


Recuperación en la nube

Kit "Hazlo tú mismo"



Esta guía te permitirá configurar la recuperación ante desastres para máquinas virtuales de VMware locales con Windows en Azure.

Temas incluidos:

1. La nube está cambiando los negocios
2. Configuración de permisos de cuenta de VMware
3. Especificación de lo que se va a replicar
4. Configuración del entorno de origen
5. Descarga de la instalación unificada de Site Recovery
6. Configuración del servidor de configuración
7. Configuración de la detección automática
8. Configuración del entorno de destino
9. Creación de una directiva de replicación
10. Habilitar replicación

1. La nube está cambiando los negocios

Estas cifras ilustran cómo la nube pública está cambiando el mundo de IT y cómo los proveedores de servicios se encuentran en una posición única de capitalizar estas



70%

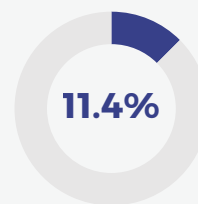
Del total de ingresos provienen de servicios administrados, servicios de seguridad y aplicaciones de "hosting".

- Aplicaciones de hosting
- Servicios administrados
- Servicios de Seguridad
- Infraestructura de Hosting

Este es un cambio respecto a los años anteriores. Los proveedores de servicios están tomando ventaja de este modelo y cada vez más buscan alejarse de ofertas de productos básicos ("commodity") para ir hacia una oferta de valor único

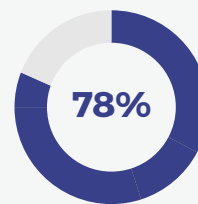
Los proveedores de servicios están respondiendo con ofertas orientadas a nube.

Más y más pequeñas y medianas empresas se están moviendo a la nube y están buscando ayuda en este camino a la nube:



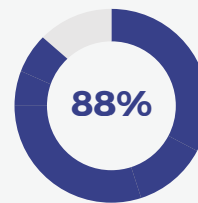
11.4%

Es la tasa de crecimiento anual compuesto (CAGR) del mercado de servicios de nube entre 2015- 2018.



78%

De las pequeñas y medianas empresas (Pyme) a nivel global estarán usando hasta 2020.



88%

De Pymes están considerando usar al menos 1 aplicación de nube en los próximos 2-3 años.

2. Configuración de permisos de cuenta de VMware

1. Cree un rol en el nivel de vCenter. Asigne el nombre **Azure_Site_Recovery** al rol.
2. Asigne los permisos siguientes al rol **Azure_Site_Recovery**.

Task	Rol o permisos	Detalles
Detección de máquina virtual	Objeto de centro de datos -> Propagar al objeto secundario, rol = solo lectura	Al menos un usuario de solo lectura. El usuario se asigna en el nivel de centro de datos y tiene acceso a todos los objetos de este. Para restringir el acceso, asigne el rol Sin acceso con Propagate to child object (Propagar a objeto secundario) a los objetos secundarios (hosts de vSphere, almacenes de datos, máquinas virtuales y redes).
Replicación completa, conmutación por error, conmutación por recuperación	Objeto de centro de datos -> Propagar a objeto secundario, rol = Azure_Site_Recovery Almacén de datos -> Asignar espacio, examinar almacén de datos, operaciones de archivo de bajo nivel, quitar archivo, actualizar archivos de máquina virtual Red -> Asignación de red Recursos -> Asignar máquina virtual al grupo de recursos, migrar apagado de máquina virtual, migrar máquinas virtuales encendidas Tareas -> Crear tarea, actualizar tarea Máquina virtual -> Configuración Máquina virtual -> Interactuar -> Responder a pregunta, conexión de dispositivos, configurar soporte de CD, Configurar soporte de disquete, apagar, encender, instalación de herramientas de VMware Máquina virtual -> Inventario -> Crear, registrar, anular registro Máquina virtual -> Aprovisionamiento -> Permitir descarga de máquina virtual, permitir carga de archivos de máquina virtual Máquina virtual -> Instantáneas -> Quitar instantáneas	El usuario se asigna en el nivel de centro de datos y tiene acceso a todos los objetos de este. Para restringir el acceso, asigne el rol Sin acceso con Propagate to child object (Propagar a objeto secundario) a los objetos secundarios (hosts de vSphere, almacenes de datos, máquinas virtuales y redes).

