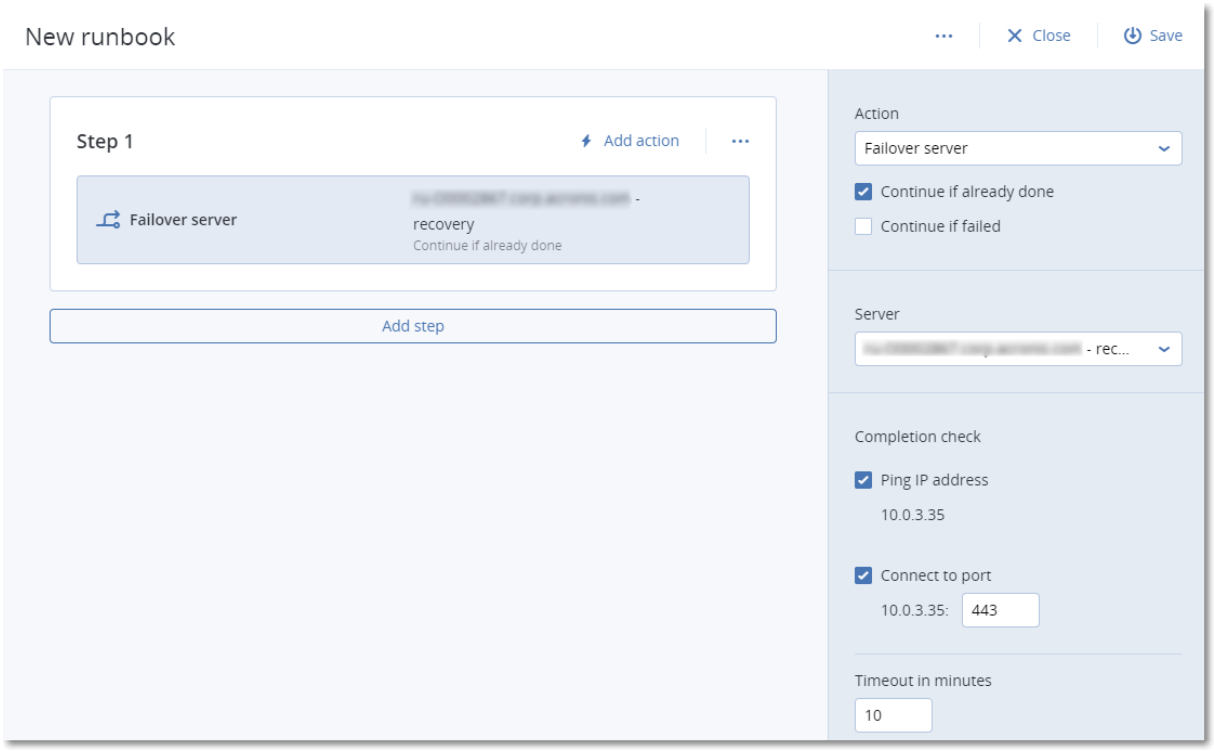
1. En la consola de Cyber Protection, vaya a **Recuperación ante desastres** > **Runbooks**.
2. Haga clic en **Crear runbook**.
3. Haga clic en **Añadir paso**.
4. Haga clic en **Añadir acción** y seleccione la acción que quiere añadir al paso.

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. 97).

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 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. 97). **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 **Recuperación ante desastres** > **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. 97). **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. 97). **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. 97).
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

Parámetro de runbook	Categoría	Disponible para actuar	Descripción
			falla. 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.

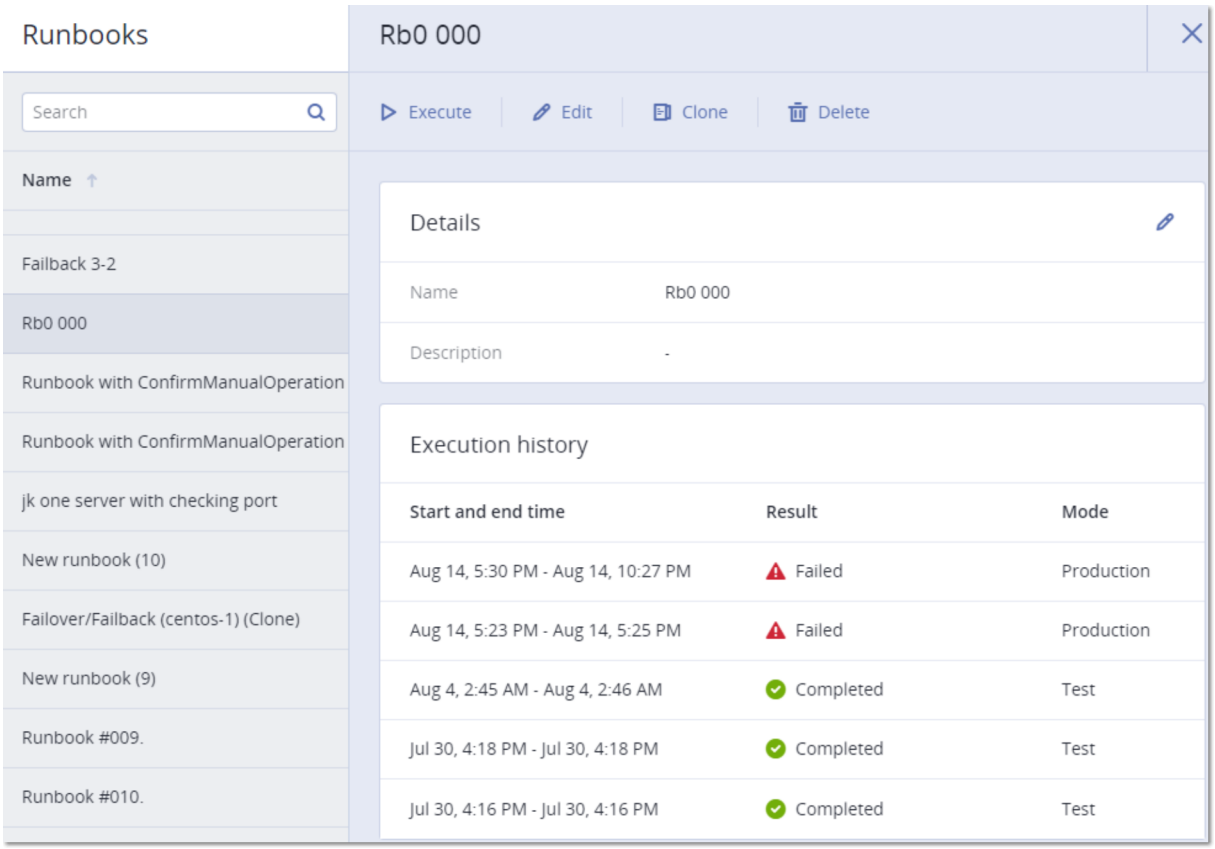
- **Modo conmutación por error y conmutación por recuperación**
  Elija si quiere ejecutar una conmutación por error de prueba (opción predeterminada) o una real (producción). El modo de conmutación por recuperación se corresponderá con el modo de conmutación por error elegido.
- **Punto de recuperación 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.


