

acens

Part of Telefónica Tech

Manual de Usuario

VMware Disaster Recovery as a Service (DRaaS)

Índice

1	Introducción	5
2	Requisitos previos	5
3	Acceso a VMware Cloud Director	5
4	Configuración de réplicas	7
4.1	Presentación del escenario de réplica.....	7
4.2	Creación de la réplica	8
4.3	Comprobación de la réplica desde destino	12
5	Test	13
5.1	Ejecutar Test	14
5.2	Ejecutar limpieza del test	18
5.2.1	<i>Test Cleanup desde origen</i>	18
5.2.2	<i>Test Cleanup desde destino</i>	18
6	Failover	19
7	Recovery Failback	23
8	Monitorización de las réplicas	28
8.1	Envío de notificaciones a vCloud	28
8.2	Eventos enviados a vCloud	29
8.3	Eventos enviados por email.....	29
9	Canales de atención	30

Índice de figuras

Figura 3.1 – Menú de navegación – Acceso a Cloud Hosting.....	6
Figura 3.2 – Acceso a servicio Cloud Datacenter	6
Figura 3.3 – Gestión de Cloud Datacenter	6
Figura 3.4 – Portal de acceso a VMware Cloud Director	7
Figura 4.1 -Presentación alto nivel del escenario	7
Figura 4.2 – VMware Cloud Director. Acceso a configuración DRaaS desde Cloud Datacenter origen	8
Figura 4.3 – Entrada a Asistente de nueva réplica saliente	8
Figura 4.4 – Asistente Nueva réplica saliente. vApps y MVs de nube. Selección de site de destino	9
Figura 4.5 – Credenciales de acceso. Convención de nombres	9
Figura 4.6 – Asistente Nueva réplica saliente. vApps y MVs de nube. Selección de vApps y MV a replicar	10
Figura 4.7 – Asistente Nueva réplica saliente. Selección de VDC destino y política de almacenamiento	10
Figura 4.8 – Asistente Nueva réplica saliente. Apartado Configuración	11
Figura 4.9 – Asistente Nueva réplica saliente. Apartado Listo para completar	11
Figura 4.10 – Nueva réplica saliente creada.	12
Figura 4.11 – Acceso a VDC destino para gestionar réplica	12
Figura 4.12 – VMware Cloud Director. Acceso a configuración DRaaS desde Cloud Datacenter destino	13
Figura 4.13 – Comprobación de réplica entrante en destino	13
Figura 5.1 – Probar réplica saliente. Test	14
Figura 5.2 – Asistente Test. Configuración de recuperación	15
Figura 5.3 – Asistente Test. Instancia de recuperación	15
Figura 5.4 – Asistente Test. Listo para completar.....	16
Figura 5.5 – Resultado Test	16
Figura 5.6 – Máquina replicada en destino	17
Figura 5.7 – Comprobación MV en destino	17
Figura 5.8 – Asignación de IP de pool de direcciones disponibles	17
Figura 5.9 – Información en destino de MV levantada.....	18
Figura 5.10 – Test cleanup desde origen	18
Figura 5.11 – Test Cleanup en destino.....	19
Figura 6.1 – Acceso a Failover.....	20
Figura 6.2 – Asistente Failover. Configuración de recuperación	20
Figura 6.3 – Asistente Failover. Instancia de recuperación	21
Figura 6.4 – Asistente Failover. Listo para completar.....	21
Figura 6.5 – Asistente Failover. Avance del proceso.....	22
Figura 6.6 – Failover. Eliminación de la réplica Madrid-Barcelona existente	22
Figura 7.1 – Recovery Failback. Configuración de réplica saliente	23
Figura 7.2 – Recovery Failback. Asistente Nueva réplica saliente. vApps y MVs de nube. Selección de site de destino.....	24
Figura 7.3 – Recovery Failback. Asistente Nueva réplica saliente. Selección de VDC destino y política de almacenamiento	24
Figura 7.4 – Recovery Failback. Asistente Nueva réplica saliente. Apartado Configuración	25
Figura 7.5 – Recovery Failback. Asistente Nueva réplica saliente. Apartado MV de inicialización	25
Figura 7.6 – Recovery Failback. Asistente Nueva réplica saliente. Apartado Listo para completar.....	26
Figura 7.7 – Recovery Failback. Asistente Nueva réplica saliente. Progreso de creación de réplica	26
Figura 7.8 – Recovery Failback. Réplica saliente creada con MV de inicialización	26
Figura 7.9 – Máquinas virtuales Cloud Datacenter Madrid	27
Figura 7.10 – Réplicas entrantes en Cloud Datacenter Madrid	27
Figura 8.1 – Eventos generados.....	28
Figura 8.2 – Eventos y notificaciones DRaaS.....	28
Figura 8.3 – Eventos enviados a vCloud	29
Figura 8.4 – Notificación de eventos a todos los administradores	30
Figura 9.1 – Acceso a Soporte.....	30
Figura 9.2 – Creación de Consulta	30
Figura 9.3 – Formulario para creación de consulta	31

Índice de tablas

Tabla 8.1 – Formas de envío de eventos a vCloud.....	29
------------------------------------------------------	----

1 Introducción

El servicio de Disaster Recovery as a Service (DRaaS) consiste en la réplica de máquinas virtuales alojadas en plataformas vmware compatibles con origen o destino el servicio de Cloud DataCenter. El objetivo del servicio asegurar la continuidad de la infraestructura replicada en caso de incidencia o indisponibilidad de la plataforma origen.

El servicio se basa en la solución **VMware Cloud Director Availability** completamente integrada en el portal de Cloud Director.

El servicio de DRaaS está disponible en tres modalidades distintas, siempre que todas las plataformas implicadas se basen en entornos VMware compatibles:

- **Cloud-to-Cloud:** se realiza la réplica de máquinas virtuales gestionadas en Cloud Datacenter en entre los Centros de Datos de acens de Madrid y Barcelona.
- **Private Cloud-to-Cloud:** se realiza la réplica de máquinas virtuales desde un Cloud Privado del cliente alojado en acens hacia soluciones de Cloud Datacenter de acens ya sea en Madrid o en Barcelona.
- **On Premise-to-Cloud:** se realiza la réplica de máquinas virtuales desde una infraestructura alojada en la sede de cliente hacia el servicio de Cloud Datacenter de acens alojado en Madrid o Barcelona.

Este manual está dirigido a la configuración del servicio DRaaS en la modalidad Cloud-to-Cloud.

2 Requisitos previos

Para la configuración del servicio DRaaS se entiende un escenario en el cual:

- Todos los servicios están contratados: Cloud Datacenter en origen, Cloud Datacenter en destino y servicio de DRaaS con el plan de réplica elegido.
- Configuración de redes necesarias para el servicio en Cloud Datacenter origen y destino.
- Funcionalidad de réplica configurada y disponible para que los servicios Cloud Datacenter se vean de forma bidireccional entre Madrid y Barcelona.

3 Acceso a VMware Cloud Director

A través del **Panel de Cliente**, podrá acceder al entorno de configuración del servicio DRaaS. Para ello, deberá utilizar las credenciales de acceso a Panel. En caso de no disponer de las credenciales, puede ponerse en contacto con acens a través de los canales de atención habituales detallados en el apartado *9 Canales de atención*.

Una vez dentro del Panel de Cliente podrá navegar por los diferentes productos contratados a través del menú de la izquierda de la pantalla del navegador. Para entrar en la configuración del servicio DRaaS, debe entrar en la sección de Cloud Hosting:

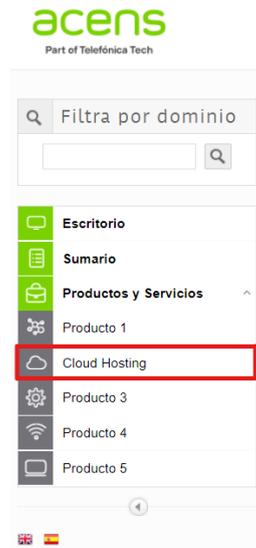


Figura 3.1 – Menú de navegación – Acceso a Cloud Hosting

Dentro de Cloud Hosting, debe seleccionar el servicio de Cloud Datacenter origen donde están las máquinas que desea replicar al Cloud Datacenter destino:



Figura 3.2 – Acceso a servicio Cloud Datacenter

Una vez seleccionado Cloud Datacenter origen, haga click en el botón **Gestionar Cloud Datacenter** para acceder al portal de VMware Cloud Director. Si no recuerda las credenciales de acceso, puede consultarlas haciendo click en el botón **Mostrar datos de acceso** en esta misma sección.

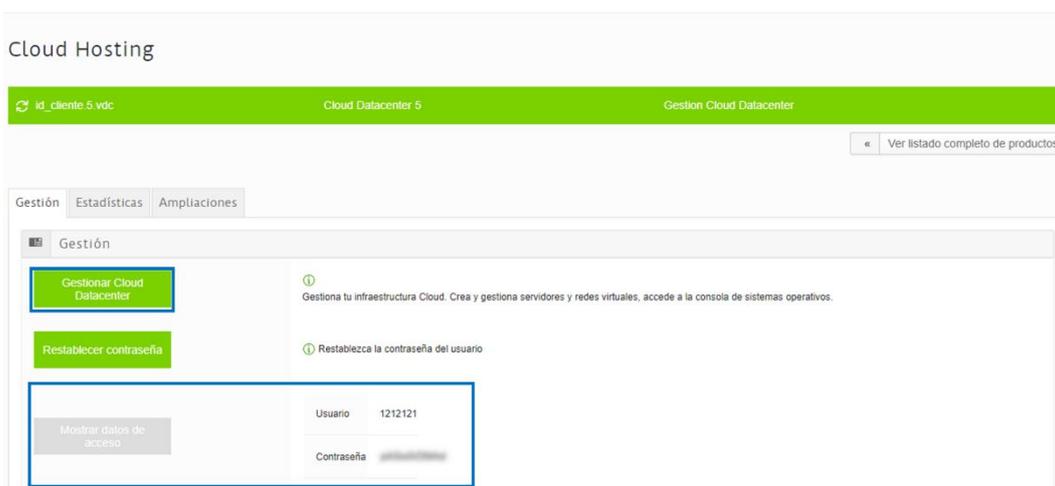


Figura 3.3 – Gestión de Cloud Datacenter

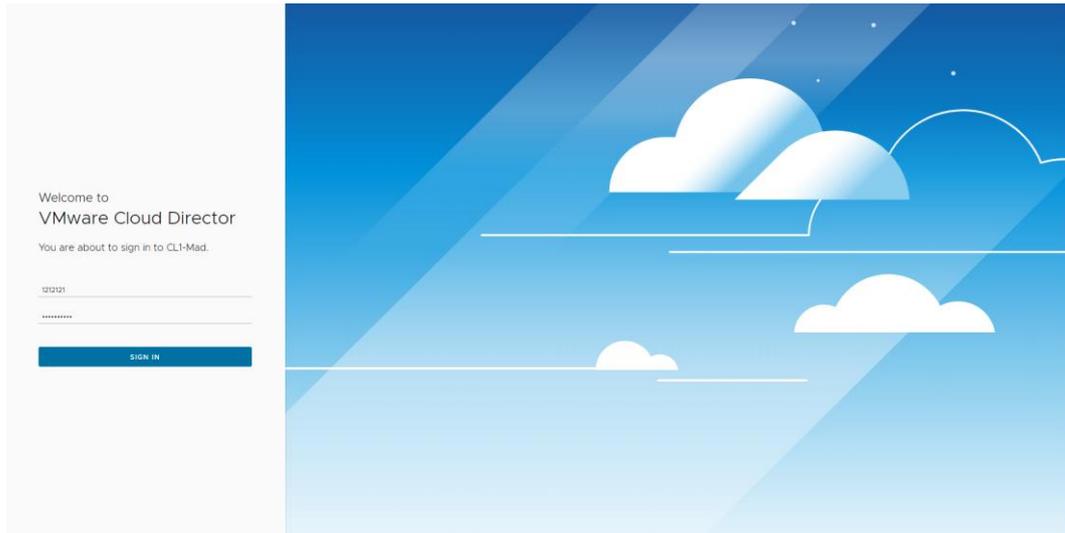


Figura 3.4 – Portal de acceso a VMware Cloud Director

4 Configuración de réplicas

4.1 Presentación del escenario de réplica

Este manual detalla la configuración del servicio DRaaS en un escenario **Cloud-to-Cloud** en el cual se realiza la réplica de máquinas virtuales alojadas en el Cloud DataCenter de Madrid al Cloud DataCenter alojado en Barcelona. El objetivo es disponer de una réplica de las MVs alojadas en origen (Madrid) para llegado el caso poder hacer failover en el entorno de destino levantando el entorno en el site de Barcelona.