3. Cree un usuario en el servidor vCenter o el host de vSphere. Asigne el rol al usuario.

3. Especificación de lo que se va a replicar

Mobility Service debe instalarse en cada máquina que quiera replicar. Site Recovery instala este servicio automáticamente cuando se habilita la replicación para la máquina virtual. Para la instalación automática, debe preparar una cuenta que Site Recovery vaya a usar para acceder a la máquina virtual.

Puede usar una cuenta local o de dominio. En el caso de las máquinas virtuales Linux, debe ser la cuenta raíz en el servidor Linux de origen. En el caso de las máquinas virtuales de Windows, si no usa una cuenta de dominio, deshabilite el control de acceso de usuarios remotos en el equipo local:

En el Registro, en `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`, agregue la entrada `DWORD LocalAccountTokenFilterPolicy` y establezca el valor en 1.

4. Configuración del entorno de origen

La configuración del entorno de origen consiste en descargar la instalación unificada de Site Recovery, configurar el servidor de configuración y registrarlo en el almacén y detectar las máquinas virtuales.

El servidor de configuración es una sola máquina virtual de VMware local para hospedar todos los componentes de Site Recovery. Esta máquina virtual ejecuta el servidor de configuración, el servidor de procesos y el servidor de destino maestro.

- El servidor de configuración coordina la comunicación entre el entorno local y Azure, además de administrar la replicación de datos.
- El servidor de procesos actúa como puerta de enlace de replicación. Recibe datos de replicación, los optimiza con almacenamiento en caché, compresión y cifrado y los envía al almacenamiento de Azure. El servidor de procesos también instala Mobility Service en las máquinas virtuales que quiere replicar, además de realizar la detección automática de máquinas virtuales en servidores de VMware locales.
- El servidor de destino maestro controla los datos de replicación durante la conmutación por recuperación desde Azure.

La máquina virtual del servidor de configuración debe ser una máquina virtual de VMware de alta disponibilidad que cumpla los requisitos siguientes:

Requisito	Detalles
Número de núcleos de la CPU	8
RAM	12 GB
Número de discos	3: disco del sistema operativo, disco de memoria caché del servidor de procesos, unidad de retención (para la conmutación por recuperación)
Espacio libre en el disco (caché del servidor de procesos)	600 GB
Espacio libre en el disco (disco de retención)	600 GB
Versión del sistema operativo	Windows Server 2012 R2
Configuración regional del sistema operativo	Español (es-es)
Versión de VMware vSphere PowerCLI	PowerCLI 6.0
Roles de Windows Server	No habilite estos roles: Active Directory Domain Services, Internet Information Services, Hyper-V
Tipo de NIC	VMXNET3
Tipo de dirección IP	estática
Puertos	443 (orquestración del canal de control) 9443 (Transporte de datos)

En la máquina virtual del servidor de configuración, asegúrese de que el reloj del sistema esté sincronizado con un servidor horario. La hora debe estar sincronizada en 15 minutos. Si la diferencia horaria es superior a 15 minutos, se produce un error de instalación.

Asegúrese de que la máquina virtual del servidor de configuración pueda acceder a estas direcciones URL:

- .accesscontrol.windows.net. Se utiliza para la administración de identidades y de control de acceso.
- .backup.windowsazure.com. Se usa para la transferencia de datos de replicación y coordinación.
- .blob.core.windows.net. Se usa para tener acceso a la cuenta de almacenamiento que almacena los datos replicados.
- .hypervrecoverymanager.windowsazure.com. Se usa para las operaciones de administración de replicación y coordinación.
- time.nist.gov y time.windows.com. Se usan para comprobar la sincronización de la hora entre el sistema y la hora global.

Direcciones URL para Azure Government Cloud:

- .ugv.hypervrecoverymanager.windowsazure.us
- .ugv.backup.windowsazure.us
- .ugi.hypervrecoverymanager.windowsazure.us
- .ugi.backup.windowsazure.us

Las reglas de firewall basadas en direcciones IP deben permitir la comunicación con los intervalos IP del centro de datos de Azure y los puertos 443 (HTTPS) y 9443 (replicación de datos). Asegúrese de permitir los intervalos de direcciones IP correspondientes a la región de Azure de la suscripción y de Oeste de EE. UU. (se usan para el control de acceso y la administración de identidades).

