

SERVICIO DE SITE RECOVERY EN AZURE PARA AMBIENTE DE CONTINGENCIA

DOCUMENTO DRP AZURE SITE RECOVERY

Corporación Maresa

Autor:
Byron Rivas

Fecha:
01/08/2018

Versión:
1.0

Tabla de Contenido

INTRODUCCIÓN	3
CONFIDENCIALIDAD	3
DEFINICIÓN DEL PROBLEMA	3
AZURE SITE RECOVERY	4
TIPOS DE FAILOVER	4
RECUPERACIÓN CENTRO DE DATOS	5
OBJETIVOS DE RPO Y RTO DE SERVICIO	5
ROLES Y RESPONSABILIDADES	6
EJECUTAR TEST FAILOVER	7
EJECUTAR FAILOVER	10
CONSIDERACIONES DE RPO Y RTO DE AZURE SOLUTIONS	14



Revisión y aprobación del documento

Historial de cambios:

Versión	Autor	Fecha	Descripción
0.1	Byron Rivas	30-07-2018	Generación del documento
1.0	Sheyla Bustos	01-08-2018	Revisión interna

Aprobado por:

Nombre	Cargo	Fecha



INTRODUCCIÓN

CONFIDENCIALIDAD

El material contenido en este documento es propiedad de **Corporación Maresa**. Este material incluye información que no debe ser discutida fuera la compañía y no puede ser duplicada para ningún efecto, lo cual significa que es de uso exclusivo del personal designado.

El sello de confidencialidad hace referencia a que esta información no puede ser reproducida ni revelada a terceros.

DEFINICIÓN DEL PROBLEMA

La evolución y funcionamiento de la plataforma de **Corporación Maresa** ha sido en general exitoso durante los últimos años, con la finalidad de garantizar la disponibilidad y continuidad del negocio, se ha implementado Azure Site Recovery.



AZURE SITE RECOVERY

El servicio de Recuperación de Sitios o Centros de Datos, contribuye a una solución robusta de Recuperación de Desastres que protege los servidores e información automatizando la replicación y transferencia de servicio hacia Azure o a un Sitio de Datos secundario.

Los pasos Generales para configurar Azure Site Recovery son:

1. Crear una Bóveda.
2. Crear los recursos en Azure para el ambiente.
3. Crear y configurar los grupos de protección.
4. Habilitar la protección de las máquinas virtuales.
5. Probar la implementación.

El objetivo de crear la infraestructura de ASR es el de proteger el centro de datos y su operación ante cualquier desastre que ocurra. Por lo tanto, una operación indispensable es la acción de habilitar el sitio de recuperación o "Failover".

TIPOS DE FAILOVER

Existen tres tipos de Failover que se detallan a continuación:

Tipo	Ejecución	Detalles
Test Failover	Para validar la estrategia de replicación o hacer una prueba del plan.	Sin pérdida de datos o tiempos caídos. Sin impacto a la replicación, sin impacto a la producción.
Failover Planeado	Para mantenimientos planeados, mantener los servicios trabajando en casos de amenazas conocidas como perdidas de energía en el caso de tener un sitio On Premise.	Sin pérdida de datos. Tiempo sin servicio durante el apagado de las máquinas virtuales en el sitio primario y el arranque en el secundario. Las máquinas virtuales de respaldo se convierten en las primarias.
Failover no Planeado	Se corre de manera reactiva cuando el sitio primario no es accesible por un incidente inesperado, ya sea por perdida de energía, u otro factor. Se puede ejecutar el Failover NO planeado incluso si el sitio primario no está disponible.	Dependiendo de la frecuencia de replicación, puede haber perdida de datos. La información estará actualizada de acuerdo a la última sincronización efectuada.

RECUPERACIÓN CENTRO DE DATOS

Para la recuperación del centro de datos, se identificó los servidores más importantes para el funcionamiento del negocio, los mismos que fueron protegidos con Azure Site Recovery y se detallan a continuación:

Servidor	IP Privada	IP Pública
Maresa-BZT-01	172.16.2.49	-
Maresa-DB-04	172.16.2.52	13.90.80.245
Maresa-DMS-01	172.16.2.27	-
Maresa-Web-01	172.16.2.13	13.82.169.247
Maresa-Erp-01	172.16.2.45	-
Maresa-Brk-02	172.16.2.22	40.114.1.66
Maresa-DB-10	17.16.2.51	-

