Proteger cargas de trabajo en Azure/AVS

NetApp Solutions

NetApp
April 26, 2024

Tabla de contenidos

Proteger cargas de trabajo en Azure/AVS

Recuperación ante desastres con ANF y JetStream

La recuperación ante desastres en el cloud es un método resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos dañados por los datos (por ejemplo, ransomware). Gracias al marco de trabajo VAIO de VMware, las cargas de trabajo de VMware locales se pueden replicar en el almacenamiento Azure Blob y recuperarse, lo que permite una pérdida de datos mínima o casi nula, y el objetivo de tiempo de recuperación casi nulo.

JetStream DR se puede utilizar para recuperar sin problemas las cargas de trabajo replicadas de las instalaciones a AVS y específicamente a Azure NetApp Files. Permite una recuperación ante desastres rentable usando unos recursos mínimos en el sitio de recuperación ante desastres y un almacenamiento en cloud rentable. Jetstream DR automatiza la recuperación en almacenes de datos de ANF mediante el almacenamiento BLOB de Azure. JetStream DR recupera máquinas virtuales independientes o grupos de máquinas virtuales relacionadas en la infraestructura de sitio de recuperación según su asignación de red y proporciona recuperación de un momento específico para la protección de ransomware.

Este documento proporciona una comprensión de los principios de operaciones de JetStream DR y sus principales componentes.

Información general sobre la puesta en marcha de la

1. Instale el software JetStream DR en el centro de datos local.
   a. Descargue el paquete de software de recuperación ante desastres JetStream desde Azure Marketplace (ZIP) y ponga en marcha JetStream DR MSA (OVA) en el clúster designado.
   b. Configure el clúster con el paquete de filtro de E/S (instale JetStream VIB).
   c. Aprovisione Azure Blob (cuenta de almacenamiento de Azure) en la misma región que el clúster de recuperación ante desastres AVS.
   d. Ponga en marcha dispositivos DRVA y asigne volúmenes de registro de replicación (VMDK a partir de un almacén de datos existente o almacenamiento iSCSI compartido).
   e. Cree dominios protegidos (grupos de máquinas virtuales relacionadas) y asigne DRVAs y Azure Blob Storage/ANF.
   f. Inicie la protección.
2. Instalar el software de recuperación ante desastres JetStream en el cloud privado de Azure VMware Solution.
   a. Utilice el comando Run para instalar y configurar JetStream DR.
   b. Agregue el mismo contenedor de Azure Blob y descubra dominios mediante la opción Scan Domains.
   c. Implementar los dispositivos DRVA necesarios.
   d. Cree volúmenes de registros de replicación con almacenes de datos VSAN o ANF disponibles.
   e. Importe dominios protegidos y configure ROCvA (recuperación va) para utilizar el almacén de datos ANF en las ubicaciones de los equipos virtuales.
   f. Seleccione la opción de conmutación por error adecuada y inicie una rehidratación continua para dominios de objetivo de tiempo de recuperación casi cero o máquinas virtuales.
3. Durante un evento de desastre, active la conmutación por error en los almacenes de datos de Azure NetApp Files en el sitio de recuperación ante desastres AVS designado.
4. Invoque la conmutación por recuperación al sitio protegido después de haber recuperado el sitio protegido.antes de comenzar, asegúrese de que se cumplen los requisitos previos tal y como se indica en este "enlace" Además, ejecute Bandwidth Testing Tool (BWT) de JetStream Software para evaluar el rendimiento potencial del almacenamiento de Azure Blob y su ancho de banda de replicación cuando se utiliza con el software JetStream DR. Tras los requisitos previos, incluida la conectividad, se han establecido, se han establecido y se han suscrito a JetStream DR para AVS de la "Azure Marketplace". Después de descargar el paquete de software, continúe con el proceso de instalación descrito anteriormente.

Cuando planifique e inicie la protección de un gran número de equipos virtuales (por ejemplo, 100+), utilice la herramienta de planificación de capacidad (CPT) del kit de herramientas de automatización de recuperación ante desastres JetStream. Proporcionar una lista de equipos virtuales que se protegerán junto a sus preferencias de grupo de recuperación y tiempo de recuperación, y luego ejecutar CPT.

CPT realiza las siguientes funciones:

- Combinación de máquinas virtuales en dominios de protección según su objetivo de tiempo de recuperación.
- Definir el número óptimo de DRVAs y sus recursos.

- Calcular el ancho de banda de replicación requerido.
- Identificación de las características del volumen de registro de replicación (capacidad, ancho de banda, etc.).
- Calculando la capacidad de almacenamiento de objetos requerida, etc.

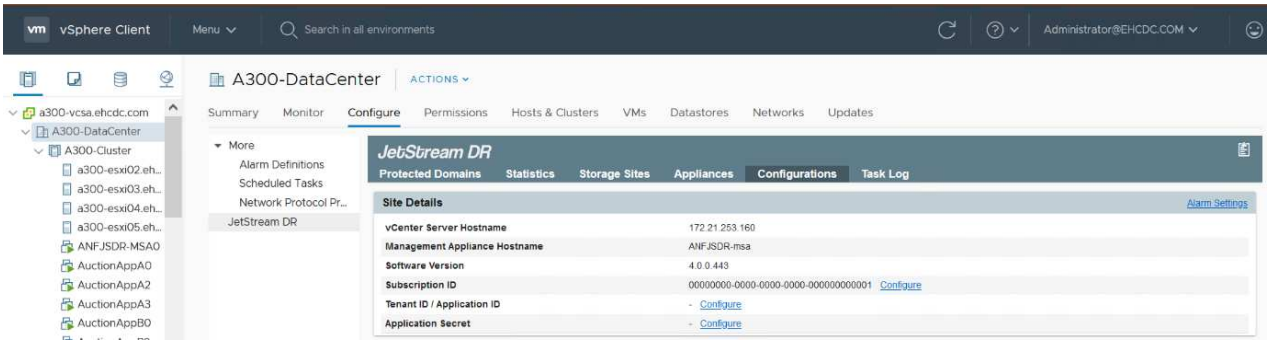
> La cantidad y el contenido de los dominios prescritos dependen de diversas características de los equipos virtuales, como la tasa media de IOPS, la capacidad total, la prioridad (que define el orden de conmutación por error), el objetivo de tiempo de recuperación, etc.

Instalar JetStream DR en el centro de datos local

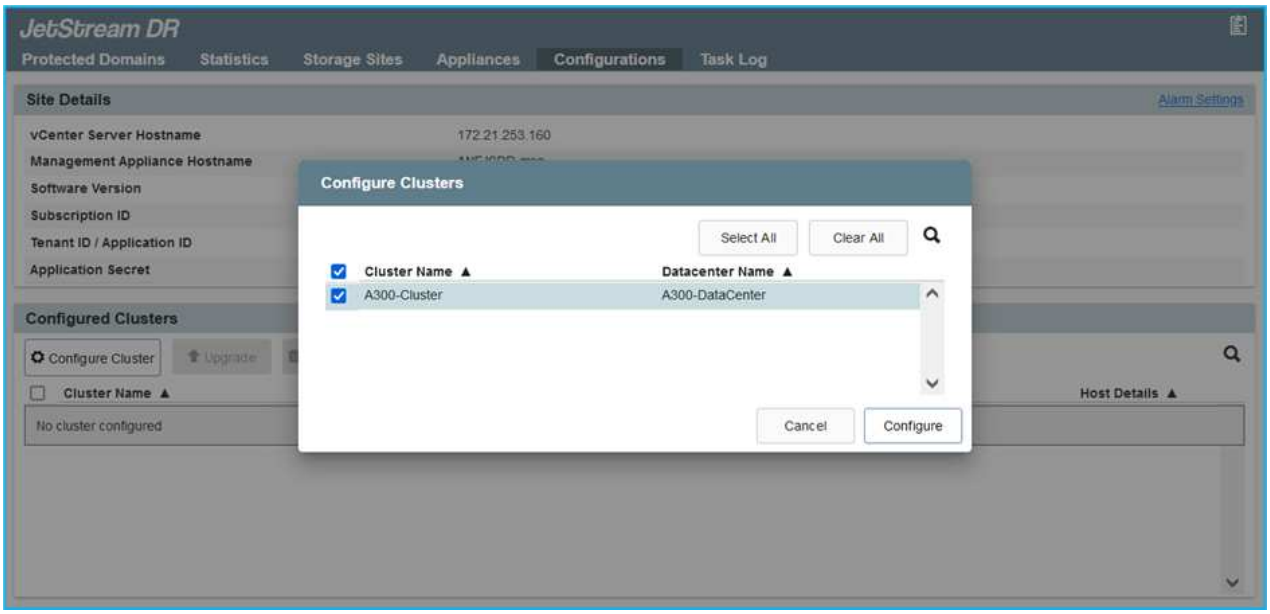
El software Jetstream DR consta de tres componentes principales: Jetstream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) y componentes host (paquetes de filtros de I/o). MSA se utiliza para instalar y configurar componentes host en el cluster informático y, a continuación, administrar el software de recuperación ante desastres JetStream. La siguiente lista proporciona una descripción de alto nivel del proceso de instalación:

Cómo instalar JetStream DR para las instalaciones

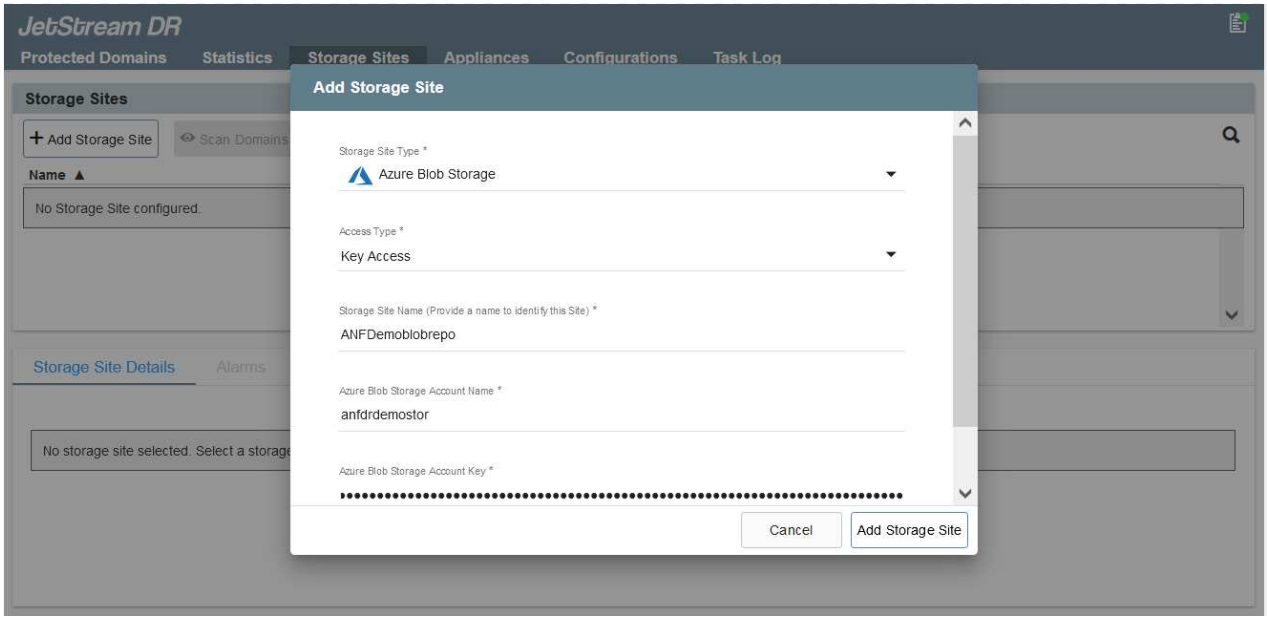
1. Compruebe los requisitos previos.
2. Ejecute la herramienta de planificación de la capacidad para realizar recomendaciones de recursos y configuración (opcional pero recomendado para pruebas de concepto).
3. Implemente JetStream DR MSA en un host de vSphere en el clúster designado.
4. Inicie MSA usando su nombre DNS en un explorador.
5. Registre el servidor vCenter con MSA.para realizar la instalación, complete los siguientes pasos detallados:
6. Una vez que se haya puesto en marcha JetStream DR MSA y se haya registrado vCenter Server, acceda al complemento de recuperación ante desastres JetStream mediante vSphere Web Client. Para ello, vaya a Datacenter > Configure > JetStream DR.



7. En la interfaz DR de JetStream, seleccione el clúster adecuado.



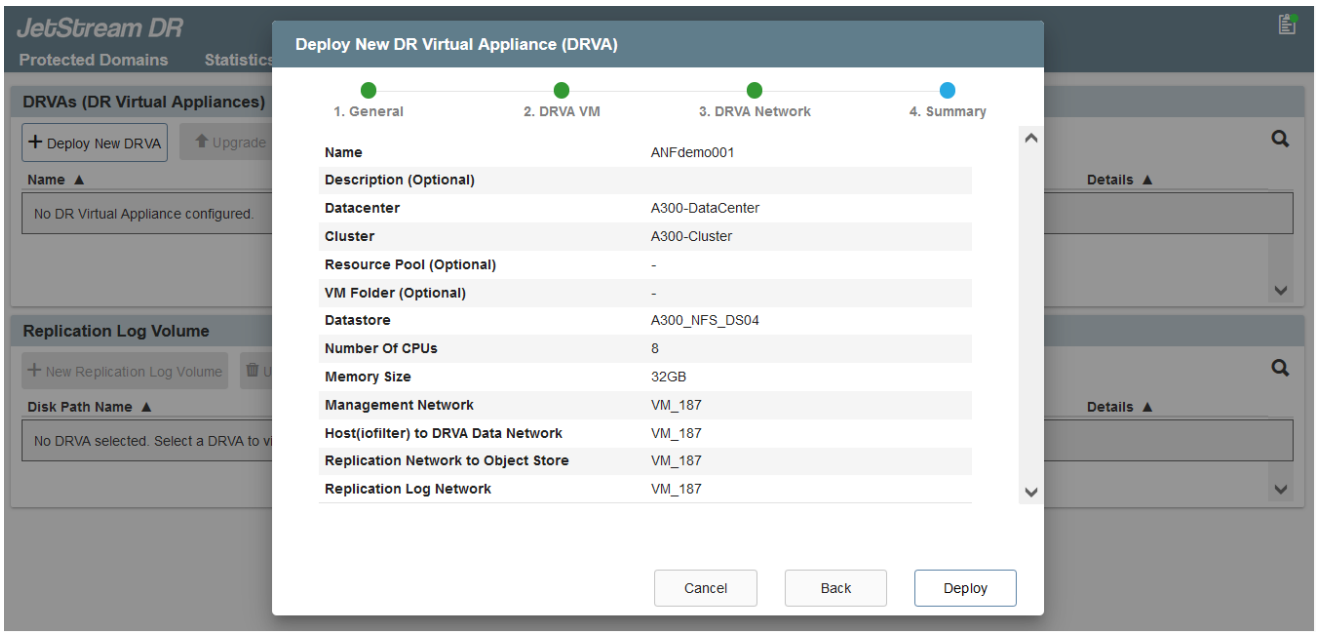
8. Configure el clúster con el paquete de filtro de I/O.



9. Añada Azure Blob Storage ubicado en el sitio de recuperación.
10. Implemente un dispositivo virtual de recuperación ante desastres (DRVA) desde la ficha Appliances (dispositivos).

> Los DRVAs se pueden crear automáticamente mediante CPT, pero para las pruebas POC recomendamos configurar y ejecutar manualmente el ciclo DR (iniciar protección > failover > conmutación por recuperación).

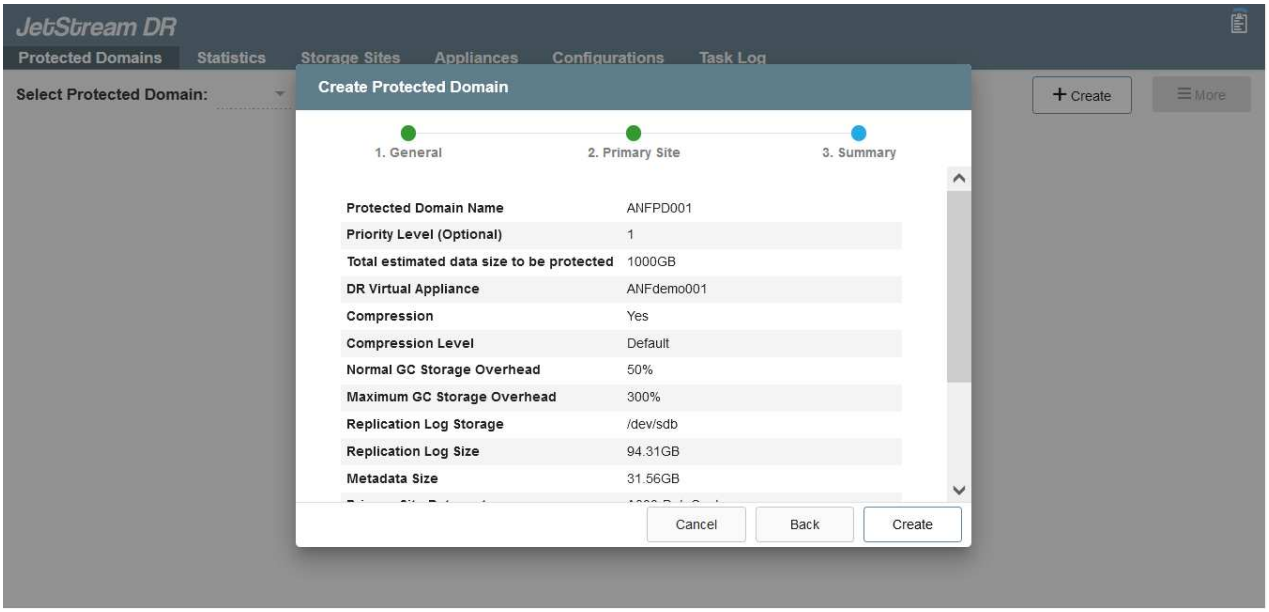
JetStream DRVA es un dispositivo virtual que facilita las funciones clave del proceso de replicación de datos. Un clúster protegido debe contener al menos un DVAD y, normalmente, un DVAD se configura por host. Cada DRVA puede gestionar varios dominios protegidos.



En este ejemplo, se crearon cuatro DRVA para 80 máquinas virtuales.

1. Crear volúmenes de registro de replicación para cada DRVA utilizando VMDK desde los almacenes de datos disponibles o grupos de almacenamiento iSCSI compartidos independientes.

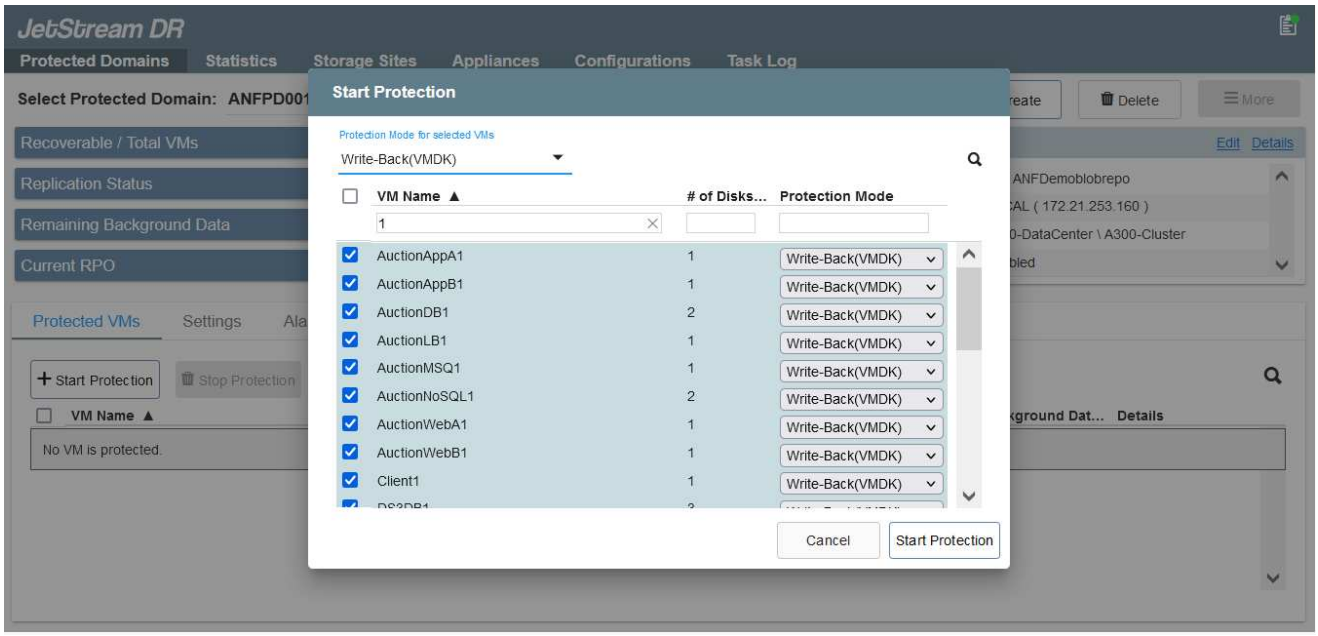
2. En la pestaña protected Domains, cree la cantidad necesaria de dominios protegidos utilizando información acerca del sitio de Azure Blob Storage, la instancia de DRVA y el registro de replicación. Un dominio protegido define una máquina virtual o un conjunto de máquinas virtuales específicos del clúster que se protegen en conjunto y asignó un orden de prioridad a las operaciones de conmutación por error y conmutación tras recuperación.



3. Seleccione las máquinas virtuales que desea proteger e iniciar la protección de máquinas virtuales del dominio protegido. Esto comienza la replicación de datos en el almacén BLOB designado.

> Compruebe que se utilice el mismo modo de protección para todas las máquinas virtuales de un dominio protegido.

> El modo Write- Back (VMDK) puede ofrecer un mayor rendimiento.



Compruebe que los volúmenes de registro de replicación se colocan en un almacenamiento de alto

rendimiento.

> Los libros de ejecución de conmutación por error se pueden configurar para agrupar los equipos virtuales (denominado Grupo de recuperación), establecer la secuencia de órdenes de arranque y modificar los ajustes de CPU/memoria junto con las configuraciones de IP.

Instalar JetStream DR para AVS en un cloud privado de Azure VMware Solution mediante el comando Run

Una práctica recomendada para un sitio de recuperación (AVS) es crear un clúster de tres nodos de luz piloto con antelación. Esto permite configurar la infraestructura del centro de recuperación, incluidos los siguientes elementos:

- Segmentos de red de destino, firewalls, servicios como DHCP y DNS, etc.
- Instalación de JetStream DR para AVS
- La configuración de volúmenes ANF como almacenes de datos y la recuperación ante desastres más moreJetStream admite un modo de objetivo de tiempo de recuperación casi cero para dominios críticos de negocio. Para estos dominios, el almacenamiento de destino debe estar preinstalado. ANF es un tipo de almacenamiento recomendado en este caso.

> La configuración de la red, incluida la creación de segmentos, se debe configurar en el clúster AVS para que coincida con los requisitos en las instalaciones.

En función de los requisitos de SLA y RTO, se puede usar el modo de conmutación por error continua o el modo de conmutación por error regular (estándar). Para lograr un objetivo de tiempo de recuperación cercano a cero, es necesario iniciar una rehidratación continua en el sitio de recuperación.

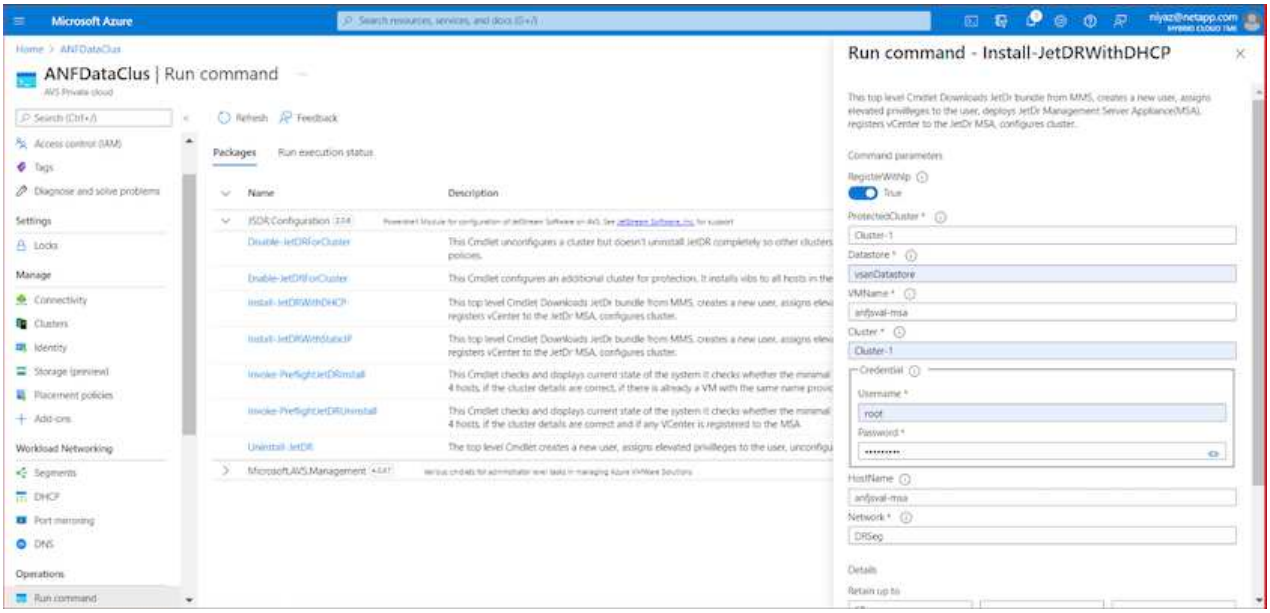
Cómo instalar JetStream DR para AVS en una nube privada

Para instalar JetStream DR para AVS en un cloud privado con Azure VMware Solution, realice los siguientes pasos:

1. En el portal de Azure, vaya a la solución Azure VMware, seleccione la nube privada y seleccione Ejecutar comando > Paquetes > JSDR.Configuration.

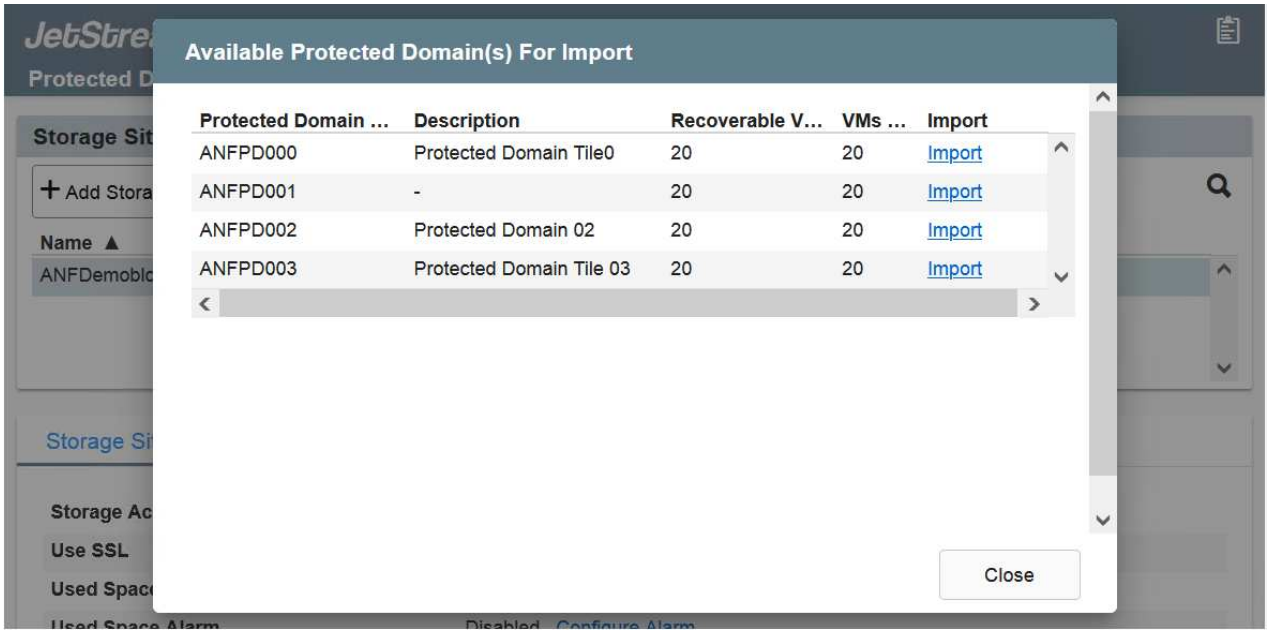
> El usuario de CloudAdmin predeterminado en la solución VMware de Azure no tiene suficientes privilegios para instalar JetStream DR para AVS. La solución VMware Azure permite una instalación simplificada y automatizada de la recuperación ante desastres de JetStream mediante la llamada al comando Azure VMware Solution Run para la recuperación ante desastres de JetStream.

La siguiente captura de pantalla muestra la instalación mediante una dirección IP basada en DHCP.



2. Una vez finalizada la instalación de JetStream DR para AVS, actualice el explorador. Para acceder a la interfaz de usuario de recuperación ante desastres de JetStream, vaya a SDDC Datacenter > Configure > JetStream DR.

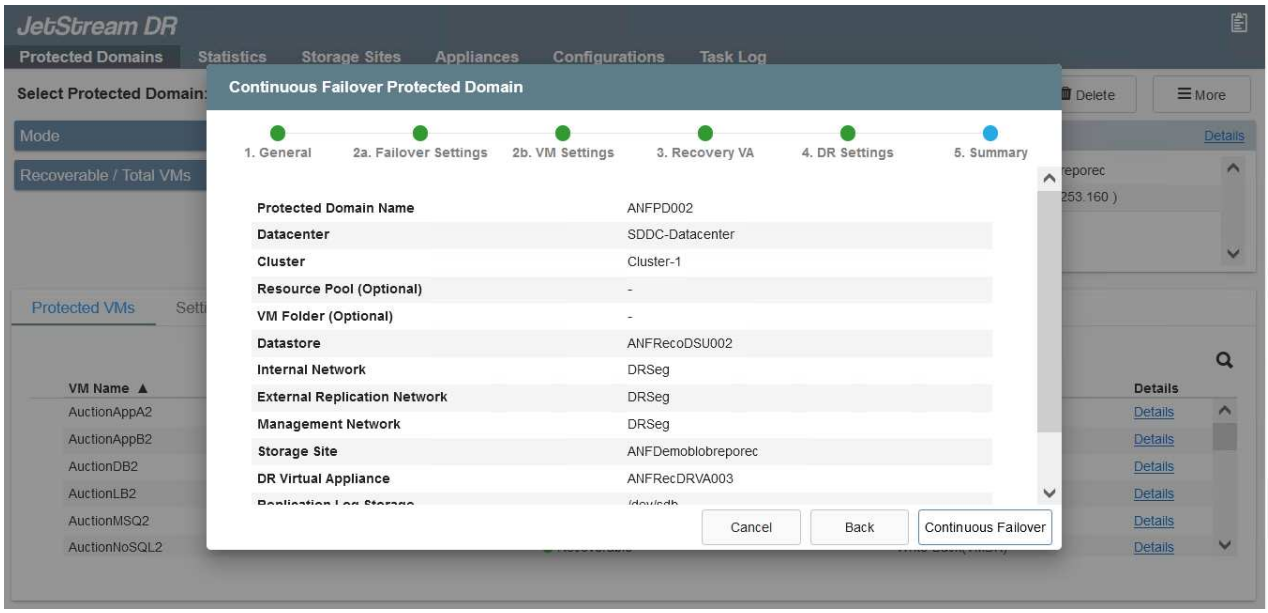
3. Desde la interfaz DR de JetStream, añada la cuenta de almacenamiento BLOB de Azure que se utilizó para proteger el clúster local como sitio de almacenamiento y, a continuación, ejecute la opción Scan Domains.



4. Después de importar los dominios protegidos, implemente dispositivos DRVA. En este ejemplo, la rehidratación continua se inicia manualmente desde el sitio de recuperación mediante la IU de recuperación ante desastres de JetStream.