5. Descarga de la instalación unificada de Site Recovery

1. Abra Azure Portal y haga clic en **Todos los recursos**.
2. Haga clic en el almacén de Recovery Service denominado **ContosoVMVault**.
3. Haga clic en **Site Recovery > Preparar infraestructura > Objetivo de protección**.
4. Seleccione **Local** como ubicación de los equipos, To Azure (En Azure) como ubicación en la que replicar los equipos y **Yes, with VMware vSphere Hypervisor** (Sí, con VMware vSphere Hypervisor). A continuación, haga clic en **Aceptar**.
5. En el panel Preparar origen, haga clic en **+Servidor de configuración**.
6. En **Agregar servidor**, compruebe que aparezca **Servidor de configuración** en **Tipo de servidor**.

7. Descargue el archivo de instalación unificada de Site Recovery.
8. Descargue la clave de registro del almacén. Se le solicitará cuando ejecute la instalación unificada. La clave será válida durante cinco días a partir del momento en que se genera.

The screenshot displays three panels from the Azure Site Recovery console, all titled 'ContosoVMVault'.

- Prepare infrastructure:** Shows a progress list with five steps: 1. Protection goal (VMware VMs/physical servers t...), 2. Source Prepare (highlighted), 3. Target Prepare, 4. Replication settings Prepare, and 5. Deployment planning Select. An 'OK' button is at the bottom.
- Prepare source:** Shows two tabs: 'Configuration Server' (active) and 'vCenter'. Under 'Step 1: Select Configuration Server', it indicates '(0 servers found)' and provides instructions to click the '+Configuration Server' button. 'Step 2: Select vCenter server/vSphere host' is also visible. An 'OK' button is at the bottom.
- Add Server:** Shows a 'Server type' dropdown set to 'Configuration Server'. An information box states: 'Adding Configuration Server may take 15 minutes to 30 minutes'. Below, it says 'Register your Configuration Server On-premises' and lists six steps: 1. Make sure server on which you plan to set up the Configuration Server is running Windows Server 2012 R2 virtual machine; 2. Configure Proxy so that server can access the Service URLs; 3. Download the Microsoft Azure Site Recovery Unified Setup; 4. Download the vault registration key (with a 'Download' button); 5. Run the installer to set up the Configuration Server and Process Server and use the vault registration key to register it with the vault. (with a 'Learn more' link); 6. Run cspconfigtool.exe to create one or more management accounts on the configuration server.

6. Configuración del servidor de configuración

1. Ejecute el archivo de instalación unificada.

2. En **Before You Begin** (Antes de comenzar), seleccione **Install the configuration server and process server** (Instalar el servidor de configuración y el servidor de procesos) y luego haga clic en **Siguiente**.

3. En **Third-Party Software License** (Licencia de software de terceros), haga clic en Acepto para descargar e instalar MySQL y luego haga clic en **Siguiente**.

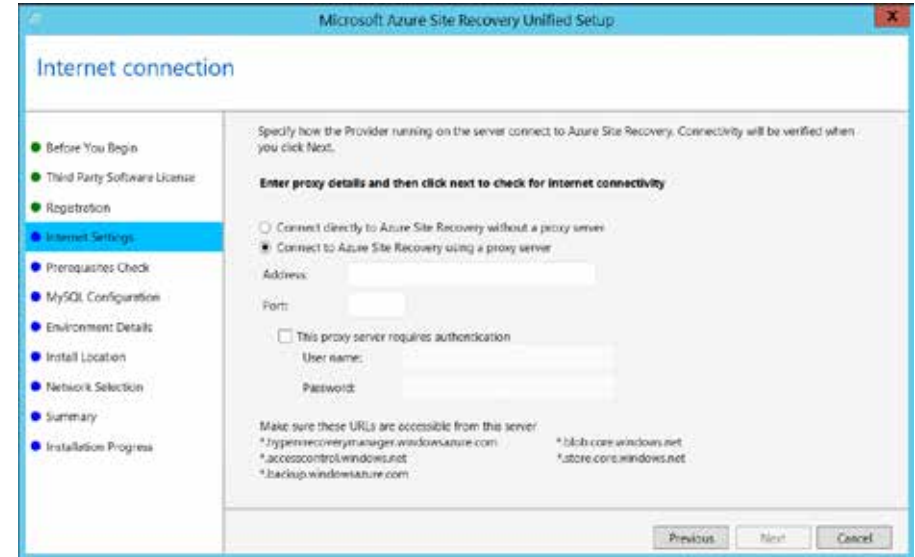
4. En **Registro**, seleccione la clave de registro que descargó del almacén.