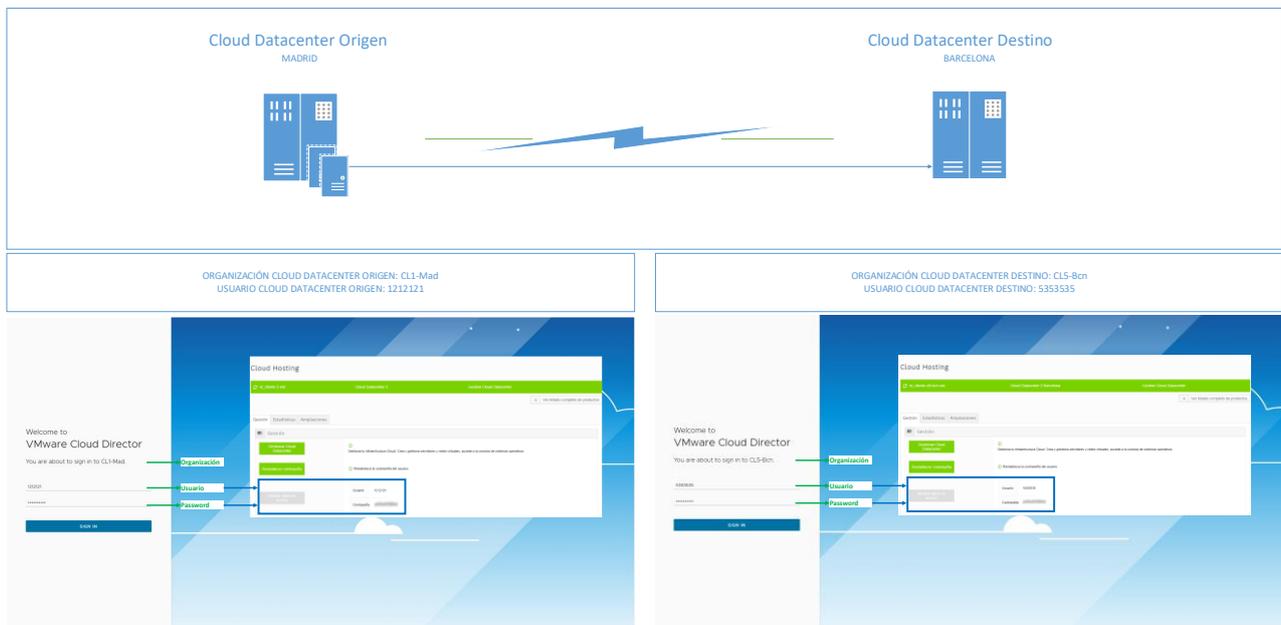


Figura 4.1 -Presentación alto nivel del escenario

Dentro de este escenario, es importante tener configuradas las redes en cada uno de los Cloud Datacenter origen y destino. En caso de tener dudas sobre la configuración de las redes, póngase en contacto con nosotros a través de alguno de los medios detallados en el apartado *9 Canales de atención*.

4.2 Creación de la réplica

Dado el escenario presentado en la

Figura 4.1, acceda al panel de configuración de Cloud Datacenter origen (Madrid) y diríjase a la opción **More → Availability (CL1 VDC)** del menú de navegación principal.

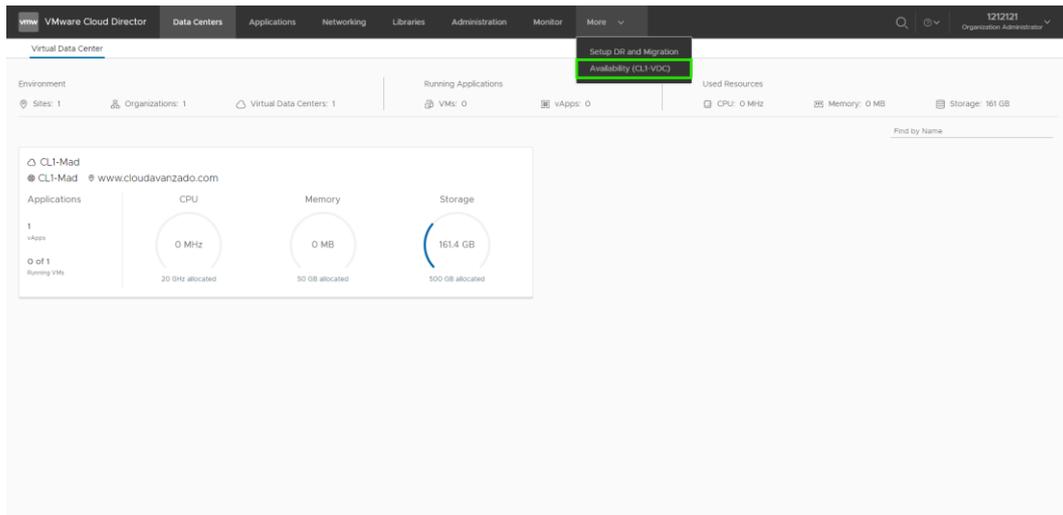


Figura 4.2 – VMware Cloud Director. Acceso a configuración DRaaS desde Cloud Datacenter origen

En el menú izquierdo, seleccione **Outgoing Replications**. A continuación, despliegue **ALL ACTIONS** y seleccione **New protection**.

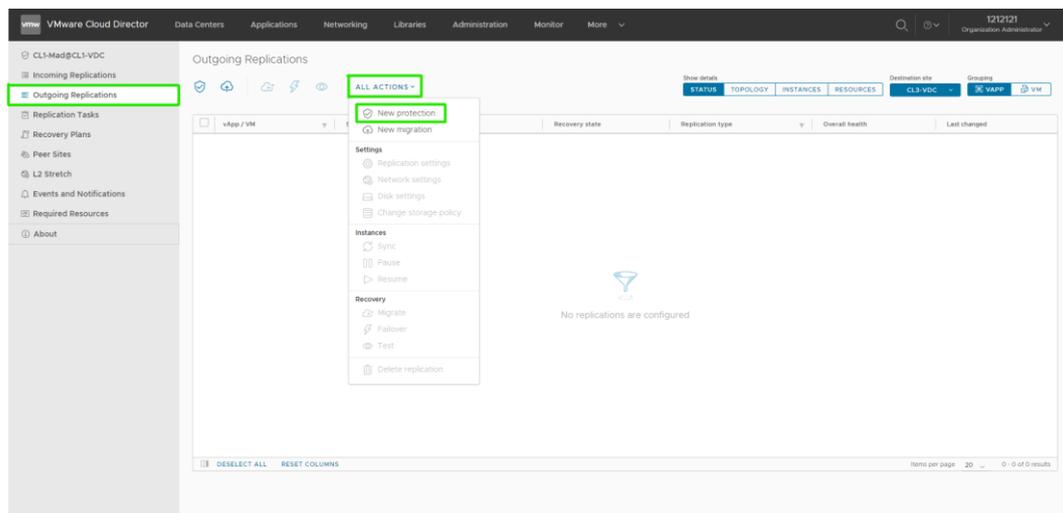


Figura 4.3 – Entrada a Asistente de nueva réplica saliente

Se abre un asistente para la configuración:

1. Cloud vApps and VMs:

- **Destination Site:** de las opciones desplegadas, seleccione en este caso **CL5-BCN-VDC** que es donde se quiere crear la réplica (entorno de Cloud Datacenter en Barcelona).

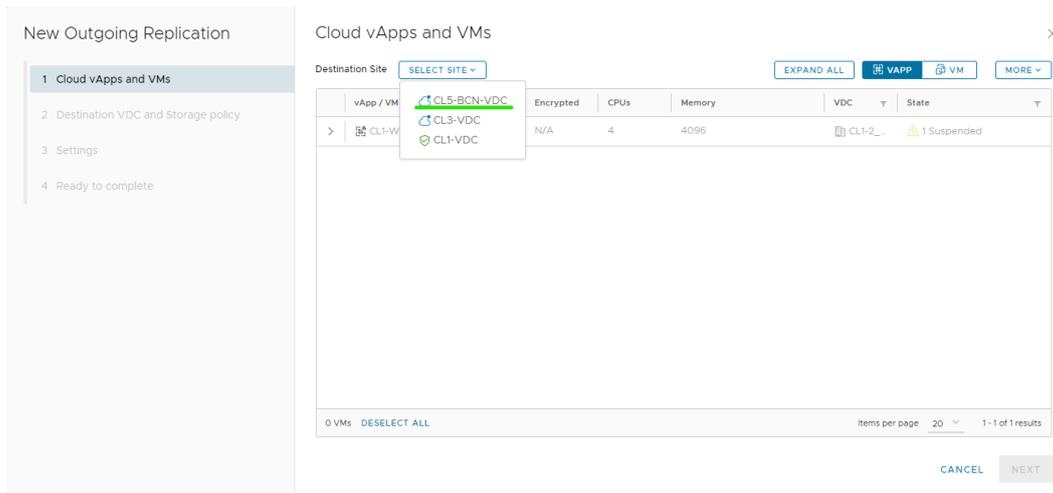


Figura 4.4 – Asistente Nueva réplica saliente. vApps y MVs de nube. Selección de site de destino

Al seleccionar el Sitio de destino, Barcelona en este caso, si no se ha autenticado previamente en el Cloud Director del Cloud Datacenter destino, se le solicitarán las credenciales de acceso. Tenga en cuenta la convención de nombres utilizada para componer el Nombre de usuario:

usuario@organización_destino

En el escenario que sirve de base al manual:

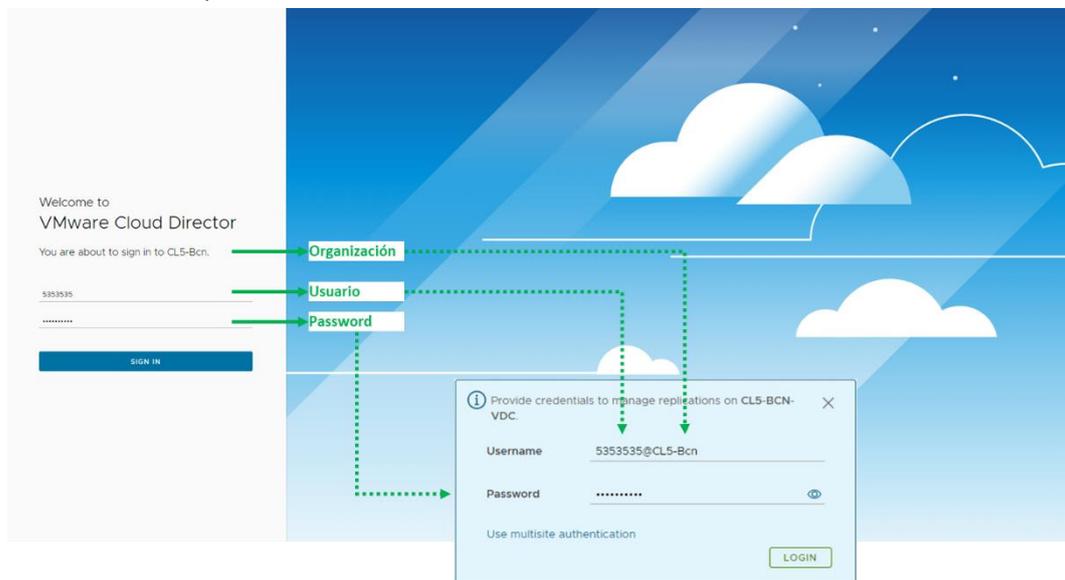


Figura 4.5 – Credenciales de acceso. Convención de nombres

Para la autenticación de la réplica, por defecto se crearán usuarios específicos con formato ***vcav.<organización_destino>*** que puede consultar en la sección Administración -> Usuarios del sitio destino. Recuerde que el formato de nombre de usuario debe seguir el patrón de ***vcav.<organización_destino>@<organización_destino>*** tal como se indicaba en el párrafo anterior.

Una vez autenticado en Cloud Datacenter destino, se vuelve al asistente para la creación de nueva réplica saliente.

- **VAPP:** seleccione la vApp o la/las máquinas virtuales que quiera replicar activando los cuadros de selección necesarios como se muestra a continuación.

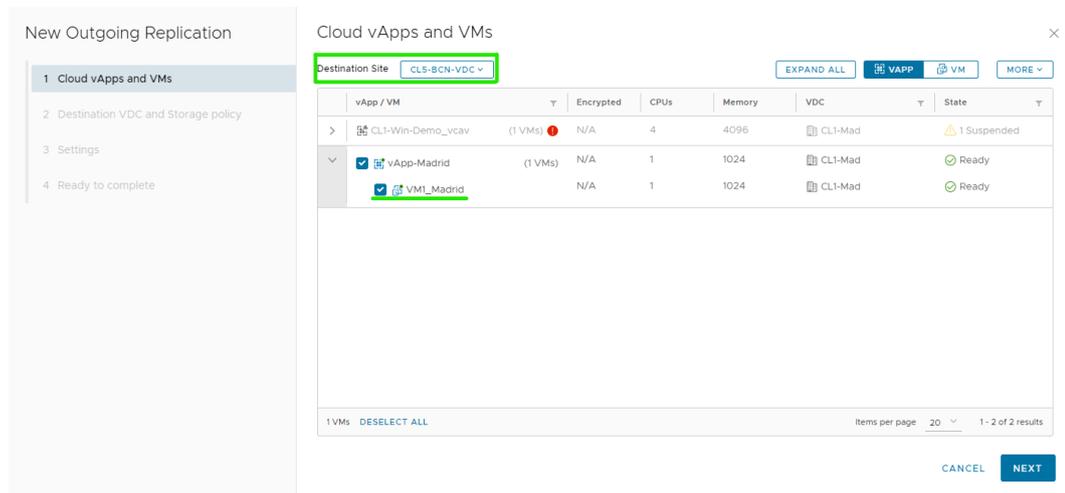


Figura 4.6 – Asistente Nueva réplica saliente. vApps y MVs de nube. Selección de vApps y MV a replicar

2. **Destination VDC and Storage policy:** muestra la información del Cloud Datacenter destino y permite seleccionar la ubicación de la política de almacenamiento para las máquinas virtuales replicadas. Las políticas de almacenamiento disponibles serán las que estén disponibles en el Cloud Datacenter destino.

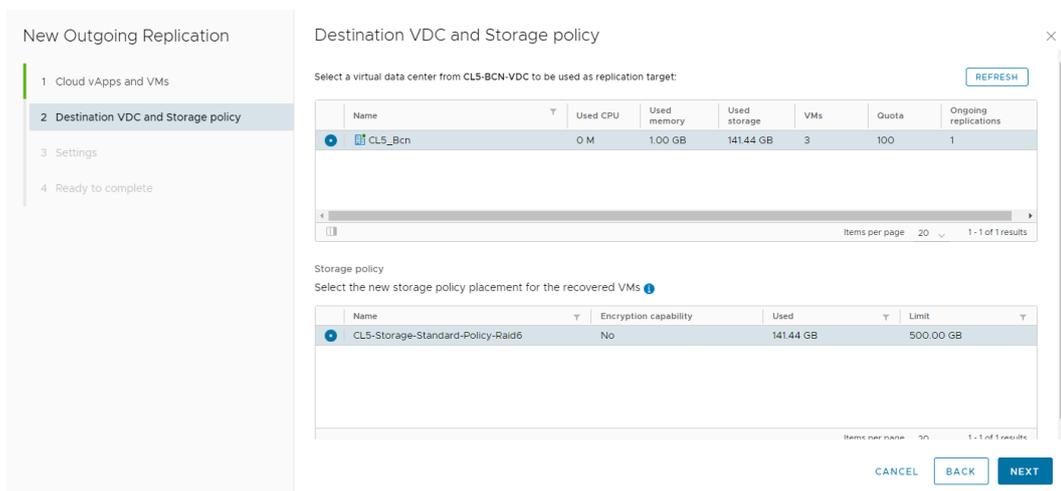


Figura 4.7 – Asistente Nueva réplica saliente. Selección de VDC destino y política de almacenamiento

3. **Settings:**

- **Use SLA Profile:** seleccione el número de replications por periodo de las opciones que se le presentan, que dependerán del Plan de Réplica contratado.