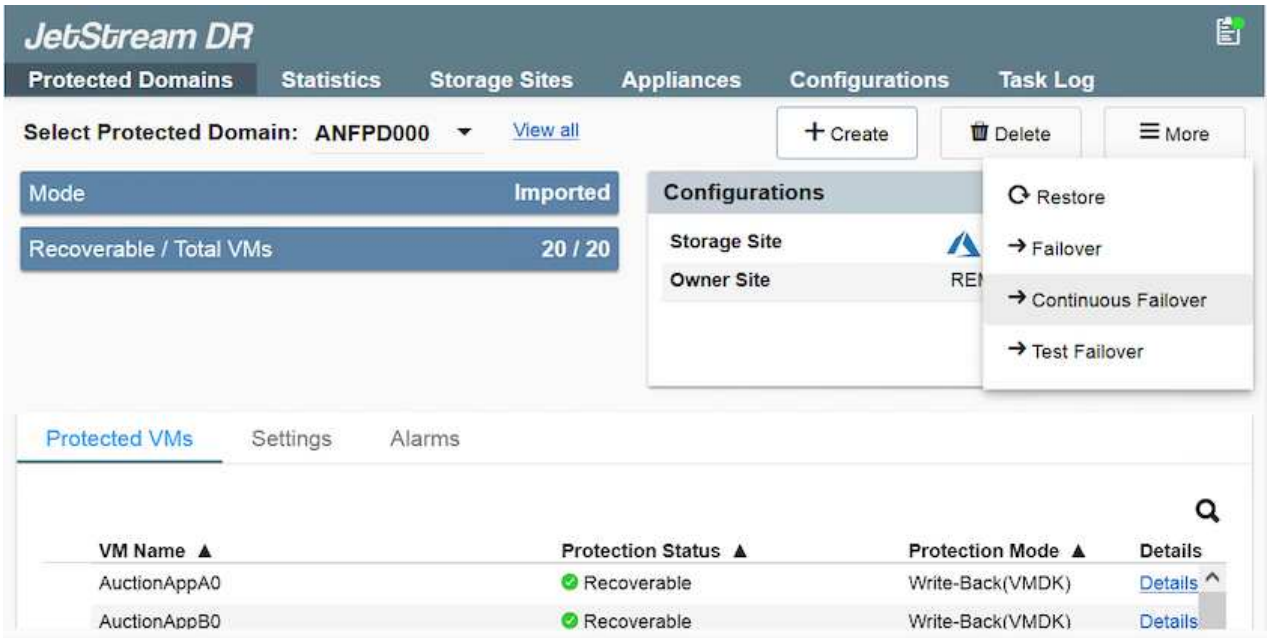
> Estos pasos también se pueden automatizar mediante planes creados por CPT.

5. Cree volúmenes de registros de replicación con almacenes de datos VSAN o ANF disponibles.
6. Importe los dominios protegidos y configure Recovery VA para utilizar el almacén de datos ANF en las ubicaciones de las máquinas virtuales.



Asegúrese de que DHCP esté habilitado en el segmento seleccionado y haya suficientes IP disponibles. Las IP dinámicas se utilizan temporalmente mientras se recuperan los dominios. Cada VM que se recupera (incluida la rehidratación continua) requiere una IP dinámica individual. Una vez finalizada la recuperación, se libera la IP y se puede volver a utilizar.

7. Seleccione la opción de conmutación por error adecuada (conmutación por error continua o conmutación por error). En este ejemplo, se selecciona la rehidratación continua (conmutación por error continua).



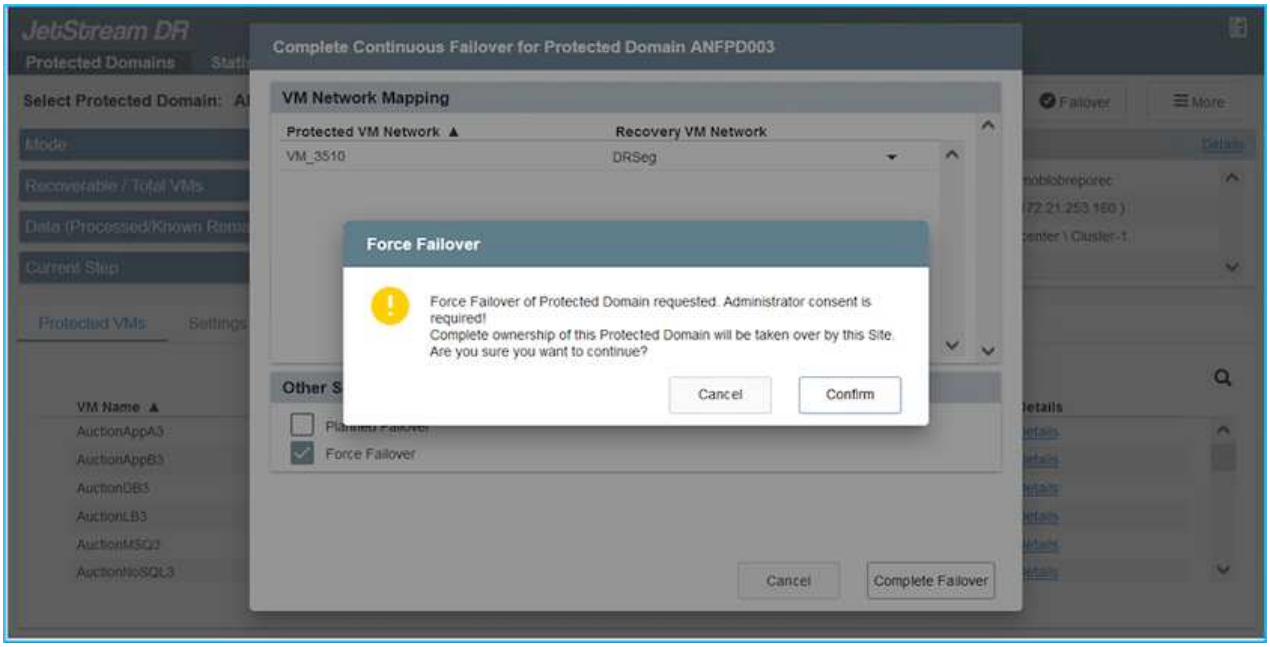
Realizar conmutación por error/conmutación por error

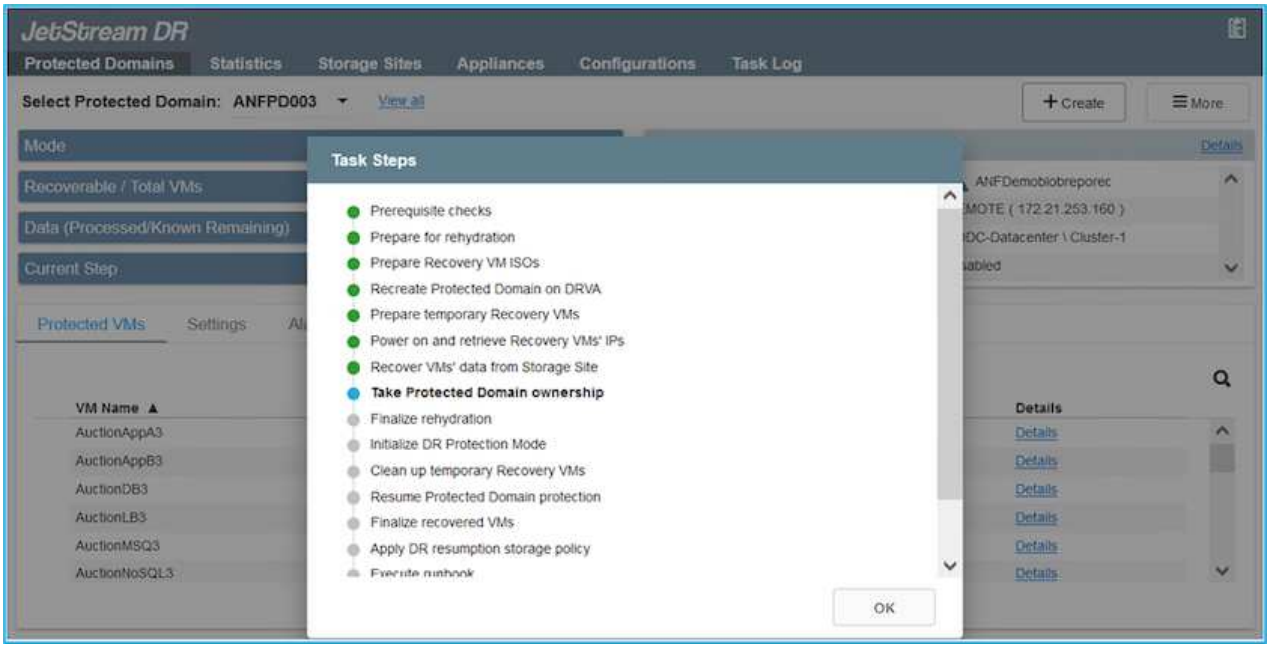
Cómo realizar una conmutación por error/conmutación por recuperación

1. Cuando se produce un desastre en el clúster protegido del entorno local (fallo parcial o total), active la conmutación al respaldo.

> CPT se puede usar para ejecutar el plan de conmutación por error y recuperar las máquinas virtuales de Azure Blob Storage en el sitio de recuperación del clúster AVS.

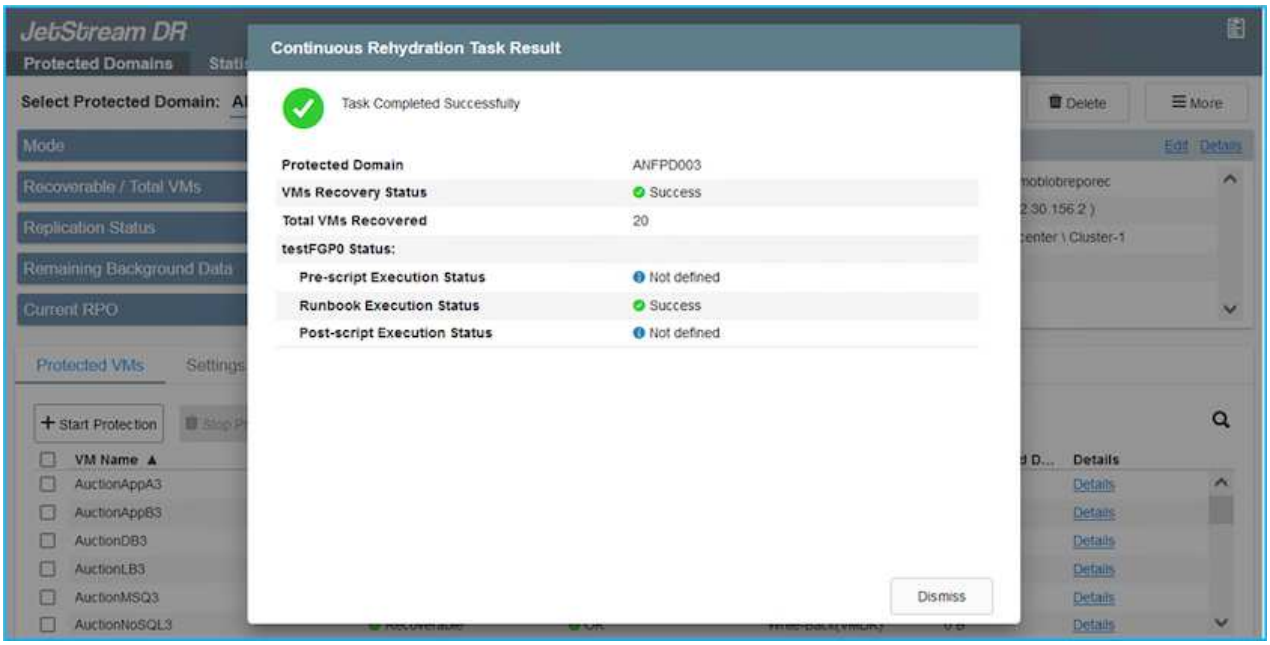
> Después de la conmutación al nodo de respaldo (para una rehidratación continua o estándar), cuando se iniciaron las máquinas virtuales protegidas en AVS, la protección se reanuda automáticamente y JetStream DR sigue replicando sus datos en los contenedores originales o adecuados en Azure Blob Storage.





La barra de tareas muestra el progreso de las actividades de failover.

2. Una vez finalizada la tarea, el acceso al equipo virtual recuperado y al negocio continúa de forma normal.

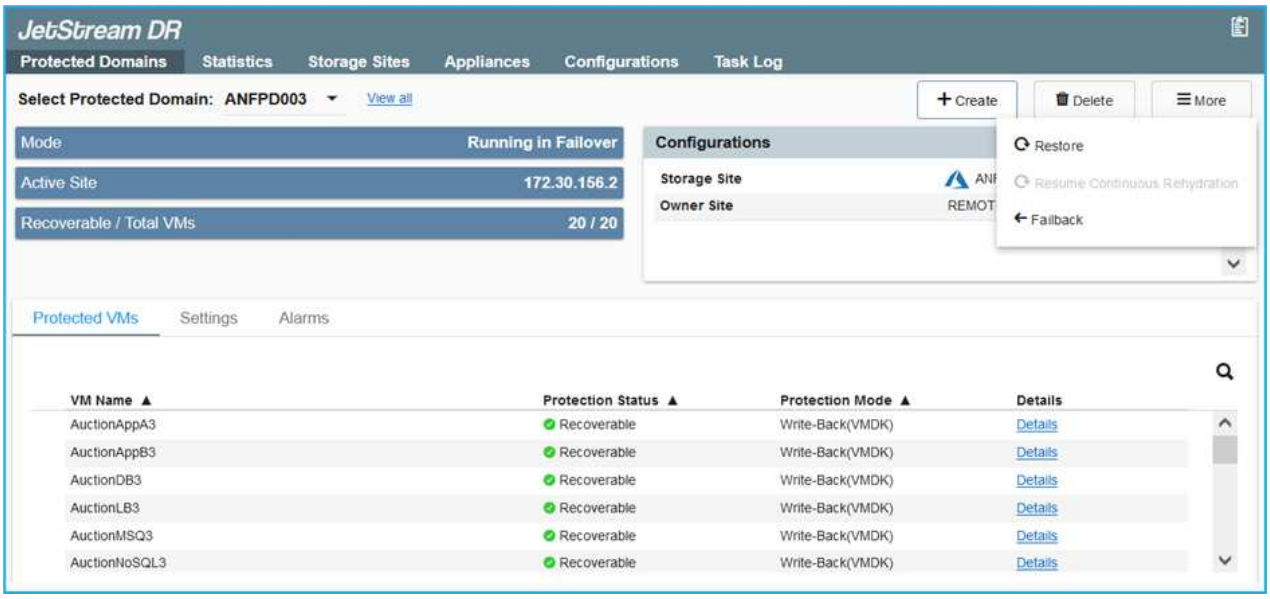


Una vez que el sitio principal esté activo y en funcionamiento de nuevo, es posible realizar la conmutación tras recuperación. La protección de equipos virtuales se reanuda y se debe comprobar la consistencia de los datos.

3. Restaure el entorno de sus instalaciones. En función del tipo de incidente de desastre, podría ser necesario restaurar o verificar la configuración del clúster protegido. Si es necesario, puede que sea necesario volver a instalar el software JetStream DR.

> Nota: La `recovery_utility_prepare_failback` El script que se proporciona en el kit de herramientas de automatización se puede utilizar para ayudar a limpiar el sitio protegido original de cualquier máquina virtual obsoleta, información de dominio, etc.

4. Acceda al entorno local restaurado, vaya a la interfaz de usuario de recuperación ante desastres de Jetstream y seleccione el dominio protegido adecuado. Una vez que el sitio protegido esté listo para la conmutación tras recuperación, seleccione la opción de conmutación por recuperación en la interfaz de usuario.



El plan de conmutación por recuperación generado por CPT también se puede usar para iniciar la devolución de los equipos virtuales y sus datos del almacén de objetos al entorno de VMware original.

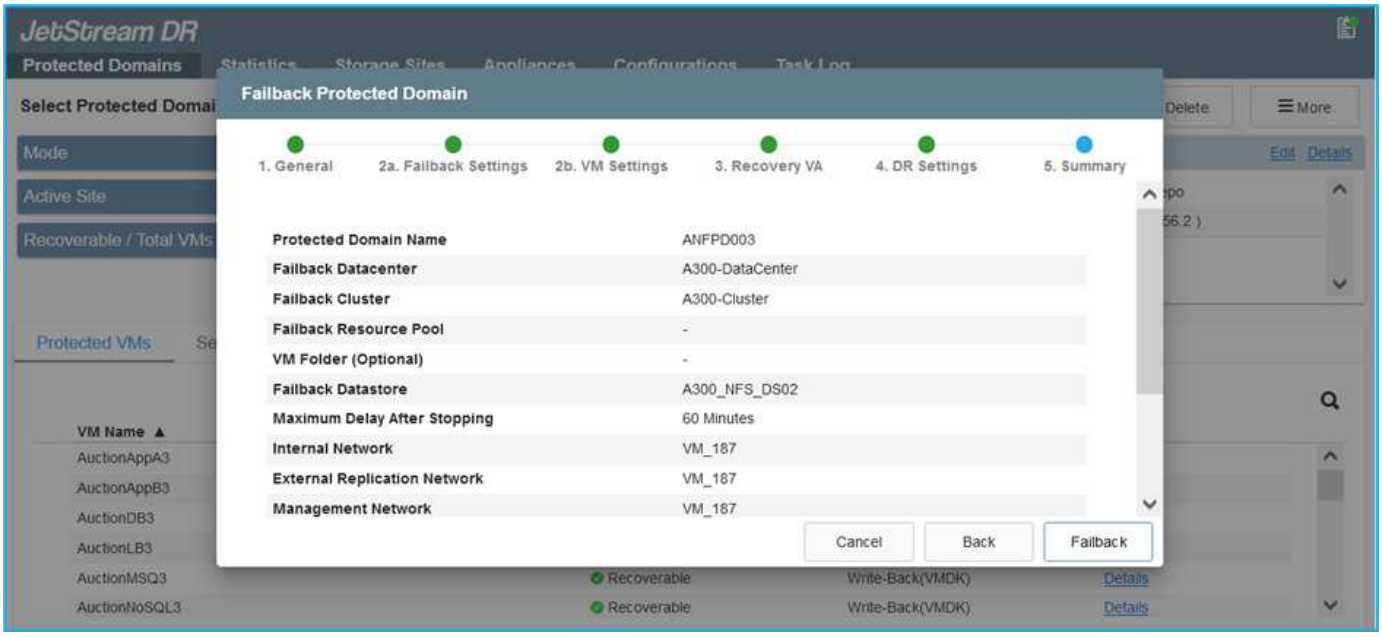
Especifique la demora máxima después de pausar las máquinas virtuales en el sitio de recuperación y reiniciar en el sitio protegido. Esta vez incluye completar la replicación después de detener las máquinas virtuales en caso de fallo, el tiempo para limpiar el sitio de recuperación y el tiempo para recrear las máquinas virtuales en el sitio protegido. El valor recomendado por NetApp es de 10 minutos.

Completar el proceso de conmutación tras recuperación y, a continuación, confirmar la reanudación de la protección de los equipos virtuales y la consistencia de datos.

Recuperación de Ransomeware

Recuperarse del ransomware puede ser una tarea abrumadora. Específicamente, puede resultar difícil para las organizaciones TECNOLÓGICAS determinar el punto de retorno seguro y, una vez determinado, cómo garantizar que las cargas de trabajo recuperadas se protejan de los ataques que vuelvan a producirse (de malware en suspensión o de aplicaciones vulnerables).

Jetstream DR para AVS junto con los almacenes de datos de Azure NetApp Files pueden resolver estos problemas al permitir que las organizaciones se recuperen de puntos disponibles en el tiempo, de modo que las cargas de trabajo se recuperen en una red funcional y aislada, en caso necesario. La recuperación permite que las aplicaciones funcionen y se comuniquen entre sí mientras no las exponen al tráfico norte-sur, dando así a los equipos de seguridad un lugar seguro para realizar el análisis forense y otra reparación necesaria.



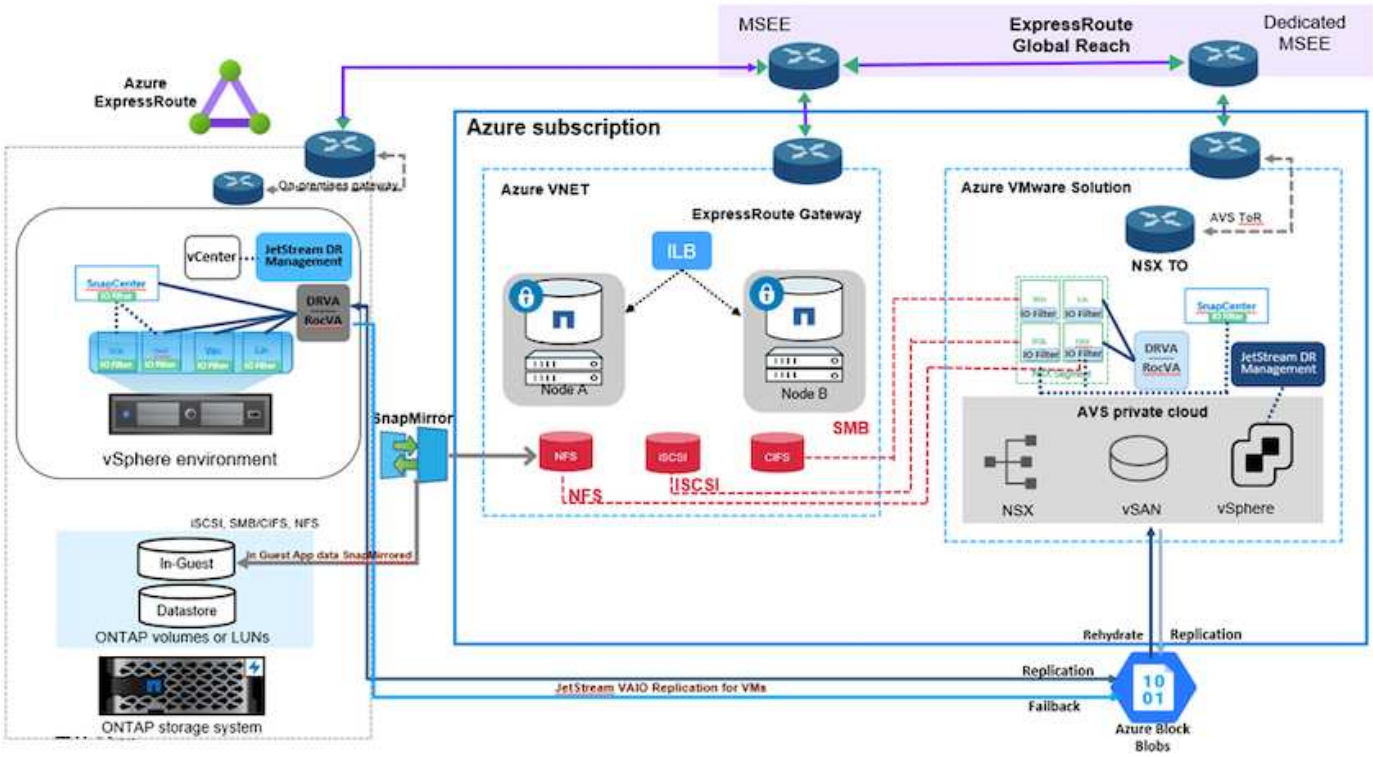
Recuperación ante desastres con CVO y AVS (almacenamiento conectado a invitado)

Descripción general

Autores: Ravi BCB y Niyaz Mohamed, NetApp

La recuperación ante desastres en el cloud es un método resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos dañados por datos como ransomware. Con SnapMirror de NetApp, las cargas de trabajo de VMware en las instalaciones que utilizan el almacenamiento conectado a invitado se pueden replicar a Cloud Volumes ONTAP de NetApp que se ejecuta en Azure. Así se tratan los datos de aplicaciones; sin embargo, ¿qué ocurre con los equipos virtuales mismos? La recuperación ante desastres debería cubrir todos los componentes dependientes, incluidos equipos virtuales, VMDK, datos de aplicaciones, etc. Para ello, SnapMirror y JetStream pueden utilizarse para recuperar sin problemas cargas de trabajo replicadas de las instalaciones a Cloud Volumes ONTAP utilizando almacenamiento VSAN para VMDK de VM.

Este documento proporciona un enfoque paso a paso para configurar y realizar la recuperación ante desastres que utiliza SnapMirror, JetStream y la solución Azure VMware (AVS) de NetApp.



Supuestos

Este documento se centra en el almacenamiento invitado para datos de aplicaciones (también conocido como «guest» conectado) y asumimos que el entorno local utiliza SnapCenter para realizar backups coherentes con las aplicaciones.

> Este documento es aplicable a cualquier solución de backup o recuperación de terceros. Dependiendo de la solución utilizada en el entorno, siga las prácticas recomendadas para crear normativas de backup que cumplan los acuerdos de nivel de servicio de la organización.

Para obtener conectividad entre el entorno local y la red virtual de Azure, utilice el alcance global de la ruta Express o una WAN virtual con una puerta de enlace VPN. Los segmentos se deben crear en función del diseño VLAN en las instalaciones.

> Existen múltiples opciones para conectar los centros de datos en las instalaciones a Azure, lo que nos impide esbozar un flujo de trabajo específico en este documento. Consulte la documentación de Azure para conocer el método de conectividad apropiado entre las instalaciones y Azure.

Implementar la solución DR

Descripción general de la puesta en marcha de soluciones

1. Asegúrese de que se realiza el backup de los datos de la aplicación mediante SnapCenter con los requisitos de punto de recuperación necesarios.
2. Aprovisione Cloud Volumes ONTAP con el tamaño de instancia correcto usando Cloud Manager dentro de la suscripción y la red virtual adecuadas.

a. Configurar SnapMirror para los volúmenes correspondientes de las aplicaciones.

b. Actualice las políticas de backup en SnapCenter para activar actualizaciones de SnapMirror después de los trabajos programados.

3. Instale el software de recuperación ante desastres JetStream en el centro de datos local y comience la protección de las máquinas virtuales.
4. Instalar el software de recuperación ante desastres JetStream en el cloud privado de Azure VMware Solution.
5. Durante un evento de desastre, rompa la relación de SnapMirror con Cloud Manager y active la conmutación por error de máquinas virtuales a Azure NetApp Files o a almacenes de datos VSAN en el sitio de recuperación ante desastres AVS designado.

   a. Vuelva a conectar las LUN ISCSI y los montajes NFS para los equipos virtuales de la aplicación.

6. Invoque la conmutación tras recuperación al sitio protegido mediante la resincronización inversa de SnapMirror una vez que se haya recuperado el sitio principal.

Detalles de la implementación

Configurar CVO en Azure y replicar volúmenes a CVO

El primer paso es configurar Cloud Volumes ONTAP en Azure ("Enlace") Y replicar los volúmenes deseados en Cloud Volumes ONTAP con las frecuencias y retentions de instantánea deseadas.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	17 seconds	idle	snapmirrored	May 6, 2022, 11:43:18 AM 105.06 KiB
	gcsdrsqlhld_sc46_copy ANFCVODRDemo	gcsdrsqlhld_sc46 ntaphci-a300e9u25	7 seconds	idle	snapmirrored	May 6, 2022, 11:42:20 AM 7.22 MiB
	gcsdrsqllog_sc46 ntaphci-a300e9u25	gcsdrsqllog_sc46_copy ANFCVODRDemo	16 seconds	idle	snapmirrored	May 6, 2022, 11:43:52 AM 130.69 KiB

Configurar los hosts AVS y el acceso a datos CVO

Dos factores importantes que se deben tener en cuenta al implementar el SDDC son el tamaño del clúster en la solución Azure VMware y el tiempo que se debe mantener el SDDC en servicio. Estas dos consideraciones clave para una solución de recuperación ante desastres ayudan a reducir los costes operativos generales. SDDC puede ser de tan solo tres hosts, hasta un clúster de varios hosts en una puesta en marcha a escala completa.

La decisión de poner en marcha un clúster AVS se basa principalmente en los requisitos de RPO/RTO. Con la solución para Azure VMware, el SDDC se puede aprovisionar justo a tiempo como preparación para pruebas o ante un desastre real. Un SDDC implementado en el tiempo ahorra en costes de host ESXi cuando no se enfrenta a un desastre. Sin embargo, esta forma de puesta en marcha afecta al objetivo de tiempo de recuperación en unas pocas horas, mientras que se aprovisiona SDDC.

La opción más común implementada es tener SDDC en funcionamiento en un modo de funcionamiento siempre activo y con luz piloto. Esta opción proporciona una huella pequeña de tres hosts siempre disponibles y también acelera las operaciones de recuperación, ya que proporciona una línea de base en ejecución para las actividades de simulación y comprobaciones de cumplimiento de normativas, lo que evita el riesgo de que se produzca una desviación operativa entre los sitios de producción y de recuperación ante desastres. El grupo piloto se puede escalar verticalmente rápidamente hasta el nivel deseado cuando es necesario para gestionar un evento de recuperación ante desastres real.

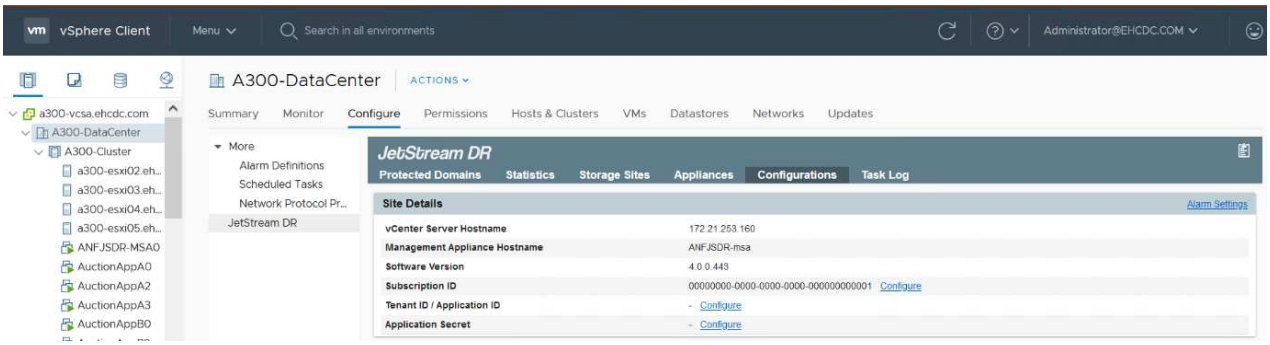
Para configurar AVS SDDC (ya sea a petición o en modo piloto), consulte "Ponga en marcha y configure el entorno de virtualización en Azure". Como requisito previo, verifique que los equipos virtuales invitados que residen en los hosts AVS pueden consumir datos de Cloud Volumes ONTAP una vez establecida la conectividad.

Una vez que Cloud Volumes ONTAP y AVS se hayan configurado correctamente, comience a configurar JetStream para automatizar la recuperación de las cargas de trabajo en las instalaciones en AVS (VM con VMDK de aplicación y equipos virtuales con almacenamiento en invitado) mediante el mecanismo VAIO y aprovechando SnapMirror para copias de volúmenes de aplicación en Cloud Volumes ONTAP.