OBJETIVOS DE RPO Y RTO DE SERVICIO

Servicio de TI	Escenario	RPO	RTO	Prioridad
<ul style="list-style-type: none"> Microsoft BizTalk Server 2016 APL Bus Transac. IIS App BZT01: Notificaciones, PolBodegas, SAV 	Error del servidor Maresa-BZT-01	1 hora	2 horas	Alta
<ul style="list-style-type: none"> Microsoft SQL Server 2016 BDD's Server 	Error del servidor Maresa-DB-04	1 hora	2 horas	Alta
<ul style="list-style-type: none"> DMS_CR_85 APL DMS GCS 	Error del servidor Maresa-DMS-01	1 hora	2 horas	Alta
<ul style="list-style-type: none"> App Web CMH: Seguridades, SAV, WebServices, HelpDeskTicket Services: EsDinamico, AgendaFord, Notificaciones 	Error del servidor Maresa-WEB-01	1 hora	2 horas	Alta
<ul style="list-style-type: none"> WS Advance Lic. Advance Server SO99: 760 Maresa, 760 Maresa Sub 	Error del servidor Maresa-ERP-01	1 hora	2 horas	Alta

<ul style="list-style-type: none"> • IIS WS CRM • WS Adv 				
<ul style="list-style-type: none"> • Bróker RDP • IIS RDWeb 	Error del servidor Maresa-BRK-02	1 hora	2 horas	Alto
<ul style="list-style-type: none"> • Microsoft SQL Server 2016 • BDD Bus Transac BZT01 	Error del servidor Maresa-DB-10	1 hora	2 horas	Alto

RPO: El proceso de Failover se ejecuta con la opción **Latest app-consistent** ya que garantiza que la VM se inicia, no hay corrupción ni pérdida de datos, los datos son consistentes con la aplicación que usa esta información. Este parámetro de sincronización está configurado para una (1) hora.

RTO: Failover **(30 min)** + Levantamiento de Servicios y Pruebas **(1 hora, 30 min)** = **2 horas**

ROLES Y RESPONSABILIDADES

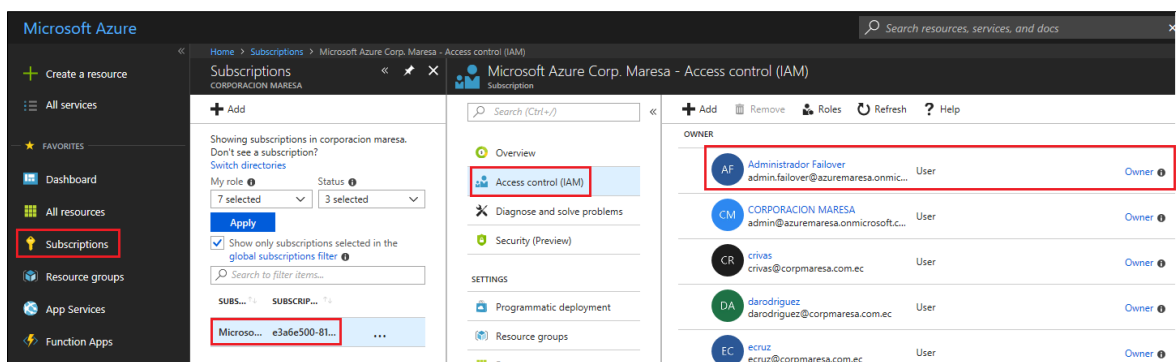
Las siguientes personas deben asumir la responsabilidad de restaurar los servicios de TI cuando se active el plan DR:

Contactos internos

Nombre	Función de trabajo	Datos de contacto	DR Process
Enrique Cruz	Jefe de Inteligencia y Seguridad Informática	ecruz@corpmaresa.com.ec 099 565 0144	Coordinador de Pruebas y ejecutar Failover Azure Site Recovery

El Rol de Administración que debe tener el usuario en la consola de Azure es de **Owner**, en caso de que el servicio de ADFS se encuentre caído se creó el usuario:

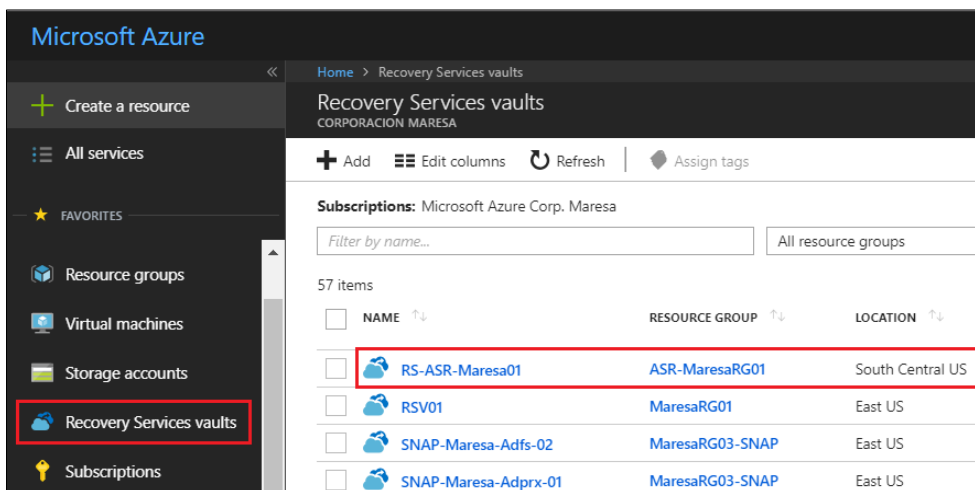
admin.failover@azuremaresa.onmicrosoft.com y la contraseña es **F@il0v3r** para iniciar sesión y ejecutar el proceso de Recuperación de Desastres.