5. En **Configuración de Internet**, especifique cómo se conecta el proveedor que se ejecuta en el servidor de configuración a Azure Site Recovery a través de Internet.

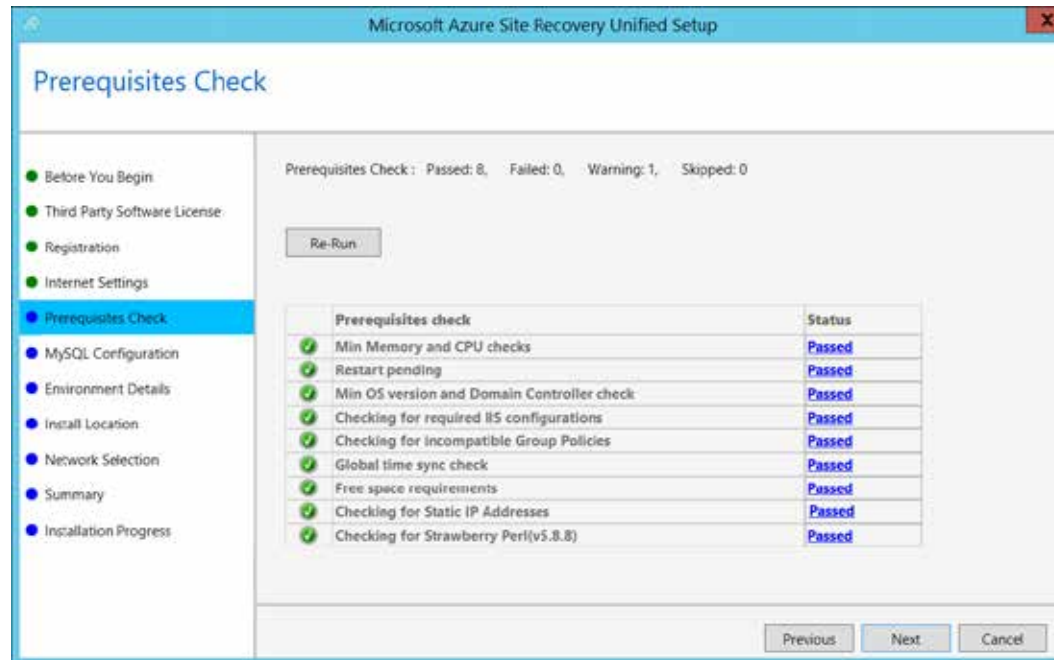
- Si quiere conectarse con el proxy configurado actualmente en la máquina, seleccione **Conectar con Azure Site Recovery con un servidor proxy**.

- Si quiere que el proveedor se conecte directamente, seleccione **Conectar directamente con Azure Site Recovery sin un servidor proxy**.

- Si el proxy existente requiere autenticación, o si quiere usar un proxy personalizado para la conexión del proveedor, seleccione **Connect with custom proxy settings** (Conectarse con una configuración de proxy personalizada) y especifique la dirección, el puerto y las credenciales.



6. En **Comprobación de requisitos previos**, el programa de instalación ejecuta una comprobación para asegurarse de que se pueda ejecutar la instalación. Si aparece una advertencia sobre la **comprobación de la sincronización de hora global**, compruebe que la hora del reloj del sistema (configuración de **fecha y hora**) es la misma que la de la zona horaria.