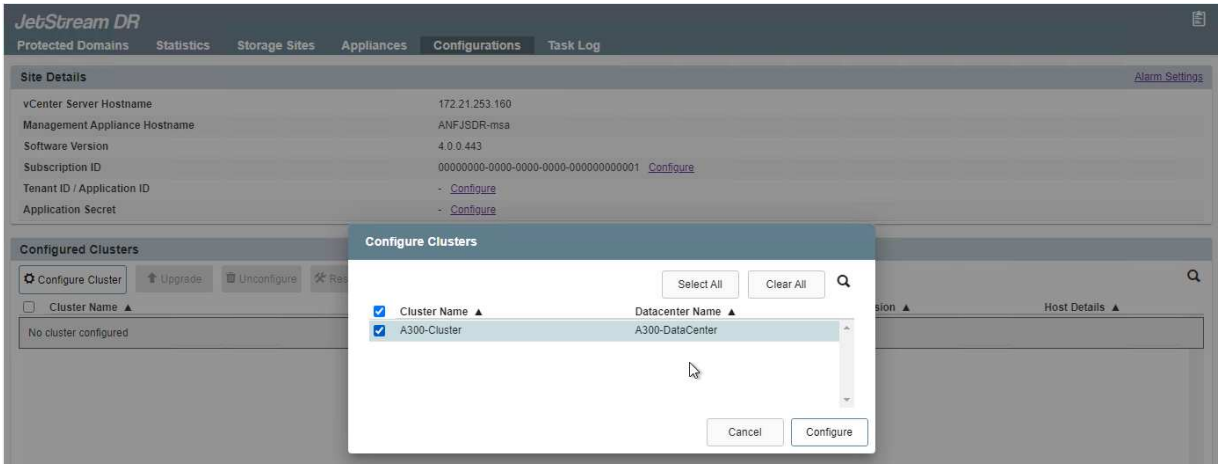
Instalar JetStream DR en el centro de datos local

El software JetStream DR consta de tres componentes principales: JetStream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) y componentes host (paquetes de filtros de I/o). MSA se utiliza para instalar y configurar componentes host en el cluster informático y, a continuación, administrar el software JetStream DR. El proceso de instalación es el siguiente:

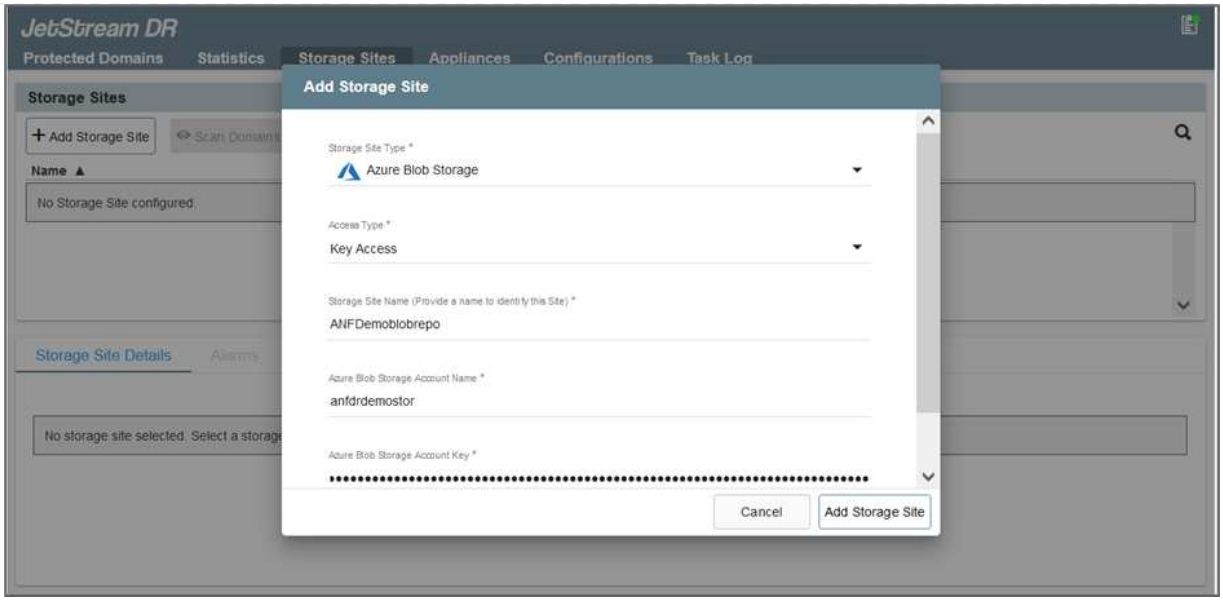
1. Compruebe los requisitos previos.
2. Ejecute la herramienta de planificación de la capacidad para realizar recomendaciones de recursos y configuración.
3. Implemente JetStream DR MSA en cada host de vSphere en el clúster designado.
4. Inicie MSA usando su nombre DNS en un explorador.
5. Registre el servidor vCenter con el MSA.
6. Una vez que se haya puesto en marcha JetStream DR MSA y se haya registrado vCenter Server, desplácese hasta el complemento de recuperación ante desastres JetStream con vSphere Web Client. Para ello, vaya a Datacenter > Configure > JetStream DR.



7. Desde la interfaz DR de JetStream, realice las siguientes tareas:
   a. Configure el clúster con el paquete de filtro de I/O.

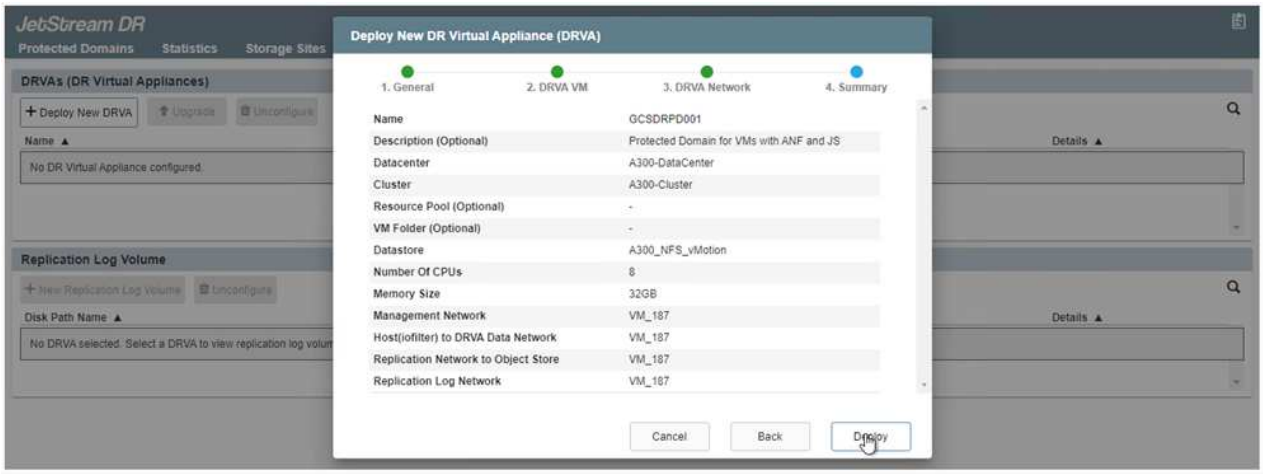


   b. Añada el almacenamiento de Azure Blob que está situado en el sitio de recuperación.

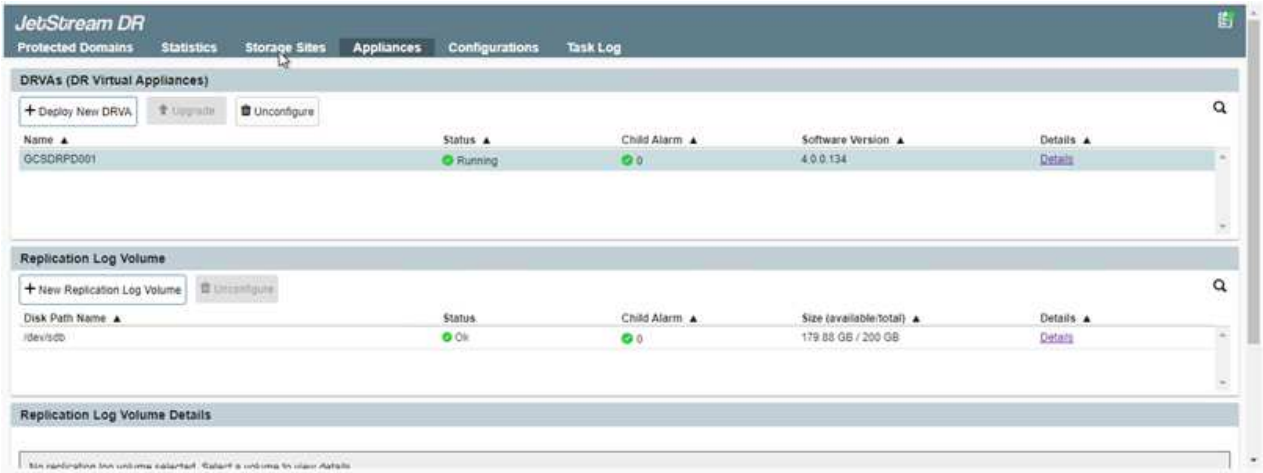


8. Implemente el número necesario de dispositivos virtuales de recuperación ante desastres (DRVAs) desde la ficha Appliances (dispositivos virtuales).

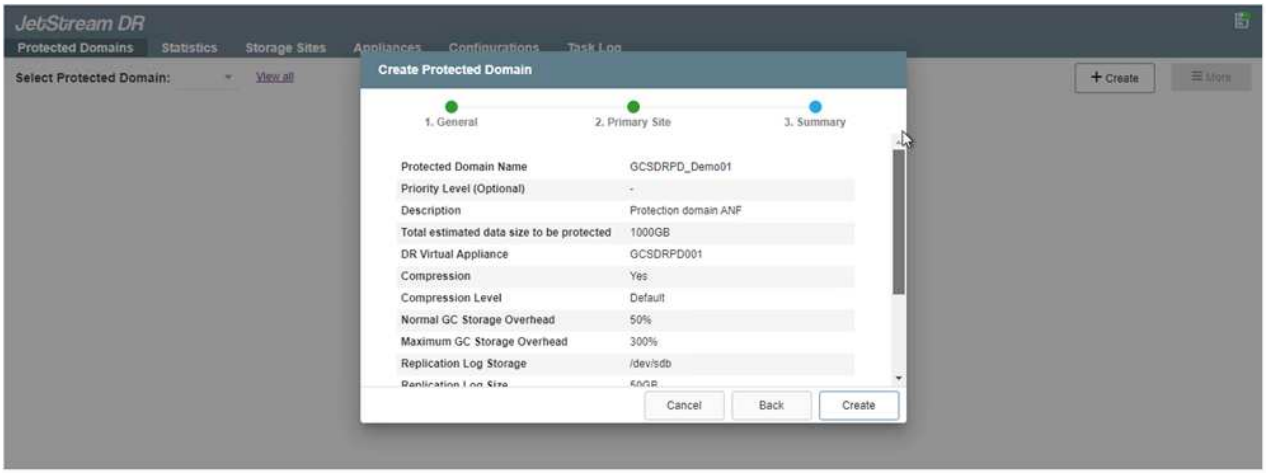
> Utilice la herramienta de planificación de la capacidad para calcular el número de DRVAs necesarios.

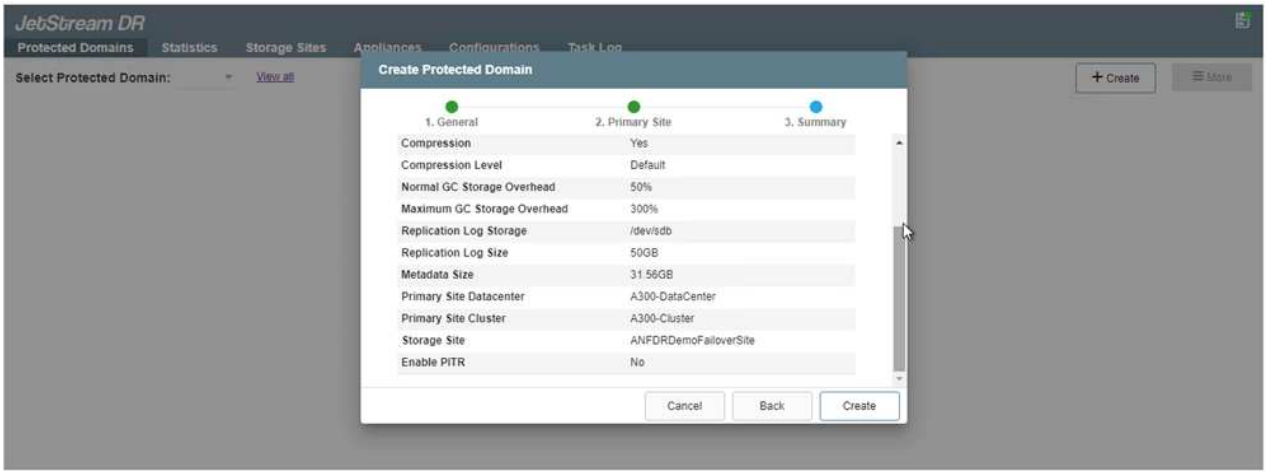


9. Cree volúmenes de registro de replicación para cada DRVA utilizando el VMDK desde los almacenes de datos disponibles o el pool de almacenamiento iSCSI compartido independiente.



10. En la pestaña Protected Domains, cree la cantidad necesaria de dominios protegidos utilizando información acerca del sitio de Azure Blob Storage, la instancia de DRVA y el registro de replicación. Un dominio protegido define una máquina virtual o un conjunto específico de máquinas virtuales de aplicación dentro del clúster que se protegen en conjunto y asignó un orden de prioridad para las operaciones de conmutación por error y conmutación tras recuperación.

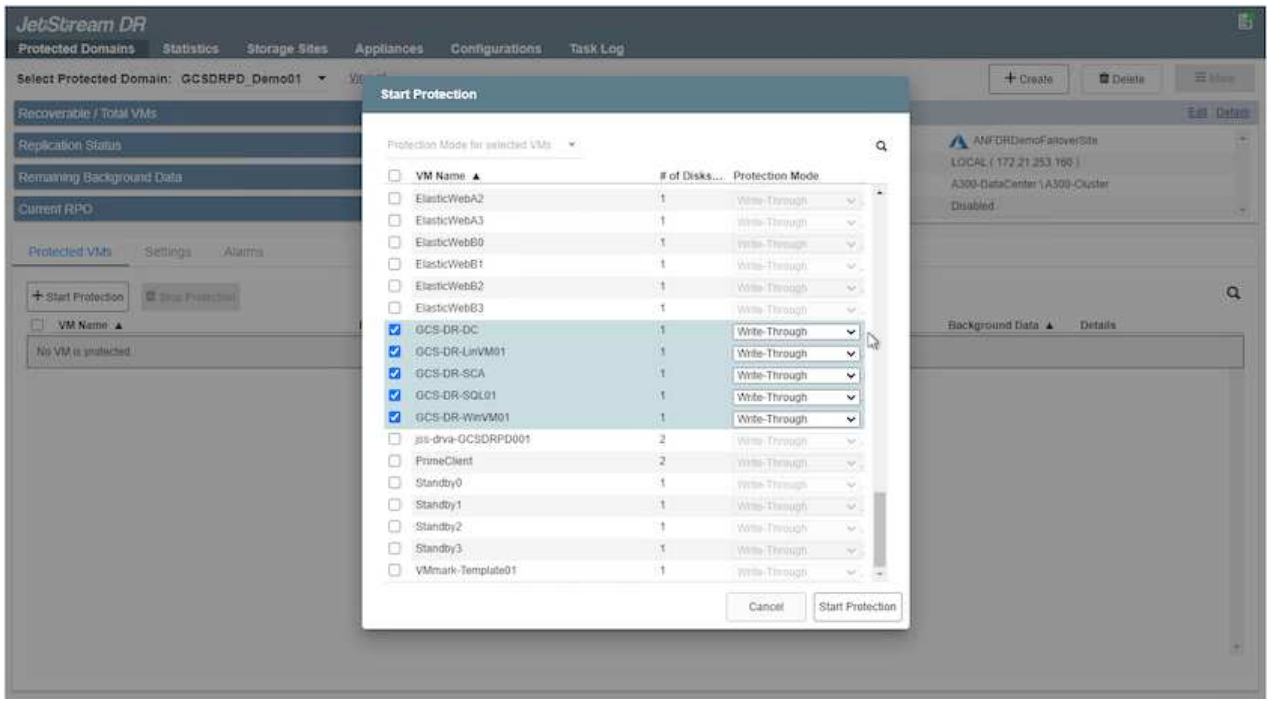




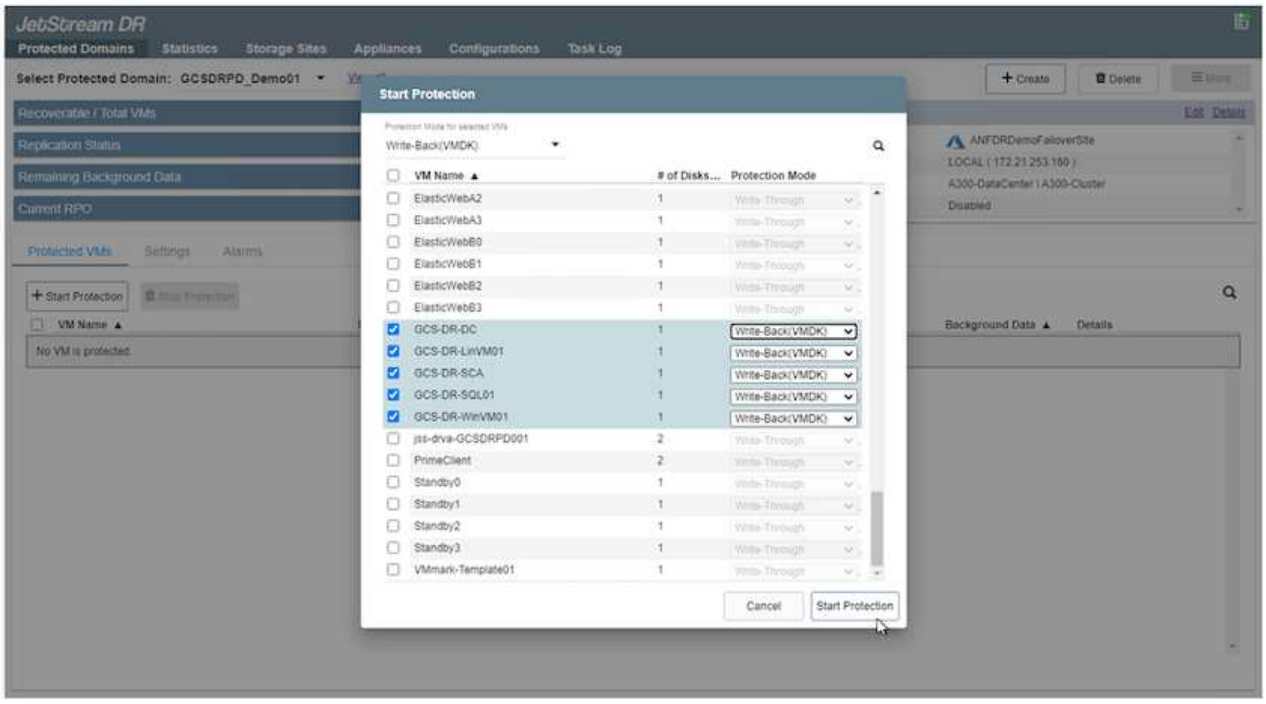
11. Seleccione las máquinas virtuales que se van a proteger y agrupe las máquinas virtuales en grupos de aplicaciones en función de la dependencia. Las definiciones de aplicaciones le permiten agrupar conjuntos de máquinas virtuales en grupos lógicos que contengan sus órdenes de arranque, retrasos de arranque y validaciones de aplicaciones opcionales que se pueden ejecutar tras la recuperación.

Asegúrese de que se utilice el mismo modo de protección para todas las máquinas virtuales de un dominio protegido.

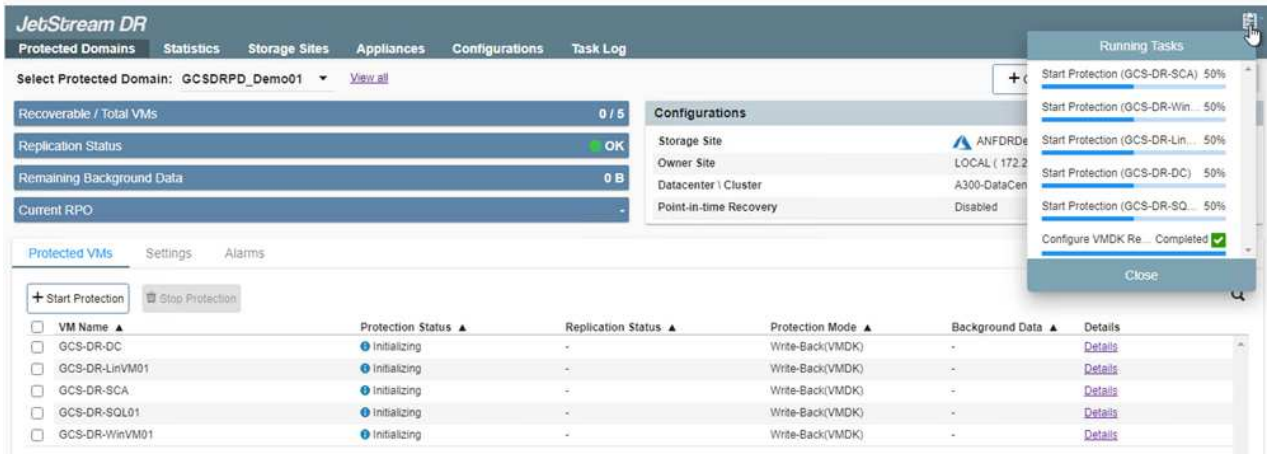
El modo Write-Back (VMDK) ofrece un mayor rendimiento.



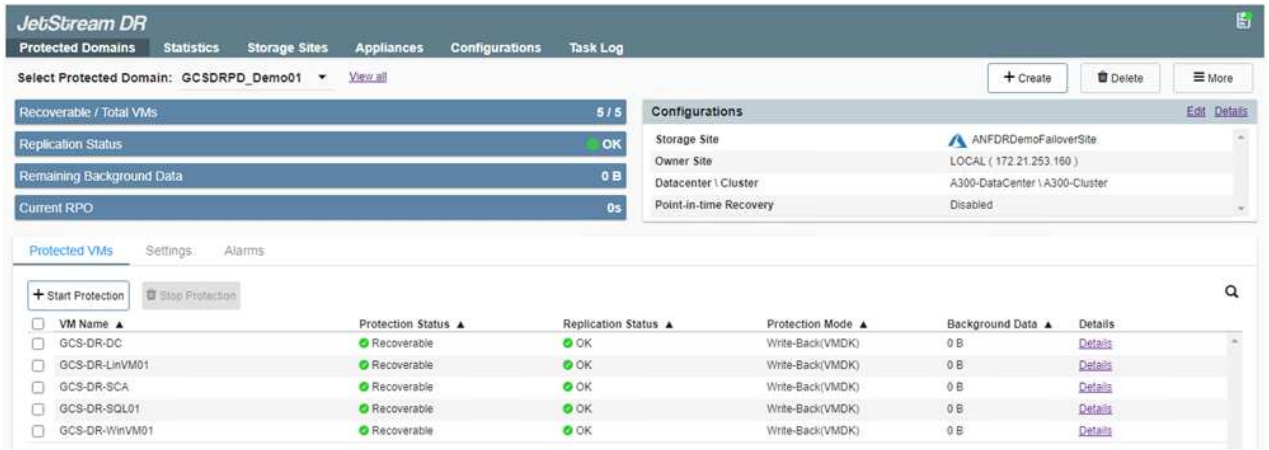
12. Asegúrese de que los volúmenes de registros de replicación se colocan en un almacenamiento de alto rendimiento.



13. Una vez que haya terminado, haga clic en Iniciar protección para el dominio protegido. Esto inicia la replicación de datos de las máquinas virtuales seleccionadas en el almacén BLOB designado.



14. Una vez finalizada la replicación, el estado de protección del equipo virtual se Marca como recuperable.

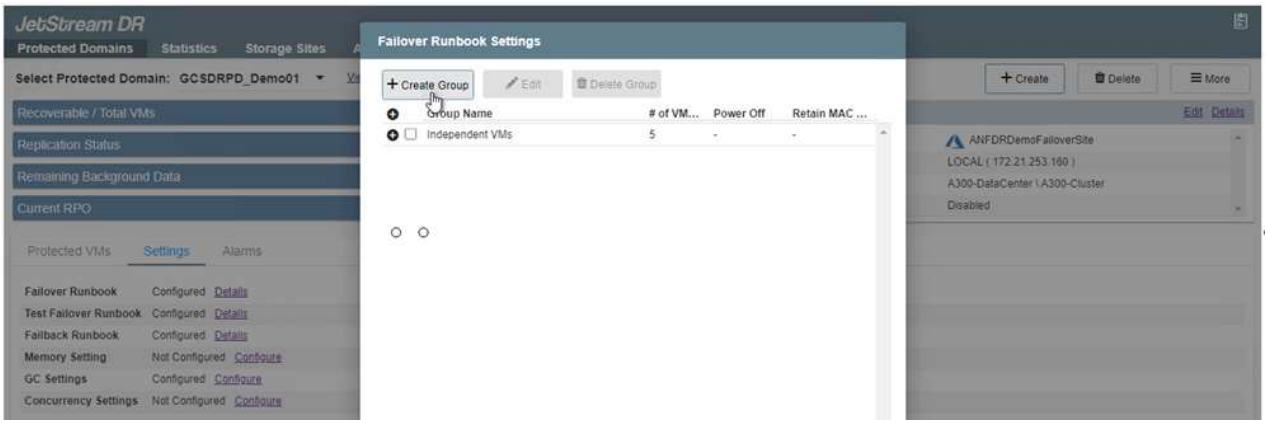


> Los runbooks pueden configurarse para agrupar los equipos virtuales (denominados «grupo de recuperación»), establecer la secuencia de órdenes de arranque y modificar la configuración de CPU/memoria junto con las configuraciones de IP.

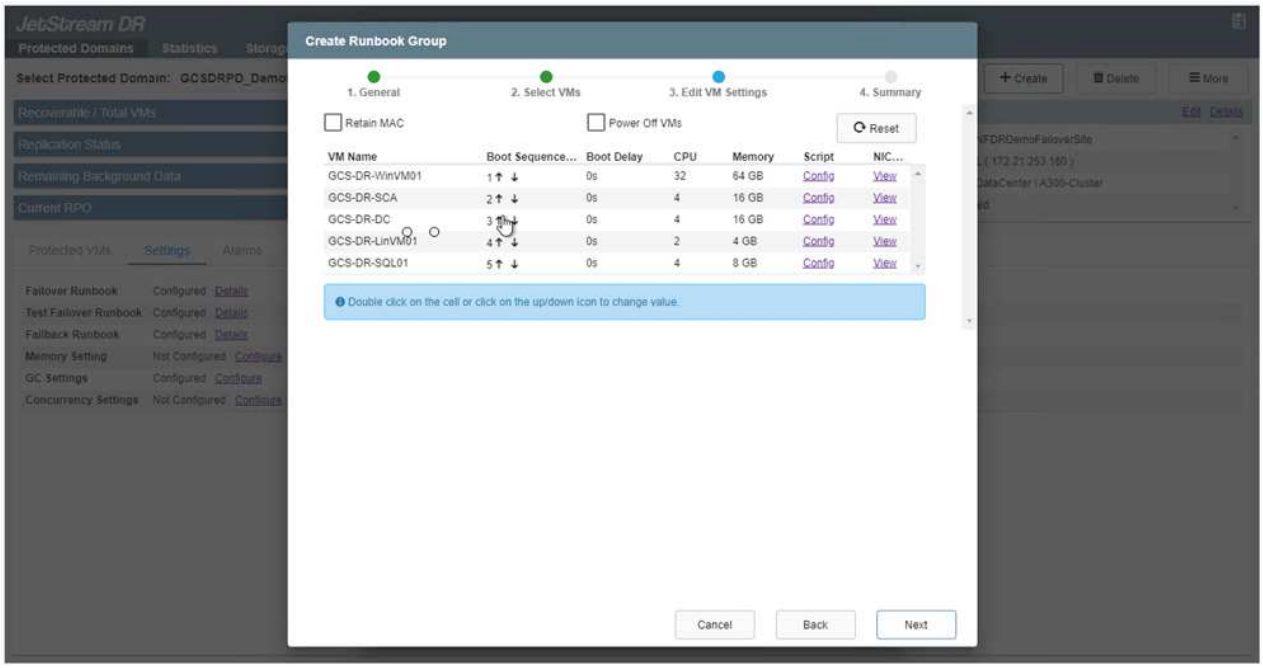
15. Haga clic en Configuración y, a continuación, en el enlace Configurar libro de ejecución para configurar el grupo de libro de ejecución.

16. Haga clic en el botón Crear grupo para comenzar a crear un nuevo grupo runbook.

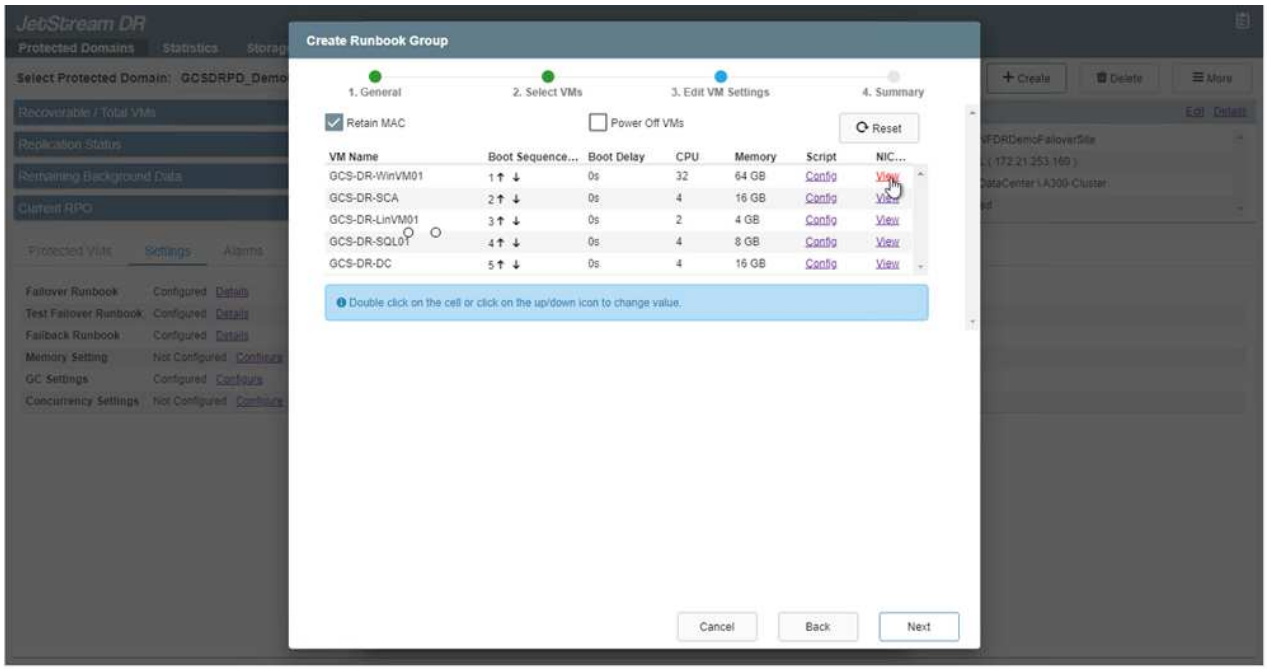
Si es necesario, en la parte inferior de la pantalla, aplique scripts previos y posteriores personalizados para que se ejecuten automáticamente antes y después del funcionamiento del grupo runbook. Asegúrese de que los scripts de Runbook residen en el servidor de administración.



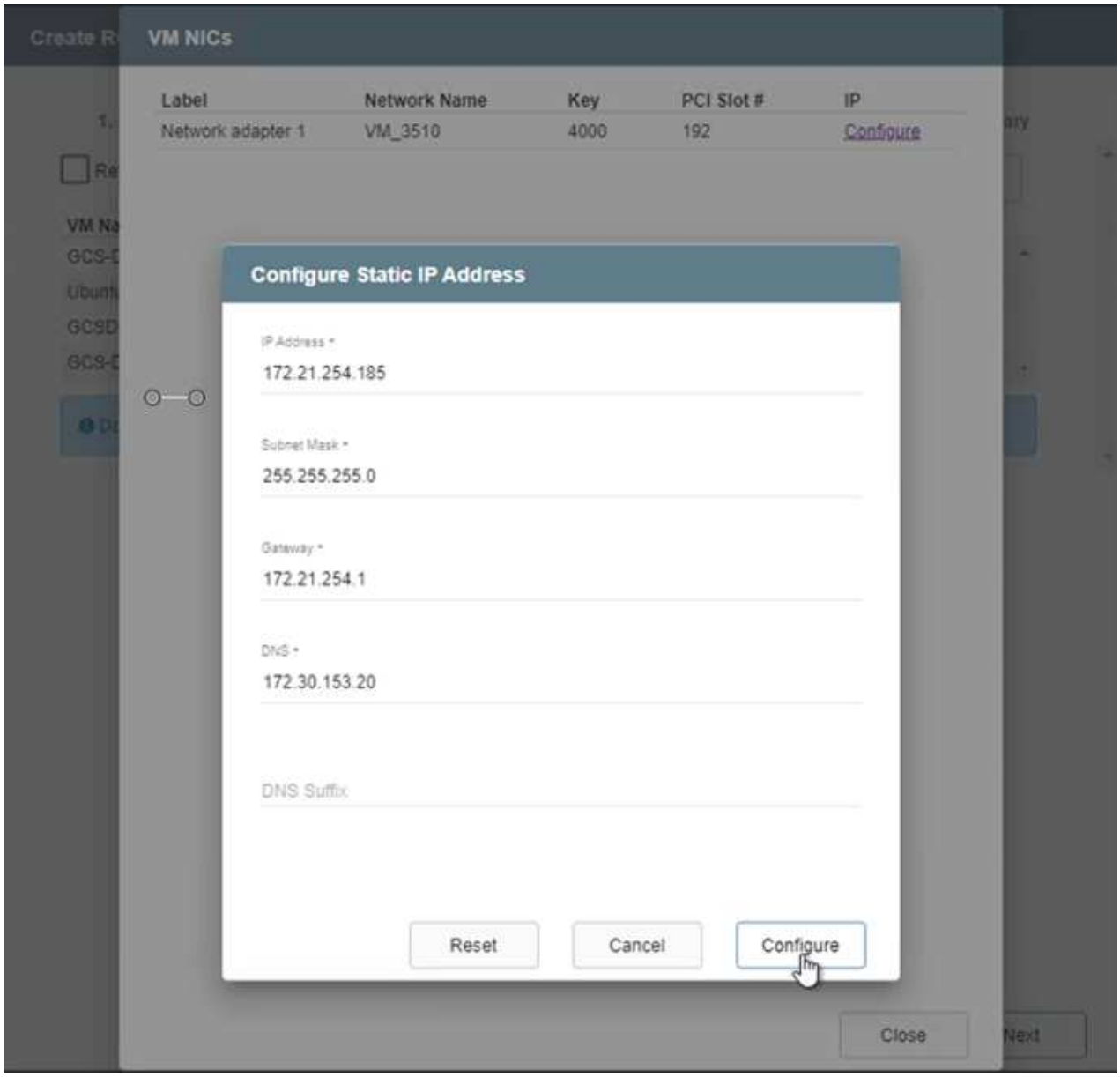
17. Edite la configuración de la máquina virtual según sea necesario. Especifique los parámetros para recuperar las VM, incluida la secuencia de arranque, el retraso de arranque (especificado en segundos), el número de CPU y la cantidad de memoria que se debe asignar. Cambie la secuencia de arranque de las VM haciendo clic en las flechas arriba o abajo. También se proporcionan opciones para conservar MAC.