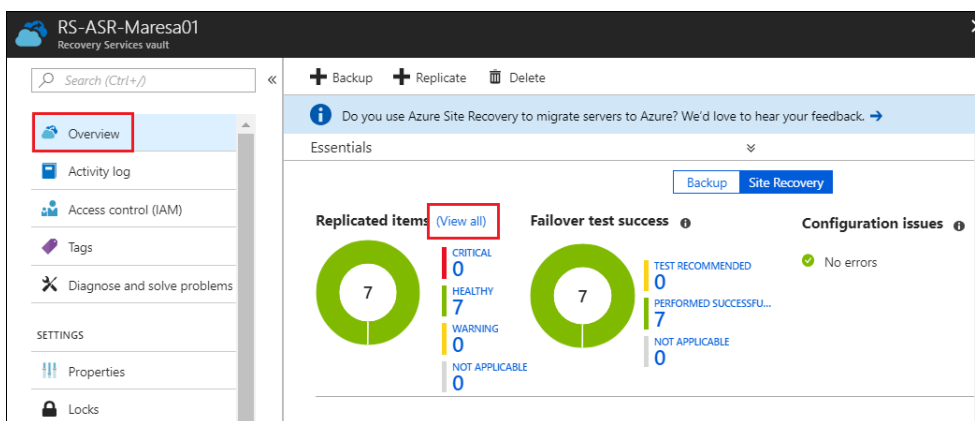
EJECUTAR TEST FAILOVER

Como se mencionó anteriormente, el proceso de Test Failover se ejecuta para validar que la replicación entre sitios sea correcta, el procedimiento a ejecutar es el siguiente:

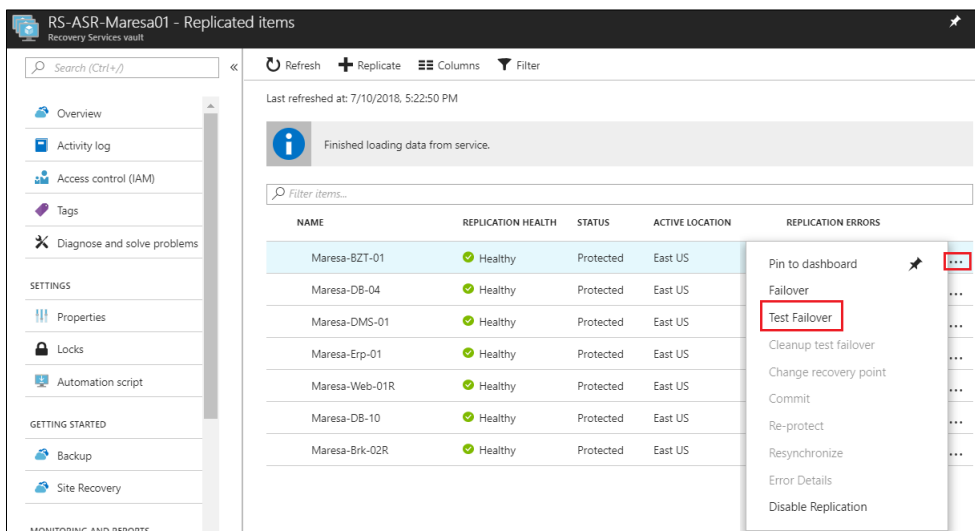
1. Iniciar sesión en el portal de Azure <https://portal.azure.com> con el usuario que tenga permisos de Administración.
2. Ir a **Recovery Services vaults** y seleccionar el baúl **RS- ASR-Maresa01**, éste contiene las 7 VMs que se están replicando.



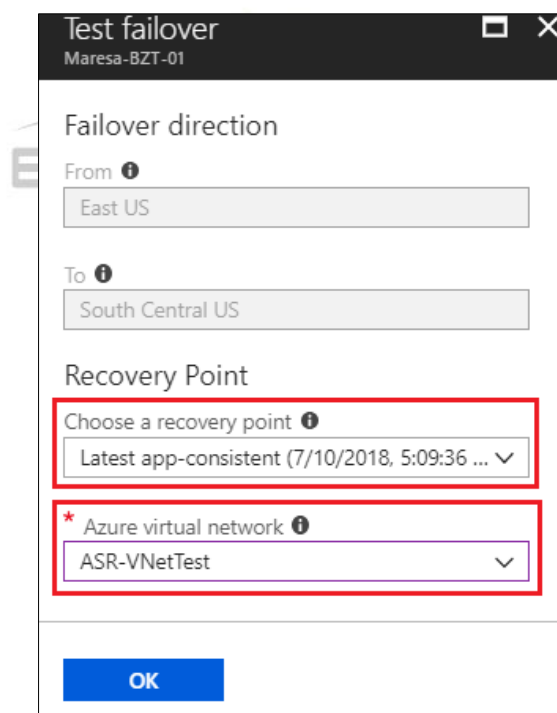
3. Se abrirá un pequeño dashboard donde se visualizará el status de la replicación. Dar clic en **View all** para que aparezcan todas las VMs.