- **Exclude disks:** si se activa permite seleccionar qué discos de los existentes en las máquinas virtuales origen incluir en la réplica en destino. Se recomienda dejar desactivado para asegurar que todo se replica.
- **Configure Seed VMs:** si se activa permite seleccionar una copia anterior existente en destino como base para la creación de la réplica, reduciéndose el tráfico y el tiempo en el proceso de réplica. Se recomienda dejar desactivado, opción por defecto.

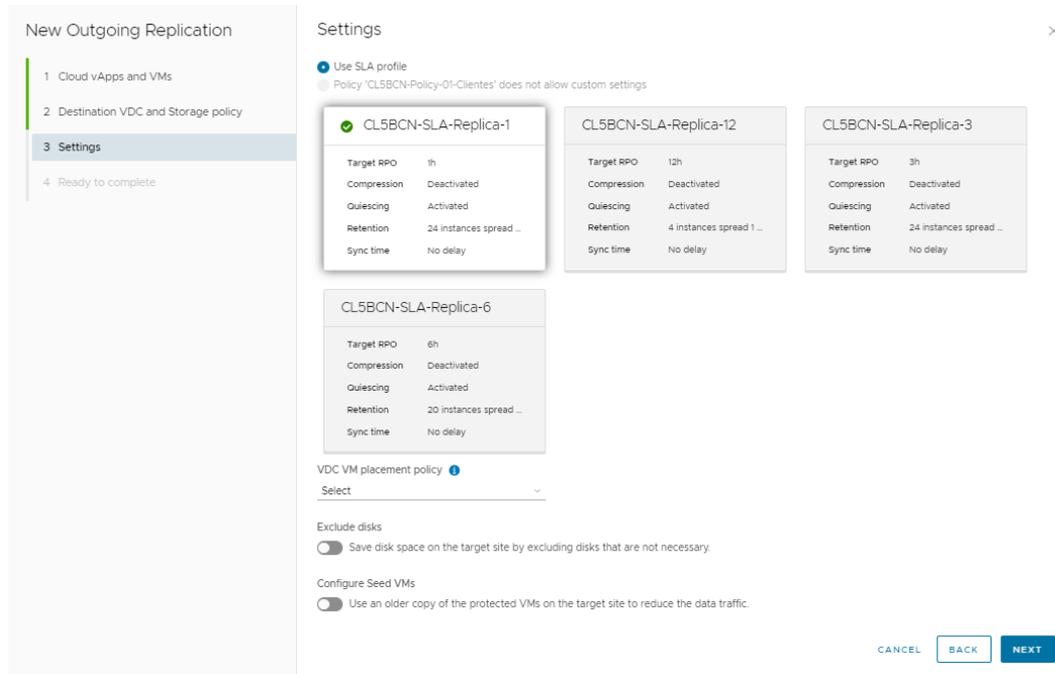


Figura 4.8 – Asistente Nueva réplica saliente. Apartado Configuración

4. **Ready to complete:** se muestra un resumen de la configuración. Compruebe que la configuración es correcta, corríjala navegando hacia atrás en el asistente o finalice el proceso haciendo click en **Finish**.

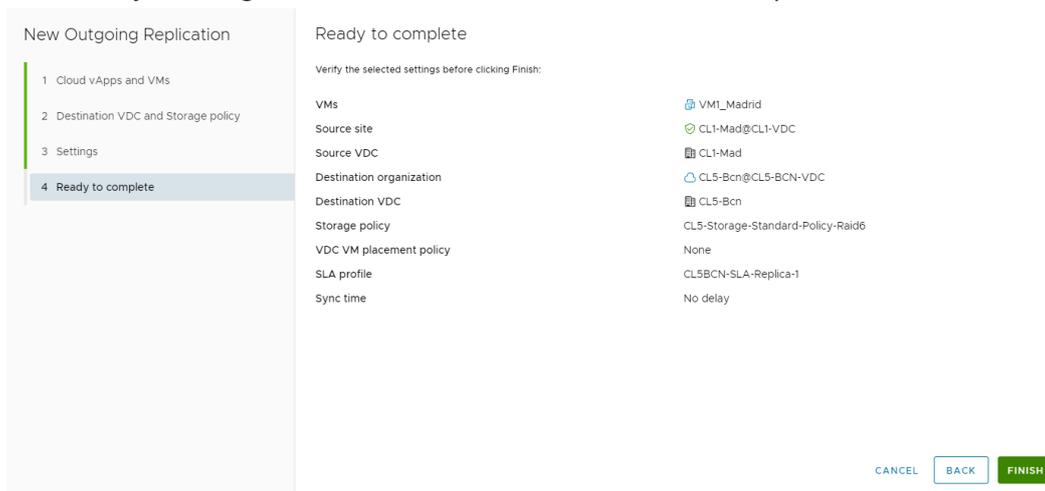


Figura 4.9 – Asistente Nueva réplica saliente. Apartado Listo para completar

En este momento comienza la protección, mostrándose en progreso en el campo **Last changed** e indicando **● Rojo** en el campo **Overall health**. Al finalizar la operación si el proceso de creación ha finalizado con éxito el campo se muestra en **● Verde**. En caso de que no se finalice correctamente revise las opciones de

configuración seleccionadas y en caso de duda póngase en contacto con nosotros a través de alguno de los medios detallados en el apartado *9 Canales de atención*.

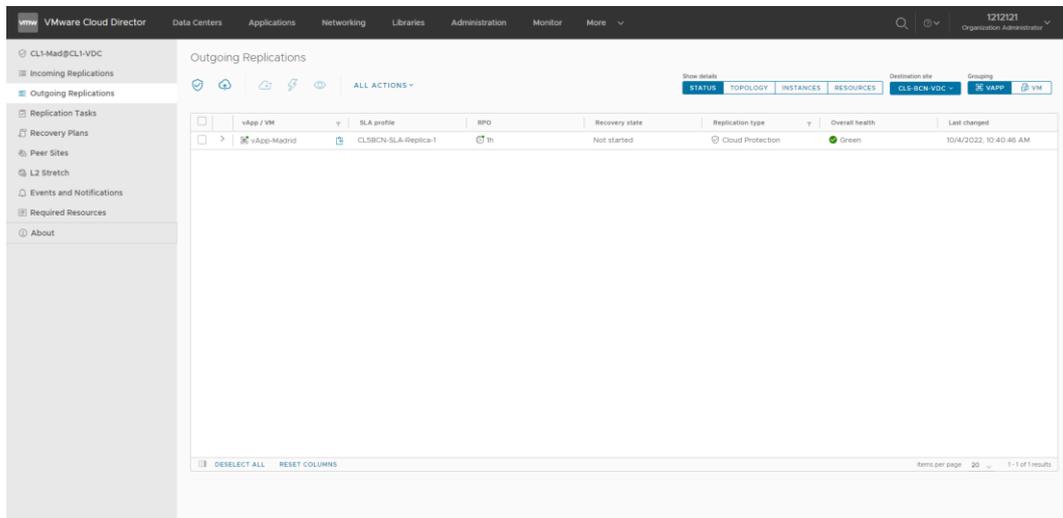


Figura 4.10 – Nueva réplica saliente creada.

4.3 Comprobación de la réplica desde destino

Para comprobar el estado de la réplica desde destino, conéctese a través de **Panel de Cliente** a Cloud Datacenter destino (Barcelona):

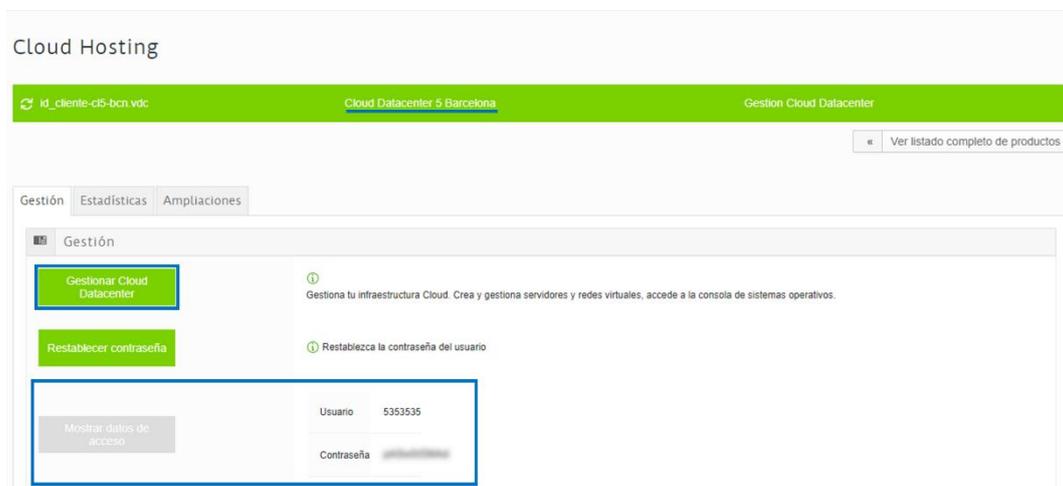


Figura 4.11 – Acceso a VDC destino para gestionar réplica

Desde el site destino, la réplica creada se verá como Réplica entrante. Para acceder a la misma, navegue en el menú principal hasta la opción **More** → **Availability (CL5-BCN-VDC)**.

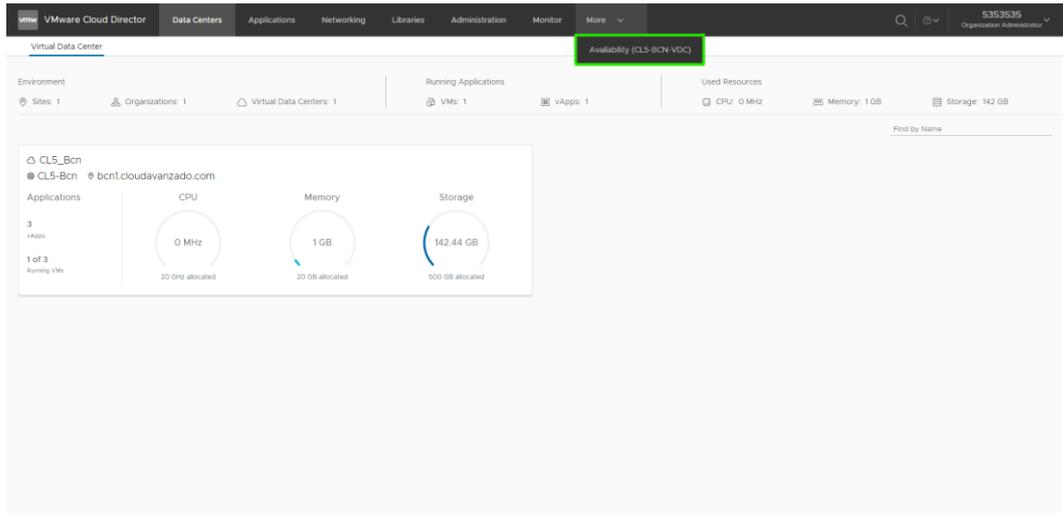


Figura 4.12 – VMware Cloud Director. Acceso a configuración DRaaS desde Cloud Datacenter destino

Dado que la réplica saliente configurada en origen se verá como réplica entrante en destino, navegue hasta réplicas entrantes a través del menú izquierdo.

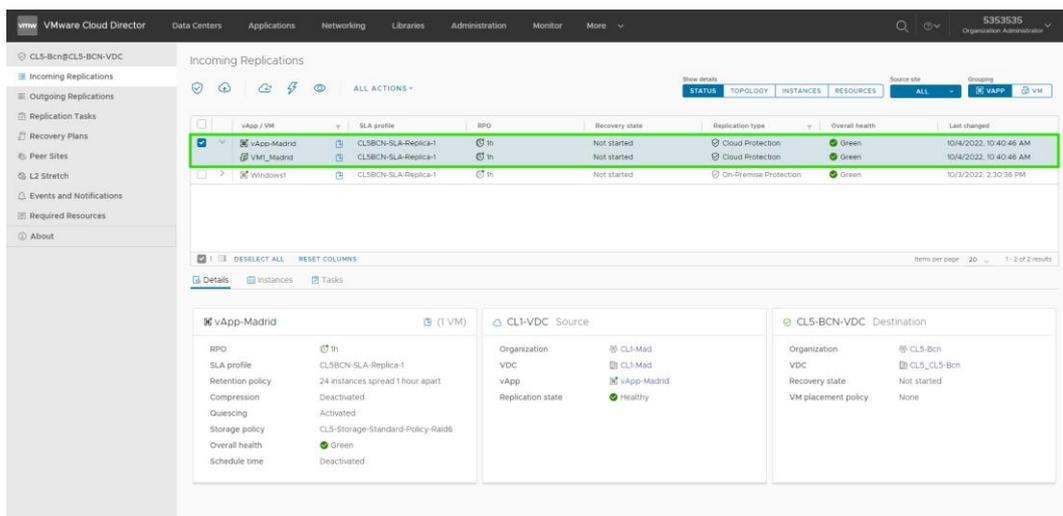


Figura 4.13 – Comprobación de réplica entrante en destino

Tenga en cuenta que en Cloud Datacenter destino, las máquinas virtuales no aparecerán en la sección de Máquinas virtuales de destino hasta que no se realice una acción de **Test** o **Failover**.