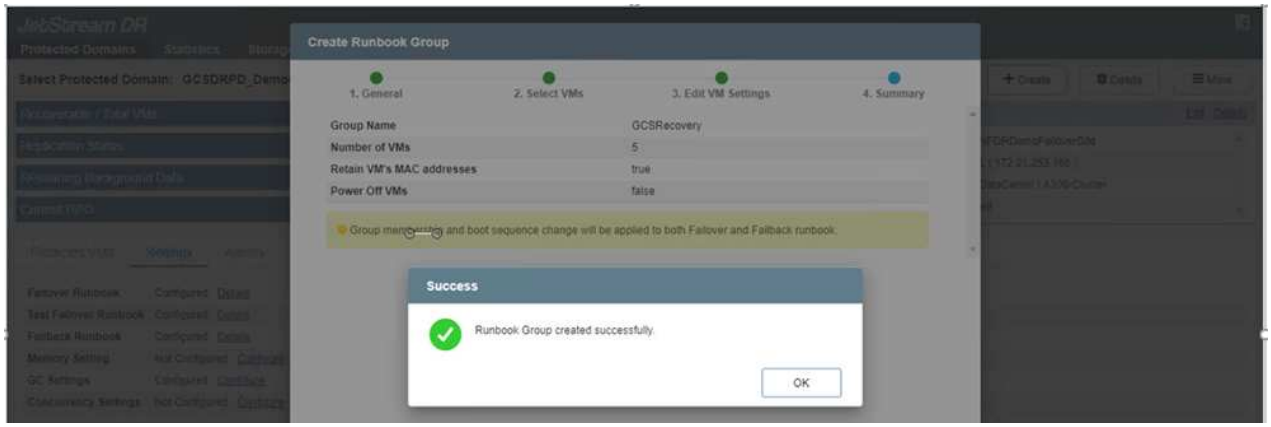


18. Las direcciones IP estáticas pueden configurarse manualmente para las máquinas virtuales individuales del grupo. Haga clic en el enlace NIC View de una máquina virtual para configurar manualmente las opciones de su dirección IP.



19. Haga clic en el botón Configure para guardar los ajustes de NIC de los equipos virtuales correspondientes.





El estado de los runbooks de conmutación por error y conmutación por recuperación se muestra ahora como configurado. Los grupos de runbooks de conmutación por error y conmutación tras recuperación se crean en parejas utilizando el mismo grupo inicial de máquinas virtuales y configuraciones. Si es necesario, la configuración de cualquier grupo runbook se puede personalizar individualmente haciendo

clic en el vínculo Detalles correspondiente y realizando cambios.

Instale JetStream DR para AVS en la nube privada

Una práctica recomendada para un sitio de recuperación (AVS) es crear un clúster de tres nodos de luz piloto con antelación. Esto permite configurar la infraestructura del centro de recuperación, lo que incluye lo siguiente:

- Segmentos de red de destino, firewalls, servicios como DHCP y DNS, etc.
- Instalación de JetStream DR para AVS
- La configuración de volúmenes ANF como almacenes de datos y mucho más

Jetstream DR admite un modo RTO casi cero para los dominios de misión crítica. Para estos dominios, el almacenamiento de destino debe estar preinstalado. ANF es un tipo de almacenamiento recomendado en este caso.

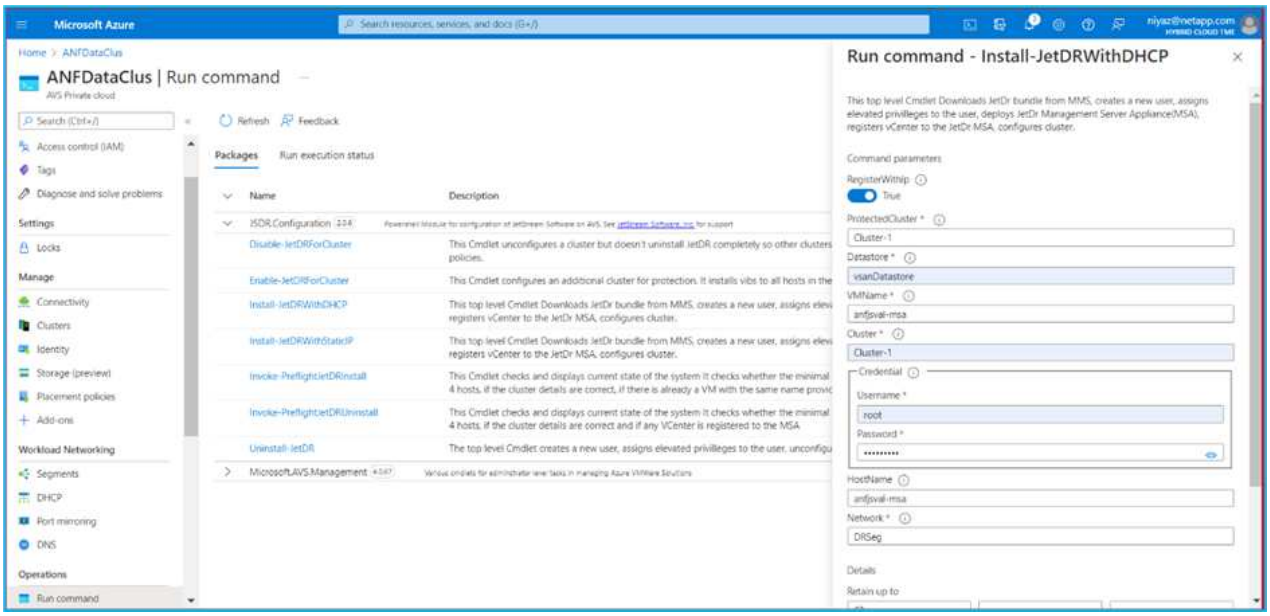
> La configuración de la red, incluida la creación de segmentos, se debe configurar en el clúster AVS para que coincida con los requisitos en las instalaciones.

> Según los requisitos del acuerdo de nivel de servicio y el objetivo de tiempo de recuperación, puede utilizar la conmutación por error continua o el modo de conmutación por error normal (estándar). Para lograr un objetivo de tiempo de recuperación cercano a cero, debe comenzar una rehidratación continua en el sitio de recuperación.

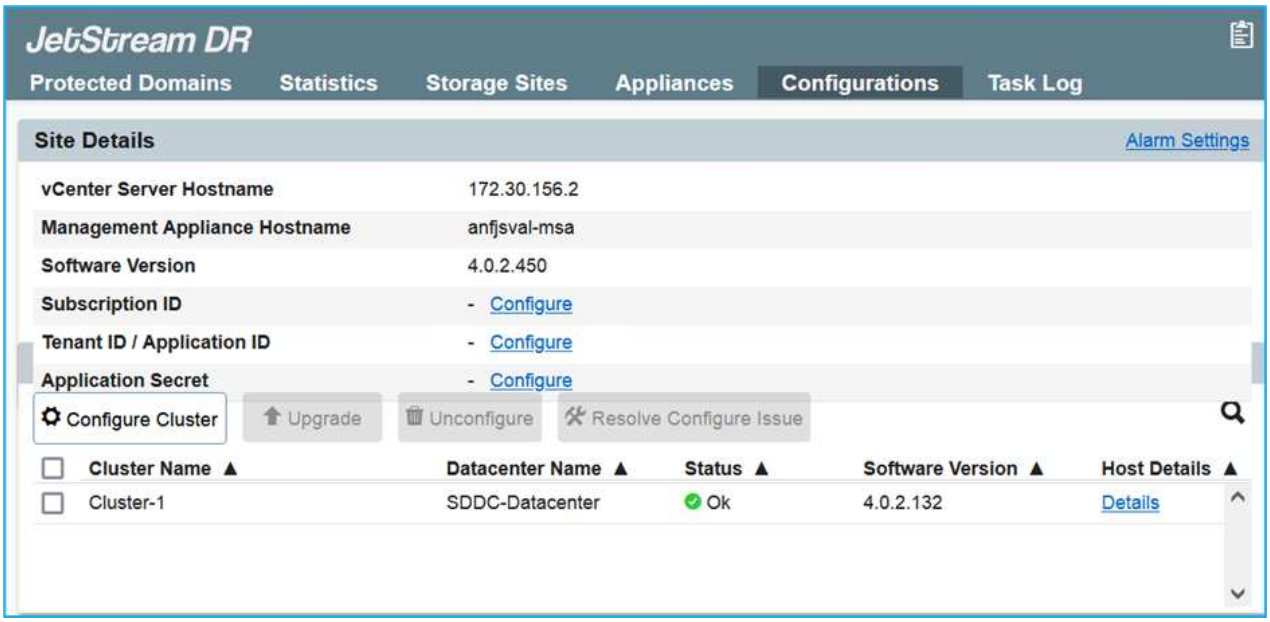
1. Para instalar JetStream DR para AVS en un cloud privado de Azure VMware Solution, utilice el comando Run. En el portal de Azure, vaya a la solución VMware de Azure, seleccione la nube privada y seleccione Ejecutar comando > Paquetes > JSDR.Configuration.

   > El usuario CloudAdmin predeterminado de la solución VMware de Azure no tiene suficientes privilegios para instalar JetStream DR para AVS. La solución Azure VMware permite una instalación simplificada y automatizada de la recuperación ante desastres de JetStream mediante la llamada al comando Azure VMware Solution Run para la recuperación ante desastres de JetStream.

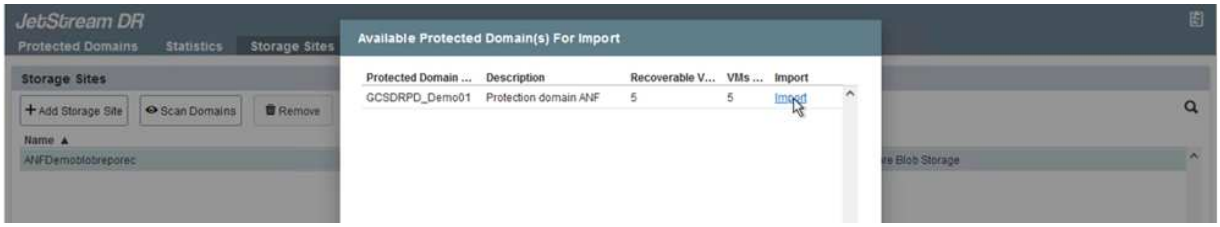
   La siguiente captura de pantalla muestra la instalación mediante una dirección IP basada en DHCP.



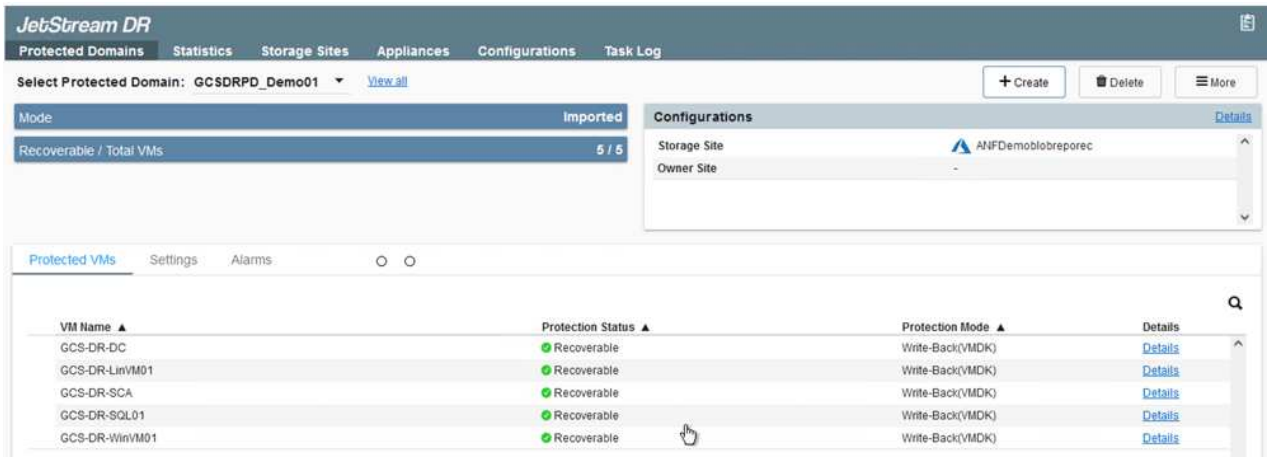
2. Una vez finalizada la instalación de JetStream DR para AVS, actualice el explorador. Para acceder a la interfaz de usuario de recuperación ante desastres de JetStream, vaya a SDDC Datacenter > Configure > JetStream DR.



3. Desde la interfaz DR de JetStream, realice las siguientes tareas:
   a. Añada la cuenta de Azure Blob Storage que se utilizó para proteger el clúster local como sitio de almacenamiento y, a continuación, ejecute la opción Scan Domains.
   b. En la ventana emergente de diálogo que aparece, seleccione el dominio protegido que desea importar y, a continuación, haga clic en el vínculo Importar.



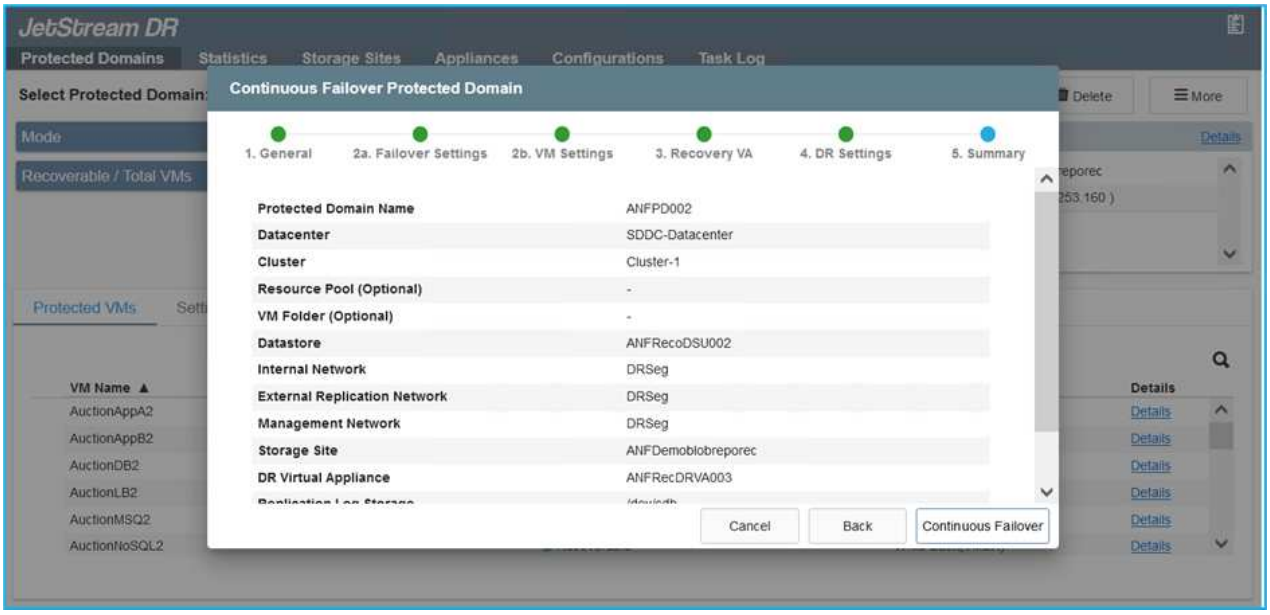
4. El dominio se importa para la recuperación. Vaya a la ficha Dominios protegidos y compruebe que el dominio deseado se ha seleccionado o elija el que desee en el menú Seleccionar dominio protegido. Se muestra una lista de las máquinas virtuales recuperables del dominio protegido.



5. Después de importar los dominios protegidos, implemente dispositivos DRVA.

> Estos pasos también se pueden automatizar mediante planes creados por CPT.

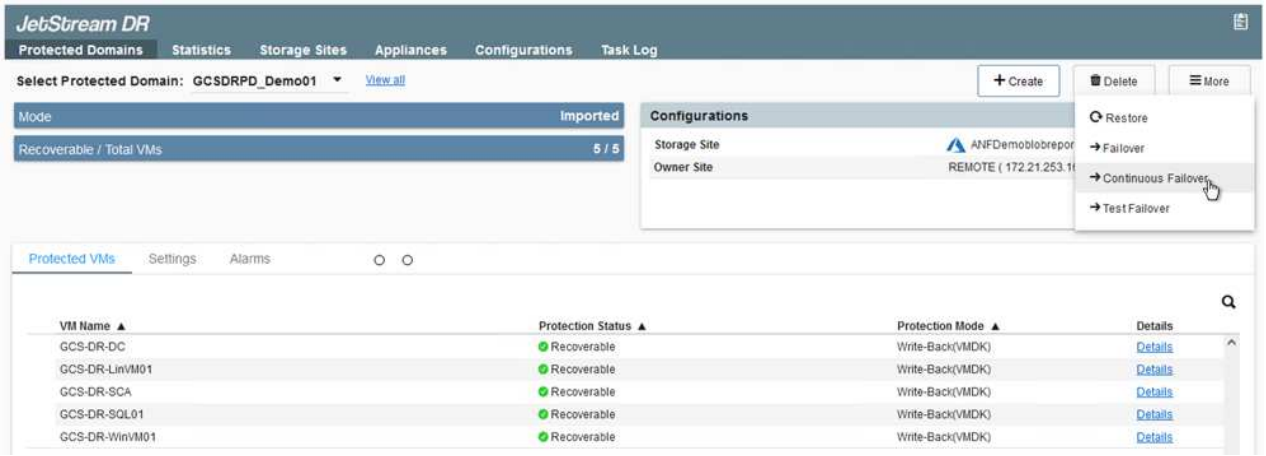
6. Cree volúmenes de registros de replicación con almacenes de datos VSAN o ANF disponibles.
7. Importe los dominios protegidos y configure el va de recuperación para utilizar un almacén de datos ANF para las ubicaciones de las máquinas virtuales.



> Asegúrese de que DHCP está habilitado en el segmento seleccionado y de que hay suficientes IP disponibles. Las IP dinámicas se utilizan temporalmente mientras se recuperan los dominios. Cada VM que se recupera (incluida la rehidratación continua) requiere una IP dinámica individual. Una vez finalizada la recuperación, se libera la IP y se puede volver a utilizar.

8. Seleccione la opción de conmutación por error adecuada (conmutación por error continua o conmutación por error). En este ejemplo, se selecciona la rehidratación continua (conmutación por error continua).

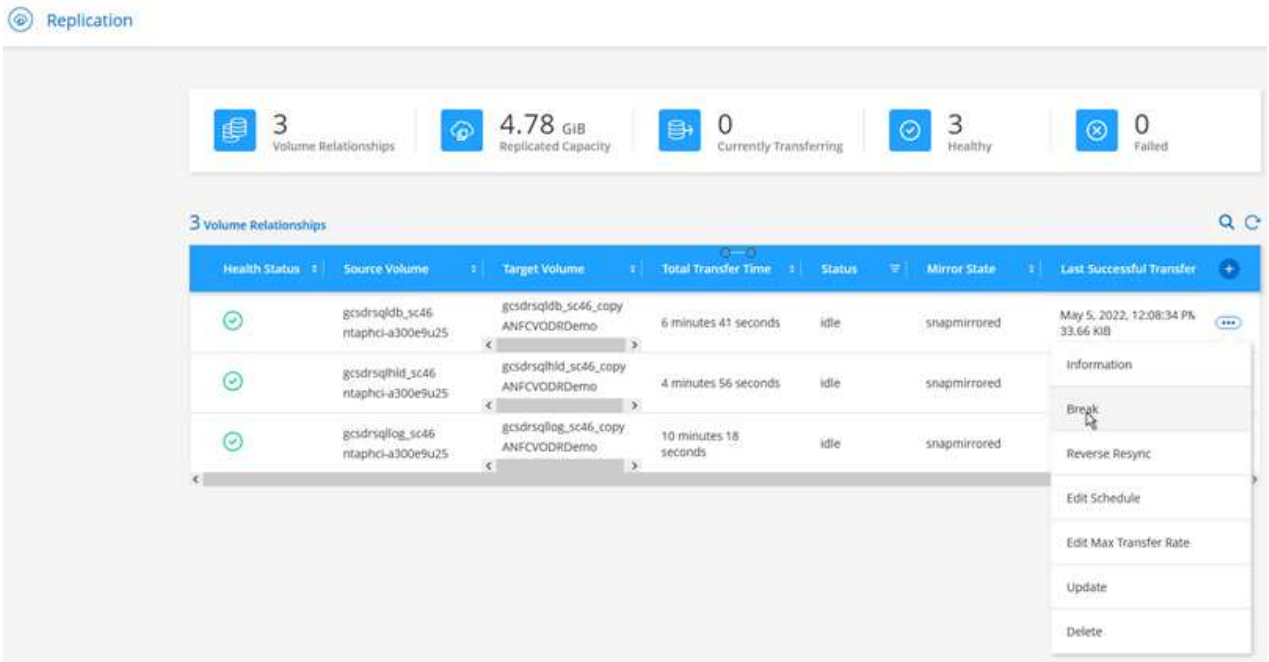
> Aunque los modos de conmutación por error continua y conmutación por error varían cuando se realiza la configuración, ambos modos de conmutación por error se configuran siguiendo los mismos pasos. Los pasos de conmutación por error se configuran y se realizan de forma conjunta en respuesta a un evento de desastre. La conmutación por error continua se puede configurar en cualquier momento y luego se puede ejecutar en segundo plano durante el funcionamiento normal del sistema. Una vez ocurrido un evento de desastre, la conmutación al respaldo continua se completa para transferir inmediatamente la propiedad de las máquinas virtuales protegidas al sitio de recuperación (objetivo de tiempo de recuperación cercano a cero).

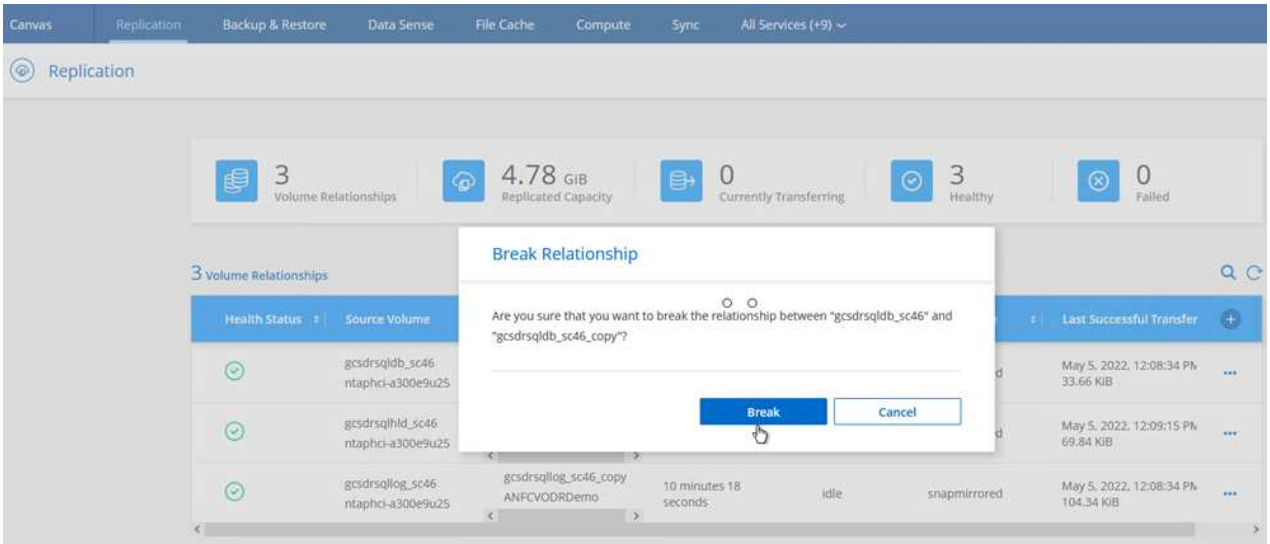


El proceso de conmutación al respaldo continua comienza y su progreso se puede supervisar desde la interfaz de usuario. Al hacer clic en el icono azul de la sección Paso actual se muestra una ventana emergente que muestra los detalles del paso actual del proceso de conmutación por error.

Conmutación por error y conmutación por recuperación

1. Cuando se produce un desastre en el clúster protegido del entorno local (fallo parcial o completo), puede activarse la conmutación por error para máquinas virtuales mediante Jetstream tras romper la relación de SnapMirror con los volúmenes de aplicaciones correspondientes.

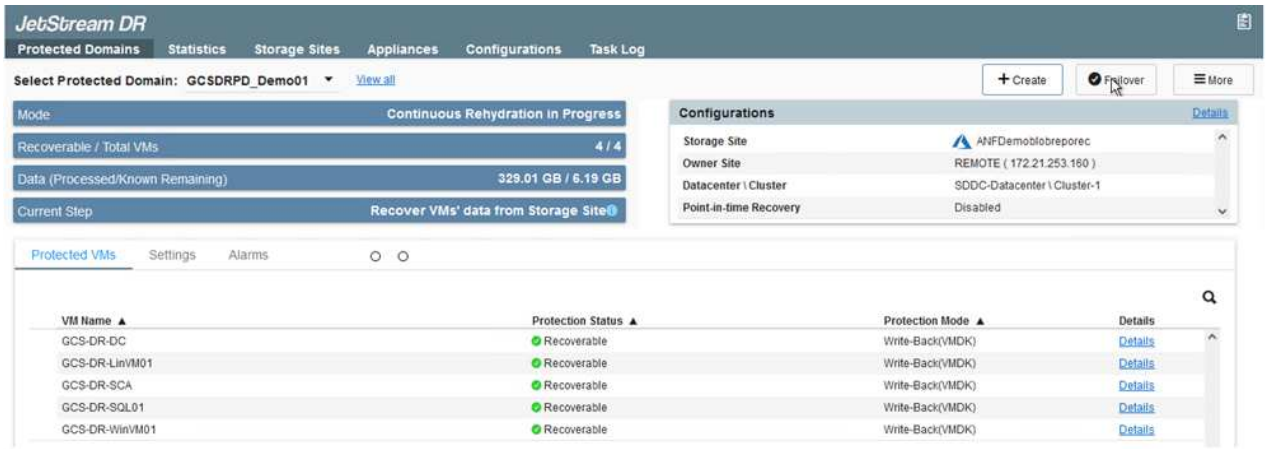


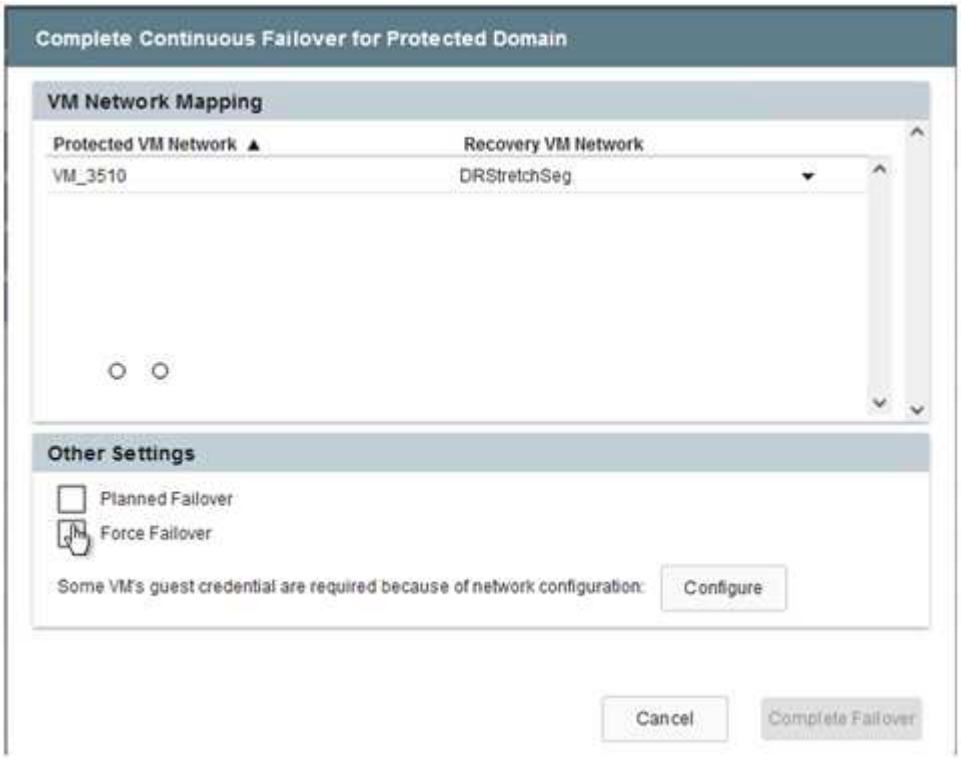


Este paso puede automatizarse fácilmente para facilitar el proceso de recuperación.

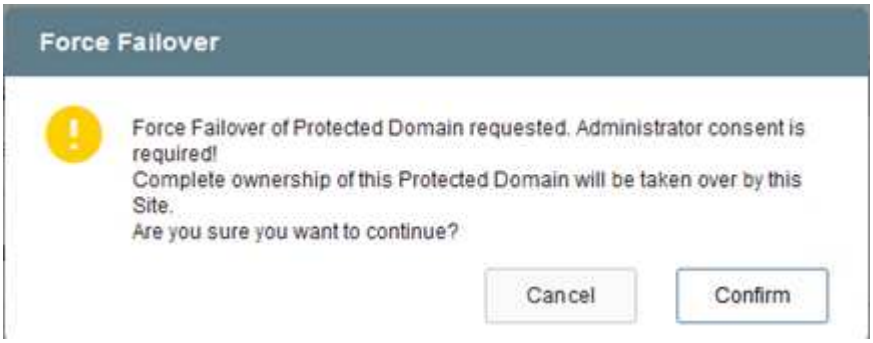
2. Acceda a Jetstream UI en AVS SDDC (destino) y active la opción de recuperación tras fallos para completar la recuperación tras fallos. La barra de tareas muestra el progreso de las actividades de failover.

