# Cyber Disaster Recovery Cloud

24.03

Guía de inicio rápido

REVISIÓN:11/04/2024

# Contenido

# Cómo configurar Cyber Disaster Recovery Cloud en su equipo con Hyper-V

No necesita ser propietario de un servidor para probar la funcionalidad principal de Cyber Disaster Recovery Cloud. Puede configurar con facilidad el servicio de Cyber Disaster Recovery Cloud en su PC y evaluar sus funciones.

Requisitos previos:

- Tiene una cuenta de administrador de clientes en Cyber Protect Cloud.
- El sistema operativo instalado en su equipo debe ser Windows 10 Pro, Windows 10 Enterprise o Windows 10 Education.

Puede implementar el servicio de Cyber Disaster Recovery Cloud en su equipo, siga estas instrucciones:

1. Active Hyper-V en su equipo.
2. Cree un equipo virtual para usar como equipo de origen para las pruebas.
3. Implemente el dispositivo VPN en su equipo.

## Paso 1. Active el servicio Hyper-V en su equipo y prepare la imagen de SO.

1. Active el servicio Hyper-V en su equipo y siga las instrucciones que se detallan en el sitio web de Microsoft.
2. Descargue la imagen de SO para instalar en el equipo virtual. Por ejemplo, descargue ubuntu-18.04.2-desktop-amd64.iso del sitio web oficial de Ubuntu.

## Paso 2. Cree un equipo virtual que será su equipo de origen del que se realizará una copia de seguridad.

1. Abra Hyper-V Manager y cree un equipo virtual del que a continuación creará una copia de seguridad y que usará para probar el servicio Cyber Disaster Recovery Cloud:
   a. Haga clic derecho en su servidor y seleccione **Nuevo** > **Equipo virtual**. Siga los pasos del asistente, teniendo en cuenta que la **Memoria inicial** debe ser de al menos 4096 MB y que la **Conexión** debe ser el **Conmutador predeterminado**.
   b. Ejecute el equipo virtual recién creado, conéctese a él e inicie la instalación del SO.
2. Instale que la gente de protección en el equipo virtual recién creado:
   a. Abra un navegador en su equipo virtual.
   b. Inicie sesión en la consola de Cyber Protect como administrador de clientes.

c. En la sección **Dispositivos**, añada el equipo virtual al hacer clic en **Añadir** y seleccione el agente de protección para un servidor de Linux. Como resultado, el agente de protección se descarga en su equipo virtual.
d. Abra la consola e instale primero los paquetes adicionales. Utilice el siguiente comando:

```
sudo apt-get install rpm gcc make -y
```

a. Abra la carpeta de **Descargas**, cambie los permisos del archivo de instalación del agente de protección para que sea ejecutable y ejecute este archivo.

```
cd Descargas
```

```
sudo chmod +x Cyber_Protection_Agent_for_Linux_x86_64.bin
```

```
sudo ./Cyber_Protection_Agent_for_Linux_x86_64.bin
```

a. Siga los pasos del asistente de instalación. En el último paso, seleccione **Mostrar información de registro**. Verá el enlace que deberá abrir en el navegador y el código de registro que se deberá especificar al registrar el equipo en la consola de Cyber Protect.
b. Como resultado, el equipo virtual quedará registrado en la consola de Cyber Protect. Cree el plan de protección y la copia de seguridad del equipo al completo. Esta copia de seguridad se utilizará para crear un servidor de copias de seguridad más adelante.

## Paso 3. Implemente el dispositivo VPN en su equipo.

Para implementar el dispositivo VPN en su equipo, siga estas instrucciones:

1. En su equipo, inicie sesión en la consola de Cyber Protect como administrador de clientes.
2. Vaya a **Recuperación ante desastres** > **Conectividad** y haga clic en **Configurar**. Se abrirá el asistente de configuración de conectividad.
3. Seleccione **Conexión de sitio a sitio** y haga clic en **Iniciar**.
   El sistema empieza a implementar la puerta de enlace de conectividad en el cloud. Este proceso tardará cierto tiempo. mientras tanto, puede continuar con el siguiente paso.
4. Haga clic en **Descargar e implementar**. Descargue el archivo comprimido con el dispositivo VPN para Hyper-V (archivo .vhd), descomprímalo e impleméntelo en su entorno local:
   a. Abra Hyper-V Manager, haga clic derecho en su servidor y seleccione **Nuevo** > **Equipo virtual**.
   b. Especifique un nombre descriptivo para el equipo virtual (por ejemplo, equipo virtual de dispositivo VPN).
   c. Siga los pasos del asistente, teniendo en cuenta que la **Conexión** debe establecerse como **Conmutador predeterminado**.
   d. En el paso **Conectar disco rígido virtual**, seleccione la opción **Usar un disco rígido virtual**