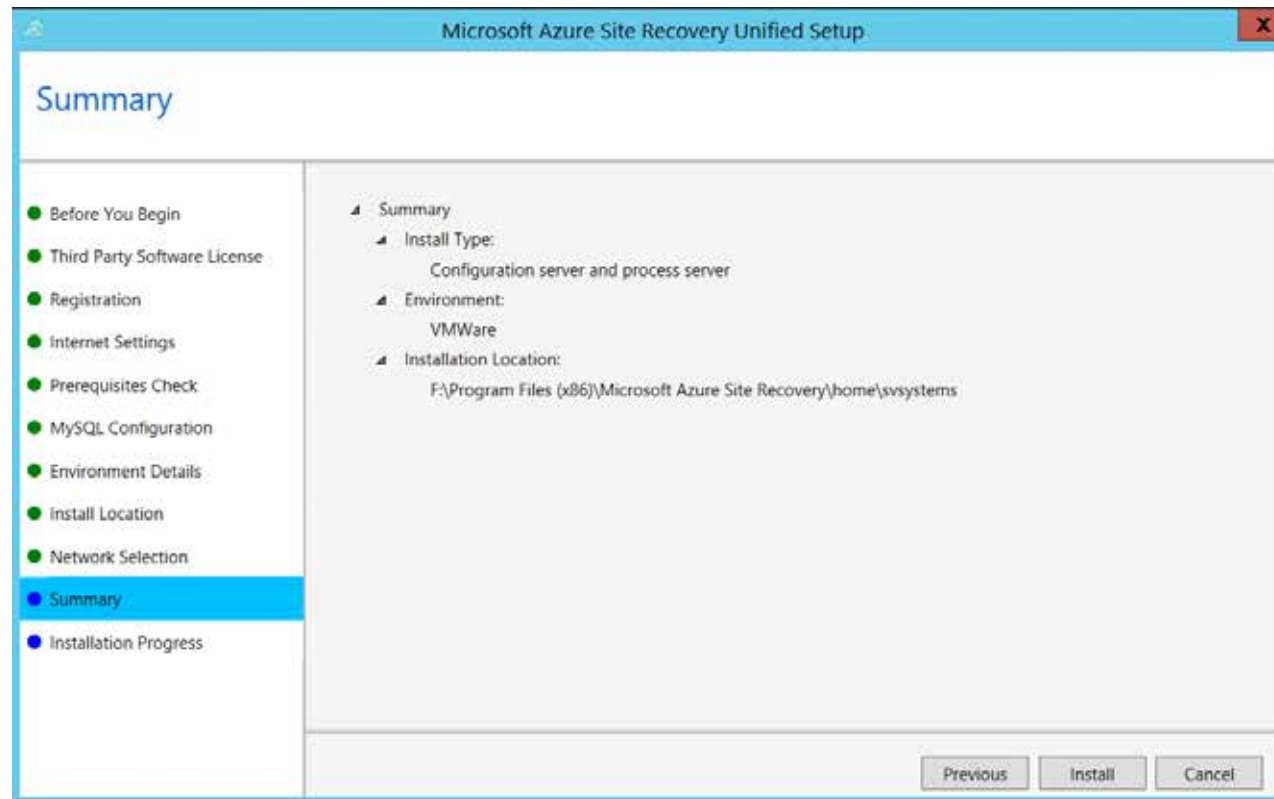
7. En **MySQL Configuration** (Configuración de MySQL), cree credenciales para iniciar sesión en la instancia de servidor MySQL que se va a instalar.

8. En **Detalles del entorno**, seleccione Sí para proteger las máquinas virtuales de VMware. El programa de instalación comprueba que PowerCLI 6.0 esté instalado.

9. En **Ubicación de instalación**, seleccione dónde quiere instalar los archivos binarios y almacenar la memoria caché. La unidad que seleccione debe tener al menos 5 GB de espacio disponible en disco, pero se recomienda usar una unidad de memoria caché con 600 GB o más de espacio libre.

10. En **Selección de red**, especifique el agente de escucha (adaptador de red y puerto SSL) en el que el servidor de configuración enviará y recibirá los datos de replicación. El puerto 9443 es el que se usa de forma predeterminada para enviar y recibir el tráfico de replicación, pero puede modificar este número de puerto para adecuarlo a los requisitos de su entorno. También se abre el puerto 443, que se usa para coordinar las operaciones de replicación. No use el puerto 443 para enviar o recibir tráfico de replicación.

11. En **Resumen**, revise la información y haga clic en **Instalar**. El programa de instalación instala el servidor de configuración y con él registra el servicio Azure Site Recovery.