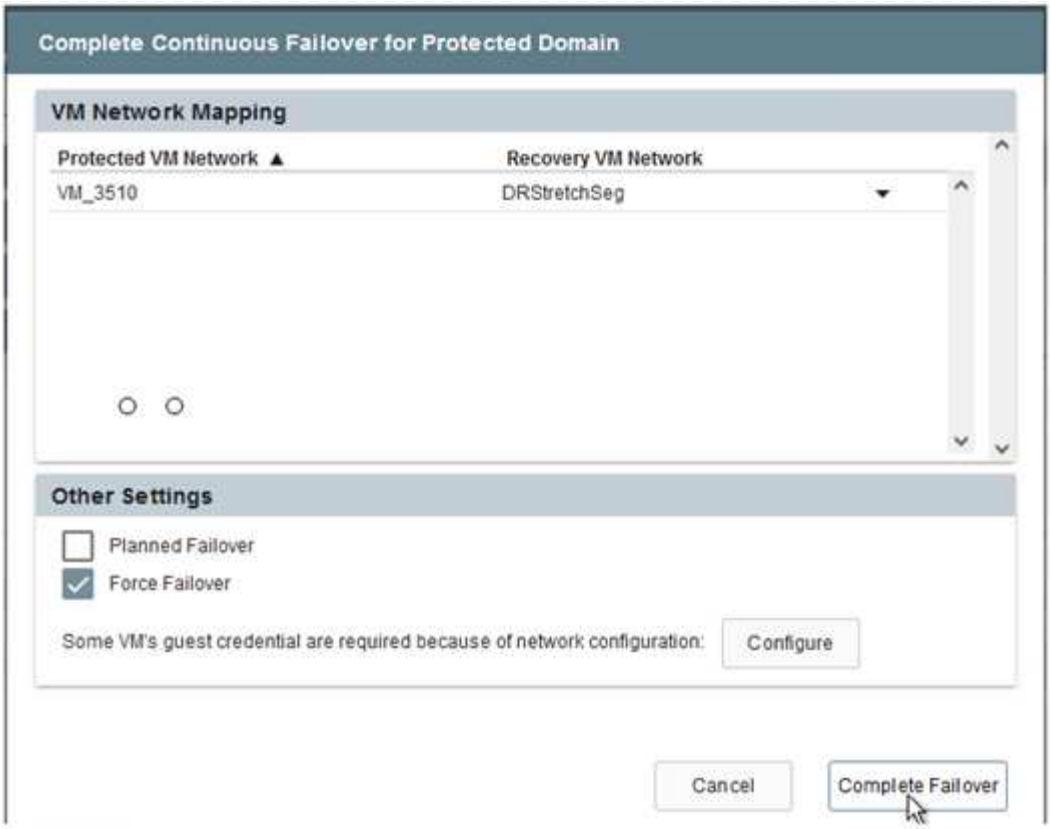
   En la ventana de diálogo que aparece al finalizar la conmutación por error, la tarea de conmutación por error se puede especificar como planificada o se supone que se fuerza.





La conmutación por error forzada asume que el sitio principal ya no está accesible y que el sitio de recuperación debería asumir directamente la propiedad del dominio protegido.



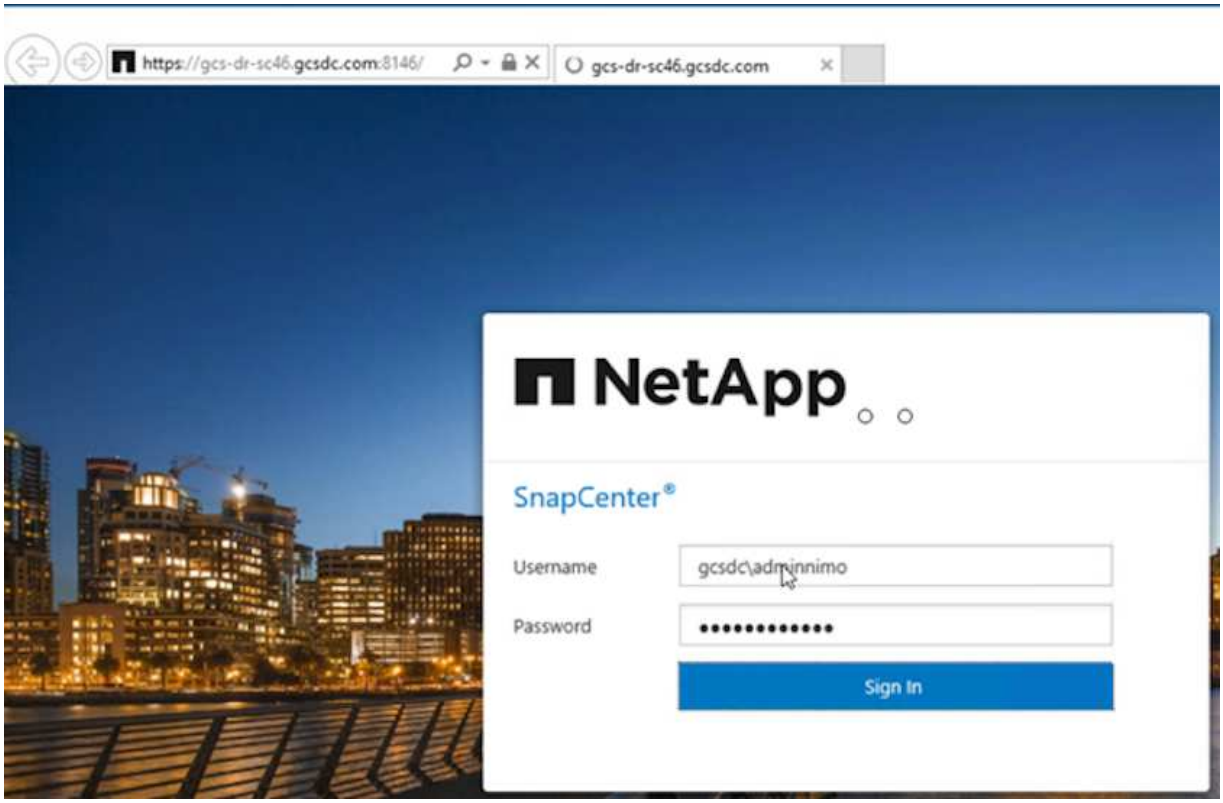


3. Una vez finalizada la conmutación por error continua, aparece un mensaje que confirma la finalización de la tarea. Una vez finalizada la tarea, acceda a los equipos virtuales recuperados para configurar sesiones ISCSI o NFS.

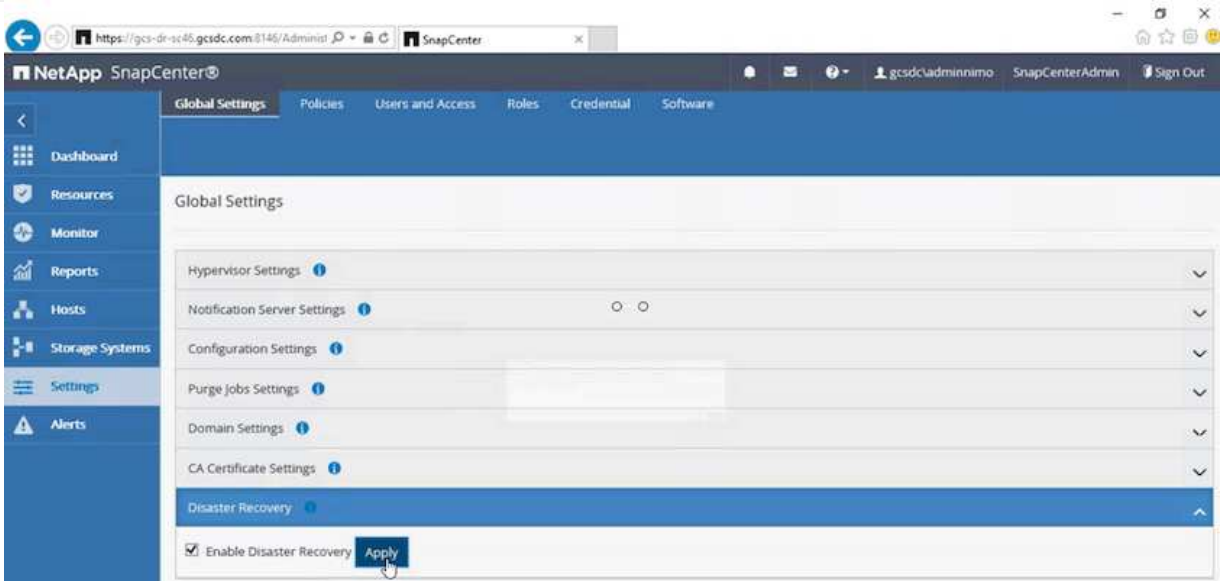
> El modo de recuperación tras fallos cambia a ejecutarse en Failover y el estado del equipo virtual es recuperable. Todas las máquinas virtuales del dominio protegido ahora se ejecutan en el sitio de recuperación con el estado especificado por la configuración de runbook para conmutación por error.

> Para verificar la configuración de recuperación tras fallos y la infraestructura, JetStream puede utilizarse en modo de prueba (opción de conmutación por error de prueba) para observar la recuperación de máquinas virtuales y sus datos desde el almacén de objetos en un entorno de recuperación de pruebas. Cuando se ejecuta un procedimiento de conmutación por error en el modo de prueba, su operación se asemeja a un proceso de conmutación por error real.

4. Después de recuperar las máquinas virtuales, utilice la recuperación ante desastres de almacenamiento para el almacenamiento invitado. Para demostrar este proceso, se utiliza SQL Server en este ejemplo.
5. Inicie sesión en el SnapCenter VM recuperado en AVS SDDC y habilite el modo de recuperación ante desastres.
   a. Acceda a la interfaz de usuario de SnapCenter mediante el comando browserN.



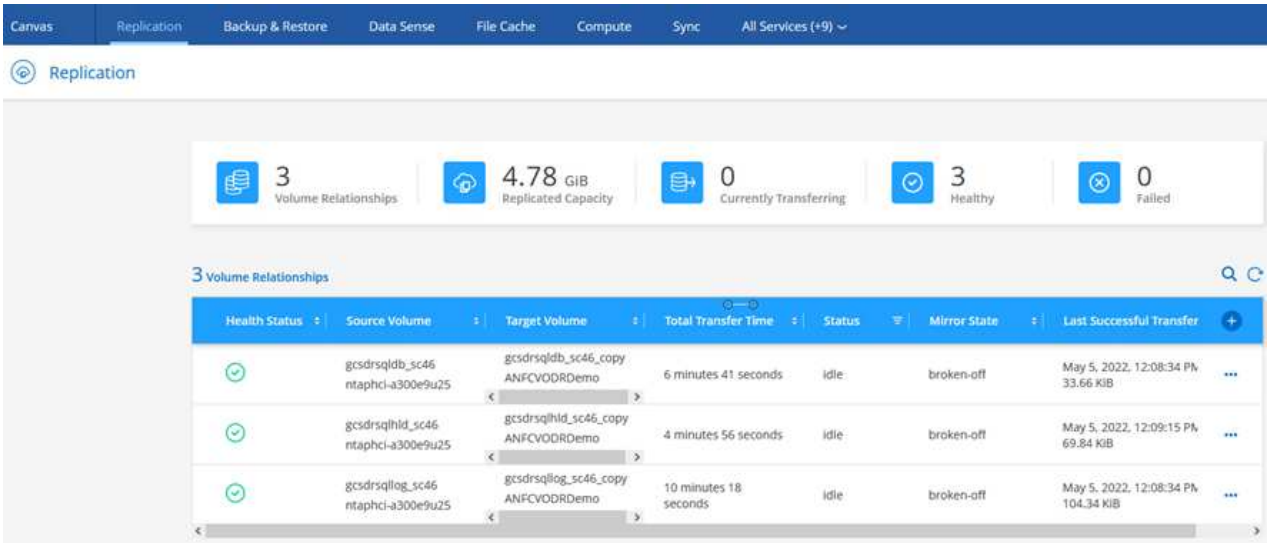
   b. En la página Settings, vaya a Settings > Global Settings > Disaster Recovery.
   c. Seleccione Enable Disaster Recovery.
   d. Haga clic en Apply.



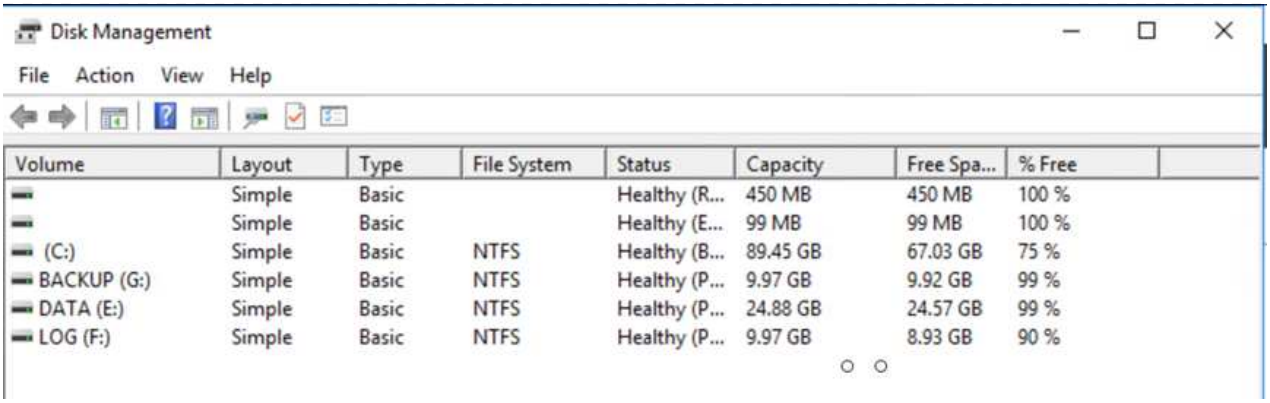
e. Compruebe si el trabajo de recuperación ante desastres está habilitado. Para ello, haga clic en Monitor > Jobs.

> NetApp SnapCenter 4.6 o posterior deben utilizarse para la recuperación ante desastres de almacenamiento. En las versiones anteriores, se deben utilizar snapshots coherentes con la aplicación (replicados mediante SnapMirror) y se debe ejecutar la recuperación manual en caso de que los backups anteriores se recuperen en el centro de recuperación ante desastres.

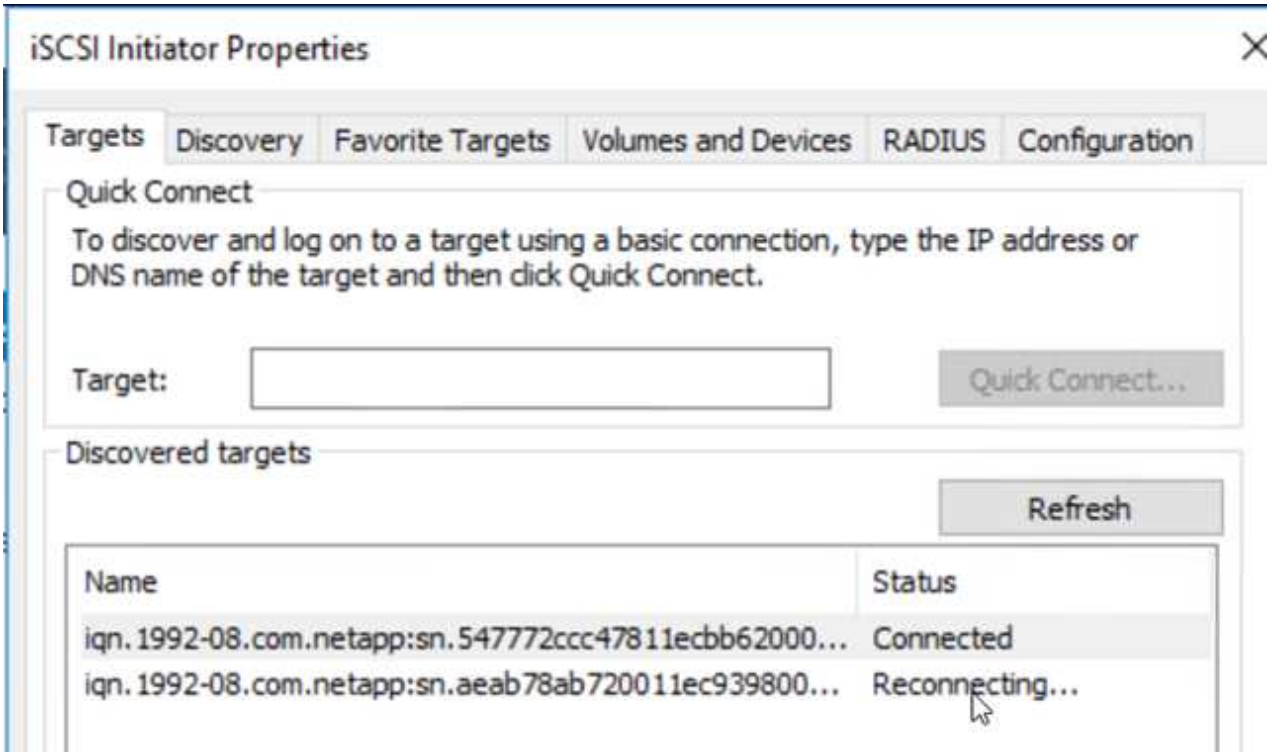
6. Asegúrese de que la relación de SnapMirror esté rota.



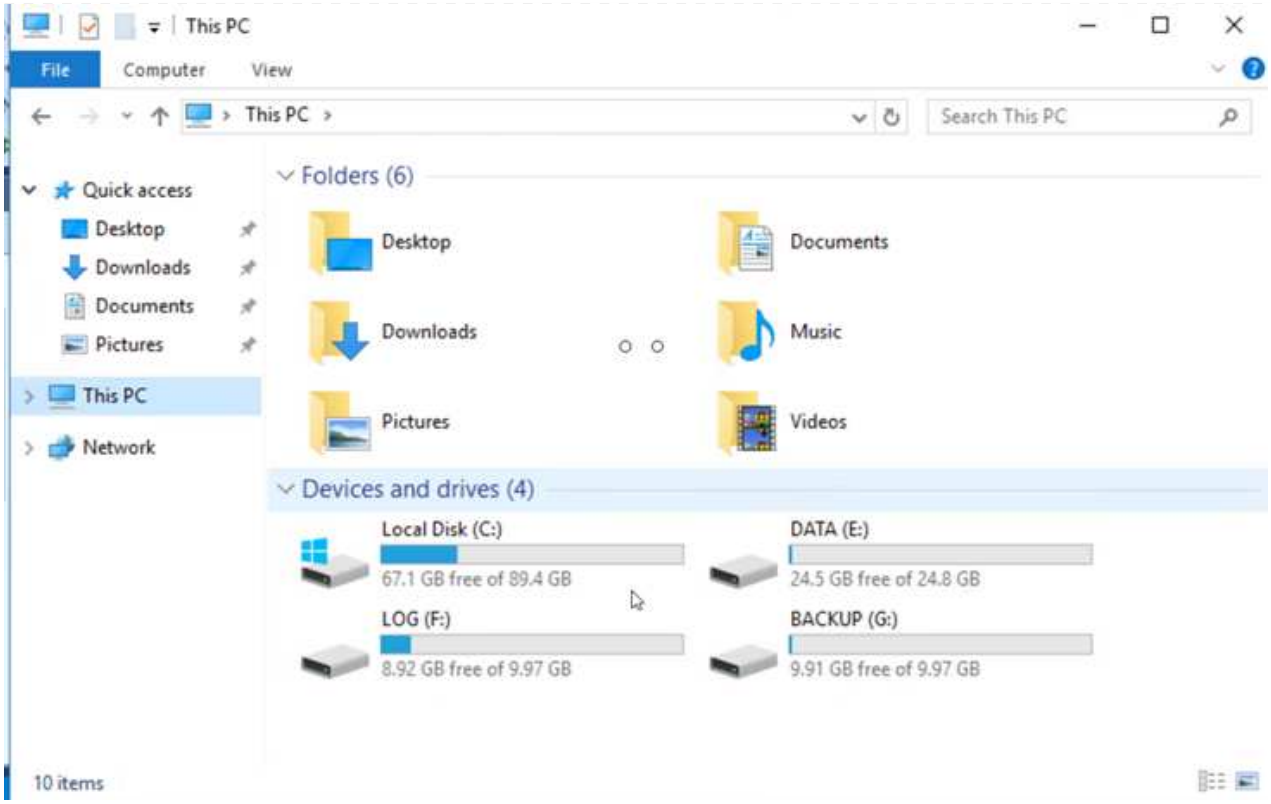
7. Asociar la LUN de Cloud Volumes ONTAP a la máquina virtual invitada de SQL recuperada con las mismas letras de unidad.



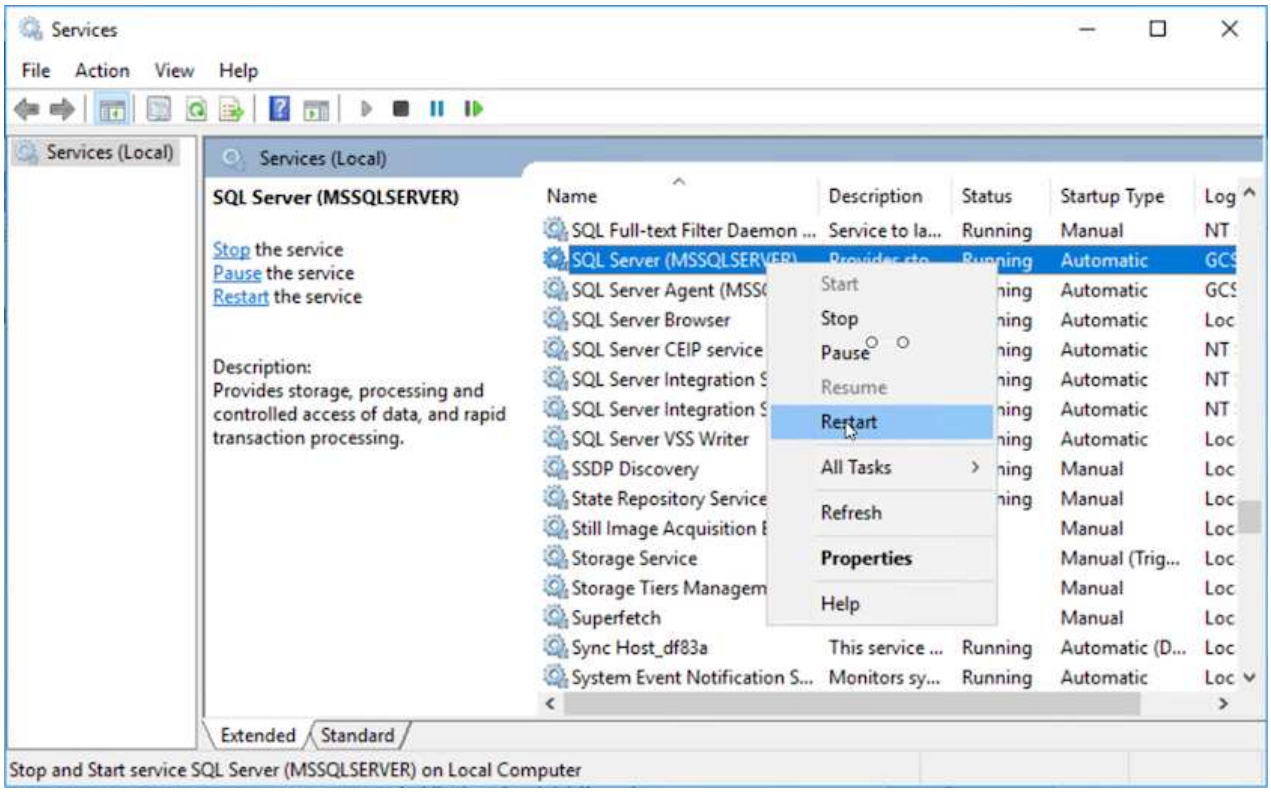
8. Abra el iniciador iSCSI, borre la sesión desconectada anterior y añada el nuevo destino junto con la multivía para los volúmenes Cloud Volumes ONTAP replicados.



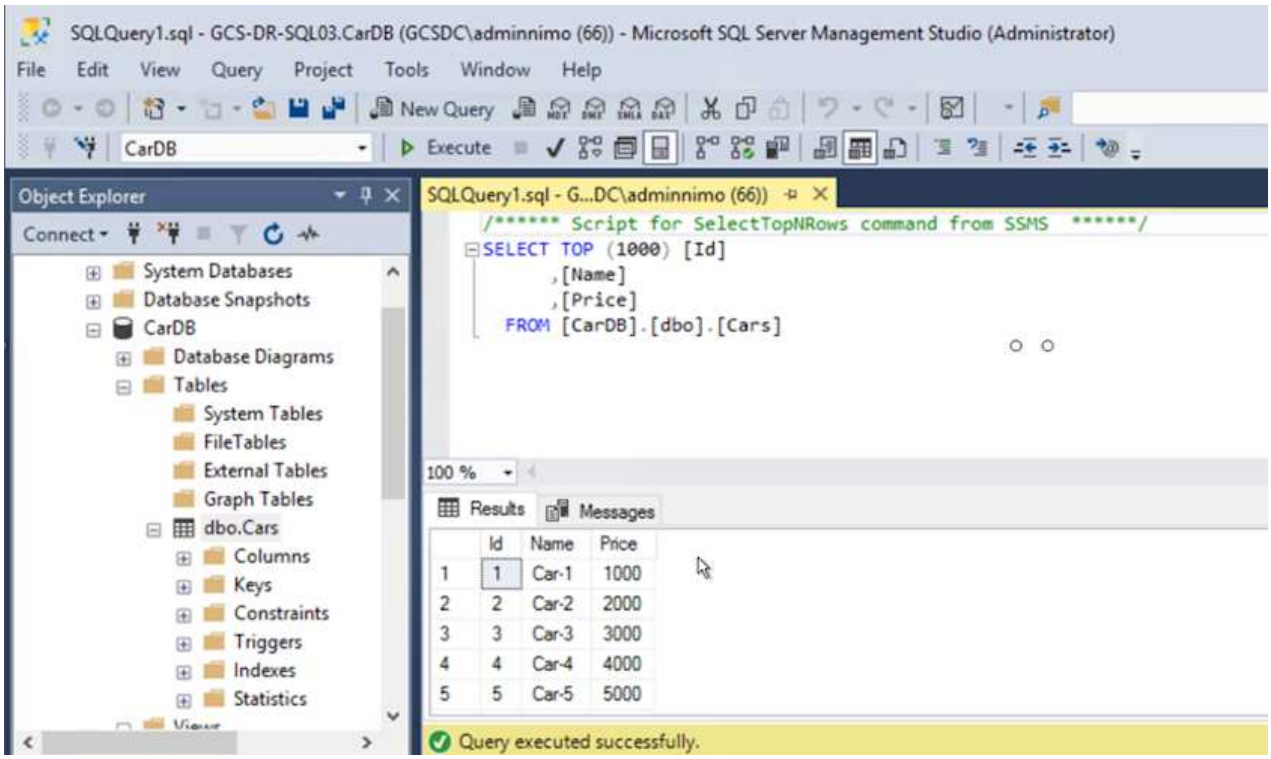
9. Asegúrese de que todos los discos están conectados utilizando las mismas letras de unidad que se usaron antes de la recuperación ante desastres.



10. Reinicie el servicio del servidor MSSQL.



11. Asegúrese de que los recursos SQL vuelven a estar en línea.



En el caso de NFS, asocie los volúmenes con el comando Mount y actualice el `/etc/fstab` entradas.

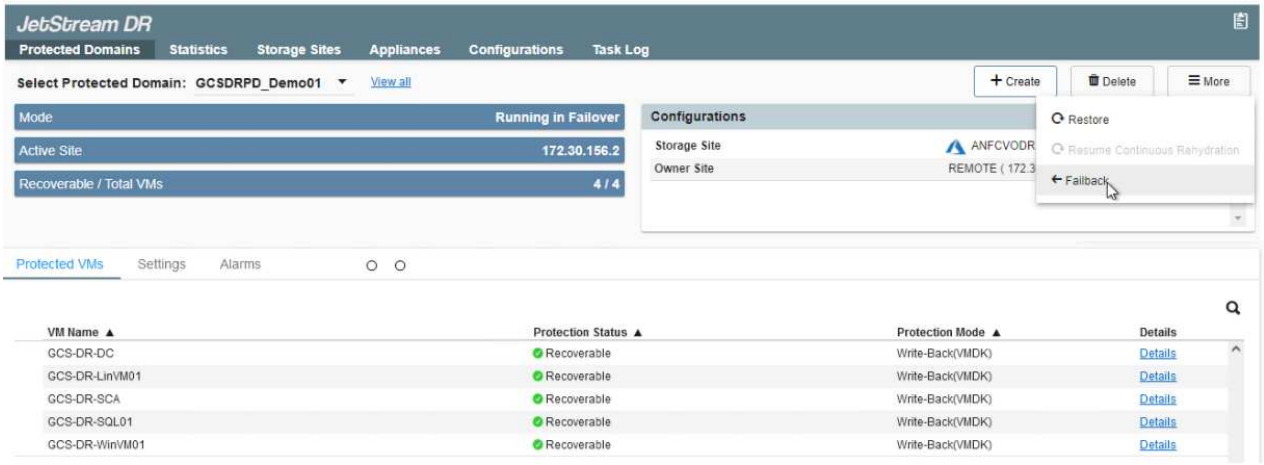
En este momento, pueden ejecutarse las operaciones y el negocio continúa de forma normal.

En el extremo de NSX-T, es posible crear una pasarela de nivel 1 dedicada separada para simular escenarios de conmutación por error. De este modo, se garantiza que todas las cargas de trabajo se puedan comunicar entre sí, pero que ningún tráfico pueda enrutarse tanto dentro como fuera del entorno, de modo que las tareas de clasificación, contención o endurecimiento se puedan realizar sin riesgo de contaminación cruzada. Esta operación se encuentra fuera del alcance de este documento, pero se puede realizar fácilmente para simular el aislamiento.

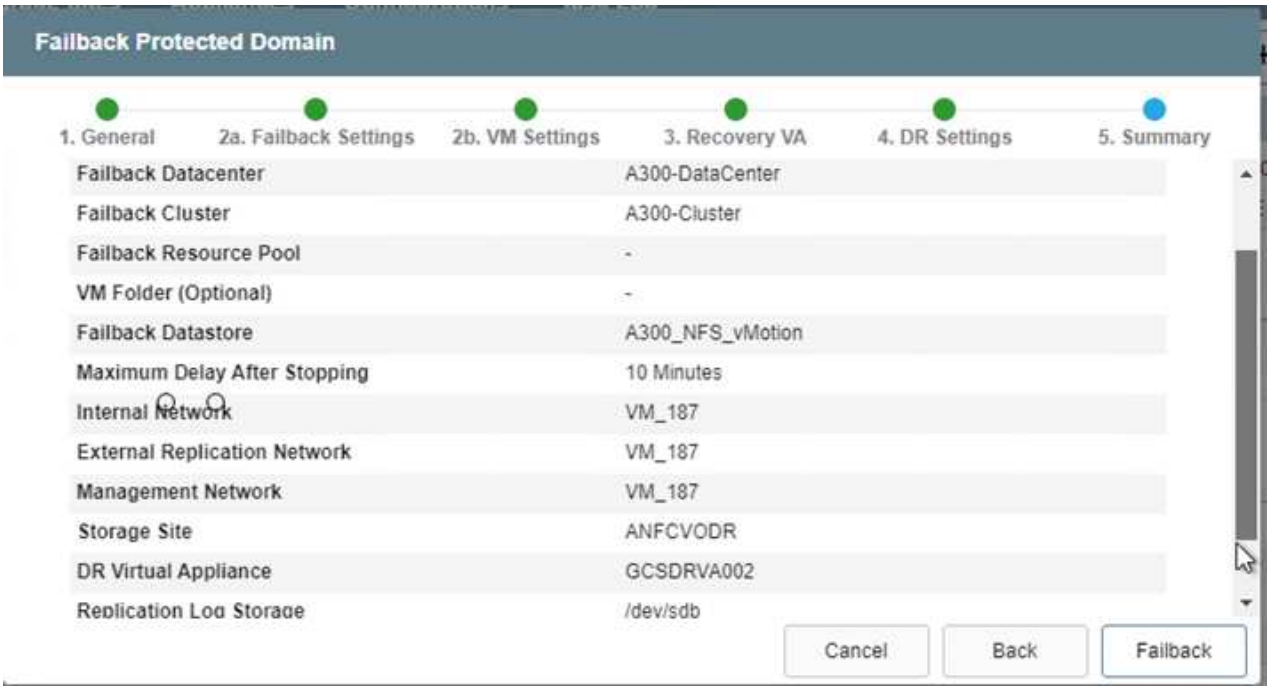
Una vez que la instalación principal esté activa y en funcionamiento de nuevo, puede realizar la conmutación tras recuperación. JetStream reanuda la protección de máquinas virtuales y debe revertirse la relación de SnapMirror.