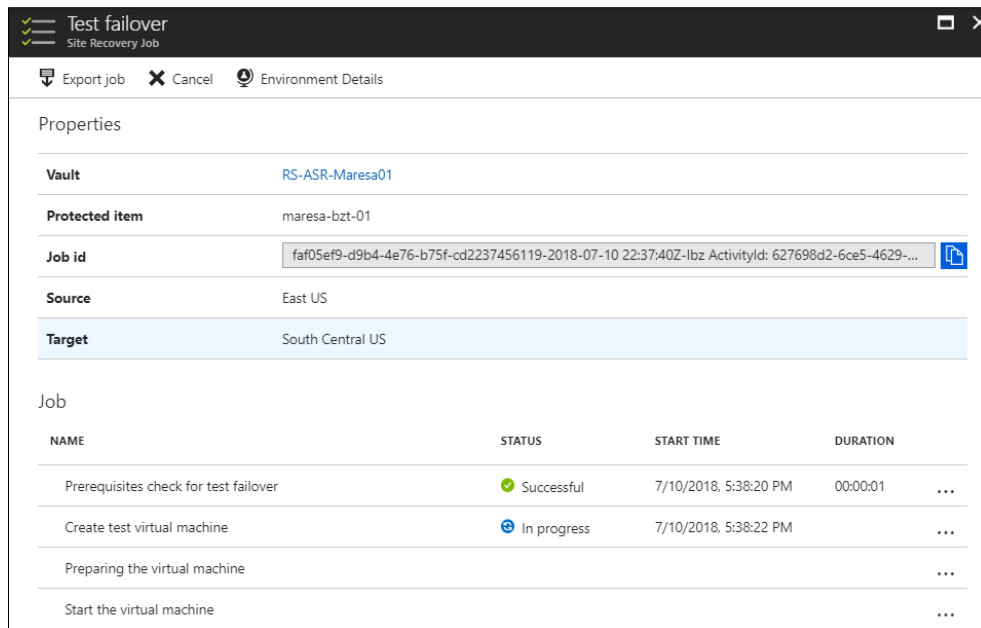


4. Dar clic sobre los tres puntos y seleccionar **Test Failover** sobre la máquina que se desea realizar la comprobación.



5. Se recomienda escoger como punto de recuperación la opción **Latest app-consistent** y seleccionar una **VNet** aislada del ambiente de producción. Clic en **OK** y el proceso de Test Failover empezará a crear la VM.





Test failover
Site Recovery Job

Export job Cancel Environment Details

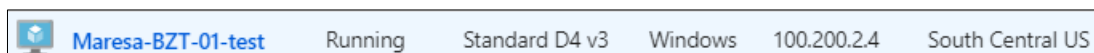
Properties

Vault	RS-ASR-Maresa01
Protected item	maresa-bzt-01
Job id	faf05ef9-d9b4-4e76-b75f-cd2237456119-2018-07-10 22:37:40Z-lbz ActivityId: 627698d2-6ce5-4629-...
Source	East US
Target	South Central US

Job

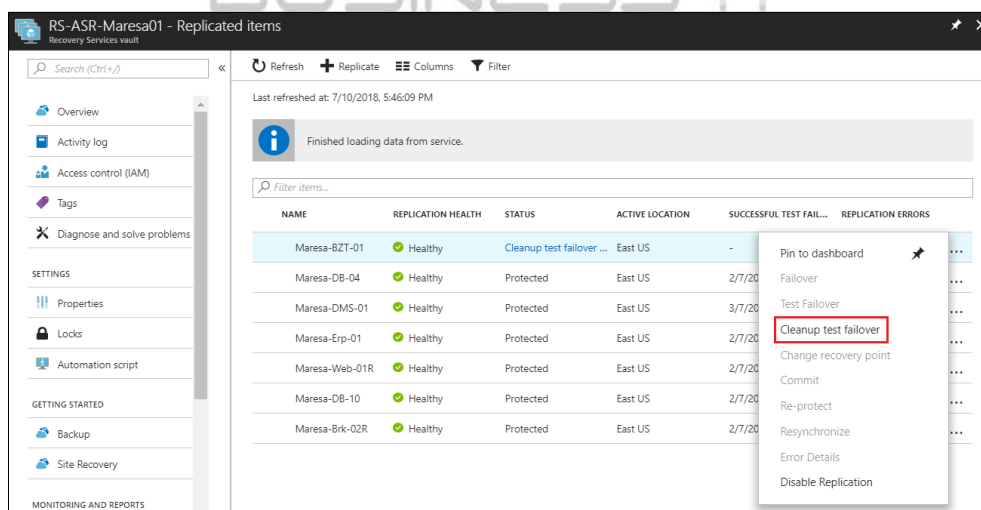
NAME	STATUS	START TIME	DURATION
Prerequisites check for test failover	Successful	7/10/2018, 5:38:20 PM	00:00:01
Create test virtual machine	In progress	7/10/2018, 5:38:22 PM	
Preparing the virtual machine			
Start the virtual machine			