5 Test

La acción **Test** permite comprobar que se puede conmutar a la réplica creada en destino simulando la caída de las máquinas en origen, manteniendo la consistencia durante el proceso. Posteriormente se puede realizar un **Test Cleanup** para que la sincronización vuelva a ejecutarse.

Durante el proceso de Test no se replican los cambios, ya que las máquinas se levantan en destino en modo lectura, aunque pueden reiniciarse y sufrir cambios en disco. Al ejecutar **Test Cleanup**, la réplica continúa desde el momento en que se lanzó la acción **Test**.

Como se ha comentado en el apartado 4.3 *Comprobación de la réplica desde destino*, las máquinas virtuales procedentes de la réplica no son visibles en destino hasta que no se realiza una acción de **Test** o **Failover**, por lo que es importante comprobar que los recursos en destino son suficientes antes de ejecutar cualquiera de las acciones mencionadas:

- vCPU disponibles \geq vCPUs de MV a migrar
- RAM disponible \geq RAM de MV a migrar
- Almacenamiento disponible = 2x almacenamiento MV a migrar.

5.1 Ejecutar Test

Entre en el Portal de Cloud Director origen y seleccione dentro de réplicas salientes la MV/vApp cuya réplica ha sido creada siguiendo los pasos del apartado 4.2 *Creación de la réplica*. A continuación, despliegue **ALL ACTIONS** y seleccione **Test**.

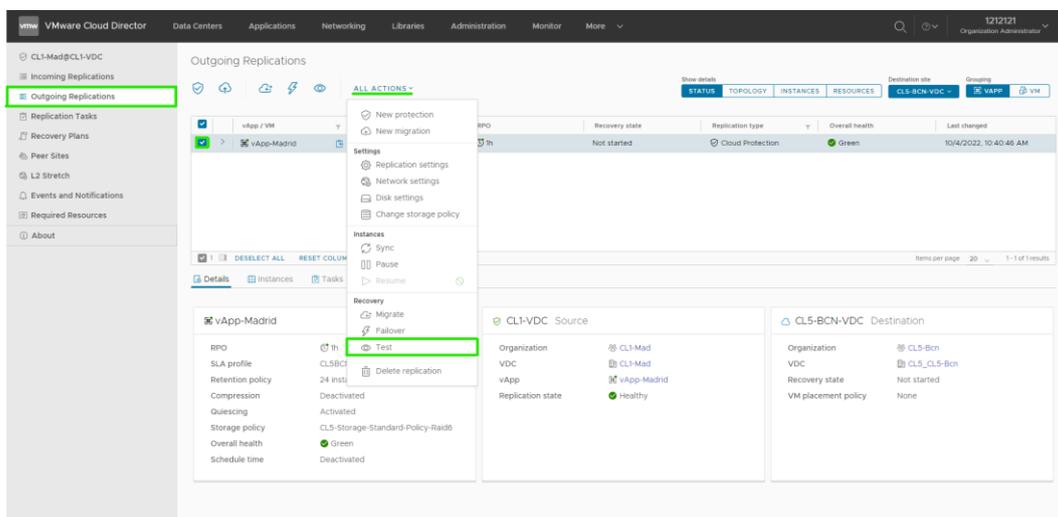


Figura 5.1 – Probar réplica saliente. Test

Se abre un asistente para la realización de la prueba.

1. **Recovery Settings:** en este apartado se puede elegir si encender las vApps recuperadas y aplicar la configuración de red preconfigurada en *Failover* o dirigir a una red específica en Cloud Datacenter destino. En este ejemplo, se procede a conectar todas las máquinas virtuales a una red de las ya configuradas en Cloud Director destino.

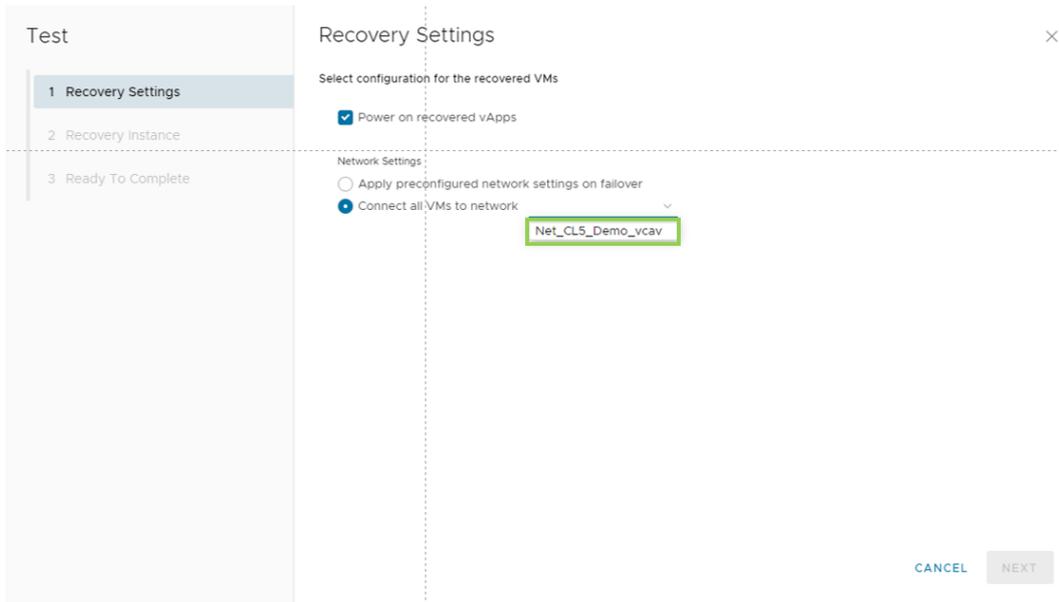


Figura 5.2 – Asistente Test. Configuración de recuperación

2. **Recovery Instance:** permite seleccionar si se quiere hacer la recuperación en el último estado sincronizado de la MV o sobre un estado anterior en el tiempo. En este caso, se realiza la prueba sobre el estado actual.

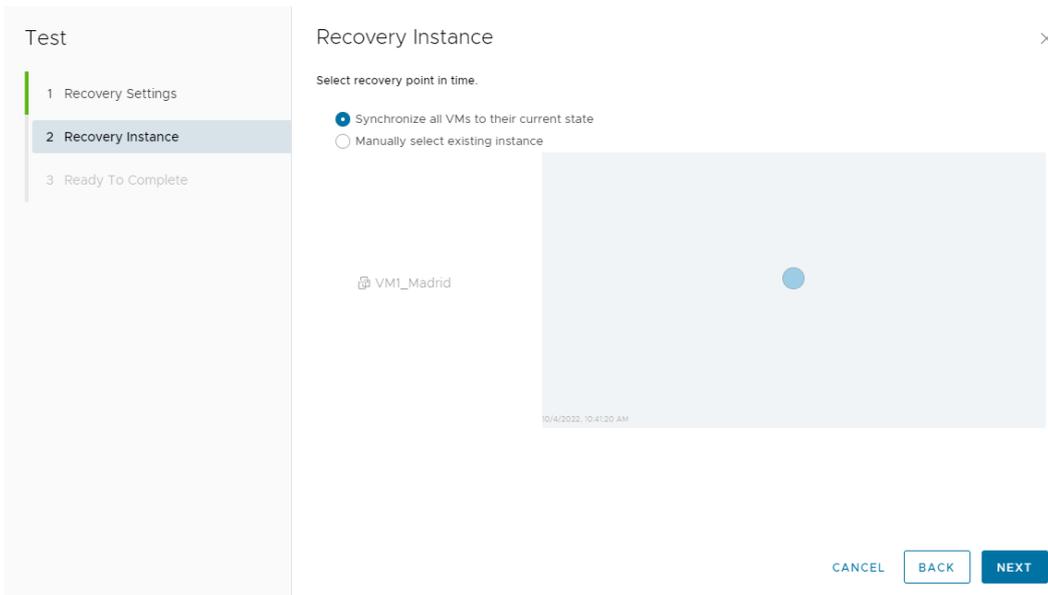


Figura 5.3 – Asistente Test. Instancia de recuperación

3. **Ready to Complete:** se muestra el resumen de los parámetros seleccionados para la prueba. Compruebe que la configuración es correcta, corríjala navegando hacia atrás en el asistente o finalice el proceso haciendo click en **Finish**.

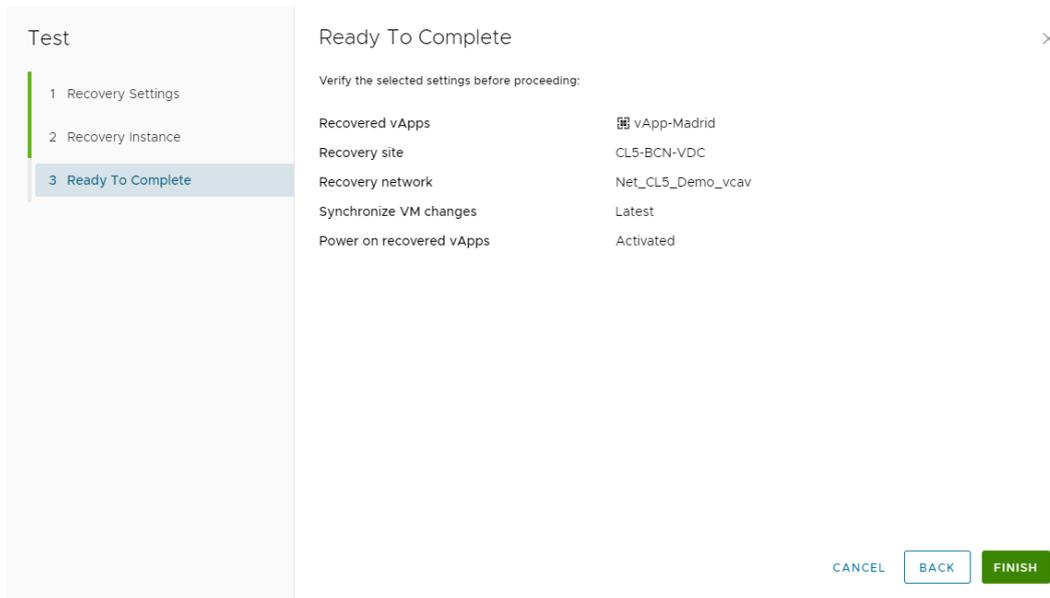


Figura 5.4 – Asistente Test. Listo para completar

En el campo **Last changed** se muestra el progreso. Al finalizar, es importante comprobar que todos los indicadores están en **Verde** y que en el campo **Overall health** aparece **Test image ready**.

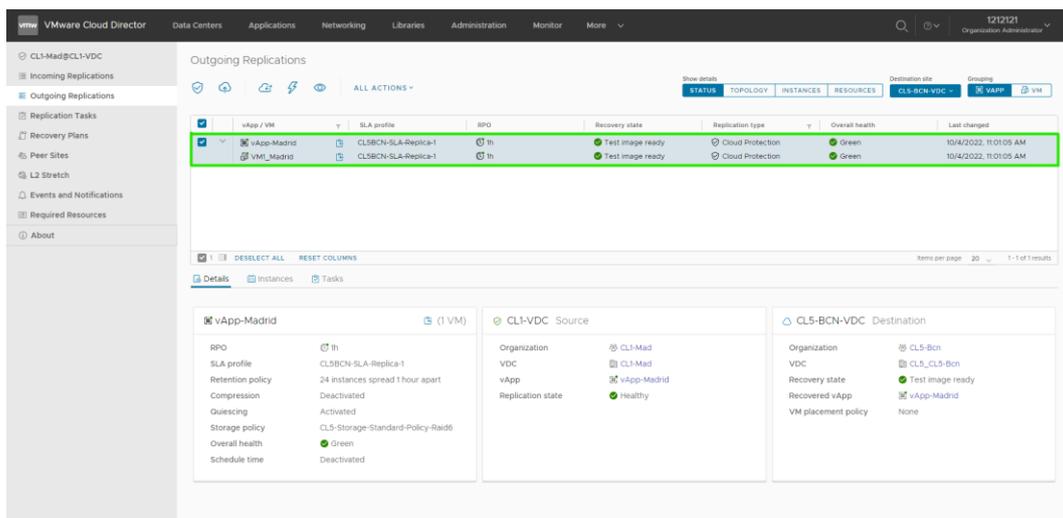


Figura 5.5 – Resultado Test

Entrando en el VDC destino, comprobamos que ahora sí aparece la MV replicada desde el VDC origen después de ejecutar **Test**.