1. Restaure el entorno de sus instalaciones. En función del tipo de incidente de desastre, podría ser necesario restaurar o verificar la configuración del clúster protegido. Si es necesario, puede que sea necesario volver a instalar el software JetStream DR.
2. Acceda al entorno local restaurado, vaya a la interfaz de usuario de recuperación ante desastres de Jetstream y seleccione el dominio protegido adecuado. Una vez que el sitio protegido esté listo para la conmutación tras recuperación, seleccione la opción de conmutación por recuperación en la interfaz de usuario.

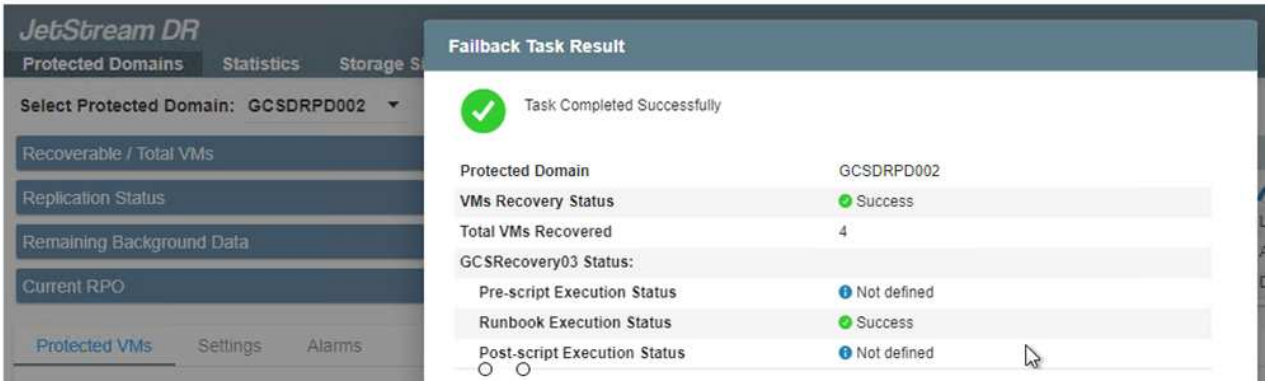
El plan de conmutación por recuperación generado por CPT también se puede usar para iniciar la devolución de los equipos virtuales y sus datos del almacén de objetos al entorno VMware original.



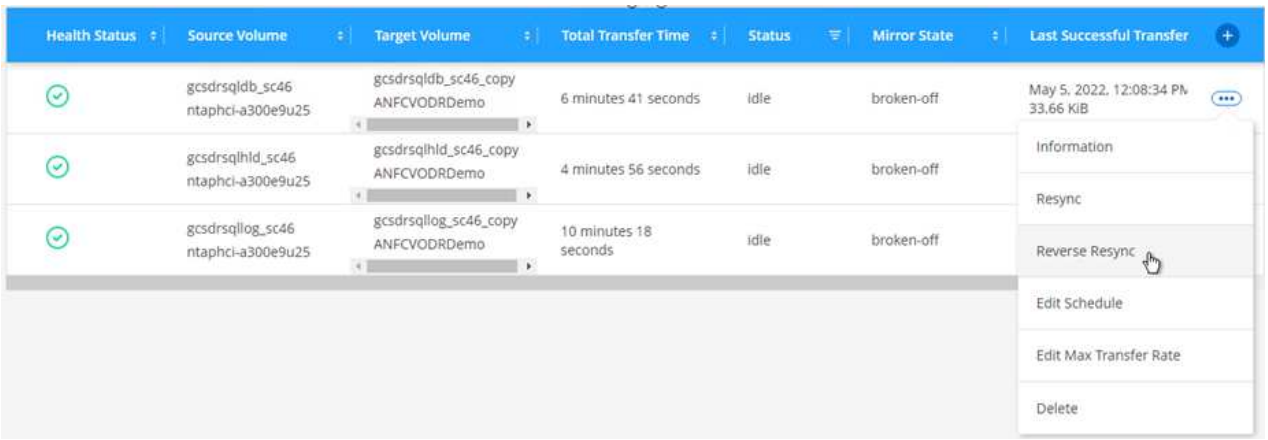
Especifique la demora máxima después de pausar las máquinas virtuales en el sitio de recuperación y reiniciarlas en el sitio protegido. El tiempo necesario para completar este proceso incluye la finalización de la replicación tras detener la conmutación por error de las máquinas virtuales, el tiempo necesario para limpiar el sitio de recuperación y el tiempo necesario para recrear las máquinas virtuales en el sitio protegido. NetApp recomienda 10 minutos.

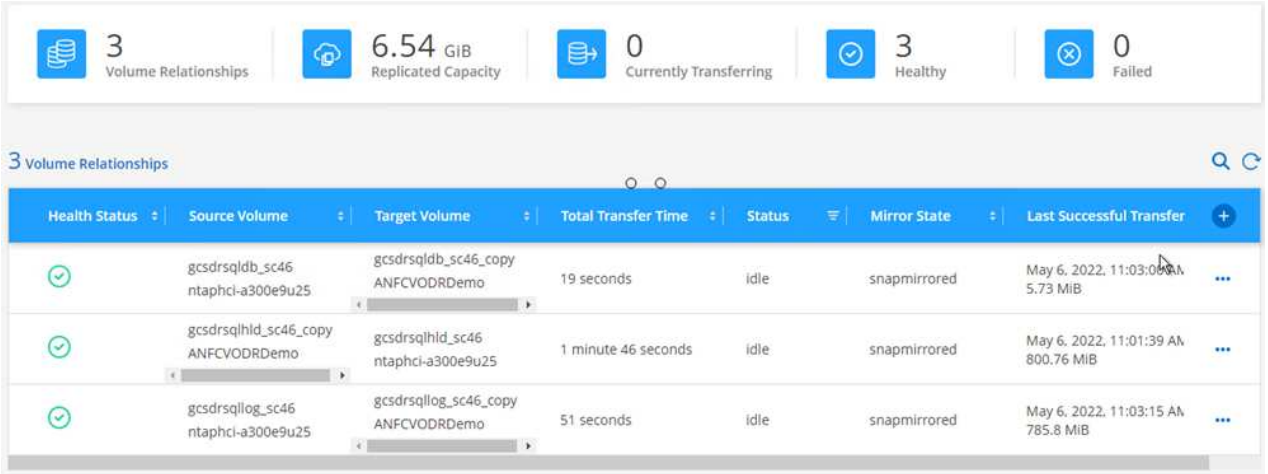


3. Completar el proceso de conmutación tras recuperación y, a continuación, confirmar la reanudación de la protección de los equipos virtuales y la consistencia de datos.

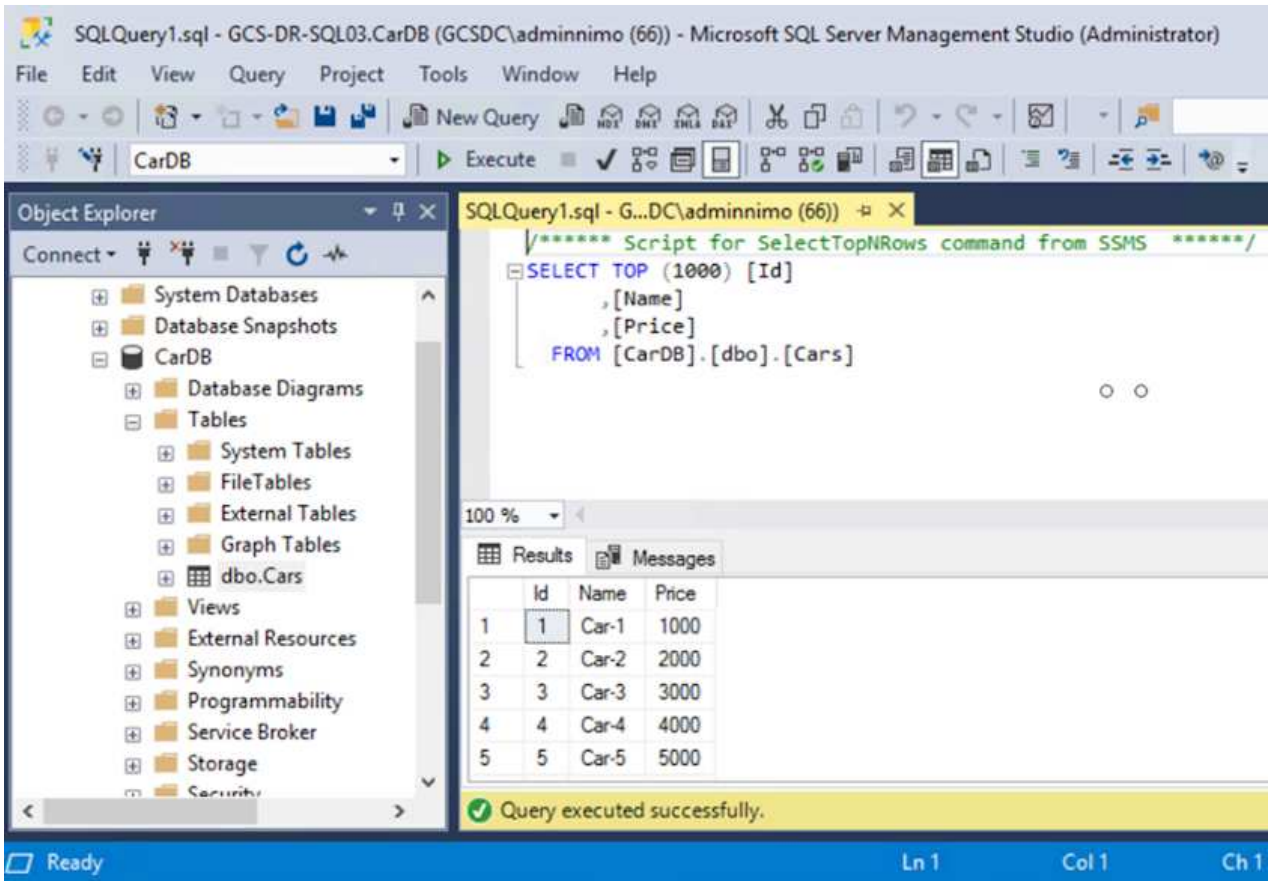


4. Una vez recuperados los equipos virtuales, desconecte el almacenamiento secundario del host y conéctelo al almacenamiento principal.





5. Reinicie el servicio del servidor MSSQL.
6. Compruebe que los recursos de SQL vuelven a estar en línea.



Para volver a realizar la conmutación tras recuperación al almacenamiento principal, asegúrese de que la dirección de la relación sigue siendo la misma que antes de la conmutación por error realizando una operación de resincronización inversa.

Para conservar las funciones de almacenamiento primario y secundario después de la operación de resincronización inversa, vuelva a realizar la operación de resincronización inversa.

Este proceso es aplicable a otras aplicaciones como Oracle, tipos de base de datos similares y cualquier otra aplicación que utilice almacenamiento conectado a «guest».

Como siempre, probar los pasos necesarios para recuperar las cargas de trabajo críticas antes de ponerlas en producción.

Ventajas de esta solución

- Usa la replicación eficiente y resiliente de SnapMirror.
- Recupera a cualquier punto disponible en el tiempo con la retención de copias Snapshot de ONTAP.
- Existe una automatización completa a disposición de todos los pasos necesarios para recuperar de cientos a miles de VM, desde los pasos de almacenamiento, computación, red y validación de aplicaciones.
- SnapCenter utiliza mecanismos de clonado que no cambian el volumen replicado.
  - Esto evita el riesgo de daños en los datos de los volúmenes y las Snapshot.

- Evita interrupciones de replicación durante los flujos de trabajo de pruebas de recuperación ante desastres.
- Aprovecha los datos de recuperación ante desastres para flujos de trabajo que van más allá de la recuperación ante desastres, como las fases de desarrollo y pruebas, pruebas de seguridad, pruebas de parches y actualizaciones, y pruebas para solucionar problemas.

- La optimización de la CPU y la RAM puede ayudar a reducir los costes del cloud al permitir la recuperación en clústeres informáticos más pequeños.

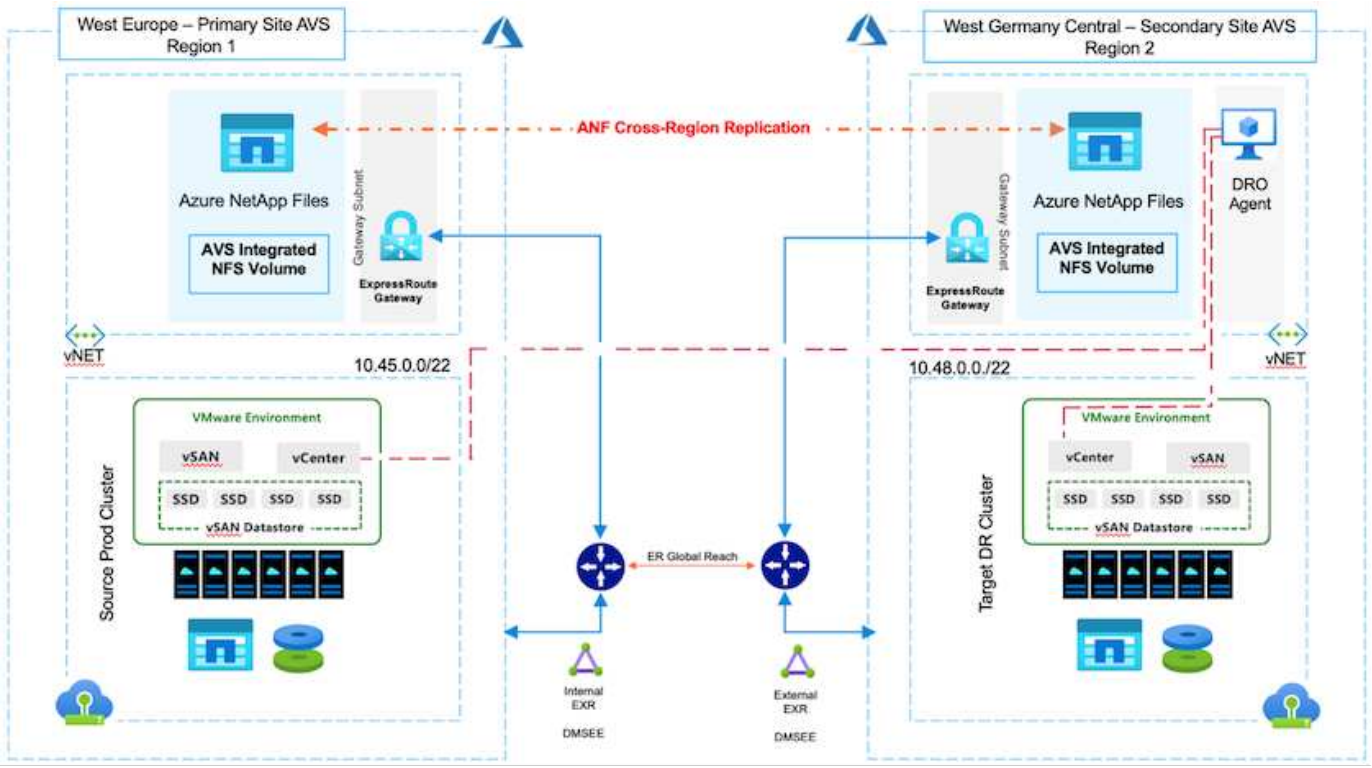
TR-4955: Recuperación ante desastres con Azure NetApp Files (ANF) y la solución VMware de Azure (AVS)

Autor(es): Niyaz Mohamed, Ingeniería de Soluciones NetApp

Descripción general

La recuperación ante desastres mediante replicación a nivel de bloques entre regiones del cloud es un método resiliente y rentable de proteger las cargas de trabajo frente a interrupciones del servicio del sitio y eventos de corrupción de datos (por ejemplo, ransomware). Con la replicación de volúmenes entre regiones de Azure NetApp Files (ANF), las cargas de trabajo de VMware que se ejecutan en un sitio SDDC de Azure VMware Solution (AVS) usando Azure NetApp Files Volumes como almacén de datos NFS en el sitio de AVS principal se pueden replicar en un sitio de AVS secundario designado en la región de recuperación de destino.

El orquestador de recuperación ante desastres (DRO) (una solución basada en secuencia de comandos con una interfaz de usuario) puede utilizarse para recuperar sin problemas las cargas de trabajo replicadas desde un SDDC de AVS a otro. DRO automatiza la recuperación rompiendo la paridad de replicación y luego montando el volumen de destino como almacén de datos, a través del registro de VM en AVS, a las asignaciones de red directamente en NSX-T (incluido con todos los clouds privados de AVS).



Requisitos previos y recomendaciones generales

- Compruebe que ha habilitado la replicación entre regiones mediante la creación de pares de replicación. Consulte "Crear replicación de volúmenes para Azure NetApp Files".
- Debe configurar ExpressRoute Global Reach entre los clouds privados de Azure VMware Solution de origen y destino.
- Debe tener un principal de servicio que pueda acceder a los recursos.
- Se admite la siguiente topología: Sitio AVS primario al sitio AVS secundario.
- Configure el "replicación" programe cada volumen de forma apropiada según las necesidades empresariales y la tasa de cambio de datos.

> No se admiten las topologías en cascada y con ventilador de entrada y salida.

Primeros pasos

Implementa la solución de VMware para Azure

La "Solución Azure VMware" (AVS) es un servicio de cloud híbrido que proporciona SDDC de VMware totalmente funcionales dentro de un cloud público de Microsoft Azure. AVS es una solución de primera parte totalmente gestionada y compatible con Microsoft y verificada por VMware que utiliza infraestructura de Azure. Por lo tanto, los clientes obtienen VMware ESXi para virtualización informática, vSAN para almacenamiento hiperconvergente y NSX para redes y seguridad, y todo ello al tiempo que aprovechan la presencia global de Microsoft Azure, instalaciones de centros de datos líderes de su clase y la proximidad al rico ecosistema de servicios y soluciones nativos de Azure. Una combinación de un SDDC de la solución para Azure VMware y Azure NetApp Files proporciona el mejor rendimiento con una latencia de red mínima.

Para configurar una nube privada AVS en Azure, siga los pasos que se indican en este "enlace" Para la documentación de NetApp y en este "enlace" Para obtener documentación de Microsoft. Se puede utilizar un entorno piloto configurado con una configuración mínima para recuperaciones ante desastres. Esta configuración solo contiene componentes principales para admitir aplicaciones esenciales y puede escalar horizontalmente y generar más hosts para asumir la mayor carga si se produce una recuperación tras fallos.

> En la versión inicial, DRO admite un clúster SDDC AVS existente. La creación bajo demanda de SDDC estará disponible en una próxima versión.

Aprovisione y configure Azure NetApp Files

"Azure NetApp Files" es un servicio de almacenamiento de archivos de uso medido, de nivel empresarial y de alto rendimiento. Siga los pasos que se indican a continuación "enlace" Para aprovisionar y configurar Azure NetApp Files como almacén de datos NFS para optimizar las puestas en marcha de cloud privado de AVS.

Crear una replicación de volumen para volúmenes de almacenes de datos que funcionan con Azure NetApp Files

El primer paso es configurar la replicación entre regiones para los volúmenes de almacén de datos deseados desde el sitio primario AVS al sitio secundario AVS con las frecuencias y retenciones apropiadas.

Siga los pasos que se indican a continuación "enlace" para configurar la replicación entre regiones mediante la creación de pares de replicación. El nivel de servicio del pool de capacidad de destino puede coincidir con el del pool de capacidad de origen. Sin embargo, para este caso de uso específico, puede seleccionar el nivel de servicio estándar y luego "modificar el nivel de servicio" En caso de desastre real o simulaciones de recuperación ante desastres.

> Una relación de replicación entre regiones es un requisito previo y debe crearse de antemano.

Instalación DE DRO

Para comenzar con DRO, use el sistema operativo Ubuntu en la máquina virtual de Azure designada y asegúrese de cumplir con los requisitos previos. A continuación, instale el paquete.

Requisitos previos:

- Principal de servicio que puede acceder a los recursos.
- Asegúrese de que existe conectividad adecuada con las instancias de SDDC y Azure NetApp Files de origen y destino.
- La resolución DNS debe estar en su lugar si está utilizando nombres DNS. De lo contrario, use direcciones IP para vCenter.

Requisitos del sistema operativo:

- Ubuntu Focal 20,04 (LTS)Los siguientes paquetes deben instalarse en la máquina virtual del agente designado:
- Docker
- Docker: Componer
- JqChange `docker.sock` para este nuevo permiso: `sudo chmod 666 /var/run/docker.sock`.

> La `deploy.sh` el script ejecuta todos los requisitos necesarios.

Los pasos son los siguientes:

1. Descargue el paquete de instalación en la máquina virtual designada:

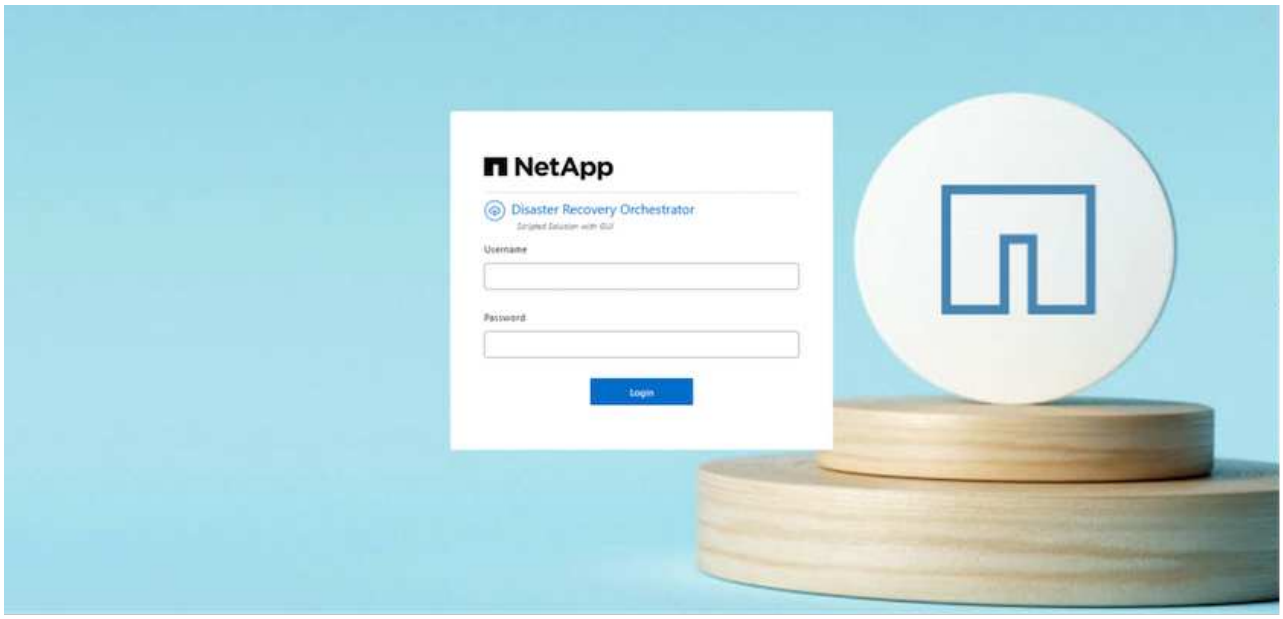
```
git clone https://github.com/NetApp/DRO-Azure.git
```

> El agente debe instalarse en la región del sitio AVS secundario o en la región del sitio AVS principal en una zona de área de servicio independiente que el SDDC.

2. Descomprima el paquete, ejecute el script de despliegue e introduzca la IP del host (por ejemplo, `10.10.10.10`).

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. Acceda a la interfaz de usuario con las siguientes credenciales:
   - Nombre de usuario: `admin`
   - Contraseña: `admin`



Configuración DE DRO

Después de que Azure NetApp Files y AVS se hayan configurado correctamente, puede comenzar a configurar DRO para automatizar la recuperación de cargas de trabajo desde el sitio AVS principal al sitio AVS secundario. NetApp recomienda la puesta en marcha del agente DRO en el sitio AVS secundario y la configuración de la conexión de puerta de enlace ExpressRoute para que el agente DRO pueda comunicarse a través de la red con los componentes de AVS y Azure NetApp Files adecuados.

El primer paso es agregar credenciales. DRO requiere permiso para descubrir Azure NetApp Files y la solución Azure VMware. Puede otorgar los permisos necesarios a una cuenta de Azure creando y configurando una aplicación de Azure Active Directory (AD) y obteniendo las credenciales de Azure que DRO necesita. Debe enlazar el principal de servicio a su suscripción de Azure y asignarle un rol personalizado que tenga los permisos necesarios relevantes. Al agregar entornos de origen y destino, se le solicita que seleccione las credenciales asociadas al principal de servicio. Debe agregar estas credenciales a DRO antes de hacer clic en Agregar nuevo sitio.

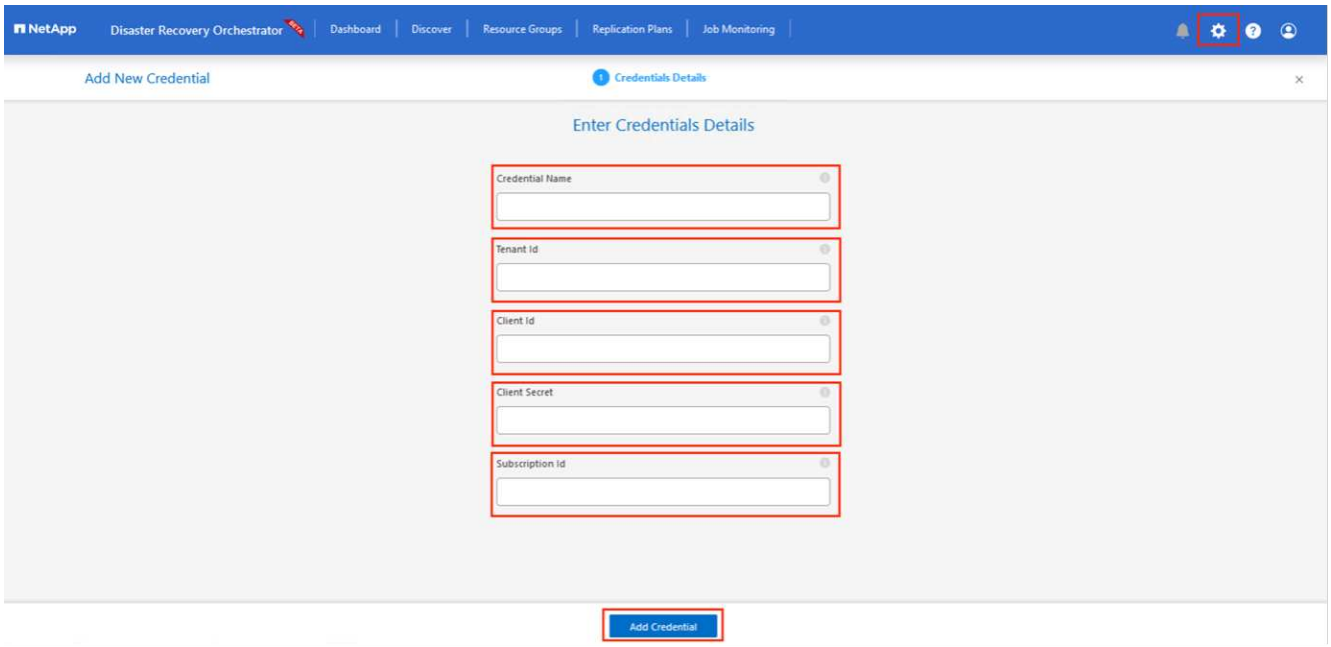
Para realizar esta operación, complete los siguientes pasos:

1. Abra DRO en un navegador compatible y utilice el nombre de usuario y la contraseña predeterminados /`admin`/`admin`). La contraseña se puede restablecer después del primer inicio de sesión mediante la

opción Cambiar contraseña.

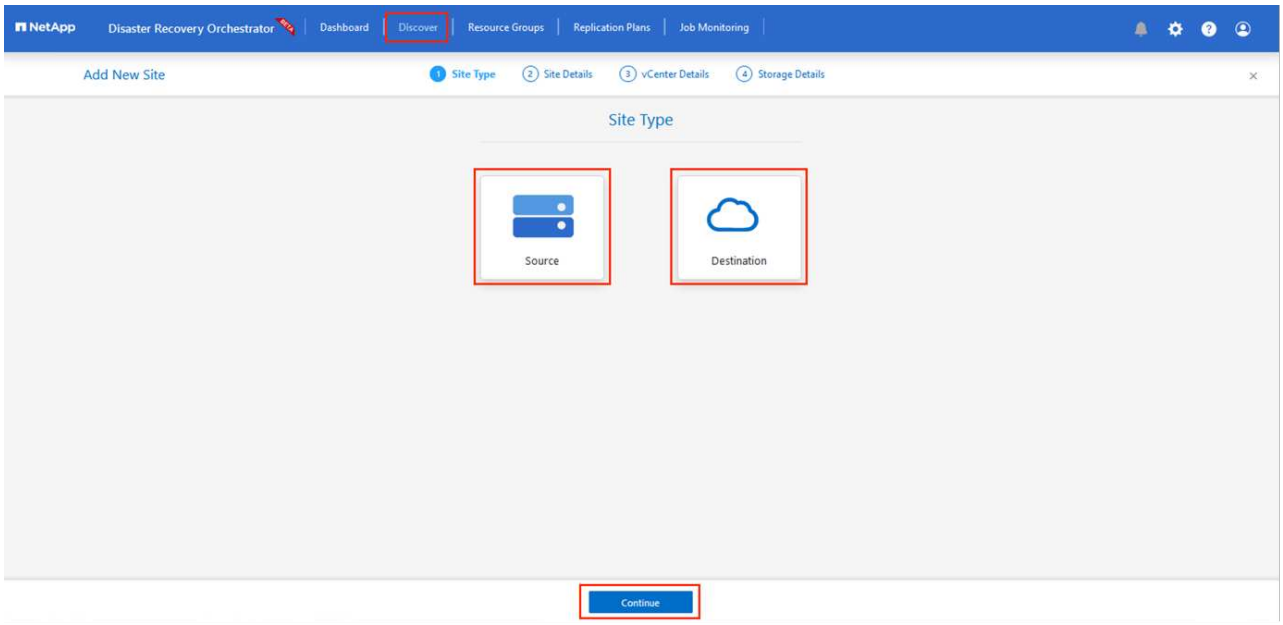
2. En la parte superior derecha de la consola de DRO, haga clic en el icono **Configuración** y seleccione **Credenciales**.
3. Haga clic en Add New Credential y siga los pasos del asistente.
4. Para definir las credenciales, introduzca información sobre el principal de servicio de Azure Active Directory que otorga los permisos necesarios:
   - Nombre de credencial
   - ID de inquilino
   - ID del cliente
   - Secreto de cliente
   - ID de suscripción

     Debe haber capturado esta información al crear la aplicación AD.
5. Confirme los detalles sobre las nuevas credenciales y haga clic en Add Credential.