6. La máquina siempre se creará con la abreviatura **Test** al final.



Maresa-BZT-01-test Running Standard D4 v3 Windows 100.200.2.4 South Central US

7. Verificar que toda la data se encuentre replicada, una vez realizada esta revisión, ir nuevamente al baúl, dar clic sobre los 3 puntos y seleccionar **Cleanup test failover**.



RS-ASR-Maresa01 - Replicated items

Search (Ctrl+/) Refresh Replicate Columns Filter

Last refreshed at: 7/10/2018, 5:46:09 PM

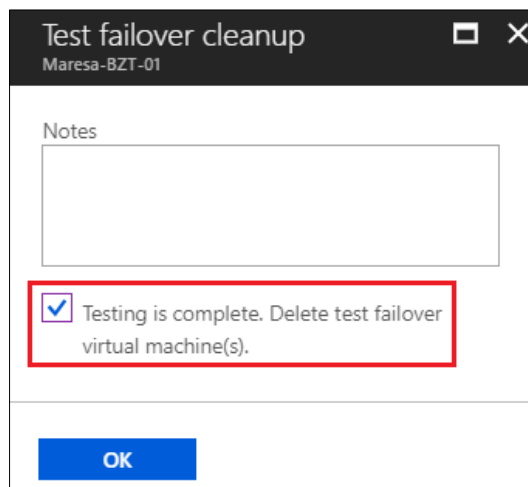
Finished loading data from service.

Filter items...

NAME	REPLICATION HEALTH	STATUS	ACTIVE LOCATION	SUCCESSFUL TEST FAIL...	REPLICATION ERRORS
Maresa-BZT-01	Healthy	Cleanup test failover ...	East US	-	
Maresa-DB-04	Healthy	Protected	East US	2/7/20	
Maresa-DMS-01	Healthy	Protected	East US	3/7/20	
Maresa-Erp-01	Healthy	Protected	East US	2/7/20	
Maresa-Web-01R	Healthy	Protected	East US	2/7/20	
Maresa-DB-10	Healthy	Protected	East US	2/7/20	
Maresa-Brk-02R	Healthy	Protected	East US	2/7/20	

Pin to dashboard
Failover
Test Failover
Cleanup test failover
Change recovery point
Commit
Re-protect
Resynchronize
Error Details
Disable Replication

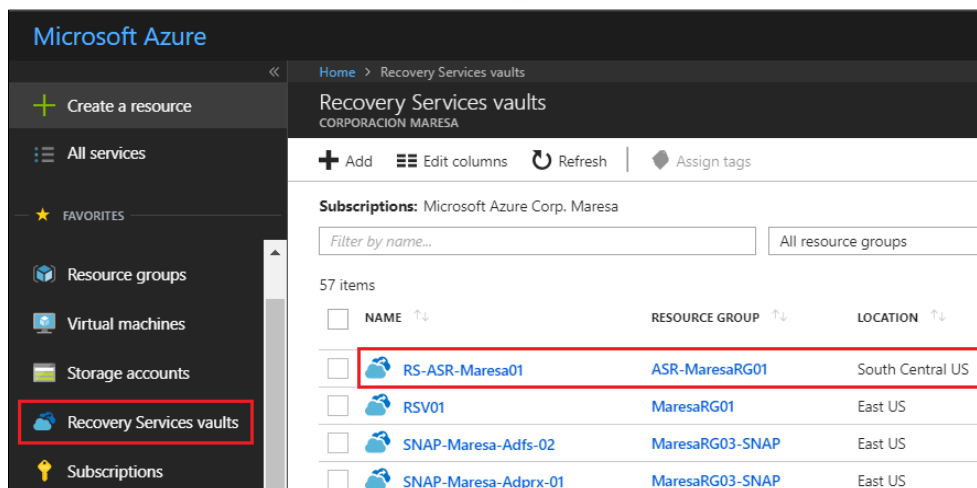
8. Marcar la casilla para eliminar la VM de test y dar clic en **OK** para finalizar el proceso de Test Failover.