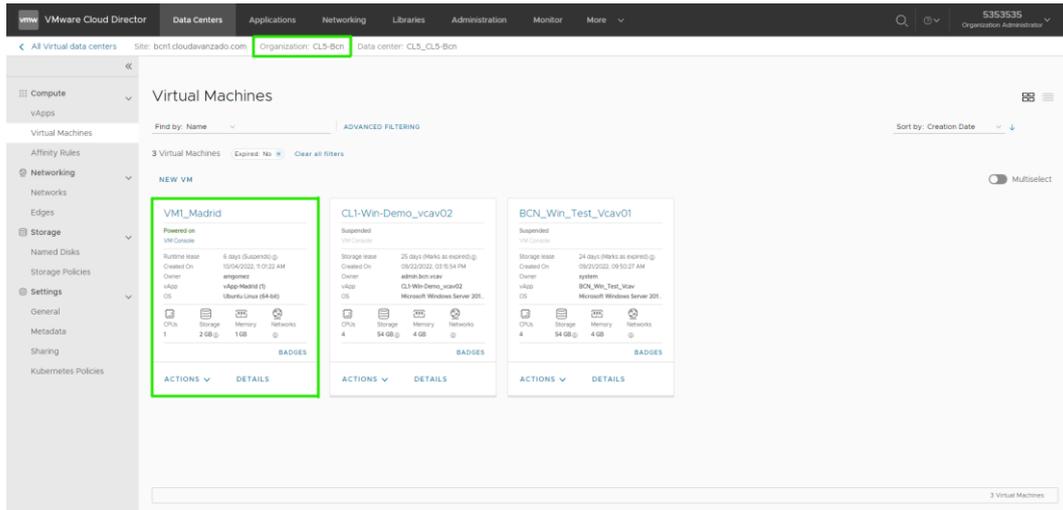


Figura 5.6 – Máquina replicada en destino

En la MV levantada en destino, haga las comprobaciones pertinentes para garantizar que, cuando se haga un failover desde la MV origen, levantará bien en destino. (acceso, integridad y conectividad)

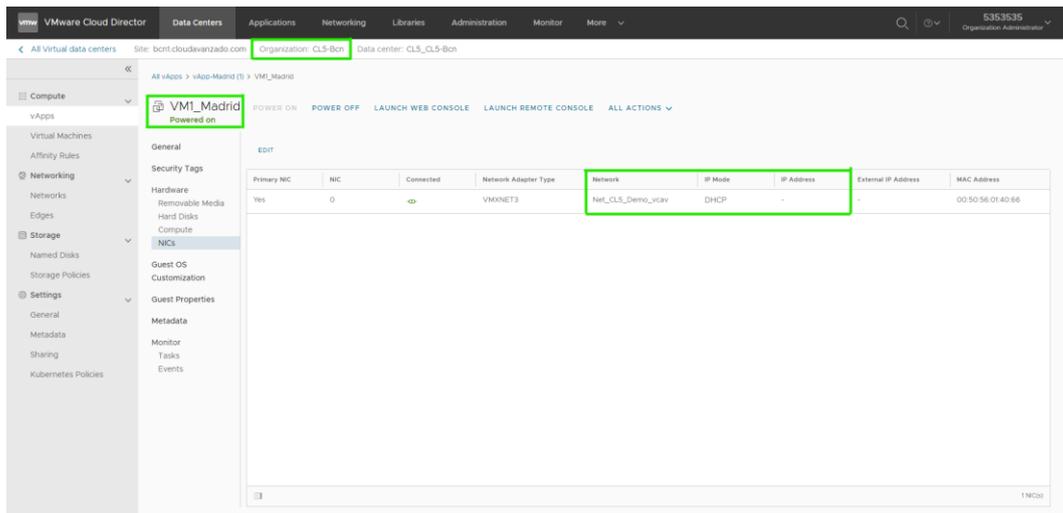


Figura 5.7 – Comprobación MV en destino

Si comprueba que no se ha asignado una IP por DHCP, puede obligar a que se asigne una IP del pool de direcciones. Para ello, haga click en **EDIT**, abra el desplegable **IP Mode** y seleccione **Static – IP Pool** y guarde.

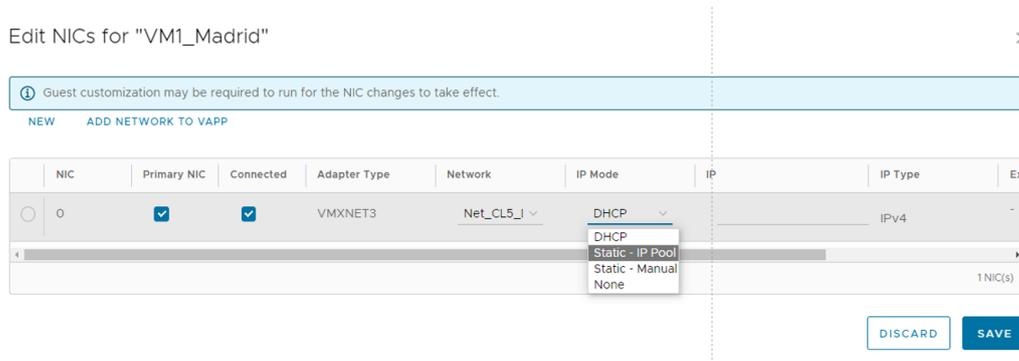


Figura 5.8 – Asignación de IP de pool de direcciones disponibles

Es necesario reiniciar la MV para asegurar la asignación de la dirección IP. Después del reinicio, aparece la información completa de la MV.

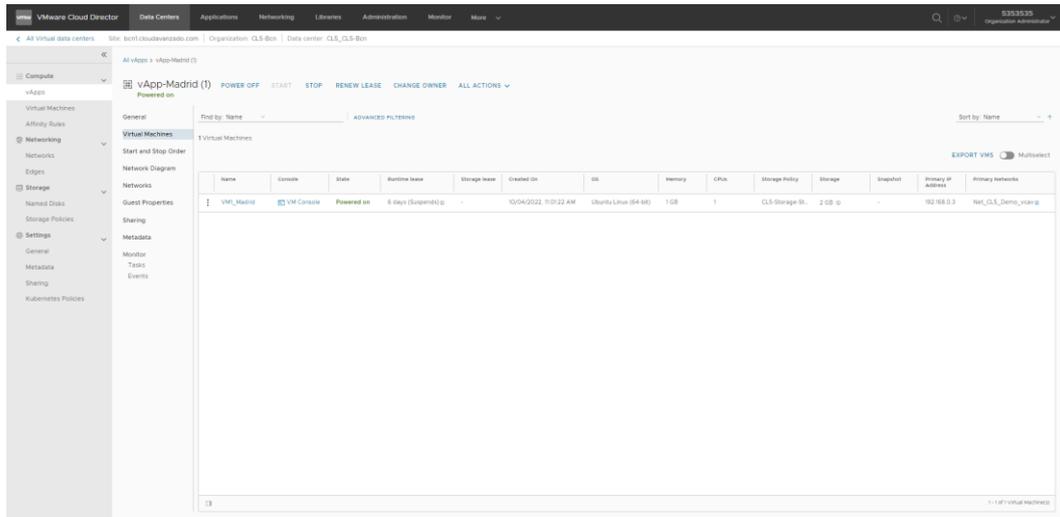


Figura 5.9 – Información en destino de MV levantada

5.2 Ejecutar limpieza del test

Una vez finalizada la prueba, la acción **Test Cleanup** borrará la MV creada durante la misma en Cloud Datacenter destino (Barcelona) reanudará la réplica creada desde el entorno de Cloud Datacenter origen (Madrid). Esta acción puede realizarse en el entorno origen o destino.

5.2.1 Test Cleanup desde origen

1. Acceda a Gestión Datacenter de Madrid.
2. Acceda a las réplicas salientes seleccionando **More → Availability CL1 (VDC)**
3. Del desplegable **ALL ACTIONS**, seleccione **Test Cleanup**.

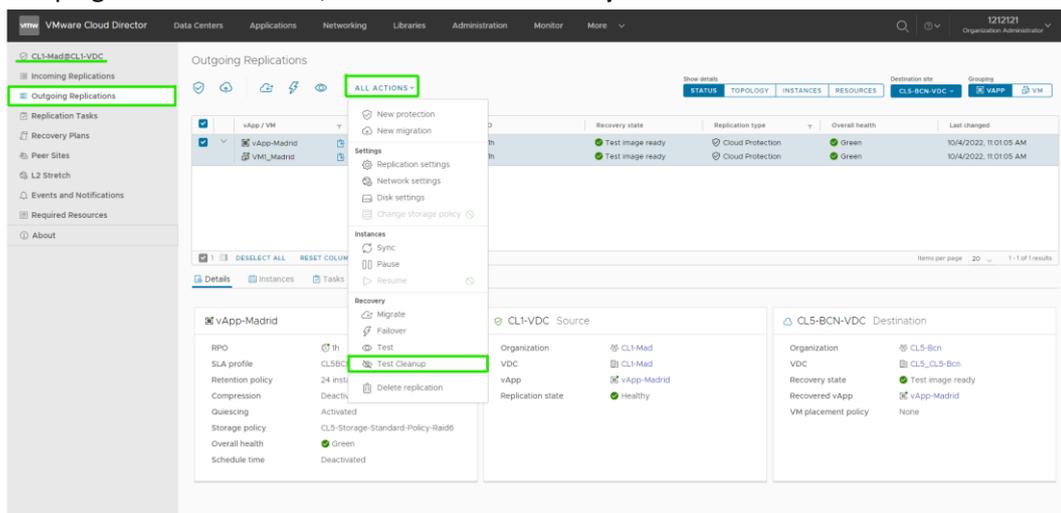


Figura 5.10 – Test cleanup desde origen

5.2.2 Test Cleanup desde destino

1. Acceda a Gestión Datacenter de Barcelona.

- Acceda a las réplicas entrantes seleccionando **More → Availability (CL5-BCN-VDC)**
- Del selector **ALL ACTIONS**, seleccione **Test Cleanup**.

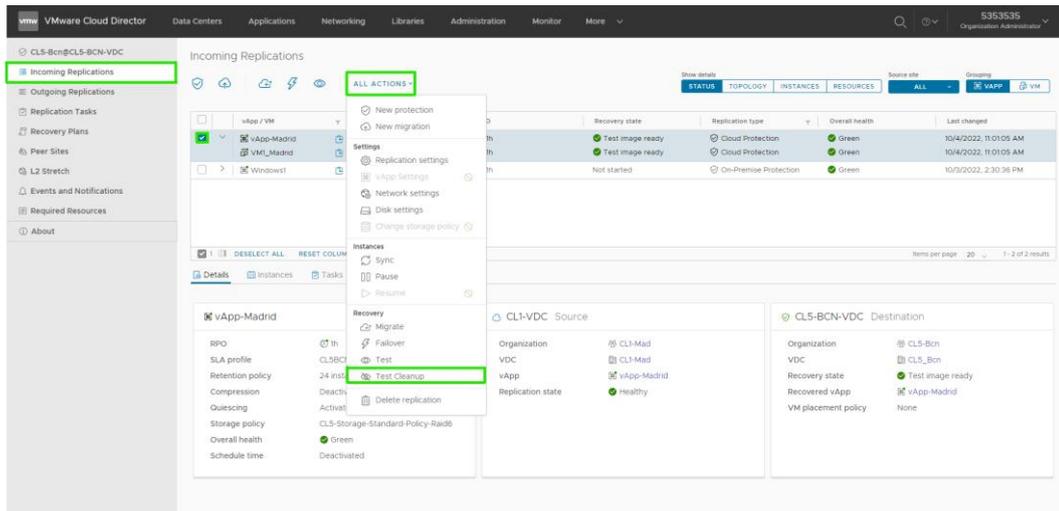


Figura 5.11 – Test Cleanup en destino

Consulte las réplicas salientes en origen (Madrid) o las réplicas entrantes en destino (Barcelona) para comprobar que el campo **Recovery state** muestra valor **Not Started** donde antes de la limpieza constaba **Test image ready**.

6 Failover

IMPORTANTE

ESTE PROCESO IMPLICA DE FORMA AUTOMÁTICA LA PARADA DEL ENTORNO ORIGEN PARA SU DESPLIEGUE EN EL ENTORNO DESTINO.

SE PERDERÁN TODOS LOS PUNTOS RPO.

Failover es un proceso manual y debe ejecutarse desde el destino, dado que se deberá realizar en caso de que los recursos en Cloud Datacenter origen no sean accesibles.

Cuando se hace un failover, no se debe cambiar de estado las MVs en origen: si está encendida se mantiene así y si hay acceso debe apagarse (**NO eliminarse**) pero siempre y cuando haya terminado el failover.

Entre en el Portal de Cloud Datacenter destino y navegue por el menú principal **More → Availability (CL5-VDC-BCN) → Incoming Replications → ALL ACTIONS → Failover**. También se puede utilizar el acceso rápido identificado con el símbolo ⚡.

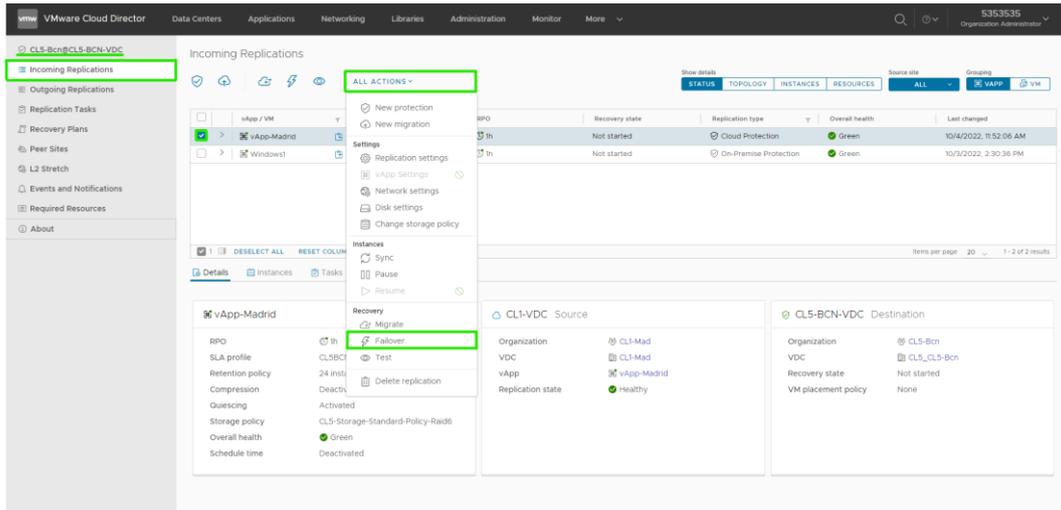


Figura 6.1 – Acceso a Failover

Se abre el asistente para realizar el Failover.