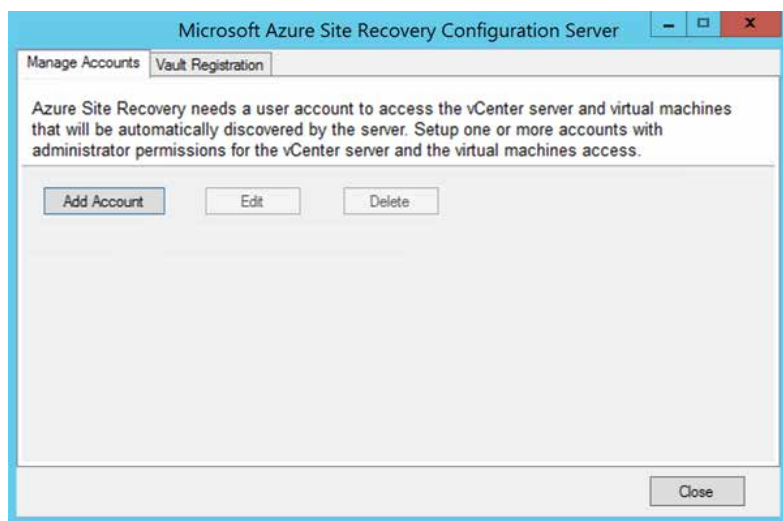
Se genera una frase de contraseña cuando finaliza la instalación. La necesitará al habilitar la replicación, así que cópiela y manténgala en una ubicación segura. El servidor se muestra en el panel **Configuración > Servidores** del almacén.

7. Configuración de la detección automática

Para detectar máquinas virtuales, el servidor de configuración tiene que conectarse a servidores de VMware locales. Para los fines de este tutorial, agregue el servidor vCenter, o hosts de vSphere, con una cuenta que tenga privilegios de administrador en el servidor.

1. En el servidor de configuración, inicie **CSPSConfigtool.exe**. Esta herramienta está disponible como acceso directo en el escritorio y se encuentra en la carpeta ubicación de instalación\home\svsystems\bin.

2. Haga clic en **Administrar cuentas > Agregar cuenta**.



En Detalles de la cuenta, agregue la cuenta que se utilizará para la detección automática.



Para agregar un servidor:

1. Abra Azure Portal y haga clic en **Todos los recursos**.
2. Haga clic en el almacén de Recovery Service denominado **Contoso-VMVault**.
3. Haga clic en Site **Recovery > Preparar infraestructura > Origen**.
4. Seleccione **+vCenter** para conectarse a un servidor vCenter o un host ESXi de vSphere.
5. En **Agregar servidor vCenter**, especifique un nombre descriptivo para el servidor. Luego, especifique la dirección IP o FQDN.
6. Deje el puerto establecido en 443, a menos que los servidores de VMware escuchen las solicitudes en otro puerto.
7. Seleccione la cuenta que se va a usar para conectarse al servidor. Haga clic en **Aceptar**.

Site Recovery se conecta a los servidores de VMware con la configuración especificada y detecta máquinas virtuales.

Nota: El nombre de la cuenta podría tardar 15 minutos o más en aparecer en el portal. Para que se actualice inmediatamente, haga clic en Servidores de configuración > nombre de servidor > Actualizar servidor.

8. Configuración del entorno de destino

Seleccione y compruebe los recursos de destino.

1. Haga clic en **Preparar infraestructura > Destino** y seleccione la suscripción de Azure que quiere usar.
2. Especifique si el modelo de implementación de destino está basado en Resource Manager o si es el clásico.
3. Site Recovery comprueba que tiene una o más cuentas de almacenamiento y redes compatibles.

Target
CostoDR - PREVIEW

+ Storage account + Network

✓ Step 1 : Select Azure subscription

* Subscription ⓘ
ASR Canary Test Subscription 3

* Select the deployment model used after failover ⓘ
Resource Manager

✓ Step 2 : Ensure that at least one compatible Azure storage account exist

Storage account(s) ⓘ
Found 30 compatible Azure storage accounts out of 50 available in the subscription

✓ Step 3 : Ensure that at least one compatible Azure virtual network exist

Network(s) ⓘ
Found 4 compatible Azure virtual networks out of 6 available in the subscription

OK

9. Creación de una directiva de replicación

Create replication policy
ContosoVMVault

* Name ⓘ
VMwareRepPolicy ✓

Source type ⓘ
VMware / Physical machines ▼


Target type ⓘ
Azure ▼

* RPO threshold in mins ⓘ
60

* Recovery point retention in hours ⓘ
24

* App-consistent snapshot frequency in mins ⓘ
60

Failback replication policy name ⓘ
VMwareRepPolicy-failback

 A replication policy for failback from Azure to on-premises will be automatically created with the same settings.