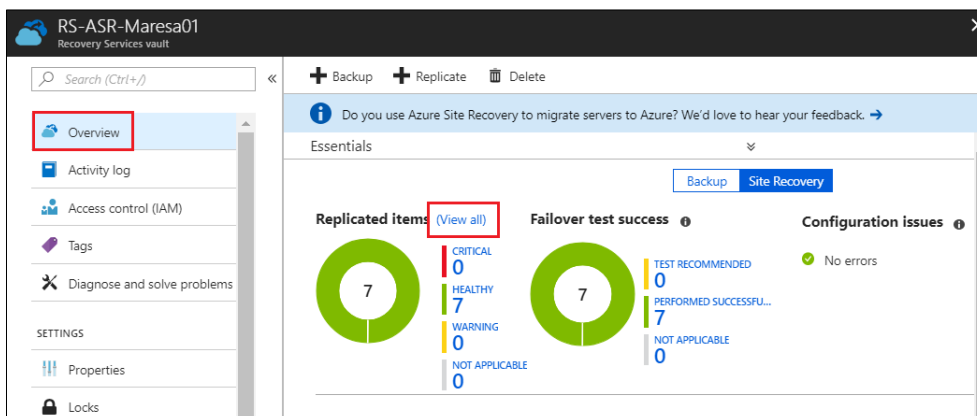
EJECUTAR FAILOVER

El proceso de Failover se ejecuta para habilitar el sitio de contingencia secundario, el mismo que pasará a ser el principal mientras se realizan las correcciones en el sitio primario. El procedimiento a ejecutar es el siguiente:

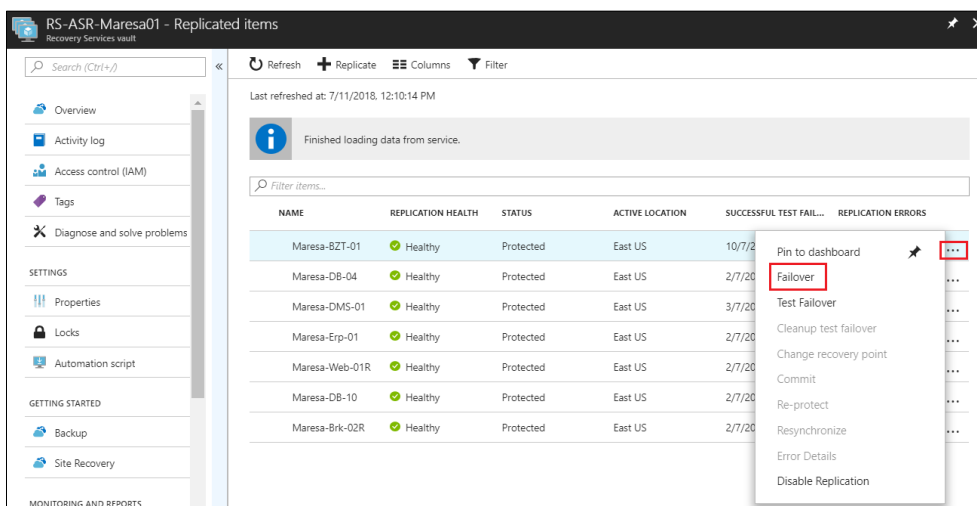
1. Iniciar sesión en el portal de Azure <https://portal.azure.com> con el usuario que tenga permisos de Administración.
2. Ir a **Recovery Services vaults** y seleccionar el baúl **RS- ASR-Maresa01**, éste contiene las 7 VMs que se están replicando.



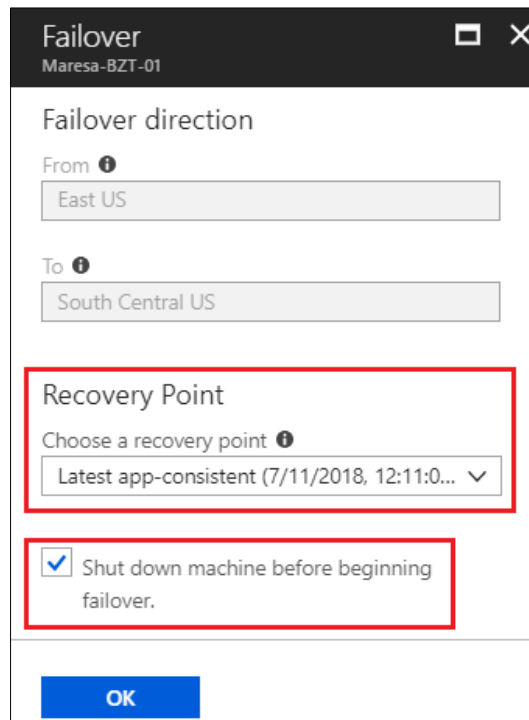
- Se abrirá un pequeño dashboard donde se visualizará el status de la replicación. Dar clic en **View all** para que aparezcan todas las VMs.



- Dar clic sobre los tres puntos y seleccionar **Failover** sobre la máquina que va a ser primaria.