1. Recovery Settings

- **Consolidate VM disks:** **IMPORTANTE**, si se selecciona esta opción, se eliminan todos los puntos de recuperación (RPO) existentes para que la máquina virtual tenga más rendimiento en destino. Es importante tener en cuenta que, si bien mantener los puntos ralentiza la máquina, es prácticamente inapreciable.
- **Power on recovered vApps:** si se selecciona, al levantarse la máquina replicada en el destino se enciende.
- **Network Settings:** se puede seleccionar una configuración de red por defecto o bien seleccionar la red deseada de las configuradas en el Cloud Datacenter destino. En el ejemplo, optamos por esta segunda opción

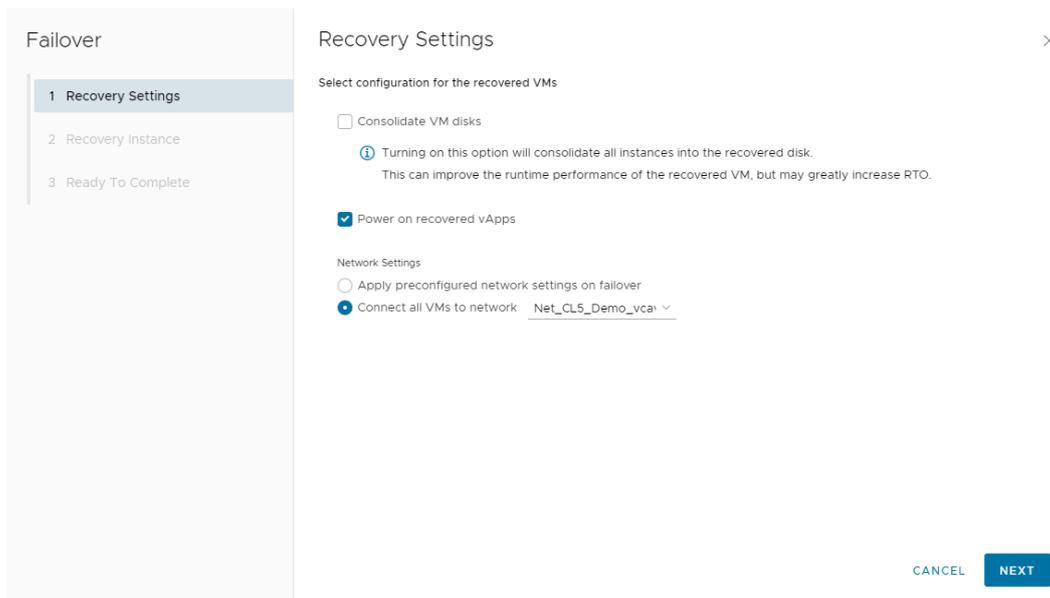


Figura 6.2 – Asistente Failover. Configuración de recuperación

2. **Recovery Instance:** seleccione el momento específico para la recuperación haciendo click en el diagrama.



Figura 6.3 – Asistente Failover. Instancia de recuperación

3. **Ready to Complete:** se muestra el resumen de la configuración del Failover. Compruebe que la configuración es correcta, en caso afirmativo finalice el proceso haciendo click en **Finish**.

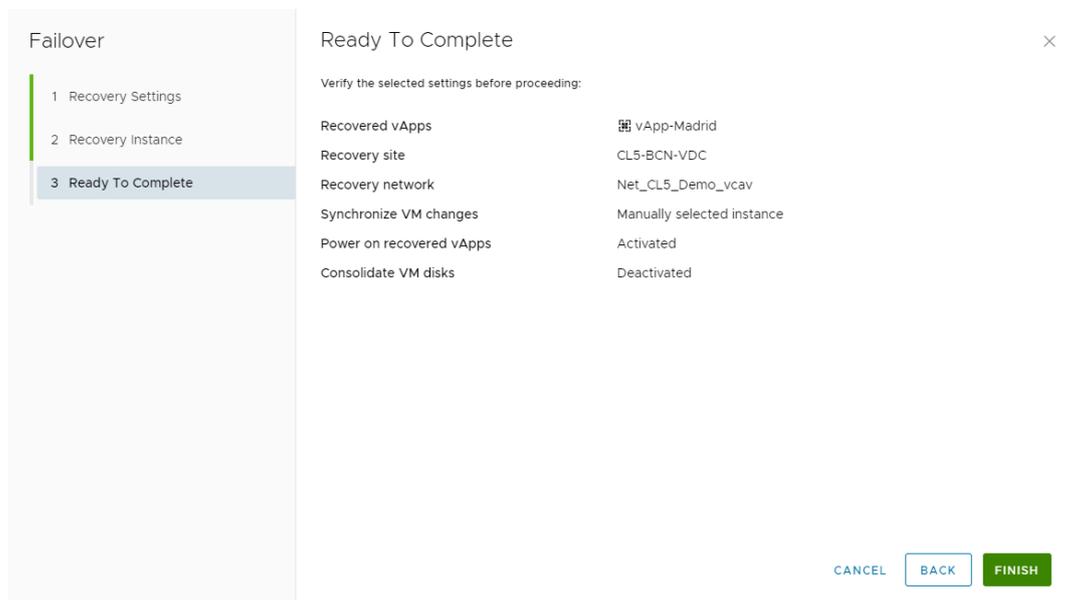


Figura 6.4 – Asistente Failover. Listo para completar

Se muestra el avance del progreso en el campo **Last changed**.

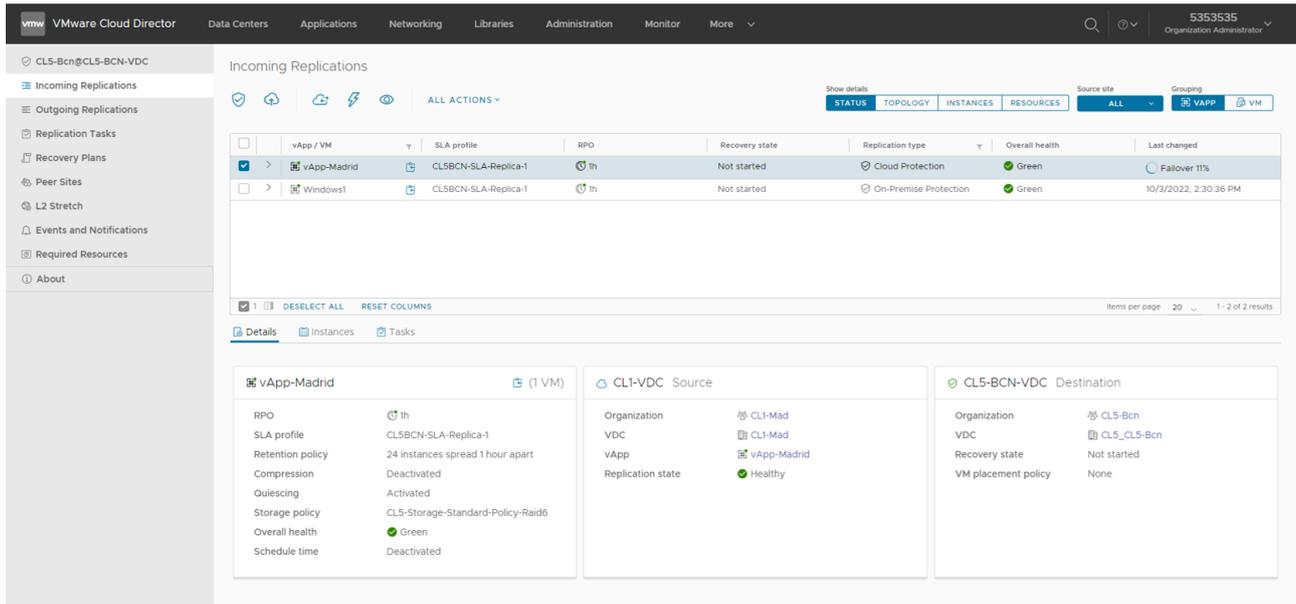


Figura 6.5 – Asistente Failover. Avance del proceso

Al finalizar el **Failover**, compruebe si se ha asignado IP a la máquina. En caso de que no se le haya asignado, fuerce la asignación de una IP del pool como se indicó en la *Figura 5.8 – Asignación de IP de pool de direcciones disponibles*. También se le podría asignar una IP fija.

Llegados a este punto, tras haber finalizado el proceso de failover, la situación es que los servicios se están ofreciendo desde el servicio Cloud Datacenter en el centro de respaldo en Barcelona.

¡¡Como parte del proceso de continuidad de sistemas, deberá establecer los procesos necesarios a nivel de red y comunicaciones para que los usuarios conmuten el acceso del sistema del Centro de Datos principal (Madrid) al Centro de Respaldo en Barcelona!!

Una vez realizado el Failover, elimine la réplica entrante que se creó en el apartado 4.2 Creación de la réplica desde el Portal Cloud Director destino. Para ello, entre en More → Availability (CL5-VDC-BCN), seleccione la réplica entrante existente y seleccione ALL ACTIONS → Delete replication.

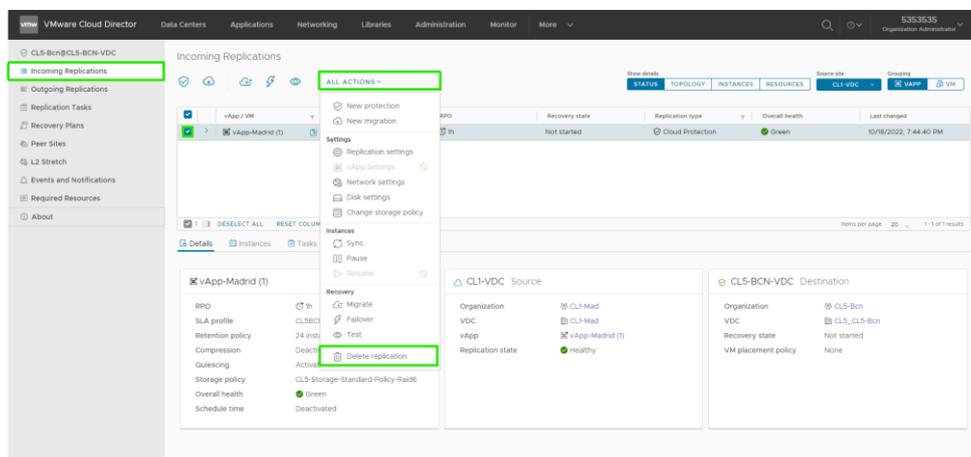


Figura 6.6 – Failover. Eliminación de la réplica Madrid-Barcelona existente

7 Recovery Failback

Cuando esté preparado para recuperar el escenario de partida resumido en la

Figura 4.1 para volver a ofrecer sus servicios desde Cloud Datacenter Madrid, debe crear una réplica desde Barcelona (nuevo origen) hacia Madrid (nuevo destino), utilizando la antigua MV de Madrid como semilla o máquina de inicialización.

Compruebe primero que la MV en Madrid esté apagada.

Configure una nueva protección saliente en Cloud Datacenter Barcelona siguiendo los pasos detallados en el apartado *4.2 Creación de la réplica* teniendo en cuenta que en este caso estamos configurando en sentido desde Barcelona hacia Madrid:

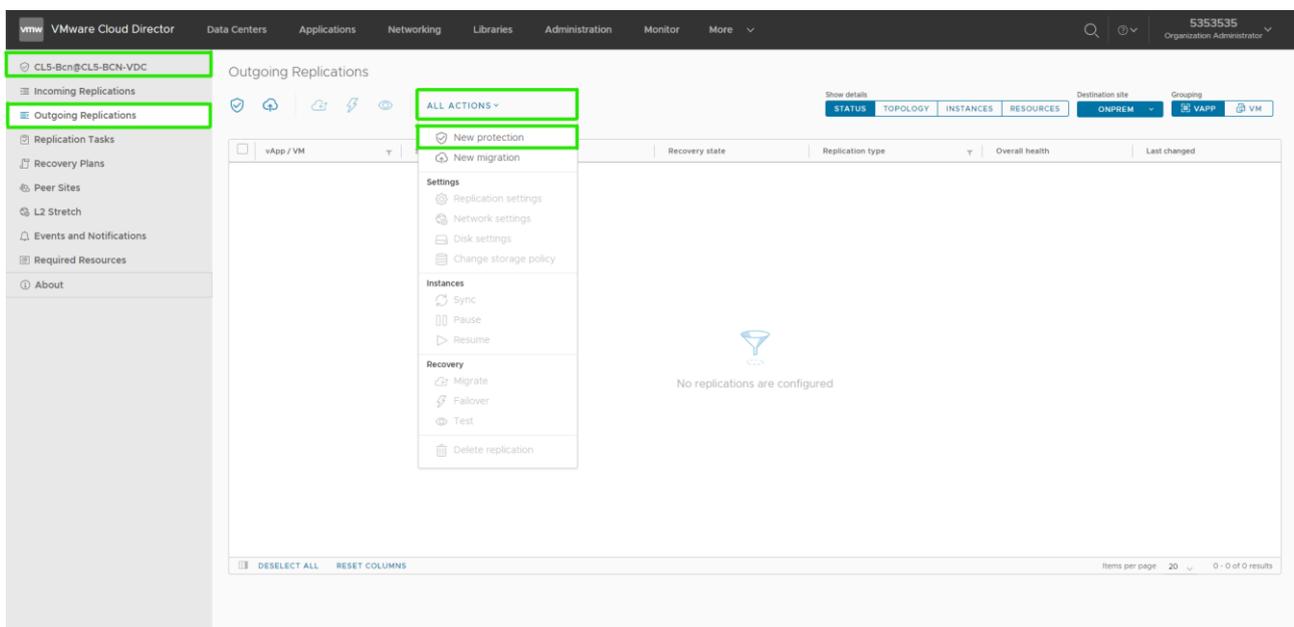


Figura 7.1 – Recovery Failback. Configuración de réplica saliente

Se abre un asistente para la configuración:

1. Cloud vApps and VMs:

- **Destination Site:** de las opciones mostradas en el desplegable **SELECT SITE**, seleccione **CL1-VDC** que es donde se quiere crear la réplica.