Después de agregar las credenciales, es hora de detectar y agregar los sitios de AVS principales y secundarios (tanto vCenter como la cuenta de almacenamiento de Azure NetApp Files) a DRO. Para agregar el sitio de origen y destino, realice los siguientes pasos:

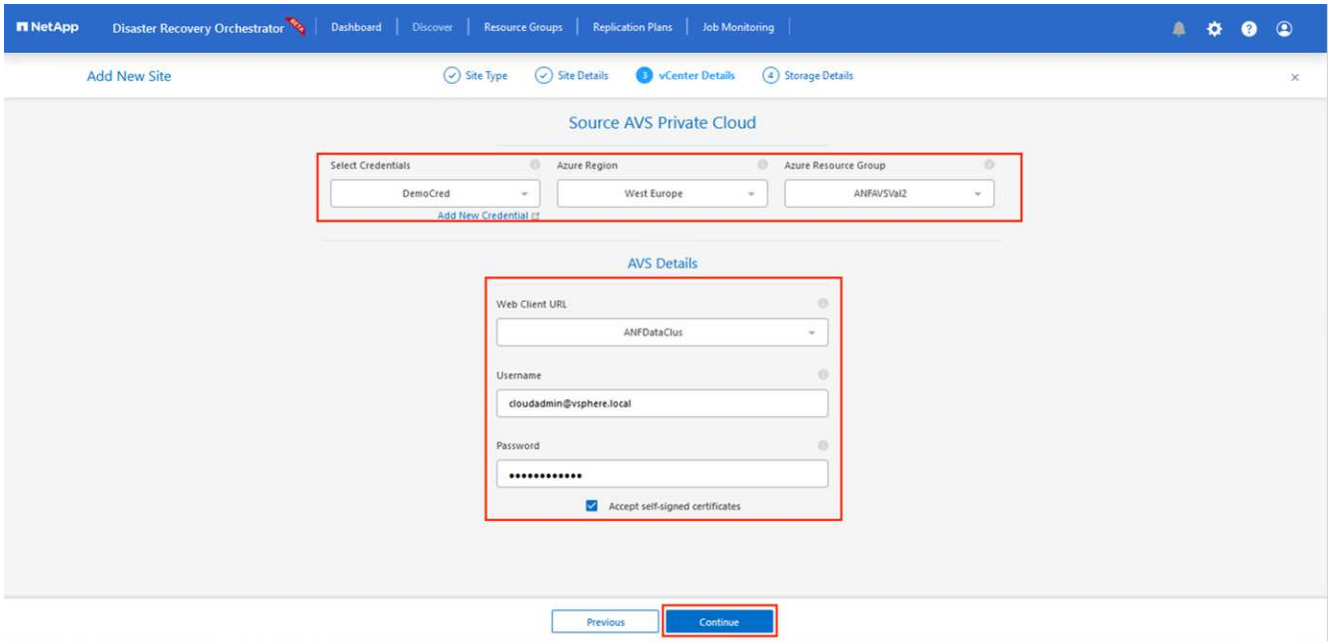
6. Vaya a la pestaña **Discover**.
7. Haga clic en **Agregar nuevo sitio**.
8. Agregue el siguiente sitio AVS principal (designado como **Source** en la consola).
   - SDDC vCenter
   - Cuenta de almacenamiento de Azure NetApp Files
9. Agregue el siguiente sitio AVS secundario (designado como **Destino** en la consola).
   - SDDC vCenter
   - Cuenta de almacenamiento de Azure NetApp Files



10. Agregue los detalles del sitio haciendo clic en **Fuente**, ingresando un nombre de sitio amigable, y seleccione el conector. A continuación, haga clic en **continuar**.

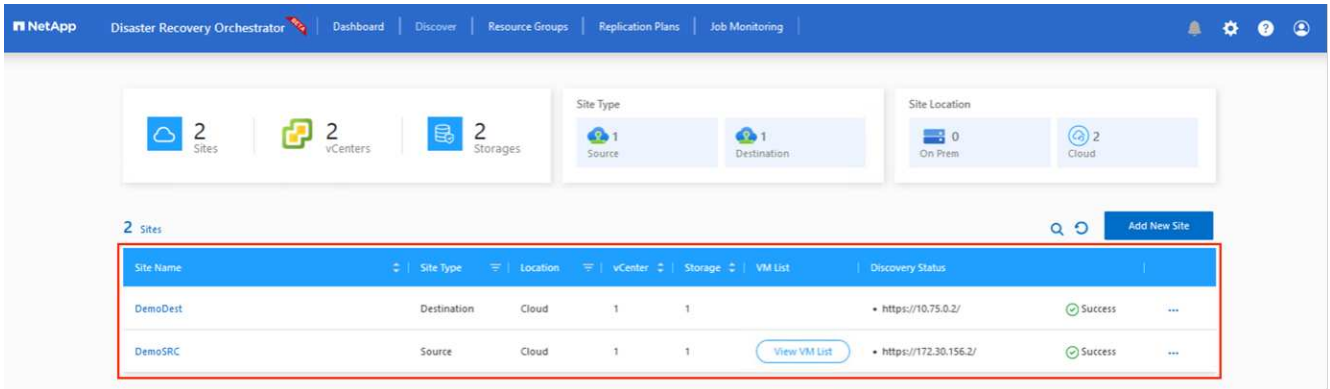
> A modo de demostración, en este documento se trata la adición de un sitio de origen.

11. Actualice los detalles de vCenter. Para ello, seleccione las credenciales, la región de Azure y el grupo de recursos del menú desplegable para el AVS SDDC principal.
12. DRO muestra todos los SDDC disponibles dentro de la región. Seleccione la URL de cloud privado designada del menú desplegable.
13. Introduzca el `cloudadmin@vsphere.local` credenciales de usuario. A esto se puede acceder desde Azure Portal. Siga los pasos mencionados en este "enlace". Una vez hecho esto, haga clic en **Continuar**.

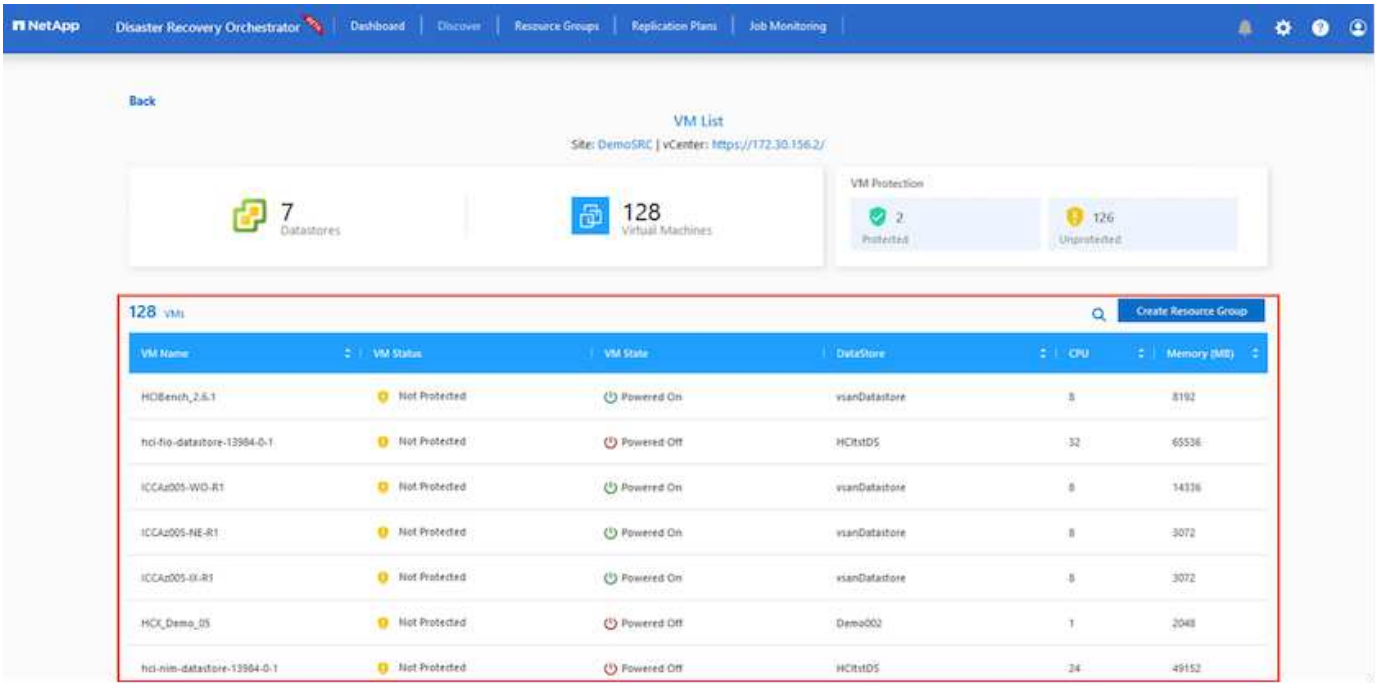


14. Seleccione los detalles de Source Storge (ANF) seleccionando el grupo de recursos de Azure y la cuenta de NetApp.

15. Haga clic en **Crear sitio**.



Una vez agregado, DRO realiza la detección automática y muestra las máquinas virtuales que tienen las réplicas entre regiones correspondientes desde el sitio de origen al sitio de destino. DRO detecta automáticamente las redes y los segmentos que utilizan las máquinas virtuales y los rellena.



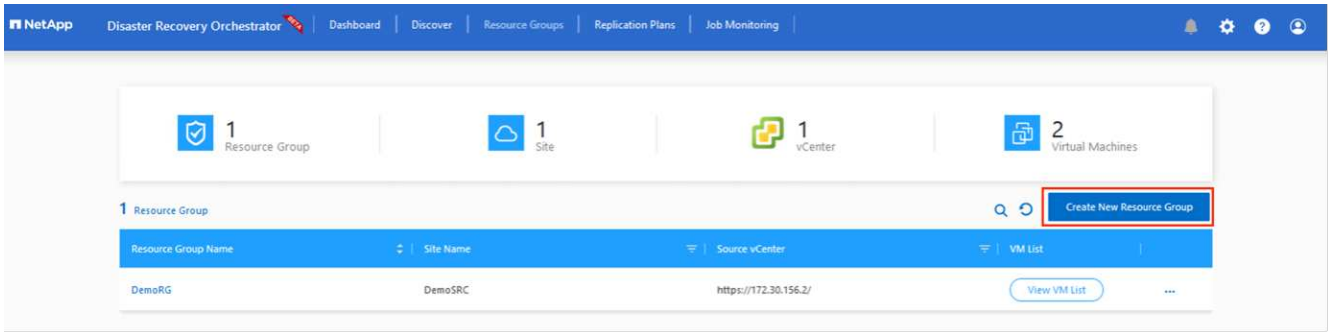
El siguiente paso es agrupar los equipos virtuales necesarios en sus grupos funcionales como grupos de recursos.

Agrupaciones de recursos

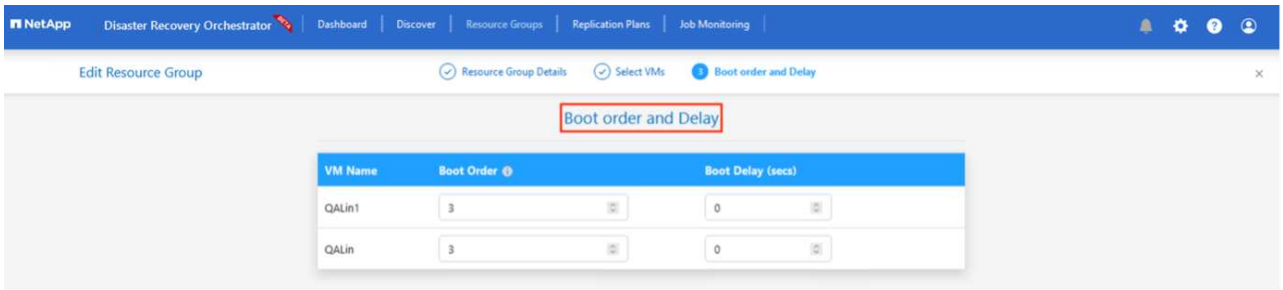
Una vez agregadas las plataformas, agrupe las máquinas virtuales que desee recuperar en grupos de recursos. LOS grupos de recursos DE DRO permiten agrupar un conjunto de máquinas virtuales dependientes en grupos lógicos que contienen sus órdenes de arranque, retrasos de arranque y validaciones de aplicaciones opcionales que se pueden ejecutar tras la recuperación.

Para comenzar a crear grupos de recursos, haga clic en el elemento de menú **Crear nuevo grupo de recursos**.

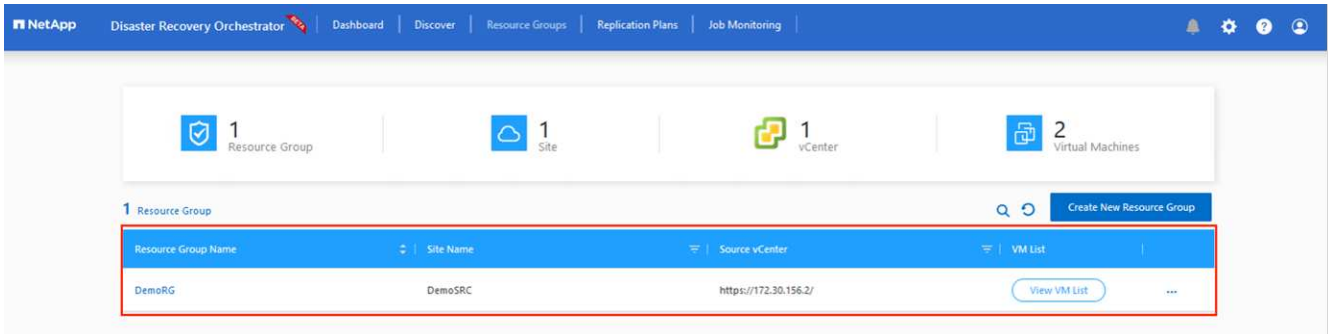
1. Acceda a **Resource Grou*ps y haga clic en *Crear nuevo grupo de recursos**.



2. En Nuevo grupo de recursos, seleccione el sitio de origen en el menú desplegable y haga clic en **Crear**.
3. Proporcione los detalles del grupo de recursos y haga clic en **Continuar**.
4. Seleccione las máquinas virtuales apropiadas mediante la opción de búsqueda.
5. Seleccione el **Boot Order** y **Boot Delay** (segundos) para todas las VM seleccionadas. Establezca el orden de la secuencia de encendido seleccionando cada máquina virtual y configurando la prioridad para ella. El valor predeterminado para todas las máquinas virtuales es 3. Las opciones son las siguientes:
   - El primer equipo virtual que se enciende
   - Predeterminado
   - La última máquina virtual que se enciende



6. Haga clic en **Crear grupo de recursos**.

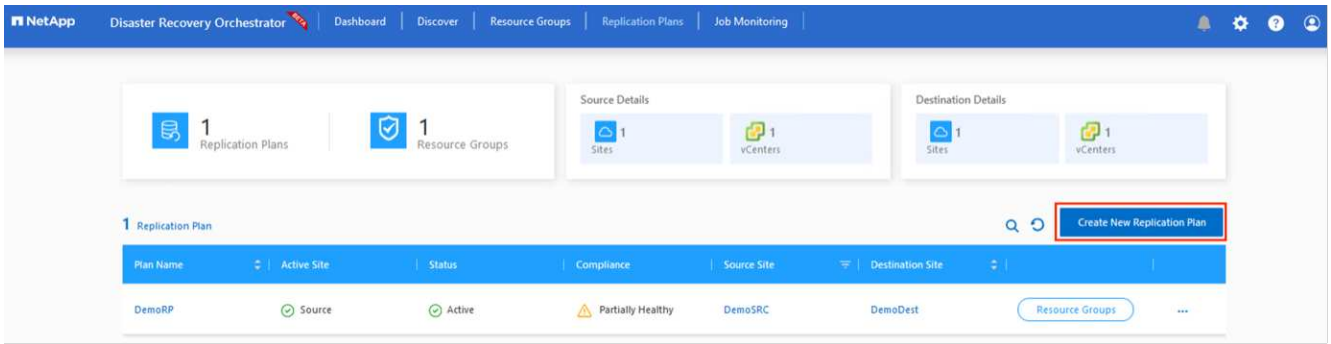


Planes de replicación

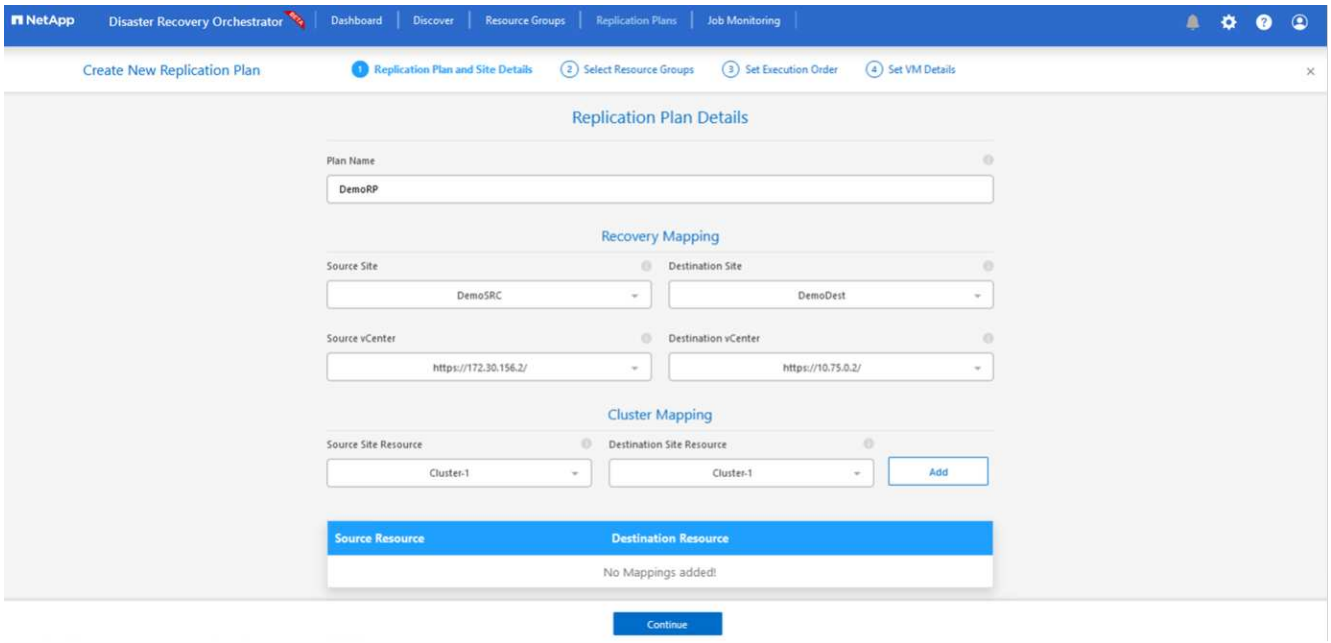
Es necesario tener un plan para la recuperación de aplicaciones en caso de desastre. Seleccione las plataformas vCenter de origen y destino en el menú desplegable, elija los grupos de recursos que se incluirán en este plan y también incluya la agrupación sobre cómo deben restaurarse y encenderse las aplicaciones (por ejemplo, controladores de dominio, nivel 1, nivel 2, etc.). A menudo, los planes también se denominan planos. Para definir el plan de recuperación, vaya a la pestaña Plan de replicación y haga clic en **Nuevo plan de replicación**.

Para comenzar a crear un plan de replicación, lleve a cabo los siguientes pasos:

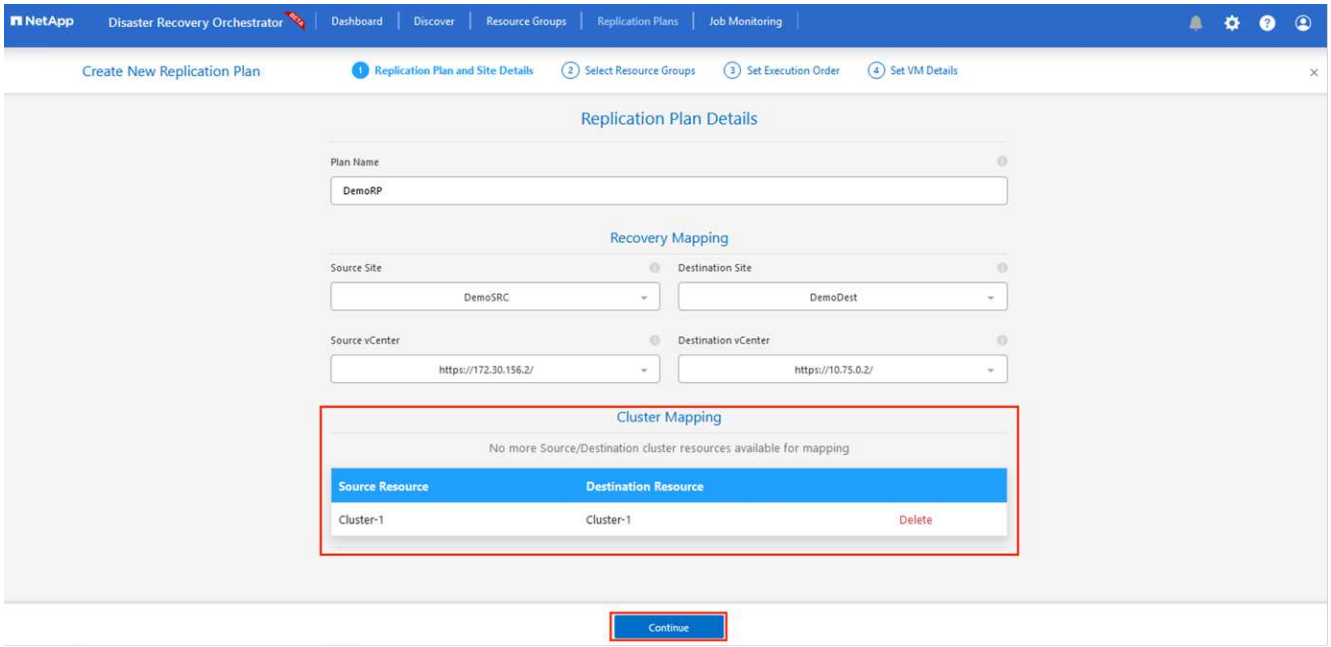
1. Vaya a **Planes de replicación** y haga clic en **Crear nuevo plan de replicación**.



2. En **New Replication Plan**, proporcione un nombre para el plan y agregue asignaciones de recuperación seleccionando el sitio de origen, vCenter asociado, el sitio de destino y vCenter asociado.

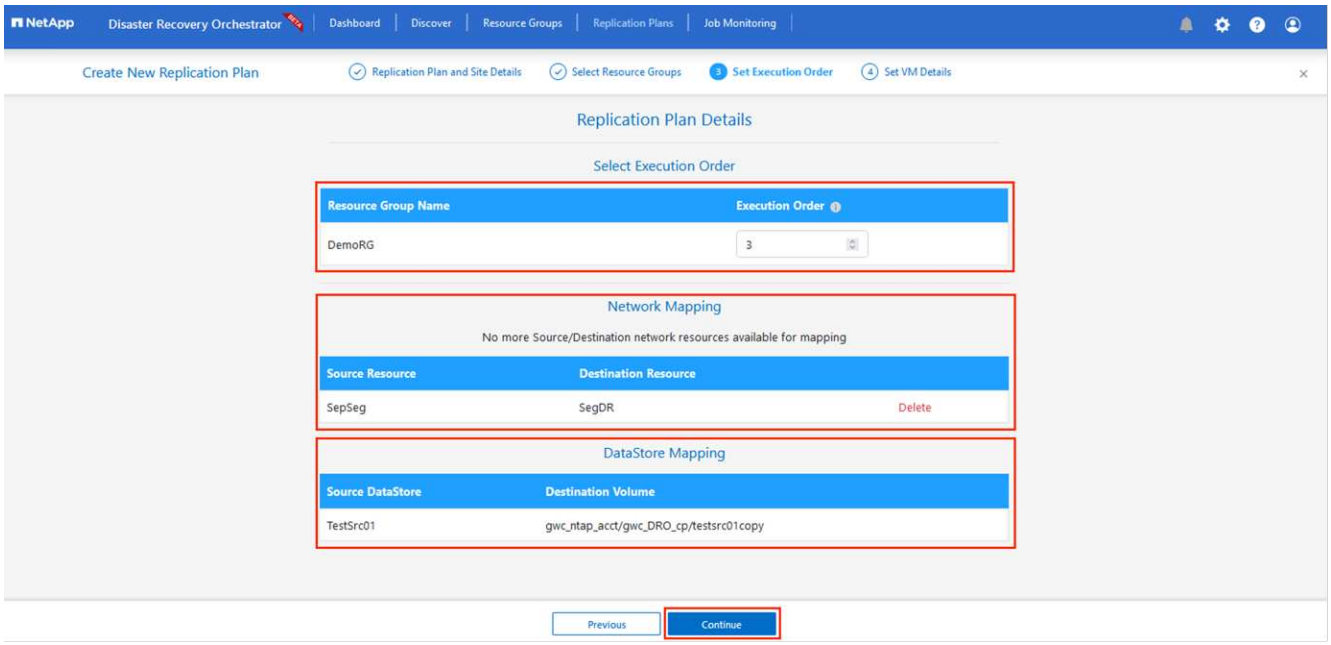


3. Después de completar el mapeo de recuperación, seleccione el **Cluster Mapping**.

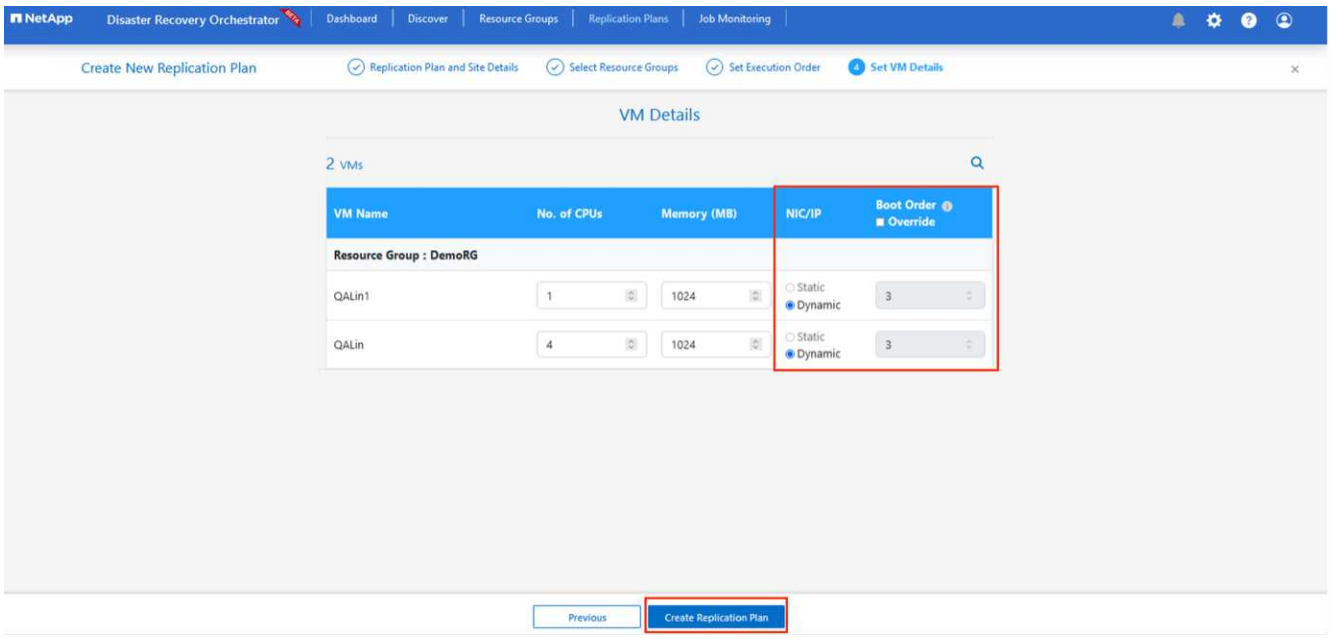


4. Seleccione **Detalles del grupo de recursos** y haga clic en **continuar**.
5. Establezca el orden de ejecución del grupo de recursos. Esta opción permite seleccionar la secuencia de operaciones cuando existen varios grupos de recursos.
6. Una vez hecho esto, defina la asignación de red en el segmento apropiado. Los segmentos ya se deben aprovisionar en el cluster AVS secundario y, para asignar las VM a ellas, seleccione el segmento apropiado.
7. Las asignaciones de almacenes de datos se seleccionan automáticamente según la selección de las máquinas virtuales.

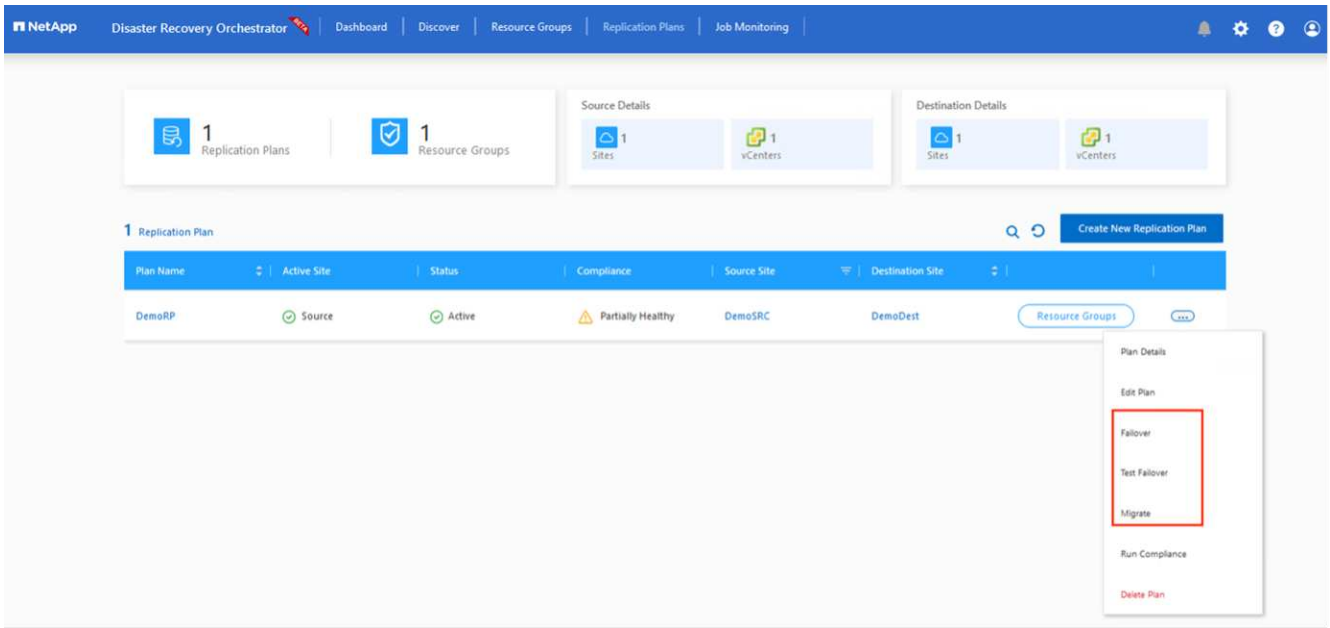
> La replicación entre regiones (CRR) se encuentra en el nivel del volumen. Por lo tanto, todas las máquinas virtuales que residen en el respectivo volumen se replican en el destino de CRR. Asegúrese de seleccionar todas las máquinas virtuales que forman parte del almacén de datos, ya que solo se procesan las máquinas virtuales que forman parte del plan de replicación.



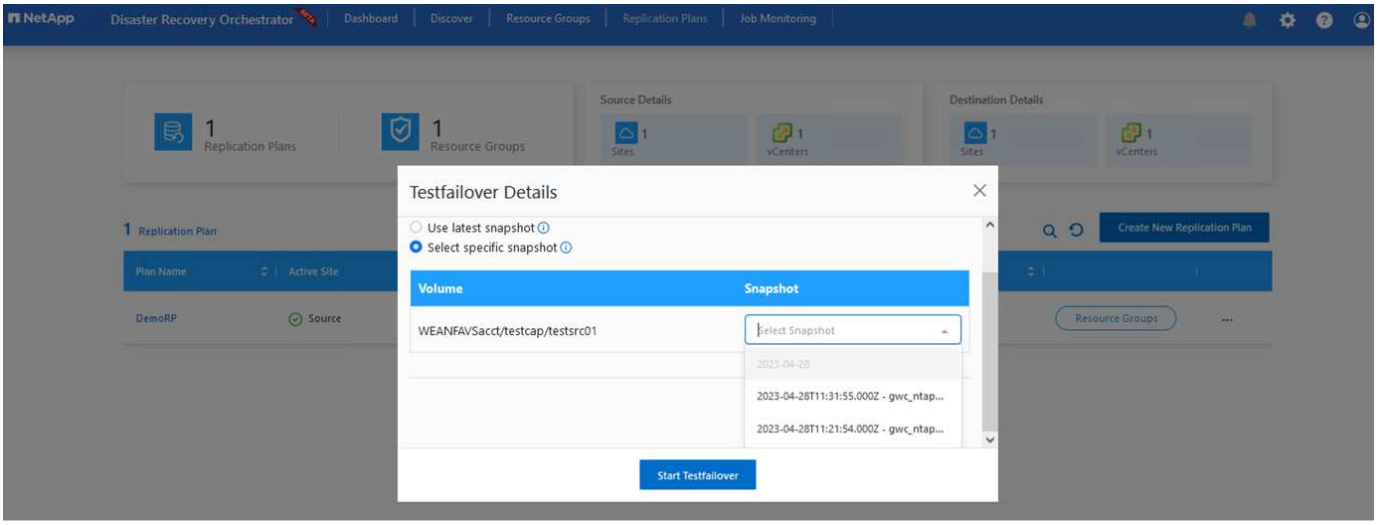
8. En Detalles de VM, opcionalmente puede cambiar el tamaño de los parámetros de CPU y RAM de VM. Esto puede ser muy útil cuando se recuperan entornos grandes en clústeres de destino de menor tamaño, o cuando se realizan pruebas de recuperación ante desastres sin tener que aprovisionar una infraestructura física de VMware uno a uno. Modifique además el orden de arranque y el retraso de inicio (segundos) para todas las máquinas virtuales seleccionadas en los grupos de recursos. Existe una opción adicional para modificar el orden de inicio si se requieren cambios en lo que seleccionó durante la selección de orden de inicio de grupo de recursos. De forma predeterminada, se utiliza el orden de inicio seleccionado durante la selección del grupo de recursos, sin embargo, se pueden realizar modificaciones en esta etapa.