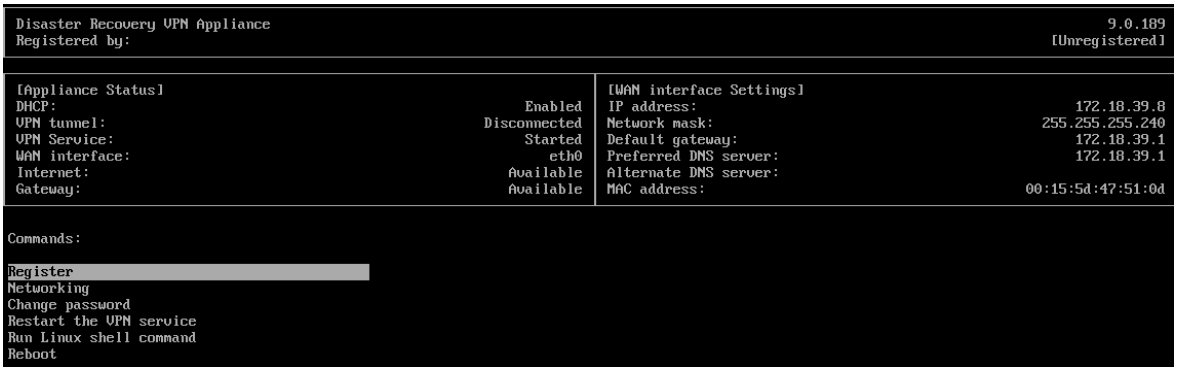
**existente**. Seleccione el archivo de dispositivo VPN descargado.

e. Complete la creación del equipo virtual.

5. Conecte el dispositivo a las redes de producción.
6. Ejecute el equipo virtual del dispositivo VPN y conéctese a él.
7. En cuanto el dispositivo arranque y aparezca la solicitud de inicio de sesión, inicie sesión en el dispositivo con las siguientes credenciales:

   **Información de inicio de sesión**: admin

   **Contraseña**: admin
8. Verá una página de inicio similar a la siguiente:

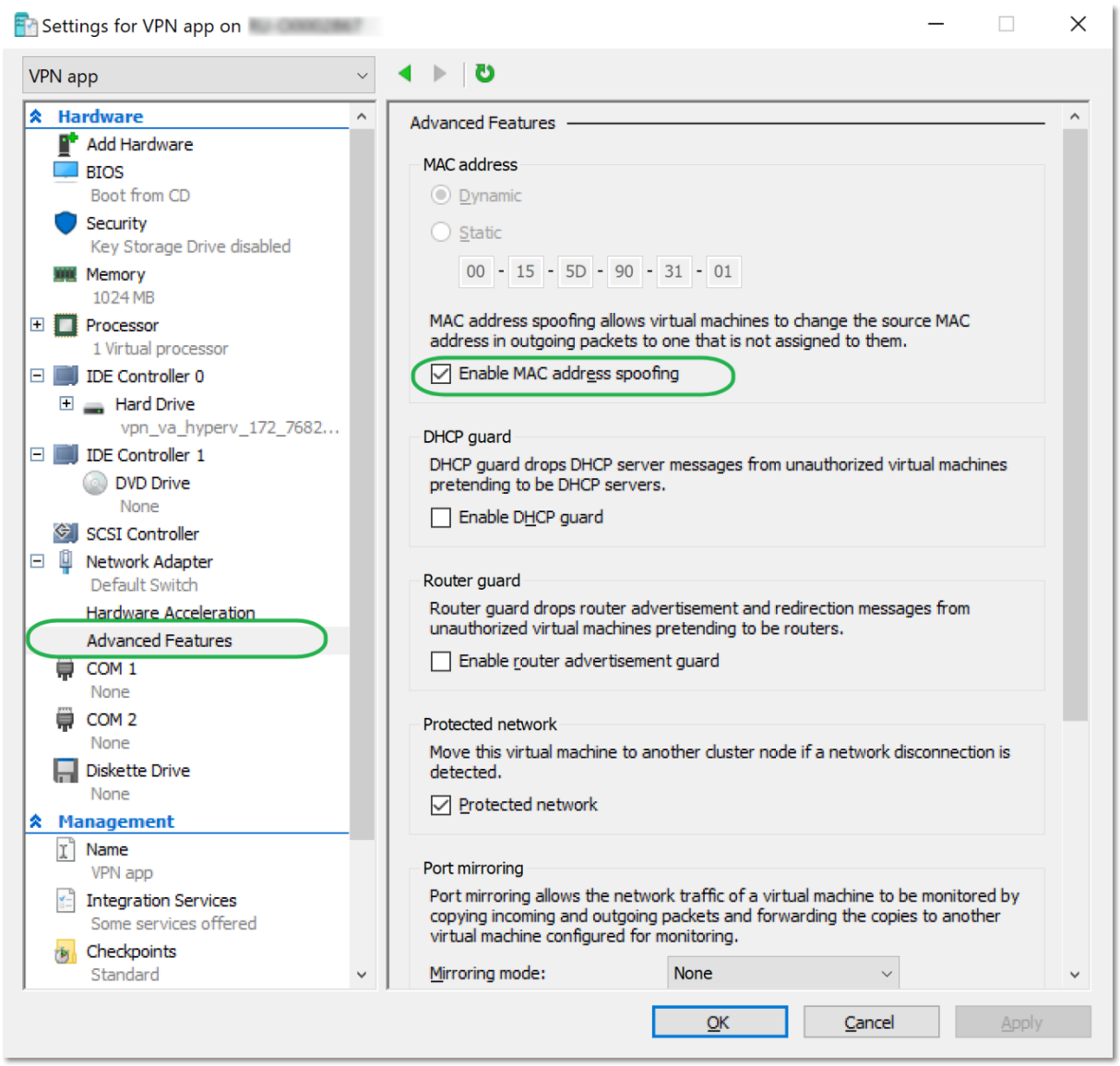



   Asegúrese de que la configuración de **Dirección IP**, **Entrada por defecto** y **Servidor DNS preferido** esté correctamente establecida. Tenga en cuenta que la configuración de **Internet** y **Puerta de enlace** que se encuentra a la izquierda de la tabla debe estar **Disponible** para que el dispositivo se pueda registrar correctamente. De no ser así, compruebe la configuración de la puerta de enlace predeterminada y de la disponibilidad de DNS antes de continuar con el registro, o bien configure manualmente la dirección IP.
9. Seleccione **Registro** en el menú y haga clic en **Introducir**.
10. Se le solicitará que introduzca la dirección URL del servicio Cyber Protection. Introduzca la misma dirección URL que está usando para acceder a la consola de Cyber Protect.


11. Especifique sus credenciales de administrador de clientes para la consola de Cyber Protect.

**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 sobre la autenticación de doble factor, consulte la **Guía del administrador del cliente**.

12. Pulse **S** para confirmar la configuración y comience el proceso de registro.
13. Tras registrarse correctamente, verá su dispositivo VPN en la consola de Cyber Protect.
14. Habilite el modo promiscuous para asegurarse de que se habilita correctamente la funcionalidad de replicación de red:
    a. Abra Hyper-V Manager.
    b. Haga clic derecho en el equipo virtual de su dispositivo VPN y seleccione **Configuración**.
    c. En la sección **Adaptador de red** > **Funciones avanzadas**, seleccione la opción **Habilitar el redireccionamiento de la dirección MAC**.




Ha configurado una conexión VPN de sitio a sitio segura entre su sitio local y su sitio de recuperación en el cloud. Ahora puede crear un servidor de recuperación para su equipo local y comprobar cómo funcionan la conmutación por error y la conmutación por recuperación. Para obtener más información, consulte la **Guía del administrador de Cyber Disaster Recovery Cloud**.