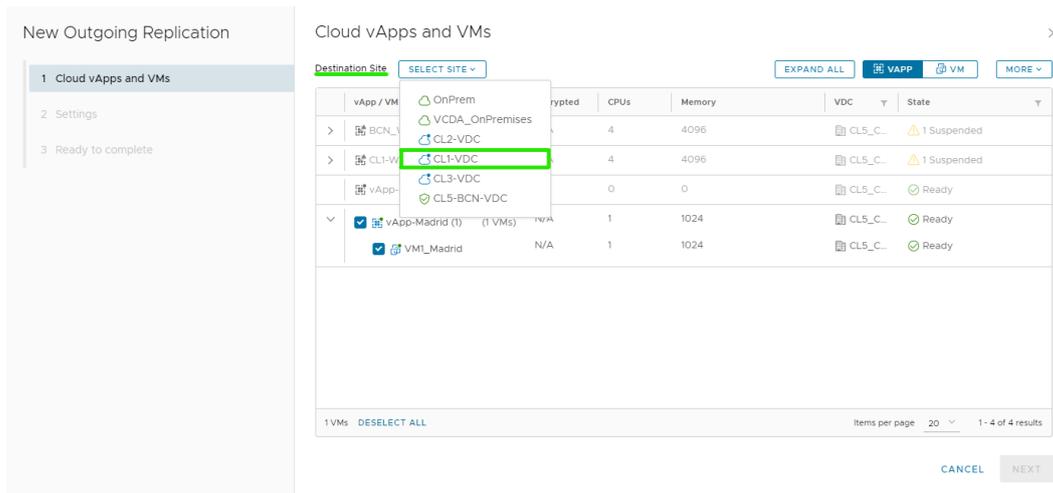


Figura 7.2 – Recovery Failback. Asistente Nueva réplica saliente. vApps y MVs de nube. Selección de site de destino

- **VAPP:** seleccione la vApp y/o la/las máquinas virtuales de las que quiere crear la réplica marcando los cuadros de selección necesarios.
2. **Destination VDC and Storage policy:** muestra la información del VDC destino y permite seleccionar la ubicación de la política de almacenamiento para las máquinas virtuales recuperadas del desplegable con las opciones configuradas en Cloud Datacenter Madrid.

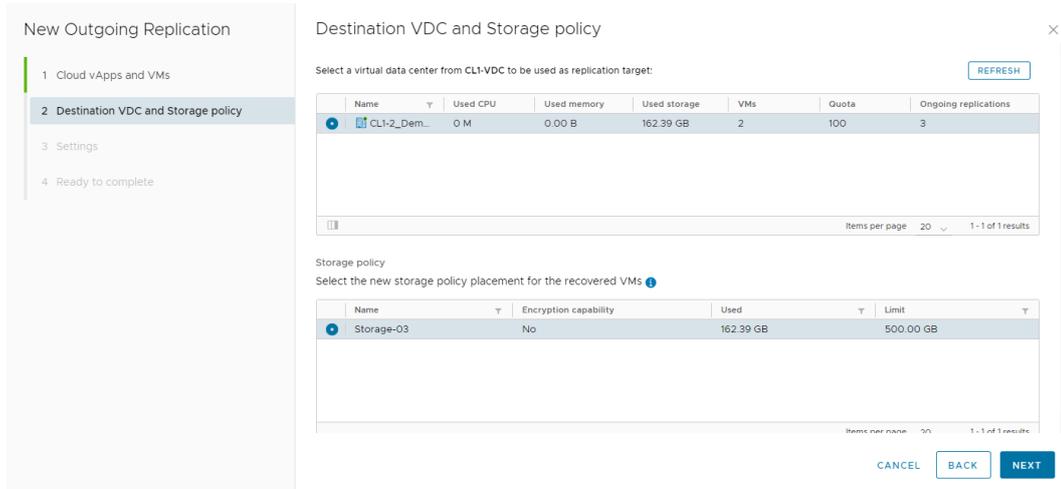


Figura 7.3 – Recovery Failback. Asistente Nueva réplica saliente. Selección de VDC destino y política de almacenamiento

3. Settings:

- **Use SLA Profile:** seleccione el número de replications por periodo de los disponibles en el seleccionable, que dependerán del producto que se haya contratado.
- **Exclude disks:** si se activa permite seleccionar qué discos de los existentes en las máquinas virtuales origen incluir en la réplica en destino, lo que permite reducir el tráfico generado y el tiempo invertido en la replicación. Se recomienda dejar desactivado para asegurar que todo se replica.
- **Configure Seed VMs:** si se activa permite seleccionar una copia anterior existente en destino como base para la creación de la réplica, reduciéndose el tráfico generado en el proceso de

réplica. En este caso, queremos utilizar como máquina de inicialización la original que prestaba los servicios desde Madrid y que hemos apagado. Seleccione dicha máquina / vApp.

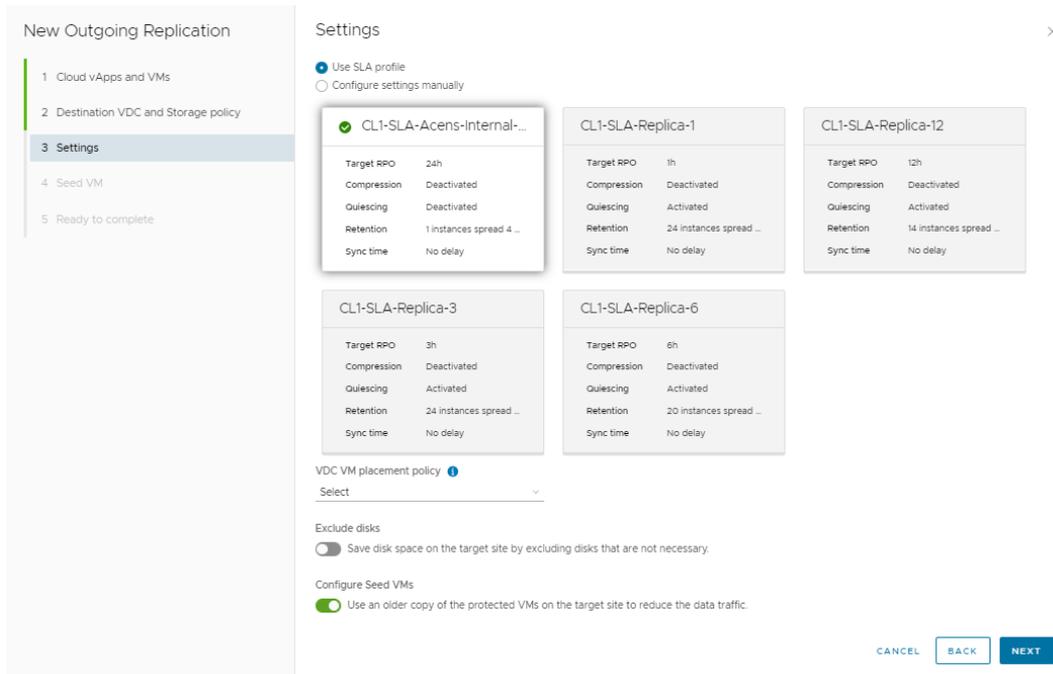


Figura 7.4 – Recovery Failback. Asistente Nueva réplica saliente. Apartado Configuración

4. **Seed VM:** este paso aparece dentro del asistente al activar la opción de uso de MV de inicialización.

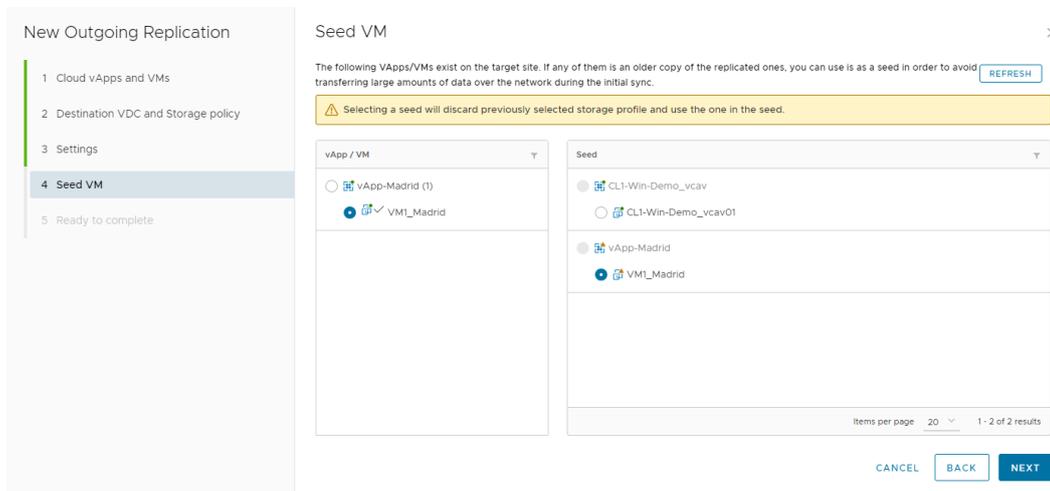


Figura 7.5 – Recovery Failback. Asistente Nueva réplica saliente. Apartado MV de inicialización

5. **Ready to complete:** se muestra un resumen de la configuración. Compruebe que es correcta, corríjala navegando hacia atrás en el asistente o finalice el proceso haciendo click en **Finish**.

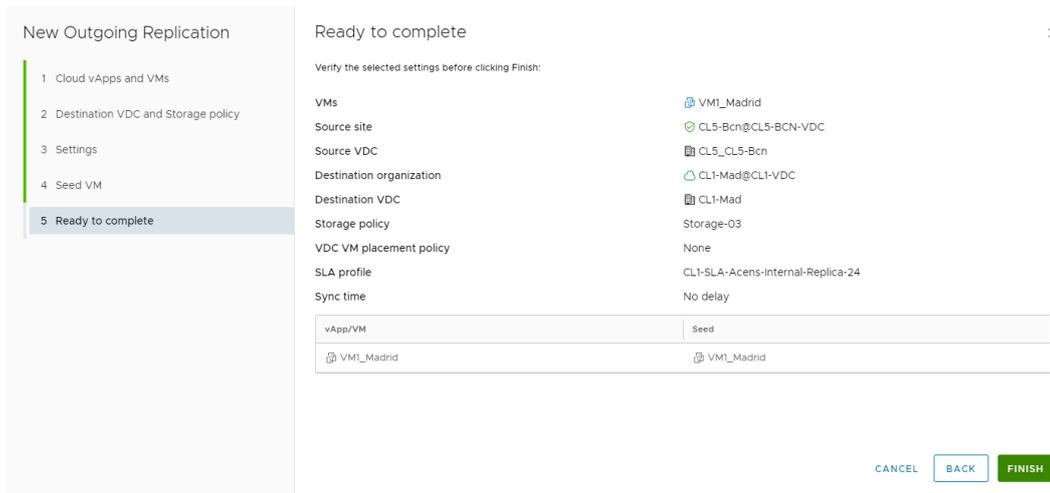


Figura 7.6 – Recovery Failback. Asistente Nueva réplica saliente. Apartado Listo para completar

En este momento comienza la protección. Se muestra el progreso y el campo **Overall health** indica valor **● Rojo**.

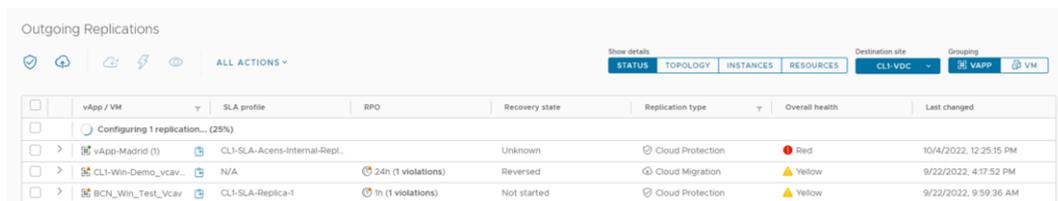


Figura 7.7 – Recovery Failback. Asistente Nueva réplica saliente. Progreso de creación de réplica

Al finalizar la acción, el campo **Overall health** muestra el valor **● Verde** para indicar que el proceso de creación ha finalizado con éxito.

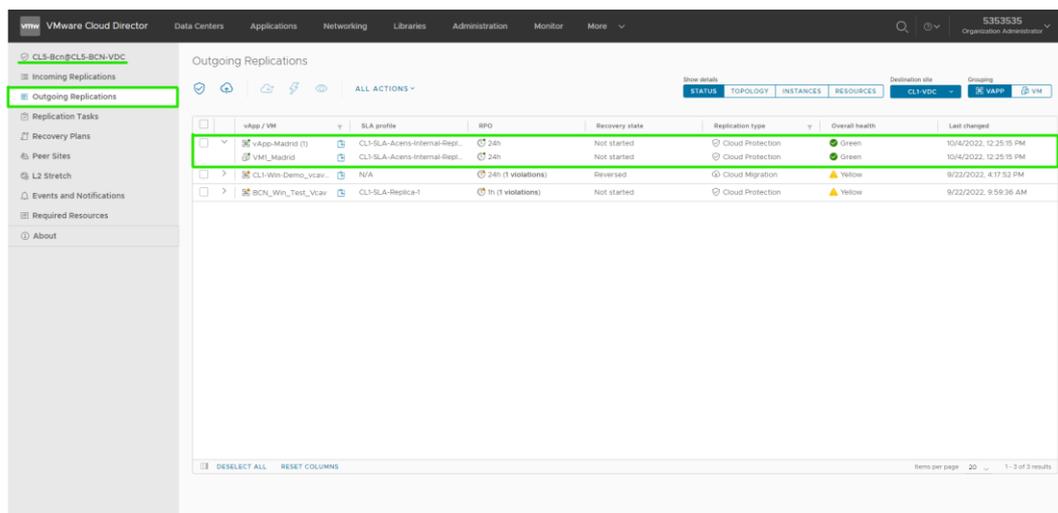


Figura 7.8 – Recovery Failback. Réplica saliente creada con MV de inicialización

Si entramos ahora en el Cloud Datacenter de Madrid, vemos como la máquina virtual origen ya no está, dado que se ha utilizado como máquina de inicialización de la réplica que se hizo desde Cloud Datacenter de Barcelona.