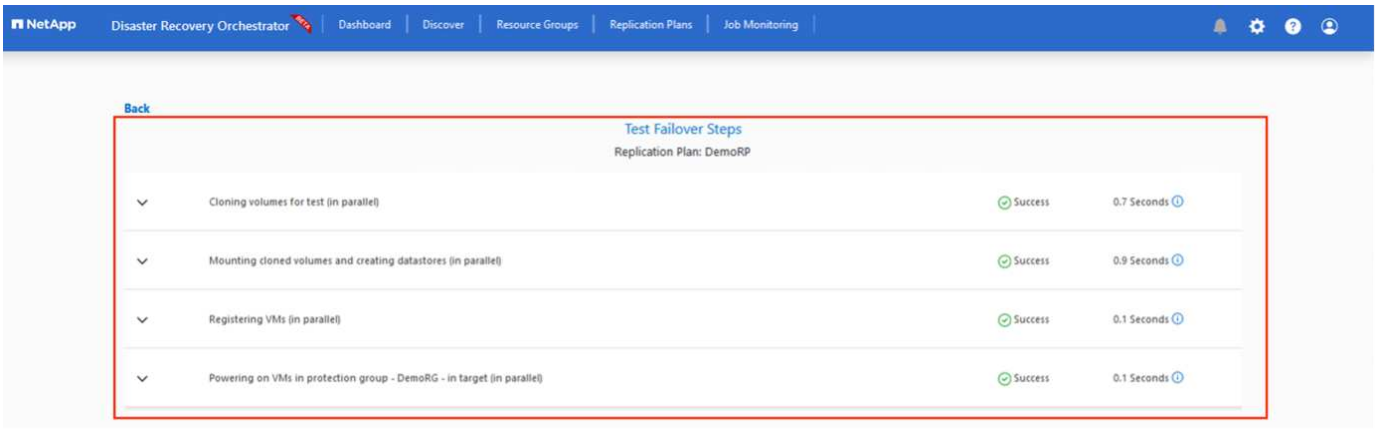
9. Haga clic en **Crear plan de replicación**.Después de crear el plan de replicación, puede ejercer las opciones de failover, failover de prueba o migración dependiendo de sus requisitos.



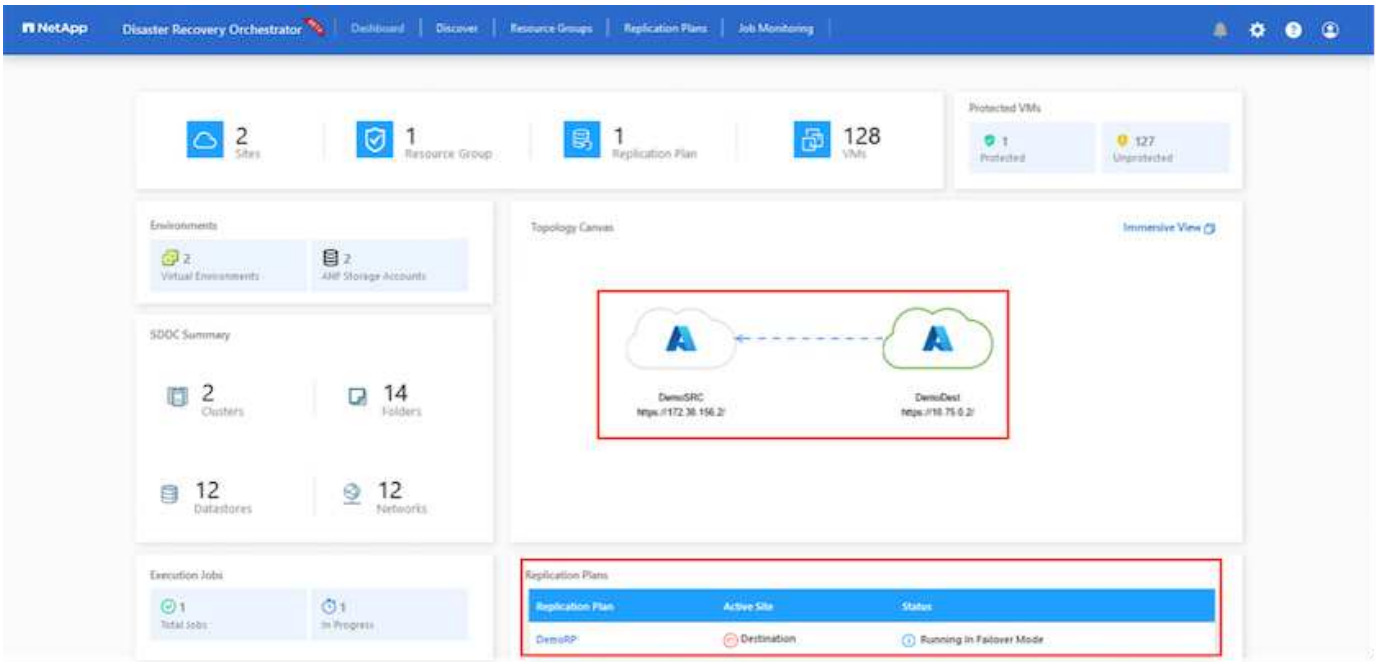
Durante las opciones de conmutación por error y conmutación por error de prueba, se utiliza la instantánea más reciente o se puede seleccionar una instantánea específica a partir de una instantánea puntual. La opción point-in-time puede ser muy beneficiosa si te enfrentas a un evento de corrupción como ransomware, donde las réplicas más recientes ya están comprometidas o cifradas. DRO muestra todos los puntos de tiempo disponibles.



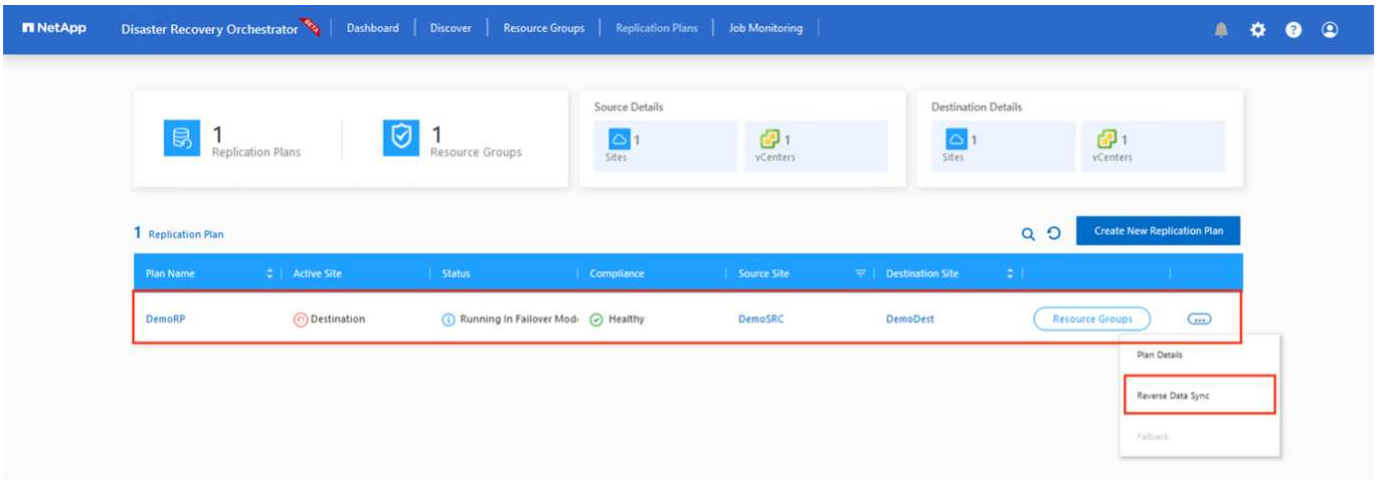
Para activar failover o failover de prueba con la configuración especificada en el plan de replicación, puede hacer clic en **Failover** o **Test Failover**. Puede supervisar el plan de replicación en el menú de tareas.



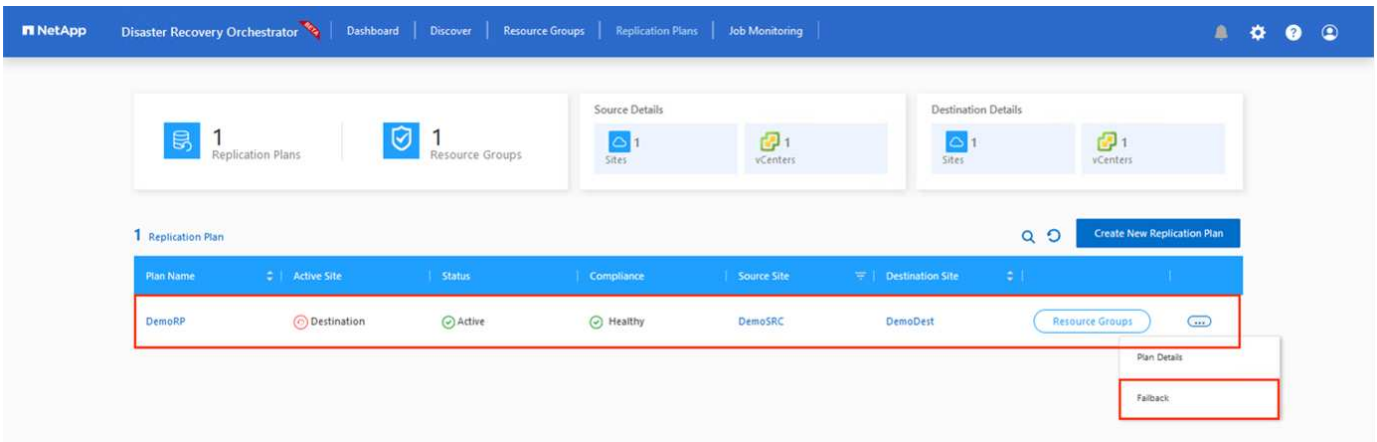
Una vez activada la conmutación al respaldo, los elementos recuperados pueden verse en el sitio secundario AVS SDDC vCenter (máquinas virtuales, redes y almacenes de datos). De forma predeterminada, las máquinas virtuales se recuperan en la carpeta Workload.

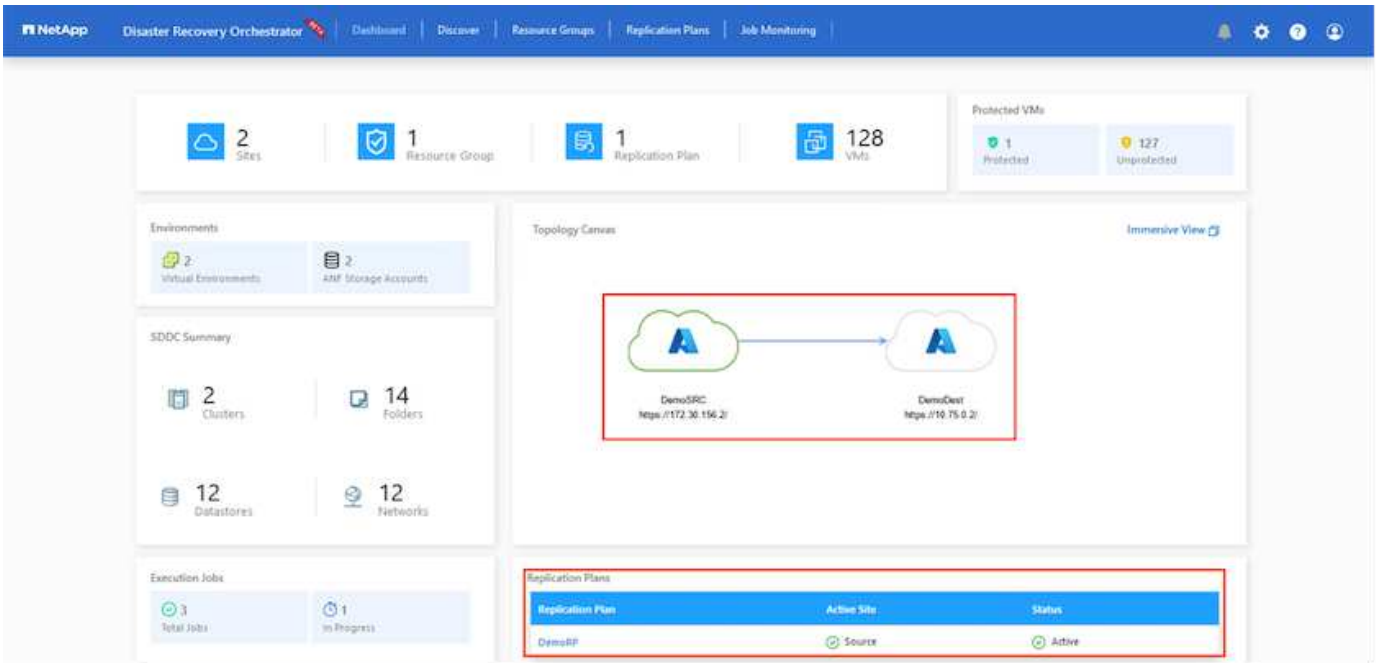


La conmutación tras recuperación se puede activar en el nivel del plan de replicación. En caso de conmutación por error de prueba, la opción de desmontaje puede utilizarse para revertir los cambios y eliminar el volumen recién creado. Los fallos relacionados con la conmutación al nodo de respaldo son un proceso de dos pasos. Seleccione el plan de replicación y seleccione **Reverse Data Sync**.



Una vez completado este paso, active la conmutación por recuperación para volver al sitio AVS principal.





Desde Azure Portal, podemos ver que el estado de la replicación se ha roto con los volúmenes apropiados que se asignaron al centro secundario AVS SDDC como volúmenes de lectura/escritura. Durante la conmutación al nodo de respaldo de prueba, DRO no asigna el volumen de destino o de réplica. En su lugar,

crea un nuevo volumen de la instantánea de replicación entre regiones necesaria y expone el volumen como almacén de datos, que consume capacidad física adicional del pool de capacidad y garantiza que el volumen de origen no se modifique. En particular, las tareas de replicación pueden continuar durante las pruebas de recuperación ante desastres o clasificar los flujos de trabajo. Además, este proceso garantiza que la recuperación se puede limpiar sin el riesgo de que la réplica se destruya en caso de que se produzcan errores o se recuperen datos dañados.

Recuperación de ransomware

Recuperarse del ransomware puede ser una tarea abrumadora. Concretamente, puede ser difícil para las ORGANIZACIONES DE TECNOLOGÍA identificar cuál es el punto de retorno seguro y, una vez determinado esto, cómo garantizar que las cargas de trabajo recuperadas se protejan de los ataques que se producen (por ejemplo, al dañar al dormir o a través de aplicaciones vulnerables).

DRO hace frente a estas preocupaciones permitiendo a las organizaciones recuperarse de cualquier momento específico disponible. A continuación, las cargas de trabajo se recuperan en redes funcionales y aisladas, de modo que las aplicaciones pueden funcionar y comunicarse entre sí, pero no están expuestas a ningún tráfico norte-sur. Este proceso proporciona a los equipos de seguridad un lugar seguro para realizar análisis forenses e identificar cualquier malware oculto o dormido.

Conclusión

La solución de recuperación ante desastres de Azure NetApp Files y Azure VMware le ofrece los siguientes beneficios:

- Aproveche la replicación entre regiones de Azure NetApp Files eficiente y resiliente.
- Recupere en cualquier momento específico disponible con retención de SnapVault.
- Automatizar por completo todos los pasos necesarios para recuperar cientos o miles de máquinas virtuales en los pasos de validación de almacenamiento, informática, red y aplicaciones.
- La recuperación de cargas de trabajo aprovecha el proceso «Crear volúmenes nuevos a partir de las instantáneas más recientes», que no manipula el volumen replicado.
- Evite el riesgo de que se dañen los datos en los volúmenes o las copias Snapshot.
- Evite las interrupciones de replicación durante los flujos de trabajo de pruebas de recuperación ante desastres.
- Aproveche los datos de recuperación ante desastres y los recursos tecnológicos en el cloud para flujos de trabajo más allá de la recuperación ante desastres, como desarrollo y pruebas, pruebas de seguridad, pruebas de revisiones y actualizaciones, y pruebas de correcciones.
- La optimización de CPU y RAM puede ayudar a reducir los costes de la nube al permitir la recuperación en clústeres de computación más pequeños.

Dónde encontrar información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- Crear replicación de volúmenes para Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Replicación entre regiones de los volúmenes de Azure NetApp Files

"https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"

- "Solución Azure VMware"

  "https://learn.microsoft.com/en-us/azure/azure-vmware/introduction"

- Ponga en marcha y configure el entorno de virtualización en Azure

  "https://docs.netapp.com/us-en/netapp-solutions/ehc/azure-setup.html"

- Pon en marcha y configura la solución Azure VMware

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Uso de la replicación de Veeam y el almacén de datos de Azure NetApp Files para recuperación ante desastres en la solución de Azure VMware

Autor: Niyaz Mohamed - Ingeniería de Soluciones NetApp

Descripción general

Los almacenes de datos de Azure NetApp Files (ANF) separan el almacenamiento de los nodos informáticos y libera la flexibilidad necesaria para que cualquier organización lleve sus cargas de trabajo al cloud. Proporciona a los clientes una infraestructura de almacenamiento flexible y de alto rendimiento que se escala independientemente de los recursos de computación. El almacén de datos de Azure NetApp Files simplifica y optimiza la implementación junto con la solución Azure VMware (AVS) como sitio de recuperación de desastres para entornos VMware en las instalaciones.

Los almacenes de datos NFS basados en volúmenes de Azure NetApp Files (ANF) pueden usarse para replicar datos desde las instalaciones con cualquier solución de terceros validada que proporcione la funcionalidad de replicación de VM. Al añadir almacenes de datos Azure NetApp Files, permitirá una puesta en marcha optimizada en costes frente a la creación de un SDDC para soluciones Azure VMware con una enorme cantidad de hosts ESXi para acomodar el almacenamiento. Este enfoque se llama un “Clúster de Luz Piloto”. Un clúster ligero piloto es una configuración de host AVS mínima (3 nodos AVS) junto con la capacidad del almacén de datos Azure NetApp Files.

El objetivo es mantener una infraestructura de bajo coste con todos los componentes principales para gestionar una recuperación tras fallos. Un clúster piloto ligero puede escalar horizontalmente y aprovisionar más hosts AVS si se produce una conmutación por error. Además, una vez finalizada la recuperación tras fallos y restablecida el funcionamiento normal, el clúster piloto puede volver a reducirse a un modo operativo de bajo coste.

Objetivos de este documento

Este artículo describe cómo usar el almacén de datos Azure NetApp Files con Veeam Backup y la replicación para configurar la recuperación de desastres para máquinas virtuales VMware (AVS) en las instalaciones usando la funcionalidad del software de replicación de Veeam VM.

Veeam Backup & Replication es una aplicación de backup y replicación para entornos virtuales. Cuando los equipos virtuales se replican, Veeam Backup & Replication se replica en AVS, el software creará una copia

exacta de los equipos virtuales en el formato nativo de VMware vSphere en el clúster SDDC de AVS de destino. Veeam Backup & Replication mantendrá la copia sincronizada con la máquina virtual original. La replicación proporciona el mejor objetivo de tiempo de recuperación (RTO) dado que hay una copia montada de un equipo virtual en el sitio de recuperación de desastres en estado listo para el inicio.

Este mecanismo de replicación garantiza que las cargas de trabajo puedan iniciarse rápidamente en un SDDC AVS en caso de desastre. El software Veeam Backup & Replication también optimiza la transmisión del tráfico para la replicación a través de WAN y conexiones lentas. Además, también filtra los bloques de datos duplicados, cero bloques de datos, archivos de intercambio y «archivos excluidos del SO invitado del equipo virtual». El software también comprimirá el tráfico de réplica. Para evitar que los trabajos de replicación consuman todo el ancho de banda de la red, se pueden utilizar aceleradores WAN y reglas de limitación de red.

El proceso de replicación en Veeam Backup & Replication está controlado por tareas, lo que significa que la replicación se realiza mediante la configuración de trabajos de replicación. En caso de desastre, se puede activar la conmutación al respaldo para recuperar las máquinas virtuales conmutando por error a su copia replicada. Cuando se realiza una conmutación por error, una máquina virtual replicada asume el rol de la máquina virtual original. La conmutación por error se puede realizar al estado más reciente de una réplica o a cualquiera de sus puntos de restauración conocidos. Esto permite la recuperación frente al ransomware o las pruebas aisladas según sea necesario. Veeam Backup & Replication ofrece múltiples opciones para gestionar diferentes escenarios de recuperación ante desastres.

[]

Puesta en marcha de la solución

Escalones de alto nivel

1. El software Veeam Backup and Replication se ejecuta en un entorno local con la conectividad de red adecuada.
2. "Pon en marcha la solución Azure VMware (AVS)" cloud privado y. "Adjunte almacenes de datos de Azure NetApp Files" A los hosts de la solución Azure VMware.

   Se puede utilizar un entorno piloto configurado con una configuración mínima para fines de recuperación ante desastres. Los equipos virtuales se conmutarán por error a este clúster en caso de que se produzca un incidente y se podrán agregar nodos adicionales).

3. Configure el trabajo de replicación para crear réplicas de máquinas virtuales con Veeam Backup and Replication.
4. Crear un plan de recuperación tras fallos y realizar una recuperación tras fallos.
5. Vuelva a los equipos virtuales de producción una vez que el evento de desastre haya finalizado y el sitio principal esté activo.

Requisitos previos para la replicación de Veeam VM en almacenes de datos AVS y ANF

1. Asegúrese de que la máquina virtual de backup de Veeam Backup & Replication está conectada al origen y a los clústeres de SDDC AVS de destino.
2. El servidor de copia de seguridad debe ser capaz de resolver nombres cortos y conectarse a vCenters de origen y destino.
3. El almacén de datos Azure NetApp Files de destino debe tener suficiente espacio libre para almacenar VMDK de máquinas virtuales replicadas.

Para obtener información adicional, consulte “Consideraciones y limitaciones” cubiertos "aquí".

Detalles de la implementación

Paso 1: Replicar máquinas virtuales

Veeam Backup & Replication aprovecha las funcionalidades de snapshot de VMware vSphere/durante la replicación, Veeam Backup & Replication solicita a VMware vSphere para crear una snapshot de máquina virtual. La snapshot de la máquina virtual es la copia de un momento específico de una máquina virtual que incluye discos virtuales, estado del sistema, configuración y metadatos. Veeam Backup & Replication utiliza la snapshot como fuente de datos para la replicación.

Para replicar equipos virtuales, siga los siguientes pasos:

1. Abra Veeam Backup & Replication Console.
2. En la vista Inicio. Haga clic con el botón derecho en el nodo JOBS y seleccione Replication Job > Virtual Machine.
3. Especifique un nombre de trabajo y seleccione la casilla de control avanzada adecuada. Haga clic en Siguiente.
   - Active la casilla de verificación Replica seeding si la conectividad entre las instalaciones y Azure tiene un ancho de banda restringido.
     *Seleccione la casilla de verificación Remapping de red (para sitios SDDC de AVS con diferentes redes) si los segmentos en SDDC de Azure VMware Solution no coinciden con los de las redes del sitio local.
   - Si el esquema de direccionamiento IP en el sitio de producción local difiere del esquema en el sitio AVS de destino, seleccione la casilla de verificación Réplica por IP (para sitios de DR con esquema de direccionamiento IP diferente).

     []
4. Seleccione las máquinas virtuales que se van a replicar en el almacén de datos Azure NetApp Files conectado a un SDDC de la solución VMware de Azure en el paso * Máquinas virtuales **. Las máquinas virtuales se pueden colocar en vSAN para llenar la capacidad de almacenes de datos vSAN disponible. En un clúster ligero piloto, la capacidad útil de un clúster de 3 nodos se verá limitada. El resto de los datos puede colocarse fácilmente en almacenes de datos Azure NetApp Files para que las máquinas virtuales se puedan recuperar. El clúster se puede expandir para cumplir los requisitos de CPU/mem. Haga clic en *Agregar**, luego en la ventana **Agregar Objeto** seleccione las VM o contenedores de VM necesarios y haga clic en **Agregar**. Haga clic en **Siguiente**.

   []
5. Después de eso, seleccione el destino como clúster/host SDDC de la solución VMware Azure y el conjunto de recursos apropiado, la carpeta de VM y el almacén de datos FSx para ONTAP para réplicas de VM. A continuación, haga clic en **Siguiente**.

   []
6. En el siguiente paso, cree la asignación entre la red virtual de origen y de destino según sea necesario.

   []
7. En el paso **Configuración del trabajo**, especifique el repositorio de copia de seguridad que almacenará metadatos para réplicas de VM, política de retención, etc.
8. Actualice los servidores proxy **Source** y **Target** en el paso **Data Transfer** y deje la selección **Automatic** (predeterminada) y mantenga seleccionada la opción **Direct** y haga clic en **Next**.

9. En el paso **Guest Processing**, selecciona la opción **Enable application-aware processing** según sea necesario. Haga clic en **Siguiente**.

   []

10. Seleccione el programa de replicación para ejecutar el trabajo de replicación con regularidad.

    []

11. En el paso **Summary** del asistente, revise los detalles del trabajo de replicación. Para iniciar el trabajo justo después de cerrar el asistente, seleccione la casilla de verificación **Ejecutar el trabajo cuando haga clic en Finalizar**, de lo contrario deje la casilla de verificación sin seleccionar. A continuación, haga clic en **Finalizar** para cerrar el asistente.

    []

Una vez que se inicia el trabajo de replicación, las máquinas virtuales con el sufijo especificado se rellenarán en el clúster/host AVS SDDC de destino.

[]

Si quiere más información sobre la replicación de Veeam, consulte "Funcionamiento de la replicación"

Paso 2: Crear un plan de failover

Una vez finalizada la replicación inicial o la propagación, cree el plan de conmutación por error. El plan de conmutación por error ayuda a realizar la conmutación por error de los equipos virtuales dependientes uno por uno o como grupo automáticamente. El plan de conmutación por error es el plan del orden en el que se procesan los equipos virtuales, incluidos los retrasos en el inicio. El plan de conmutación por error también ayuda a garantizar que los equipos virtuales cruciales dependientes ya se estén ejecutando.

Para crear el plan, navegue a la nueva subsección llamada **replicas** y seleccione **Failover Plan**. Seleccione los equipos virtuales adecuados. Veeam Backup & Replication buscará los puntos de restauración más cercanos a este punto en el tiempo y los utilizará para iniciar réplicas de máquinas virtuales.

> El plan de conmutación por error solo se puede agregar una vez que la replicación inicial se haya completado y las réplicas de las máquinas virtuales estén en estado Listo.

> El número máximo de equipos virtuales que se pueden iniciar simultáneamente cuando se ejecuta un plan de conmutación al nodo de respaldo es de 10

> Durante el proceso de conmutación al nodo de respaldo, los equipos virtuales de origen no se apagarán

Para crear el **Failover Plan**, haga lo siguiente:

1. En la vista Inicio. Haga clic con el botón derecho en el nodo replicas y seleccione Failover Plans > Failover Plan > VMware vSphere.

   []

2. A continuación, proporcione un nombre y una descripción al plan. El script previo y posterior al failover se puede agregar según sea necesario. Por ejemplo, ejecute un script para cerrar los equipos virtuales antes de iniciar los equipos virtuales replicados.

   []

3. Agregue las máquinas virtuales al plan y modifique el orden de arranque de la máquina virtual y los retrasos de arranque para cumplir con las dependencias de la aplicación.

   []

Para obtener más información sobre la creación de trabajos de replicación, consulte "Creación de trabajos de replicación".

Paso 3: Ejecute el plan de failover

En caso de fallo, la máquina virtual de origen del sitio de producción cambia a su réplica en el sitio de recuperación de desastres. Como parte del proceso de conmutación por error, Veeam Backup & Replication restaura la réplica de la máquina virtual al punto de restauración deseado y mueve todas las actividades de I/O del equipo virtual de origen a su réplica. Las réplicas pueden usarse no solo en caso de desastre, sino también para simular simulacros de recuperación ante desastres. Durante la simulación de recuperación tras fallos, la máquina virtual de origen sigue ejecutándose. Una vez realizadas todas las pruebas necesarias, puede deshacer la conmutación por error y volver a las operaciones normales.

> Asegúrese de que la segmentación de la red está en su lugar para evitar conflictos de IP durante la conmutación por error.

Para iniciar el plan de conmutación por error, simplemente haga clic en la pestaña **Planes de conmutación por error** y haga clic con el botón derecho en su plan de conmutación por error. Selecciona ***Inicio**. Se conmutará al nodo de respaldo usando los puntos de restauración más recientes de réplicas de equipos virtuales. Para conmutar por error a puntos de restauración específicos de réplicas de VM, seleccione **Iniciar a**.

[]

[]

El estado de la réplica de VM cambia de Ready a Failover y VMs se iniciará en el clúster/host SDDC de Azure VMware Solution (AVS) de destino.

[]

Una vez finalizada la conmutación por error, el estado de las máquinas virtuales cambiará a «Failover».

[]

> Veeam Backup & Replication detiene todas las actividades de replicación de la máquina virtual de origen hasta que su réplica vuelve al estado Ready.

Para obtener información detallada sobre los planes de conmutación por error, consulte "Planes de conmutación al respaldo".

Paso 4: Conmutación por recuperación al sitio de producción

Cuando se ejecuta el plan de failover, se considera un paso intermedio y debe finalizarse según el requisito. Las opciones incluyen las siguientes:

- **Failback to production** - cambia de nuevo a la VM original y transfiere todos los cambios que tuvieron lugar mientras la réplica de la VM se estaba ejecutando a la VM original.

> Al realizar la conmutación por recuperación, los cambios solo se transfieren pero no se publican. Seleccione **Commit failback** (una vez que la VM original se confirme para funcionar como se esperaba) o Deshacer failback para volver a la réplica de la VM Si la VM original no funciona como se esperaba.

- **Deshacer failover** - cambiar de nuevo a la VM original y descartar todos los cambios realizados en la réplica de la VM mientras se estaba ejecutando.
- **Failover permanente** - Cambie permanentemente de la VM original a una réplica de VM y utilice esta réplica como la VM original.

En esta demostración se eligió la conmutación de retorno tras recuperación en producción. Se ha seleccionado la conmutación por recuperación a la VM original durante el paso de destino del asistente y la casilla de verificación “Power on VM after restoring” estaba activada.

[]

[]

[]

[]

La confirmación de conmutación por recuperación es una de las formas de finalizar la operación de conmutación por recuperación. Cuando se confirma la conmutación por recuperación, confirma que los cambios enviados a la máquina virtual que se devuelve una conmutación por error (la máquina virtual de producción) funcionan según lo esperado. Tras la operación de confirmación, Veeam Backup & Replication reanuda las actividades de replicación para la máquina virtual de producción.

Para obtener información detallada sobre el proceso de conmutación por recuperación, consulte la documentación de Veeam para "Conmutación al nodo de respaldo y conmutación de retorno tras recuperación para replicación".

[]

Una vez que la conmutación de retorno tras recuperación en producción se realiza correctamente, las máquinas virtuales se restauran de nuevo en el sitio de producción original.

[]

Conclusión

La funcionalidad de almacén de datos Azure NetApp Files permite a Veeam o cualquier herramienta de terceros validada proporcionar una solución de recuperación ante desastres de bajo coste mediante el uso de clústeres ligeros de Pilot en lugar de establecer un gran clúster solo para acomodar réplicas de máquinas virtuales. Esto proporciona una forma eficaz de manejar un plan de recuperación ante desastres

personalizado y personalizado, y de reutilizar productos de backup existentes internamente para recuperación ante desastres, lo que permite la recuperación ante desastres basada en el cloud mediante la salida de centros de datos de recuperación ante desastres en las instalaciones. Es posible conmutar al respaldo haciendo clic en un botón en caso de desastre o conmutando automáticamente al respaldo en caso de desastre.

Para obtener más información sobre este proceso, puede seguir el vídeo detallado del tutorial.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278