Runbooks
Search
Name
Failback 3-2
Rb0 000
Runbook with ConfirmManualOperation
Runbook with ConfirmManualOperation
jk one server with checking port
New runbook (10)
Failover/Failback (centos-1) (Clone)
New runbook (9)
Runbook #009.
Runbook #010.
Rb0 000
Execute
Edit
Clone
Delete
Details
Name
Rb0 000
Description
-
Execution history
Start and end time
Result
Mode
Aug 14, 5:30 PM - Aug 14, 10:27 PM
Failed
Production
Aug 14, 5:23 PM - Aug 14, 5:25 PM
Failed
Production
Aug 4, 2:45 AM - Aug 4, 2:46 AM
Completed
Test
Jul 30, 4:18 PM - Jul 30, 4:18 PM
Completed
Test
Jul 30, 4:16 PM - Jul 30, 4:16 PM
Completed
Test

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 realizar una conmutación por error (ejecutar la máquina virtual de 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.

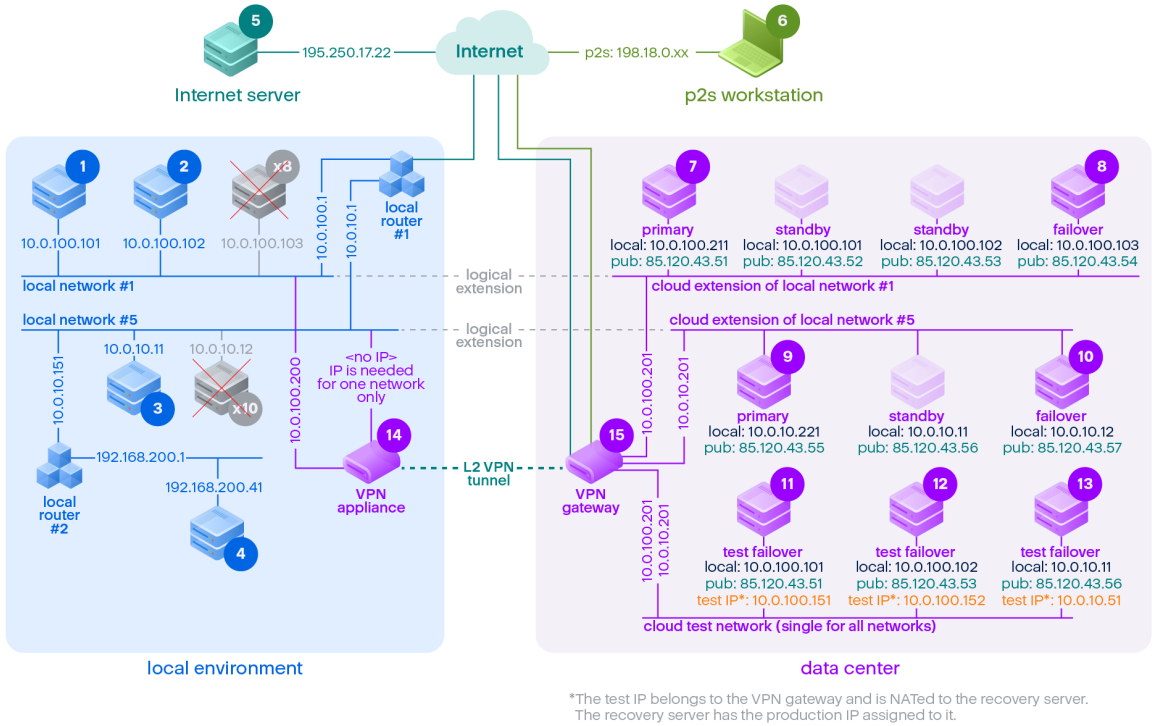
Para acceder a un servidor de prueba desde su sitio local, tiene que usar la **Dirección IP de prueba**.

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 la recuperación ante desastres:
   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 la recuperación ante desastres (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 la recuperación ante desastres.
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