OK

1. Abra Azure Portal y haga clic en **Todos los recursos**.
2. Haga clic en el almacén de Recovery Service denominado **ContosoVMVault**.
3. Para crear una directiva de replicación, haga clic en **Infraestructura de Site Recovery > Directivas de replicación > +Directiva de replicación**.
4. En **Crear la directiva de replicación**, especifique un nombre de directiva **VMwareRepPolicy**.
5. En **Umbral de RPO**, use el valor predeterminado de 60 minutos. Este valor define la frecuencia de creación de puntos de recuperación. Se genera una alerta cuando la replicación continua supera este límite.
6. En **Retención de punto de recuperación**, use el valor predeterminado de 24 horas como duración del período de retención de cada punto de recuperación. En este tutorial se selecciona 72 horas. Las máquinas virtuales replicadas se pueden recuperar a cualquier momento de un período.
7. En **Frecuencia de instantánea coherente con la aplicación**, use el valor predeterminado de 60 minutos como frecuencia de creación de instantáneas coherentes con la aplicación. Haga clic en **Aceptar** para crear la directiva.

La directiva se asocia automáticamente al servidor de configuración. De forma predeterminada, se crea automáticamente una directiva correspondiente para la conmutación por recuperación. Por ejemplo, si la directiva de replicación es **rep-policy**, la directiva de conmutación por recuperación será **rep-policy-failback**. Esta directiva no se usa hasta que se inicie una conmutación por recuperación desde Azure.

10. Habilitar replicación

Site Recovery instala Mobility Service cuando se habilita la replicación para una máquina virtual. Los cambios pueden tardar 15 minutos o más en aplicarse y aparecer en el portal.

Habilite la replicación como se indica a continuación:

1. Haga clic en **Replicar la aplicación > Origen**.
2. En **Origen**, seleccione el servidor de configuración.
3. En **Tipo de máquina**, seleccione **Máquinas virtuales**.
4. En **vCenter/vSphere Hypervisor**, seleccione el servidor vCenter que administra el host de vSphere, o bien seleccione el host.
5. Seleccione el servidor de procesos (servidor de configuración). Luego haga clic en Aceptar.
6. En **Destino**, seleccione la suscripción y el grupo de recursos donde desee crear las máquinas virtuales conmutadas por error. Elija el modelo de implementación que desee usar en Azure (clásico o de Resource Manager) para las máquinas virtuales conmutadas por error.
7. Seleccione la cuenta de Azure Storage que desea usar para los datos de replicación.
8. Seleccione la red y la subred de Azure a la que se conectarán las máquinas virtuales de Azure cuando se creen después de la conmutación por error.

9. Seleccione la opción **Configurar ahora para las máquinas seleccionadas** con el fin de aplicar la configuración de red a todas las máquinas que seleccione para su protección. Seleccione **Configurar más tarde** para seleccionar la red de Azure por máquina.

10. En **Máquinas virtuales > Seleccionar máquinas virtuales**, haga clic en cada máquina que desea replicar y selecciónela. Solo puede seleccionar aquellas máquinas en las que se pueda habilitar la replicación, y, a continuación, haga clic en Aceptar.

11. En **Propiedades > Configurar propiedades**, seleccione la cuenta que va a usar el servidor de procesos para instalar automáticamente Mobility Service en el equipo.

12. En **Configuración de la replicación > Establecer configuración de replicación**, compruebe que se ha seleccionado la directiva de replicación correcta.

13. Haga clic en **Enable Replication**.

Puede hacer un seguimiento del progreso del trabajo **Habilitar protección en Configuración > Trabajos > Trabajos de Site Recovery**. La máquina estará preparada para la conmutación por error después de que finalice el trabajo **Finalizar la protección**.

Para supervisar las máquinas virtuales que agregue, puede comprobar la última hora de detección de máquinas virtuales en **Servidores de configuración**.

Último contacto. Para agregar máquinas virtuales sin esperar a la detección programada, resalte el servidor de configuración (no haga clic en él) y haga clic en Actualizar.



 **INTCOMEX**



Te llevamos + alto