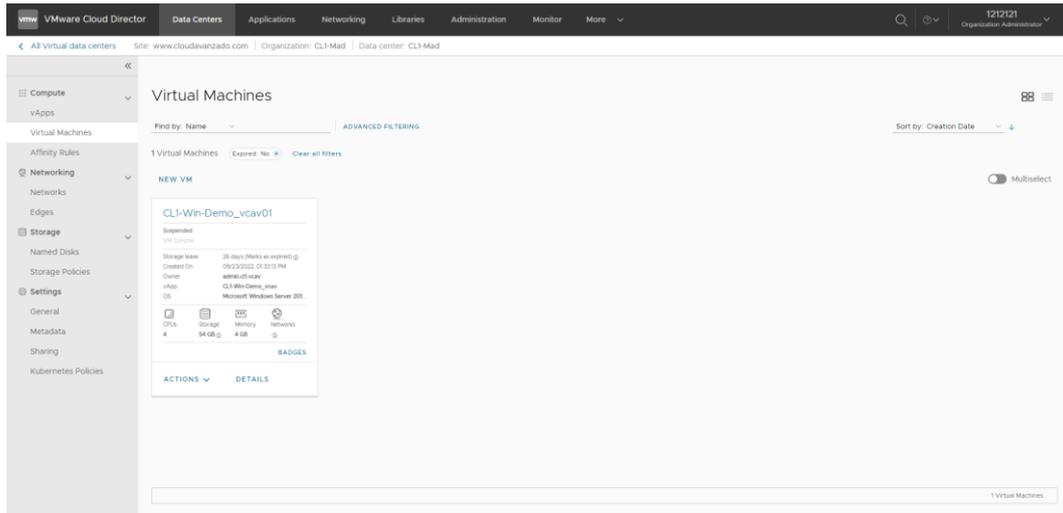


Figura 7.9 – Máquinas virtuales Cloud Datacenter Madrid

Si entramos en réplicas entrantes comprobamos que vemos la réplica que se está haciendo desde Barcelona.

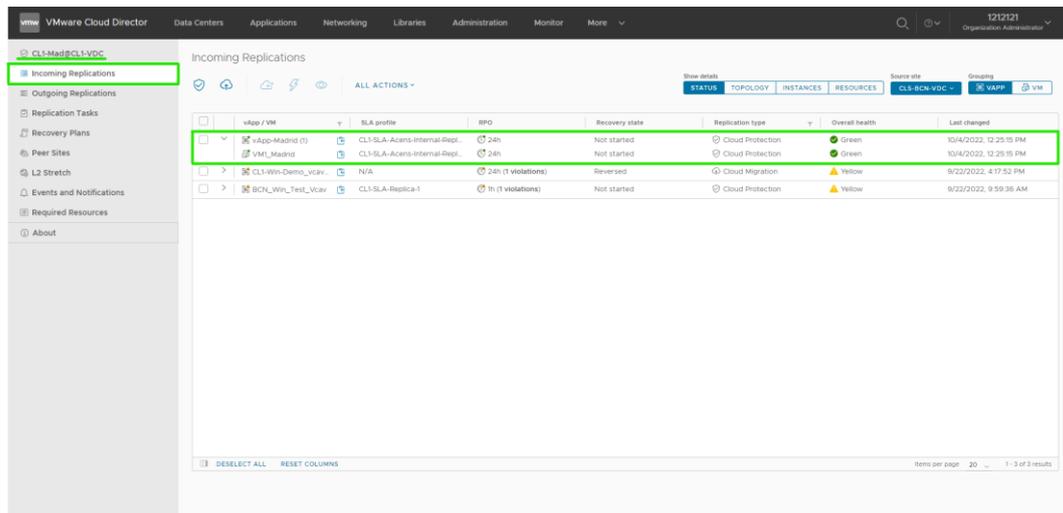


Figura 7.10 – Réplicas entrantes en Cloud Datacenter Madrid

Por tanto, el escenario en este punto es que tenemos el servicio activo en Cloud Datacenter en Barcelona y estamos protegiendo mediante réplica en Madrid.

Si queremos volver al estado inicial en el que el servicio se ofrece desde Cloud Datacenter Madrid y la protección se hace desde Cloud Datacenter en Barcelona se realizan los pasos de Conmutación por error (Failover) y Reverse en orden inverso:

1. Lanzar **Failover** en Madrid.
2. Apagar la MV en Barcelona.
3. Borrar la réplica saliente en Barcelona.
4. Configurar la protección desde Madrid hacia Barcelona.
5. Configurar la red si fuera necesario.

En este punto estamos en la situación de partida mostrada en la **Figura 4.1**.

8 Monitorización de las réplicas

Haciendo click en las flechas  situadas en la esquina inferior derecha de la pantalla, podemos acceder a la Consola y ver los eventos generados.

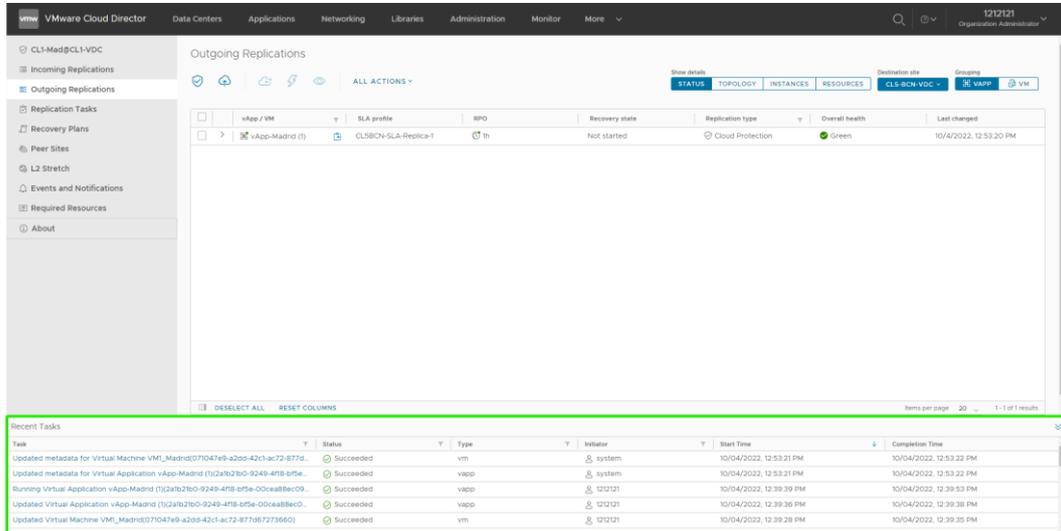


Figura 8.1 – Eventos generados

Por lo general, los eventos pueden ser compartidos por dos posibles vías:

- Enviar a vCloud.
- Enviar por correo electrónico.

8.1 Envío de notificaciones a vCloud

Acceda al entorno Cloud Director, ya sea en Cloud Datacenter origen o destino, y navegue por el menú principal **More** → **Availability (CL1-VDC)** o **More** → **Availability (CL5-VCD-BCN)** según corresponda. A continuación, seleccione **Events and Notifications** en el menú izquierdo.

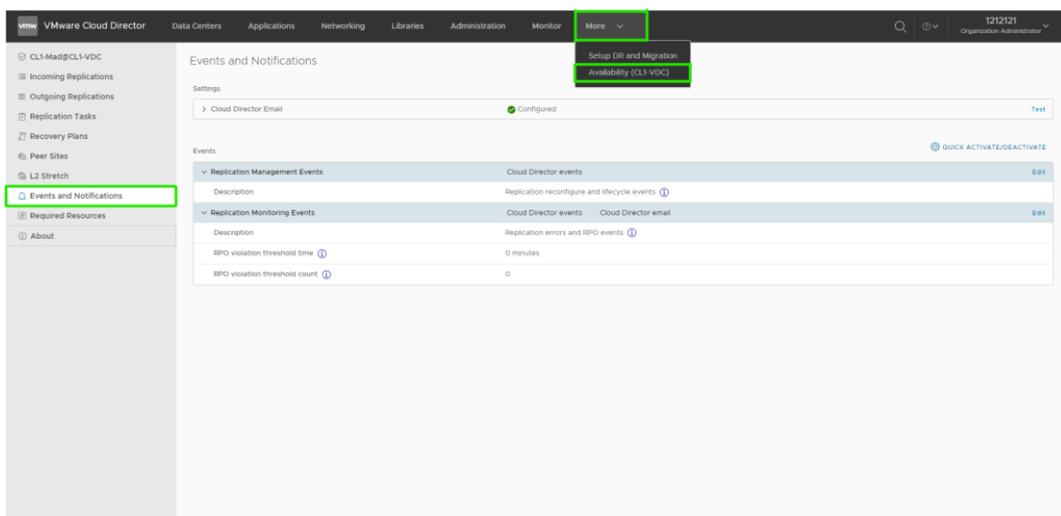


Figura 8.2 – Eventos y notificaciones DRaaS

Dependiendo del tipo de evento, existen dos vías para su envío a vCloud:

Tipo de evento	Envío vCloud	Envío por email
Eventos de administración de las réplicas (reconfiguración, inicio, parada, etc.)	✓	
Eventos de supervisión de réplicas (por errores en réplicas)	✓	✓

Tabla 8.1 – Formas de envío de eventos a vCloud

8.2 Eventos enviados a vCloud

Los eventos enviados directamente a vCloud, están visibles navegando por el menú principal **Monitor** → **Events**.

Description	Status	Type	Target	Owner	Occurred At	Service Namespace
Task 'Update metadata' complete	Succeeded	task	METADATA_UPDATE	system	10/04/2022, 12:53:22 PM	com.vmware.vcloud
Task 'Update metadata' complete	Succeeded	task	METADATA_UPDATE	system	10/04/2022, 12:53:22 PM	com.vmware.vcloud
VM 'VMI_Madrid' (071047e9-a2d8-42c1-ac72-877b67273660) modification	Succeeded	vm	VMI_Madrid	system	10/04/2022, 12:53:21 PM	com.vmware.vcloud
vApp 'vApp-Madrid (1)' (2a1b21d0-9249-4f1b-8f5e-00ca88ec09e) modification	Succeeded	vapp	vApp-Madrid (1)	system	10/04/2022, 12:53:21 PM	com.vmware.vcloud
Task 'Update metadata' start	Succeeded	task	METADATA_UPDATE	system	10/04/2022, 12:53:21 PM	com.vmware.vcloud
Task 'Update metadata' start	Succeeded	task	METADATA_UPDATE	system	10/04/2022, 12:53:21 PM	com.vmware.vcloud
Task 'Update metadata' creation	Succeeded	task	METADATA_UPDATE	system	10/04/2022, 12:53:21 PM	com.vmware.vcloud
Task 'Update metadata' creation	Succeeded	task	METADATA_UPDATE	system	10/04/2022, 12:53:21 PM	com.vmware.vcloud
Task 'Deploy vApp' complete	Succeeded	task	VAPP_DEPLOY	1212121	10/04/2022, 12:39:53 PM	com.vmware.vcloud
VM 'VMI_Madrid' (071047e9-a2d8-42c1-ac72-877b67273660) power state change (state=1)	Succeeded	vm	VMI_Madrid	system	10/04/2022, 12:39:51 PM	com.vmware.vcloud
VM 'VMI_Madrid' (071047e9-a2d8-42c1-ac72-877b67273660) power on	Succeeded	vm	VMI_Madrid	1212121	10/04/2022, 12:39:48 PM	com.vmware.vcloud
vApp 'vApp-Madrid (1)' (2a1b21d0-9249-4f1b-8f5e-00ca88ec09e) start	Succeeded	vapp	vApp-Madrid (1)	1212121	10/04/2022, 12:39:47 PM	com.vmware.vcloud
Network 'net-c1-2-demo_vcsa' (6125a86c-70c-4580-d8e0-03c4f8e056) deploy	Succeeded	network	net-c1-2-demo_vcsa	1212121	10/04/2022, 12:39:45 PM	com.vmware.vcloud
Task 'Deploy vApp' start	Succeeded	task	VAPP_DEPLOY	1212121	10/04/2022, 12:39:40 PM	com.vmware.vcloud
Starting vApp 'vApp-Madrid (1)' (2a1b21d0-9249-4f1b-8f5e-00ca88ec09e)	Succeeded	vapp	vApp-Madrid (1)	1212121	10/04/2022, 12:39:39 PM	com.vmware.vcloud

Figura 8.3 – Eventos enviados a vCloud

8.3 Eventos enviados por email

Todas las organizaciones disponen, por defecto, de un relay de correo para el envío de notificaciones a todos los usuarios que tengan rol **“Organization Administrator”**. Se puede acceder a la configuración a través de la opción **Administration à Email**.

TEST EDIT

Using system default SMTP server

SMTP server name

SMTP server port

Requires authentication

Using system default notification settings

Sender's email address: soporte-plus@acens.com

Email subject prefix: [vcloud]

Send system notifications to: All organization administrators

Figura 8.4 – Notificación de eventos a todos los administradores

9 Canales de atención

Los canales de atención de acens son:

- Consulta a través de **Panel de Cliente**.
- Teléfono 900 103 293.
- Email soporte@acens.com.
- **Chat** con un operador.

Si dispone de las credenciales de Panel de Cliente, puede abrir una nueva consulta haciendo click en Soporte, en los accesos directos existentes en la parte superior de la ventana.



Figura 9.1 – Acceso a Soporte

Dentro del área de Soporte, haga click en el botón de Abrir Consulta.



Figura 9.2 – Creación de Consulta

Se abrirá un formulario en el que podrá facilitar los datos de su consulta, ya sea genérica o relacionada con uno de los servicios contratados.

Crear nueva consulta

Crear nueva consulta

Tipo de consulta * Consulta general
 Consulta sobre un producto

Producto 1 - IDcliente.producto.caract

Asunto *

Texto *

B I U

Adjuntar archivo Ninguno archivo selec.

Archivos válidos: jpg, gif, png, pdf, xls/x, doc/x. Máximo 5Mbytes.

Enviar copia a Email

Rellene los campos del formulario para generar un nuevo ticket de soporte.

Cancelar Crear consulta

Figura 9.3 – Formulario para creación de consulta

La consulta se seguirá a través del email informado en el formulario o desde el propio panel de cliente, en el listado de consultas visible al acceder a Soporte, como se muestra en la *Figura 9.2*.