- Se recomienda escoger como punto de recuperación la opción **Latest app-consistent**, marcar la casilla para que se apague la VM que está en producción y dar clic en **OK**.



Failover
Maresa-BZT-01

Failover direction

From ⓘ
East US

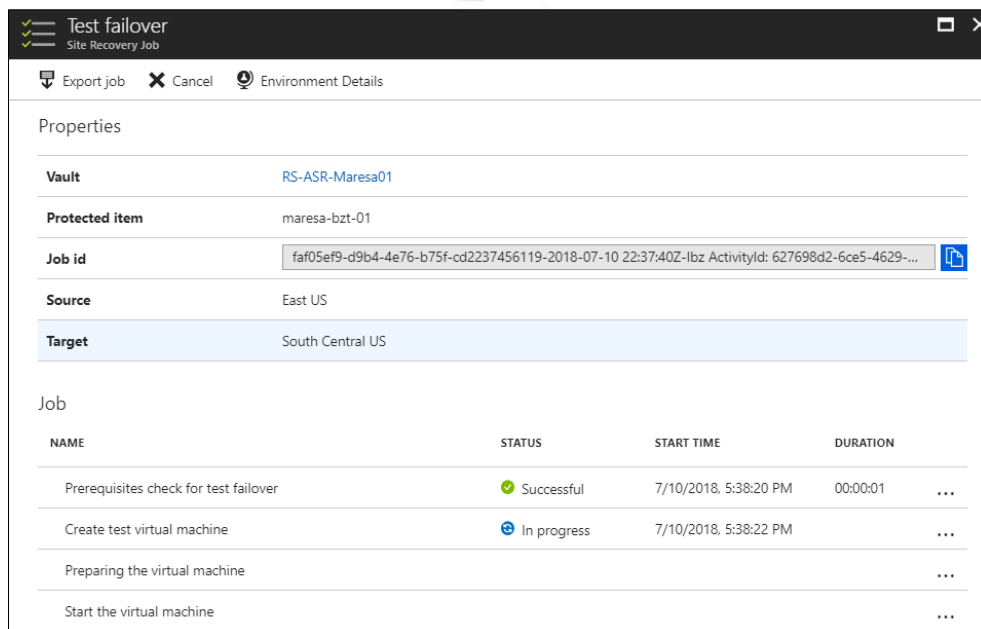
To ⓘ
South Central US

Recovery Point

Choose a recovery point ⓘ
Latest app-consistent (7/11/2018, 12:11:0... ▼

☒ Shut down machine before beginning failover.

OK



Test failover
Site Recovery Job

Export job Cancel Environment Details

Properties

Vault RS-ASR-Maresa01

Protected item maresa-bzt-01

Job id faf05ef9-d9b4-4e76-b75f-cd2237456119-2018-07-10 22:37:40Z-lbz ActivityId: 627698d2-6ce5-4629-...

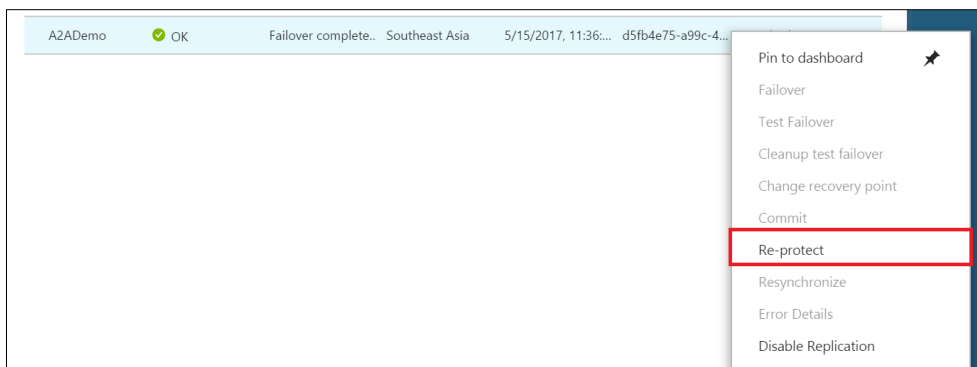
Source East US

Target South Central US

Job

NAME	STATUS	START TIME	DURATION
Prerequisites check for test failover	✓ Successful	7/10/2018, 5:38:20 PM	00:00:01 ...
Create test virtual machine	🔄 In progress	7/10/2018, 5:38:22 PM	...
Preparing the virtual machine			...
Start the virtual machine			...

- Al encenderse la VM de contingencia, ingresar y realizar un **ipconfig /registerdns**.
- Una vez que la el Failover haya finalizado, dar clic sobre los 3 puntos y seleccionar **Commit** para eliminar todos los puntos de recuperación disponibles con el servicio.
- En los elementos replicados, seleccionar la VM que se ejecutó el Failover y dar clic en **Re-protect**.



9. Revisar la información de grupos de recursos, redes, almacenamiento y disponibilidad. Cualquier recurso marcado (nuevo) se crea como parte de la operación de re-protección.
10. Dar clic en **OK** para activar la re-protección. Este trabajo genera el sitio objetivo con los últimos datos. Luego, replica los deltas a la región primaria. La VM ahora está en un estado protegido.

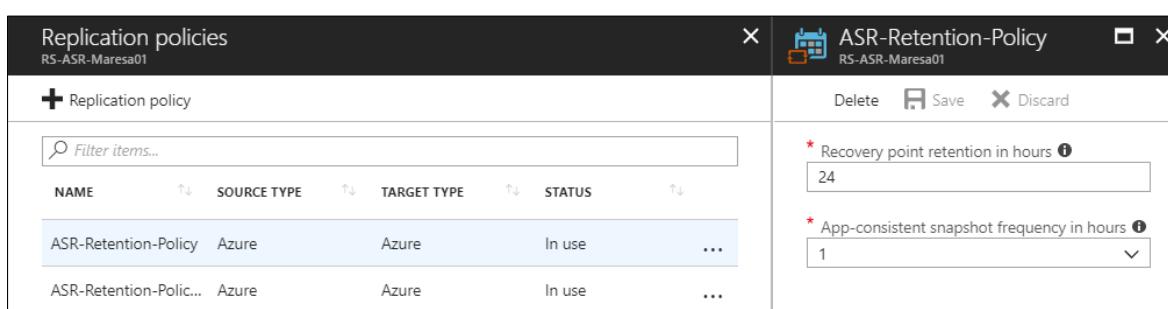


CONSIDERACIONES DE RPO Y RTO DE AZURE SOLUTIONS

RPO – Punto Objetivo de Recuperación

Este concepto se utiliza para definir el tiempo transcurrido desde la última replicación o punto de recuperación de datos, y el momento de la eventualidad de interrupción de servicio, y representa la potencial pérdida de datos en el plan de continuidad de negocio.

Las políticas de replicación para los servidores de Maresa se encuentran configurados con un tiempo de retención de 24 H y captura de Snapshots cada hora.



The screenshot shows two windows from the Azure portal. The left window, titled 'Replication policies', displays a table of policies. The right window, titled 'ASR-Retention-Policy', shows the configuration for a specific policy.

NAME	SOURCE TYPE	TARGET TYPE	STATUS
ASR-Retention-Policy	Azure	Azure	In use
ASR-Retention-Polic...	Azure	Azure	In use

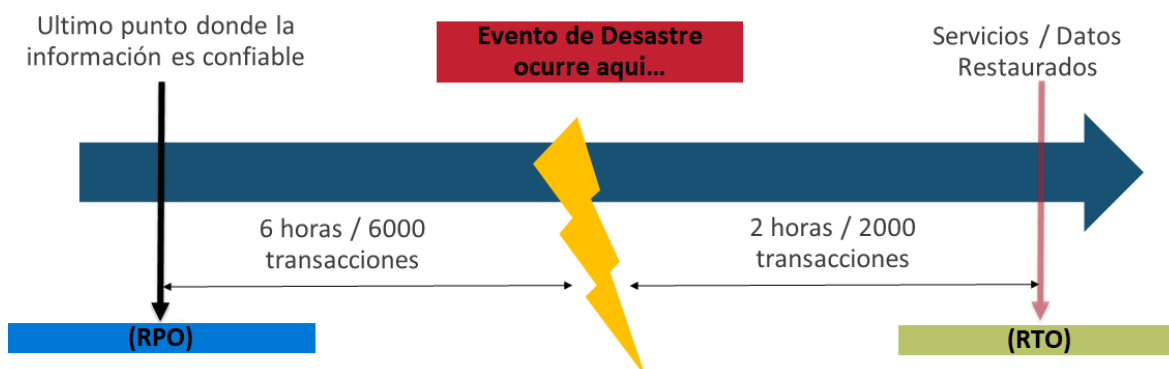
The 'ASR-Retention-Policy' configuration window shows the following settings:

- Recovery point retention in hours: 24
- App-consistent snapshot frequency in hours: 1

RTO – Tiempo Objetivo de Recuperación

Este concepto se utiliza para definir el tiempo transcurrido desde que ocurre la eventualidad de interrupción del servicio hasta que los sistemas están cien por ciento en operación para los usuarios finales.

En las pruebas realizadas con los servidores replicados de Maresa, el RTO es de aproximadamente 1 hora.



APROBACIÓN DEL DOCUMENTO

CORPORACIÓN MARESA

BIT

Enrique Cruz	Byron Rivas
Fecha: 01 de agosto de 2018	

Si este documento no ha sido revisado y aprobado por parte del personal asignado al proyecto de **CORPORACIÓN MARESA** dentro de 3 (tres) días después de enviado, automáticamente se dará por aprobado.

